Парадигма развития науки

Методологическое обеспечение

А.Е. Кононюк

ДИСКРЕТНО-НЕПРЕРЫВНАЯ МАТЕМАТИКА

Книга 4

Алгебры

(четкие и нечеткие)

Часть 1

Киев
Освіта України
2011


Структурная схема развивающейся панмедийной системы наук
I. Группа междисциплинарных наук
ПН Теория понятий
ЛГ Теория лингвистики
ПЗ Теория познания
СЗ Теория созидания
ПТ Общая теория понятоведения
II. Группа наук познания (фундаментальных наук)
ИН Теория информации
СТ Теория систем
РС Теория распознавания
КС Теория консалтинга (консультирования)
ПР Теория принятия решения
РР Теория реализации принятых решений
III. Группа наук созидания (прикладных наук)
СС Теория социальных систем
ЖО Теория жизнеобеспечения
КМ Теория коммуникаций и транспортирования
ОБ Теория образования (обучения)
СР Теория сохранения (защиты и охраны)
РЗ Теория развития
IV. Группа общедисциплинарных наук (обеспечивающих наук)
ДМ Теория дискретно-непрерывной математики (четкая и нечеткая)
НИ Теория научных исследований
ММ Теория моделей и моделирования
ОМ Теория оптимизации

УДК 51 (075.8)
ББК В161.я7
К 213

Рецензент: *Н.К.Печурин* - д-р техн. наук, проф. (Национальный авиационный университет).

Кононюк А.Е.
К65. Дискретно-непрерывная математика. Алгебры. К.4.Ч.1.
К.4:"Освіта України", 2011. - 452 с.
ISBN 978-966-7599-50-8

Многотомная работа содержит систематическое изложение математических дисциплин, исспользуемых при моделировании и исследованиях математических моделей систем.

В работе излагаются основы теории множеств, отношений, поверхностей, пространств, алгебраических систем, матриц, графов, математической логики, теории формальных грамматик и автоматов, теории алгоритмов, которые в совокупности образуют единную методолгически взамосвязанную математическую систему «Дискретно-непрерывная математика».

Для бакалавров, специалистов, магистров, аспирантов, докторантов и просто ученых и специалистов всех специальностей.

ББК В161.я7

ISBN 978-966-7599-50-8

Оглавление

Введение

Алгебра - раздел математики, которая изучает алгебраические системы. Понятие алгебра происходит от арабского аль джабр, аль габр. Алгебра возникла вследствие поиска общих методов решения сложных арифметических задач, которые выдвигались человеческой практикой. От арифметики отличается внедрением буквенной символики, которую используют при исследовании числовых систем, составлении и решении уравнений. Отдельные примеры решения алгебраических задач были уже у математиков Старинного Вавилона и Египта. Теорию уравнений развили древнегреческие математики, особенно Диофант. Высокого развития достигла алгебра в Китае в ранние и средние века. Значительный вклад в алгебра внесли среднеазиатские ученые. В 9 ст. после работ узбекского математика Г. Хорезме алгебра целиком отделилась от арифметики и геометрии. Тогда же были разработаны общие методы решения алгебраических уравнений 1 и 2-го степеней. В 16 ст. итальянским ученым удалось найти общие методы решения алгебраических уравнений 3 и 4-го степеней. С этих пор начинается бурное развитие алгебры в Европе. Уточняется и обобщается понятие числа, создается современная буквенная символика (Ф. Вьет, Р. Декарт). Возникновение в 17 ст. аналитической геометрии открыло возможности для широкого внедрения алгебраических методов в геометрию и привело к полному признанию отрицательных чисел. В нач. 19 ст. в связи с потребностью решать алгебраические уравнения были внедренные мнимые числа. На границе 18 и 19 ст. начинается деление алгебры на ряд самостоятельных разделов. Еще в 18 ст. от общей теории алгебраических уравнений отделилась теория системы уравнений 1-го степени, которая представляет предмет т.з. линейной алгебры. Значительных успехов достигла алгебра многочленов, которая изучает алгебраические уравнения высших степеней, в частности была доказана основная теорема алгебры. В нач. 19 ст. Н. Г. Абель и Э. Галуа установили факт неразрешимости в радикалах произвольных уравнений 5-го и высших степеней, что привело к созданию теории алгебраических чисел. Как доказано теорией Галуа, вопрос о решении алгебраических уравнений тесно связан с изучением полей алгебраических чисел и свойствами особых образований, т.н. групп подстановок. Эти группы представляют отдельный пример более общих групп преобразований (групп Ли), которые в конце 19 ст. начали широко применяться в геометрии и теории дифференциальных

уравнений. Значительный вклад в развитие алгебры внесли работы К.Ф. Гаусс. В 19 – в нач. 20 ст. заложены основы алгебраической геометрии. Развитие линейной алгебры привело к возникновению алгебры тензоров и алгебры теории инвариантов, а нач. 20 ст. стало основой для создания функционального анализа и общей теории векторных пространств. Со 2-й четверти 20 ст. основное место в алгебре занимает не алгебра многочленов и решение уравнений, а изучение абстрактных систем объектов с теми или другими операциями - абстрактная теория групп, колец, полей. В развитие современной алгебры выдающийся вклад внесли О. Г. Курош, А. И. Мальцев, О. Ю. Шмидт и др. В ряде областей алгебра, напр., в теории групп, в теории радикалов, занимает ведущее место в математике. Среди украинских ученых весомый вклад в развитие алгебры внесли Г.Ф. Вороной, С. Й. Шатуновський и Д. О. Граве, который воспитал известных алгебраистов М. Г. Чеботарьова, Б. М. Делоне и др. Ряд оригинальных работ по алгебре в 20 – в нач. 30-х гг. выполнил украинский математик М. П. Кравчук. Алгебраическую школу в области теории обобщенных групп создал в Харькове А. К. Сушкевич. С 1955 в Киев. университете восстановились алгебраические исследования в области абстрактной теории групп (Л. А. Калужнин) и теории топологических групп (В. Г. Глушков). В 1965 начались исследование по общим вопросам алгебры в Институте математики АН Украины (С. М. Черников) и в Киев. университете (В. С. Чарин и др.). Работа в области алгебры ведется и в ряде других научных центров Украины. Понятия и методы современной алгебры все шире используются во многих разделах математики и составляют одну из основ ее прогресса.

Переход от арифметических задач к алгебраическим находит свое выражение в том, что в задачах числовые данные заменяют буквенными. Обозначение чисел буквами отвлекает нас от специальных числовых данных, которые фигурируют в той или другой задаче, и приучает решать задачи в общем виде, т.е. для любых числовых значений величин, которые у нее входят.

Согласно этому, в начальных, важнейших, главах курса алгебры изучаются правила действий над буквенными выражениями, или, что то же самое, законы так называемых тождественных преобразований алгебраических выражений. Выясним это понятие.

Каждое алгебраическое выражение представляет собой совокупность букв, связанных между собой знаками алгебраических

действий; при этом для простоты мы будем рассматривать лишь действия сложение, вычитание и умножение. Содержание каждого алгебраического выражения заключается в следующему: если буквы, которые принимают участие в выражении, заменить числами, то выражение показывает, какие действия и в каком порядке необходимо выполнить над этими числами; иначе говоря, всякое алгебраическое выражение представляет собой некоторый, записанный в общем виде, алгоритм для обычного арифметического вычисления. Тождественное преобразование алгебраического выражения означает переход от одного выражения к другому, связанному с первым следующим соотношением: если мы в обеих выражениях каждой букве дадим совсем произвольное числовое значение с одним условием, чтобы та самая буква, которая входит в оба выражения, получила в обеих случаях то самое значение, и если после этого выполним указанные действия, то оба выражения дадут один и тотже числовой результат. Тождественное преобразование записывается в виде равенства двух алгебраических выражений; равенства эти справедливы при любой замене входящих в них букв числами (как указано выше). Равенства этого вида называются, как известно, тождествами. Например:

$$a-a = 0, \qquad (1)$$

$$(a+b)c = ac + bc. \qquad (2)$$

Всякое тождество выражает некоторое свойство входящих в него действий. Так, например, тождество (1) говорит нам, что вычитая из какого-нибудь числа это самое число, мы всегда получим олин и тот же результат, а именно нуль. Тождество (2) утверждает следующее свойство действий сложения и умножения: произведение суммы двух чисел на третье число равно сумме произведения каждого из слагаемых на это третье число.

Тождеств существует бесконечно много. Однако можно установить небольшое число основных тождеств, подобных вышеизложенным, так, что любое тождество является следствием из этих основных тождеств.

Всякое алгебраическое вычисление, т.е. всякое как угодно сложное тождественное преобразование одного алгебраического выражения в другое, является, таким образом, комбинацией небольшого числа основных или элементарных тождественных преобразований, которые излагаются в элементарной алгебре под названием правил раскрытия скобок, правил знаков и т.п. Выполняя эти комбинации элементарных преобразований, обычно, даже забывают о том, что каждая буква в алгебраическом выражении есть только символ, знак, который обозначает некоторое число: вычисление, как говорят, делают

механически, забывая о реальном содержании выполняемого в каждый момент преобразования, а заботясь лишь о соблюдении правил этих преобразований. Так делают, по обыкновению, и опытные математики и начинающие ученики. Однако в последнем случае иногда, к сожалению, бывает, что это реальное содержание выполненных преобразований вообще выскальзывает с сознания.

В механическом осуществлении алгебраических операций есть и другая, более серьезная сторона. Она заключается в том, что под буквами, которые входят в алгебраическое выражение, во многих случаях можно понимать не число, а разнообразные другие объекты математического исследования: не только над числами, но и над другими объектами — примеры этому мы увидим — можно делать действия, которые имеют ряд общих основных свойств с алгебраическими действиями, и которые поэтому естественно назвать сложением, умножением и т.д. Например, силы в механике не являются числами: они являются векторами, т.е. величинами, которые имеют не только числовое значение, но и направление. Тем временем силы можно складывать, и это сложение имеет основные свойства обычного алгебраического сложения чисел. Это приводит к тому, что над силами можно делать вычисление по правилам алгебры. Таким образом, могущество алгебраических преобразований идет намного дальше, чем запись в общей форме действий над числами: *алгебра учит вычислениям с любыми объектами, для которых определены действия, которые удовлетворяют основным алгебраическим аксиомам.*

Модуль 1.
Введение в алгебры

Микромодуль 1.
Основные понятия арифметики

1.1. Операции и их свойства

Определение. *Операцией над множеством* S называется функция f: $S^n \to S$, $n \in$ N.

В этом определении есть два важных момента, которые заслуживают особого вспоминания. Во-первых, раз операция является функцией, то результат применения операции *однозначно определен.* Поэтому данный упорядоченный набор из n элементов S функция f переводит только в один элемент S. Во-вторых, поскольку область значений операции лежит в S, на которое операция действует, будем говорить, что операция *замкнута* на S,

Говорят, что операция $S^n \to S$ *имеет порядок г.* Ограничимся рассмотрением ситуаций, когда порядок равен 1 или 2. В этом случае операции называют *монадическими* (или *унарными)* и *диадическими* (или *бинарными)* соответственно. Элементы набора из n элементов в области определения называют ***операндами***. Операции обычно обозначают символами, которые называют ***операторами***. В случае унарных операций обычно символ оператора ставят перед операндом.

Наиболее простым примером является операция изменения знака на R. В предположении, что операция сложения уже определена, $-x$ определяет операцию $x \square$ y: $x+y=0$ (x отображается в y: $x+y=0$).

Определение. Бинарные операции обозначают одним из трех способов. В первом случае оператор ставится между операндами *(infix),* во второму — перед операндами *(prefix)* и в третьему — после операндов *(postfix).*

Пример 1.

$a+b$ *infix,*
$+ab$ *prefix,*
$ab+$ *postfix.*

Переход от одной формы к другой нетруден и лучше всего описывается в терминах ориентированных графов, которые будут обсуждаться в дальнейших модулях,

Согласно большинству математических текстов, кроме некоторых работ по алгебре и формальной логике, мы будем использовать обозначение *infix*. Другие обозначения имеют то преимущество, что не требуют скобок при определении порядка вычислений сложных выражений, и это делает их особенно удобными для автоматической обработки. Можно проверить соответствие между следующими парами выражений, которые записаны в формах *infix* и *postfix* соответственно:

а) $a+b\bullet\ c+(d+e\bullet\ (f+g),$

$abc\bullet\ +\ defg+\bullet\ ++;$

б) $(a+b)\bullet\ c+d+e\bullet\ f+g,$

$ab+c\bullet\ d+ef\bullet\ +g+;$

в) $a+(b\bullet\ (c+d)+e)\bullet\ f+g,$

$abed+\ e+f\ +g+.$

Пример 2. Рассмотрим алгебраическое выражение

$$a + b \bullet c + (d + e \bullet (f + g))$$

и его представление на рис. 1.1, корое называют деревом.

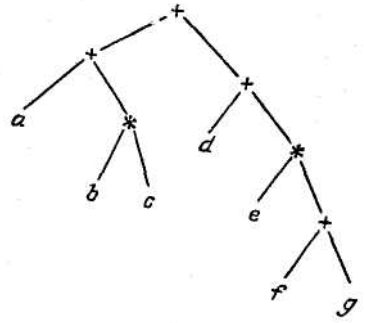


Рис. 1.1

Из свойств арифметических операций мы знаем, что значение этого выражения можно вычислить многими способами. Однако если двигаться слева направо и снизу вверх, то получаем

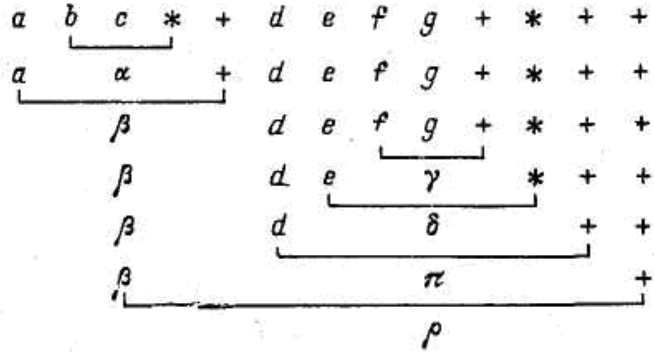
$$\alpha \leftarrow b \bullet c,\ \ \beta \leftarrow a + \alpha,\ \ \gamma \leftarrow f + g,$$

$$\delta \leftarrow e \bullet \gamma,\ \ \pi \leftarrow d + \delta,\ \ \rho \leftarrow \beta + \pi.$$

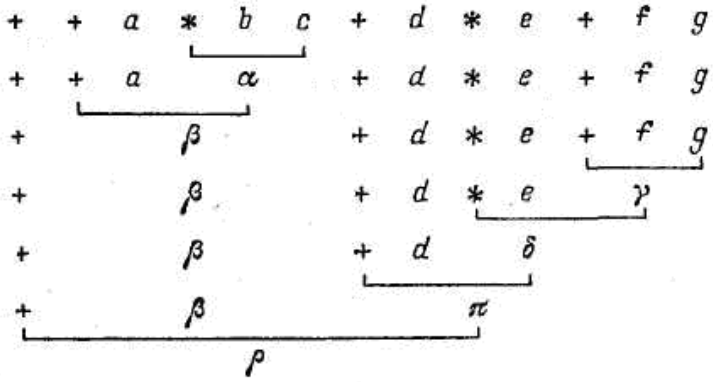
Здесь греческими буквами обозначаются промежуточные результаты, за исключением ρ - искомого результата.

Вычисление значения этого выражения с помощью дерева выполняется очень просто, однако если работать непосредственно с исходным выражением, то это можно сделать по-иному. Действительно, обычно *(infix)* выражение, как это показано в примере, нерегулярно потому, что некоторые подвыражения заключены в скобки, а некоторые нет. Особенно такая ситуация будет наблюдаться в том случае, если проинтегровать информацию о различных символах на дереве (поскольку на самом деле его нет). Очевидно, что формы записи *prefix* и *postfix* этого выражения несут больше информации.

Вычисление значения выражения в форме *postfix* осуществляется следующим образом:



Аналогично в форме *prefix* вычисления осуществляются следующим образом:



«Переходы» по дереву показаны на рис. 1.2, *a* (форма *prefix),* на рис. 1.2,*b* (форма *postfix)* и на рис. 1.2, *c* (форма *infix)* со скобками:

((a + (b• c)) + (d + (e• (g + g)))).

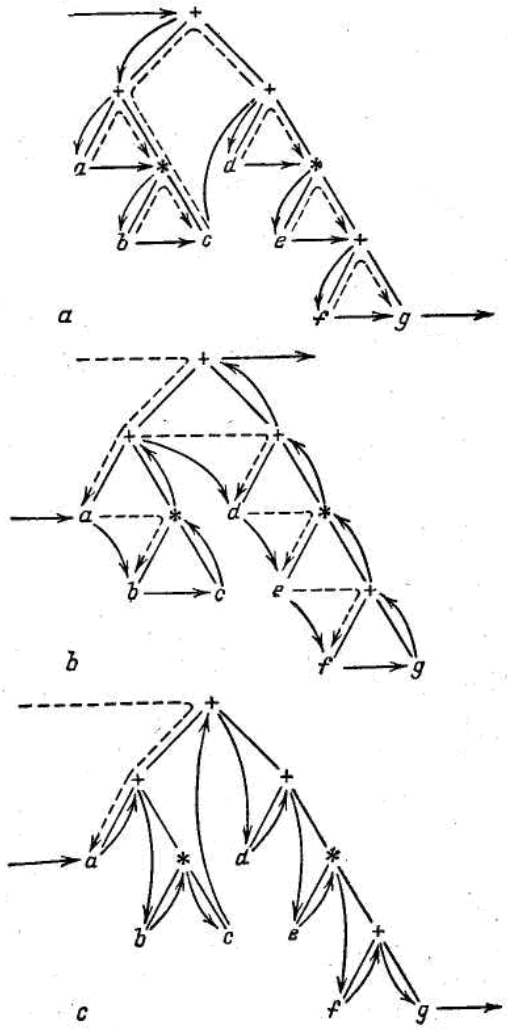


Рис. 1.2

К этим вопросам мы возвратим позднее.

Мы уже знакомые со многими бинарными операциями, например с арифметическими операциями +, •, —, / и операциями над множествами — объединением ($\square$) и пересечение (I).

Операции, которые определены на конечных множествах, часто удобнее задавать при помощи таблиц.

Пример 3. Пусть операция $\otimes$ определена на множестве $\{a, b, c\}$ при помощи таблицы

$\otimes$	a b c
a	a a b
b	b a c
c	a b b

Следовательно,

$$a \otimes b = a,$$
$$b \otimes b = a,$$
$$c \otimes b = b, \text{ и т.д.}$$

Такие символы, как $\otimes$ и $\oplus$, будут использоваться для обозначения различных операций, которые будут вводиться в процессе изложения материала.

Очевидно, что использование таблиц имеет важное значение, так как некоторые операции, с которыми приходится иметь дело в дискретной математике, непригодны для словесного задання.

Обратим теперь внимание на свойства операций. Операции вместе со своими следствиями обеспечивают основу всех алгебраических вопросов математики, так как они определяют порядок работы с объектами.

Определение. Говорят, что бинарная операция $\otimes$ на множестве A *коммутативна,* если

$$a \otimes b = b \otimes a \quad \text{для всех} \quad a, b \in A.$$

Следовательно, обычная операция сложения на Z коммутативна, а вычитание — нет.

Определение. Говорят, что операция $\otimes$ на множестве A *ассоциативна,* если

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \quad \text{для всех} \quad a,b,c \in A.$$

Заметим, что в определении ассоциативности порядок операндов a, b и c сохранен (операция может быть некоммутативной!) и

использованы круглые скобки, чтобы определить порядок вычислений.

Таким образом, выражение $(a \otimes b) \otimes c$ требует, чтобы сначала вычислялось $a \otimes b$ и результат этого (скажем, x) участвовал в операции с c, т.е. давал $x \otimes c$. Если операция ассоциативна, то порядок вычислений несуществен и, следовательно, скобки не нужны.

Пример 4. Над Z имеем

$$(1+2)+3 = 1+2+3 = 1+(2+3),$$

но

$$(1-2)-3 = -4 \text{ и } 1-(2-3) = 2.$$

Таким образом, операция вычитания не ассоциативна.

Комутативность и ассоциативность являются двумя важнейшими свойствами, которые могут быть определены для простых операций. Перед тем как описывать свойства, которые связывают две операции, определим некоторые термины, относящиеся к специальным элементам множеств, к которым эти операции применяются.

Определение. Пусть $\otimes$ — бинарная операция на множестве A и $l \in A$ такая, что

$$l \otimes a = a \text{ для всех } a \in A.$$

Тогда l называется *левой единицей* по отношению к $\otimes$ на A. Аналогично, если существует $r \in A$ такое, что

$$r \otimes a = a \text{ для всех } a \in A,$$

то r является *правой единицей* по отношению к $\otimes$. Далее, если существует элемент e, который является и левой и правой единицей, т.е.

$$e \otimes a = a \otimes e = a \text{ для всех } a \in A,$$

то e называется *(двусторонней) единицей* по отношению к $\otimes$.

Пример 5. Над R 0 является правой единицей по отношению к вычитанию и единицей по отношению к сложению, так как

$$a - 0 = a,$$

но

$$0 - a \neq a, \text{ если } a \neq 0;$$
$$a + 0 = a \text{ и } 0 + a = a \text{ для всех } a.$$

Определение. Пусть $\otimes$ — операция на A с единицей e и $x \otimes y = c$. Тогда говорят, что x — *левый обратный* элемент к y, а y — *правый обратный* элемент к x. Далее, если x и y такие, что

$$x \otimes y = e = y \otimes x,$$

это y называется *обратным элементом* к x по отношению к $\otimes$, и наоборот.

Замечание. В некоторых работах левые (правые) обратные элементы относят к левой (правой) единице, однако, как мы в скором времени увидим, в большинстве случаев единицы являются двусторонними и, следовательно, не требуется делать никаких различий. Для решения уравнений необходимо существование и единственность единиц и обратных элементов. Менее общим свойством операций является идемпотентность, хотя оно используется в алгебре логики.

Определение. Пусть операция $\otimes$ на множестве A и произвольный элемент $x \in A$ таковы, что $x \otimes x = x$. Тогда говорят, что x *идемпотентен* по отношению к $\otimes$.

Очевидно, что любое подмножество идемпотентно по отношению к операциям пересечения и объединения.

Определение. Пусть дано множество A, на котором определено две операции $\otimes$ и $\oplus$. Тогда, если

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

для всех $a,b,c \in A$, то говорят, что $\otimes$ *дистрибутивна* по отношению к $\oplus$.

Если сказанное выше не совсем понятно, следует провести соответствие между этим тождеством и обычной арифметикой на R, например,

$$3*(1 + 2) = (3*1)+(3*2).$$

Наиболее общеизвестная алгебра может быть построена из относительно небольшого набора основных правил. Сейчас мы продемонстрируем, как из элементарных предположений можно извлечь некоторые простые следствия; большинство примеров даны в виде упражнений.

Пример 6. Пусть $\otimes$ — операция на множестве A и существует единица по отношению к $\otimes$. Тогда единичный элемент единствен.

Доказательство. Предположим, что x и y — единицы по отношению к $\otimes$, т.е.

$$x \otimes a = a \otimes x = a,$$

$$y \otimes a = a \otimes y = a \quad \text{для всех } a \in A.$$

Тогда $x = x \otimes y$, так как y — единица, и $x \otimes y = y$, поскольку x — единица. Следовательно, $x = y$.

Пример 7. Пусть $\otimes$ — ассоциативная операция на множестве A и e — единица по отношению к $\otimes$. Тогда если $a \in A$ и x имеет обратный элемент, то обратный элемент едининствен по отношению к $\otimes$.

Доказательство. Предположим, что x' и x'' - обратные элементы к x, так что

$$x \otimes x' = x' \otimes x = e \text{ и } x \otimes x'' = x'' \otimes x = e.$$

Тогда

$$x' = x' \otimes e = x' \otimes (x \otimes x'') = (x' \otimes x) \otimes x'' = e \otimes x'' = x''.$$

Итак, мы определили операции и описали некоторые их свойства. Теперь посмотрим, что можно сделать с совокупностью операций, заданных на множестве.

Множество с заданными на ней операциями называют ***алгебраической структурой***

Некоторые из алгебраических структур, которые наиболее часто встречаются, будут рассмотрены позднее. Прежде чем приступить к их рассмотрению, посмотрим на арифметику с неформальной точки зрения. В большинстве случаев мы будем опускать формальные определения, делая ударения на «следствия из правил», даже в тех случаях, когда это приводит к непривычным способам использования известных символов, которые обычно используются для представления десятичных чисел,

1.2. «Малая» конечная арифметика

Арифметику *можно рассматривать как* ***множество с двумя операциями****, которые действуют подобно* ***сложению и умножению.***

Ее можно изучать многими способами. Чтобы уяснить требования ***арифметической системы***, примем конструктивное приближение и рассмотрим целые числа (0, 1, 2, ..,) просто как символы. В дальнейшем будем рассматривать только конечную арифметику, в которой используется лишь конечное множество чисел; сначала это множество будет небольшим. Имеется в виду, что если $A \sim N_m$, то требуется m различных символов, при этом никакие комбинации символов не разрешаются. Если используются только десятичные числа, то $m \leq 10$. Поскольку все множества данного размера биективны, то можно рассматривать только множества N_m.

Для большей наглядности рассмотрим множество N_6. Для этого необходимо построить таблицы умножения и сложения. Множество N_6

достаточно велико для того, чтобы изучать свойства основной структуры. Можно подумать, что для этой цели более уместным является множество N_2, однако это не так. Начнем со сложения.

Операция сложения имеет единицу, которая обычно обозначается символом 0, однако $0 \notin N_6$. Поэтому будем использовать множество $Z_6 = \{0, 1, 2, 3, 4, 5\}$, которое более удобно. Очевидно, что $Z_6 \sim N_6$. Поэтому можно работать с Z_6, не теряя никаких свойств. Таким образом, мы можем построить соответствующую табл. 1.1.

Таблица 1.1

+	0 1 2 3 4 5
0	0 1 2 3 4 5
1	1
2	2
3	3
4	4
5	5

Так как операция коммутативна, то таблица должна быть симметричной. Труднее отстоит дело с ассоциативностью. Если мы хотим, чтобы операция была ассоциативной, и требуем, как обычно, существование обратных элементов по сложению, то любой элемент должен входить ровно один раз в каждую строку и каждый столбец. Объясним это высказывание.

Если $a + b = a + c$, то

$$-a+(a + b)=- a + (a + c),$$
$$(-a + a)+ b = (-a + a) + c,$$
$$0 + b = 0 + c,$$
$$b=c.$$

Рассмотрим теперь операцию, определенную в табл. 1.2.

Таблица. 1.2

A	0 1 2 3 4 5 B	0 1 2 3 4 5 C	0 1 2 3 4 5
0	0 1 2 3 4 5 0	0 1 2 3 4 5 0	0 1 2 3 4 5
1	1 2 0 4 5 3 1	1 1 2 3 4 5 1	1 5 3 4 2 0
2	2 0 1 5 3 4 2	2 2 2 3 4 5 2	2 3 1 5 0 4
3	3 5 4 0 2 1 3	3 3 3 3 4 5 3	3 4 5 0 1 2
4	4 3 5 1 0 2 4	4 4 4 4 4 5 4	4 2 0 1 5 3
5	5 4 3 2 1 0 5	5 5 5 5 5 5 5	5 0 4 2 3 1

Из трех возможностей для операции сложения на Z_6 только *C* удовлетворяет всем условиям, что выглядит несколько необычно.

Операция *A* не коммутативна, а в *B* нарушен критерий «едининственности результата». Как же построить соответствующую операцию, удовлетворяющую всем обсуждаемым выше свойствам? Из дальнейшего изложения будет видно, что наиболее трудно обеспечить выполнение свойства ассоциативности. В предложенной ниже процедуре мы используем ассоциативность как основной шаг построения, и, следовательно, это свойство будет выполняться автоматически.

Шаг 1. Число 0 является единицей для операции сложения. Поэтому получаем табл. 1.3.

Таблица 1.3

+	0 1 2 3 4 5
0	0 1 2 3 4 5
1	1
2	2
3	3
4	4
5	5

Шаг 2. Определим следующую строку таблицы, удовлетворяющую условию «единственности результата». Чтобы подчеркнуть используемую технику, специально выберем результат, который отличается от привычного. Возьмем

+	0 1 2 3 4 5
1	1 3 0 5 2 4

Так как операция должна быть коммутативной, заполним соответствующий столбец табл. 1.4.

Таблица 1.4

+	0 1 2 3 4 5
0	0 1 2 3 4 5
1	1 3 0 5 2 4
2	2 0
3	3 5
4	4 2
5	5 4

Шаг 3. Заполним другие клетки таблицы, используя ассоциативность. Проследим подробно за каждой деталью:

$2 + 2 = 2 + (1 + 4) = (2 + 1)+4 = 0 + 4 = 4,$

$2 + 3 = 2 + (1 + 1) = (2+1)+1 = 0+1 = 1,$

$2 + 4 = (2+1) + 5 = 0 + 5 = 5,$

$2 + 5=(2 + 1)+3 = 0 + 3 = 3.$

Здесь мы использовали соотношение 2+1 = 0 и 0 + *x*= *x*. Далее

$$3 + 3=(1 + 1) + 3 = 1 + (1 + 3)=1 + 5 = 4 \text{ и т.д.}$$

Таким образом, на основе значений 1+*x* получаем таблицу для операции + (табл. 1.5).

Таблица 1.5

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	3	0	5	2	4
2	2	0	4	1	5	3
3	3	5	1	4	0	2
4	4	2	5	0	3	1
5	5	4	3	2	1	0

При выполнении процесса надо учитывать дополнительные ограничения на шаге 2. Значения в нулевой строке должны выбираться так, чтобы они «продолжали» все Z_6. Например, начиная с 1 (как мы делали), получаем

$$1 + 1 = 3, \quad 3+1 = 5, \quad 5+1 = 4, \quad 4+1 = 2, \; 2 + 1 = 0, \quad 0+1 = 1.$$

Следовательно, прибавляя только 1, можно получить все Z_6.

Перейдем теперь к умножению. Сначала заметим, что единица для операции умножения должна отличаться от нуля. В противном случае для любых *x* и *y* мы имели бы

$$x = 0*x = x*0, \quad y = 0 + y = y + 0,$$

поэтому

$$x*y = x*(0 + y) = (x* 0) + (x* y) = x + (x*y),$$

а значит, *x*= 0. Поэтому 0 не является единицей для умножения.

На самом деле нам требуется число, которое будет порождать Z_6. Следовательно, мы могли бы определить аналогичным образом операцию умножения на основе частной табл. 1.6.

Таблица 1.6

*	0	1	2	3	4	5
0		0				
1	0	1	2	3	4	5
2		2				
3		3				
4		4				
5		5				

Однако в этом случае мы не должны тредовать выполнения критерия «единственности результата». (В обычной арифметике не существует целого числа, которое при умножении на 2 давало бы 1! Поэтому в конечном множестве могут быть повторения.)

Вместо того чтобы повторять процедуру построения таблицы для умножения, вернемся к проблеме связи двух операций - дистрибутивности умножения относительно сложения. Эта проблема связана с ассоциативностью. Рассмотрим (уже построенную) операцию сложения.

Заметим, что 1+1= 3. Поэтому из предположения дистрибутивности получаем, что

3*0-(1 + 1)*0=(1*0) + (1*0)=0 + 0=0,
3*2 = (1*2) + (1*2) = 2 + 2 = 4,
3*3 = (1*3) + (1*3)=3 + 3 = 4,
3*4 = (1*4) + (1*4)=4 + 4=3,
3*5=(1*5) + (1*5)=5 + 5 = 0.

Теперь 3 + 3 = 4, 3+1 = 5, 1 + 4 = 2 и 1 + 2 = 0. Действуя как и ранее, получаем следующую операцию (табл. 1.7).

Таблица 1.7

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	1	4	3	5
3	0	3	4	4	3	0
4	0	4	3	3	4	0
5	0	5	5	0	0	5

Следовательно, начиная с почти произвольного выбора строки в таблице, не содержащей 1 по сложению, и накладывая ряд простых ограничений, мы приходим к приемлемой арифметической системе. Теперь достаточно установить, что полученная система не находится в противоречии с высказанными ранее соображениями, т.е., что 1+1 действительно существует. Короче говоря, если в нормальной (бесконечной) арифметике $a+b=c$ и $c \in Z_6$, то хотелось бы, чтобы и в нашей арифметике ответ был c. Следовательно, мы пришли к выбору

+	0	1	2	3	4	5
1	1	2	3	4	5	?

Недостающим элементом должен быть 0, поскольку $6 \notin Z_6$, и 0 является единственным элементом Z_6, которого нет в строке. В результате такого выбора получаем соответствующую табл. 1.8.

Таблица 1.8

+	0 1 2 3 4 5	*	0 1 2 3 4 5
0	0 1 2 3 4 5	0	0 0 0 0 0 0
1	1 2 3 4 5 0	1	0 1 2 3 4 5
2	2 3 4 5 0 1	2	0 2 4 0 2 4
3	3 4 5 0 1 2	3	0 3 0 3 0 3
4	4 5 0 1 2 3	4	0 4 2 0 4 2
5	5 0 1 2 3 4	5	0 5 4 3 2 1

Она определяет так называемую арифметику по модулю (основанию) 6. (Эта арифметика работает точно так же, как и обычная целочисленная арифметика, за исключением того, что все целые числа заменяют на остатки от деления их на 6.)

1.3. «Большая» конечная арифметика

Мы уже построили арифметику для Z_6. Возникает вопрос: как можно расширить эту систему, чтобы иметь возможность считать после 5? Для этого достаточно иметь множество *n*-значных чисел (наборов из *n* элементов из Z_6) с арифметикой над Z_6. Чтобы проиллюстрировать это, рассмотрим упорядоченную тройку из Z_6, т.е. элементы множества $Z_6 \times Z_6 \times Z_6$. Если Z_6 упорядочено обычным способом, т.е. $0<1<2<3<4<5$, тогда определим порядок на $Z_6 \times Z_6 \times Z_6$ по правилу

$$(a,b,c) < (x, y, z),$$

если $a<x$ или $a = x$ и $b < y$ или $a= x$, $b=y$ и $c< z$.

В этом случае элементы $Z^3_6 = Z_6 \times Z_6 \times Z_6$ будут упорядочены следующим образом:

(0,0,0), (0,0, 1), ... (0,0, 5),
(0,1,0),..., (0,1,5),
……
(0,5,0),....., (0,5,5),
(1,0,0),..., (1,0,5),
(5,5,0),..., (5,5,5).

Таким образом, существует $6^3 = 216$ различных троек. Поэтому нужно уметь делать арифметические вычисления над Z^3_6 в пределах от 0 до 215. В приведенном выше упорядочивании элементов из Z^3_6

(0, 0, 5) непосредственно предшествует (0, 1, 0).
(0, 1, 5) непосредственно предшествует (0, 2, 0),
.....
(0, 5, 5) непосредственно предшествует (1, 0, 0).

Следовательно, хотелось бы, чтобы выполнялось соотношение

$$(0, 0, 5)+1=(0, 1,0).$$

Однако до сих пор не было представления 1 в Z^3_6. И хотя это соотношение выглядит естественным, мы должны заботится о том, чтобы не использовать ни одного не определенного понятия. Для облегчения описания представим Z^3_6 как $A_2 \times A_1 \times A_0$ и рассмотрим сумму $(a_2, a_1 a_0)$ и (b_2, b_1, b_0). Покомпонентное сложение дает $(a_2+b_2, a_1+b_1, a_0+b_0)$, где сложение осуществляется в Z_6, и пока, как кажется, этого достаточно.

Пример.1. Рассмотрим соотношение

$$(0, 1,3)+ (4, 2, 1) = (4, 3, 4),$$

которое будет более наглядным, если записать его в виде

0, 1, 3
+
4, 2, 1
= 4, 3, 4

Однако

1, 2, 5 и 0, 0, 5
\+ +
2, 3, 1 0, 0, 1 (=1?)
=3, 5, 0 =0, 0, 0 (=0?).

В результате операции сложение множество A_0 переходит в себя. Однако для того чтобы сумма достаточно больших чисел (таких, как 5+1) могла бы выйти за пределы A_0, нам необходимо производить некоторые действия в A_1 и также, возможно, в A_2. (Это иллюстрируется табл. 1.9).

Таблица 1.9

$+_s$	0 1 2 3 4 5	$+_c$	0 1 2 3 4 5
0	0 1 2 3 4 5	0	0 0 0 0 0 0
1	1 2 3 4 5 0	1	0 0 0 0 0 1
2	2 3 4 5 0 1	2	0 0 0 0 1 1
3	3 4 5 0 1 2	3	0 0 0 1 1 1
4	4 5 0 1 2 3	4	0 0 1 1 1 1
5	5 0 1 2 3 4	5	0 1 1 1 1 1

Возьмем любые два числа a и b с Z_6. Тогда их сумма (в Z) составляет

$$6*(a +_c b) + (a +_s b).$$

Пример 2. 4 плюс 4 дает 6*(1) + (2) = 8 в Z.

Таблица $+_s$ дает «обычную» сумму двух элементов из Z_6, в то время как таблица $+_c$ показывает, когда необходим «переход» в следующее множество Z_6, и содержит только нули и единицы. Значения в $+_c$ ограничены, так как если

$$0 \le x < n \quad \text{и} \quad 0 \le y < n,$$

то

$$0 \le x \le x + y < x + n < n + n = 2n \text{ (и } n = 6 \text{ в } Z_6).\ ,$$

В действительности можно получить лучшую оценку, поскольку

$$0 \le x \le n\text{-}1 \quad \text{и} \quad 0 \le y \le n\text{-}1,$$

и, следовательно,

$$0 \le x + y \le 2n\text{-}2 < 2n - 1.$$

Возвращаясь к сложению (a_2, a_1, a_0) и (b_2, b_1, b_0) и обозначая ответ через (d_2, d_1, d_0), получим -

$$\begin{aligned}
&d_0 = a_0 +_s b_0,\\
&x_0 = a_0 +_c b_0,\\
&d_1 = a_1 +_s b_1 +_s x_0,\\
&x_1 = \text{если } a_1 +_c b_1 = 1 \text{ тогда } 1,\\
&\qquad \text{иначе } (a_1 +_s b_1) +_c x_0,\\
&d_2 = a_2 +_s b_1 +_s x_1,\\
&x_2 = \text{если } a_2 +_s b_2 = 1 \text{ тогда } 1,\\
&\qquad \text{иначе } (a_2 +_s b_2) +_c x_1.
\end{aligned}$$

Поскольку $0 \le a_i + b_i < 2n - 1$ и $x_i = 0$ или $x_i = 1$, то переносимый результат из $a_i + b_i + x_{i-1}$ никогда не может быть больше 1.

Заметим, что в наших определениях числа (0, 0, 0) и (0, 0, 1) в Z^3_6 действуют, как 0 и 1 в новой арифметике. Кроме этого, если x_2=5, то результат сложения может оказаться слишком большим для Z^3_6. В этом случае говорят, что состоялось «переполнение». Этот случай мы обсудим более подробно в п.1.4, а до конца этого пункта возможность переполнения будем игнорировать,

Аналогично можно использовать операции $*_p$ и $*_c$ (таблицы произведения и переноса), заданные в табл. 1.10 для того, чтобы производить умножение над Z^3_6, однако мы не будем этим заниматься.

Таблица 1.10

$*_p$	0 0 1 2 3 4 5	$*_c$	0 0 1 2 3 4 5
0	0 0 0 0 0 0 0	0	0 0 0 0 0 0 0
1	0 1 2 3 4 5	1	0 0 0 0 0 0 0
2	0 2 4 0 2 4	2	0 0 0 1 1 1
3	0 3 0 3 0 3	3	0 0 1 1 2 2
4	0 4 2 0 4 2	4	0 0 1 2 2 3
5	0 5 4 3 2 1	5	0 0 1 2 3 4

До сих пор мы рассматривали только символы, которые имеют вид положительных чисел. Конечно, с символами 0, 1, 2, ... можно обращаться «естественным» образом, и, следовательно, их можно интерпретировать как неотрицательные числа. Арифметика над Z^3_6 оперирует с числами от 0 = (0, 0, 0) до 215 = (5, 5, 5), которые были получены из последовательности (от 0 до 5) в Z_6. Если взять множество {—3, —2, —1, 0, 1, 2} вместо Z_6, то получим систему, которая содержит отрицательные числа, но ведет себя странным образом.

Если мы возьмем два множества Z_6 и множество {—3, —2, —1, 0, 1, 2}, которое назовем $\bar{Z}_6$, и образуем множество $\bar{Z}_6 \times Z_6 \times Z_6$, то можно построить арифметику с числами от —108 до 107. На самом деле арифметика является той же самой, за исключением того, что значение 3, 4 и 5 в A_2 сейчас интерпретируются як —3, —2, —1 соответственно. Поэтому, например, (-2, 4, 2) исчисляется в Z как

$$(-2*36) + (4*6)+2 = -46.$$

Биекция между двумя системами, определенная следующим образом:

3-3 □ ,
4-2 a ,
5-1 a ,
x a *x* в других случаях,

может быть применена в любой момент при условии, что результат вычислений не имеет цифр 3, 4 или 5 в A_2. Мы выбираем обозначения из соображения удобства, не вводя ограничений на случаи, когда можно применять биекцию или обратное отображение. На этом этапе мы советуем игнорировать любые очевидные противоречия, которые относятся к переполнению A_2. Этот случай будет подробно рассмотрено в следующих пунктах на более простом примере. Отметим, что новая система «переходит» от положительных чисел к отрицательным. Например,

$$(2, 2, 5) + (1, 0, 1) = \begin{cases} (3, \quad 0, 0) & \textit{в старой системе} \\ (-3, 0, 0) & \textit{в новой системе} \end{cases}$$

(В Z это дает 107 + 1 = -108!)

Вычисления, которые включают у себя сложение и вычитание, в новой арифметике довольно просты и зависят от двух тождеств. Первое имеет вид

(5,5, 5) + (0, 0, 1) = (0,0,0)

((5, 5, 5) эквивалентно (-1, 5, 5)), а вторая - вид

$(a_2, a_1, a_0) + (b_2, b_2, b_0) = (5,5, 5)$.

Они имеют место тогда и только тогда, когда

$$a_2 + b_2 = 5, \quad a_1 + b_1 = 5, \quad a_0 + b_0 = 5.$$

Таким образом, чтобы вычислить обратное по сложению число к (a_2, a_1, a_0), мы должны сначала найти число (b_2, b_1, b_0), которое называют *дополнением по* 5, и затем прибавить 1=(0, 0, 1). Это даст дополнение до 6. Проиллюстрируем этот процесс на следующем примере.

Пример 3. Найдем обратные элементы к (-3, 4, 1) и (3, 4, 1).

Из 3, 4, 1

получаем 2, 1, 4 (дополнение к 5)

\+ 1

2, 1, 5 (дополнение к 6)

Проверим результат 3, 4, 1

\+

2, 1, 5

= 0, 0, 0

Поэтому - (-3, 4, 1) = (2, 1, 5).

Таким образом, вычисление сводится к сложению с соответствующим дополнением.

Пример 4. Вычислим (1, 3, 4) -(2, 1, 5).

Берем 2, 1, 5

получаем 3, 4, 0 (дополнение к 5)

результат 3, 4, 1 (дополнение к 6)

прибавим (1, 3, 4) (1, 3, 4)

5, 1, 5=(-1, 1, 5).

Проверяя вычисление над Z, получаем 58—83=—25. Конечно, причиной образования так называемых дополнений к 5 и 6 является тот факт, что мы проводим вычисления над N_6 (или Z_6).

В общем случае, если вычисление производится в N_m, мы должны использовать дополнение к m—1 и m соответственно.

Надо подчеркнуть, что в вычислениях на ЭВМ мы обычно имеем дело с Z^n_m для некоторых фиксированных m и n и очень редко — с множеством Z. Таким образом, совокупность имеющихся в нашем распоряжении чисел всегда ограничена, и, хотя границы могут быть очень большими, мы не должны забывать о том, что они существуют. Риск тем более велик по той причине, что в записи обычно опускают комы и все нули, которые стоят слева от первой ненулевой цифры за исключением числа (0, 0, 0). Следовательно (1, 3, 4) запишется как 134, (0, 0, 6) как 6 и (0, 0, 0) как 0.

1.4. Двоичная арифметика

Из уже построенных арифметик над Z^n_m и Z^{n-}_m легко выделить основы двоичной арифметики. Существуют две так называемые двоичные арифметики. Первая — это *знаковая* и *модульная форма,* которая определена на {—, +}×Z^n_2, т.е. Z^n_2 (определенное в предыдущем пункте) с добавленным знаком, который расширяет элементы Z^n_2. Знак обычно кодируют в бинарной форме: 0 для «+» и 1 для «-».

Вторая арифметика *(двоичная арифметика дополнений)* — это Z^{n-}_2 с элементами {0, 1} во всех n позициях. Этот вид двоичной арифметики используется в большинстве компьютеров. Поэтому ограничим наши рассмотрения Z^{n-}_2. Чтобы сделать обсуждение более конкретным, рассмотрим Z^{5-}_2 , элементы которого лежат в пределах от 10 000 (=-16) до 01 111 (=+15) (т.е. содержит $32=2^5$ разных чисел). Число —1 представляется в Z^{5-}_2 как 11 111. Поэтому легко найти двоичное дополнение. Для этого надо слегка изменить все двоичные цифры, которые называоть *битами,* чтобы получить дополнение к 1, а затем прибавить 1, чтобы получить дополнение к 2.

Пример 1.

— (01 011)
10 100
+
1
10 101
(=$-2^4 + 2^2 + 2^0$ = -ll);
-(10110)
+01 001
1
01 010
(=$2^3 + 2^1$= 10).

Очевидно, что могут возникнуть проблемы, вызванные ограниченностью чисел. Мы не можем их избежать, однако следует знать, когда возможна «ошибка». Форма дополнения делает проверку условия переполнения относительно легкой, использующей только значение старшего значащего бита. (В Z^{5}_{-2} это бит с номером 2^4.) Этот бит обозначает знак представляемого числа и называется знаковым битом или знаковым разрядом. Перед тем как проверить, какое значение имеет знаковый бит, напомним, что прибавление 1 к максимальному положительному числу в Z^{n}_{-m} дает максимальное отрицательное число (наибольшее отрицательное число — это отрицательное число, которое отстоит дальше всего от нуля). Другими словами, числа повторяются циклическим образом. В Z^{5}_{-2} мы имеем ситуацию, которая изображена на рис. 1.3.

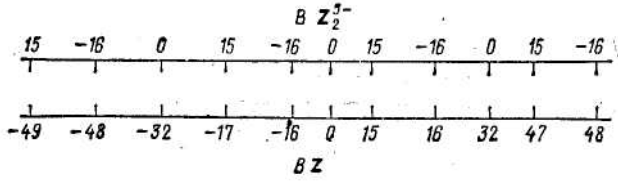


Рис. 1.3.

Что же произойдет, если мы сложим два числа x и y, где

$$-a \le x < a \text{ и } -a \le y < a \quad (\text{в } Z^{5}_{-2},\ a = 16)?$$

Сумма $x + y$ будет ограничена:

$$2a \le x + y \le 2a - 2 < 2a - 1.$$

Само по себе это неравенство ничего не дает. Поэтому мы рассмотрим три случая;

(I) если $-a \le x < 0$ и $-a \le y < 0$
тогда $-2a \le x + y < 0$;

(II) если $0 \le x < a$ и $0 \le y < a$
тогда $0 \le x + y \le 2a - 2 < 2a - 1$;

(III) если $-a \le x < 0$ и $0 \le y < a$
тогда $-a \le x + y < a$.

Вначале заметим, что результат в случае (III) находится в требуемых границах и, следовательно, всегда правильный. Чтобы понять, как могут возникать ошибки в случаях (I) и (П), необходимо вспомнить, что если $z \in Z$ и $-2a \le z < -a$, то число z представимо в конечной арифметике числом z', где $z' = z + 2a$ и $0 \le z' < a$. Аналогично, если $a \le z < 2a - 1$, то z представимо z", где $z'' = z - 2a$ и $-a \le z'' < 0$.

Следовательно, ответ будет неправильный, если он в случае (I) положительный или в случае (II) отрицательный.

Чтобы объяснить эти заключения в терминах свойств знакового разряда, рассмотрим различные возможности сложения двух чисел:

а) оба числа отрицательны;

б) оба числа положительны;

в) числа имеют различные знаки.

Анализируя эти случаи, видим, что *переполнение* (ошибка переполнения) встречается тогда и только тогда, когда существует перенос в знаковый разряд или перенос из знакового разряда, *но не оба вместе.* Для иллюстрации этого рассмотрим несколько примеров в Z^{5-}_{2}. Попытаемся сопоставить эти примеры со случаями (I)-(III) и а) - в), рассмотренными выше.

Пример 2. Напомним, что вычисление проводятся в Z^{5-}_{2}:

```
  1 0 1 0 1        1 1 1 0 0
+ 1 1 0 1 0      + 1 0 1 1 1
-----------      -----------
1 0 1 1 1 1      1 1 0 0 1 1
  ↑ |              ↑ |↑ |

  1 1 1 0 1        0 0 1 0 1
+ 0 0 1 1 0      + 0 0 1 1 1
-----------      -----------
1 0 0 0 1 1        0 1 1 0 0

    0 1 1 0 0
  + 0 1 0 1 0
  -----------
    1 0 1 1 0.
```

Вернемся теперь к умножению и делению. Сначала рассмотрим умножение. Напомним, что в Z (или, более точно, в Z^{n}_{10} для достаточно большого n) умножение на 10 можно получить «сдвигом» всех цифр на одну позицию влево и записью в 0-й позиции цифры 0. (В Z^{n}_{m} умножение на m также всегда можно осуществить сдвигом влево.)

Следовательно, мы имеем простой способ умножения на неотрицательные степени числа 2 в Z^{n}_{2} — сдвиг каждой цифры слева на соответствующее число позиций.

Пример 3. (Вычисление проводятся в Z^{5-}_{2}.)

```
0 0 0 11   (3)        111 1 0   (-2)
0 0 110    (*2)       111 0 0   (*2)
0 1 100    (*2=12)    110 0 0   (*2 = -8)
             0 0 1 0 1   (5)
             0 1 0 1 0   (*2)
             1 0 1 0 0   (*2)
             0 1 0 0 0   (*2 = 8).
```

Из этих примеров видно, что метод также хорошо работает для отрицательных чисел, но результат будет с ошибкой (переполнение), если на каждом этапе менялся знак и если потом он опять изменился. Для умножения произвольного целого числа (элемента N) используем свойство дистрибутивности умножения по отношению к сложению и представим множитель как сумму степеней числа 2.

Пример 4. (Вычисление проводятся в $Z^{5-}{}_2$).

$$3*5 = 3*2^2 + 3*2^0(2^0=1)$$
$$(-5)*3 = (-5)*2^1 + (-5)*2^0.$$

Поэтому

```
 0 0 0 1 1          1 1 0 1 1
+                  +
 0 1 1 0 0          1 0 1 1 0
 0 1 1 1 1         1 1 0 0 0 1  .
```

Точно так же, как умножение производилось сдвигами влево деление на положительные степени числа 2 осуществляется сдвигом вправо. (Деление на другие целые числа должно получаться путем сведения к вычитанию степеней числа 2. Этот процесс мы обсуждать не будем.) Однако специального рассмотрения требуют отрицательные числа. Отметим также, что в общем случае ожидаемый результат (т.е. арифметически ожидаемый результат в R) будет не целым, а дробным.

Пример 5. Попытаемся в $Z^{5-}{}_2$ вычислить 12/4, (—6)/2 и 7/4 сдвигом на 2, 1 и 2 позиции соответственно. Имеем

```
 0 1 1 0 0      (12)          1 1 0 1 0     (-6),
 0 0 0 1 1| 0 0  (3 = 12/4)   0 1 1 0 1|0   (13 ≠-6/2)
0 0 1 1 1 |      (7)
0 0 0 0 1 | 1 1  (1≈7/4).
```

Сдвиг на одну позицию вправо автоматически переводит любое отрицательное число к положительному. В $Z^{5-}{}_2$ сдвиг переводит —16 к +8. Чтобы исправить это, следует отнять от результата число 16, что даст -8 (т.е. -16/2). То же самое можно получить, устанавливая знаковый разряд равным 1. Следовательно, правильный результат достигается использованием знакового разряда, значение которого равно 0 или 1 (в зависимости от знака числа), для того чтобы заполнить «пропуска», создаваемые в результате сдвига вправо.

Следовательно, (-6)/2 приводит к

$$11101 = -3.$$

Действие битов (со значением 1), «выпадающих» из числа в результате сдвига вправо, должно усекать результат. Поэтому 7/4 дает 1. Существует общепринятая практика округлять число (вверх независимо от знака) прибавлением к числу утерянного последнего

бита. Это отвечает обычному арифметическому правилу округления, поскольку 1 в первом бите остатка представляет собой 0.5. Следовательно, 7/4 дает 2.

1.5. Логическая арифметика

Строго говоря, булева арифметика оперирует на множествах Z_2 и Z^n_2 и, следовательно, включает только числа 0 и 1. Для того чтобы подчеркнуть такую структуру, начнем с рассмотрения логической арифметики на «относительно большом» множестве Z_5. Она дает основу многозначной логики. Отсюда легко получить более простой случай Z_2. Возьмем множество $Z_5 = (0, 1, 2, 3, 4\}$ и операции $\vee$ и $\wedge$, которые определены в табл. 1.11.

Таблица 1.11

$\vee$	0 1 2 3 4	$\wedge$	0 1 2 3 4
0	0 1 2 3 4	0	0 0 0 0 0
1	1 1 2 3 4	1	0 1 1 1 1
2	2 2 2 3 4	2	0 1 2 2 2
3	3 3 3 3 4	3	0 1 2 3 3
4	4 4 4 4 4	4	0 1 2 3 4

Упорядочивая Z_5 обычным образом (порядок индуцируется Z и R), видим, что

$$a \vee b = \max \{a, b\},$$
$$a \wedge b = \min \{a, b\}.$$

Обе операции коммутативны и ассоциативны, 0 является единицей для $\vee$, а 4 является единицей для $\wedge$; $\wedge$ дистрибутивна по отношению к $\vee$, но не наоборот.

Пример 1. Возьмем множество Z_m с естественным порядком элементов. Введем операции $\wedge$ и $\vee$. Рассмотрим шесть возможных случаев упорядочивания трех произвольных элементов *a, b, c* с Z_m:

(I) $a \le b \le c$;
(II) $a \le c \le b$;
(III) $b \le a \le c$;
(IV) $b \le c \le a$;
(V) $c \le a \le b$;
(VI) $c \le b \le a$.

Использование символа $\le$ является интуитивным, однако может быть обосновано с помощью следующего определения:

$a \le b$ тогда и только тогда, когда $a \vee b = b$.

Для проверки условия дистрибутивности нужно показать, что

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Это можно сделать проверкой того, что обе части выражения совпадают для каждого из наборов a, b и c. Будем одновременно вычислять и сопоставлять соответствующие выражения:

(I) $a \wedge (b \vee c) = a \wedge c = a$,
$(a \wedge b) \vee (a \wedge c) = a \vee a = a$;

(II) $a \wedge (b \vee c) = a \vee b = a$,
$(a \wedge b) \vee (a \wedge c) = a \vee a = a$;

(III) $a \wedge (b \vee c) = a \wedge c = a$,
$(a \wedge b) \vee (a \wedge c) = b \vee a = a$;

(IV) $a \wedge (b \vee c) = a \wedge c = c$,
$(a \wedge b) \vee (a \wedge c) = b \vee c = c$;

(V) $a \wedge (b \vee c) = a \wedge b = a$,
$(a \wedge b) \vee (a \wedge c) = a \vee c = a$;

(VI) $a \wedge (b \vee c) = a \wedge b = b$,
$(a \wedge b) \vee (a \wedge c) = b \vee c = b$.

Следовательно, $\wedge$ дистрибутивна по отношению к $\vee$.

Можно также показать, что $\vee$ дистрибутивна по отношению к $\wedge$, т.е. что

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Проверку этого свойства оставляем как упражнение.

Перед тем как закончить обсуждение общего случая, давайте возвратимся к табл. 1.11, определяющим $\vee$ и $\wedge$. Элементы, которые имеют одинаковые значения в таблицах, расположены относительно единичных элементов так, как показано на рис. 1.4.

Рис. 1.4.

На самом деле каждая из этих операций является «отображением» другой и связь, которая позволяет одну операцию менять на другую, определяется (в Z_5) парами (0, 4), (1, 3), (2, 2), (3, 1), (4, 0). В сущности, это принцип двойственности, который будет обсуждаться в следующих разделах. Возвращаясь к Z_2, имеем

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

В Z_2 операцию $\vee$ обычно интерпретируют как ***или*** (результат равен 1, если один из операндов равен 1, включая случай, когда они оба равны 1). Аналогично $\wedge$ читается как ***и***. Число 0 является единичным элементом по отношению к ***или***, число 1 является единичным элементом по отношению к ***и***. Можно распространить эти результаты на более высокие размерности (переходя от Z_2 к Z^n_2), расширяя компоненты и учитывая то, что не существует переноса из одной копии Z_2 к другой.

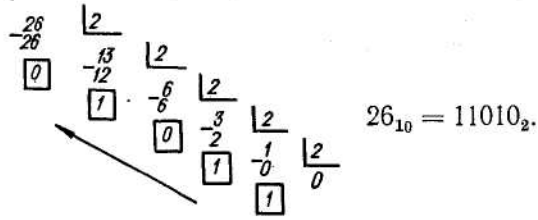
Пример 2.

$$\begin{array}{r} 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \\ \wedge \\ \underline{0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1} \\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1. \end{array}$$

Микромодуль 1.
Примеры решения задач

Рассмотрим пример перевода целых десятичних чисел в двоичные.

Перевод целых десятичних чисел в двоичнные выполняется последовательным делением исходного числа и каждого частного на два. Получаемые при этом остатки (0 или 1), записанные в обратном порядке, и дают представление десятичного числа в двоичной системе счисления. Например:

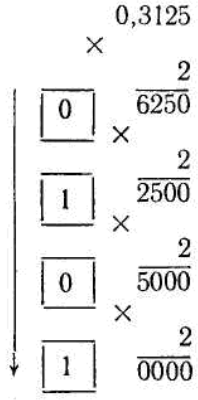


$26_{10} = 11010_2.$

Действительно, проверяя полученный результат, получаем

$1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 16 + 8 + 2 = 26.$

Дробное число переводится в двоичную систему счисления методом последовательного умножения на два. При этом каждый раз после запятой двоичного числа записывается 0 или 1 соответственно целой части результата умножения. Последовательное умножение продолжается до тех пор, пока дробная часть не обратится в нуль или пока не получим требуемое количество двоичных знаков после запятой. Например, двоичное представление числа 0,3125 получается следующим образом:



$0{,}3125_{10} = 0{,}0101_2.$

Проверка полученного результата дает:

$$0 \cdot 2^{-1} + 1 \cdot 2^{-2} + 0 \cdot 2^{-3} + 1 \cdot 2^{-4} = (1/4) + (1/16) = 5/16 = 0{,}3125.$$

Если число является смешанным, т.е. его целая и дробная части отличны от нуля, то оно переводится в двоичную систему раздельно: целая часть - последовательным делением, а дробная - последовательным умножением.

Арифметические операции над числами сводятся к операциям сложения и умножение одноразрядных чисел. В двоичной системе счисления умножения задается таблицей конъюнкции: 0•0=0; 1•0=0; 0 •1 = 0 и 1•1 = 1. Сложение выполняется по правилу: 0 + 0 = 0; 1+0= 1; 0+1=1 и 1+1=10 (10 - это двоичное число, соответствующее десятичному числу 2). Операции над двоичными числами выполняются по правилам, аналогичным для десятичных чисел, но эти правила предельно упрощаются (особенно для умножения). Например, десятичные операции 41+27=68 и 41 5=205 выглядят следующим образом:

$$\begin{array}{r} 101001 \\ +\ 11011 \\ \hline 1000100 \end{array} \qquad \begin{array}{r} 101001 \\ \times\ \ 101 \\ \hline 101001 \\ +\ 101001 \\ \hline 11001101 \end{array}.$$

Как видно, умножение двоичних чисел сводится к сложению чисел, образованных сдвигом влево первого сомножителя. Поразрядное сложение осуществляется в соответствии с таблицей

x_1	x_2	
	0	1
0	0	1
1	1	0

,

причем в случае $x_1 = x_2 = 1$ образуется единица переноса в старший разряд.

Операция, задаваемая этой таблицей, называется *сложением по модулю 2*. Если при сложении перенос не учитывается, то эта операция вместе с операцией умножения определяет на множестве двоичных чисел *арифметику по модулю 2*.

Микромодуль 1.
Индивидуальные тестовые задачи

1. Рассмотреть указанные ниже «определения» $\otimes$. Решить, правильно, или нет каждое из них определяет бинарную операцию, и если так, то является ли операция коммутативной. Найти, если это возможно, единицу и обратный элемент к x. Предполагаются выполненными обычные свойства арифметики:

а) $x \otimes y = x\text{-}y$ на N;

б) $x \otimes y = (x * y) - 1$ на Z;

в) $x \otimes y = \max(x, y)$ на N;

г) $x \otimes y = \sqrt{x^2 + y^2}$ на $\{x: 0 \le x, x \in \mathrm{R}\}$;

д) $x \otimes y = x/y$ на $\{x: 0< x, x \in R\}$.

2. Определим операцию φ на множестве $\{a, b, c\}$, как указано ниже. Проверить, что φ ассоциативна и коммутативна и найти единичный элемент.

φ	a b c
a	b c a
c	a b c
b	c a b

3. Предполагая обычные свойства операций +, -, * и / на R, доказать, что операция ψ, определенная на $[1, \infty[$ следующим образом:

$$a\psi b = \frac{(a*b)+1}{a+b},$$

ассоциативна. Обосновать ответ.

Указание: не следует особенно обращать увагу на область определения.

4. Пусть $\otimes$ — ассоциативная операция на множестве A с единицей e такая, что каждый элемент $a \in A$ может быть обратным и обратный обозначается через a'. Показать, что

$$(a \otimes b)' = b' \otimes a'.$$

5. Показать, что если $\otimes$ — ассоциативная операция на множестве A с единицей e такая, что $a \otimes a = e$ для каждого $a \in A$, то $\otimes$ коммутативна.

6. Пусть $\otimes$ — ассоциативная операция на множестве A такая, что для любых $a, b \in A$, если $a \otimes b = b \otimes a$, то $a = b$. Показать, что каждый элемент A идемпотентен по отношению к $\otimes$. Что можно сказать про $\otimes$, если операция имеет единицу?

7. По аналогии с «естественной» арифметикой, полученной для Z_6, построить аналогичную арифметику для Z_{16}, используя символы {0, 1, ,.., 9, *A, B, ..., F*}.

8. Построить арифметику для Z_6, которая согласуется со строкой

+	0	1	2	3	4	5
2	2	3	4	0	5	1

9. Рассматривая 1+3, показать, что следующая таблица приводит к противоречию:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2

10. Обозначим $Z^{-}_{m} \times Z^{n-1}_{m}$ через Z^{n-}_{m}, где

$$Z^{-}_{m} = \{— (m/2), .,., 0, ..., (m/2) — 1\}, \quad \text{если } m \text{ четное,}$$

и

$$Z^{-}_{m} = \{— (m\text{-}1/2), .,., 0, ..., (m\text{-}1/2)\}, \quad \text{если } m \text{ нечетное.}$$

Вычислить: а) 10-7; б) 17-23; в) (-8)+(-21) в каждой из «естественных» арифметик Z^{4-}_{7}, Z^{3-}_{10}, Z^{5-}_{5}, Z^{2-}_{12}.

Замечание: числа в примерах заданы над Z; поэтому вначале требуется перевести их в соответствующую систему, а потом проводить вычисления.

11. Быстрый способ вычисления дополнения до 2 от данного битового элемента в Z^{n-}_{2} заключается в следующем. Начиная из правого конца, копируем все идущие подряд нули и первую встретившуюся единицу. Затем все оставшиеся биты изменяем. Показать, что этот способ работает в большинстве случаев, и рассмотреть случаи, когда он не работает.

12. Пусть в Z^{5-}_{2} производятся следующие вычисления. Складывают два числа x и y (обозначим их сумму через z). Если от z отнять y, то получим некоторый результат c, а если от z отнять c, то получим некоторое число d. Что можно сказать о c и d? Как отличаются результаты, если вычисления производятся в Z^{n-}_{2}?

13. Переведите в двоичную систему счисления десятичные числа:
а) 51; б) 64; в) 125; г) 1000.

14. Выполните в двоичной системе следующие операции над десятичними числами:
а) 21 + 37; б) 31 + 105; в) 25 8; г) (8 + 19)11; д) 24 8 - 17. Проверьте полученные результаты в десятичной системе.

15. Переведите в двоичную систему счисления с точностью до пяти двоичных знаков после запятой числа: а) 0,131; б) 0,25; в) 175,26.

16. Дайте обоснование правил перевода десятичных чисел в двоичные.

17. Сложите двоичные числа 11001110 и 11010111 по обычному правилу и по модулю два. Найдите разность полученных результатов и объясните ее смысл.

18. Определяя операции $\wedge$ и $\vee$ как минимум и максимум, показать для произвольного Z_n, что

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Микромодуль 2.
Арифметика с нечеткими числами

1.6. Нечеткие числа и функции

1.6.1. Нечеткая и лингвистическая переменные.

Нечеткая переменная определяется кортежем <X, *U*, $\tilde{X}$>, где *X*— наименование нечеткой переменной; $U=\{u\}$ - область ее определения, или универсальное множество;

$$\tilde{X} = \bigcup_{u \in U} \mu_u / u$$

— нечеткое множество на *U* описывающее ограничение на возможные числовые значения нечеткой переменной *X*.

Лингвистическая переменная определяется кортежем

$$<\beta, T, U, G, M>,$$

где β — наименование лингвистической переменной; *T* — множество ее значений, или термов, представляющих собой наименование нечетких переменных, областью определения каждой из которых есть множество *U*. Например, для лингвистической переменной, которая представлена на рис. 1.5,

$T=\{T_1, T_2, T_3\}$, $u_0<u_2<u_1<u_4<u_+$, $U=[u_0, u_+]$.

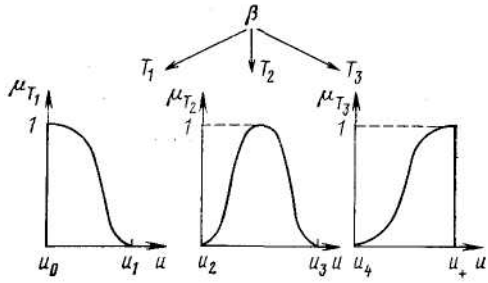


Рис. 1.5. Взаимосвязь лингвистической и нечеткой переменных

Пары точек (u_0, u_+) будем называть ***предельной парой***. В дальнейшем без особой необходимости не будем различать переменную и ее наименование.

Множество *T* будем называть базовым терм-множеством лингвистической переменной; *G* — синтаксическая процедура, которая описывает процесс образования из множества *T* новых, осмысленных

для данной задачи принятия решений значений лингвистической переменной. Множество $T^*=T \cup G(T)$ назовем расширенным терм-множеством лингвистической переменной; M — семантическая процедура, позволяющая приписать каждому новому значению, образуемому процедурой G, некоторую семантику путем формирования соответствующего нечеткого множества, т.е. отобразить новое значение в нечеткую переменную.

Рассмотрим пример лингвистической переменной. Пусть оценивается посадочная скорость летательных аппаратов с помощью понятий «малая», «небольшая», «средняя», «высокая». При этом максимальная посадочная скорость равна 300 км/ч. Формализация такого описания может быть проведена с помощью лингвистической переменной <СКОРОСТЬ, {МАЛАЯ, НЕБОЛЬШАЯ, СРЕДНЯЯ, ВЫСОКАЯ}, [0, 300], G, M>, где G — процедура перебора элементов базового терм-множества, M — процедура экспертного опроса.

1.6.2. Нечеткие числа и функции

В зависимости от характера множества U лингвистические переменные могут быть разделены на числовые и нечисловые. Числовой называется лингвистическая переменная, у которой $U \subset R^1$, где $R^1=(-\infty, \infty)$, и которая имеет измеримую базовую переменную.

Нечеткие переменные, соответствующие значениям числовой лингвистической переменной, будем называть нечеткими числами. Если $|U|<\infty$, то нечеткие числа будем считать дискретными, если же $|U|=|R^1|$ - то непрерывными. Приведенная выше лингвистическая переменная СКОРОСТЬ является числовой, а нечеткие переменные из ее терм-множества - непрерывными нечеткими числами.

Примером нечисловой лингвистической переменной может служить переменная СЛОЖНОСТЬ, которая формализует понятие «сложность разработки», со значениями НИЗКАЯ, СРЕДНЯЯ, УМЕРЕННАЯ, ВЫСОКАЯ.

К функциям принадлежности нечетких чисел обычно предъявляется ряд требований, которые обсуждаются дальше.

Пусть $U=\{u\}$, $V=\{v\}$ — два универсальных множества; $F(U)$ - система всех нечетких множеств, заданных на U. Используя данные обозначения, определяем три типа функций:

четкая функция нечеткого аргумента

$$H_1: F(U) \rightarrow V,$$

нечеткая функция четкого аргумента

$H_2: U \to F(V)$,

нечеткая функция нечеткого аргумента

$H_3: F(U) \to F(V)$.

1.7. Арифметические операции над нечеткими числами

1.7.1. Принцип обобщения.

Как мы уже говорили, под нечетким числом здесь будем понимать нечеткое множество с областью определения в виде интервала действительной оси R^1. Множество всех нечетких чисел, определенных на R^1, обозначим через $\overline{R}^1$. Пусть A и B — два нечетких числа с носителями $S_A = (a_1, a_2)$ и $S_B = (b_1, b_2)$ соответственно; $a_2 > a_1$, $b_2 > b_1$; $g: R^1 \times R^1 \to R^1$ — некоторая функция. Тогда согласно принципу обобщения нечеткое число $D = g(A, B)$ определяется функцией принадлежности

$$\mu_D(x) = \sup_{\substack{g(a,b)=x \\ a \in S_A,\ b \in S_B}} \min\{\mu_A(a),\ \mu_B(b)\}. \tag{1.1}$$

Пусть $\#$ - одна из четырех арифметических операций: +, —, •, /; $g(a,b) = a \# b$. Тогда (1.1) определяет результат арифметической операции $\#$ над нечеткими числами A и B. Если $g(\bullet)$ — функция не двух, а n аргументов, то принцип обобщения формулируется аналогично (1.1).

Первоначально принцип обобщения был введен как некоторый эвристический прием. Потом он был получен дедуктивно, а его физический смысл был объяснен в рамках вероятностной интерпретации функции принадлежности, в соответствии с которой

$$\mu_D(x) = P(x \in D).$$

Носитель S_D нечеткого числа D можно найти по правилам интервальной арифметики, так как из (1.1) следует, что

$$S_D = \{x : x = a \# b,\ a \in S_A,\ b \in S_B\}.$$

Очевидно, что в множестве $S_A \times S_B$ для любого $x \in S_A \# S_B$, где операция $\#$ над носителями нечетких чисел A и B выполняется по правилам интервальной арифметики, существует бесконечно много пар (a, b), таких, что $x = a \# b$. Поэтому $\mu_D(x)$ как $P(x \in D)$) зависит от того, какая именно пара чисел (a, b) была предъявлена. Пусть (a', b'), (a'', b'') — две такие пара. Их предъявления субъекту — несовместимые события,

а величины $\mu_A(a')\mu_B(b')$ и $\mu_A(a'')\mu_B(b'')$ - условные вероятности. Например,

$\mu_A(a')\mu_B(b') = P(x \in D|$ субъекту предъявленны a' и $b') \neq P(x \in B)$ при условии, что процессы отнесения a' к A и b' к B независимы.

Таким образом, для того чтобы ответить на вопрос, какова вероятность $P(x \in D)$, а значит, и степень принадлежности $\mu_D(x)$, необходимо знать, как именно получен элемент x (или какая именно пара чисел (a, b) была предъявлена). Возможные две ответа на этот вопрос. Первый из них связан с определением $\mu_D(x)$ на основе измерения и использования плотностей вероятности $f_A(a)$, $f_B(b)$ предъявления элементов a и b субъекту. Если определить данные плотности вероятности по какой-то причине невозможно, то результат операции $A \# B$ можно получить с учетом следующих соображений.

При любых распределениях вероятностей $f_A(a)$ и $f_B(b)$

$$\mu_D(x) \leqslant \sup_{\substack{a \circledast b = x \\ a \in S_A,\ b \in S_B}} \mu_A(a)\,\mu_B(b). \tag{1.2}$$

Величина $p=\mu_A(a)\mu_B(b)$ может рассматриваться как вероятность того, что одновременно a будет отнесено к A и b — к B (считая a и b предъявленными), только если эти отнесения независимы. В общем случае (при наличии зависимости) величина p может быть и выше, но

$$p \leqslant \min\{\mu_A(a),\ \mu_B(b)\}, \tag{1.3}$$

так как $\mu_A(a')$ и $\mu_B(b')$ будут представлять собой безусловные вероятности в зависимых процессах отнесения.

Из (1.2) и (1.3) заключаем, что в общем случае величину

$$\sup_{\substack{a \circledast b = x \\ a \in S_A,\ b \in S_B}} \min\{\mu_A(a),\ \mu_B(b)\}$$

можно рассматривать как верхнюю оценку для $\mu_D(x)$ в (1.1) — когда неизвестны ни распределения вероятностей на S_A, S_B, ни вид зависимости процессов отнесения аргументов к нечетким числам A и B. Из (1.2) следует, что принцип обобщения (1.1) может быть определен также выражением

$$\mu_D(x) = \sup_{\substack{a \circledast b = x \\ a \in S_A,\ b \in S_B}} \mu_A(a)\,\mu_B(b). \tag{1.4}$$

Для его использования обязательно упомянутое выше условие независимости.

При вычислениях на основе (1.1) часто применяется разложение нечеткого множества A по системе α-уровневых множеств A_α:

$$A = \bigcup_{\alpha \in (0,\ 1]} \alpha A_\alpha, \tag{1.5}$$

где A_α — четкое множество $\{a : \mu_A(a) \geq \alpha\}$; αA_α-нечеткое множество $\{(\alpha, a) : a \in A_\alpha\}$.

Доказано, что для любой непрерывной функции

$$f: R^1 \times R^1 \to R^1$$

высказывание

$$(\forall \alpha \in (0,1])\ [f(A,\ B)]_\alpha = f(A_\alpha,\ B_\alpha) \tag{1.6}$$

справедливо, если и только если дополнения S_A и S_B компактны, а $\mu_A(a)$ и $\mu_B(b)$ полунепрерывные сверху. В частности, при этих условиях из (1.6) получаем

$$(A + B)_\alpha = A_\alpha + B_\alpha;$$
$$(A \cdot B)_\alpha = A_\alpha \cdot B_\alpha.$$

Рассмотрим пример выполнения арифметических операций над дискретными ($|S_A|, |S_B| < \infty$) нечеткими числами A и B. Пусть

$$A = \{0{,}1/5;\ \ 0{,}8/6;\ \ 0{,}4/7\},$$
$$B = \{0{,}2/4;\ \ 0{,}9/5;\ \ 0{,}3/6\}.$$

Тогда согласно (1.1)

$$A + B = \{0{,}1/9;\ \ 0{,}2/10;\ \ 0{,}8/11;\ \ 0{,}4/12;\ \ 0{,}3/13\};$$
$$AB = \{0{,}1/20;\ \ 0{,}2/24;\ \ 0{,}1/25;\ \ 0{,}2/28;\ \ 0{,}8/30;$$
$$0{,}4/35;\ \ 0{,}3/36;\ \ 0{,}3/42\}.$$

Пример арифметических операций над непрерывными нечеткими числами A и B ($|S_A| = |S_B| = |R^1|$) приведен на рис. 1.6.

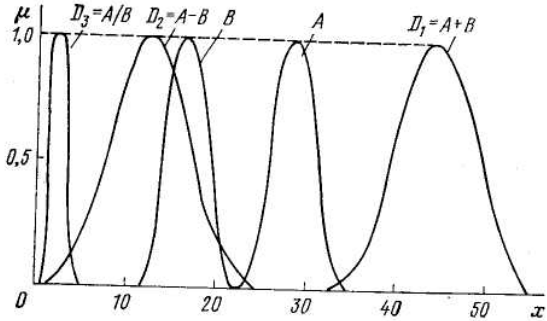


Рис. 1.6. Примеры арифметических операций над непрерывными нечеткими числами A и B

1.7.2. Свойства арифметических операций.

Впервые анализ свойств арифметических операций над нечеткими числами проведен Мазумото и Танака, которые рассмотрели свойства выпуклости и нормальности результатов операций и показали, что:
а) нечеткое число не имеет противоположного и обратного чисел и
б) сложение и умножения коммутативны, ассоциативны и в общем случае недистрибутивны.

Доказано, что если в (1.1) нечеткие числа *A, B* и *D* такие, что

$$A(B + D)=AB+AD,$$

то при определении (1.4)

$$AB+AD \subseteq A(B+D).$$

В ряде работ показано, что при сложении большого количества одинаковых нечетких чисел результат, полученный на основе (1.1), нечувствителен к виду функции принадлежности исходного нечеткого числа, в то время как при определении (1.4) форма функции принадлежности результата зависит от формы исходной функции принадлежности.

Существуют возможность построения математических моделей систем с использованием лингвистических переменных и обычных арифметических операций. Математической основой для построения таких моделей является алгебра нечетких чисел.

Нечетким числом (НЧ) *A*, как мы уже определили, называется нечеткое подмножество числовой оси $\mathcal{R}$, имеющее функцию принадлежности $\mu_A: \mathcal{R} \to [0, 1]$, где $\mathcal{R}$ — множество действительных чисел, $\mathcal{F}(\mathcal{R}) = \{\mu | \mu: \mathcal{R} \to [0, 1]\}$ — множество всех нечетких подмножеств числовой оси.

Нечеткое число называется нормальным, если

$$\max_x \mu_A(x) = 1, \quad x \in \mathcal{R}. \tag{1.7}$$

Нечеткое число называется выпуклым, если $\forall x, y, z \in \mathcal{R}$, $x \le y \le z$,

$$\mu_A(y) \geqslant \mu_A(x) \wedge \mu_A(y), \quad \mu_A \in \mathcal{F}(\mathcal{R}). \tag{1.8}$$

Если $\mu_A \in \mathcal{F}(\mathcal{R})$, то множество α-уровня нечеткого числа *A* определится как

$$A_\alpha = \{x \in \mathcal{R} | \mu_A(x) \geqslant \alpha\}, \quad \alpha \in [0, 1]. \tag{1.9}$$

Подмножество $S_A \subset \mathcal{R}$ называется носителем (суппортом) НЧ *A,* если

$$S_A \triangleq \operatorname{supp} A = \{x \mid \mu_A(x) > 0\}. \tag{1.10}$$

Если A — выпуклое нормальное НЧ, то

$$A_\alpha = [\delta_A(\alpha),\ \gamma_A(\alpha)], \tag{1.11}$$

где $\delta_A(\alpha) = \mu_{\uparrow}^{-1}(\alpha)$, $\gamma_A(\alpha) = \mu_{\downarrow}^{-1}(\alpha)$; здесь $\mu_{\uparrow}^{-1}(\alpha)$, $\mu_{\downarrow}^{-1}(\alpha)$ являются обратными функциями для возрастающей и убывающей частей $\mu_A(x)$ соответственно.

Унимодальное НЧ A называется положительным, если $\forall x \in S_A$, $x > 0$, и отрицательным, если $\forall x \in S_A$, $x < 0$.

Выпуклое НЧ A называется нечетким нулем, если

$$\mu_A(0) = \sup(\mu_A(x)). \tag{1.12}$$

Расширенная бинарная арифметическая операция, обозначаемая $\tilde{*}$, для нечетких чисел $\mu_A,\ \mu_B,\ \mu_C \in \mathscr{F}(\mathscr{R})$; $\forall x, y, z \in \mathscr{R}$ определяется следующим образом:

$$C = A \tilde{*} B \Leftrightarrow \mu_C(z) = \bigvee_{z=x*y} (\mu_A(x) \wedge \mu_B(y)). \tag{1.13}$$

Согласно (1.13) арифметические операции расширенного сложения, вычитания, умножения и деления $(\tilde{+},\ \tilde{-},\ \tilde{\cdot},\ \tilde{:})$ над $A,\ B,\ C$, т. е. $\forall \mu_A,\ \mu_B,\ \mu_C \in \mathscr{F}(\mathscr{R})$ можно интерпретировать как

$$C = A \tilde{+} B \Leftrightarrow \mu_C(z) = \bigvee_{z=x+y} \mu_A(x) \wedge \mu_B(y); \tag{1.14}$$

$$C = A \tilde{-} B \Leftrightarrow \mu_C(z) = \bigvee_{z=x-y} \mu_A(x) \wedge \mu_B(y); \tag{1.15}$$

$$C = A \tilde{\cdot} B \Leftrightarrow \mu_C(z) = \bigvee_{z=xy} \mu_A(x) \wedge \mu_B(y); \tag{1.16}$$

$$C = A \tilde{:} B \Leftrightarrow \mu_C(z) = \bigvee_{z=x/y} \mu_A(x) \wedge \mu_B(y). \tag{1.17}$$

Для расширенных операций $\widetilde{\max}$ и $\widetilde{\min}$ выражение (1.13) примет вид:

$$C = \widetilde{\max}(A, B) \Leftrightarrow \mu_C(z) = \bigvee_{z=\max(x,y)} \mu_A(x) \wedge \mu_B(y); \tag{1.18}$$

$$C = \widetilde{\min}(A, B) \Leftrightarrow \mu_C(z) = \bigvee_{z=\min(x,y)} \mu_A(x) \wedge \mu_B(y). \tag{1.19}$$

Отношоиие порядка для почетких чисел имеет вид:

$$A \tilde{\subseteq} B \Leftrightarrow \widetilde{\min}(A, B) = A, \tag{1.20}$$

$$A \tilde{\subseteq} B \Leftrightarrow \widetilde{\max}(A, B) = B. \tag{1.21}$$

Отметим следующие свойства операций над нечеткими числами:

$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$
$$(A \odot B) \odot C = A \odot (B \odot C),$$
$$A \oplus B = B \oplus A,$$
$$A \odot B = B \odot A,$$
$$A \oplus (-A) \neq 0,$$
$$A \odot (1/A) \neq 1.$$

Если A есть положительное или отрицательное НЧ и если B, C — оба положительные или оба отрицательные НЧ, тогда

$$A \odot (B \oplus C) = (A \odot B) \oplus (A \odot C).$$

Операции $\widetilde{\max}$ и $\widetilde{\min}$ являются ассоциативными и коммутативными операциями. Закон Де Моргана для $\widetilde{\max}$ и $\widetilde{\min}$ имеет вид:

$$1 \ominus \widetilde{\min}(A, B) = \widetilde{\max}(1 \ominus A, 1 \ominus B);$$
$$1 \ominus \widetilde{\max}(A, B) = \widetilde{\min}(1 \ominus A, 1 \ominus B).$$

Дистрибутивность:

$$\widetilde{\min}(A, \widetilde{\max}(B, C)) = \widetilde{\max}(\widetilde{\min}(A, B), \widetilde{\min}(A, C)),$$
$$\widetilde{\max}(A, \widetilde{\min}(B, C)) = \widetilde{\min}(\widetilde{\max}(A, B), \widetilde{\max}(A, C)).$$

Поглощение:

$$\widetilde{\max}(A, \widetilde{\min}(A, B)) = A,$$
$$\widetilde{\min}(A, \widetilde{\max}(A, B)) = A,$$
$$\widetilde{\max}(A, B) \oplus \widetilde{\min}(A, B) = A \ominus B.$$

При решении практических задач всегда удобнее пользоваться множествами α-уровня для реализации арифметических операций над НЧ.

Можно доказать справедливость следующего утверждения.

Утверждение 1. Если $\forall \alpha \in [0, 1]$ операция $\tilde{*}$ — является расширенной бинарной операцией и нормальные унимодальные нечеткие числа A, B, C: μ_A, μ_B, $\mu_C \in \mathcal{F}(\mathcal{R})$ имеют носители такие, что $\forall x \in S_A$, $x > 0$ или $\forall x \in S_A$, $x < 0$, то будет справедливо следующее:

$$C = A \tilde{*} B = \bigcup \alpha [\delta_C(\alpha), \gamma_C(\alpha)],$$
$$\delta_C(\alpha) = \delta_C = \inf \{\delta_A * \delta_B, \gamma_A * \delta_B, \delta_A * \gamma_B, \gamma_A * \gamma_B\},$$
$$\gamma_C(\alpha) = \gamma_C = \sup \{\delta_A * \delta_B, \gamma_A * \delta_B, \delta_A * \gamma_B, \gamma_A * \gamma_B\},$$

где

$$\bigcup_{\alpha} \triangleq \bigcup_{\alpha\in[0,1]}, \quad \gamma_A(\alpha) \triangleq \gamma_A; \quad \gamma_B(\alpha) \triangleq \gamma_B, \quad \delta_A(\alpha) \triangleq \delta_A, \quad \delta_B(\alpha) \triangleq \delta_B,$$

Таким образом, выражения (1.14) — (1.19) для положительных НЧ примут вид:

$$A \oplus B = \bigcup_{\alpha} \alpha(A_\alpha + B_\alpha) = \bigcup_{\alpha} \alpha[\delta_A + \delta_B, \gamma_A + \gamma_B], \tag{1.22}$$

$$A \odot B = \bigcup_{\alpha} \alpha(A_\alpha \cdot B_\alpha) = \bigcup_{\alpha} \alpha[\delta_A\delta_B, \gamma_A\gamma_B], \tag{1.23}$$

$$A \ominus B = \bigcup_{\alpha} \alpha(A_\alpha - B_\alpha) = \bigcup_{\alpha} \alpha[\delta_A - \gamma_B, \gamma_A - \delta_B], \tag{1.24}$$

$$A \oslash B = \bigcup_{\alpha} \alpha(A_\alpha \div B_\alpha) = \bigcup_{\alpha} \alpha[\delta_A/\gamma_B, \gamma_A/\delta_B], \tag{1.25}$$

$$\widetilde{\max}(A, B) = \bigcup_{\alpha} \alpha[\delta_A \vee \delta_B, \gamma_A \vee \gamma_B], \tag{1.26}$$

$$\widetilde{\min}(A, B) = \bigcup_{\alpha} \alpha[\delta_A \wedge \delta_B, \gamma_A \wedge \gamma_B]. \tag{1.27}$$

1.7.3. Нечеткие числа *(L— R)*-типа

При решении задач математического моделирования нечетких систем можно использовать нечеткие числа *(L — R)*-типа, которые предполагают более простую интерпретацию расширенных бинарных операций. НЧ *(L — R)*-типа может быть задано с помощью функции принадлежности *(L — R)*-типа, удовлетворяющей свойствам

а) $L(-x) = L(x), \quad R(-x) = R(x),$

б) $L(0) = R(0) = 1,$

где *L* и *R* — невозрастающие функции на множестве неотрицательных действительных чисел.

Примерами *(L — R)*-функций могут служить $L(y) = e^{-|y|^p}, \ p \geq 0,$

$$L(y) = \frac{1}{1+|y|^p}, \quad p \geqslant 0, \quad L(y) = \begin{cases} 1, & \text{при } y \in [-1, 1], \\ 0 & \text{в противном случае.} \end{cases}$$

Нечеткое унимодальное число *A* является НЧ *(L — R)* -типа тогда и только тогда, когда

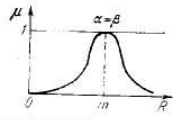
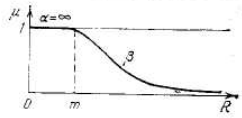
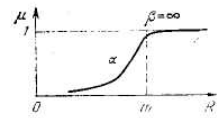
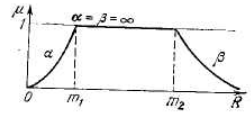
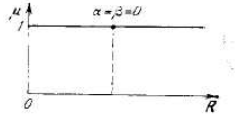
$$\mu_A(x) = L((a-x)/\alpha) \quad \forall x \leqslant a, \quad \alpha > 0,$$

$$\mu_A(x) = R((x-a)/\beta) \quad \forall x \geqslant a, \quad \beta > 0,$$

где *a* — среднее значение (мода) нечеткого числа, а α, β — левый и правый коэффициенты нечеткости соответственно.

Тмким образом, НЧ можно представить в виде тройки параметров $A = (a, \alpha, \beta)$. (см. табл. 1.12)

Таблица 1.12

Терм ЛП	$(L-R)$-представление	Графическое представление
Средний	$M = (m, \alpha, \beta)_{LR}$ $\alpha = \beta > 0$	
Малый	$M = (m, \infty, \beta)_{LR}$ $\alpha = \infty$	
Большой	$M = (m, \alpha, \infty)_{LR}$ $\beta = \infty$	
Разнообразный (зона полной неопределенности)	$M = (m, \infty, \infty)_{LR}$ $\mu_M(x) = \text{const}\ \forall x \in R$	
Приблизительно в диапазоне (зона частичной неопределенности)	$M = (m_1, m_2, \alpha, \beta)_{LR}$ толерантное (плоское) НЧ	
Определенный	$M = (m_1, 0, 0)$ $\alpha = \beta = 0$ обычное число	

Носителем НЧ называется интервал $\left[\lim\limits_{a \to 0_+} \mu_{\uparrow}^{-1}(a),\ \lim\limits_{a \to 0_+} \mu_{\downarrow}^{-1}(a)\right]$.

Толерантное НЧ (L — R)-типа определяется четверкой параметром $A = (a_1, a_2, \alpha, \beta)$, где a_1 и a_2— границы интервала толерантности (см. табл. 1.1).

Рассмотрим операции с нечеткими числами *(L — R)*-типа.

Если $A \triangleq (a, \alpha, \beta)$, $B \triangleq (b, \gamma, \delta)$, то операции над нечеткими числами *(L — R)*- типа как частный случай (1.22) — (1.27) примут вид

1. Сложение НЧ:

$$(a, \alpha, \beta)_{LR} \oplus (b, \gamma, \delta)_{LR} = (a + b, \alpha + \gamma, \beta + \delta)_{LR}. \qquad (1.28)$$

2. Вычитание НЧ: если $-(a, \alpha, \beta)_{LR} = (-a, \beta, \alpha)_{RL}$, то

$$(a, \alpha, \beta)_{LR} \ominus (b, \gamma, \delta)_{RL} = (a - b, \alpha + \delta, \beta + \gamma)_{LR}. \qquad (1.29)$$

3. Умножение 3 НЧ:

3а) $\forall A, B$ **таких, что** $\mu_A, \mu_B \in \mathcal{F}(\mathcal{R}^+)$, $a > 0$, $b > 0$,

$$(a, \alpha, \beta)_{LR} \odot (b, \gamma, \delta)_{LR} \simeq (ab, a\gamma + b\alpha, a\delta + b\beta)_{LR}; \qquad (1.30)$$

3б) $\forall A, B$ таких, что $\mu_A, \mu_B \in \mathcal{F}(\mathcal{R})$, $a < 0$, $b > 0$,

$$(a, \alpha, \beta)_{RL} \odot (b, \gamma, \delta)_{LR} \simeq (ab, b\alpha - a\delta, b\beta - a\gamma)_{RL}; \qquad (1.31)$$

3в) $\forall A, B$: $\mu_A, \mu_B \in \mathcal{F}(\mathcal{R})$, $a < 0$, $b < 0$,

$$(a, \alpha, \beta)_{LR} \odot (b, \gamma, \delta)_{LR} \approx (ab, -b\beta - a\delta, -b\alpha - a\gamma)_{RL}. \qquad (1.32)$$

4. Обратное НЧ: $\forall A$: $\mu_A \in \mathcal{F}(\mathcal{R}^+)$, $a > 0$,

$$(a, \alpha, \beta)_{LR}^{-1} = (1/a, \beta/a^2, \alpha/a^2)_{RL}. \qquad (1.33)$$

5. Делепие НЧ: $\forall A, B$: $\mu_A, \mu_B \in \mathcal{F}(\mathcal{R}^+)$, $a > 0$, $b > 0$,

$$(a, \alpha, \beta)_{LR} \oslash (b, \gamma, \delta)_{RL} \simeq \left(\frac{a}{b}, \frac{a\delta + b\alpha}{b^2}, \frac{a\gamma + b\beta}{b^2}\right). \qquad (1.34)$$

Выражения (1.30) — (1.34) можно применять в случаях малых значений коэффициентов нечеткости α, β, γ, δ.

В качестве примера рассмотрим операцию расширенного сложения для нечетких чисел, имеющих функцию принадлежности вида (рис. 1.7).

$$A = (6, 1, 2), \quad B = (8, 3, 3), \quad C_{LR} = A_{LR} \oplus B_{LR} = (14, 4, 5).$$

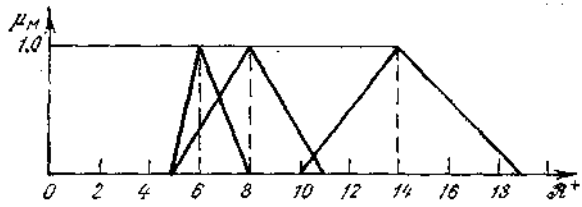


Рис. 1.7. Пример операции сложения на нечетких числах

Для A=(3, 0,5, 0,2); B =(4, 0,3, 0,2) можно получить, согласно (1.28), $C_{LR} = A_{LR} \oplus B_{LR} = (7,\ 0{,}8,\ 0{,}4)$. Функция принадлежности вычисляемого нечеткого числа $(L — R)$-типа имеет вид:

$$\mu_C(x) = \begin{cases} L(\cdot) = \max\left(0,\ 1 - \left|\frac{7-x}{0{,}8}\right|\right) & \forall x \leqslant 7; \\ R(\cdot) = \exp\left(-\left|\frac{x-7}{0{,}4}\right|\right) & \forall x \geqslant 7. \end{cases}$$

1.7.3. Алгоритмы выполнения арифметических операций.

Для вычисления результата выполнения арифметической операции разработано несколько алгоритмов. Так, например, предложенный алгоритм перебора, позволяет найти приблизительное (с любой точностью) значение функции принадлежности для любой точки носителя результата при определениях (1.1) и (1.4).

В одном из алгоритмов рассматриваются нечеткие числа с кусочно-непрерывной функцией принадлежности; доказана теорема, позволяющая довольно легко отыскивать точное значение степени принадлежности для любого элемента носителя результата арифметической операции. Этот алгоритм применим для определения (1.1) и выполняет числовое решение нелинейных уравнений. Схема его выполнения приведена на рис. 1.8.

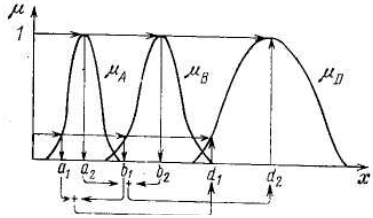


Рис. 1.8. Иллюстрация работы алгоритма Дюбуа-Прада при сложении нечетких чисел.

В некоторых роботах предложен также алгоритм быстрого приближенного вычисления результата арифметической операции. Его идея заключается в том, что левые ветви функций принадлежности операндов A и B аппроксимируются одной монотонно возрастающей функцией L, которая зависит от двух параметров, подбираемых для каждого операнда отдельно: $L\ (m_A,\ \gamma_A)$ и $L\ (m_B,\ \gamma_B)$. Аналогично для правых ветвей и монотонно убывающей функции R имеем $R(m_A,\ \delta_A)$ и $R(m_B,\ \delta_B)$. Полученные аппроксимации называются $L—R$ нечеткими

числами и обозначаются через $(m_A, \gamma_A, \delta_A)$, $(m_B, \gamma_B, \delta_B)$. Доказано, что результат сложения и вычитания *L—R* нечетких чисел есть также *L—R* нечеткое число вида $(m_A \pm m_B, \gamma_A+\gamma_B, \delta_A + \delta_B)$. Результат умножения и деления *L—R* нечетких чисел будет *L—R* нечетким числом лишь приблизительно. Например, результат умножения приблизительно имеет вид $(m_A m_B,\ m_A\gamma_B+m_B\gamma_A,\ m_A\delta_B+m_B\delta_A)$. *L— R* - аппроксимация полезная тем, что сами функции $L(\cdot)$ и $R(\cdot)$ в промежуточных вычислениях не участвуют, а используются лишь при получении окончательного ответа.

1.7.4. Многоместные арифметические операции.

Пусть *A, B, D* — нечеткие числа, такие, что $D=A/(A+B)$. Обычно в литературе по нечеткой арифметике значения *D* вычисляют в два этапа — сначала находят сумму $A+B$, а потом — частное от деления *A* на $A + B$. При этом

$$S_{D'} = \frac{S_A}{S_A + S_B} = \left\{ d \in \frac{S_A}{S_{AB}} \right\}, \quad S_{AB} = S_A + S_B,$$

$$\mu_{D'}(d) = \sup_{\frac{a}{a'+b}=d,\ a,a' \in S_A,\ b \in S_B} \min\{\mu_A(a),\ \mu_A(a'),\ \mu_B(b)\}. \tag{1.35}$$

Если, однако, считать, то в определение *D* входит одно и то же число *A,* то должно быть

$$S_{D''} = \left\{ d : d = \frac{a}{a+b},\quad a \in S_A,\quad b \in S_B \right\},$$

$$\mu_{D''}(d) = \sup_{\frac{a}{a+b}=d,\ a \in S_A,\ b \in S_B} \min\{\mu_A(a),\ \mu_B'(b)\}. \tag{1.36}$$

Существует доказательство, что

$$S_{D''} \subseteq S_{D'},\ D'' \subseteq D',$$

где D' определяется функцией принадлежности (1.35), а D'' — функцией (1.36).

Таким образом, если значением величины *D* считать нечеткое число D'', то число D' будет лишь «охватывающей» оценкой, для *D.* Заметим, что изложенное остается справедливым и при более сложных нечетких арифметических выражениях.

Для вычисления значений типа D'' сложных арифметических выражений в качестве первого приближения может быть использован следующий алгоритм.

Пусть Y, X_i $(i \in 1,2,..,n)$ — нечеткие числа; $Y=f(X_1, ...,X_n)$; f — арифметическая функция переменных $X_1, ..., X_n$.

Шаг 1. С помощью зависимости f и носителей $S_1, S_2,...$, S_n нечетких чисел $X_1, X_2,..., X_n$ определить носитель S_Y. (Поскольку вычисляется результат типа D'', при нахождении S_Y непосредственное использование определений интервальной арифметики здесь невозможно).

Шаг. 2. Выполнить дискретизацию $S_1...,S_n$ на равное число точек.

Шаг 3. Дискретизировать S_Y. Выбрать очередной элемент $y \in S_Y$.

Шаг 4. Определить нечеткое число Y, пользуясь процедурой перебора

$$\mu_Y(y) = \sup_{f(x_1 \cdots, x_n)=y} \min_i \{\mu_{X_i}(x_i)\},$$

где $x_i \in S_i$.

В многоместных арифметических операциях кроме рассмотренного случая повторного вхождения переменной возможно наличие более сложного взаимодействия переменных.

Анализу процедуры сложения взаимодействующих переменных посвящен ряд работ. В некоторых из них описан алгоритм решения задачи вычисления нечеткой ожидаемой полезности U альтернативы для случая, когда альтернатива имеет n результатов, полезность j-го из которых равна u_j, а вероятность есть нечеткое число P_j с носителем S_j и функцией принадлежности $\mu_j(p_j)$:

$$U = \sum_{j=1}^{n} P_j u_j, \quad \sum_{j=1}^{n} p_j = 1.$$

Согласно (1.1) с учетом условия нормировки получаем

$$\mu_U(u) = \sup_{p_j \in S_j,\ j \in \overline{1,n}} \mu_j(p_j),$$

при ограничениях

$$\sum_{j=1}^{n} p_j u_j = u, \quad \sum_{j=1}^{n} p_j = 1.$$

Первое выражение данной системы ограничений соответствует выполняемому действию - нахождению математического ожидания полезности, а второе выражение как раз и является примером более сложной связи четких значений нечетких чисел.

1.8. Нечеткие уравнения

1.8.1. Линейные нечеткие уравнения.

В рамках аксиоматического подхода к принятию решений функция полезности измерится в шкале интервалов и строится на основе аксиомы непрерывности, которая утверждает, что для исходов x_1 f x_2 f x_3 и лотереи (p, x_1; (1— p), x_3) существует вероятность p_0, такая, что (p_0, x_1; (1— p_0), x_3) ~x_2. Тогда если полезности $U(x_1)=u_1$ и $U(x_2)=u_2$, то

$$u_2 = p_0u_1+(1- p_0) U(x_3). \qquad (1.37)$$

Отсюда $U(x_3)$ - корень линейного уравнения (1.37). В задачах принятия решений в нечеткой среде числа, которые входят у уравнение (1.37), могут быть нечеткими. Поэтому при построении нечеткой функции полезности возникает необходимость решения линейного нечеткого уравнения вида

$$AX + B = D, \qquad (1.38)$$

где A, B, D — нечеткие числа, а арифметические операции выполняются на основе принципа обобщения (1.1).

Уже в первой работе по нечеткой арифметике было доказано, что пары операций «сложение - вычитание» и «умножение - деление» не позволяют отыскать соответственно противоположное и обратное нечеткие числа, так как

$$(\forall A,\ A'\in\tilde{R}^1)\,A+A'\neq 0,$$
$$(\forall A,\ A''\in\tilde{R}^1)\,AA''\neq 1.$$

Кроме того,

$$(A-B)+B\neq A,\ (A/B)B\neq A.$$

На основе этот результат сделан вывод о невозможности точного решения нечетких уравнений.

1.8.2. Арифметическая операция «дополнительное вычитание».

Рассмотрим сложение нечетких чисел. Пусть $S_A = (a_1, a_2)$, $S_B=(b_1,b_2)$, $S_D=(d_1,d_2)$ — носители нечетких чисел A, B и D соответственно.

Известно, что если $U = A + B$, то

$$(d_1, d_2) = (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2).$$

Очевидно, что в общем случае

$$(b_1, b_2) \neq (d_1, d_2) — (a_1, a_2) = (d_1 — a_2, d_2 — a_1),$$

т.е. пользуясь операцией вычитания интервалов, носитель неизвестной X в нечетком уравнении $A+X = D$ найти нельзя, а значит, исходя из принципа обобщения (1.1), нельзя найти и величину X.

Введем операцию «дополнительное вычитание» (обозначим ее через — —) так, чтобы при выполнении равенства $X=D— —A$ было справедливо $A + X=D$. Для носителей нечетких чисел определим операцию «— —» следующим образом:

$$(d_1, d_2) — — (a_1, a_2) = (d_1 - a_1, d_2 - a_2). \qquad (1.39)$$

Тогда

$$(b_1, b_2) = (d_1, d_2) — — (a_1, a_2)$$

для любых интервалов S_A, S_B, для которых $S_D=S_A+S_B$.

Степень принадлежности для любой точки $b' \in S_B$ при известных A и D (в равенстве $D=A+B$) можно определить по алгоритму, который иллюстрируется на рис. 1.9, где $b'= d'-a'$, $b''= d'' -a''$.

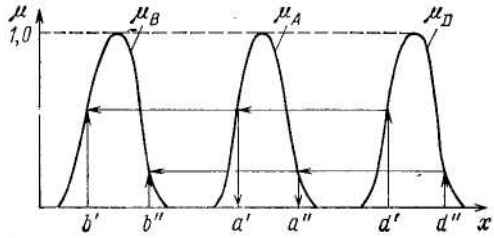


Рис. 1.9. Иллюстрация работы алгоритма выполнения операций дополнительного вычитания и деления нечетких чисел.

Справедливость алгоритма следует из теоремы Дюбуа - Прада. Соответствующее аналитическое выражение имеет вид

$$X = D — — A \Rightarrow \mu_X(x) = \inf_z \sup \{a \in [0,1] : \min \{\mu_A(z - x),\ a\} \leqslant \mu_D(z)\}, \qquad (1.40)$$

или после упрощения,

$$\mu_X(x) = \inf_z \begin{cases} 1, \text{ если } \mu_A(z-x) \leq \mu_D(z), \\ \mu_D(z), \text{ если } \mu_A(z-x) > \mu_D(z). \end{cases}$$

Для решения нечетких уравнений Дюбуа — Прада предложена дополнительная операцию) + (вычитания интервалов $G= (g_1, g_2)$ и $H= (h_1, h_2)$, такую, что

$$(G+H) \ )+(\ (-H) = G.$$

Она определяется выражением

$$G)+(Y=\begin{cases}[g_1+h_2,\ h_2+g_1], \textit{если } h_2+g_1\geq g_1+h_2,\\ 0-\textit{в противном случае}\end{cases}$$

Можно показать, что

$$A)+(\ (\ -B)\equiv A-\!-\!-B$$

и, значит,

$$(A+B)\ )+(\ (\ -B)=(A+B)-\!-\!-B.$$

Таким образом, операция дополнительного вычитания — — (1.39)
и дополнительная операция) + (аналогичны.

1.8.3. Арифметическая операция «дополнительное деление».

Рассмотрим умножение нечетких чисел. Известно, что если

$$D=A*\mathrm{B},\ \alpha_{ij}=a_ib_j\ (i,j\in 1,2),$$

то

$$d_1=\min_{i,\ j}\{\alpha_{i,j}\},\ d_2=\max_{i,\ j}\{\alpha_{ij}\}$$

или

$$(d_1,d_2)=(a_1,a_2)*(b_1,b_2),$$

где умножение носителей выполняется по правилам интервальной арифметики. Аналогично сложению при $0\notin S_A$ имеем

$$(b_1,b_2)\neq(d_1,d_2)/(a_1,a_2)=(d_1,d_2)\ (1/a_2)\ 1/a_1).$$

Значит, на основе операции деления носитель неизвестного Y в нечетком уравнении $AY=D$ найти нельзя. Поэтому определим новую операцию // («дополнительное деление») так, чтобы при выполнении равенства $Y=D//A$ было справедливо равенство $AY=D$.

Для носителей нечетких чисел операция // определяется следующим образом:

$$\left.\begin{array}{l}S_A>0,\quad S_D>0\Rightarrow\\ \quad(d_1,\ d_2)//(a_1,\ a_2)=(d_1/a_1,\ d_2/a_2),\\ S_A>0,\quad S_D<0\Rightarrow\\ \quad(d_1,\ d_2)//(a_1,\ a_2)=(d_1/a_2,\ d_2/a_1)\end{array}\right\}\qquad(1.41)$$

и т.д. Алгоритм вычисления степеней принадлежности для любой точки $b'\in S_B$ при известных A и D (в равенстве $D=AB$) иллюстрируется на рис. 1.9, где $b'=d'/a'$, $b''=d''/a''$. Справедливость алгоритма следует из теоремы Дюбуа - Прада.

Данному алгоритму соответствует следующее аналитическое выражение:

$$\bar{X} = D//A \Rightarrow \mu_X(x) = \inf_t \sup \{a \in [0,\ 1]: \min\{\mu_A(t/x), a\} \leqslant \mu_D(t)\}, \tag{1.42}$$

или после упрощения

$$\mu_X(x) = \inf_t \begin{cases} 1, \text{если } \mu_A(t/x) \le \mu_D(t), \\ \mu_D(t), \text{если } \mu_A(t/x) > \mu_D(t). \end{cases}$$

1.8.4. Решение уравнений с нечеткими числами

Ряд задач анализа математических моделей нечетких систем предполагает необходимость решения уравнений с нечеткими числами. С практической точки зрения интересно рассмотреть уравнения с обычными математическими термами и нечеткими математическими отношениями и уравнения с нечеткими числами и обычными математическими отношениями.

В общем случае нечеткими уравнениями называются уравнения, в которых коэффициенты и/или переменные являются нечеткими числами.

1. Уравнения с нечеткими отношениями и обычными математическими термами.

Определение 1. Математическим термом называется конструкция из элементов $x \in \mathcal{R}^1$ и связывающих их операций: +, ×, -, :.

Определение 2. Если $\mu_A \in \mathcal{F}(\mathcal{R}^2)$, $\mu_A: \mathcal{R}^2 \to [0,\ 1]$, то A называется нечетким отношением, а $\mu_A(x, y)$ указывает на то, с какой степенью (x, y) удовлетворяет A. Примером A может быть $A \stackrel{\Delta}{=}$ «приблизительно равно».

Определение 3. Если f_1 и f_2 математические термы и A нечеткое отношение, т. е. $\mu_A: R^2 \to [0,\ 1]$, то $f_1 A f_2$ называется нечетким уравнением с нечетким отношением.

Теорема 1. Предположим, что f_1 и f_2 математические термы, A является нечетким отношением и имеет место уравнение $f_1 A f_2$. Тогда, если $a \in \mathcal{R}^1$, то

$$\begin{aligned} &1) \quad (f_1 + a)(A + a)(f_2 + a), \\ &2) \quad (f_1 \cdot a)(A \cdot a)(f_2 \cdot a). \end{aligned} \tag{1.43}$$

В дальнейшем $\mu_A(x, y)$ будем обозначать $A(x, u)$.

Если $A = \{(x,\ y),\ \mu_A(x,\ y)\} \in \mathcal{F}(\mathcal{R}^2)$, $A(x,\ y) = a$, то $\forall a \in$

$\in [0, 1]$, $b \in \mathscr{R}^1$ нечеткое отношение A а) симметрично, если $A(x, y) = A(y, x)$; б) аддитивно независимо относительно b, $A+b=A$; в) мультипликативно независимо относительно b, $b \bullet A=A$.

Теорема 2. Нечеткое отношоиио A является аддитивно независимым тогда и только тогда, когда

$$A(x, y) = A(|x - y|). \quad (1.44)$$

Теорема 3. Нечеткое отношение A является мультипликативно независимым тогда и только тогда, когда

$$A(x, y) = A((x/y)^h), \quad h \geqslant 1. \quad (1.45)$$

Определение 4. Нечетким математическим термом называется конструкция из элементов $\mu_{A_i} \in \mathscr{F}(\mathscr{R}^1)$, $i \in \mathbf{N}$, связанных операциями $\odot, \oplus, \ominus, \odot, \widetilde{\max}, \widetilde{\min}$.

В литературе рассматриваются примеры решения уравнений с нечеткими отношениями и обычными математическими термами на основании вышеуказанных теорем.

2. Уравнения с обычными отношениями и нечеткими математическими термами. Широкий класс задач математического программирования в нечетких условиях и анализа нечетких систем предполагает необходимость решения уравнений с нечеткими термами и обычными отношениями. Поскольку семейство выпуклых нормальных нечетких чисел образует только коммутативное полукольцо, то решение уравнения с нечеткими термами возможно только при использовании разложения нечетких термов по α-уровням. Метод, описанный в литературе, неизбежно приводит к нечетким нулям и в конечном счете к изменению степени истинности математических отношений.

Определение 5. Скобочной формой уравнения $f_1 A f_2$ называется следующее разложение по α -уровням:

$$\left(\bigcup_\alpha \alpha f_1 \alpha\right) A \left(\bigcup_\alpha \alpha f_2 \alpha\right) = \left(\bigcup_\alpha \alpha \left[\delta_{f_1}, \gamma_{f_1}\right]\right) A \left(\bigcup_\alpha \alpha \left[\delta_{f_2}, \gamma_{\delta_2}\right]\right). \quad (1.46)$$

Пример:

пусть

$$\mu_A > 0, \quad \mu_X > 0, \quad \mu_C > 0, \quad f_1 \triangleq \mu_C, \; f_2 \triangleq \mu_A \odot \mu_X;$$

тогда

$$\mu_C = \mu_A \odot \mu_X \Leftrightarrow \bigcup_\alpha \alpha [\delta_C, \gamma_C] = \bigcup_\alpha \alpha [\delta_A \delta_X, \gamma_A \gamma_X]. \quad (1.47)$$

Если все нормальные унимодальные числа, из которых состоят нечеткие термы f_1, f_2, имеют носители $S_{f_{1,2}}$ такие, что они не

содержат одновременно положительных и отрицательных элементов, то будет справедливо следующее соотношение

$$f_1 A f_2 \Leftrightarrow \begin{cases} (\delta_{f_1})\, A\, (\delta_{f_2}) & \forall \alpha \in [0,\ 1]. \\ (\gamma_{f_1})\, A\, (\gamma_{f_2}) & \forall \alpha \in [0,\ 1]. \end{cases} \quad (1.48)$$

Поскольку элементы скобочной формы и A являются обычными математическими термами и отношениями, то для скобочной формы будут справедливы соответствующие условия аддитивной и мультипликативной независимости, которые справедливы для любых обычных уравнений.

Таким образом, чтобы решить уравнение вида $f_1(x)Af_2(x)$, необходимо привести его к виду (5.46) и решить отдельно относителыго δ_x и γ_x. Условием адекватности решения является выпуклость и нормальность IIЧ (1.1), (1.2).

В случае L — R нечетких чисел уравнение с НЧ можно решить, получив соответствующую скобочную форму. При этом необходимо учитывать приближенный характер операций e и ⊙ для нечетких чисел $(L$ — й)-типа.

Условие адекватности решения в этом случае примет вид

$$\alpha_x \geqslant 0, \quad \beta_x \geqslant 0, \quad (1.49)$$

где α_x и β_x — соответствующие коэффициенты нечеткости. Следует отметить, что разложение по α-уровням выпуклых нечетких подмножеств дает возможность производить дальнейший анализ задач с НЧ с помощью методов интервального анализа.

1.8.5. Свойства дополнительных операций.

Решение линейного нечеткого уравнения (1.38) с использованием дополнительных операций (1.39)—(1.42) имеет вид $X=(C$— -В$)//A$. Свойства дополнительных операций состоят в следующему:

1. Операция дополнительного отнимания A— —B определена не для всех $A, B \in \overset{0}{R}{}^{0}$, а только для таких нечетких чисел, в которых $a_1–b_1 \leq a_2–b_2$, или $a_2–a_1 \geq b_2–b_1$ т.е. у уменьшаемого длина интервала (носителя) должна быть больше чем у вычитаемого. Отсюда $\forall A \in \overset{0}{R}{}^{0}$ операция 0— —A не определена.

2. Операция дополнительного деления определена также не на всем множестве $\overline{R}$. Например, если $S_A>0$, $S_B>0$, то операция $B//A$ определена лишь при условии, что $b_2/b_1 \geq a_2/a_1$.

3. Операция) + (определена при том же условии, что и операция дополнительного вычитания.

4. В то время, как

$$(\forall\ A \in \overline{R})A \neq 0,\ A - - A \in \overline{R},$$

имеет место равенство $A - - -B = 0$.

5. Если операция «— —» определена в обеих частях выражения, то

$$A - - -A\ (B - - -C) \neq (A - - -B) - - -G.$$

Неравенство справедливо, так как носитель левой части есть

$$(a_1 - b_1 + c_1,\ a_2 - b_2 + c_2),$$

правой части

$$(a_1 - b_1 - c_1,\ a_2 - b_2 - c_2).$$

6. Если операция $A - - -B$ определенная, то $S_{A--B} \subset S_{A-B}$. Действительно, согласно (1.39) носитель в левой части есть $(a_1 - b_1,\ a_2 - b_2)$, а в правой части $(a_1 - b_2,\ a_2 - b_1)$. Но $a_1 - b_1 > a_1 - - b_2 (b_2 \geq b_1)$ и $a_2 - - b \geq a_2 - - b_2$ (по той же причине), значит, утверждаемое справедливо. Поэтому число $A-B$ является, по-видимому, «охватывающей» оценкой числа $A - - -B$: $A - - -B \subset A - - B$.

В ряде работ предложена схема приближенного решения нечеткого уравнения вида $P_1 R P_2$, где P_1 и P_2 — алгебраические выражения, которые включают нечеткие числа, а R — некоторое отношение. Если введенные выше дополнительные операции определены, то на их основе по данной схеме уравнения можно решать точно.

Получение условий существования точных решений нечетких уравнений даже в линейном случае достаточно трудоемко. Например, можно показать, что для существования точного нечеткого решения уравнения $AX+B=C$, где $A, B, C \in \overline{R}$ и $A, B, C>0$, необходимо, чтобы выполнялось условие $b_2 - - b_1 \leq c_2 - - c_1$ и одно из условий:

а) если $c_1 - b_1 \geq 0$, то при $(c_2 - b_2)/(c_1 - b_1) \geq a_2/a_1$ решение существует;

б) если $c_1 - - b_1 < 0$ и $c_2 - - b_2 > 0$, то решение существует;

в) если $c_2 - - b_2 < 0$, то при $(c_2 - - b_2)/(c_1 - - b_2) \leq a_2/a_1$ решение существует.

1.8.6. Дополнительные возможности решения уравнений.

Анализ показывает, что вопрос, аналогичный рассмотренному выше, изучался в рамках интервальной арифметики. Здесь, однако, предложенные операции дополнительного вычитания и деления,

определенные для любой пары интервальных чисел $S_A=(a_1, a_2)$ и $S_B= (b_1, b_2)$. Например,

$$S_A) — (S_B =(\min\{ a_1- b_1, a_2-b_2\}, \max\{a_1- b_1, a_2- b_2\}). \quad (1.50)$$

В ряде работ исследуется задача построения нечеткого отношения $T \subset X \times Y$ по нечетким множествам $A \subset X$ и $B \subset Y$, которые связаны с T нечетким реляційним уравнением $Y = X \circ T$, где

$$\mu_Y (y) = \sup_{x \in S_X} \min \{\mu_X (x), \mu_T (x, y)\}. \quad (1.51)$$

Выражение (1.51) определяет композиционное правило вывода. Доказано, что при заданных множествах X и Y выражению (1.51) удовлетворяет множество отношений T.

1.9. Нечеткие функции

1.9.1. Виды нечетких функций.

Рассмотрим функцию $f: R^1 \to R^1$. Ее аргументом или значением может оказаться нечеткое число. В первом случае функция f обобщается до функции $\chi: \tilde{R}^1 \to R^1$, а во второму — до функции $\varphi: R^1 \to \tilde{R}^1$.

Если и аргументы, и значения функции f — нечеткие числа, то она обобщается до функции $\psi: \tilde{R}^1 \to \tilde{R}^1$.

Необходимо различать функцию типа φ и так называемый нечеткий пучок F функций f: $X \to Y$, $(X, Y \subset R^1)$, который определяется как нечеткое подмножество Y^X, где каждая функция f имеет степень принадлежности $\mu_F(f)$ к пучку F.

Функции типа χ представляют интерес в основном в рамках задачи о выборе (см. п. 1.10.1). Здесь рассмотрим ряд задач, связанных с нечеткими функциями типов φ и ψ.

1.9.2. Интерполяция нечетких функций.

Обычно результаты опроса специалистов о функциональных зависимостях представляются таблицами. В связи с этим возникает задача интерполяции нечетких функций.

Пусть дано

$$x_1, x_2 \in R^1, x_2 > x_1 \text{ и } \varphi_1 = \varphi(x_1) = \bigcup_{y \in S_1} \mu(y, x_1)/y,$$

$$\varphi_2 = \varphi(x_2) = \bigcup_{z \in S_2} \mu\,(z, x_2)/z,$$

где $S_i = (a_i, b_i) = S_{\varphi_i}$ - носитель нечеткого числа φ_i ($i \in$ l, 2). Пусть $x \in (x_1, x_2)$. Задача интерполяции состоит в определении нечеткого числа

$$\varphi = \varphi\,(x) = \bigcup_{t \in S_\varphi} \mu(t, x)/t,\ S_\varphi \text{-носитель } \varphi.$$

Исходя из того, что решение должно вычисляться как можно быстрее, а схема вычисления должна быть по возможности более простоя, построим ее на основе линейной интерполяции (рис. 1.10).

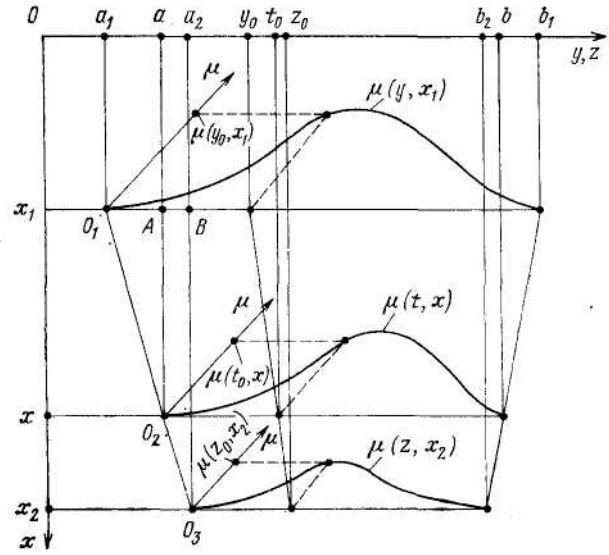


Рис. 1.10. Схема линейной интерполяции значений нечеткой функции четкого аргумента

Из подобных треугольников O_1AO_2 и O_1BO_3 получаем

$$\frac{a - a_1}{a_2 - a_1} = \frac{x - x_1}{x_2 - x_1} \Rightarrow a = a_1 + \frac{a_2 - a_1}{x_2 - x_1}(x - x_1).$$

Аналогично

$$b = b_1 + \frac{b_2 - b_1}{x_2 - x_1}(x - x_1).$$

Тогда $S_\varphi=(a, b)$.Величину $\mu(t,x)$ визначемо $\forall\, t_0 \in S_\varphi$ выражением

$$\mu(t_0,\ x) = \mu(y_0,\ x_1)\frac{x_2 - x}{x_2 - x_1} + \mu(z_0,\ x_2)\frac{x - x_1}{x_2 - x_1}, \qquad (1.52)$$

где y_0 и z_0 делят носители S_1 и S_2 соответственно в той же пропорции, в которой величина t делит отрезок S_φ :

$$\frac{y_0 - a_1}{b_1 - a_1} = \frac{t_0 - a}{b - a} \Rightarrow y_0 = a_1 + \frac{b_1 - a_1}{b - a}(t_0 - a).$$

Аналогично

$$z_0 = a_2 + \frac{b_2 - a_2}{b - a}(t - a).$$

Таким образом, линейная интерполяция значений функции φ определена.

Функция ψ является нечеткой функцией нечеткого аргумента. Для нее интерполяция определяется на основе результатов по функции φ. Пусть даны:

$$X_1 X_2 \in \tilde{R}^1;\ X_i = \bigcup_{x_i \in S_i} \mu(x_i,\ X_i)/x_i\ (i \in \overline{1,\ 2});$$

S_i — носитель нечеткого числа; X_i — интервал на R^1; $\psi_1 = \psi(X_1)$, $\psi_2 = \psi(X_2)$; $\psi_1,\ \psi_2 \in \tilde{R}$, T_i — носитель нечеткого числа ψ_i. Число ψ_i можно представить в виде

$$\psi_i = \bigcup_{x_i \in S_i} \mu_i(x_i)/\nu_i(x_i),\ i \in \overline{1,\ 2},$$

где ν_i: $R^1 \to \tilde{R}$ — функция типа φ. Пусть $X \in \tilde{R}$, $S_{12} = S_1 \cup S_2$, носитель $S_X \subset (\inf S_{12}, \sup S_{12})$. Тогда задача интерполяции функции ψ состоит в определении нечеткого числа

$$\Psi = \psi(X) = \bigcup_{x \in S_X} \mu(x)/\nu(x).$$

Имея решение для функции φ, интерполяцию функции ψ выполняем по принципу обобщения:

$$\Psi = \bigcup_{x \in S_X} \bigcup_{x_1 \in S_1} \bigcup_{x_2 \in S_2} \min\{\mu_1(x_1),\ \mu_2(x_2)\}/\nu(x).$$

Здесь $\nu(x)$ исчисляется согласно (1.52) по исходным: X, X_1, $\nu_1(X_1)$, X_2, $\nu_2(X_2)$. Пусть S_X — носитель числа $\nu(X)$, $\mu_x(\cdot)$ - функция принадлежности $\nu(X)$. Тогда

$$\Psi = \bigcup_{x \in S_X} \bigcup_{x_1 \in S_1} \bigcup_{x_2 \in S_2} \min\{\mu_1(x_1),\ \mu_2(x_2)\}/[\bigcup_{t \in S_X} \mu_X(t)/t] =$$

$$= \bigcup_{x \in S_X} \bigcup_{x_1 \in S_1} \bigcup_{x_2 \in S_2} \bigcup_{t \in S_X} \min\{\mu_1(x_1), \mu_2(x_2),\ \mu_X(t)\}/t. \qquad (1.53)$$

Способ вычисления $\varphi(x)$ и $v(x)$ на основе (1.52) очевиден; вычисление $\psi(X)$ по (1.53) можно провести в соответствии с процедурой перебора, дискретизируя множества S_X, S_1 и S_2 с учетом необходимой точности результата.

В ряде работ приводится способ интерполяции нечетких функций, основанный на композиционном правиле вывода. Пусть даны пары нечетких чисел (Y_i, X_i), которые таблично задают нечеткую функцию ψ: $R \to R$. Построим нечеткое отношение $T = \bigcup_i Y_i \times X_i$, где $\times$ - знак декартова произведения нечетких множеств. Пусть X — нечеткое значение аргумента функции ψ. Тогда $\psi(X) = X \circ T$, где композиция X и T вычисляется по (1.51).

Различие между композиционной и линейной интерполяцией можно проиллюстрировать на примере интерполяции четкой функции. К такой интерполяции в принципе возможны два подхода. Первый заключается в том, что если значение аргумента не содержится в таблице, определяющей функцию, то значение функции считается неопределенным. Второй подход соответствует какой-нибудь из схем интерполяции (линейной, квадратичной и т.д.); здесь привлекается дополнительная информация (линейность функции на отрезке, монотонность функции и т.п.), которая явным образом в исходных данных не содержится. Интерполяция нечеткой функции по композиционному правилу вывода отвечает первому подходу, а интерполяция по (1.53) - второму подходу.

При оценке первого подхода к интерполяции следует иметь в виду его отрицательное качество: для всех пар (X_i, Y_i), участвовавших в формировании отношения T, $Y_i \neq X_1 \circ T$. Кроме того, если $(\forall i) X_i \cap X = \varnothing$, то $X \circ T = \varnothing$, что как раз и соответствует первому подходу к интерполяции.

1.9.3. Интегрирование нечетких функций.

Рассмотрим интегрирование функции $\varphi: R^1 \to R$ для двух случаев: с четкими пределами интегрирования и с пределами интегрирования, заданными нечеткими числами.

Пусть $a, b \in R^1$, $a < b$ — пределы интегрирования; $X = [a, b]$;

$$(\forall x \in X)\,\varphi(x) = \bigcup_{y \in S_x} \mu_x(y)/y; \quad S_x = (y_1, \ y_2)$$

- носитель $\varphi(x)$; $y_1\ y_1 \in R^1$. Нечеткое число $\varphi(x)$ можно представить и в следующем виде:

$$\varphi(x) = \bigcup_{z \in Z_\varphi} \mu_z / z(x),$$

где

$$Z_\varphi = \{z : X \to R^1 \mid (\forall x \in X)\, z(x) \in S_x,$$

z — однозначная непрерывная функция$\}$, а $\mu_z = \min\limits_{x \in X} \mu_x.(z(x))$. Тогда

по принципу обобщения искомый интеграл можно определить следующим оьразом:

$$I_\varphi = \int_a^b \varphi(x)\,dx = \int_a^b \left[\bigcup_{z \in Z_\varphi} \mu_z / z(x)\right] dx = \bigcup_{z \in Z_\varphi} \mu_z \Big/ \int_a^b z(x)\,dx. \tag{1.54}$$

Из (1.54) следует, что I_φ — нечеткое число. Его физический смысл тот же, что и в четком случае: I_φ - это площадь под графиком интегрируемой функции с учетом знака последней. Пусть S_I — носитель I_φ. Из (1.54) следует, что

$$\inf S_I = \int_a^b [\inf S_x]\,dx,$$

$$\sup S_I = \int_a^b [\sup S_x]\,dx.$$

Пусть теперь пределы интегрирования $A = \bigcup\limits_{a \in S_A} \mu_a / a$ и $B = \bigcup\limits_{b \in S_B} \mu_b / b$ — нечеткие числа, S_A и S_B — их носители. Пусть также $z : X \to R^1$ — непрерывная функция. Определим интеграл от нее при нечетких пределах интегрирования следующим образом:

$$\int_A^B z(x)\,dx = \bigcup_{a \in S_A} \bigcup_{b \in S_B} \min\{\mu_a, \ \mu_b\} \Big/ \int_a^b z(x)\ dx. \tag{1.55}$$

Тогда интеграл от функции φ в пределах от A до B с учетом (1.54) и (1.55) можно определить выражением

$$\int_A^B \varphi(x)\,dx = \bigcup_{z\in Z_\varphi} \mu_z \Big/ \int_A^B z(x)\,dx =$$

$$= \bigcup_{a\in S_A} \bigcup_{b\in S_B} \bigcup_{z\in Z_\varphi} \min\{\mu_a, \mu_b, \mu_z\} \Big/ \int_a^b z(x)\,dx. \quad (1.56)$$

Приблизительно интеграл (1.54) можно вычислить по известным формулам прямоугольников или трапеций. При этом арифметические операции в них будут выполняться с нечеткими числами по соответствующим правилам. Значения функции φ в требуемых точках можно вычислить по интерполяционной формуле (1.52). Интеграл (1.56) приблизительно можно вычислить путем дискретизации множеств S_A и S_B, используя далее интеграл (1.54). Детальное изложение проблем интегрирования нечетких функций приводится в ряде работ, где получены определения, аналогичные (1.54) — (1.56). Рассмотрен ряд свойств нечетких функций и интегралов от нечетких функций в нечетких пределах. Получены выражения для вычисления интегралов от *L—R* нечетких функций, определенных на основе *L—R* нечетких чисел. Введено понятия производной от нечеткой функции и ее первообразной. Показано, что между интегралом от нечеткой функции и ее первообразной существует связь, аналогичная той, которая имеется для четких функций. Получены выражения для вычисления производных от *L—R* нечетких функций.

1.10. Сравнение нечетких чисел

1.10.1. Связь четких и нечетких значений лингвистических переменных.

Рассмотрим следующий пример**.**

Система управления запасами сформировала решение: «Закупить небольшое количество деталей». Нечеткое понятие («небольшое количество» задано дискретным нечетким числом

<«НЕБОЛЬШОЕ КОЛИЧЕСТВО», $\overline{1,50}$, C^+>,

где

C^+ = {0/1;...; 0/10; 0,1/11; 0,15/12; 0,2/13; 0,25/14;
0,3/15; 0,4/16; 0,5/17; 0,6/18; 0,7/19; 0,8/20;
0,9/21; 1,0/22;...; 1,0/30; 0,9/29; 0,8/30;
0,7/31; 0,6/32; 0,4/33; 0,2/34; 0/35; 0/36;...}.

Поскольку закупить можно лишь четкое целое число деталей, необходимо произвести выбор четкого значения лингвистической переменной КОЛИЧЕСТВО ДЕТАЛЕЙ при наличии ее нечеткого значения НЕБОЛЬШОЕ. Очевидно, что аналогичных ситуаций в реальных задачах принятия решений довольно много.

Формализацию подобной ситуации назовем задачей о выборе. Пусть дано некоторое понятие естественного языка ε и формализующая его нечеткая переменная <ε, *X, C*ε >, где $C_\varepsilon = \bigcup_{x \in X} \mu_\varepsilon(x) / x$.

Построить процедуру выбора конкретного элемента $x \in X$ по исходным данным ε, *X, C*ε.

Приведем точную формулировку тезиса о выборе, исходя из которой будем решать поставленную задачу.

Пусть данная нечеткая переменная < ε, *X, C*ε >, формализующая некоторое понятие ε. Вероятность выбора лицом, принимающим решение, элемента $x \in X$, пропорциональна значению функции принадлежности με*(x)* нечеткого множества *C*ε. Выбор в каждом конкретном случае определяется разыгрыванием соответствующей случайной величины.

Пусть ε — нечеткое число. На основе тезиса о выборе построим законы распределения случайной величины, порождаемой непрерывным нечетким числом < ε, *X, C*ε >.

Пусть *S*ε-носитель нечеткого множества *C*ε, $|S_\varepsilon| = |R^1|$, $x, y \in R^1$. Введем обозначения

$$x_1 = \inf_{y \in S_\varepsilon} y, \quad x_2 = \sup_{y \in S_\varepsilon} y.$$

Построим две функции: *v*ε*(x)* — плотности вероятности и ωε*(x)* — вероятности того, что в качестве точного значения нечеткого числа ε ЛПР выберет величину *y*<*x*. По определению

$$\int_{x_1}^{x_2} \nu_\varepsilon(x)\, dx = 1, \tag{1.57}$$

$$\omega_\varepsilon(x) = \int_{x_1}^{x} \nu_\varepsilon(y)\, dy. \tag{1.58}$$

Исходя из тезиса о выборе определим функцию плотности вероятности

$$\nu_\varepsilon(x) = k\, \mu_\varepsilon(x)\, f(x,\ C_\varepsilon), \tag{1.59}$$

где *k* — нормирующий множитель, обеспечивающий выполнение равенства (1.57); *f(x, C*ε*)* - функция, которая описывает ограничения выбора. Из (1.57) и (1.59) находим

$$k = \left[\int_{x_1}^{x_2} \mu_\varepsilon(y) f(y, C_\varepsilon)\, dy \right]^{-1}. \tag{1.60}$$

В частности, в качестве $f(x,C_\varepsilon)$ может быть выбрана функция плотности вероятности предъявления элемента x лицу, принимающему решения. При отсутствии данных принимается, что $(\forall x) f(x, C_\varepsilon) = \text{const}$. Тогда из (1.59) и (1.60) получаем

$$\nu_\varepsilon(x) = \mu_\varepsilon(x) \left[\int_{x_1}^{x_2} \mu_\varepsilon(y)\, dy \right]^{-1}. \tag{1.61}$$

Для любого x значение функции $\omega_\varepsilon(x)$ можно вычислить исходя из (1.58) и (1.59) или (1.61).

Таким образом, задача о выбор решена.

Для решения задачи о выборе в литературе предложены и другие процедуры, например:

1) каждый раз выбирать

$$x^* = \arg \sup_{x \in X} \mu_\varepsilon(x); \tag{1.62}$$

2) всегда выбирать такой элемент $x_0 \in X$, который делит площадь под графиком функции принадлежности пополам:

$$\int_{-\infty}^{x_0} \mu_\varepsilon(x)\, dx = \frac{1}{2} \int_{-\infty}^{\infty} \mu_\varepsilon(x)\, dx. \tag{1.63}$$

Однако процедуры (1.62) - (1.63) не учитывают деталей формы функции принадлежности, а используют имеющуюся информацию лишь «в целом».

1.10.2. Отношения порядка на множестве нечетких чисел.

Рассмотрим два нечетких числа: $<A, R^1, C_A>$ и $<B, R^1, C_B>$, в которых пересечение носителей $S_A \mid S_B \neq \varnothing$ (рис. 1.11).

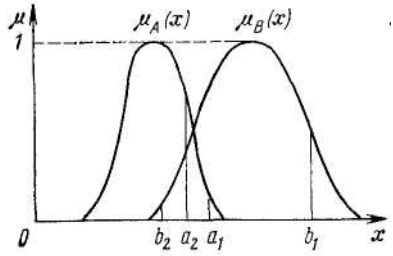


Рис. 1.11. К отношению нечеткого порядка на множестве нечетких чисел

Из анализа задачи о выборе ясно, что в разных реализациях выбора четкого значения нечеткого числа соотношения между четкими значениями нечетких чисел (а значит, и между именами нечетких чисел) может быть различным. Пусть в первой реализации четкие значения нечетких чисел A и B оказались равными соответственно a_1 и b_1, а во второй реализации — a_2 и b_2. Из рис. 1.11 видно, что в первой ситуации $A<B$ (так как $a_1<b_1$), а во второй ситуации $A>B$ (поскольку $a_2>b_2$).

Таким образом, в общем случае отношения порядка типа «больше», «меньше» и т.п. на множестве нечетких чисел являются нечеткими. Лишь в том случае, когда пересечение носителей нечетких чисел A и B пусто, отношение между числами будет четким. Например, пусть A_0 и B_0 — нечеткие числа (рис. 1.12).

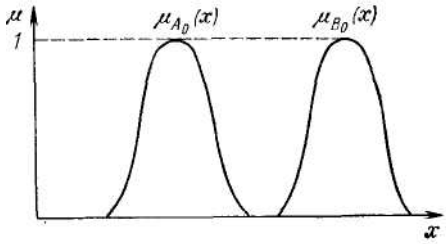


Рис. 1.12. Нечеткие числа с четким отношением порядка

Исходя из рис. 1.12 и сказанного выше можно заключить, что $A_0<B_0$, $B_0>A_0$.

1.10.3. Индексы ранжирования нечетких чисел.

Результат расчетов в модели ПР в нечеткой среде (интегральная оценка альтернативы), как правило, является нечетким числом. Поэтому необходимо определить процедуру сравнения нечетких чисел. Пусть A и B — два непрерывных нечетких числа:

$$\bigcup_{a \in S_A} \mu_a / a$$

и

$$\bigcup_{b \in S_B} \mu_b / b.$$

Все предложенные процедуры основаны на вычислении некоторой четкой функции $H(A, B)$ от нечетких аргументов A и B, которая называется индексом ранжирования. Значение индекса для конкретной

пары чисел дает основание решить вопрос о том, какое из двух чисел больше (или - с какой степенью больше). Приведем ряд индексов ранжирования.

$$1.\ H_1(A,\ B) = \sup_{a \in S_A,\ b \in S_B} \min\{\mu_a,\ \mu_b,\ \mu_V(a,\ b)\}, \tag{1.64}$$

где $\mu_V(a,\ b)$ — функция принадлежности нечеткого отношения предпочтения между четкими числами a и b. В частности, в качестве V может быть избрано четкое отношение V_1 с функцией принадлежности

$$\mu_{V_1}(a,\ b) = 1 \Leftrightarrow a \geq b$$

и

$$\mu_{V_1}(a,\ b) = 0 \Leftrightarrow a < b.$$

Тогда H_1 совпадает с индексом, в общем случае

$$H_1(A,\ B) \geq H_1\{B,\ A) \Rightarrow A \geq B.$$

$H_1(A,\ B)$ — это степень принадлежности пары нечетких чисел A и B к нечеткому отношению $\geq \subset R^{0\%} \times R^{0\%}$.

$$2.\ H_2(A,\ B) = H_+(A) - H_+(B),\quad H_+(A) = \int_0^1 M(A_\alpha)\, d\alpha, \tag{1.65}$$

где A_α — α-уровневое множество нечеткого числа A,

$$M(A_\alpha) = = (a^0 + a^+)/2,\ a^0 = \inf_{a \in A_\alpha} a,\quad a^+ = \sup_{a \in A_\alpha} a.$$

Имеется более простое выражение для индекса H_2: вместо $H_+(A)$ берется величина

$$H_*(A) = H_+(A) \ /\ \sup_{\alpha\,:\,A_\alpha \neq \varnothing} \alpha.$$

Здесь $H_2(A,\ B) \geq 0 \Rightarrow A \geq B$.

3. Индекс, предложенный в одной из работ, определяется как вероятность того, что четкое значение $\mathrm{pv}(A)$ нечеткого числа A будет больше или равно четкому значению $\mathrm{pv}(B)$ нечеткого числа B:

$$H_3(A,\ B) = P(\mathrm{pv}(A) \geq \mathrm{pv}(B)). \tag{1.66}$$

Пусть

$$C = \int_{a_1}^{a_2} \mu_a\, da \int_{b_1}^{b_2} \mu_b\, db,$$

где $(a_1,\ a_2) = S_A$, $(b_1,\ b_2) = S_B$. Тогда в частном случае (при независимых вероятностных распределениях)

$$H_3(A,\ B)=\int_{a_1}^{a_2}\nu_A(a)\,da\int_{b_1}^{a}\nu_B(b)\,db=\int\limits_{\substack{a\in S_A,\ b\in S_B\\ a\geq b}}\mu_a\,\mu_b\,da\,db/C,$$

где $v_A(\cdot)$,$v_B(\cdot)$ вычисляются по (1.61). Если $H_3(A,\ B)\geq H_3(B,\ A)$, то $A\geq B$, или

$$H_3(A,\ B)\geq 0{,}5 \Rightarrow A\geq B.$$

4. Еще один индекс, предложен в одной из работ,

$$H_4(A,\ B)=\int_0^{0,5}[1-\mu_D(z)]\,dz+\int_{0,5}^{1}\mu_D(z)\,dz, \tag{1.67}$$

где $D=A/(A+B)$. При этом $H_4(A,\ B)\geq 0{,}5 \Rightarrow A\geq B$.

5. Еще один индекс, предложен в одной из работ:

$$H_5^1(A,\ B)=\sup_{a\geq b}\min\{\mu_a,\ \mu_b\}; \tag{1.68}$$

$$H_5^2(A,\ B)=\sup_{a}\inf_{b\geq a}\min\{\mu_a,\ 1-\mu_b\}; \tag{1.69}$$

$$H_5^3(A,\ B)=\inf_{a}\sup_{b\leq a}\max\{1-\mu_a,\ \mu_b\}; \tag{1.70}$$

$$H_5^4(A,\ B)=1-\sup_{a\leq b}\min\{\mu_a,\ \mu_b\}. \tag{1.71}$$

Здесь $H^i{}_5(A,\ B)\geq H^i{}_5(B,\ A) \Rightarrow A\geq B$ (i=1,2,3,4).

Процедуры ранжирования n нечетких чисел обсуждаются в некоторых роботах. Здесь в качестве степени предпочтительности числа A_i над остальными числами выбрана величина

$$\mu_i=\min_{j\neq i}\{H(A_i,\ A_j)\}, \tag{1.72}$$

где $H(A_i,\ A_j)$ - степень принадлежности пары нечетких чисел $(A_i,\ A_j)$ к нечеткому отношению «>», вычисляемое по одной из формул (1.64) - (1.71).

1.10.4. Анализ индексов ранжирования.

В ряде работ показано, что

$$H^1{}_5(A,\ B)\geq\max\{H^2{}_5(A,\ B),\ H^3{}_5(A,\ B)\},$$

$$\min\{H^2{}_5(A,\ B),\ H^3{}_5(A,\ B)\}\geq H^4{}_5(A,\ B).$$

Рассмотрим связь индексов H_3 и H_4. Согласно определению H_3 нечеткое число $D=A/(A+B)\geq 0{,}5$, если $H_3(D\ ,\ 0{,}5)\geq 0{,}5$, или

$$1-\int_0^{0,5}\mu_D(z)\,dz\Big/\int_0^{1}\mu_D(z)\,dz\geq 0{,}5.$$

Отсюда

$$\int_0^{0,5} \mu_D(z)\,dz \leqslant \int_{0,5}^{1} \mu_D(z)\,dz,$$

т.е. $H_4(A, B) \geq 0{,}5$. Значит, определения отношения «>» по индексам H_3 и H_4 связаны: $A \geq B$ по индексу $H_4 (H_4 \geq 0{,}5)$, если не меньше 0,5 вероятность того, что четкое значение нечеткого числа $D = A/(A + B)$ больше 0,5 (т.е. $H_3(D, 0{,}5) \geq 0{,}5$).

Рассмотрим индексы H_3 и H^1_5. Физическое содержание величины $H^1_5(A, B)$ - возможность того, что $\mathrm{pv}(A) \geq \mathrm{pv}(B)$; смысл величины $H_3(A, B)$ - вероятность того, что $\mathrm{py}(A) \geq \mathrm{pv}(B)$. Пусть

$$K = \{(a, b) : a \geq b,\ a \in S_A,\ b \in S_B\}.$$

С учетом определений рассматриваемых индексов и того, что значения функций принадлежности находятся на отрезке [0, 1], получаем

$$H_3(A, B) = \iint_K \mu_a \mu_b\,da\,db/C \leqslant$$

$$\leqslant \iint_K \min\{\mu_a, \mu_b\}\,da\,db/C \leqslant$$

$$\leqslant H^1_5(A, B) \iint_K da\,db/C.$$

Величину C можно представить в виде

$$C = \int_{a_1}^{a_2} \int_{b_1}^{b_2} \mu_a \mu_b\,dadb = \iint_{S_A \times S_B} \mu_a \mu_b\,dadb.$$

Отсюда

$$C \geqslant \iint_K \mu_a \mu_b\,dadb$$

и

$$H_3(A, B) \leqslant H^1_5(A, B)\left[\iint_K dadb / \iint_K \mu_a \mu_b\,dadb\right].$$

Нетрудно показать, что выражение в квадратных скобках не меньше единице, поэтому

$$H_3(A, B) \leqslant H^1{}_5(A, B)\,t,\ t \geqslant 1.$$

В ряде работ показано, что индекс H^1_5 выделяет в качестве наибольшего нечеткое число A, у которого величина

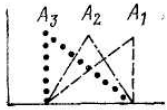
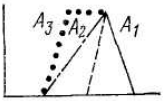
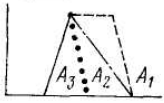
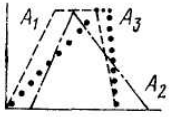
$$\sup \arg \sup_{x \in S_A} \mu_A(x)$$

является наибольшей (т.е. число, у которого конец «пика» функции принадлежности расположен правее). При этом форма функции принадлежности не учитывается, что снижает «розделяющую» способность индекса. Из вышеперечисленных индексов ранжирования форму функции принадлежности учитывают индексы H_2, H_3, H_4. Высказана гипотеза о том, что для простых функций принадлежности

эти индексы дают одинаковые ранжировки. Вычисление значений индексов ранжирования, которые проведены по программе на Фагол, дали результаты, которые представлено в табл. 1.13.

Таблица 1.13

Результаты ранжирования

Исходные данные (функции принадлежности нечетких чисел A_i)	i	Веса нечетких чисел A_i по индексам				
		H_1, H'_5	H_2 (ранги)	H_3	H_4	Болдуина — Гилда (линейный вариант) [93]
 I	1	1	1	0,53	0,887	0,43
	2	0,75	2	0,21	0,815	0,33
	3	0,6	3	0,06	0,733	0,3
 II	1	1	1	0,50	0,5	0,29
	2	1	1	0,50	0,5	0,29
 III	1	1	1	0,44	0,961	0,44
	2	1	2	0,23	0,749	0,33
	3	1	3	0,10	0,702	0,33
 IV	1	1	1	0,43	0,861	0,57
	2	1	2	0,24	0,835	0,44
	3	1	3	0,10	0,79	0,33
 V	1	1	1	0,52	0,816	0,33
	2	0,8	2	0,47	0,787	0,4
 VI	1	1	3	0,131	0,69	Нет результатов
	2	8/9	2	0,332	0,73	
	3	1	1	0,290	0,72	

Еще одна возможность ранжирования состоит в использовании обобщенных максимума и минимума. Для нечетких чисел A и B обобщенные максимум $\widetilde{\max}\{A, B\}$ и минимум $\widetilde{\min}\{A, B\}$ определяются функциями принадлежности $\mu_{\max}$ и $\mu_{\min}$ соответственно:

$$\mu_{\max}(z) = \sup_{\substack{\max\{a, b\}=z \\ a\in S_A,\ b\in S_B}} \min\{\mu_A(a),\ \mu_B(b)\};$$

$$\mu_{\min}(z) = \sup_{\substack{\min\{a, b\}=z \\ a\in S_A,\ b\in S_B}} \min\{\mu_A(a),\ \mu_B(b)\}. \qquad (1.73)$$

Тогда результат ранжирования — нечеткое число $\widetilde{\max}\{A, B\}$, которое в общем случае не совпадает ни с A ни с B. Выражения (1.73) получены по принципу обобщения из обычных определений максимума и минимума и могут быть распространены на случай n нечетких чисел.

Микромодуль 3.
Основные понятия и фундаментальные алгебры

1.11. Основные понятия

Алгеброй A называется совокупность < > множества M с заданными в нем операциями $S=\{f_{11},f_{12},...,f_{1n_1},f_{21}, f_{22},\ldots,f_{2n_2},\ldots,f_{m1},f_{m2},\ldots,f_{mn_m}\}$, $A=<(M,S)>$, где множество M — *носитель, S — сигнатура* алгебры. Первый нижний индекс у идентификатора операции указывает ее *местность.*

Замечание. Для идентификации единого целого, содержащего объекты, которые имеют различное математическое построение, например множества и операций в нем, было предложено использовать термин *совокупность* и обозначать его угловыми скобками < >.

Рассмотрим *фундаментальные алгебры.* Алгебра вида $<M, f_2>$ называется *группоидом.*

Если f_2 — операция типа умножения (×), то группоид называют *мультипликативным;* если f_2 — операция типа сложения (+), то *аддитивным.*

Пусть $A = \langle M, f_2 \rangle$ — группоид; обозначим операцию f_2 как $\llcorner$. Тогда элемент $e \in M$ называется *правым нейтральным элементом* группоида A, если для всякого $m \in M$ выполняется равенство $m \circ e = m$; элемент $e \in M$ группоида $A = \langle M, \circ \rangle$ называется *левым нейтральным элементом,* если для всех $m \in M$ выполняется равенство $e \circ m = m$. В этих определениях использовались выражения «все элементы», «всякий элемент». В дальнейшем для краткости вместо слов «все» или «всякий» будем использовать символ $\forall$ (перевернутая буква A — первая буква английского слова All— все). Если элемент e, $e \in M$, группоида $A = \langle M, \circ \rangle$ является одновременно левым и правым нейтральным элементом, то его называют *двусторонним нейтральным элементом* или просто *нейтральным элементом.* Никакой группоид не может иметь более одного нейтрального элемента. Действительно, если

$$m \circ e = e \circ m = m \text{ и } m \circ e — e' \circ m = m$$

справедливо для всех $m \in M$, то

$$e' = e' \circ e = e.$$

Если группоид $\langle M, \circ \rangle$ мультипликативный, то нейтральный элемент называется *единицей* и обозначается 1; если аддитивный, то нейтральный элемент называется *нулем* и обозначается 0.

Группоид $A = \langle M, \circ \rangle$ называется *идемпотентным,* если его сигнатура удовлетворяет закону идемпотентности

$$(\forall\ m \in M)(m \circ m = m).$$

Группоид $\langle M, \circ \rangle$, сигнатура которого удовлетворяет закону коммутативности

$$(\forall\ x, y \in M)(x \circ y = y \circ x),$$

называется *коммутативным* или *абелевым.* Группоид $\langle M, \circ \rangle$, в котором выполняется закон ассоциативности

$$(\forall\ x, y, z \in M)(x \circ (y \circ z) = (x \circ y) \circ z),$$

называется *ассоциативным* или *полугруппой.*

Полугруппа $\langle M, \circ \rangle$, в которой могут быть осуществлены обратные операции: для любых $a, b \in M$ каждое из уравнений $a \circ x = b$, $y \circ a = b$ обладает единственным решение, называется *группой.*

Проиллюстрируем понятие группы на примере *группы подстановок,* которая содержит шесть элементов. Группу подстановок исследовал выдающийся французский математик Галуа в связи с решением уравнений в радикалах.

Подстановкой n-й степени называется взаимно однозначное отображение множества из n элементов на себя.

Рассмотрим три элемента: x_1, x_2, x_3. Существует шесть перестановок из трех элементов: $x_1x_2x_3$, $x_2\ x_3x_1$, $x_1x_3x_2$, $x_3x_1x_2$, $x_2x_1x_3$, $x_3x_2x_1$. Запишем две перестановки из трех элементов одна под другой

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}.$$

Эта запись означает, что x_1 переходит в x_2, x_2 — в x_3, x_3 — в x_1.
Число возможных подстановок равно числу перестановок. Введем следующие обозначения для шести возможных подстановок:

$$a = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix},\ b = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix},\ c = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$$

$$d = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix},\ e = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix},\ f = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}.$$

Введем операцию умножения × над подстановками. *Произведением* подстановок называется подстановка, которая получается в результате последовательного выполнения сначала первой, а потом второй из перемноженных подстановок. Например,

$$c \times b = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \times \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} = e.$$

Выражение $\alpha\times\beta$, $\alpha, \beta = a, b, c, d, e, f$ определяет табл. 1.14.

Таблица 1.14

α	β					
	a	*b*	*c*	*d*	*e*	*f*
a	*a*	*b*	*c*	*d*	*e*	*f*
b	*b*	*a*	*d*	*c*	*f*	*e*
c	*c*	*e*	*a*	*f*	*b*	*d*
d	*d*	*f*	*b*	*e*	*a*	*c*
e	*e*	*c*	*f*	*a*	*d*	*b*
f	*f*	*d*	*e*	*b*	*c*	*a*

В рассмотренной алгебре $<M, \times>$ выполняется закон ассоциативности, но не выполняется закон коммутативности.

Алгебра $<M, \times, +>$, которая по умножению является мультипликативным группоидом, по сложению — абелевою группой, причем умножение связано со сложением законами *дистрибутивности*

$$a\times (b + c) = a\times b + a\times c,$$
$$(b + c) \times a = b\times a + c\times a,$$

называется *кольцом.* Кольцо, в котором все отличные от нуля элементы составляют группу по умножению, называется *телом.* Тело, у которого мультипликативная группа абелева, называется *полем.*

Рассмотрим *алгебру множеств (алгебру Кантора)*

$$A_k = \langle B(\mathbf{1}), \square, \cap, \bar{} \rangle,$$

носителем которой есть булеан универсального множества **1**, сигнатурой — операции объединения $\cup$, пересечения $\cap$ и дополнения $\bar{}$. Для операций алгебры Кантора выполняются следующие законы:

комутативности объединения и пересечения

$$M_a \cup M_b = M_b \cup M_a,\ M_a \cap M_b = M_b \cap M_a;$$

ассоциативности объединения и пересечения

$$M_a \cup (M_b \cup M_c) = (M_a \cup M_b) \cup M_c$$

$$M_a \cap (M_b \cap M_c) = (M_a \cap M_b) \cap M_c;$$

дистрибутивности пересечения относительно объединения и объединения относительно пересечения

$$Ma \cap (M_b \cup M_c) = M_a \cap M_b \cup M_a \cap M_c,$$

$$M_a \cup (M_b \cap M_c) = (M_a \cup M_b) \cap (M_a \cup M_c);$$

идемпотентности объединения и пересечения

$$M_a \cup M_a = M_a,\ M_a \cap M_a = M_a;$$

действия с универсальным **1** *и пустым* $\varnothing$ *множествами*

$$M \cup \varnothing = M,\ M \cap \varnothing = \varnothing,\ M \cup \mathbf{1} = \mathbf{1},\ M \cap \mathbf{1} = M,\ M \cup \bar{M} = \mathbf{1},$$

$$M \cap \bar{M} = \varnothing;$$

де-Моргана

$$\overline{M_a \cap M_b} = \bar{M}_a \cup \bar{M}_b,\ \overline{M_a \cup M_b} = \bar{M}_a \cap \bar{M}_b;$$

двойного дополнения

$$\bar{\bar{M}} = M.$$

Алгебра Кантора по аддитивной операции объединения и мультипликативной операции пересечения является абелевой полугруппой, так как для этих операций выполняются законы коммутативности и ассоциативности, но она не является группой, поскольку уравнения $M_a \cup X = M_b$, $M_a \cap X = M_b$ не имеют решения, например для случая, когда множества не пересекаются: $M_a \cap M_b = \varnothing$. Следовательно, алгебра Кантора по двуместным операциям $\cup$ и $\cap$ не является кольцом. Эта алгебра принадлежит к другому классу

фундаментальных алгебр - к классу *решеток*, который будет рассмотрен дальше.

1.12. Свойства бинарных алгебраических операций.

Для того чтобы следующие соотношения выглядели более привычно, условимся результат применения бинарной операции φ к элементам *a, b* записывать не в функциональном виде *φ(a, b),* а в виде *aφb,* так, как это принято для арифметических операций.

Операция φ называется *ассоциативной,* если для любых элементов *a, b, c*

$$(a\varphi b)\,\varphi c = a\varphi(b\varphi c).$$

Выполнение этого условия (свойства ассоциативности) означает, что скобки в выражении *aφbφc* можно не проставлять. Сложение и умножение чисел ассоциативны, что и позволяет не ставить скобки в выражениях *a+b+c* и *abc.* Пример неассоциативной операции — возведение в степень a^b: $(a^b)^c \neq a^{(b^c)}$ Правда, запись a^{b^c} считается допустимой, но служит сокращением выражения $a^{(b^c)}$ а не $(a^b)^c$, еоторое равно более компактному выражению ab^c.

Важным примером ассоциативной операции яаляется композиция отображений.

Операция φ называется *коммутативной,* если для любых элементов *a, b*

$$a\varphi b = b\varphi a.$$

Сложение коммутативно («от перемены мест слагаемых сумма не меняется»), равно как и умножение; вычитание и деление некоммутативны. Некоммутативным является умножение матриц, например

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\times\begin{pmatrix}2 & 2\\ 0 & 1\end{pmatrix}=\begin{pmatrix}2 & 3\\ 0 & 1\end{pmatrix},$$

но

$$\begin{pmatrix}2 & 2\\ 0 & 1\end{pmatrix}\times\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}2 & 4\\ 0 & 1\end{pmatrix}.$$

Операция φ называется *дистрибутивной слева* относительно операции ψ, если для любых *a, b, c*

$$a\varphi(b\psi c) = (a\varphi b)\psi(a\varphi c),$$

и *дистрибутивной справа* относительно ψ, если

$$(a\psi b)\varphi c = (a\varphi c)\psi(b\varphi c).$$

Дистрибутивность позволяет раскрывать скобки. Например, умножение дистрибутивно относительно сложения слева и справа. Возведение в степень дистрибутивно относительно умножения справа: $(ab)^c=a^cb^c$, но не слева: $a^{bc}\neq a^b a^c$. Сложение не дистрибутивно относительно умножения: $a+bc\neq(a+b)(a+c)$. Операции пересечения и объединения множеств дистрибутивны относительно друг друга слева и справа.

Гомоморфизм и изоморфизм. Алгебры с различными типами, очевидно, имеют существенным образом разное строение. Если же алгебры имеют одинаковый тип, то наличие в них сходства характеризуется с помощью понятий гомоморфизма, которые вводятся ниже, и изоморфизма.

Пусть дано две алгебры $A=(K;\ \varphi_1, \ldots, \varphi_p)$ и $B=(M;\ \psi_1, \ldots, \psi_p)$ одинакового типа.

Гомоморфизмом алгебры A в алгебру B называется отображение Γ: $K\rightarrow M$, которое удовлетворяет условию

$$\Gamma(\varphi_i(k_{j_1} \ldots .. k_{j_{l(i)}}))=\psi_i(\Gamma(k_{j_1}),\ldots,\Gamma(k_{j_{l(i)}})) \qquad (1.74)$$

для всех $i= 1, \ldots, p$ [$l(i)$ — арность операций φ_u и ψ_i, которая в них по условию одинакова] и всех $k_{j_r} \in K$. Смысл условия (1.74) в том, что, независимо от того, выполнена ли сначала операция φ_i в A и потом выполнено отображения Γ, или сначала выполнено отображения Γ, а затем в B выполнена соответствующая операция ψ_i, результат будет одинаков.

Изоморфизмом алгебры A на алгебру B называется взаимооднозначный гомоморфизм. В этом случае существует обратное отображение Γ^{-1}:$M\rightarrow K$, которое является также взаимооднозначным. Пусть $\Gamma(k_i)= m_i,\ m_i\in M$. Тогда $k_i = \Gamma^{-1}m_i$. Заменим в условии (1.74) левые части этих равенств на правые и применим Γ^{-1} к обеим частям равенства, которые получены. Так как $\Gamma^{-1}\Gamma$ является тождественным отображением: $\Gamma^{-1}\Gamma(a) = a$, то получим:

$$\varphi_u(\Gamma^{-1}(m_{i_1}).....\Gamma^{-1}(m_{i_{l(i)}})=\Gamma^{-1}\psi_i(m_{i_1},\ldots,m_{i_{l(i)}})) \qquad (1.75)$$

Равенство (1.75) — это то же равенство (1.74) с заменой Γ на Γ^{-1}, элементов K на элементы M и переменной мест φ_i и ψ_i; другими словами, Γ^{-1} — это изоморфизм B на A. Следовательно, если существует изоморфизм A на B, то существует изоморфизм B на A; при этом алгебры A и B называются *изоморфными*. Мощности основных

множеств изоморфных алгебр равны (при гомоморфизме это равенство может не выполняться). Если $A = B$, то изоморфизм называется изоморфизмом на себя, или автоморфизмом; если $B \subset A$, то изоморфизм называется изоморфизмом в себя.

Отношение изоморфизма является отношением эквивалентности на множестве алгебр. Рефлексивность его очевидна, симметричность следует из существования обратного изоморфизма, а транзитивность устанавливается следующим образом: если Γ_1 — изоморфизм A на B, Γ_2 — изоморфизм B на C, то изоморфизмом A на C будет композиция Γ_1 и Γ_2. Классами эквивалентности в разбиении относительно изоморфизма есть классы изоморфных между собой алгебр.

Понятие изоморфизма является одним из важнейших понятий в математике. Его сущность можно выразить следующим образом: если алгебры A и B изоморфны, то элементы и операции B можно переименовать так, что B совпадет с A. Из условия (1.74) изоморфизма следует, что любое эквивалентное соотношение в алгебре A сохраняется в любой изоморфной ей алгебре A'. Это позволяет, получив такие соотношения в алгебре A, автоматически распространить их на все алгебры, которые изоморфны A. Распространенное в математике выражение «рассматривать объекты с точностью до изоморфизма» означает, что рассматриваются только те свойства объектов, которые сохраняются при изоморфизме, т.е. являются общими для всех изоморфных объектов. В частности, изоморфизм сохраняет ассоциативность, коммутативность и дистрибутивность.

1.13. Основные определения полугрупп и групп

Полугруппы. Напомним некоторые определения. *Полугруппой* называется алгебра с одной ассоциативной бинарной операцией. Эта операция обычно называется умножением, поэтому результат ее применение к элементам a и b записывается как $a \cdot b$ или ab. Такая запись называется мультипликативной. В частности, aa принято записывать как a^2, aaa как a^3 и т.д. В общем случае $ab \neq ba$. Если же умножение коммутативно, то полугруппа называется коммутативной, или абелевой. Если полугруппа содержит такой элемент e, что для любого a $ae=ea=a$, то e называется *единицей*. Полугруппа с единицей называется *моноидом*. Единица в полугруппе всегда единственна. Действительно, если есть две единицы e_1 и e_2, то $e_1e_2 = e_1$ и $e_1e_2 = e_2$ итак, $e_1 = e_2$.

Композиция отображений является ассоциативной операцией. Поэтому всякое множество преобразований (отображений некоторого множества у себя), замкнутое относительно композиции, является полугруппой. Рассмотрим пример. Пусть на множестве {1, 2, 3} заданы преобразования

$$\alpha = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,2 \end{pmatrix} \text{ и } \beta = \begin{pmatrix} 1\,2\,3 \\ 3\,3\,2 \end{pmatrix}$$

Их произведения имеют вид

$$\alpha\beta = \begin{pmatrix} 1\,2\,3 \\ 3\,3\,3 \end{pmatrix} \text{ и } \beta\alpha = \begin{pmatrix} 1\,2\,3 \\ 2\,2\,2 \end{pmatrix}$$

Т.е., не совпадают с α и β. Поэтому множество { α, β } не замкнуто относительно композиции и не образует полугруппы. Однако если к нему прибавить преобразования

$$\gamma = \beta^2 = \begin{pmatrix} 1\,2\,3 \\ 2\,2\,3 \end{pmatrix}, \ \delta = \alpha\beta \text{ и } \zeta = \beta\alpha ,$$

то можно убедиться, что получено множество Г={ α, β, γ, δ, ζ} вместе с операцией композиции образует полугруппу. Таблица Кели этой полугруппы имеет вид:

Таблица 1.15

	α	β	γ	δ	ζ
α	α	δ	ζ	δ	ζ
β	ζ	γ	β	δ	δ
γ	ζ	δ	γ	δ	δ
δ	ζ	ζ	ζ	δ	δ
ζ	ζ	ζ	ζ	δ	δ

Если же к Г прибавить тождественное отображение

$$\varepsilon = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix},$$

получим полугруппу с единицей.

Теорема 1. Любая полугруппа с единицей изоморфна некоторой полугруппе преобразований.

Действительно, пусть задана полугруппа с множеством $M=\{e, a_1, a_2 ...\}$. Каждому элементу a_i полугруппы поставим в соответствие преобразования f_i множества M следующим образом: $f_i(x)=xa_i$ для всех $x \in M$. Тогда произведению $a_i a_j$ будет соответствовать преобразование

$$f_{ij}(x)=xa_ia_j= f_i(x)a_j= f_j(f_i(x)),$$

т.е. композиция преобразований a_j и f_j; следовательно, условие (1.74) гомоморфизма выполнено. Кроме того, разным элементам M соответствуют разные отображения, так как $f_i(e)=a_i$, $f_i(e)=a_j$ и, следовательно, $f_i \neq f_j$. Таким образом, соответствие $a_i \rightarrow f_i(x)$ является изоморфизмом.

Если любой элемент полугруппы $P(M, \sqsubset)$ можно представить как произведение некоторого числа элементов множества $M_0 \subset M$, то множество M_0 называется порождающим множеством, или *системой, образующих* полугруппы P, а его элементы *называются образующими.* В нашем примере образующими являются α и β, так как $\gamma = \beta^2$, $\delta = \alpha\beta$, $\zeta = \beta\alpha$. В полугруппе $(N; \bullet)$ порождающим множеством, служит бесконечное множество простых чисел. Если полугруппа имеет только одну образующую, то все элементы являются степенями этой образующей. Такая полугруппа называется *циклической.* Циклической полугруппой является, например, полугруппа $(N; +)$, так как ***все натуральные числа — это суммы некоторого количества единиц.*** Пусть полугруппа P имеет конечное множество образующих $\{a_1, ..., a_n\}$. Если обозначения операции опустить (как это обычно делается для умножения), то все элементы P можно рассматривать как слова в алфавите $\{a_1,...,a_n\}$. Некоторые различные слова могут оказаться равными как элементы. В нашем примере полугруппы преобразований выполняются, например, равенства $\beta^3=\beta$, $\beta\alpha=\alpha\beta^2$. В коммутативной полугруппе для любых элементов a, b выполняются равенства $ab=ba$. Такие равенства называются *определяющими соотношениями.* Если же в полугруппе нет определяющих соотношений, т.е. любые два различных слова являются различными элементами полугруппы, то полугруппа называется *свободной.*

Всякую полугруппу можно получить из свободной полугруппы введением некоторых определяющих соотношений. Элементы заданной так полугруппы - это слова в алфавите образующих, причем некоторые слова равны (т.е. задают один и тот же элемент) в силу определяющих соотношений. Отношение равенства слов является отношением эквивалентности. Из любого слова, используя определяющие соотношения, легко можно получить различные эквивалентные ему слова. Намного более сложна такая проблема: для двух данных слов выяснить, можно ли получить одно из другого,

используя определяющие соотношения. Ее исследование повлияло на теорию алгоритмов. Более точная постановка этой проблемы будет рассмотрена в пособии „Дискретна математика. Теория алгоритмов".

Группы. *Группой* называется полугруппа с единицей, в которой для каждого элемента a существует элемент a^{-1}, который называют *обратным* к a и удовлетворяющий условию $aa^{-1}=a^{-1}a=e$. Число элементов группы называется порядком группы. Группа, в которой операция коммутативна, называется коммутативной, или абелевой. Группа, все элементы которой явдяются степенями одного элемента a, называется циклической. Циклическая группа всегда абелева. Для абелевых групп часто употребляется аддитивная запись: операция обозначается как сложение, а единица обозначается 0.

В любой конечной группе ее операция (умножение) может быть задана таблицей Кели. Для групп таблица Кели имеет важную особенность: любой ее столбец содержит все элементы группы. Действительно, если столбец a_i не содержит какого-нибудь элемента, то некоторый другой элемент a_j в нем должен встретиться дважды, скажем, в k-й и l-й строках. Но тогда $a_ka_i=a_j$, $a_la_i=a_j$ и, следовательно, $a_ka_i=a_la_i$. Умножая обе части равенства на a_i^{-1}, получаем $a_k=a_l$, что неверно. Таким образом, i-й столбец таблицы Кели, т.е. умножение на a_i, является подстановкой на множестве элементов группы. Проверив, что это соответствие является изоморфизмом (аналогичную проверку мы делали для полугрупп преобразований), получаем теорему Кели.

Теорема 2. Любая конечная группа изоморфна группе подстановок на множестве ее элементов.

Из сравнения теорем о связи полугрупп с преобразованиями и групп с подстановками видно, что ***группа — это полугруппа взаимнооднозначных преобразований***, причем именно взаимная однозначность гарантирует наличие обратного преобразования. Можно сказать, что в группе при любом числе умножений не теряется информация об исходном элементе: если известно, на что умножали, всегда можно узнать, что̀ умножали. Для полугруппы это верно не всегда. Используя терминологию дискретных систем (например, конечных автоматов, о которых будет идти речь в пособии „Дискретная математика. Автоматы"), то же самое можно сказать следующим образом. Пусть имеется дискретная система с конечным числом состояний $S = \{s_1, ..., s_n\}$, на вход которой может быть подано входное воздействие из множества $\{x_1 ..., x_m\}$. Всякое входное воздействие однозначно переводит состояние системы в некоторое другое состояние и, следовательно, является преобразованием множества S. Последовательности воздействие — это композиции

преобразований; следовательно, множество всех последовательностей является полугруппой с образующими $\{x_1, .,., x_m\}$. Если такая полугруппа оказывается группой, то это означает, что по любой входной последовательности и заключительному состоянию системы можно однозначно определить начальное состояние системы.

1.14. Алгебраичные системы

1.14.1. Законы композиции

1. Композиция объектов. В математике и ее приложениях большое значение имеют отношение, которые ставят в соответствие пары каких-либо объектов *(a, b)* третий объект *c*. Примерами таких отношений являются действия над числами. В общем случае отношение может представлять собой некоторую *операцию* не только между числами, но и между объектами любой природы. При этом запись $a \bullet b=c$, или $a \perp b=c$, означает, что *a* в композиции с *b* дает *c*. Символ $\bullet$ (или $\perp$) обозначает операцию, объекты *a* и *b* *называют операндами,* а объект *c* - *результатом операции* или *композицией объектов a* и *b.*

Обозначим множества операндов соответственно через *A* и *B* ($a \in A$ и $b \in B$), а множества результатов операции — через *C* ($c \in C$). Так как множество всех пар (*a*, *b*) есть прямое произведение $A \times B$, то операцию определяют как отображение множества $A \times B$ в *C*, т.е. $A \times B \rightarrow C$, и часто называют *законом композиции,*

2. Таблица Кели. Любой закон композиции $A \times B \rightarrow C$ над конечными множествами можно задавать прямоугольной матрицей *(таблицей Кели).* Строки таблицы отвечают элементам множества *A,* столбцы — элементам множества *B.* На пересечении строки и столбца, соответствующих паре (*a*, *b*), располагается элемент $c=a \bullet b$.

Хорошо известными примерами являются таблицы сложения и умножение одноразрядных чисел. В общем случае таблица, которая определяет бинарную операцию, имеет вид:

$\top$	b_1	b_2	b_3	b_4	b_5	...
a_1	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	...
a_2	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	...
a_3	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}	...
a_4	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	...
...	...	...	...	...	...	...

Законы композиции на множестве. Множества *A, B, C,* которые принимают участие в операции $A \times B \rightarrow C$, не обязательно должны быть различными. Если $B=C=S$, то говорят, что закон композиции *определен на множестве S.*

Различают *внутренний* закон композиции $S \times S \rightarrow S$ и *внешний* закон композиции $\Omega \times S \rightarrow S$, где Ω и S — различные множества. В случае внутреннего закона говорят, что множество образует *групоид* относительно операции $\top$. В случае внешнего закона композиции элементы $\alpha \in \Omega$ называют *операторами,* а Ω — *множеством операторов* на множестве *S.*

Примерами внутреннего закона композиции являются сложение $a+b=c$ и умножение $ab=c$ на множестве действительных чисел, а также геометрическое суммирование векторов на плоскости. Умножение вектора на скаляр может быть примером внешнего закона композиции на множестве векторов, причем операторами являются скаляры — элементы множества действительных чисел.

Пусть S — множество диференцируемых функций $f_i(x_1, x_2, ... x_n)$ и Ω - множество операторов дифференцирования $\partial/\partial x_j$ $(j = 1, 2, ..., n)$. Тогда паре $(\partial/\partial x_j, f_i)$ можно поставить в соответствие частную производную df_i/dx_j, т.е. имеем внешний закон композиции на множестве диференцируемых функций.

Ниже речь будет идти о внутренних законах композиции.

Матрица и граф группоида. Конечный группоид S относительно закона $\top$ определяется квадратной матрицей n-го порядка *(n* — число элементов группоида), например,

$\top$	a	b	c	d
a	b	c	a	b
b	a	b	c	a
c	b	a	d	d
d	d	b	d	b

Построение графа группоида основано на представлении бинарного соотношения $a \bullet b=c$ (рис. 1.31 *а),* где дуги графа изображают элементы $a, b, c \in S$, причем операнды образуют некоторый путь, а дуга результата операции замыкает этот путь. Если $a \bullet b=a$, то b изображается петлей в конечной вершине дуги a. При построении графа сначала наносят дуги для всех элементов группоида как выходяшие из одной вершины, а затем последовательно изображают все бинарные соотношения.

На рис. 1.31, *бы* изображен граф группоида, заданного приведенной выше матрицей.

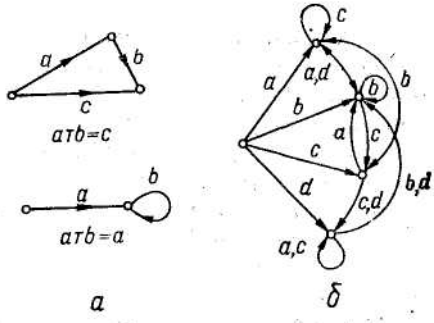


Рис. 1.31. Граф операции на множестве:
а - операнды *a, b* и результат операции *c; б* — граф группоида

Дуги *a, b, c, d,* выходящие из одной вершины, соответствуют элементам группоида. Так как $a \bullet a = b$, $a \bullet b=c$, $a \bullet c = a$ и $a \bullet d=b$, то из конца дуги *a* проводят дуги *a, b, c, d* соответственно к

конечным вершинам дуг *b, c a, b*. Две параллельные дуги *a* и *d,* направленные к конечной вершине дуги *b*, условно изображают одной дугой *a, d.* Дуга *c* начинается и заканчивается в конечной вершине дуги *a,* т.е. образует петлю. Аналогично изображают на графе и остальные соотношения, определяемые матрицей группоида.

Свойства внутреннего закона композиции. Операции на множестве *S* могут обладать некоторыми общими свойствами, которые обычно выражаются соотношениями между элементами с *S*:

коммутативность $a \top b = b \top a$;

ассоциативность $a \top (b \top c) = (a \top b) \top c$;

дистрибутивность слева $(a \top b) \perp c = (a \perp c) \top (b \perp c)$

и справа $c \perp (a \top b) = (c \perp a) \top (c \perp b)$.

На множестве действительных чисел сложение и умножение ассоциативны и коммутативны. Умножение дистрибутивно (слева и справа) относительно сложения, но сложение не дистрибутивно относительно умножения, так как вообще $a + bc \neq (a + b)(a+c)$.

Возведение в степень не ассоциативно $(a^b)^c \neq a^{(b^c)}$, не коммутативно $a^b \neq b^a$, но дистрибутивно справа относительно умножения, так как $(ab)^c = a^c b^c$.

Пересечение и объединение множеств взаимно дистрибутивны относительно друг друга. Если в множестве $F \subset S$ композиция любых двух элементов из *F* также принадлежит *F,* то *F* называется *замкнутым* относительно рассматриваемого закона композиции (подмножество четных чисел является замкнутым относительно сложения и умножения).

Регулярный, нейтральный и симметричный элементы. Закон композиции наделяет элементы множества некоторыми общими свойствами. При различных законах одни и те же элементы могут обладать различными свойствами. Поэтому имеет смысл говорить о свойствах элементов множества *S* относительно заданного на нем закона композиции $\top$.

Элемент *a* называется *регулярным,* если из соотношений $a \top x = a \top y$ и $x \top a = y$ следует $x = y$ *(сокращение* на регулярный элемент). Всякое число регулярно относительно сложения, а для умножения ь регулярно всякое число, кроме нуля *(*$0x = 0y$ не влечет $x = y$*).*

Нейтральным элементом $e \in S$ называют такой элемент, что для всех элементов *x* из *S* справедливо $e \top x = x \top e = x$ (если нейтральный элемент существует, то он единственен и регулярный). Среди чисел нуль — нейтральный элемент относительно сложения, а единица — относительно умножения. Пустое множество является нейтральным

элементом относительно объединения, а основное множество (универсум) — относительно пересечения. На множестве всех квадратных матриц *n*-го порядка с числовыми элементами нулевая и единичная матрицы служат соответственно нейтральными элементами относительно сложения и умножения.

Если множество содержит нейтральный элемент *e* относительно закона композиции $\top$, то элемент *b* называется *симметричным (обратным, противоположным)* элементу *a,* если $a \top b = b \top a = e$; при этом *a* называют *симметризуемым* элементом и *b* обозначается через $\overline{a}$, т.е. $b = \overline{a}$. Относительно ассоциативного закона $\top$ элемент $\overline{a}$, симметричный элементу *a* (если он существует), единственен и регулярен.

При сложении симметричным некоторому числу *x* будет *-x,* а при умножении x^{-1}. Например, симметричными элементами на множестве квадратных матриц *n*-го порядка относительно умножения есть взаимо-обратные матрицы. Множество всех собственных подмножеств относительно объединения или пересечение не содержит симметричных элементов. Множество, в котором всякий элемент имеет симметричный, называется *симетризуемоюым.*

Аддитивнные и мультипликативные обозначения. Свойства законов композиции можно представить в двух формах. В аддитивных обозначениях операция $\top$ записывается символом сложения (+), а в мультипликативных — символом умножения (•). Если множество наделено двумя законами композиции, то чаще всего первый из них $\top$ считается *аддитивным,* а второй $\perp$ — *мультипликативным.* В аддитивной записи нейтральный элемент обозначается через 0 и называется *нулем,* а симметричный элементу *a* — через (*-a*). В мультипликативной записи нейтральный элемент обозначается через 1 и называется *единицей,* а симметричный элементу *a* — через a^{-1}.

Если закон композиции ассоциативный и коммутативный, а элементы множества $x_1, x_2, ..., x_n \in S$ отмечены *операторным индексом* i, то в аддитивной записи

$$x_1 + x_2 + \ldots + x_n = \sum_{i=1}^{n} x_i$$

и в мультипликативной записи

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i \ .$$

Следует подчеркнуть, что здесь, в отличие от элементарной алгебры, знаки (+) и (•) не обязательно означают сложение и умножение чисел. Они просто заменяют в различных соотношениях символы $\top$ и $\perp$, указывая на то, что над элементами множества (не обязательно числами) выполняются некоторые операции. Эти операции могут лишь извне напоминать обычные операции сложения или умножение чисел, но по существу в общем случае — это другие операции. Удобство аддитивных и мультипликативных обозначений заключается в том, что при операциях над числами разлияные соотношения совпадают с общепринятой формой записи.

До сих пор рассматривались алгебры, т.е. множества, на которых заданы операции. Множества, на которых кроме операций заданы отношения, называются *алгебраическими системами*. Таким образом, алгебры можно считать частным случаем алгебраических систем (в которых множество отношений пусто). Другим частным случаем алгебраических систем являются ***модели — множества, на которых заданы только отношения***. Понятие изоморфизма для алгебраических систем вводится аналогично тому, как это было сделано ранее для алгебр, с той разницей, что к условию

$$\Gamma\left(\varphi_i\left(k_{j_1}, \ldots, k_{j_{l(i)}}\right)\right) = \psi_i\left(\Gamma\left(k_{j_1}\right), \ldots, \Gamma\left(k_{j_{l(i)}}\right)\right)$$

сохранения операций добавляется условие сохранения отношений при изоморфизме.

В таблице 1.16 приведены наиболее употребительные системы, где звездочка (*) показывает, что данный закон обладает отмеченными свойствами, и множество содержит относительно этого закона соответствующие элементы.

Таблица 1.16

Алгебраические системы (модели)

Название алгебраических систем	Первый закон (аддитивный)				Второй закон (мультипликативный)			
	Свойства		Элементы		Свойства		Элементы	
	Ассоциативность	Коммутативность	Нейтральный	Симметричный	Ассоциативность	Коммутативность	Нейтральный	Симметричный
Полугруппа (моноид)	*							
Абелева (коммутативная)	*	*						

полу-группа								
Полу-группа с нулем (единицей)	*		*					
Абелева полу-группа с нулем (едини-цей)	*	*	*					
Группа	*		*	*				
Абелева (коммута-тивная) группа	*	*	*	*				
Асоциа-тивное кольцо	*	*	*	*	*			
Абелево (коммута-тивное) кольцо	*	*	*	*	*	*		
Кольцо с едини-цей (унитар-ное кольцо)	*	*	*	*	*		*	
Абелево кольцо с едини-цей	*	*	*	*	*	*	*	
Тело	*	*	*	*	*		*	*
Поле (коммута-тивное тело)	*	*	*	*	*	*	*	*

Примечание: 1. Второй закон композиции (если он определен) является дистрибутивным слева и справа относительно первого закона.
2. Симметричные элементы относительно второго закона определены для всех элементов, кроме нейтрального относительно первого закона (нуля).

Так, *группа* — это наделенное ассоциативным законом множество, содержащее нейтральный элемент и симметризуемое относительно этого закона. Если, кроме того, закон композиции коммутативный, то группу называют *абелевой (коммутативной).*

Во всякой группе соотношения (уравнения) $a \top x = b$ и $y \top a = b$ допускают единственное решение $x = \bar{a} \top b$ *(частное справа)* и $y = b \top \bar{a}$ *(частное слева).* Имеет место также соотношение $\overline{(a \top b)} = \bar{b} \top \bar{a}$ или $-(a+b) = -b-a$ (в аддитивной записи) и $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ (в мультипликативной записи).

Кольцо — это множество, которое наделено двумя законами композиции: относительно первого (аддитивного) оно образует абелеву группу, а второй закон (мультипликативный) является ассоциативным, а также дистрибутивным относительно первого закона.

Телом называют кольцо с единицей, в котором каждый отличный от нуля элемент обладает симметричным относительно второго (мультипликативного) закона.

Поле — это коммутативное тело.

Изучение алгебраических систем позволяет выявить общие свойства операций на множестве объектов различной природы. Эти свойства используются при решении многих научных и технических задач. Из приведенных алгебраических систем наиболее широкими понятиями являются моноид и группа, а наиболее узкими - тело и поле. Последние обслуживают в основному числовые множества, в то время как более широкие понятия распространяются и на более далекие от чисел совокупности объектов.

Подсистемы. Всякую часть системы, которая снова является системой относительно тех же законов, называют *подсистемой.* В частности, всякая *подгруппа* должна содержать нейтральный элемент группы. *Подкольцо* образует подгруппу адитивной группы кольца и замкнуто относительно мультипликативного закона.

Подкольцо I абелева кольца K называется *идеалом* (в этом кольце), если I есть аддитивная подгруппа кольца (композиция любых элементов a и b из I относительно первого закона также принадлежат I, т.е. $a + b \in I$ и $a - b \in I$), и в результате применения к элементу из I и любому элементу из K второго закона получаем элемент из I (т.е. для любых $a \in I$ и $x \in K$ имеет место $a \cdot x \in I$). Например, множество четных чисел есть идеал в кольце целых чисел, который рассматривается как аддитивная группа, а вторым законом является

операция умножения (произведение четного числа на любое целое число дает четное число).

1.15. Примеры алгебраических систем

1. Кольцо многочленов. Рассмотрим множество *многочленов (полиномов)* от переменной x над числовым полем P, т.е. выражение вида

$$f(x)=a_0 + a_1x + ... + a_nx^n,$$

где n — целое неотрицательное число, а *коэффициенты* многочлена $a_0, a_1, ..., a_n$ — числа из поля P (действительные или комплексные). Наибольшее число n, при котором $a_n \neq 0$, называется *степенью многочлена* и обозначается $\deg f(x)$. Два многочлена

$$f(x) =a_0 + a_1x+ ... + a_nx^n$$

и

$$g(x) = b_0 + b_1x + ... + b_mx^m$$

тождественно равны, если $n=m$ и $a_i= b_i$ $(i = 1, 2, ..., n)$.

Определим на множестве многочленов два внутренних закона - аддитивный и мультипликативный.

Сумма двух многочленов $f(x)+g(x)$ — это многочлен, у которого коэффициент при каждой степени переменного x равен сумме коэффициентов многочленов $f(x)$ и $g(x)$ при той же степени x. Если степени n и m многочленов слагаемых не равны, то многочлен меньшей степени дополняется до старшей степени членами с нулевими коэффициентами. При этом

$$\deg[f(x) + g(x)] \leq \max[\deg f(x), (\deg g(x)].$$

Например:

$$f(x) = 2x^3 + 3x^2 — x + 6;$$
$$g(x) = x^2 — 1;$$
$$f(x) + g(x)= 2x^3 + 4x^2 — x + 5.$$

Операция сложения многочленов ассоциативна и коммутативна. Нейтральным элементом относительно сложения является многочлен, все коэффициенты которого нули. Всякий многочлен $f(x)$ обладает симметричным ему, все коэффициенты которого противоположны коэффициентам $f(x)$, т.е. $f(x)= —f(x)$. Следовательно, множество многочленов является абелевой группой относительно сложения.

Произведение двух многочленов определяется как многочлен $f(x)g(x)$, который получают умножением каждого члена многочлена $f(x)$ на каждый член многочлена $g(x)$, суммированием полученных произведений и приведением подобных членов. Очевидно,

$$\deg[f(x)g(x)] \le \deg f(x) + \deg g(x).$$

Например:

$$f(x) = x^2 - 3x + 2;$$
$$g(x) = x^2 + 2x - 3;$$
$$f(x)g(x) = x^4 + 2x^3 - 3x^2 - 3x^3 - 6x^2 + 9x + 2x^2 + 4x - 6 =$$
$$= x^4 - x^3 - 7x^2 + 13x - 6.$$

Операция умножения многочленов ассоциативна, коммутативна и дистрибутивна относительно сложения. Нейтральным элементом относительно умножения служит многочлен, у которого $a_0 = 1$, а все другие коэффициенты равны нулю.

Таким образом, множество многочленов является коммутативным кольцом. Это кольцо также унитарное (кольцо с единицей). Можно показать, что множество многочленов не имеет делителей нуля, следовательно, она есть кольцо целостности.

Любой многочлен можно единственным образом представить в виде:

$$f(x) = g(x)\,q(x) + r(x),$$

где $q(x)$ — *частное* от деления $f(x)$ на $g(x)$ (по убывающим степеням) и $r(x)$ — *остаток*. При этом $\deg r(x) < \deg g(x)$, а также если $\deg f(x) \ge \deg g(x)$, то $\deg q(x) = \deg f(x) - \deg g(x)$.

2. Нули многочлена. Число λ называют *нулем многочлена* $f(x)$, если $f(\lambda)=0$. Говорят также, что λ есть *корень уравнения* $f(x)=0$.

Для того чтобы λ был нулем многочлена $f(x)$, необходимо и достаточно, чтобы этот многочлен делился без остатка на $x-\lambda$. Если многочлен $f(x)$ делится без остатка на $(x-\lambda)^s$, где s — наибольшее натуральное число, для которого такое деление возможно, то λ называется нулем *кратности* s. Нуль кратности единица называется *простым*.

Основная теорема алгебры утверждает, что многочлен n-й степени с действительными или комплексными коэффициентами имеет не меньше одного и не больше n *различных* действительных или комплексных нулей. С учетом кратности корней их общее число всегда равно n.

Пусть $\lambda_1, \lambda_2, \ldots, \lambda_k$ — нули многочлена степени n, а $s_1, s_2, \ldots, s_k$ — их кратности. Тогда многочлен можно с точностью до постоянной представить в виде:

$$f(x) = (x-\lambda_1)^{s_1}\,(x-\lambda_2)^{s_2}\,\ldots\,(x-\lambda_k)^{s_k}\ .$$

Если λ_i — нуль кратности s_i, то дифференцируя $f(x)$ s_i раз, убеждаемся, что

$$f(\lambda_i) = f'(\lambda_i) = \ldots = f^{(s_i-1)}(\lambda_i) = 0,$$

но

$$f^{(s_i)}(\lambda_i) \neq 0.$$

Например:

$$f(x) = x^5 + x^4 - 5x^3 - x^2 + 8x - 4 = (x - 1)^3 (x + 2)^2;$$

$$f(1) = f'(1) = f''(1) = 0,$$

но

$$f'''(1) = 54.$$

Имеется большое количество методов определения нулей многочленов, а также различных теорем, определяющих их расположение в поле комплексных чисел. Основные трудности решения этой задачи связаны с тем, что алгебраические уравнения $f(x)=0$ неразрешимы в радикалах, если степень многочлена высший четвертой. Эти трудности преодолеваются применением приближенных методов вычисления.

3. Кольцо множеств. Непустая система множеств образует кольцо множеств, если для любых A и B этой системы $A + B$ и $A \cap B$ также принадлежат к этой системе множеств. Здесь определено два внутренних закона композиции: дизъюнктивная сумма и пересечение. Нейтральным элементом относительно суммы служит пустое множество $\varnothing$, так как $A + \varnothing = A$. Симметричным для каждого A является само это множество, так как $A + A = \varnothing$.

Второй закон - ассоциативный

$$A \cap (B \cap C) = (A \cap B) \cap C$$

и дистрибутивный относительно первого, т.е.

$$A \cap (B + C) = (A \cap B) + (A \cap C).$$

Нейтральный элемент (единица) U относительно второго закона (пересечения) определяется соотношением $A \cap U = A$, откуда следует, что U есть не что иное, как максимальное множество этой системы, которая содержит все другие входящие в систему множества (универсум U). Если такой элемент существует, то имеем кольцо с единицей (унитарное кольцо). Так, унитарное кольцо образует система всех подмножеств произвольного множества V. Примером кольца (без единицы) может служить множество всех ограниченных отрезков числовой прямой (не существует ограниченного отрезка, который служил бы единицей кольца, т.е. содержал все ограниченные отрезки прямой).

Так как для любых A и B справедливы соотношения:

$$A \cup B = (A + B) + (A \cap B)$$

и

$$A \setminus B = A + (A \square B),$$

это кольцо множеств содержит также $A \cap B$ и $A \setminus B$. Говорят, что кольцо замкнуто относительно объединения и пересечение, разности и дизъюнктивной суммы.

4. Тело кватернионов. Первой системой на пути обобщения комплексных чисел появились *кватернионы*, т.е. выражения вида

$$x = a + bi + cj + dk,$$

где a, b, c, d — действительные числа, а символы i, j, k также называют кватернионами (например, j — это кватернион при $a=b=d=0$ и $c = 1$). Число a — *действительная часть,* а сумма $bi+cj+dk$ — *векторная часть* кватерниона.

На множестве кватернионов определяют два внутренних закона. Аддитивный закон задается подобно сложению комплексных чисел, т.е. сумма

$$x_1 = a_1 + b_1 i + c_1 j + d_1 k$$

и

$$x_2 = a_2 + b_2 i + c_2 j + d_2 k$$

есть

$$x_1 + x_1 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Очевидно, этот закон ассоциативный и коммутативный. Нейтральным элементом относительно сложения служит

$$0 = 0 + 0i + 0j + 0k,$$

а симметричным к элементу x есть элемент

$$-x = -a_1 - b_1 i - c_1 j - d_1 k = \bar{x} \ .$$

Чтобы множество кватернионов была телом, мультипликативный закон (умножение кватернионов) должен быть ассоциативным и дистрибутивным относительно сложения. Это достигается, с одной стороны, определением мультипликативного закона подобно умножению многочленных алгебраических выражений и, с другой стороны, заданиям правила умножения кватернионов, которое в наиболее лаконичной записи имеет вид:

$$i^2 = j^2 = k^2 = ijk = -1,$$

где порядок сомножителей в произведении ijk строго фиксирован. Отсюда также следует

$$ij = -ji = k; \quad jk = -kj = i; \quad ki = -ik = j.$$

Действительно, умножая справа на k обе части равенства $ijk = -1$, имеем $ijk^2 = -k$ или $ij = k$. Умножая полученное уравнение на j справа или на i слева, получаем соответственно $-i = kj$ или $-j = ik$ и т.д.

Как видно, мультипликативный закон (умножение кватернионов) не коммутативный, т.е.

$x_1x_2 = (a_1 + b_1i + c_1j + d_1k)(a_2 + b_2i + c_2j + d_2k) = a_1a_2 + a_1b_2i +$
$+ a_1c_2j + a_1d_2k + b_1a_2i + b_1b_2i^2 + b_1c_2ij + b_1d_2ik + c_1a_2j + c_1b_2ji +$
$+ c_1c_2j^2 + c_1d_2jk + d_1a_2k + d_1b_2ki + d_1k_2j + d_1d_2k^2 =$
$=(a_1a_2 — b_1b_2 — c_1c_2 — d_2d_2) + (a_1b_2 + b_1a_2 + c_1d_2 — d_1c_2)i +$
$+(a_1c_2 + c_1a_2 — b_1d_2 + d_1b_2)j + (a_1d_2 + d_1a_2 + b_1c_2 — c_1b_2)\, k \neq x_2x_1.$

Нейтральным элементом относительно умножения служит единица, рассматриваемая как кватернион, у которого $a=1$ и $b=c=d=0$. Можно также показать, что относительно умножения всякий кватернион

$$x = a + bi + cj + dk$$

имеет симметричный (обратный) ему

$$x^{-1} = (1/m^2)(a — bi — cj — dk),$$

где число

$$m = \sqrt{a^2 + b^2 + c^2 + d^2}$$

называют *нормой кватерниона.* Итак, множество кватернионов, наделенное описанными выше двумя внутренними законами композиции, образует тело.

Произвольный кватернион $\alpha = a + bi + cj + dk$ можно представить как совокупность числа a и трехмерного вектора $\vec{\alpha} = (b, c, d)$, который выходит из начала координат и который имеет числа b, c и d своими проекциями на оси координат, т.е. $\alpha = (a, \vec{\alpha})$. С другой стороны, всякому вектору $\vec{\xi} = (x, y, z)$ взаимно-однозначно соответствует *векторный кватернион* $\xi = bi + cj + dk$.

5. Вращение твердого тела. С помощью кватернионов изящно решаются задачи, которые связаны с композицией поворотов твердого тела в пространстве. Пусть, например, твердое тело поворачивается на угол φ_1 вокруг некоторой оси, которая проходит через точку O, а затем поворачивается вокруг другой оси, которая проходит через ту же точку O, на угол φ_2. Требуется определить, на какой угол φ и вокруг какой оси следует повернуть тело, чтобы оно из первого положения сразу перешло в третье (рис. 1.32, *а).*

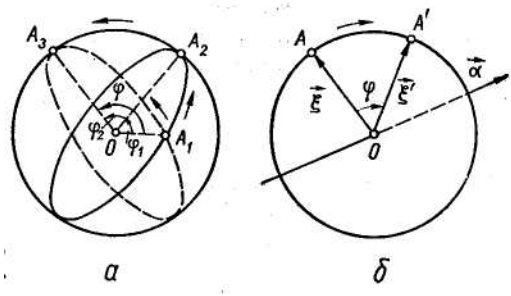


Рис. 1.32. Вращение твердого тела:
а — композиция вращений; *б* — поворот на угол φ.

Пусть положение твердого тела в пространстве определяется вектором $\vec{\xi} = (x, y, z)$, который выходит с O. Тогда повороту тела на угол φ ($0 < \varphi < 2\pi$) вокруг оси, задаваемой выходящим из начала координат вектором $\vec{\alpha} = (b, c, d)$, отвечает такой же поворот вектора $\vec{\xi}$, переводящий его в $\vec{\xi}' = (x', y', z')$. Векторам $\vec{\xi}$ и $\vec{\xi}'$ соответствуют векторные кватернионы ξ и ξ'. Рассматриваемому повороту взаимно-однозначно соответствует кватернион $\alpha = (a, \vec{\alpha})$, где

$$a = m\cos(\varphi/2); \quad m = \sqrt{a^2 + b^2 + c^2 + d^2}\ .$$

Можно показать, что $\xi' = \alpha^{-1}\xi\alpha$. Если известны $\vec{\xi}$, φ и $\vec{\alpha}$, то находим α, потом ξ' и $\vec{\xi}'$, определяющий положение тела после поворота (рис. 1.32, б). Таким образом, поворотам твердого тела соответствуют указанные действия над кватернионами.

Если последовательно совершаются два поворота вокруг осей $\vec{\alpha}_1 = (b_1, c_1, d_1)$ и $\vec{\alpha}_2 = (b_2, c_2, d_2)$ соответственно на углы φ_1 и φ_2, то для произвольного вектора $\vec{\xi}$ первый поворот дает $\alpha_1^{-1}\xi\alpha_1$, а второй поворот $\alpha_2^{-1}(\alpha_1^{-1}\xi\alpha_1)\alpha_2 = (\alpha_1\alpha_2)^{-1}\xi(\alpha_1\alpha_2)$. Следовательно, результирующий поворот определяется кватернионом $\alpha = \alpha_1\alpha_2$, т.е. композиции поворотов отвечает перемножение (в соответствующем порядке) определяющих их кватернионов.

6. Множество классов вычетов по модулю *m*. Как известно, сравнение по модулю m есть отношение эквивалентности на

множестве (кольце) целых чисел. Множество всех целых чисел разбивается на m классов эквивалентности $M_0, M_1..., M_{m-1}$, причем класс M_j объединяет числа $j + km$ (k — произвольное целое число), вычеты которых равны j. Совокупность классов відніманнь по модулю m определяется системой представителей $j = 0, 1, 2, ..., m — 1$.

Сумма (произведение) двух классов вычетов по модулю m определяется как класс, который содержит сумму (произведение) представителей этих классов. Поэтому действия над классами можно представить как арифметические действия над их представителями по модулю m. Например, при m=4 сложение и умножения задается таблицами (числа являются представителями классов):

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

;

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

Сложение классов вычетов ассоциативно и коммутативно. Существует нейтральный элемент 0 (j+0=j), и каждый элемент j имеет симметричный ему $\bar{j}$ такой, что $j+\bar{j}=0 \pmod m$. Так, для представителей 0, 1, 2, 3 симметричными являются соответственно 0, 3, 2, 1. Отсюда следует, что множество классов вычетов при любом m образует *абелеву группу* относительно сложения.

Умножение классов вычетов также ассоциативно и коммутативно. Существует нейтральный элемент 1 ($j \cdot 1 = 1 \cdot j = j$). Но относительно умножения не каждый элемент j имеет симметричный $\bar{j}$ такой, что $j\,\bar{j} = 1 \pmod m$. Действительно, как видно из таблицы, при m=4 это соотношение имеет место только для 1 и 3, поскольку $1 \cdot 1 = 1 \pmod 4$ и $3 \cdot 3 = 9 = 1 \pmod 4$, т.е. 1 и 3 симметричны самим себе, а элементы 0 и 2 не имеют симметричных. Следовательно, множество классов вычетов относительно умножения не является группой, а образует моноид (полугруппу).

Если m — простое число, то каждый отличный от нуля элемент j имеет симметричный ему $\bar{j}$ и относительно умножения классов

вычетов по модулю *m*. Действительно, из условия симметричности множества классов вычетов $j\,\bar{j} = 1 \pmod m$ можно записать:

$j\,\bar{j} = 1+km$, где k — целое число. Это значит, что симметричные элементы получаются делением $1+km$ на $j = 1, 2, ..., m — 1$, причем в результате этого деления должны получаться целые числа $\bar{j} < m$. А это возможно только при условии, что m — простое число. Заметим, что элементы 1 и m—1 всегда симметричны сами себе. Элемент 0 не имеет симметричного ни при каком $m>1$.

Таким образом, множество классов вычетов по модулю m относительно первого закона композиции (сложение) и второго закона (умножение) при любому m образует *абелево кольцо с единицей,* а при простых m — *поле.*

7. Поле комплексных чисел. Комплексное число $z= a + bi$, где a=Re z - действительная *часть* и b= Im z — *мнимая часть,* можно рассматривать как упорядоченную пару (a, b) двух действительных чисел, которые являются элементами множества R.

На множестве комплексных чисел определяются два внутренних закона — *сложение*

$$z_1+z_2= (a_1 + a_1, b_1 + b_2)$$

и *умножение*

$$z_1z_2 = (a_1a_2 — b_1b_2, a_1b_2 + a_2b_1).$$

Два числа z_1 и z_2 равны, если $a_1 = a_2$ и $b_1 = b_2$.

В принятых обозначениях $i=(0,1)$, следовательно, $i^2=(0,1)(0,1)=(—1,0)$ или $i^2=—1$. Действия над комплексными числами в форме $z=a+bi$ можно выполнять как с действительными числами, заменяя всякий раз i^2 на —1.

Комплексно-сопряженным с числом $z = a + bi$ является число $z^* = a — bi$. Справедливы следующие соотношения:

$$z + z^* = 2a;$$
$$z\,z^* = a^2 + b^2;$$
$$(z_1 + z_2)^* = z_1^* + z_2^*;$$
$$(-z)^* = -z^*;$$
$$(z_1 \cdot z_2)^* = z_1^* z_2^*.$$

Множество комплексных чисел составляет *коммутативную группу* относительно сложения. Действительно, сложение коммутативно и ассоциативно, нейтральным элементом служит нуль (0, 0), а симметричное числу $z = (a, b)$ есть $—z = (-a, -b)$.

Относительно умножения нейтральным элементом является единица (1, 0), и всякое отличное от нуля комплексное число $z=a+bi$ имеет симметричное (обратное)

$$\frac{1}{z}=\frac{1}{|z|^2}(a-bi)=z^{-1},$$

где $|z|=\sqrt{a^2+b^2}$ - модуль комплексного числа.

Так как умножение дистрибутивно относительно сложения, то множество комплексных чисел составляет *поле.*

Комплексное число представляется в *тригонометрической* и *экспонентной* форме соотношением

$$z=|z|\ (\cos\varphi + i\sin\varphi) =|z|e^{i\varphi}.$$

Здесь z - модуль и φ - аргумент комплексного числа, определяемый с точностью до целого кратного 2π, причем

$$\varphi = argz = \operatorname{arctg}(b/a).$$

Произведение двух комплексных чисел

$$z_1z_2=|z_1|\cdot|z_2|[\cos\varphi + \varphi_{2)} + i\ \sin(\varphi_1 + \varphi_{2)}],$$

т.е.

$$|z_1z_2| =|z_1|\cdot|z_2| \text{ и } \arg|z_1z_2|= \arg z_1 + \arg z_2.$$

При геометрическом представлении комплексных чисел в прямоугольной системе координат ось абсцисс используется для изображения действительной, а ось ординат — мнимой частей. Их соответственно называют действительной и мнимой осями на *плоскости комплексной переменной* (рис. 1.33, *а*).

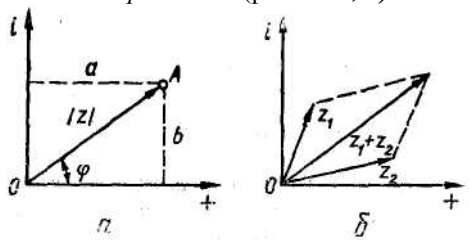


Рис. 1.33. Геометрическое представление комплексных чисел:
а — комплексная плоскость; *б* — суммированием комплексных чисел.

Числу $z= a + bi$ соответствует вектор OA и точка A с координатами a и b, которая называется *аффиксом* числа z. Суммированию комплексных чисел соответствует геометрическое сложение векторов на

комплексной плоскости (рис. 1.33, *б)*. Отсюда, в частности, следует $|z_1+z_2| \le |z_1|+|z_2|$ *(правило треугольника).*

8. Поле Галуа. Хорошо известные поля целых и действительных чисел — это бесконечные множества (соответственно счетное и континуальное). Конечное поле называют *полем Галуа.* Так, множество с четырех элементов 0,1, *A* и *B* образует поле Галуа, операции сложения и умножения в котором определяются следующими двумя таблицами:

+	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

;

·	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

.

Эти операции являются ассоциативными, коммутативными и дистрибутивными одна относительно другой. Элемент 0 является нейтральным относительно сложения, а 1 - относительно умножения. **Элементы *A* и *B* могут означать не только числа, но и объекты любой природы, отношение между которыми определяются приведенными таблицами.**

С помощью поля Галуа можно, например, проверять алгебраические тождеста. Так, известное из алгебры выражение

$$(A+B)\times(A-B)=A^2-B^2$$

справедливо и для поля Галуа. Действительно, для левой части из первой таблицы имеем $A + B = 1$ и $A — B = 1$ *(A — B* — это такое число, которое в сумме с *B* дает *A),* а из второй таблицы $1 \cdot 1 = 1$. Для правой части по второй таблице находим $A^2=AA=B$ и $B^2=BB=A$, а в соответствии с первой таблицей $A^2 - B^2 = B-A = 1$. Так как для левой и правой частей получены одинаковые результаты, то это означает их тождественность.

Хотя поля Галуа возникли в результате абстрактных математических соображений, они находят практическое применение, например, при решении задач, связанных с надежным кодированием информации в вычислительных машинах и системах передачи данных.

9. Гомоморфизм и изоморфизм. Рассмотрим два группоида: множества Q с законом композиции $\top$ и множества S с законом композиции $\perp$. Пусть каждому элементу из Q соответствует некоторый элемент из S, причем если паре $(a, b) \in Q$ соответствует пара $(a', b') \in S$, то элементу $a \perp b = c$ из Q соответствует $a' \top b'$ из S. Такое отображение $Q \to S$ называют *гомоморфизмом* Q в S. Иначе говоря, если $f : Q \to S$ такое, что для всякой пары (a, b) из Q справедливо соотношение $f(a \top b) = f(a) \perp f(b)$, то Q гомоморфно отображается в S относительно операций $\top$ и $\perp$ (рис. 1.34).

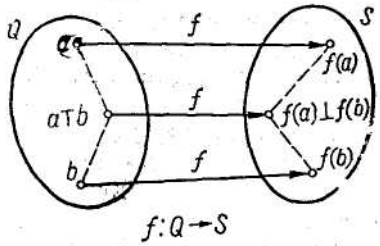


Рис. 1.34. Гомоморфизм Q в S.

В случае сюръективного отображения f имеем гомоморфизм Q на S, который называют *эпиморфизмом.*

Например, если каждой неособой матрице n-го порядка с действительными элементами поставить в соответствие ее определитель, то получим гомоморфизм мультипликативной группы таких матриц на мультипликативную группу всех отличных от нуля действительных чисел. Если на множестве целых чисел задана операция сложения по модулю m, то отображение этого множества на множество классов эквивалентности (оно состоит из m элементов) есть гомоморфизм.

Взаимно-однозначный (биективный) гомоморфизм называют *изоморфизмом.* Изоморфные множества Q и S обладают одинаковыми свойства относительно определенных на них операций. Например, если операция $\top$ коммутативна на множестве Q, то операция $\perp$ также коммутативна на множестве S; если для каждого элемента из Q существует симметричный элемент относительно операции $\top$, то и для каждого элемента из S, соответствующего элементу из Q, существует симметричный относительно операции $\perp$.

Замечательным примером изоморфизма является взаимно-однозначное отображение $x \to \lg x$. Так как $\lg(ab) = \lg a + \lg b$, то

произведению двух чисел из множества положительных чисел соответствует *сумма* двух соответствующих чисел *(логарифмов)* из множества всех действительных чисел. Таким образом, операция умножения чисел заменяется сложением их логарифмов и результат умножения получается обратным отображением $\lg x \to x$. Так делают в тех случаях, когда изоморфная операция более проста, чем исходная. Правда, упрощение не дается даром, так как необходимо с помощью обратного преобразования вернуться в исходное множество.

Аналогично определяются понятия гомоморфизма и изоморфизма как отображений множеств, наделенных не одним, а несколькими законами композиции.

1.16. Алгебраические структуры

Рассмотрим еще один пример алгебраической системы, который наболее часто встречается в теоретической алгебре и ее применениях. Этот пример — *структура*.

Пусть задано частично упорядоченное множество M. Отношение порядка в дальнейшем будем обозначать $\leq$. Для элементов a и b из M их верхней гранью называется любой элемент $c \in M$, такой, что $c \geq a$, $c \geq b$, а их нижней гранью — любой элемент $d \in M$, такой, что $d \leq a$, $d \leq b$. В общем случае для некоторых элементов a и b верхняя или нижняя грань может не существовать или быть неединственной, причем различные верхние (или нижние) грани могут быть несравнимыми.

Структурой (в некоторых книгах структуры, следуя английскому термину lattice, называют *решетками*) называется частично упорядоченное множество, в котором для любых двух элементов a и b существует их *пересечение* $a \sqcap b$ — такая нижняя грань a и b, что любая другая нижняя грань a и b меньше c; их *объединение* $a \cup b = d$ — такая верхняя грань a и b, что любая другая верхняя грань a и b больше d. Таким образом, *структура — это алгебраическая система* $\{M; \leq; \cap, \cup\}$ *с одним бинарным отношениям и двумя бинарными операциями.*

Пересечение и объединение ассоциативны (предлагаем читателю это доказать!), поэтому можно говорить о пересечении и объединении любого конечног подмножества элементов структуры.

Конечное упорядоченное множество можно изобразить диаграммой, в которой элементам соответствуют точки; из точки a ведет стрелка в

точку *b*, если $a < b$ и нет такого *c*, что $a < c < b$. Например, структура B_3 изображается диаграммой, которая приведена на рис.1.35, *а*.

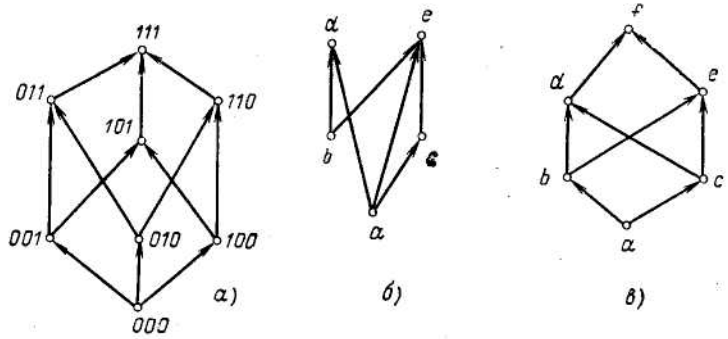


Рис. 1.35.

На языке диаграмм хорошо иллюстрируются все основные понятия, которые связаны со структурами: $a \leq b$, если и только если существует путь из стрелок, который ведет из *a* в *b*; верхняя грань *a* и *b* — это элемент, в который есть путь из *a* и из *b;* нижняя грань *a* и *b* — это элемент, из которого есть путь и в *a,* и в *b*.

Когда упорядоченное множество не является структурой? В двух случаях:

1) когда какие-либо два элементы не имеют верхней или нижней грани (на рис. 1.35,*б* элементы *d* и *e*, *c* и *d* не имеют верхней грани, элементы *b* и *c* не имеют нижней грани);

2) когда для некоторой пары элементов наименьшая верхняя (или наибольшая нижняя) грань не единственна (на рис. 1.35,*в* все элементы имеют верхние и нижние грани, однако *b* и *c* имеют две наименьшие и несравнимые верхние грани, *d* и *e* имеют две наибольшие нижние грани, поэтому изображенное на этом рисунке множество не является структурой).

Конкретный пример первого случая можно получить из структуры удалением некоторых ее элементов. Из рис. 1.35,*а* видно, что после удаления 101 B_3 остается структурой, а после удаления 111— нет. Удалением элементов из структуры можно получить и пример второго случая: если в B_4 удалить все элементы, кроме 0000, 0010, 0100, 0111, 1110, 1111, то диаграмма для оставшихся элементов в точности совпадет с рис. 1.35, *в*.

Структура, в которой пересечение и объединение существуют для любого подмножества ее элементов, называется *полной.* Ввиду

отмеченой ранее ассоциативности пересечения и объединения конечная структура всегда полна. Объединение всех элементов полной структуры — это максимальный элемент структуры, называемый *единицей* структуры. Пересечение всех элементов полной структуры — это минимальный элемент структуры, называемый *нулем* структуры. Структура из примера 4 (см. „Микромодуль 3. Примеры решения типовых задач"), всегда полная (в том числе и для бесконечного *A).* Единицей этой структуры служит само множество (содержащее любое свое подмножество), нулем - пустое множество.

Напомним, что *алгебраической структурой* называется множество вместе с операциями (замкнутыми), которые определены на этом множестве.

Обычно операции имеют некоторые характерные свойства, которые могут быть обоснованы в виде теорем и которые используются в вычислениях. (Структуру вместе со всеми теоремами, правилами вычислений и вывода иногда называют *алгебраической системой.)*

К каждой структуре применимо понятие подструктуры. Чтобы это продемонстрировать, рассмотрим *гипотетическую* структуру, называемую *указателем*. Пусть A — указатель. Предположим, что имеется только одна операция $\otimes$, которая определена на A. Следовательно, более точно это может быть записано как $(A, \otimes)$, т.е. указатель состоит из множества A с операцией $\otimes$. Теперь, если $B \subseteq A$ и $(B, \otimes)$ также является указателем, в частичности, $\otimes$ может быть замкнута на B, то $(B, \otimes)$ называется *подуказателем.*

Возьмем другую структуру, которая состоит из множества C и операции $\oplus$. ($\oplus$ и $\otimes$ должны иметь тот самый порядок. Например, если одна из них есть бинарной, то и другая должна быть такой же. Можно ввести и другие операции на C, однако здесь мы их не рассматриваем). Если существует отображение $\varphi: A \rightarrow C$ такое, что

$$\varphi(x \otimes y) = \varphi(x) \oplus \varphi(y)$$

для любых x и y из A, то φ называют *гомоморфизмом.* Если существует гомоморфизм между A и C, то в некотором смысле *образ* $(\varphi(A), \oplus)$ гомоморфизма из $(A, \otimes)$ ведет себя подобно прообразу, так как мы можем выполнить операцию $\otimes$ на A, а затем отобразить в C (посредством φ) или сначала отобразить в C, а затем выполнить операцию $\oplus$. В обеих случаях результат будет один и тот же. Поэтому мы можем делать так, как нам удобнее. Эту ситуацию можно пояснить с помощью коммутативных диаграмм, изображенных на рис. 1.36.

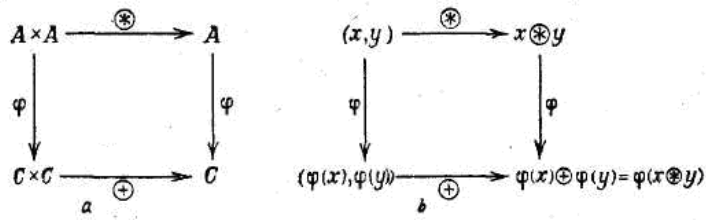


Рис. 1.36

Диаграмма на рис. 1.36, *a* указывает включаемые множества или структуры, а диаграмма на рис. 1.36, *b* связывает отдельные элементы. На рис. 1.36, *b* справа зображены две разлияные формы одного и того же результата. Коммутативность диаграммы следует из определения операций.

На самом деле мы получаем $\varphi \sqcup \otimes = \oplus \circ \varphi$, что не является в строгом смысле коммутативностью, так как $\otimes$ и $\oplus$ существено разлияны. Однако обе части равенства означают комбинации операций одного и того же порядка и, следовательно, подходят под общее определение

отображение o *операция* = *операция* o *отображения.*

Напомним еще одно определение. Гомоморфизм, который является инъекцией, называют *мономорфизмом,* гомоморфизм, который является сюръекцией, называют *эпиморфизмом,* а гомоморфизм, который является биекцией, называют *изоморфизмом.* Если существует изоморфизм между двумя структурами, то говорят, что они *изоморфны.*

Как мы знаем, слово «изоморфное» означает «той же самой формы», и поэтому, кажется, разумно ожидать, что изоморфизм должен быть в состоянии разделить множества всех алгебраических структур на классы эквивалентности .

Пример 1. Структуры $(\{\varnothing, E\}, \cap, \cup)$(где E - разбивка), и $(\{0, 1\} \wedge, \vee)$ изоморфны.

Доведение. Пусть $\varphi(\varnothing)=0$ и $\varphi(E)=1$. Ясно, что φ - биекция. Тогда

$\varphi(E \cap \varnothing) = \varphi(\varnothing) = 0 = 0 \wedge 0 = \varphi(\varnothing) \wedge \varphi(\varnothing)$,

$\varphi(\varnothing \cap E) = \varphi(\varnothing) = 0 = \varnothing \wedge 1 = \varphi(\varnothing) \wedge \varphi(E)$,

$\varphi(E \cap \varnothing) = \varphi(\varnothing) = 0 = 1 \wedge 0 = \varphi(E) \wedge \varphi(\varnothing)$,

$\varphi(E \cap E) = \varphi(E) = 1 = 1 \wedge 1 = \varphi(E) \wedge \varphi(E)$,

$\varphi(\varnothing \cup \varnothing) = \varphi(\varnothing) = 0 = 0 \vee 0 = \varphi(\varnothing) \vee \varphi(\varnothing)$,

$\varphi(\varnothing \cup E) = \varphi(E) = 1 = 0 \vee 1 = \varphi(\varnothing) \vee \varphi(E)$,

$\varphi(E \square \varnothing) = \varphi(E) = 1 = 1 \vee 0 = \varphi(E) \vee \varphi(\varnothing)$,

$\varphi(E \cup E) = \varphi(E) = 1 = \vee 1 = \varphi(E) \vee \varphi(E)$.

Таким образом, φ является гомоморфизмом и, следовательно, изоморфизмом.

В заключение отметим, что структура может быть изоморфна самой себе (имеется в виду изоморфизм, отличный от тривиального) и может также быть изоморфна одной из своих подструктур (это возможно лишь для бесконечных множеств).

Определение. Если область определения и область значений отображения совпадают, гомоморфизм называют *эндоморфизмом,* а изоморфизм называют *автоморфизмом.*

Пример 2. Для заданного множества *A* структура $(\mathcal{P}(A), \cup, \cap)$ изоморфна $(\mathcal{P}(A), \cap, \cup)$ с отображением $\varphi: X \to X'$.

Доказательство. Очевидпо, что φ інъективно и сюръективно. Если $B, C \in \mathcal{P}(A)$, то

$$\varphi(B \cap C) = (B \cap C)' = B' \cup C' = \varphi(B) \cup \varphi(C),$$

$$\varphi(B \cup C) = (B \cup C)' = B' \cap C' = \varphi(B) \cap \varphi(C).$$

Позднее мы увидим, что эти соотношения явно показывают самодвойственность булевой алгебры множеств и φ является автоморфизмом.

Микромодуль 3
Примеры решения типовых задач

1.1) Алгебра $(R; +, \bullet)$ называется *полем действительных чисел.* Обе операции — бинарные, поэтому тип этой алгебры (2, 2). Все конечные подмножества *R,* кроме {0}, не замкнуты относительно обеих операций. Подалгеброй этой алгебры является, например, поле рациональных чисел.

2) Пусть $N_p = \{0, 1, 2, ..., p — 1\}$. Определим на N_p операции $\oplus$ («сложение по модулю *p*») и $\otimes$ («умножение по модулю *p*») таким образом: $a \oplus b = c$, $a \oplus b = d$, где *c* и *d* — остатки от деления на *p* чисел $a + b$ и $a \cdot b$ соответственно. Например, если $p=7$, то $N_p = \{0, 1, ..., 6\}$, $3 \oplus 4 = 0$, $3 \otimes 4 = 5$, $4 \oplus 6 = 3$. Часто операции $\otimes$ и $\oplus$ обозначают как $a + b \equiv c \pmod p$, $a \otimes b = d \pmod p$. Если *p* — простое число, то алгебра $\{N_p, \oplus, \otimes\}$ называется *конечным полем характеристики p.*

3) Пусть задано множество *U*. Множество всех его подмножеств называется *булеаном U* и обозначается через $\mathcal{B}(U)$. Алгебра $B = (\mathcal{B}(U); \cap, \cup, \bar{\ })$ называется *булевой алгеброй множеств* над *U*, ее тип (2, 2, 1). Элементами основного множества этой алгебры являются множества (подмножества *U*). Для любого $U' \subset U$ $B' = (\mathcal{B}(U'); \cap, \cup, \bar{\ })$ является подалгеброй *B*. Например, если $U = \{a, b, c, d\}$, то основное множество алгебры *B* содержит 16 элементов; алгебра $B' = \{\mathcal{B}(\{a, c\}); \cap, \cup, \bar{\ }\}$ — подалгебра *B;* ее основное множество содержит четыре элемента.

4) Множество *F* одноместных функций на *R*, т.е. функций $f: R \to R$, вместе с операцией дифференцирования является алгеброй. Элементы основного множества — функции типа $R \to R$, единственной операцией этой алгебры служит дифференцирование — унарная операция типа $F \to F$ (производной функции на *R* является снова функция на *R*). Множество элементарных функций, как мы знаем, замкнуто относительно дифференцирования - производные элементарных функций элементарны - и, следовательно, образуют подалгебру данной алгебры.

5) Рассмотрим квадрат с вершинами в точках a_1, a_2, a_3, a_4 и повороты квадрата вокруг центра (против часовой стрелки), переводящие вершины в вершины. Таких поворотов — бесконечное множество: на углы 0, $\pi/2$, π, $3\pi/2$, 2π, $5\pi/2$..., однако они задают всего четыре различных отображения множества вершин в себя, соответствующих первым четырем поворотам. Таким образом, получаем алгебру с основным множеством $\{a_1\ a_2, a_3, a_4\}$ и четырьмя унарными операциями α, β, γ, δ. Их можно задать табл. 1.17, в которой на пересечении, например, строки a_3 и столбца γ написано значение функции $\gamma(a_3)$.

Таблица 1.17

	α	β	γ	δ
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

Операция α, отображающая любой элемент в себя, называется тождественной операцией. Она соответствует нулевому повороту. Подалгебр в этой алгебре нет.

6) Множество O={ α, β, γ, δ } отображений вершин в себя из предыдущего примера вместе с бинарной операцией ⊔ композиции отображений образует алгебру {O; o}. Элементами множества O являются отображения (повороты). Композиция отображений — это последовательное выполнение двух поворотов. Она задается табл. 1.18 (в ней на пересечении строки α и столбца γ написан результат композиции α o γ).

Таблица 1.18

	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ

Такая таблица, задающая бинарную операцию, как мы занем,называется таблицей Кели. Множество { α,γ }, т.е. повороты 0, π, образует подалгебру алгебры (O; o}.

2. 1) Пусть Q_N — множество всех целых чисел, Q_{2N} — множество всех четных чисел. Алгебры $(Q_N; +)$ и $(Q_{2N}; +)$ изоморфны; изоморфизмом являются отображения $\Gamma_{2n} : n \to 2n$, причем условие (1.1) здесь имеет вид $2(a+b) = 2a + 2b$. Поскольку $Q_{2N} \subset Q_N$, то Γ_{2n} — изоморфизм $(Q_N; +)$ в себя. Отображение $\Gamma_{-n} : n \to (-n)$ является для алгебры $(Q_N; +)$ автоморфизмом; условие (1.1) имеет вид $(-a)+(-b) = -(a+b)$. Для алгебры $(Q_N; \cdot)$ Γ_{-n} не является автоморфизмом, так как $(-a)(-b) \neq -(ab)$.

2) Рассмотрим алгебры $(N; +; \cdot)$ и $(N_7; \oplus, \otimes)$ (см. пример 1) и определим отображение $\Gamma_7 : N \to N_7$ следующим образом: $\Gamma(n)$ равно остатку от деления n на 7; иначе говоря, если $n = 7a + b$ $(b < 7)$, то $\Gamma(n) = b$. Пусть $n_1 = 7a_1 + b_1$, $n_2 = 7a_2 + b_2$. Проверим условие (1.1). Для сложения имеем

$$\Gamma(n_1 + n_2) = \Gamma(b_1 + b_2) = b_1 \oplus b_2 = \Gamma(n_1) \oplus \Gamma(n_2).$$

Для умножения имеем

$$\Gamma(n_1 n_2) = = \Gamma(b_1 b_2) = b_1 \otimes b_2 = \Gamma(n_1) \otimes \Gamma(n_2).$$

Таким образом, условие (1.1) выполненная и Γ_7 — гомоморфизм. Очевидно, Γ_7 не является изоморфизмом, так как нет взаимной однозначности. Этот пример показывает, что возможен гомоморфизм

бесконечной алгебры (т.е. алгебры с бесконечным основным множеством) в конечную алгебру. При этом N разбивается на семь классов эквивалентности по отношению E_7 : aE_7b, если и только если $\Gamma_7(a) = \Gamma_7(b)$.

3) Изоморфизмом между алгебрами $(R_+, \cdot)$ и $(R, +)$, где R_+ — положительная часть R, является отображения $a \to \log a$. Условие (1.1) имеет вид равенства $\log(ab) = \log a + \log b$.

4) Рассмотрим алгебры (K, φ) и (M, ψ), где $K=\{a_1, a_2, a_3, a_4\}$;
$M = \{b_1, b_2, b_3, b_4\}$, а бинарные операции φ и ψ заданы следующими таблицами (табл. 1. 19, *а, б)*:

Таблица 1. 19

φ	a_1	a_2	a_3	a_4
a_1	a_3	a_2	a_2	a_1
a_2	a_1	a_4	a_4	a_2
a_3	a_4	a_2	a_2	a_1
a_4	a_1	a_1	a_3	a_3

а)

ψ	b_1	b_2	b_3	b_4
b_1	b_4	b_4	b_3	b_1
b_2	b_1	b_1	b_4	b_3
b_3	b_1	b_1	b_2	b_3
b_4	b_3	b_2	b_3	b_2

б)

Отображение $\Gamma: a_1 \to b_3$, $a_2 \to b_1$, $a_3 \to b_2$, $a_4 \to b_4$ является изоморфизмом.

Буквальная проверка условия (1.1) заключается в следующему: в клетках (во внутренней части) таблицы φ заменяем a_i на b_i в соответствии с Γ и получаем левую часть (1.1), т.е. таблицу функции $\Gamma_\varphi(a_i, a_j)$; во внешней части таблицы ψ заменяем b_i на a_i и получаем правую часть (1.1); сравнением полученных двух таблиц убеждаемся, что они задают одну и ту же функцию. В действительности достаточно в таблице φ переименовать все a_i в b_j и сравнить полученную таблицу с ψ .

Заметим, что можно было бы рассматривать алгебры (K, φ) и (K, ψ), где в таблице ψ все b_i заменены на a_i (с тем же индексом). Тогда отображение Γ: $a_1 \to a_3$, $a_2 \to a_1$, $a_3 \to a_2$, $a_4 \to a_4$ также является изоморфизмом.

5) Рассмотрим булевы алгебры (см. пример 1, п. 3), которые образованы двумя различными множествами U, U' одинаковой мощности. Эти две алгебры изоморфны: операции у них просто одинаковы а отображением Γ может служить любое взаимно-однозначна соответствие между U и U'.

3. 1) Множество рациональных чисел, не удержащее нуля, с операцией умножения является абелевою группой. Обратным к элементу *a* является элемент 1*/a.*

2) Множество целых чисел с операцией сложения есть абелевой циклической группой. Роль единицы здесь играет 0, обратным к элементу *a* является элемент — *a*.

3) Множество невырожденных квадратных матриц порядка *n* (с отличным от 0 определителем) с операцией умножения является некоммутативной группой.

4) Множество {0, 1, 2, 3, 4} с операцией «сложения по mod 5» — конечная абелева циклическая группа. В этой группе $3^{-1} = 2$, $\Gamma^{-1} = 4$.

5) Алгебра {O, ∟} из примера 1, п. 6, где O — множество поворотов квадрата, а o — их композиция, является циклической группой: $\gamma = \beta^2$, $\delta = \beta^3$, $\alpha = \beta^4$. Единицей в ней служит тождественное отображение α (поворот на нулевой угол); обратным к данному повороту служит поворот, дополняющий его до 2π: $\beta^{-1} = \delta$, $\gamma^{-1} = \gamma$, $\delta^{-1} = \beta$.

6) Рассмотрим множество S всех взаимно-однозначных преобразований конечного множества *M* в себя. Такие преобразования называются подстановками. Алгебра $\sum_M = \{S_M; o\}$ представляет собой группу, которая называется *симметрической.* Поскольку число подстановок равно числу перестановок в списке элементов *M,* то порядок $\sum_M$ равен |M|!. Симметрическая группа не является абелевой. Пусть, например,

$$M = \{1, 2, 3, 4\}, \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Тогда

$$\alpha\beta = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,2\,4 \end{pmatrix}, \ \beta\alpha = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,4\,3 \end{pmatrix}, \ \alpha^{-1} = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,3\,2 \end{pmatrix}, \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

4. 1) Любое полностью упорядоченное множество *M* (например, множество целых чисел) можно превратить в структуру, определив для любых

$$a, b \in M \; a \cup b = \max(a, b), \; a \cap b = \min(a, b).$$

2) Определим на *N* отношение частичного порядка следующим образом: $a \leq b$, если *a* делит *b*. Тогда $a \cup b$ — наименьший общий делитель *a* и *b*, $a \cap b$ — наибольший общий делитель *a, b.* Например, $9 \cup 12 = 36$, $9 \cap 12 = 3$, $5 \cap 7 = 1$, $5 \cup 7 = 35$.

3) Система всех подмножеств $\mathcal{B}(A) = \{M_i\}$ любого множества A частично упорядочена по включению: $M_i \leq M_j$, если и только если $M_i \subseteq M_j$. Эта система является структурой, элементами которой являются множества, а операциями - обычные теоретико-множественные операции объединения и пересечение (см. пример 1, п. 3).

4) Рассмотрим множество B_n двоичных векторов длины n, частично упорядоченное. Для двоичных векторов это упорядочение выглядит так: $v \leq w$, если в векторе w единицы стоят на всех тех местах, на которых они стоят в v (и, может быть, еще на некоторые). Например, (010)≤(011), а (010) и (100) не сравнимы. Множество B_n, упорядоченное таким образом, является структурой; в ней $v \sqcup w$ — это вектор, в котором единицы стоят на тех (и только тех) местах, где есть единицы либо в v, либо в w, а $v \sqcap w$ — это вектор, в котором единицы стоят на те и только тех мест, где единицы есть и в v, и в w. Например,

$$(010) \cup (100) = (110),$$

$$(010) \cap (100) = 000.$$

При доказательстве теоремы 2 было установлено взаимно-однозначное соответствие между множеством B_n и системой всех подмножеств любого множества A мощности n. Легко проверить, что это соответствие является изоморфизмом соответствующих структур; таким образом, струтура, которая описана в примере 1 (см. „Микромодуль 3. Примеры решения типовых задач"), и структура из настоящего примера изоморфны.

5. Пусть отображение θ, $\theta: Z \to Z_{10}$ — остаток от деления на 10. Тогда

$$\theta(20) = 0,$$

$$\theta(17) = 7, \ldots$$

Если мы рассмотрим простейшие системы $(Z, +)$ и $(Z_{10}, +)$ с операцией +, определенной естественным образом на Z и на «единичном столбце» для Z_{10}, то легко видеть, что θ является гомоморфизмом. Например,

$$\theta(24 + 38) = \theta(62) = 2,$$

$$\theta(24) + \theta(38) = 4 + 8 = 2 \quad (\text{в } Z_{10}).$$

В этом случае диаграмма будет выглядеть так, как это изображено на рис. 1.37.

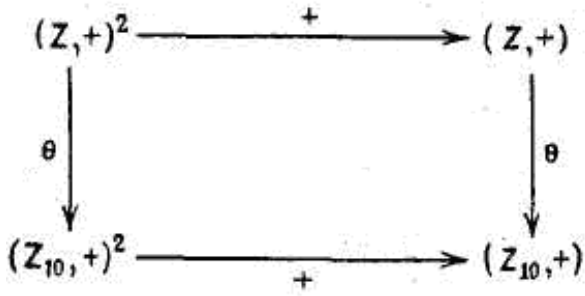


Рис. 1.37

Таким образом, как мы уже говорили раньше, гомоморфизм одной структуры в другую является отображением, которое сохраняет структуру.

Можно вводить ограничение на ранг отображения, чтобы получить, например, сюръективность или инъективность. Поэтому, если отображение является гомоморфизмом, можно надеяться, что это обеспечит механизм перехода от структуры е структуре (и обратно!) без какой-либо потери информации.

Микромодуль 3.
Индивидуальные тестовые задачи

1. Следующих шесть операций, которые переводят вершины равностороннего треугольника, совмещают его с самим собой (рис. 1.38);

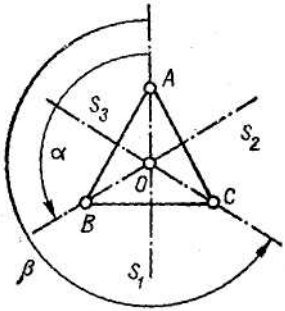


Рис. 1.38. Операции, совмещающие треугольник с самим собой.

1 - тождественная операция, оставляющая все вершины на месте;

α — поворот на 120° вокруг центра *O,* что переводит *A* в *B, B* в *C, C* в *A;*

β — поворот на 240° вокруг центра *O,* переводящий *A* в *C, B* в *A, C* в *B;*

S_1 — симметрия, переводящая *B* в *C* и *C* в *B;*

S_2 - симметрия, переводящая *A* в *C* и *C* в *A;*

S_3 - симметрия, переводящая *A* в *B* и *B* в *A*.

Композиция любых двух операций приводит к тому же результату, что и некоторая операция из множества $G=\{1, \alpha, \beta, S_1, S_2, S_3\}$, например композиция S_2 и S_1 дает β.

Запишите этот закон композиции в виде таблицы, исследуйте его свойства и определите тип соответствующей алгебраической системы.

2. Представьте каждую операцию из задачи 1 соответствующей ей подстановкой третьей степени на множестве вершин треугольника $\{A, B, C\}$, например

$$S_1 = \begin{pmatrix} ABC \\ ACB \end{pmatrix}$$ и т.д.

Покажите, что:

а) множество всех таких подстановок образует симметрическую группу шестого порядка, изоморфную группе операций в задаче 1;

б) каждое из подмножеств $\{1, \alpha, \beta\}$, $\{1, S_1\}$, $\{1,S_2\}$, $\{1, S_3\}$ является группой подстановок.

3. Для группы *G* из задачи 1 постройте изоморфную ей группу подстановок шестой степени, элементами которых являются операции, которые совмещают треугольник с самим собой.

4. Даны многочлены:

$$f(x) = 1 + 5x^6;$$
$$g(x) = 1 + 2x + x^2;$$
$$q(x) = 25 - 20x + 15x^2 - 10x^3 + 5x^4;$$
$$r(x) = -24 - 30x.$$

Покажите, что

$$f(x) = g(x)q(x)+r(x)$$

двумя способами:

а) умножением и сложением многочленов;

б) делением (по убывающим степеням) многочлена $f(x)$ на $g(x)$.

5. Многочлен называется простым или неприводимым, если он не имеет других делителей, кроме самого себя и ненулевых постоянных.

Укажите числовые поля (рациональное, действительное, комплексное) коэффициентов, в которых многочлен неприводим:

а) $x^2 - 4$; б) $x^2 - 2$; в) $x^2 + 1$.

6. Разделите многочлен $1+5x^6$ на многочлен $1+2x+x^2$ по возрастающим степеням и сравните результат с полученным в задаче 4,б. Покажите на этом примере, что если $f(x)$ не делится на $g(x)$, то деление по возрастающим степеням может продолжаться до любой степени частного.

7. Делением по возрастающим степеням представьте бесконечными рядами выражения:

$$\text{а)}\ \frac{1}{1-x}\ ;\ \text{б)}\ \frac{1}{1-x^2};\ \text{в)}\ \frac{x}{1+x^2}$$

8. Определите нули многочленов:

а) $10 - 3x - x^2$;

б) $1 - x - x^2 + x^3$.

9. Покажите, что многочлен

$$x^4 - 8x^3 + 24x^2 - 36x + 27$$

имеет двукратный нуль $\lambda_1 = 3$ и комплексно-сопряженные нули

$$\lambda_2 = 1 + i\sqrt{2} \text{ и } \lambda_3 = 1 - i\sqrt{2}.$$

10. Запишите таблицы умножения и сложения классов вычетов по модулю m для m, равного 5 и 6. Определите в обоих случаях симметричные элементы относительно умножения (если они существуют) и объясните различие между этими двумя случаями. Покажите, что множество классов вычетов при $m = 5$ образует поле Галуа.

Модуль 2
Введение в теорию групп

Микромодуль 4
Основные понятия и действия с группами

2.1. Примеры групп

1. Действия над целыми числами. Сложение целых чисел удовлетворяет следующим условиям, которые называются аксиомами сложения:

I. Всякие два числа можно сложить (т.е. для любых двух чисел a и b существует вполне определенное число, которое называют их суммой: $a+ b)$.

II. Условие совместимости или ассоциативности:

Для любых трех чисел a, b, c имеет место тождество:

$$(a + b) + c = a + (b + c).$$

III. Среди чисел существует одно определенное число, нуль, которое удовлетворяет для всякого числа a соотношению

$$a + 0 = a.$$

IV. Для каждого числа a существует противоположное ему число, $-a$, обладающее тем свойством, что сумма $a+(-a)$ равняется нулю:

$$a + (-a) = 0.$$

V. Условие переместительности или коммутативности:

$$a + b = b + a.$$

2. Действия над рациональными числами. Рассмотрим теперь множество Q, которое состоит из всех положительных и отрицательных рациональных чисел, т.е. из всех рациональных чисел, *отличных* от нуля. Умножение этих чисел удовлетворяет ***аксиомам умножения.*** Перечислем их.

I. *Всякие два числа из* Q *можно перемножить* (т.е. для любых двух чисел a и b существует вполне определенное число, которое называют их произведением: $a \cdot b)$.

II. Условие совместимости или ассоциативности. *Для любых трех чисел a, b, c из множества* Q *имеет место тождество:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

III. *Среди чисел множества* Q *существует единственное число — единица, которая удовлетворяет для всякого числа a соотношению*

$$a \cdot 1 = a.$$

IV. *Для каждого числа a из Q существует обратное ему число* a^{-1}, *обладающее тем свойством, что произведение* $a \cdot a^{-1}$ *равняется единице:*

$$a \cdot a^{-1} = 1.$$

V. Условие коммутативности:

$$a \cdot b = b \cdot a.$$

Сравнивая примеры пп. 1 и 2, нетрудно заметить полное сходство аксиом, которым удовлетворяет операция сложения для целых чисел и операция умножения для ненулевых рациональных чисел. Ниже мы увидим, что это сходство не случайное и проявляется при рассмотрении разнообразных конкретных операций.

3. Повороты правильного треугольника. Покажем, что не только числа, но и много других объектов можно перемножать и притом с соблюдением только что перечисленных условий.

Пример 1. Рассмотрим всевозможные повороты правильного треугольника вокруг его центра *O* (рис. 2.1).

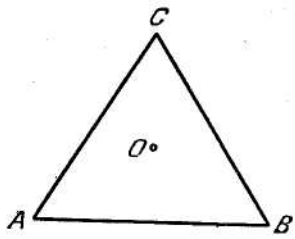


Рис. 2.1

При этом мы будем считать два поворота совпадающими, если они отличаются один от другого на целое число полных оборотов (т.е. на целочисленное кратное 360°). (Так как поворот на целочисленное кратное 360, очевидно, ставит каждую вершину на ее первоначальное место, то естественно объявить такой поворот совпадающим с нулевым и вообще считать совпадающими два поворота, которые отличаются друг от друга на целое число полных оборотов). Легко видеть, что из всех возможных поворотов треугольника лишь три поворота переводят треугольник в себя, а именно: повороты на 120°, на 240° и так называемый *нулевой* поворот, который оставляет все вершины, а следовательно, и все стороны треугольника на месте. Первый поворот переводит вершину *A* в вершину *B*, вершину *B* в вершину *C*, вершину *C* в вершину *A* (он перемещает, как говорят, вершины *A, B, C* в

циклическом порядку). Второй поворот перемещает *A* в *C, B* в *A, C* в *B* (т.е. перемещает в циклическом порядке *A, C, B).*

Введем следующее определение.

Умножить два поворота - значит, последовательно произвести их один за другим.

Таким образом, поворот на 120°, умноженный с самим собой, дает поворот на 240°, умноженный с поворотом на 240° дает поворот на 360°, т.е. нулевой поворот. Два поворота на 240° дают поворот на 480° = 360° + 120°, т.е. их произведение есть поворот на 120°.

Если мы нулевой поворот обозначим через a_0, поворот на 120° через a_1, поворот на 240° через a_2, то получим следующие соотношения:

$$a_0 \cdot a_0 = a_0, \quad a_0 \cdot a_1 = a_1 \cdot a_0 = a_1,$$
$$a_0 \cdot a_2 = a_2 \cdot a_0 = a_2, \quad a_1 \cdot a_1 = a_2,$$
$$a_1 \cdot a_2 = a_2 \cdot a_1 = a_0, \quad a_2 \cdot a_2 = a_1.$$

Итак, для каждых двух поворотов определено их произведение. Читатель легко проверит, что это умножение удовлетворяет сочетательному закону; очевидно также, что оно удовлетворяет переместительному закону. Далее, среди этих поворотов имеется также нулевой поворот a_0, который удовлетворяет условию

$$a \cdot a_0 = a_0 \cdot a = a$$

для любого поворота *a*.

Наконец, каждый с трех поворотов имеет обратный ему поворот, который дает в произведении с данным поворотом нулевой поворот: нулевой поворот, очевидно, обратен самому себе, $a^{-1}=a_0$, так как $a_0 \cdot a_0 = a_0$, тогда как $a_1^{-1}=a_2$ и $a_2^{-1}=a_1$ (так как $a_1 \cdot a_2 = a_0$). Итак, умножение поворотов правильного треугольника, удовлетворяет всем перечисленным аксиомам умножения. Запишем еще раз правило умножения поворотов более компактным образом в виде следующей *пифагоровой таблицы умножения:*

Таблица 2.1

	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

Произведение двух элементов в этой таблице находим на пересечении строки, отмеченной первым элементом, и столбца, отмеченного вторым элементом.

Читатель, который будет вычислять с поворотами механически, возьмет просто три буквы: a_0, a_1, a_2 и будет множать их, пользуясь только что выписанной таблицей умножения; при этом он может совсем забыть, что именно эти буквы обозначали.

4. Клейновская группа четвертого порядка.

Пример 2. Рассмотрим совокупность четырех букв a_0, a_1, a_2, a_3, умножение которых определено следующей таблицей:

Таблица 2.2

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

или в развернутом виде:

$$a_0 \cdot a_0 = a_0,\ a_0 \cdot a_1 = a_1 \cdot a_0 = a_1,$$
$$a_0 \cdot a_2 = a_2 \cdot a_0 = a_2,\ a_0 \cdot a_3 = a_3 \cdot a_0 = a_3,$$
$$a_1 \cdot a_1 = a_0,\ a_2 \cdot a_2 = a_0,$$
$$a_1 \cdot a_2 = a_2 \cdot a_1 = a_3,\ a_2 \cdot a_3 = a_3 \cdot a_2 = a_1.$$
$$a_1 \cdot a_3 = a_3 \cdot a_1 = a_2,\ a_3 \cdot a_3 = a_0.$$

Умножение определено для любых двух букв из числа четырех. Непосредственная проверка сразу показывает, что это умножение удовлетворяет условию ассоциативности и коммутативности.

Буква a_0 обладает основновным свойством единицы: произведение двух сомножителей, из которых одно есть a_0, равно другому сомножителю.

Таким образом, условия, аналогичные условиям I, II, III, V из пп. 1-2, оказываются выполненными в «алгебре четырех букв». Для того

чтобы убедиться, что условие IV также выполнено, лостаточно заметить, что мы положили

$$a_0 \cdot a_0 = a_0, \quad a_1 \cdot a_1 = a_0, \quad a_2 \cdot a_2 = a_0, \quad a_3 \cdot a_3 = a_0,$$

т.е. каждая буква сама себе обратна (дает при умножении с самой собой единицу).

Наша «алгебра четырех букв» на первый взгляд может показаться своего рода математической игрой, забавой, которая лишена реального содержания. В действительности законы этой алгебры, выраженные таблицей 2, имеют вполне реальный смысл, с которым мы в скором времени познакомимся; заметим, более того, что эта «алгебра четырех букв» имеет важное значение и в высшей алгебре. Она называется *клейновской группой четвертого порядка.*

5. Повороты квадрата.

Пример 3. Некоторую «алгебру четырех букв», отличную от предыдущей, можно построить в полной аналогии с тем, что мы делали в первом примере. Рассмотрим квадрат *ABCD* и повороты вокруг его центра, которые переводят фигуру в самое себя. Опять будем считать совпадающими всякие два поворота, отличающиеся друг от друга на целочисленное кратное 360°. Таким образом, будем иметь всего четыре поворота, а именно: нулевой, поворот на 90°, на 180° и на 270°.

Эти повороты обозначим соответственно через a_0, a_1, a_2, a_3. Если под умножением двух поворотов понимать опять последовательное осуществление двух поворотов, то получим следующую таблицу умножения, вполне аналогичную второму примеру:

Таблица 2.3

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

Таким же точно образом как в этом и в первом примере, можно рассматривать повороты правильного пяти-, шести- и вообще n-угольника.

2.2. Основные теоремы о группах

Прежде чем идти дальше в изучении отдельных примеров, подведем итог уже рассмотренным примерам, введя основное определение.

Пусть задано некоторое (конечное или бесконечное) множество G, на котором определена ***операция умножения,*** т.е. определен закон, который сопоставляет любой паре a, b элементов из G некий элемент из G называемый *произведением* a и b и обозначаемый символом $a\cdot b$. Предположим, что эта операция умножения удовлетворяет следующим условиям:

I. Условие ассоциативности. Для любых трех элементов a, b, c множества G справедливо соотношение:

$$(a\cdot b)\cdot c = a\cdot(b\cdot c).$$

Это значит следующее. Обозначим через d элемент множества G, который является произведением элементов a и b; точно так же обозначим через e элемент $b\cdot c$ множества G. Тогда $d\cdot c$ и $a\cdot e$ являются одним и тем же элементом множества G.

II.Условие существования нейтрального элемента. *Среди элементов множества G имеется некоторый определенный элемент, который называют* ***нейтральным*** *элементом и обозначают символом* 1, *такой, что*

$$a\cdot 1 = 1\cdot a = a$$

при любом выборе элемента a.

III. Условие существования обратного элемента к каждому данному элемента. *К каждому данному элементу a множества G можно подобрать такой элемент b того же множества G, что*

$$a\cdot b = b\cdot a = 1.$$

Элемент b называется ***обратным*** к элементу a и обозначается a^{-1}.

Множество G с определенной в нем операцией умножения, удовлетворяющей только что перечисленным трем условиям, называется ***группой;*** сами эти условия называются ***аксиомами группы.***

Операция умножения, которое удовлетворяет аксиомам группы, иногда называется ***групповой операцией*** или ***групповым законом.*** Мы будем пользоваться всеми этими терминами, не оговаривая каждый раз их эквивалентность.

Пусть в группе G, кроме указанных выше трех аксиом, оказывается выполненным еще и следующее условие:

IV. Условие коммутативности:

$$a \cdot b = b \cdot a.$$

В этом случае группа G называется ***коммутативной*** или ***абелевой группой.***

Группа называется ***конечной,*** если она состоит из конечного числа элементов; в противном случае она называется ***бесконечной.***

Число элементов конечной группы называется ее ***порядком или мощностью.***

Познакомившись с определением группы, мы видим, что приведенные раньше примеры являются примерами групп. Действительно, мы познакомились последовательно:

1) с группой целых чисел (групповая операция - обычное сложение целых чисел);

2) с группой отличных от нуля рациональных чисел (групповая операция - обычное умножение рациональных чисел);

3) с группой поворотов правильного треугольника (групповая операция - композиция поворотов);

4) из клейновскою группой порядка 4 (групповая операция — умножение букв a_0, a_1, a_2, a_3, задаваемая таблицей 1.2);

5) с группой поворотов правильного четырехугольника (групповая операция - композиция поворотов);

6) с группой поворотов правильного n-угольника.

Все эти группы коммутативны. Группа целых чисел и группа ненулевых рациональных чисел бесконечны; остальные - конечные группы.

Рассмотрим простейшие теоремы о группах

1. Произведение любого конечного числа элементов группы. Первое правило раскрытия скобок.

Аксиома ассоциативности имеет в теории групп и, соответственно, во всей алгебре очень большое значение: она позволяет определить произведение не только двух, но и трех и вообще любого конечного числа элементов группы и пользоваться при рассмотрении этих произведений обычными правилами раскрытия скобок (при этом необходимо только помнить, что в случае некоммутативных групп нельзя, вообще говоря, изменять порядок сомножителей).

В самом деле, если даны, например, три элемента a, b, c, то мы еще пока не знаем, что значит умножить эти *три* элемента: ведь аксиомы групп говорят лишь о произведениях *двух* элементов и выражения вида $a \cdot b \cdot c$ еще не определены. Однако условие ассоциативности говорит,

что умножая, с одной стороны, элемент a на элемент $b\cdot c$ и, с другой стороны, элемент $a\cdot b$ на элемент c мы получим *один и тот же элемент в качестве произведения*. Вот этот элемент, являющийся произведением двух элементов a и $b\cdot c$, а также произведением двух элементов $a\cdot b$ и c, и представляется естественным *определить в качестве* произведения трех элементов a, b, c в том порядка, как они здесь выписаны, и обозначить его через $a\cdot b\cdot c$. Таким образом, на равенство

$$a\cdot b\cdot c = a\cdot (b\cdot c) = (a\cdot b)\cdot c$$

необходимо смотреть, как на определение abc произведения трех элементов a, b, c (здесь знак умножения для удобства опущен).

Таким же точно образом можно определить произведение четырех элементов $a, b, c, d,$ например, как $a\cdot(bcd)$. Докажем, что при этом

$$a(bcd) =(ab)\ (cd) = (abc)\ d.$$

По только что сказанному имеет прежде всего место равенство:

$$a(bcd) = a[b(cd)].$$

Но для трех элементов a, b, cd мы имеем:

$$a[b(cd)] = (ab)(cd).$$

С другой стороны, имеем для трех элементов ab, c, d:

$$(ab)(cd) = [(ab)c]d = (abc)d,$$

что и требовалось доказать.

Предположим, что произведение любых n—1 элементов уже определено. Определим произведение n элементов $a_1a_2 \ldots a_n$ как $a_1(a_2 \ldots a_n)$. Таким образом, выражение $a_1a_2 \ldots a_n$ может считаться определенным методом математической (полной) индукции для любого n.

Теорема. *Пусть n - любое натуральное число. Для любого натурального числа $m\le n$ справедливо тождество* (первое правило раскрытия скобок):

$$(a_1, \ldots a_m)(a_{m+1} \ldots a_n)= a_1, \ldots a_n. \qquad (2.1.)$$

Доказательство. Доказательство будем вести методом полной индукции: для n=1 теорема выражает тождество $a_1=a_1$. Предположим, что она справедливая для $n\le k$—1 и докажем ее для $n=k$. Рассмотрим сначала случай n=1. Тогда формула (2.1) превращается в

$$a_1 (a_2 \ldots a_k) = a_1 \ldots a_k.$$

Но это есть *определение* выражения $a_1 \ldots a_k$.

Итак, для данного $n=k$ и m=1 формула (2.1) справедлива.

Теперь, фиксируя $n=k$, предположим, что наша формула доказана для $m=q$—1; докажем ее для $m=q$. Так как при $m=n$ формула (2.1), очевидно, справедлива, можем предположить $q<k$. Тогда, так как теорема предположена справедливой для $n\le k$—1, то

$$(a_1 \dots a_q)(a_{q+1} \dots a_k) = [(a_1 \dots a_{q-1})\, a_q](a_{q+1} \dots a_k).$$

Условие ассоциативности, примененное к трем элементам $(a_1 \dots a_{q-1})$, a_q, $(a_{q+1} \dots a_k)$, дает

$$[(a_1 \dots a_{q-1})\, a_q]\,(a_{q+1} \dots a_k) = (a_1 \dots a_{q-1})\,[a_q\,(a_{q+1} \dots a_k)].$$

Но выражение, стоящее справа в квадратных скобках, есть, по определению,

$$a_q a_{q+1} \dots a_k.$$

Итак, получаем:

$$(a_1 \dots a_q)\,(a_{q+1} \dots a_k) = (a_1 \dots a_{q-1})\,(a_q \dots a_k),$$

но в силу предположенной справедливости формулы (2.1) для $n=k$ и $m=q-1$, правая часть последнего равенства есть $a_1 \dots a_k$. Отсюда следует равенство

$$(a_1 \dots a_q)(a_{q+1} \dots a_k) = a_1 \dots a_k,$$

что и требовалось доказать.

2. Нейтральный элемент. Условие существования нейтрального элемента говорит: *в группе существует некоторый элемент* 1, *такой, что для любого элемента a группы выполнено условие*

$$a \cdot 1 = 1 \cdot a = a. \qquad (2.2)$$

В этом условии не содержится утверждения, что не может быть в данной группе второго элемента $1'$, отличного от 1, но обладающего тум же свойством

$$a \cdot 1' = 1' \cdot a = a \qquad (2.3)$$

для любого a.

Отсутствие такого элемента $1'$ вытекает из следующей более сильной теоремы, которую иногда называют *теоремой о единственности нейтрального элемента.*

Теорема. *Если для какого-нибудь определенного элемента a группы G найден элемент* 1_a, *удовлетворяющий одному из условий*

$$a \bullet 1_a = a \quad или \quad 1 \bullet a = a,$$

это непременно

$$1_a = 1$$

Доказательство. Предположим сначала, что $a \bullet 1_a = a$. Заметим прежде всего, что для любого элемента b имеем

$$b \bullet 1_a = (b \bullet 1) \bullet 1_a,$$

что при замене 1 на $a^{-1} \bullet a$ дает

$$b \bullet 1_a = b \bullet a^{-1} \bullet a \bullet 1_a = b \bullet a^{-1}\,(a \bullet 1_a) = b \bullet a^{-1} a = b.$$

Точно так же имеем

$$1_a \bullet b = (1 \bullet 1_a) \bullet b = a^{-1} \bullet a \bullet 1_a \bullet b = a^{-1}\,(a \bullet 1_a) \bullet b = a^{-1} a \bullet b = b.$$

Итак, *для любого* b имеем

$$b \bullet 1_a = 1_a \bullet b = b\ .$$

Возьмем, в частности, $b = 1$. Получаем

$$1\bullet 1_a = 1. \qquad (2.4)$$

Но по определению элемента 1 имеем, с другой стороны,

$$1\bullet 1_a = 1_a . \qquad (2.5)$$

Из уравнений (2.4) и (2.5) следует $1_a=1$, что и требовалось доказать.

Совершенно аналогичным образом можно вывести тождество $1_a=1$ из предположение $1_a\bullet a = a$.

3. Обратный элемент. Условие существования обратного элемента говорит: *для каждого элемента a существует определенный элемент* a^{-1} *такой, что*

$$a^{-1}\bullet a = a\bullet a^{-1} = 1.$$

Здесь опять-таки утверждается лишь *существование* элемента a^{-1}, а никак не *единственность* его. Докажем эту единственность, т.е. докажем следующую теорему.

Теорема. *Если для данного a имеем какой-нибудь элемент a′, удовлетворяющий одному из условий*

$$a\bullet a' = 1 \quad или \quad a'\bullet a = 1,$$

то непременно

$$a' = a^{-1}.$$

Доказательство. Пусть

$$a\bullet a' = 1.$$

Отсюда следует, что

$$(a^{-1})\bullet (a\bullet a') = a^{-1}\bullet 1 = a^{-1},$$

т.е.

$$(a^{-1}\bullet a)\bullet a' = a^{-1}$$

т.е.

$$1\bullet a' = a^{-1}$$

т.е.

$$a' = a^{-1}.$$

Совершенно аналогичным образом можно из предположения $a'\bullet a=1$ вывести $a'=a^{-1}$.

Итак, для данного a существует *единственный* элемент x, что удовлетворяет равенству $ax=1$ или равенствуа $xa=1$, а именно элемент $x = a^{-1}$.

Возьмем теперь элемент a^{-1}. Элемент a удовлетворяет равенству

$$a^{-1}\bullet a = 1,$$

т.е. является для элемента a^{-1} как раз тем элементом $x = (a^{-1})^{-1}$, о котором только что шла речь. Итак,

$$(a^{-1})^{-1} = a.$$

Пусть теперь a, b — некоторые элементы группы G. Рассмотрим в этой группе уравнения

$$xa = b. \qquad (2.6)$$

Очевидно, что это уравнение имеет решение

$$x = ba^{-1}.$$

Это решение - единственно, так как если элемент c является решением уравнения (2.6), то $ca = b$, значит,

$$c = caa^{-1} = ba^{-1}.$$

Точно так же уравнение

$$ax = b \qquad (2.7)$$

имеет своим единственным решением элемент $a^{-1}b$

Следствие. *Если $ab = ac$, а также, если $ba = ca$, то $b= c$.*

Докажем теперь следующее важное тождество:

$$(ab)^{-1}= b^{-1}a^{-1}. \qquad (2.8)$$

В самом деле, элемент $(ab)^{-1}$ есть единственный элемент x группы, которые удовлетворяющий условию

$$ab\bullet x=1 \qquad (2.9)$$

но

$$ab\bullet (b^{-1}a^{-1}) = a\,(bb^{-1})a^{-1} = a \bullet 1 \bullet a^{-1} = aa^{-1} = 1.$$

Отсюда элемент $x=b^{-1}a^{-1}$ как раз удовлетворяет условию (2.9), таким образом, действительно,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Методом математической индукции легко получаем общий результат

$$(a_1 \ldots a_n)^{-1} = a_n^{-1}\, a_{n-1}^{-1} \ldots a_1^{-1.}$$

Отсюда, в частности, следует тождество

$$c(a_1 \ldots a_n)^{-1} = ca_n^{-1}\, a_{n-1}^{-1} \ldots a_1^{-1.}$$

которое называется вторым правилом раскрытия скобок.

4. Замечания об аксиомах группы. Мы не ставим себе задачей дать *меньшее* число требований, достаточных для определения понятия группы. Действительно, мы потребовали, чтобы нейтральный элемент удовлетворял сразу условиям

$$a \bullet 1 = 1 \bullet a = a,$$

а обратный элемент a^{-1} к любому элементу a условиям

$$a \bullet a^{-1} = a^{-1} \bullet a = 1.$$

Между тем на основании доказанного в пунктах 2 и 3 достаточно было бы потребовать выполнение *одного* какого-нибудь из условий

$$a\bullet 1=a \quad \text{или} \quad 1\bullet a = a,$$

а также *одного* какого-нибудь из условий

$$a \bullet a^{-1} = 1 \quad \text{или} \quad a^{-1} \bullet a = 1.$$

Наконец, заметим, что в определении группы аксиомы II и III, т.е. условие существования обратного элемента ко всякому данному, можно было бы заменить одной следующей аксиомой *(«условие неограниченной возможности деления»):*

Ко всяким двум элементам a и b можно найти элементы x и y такие, что ax=b и ya = b.

5. «Мультипликативная» и «аддитивная» терминология в теории групп. Составными частями понятия группы являются:

а) множество тех объектов (числа, подстановки, повороты и т.д.), которые являются элементами группы;

б) определенная *операция* или *действие,* которое мы назвали умножением и которое позволяет для каждых двух элементов a и b группы найти третий элемент $a \cdot b$ той же группы.

Мы выбрали термин *умножение* для обозначения операции, имеющей место в каждой группе. Выбор того или иного термина на существо дела, конечно, влияния не оказывает; в применении к каждой группе можно было бы говорить о *сложении* ее элементов (а не об умножении их) и рассуждать не на *мультипликативной,* а на *аддитивном* языке. С мультипликативным языком, или, как говорят, с мультипликативной записью группы, мы уже познакомились. Теперь сообразим, какое выражение получают групповые аксиомы на аддитивном языке («в аддитивной записи»).

Прежде всего, мы требуем, чтобы для каждых двух элементов a и b множества G был однозначно определен элемент $a+b$ - сумма двух элементов a и b.

Групповые аксиомы примут при этом следующий вид:

I. Условие ассоциативности. *Для любых трех элементов a, b, c множества G справедливо соотношение*

$$(a + b) + c = a + (b + c).$$

II. Условие существования нейтрального элемента. *Среди элементов множества G имеется некоторый определенный элемент, который называют нейтральным элементом, и обозначают через* 0, *такой, что*

$$a+0=0+a=a$$

при любом выборе элемента a.

III. Условие существования противоположного элемента. *К каждому данному элементу a множества G можно подобрать такой элемент -a того же множества G, что*

$$a + (-a) = (-a)+a = 0.$$

Мы видим, что если операцию, которая определяет данную группу, переименовать из умножения в сложение, то оказывается естественным нейтральный элемент переименовать из единицы в нуль и говорить о *противоположных* элементах ($-a$) вместо обратных от a^{-1}.

Условие коммутативности в аддитивной записи имеет вид

$$a + b = b + a.$$

Мультипликативная терминология является исторически первой и употребляется многими авторами. Наиболее удобно в одних случаях рассуждать о группах на мультипликативном, в других случаях на аддитивном языке. Наконец, имеется много случаев, когда оба языка оказываются одинаково удобными.

Как на пример, где удобнее использовать аддитивный язык, укажем на группу целых чисел: групповой операцией являктся здесь обыкновенное арифметическое сложение, нейтральный элемент есть обыкновенный арифметический нуль, и понятие противоположных чисел имеет также свой обычный арифметический смысл.

Едва или можно спорить о том, что непривычно и неудобно было бы обычное арифметическое сложение называть умножением, нуль единицей и т.д. Однако читатель должен хорошо понять, что, несмотря на все неудобства такого переименования, оно вполне возможно и не приведет ни к какому противоречию до тех пор, пока мы ограничиваемся изучением группы целых чисел, т.е. рассматриваем единственную операцию над целыми числами, а именно, арифметическое сложение.

Если мы наряду с арифметическим сложением стали бы рассматривать еще и умножение (также в элементарном, арифметическом смысле слова), то переименование сложения в умножение, о котором идет речь, конечно, совершенно запутало бы терминологию. Как пример группы, для которой мультипликативный язык более удобен, можно назвать группу Q ненулевых рациональных чисел.

Чтобы покончить с вопросами терминологии, отметим, что становится все более и более общепринятым говорить об общих группах на мультипликативном языке, а о *коммутативных группах* на аддитивном языке (хотя мы только что видели исключение из этого правила, когда упоминали о группе отличных от нуля рациональных чисел).

2.3. Группы подстановок

1. Определение групп подстановок. Если три мужчины Сидор, Иван и Петр сидят на скамйке, предположим, слева направо, то их можно пересадить шестью различными способами, а именно (считая все время слева направо):

(1) Сидор, Иван, Петр;

(2) Сидор, Петр, Иван;

(3) Иван, Сидор, Петр;
(4) Иван, Петр, Сидор;
(5) Петр, Сидор, Иван;
(6) Петр, Иван, Сидор.

Переход от одного какого-нибудь порядка, в котором они сидят, к любому другому порядку называется *подстановкой*. Подстановка записывается так:

$$\begin{pmatrix} Сидор, Иван, Петр \\ Иван, Петр, Сидор \end{pmatrix}$$

и означает, что Иван сел на место Сидора, Петр на место Ивана, Сидор - на место Петра.

В таком смысле можно говорить о подстановках любых предметов. Так как при этом природа пересталяемых предметов значения не имеет, то эти предметы обычно обозначаются числами, и речь идет о *подстановках* чисел. Из трех чисел 1, 2, 3 можно сделать следующие подстановки:

$$\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}$$

Каждая подстановка заключается в том, что на место числа, стоящего в верхней строке, ставится подписанное под ним число из нижней строки. Первая подстановка $\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}$ называется *тождественной,* в ней каждое число остается на своем месте. Вторая подстановка $\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}$ заключается в том, что число 1 остается на месте, число 3 ставится на место числа 2, а число 2 — на место числа 3 и т.д.

Общий вид подстановки из чисел 1, 2, ..., n таков:

$$\begin{pmatrix} 1 & 2 \mathrm{L}\ n \\ i_1 & i_2 \square i_n \end{pmatrix}$$

Здесь $i_1, i_2, ..., i_n$ — это те же числа 1, 2, ..., n, но только записанные в другом порядке. Например, пусть

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,4\,5\,2 \end{pmatrix}$$

тогда, очевидно, $n = 5$, $i_1 = 3$, $i_2 = 1$, $i_3 = 4$, $i_4 = 5$, $i_5 = 2$.

Из n чисел можно сделать $n!$ различных подстановок. Докажем это. Каждая подстановка из чисел 1, 2, ..., n имеет вид

$$\begin{pmatrix} 1 & 2 \mathrm{L} & n \\ i_1 & i_2 \square & i_n \end{pmatrix}$$

где все $i_1, ..., i_n$ различны и каждое из них есть одно из чисел 1, 2, ..., n. Значит, i_1 принимает n возможных значений. После того как одно из них выбрано, мы имеем для выбора значения i_2 уже только n — 1 возможностей. Остановившись на одной из них, имеем для выбора значения i_3 лишь n —2 возможностей. И так далее, пока для i_n останется лишь одна возможность. Всего таким образом имеется $n(n$ — 1) • $(n$ — 2)... 2 • 1 = $n!$ возможностей, что и требовадось доказать.

Возвратимся к подстановкам из трех цифр. По определению, будем считать, что *перемножить* две подстановки, значит последовательно произвести их одну за другой. В результате получится опять подстановка, которую называют ***произведением*** двух данных подстановок.

Перемножим, например, подстановки

$$\begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \text{и} \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}$$

В силу первой подстановки единица заменится двойкой, в силу второй подстановки эта двойка останется на месте; итак, после последовательного осуществления обеих подстановок *единица перейдет в двойку.* Точно так же после последовательного осуществления обеих подстановок *двойка перейдет в тройку, тройка перейдет в единицу:*

$$\begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \bullet \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} \qquad (2.11)$$

Таким же точно образом можно перемножить любые две подстановки. Для того чтобы удобно записать результаты всех этих перемножений, введем следующие обозначения:

$$P_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ P_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ P_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$P_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ P_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ P_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

P_0 — тождественная подстановка.

Тогда имеем следующую *таблицу умножения:*

Таблица 2.4

первый множитель	второй множитель					
	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_0	P_3	P_2	P_5	P_4
P_2	P_2	P_4	P_0	P_5	P_1	P_3
P_3	P_3	P_5	P_1	P_4	P_0	P_2
P_4	P_4	P_2	P_5	P_0	P_3	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

Для того чтобы найти произведение двух подстановок, например, $P_2 \bullet P_4$, необходимо взять строку, в заголовке которой («первый сомножитель») стоит первая подстановка (в нашем случае P_2), и столбец, в заголовке которого («второй сомножитель») стоит вторая подстановка (в нашем случае P_4). В пересечении выбранной строки с выбранным столбцом и будет стоять искомое произведение: $P_2 \bullet P_4 = P_1$.

Проведем вычисление в развернутом виде; пусть

$$P_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ P_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix};$$

с помощью тех же соображений, что и в случае равенства (2.11), получаем

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\bullet\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

т.е. действительно:

$$P_2\bullet P_4 = P_1.$$

Непосредственной проверкой можно убедиться в том, что наше умножение удовлетворяет ассоциативному закону.

Тождественная подстановка P_0 есть единственная подстановка, которая удовлетворяет условию

$$P_0\bullet P_i = P_i\bullet P_0 = P_i$$

для любой подстановки P_i.

Наконец, к каждой подстановке есть обратная к ней, которая дает в произведении с данной тождественную подстановку: обратная подстановка к данной ставит все числа, смещенные подстановкой, на их прежние места. Так, например,

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Чтобы в таблице умножения найти сразу подстановку, обратную к данной подстановке, надо в строке, отмеченной слева данной подстановкой, найти элемент P_0; в заголовке столбца, в котором лежит этот элемент, и стоит подстановка, обратная данной. Имеем, как легко видеть:

$$P^{-1}{}_0 = P_0\,,\quad P_3{}^{-1} = P_3,$$
$$P^{-1}{}_1 = P_1,\quad P_4{}^{-1} = P_4,$$
$$P^{-1}{}_2 = P_2,\quad P_5{}^{-1} = P_5.$$

Итак, умножение подстановок удовлетворяет всем групповым аксиомам и, следовательно, совокупность всех подстановок из трех элементов есть группа. Мы обозначим эту группу через S_3. Группа S_3 конечна, ее порядок равен 6.

Заметим, что умножение подстановок, вообще говоря, не обладает свойством переместительности (коммутативности): произведение двух подстановок зависит, в общем случае, от порядка множителей. Так, мы имеем, например,

$$P_2\bullet P_3 = P_5,\ P_3\bullet P_2 = P_1.$$

Подгруппы. Возникает вопрос: нельзя ли получить группу, взяв не все, а только некоторые из числа наших подстановок (из трех чисел) и сохранив для них тот же закон умножения? Нетрудно убедиться, что ответ на этот вопрос утвердительная.

В самом деле, рассмотрим, например, пары элементов P_0 и P_1. Наша таблица умножения дает нам непосредственно:

$$P_0 \bullet \Gamma_0 = P_0, \quad P_0 \bullet P_1 = P_1, P_1 \bullet P_0 = P_1, \quad P_1 \bullet P_1 = P_0.$$

Мы видим, что все групповые аксиомы выполнены (в частности, $P^{-1}{}_0 = P_0$ и $P^{-1}{}_1 = P_1$), значит, два элемента P_0 и P_1 образуют группу, которая составляет часть группы всех подстановок из трех чисел.

Точно так же можно убедиться, что пары элементов P_0 и P_2 в свою очередь образуют группу, как и пары P_0 и P_5.

Что же касается пары P_0 и P_3 (и также пары P_0 и P_4), то она группы не образует, так как $P_3 \bullet P_3 = P_4$ (т.е. произведение элемента P_3 с самим собой не есть элемент нашей пары). Эти простые соображения оправдывают введение следующего общего определения.

Определение. Пусть задана какая-нибудь группа G; тогда, если множество H, которое состоит из некоторых элементов группы G, образует (при законе умножения, заданном в G) группу, то такая группа H называется *подгруппой* группы G.

Таким образом, пары элементов (P_0, P_1), (P_0, P_2), (P_0, P_5), каждая, являются подгруппами порядка 2 группы S_3. Других подгрупп порядка 2 группа S_3 не имеет: из определения подгруппы следует, что всякая подгруппа H группы G содержит нейтральный элемент группы G, значит, всякая подгруппа порядка 2 группы S_3 имеет вид (P_0, P_i), где i - одно из чисел 1, 2, 3, 4, 5; но мы видели, что i не может равняться ни 3, ни 4, значит, остаются только рассмотренные подгруппы

$$(P_0, P_1), (P_0, P_2), (P_0, P_5).$$

В группе S_3 есть также подгруппа, которая состоит из трех элементов (подгруппа порядка 3). Это будет подгруппа (P_0, P_3, P_4). Читателю предлагается самому убедиться, что эта подгруппа есть единственная подгруппа порядка 3, которая содержится в S_3. Подгрупп порядка 4 и 5 в группе S_3 не имеется вовсе.

Замечание. В том что подгрупп порядка 4 и 5 в группе S_3 не имеется вовсе, можно убедиться, разобрав все 10 подмножеств группы S_3, которые содержат элемент P_0 и состоят из четырех элементов, а также все 5 подмножеств, которые содержат 5 элементов, включая непременно P_0. Однако отсутствие подгрупп порядка 4 и 5 в группе вытекает непосредственно из следующей общей теоремы, которую будет доказано позже: *порядок всякой подгруппы H конечной группы G есть делитель порядка G.*

Итак, подгруппы порядка S_3 суть: три подгруппы порядка 2, а именно: (P_0, P_1), (P_0, P_2), (P_0, P_5), одна подгруппа порядка 3, а именно: (P_0, P_3, P_4).

Таким же образом, как мы изучили группу S_3, можно было бы изучить группу S_4, состоящую из всех подстановок из четырех чисел.

Группа S_4 имеет порядок $1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Да и вообще, при любом n подстановки из n чисел образуют группу S_n порядка $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$

Закон умножения во всех этих группах тот самый: умножить две подстановки из n чисел, означает, последовательно сделать эти подстановки одну за другой.

Отметим, наконец, что группа S_n всех подстановок из n элементов называется *симметрической группой* (подстановок из n элементов).

Любая подгруппа группы S_n называется *группой подстановок* из n элементов.

Для того, чтобы подмножество группы было подгруппой необходимо выполнить ряд условий.

При доказательстве того, что некоторое подмножество H группы G является подгруппой, удобнее всего бывает пользоваться следующей общей теоремой:

Подмножество H группы G тогда и только тогда является подгруппой группы G, *когда выполнены следующие условия:*

1. *Произведение двух элементов a и b из H (в смысле умножения, определенного в G) есть элемент множества H.*

2. *Нейтральный элемент группы G есть элемент множества H.*

3. *Элемент, обратный к какого-нибудь элементу множества H, есть элемент множества H.*

Для доказательства достаточно заметить, что наши условия выражают в точности требования, чтобы операция умножения, которая определена в G, но применяемая лишь к элементам множества H, удовлетворяла всем аксиомам группы (ассоциативности требовать не нужно: будучи выполнена при умножении любых элементов множества G, она тем более выполнена в частном случае, когда эти элементы являются элементами множества H).

Подстановки как отображения. Мы изложили понятие подстановки тем элементарным и несколько кустарным способом, каким это обычно и делается. Если не бояться общематематических терминов, то подстановку из n элементов следует определить просто как *взаимно однозначное отображение f множества данных n элементов на себя.*

Если наши элементы суть числа 1, 2, 3,... ... , n, то подстановка

$$\begin{pmatrix} 1 & 2 & \text{L} & n \\ a_1 & a_2 & \square & a_n \end{pmatrix}$$

задается как функция

$$a_k = f(k), \quad k=1, 2, \ldots, n,$$

причем и значения аргумента и значения функции суть числа 1, 2, 3, ... *n*.

Для двух данных значений аргумента значения функции всегда различны.

В частности, подстановка целиком определена, если для каждого *k* указано значение *f(k)*, т.е. a_k.

Отсюда следует, что совершенно несущественно, в каком порядке записаны числа в верхней строке: важно только, чтобы под числом *k* было подписано именно a_k. Например,

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,4\,3\,5\,1 \end{pmatrix} \text{ и } \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,1\,4\,2 \end{pmatrix}$$

представляют собой две записи одной и той же подстановки. Этому, в сущности, самоочевидному замечанию можно придать и такую форму.

Пусть дана подстановка

$$A=\begin{pmatrix} 1 & 2 & 3 & \text{L} & n \\ a_1 & a_2 & a_3 & \text{L} & a_n \end{pmatrix} \qquad (2.12)$$

Если

$$P=\begin{pmatrix} 1 & 2 & 3 & \text{L} & n \\ p_1 & p_2 & p_3 & \text{L} & p_n \end{pmatrix} \qquad (2.13)$$

есть какая-нибудь подстановка тех же чисел 1, 2, 3, ... , *n*, то подстановка (2.12) может быть записана в виде

$$\begin{pmatrix} p_1 & p_2 & p_3 & \text{L} & p_n \\ a_{p_1} & a_{p_2} & a_{p_3} & \text{L} & a_{p_n} \end{pmatrix}$$

Четные и нечетные подстановки. Пусть дана подстановка

$$A=\begin{pmatrix} 1 & 2 & 3 & \text{L} & n \\ a_1 & a_2 & a_3 & \text{L} & a_n \end{pmatrix}$$

Рассмотрим множество, которое состоит из двух каких-нибудь чисел набора 1, 2,... , *n*, положим для определенности из чисел *i* и *k*. Такое множество назовем *парой* чисел, а именно парой, которая состоит из элементов *i* и *k;* обозначим ее (*i, k).*

Здесь с понятием пары не связано никакое предположение о *порядке* следования элементов пары: (*i, k)* и *(k, i)* суть два записи одной и той же пары. Такие пары элементов, взятые из числа данных *n* элементов, называются также *сочетаниями* из *n* элементов по 2.

Число всех пар, которые можно составить из данных *n* элементов, нетрудно подсчитать. Сначала вычислим, сколько различных *упорядоченных* подмножеств из двух элементов содержится в множестве из *n* элементов. Обозначим число таких подмножеств через A^2_n и покажем, что

$$A^2_n = n(n\text{-}1).$$

Действительно, для того чтобы распределить два элемента, взятых из данных *n* элементов, по двум местам, можно сначала выбрать какой-нибудь один элемент и поместить его на первое место. Это можно сделать *n* способами. На второе место теперь остается *n* — 1 «кандидатов» и значит, *n* — 1 способ выбора второго элемента. Следовательно, всего мы получим *n(n*— 1) способов размещения, что и требовалось доказать.

Пусть C^2_n — число всех пар, которые можно составить из *n* элементов. Покажем, что

$$C^2_n = \frac{1}{2} A^2_n \frac{n(n-1)}{2}$$

или, что то же самое,

$$A^2_n = 2\, C^2_n$$

В самом деле, чтобы образовать упорядоченное множество, которое содержит два элемента из данных *n,* необходимо выделить какие-либо два с этих *n* элементов, что можно сделать C^2_n способами, а затем упорядочить выделенные два элемента, что можно сделать двумя способами. Итак,

$$A^2_n = 2\, C^2_n$$

что и требовалось доказать.

Пара, которая состоит из элементов *i* и *k,* называется *правильной по отношению к подстановке А,* если разности $i - k$ и $a_i - a_k$ имеют один и тот же знак; это значит: если $i<k$, то должно быть $a_i<a_k$; если же $i > k$, то должно быть $a_i > a_k$. В противном случае говорят, что наша пара *неправильна в подстановке А* или образует в ней *инверсию.*

Следовательно, если пара *(i, k)* образует инверсию, то имеем или $i<k$ и $a_i>a_k$ или, наоборот, $i > k$ и $a_i<a_k$. Рассмотрим, в качестве примера, подстановки группы S_3.

В подстановке $P_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ нет ни одной инверсии — все пары правильны.

В подстановке $P_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ имеется единственная инверсия (2, 3), так как при $i = 2$, $k = 3$ имеем $a_i = 3$ и $a_k = 2$.

В подстановке $P_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ имеется единственная инверсия (1, 2).

В подстановке $P_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ имеется две инверсии: (1, 3), (1, 2).

В подстановке $P_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ имеется две инверсии: (1, 3), (2, 3).

В подстановке $P_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ имеется три инверсии: (1, 2), (1, 3), (2, 3).

Определение. Подстановка, которая содержит четное число инверсий, называется *четной* подстановкой; подстановка, которая содержит нечетное число инверсий, *нечетной* подстановкой.

Мы видим, что в группе S_3 четные подстановки $(P_0, P_3$ и $P_4)$ образуют подгруппу. Наша задач - доказать, что это замечание справедливо для любой группы S_n.

Доказательство опирается на некоторые следующие предварительные замечания.

Знаком подстановки A называется число +1, если подстановка A четная, и число —1, если она нечетная.

Отвлекаясь от обычного словоупотребления, назовем теперь *знаком* рационального числа r число +1, если число r положительно, число — 1, если r отрицательно, и число 0, если $r = 0$. Знак числа r в только что установленном смысле обозначим так: *(зн r)*.

При этих обозначениях ясно, что знак подстановки A равен произведению знаков всех $\frac{n(n-1)}{2}$ чисел $\frac{i-k}{a_i-a_k}$, причем дробь

$$\frac{i-k}{a_i-a_k}=\frac{k-i}{a_k-a_i}$$

строится по одному разу для каждой пары, взятой из чисел 1, 2, 3, ... , n.

Этим замечанием мы воспользуемся для доказательства следующей теоремы.

Теорема 1. *Знак произведения двух подстановок равен произведению знаков сомножителей.*

Доказательство. Пусть даны две подстановки:

$$A=\begin{pmatrix}1 & 2 & 3 & \text{L} & n\\ a_1 & a_2 & a_3 & \square & a_n\end{pmatrix},\quad B=\begin{pmatrix}1 & 2 & 3 & \text{L} & n\\ b_1 & b_2 & b_3 & \text{L} & b_n\end{pmatrix}$$

Их произведение есть, очевидно, подстановка

$$A\bullet B=\begin{pmatrix}1 & 2 & 3 & \text{L} & n\\ b_{a_1} & b_{a_2} & b_{a_3} & \text{L} & b_{a_n}\end{pmatrix}$$

Знаки A и B равны соответственно произведениям всех знаков

$$\frac{i-k}{a_i-a_k}\ \text{и}\ \frac{i-k}{b_i-b_k}$$

Но так как можно также написать

$$B=\begin{pmatrix}a_1 & a_2 & a_3 & \text{L} & a_n\\ b_{a_1} & b_{a_2} & b_{a_3} & \text{L} & b_{a_n}\end{pmatrix}$$

то имеем:

знак B равен произведению всех знаков $\frac{a_i-a_k}{b_{a_i}-b_{a_k}}$.

Отсюда следует:

(зн A) • *(зн B)* =произведению всех $\left(зн\ \frac{i-k}{a_i-a_k}\right)\cdot\left(зн\ \frac{a_i-a_k}{b_{a_i}-b_{a_k}}\right)=$

$=$ произведению всех $\left(зн\ \frac{i-k}{a_i-a_k}\cdot зн\ \frac{a_i-a_k}{b_{a_i}-b_{a_k}}\right)=$

$=$ произведению всех $\left(зн\ \frac{a_i-a_k}{b_{a_i}-b_{a_k}}\right).$

Но последнее произведение есть знак подстановки

$$\begin{pmatrix}1 & 2 & 3 & \mathrm{L} & n\\ b_{a_1} & b_{a_2} & b_{a_3} & \square & b_{a_n}\end{pmatrix}$$

т.е. подстановки $A \cdot B$, что и требовалось доказать.

Из доказанной теоремы непосредственно следует: *произведение двух подстановок одинаковой четности (*т.е. произведение двух четных или двух нечетнных подстановок) *есть четная, а произведение двух подстановок различной четности (*т.е. произведение четной и нечетной или нечетной и четной подстановок) *есть нечетная подстановка.* Тождественная подстановка не содержит ни одной инверсии и, следовательно, есть четная подстановка. Далее,

$$A \cdot A^{-1} = E$$

(E - тождественная подстановка), т.е. произведение данной подстановки A и обратной ей подстановки есть четная подстановка; отсюда по только что доказанному следует, что любая подстановка имеет ту же четность, что и обратная ей.

Итак, *произведение двух четных подстановок есть четная подстановка; тождественная подстановка есть четная подстановка, обратная четной подстановке есть четная подстановка.*

Отсюда следует, что совокупность всех четных подстановок из n элементов есть подгруппа группы S_n всех вообще подстановок из n элементов. Группа четных подстановок из n элементов называется ***знакопеременной*** или ***альтернирующей*** группой подстановок из n элементов, и обозначается через A_n.

Теорема 2. *Порядок группы A_n равен* $\frac{n!}{1}$.

Другими словами, в группу A_n входит ровно половина всех подстановок из n элементов. Для того чтобы убедиться в этом,

достаточно установить взаимно-однозначное соответствие между множеством всех четных и множеством всех нечетных подстановок из n элементов. Такое соответствие устанавливается, если выбрать какую-нибудь определенную нечетную подстановку P и каждой четной подстановке A поставить в соответствие подстановку $P \bullet A$. Тогда:

1) каждой четной подстановке будет соответствовать нечетная подстановка;

2) двум различным четным подстановкам будут соответствовать различные нечетные подстановки;

3) каждая нечетная подстановка B окажется поставленной в соответствие одной (и только одной) четной подстановке, а именно: четной подстановке $P^{-1} \bullet B$.

Таким образом, наше соответствие есть взаимно-однозначное соответствие между множеством всех четных и множеством всех нечетных подстановок.

2.4. Изоморфные и циклические группы

Рассмотрим, с одной стороны, группу поворотов R_3 правильного треугольника, а с другой стороны, группу, которая содержится в группе всех подстановок из трех цифр подгруппу A_3, которая состоит из трех элементов P_0, P_3, P_4. Мы обозначили элементы группы R_3 через a_0, a_1, a_2. Установим теперь между элементами группы R_3 и элементами группы A_3 следующее взаимно-однозначное соответствие:

$$a_0 \leftrightarrow P_0,$$
$$a_1 \leftrightarrow P_3,$$
$$a_2 \leftrightarrow P_4.$$

Это соответствие сохраняет умножение в следующем смысле. Если какой-либо элемент в левом столбце может быть записан в виде произведения двух элементов (конечно, того же левого столбца), например, $a_0 a_1 = a_1$ или $a_1 a_1 = a_2$ или $a_1 a_2 = a_0$, и если мы каждый элемент полученного равенства заменим соответствующим элементом правого столбца, то равенство останется справедливым.

Мы видим, что группы R_3 и A_3 хотя и состоят из элементов различной природы (одна группа состоит из поворотов треугольника, а другая из подстановок цифр), но *устроены они одинаково:* таблицы умножения этих групп отличаются лишь обозначениями и, следовательно, заменой обозначений, т.е. переименованием элементов, они могут быть приведены к одинаковому виду. Такие *группы, которые при надлежащем выборе обозначений элементов таблицы*

умножения оказываются тождественными (одинаковыми), называются ***изоморфными*** *группами.*

Обычное понятие изоморфизма высказывают в немного отличной форме. Дело в том, что «переименование» элементов в таблице умножения, о котором шла речь в нашем определении изоморфизма, в сущности говоря, сводится к установлению взаимно однозначного соответствия между элементами двух групп. Мы теперь приведем определение изоморфизма, которое непосредственно исходит из понятия взаимно-однозначного отображения.

Определение I. Пусть дано взаимно-однозначное соответствие

$$g \leftrightarrow g'$$

между множеством всех элементов группы G и множеством всех элементов группы G'. Мы скажем, что это соответствие есть ***изоморфное соответствие*** (или ***изоморфизм)*** между двумя группами, если выполнено условие сохранения умножения, гласящее:

которое бы не было соотношение вида

$$g_1 \cdot g_2 = g_3$$

между элементами одной группы, например, G, соотношение, получаемое при замене элементов g_1, g_2, g_3, группы G соответствующими им в группе G' элементами g'_1, g'_2, g'_3 также оказывается справедливым:

$$g'_1 \cdot g'_2 = g'_3.$$

Определение II. Две группы называются ***изоморфными,*** если между ними возможно установить изоморфное соответствие.

Примечание. Если требовать, чтобы всегда из равенства

$$g_1 \cdot g_2 = g_3 \quad \text{(в группе } G\text{)}$$

следовало равенство

$$g'_1 \cdot g'_2 = g'_3$$

для элементов группы G', соответствующих элементам g_1, g_2, g_3, то имеет место и обратное, а именно:

если для каких-либо трех элементов g'_1, g'_2, g'_3 группы G' имеет место соотношения

$$g'_1 \cdot g'_2 = g'_3,$$

это для элементов g_1, g_2, g_3 группы G, соответствующих элементам g'_1, g'_2, g'_3, также выполнено соотношение

$$g_1 \cdot g_2 = g_3 \qquad (2.15)$$

В самом деле, если бы соотношение (2.15) не имело места, то было бы

$$g_1 \cdot g_2 = g_4 \neq g_3.$$

В силу взаимной однозначности соответствия между G и G' элементу группы g_4 соответствует в группе G' элемент $g'_4 \neq g'_3$ и в силу нашего предположения из

$$g_1 \bullet g_2 = g_4$$

должно вытекать

$$g'_1 \bullet g'_2 = g'_4$$

вопреки потому, что

$$g'_1 \bullet g'_2 = g'_3$$

Теорема. *При изоморфном отображении*

$$g \leftrightarrow g'$$

группы G на группу G' нейтральному элементу одной группы соответствует нейтральный элемент другой группы, и всякой паре взаимно обратных элементов одной группы соответствует пара взаимно обратных элементов другой группы.

В самом деле, пусть g_0 - нейтральный элемент группы G, и пусть ему при данном изоморфном соответствии между группами G и G' соответствует элемент g'_0 группы G'. Докажем, что g_0 есть нейтральный элемент группы G'. В самом деле, так как g_0 — нейтральный элемент группы G, то имеем для произвольного элемента g той же группы

$$g \bullet g_0 = g;$$

в силу изоморфности отображения $g \leftrightarrow g'$ имеем:

$$g' \bullet g'_0 = g',$$

откуда и следует, что g'_0 есть нейтральный элемент группы G'.

Пусть g_1 и g_2 - пара обратных элементов в группе G:

$$g_1 \bullet g_2 = g_0$$

(где g_0 по-прежнему — нейтральный элемент группы G).
Отсюда

$$g'_1 \bullet g'_2 = g'_0$$

Так как g'_0 — нейтральный элемент группы G', то g'_1 и g'_2 взаимно обратны.

Примеры.

1) Показать, что группа, которая состоит из двух элементов a_0 и a_1 с таблицей умножения

	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

изоморфна группе поворотов отрезка (вокруг его середины).

2) Доказать, что все группы порядка 2 изоморфны между собой.

3) Доказать, что все группы порядка 3 изоморфны между собой.

Решение. Пусть a_0, a_1, a_2 — элементы группы; пусть a_0 — единичный элемент. Тогда

$$a_0 \cdot a_0 = a_0; \quad a \cdot a_1 = a_1; \quad a_0 \cdot a_2 = a_2.$$

Не может быть, чтобы $a_1 \cdot a_1 = a_1$, так как тогда $a_1 = a_0$.

Итак,

$$a_1 \cdot a_1 = a_2$$

Аналогично,

$$a_1 \cdot a_2 \neq a_2 \text{ и } a_1 \cdot a_2 \neq a_1.$$

Следовательно,

$$a_1 \cdot a_2 = a_0.$$

Таким же точно образом заключаем, что

$$a_2 \cdot a_1 = a_0.$$

Наконец, поскольку

$$a_2 \cdot a_2 \neq a_2 \text{ (так как тогда имели бы } a_2 = a_0)$$

и

$$a_2 \cdot a_2 \neq a_0 \text{ (так как } a_1 \cdot a_2 = a_0),$$

то

$$a_2 \cdot a_2 = a_1.$$

Итак, для группы порядка 3 возможна лишь одна таблица умножения, а именно:

	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

Таорема Кэли. Докажем следующую теореме, которую сформулировал Кэли.

Теорема. *Всякая конечная группа изоморфна некоторой группе подстановок.*

Доказательство. Пусть G — конечная группа, n — ее порядок, a_1, a_2, ..., a_n — ее элементы, среди них a_1 — нейтральный элемент.

Напишем для каждого i=l, 2, ..., n

$$a_1 \cdot a_i, \quad a_2 \cdot a_i, \ldots, a_n \cdot a_i.$$

Все эти элементы различны; число их равно n; значит, это суть те же элементы $a_1, a_2, ..., a_n$, но только записанные в другом порядке, а именно: пусть

$$a_1 \bullet a_i = a_{i_1}\ , \quad a_2 \bullet a_i = a_{i_2}\ , ..., a_n \bullet a_i = a_{i_n}\ .$$

Итак, элементу a_i соответстует подстановка

$$P_i = \begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_i & a_2 \cdot a_i & \square & a_n \cdot a_i \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_{i_1} & a_{i_2} & \text{L} & a_{i_n} \end{pmatrix}$$

или подстановка

$$P'_u = \begin{pmatrix} 1 & 2 \text{L} & n \\ i_1 & i_2 \text{L} & i_n \end{pmatrix},$$

отличающаяся от подстановки P_i только тем, что в P_i переставляются элементы группы G, а в P'_u — взаимно однозначно соответствующие этим элементам их номера.

Если $i \neq k$, то $P_i \neq P_k$, так как в подстановке P_i под элементом a_1 расположен $a_1 \bullet a_i = a_i$, а в подстановке P_k под элементом a_1 расположен $a_1 \bullet a_k = a_k$, $a_k \neq a_i$.

Итак, имеем взаимно-однозначное соответствие между элементами $a_1, a_2, .., a_n$ группы G и подстановками $P_1, P_2, ..., P_n$.

Теперь нужно доказать, что во-первых, подстановки $P_1, P_2, ..., P_n$ образуют группу по отношению к обычному умножению подстановок и, во-вторых, что эта группа изоморфна группе G.

Заметим прежде всего:

I. *Среди подстановок $P_1, P_2, ..., P_n$ содержится тождественная подстановка.*

В самом деле, так как a_1 есть, по предположению, нейтральный элемент группы G, то подстановка

$$P_1 = \begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_1 & a_2 \cdot a_1 & \text{L} & a_n \cdot a_1 \end{pmatrix}$$

есть тождественная подстановка.

Далее докажем: если $a_h = a_i \bullet a_k$, то $P_h = P_i \bullet P_k$.

Сначала заметим, что

$$\begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_k & a_2 \cdot a_k & \text{L} & a_n \cdot a_k \end{pmatrix}$$

и

$$\begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \text{L} & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \square & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

представляют два записи одной и той же подстановки P_k; в самом деле, обе записи означают, что каждому элементу a группы G ставится в соответствие элемент $a \bullet a_k$ той же группы.

Итак, мы можем записать

$$\begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \text{L} & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \text{L} & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

Заметив это, видим, что подстановка

$P_i \bullet P_k =$

$$= \begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_k & a_2 \cdot a_k & \text{L} & a_n \cdot a_k \end{pmatrix} \bullet \begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \text{L} & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \text{L} & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

на основании общего определения умножения подстановок тождественна с подстановкой

$$\begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \text{L} & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

Но если $a_i \bullet a_k = a_h$, то

$$\begin{pmatrix} a_1 & a_2 & \text{L} & a_n \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \text{L} & a_n \cdot a_i \cdot a_k \end{pmatrix} = P_{h,}$$

т.е.

$$P_i \bullet P_k = P_h$$

Только что доказанное можно сформулировать так:

IIa. *Произведению двух элементов группы G соответствует произведение подстановок, соответствующих этим элементам.*

Отсюда следует:

IIb. *Произведение любых двух из числа подстановок $P_1, P_2, ..., P_n$ есть одна из подстановок $P_1, P_2, ..., P_n$.*

Рассмотрим подстановку P_i, элемент a_i и элемент $a_i^{-1} = a_k$. Так как $a_i \bullet a_k = a_1$, то по только что доказанному $P_i P_k = P_1$; но P_1 есть, как мы видели, тождественная подстановка, поэтому $P_k = P_i^{-1}$.

Итак, мы доказали еще одно утверждение.

III. *Подстановка* P_i^{-1} *для любого* i=1, 2, ..., n *есть одна из подстановок* $P_1, P_2, ..., P_n$.

Из IIb, I и III следует, что совокупность подстановок $P_1, P_2, ..., P_n$ есть группа при обычном определении умножения подстановок. Из IIa следует, что эта группа изоморфна группе G.

Теорема Кэли, таким образом, доказана.

Циклические группы

Пусть a — произвольный элемент группы G. Умножим его на себя, т.е. возьмем элемент $a \cdot a$. Этот элемент *обозначим* через a^2. Точно так же *обозначим* $a \cdot a \cdot a$ через a^3 и вообще положим

$$\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}} = a^n.$$

Рассмотрим, далее, элемент a^{-1} и обозначим последовательно

$a^{-1} \cdot a^{-1}$ через a^{-2},

$a^{-1} \cdot a^{-1} \cdot a^{-1}$ через a^{-3},

.....

$\underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n \text{ раз}}$ через a^{-n}.

Обозначения эти оправданы тем, что, действительно,

$$a^n \cdot a^{-n} = 1.$$

Для доказательства последнего утверждения заметим прежде всего, что в случае n=1 оно очевидно (следует из самого определения a^{-1}). Предположим, что оно верно для n — 1 и докажем в этом предположении его справедливость для n. Имеем

$$a^n \cdot a^{-n} = (a \cdot a^{n-1})\,(a^{-(n-1)} \cdot a^{-1}) = a \cdot \{a^{n-1} \cdot a^{-(n-1)}\} \cdot a^{-1}.$$

Но в силу нашего предположения фигурная скобка равна единице, значит,

$$a^n \cdot a^{-n} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1,$$

что и требовалось доказать.

Мы определили выражение a^n для любого положительного и для любого отрицательного значения n. Положим, наконец, что, по определению, a^0=1.

Пусть теперь p и q — два целых числа. Из наших определений следует, что для любых целых p и q имеем

$$a^p \cdot a^q = a^{p+q}.$$

Мы получаем следующий результат:

Множество H(a) тех элементов группы G, которые могут быть представлены в виде a^n *при целом n с той групповой операцией, которая задана в группе G, образует группу H(a).*

В самом деле:

1) произведение двух элементов, которые принадлежат *H(a),* есть опять элемент *H(a)*;

2) единица принадлежит *H(a);*

3) к каждому элементу a^m из *H(a)* найдется элемент a^{-m}, который также принадлежит *H(a).*

Итак, *H(a)* есть подгруппа *G.* Эта подгруппа называется ***циклической подгруппой группы*** *G, порожденной элементом a.*

Поскольку в группе *H(a)*

$$a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m,$$

то группа *H* (*a*) *коммутативна.*

Мы определили понятие циклической подгруппы *H(a),* порожденной некоторым элементом *a* данной группы *G.* Станем теперь на более абстрактную точку зрения и рассмотрим группу *H* такую, что каждый ее элемент имеет вид a^n для некоторого фиксированного элемента *a* из *H* и некоторого числа *n*. Такую группу мы назовем *циклической группой, порожденой элементом a*, и будем обозначать, как и ранее, *H(a*). Теперь нет нужлы считать, что группа *H=H(a)* содержится в какой-либо объемлющей группе.

Так как группа *H(a)* коммутативна, то ее групповую операцию принято записывать на аддитивном языке. Итак, операция в *H(a)* теперь обозначается +, нейтральный элемент 0, элемент

$$\underbrace{a + a + \ldots + a}_{n \text{ раз}}$$

через *na* и т.д.

Конечные и бесконечные циклические группы.

Группу *H(a*) мы определили как состоящую из всех тех элементов, которые могут быть записаны в виде *ma.* При этом мы не ставили вопроса: будут ли две записи m_1a и m_2a при различных целых m_1 и m_2 всегда давать два различных элемента группы *H(a*) или же может случиться, что $m_1a = m_2a$, хотя m_1 и m_2 различны?

Пусть существуют два различных между собой целых числа m_1 и m_2 таких, что $m_1a=m_2a$. Прибавляя до обеим частям последнего равенства элемент $-m_1a$, получим

$$0 = (m_2 - m_1)a.$$

Следовательно, существуют такие целые числа *m,* что

$$ma = 0.$$

Так как из $ma=0$ следует $-ma=0$, то всегда можно предположить, что число *m* в равенстве $ma=0$ положительно.

Возьмем теперь среди всех натуральных чисел, удовлетворяющих условию $ma=0$, наименьшее и обозначим его через a. Имеем

$$a\neq 0,\quad 2a\neq 0,\ \ldots,\quad (\alpha-1)a\neq 0,\quad \alpha a = 0.$$

Докажем, что все элементы

$$0 = 0a,\ a,\ 2a,\ \ldots,\ (\alpha-1)\,a \qquad (2.16)$$

различны между собой. В самом деле, если бы было

$$pa = qa \quad \text{при} \quad 0\leq p<q\leq \alpha - 1,$$

то имели бы, прибавляя к обеим частям последнего равенства по $-pa$:

$$(q-p)a = 0,$$

а это противоречит определению числа a, так как в наших условиях

$$0< q-p\leq \alpha - 1.$$

Итак, все элементы (2.16) различны между собой. Докажем, что вся группа $H(a)$ исчерпывается элементами (2.16), т.е., что для любого целочисленного m имеем

$$ma = ra, \text{ причем } 0\leq r\leq \alpha - 1.$$

Для этого разделим число m на число α с остатком (по правилу деления целых чисел), а именно - представим его в виде

$$m = q\alpha + r, \qquad (2.17)$$

где q есть неполное частное, а r - остаток, который удовлетворяет условию

$$0\leq r<\alpha.$$

(При отрицательном m остаток r при делении на $\alpha>0$ все же берется положительным. В самом деле, пусть m отрицательно; тогда $-m$ положительно и может быть записано в виде

$$-m = q'\alpha + r', \quad 0\leq r'<\alpha,$$

где q' и r' - неотрицательные. Тогда $m = -q'\alpha - r' = -(q'+1)\alpha+(\alpha-r')$. В этих условиях число $-(q'+1)$ называется неполным частным от деления отрицательного числа m на положительное число α, а неотрицательное число $r=\alpha-r'<\alpha$ называется остатком при этом делении).

Имеем

$$ma = (q\alpha + r)a=q\alpha\cdot a+ra,$$

но

$$q\alpha\cdot a=q(\alpha a)= q\cdot 0 = 0,$$

значит,

$$ma = ra.$$

Итак, если существуют два такие числа m_1 и m_2, что $m_1a=m_2a$, то существует натуральное число α, такое, что вся группа $H(a)$ исчерпывается α различными между собой элементами:

$$0,\ a,\ 2a,\ \ldots.\ (\alpha-1)a, \qquad (2.18)$$

тогда как $\alpha a = 0$.

Положение получается такое: весь ряд

$$..., -ma, ..., -a, 0, a, ..., ma, ...$$

представляет собой бесконечное повторение (в обе стороны – направо и налево) своего «отрезка» (2.18).

В самом деле,

$$(\alpha + 1)a = \alpha a + a = a,$$
$$(\alpha + 2)a = \alpha a + 2a = 2a,$$
$$.....$$
$$(2\alpha - 1)a = \alpha a + (\alpha - 1)a = (\alpha - 1)a,$$
$$2\alpha a = 0,$$
$$(2\alpha + 1)a = a \text{ и т.д.}$$

И аналогично в левую сторону:

$$-a = \alpha a - a = (\alpha - 1)a,$$
$$2a = \alpha a - 2a = (\alpha - 2)a,$$
$$.....$$
$$-(\alpha - 1)a = \alpha a - (\alpha - 1)a = a,$$
$$— \alpha a = 0 \text{ и т.д.}$$

Чтобы найти, какой именно элемент группы $H(a)$ мы получаем, взяв сумму

$$\underbrace{a + a + \ldots + a}_{n \text{ раз}} = ma$$

или

$$\underbrace{(-a) + (-a) + \ldots + (-a)}_{n \text{ раз}} = -ma$$

необходимо разделить m (или $-m$) на α. Неотрицательный остаток r, полученный при этом делении, $0 \le r \le \alpha - 1$ и дает нам ответ на наш вопрос:

$$ma = ra.$$

Отсюда также ясно, как складываются элементы группы $H(a)$:

$$pa + qa = (p + q)a = ra,$$

где r есть остаток при делении $p+q$ на α.

Рассмотрим теперь правильный α-угольник; центральный угол, опирающийся на сторону нашего многоугольника, есть

$$\varphi = \frac{2\pi}{\alpha}$$

Многоугольник переходит сам в себя при поворотах на углы: 0 («тождественный» поворот), φ, 2φ, ..., $(\alpha—1)\varphi$. Если считать тождественными повороты, отличающиеся друг от друга на целое

число полных оборотов, то никакие другие повороты, кроме перечисленных α, не переводят наш многоугольник в самого себя. При этом композиция поворота на угол $p\varphi$ и поворота на угол $q\varphi$ есть поворот на угол $r\varphi$, где r есть остаток при делении $p+q$ на α.

Мы видим: если повороту нашего многоугольника на угол $m\varphi$ поставить в соответствие элемент ma группы $H(a)$ получается изоморфное отображение группы $H(a)$ на группу поворотов правильного α -угольника.

Группы, изоморфные группам поворотов правильных многоугольников, называются ***конечными циклическими группами.***

Итак, если $m_1a = m_2a$ для некоторых m_1 и m_2, то конечная группа $H(a)$ есть конечная циклическая группа.

Таблица сложения для циклической группы порядка m имеет вид

Таблица 2.5

	a_0	a_1	a_2	a_3	...	a_{m-1}
a_0	a_0	a_1	a_2	a_3	...	a_{m-1}
a_1	a_1	a_2	a_3	a_4	...	a_0
a_2	a_2	a_3	a_4	a_5	...	a_1
a_3	a_3	a_4	a_5	a_6	...	a_2
⋮	⋮	⋮	⋮	⋮	⋮⋮	⋮
a_{m-3}	a_{m-3}	a_{m-2}	a_{m-1}	a_0	...	a_{m-4}
a_{m-2}	a_{m-2}	a_{m-1}	a_0	a_1	...	a_{m-3}
a_{m-1}	a_{m-1}	a_0	a_1	a_2	...	a_{m-2}

Эта таблица сложения может служить вторым определениям циклической группы порядка m.

Мы исследовали случай, когда для данного элемента a группы $H(a)$ имеется два таких целых числа m_1 и m_2, что $m_1a = m_2a$.

Рассмотрим теперь случай, когда таких двух целых чисел нет, т.е. когда все элементы

$$..., -ma, —(m— 1)a, ...,$$
$$-3a, —2a, -a, 0, a, 2a, 3a, ..., ma, ... \qquad (2.19)$$

различны. Элементы (2.19) находятся в этом случае во взаимно однозначном соответствии с целыми числами:

элементу ma соответствует целое число m и обратно. Если при этом

$$m_1a + m_2a = m_3a,$$

то

$$m_1 + m_2 = m_3.$$

Отсюда следует, что данное взаимно-однозначное соответствие есть изоморфное соответствие между группой *H(a)* и группой всех целых чисел.

Группы, изоморфные группе целых чисел, называются ***бесконечными циклическими группами.***

Так как группы *A* и *B,* изоморфные одной и той же группе *C,* очевидно, изоморфны между собой, то все бесконечные циклические группы между собой изоморфны. Изоморфны между собой (по той же причине) и все конечные циклические группы того же порядка *m.*

Системы образующих

Вернемся к циклической группе *H(a), порожденной* элементом *a* группы *G*. Элемент *a* в том смысле порождает группу *H(a),* что всякий ее элемент является произведением нескольких сомножителей (в «аддитивной» терминологии: суммой нескольких слагаемых), каждый из которых есть или *a* или a^{-1}. Вместо того чтобы говорить: элемент *a* порождает группу *H*(*a*), часто говорят: элемент *a* есть *образующий элемент* группы *H(a).*

Однако не всякая группа есть циклическая, не всякая группа порождается одним элементом — нециклические группы порождаются не одним, а с необходимостью несколькими (иногда бесконечным числом) элементами; понятию одного образующего элемента приходит на смену понятие *системы образующих* (очевидно, совокупность всех элементов какой-нибудь группы есть (тривиальная) система образующих этой группы. Итак, *всякая группа имеет систему образующих).*

Определение. Некоторое множество *E* элементов группы *G* называется ***системой образующих*** этой группы, если всякий элемент группы *G* есть произведение конечного числа сомножителей, каждый из которых либо есть элемент множества *E,* либо есть обратным некоторому элементу множества *E.*

Микромодуль 4.
Примеры решения типовых задач

Пример 1. Рассмотрим все возможные повороты правильного треугольника вокруг его центра *O* (рис. 2.2).

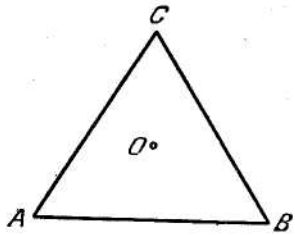


Рис. 2.2.

При этом мы будем считать два поворота совпадающими, если они отличаются один от другого на целое число полных оборотов (т.е. на целочисленное кратное 360°). (Так как поворот на целочисленное кратное 360, очевидно, ставит каждую вершину на ее первоначальное место, то естественно объявить такой поворот совпадающим с нулевым и вообще считать совпадающими два поворота, которые отличаются друг от друга на целое число полных оборотов). Легко видеть, что из всех возможных поворотов треугольника лишь три поворота переводят треугольник в себя, а именно: повороты на 120°, на 240° и так называемый *нулевой* поворот, который оставляет все вершины, а следовательно, и все стороны треугольника на месте. Первый поворот переводит вершину *A* в вершину *B*, вершину *B* в вершину *C*, вершину *C* в вершину *A* (он перемещает, как говорят, вершины *A, B, C* в циклическом порядку). Второй поворот перемещает *A* в *C, B* в *A, C* в *B* (т.е. перемещает в циклическом порядке *A, C, B).*

Пример 2. Рассмотрим совокупность четырех букв a_0, a_1, a_2, a_3, умножение которых определено следующей таблицей:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

или в развернутом виде:

$a_0 \cdot a_0 = a_0$, $a_0 \cdot a_1 = a_1 \cdot a_0 = a_1$,

$a_0 \cdot a_2 = a_2 \cdot a_0 = a_2$, $a_0 \cdot a_3 = a_3 \cdot a_0 = a_3$,

$a_1 \cdot a_1 = a_0$, $a_2 \cdot a_2 = a_0$,

$a_1 \cdot a_2 = a_2 \cdot a_1 = a_3$, $a_2 \cdot a_3 = a_3 \cdot a_2 = a_1$.

$a_1 \cdot a_3 = a_3 \cdot a_1 = a_2$, $a_3 \cdot a_3 = a_0$.

Умножение определено для любых двух букв из числа четырех. Непосредственная проверка показывает, что это умножение удовлетворяет условию ассоциативности и коммутативности.

Буква a_0 обладает основным свойством единицы: произведение двух сомножителей, из которых одно есть a_0, равно другому сомножителю.

Таким образом, условия, аналогичные условиям I, II, III, V из пп. 1-2, оказываются выполненными в «алгебре четырех букв». Для того чтобы убедиться, что условие IV также выполнено, достаточно заметить, что мы положили

$$a_0 \cdot a_0 = a_0, \quad a_1 \cdot a_1 = a_0, \quad a_2 \cdot a_2 = a_0, \quad a_3 \cdot a_3 = a_0,$$

т.е. каждая буква сама себе обратна (дает при умножении с самой собой единицу).

Пример 3. Некоторую «алгебру четырех букв», отличную от предыдущей, можно построить в полной аналогии с тем, что мы делали в первом примере. Рассмотрим квадрат *ABCD* и повороты вокруг его центра, которые переводят фигуру в самое себя. Опять будем считать совпадающими всякие два поворота, отличающиеся друг от друга на целочисленное кратное 360°. Таким образом, будем иметь всего четыре поворота, а именно: нулевой, поворот на 90°, на 180° и на 270°.

Эти повороты обозначим соответственно через a_0, a_1, a_2, a_3. Если под умножением двух поворотов понимать снова последовательное

осуществление двух поворотов, то получим следующую таблицу умножения, вполне аналогичную второму примеру:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

Таким же точно образом как в этом и в первом примере, можно рассматривать повороты правильного пяти-, шести- и вообще *n*-кутника.

Пример 4. Рассмотрим плоскость с выбранной на ней системой декартовых координат. Обозначим через *G* множество тех точек *P=(x, y),* обе координаты которых *x* и *y* - суть целые числа. Установим следующее правило сложения точек: суммой двух точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ называется точка $P_3 = (x_3, y_3)$ с координатами $x_3=x_1+x_2$ и $y_3=y_1+y_2$. Легко убедиться, что это определение сложения превращает множество *G* в коммутативную группу и что точки (0, 1) и (1; 0) составляют систему образующих этой группы.

Замечание. Читатель, знакомый с понятием комплексного числа, сразу поймет, что только что построенная группа изоморфна группе целых комплексных чисел (со сложением в качестве групповой операции). При этом комплексное число $x+iy$ называется целым, если *x* и *y* суть целые числа.

Микромодуль 4.
Идивидуальные тестовые задачи

1. Найти произведение двух подстановок с использованием таблицы умножения (таблица 2.4).

2. Показать, что группа, которая состоит из двух элементов a_0 и a_1 с таблицей умножения изоморфна группе поворотов отрезка (вокруг его середины).

	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

3. Доказать, что все группы порядка 2 изоморфны между собой.
4. Доказать, что все группы порядка 3 изоморфны между собой.
5. Доказать, что любая коммутативная группа порядка 4 изоморфна или клейновской группе, или группе поворотов правильного четырехугольника (две последние группы между собой неизоморфны; почему?).
6. Доказать, что группа всех положительных чисел (с арифметическим умножением как групповой операции) изоморфна группе всех действительных чисел (с арифметическим сложением как групповой операции).
Указание: изоморфное отображение осуществляется логарифмированием.
7. Доказать, что всякая система натуральных чисел, наибольший общий делитель которых равен единице, есть система образующих группы всех целых чисел.

Микромодуль 5.
Группы самосовмещений и ивариантные подгруппы

2.5. Простейшие группы самосовмещений

2.5.1. Примеры и определения групп самосовмещений геометрических фигур

1. Самосовмещения правильных многоугольников в их плоскости. Большой и очень важный класс разнообразных групп как

конечных, так и бесконечных составляют группы «самосовмещений» геометрических фигур. Под ***самосовмещением*** данной геометрической фигуры F понимают такое *перемещение фигуры* F (в пространстве или на плоскости), *которое переводит* F *в самое себя,* т.е. совмещает фигуру F с самой собой.

Мы уже познакомились с простейшими группами самосовмещений, а именно: с группами поворотов правильных многоугольников.

Пусть дан в плоскости правильный многоугольник $A_0A_1...A_n$ (рис. 2.3), например, правильный восьмиугольник $A_0A_1A_2A_3A_4A_5A_6A_7$ (вершины все перенумерованы подряд в одном направлении, например, против часовой стрелки).

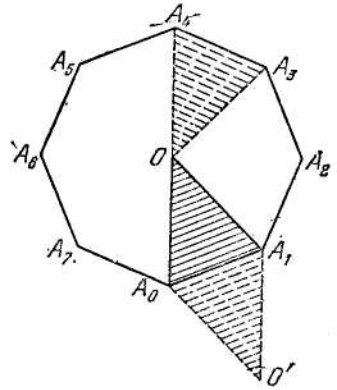


Рис. 2.3

Требуется найти те перемещения многоугольника в его плоскости, которые совмещают его с самим собой. При этом перемещении всякая вершина многоугольника должна перейти в вершину, всякая сторона - в сторону, а центр многоугольника - в самого себя. Пусть при некотором определенном перемещении вершина A_0 перейдет, например, в A_k (на рисунке k=4).

Тогда сторона A_0A_1 должна перейти или в сторону A_kA_{k+1} или в сторону A_kA_{k-1}. Но если бы сторона A_0A_1 перешла в сторону A_kA_{k-1}, то треугольник A_0A_1O перешел бы в треугольник $A_kA_{k-1}O$. Этот последний треугольник можно было бы, передвигая его в плоскости, перевести у положение A_0A_1O', что является зеркальным отражением треугольника $A_0A_1Oб$ относительно стороны A_0A_1. В результате оказалось бы, что мы треугольник A_0A_1O перемещением в его плоскости перевели в его зеркальное отражение, а это невозможно.

Итак, сторона A_0A_1 должна перейти в сторону A_kA_{k+1}. Точно таким же образом мы убеждаемся в том, что сторона A_1A_2 переходит в $A_{k+1}A_{k+2}$, сторона A_2A_3 переходит в $A_{k+2}A_{k+3}$ и т.д. Другими словами, наше перемещение есть поворот многоугольника в его плоскости на угол $k\bullet(2\pi/n)$. Итак, мы показали, что:

а) *всякое самосовмещение правильного n-угольника в его плоскости есть поворот многоугольника на угол* $k(2\pi/n)$*, где k — целое число;*

б) таким образом, самосовмещений имеется n;

в) эти самосовмещения, как мы знаем, образуют группу.

2. Самосовмещение правильного многоугольника в трехмерном пространстве. Предыдущее рассуждение существенно предполагало, что мы рассматриваем лишь самосовмещения многоугольника в его плоскости. Если бы мы рассматривали совмещения n-угольника с самим собой в пространстве, то к перечисленным поворотам прибавились бы еще «опрокидывания» многоугольника, т.е. повороты на угол 180° вокруг осей симметрии многоугольника. Осей симметрии правильный n-угольник имеет n: в случае четного n осями симметрии являются $n/2$ прямых, которые соединяют пары противоположных вершин многоугольника, и $n/2$ прямых, которые соединяют середины его противоположных сторон; в случае нечетного n оси симметрии суть прямые, соединяющие вершины с серединами противоположных сторон многоугольника. Доказательство того, что n поворотами и n «опрокидываниями» правильного n-угольника исчерпываются все самосовмещения n-угольника, т.е. все перемещения его в пространстве, которые переводят многоугольник в самого себя, содержится в рассуждениях в п. 2.5.3 этого раздела.

3. Общее определение группы самосовмещений данной фигуры в пространстве или на плоскости. Пусть в пространстве или на плоскости дана фигура F. Рассмотрим все самосовмещения этой фигуры, т.е. все перемещения ее (в пространстве или на плоскости), совмещающие эту фигуру с нею самой.

В качестве произведения $g_1\bullet g_2$ двух самосовмещений g_1 и g_2 определим перемещение, которое возникает в результате последовательного осуществления сначала перемещения g_2, а потом перемещения g_1. Очевидно, что перемещение $g_1\bullet g_2$ также является совмещением фигуры F с собой, в предположении, что перемещения g_1 и g_2 порознь являются таковыми.

Совокупность всех самосовмещений фигуры F с только что определенной операцией произведения *образует группу*. В самом деле, умножение перемещений удовлетворяет условию ассоциативности;

далее, в совокупности самосовмещений имеется *единичное,* или *тождественное,* самосовмещение (а именно, «покой», т.е. перемещение, оставляющее каждую точку фигуры на месте). Наконец, к каждому самосовмещению g имеется обратное ему самосовмещение g^{-1} (передвигающее каждую точку назад, в исходное положение, из положения, которое оно заняло после перемещения g).

2.5.2. Группы самосовмещений прямой и окружности

Группы самосовмещений правильных многоугольников — *конечны*. В этом же пункте мы познакомимся и с другими конечными группами самосовмещений, а именно, с группами самосовмещений некоторых многогранников. А сейчас дадим несколько примеров бесконечных групп самосовмещений.

Первый пример— группа всех самосовмещений прямой в какой-либо проходящей через нее плоскости. Эта группа состоит: из *скольжений* прямой по себе (самосовмещения *первого рода)* и из поворотов прямой в выбранной плоскости на угол 180° вокруг любой из ее точек (самосовмещение *второго рода).*

Группа самосовмещений прямой некоммутативна.

Чтобы убедиться в этом, достаточно перемножить два самосовмещения, из которых одно первого, а другое — второго рода: результат этого перемножения изменится при изменении порядка сомножителей. Очевидно, *все самосовмещения второго рода можно получить, перемножая* (т.е. последовательно осуществляя) *всевозможные скольжения прямой с одним каким-нибудь поворотом* на 180° (т.е. поворотом на 180° вокруг одной определенной, но произвольно выбранной точки этой прямой).

Скольжение прямой по самой себе составляют подгруппу всех ее самосовмещений. Эти скольжения суть единственные перемещения прямой самой по себе. Каждому скольжению прямой самой по себе взаимно однозначным образом соответствует некоторое действительное число, которое указывает, на какую длину и в котором с двух возможных направлений мы сдвинули прямую по ней самой. Отсюда легко заключить, что *группа всех скольжений прямой по самой себе изоморфна группе действительных чисел* (с операцией обычного арифметического сложения в качестве групповой операции).

Как второй пример рассмотрим группу всех самосовмещений окружности в ее плоскости. Эта группа состоит из всевозможных поворотов окружности в ее плоскости вокруг ее центра, причем, как всегда, повороты на углы, кратные 2π, считаются тождественными.

Каждому элементу нашей группы соответстует, таким образом, определенный угол φ. Измеряя этот угол в отвлеченной (радианной) мере, мы получим действительное число *x*. Но, так как угды, отличающиеся на целочисленные кратные 2π, определяют один и тот же поворот окружности, то каждому элементу группы поворотов окружности соответстует не только данное число *x,* но и все числа вида $x+2\pi\cdot k$, где k — любое целое число.

С другой стороны, каждому действительному числу *x* соответстует единственный вполне определенный поворот окружности, а именно: поворот на угол, отвлеченная мера которого равна *x*. Таким образом, между поворотами окружности и действительными числами установлено следующее соответствие: *каждому действительному числу x соответстует один-единственный вполне определенный поворот, а именно поворот на угол x. Но при этом каждый поворот оказывается поставленным в соответствие не одному, а бесконечному множеству действительных чисел, которые все отличаются друг от друга на целочисленные кратные* 2π.

Группа поворотов окружности обозначается ***SO(2).***

Все только что рассмотренные группы, а именно: группы самосовмещений прямой и окружности, имеют следующие особенности: все эти группы состоят из перемещений соответствующей фигуры в себя. Другими словами, в течении каждого перемещения вся фигура - окружность, прямая - остается совмещенной из самой собой. Это свойство не имеет места при самосовмещениях правильных многоугольников: при этих последних конечное положение перемещающейся фигуры, совмещено с начальным, но промежуточные положение, которые фигура занимает в процессе перемещения, отличаются от ее начального и конечного положений. Таково же положение вещей и при перемещениях многогранников, к которым мы сейчас переходим.

2.5.3. Группы поворотов правильной пирамиды и двойной пирамиды

1. Пирамида. Группа поворотов правильной (рис. 2.4) *n*-угольной пирамиды (вокруг ее осы), изоморфна группе поворотов правильного *n*-угольника, лежащего в ее основании; эта группа есть, таким образом, циклическая группа порядка *n*. Легко убедиться, что поворотами пирамиды вокруг оси (на углы $0, (2\pi/n), \ldots, (n-1)(2\pi/n)$) исчерпываются все перемещения, которые совмещают пирамиду с самой собой.

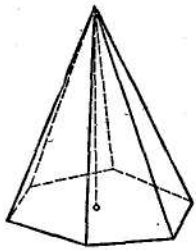


Рис. 2.4

2. Двойная пирамида (диэдр). Определим теперь группу самосовмещений тела, известного под названием «двойной правильной *n*-угольной пирамиды» или *n*-угольного *диэдра* (рис. 2.5).

Это тело состоит из правильной *n*-угольной пирамиды и ее зеркального отражения в плоскости основания. Мы сейчас доеажем, что группа самосовмещений диэдра состоит из следующих элементов:

1) поворотов вокруг оси пирамиды (на углы 0, $(2\pi/n)$, ..., $(n-1)(2\pi/n)$)

2) так называемых опрокидываний, т.е. поворотов на угол π вокруг каждой из осей симметрии *«основания диэдра»*, т.е. правильного многоугольника, являющегося общим основанием обеих пирамид, составляющих диэдр. Таких осей симметрии имеется, как мы видели, *n*, так что перемещений второго рода имеется тоже *n*.

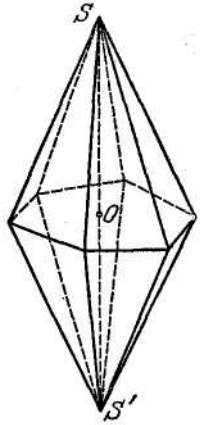


Рис. 2.5

Число всех полученных перемещений есть, таким образом, $2n$. Чтобы убедиться в том, что (за исключением случая $n=4$) не имеется никаких других перемещений, которые переводят n-угольный диэдр в самого себя, заметим прежде всего, что в случае $n\neq 4$ всякое совмещение диэдра с самим собой должно либо оставлять на месте точки S и *S′ (самосовмещение первого рода),* либо менять их местами *(самосовмещение второго рода).* Далее, основание диэдра должно переходить при таком перемещении в самого себя. Заметим, наконец, что произведение (т.е. последовательное осуществление) двух самосовмещений первого рода дает самосовмещение первого рода, произведение самосовмещений первого рода с самосовмещениями второго рода дает самосовмещение второго рода, а произведение двух самосовмещений второго рода дает самосовмещение первого рода.

При этом произведение двух самосовмещений, из которых одно — первого, а другое - второго рода, зависит от порядка сомножителей: если a — самосовмещение первого, а b — самосовмещение второго рода, то $ab = ba^{-1}$.

Рассмотрим сначала самосовмещение первого рода. При таких самосовмещениях основание переходит в само себя, оставаясь в своей плоскости; оно испытывает, таким образом, поворот на один из углов:

$$0, (2\pi/n), ..., (n-1)(2\pi/n).$$

Таким образом, и все перемещение диэдра оказывается поворотом вокруг оси диэдра на тот же угол.

Итак, самосовмещение первого рода имеется (включая тождественное самосовмещение, т.е. покой) ровно n. Эти самосовмещения суть не что иное, как повороты диэдра вокруг его оси на углы

$$0, (2\pi/n), ..., (n-1)(2\pi/n).$$

Пусть дано некоторое целиком определенное самосовмещение второго рода, т.е. такое самосовмещение диэдра с самим собой, при котором вершины S и S' меняются местами.

Произведем после данного самосовмещения второго рода некоторое целиком определенное опрокидывание диэдра, т.е. перемещение, заключающееся в повороте диэдра на угол π вокруг *одной какой-нибудь, раз навсегда выбранной, оси симметрии основания.* Получим самосовмещение первого рода (на самом деле, этот поворот есть самосовмещение второго рода, а произведение двух самосовмещений второго рода есть самосовмещение первого рода), т.е. поворот диэдра вокруг его оси.

Итак, всякое самосовмещение второго рода переходит после одного и того же опрокидывания в некоторое самосовмещение первого рода.

Отсюда следует: всякое самосовмещение второго рода можно получить, производя (до или после некоторого самосовмещения первого рода) одно и то же опрокидывание. Отсюда, далее следует, что число самосовмещениий второго рода равно числу самосовмещениий первого рода, т.е. n.

С другой стороны, ясно, что все опрокидывания являются самосовмещениями второго рода. Так как этих опрокидываний имеется ровно n, то ими и исчерпывается вся совокупность самосовмещений второго рода.

Итак, мы доказали следующее: *группа самосовмещений n-угольного диэдра есть некоммутативная группа порядка* $2n$*, состоящая из n поворотов вокруг оси диэдра SS' и из n опрокидываний, т.е. поворотов на угол* π *вокруг осей симметрии основания диэдра. Все n опрокидываний получаются умножением одного из них на n поворотов диэдра вокруг его оси SS'.*

Так как все повороты диэдра вокруг его оси получаются умножением с самим собой одного поворота - а именно, поворота на угол $2\pi/n$, то группа всех самосовмещений имеет систему образующих из двух элементов: поворота на угол $2\pi/n$ и одного какого-нибудь опрокидывания.

Случай $n=4$ является особым потому, что частным случаем четырехугольного диэдра является октаэдр, который допускает не 8, как мы увидим ниже, а 24 самосовмещения. Это объясняется тем, что при самосовмещении некоторых четырехугольных диэдров, а именно правильных октаэдров, вершина S может совмещаться не только с вершиной *S'*, но и с каждой из вершин основания. Одно из необходимых для этого условий - одинаковое число граней (а также и ребер), примыкающих к каждой вершине, выполнено, очевидно, в случае любого четырехугольного диэдра. В случае правильного октаэдра и все углы, телесные и плоские, при любых двух вершинах оказываются соответственно равными так же, как и сами грани и ребра.

3. Случай вырождения: группы поворотов отрезка и ромба. Наименьшее всего число вершин, которое может иметь многоугольник, есть 3; в известном смысле, однако, отрезок может рассматриваться как случай «вырождения» многоугольника, или, как «многоугольник с двумя вершинами».

Возможность такой точки зрения, в частности, подтверждается тем, что группа самосовмещений отрезка в какой-нибудь плоскости, содержей его, есть циклическая группа, и притом порядка 2: она состоит из тождественного самосовмещения и из поворота отрезка на угол 180°.

Подобно этому равнобедренный треугольник будет случаем вырождения правильной пирамиды: группа самосовмещений равнобедренного треугольника в пространстве также есть группа порядка 2.

Далее, вырождением диэдра или двойной пирамиды будет ромб. Группа самосовмещений или поворотов ромба (в пространстве) состоит из четырех элементов: из тождественного преобразования a_0, из поворотов a_1 и a_2 вокруг каждой из диагоналей ромба на 180° и из поворота a_3 ромба в его плоскости вокруг его центра на 180° (этот поворот есть произведение двух предыдущих). (Рассматривая одну из диагоналей ромба как «основаеие», другую - как ось диэдра, мы получим эти четыре перемещения из поворотов вокруг «оси» (на угол π) и «опрокидывния» относительно основания). Таблица умножения для нашей группы имеет вид:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

Она совпадает с таблицей умножения клейновской группы порядка 4, приведенной нами в качестве второго примера в раз. 2.1, п. 4. В этом легко убедиться непосредственно, а еще проще — рассматривая вместо группы самых поворотов ромба изоморфную ей группу подстановок его четырех вершин *A, B, C, D:* очевидно, поворотам a_0, a_1, a_2, a_3 соответствуют следующие подстановки вершин (мы принимаем за a_1 поворот вокруг диагонали *CD*, за a_2 — поворот вокруг диагонали *AB):*

$$\begin{pmatrix} A\,B\,C\,D \\ A\,B\,C\,D \end{pmatrix}, \begin{pmatrix} A\,B\,C\,D \\ B\,A\,C\,D \end{pmatrix}, \begin{pmatrix} A\,B\,C\,D \\ A\,B\,D\,C \end{pmatrix}, \begin{pmatrix} A\,B\,C\,D \\ B\,A\,D\,C \end{pmatrix}.$$

2.5.4. Группа поворотов правильного тетраэдра

Под тетраэдром здесь и везде дальше понимаем *правильный* траедр. Для определения всех самосовмещений тетраэдра $A_0A_1A_2A_3$ (рис. 2.6) рассмотрим сначала те из них, которые одну определенную вершину, пусть например A_0, оставляют недвижимой.

Такие самосовмещение совмещают и треугольник $A_1A_2A_3$ с самим собой, поворачивая его вокруг его центра B_0 на один из углов 0, $2\pi/3$, $4\pi/3$. Отсюда следует, что самосовмещений тетраэдра $A_0A_1A_2A_3$, оставляющих вершину A_0, на месте, имеется ровно три: тождественное самосовмещение a_0, оставляее на месте все элементы тетраэдра, и два поворота a_1 и a_2 вокруг осы A_0B_0 соответственно на углы $2\pi/3$ и $4\pi/3$. Обозначим теперь через x_i какое-нибудь определенное самосовмещение тетраэдра, переводящее вершину A_0 в вершину A_i, i=1, 2, 3 (вершина A_0 переводится в A_1 и A_3, например, посредством поворотов вокруг оси A_2B_2 (соединяющей вершину A_2 с центром противоположной грани); A_0 переводится в A_2, например, посредством поворота вокруг оси A_3B_3); через x_0 обозначим снова тождественное самосовмещение.

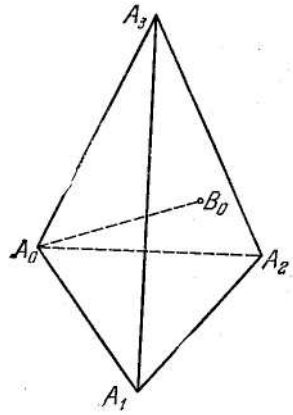


Рис. 2.6

Докажем, что всякое самосовмещение b тетраэдра может быть записано в виде

$$b = a_i \cdot x_k, \qquad (2.20)$$

где $i = 0, 1, 2$ и $k = 0, 1, 2, 3$ являются однозначно определенными (последнее утверждение означает, что если $b=a_i \cdot x_k$, $b'= a_{i'} \cdot x_{k'}$ и по крайней мере одно из неравенств $i \neq i'$, $k \neq k'$ имеет место, то непременно $b \neq b'$).

Итак, пусть дано какое-нибудь самосовмещение b; оно переводит вершину A_0 в некоторую определенную вершину A_k, где $k = 0, 1, 2, 3$; но тогда самосовмещение bx_k^{-1} оставляет вершину A_0 на месте и есть следовательно, некоторое вполне определенное a_i, так что $bx_k^{-1}=a_i$ и $b=a_ix_k$, где i и k определены однозначно. Так как и обратно каждой паре (i, k) соответствует по записи (2.20) некоторое самосовмещение тетраэдра, то имеется взаимно однозначное соответствие между всеми самосовмещениями тетраэдра и всеми парами (i, k), где i принимает значения 0, 1, 2, а k — значения 0, 1, 2, 3. Отсюда следует, что имеется ровно 12 самосовмещений тетраэдра.

Каждое самосовмещение тетраэдра означает некоторую подстановку его вершин, т.е. некоторую подстановку их номеров 0, 1, 2, 3. Но всех подстановок с четырех элементов имеется 24; из них, как мы сейчас видели, только 12 осуществляются перемещениями тетраэдра в пространстве. Посмотрим, какие это перемещение и какие подстановки.

Назовем для краткости *граневой медианой* тетраэдра прямую, которая проходит через какую-нибудь вершину A_i тетраэдра и через центр B_i грани, противоположной этой вершине. *Реберной медианой* назовем прямую, которая проходит через середины двух каких-нибудь взаимно противоположных ребер тетраэдра.

Каждой граневой медиане соответствует два нетождественных самосовмещения тетраэдра, а именно: поворот вокруг этой медианы на углы $2\pi/3$ и $4\pi/3$. Всего, таким образом, получаем восемь поворотов, которые в виде подстановок номеров записываются так:

$$a_1=\begin{pmatrix}0&1&2&3\\0&2&3&1\end{pmatrix},\quad a_2=\begin{pmatrix}0&1&2&3\\0&3&1&2\end{pmatrix},\quad a_3=\begin{pmatrix}0&1&2&3\\2&1&3&0\end{pmatrix},$$
$$a_4=\begin{pmatrix}0&1&2&3\\3&1&0&2\end{pmatrix},\quad a_5=\begin{pmatrix}0&1&2&3\\1&3&2&0\end{pmatrix},\quad a_6=\begin{pmatrix}0&1&2&3\\3&0&2&1\end{pmatrix},$$
$$a_7=\begin{pmatrix}0&1&2&3\\1&2&0&3\end{pmatrix},\quad a_8=\begin{pmatrix}0&1&2&3\\2&0&1&3\end{pmatrix}. \qquad (2.21)$$

Вокруг каждой реберной медианы имеем один нетождественный поворот на угол π, что дает нам (так как реберных медиан имеется три) еще три поворота, которые записываются в виде подстановок:

$$a_9 = \begin{pmatrix} 0\,1\,2\,3 \\ 1\,0\,3\,2 \end{pmatrix}, a_{10} = \begin{pmatrix} 0\,1\,2\,3 \\ 2\,3\,0\,1 \end{pmatrix}, a_{11} = \begin{pmatrix} 0\,1\,2\,3 \\ 3\,2\,1\,0 \end{pmatrix}. \qquad (2.22)$$

Эти 11 поворотов вместе с тождественным самосовмещением («тождественным поворотом») a_0 и дают нам все 12 самосовмещений тетраэдра. Каждое из них является поворотом вокруг одной из семи осей симметрии тетраэдра (эти семь осей симметрии суть четыре граневые и три реберные медианы тетраэдра. В широком смысле слова осью симметрии геометрической фигуры называется всякая прямая, вокруг которой фигуру можно повернуть на отличный от нуля угол таким образом, что она совместится сама с собой. Заметим в связи с этим, чго всякое перемещение твердого тела в пространстве, оставляющее недвижимой какую-нибудь точку *O* этого тела, является поворотом этого тела вокруг некоторой оси, которая проходит через точку *O*); поэтому группу самосовмещений и называют группой поворотов тетраэдра.

Легко проверить, что все подстановки (2.21) и (2.22) - четные; так как всех четных подстановок из четырех элементов (вершин тетраэдра) имеется 12, то перед нами взаимно однозначное и изоморфное соответствие между группой поворотов тетраэдра и знакопеременной группой подстановок из четырех элементов.

Посмотрим теперь, какие подгруппы группы поворотов тетраэдра. В ней, как и во всякой группе, имеется прежде всего две так называемые несобственные подгруппы: это, во-первых, вся рассматриваемая группа и, во-вторых, подгруппа, которая состоит из одного нейтрального элемента. Нас интересуют остальные, так называемые *собственные* подгруппы поворотов тетраэдра. (Подгруппа H группы G называется *собственной,* если она содержит по крайней мере два элемента и $H \neq G$). Их имеется восемь. Прежде всего заметим, что произведение поворотов на угол π вокруг двух разных реберных медиан дает нам поворот на тот же угол π вокруг третьей реберной медианы (в этом можно убедиться как геометрически, так и непосредственным умножением двух каких-нибудь из подстановок (2.22)). Отсюда следует, что повороты на угол π вокруг всех трех реберных медиан образуют вместе с тождественным поворотом группу четвертого порядка; она изоморфна клейновской группе (т.е. группе всех поворотов ромба). Эту группу обозначим через H. Среди всех подгрупп группы поворотов тетраэдра она имеет наибольший порядок. В ней содержатся три подгруппы второго порядка, которые состоят из поворотов на углы 0 и π вокруг каждой

данной реберной медианы. Эти подгруппы обозначим через H_{01}, H_{02}, H_{03}. Кроме указанных групп имеются еще четыре подгруппы третьего порядка, а именно: H_i, i=0, 1, 2, 3, состоящие каждая с трех поворотов на углы 0, 2π/3, 4π/3 вокруг соответствующей граневой медианы.

Для того чтобы доказать, что никаких других подгрупп в группе поворотов тетраэдра нет, достаточно показать, что любые два отличных от нуля элемента, взятые из двух различных групп H_i или взятые один из какой-нибудь группы H_i, а другой из какой-нибудь группы H_{0k}, уже дают систему образующих всей группы поворотов тетраэдра. Для этого в свою очередь достаточно рассмотреть любые два элемента из числа элементов a_1, a_3, a_5, a_7, например, a_1 и a_3, а также какой-нибудь из элементов a_2, a_4, a_6, a_8 и какой-нибудь из элементов a_9, a_{10}, a_{11}. Можно достигнуть того же результата и непосредственно вычислениями. Следующие тождества доказывают, например, что элементы a_1 и a_3 составляют систему образующих группы поворотов тетраэдра:

$$
\begin{aligned}
a_0 &= a_1 a_1^{-1}, & a_7 &= a_1 a_3 a_1^{-1},\\
a_2 &= a_1^2, & a_8 &= a_1^2 a_3,\\
a_4 &= a_3^2, & a_9 &= a_3^{-1} a_1 a_3^2,\\
a_5 &= a_3^{-1} a_1 a_3, & a_{10} &= a_1^{-1} a_3,\\
a_6 &= a_3^{-1} a_1^2 = a_3, & a_{11} &= a_3 a_1.
\end{aligned}
$$

Не следует думать, что каждый элемент единственным образом выражается через образующие; например, $a_7 = a_1 a_3 a_1^{-1}$ и в тот же время

$$a_7 = a_3^{-1} a_1^{-1} a_3 a_1 a_3.$$

Группа поворотов тетраэдра некоммутативна.

Например,

$$a_1 a_3 = a_{10}, \quad a_3 a_1 = a_{11}.$$

Следующая общая теорема говорит: *некоторое множество E элементов группы G тогда и только тогда является системой образующих этой группы, когда не существует никакой собственной подгруппы группы G, которая содержала бы все элементы множества E.*

Пользуясь этой теоремой, можно, например, найти все системы образующих группы поворотов тетраэдра (состящие не более чем из трех элементов каждая).

Уже из этого примера будет видно, как много различных систем образующих может иметь конечная группа.

2.5.5. Группы поворотов куба и октаэдра

1. Для того чтобы установить все самосовмещения куба, сделаем так же, как и в случае тетраэдра: рассмотрим сначала лишь те самосовмещения куба *ABCDA'B'C''* (рис. 2.7), которые одну из вершин,— пусть *A*, - совмещают с самой собой.

При каждом самосовмещении куба вершина переходит в вершину, ребро в ребро, грань в грань; также и диагонали куба переходят в самих себя. Если данное самосовмещение оставляет вершину *A* неподвижной, то оно оставляет неподвижной и диагональ *ACC'* (так как существует лишь одна диагональ куба, которая выходит из вершины *A*). Итак, наше самосовмещение есть поворот куба вокруг диагонали *ACC'*. Таких поворотов, кроме тождественного, имеется два: на угол $2\pi/3$ и на угол $4\pi/3$.

Итак, есть всего три самосовмещения куба, которые переводят вершину *A* в саму себя. Но вершину *A* надлежащее подобранным поворотом можно перевести в каждую из восьми вершин куба; отсюда, повторяя те же соображения, которые и в случае тетраэдра, легко выводим, что всех самосовмещений куба имеется $3 \cdot 8 = 24$.

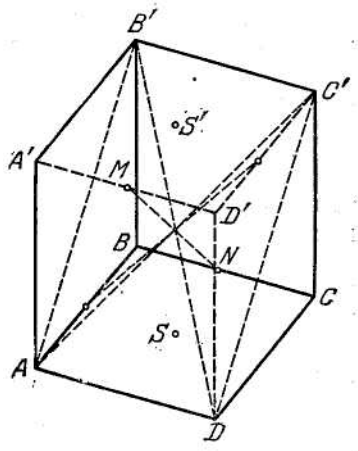


Рис. 2.7

Постараемся определить каждое из этих самосовмещений. Заметим прежде всего, что у куба имеются следующие 13 осей симметрии: четыре диагонали, три прямые, соединяющие попарно середины

граней куба, шесть прямых, соединяющих попарно середины противоположных ребер куба. Вокруг каждой из четырех диагоналей имеется два нетождественных поворота куба, совмещающих куб с самим собой, всего имеем восемь поворотов вокруг диагоналей.

Вокруг каждой из прямых, соединяющих центры противоположных граней куба, имеется три нетождественных поворота. Следовательно, всего таких поворотов 9.

Наконец, имеем один нетождественный поворот (на угол π) вокруг прямой, соединяющей середины двух противоположных ребер; общее число этих поворотов равно шести.

Итак, имеем 8+9+6=23 нетождественных поворота, совмещающих куб с самим собой. Если присоединить к ним еще тождественный поворот, получим 24 самосовмещения, т.е. все самосовмещения куба, какие только имеются.

Итак,

поворотами куба вокруг его осей симметрии исчерпываются все его самосовмещения.

Поэтому, так же как и в случае тетраэдра, группа самосовмещений куба называется ***группой поворотов куба.***

Прежде чем идти дальше в изучении построения группы поворотов куба, докажем следующую лемму:

Лемма. *Единственный поворот куба, переводящий каждую из его четырех диагоналей в самое себя, есть тождественный поворот*.

(Не следует упускать из виду следующее обстоятельство: если при данном повороте куба данная диагональ, положим *AC',* переходит в самое себя, то это не значит, что вершины, определяющие эту диагональ (в нашем случае вершины *A* и *C'*), непременно остаются неподвижными: они могут поменяться местами (т.е. *A* может перейти в *C'*, а *C'* в *A*).

В самом деле, заметим сначала, что всякий поворот, который переводит в себя любые две диагонали куба, положим, *AC'* и *DB',* — переводит в себя и диагональную плоскость *ADC'B'* (см. рис. 2.7). Всякий нетождественный поворот, который переводит в себя некоторую плоскость, имеет своей осью либо прямую, лежащую в данной плоскости, - в этом случае угол поворота равен π, либо прямую, перпендикулярную к этой плоскости. Но поворот плоскости на угол π вокруг оси, лежащей в этой плоскости, переводит у самих себя, кроме оси поворота, лишь прямые, перпендикулярные к этой оси. Так как прямоугольник *ADC'B'* не является квадрат, то диагонали его, не будучи взаимно перпендикулярными, не могут переходить каждая в себя саму при повороте вокруг которой бы то ни было оси,

лежащей в плоскости прямоугольника. Итак, AC' и DB' могут переходить в самих себя лишь при поворотах куба вокруг осы, перпендикулярной к плоскости $ADC'B'$. Такой осью является прямая MN, соединяющая середины сторон $A'D'$ и BC. Единственный нетождественный поворот куба вокруг прямой MN есть поворот на угол π. Значит, только при этом повороте каждая из диагоналей AC' и DB' переходит в саму себя. Но при этом повороте две другие диагонали BD' и CA' меняются местами, так что нетождественного поворота, который переводит в самих себя все четыре диагонали куба, вовсе нет.

Таким образом, при каждом нетождественном повороте куба четыре его диагонали выполняют нетождественную подстановку. Отсюда следует: при двух различных поворотах a и b диагонали испытывают различные подстановки, так как если бы при поворотах a и b происходила та же самая подстановка диагоналей, то при повороте ab^{-1} все диагонали оставались бы на месте, и значит, ab^{-1} было бы тождественным поворотом, а потому повороты a и b совпадали бы между собой.

Итак, всем 24 различным поворотам куба соответствуют различные подстановки четырех диагоналей, производимые этими поворотами. Но всех различных подстановок из четырех элементов имеется, как известно, $1 \cdot 2 \cdot 3 \cdot 4 = 24$

Отсюда следует: между группой всех поворотов куба и группой всех подстановок его четырех диагоналей имеется взаимно однозначное соответствие. Так как при установленном нами соответствии произведению поворотов соответствет произведение подстановок, то имеем следующую теорему (ведь произведение двух поворотов состоит в последовательном осуществлении этих поворотов, произведение подстановок - в последовательном осуществлении этих подстановок, тогда как взаимно однозначное соответствие между поворотом и подстановкой диагоналей заключается в соответствии данного поворота с фактически производимой им подстановкой диагоналей):

Группа поворотов куба изоморфна группе всех подстановок из четырех элементов.

Среди подгрупп поворотов куба отметим прежде всего циклические подгруппы второго, третьего и четвертого порядков, которые состоят соответственно из поворотов вокруг каждой из 13 осей симметрии куба. Циклических подгрупп второго порядка шесть (по числу осей, которые соединяют середины двух противоположных ребер), циклических подгрупп третьего порядка четыре (по числу диагоналей),

циклических подгрупп четвертого порядка имеется три (по числу соединяющих центры противоположных граней).

Значительно больший интерес представляют следующие перечисленные ниже подгруппы.

а) Подгруппа двенадцатого порядка, состоящего из поворотов, переводящих в себя (одновременно) каждый с двух тетраэдров *ACB'D'* и *BDA'C'* (рис. 2.8), вписанных в куб. Эта подгруппа состоит из 2·4 = 8 нетождественных поворотов вокруг диагоналей куба, из трех поворотов, каждый на угол π, вокруг осей, которые соединяют центры противоположных граней, и из тождественного поворота.

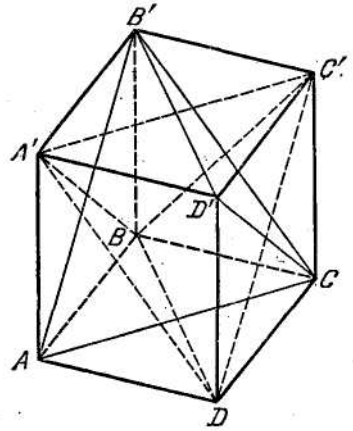


Рис. 2.8

б) Три подгруппы восьмого порядка, изоморфные группе четырехугольной двойной пирамиды (диэдра).

Каждая из этих подгрупп состоит из тех поворотов куба, которые переводят в самое себя одну из прямых, соединяющих центры двух противоположных граней, например, точки *S* и *S'* (октаэдр, вписанный в куб, является частичным случаем четырехугольного диэдра; группа его поворотов, которые оставляют недвижимыми или меняющих местами две вершины его S и S', и будет группой четырехугольного диэдра).

Эта подгруппа восьмого порядка получается из следующих восьми поворотов: четырех поворотов вокруг оси *SS*' (включая тождественный); двух поворотов на угол π вокруг осей, которые соединяют соответственно середины ребер *AA'* и *CC', BB'* и *DD';* двух

поворотов на угол π вокруг осей, которые соединяют соответственно центры граней *ABB'A'* и *CDD'C'*, *ADD'A'* и *BCC'B'*.

в) Подгруппа четвертого порядка, состоящая из тождественного преобразования и трех поворотов на угол π вокруг каждой из осей, которые соединяют центры двух противоположных граней. Эта группа состоит из тех поворотов, которые входят в каждую из перечисленных в п. б) трех подгрупп восьмого порядка. Эта подгруппа четвертого порядка коммутативна и изоморфна группе поворотов ромба (т.е. клейновской группе порядка 4).

Кроме упомянутых, имеются еще подгруппы четвертого порядка, которые также изоморфны группе самосовмещений ромба.

2. *Группа самосовмещений или поворотов правильного октаэдра изоморфна группе поворотов куба.*

Чтобы убедиться в этом, достаточно описать куб вокруг правильного октаэдра (рис. 2.9) или вписать куб в правильный октаэдр (рис. 2.10).

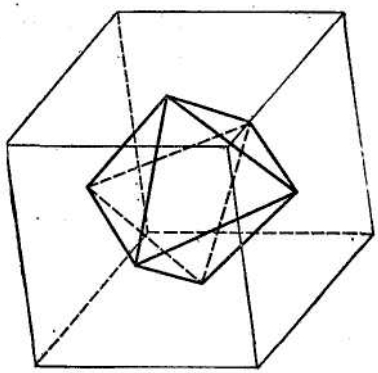


Рис. 2.9

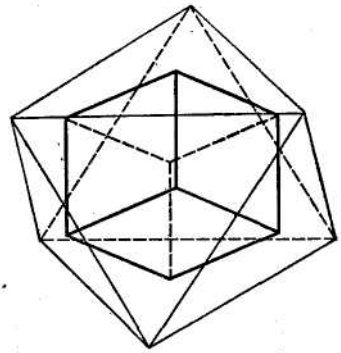


Рис. 2.10

Каждое самосовмещение октаэдра соответствует некоторому самосовмещению куба, и наоборот.

Это положение вещей есть одним из проявлений отношения *двойственности,* имеющего место между кубом и октаэдром; сейчас мы его определим.

Прежде всего мы назовем два элемента (вершина, ребро, грань) какого-нибудь многогранника ***инцидентными***, если один из этих двух элементов принадлежит второму (как его элемент). Таким образом, вершина и грань, имеющая эту вершину среди своих вершин, а также

грань и ребро этой грани, наконец вершина и ребро, одним из концов которого является эта вершина - суть пары инцидентных элементов.

Два многогранника называются ***двойственными***, если элементы одного могут быть таким образом поставлены во взаимно однозначное соответствие с элементами другого, что при этом пары инцидентных элементов одного многогранника соответствуют парам инцидентных элементов другого, и при этом:

вершины первого многогранника соответствуют граням второго, ребра первого многогранника соответствуют ребрам второго, грани первого многогранника соответствуют вершинам второго. Нетрудно видеть, что куб и октаэдр в этом смысле двойственны друг другу, а тетраэдр двойствен самому себе.

2.5.6. Группа поворотов икосаэдра и додекаэдра

1. Среди всех пяти правильных многогранников нам осталось рассмотреть два: икосаэдр и додекаэдр (рис. 2.11, 2.12).

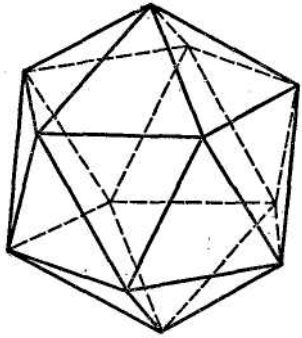


Рис. 2.11

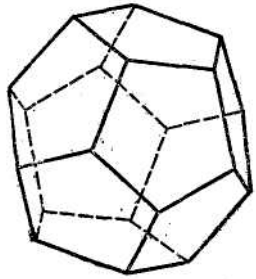


Рис. 2.12

Эти многогранники двойственны между собой и группы их самосовмещений изоморфны.

Для того чтобы убедиться в этом, достаточно вписать икосаэдр в додекаэдр (рис. 2.13) или додекаэдр в икосаэдр (рис. 2.14).

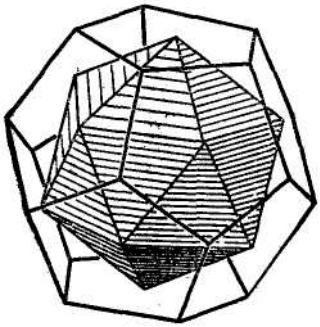


Рис. 2.13

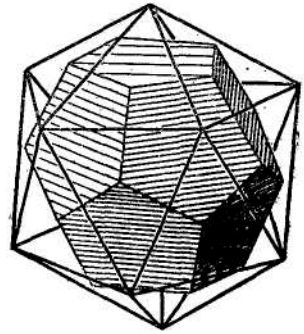


Рис. 2.14

Поэтому нам достаточно ознакомиться с группой самосовмещений икосаэдра. Чтобы определить число ее элементов, мы поступим так же, как и в случае тетраэдра и куба. А именно, мы сначала рассмотрим те самосовмещения икосаэдра, которые оставляют неподвижной одну какую-нибудь из его вершин. Таких самосовмещений имеется пять, а именно: пять поворотов вокруг оси, которая соединяет данную вершину с противоположной ей. Так как всех вершин 12, то число самосовмещений икосаэдра есть 5·12=60. Все эти самосовмещения оказываются поворотами икосаэдра вокруг его осей симметрии. В самом деле, имеются следующие оси симметрии икосаэдра:

Шесть осей, которые соединяют противоположные вершины: вокруг каждой из них имеем четыре нетождественных поворота (на углы $2\pi/5$, $4\pi/5$, $6\pi/5$, $8\pi/5$), совмещающих икосаэдр с самим собой; всего, значит, получаем $4 \cdot 6 = 24$ поворота;

10 осей, которые соединяют центры противоположных граней; вокруг каждой из этих осей имеем два нетождественных поворота (на угол $2\pi/5$ и $4\pi/5$), а всего 20 поворотов;

15 осей, которые соединяют середины противоположных ребер и дающих по одном нетождественному повороту (на 180°);

итак, имеем 24+20+15 нетождественных поворота и один тождественный поворот - всего 60 поворотов.

Как всегда, из этого рассуждения следует, что икосаэдр имеет 31 ось симметрии.

Ввиду достаточной сложности группы поворотов икосаэдра мы не будем здесь далее останавливаться на ее изучении. Заметим только, что эта группа изоморфна знакопеременной группе подстановок из пяти элементов.

2. Мы определяли группы поворотов многоугольников и многогранников как группы самосовмещений.

Рассмотрим как бы два экземпляра пространства, вложенных один в другой. Одно пространство представляем себе в виде бесконечно распространяющегося во все стороны твердого тела и назовем его *твердым пространством.* Другое пространство представляем себе в виде *пустого пространства.*

Твердое пространство помещаем в пустое, в котором оно может перемещаться. Наш многогранник представляем как часть твердого пространства, недвижимую в нем и способную перемещаться лишь вместе с ним. При такой точке зрения можно рассматривать повороты всего *«твердого»* пространства в *«пустом»* пространстве (вокруг тех или иных осей), которые совмещают данный многогранник с самим собой, т.е. делают самосовмещения его. Так как каждое самосовмещение рассмотренных нами многогранников оказывалось поворотом вокруг той или иной оси и каждый поворот многогранника вокруг оси можно представлять себе как порожденный поворотом всего пространства вокруг той же оси, то группа самосовмещений данного многогранника изоморфна группе поворотов пространства, совмещеющих этот многогранник с самим собой. Эту последнюю группу обычно и имеют в виду, когда говорят о группе поворотов данного правильного многогранника. Часто ее даже называют просто «группой правильного многогранника».

Группы правильных пирамид (т.е. конечные циклические группы), группы диэдров и только что рассмотренные группы правильных многогранников суть единственные *конечные* подгруппы группы *всех перемещений* пространства.

2.6. Ивариантные подгруппы

2.6.1. Сопряженные элементы и подгруппы

1. Трансформация одного элемента группы при помощи другого. Рассмотрим в группе G два каких-нибудь элемента a и b. *Элемент*

$$b^{-1}ab$$

называется ***трансформацией*** *элемента a при помощи элемента b.*

Посмотрим, при каких условиях имеет место равенство

$$b^{-1}ab=a. \qquad (2.23)$$

Если равенство (2.23) выполнено, то умножая ее части слева на b, получим

$$ab = ba. \qquad (2.24)$$

Итак, если выполнено (2.23), то выполнено и (2.24), т.е. элементы a и b переместительны. Обратно, если выполнено (2.24), то умножая обе ее части на b^{-1} слева, получим

$$b^{-1}ab = b^{-1}ba = a,$$

т.е. имеет место и равенство (2.23). Итак, мы видим, что *для того, чтобы при данных a и b имело место равенство* (2.23), *т.е. чтобы трансформация элемента a при помощи элемента b равнялось самому элементу a, необходимо и достаточно, чтобы элементы a и b были переместительными (удовлетворяли равенства* (2.24)).

В частности, в коммутативных группах равенство (2.23) имеет место для любых элементов a и b.

В качестве иллюстрации понятия трансформации рассмотрим группу G всех подстановок из n элементов; пусть

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}.$$

Тогда очевидно,

$$b^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix},$$

$$b^{-1}a = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix},$$

$$b^{-1}ab = \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ b_{a_1} & b_{a_2} & b_{a_3} & \dots & b_{a_n} \end{pmatrix}. \qquad (2.25)$$

Формула (2.25) может быть записана в виде следующего правила: *пусть*

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \text{ и } b = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix};$$

чтобы получить трансформацию подстановки a при помощи подстановки b, нужно в обеих строках обычной записи подстановки a сделать подстановку b.

Объясним это правило еще частыми примерами. Пусть, например, $n = 3$ и

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Получаем

$$b^{-1}ab = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq a.$$

Намного проще понять только что выведенное правило, пользуясь термином отображения или функция.

Подстановка *a* означает функцию $y=f(x)$, $x = 1, 2, ..., n$, $y=1, 2, 3,...,n$, где двум различным значениям x всегда соответствуют два различных значения y, так что f есть взаимно однозначное отображение множества $\{1, 2, ... , n\}$ на себя.

Подстановка b есть функция $\varphi=f(x)$ той же природы, что и $f(x)$. Подстановка $b^{-1}ab$ есть функция $y=F(x)$, определенная формулой

$$F(x) = \varphi\{f[\varphi^{-1}(x)]\}. \tag{2.26}$$

Она получается, если элементу $\varphi(x)$ поставить в соответствие элемент $\varphi[f(x)]$; это непосредственно видно, если в формуле (2.26) поставить $\varphi(x)$ вместо x и заметить, что

$$\varphi^{-1}[\varphi(x)]=x.$$

Так как x пробегают все числа 1, 2, 3, ..., n, то и $\varphi(x)$ пробегает все те же числа, только в другом порядке, и формулой

$$F[\varphi(x)] = \varphi[f(x)] \tag{2.27}$$

функция $F(x)$, т.е. подстановка $b^{-1}ab$, вполне определена. Формула (2.27) представляет собой только другая запись формулы (2.25). Наконец, если обозначить $f(x)$ через y, полученный результат можно сформулировать еще и так:

подстановка F заключается в том, что элемент $\varphi(x)$ заменяется элементом $\varphi(y)$.

Так как всякая конечная группа изоморфна некоторой группе подстановок, то формула (2.25) выясняет содержание понятия «трансформация», по крайней мере для всех конечных групп.

2. Пример группы тетраэдра. Рассмотрим в виде дальнейшего примера группу поворотов тетраэдра *ABCD* (рис. 2.15).

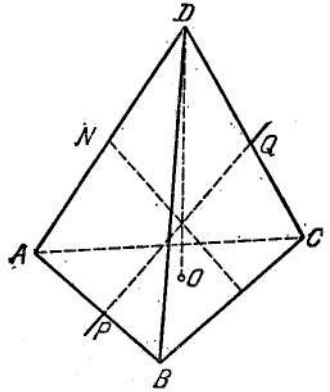


Рис. 2.15

Пусть a есть поворот тетраэдра вокруг оси MN (которая соединяет середины ребер BC и AD) на угол π, пусть b есть поворот вокруг оси DO, переводящей A в C, B в A, C в B; тогда $b^{-1}ab$ есть поворот на угол π вокруг оси PQ, соединяющей середины ребер AB и CD. В этом можно убедиться как непосредственно, так и замечая, что поворот a производит подстановку вершин

$$\begin{pmatrix} A\,B\,C\,D \\ D\,C\,B\,A \end{pmatrix},$$

тогда как b производит подстановку

$$\begin{pmatrix} A\,B\,C\,D \\ C\,A\,B\,D \end{pmatrix}.$$

Производя в каждой строке выражения $\begin{pmatrix} A\,B\,C\,D \\ D\,C\,B\,A \end{pmatrix}$ подстановку $\begin{pmatrix} A\,B\,C\,D \\ C\,A\,B\,D \end{pmatrix}$, получим $\begin{pmatrix} A\,B\,C\,D \\ D\,B\,A\,C \end{pmatrix}$, т.е. $\begin{pmatrix} A\,B\,C\,D \\ B\,A\,D\,C \end{pmatrix}$, соответствующую повороту вокруг оси PQ на угол π.

Таким же точно образом убедимся, что

$$a^{-1}ba$$

есть поворот, переводящий B в C, C в D, D в B вокруг оси, соединяющей вершину A с центром грани BCD. Этому повороту соответстует подстановка

$$\begin{pmatrix} A\,B\,C\,D \\ A\,C\,D\,B \end{pmatrix}$$

3. Сопряженные элементы. Пусть G — какая-нибудь группа.

Лемма 1. *Если элемент b есть трансформация элемента a при помощи элемента c, то элемент a есть трансформация элемента b при помощи элемента c^{-1}.*

В самом деле, из соотношение

$$b= c^{-1}acc,$$

умножая обе части слева на c, а справа на c^{-1}, получаем

$$cbc^{-1} = a,$$

т.е.

$$a=(c^{-1})^{-1}bc^{-1},$$

что и требовалось доказать.

Определение. Два элемента группы называются ***сопряженными элементами,*** если один из них есть трансформация другого.

Лемма 2. *Если a сопряжен с b, b сопряжен с d, то a сопряжен с d.*

В самом деле, так как *a* сопряжен с *b,* то существует такой элемент *c,* что

$$b = c^{-1}ac. \qquad (2.28)$$

Так как *b* сопряжен с *d,* то существует такой элемент *e,* что

$$b = e^{-1}de, \qquad (2.29)$$

так что $c^{-1}ac=e^{-1}de$. Умножая обе части последнего равенства слева на *c,* а справа на c^{-1}, получим

$$a = (ce^{-1})d(ec^{-1}) = (ec^{-1})^{-1}d(ec^{-1}),$$

т.е. *a* есть трансформация элемента *d* с помощью элемента ec^{-1}, что и требовалось доказать.

Лемма 3. *Каждый элемент сопряжен самому себе.*

В самом деле, совсем очевидно, что

$$a=1^{-1}\cdot 1.$$

Содержание лемм 1 - 3 заключается в том, что сопряженность двух элементов группы обладает свойствами симметрии, транзитивности и рефлексивности. Отсюда на основании теоремы 3 п. 1, п. 1.4 следует

Теорема 1. *Всякая группа G распадается на классы попарно сопряженных между собой элементов.*

При этом класс какого-нибудь элемента a группы G состоит из всех сопряженных с a элементов группы G, т.е. трансформаций элемента a при помощи всевозможных элементов группы G.

Заметим, что *класс нейтрального элемента всякой группы G состоит из одного этого элемента* (так как при любому *a* имеем $a^{-1}\cdot 1\cdot a=1$).

4. Трансформация подгруппы. Класс сопряженных элементов, к которому принадлежит данный элемент *a* группы *G*, состоит из трансформаций элемента *a* при помощи всевозможных элементов *b* группы *G*. Теперь возьмем какую-нибудь подгруппу *H* группы *G* и будем рассматривать трансформацию всевозможных элементов *x* этой подгруппы при помощи одного и того же произвольно выбранного элемента *b* группы *G*. Полученное множество элементов, т.е. *совокупность всех элементов вида*

$$b^{-1}xb,$$

где b - избранный нами определенный элемент группы G, а x пробегает множество всех элементов подгруппы H, называется

трансформацией подгруппы *H при помощи элемента b и обозначается через*

$$b^{-1}Hb.$$

Докажем, что $b^{-1}Hb$ *есть группа.*

В самом деле: 1. Пусть имеем два элемента c_1 и c_2, принадлежащие к $b^{-1}Hb$. Докажем, что c_1c_2 принадлежит к $b^{-1}Hb$. Имеем:

$$\left.\begin{aligned} c_1 &= b^{-1}x_1b, \\ c_2 &= b^{-1}x_2b \end{aligned}\right\} \qquad (2.30)$$

где x_1 и x_2 суть элементы группы H.

Из уравнений (2.30) следует непосредственно:

$$c_1c_2 = b^{-1}x_1x_2b; \qquad (2.31)$$

итак, c_1c_2 есть трансформация элемента x_1x_2 при помощи b, а потому c_1c_2 принадлежит к $b^{-1}Hb$.

2. Докажем, что нейтральный элемент 1 группы G принадлежит к $b^{-1}Hb$. Так как 1 принадлежит к H, и так как

$$b^{-1}\cdot 1\cdot b=1,$$

то 1 принадлежит и к $b^{-1}Hb$.

3. Наконец, если a принадлежит к $b^{-1}Hb$, то и a^{-1} принадлежит $b^{-1}Hb$. В самом деле, если a принадлежит к $b^{-1}Hb$, то $a=b^{-1}xb$, где x есть некоторый элемент H. Но тогда элемент $a^{-1}= (b^{-1}xb)^{-1}=b^{-1}x^{-1}b$, т.е. a^{-1} есть трансформация элемента x^{-1} группы H при помощи b, следовательно, a^{-1} есть элемент множества $b^{-1}Hb$.

Итак, $b^{-1}Hb$ *есть группа.*

Каждому элементу x группы H соответствует вполне определенный элемент группы $b^{-1}Hb$, а именно элемент $b^{-1}xb$ группы $b^{-1}Hb$. При этом двум разным элементам x_1 и x_2 соответствуют различные элементы $b^{-1}x_1b$ и $b^{-1}x_2b$, так как если x_1 и x_2 различны, то различны и элементы x_1b и x_2b (в свмом деле, если $x_1b=x_2b= c$, то $x_1=cb^{-1}$ и $x_2 = cb^{-1}$); а если различны элементы x_1b и x_2b, то различны и элементы $b^{-1}x_1b$ и $b^{-1}x_2b$ (так, если $b^{-1}x_1b = b^{-1}x_2b = c$, то $x_1b = bc$ и $x_2b = bc$).

Итак**,** поставив в соответствие элементу x группы H элемент $b^{-1}xb$ группы $b^{-1}Hb$, мы получаем взаимно однозначное соответствие между H и $b^{-1}Hb$. В силу равенств (2.30) и (2.31) произведению двух элементов x_1 и x_2 соответствует при этом произведение элементов $b^{-1}x_1b$ и $b^{-1}x_2b$, т.е. наше соответствие есть изоморфное соответствие между группами H и $b^{-1}Hb$. Таким образом, нами доказана следующая

Теорема 2. *Трансформация подгруппы H группы G при помощи элемента b группы G есть подгруппа группы G, изоморфная группе H.*

Замечание. Непосредственно вытекают из определений следующие предложения:

1) Если G — коммутативная группа, а H - ее подгруппа, то трансформация подгруппы H при помощи любого элемента b группы G есть сама группа H (ведь в этом случае трансформация любого элемента x при помощи b есть сам этот элемент x: $b^{-1}xb = x$).

2) Если G — любая группа, H - ее подгруппа, b — элемент H, то

$$b^{-1}Hb = H,$$

так как для всякого элемента x группы H при b, принадлежащем H, принадлежит H и элемент $b^{-1}xb$.

3) Если подгруппа H_2 есть трансформация подгруппы H_1 при посредстве элемента b, то H_1 есть трансформация подгруппы H_2 при посредстве элемента b^{-1}.

Доказательство непосредственно следует из леммы 1, п. 3.

Определение. Две подгруппы группы G, из которых одна является трансформацией другой, называются ***сопряженными подгруппами.***

Так как $1^{-1}\cdot H \cdot 1 = H$, то каждая группа сопряжена с самой собой.

Из леммы 2 п. 4 следует, что две подгруппы, которые сопряжены третьей, сопряжены между собой, так что множество всех подгрупп группы G распадается на классы сопряженых между собой подгрупп.

Мы уже знаем (теорема 2 этого пункта), что *все сопряженные между собой подгруппы изоморфны между собой*.

5. Примеры. В группе поворотов правильного тетраэдра есть, как мы видели, следующие подгруппы:

1. Две несобственные подгруппы: первая, состоящая из одного нейтрального элемента, и вторая, состоящая из всех двенадцати поворотов тетраэдра. Каждая из этих подгрупп, очевидно, сапряжена с самой собой.

2. Три подгруппы второго порядка: H_{01}, H_{02}, H_{03}, каждая из которых состоит из поворотов на углы 0 и π вокруг некоторой реберной медианы. *Все эти группы образуют один класс сопряженных подгрупп.*

3. Группа H четвертого порядка (клейновская), являющаяся объединением (в смысле теории множеств) трех групп H_{01}, H_{02}, H_{03} (т.е. состоящая из тождественного поворота и из поворотов на угол π вокруг каждой с трех реберных медиан). Из определения группы H как объединения групп H_{01}, H_{02}, H_{03} и из того, что группы H_{01}, H_{02}, H_{03} образуют один класс сопряженных подгрупп, следует, что *группа H сопряжена лишь с самой собой*.

4. Четыре подгруппы третьего порядка: H_0, H_1, H_2, H_3; каждая из них состоит из поворотов на углы 0, $2\pi/3$, $4\pi/3$ вокруг некоторой

граневой медианы. *Все эти группы также образуют один класс сопряженных подгрупп.*

Итак, все 10 подгрупп группы поворотов правильного тетраэдра следующим образом распадаются на классы сопряженных подгрупп:

три класса, состоящие каждый из одного элемента:

классы, содержащие лишь по одной несобственной подгруппе, и

класс, состоящий из одной подгруппы H четвертого порядка;

класс, состоящий из трех подгрупп второго порядка;

класс, состоящий из четырех подгрупп третьего порядка.

2.6.2. Инвариантные подгруппы (нормальные делители)

1. Определение. Если подгруппа H данной группы G не имеет никакой отличной от себя, сопряженной подгруппы (т.е. если класс всех подгрупп, сопряженных в группе G подгруппе H, состоит лишь из одной группы H), то подгруппа H называется *инвариантной подгруппой* (или *нормальным делителем) группы G.*

Укажем, что инвариантная - в переводе с латинского «неизменяемая» (относительно операции трансформирования подгруппы).

В данное время в математической литературе вместо термина инвариантная все большее распространение получает термин нормальная подгруппа. По нашему мнению, этот термин совершенно не отражает основного свойства рассматриваемых подгрупп: инвариантости по отношению операции трансформирования подгрупп.

Очевидно, определение инвариантной подгруппы можно сформулировать и так:

подгруппа H группы G называется ***инвариантной,*** *если трансформация любого элемента группы H с помощью любого элемента группы G есть элемент группы H.*

Понятие инвариантной подгруппы - одно из важнейших понятий всей алгебры: если и невозможно в этом кратком изложении довести читателя до полного понимания всей важности этого понятия, раскрывающегося в алгебре, особенно в так называемой теории Галуа, то можно все-таки надеяться, что из рассуждений этого и следующего разделов читатель поймет, насколько большое значение инвариантных подгрупп в логическом построении самой теории групп.

2. Примеры. Тривиальными примерами инвариантных подгрупп являются обе несобственные подгруппы любой группы. Кроме того,

любая подгруппа коммутативной группы является, очевидно, инвариантной.

Укажем некоторые менее тривиальные примеры.

1. Группа скольжений прямой самой по себе есть инвариантная подгруппа группы всех самосовмещений прямой .

2. Циклическая группа A порядка n, состоящая из всех самосовмещений первого рода n-угольного диэдра, есть инвариантная подгруппа группы всех поворотов n-угольного диэдра (так как, если a - есть самосовмещения первого, а b — самосовмещение второго рода, то имеем (как было указано ранее) $ab=ba^{-1}$, откуда $b^{-1}ab=a^{-1}$; так как это справедливо для любого элемента подгруппы A, то $b^{-1}Ab = A$).

3. Знакопеременная группа A_n подстановок из n элементов есть инвариантная подгруппа группы S_n всех подстановок из n элементов. В самом деле, если b есть произвольная четная подстановка, а a есть любой элемент группы S_n (т.е. каждая подстановка - четная или нечетная), то подстановка $a^{-1}ba$ имеет в качестве знака произведение трех чисел, равных + 1 или — 1:

$$(зн\ a^{-1})\cdot (\ зн\ b)\cdot (зн\ a).$$

Так как $(зн\ a^{-1})=зн\ a$, то $(зн\ a^{-1})\cdot(зн\ a)$ в каждом случае (т.е. для любого a) равняется +1; следовательно,

$$(зн\ a^{-1}ba) = (зн\ a^{-1}) \bullet (зн\ b) \bullet (зн\ a) = (зн\ b) = +1,$$

а это значит, что $a^{-1}ba$ есть четная подстановка, т.е. элемент группы A_n.

Итак, трансформация любого элемента b группы A_n есть элемент группы A_n (вообще говоря, отличный от a), т.е. A_n есть инвариантная подгруппа группы S_n.

Возвращаемся к примерам инвариантных и неинвариантных подгрупп.

Мы уже видели, что в группе всех поворотов тетраэдра есть одна собственная инвариантная подгруппа четвертого порядка. Так как группа всех поворотов тетраэдра изоморфна знакопеременной группе A_4 подстановок из четырех элементов (т.е. группе всех четных подстановок из четырех элементов), то полученный результат можно сформулировать и так:

знакопеременная группа подстановок из четырех элементов имеет инвариантную подгруппу четвертого порядка.

Это обстоятельство заслуживает внимания: оказывается, при $n>4$ знакопеременная группа A_n подстановок из n элементов не содержит никакой инвариантной подгруппы (кроме двух несобственных подгрупп). Этот факт, имеет большое значение в алгебре: он тесно связан с тем, что общее уравнение степени $n>4$ не может быть разрешимо в радикалах.

Группа поворотов куба, как мы знаем, изоморфна группе S_4. Значит, в ней имеется инвариантная подгруппа, изоморфная группе A_4; эта группа нам уже знакома: она состоит из поворотов, переводящих в себя каждый из двух тетраэдров, вписанных в куб.

Мы уже упоминали также о трех подгруппах восьмого порядка, которые содержатся в группе самосовмещений куба. Эти три группы образуют класс сопряженных между собой групп; следовательно, ни одна из них не инвариантна. Зато инвариантной подгруппой является пересечения этих трех групп, которое, как мы знаем, представляет собой группу, которая состоит из нейтрального элемента и из трех поворотов куба на 180° вокруг каждой из трех прямых, соединяющих центры двух противоположных его граней.

Существует общая теорема: *пересечение всех групп, входящих в некоторый класс сопраженных между собой подгрупп, есть инвариантная подгруппа.*

Никаких инвариантных собственных подгрупп, кроме указанных групп двенадцатого и четвертого порядка, и группе самосовмещений куба не имеется.

Упомянем еще следующие классы сопряженных групп:

1. Класс, состоящий из трех циклических групп порядка 4 (каждая из этих групп состоит из поворотов вокруг одной из осей, которые соединяют центры двух противоположных граней куба).

2. Класс, состоящий из четырех циклических групп порядка 3 (каждая из этих групп состоит из поворота вокруг одной из диагоналей).

3. Класс, состоящий из шести циклических групп порядка 2 (каждая из этих групп состоит из поворота вокруг одной из осей, которые соединяют середины двух противоположных ребер).

Микромодуль 5.
Примеры решения типовых задач

Пример 1. В группе поворотов правильного тетраэдра есть, как мы видели, следующие подгруппы:

1. Две несобственные подгруппы: первая, состоящая из одного нейтрального элемента, и вторая, состоящая из всех двенадцати поворотов тетраэдра. Каждая из этих подгрупп, очевидно, сапряжена с самой собой.

2. Три подгруппы второго порядка: H_{01}, H_{02}, H_{03}, каждая из которых состоит из поворотов на углы 0 и π вокруг некоторой реберной

медианы. *Все эти группы образуют один класс сопряженных подгрупп.*

3. Группа H четвертого порядка (клейновская), являющаяся объединением (в смысле теории множеств) трех групп H_{01}, H_{02}, H_{03} (т.е. состоящая из тождественного поворота и из поворотов на угол π вокруг каждой с трех реберных медиан). Из определения группы H как объединения групп H_{01}, H_{02}, H_{03} и из того, что группы H_{01}, H_{02}, H_{03} образуют один класс сопряженных подгрупп, следует, что *группа H сопряжена лишь с самой собой.*

4. Четыре подгруппы третьего порядка: H_0, H_1, H_2, H_3; каждая из них состоит из поворотов на углы 0, $2\pi/3$, $4\pi/3$ вокруг некоторой граневой медианы. *Все эти группы также образуют один класс сопряженных подгрупп.*

Итак, все 10 подгрупп группы поворотов правильного тетраэдра следующим образом распадаются на классы сопряженных подгрупп:

три класса, состоящие каждый из одного элемента:

классы, содержащие лишь по одной несобственной подгруппе, и

класс, состоящий из одной подгруппы H четвертого порядка;

класс, состоящий из трех подгрупп второго порядка;

класс, состоящий из четырех подгрупп третьего порядка.

Пример 2. Тривиальными примерами инвариантных подгрупп являются обе несобственные подгруппы любой группы. Кроме того, любая подгруппа коммутативной группы является, очевидно, инвариантной.

Укажем некоторые менее тривиальные примеры.

1. Группа скольжений прямой самой по себе есть инвариантная подгруппа группы всех самосовмещений прямой .

2. Циклическая группа A порядка n, состоящая из всех самосовмещений первого рода n-угольного диэдра, есть инвариантная подгруппа группы всех поворотов n-угольного диэдра (так как, если a - есть самосовмещения первого, а b — самосовмещение второго рода, то имеем (как было указано ранее) $ab=ba^{-1}$, откуда $b^{-1}ab=a^{-1}$; так как это справедливо для любого элемента подгруппы A, то $b^{-1}Ab = A$).

3. Знакопеременная группа A_n подстановок из n элементов есть инвариантная подгруппа группы S_n всех подстановок из n элементов. В самом деле, если b есть произвольная четная подстановка, а a есть любой элемент группы S_n (т.е. каждая подстановка - четная или нечетная), то подстановка $a^{-1}ba$ имеет в качестве знака произведение трех чисел, равных + 1 или — 1:

$$(зн\ a^{-1})\cdot (\ зн\ b)\cdot (зн\ a).$$

Так как $(зн\ a^{-1}) = зн\ a$, то $(зн\ a^{-1}) \cdot (зн\ a)$ в каждом случае (т.е. для любого a) равняется +1; следовательно,

$$(зн\ a^{-1}ba) = (зн\ a^{-1}) \bullet (зн\ b) \bullet (зн\ a) = (зн\ b) = +1,$$

а это значит, что $a^{-1}ba$ есть четная подстановка, т.е. элемент группы A_n.

Итак, трансформация любого элемента b группы A_n есть элемент группы A_n (вообще говоря, отличный от a), т.е. A_n есть инвариантная подгруппа группы S_n.

Микромодуль 5.

Индивидуальные тестовые задачи

1. Взять два каких-нибудь определенных самосовмещения первого и второго рода и построить их произведение для одного и другого порядка сомножителей.
2. Доказать геометрически, а именно: показать, что каждый поворот тетраэдра может быть получен умножениям соответствующей пары поворотов.
3. Доказать следующую общую теорему: *некоторое множество Е элементов группы G тогда и только тогда является системой образующих этой группы, когда не существует никакой собственной подгруппы группы G, которая содержала бы все элементы множества Э.*

Пользуясь этой теоремой, найти все системы образующих группы поворотов тетраэдра (состоящие не более чем из трех элементов каждая).

4. Требуется доказать, что группа поворотов тетраэдра распадается на следующие классы сопряженных элементов:

1) класс, состоящий из одного нейтрального элемента;
2) класс, состоящий из поворотов на угол $(2/3)\pi$ вокруг каждой из четырех осей, которые соединяют вершину тетраэдра с центром противоположной грани;
3) класс, состоящий из четырех поворотов на угол $(4/3)\pi$ вокруг тех же осей (всюду по (или против) часовой стрелки, если смотреть из неподвижной вершины);
4) класс, состоящий из поворотов на угол π вокруг каждой из трех осей, которые соединяют середины двух противоположных ребер тетраэдра.

Исследовать классы сопряженных элементов в других группах поворотов.

5. Доказать следующую общую теорему: пересечение всех групп, которые входят в некоторый класс сопряженных между собой подгрупп, есть инвариантная подгруппа.

Микромодуль 6.
Гомоморфные отображения и группы перемещений

2.7. Гомоморфные отображения

2.7.1. Определение гомоморфнго отображения и его ядра

Пусть каждому элементу a группы A поставлен в соответствие элемент

$$b= f(a)$$

группы B. Совокупность всех полученных таким образом элементов $b=f(a)$ группы B обозначим через $f(A)$. Мы говорим, что имеем отображение f группы A в группу B, а именно: на множество $f(A) \subset B$.

Введем теперь следующее фундаментальное определение.

Отображение f группы A в группу B называется *гомоморфным*, если для любых двух элементов a_1 и a_2 группы A выполнено условие

$$f(a_1 \bullet a_2)=f(a_1) \bullet f(a_2), \qquad (2.32)$$

причем знак • в левой части равенства (2.32) необходимо, естественно, понимать как *знак умножения в группе A,* а в правой части равенства (2.32) как *знак умножения в группе B.*

Теорема. *Если f есть гомоморфное отображение группы A в группу B, то множество $f(A) \subset B$ есть подгруппа группы B.*

Доказательство. Достаточно показать, что:

1) если b_1 и b_2 суть элементы множества $f(A)$, то, $b_1 \bullet b_2$ есть также элемент множества $f(A)$;

2) нейтральный элемент группы B есть элемент множества $f(A)$;

3) если b есть элемент множества $f(A)$, то b^{-1} есть также элемент множества $f(A)$.

Докажем последовательно утверждения 1), 2), 3).

1) Пусть b_1 и b_2 суть два элемента множества $f(A)$. Это значит, что существуют такие элементы a_1, и a_2 группы A, что

$$f(a_1) = b_1, \quad f(a_2) = b_2.$$

Но в силу гомоморфности отображения f имеем:

$$f(a_1 \cdot a_2) = b_1 \cdot b_2.$$

Следовательно, $b_1 \cdot b_2$ как образ при отображении f элемента $a_1 \cdot a_2$ группы A есть элемент множества $f(A)$. Первый пункт, таким образом, доказан.

2) Пусть 1 — нейтральный, а a — какой-нибудь элемент группы A. Имеем (в группе A)

$$a \cdot 1 = a,$$

откуда (в группе B) получаем

$$f(a \cdot 1) = f(a),$$

и в силу гомоморфностиі отображения f левую часть последнего равенства можно переписать в виде

$$f(a) \cdot f(1) = f(a);$$

отсюда видно, что $f(1)$ есть нейтральный элемент группы B. Этим доказан второй пункт.

3) Пусть b — произвольный элемент множества $f(A) \subset B$. Существует такой элемент a группы A, что

$$f(a) = b.$$

Обозначим через b' элемент $f(a^{-1})$ множества $f(A)$. Докажем, что

$$b' = b^{-1}.$$

В самом деле,

$$a \cdot a^{-1} = 1.$$

Следовательно,

$$f(a) \cdot f(a^{-1}) = 1$$

(1 справа означает нейтральный элемент группы B), т.е.

$$b \cdot b' = 1,$$

и следовательно,

$$b' = b^{-1}$$

что и требовалось доказать.

Итак, *всякое гомоморфное отображение группы A в группу B есть гомоморфное отображение группы A на некоторую подгруппу группы B.*

Замечание 1. В только что проделанных рассуждениях содержится доказательство следующих важных утверждений, справедливых для всякого гомоморфного отображение группы A в группу B:

$$f(1) = 1 \qquad (2.33)$$

(где слева 1 есть нейтральный элемент группы A, а справа - нейтральный элемент группы B),

$$f(a^{-1}) = f(a)^{-1}. \qquad (2.34)$$

Замечание 2. На основании примечания в п. 2.4.1 мы можем сказать:

Взаимно однозначное гомоморфное отображение группы A на группу B есть изоморфное отображение.

Определение. Пусть f есть гомоморфное отображение группы A в группу B. Множество всех элементов x группы A, отображающихся в силу f на нейтральный элемент группы B, называется ***ядром*** гомоморфного отображения f и обозначается через $f^{-1}(1)$.

Теорема. *Ядро гомоморфного отображения f группы A в группу B есть инвариантная подгруппа группы A.*

Доказательство. Из определения гомоморфного отображения непосредственно следует, что, если

$$f(a_1) = 1, \quad f(a_2) = 1, \text{ то } f(a_1 \cdot a_2) = 1,$$

т.е. если a_1 и a_2 суть элементы $f^{-1}(1)$, то и $a_1 \cdot a_2$ есть элемент $f^{-1}(1)$.

Далеше, мы видели при доказательстве предыдущей теоремы, что $f(1)$ есть нейтральный элемент группы B, т.е. 1 есть элемент $f^{-1}(1)$.

Наконец, если $f(a)=1$, то $f(a^{-1})=f(a)^{-1}=1$, т.е. если a есть элемент $f^{-1}(1)$, то a^{-1} есть также элемент $f^{-1}(1)$. Отсюда уже следует, что $f^{-1}(1)$ есть подгруппа группы A.

Чтобы доказать, что $f^{-1}(1)$ есть инвариантная подгруппа группы A, надо убедиться в том, что трансформация $a^{-1}xa$ произвольного элемента x группы $f^{-1}(1)$ при помощи любого элемента a группы A есть элемент группы $f^{-1}(1)$. Другими словами, надо убедиться в том, что

$$f(a^{-1}xa)=1,$$

если только $f(x)=1$. Но это почти очевидно, так как при $f(x)=1$ имеем

$$f(a^{-1}xa) = f(a)^{-1} \cdot f(x) \cdot f(a) = f(a)^{-1} \cdot 1 \cdot f(a) = f(a)^{-1} \cdot f(a) = 1.$$

Итак, наша теорема полностью доказана.

В дальнейшем мы увидим, что и обратно, всякая инвариантная подгруппа группы A есть ядро некоторого гомоморфного отображения группы A.

2.7.2. Примеры гомоморфних отображений

1. Рассмотрим группу G всех целых чисел

$$\ldots. -n, —(n-1), \ldots\ldots —2. —1, 0, 1, 2, \ldots, (n-1), n, \ldots$$

и группу второго порядка G_2. Эта группа является абелевой. Пусть ее элементы будут b_0, b_1, а таблица сложения такая:

$$b_0 + b_0 = b_0, \quad b_0 + b_1 = b_1 + b_0 = b_1, \quad b_1 + b_1 = b_0.$$

Очевидно, что b_0 есть нейтральный элемент группы G_2.

Установим следующее отображение f группы G на группу G_2. Каждому четному числу ставим в соответствие элемент b_0 группы G_2, каждому нечетному числу ставим в соответствие элемент b_1 группы G_2.

Это отображение *гомоморфно.* В самом деле, пусть a и a' - два целых числа. Если a и a' оба четных числа, то $a+a'$ тоже четное, и мы имеем

$$f(a + a') = f(a)=f(a') = b_0 = f(a) + f(a').$$

Если одно из двух чисел a и a' (пусть a) четное, а другое нечетное, то $a+a'$ нечетное, так что

$$f(a) = b_0,\ f(a') = b_1, f(a + a') = b_1 = b_0 + b_1 = f(a)+ f(a').$$

Если, наконец, и a и a' нечетные числа, то $a+a'$ четное, и мы имеем:

$$f(a)=f(a') = b_l,\ f(a+a') = b_0 = b_1 + b_1 = f(a)+f(a').$$

Ядром нашего гомоморфизма, очевидно, является группа всех четных чисел.

Обобщим этот пример. Пусть дано произвольное натуральное число $m\geq 2$. Рассмотрим циклическую группу G_m порядка m с элементами $b_0, b_l, b_2, \ldots, b_{m-1}$ и таблицей сложения:

	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_0	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_1	b_1	b_2	b_3	...	b_{m-1}	b_0
b_2	b_2	b_3	b_4	...	b_0	b_1
⋮	⋮	⋮	⋮	⋮	⋮	⋮
b_{m-2}	b_{m-2}	b_{m-1}	b_0	...	b_{m-4}	b_{m-3}
b_{m-1}	b_{m-1}	b_0	b_1	...	b_{m-3}	b_{m-2}

(нейтральный элемент обозначен через b_0).

Установим гомоморфное отображение f группы G всех целых чисел на группу G_m.

Для этого напомним прежде всего следующую арифметическую теорему:

Каждое целое число a при делении на натуральное число m дает как остаток одно из чисел 0, 1,... ..., m — 1. *При этом остаток числа a определяется как единственное неотрицательное целое число r, удовлетворяющее соотношениям*

$$a=mq + r,\quad 0\leq r\leq m—1, \qquad (2.35)$$

при целому q (называемом неполным частным при делении a на m).

Теорема эта всем, конечно, известна для случая положительного a. Для $a = 0$ имеем, очевидно,

$$0 = m\cdot 0 + 0,$$

т.е. при делении нуля на любое натуральное число и в частном и в остатоке получается нуль.

Случай отрицательного a требует некоторых разъяснений. Если a отрицательно, то $-a$ положительно. Разделим натуральное число $-a$ на натуральное число m, обозначим частное через q' и остаток через r'. Можем предположить, что $r' > 0$ (так как если бы $r' = 0$, то $-a$, а следовательно, и a делилось бы на m без остатка). Итак,

$$-a = mq' + r', \quad 0 < r' \le m - 1$$

или

$$a = -mq' - r' = -m - mq' + m - r' = m(-1 - q') + (m - r').$$

Из $0 < r' \le m - 1$ следует,

$$0 \le m - r' \le m - 1.$$

Поэтому, полагая $q = -1 - q'$, $r = m - r'$, имеем для целых чисел a, q соотношение

$$a = mq + r, \quad 0 \le r \le m - 1. \tag{2.36}$$

Легко убедиться в том, что представление целых чисел a в виде уравнений (2.36) при данном целом m и целых q и r, $0 \le r \le m - 1$ единственно, т.е. что целые числа q и r условиями (2.36) вполне определены.

В самом деле, пусть

$$a = mq_1 + r_1, \quad 0 \le r_1 \le m - 1. \tag{2.37}$$

Тогда вычтем почленно равенство (2.37) из равенства (2.36). Получим

$$0 = m(q - q_1) + (r - r_1)$$

или

$$r - r_1 = m(q_1 - q).$$

Отсюда следует, что целое число $r - r_1$ делится без остатка на m. Но $r - r_1$ есть разность двух неотрицательных чисел, не превосходящих $m - 1$; следовательно, абсолютная величина этой разности также не превосходит $m - 1$; в этих условиях число $r - r_1$ может делиться без остатка на m только в том случае, если оно есть нуль.

Итак,

$$r - r_1 = 0, \quad \text{т.е. } r = r_1$$

и, заменяя r_1 на r в формуле (2.37), получаем

$$a = mq_1 + r. \tag{2.38}$$

Из равенств (2.38) и (2.36) получаем

$$q_1 = \frac{a - r}{m}, \quad q = \frac{a - r}{m},$$

т.е. $q_1 = q$, что и требовалось доказать.

Целому числу r в силу неравенства

$$0 \le r_1 \le m - 1$$

соответствует элемент b_r группы G_m. Итак, при зафиксированном натуральном числе $m \ge 2$ каждому целому числу a соответствует вполне определенный элемент циклической группы G_m порядка m, а именно: элемент b_r, где r есть остаток при делении a на m. Этот *элемент* b_r *называется* ***вычетом числа*** a ***по модулю*** m.

Только что указанным соответствием и устанавливается отображение f группы G на группу G_m. Докажем, что отображение f гомоморфно.

Пусть a a' два целых числа и пусть

$$\left.\begin{aligned} a &= mq + r, \quad 0 \le r \le m-1, \\ a' &= mq' + r', \quad 0 \le r' \le m-1. \end{aligned}\right\} \tag{2.39}$$

Тогда

$$a + a' = m(q + q') + r + r'.$$

Однако $r+r'$, удовлетворяя, конечно, неравенству $0 \le r+r'$, может не удовлетворять неравенству $r + r' \le m - 1$.

Но во всяком случае

$$r + r' = mq'' + \rho,$$

где q" есть частное от деления $r + r'$ на m (оно, как нетрудно видеть, равно 0 или 1) и ρ есть остаток при этому делении, так что

$$a + a' = m(q + q' + q'') + \rho, \quad 0 \le \rho < m\text{-l}.$$

Итак, элементу $a+a'$ при нашем отображении f соответствует элемент b_ρ группы G_m.

Рассматривая таблицу сложений в циклической группе порядка m, видим, что

$$b_r + b_{r'} = b_\rho$$

(где ρ по-прежнему есть остаток при делении $r+r'$ на m). Итак,

$$f(a + a') = b_\rho = b_r + b_{r'} = f(a) + f(a'),$$

чем и доказано, что отображение f гомоморфно.

Только что построенное гомоморфное отображение f группы всех целых чисел в циклическую группу порядка m является основным фактом элементарной теории чисел; мы это гомоморфное отображение будем обозначать через f_m.

Ядром гомоморфизма f_m является группа всех целых чисел, делящихся без остатка на m.

2. В 2.5.2, второй пример, было указано, что каждому действительному числу соответствует некоторый элемент группы ***S0(2).*** Этим соответствием устанавливается гомоморфное отображение

группы всех действительных чисел на группу ***S0(2),*** причем ядром этого отображения является бесконечная циклическая группа, которая состоит из всех действительных чисел, являющихся целочисленными кратными 2π.

2.8. Разбиение группы на классы по данной подгруппе. Факторгруппа

2.8.1. Левосторонние и провосторонние классы

1. Левосторонние классы. Пусть даны группа G и ее подгруппа U. Наша задача состоит сейчас в том, чтобы показать следующее: задача подгруппы U определяет (и притом, вообще говоря, двумя различными способами) разбиение группы G на некоторую систему попарно непересекающихся подмножеств, одно из которых есть сама подгруппа U, а остальные некоторым довольно простым законом могут быть взаимно однозначно отображены на U.

Для получения этого разбиения будем поступать так.

Назовем два элемента a и b группы G ***эквивалентными,*** если элемент $a^{-1}b$ есть элемент подгруппы U.

Эта эквивалентность (назоваемая *левой* эквивалентностью) имеет свойство *симметрии,* так как, если

$$a^{-1}b = u,$$

где u есть элемент подгруппы U, то

$$b^{-1}a = (a^{-1}b)^{-1} = u^{-1}$$

также есть элемент подгруппы U.

Наша эквивалентность обладает, далее, свойством транзитивности, так как, если

$$a^{-1}b = u_1,$$
$$b^{-1}c = u_2,$$

где u_1 и u_2 — суть элементы подгруппы U, то

$$a^{-1}c = a^{-1}b\cdot b^{-1}c = u_1u_2$$

также есть элемент подгруппы U.

Наша эквивалентность обладает, наконец, свойством рефлексивности, так как

$$a^{-1}a = 1$$

есть элемент подгруппы U.

Итак, группа G распадается на классы элементов, эквивалентных между собой относительно подгруппы U. Эти классы называются ***левосторонними классами*** *группы G по подгруппе U.* Заметим, что

левосторонний класс $'K_a$ элемента a группы G состоит из всех таких элементов x, что $a^{-1}x = u$ есть элемент группы U, т.е. другими словами, *из всех элементов вида* $x = au$, *где* u *есть элемент подгруппы* U.

Заметим еще, что если a есть элемент U (в частности, если a=1), то $'K_a=U$, так как в этом случае au при любому u, принадлежащем к U, есть элемент группы U, и всякий элемент u группы U может быть представлен в виде au_1, где $u_1 = a^{-1}u$ есть элемент группы U. Так как всякий элемент множества $'K_a$ может быть представлен в виде au, и при различных элементах u_1 и u_2 группы U элементы au_1 и au_2 множества $'K_a$ различны, то мы получим *взаимно однозначное соответствие* между U и любым $'K_a$, если каждому *элементу* u *группы* U *поставим в соответствие элемент* au *класса* $'K_a$.

Заметим, наконец, что *среди всех классов* $'K_a$ *есть лишь один класс, являющийся подгруппой группы* G, *а именно* U.

В самом деле, если $'K_a$ есть подгруппа, то нейтральный элемент группы G должен входить в $'K_a$; он, следовательно, является общим элементом класса $'K_a$ и класса U, а потому $'K_a$ совпадает с U.

2. Случай конечной группы *G*. В силу взаимно однозначного соответствия, которое существует между каждым из $'K_a$ и подгруппой U, все $'K_a$ — в случае конечности группы G - состоят из того самого числа элементов m, где m есть порядок группы U. Если число всех различных классов равна j, а n есть порядок группы G, то имеем, очевидно,

$$n = mj.$$

Отсюда, в частности, следует ранее упомянутый нами факт (п.2.2), а именно:

Теорема Лагранжа. *Порядок всякой подгруппы конечной группы* G *есть делитель порядка группы* G.

Число j, т.е. число левосторонних классов группы G по подгруппе U, называется *индексом подгруппы* U *в группе* G. Это число может быть конечным и в случае бесконечной группы G, например, если G есть группа всех целых чисел, а U — подгруппа G, состоящая из всех чисел, которые делятся без остатка на целое число $m \geq 2$.

3. Правосторонние классы. Назовем два элемента a и b *эквивалентными, (правая эквивалентность)* относительно подгруппы U, если ba^{-1} есть элемент подгруппы U. Легко убеждаемся, что свойства симметрии, транзитивности и рефлексивности при этом выполнены.

В самом деле, из

$$ba^{-1} = u,$$

где u — элемент группы U, следует

$$ab\text{-}^{1} = (ba^{-1})^{-1} = u^{-1},$$

а из

$$ba^{-1} = u_{l,}\quad cb^{-1} = u_2$$

при u_1 и u_2, принадлежащих к U, следует:

$$ca^{-1} = cb^{-1} \bullet ba^{-1} = u_2 \bullet u_{1.}$$

Наконец,

$$aa^{-1} = 1$$

принадлежит к U.

Правая эквивалентность определяет разбиение группы G на *правосторонние* классы, причем *правосторонний класс* K'_a *данного элемента* a состоит из всех таких элементов x, для которых $xa^{-1} = u$ есть элемент группы U, т.е. из всех элементов вида

$$x = ua,$$

где u принадлежит U.

Для a, принадлежащего U, класс K'_a совпадает с U.

Ставя в соответствие элементу u подгруппы U элемент ua класса K'_a, получим взаимно однозначное соответствие между U и любым классом K'_a. В случае, если подгруппа U конечна, все классы K'_a по этой подгруппе конечны и состоят из того же числа элементов, что и U. Если группа G конечна и имеет порядок n, а подгруппа U имеет порядок m, то имеем, как прежде,

$$n = mj,$$

где j - число всех различных првосторонних классов по подгруппе U, равное, таким образом, числу всех различных левосторонних классов.

Итак, *индекс подгруппы U относительно конечной группы G может быть определен и как число левосторонних, и как число правосторонних классов группы G по подгруппе U:* он равен частному от деления порядка группы G на порядок группы U.

4. Совпадение правосторонних классов с левосторонними в случае инвариантных подгрупп. Зададим себе вопрос: в каком случае для всякого элемента a группы G выполняется равенство

$$'K_{a=} K'_a?$$

Для этогонеобходимо и достаточно, чтобы всякий элемент вида au равнялся некоторому $u'a$ и, наоборот, всякий элемент ua равнялся некоторому элементу au' (при этом всегда u, u' и так далее обозначают элементы подгруппы U). Оба условия при этом эквивалентны. В самом деле, первое условие означает: к каждому a из G и u из U можно подобрать такое u' из U, чтобы

$$au = u'a,$$

т.е. чтобы

$$aua^{-1} = u',$$

или

$$(a^{-1})^{-1} Ua^{-1} = U.$$

Так как любой элемент группы G может быть при надлежащем выборе элемента a представлен в виде a^{-1}, то первое условие означает просто: трансформация подгруппы U при помощи любого элемента группы G совпадает с U, или *U есть инвариантная подгруппа группы G.*

Второе условие говорит: к каждому a из G и u из U можно подобрать u' из U так, чтобы

$$ua = au',$$

т.е.

$$a^{-1}ua = u',$$

т.е.

$$a^{-1}Ua = U.$$

Таким образом, второе условие также выражает требование, чтобы U была инвариантной подгруппой группы G.

Итак, мы видим, что верна следующая

Теорема. *Пусть U - подгруппа группы G. Для того чтобы для каждого элемента a группы G левосторонний класс этого элемента относительно подгруппы U совпадал с правосторонним классом того же элемента, необходимо и достаточно, чтобы U была инвариантной подгруппой группы G.*

Так как в случае инвариантной подгруппы U для любого элемента a группы G выполняется равенство

$$'K_a = K'_a,$$

то можно вместо $'K_a$ и K'_a писать $K_a='K_a=K'_a$, и это множество называть просто *классом элемента a относительно инвариантной подгруппы U.*

В частности, совпадение правсторонних классов с левосторонними имеет место, если U есть подгруппа коммутативной группы G, так как все подгруппы коммутативных групп инвариантны.

5. Примеры. I. Пусть G — группа всех целых чисел, а $U \subset G$ — группа всех чисел, которые делятся без остатку на m.

Если a — произвольное целое число, то K_a состоит из всех чисел вида $a+mq$ при целом q: это будут все те числа, которые при делении на m дают тот же остаток, что и число a. Таким образом, различных классов будет столько же, сколько имеется различных остатков при делении на m; а этих последних имеется m, так как в качестве остатков при делении на m появляются числа 0, 1, 2, ..., m— 1, и только они. Итак, мы имеем следующие классы:

0) Класс всех чисел, которые дают при делении на m остаток 0. Этот класс совпадает с группой U и состоит из чисел

..., —qm, —(q—1)m, ..., —3m, —2m, — m,0, m, 2m, 3m, ..., qm, ...

1) Класс всех чисел, которые дают при делении на m остаток 1. Это будут:

..., -qm+1, —(q-l)m+l, ... — 3m+l, — 2m+1, —m+l, 1, m+1, 2m+1, 3m+1,…

2) Класс всех чисел, которые дают при делении на m остаток 2. Это будут:

-qm + 2, -(q-1)m + 2, ..., -3m + 2,
-2m+ 2, -m + 2, 2, m + 2....., qm + 2, ...
……

m—1) Класс всех чисел, которые дают при делении на m остаток (m—1). Этот класс состоит из чисел:

..., -qm + (m-l), -(q-1)m + (m-1)....,
— 3m+(m—1), — 2m + (m—1),
-m + (m-1), (m-1), m + (m-1), 2m + +(m- 1),....

или, что то же самое,

.... -2m-1, -m-1, -1, m-1, 2m-1, 3m-1,....

2.8.2. Факторгруппа по данной инвариантной подгруппе

1. Определение. Пусть U есть инвариантная подгруппа некоторой данной группы G. Рассмотрим множество всех классов, на которые распадается группа G относительно U. Это множество обозначим через V и докажем, что в ней можно определить операцию умножения таким образом, который V станет группой, на которую группу G можно будет гомоморфно отобразить.

Пусть v_1 и v_2 — два произвольных элемента из V; таким образом, v_1 и v_2 суть два класса группы G по инвариантной подгруппе U. Выберем в каждом из этих классов по одному элементу, а именно: выберем элемент x_1 из класса v_1 и элемент x_2 из класса v_2. Обозначим через v_3 класс, к которому принадлежит элемент x_1x_2 группы G.

Докажем, что класс v_3 не зависит от того, какие именно элементы x_1 и x_2 мы выбрали из классов v_1 и v_2. Другими словами, докажем: если x'_1 есть какой-нибудь элемент класса v_1, вообще говоря, отличный от x_1, а x'_2 какой-нибудь элемент класса v_2, вообще говоря, отличный от x_2, то элемент $x'_1x'_2$ принадлежит к тому же класса v_3, к которому принадлежит x_1x_2.

В самом деле, два элемента a и b принадлежат тогда и только тогда к одному и тому же классу относительно инвариантной подгруппы U, если элемент ab^{-1} принадлежит к U.

Рассмотрим элемент

$$x_1x_2\,(x'_1x'_2)^{-1} = x_1x_2\,(x'_2)^{-1}(x'_1)^{-1} = x_1\cdot(\,x_2\,(x'_2)^{-1})(x'_1)^{-1}.$$

Так как x_2 и x'_2 принадлежат одному и тому же классу v_2, то

$$x_2(x'_2)^{-1} = u_2,$$

где u_2 есть некоторый элемент U, и мы имеем

$$x_1x_2(x'_1x'_2) = x_1u_2(x'_1)^{-1}. \qquad (2.40)$$

Но U есть инвариантная подгруппа, поэтому $x_1u_2 = u'x_1$, где u' есть некоторый элемент группы U. Подставляя это в формулу (2.40), получаем

$$x_1x_2(x'_1x'_2)^{-1} = u'x_1(x'_1)^{-1}.$$

Но x_1 и x'_1 принадлежат к одному и тому же классу v_1, поэтому $x_1(x'_1)^{-1} = u_1$, где u_1 — некоторый элемент группы U. Следовательно,

$$x_1x_2(x'_1x'_2)^{-1} = u'u_1,$$

т.е. $x_1x_2(x'_1x'_2)^{-1}$ есть некоторый элемент $u=u'u_1$ группы U, что и нужно было доказать.

Так как класс v_3, таким образом, определен, коль скоро определены классы v_1 и v_2, то полагаем:

$$v_1\cdot v_2 = v_3. \qquad (2.41)$$

Это есть *определение* произведения $v_1\cdot v_2$ двух классов v_1 и v_2. Итак:

произведением *двух классов v_1 и v_2 называется класс v_3 построенный по следующему правилу: в каждом из классов v_1 и v_2 выбираем по произвольному элементу, перемножаем эти два элемента и берем класс, к которому принадлежит их произведение; этот класс и есть класс v_3.*

Из этого определения и из того, что произведение элементов в группе G удовлетворяет условию ассоциативности, непосредственно следует, что и умножение классов удовлетворяет условию ассоциативности.

Докажем, что класс U по отношению к только что определенному умножению играет роль нейтрального элемента, т.е. что для всякого класса v справедливо равенство

$$v\cdot U = U\cdot v = v. \qquad (2.42)$$

Для этого выберем произвольный элемент x класса v, а в качестве элемента класса U выберем нейтральный элемент 1. Тогда, по определению умножения, класс $v\cdot U$ есть класс, который содержит элемент $x\cdot 1=x$, т.е. тот же класс v. Точно так же класс $U\cdot v$ есть класс, который содержит элемент $1\cdot x = x$, т.е. тот же класс v. Этим формула (2.42) доказана.

Докажем наконец, что к каждому классу K имеется некоторый обратный класс, который обозначим через K^{-1} и который удовлетворяет условию

$$K\cdot K^{-1} = K^{-1}\cdot K = U.$$

Для этого возьмем в классе K какой-нибудь элемент a и определим класс K^{-1} как класс, который содержит элемент a^{-1}. По определению произведений классов, каждое из двух произведений $K\cdot K^{-1}$ и $K^{-1}\cdot K$ представляет собой класс, который содержит элемент $a\cdot a^{-1}=a^{-1}\cdot a=1$, а это и есть класс U.

Итак, определенное нами умножение удовлетворяет всем аксиомам понятия групп. следовательно, *при нашем определении произведения множество классов группы G по ее инвариантной подгруппе U есть некоторая группа V. Класс U при этом есть нейтральный элемент группы V.*

Группа V называется ***факторгруппой*** *группы G по ее инвариантной подгруппе U.*

2. Теорема о гомоморфных отображениях. Пусть по-прежнему даны группа G и ее инвариантная подгруппа U. Каждому элементу x группы G поставим в соответствие определенный элемент факторгруппы V, а именно: тот класс, который содержит в себе элемент x.

Этим устанавливается отображение φ группы G на группу V и из определения умножения в группе V непосредственно следует, что это отображение гомоморфно.

Какие элементы группы G отображаются на нейтральный элемент группы V? Так как этим нейтральным элементом является U, то очевидным ответом на наш вопрос есть:

Все элементы инвариантной подгруппы U и только они при отображении φ *отображаются на нейтральный элемент группы U.*

Из этого и предыдущего пунктов следует: всякая инвариантная подгруппа U группы G является ядром некоторого гомоморфного отображения группы G, а именно, гомоморфного отображения группы G на ее факторгрупу по отношению к U.

Пусть теперь дано произвольное гомоморфное отображение f какой-нибудь группы A на какую-нибудь группу B. Пусть U есть ядро этого гомоморфного отображения. Мы знаем, что U — инвариантная подгруппа группы A. Обозначим через V факторгруппу группы A по отношению к U.

Пусть b есть какой-нибудь элемент группы B. Существует по крайней мере один элемент a группы A, отображающийся отображением f на элемент b:

$$b = f(a).$$

Определим полный прообраз элемента b при отображении f, т.е. множество элементов x группы A, отображающихся отображением f на b. Этот полный прообраз обозначим, как обычно, через $f^{-1}(b)$.

Итак, $f^{-1}(b)$, по определению, есть множество всех тех элементов x группы A, для которых справедливо равенство

$$f(x) = b.$$

Пусть, как уже было сказано, a — какой-нибудь элемент, отображающийся на b; если x есть другой элемент множества $f^{-1}(b)$, то $f(a) = b$, $f(x) = b$,

$$f(a^{-1}) = b^{-1},$$
$$f(xa^{-1}) = b\cdot b^{-1} = 1$$

(единица справа есть нейтральный элемент группы B); это значит, что xa^{-1} есть некоторый элемент u группы U, т.е. $x=au$ есть элемент того класса по инвариантной подгруппе U, к которому принадлежит a. Обратно, если a и x принадлежат к одному классу, то

$$x= a\,u,$$
$$f(x) = f(a)\cdot f(u)=f(a)\cdot 1=f(a),$$

т.е. a и x отображаются в один и тот же элемент b группы B, или, другими словами, содержатся в том же полном прообразе $f^{-1}(b)$.

Итак, полные прообразы $f^{-1}(b)$ элементов группы B суть классы группы A по инвариантной подгруппе U.

Этим обстоятельством устанавливается взаимно однозначное соответствие ψ между группой B и группой V.

Каждому элементу группы V, который есть некоторый класс группы A по инвариантной подгруппе U, т.е. полный прообраз некоторого элемента b группы B, соответствует именно этот элемент b группы B; при этом каждый элемент b группы B оказывается поставленным в соответствие одному-единственному классу, т.е. одному-единственному элементу группы V, именно тому классу, который является полным прообразом элемента b. Отображение ψ гомоморфно: пусть v_1 и v_2 - два элемента группы V и

$$v_1\cdot v_2 = v_3. \qquad (2.43)$$

Пусть a_1 есть какой-нибудь элемент класса v_1, a_2 — какой-нибудь элемент класса v_2, $a_3=a_1\cdot a_2$. Мы знаем, что тогда a_3 принадлежит v_3. Положим

$$f(a_1) = b_1,\ f(a_2)=b_2, f(a_3) = b_3.$$

Так как f гомоморфно, то

$$b_1\cdot b_2 = b_3. \qquad (2.44)$$

Но так как v_1, v_2, v_3 суть соответственно полные прообразы элементов b_1, b_2, b_3, то

$$\psi(v_1) = b_1, \quad \psi(v_2)=b_2, \quad \psi(v_3)=b_3,$$

так что равенство (2.44) может быть переписано в виде

$$\psi(v_1)\cdot \psi(v_2) = \psi(v_3),$$

чем и доказан гомоморфный характер отображения ψ. Как взаимно однозначное гомоморфное отображение группы V на группу B, отображение ψ есть изоморфное отображение V на B. Итогом всего предыдущего является следующая теорема.

Теорема Э. Нетера о гомоморфных отображениях.

Всякое гомоморфное отображение одной группы A на другую группу B имеет своим ядром некоторую инвариантную подгруппу группы A. Обратно, всякая инвариантная подгруппа U группы A есть ядро некоторого гомоморфного отображения φ *группы A на факторгруппу V группы A по подгруппе U. Отображение* φ *получается, если каждому элементу группы A поставить в соответствие его класс относительно инвариантной подгруппы U. Если f есть произвольное гомоморфное отображение группы A на группу B, то полные прообразы элементов группы B при этом отображении суть классы группы A по ядру U отображения f и группа B изоморфна факторгруппе группы A по подгруппе U.*

Итак, инвариантные подгруппы данной группы A совпадают с ядрами всевозможных гомоморфных отображений этой группы, а все группы, являющиеся гомоморфными образами группы A, совпадают с группами, изоморфными факторгруппам группы A по всевозможным ее инвариантным подгруппам.

Следствие. *Для того чтобы гомоморфное отображение группы A на группу B было изоморфным, необходимо и достаточно, чтобы ядро этого отображения состояло из одного нейтрального элемента группы A.*

2.9. Группа перемещений плоскости и пространства и их подгрупп

2.9.1. Группа перемещений плоскости.

Напомним, что перемещением плоскости называется такое преобразование, которое сохраняет расстояния. Другими словами, преобразование F называется перемещением, если для любых двух различных точек A и B плоскости справедливо соотношение $|AB| = |A'B'|$, где $A'=F(A)$ и $B'=F(B)$. Примеры перемещений хорошо известны читателю со школьного курса геометрии. Это *параллельный*

перенос T_a, *поворот* R^{α}_{O} вокруг точки O на угол α, *симметрия* S_l относительно оси l, а также *скользящая симметрия* $S^{a}_{l}(a||b)$, которая по определению есть композиция $S^{a}_{l}=T_a \sqcup S_l=S_l \circ T_a$. Оказывается, что других перемещений плоскости нет.

Теорема 1 (Шаль). *Любое перемещение плоскости есть либо параллельный перенос, либо поворот, либо скользящая симметрия (в частности, симметрия, если* $a = 0$*).*

Доказательство. Доказательство этого утверждения основано на так называемой *«аксиоме подвижности плоскости»*, согласно которой существует ровно два перемещения, которые переводят пару (различных) точек A, B плоскости в любую другую пару точек A_1, B_1, для которых $|A_1B_1|=|AB|$. Пусть теперь F — некоторое перемещение, A_0 — некоторая точка на плоскости, $A_1=F(A_0)$, $A_1=F(A_1)$. Рассмотрим три случая:

1) $A_2 = A_0$;
2) $A_2 \neq A_0$, но точка A_2 лежит на прямой (A_0A_1);
3) точка A_2 не лежит на прямой (A_0A_1).

Если в каждом из этих трех случаев мы найдем по два различных перемещения из тех, которые бели указаны в формулировке теоремы, то в силу упомянутой выше аксиомы это и является доказательсьвом теоремы.

В случае 1) эти перемещения суть поворот вокруг середины отрезка $[A_0A_1]$ на угол π и симметрия относительно прямой, перпендикулярной к $[A_0A_1]$ и проходящей через ее середину.

В случае 2) требуемыми перемещениями являются параллельный перенос на вектор $a = \overrightarrow{A_0A_1}$ и симметрия относительно прямой, перпендикулярной к (A_0A_2) и проходящей через точку A_1.

В случае же 3) это поворот вокруг точки O – точки пересечение перпендикуляров, восстановленных из середины отрезков $[A_0A_1]$ и $[A_1A_2]$ (рис. 2.16) и скользящая симметрия, ось которой параллельна оси (A_0A_2) и проходит через середину $[A_1A'_1]$, где A'_1 — прямоугольная проекция точки A_1 на (A_0A_2), а вектор $\boldsymbol{a}= \overrightarrow{A_0A'_1}$ (рис. 2.17). Теорема доказана.

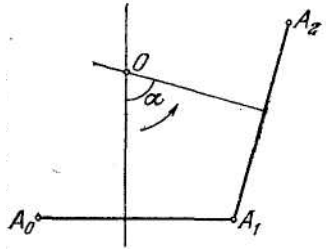


Рис. 2.16

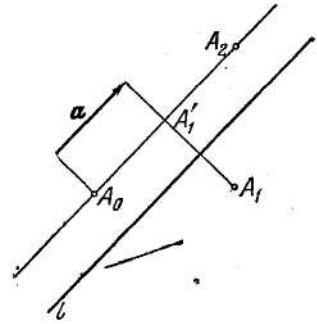


Рис. 2.17

Параллельный перенос и поворот называются перемещениями *первого рода,* а симметрия и скользящая симметрия — *перемещениями второго рода.*

Имеет место следующее утверждение: *композиций двух перемещений первого рода есть перемещение первого рода, композиция перемещений первого и второго рода есть перемещение второго рода, а композиция перемещений второго рода есть перемещение первого рода.*

Приведем краткое доказательство этого утверждения.

Доказательство основывается на следующем простом факте: композиция двух симметрий $S_{l_2} \sqcup S_{l_1}$ есть параллельный перенос T_a в случае, когда $l_1 \parallel l_2$ и поворот R^{α}_{O}, когда эти прямые пересекаются в точке O. Кроме того, вектор $\boldsymbol{a}$ в перемещении T_a перпендикулярен к l_1 и l_2, направлен от l_1 к l_2 и по величине равен удвоенному расстоянию между этими прямыми. Угол α в повороте R^{α}_{O} есть удвоенный угол между прямыми l_1 и l_2,

Из этого факта вытекает, что любой параллельный перенос и любой поворот можно представить в виде композиции двух симметрий. Например, чтобы получить такое представление для данного параллельного переноса T_a, выбираем произвольную прямую l_1 перпендикулярную к $\boldsymbol{a}$ и параллельно переносим ее с помощью $T_{a/2}$; тогда $T_a = S_{l_2} \circ S_{l_1}$, где $l_2 = T_{a/2}(l_1)$. Аналогично и для поворота. Значит, любое перемещение плоскости есть композиция некоторого числа симметрий: поворот и параллельный перенос - композиция двух симметрий, самая симметрия — композиция одной симметрии, скользящая симметрия - композиция трех симметрий. Заметим, что перемещение первого рода суть *композиции четного числа симметрий,*

а перемещение второго рода — *композиции нечетного числа симметрий*. Верно и обратное: если перемещение первого (второго) рода каким бы то ни было способом представлено в виде композиции некоторого числа симметрий, то это число симметрий четное (нечетное). (*Указание*. Оно эквивалентно следующему утверждению: *не существует представления тождественного преобразования в виде нечетного числа симметрий.)*

В силу сказанного высше перемещения первого и второго рода можно определить как такие перемещения, которые разлагаются в композиции соответственно четного и нечетного числа симметрий. Следовательно, композиция двух перемещений первого рода есть перемещение первого рода, композиция перемещений первого и второго рода - перемещение второго рода, а композиция двух перемещений второго рода - перемещение первого рода, что и требовалось.

Все перемещения плоскости образуют группу, *операцией* в которой является *композиция перемещений.* Действительно, если два преобразования сохраняют расстояние между точками, то сохраняет его и композиция этих преобразований, т.е. ***композиция перемещений есть <u>перемещение</u>***. Аксиома ассоциативности выполнена, поскольку она выполнена для всех вообще преобразований плоскости. Далее, тождественное преобразование есть перемещения. И наконец, преобразование, обратное к перемещению, также сохраняет расстояние, т.е. является перемещением.

Группа всех перемещений плоскости обозначается ***E(2).*** Она содержит бесконечное число подгрупп. Прежде всего, в силу сказанного выше подгруппу образуют все перемещения первого рода. Мы будем обозначать эту подгруппу через $\boldsymbol{E_0(2)}$**.** Если F — перемещение первого рода, а G — произвольное перемещение, то $G \sqcup F \circ G^{-1}$ есть непременно перемещение первого рода, поэтому подгруппа перемещений первого рода $\boldsymbol{E_0(2)}$ инвариантна в группе всех перемещений ***E(2).*** Легко видеть, что существуют ровно два класса по этой подгруппе: она сама и класс перемещений второго рода. Следовательно, подгруппа $\boldsymbol{E_0(2)}$ имеет индекс 2 в группе всех перемещений ***E*(2)** и факторгруппа ***E*(2)** по $\boldsymbol{E_0(2)}$ является циклической группой из двух элементов.

Займемся теперь группой $\boldsymbol{E_0(2)}$. Среди подгрупп этой группы отметим прежде всего бесконечное число *групп поворотов:* совокупность всех поворотов плоскости вокруг какой-нибудь определенной ее точки образует группу, и каждая из этих групп, как

нетрудно видеть, изоморфна группе ***SO (2)*** (см. п.2.5.2); следовательно, *все эти группы коммутативны.*

Совокупность всех поворотов подгруппы не образует. Чтобы убедиться в этом, достаточно рассмотреть два поворота вокруг двух различных точек на углы, в сумме составляющие 2π — их композицией будет *параллельный перенос*.

Возле с группами поворотов, в группе $\boldsymbol{E_0(2)}$ есть *подгруппы параллельных переносов вдоль различных прямых.*

Если задана прямая l, то *параллельные переносы вдоль l — это такие переносы, векторы которых параллельны l.* Очевидно, что такие параллельные переносы образуют подгруппу в $\boldsymbol{E_0(2)}$. Так как любой такой параллельный перенос однозначно характеризуется длиной и направлением вектора переноса, то группа всех параллельных переносов вдоль данной прямой l *изоморфна группе всех действительных чисел* (с обыкновенным сложением в качестве групповой операции).

Рассмотрим два параллельных переноса T_a и T_b, векторы которых не параллельны. Композиция этих параллельных переносов в любом порядке есть параллельный перенос T_{a+b}. Поэтому множество всех параллельных переносов плоскости образует коммутативную подгруппу в группе $\boldsymbol{E_0(2)}$. Эта подгруппа обозначается $\boldsymbol{T(2)}$.

Пусть даны два перемещения F и G из группы $\boldsymbol{E_0(2)}$. Выясним, что происходит при трансформации перемещения F с помощью перемещения G. По определению, это будет перемещение

$$H(P) = G \sqcup F \circ G^{-1}(P). \qquad (2.45)$$

Так как G - взаимно однозначное отображение плоскости, то перемещение H будет вполне описано, если будет указано, куда в результате этого перемещения перейдет точка $G(P)$ при любом P. Другими словами, отображение H будет определено для любой точки P, если мы будем знать, куда оно переводит точку $G(P)$.

Поэтому, заменяя в формуле (2.45) точку P точкой $G(P)$, и учитывая, что $G^{-1} \circ G(P) = P$, мы получим

$$H \circ G(P) = G \circ F(P). \qquad (2.46)$$

Эта формула определяет перемещение $H(P)$. Обозначим $F(P)=Q$. тогда

$$H \circ G(P) = G(Q),$$

т.е. перемещение H переводит точку $G(P)$ в точку $G(Q)$.

Предложение 1. *Если F - поворот вокруг точки O на угол α, то H — поворот вокруг точки $G(O)$ также на угол α.*

Доказательство. Так как F - поворот вокруг точки O, то $F(O)=O$, откуда по формуле (2.46)

$$H \circ G(O) = G(O),$$

т.е. H есть поворот вокруг точки $G(O)$.

Поскольку перемещение переводит угол в конгруэнтный ему угол, то угол поворота H, по-прежнему, равен α, что и требовалось доказать.

Следствие. *Трансформация группы поворотов плоскости вокруг точки P при помощи произвольного перемещения F есть группа поворотов плоскости вокруг точки $F(P)$. В частности, никакая группа поворотов не является инвариантной подгруппой в* $\boldsymbol{E_0(2)}$.

Рассмотрим теперь группу параллельных переносов. Для нее справедливо следующее предложение.

Предложение 2. *Группа* $\boldsymbol{T(2)}$ *всех параллельных переносов плоскости является инвариантной подгруппой в группе* $\boldsymbol{E_0(2)}$.

Доказательство. Пусть F — некоторый параллельный перенос, а G — произвольное перемещение плоскости. Пусть l — некоторая прямая, параллельная вектору переноса F. Тогда имеет место равенство

$$F(l) = l,$$

означающее, что при перемещении F прямая l переходит в себя. Перемещение G переводит прямую l в прямую $G(l)$. Из формулы (2.46), примененной к любой точке P прямой l, следует

$$H \llcorner G(l) = G(l);$$

т.е. перемещение H переводит прямую $G(l)$ в себя и, следовательно, является параллельным переносом вдоль этой прямой. Поскольку G — перемещение, то расстояние между точками P и $Q=F(P)$ равно расстоянию между точками $G(P)$ и $G \circ F(P)$, т.е. между $G(P)$ и $H \circ G(P)$. Следовательно, вектор параллельного переноса H совпадает с вектором параллельного переноса F. Предложение доказано.

Выделив в группе $\boldsymbol{E_0(2)}$ подгруппу $\boldsymbol{T(2)}$ параллельных переносов и подгруппы поворотов вокруг различных точек, естественно задать такой вопрос: можно ли представить любое перемещение из $\boldsymbol{E_0(2)}$ как композицию переноса из $\boldsymbol{T(2)}$ и поворота вокруг некоторой фиксированной точки.

Ответ на этот вопрос есть утвердительным, что вытекает со следующего предложения.

Предложение 3. *Любое перемещение первого рода можно однозначно представить в виде композиции* $R^{\alpha}_{O} \circ T_a$ *параллельного переноса и поворота вокруг фиксированной точки O плоскости.*

Доказательство. Пусть F — некоторое перемещение первого рода, O'-*Прообраз* точки O при перемещении F, т.е. $O'=F^{-1}(O)$. Рассмотрим композицию $T_{\overline{O'O}} \circ F^{-1}$. Это перемещение, очевидно, оставляет точку O на месте и является перемещением первого рода. Поэтому $T_{\overline{O'O}} \circ F^{-1}$

поворот. Так как перемещение, обратное повороту, есть поворот, мы получаем необходимую композицию. Единственность этой композиции непосредственно следует из единственности параллельного переноса $T_{\overrightarrow{O'O}}$. Предложение доказано.

Замечание. Верно, кроме того, и следующее утверждение: *любое перемещение первого рода однозначно разлагается в композицию* $T_b \sqcup R^{\beta}_{O}$ *поворота вокруг фиксированной точки плоскости и параллельного переноса.*

Для доказательства рассмотрим некоторое перемещение первого рода G. Пусть $G(O) = O'$. Тогда композиция $T_{\overrightarrow{O'O}} \circ G$ переводит точку O в себя и, значит, есть поворот вокруг этой точки:

$$T_{\overrightarrow{O'O}} \circ G = R^{\beta}_{O}$$

Рассмотрим композицию поворота R^{β}_{O} и параллельного переноса $T_{\overrightarrow{OO'}}$. Имеем

$$T_{\overrightarrow{OO'}} \circ R^{\beta}_{O} = T_{\overrightarrow{OO'}} \circ T_{\overrightarrow{O'O}} \circ G = G,$$

что и требовалось.

Пусть G_1 и G_2 - два перемещения из группы $\boldsymbol{E_o}$**(2).** В силу только что доказанного предложения $G_1 = R^{\alpha}_{O} \circ T_a$ и $G_2 = R^{\beta}_{O} \circ T_b$. Композиция $G_2 \circ G_1$ этих перемещений, с одной стороны, есть перемещение $R^{\beta}_{o} \circ T_b \circ R^{\alpha}_{o} \circ T_a$, а с другой стороны, согласно предложению $G_2 \circ G_1 = R^{\gamma}_{O} \circ T_c$ для некоторого угла γ и вектора $\boldsymbol{c}$. Угол γ и вектор $\boldsymbol{c}$ нетрудно вычислить, зная углы α, β и векторы $\boldsymbol{a}$, $\boldsymbol{b}$. Мы оставляем читателю эти вычисления и укажем здесь лишь окончательный ответ

$$\gamma = \alpha+\beta, \quad \boldsymbol{c} = \boldsymbol{a} + R^{-\alpha}_{O}(\boldsymbol{b}).$$

Полученный результат можно сформулировать так.

Каждый элемент группы $\boldsymbol{E_o}$**(2)** однозначно представляется в виде упорядоченной пары (R^{α}_{o}, T_a), где $R^{\alpha}_{O} \in$ ***SO (2),*** $T_a \in$ ***T*(2).** Умножение упорядоченных пар (R^{α}_{O}, T_a) и (R^{β}_{O}, T_b) в группе $\boldsymbol{E_o}$**(2)** выполняется по формуле

$$(R^{\beta}_{O}, T_b) \circ (R^{\alpha}_{O}, T_a) = (R^{\alpha+\beta}_{O}, T_{a+R_O^{-\alpha}(b)}).$$

2.9.2. Группа перемещений пространства.

Аналогично перемещением плоскости перемещения пространства определяются как преобразование пространства, сохраняющие расстояния между точками. К ним прежде всего относится

параллельный перенос T_a на вектор $\boldsymbol{a}$, определение которого дословно повторяет соответствующее определение для плоскости. Другими примерами перемещений пространства являются *поворот* R^{α}_{l} *вокруг оси* l *на угол* α, *винтовое перемещение* $S^{a}_{l,\alpha}$, *симметрия* S_{π} *относительно плоскости* π, *скользящая симметрия, поворотная симметрия*. Эти перемещения определяются следующим образом:

а) Поворот R^{α}_{l} вокруг оси l на угол α - это перемещение, состоящее в повороте каждой точки пространства в плоскости, которая проходит через эту точку и перпендикулярной к данной прямой l (оси поворота), на данный угол α (угол поворота) вокруг точки пересечения этой плоскости с осью.

Ось и угол поворота задают поворот неоднозначно. Действительно, один и тот же результат можно получить, выполняя поворот вокруг данной оси на угол α в одном направлении и на угол $2\pi-\alpha$ в другом направлении .

Впрочем, такая же неоднозначность существует и для поворотов на плоскости. Чтобы избежать этой неоднозначности, на плоскости вводят понятие положительного направления поворота - это поворот против часовой стрелки. В случае поворотов в просторные поступают так: выбирают на оси поворота определенное направление и считают, что поворот является положительным относительно данного направления на оси, если любая точка поворачивается в своей плоскости против часовой стрелки для зрителя, который стоит вдоль оси так, что направление от его ног к его главе и есть направление, которое было выбрано на оси.

В случае, когда угол поворота равен π, поворот называют *опрокидыванием* относительно данной оси (другое название перемещения R^{π}_{j} — осевая симметрия).

В этом случае нет потребности указывать направление поворота. Опрокидывание R^{π}_{j} обладает следующим свойством: $R^{\pi}_{j} \sqcup R^{\pi}_{j} = E$, где E — тождественное перемещение.

b) *Винтовым перемещением* $S^{a}_{l,\alpha}$ называется композиция поворота R^{α}_{j} вокруг оси l и параллельного переноса T_a, при условии, что вектор $\boldsymbol{a}$ параллелен оси поворота.

Порядок, в котором выполняются указанные перемещения, безразличен (что не имело бы места, если бы вектор $\boldsymbol{a}$ не был параллелен оси l).

Частными случаями винтового перемещения являются поворот и параллельный перенос.

Если задано некоторое винтовое перемещение, то тем самым задано и направление на оси поворота — это направление вектора $\boldsymbol{a}$. В

соответствии с этим винтовое перемещение называется *положительным* (правым) или *отрицательным* (левым), в зависимости от того, имеет ли данный поворот положительное или отрицательное направление оси относительно направления $\boldsymbol{a}$.

c) *Симметрия S_π относительно плоскости* π - это перемещение, которое оставляет все точки данной плоскости π на месте, а любую другую точку A пространства переводит в точку A' такую, что прямая (AA') перпендикулярна к плоскости π и $|AO|=|OA'|$, где O - точка пересечения прямой (AA') и плоскости π.

d) *Скользящая симметрия* — это композиция $T_a \circ S_\pi = S_\pi \circ T_a$, где вектор $\boldsymbol{a}$ параллелен плоскости π (благодаря чему порядок операций в композиции безразличен).

e) *Поворотная симметрия* — это композиция $R_l^{180^\square} \circ S_\pi = S_\pi \circ R_l^{180^o}$, где ось l перпендикулярна к плоскости π (что снова делает безразличным порядок операций в композиции).

Оказывается, что этими примерами исчерпываются все перемещения пространства; точнее, справедлива следующая теорема (которую мы приведем без доказательства).

Теорема 1. *Любое перемещение пространства есть либо параллельный перенос, либо поворот вокруг оси, либо винтовое перемещение, либо симметрия относительно плоскости, либо скользящая симметрия, либо поворотная симметрия.*

Чтобы рассматривать дальнейший матерал, нам понадобится некоторые сведения о композиции пространственных перемещений.

Теорема 2. *Композиция двух опрокидываний относительно различных осей представляет собой:*

a) *если оси параллельны — параллельный перенос, перпендикулярный к обеим осям, равный удвоенному переносу, переводящему первую ось во вторую;*

b) *если оси пересекаются — поворот вокруг общего перпендикуляра к обеим осям, проходящего через точку пересечение, на угол, равный удвоенному углу поворота, переводящего первую ось во вторую;*

c) *если оси не лежат в одной плоскости — винтовое перемещение, имеющее своей осью общий перпендикуляр к обеим осям и равное удвоенному винтовому перемещению, переводящему первую ось во вторую* (существование такого перемещения будет следовать из доказательства теоремы). (Термин удвоенное винтовое перемещение означает следующее. Если $S^{\boldsymbol{a}}_{l,\alpha}$ некоторое винтовое перемещение, то удвоенное по отношению к $S^{\boldsymbol{a}}_{l,\alpha}$ винтовое перемещение – это $S^{2\boldsymbol{a}}_{l,2\alpha}$).

Доказательство. а) Пусть l_1 и l_2 — оси данных опрокидываний, A - некоторая точка пространства, a_1 — ее прямоугольная проекция на ось l_1, A'- образ точки A при опрокидывании относительно оси l_1 ,a_2 — прямоугольная проекция точки A' на ось l_2 и A'' — образ точки A' при опрокидывании относительно оси l_2 (рис. 2.18).

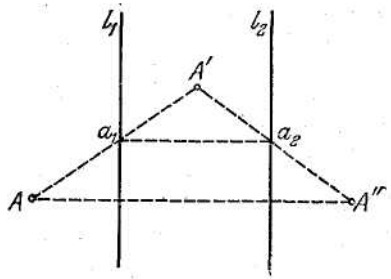


Рис. 2.18

Плоскость, перпендикулярная осям l_1 и l_2 и проходящая через точку A, проходит через прямую (AA') перпендикулярную к l_1, и через прямую (AA''), перпендикулярную к l_2. Поэтому прямая (a_1a_2) является общим перпендикуляром к прямым l_1 и l_2, а точка A'' получается из точки A параллельным переносом, равным удвоенному переносу, который переводит прямую l_1 в прямую l_2.

b) Пусть O - точка пересечения осей l_1 и l_2, π - содержащая их плоскость, (OC) — перпендикуляр к этой плоскости, которая проходит через точку O (рис. 2.19).

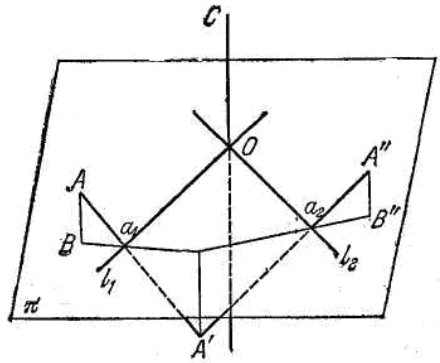


Рис. 2.19

Пусть, далее A — произвольная точка пространства, A' — ее образ при опрокидывании относительно оси l_1 (причем прямая (AA')

пересекает ось l_1 в точке a_1) и A'' - образ точки A' при опрокидывании относительно оси l_2 (причем прямая $(A'A'')$ пересекает ось l_2 в точке a_2).

Опрокидывание относительно осей l_1 и l_2 переводят плоскость π в себя. Поэтому если мы спроектируем точки A, A', A'' на эту плоскость в точки B, B' и B'', то точки B и B'' будут получаться из B' с помощью опрокидываний относительно осей l_1 и l_2 соответственно. Значит, точка A''- получается из точки A поворотом вокруг оси (OC) на угол, равный удвоенному углу между l_1 и l_2. Так как отрезки $[BA]$ и $[B''A'']$ конгруэнтны, параллельны (OC) и направлены в одну и ту же сторону, то этот же поворот вокруг оси (OC) совмести точку A с точкой A''.

с) Пусть теперь оси l_1 и l_2 не лежат в одной плоскости. Обозначим через (O_1O_2) общий перпендикуляр к l_1 и l_2, причем точка O_1 лежит на оси l_1, а точка O_2 лежит на оси l_2 (рис. 2.20).

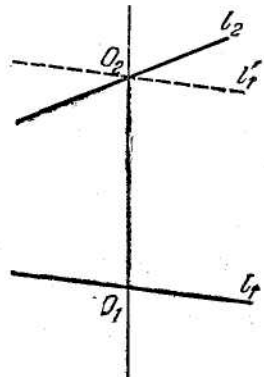


Рис. 2.20

Проведем через точку O_1 прямую l'_1, параллельную l_1. Рассмотрим композицию следующих четырех опрокидываний:

$$R^{\pi}_{l_2} \sqcup R^{\pi}_{l_1'} \circ R^{\pi}_{l_1'} \circ R^{\pi}_{l_1}.$$

Так как $R^{\pi}_{l_1'} \circ R^{\pi}_{l_1'}$ — тождественное преобразование, то эта композиция совпадает с искомой композицией $R^{\pi}_{l_2} \circ R^{\pi}_{l_1}$. С другой стороны, $R^{\pi}_{l_1'} \circ R^{\pi}_{l_1'}$ есть параллельный перенос, равный удвоенному переносу, переводящему ось l_1 в ось l'_1; композиция же $R^{\pi}_{l_2} \circ R^{\pi}_{l_1'}$, есть поворот вокруг прямой (O_1O_2) на угол, равный удвоенному углу между осями l'_1 и l_2. Следовательно, исходная композиция $R^{\pi}_{l_2} \circ R^{\pi}_{l_1}$ представляет собой винтовое перемещение, равное

удвоенному винтовому перемещению, переводщему l_1 в l_2. Теорема доказана.

Последняя теорема позволяет разложить любое винтовое перемещение в композицию двух опрокидываний. А именно, имеет место следующая теорема.

Теорема 3. *Любое винтовое перемещение можно представить в виде композиции двух опрокидываний относительно двух различных прямых.*

Эти прямые удовлетворяют следующим условиям:

а) *если винтовое перемещение есть параллельный перенос, то они перпендикулярны к направлению перемещения;*

b*) если винтовое перемещение есть поворот или винтовое перемещение в собственном смысле слова, то они пересекают ось под прямым углом.*

Одну из этих прямых можно выбрать в остальном произвольно; другая прямая при этом определяется однозначно.

С помощью теоремы 3 можно установить следующий важный результат.

Теорема 4. *Композиция двух винтовых перемещений есть винтовое перемещение.*

Если эти винтовые перемещения суть повороты вокруг осей, проходящих через одну точку, то их композиция есть также поворот вокруг оси, проходящей через ту же точку.

Если эти винтовые перемещения суть параллельные переносы, то их композиция также будет параллельным переносом.

Доказательство. Рассмотрим два винтовых перемещения, которые имеют своими осями прямые l_1 и l_2 (рис. 2.21).

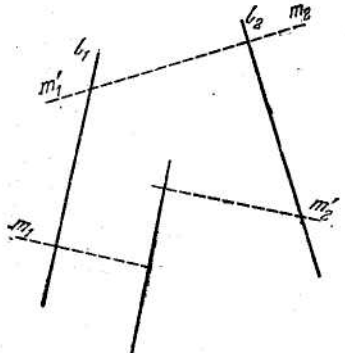


Рис. 2.21

Первое из них есть композиция двух опрокидываний относительно осей m_1 и m'_1, причем m'_1 можно взять произвольно среди прямых, пересекающих l_1 под прямым углом. Аналогично, второе винтовое перемещение есть композиция опрокидываний относительно осей m_2 и m'_2, причем m_2 можно взять произвольно среди прямых, пересекающих l_2 под прямым углом. Совместим теперь прямые m'_1 и m_2 с общим перпендикуляром к осям l_1 и l_2. Тогда эти прямые совпадут и опрокидывания относительно них взаимно уничтожатся. В результате останутся лишь опрокидывания относительно прямых m_2 и m'_2, композиция которых в силу теоремы 2 будет винтовым перемещением.

Если данные винтовые перемещения являются поворотами вокруг осей l_1 и l_2, проходящих через точку O, то через эту же точку пройдут прямые m'_1, m_1 и m'_2. Поэтому композицией этих перемещений будет поворот вокруг оси, которая проходит через точку O.

Если же данные перемещения суть параллельные переносы, то прямые m_1, m'_1 и m'_2 параллельны между собой. Следовательно, результирующее перемещение также будет паралельим переносом, что требовалось.

Рассмотрим теперь композицию двух симметрий S_{π_1} и S_{π_2}.

Теорема 5. *Композиция* $S_{\pi_2} \sqcup S_{\pi_1}$ *представляет собой:*

a) *если плоскости* π_1 *и* π_2 *параллельны — параллельный перенос, перпендикулярный к обоим плоскостям и равный удвоенному переносу, переводящему плоскость* π_1 *в плоскость* π_2*;*

b) *если плоскости* π_1 *и* π_2 *пересекаются по прямой* l *— поворот вокруг* l *на угол, равный удвоенному углу между плоскостями* π_1 *и* π_2.

Доказательство. Пусть A - некоторая точка пространства. Так как симметрии S_{π_1} и S_{π_2} переводят у себя плоскость, которая проходит через A и перпендикулярную к плоскостям π_1 и π_2, то теорема сводится к изучению композиции двух осевых симметрий на плоскости. Эта композиция есть либо параллельный перенос, перпендикулярный к осям, равный удвоенному переносу, переводящему первую ось во вторую, либо же поворот вокруг точки пересечения осей на удвоенный угол между ними. Отсюда следует утверждение теоремы.

Теорема 5 позволяет представить параллельный перенос и поворот в виде композиции двух симметрий. В частности, опрокидывание есть композиция двух симметрий относительно перпендикулярных плоскостей. Так как винтовое перемещение представляет собой композицию двух опрокидываний, то его можно разложить в композицию четырех симметрий.

Назовем параллельный перенос, поворот и винтовое перемещение — *перемещениями первого рода*, а симметрию относительно плоскости, скользящую симметрию и поворотную симметрию — *перемещениями второго рода*.

Так же как и для перемещений плоскости, имеет место следующее утверждение:

композиция двух перемещений первого рода есть перемещение первого рода, композиция перемещений первого рода и второго рода есть перемещение второго рода и композиция двух перемещений второго рода есть перемещение первого рода.

Доказательство этого утверждения аналогично доказательству соответствующего утверждения для плоскости. Прежде всего, в силу теоремы 5 любое перемещение пространства можно представить в виде композиции некоторого числа симметрий относительно различных плоскостей. А именно, параллельный перенос и поворот есть композиция двух таких симметрий, винтовое перемещение - композиция четыре симметрий, сама симметрия - композиция одной симметрии, скользящоя симметрия и поворотная симметрия - композиция трех симметрий. Следовательно, любое перемещение первого рода есть композиция четного числа симметрий, любое перемещение второго рода - композиция нечетного числа симметрий.

Обратное тоже верно: если перемещение есть композиция четного числа симметрий, то это перемещение первого рода; если же перемещение есть композиция нечетного числа симметрий, то это перемещение второго рода.

Для доказательства предположим, что некоторое перемещение раслагается в композицию симметрии двумя способами:

$$F = S_{2k} \sqcup S_{2k-1} \circ \ldots \circ S_2 \circ S_1$$

и

$$F = S'_{2l+1} \circ S'_{2l} \circ \ldots \circ S'_2 \circ S'_1,$$

причем в одном случае число эти симметрий четное, а в другом - нечетное. Тогда имеем тождество

$$S_{2k} \circ S_{2k-1} \circ \ldots \circ S_2 \circ S_1 = S'_{2l+1} \circ S'_{2l} \circ \ldots 'S'_2 \circ S'_1.$$

Рассмотрим композицию левой и правой части этого тождества с S'_{2l+1}. Учитывая, что $S'_{2l+1} \circ S'_{2l+1} = E$ — тождественное перемещение, получим

$$S'_{2l+1} \circ S_{2k} \circ S_{2k-1} \circ \ldots \circ S_2 \circ S_1 = S'_{2l} \circ \ldots \circ S'_2 \circ S'_1,$$

т.е. мы «перенесли симметрию S'_{2l+1} в левую часть». Продолжая эту процедуру, в конце концов мы придем к тождеству

$$S'_1 \circ S'_2 \circ \ldots \circ S'_{2l} \circ S'_{2l+1} \circ S_{2k} \circ S_{2k-1} \circ \ldots \circ S_2 \circ S_1 = E, \qquad (2.47)$$

где в левой части стоит нечетное число симметрий. Доказав, что такое невозможно, мы получим, что для любого перемещения четность или нечетность числа симметрий, которые входят в произвольное разложение этого перемещения в виде композиции симметрии, не зависит от конкретного разложения. Это и будет означать, что четность или нечетность числа симметрий полностью определяет род перемещения. Из всего сказанного следует, что перемещение первого (второго) рода можно определить как перемещения, разлагающиеся в композиции четного (нечетного) числа симметрий, откуда вытекает требуемое утверждение.

Замечание 1. Тот факт, что композиция перемещений первого рода есть перемещение первого рода, непосредственно следует из теоремы 4, что является еще одним его доказательством.

Замечание 2. Мы не имеем возможности осветить все аспекты теории пространственных перемещений. Подробно эта теория изложена в книге Коксетера «Введение в геометрию».

Равно как в случае плоскости, множество всех перемещений пространства образовывает группу, операцией в которой есть композиция перемещений. Эта группа обозначается ***E*(3).**

Согласно сказанному выше множество всех перемещений первого рода образует подгруппу $\boldsymbol{E_o}$**(3)** в группе ***E*(3).** Поскольку трансформация $G^{-1}{\circ}F{\circ}G$ произвольного перемещения первого рода есть снова перемещение первого рода, то эта подгруппа инвариантна в группе ***E(3).*** Аналогично случаю плоскости существует ровно два класса по этой подгруппе: она сама и класс перемещений второго рода. Поэтому $\boldsymbol{E_o}$**(3)** имеет индекс 2 в группе ***E(3)*** и факторгруппа ***E*(3)** по $\boldsymbol{E_o}$**(3)** есть циклическая группа из двух элементов.

Рассмотрим теперь подгруппы группы $\boldsymbol{E_0}$***(3).*** В качестве своей подгруппы эта группа содержит группу ***T*(3)** всех параллельных переносов пространства. Этот факт непосредственно следует из теоремы 4, согласно которой композиция двух параллельных переносов есть снова параллельный перенос. Группа ***T*(3)** коммутативна. Проще всего это установить, если заметить, что композиция двух параллельных переносов изображается диагональю параллелограмма, сторонами которых служат эти параллельные переносы.

Дословным повторением доказательства предложения 3 выходит

Предложение 5. *Группа* ***T*(3)** *является инвариантной подгруппой в группе перемещений первого рода* $\boldsymbol{E_0}$**(3).**

Бесконечную серию подгрупп группы $\boldsymbol{E_o}$***(3)*** образуют подгруппы поворотов вокруг фиксированных осей. Действительно, если *l* -

некоторая ось, R^{α}_{l}, R^{β}_{l} — два поворота вокруг нее, то композиция $R^{\alpha}_{l} \circ R^{\beta}_{l}$ есть поворот вокруг этой же оси на угол $\alpha+\beta$. Тождественное перемещение можно рассматривать как поворот вокруг оси l на нулевой угол. И, наконец, обратным к повороту R^{α}_{l} есть поворот вокруг оси l на угол $-\alpha$. Поскольку $R^{\alpha}_{l} \circ R^{\beta}_{l} = R_l^{\alpha+\beta} = R_l^{\beta+\alpha} = R^{\beta}_{l} \circ R^{\alpha}_{l}$, то группа поворотов вокруг фиксированной оси коммутативна.

Более интересную серию подгрупп в $\boldsymbol{E_o(3)}$ образуют перемещения первого рода, которые имеют данную недвижимую точкуку. Пусть A - некоторая точка пространства. Рассмотрим все такие перемещения из $\boldsymbol{E_o(3)}$, для которых точка A является неподвижной, т.е. такие перемещение F, что $F(A)=A$. Если F_1 и F_2 — два таких перемещения, то для $F_2 \sqsubset F_1$ имеем $F_2 \circ F_1(A)=F_2(A)=A$. Значит, для $F_2 \circ F_1$ точка A также является неподвижной. Ясно, что тождественное перемещение оставляет точку A на месте. Кроме того, если $F(A)=A$, то $F^{-1}(A)= A$. Это доказывается так:

Поскольку $F^{-1} \circ F = E$— тождественное перемещение,
то

$$A = F^{-1} \circ F(A) = F^{-1}(A).$$

Таким образом, перемещение, обратное к перемещению с недвижимой точкой A, само есть перемещения с недвижимой точкой A.

Итак, перемещения, имеющие данную недвижимую точку, *образуют группу*. Понятно, что эта группа является подгруппой в $\boldsymbol{E_o(3)}$. Кроме того, любые такие подгруппы, одна из которых оставляет неподвижной какую-нибудь точку A, а другая - точку A', — изоморфны между собой. Эти изоморфные группы принято обозначать $\boldsymbol{SO(3)}$ или $\boldsymbol{SO(3)_A}$, если мы хотим указать конкретную неподвижную точку A.

Группа $\boldsymbol{SO(3)_A}$ содержит в качестве подгрупп все группы поворотов вокруг осей, проходящих через точку A. Более подробная информация о группе $\boldsymbol{SO(3)_A}$ получается из следующего предложения.

Предложение 6. *Любое перемещение F из $\boldsymbol{SO(3)_A}$ имеет вид*

$$F = R^{\beta}_{l_2} \circ R^{\alpha}_{l_1},$$

где l_1 и l_2 — некоторые прямые, которые проходят через точку A.

Доказательство. Пусть B — некоторая точка пространства, которая отличная от A и $B'=F(B)$. Имеем $|AB|=|AB'|$; следовательно, точку B' можно совместить с точкой B посредством поворота $R^{\gamma}_{l_2}$ вокруг оси l_2, перпендикулярной к плоскости BAB' (и которая проходит через точку A) на угол γ, равный углу $B'AB$. Таким образом, композиция $R^{\gamma}_{l_2} \circ F$ оставляет на месте точки A и B, а значит, и любую точку

прямой $l_1 = (AB)$. Следовательно, перемещение $R^{\gamma}_{l_2} \sqcup F$ есть поворот вокруг оси l_1 на некоторый угол α:

$$R^{\gamma}_{l_2} \circ F = R^{\alpha}_{l_1} .$$

Возьмем композицию этого поворота $R^{\alpha}_{l_1}$ и поворота $R^{\beta}_{l_2} = R^{-\gamma}_{l_2}$:

$$R^{\beta}_{l_2} \circ R^{\alpha}_{l_1} = R^{-\gamma}_{l_2} \circ R^{\alpha}_{l_1} = R^{-\gamma}_{l_2} \circ R^{\gamma}_{l_2} \circ F = R^{-\gamma+\gamma}_{l_2} \circ F = F,$$

что и требовалось доказать.

Выясним теперь, что происходит при трансформации группы $\boldsymbol{SO(3)_A}$ некоторым элементом $G \in \boldsymbol{E_0(3)}$. Прежде всего заметим, что для перемещений пространства дословно остаются в силе рассуждения, предшествующие предложению 2 предыдущего пункта. А именно, если F и G два перемещения из $\boldsymbol{E_0(3)}$ и $H = G \circ F \circ G^{-1}$, то перемещение H полностью определяется формулой

$$H°G(P) = G°F(P),$$

совпадающей с формулой (2.46) предыдущего пункта. Поэтому имеет место следующее утверждение.

Предложение 7. *Если F — перемещение с $\boldsymbol{SO(3)_A}$, то $H = G \circ F \circ G^{-1}$ есть перемещение из группы $\boldsymbol{SO(3)_{G(A)}}$.*

Доказательство. Так как $F(A)=A$, то указанная выше формула принимает вид

$$H \circ G(A) = G \circ F(A) = G(A),$$

т.е. перемещение H оставляет неподвижной точку $G(A)$. Следовательно,

$$H \in \boldsymbol{SO(3)_{G(A)}}.$$

Из этого утверждения вытекает, в частности, что никакая из групп $\boldsymbol{SO(3)_A}$ не является инвариантной подгруппой в $\boldsymbol{E_0(3)}$.

Замечание. Предложение 7 можно усилить. А именно, можно показать, что если перемещение $F \in \boldsymbol{SO(3)_A}$ разложено в композицию $F = R^{\beta}_{l_2} \circ R^{\alpha}_{l_1}$, то $H \in \boldsymbol{SO(3)_{G(A)}}$ представляется в виде композиции $H = R^{\beta}_{m_2} \circ R^{\alpha}_{m_1}$, где прямые m_1 и m_2 проходят через точку $G(A)$, причем угол между этими прямыми равен углу между прямыми l_1 и l_2. Доказательство этого утверждения мы оставляем читателю.

И, наконец, имеет место предложение, аналогичное предложению 4.

Предложение 8. (1) *Любое перемещение из $\boldsymbol{E_0(3)}$ однозначным образом представляется в виде композиции*

$$F \circ T_a,$$

где $F \in \boldsymbol{SO(3)_A}$ — перемещение, имеющее данную неподвижную точку A, а T_a — параллельный перенос.

(2) *Любое перемещение из* $\boldsymbol{E_0(3)}$ *однозначным образом представляется в виде композиции*

$$T_b \sqcup G,$$

где $G \in \boldsymbol{SO(3)_A}$ *— перемещение, , имеющее данную неподвижную точку A, а* T_b *— параллельный перенос.*

Доказательство этого предложения почти дословно совпадает с доказательством предложения 4 и поэтому мы его опускаем.

2.9.3. Конечные подгруппы группы перемещений пространства.

В п. 2.5 были рассмотрены группы самосовмещений правильных пирамид, группы диэдров (двойных пирамид) и группы самосовмещений правильных многогранников. Все эти группы имели конечный порядок. Решим теперь обратную задачу: найти все группы, которые состоят из конечного числа перемещений пространства, Оказывается, что *это именно только что перечислении группы и никакие другие.* Тем самым мы получаем полный список конечных подгрупп группы перемещений пространства.

Пусть *Г* - такая конечная группа. Установим прежде всего следующий результат.

Предложение 9. *Группа Г состоит только из поворотов пространства.*

Доказательство. Пусть *X* — некоторое перемещение, которое содержится в группе *Г;* тогда *Г* будет содержать также и все последовательные степени X^2, X^3, ... перемещения *X*. Поэтому прежде всего необходимо, чтобы среди этих степеней было конечное число различных элементов. Следовательно, перемещение *X* не может быть параллельным переносом.

Действительно, предполагая противное, обозначим через *a* длину вектора параллельного переноса *X*. Степени *X* также будут параллельными переносами, длины векторов которых равны 2*a,* 3*a* и т.д. Все эти параллельные переносы различны между собой и их имеется бесконечное число.

Далее, перемещение *X* не может быть винтовым перемещением. В самом деле, если обозначить через *a* длину вектора параллельного переноса, который входит в винтовое перемещение *X,* то перемещение X^2, X^3 и т.д. будут содержать параллельные переносы, длины векторов которых равны 2*a,* 3*a,* … Следовательно, все такие винтовые

перемещения будут различны. Остаются только повороты. Предложение доказано.

Предложение 10. *Все повороты группы Г, имеющие общую ось, являются степенями одного из них, именно того, которому соответствует наименьший угол поворота.*

Доказательство. Пусть $A \subset \Gamma$ — подмножество поворотов из группы Γ, имеющих общую ось, $R \in A$ — поворот, имеющий наименьший угол α. Покажем, что $\alpha = 2\pi/n$, где n — положительное целое число. Действительно, в противном случае мы имели бы $k\alpha < 2\pi < (k+1)\alpha$ (k — целое число). Поэтому углы $\alpha_1 = 2\pi - k\alpha$ и $\alpha_2 = (k+1)\alpha - 2\pi$ были бы отличны от нуля и не превышали угла α. Кроме того, углы α_1 и α_2 были бы углами поворотов около той же оси, что противоречит предположению.

Итак, мы показали, что поворот R, который имеет наименьший угол среди всех поворотов с общей осью, удовлетворяет условию

$$R^n = E.$$

Докажем теперь, что всякий поворот из множества A является степенью R. Действительно, если это не так, то аналогично только что доказанному соответствующий повороту угол β будет удовлетворять неравенствам $m\alpha < \beta < (m+1)\alpha$. Значит, поворот, которому соответствует угол $\beta - m\alpha$, и который, очевидно, принадлежит множеству A, будет иметь угол, строго меньший α. Предложение доказано.

Число n, фигурирующее в этом предложении (т.е. такое наименьшее положительное число, что $R^n = E$), называется ***порядком поворота.***

Предложение 11. *Оси всех поворотов, которые принадлежат группе Г, проходят через одну точку.*

Доказательство. Пусть R_1 и R_2 — два поворота из группы Γ. Покажем прежде всего, что их оси лежат в одной плоскости. Предположим противное, т.е., что оси l_1 и l_2 поворотов R_1 и R_2 являются скрещивающимися прямыми. Согласно теореме 3 поворот R_1 есть композиция двух опрокидываний относительно пересекающихся осей m_1 и m'_1, пересекающих l_1 под прямыми углами, причем m'_1 можно взять произвольно. Точно так же поворот R_2 есть композиция двух опрокидываний относительно пересекающихся осей m_1 и m'_1, пересекающих l_2 под прямыми углами, причем m'_2 можно выбрать произвольно. Соединим прямые m'_1 и m'_2 с общим перпендикуляром к осям l_1 и l_2. Опрокидывания относительно них взаимно уничтожаются, так что композиция $R_2 \circ R_1$ представляет собой композицию опрокидываний относительно прямых m_1 и m_2. Прямые m_1 и m_2 не могут пересекаться. В противном случае определяемая ими плоскость

содержала бы общий перпендикуляр к l_1 и l_2. Поэтому прямые l_1 и l_2 оказались бы перпендикулярными к этой плоскости (как прямые, перпендикулярные каждая к двум прямым, лежащим в плоскости) и, значит, параллельными у противоречие с предположением. Следовательно, прямые m_1 и m_2 не имеют общих точек, т.е. $R_2 \circ R_1$ не является поворотом.

Итак, мы доказали, что оси любых двух поворотов из группы Γ лежат в одной плоскости.

Дальше, эти оси не могут быть параллельными. Действительно, если бы повороты R_1 и R_2 вокруг параллельных осей имели равные, но имеющие противоположные направления углы поворота, то $R_2 \circ R_1$ было бы нетождественным параллельным переносом. Если же повороты R_1 и R_2 вокруг параллельных осей имели бы неравные углы или же равные и одинаково направленные углы, то композиции $R_1 \circ R_2$ и $R_2 \circ R_1$ были бы поворотами на один и тот же угол вокруг различных осей, так что композиция $R_1 \circ R_2 \circ (R_2 \circ R_1)^{-1} = R_1 \circ R_2 \circ R_1^{-1} \circ R_2^{-1}$ (очевидно, принадлежащая группе Γ) была бы нетождественным параллельным переносом.

Итак, *оси двух поворотов обязательно пересекаются в некоторой точке О.*

Покажем теперь, что в группе Γ содержится поворот R, ось которого проходит через точку O и не лежит в плоскости, которая проходит через оси поворотов R_1 и R_2.

В самом деле, если R_1 и R_2 опрокидывания, то таким поворотом будет композиция $R_2 \circ R_1$. В противном случае, если один из поворотов, скажем, R_1, не является опрокидыванием, то таким поворотом будет $R_1 \circ R_2 \circ R_1^{-1}$. Следовательно, ось любого поворота из группы Γ должна проходить через точку O, так как она должна пересекать оси поворотов R_1, R_2 и R. Предложение 11 доказано.

Пусть O - точка пересечения всех осей поворотов, которые принадлежат группе Γ. Примем эту точку за центр сферы S единичного радиуса. Для того чтобы изучить повороты, которые принадлежат Γ, достаточно изучить их действия на сфере S.

Любая ось поворота пересекает сферу S в двух точках. Очевидно, что эти точки будут единственными неподвижными относительно данного поворота точками на сфере. Назовем их ***полюсами данного поворота***. Полюс поворота может принадлежать сразу нескольким поворотам группы Γ. Пусть, например, некоторому полюсу соответствуют повороты $R_1, \ldots, R_k$ с углами $\alpha_1, \ldots, \alpha_k$, причем угол α_1 наименьший из них. Тогда α_1 необходимо имеет вид $\alpha_1 = 2\pi/n$ (n — целое положительное число). Действительно, если бы было не так, т.е. $\alpha_1 = (m/n)(2\pi)$, где m и n — взаимно простые, т.е. наибольший общий

делитель m и n равен единице, то в группе Γ содержался бы поворот на угол, строго меньший α_1.

Для того чтобы доказать это, будем считать, что $m<n$ (случай $m>n$ рассматривается аналогично). Представим число n в виде

$$n = lm+r,$$

где $0<r<m$, и рассмотрим поворот R_1^{-1}, очевидно принадлежащий группе Γ. Наименьший положительный угол этого поворота равен

$$2\pi - \frac{lm}{n}2\pi = 2\pi\frac{n-lm}{n} = \frac{r}{n}\cdot 2\pi < \alpha_1,$$

что и требовалось доказать.

Все другие повороты R_2, ..., R_k будут степенями поворота R_1 Действительно, если бы угол γ, соответствующий одному з этих поворотов, удовлетворял неравенствам

$$\frac{m}{n}\cdot 2\pi < \beta < \frac{m+1}{n}2\pi,$$

то, взяв композицию этого поворота и поворота R_1^{-m} мы получили бы поворот той же оси на угол, строго меньший $2\pi/n=\alpha_1$, что противоречит сделанному предположению.

Назовем число n ***порядком*** данного полюса поворота. Легко видеть, что полюс n-го порядка принадлежит n — 1 поворотам, не считая тождественного.

Нашей ближайшей целью являются получение формулы, связывающкй порядок N группы Γ и порядки n_1 ..., n_k различных полюсов поворота. Для этого введем следующее определение.

Точки P_1 и P_2 на сфере S называются *эквивалентными* относительно группы Γ, если существует такой поворот $R \in F$, что $R(P_1)=P_2$.

Таким образом, любая точка P на сфере S имеет N эквивалентных ей точек, которые получаться, если применять к P все повороты из группы Γ. Если точка P не является полюсом, то все эквивалентные ей точки разлисны между собой. В самом деле, если несколько эквивалентных точек совпадают с точою P', то эта точка будет полюсом некоторого поворота R', но тогда точка P будет полюсом поворота R.

Если же точка P есть полюс n-го порядка для поворота R, то она совпадает с n — 1 эквивалентными ей точками. Пусть теперь P' — некоторая точка, эквивалентная точке P и получающаяся из нее поворотом R': $P' = R'(P)$. Тогда n из точек, эквивалентных точке P, а именно точки $R'(P)$, $RR'(P)$, $R^2R'(P)$.....$R^{n-1}R'(P)$, будут совпадать с точкой P'.

Других точек, эквивалентных точке P и совпадающих с P', не существует. Действительно, если бы такие точки существовали, то P' была бы полюсом поворота порядка m, причем $m>n$. Но тогда и точка P, которая получается из P' поворотом $(R')^{-1}$, была бы полюсом поворота порядка m. Следовательно, все N точек, эквивалентных полюсу n-го порядка P, по n совпадают между собой. Таким образом, в этом случае точка P имеет всего лишь N/n различных эквивалентных ей точек, учитывая и самое точку P.

Пусть теперь $P_1, \ldots, P_k$ — неэквивалентные полюсы поворотов, которые входят в группу Γ, $n_1, \ldots, n_k$ — порядки этих полюсов и N — порядок группы Γ.

Предложение 12. *Числа N, $n_1, \ldots, n_k$ связаны между собой следующим соотношением:*

$$\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\ldots+\left(1-\frac{1}{n_k}\right)=2-\frac{2}{N}. \tag{2.48}$$

Доказательство. Подсчитаем число поворотов, которым принадлежат данные неэквивалентные полюсы $P_1, \ldots, P_k$. Полюс P_1 имеет порядок n_1; только что мы установили, что эта точка имеет N/n_1 различных эквивалентных ей точек. В то же время P_1 есть полюс n_1—1 поворотов, не считая тождественного. Каждая из точек, эквивалентных точке P_1, также будет полюсом n_1 — 1 поворотов. Поэтому всего мы имеем — $(N/n_1)(n_1-1)=N(1-1/n_1)$ поворотов. Аналогичные вычисления можно проделать и для всех остальных полюсов, в результате чего мы получим полное число поворотов

$$N\left[\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\ldots+\left(1-\frac{1}{n_k}\right)\right].$$

В это число не вошел тождественный поворот, зато каждый из N —1 оставшихся поворотов вошел ровно два раза (ведь все полюсы разбиваются на пары диаметрально противоположных). Следовательно,

$$N\left[\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\ldots+\left(1-\frac{1}{n_k}\right)\right]=2(N-1),$$

откуда

$$\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\ldots+\left(1-\frac{1}{n_k}\right)=2-\frac{2}{N},$$

что и требовалось доказать.

Соотношение (2.48) позволяет описать все конечные подгруппы группы перемещений пространства.

Теорема 5. *Конечные циклические группы (группы правильных пирамид), группы диэдров и группы правильных многогранников являются единственными конечными подгруппами группы перемещений пространства.*

Доказательство. Так как числа n_1.....n_k в соотношении (2.48) больше или равны 2, то $1-(1/n_j)>1/2$ для всех j=1,..., k. Поэтому число k не может превосходить трех, поскольку правая часть $2—(2/N)$ соотношения (2.48) строго меньше 2. В то же время $2—(2/N)\geq 1$
а каждая из скобок в левой части (2.48) меньше 1. Следовательно, число k не может быть равным 1. Итак, для числа k имеются две возможности: k=2 и k=3.

I. k=2. В этом случае соотношения (2.48) превращается в

$$\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)=2-\frac{2}{N}$$

или в

$$\frac{1}{n_1}+\frac{1}{n_2}=\frac{2}{N}. \qquad (2.49)$$

Уравнение (2.49) имеет единственное решение $n_1=n_2=N$. Действительно, в противном случае одно из чисел n_1 или n_2 превосходило бы N, что невозможно, поскольку N должно быть кратным чисел n_1 и n_2.

Так как $N/n_1= N/n_2= 1$, то имеется всего лишь два различных полюса поворота и, значит, единственная ось поворота.

Все повороты вокруг этой оси представляют собой степени данного из них, т.е. мы имеем циклическую группу конечного порядки. Такую группу самосовмещения правильного многогранного угла, или, что то же самое, самосовмещения правильной пирамиды.

II. k =3. В этом случае по крайней мере одно из чисел n_1, n_2 или n_3 равно 2, так как если бы одновременно $n_1\geq 3$, $n_2\geq 3$ и $n_3\geq 3$, то

$$1-1/n_1\geq 2/3,\ 1-1/n_2\geq 2/3,\ 1-1/n_3\geq 2/3,$$

откуда

$$\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\left(1-\frac{1}{n_3}\right)\geqslant 2,$$

что невозможно. Положим n_3=2. Тогда соотношение (2.48) примет вид

$$\left(1-\frac{1}{n_1}\right)+\left(1-\frac{1}{n_2}\right)+\left(1-\frac{1}{2}\right)=2-\frac{2}{N}$$

или

$$\frac{1}{n_1}+\frac{1}{n_2}=\frac{1}{2}+\frac{2}{N}\,. \tag{2.50}$$

Решим уравнение (2.50) в целых положительных числах. Прежде всего заметим, что если одно из искомых чисел, например, n_1, равно 2, то другое число n_2 находится из формулы

$$n_2=\frac{N}{2}\,.$$

В этом случае имеются два полюса и, следовательно, единственная ось n_2-го порядка. Все остальные повороты, оси которых отличны от этой оси, будут опрокидываниями. Очевидно, что оси этих опрокидываний будут перпендикулярны к оси n_2-го порядка и составляют между собой равные углы.

Такую группу образуют самосомещения правильного многоугольника в трехмерном пространстве или двойной пирамиде (диэдра).

Итак, мы рассмотрели случай, когда одно из чисел n_1 или n_2 равно 2. Исключая его, мы имеем, одновременно $n_1\geq 3$ и $n_2\geq 3$. Однако оба эти числа не могут быть больше 3, так как для $n_1\geq 4$ и $n_2\geq 4$ мы имеем $1/n_1+1/n_2\leq 1/2<1/2+2/N$. Следовательно, в крайнему разе одно из чисел n_1 и n_2 равно 3. Будем считать, что это число n_1 (в противном случае можно поменять местами в уравнении (2.50) числа n_1 и n_2); тогда

$$\frac{1}{3}+\frac{1}{n_2}=\frac{1}{2}+\frac{2}{N}>\frac{1}{2}\,,$$

откуда $n_2<6$. Итак, n_2 может принимать только три значения, 3, 4, 5. Поэтому (с учетом симметрии уравнения (2.50) относительно переменных n_1 и n_2) мы получаем следующие пять решений:

1) $n_1=n_2=3,\ N=12;$
2) $n_1=3,\ n_2=4,\ N=24;$
3) $n_1=4,\ n_2=3,\ N=24;$
4) $n_1=3,\ n_2=5,\ N=60;$
5) $n_1=5,\ n_2=3,\ N=60.$

Для того чтобы завершить доказательство теоремы нужно показать еще, что каждому полученному таким образом решению соответствует некоторый правильный многогранник, и, следовательно, группа всех его самосовмещений. Эту часть доказательства мы опускаем.

В заключение отметим, что перечисленными подгруппами отнюдь не исчерпывается множество всех подгрупп, лежащих в группах ***E* (2)** и ***E*(3).** Среди всех подгрупп ***E*(2)** и ***E*(3)** особое значение для различных областей естествознания имеют так называемые кристаллографические группы. Они определяются следующим образом.

Назовем *пространственной решеткой Бравэ* (или *пространственным кристаллом)* множество *L,* образованное всеми точками пространства с радиусами-векторами **R** вида

$$\mathbf{R} = n_1\mathbf{e}_1 + n_2\mathbf{e}_2 + n_3\mathbf{e}_3,$$

где $\mathbf{e_1}$, $\mathbf{e_2}$ и $\mathbf{e_3}$ — три некомпланарных вектора, а n_1, n_2 и n_3 — всевозможные целые числа. Аналогично определяется *плоская решетка Бравэ (плоский кристалл).*

Множество перемещений пространства (соответственно плоскости), переводящих решетку *L* в себя, называется *пространственной кристаллографической группой* (соответственно *плоской кристаллографической группой)* и обозначается через $G_3(L)$ (соответственно $G_2(L)$). Ясно, что множество $G_3(L)$ (соответственно $G_2(L)$) является подгруппой группы ***E*(3)** (соответственно группы ***E*(2)**). Аналогично тому, как мы описали конечные группы перемещений, можно получить полную классификацию всех кристаллографических групп (правда, затратив на это значительно больше времени и усилий). ***Оказывается, что существует ровно 17 неизоморфных друг другу плоских кристаллографических групп и 230 неизоморфных пространственных кристаллографических групп***. Каждой из этих групп отвечают соответствующая плоская или пространственная решетка. Интересно отметить, что эти плоские решетки были обнаружены еще в древности египетскими архитекторами и художниками, в то время как классификация трехмерных решеток была получена лишь в конце позапрошлого столетия.

Микромодуль 6.
Примеры решения типовых задач

1. Пусть *G* есть группа S_3 всех подстановок из трех элементов, а *U* - подгруппа порядка 2 (следовательно, индекса 3), состоящая из подстановок

$$P_0 = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix} \text{ и } P_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$$

Распадение группы G на лево- и правосторонние классы видно из следующей таблицы:

Левосторонние классы	Правосторонние классы
$U=\{P_0,\ P_2\}$	$U=\{P_0,\ P_2\}$
$\{P_1,\ P_3\}$	$\{P_1,\ P_4\}$
$\{P_4,\ P_5\}$	$\{P_3,\ P_5\}$

2. Знакопеременная группа A_n подстановок из n элементов представляет собой инвариантную подгруппу индекса 2 симметрической группы S_n. Два класса, определяемые этой подгруппой, суть: сама группа A_n и класс всех нечетных подстановок.

3. В группе поворотов n-угольного диэдра самосовмещения первого рода образуют инвариантную подгруппу индекса 2. Один из двух классов по этой подгруппе есть она сама, другой класс состоит из всех самосовмещений второго рода.

4. Группа U всех скольжений прямой по самой себе есть инвариантная подгруппа индекса 2 в группе G всех самосовмещений прямой. Два класса, определяемые этой подгруппой, суть: сама группа U и класс всех самосовмещений второго рода.

5. Пусть G есть группа всех комплексных чисел (с операцией обычного сложения как групповой операцией). Пусть U — подгруппа всех действительных чисел. Классы, на которые распадается коммутативная группа G относительно своей подгруппы U, суть множества K_β, каждое из которых состоит из всех комплексных чисел вида

$$x+i\beta,$$

где x и β — действительные числа, β дано, а x пробегают все действительные значения. Если, как это обычно делается, изображать комплексные числа в виде точек плоскости (считая за изображение комплексного числа $x+iy$ точку плоскости с координатами (x, y)), то каждый класс изобразится в виде прямой, параллельной действительной оси (т.е. оси абсцисс).

Микромодуль 6.
Идивидуальные тестовые задачи

1. Требуется доказать, что группа поворотов тетраэдра распадается на следующие классы сопряженных элементов:
1) класс, который состоит из одного нейтрального элемента;
2) класс, который состоит из поворотов на угол (2/3)π вокруг каждой из четырех осей, которые соединяют вершину тетраэдра с центром противоположной грани;
3) класс, который состоит из четырех поворотов на угол (4/3) π вокруг тех же осей (всюду по (или против) часовой стрелки, если смотреть из неподвижной вершины);
4) класс, который состоит из поворотов на угол π вокруг каждой из трех осей, которые соединяют середины двух противоположных ребер тетраэдра.
Исследовать классы сопряженных элементов в других группах поворотов.
2. Доказать следующую общую теорему: пересечение всех групп, которые входят в некоторый класс сопряженных между собой подгрупп, есть инвариантная подгруппа.
3. Доказать, что тождество (2.47) не выполняется ни при каком выборе нечетного числа симметрий.
4. Доказать, что множество всех поворотов в пространстве подгруппы не образует. (*Указание:* проверить, что композиция двух поворотов вокруг осей, которые не лежат в одной плоскости, представляет собой винтовое перемещение в собственном смысле слова; другими словами, в такую композицию входит нетождественный параллельный перенос.)
5. Доказать утверждение, что если перемещение $F \in \boldsymbol{SO(3)_A}$ разложено в композицию $F = R^{\beta}_{l_2} \sqcup R^{\alpha}_{l_1}$, то $H \in \boldsymbol{SO(3)_{G(A)}}$ представляется в виде композиции $H = R^{\beta}_{m_2} \circ R^{\alpha}_{m_1}$, где прямые m_1 и m_2 проходят через точку G *(A),* причем угол между этими прямыми равен углу между прямыми l_1 и l_2.

Модуль 3
Алгебраическая теория полугрупп

Микромодуль 7
Полугруппы. Определения и примеры

3.1. Определения

Среди законов композиции, наиболее общими есть те, которые образуют полугруппы (моноиды), т.е. имеют единичный элемент и ассоциативны.

Известно, что в действительности важность теории моноидов или полугрупп проявляется там, где имеется связь с теорией информации, кодами, автоматами, системами команд и т.д.

В этом микромодуле мы вводим основные понятия теории полугрупп (моноидов), которые необходимы для дальнейшего изложения. Для понимания излагаемого материала не потребуется знаний никаких результатов теории полугрупп, кроме тех, которые будут приведены. Однако, читатель должен обладать необходимыми знаниями из элементарной теории групп.

Большая часть фактов, которые содержатся в приведенном материале — стандартный аппарат теории полугрупп, хотя само изложение, кое в чем отличается от общепринятого.

В основному нам придется иметь дело с конечными полугруппами и это позволит излагать результаты в виде, удобном читателю, который интересуется теорией полугрупп с точки зрения ее приложения, прежде всего, к теории автоматов.

1. **Определение**. *Полугруппой* называется *упорядоченная пара* $(S, \bullet)$. где символ S означает непустое множество, а точка — ассоциативную бинарную операцию, т.е. функцию $(s_1, s_2) \to s_1 \bullet s_2$ из декартова произведения $S \times S$ в множество S, такую, что для любых элементов $s_1, s_2, s_3 \in S$ выполняется соотношение $(s_1 \bullet s_2) \bullet s_3 = s_1 \bullet (s_2 \bullet s_3)$. В дальнейшем вместо $(S, \bullet)$ будем сокращенно писать S, а вместо $s_1 \bullet s_2$ — $s_1 s_2$.

Мощность множества S называется *порядком* полугруппы S, он обозначается как $|S|$. *Предполагается, что все рассматриваемые в дальнейшем полугруппы имеют конечный порядок,* если только не оговорено противное.

Элемент $e \in S$ называется *идемпотентом* тогда и только тогда, когда $e^2=e$; *левой (правой) единицей* его называют тогда и только тогда, когда для любого элемента $s \in S$ $es=s$ *(*$se=S$*),* а *левым (правым) нулем* тогда и только тогда, когда для любого элемента $s \in S$ $es=e$ *(*$se=e$*).* Если элемент e — левая, а элемент f — права единицы, то $e=ef=f$. Любая левая (права) единица или нуль представляют собой идемпотенты.

Элемент $e \in$ S называется *единицей* тогда и только тогда, когда для любого элемента $s \in S$ выполняются соотношение $se=s=es$; его называют *нулем* тогда и только тогда, когда для любого элемента $s \in S$ выполняются соотношение $se=e=es$. Полугруппа S может обладать только одной единицей и только одним нулем, в самом деле, если e_1 и e_2 — две единицы (или два нуля), то $e_1=e_1e_2=e_2$. Нули и единицы будут обозначаться символами 0 и 1 соответственно.

Моноид — это полугруппа с единицей.

Группой называется моноид S, обладающий следующим свойством. Для каждого элемента $s \in S$ существует элемент $s^{-1} \in S$, называемый обратным для элемента s, такой, что $ss^{-1}=e=ss^{-1}$, где e— единица моноида S. Любой элемент моноида S может иметь только один обратный, так как если s_1 и s_2 — обратные элементы для s, то $s_1=s_1ss_2=s_2$.

Если для любых элементов $s_1, s_2 \in S$ выполнено соотношение $s_1s_2 = s_2s_1$, то полугруппа будет *коммутативной,* или *абелевой.*

Пусть $s_1 ..., s_n$ — элементы полугруппы S, по определению $s_1s_2 ... s_n=s_1(s_2... (s_{n-1}s_n)...)$, тогда любое другое произведение, полученное в результате расстаноки скобок в конечной последовательности $s_1...s_n$, равно $s_1 ... s_n$. Кроме того, если S — коммутативная полугруппа, то для любой перестановки π индексов $\{1, ..., n\}$ выполнено соотношение $s_1 ..,s_n=s_{\pi(1)} ... s_{\pi(n)}$. Эти результаты, иногда называемые обобщенным ассоциативным и обобщенным коммутативным законами соответственно, могут быть доказаны индукцией по n.

Для любого элемента s полугруппы S определим степень элемента s следующим образом. Положим $s^1=s$; тогда для целого числа $n > 1$ по определению $s^n = s^1s^{n-1}$. Если S — группа с единицей e, положим $s^0 = e$ и для целого числа $n > 0$, пусть тогда $s^{-n} = (s^{-1})^n$, где s^{-1} — обратный для элемента s.

2. Определение. Пусть S-полугруппа. Тогда подмножество $T \subseteq S$ называется *подполуруппой* для S, если $T \neq \varnothing$ и если для любых элементов $t_1, t_2 \in T$ элемент $t_1t_2 \in T$. T будет *подгруппой S,* если T —

подполугруппа для S, а T — группа. T называется *максимальной собственной подполуруппой* для S, если $T \neq S$ и если из условия $T \subseteq V \subseteq S$, где V — подполугруппа для S, вытекает, что $T=V$ или $V = S$. T будет *максимальной подгруппой* для S, если T — подгруппа для S и если из условия $T \subseteq V \subseteq S$, где V— подгруппа для S, вытекает, что $T=V$.

Если X — непустое подмножество полугруппы S, то *подполуруппу, порожденную множеством X*, образует наименьшая подполугруппа в S, содержащая X, она обозначается как $\langle X \rangle$. Очевидно, что $\langle X \rangle$ есть пересечение всех подполугрупп полугруппы S, содержащих множество X. Легко видеть, что пересечение подполугрупп некоторой полугруппы есть либо пустое множество, либо подполугруппа этой полугруппы. Множество всех конечных произведений $x_1x_2 \ldots x_n$ элементов из X совпадает с подполугруппой $\langle X \rangle$.

Говорят, что множество X *порождает* полугруппу S, если $\langle X \rangle = S$. Очевидно, справедливо соотношение $\langle S \rangle = S$. Пусть $a \in S$. Тогда полугруппа $\langle a \rangle$ называется *циклической подполугруппой полугруппы S,* порожденной элементом a, здесь $\langle a \rangle = \langle \{a\} \rangle$. S будет *циклической полугруппой,* если $S = \langle a \rangle$ для некоторого элемента $a \in S$.

Говорят, что S — *периодическая полугруппа,* если для любого элемента $a \in S$ подполугруппа $\langle a \rangle$ конечная.

3. Определение. Пусть S_1 и S_2 — полугруппы. Тогда отображение $\varphi: S_1 \to S_2$ представляет собой *гомоморфизм,* если для любых элементов $s_1, s_2 \in S_1$ выполнено соотношение $\varphi(s_1 s_2) = \varphi(s_1)\varphi(s_2)$. Если $X \subseteq S_1$, то $\varphi(X)$ обозначает множество $\{y \in S_2: y = \varphi(s)$ для некоторого элемента $s \in X\}$. Если $\varphi(S_1)=S_2$, то гомоморфизм φ будет *эпиморфизмом,* который записывается в виде $\varphi: S_1 \to\to S_2$. Полугруппа S_2 называется *гомоморфным образом полугруппы* S_1. Если для любых элементов $s, t \in S_1$, таких, что $s \neq t$, справедливо неравенство $\varphi(s) \neq \varphi(t)$ то φ — взаимнооднозначный (обозначается 1:1) гомоморфизм, или *мономорфизм. Изоморфизмом* называется взаимнооднозначный эпиморфизм. Полугруппа S_1 *изоморфна* полугруппе S_2, $S_1 \cong S_2$, если существует изоморфизм $\varphi: S_1 \to\to S_2$. Если $\varphi : S_1 \to\to S_2$ — изоморфизм, можно определить обратное $\varphi^{-1} : S_2 \to\to S_1$ для отображения φ, полагая, что $\varphi^{-1}(s)$ - единственный элемент из S_1, для которого $\varphi [\varphi^{-1}(s)] = s$. Очевидно, что отображение $\varphi^{-1}: S_2 \to\to S_1$ представляет собой изоморфизм. Из этого легко вывести: ($\cong$) есть отношение эквивалентности на классе полугрупп.

3.2. Примеры (определения, обозначения, дополнения).

Далее приведены примеры полугрупп. Они помогут читателю овладеть введенными понятиями и облегчат изучение последующего материала.

1. Пусть A — непустое множество. Тогда A^r (соответственно A^l) обозначает полугруппу $(A, \bullet)$, для которой $a_1 \bullet a_2 = a_2$ (соответственно $a_1 \bullet a_2 = a_1$), где a_1, a_2 - произвольные элементы множества A. Когда $|A|>1$, A^r и A^l являются полугруппами и не являются группами. Следовательно, A^r (соответственно A^l) есть множество A, которое мы превратили в полугруппу, потребовав, чтобы каждый элемент из A действовал как правый (соответственно, левый) нуль.

2. Пусть X - некоторое множество, а 2^x обозначает множество всех подмножеств множества X. Тогда $(2^x, \square)$ есть абелева полугруппа. Полугруппа $(2^x, \cup)$ изоморфна полугруппе $(2^x, \cap)$, изоморфизм задается отображением

$$A \to X - A = \{x \in X : x \notin A\}.$$

3. Пусть S— полугруппа, A и B - *подмножества* в S. Положим $A \bullet B = \{ab : a \in A, b \in B\}$ (сокращенно это записывается как AB). Тогда отображение $s \to \{s\}$ есть мономорфизм полугруппы S в $(2^s, \bullet)$. Условимся, что $A \bullet \varnothing = \varnothing \bullet A = \varnothing$, где $\varnothing$ — пустое множество.

4. Пусть X — множество. *Отношением* R на X называется любое подмножество $R \subseteq X \times X$. Будем писать $x_1 R x_2$ или $x_1 \equiv x_2 \pmod R$ тогда и только тогда, когда $(x_1, x_2) \in R$. Тогда $(2^{X \times X}, \bullet)$ есть полугруппа всех отношений на множестве X, закон композиции для нее определяется следующим образом:

$$R_1 \bullet R_2 = \{(x, y): \text{ для некоторого } z \in X, (x, z) \in R_1, (z, y) \in R_2\}.$$

Если R — отношение, то по определению $R^{-1} = \{(y, x) : (x, y) \in R\}$. Тогда $(R \bullet S)^{-1} = S^{-1} R^{-1}$ для любых отношений S и R на множестве X. *Тождественное* отношение на множестве X есть $\Delta(X) = \{(x, x) : x \in X\}$. Отношение R называется *отношением эквивалентности* тогда и только тогда, когда

1) $\Delta(X) \subseteq R$ *(R рефлексивно);*

2) $R = R^{-1}$ *(R симметрично);*

3) $R \bullet R \subseteq R$ *(R транзитивно).*

Включение отношений (как множеств) определяет частичную упорядоченность на множестве всех отношений на X. Если ограничиться рассмотрением только отношений эквивалентности, то

эта частичная упорядоченность сведется к структуре. [Структура есть частично упорядоченное множество, для любых двух элементов которого существует точная нижняя (LUB) и точная верхняя грань (GLB)]. Если R_1 и R_2 — отношения эквивалентности, то $GLB(R_1, R_2)=R_1 \sqcap R_2$ и $LUB(R_1, R_2)=\bigcup\{(R_1 \cup R_2)^n : 1\le n\le\infty\}$, т.е. $LUB(R_1, R_2)$ есть *транзитивное замыкание* множества $R_1 \cup R_2$. Следовательно, x эквивалентен y в $LUB(R_1, R_2)$ тогда и только тогда, когда существует последовательность элементов $x=x_0, x_1, x_2, ..., x_n=y$, таких, что $x_1 R_1 x_{i+1}$ или $x_1 R_2 x_{i+1}$ при $i = 0, 1, ..., n$— 1. Если R_1 и R_2 — отношение эквивалентности, для которых $R_1 \bullet R_2 = R_2 \bullet R_1$, то легко видеть, что $R_1 \bullet R_2$ — отношение эквивалентности и, следовательно, $R_1 \bullet R_2 = LUB(R_1, R_2)$.

5. Пусть S — полугруппа. Отношение эквивалентности $\equiv$ на S называется *конгруэнтностью,* если для любых элементов $s_1, s_2 \in S$, таких, что $s_1 \equiv s_2$, и любого элемента $s \in S$ справедливые соотношения $ss_1 \equiv ss_2$ и $s_1 s \equiv s_2 s$. Отношение $\equiv$ называется *левой* или *правой конгруэнтностью,* если справедливо первое или второе из предыдущих соотношений. Если $\equiv$ есть конгруэнтность на S, обозначим через $[s]$ класс элементов, эквивалентных $s \in S$. Пусть $S/\equiv$ представляет собой множество таких классов эквивалентности, а отображение $\eta_{\equiv}: S \to\to S/\equiv$ определяется как $\eta_{\equiv}(s)=[s]$. Тогда умножение $[s]\bullet[t]=[st]$ корректно, множество $S/\equiv$ с таким умножением — полугруппа, а отображение $\eta_{\equiv}$ — эпиморфизм.

Наоборот, если $\varphi : S \to\to S_1$ есть эпиморфизм, то с его помощью можно определить конгруэнтность на S, а именно $s_1 (\mathrm{mod}\ \varphi) s_2$ тогда и только тогда, когда $\varphi(s_1) = \varphi(s_2)$. Следовательно, определено отображение $\varphi^*: S/(\mathrm{mod}\ \varphi) \to S_1$, $\varphi^*([s])=\varphi(s)$, которое будет изоморфизмом, и $\varphi = \varphi^* \eta_{(\mathrm{mod}\ \varphi)}$.

6. Пусть A — непустое множество. Тогда *свободной некоммутативной полугруппой без единицы* $\sum A$, п*орожденной A,* называется множество всех конечных непустых упорядоченных последовательностей элементов из A с полугрупповой операцией, которая задается сшиванием последовательностей, т.е.,

$$(a_1, ..., a_n) \bullet (b_1..., b_m) = (a_1, ..., a_n, b_1, ..., b_m).$$

$\sum A$ есть бесконечная полугруппа.

$\sum A$ называется свободной полугруппой на множестве A, поскольку любое отображение φ множества A в полугруппу S может быть единственным способом продолжено до гомоморфизма φ^{Γ} полугруппы $\sum A$ в S; φ^{Γ} определяется по формуле $\varphi^{\Gamma}(a_1 ..., a_n) = \varphi(a_1) ... \varphi(a_n)$. В частности, если A — множество, которое порождает полугруппу S, а φ

— тождественное отображение, то $\varphi^{\Gamma}: \sum A \rightarrow S$ есть эпиморфизм. Следовательно, каждая полугруппа есть гомоморфным образом свободной полугруппы.

7. Z обозначает множество целых чисел $\{0, \pm 1, \pm 2, \ldots\}$. $(Z, +)$ есть группа целых чисел с обычной операцией сложения. Z^+ обозначает множество неотрицательных целых чисел. $(Z^+, +)$ — подполугруппа группы $(Z, +)$. Обозначим через (n) конгруэнтность на группе $(Z, +)$, для которой $z_1(n)z_2$ [обычно это записывается $z_1 \equiv z_1 \pmod n$] тогда и только тогда, когда $z_1 - z_2 = kn$ для некоторого $k \in Z$. $Z_n = Z/(n)$ называется циклической группой порядка n или аддитивной группой целых чисел по модулю n.

8. Пусть S — произвольная полугруппа.

1) Определим полугруппу S^1. Если S — моноид, то по определению $S^1=S$; в противном случае $S^1=S \cup \{1\}$, где символ $1 \notin S$. Распространим операцию умножения, заданную в S, на множество $S \cup \{1\}$, полагая $11 = 1$ и $1s = s1 = s$ для любого $s \in S$.

2) Определим полугруппу S^0. Если S содержит нуль и $|S|>1$, то $S^0=S$. В противном случае $S^0=S \cup \{0\}$, где символ $0 \notin S$. Распространим операцию умножения, заданную в S на множество $S \cup \{0\}$, полагая $00 = 0s = s0 = 0$ для любого элемента $s \in S$.

3) Определим полугруппу $S^I = S \cup \{I\}$, где $I \notin S$. Распространим операцию умножения, заданную в S, на множество $S \cup \{I\}$, полагая $II = I$, $Is = sI = s$ для любого элемента $s \in S$.

Будем отождествлять единицу полугруппы $(\sum A)^1$ с пустым множеством. В некоторых разделах настоящей работы свободный моноид $(\sum A)^1$ обозначается как A^*.

9. Пусть A и B— непустые множества. Тогда $F(A, B)$ обозначает множество всевозможных отображений из A в B. Запишем множество $F(A, A)$ в виде $F(A)$. Обозначим через $F_L(A)$ полугруппу $[F(A), \bullet]$, для которой умножение определяется соотношением $(fg)(a)=f[g(a)]$, где элемент $a \in A$. Обозначим через $F_R(A)$ полугруппу $[F(A), \circ]$, для которой умножение определяется соотношением $(f \circ g)(a)=g[f(a)]$, $a \in A$. Иногда, имея дело с полугруппой $F_R(A)$, вместо $f(a)$ будем писать $a(f)$. Следовательно, $(a)(f \circ g)=[(a)f]\,g$. Пусть символы $SYM_L(A) \subseteq F_L(A)$ и $SYR_R(A) \subseteq F_R(A)$ обозначают подгруппы, которые состоят из взаимно однозначных отображений множества A.

Пусть S — полугруппа, определим отображение $L : S \to F_L(S^1)$, для которого $L(s)(r)=sr$, где $s \in S$ и $r \in S^1$. Отображение L — взаимно однозначный гомоморфизм, так как

$$L(s_1s_2)(r) = s_1s_2r = L(s_1)[L(s_2)(r)] = L(s_1)L(s_2)(r)$$

и $L(s)(1)=s$ для любых элементов $s, s_1, s_2 \in S$ и любого элемента $r \in S^1$. Мономорфизм L называется *левым регулярным представлением полугруппы S.* Следовательно, каждая полугруппа изоморфна подполугруппе из $F_L(A)$ для некоторого множества A.

Аналогично отображение $R:S \to F_R(S^1)$, определяемое соотношением $(r)\ R(s) = rs$, где $r \in S^1$, $s \in S$, является мономорфизмом, который называется *правым регулярным представлением полугруппы S.*

Заметим, что полугруппа $F_R(X)$ изоморфна подполугруппе из $(2^{X\times X}, \bullet)$. Элементы этой подполугруппы — всевозможные отношения R, которые обладают следующим свойством: для каждого элемента $x \in X$ существует один и только один элемент $y \in X$, такой, что $(x, y) \in R$. Полугруппа $F_L(X)$ изоморфна из $(2^{X\times X}, \bullet)$, что состоящей из всевозможных отношений, для которых для элемента y существует единственный элемент x, такой, что $(x, y) \in R$.

10. Пусть X - конечное множество. *Симметричной инверсной полугруппой* на множестве X называется множество всех взаимно однозначных эпиморфных отображений, областью определения и областью значения которых являются подмножества из X*. Пусть $f:A \to B$ и $g:C \to D$ — отображения с такими свойствами. Тогда отображение gf имеет область определения $f^{-1}(B \cap C)$ и область значения $g(B \cap C)$, отображение gf удовлетворяет соотношению $gf(a)=[gf(a)]$. Построенная полугруппа обозначается $SIS_L(X)$. Аналогично определяется полугруппа $SIS_R(X)$.

11. Пусть S - полугруппа. Тогда по определению $r(S)$ есть полугруппа $(S, \bullet)$, для которой $s_1 \bullet s_2 = s_2s_1$, где $s_1, s_2 \in S$. Очевидно, $r[r(S)] = S$. Равенство $r(S)=S$ выполнено тогда и только тогда, когда полугруппа S — абелева. Если S представляет собой группу, то отображение $x \to x^{-1}$ определяет изоморфизм группы S с группой $r(S)$, поскольку $(xy)^{-1}=y^{-1}x^{-1}$. Однако при $|A| \geq 2$ полугруппа A^l не изоморфа полугруппе $r(A^l) = A^\Gamma$.

Определение, теорема, конструкция и т.д., которые сформулированы для полугруппы S, всегда имеют двойственный аналог для полугруппы $r(S)$, т.е. соответствующее определение, теорему, конструкцию относительно полугруппы $r(S)$. Мы не будем давать точного определения понятия двойственности, однако, когда оно будет появляться, его смысл всегда будет ясен для конкретной

ситуации. Например, понятие левого регулярного представления и правого регулярного представления — двойственные конструкции.

12. Пусть A — непустое множество и для каждого элемента $a \in A$ задано множество X_a. Тогда *декартовым произведением множеств* X_a называется функция $f : A \to \square \{X_a : a \in A\}$, такая, что для любого элемента $a \in A$, $f(a) \in X_a$. Декартово произведение обозначается как $\Pi\{X_a : a \in A\}$, его можно представить как множество последовательностей длины A, причем для любой последовательности элемент с номером a принадлежит множеству X_a. Если для всех $a \in A$ множество $X_a = B$, то справедливое соотношение

$$\Pi \{X_a : a \in A\} = F(A, B) \quad \text{(см. 9)}.$$

Если для каждого $a \in A$ множество S_a — полугруппа, то на множестве $\Pi \{S_a : a \in A\}$ можно определить структуру полугруппы, положив $(f \cdot g)(a) = f(a) \cdot g(a)$. Эта полугруппа называется *прямым произведением полугрупп* S_a. В частности, если S — полугруппа, то множество $F(A, S)$ будет полугруппой, для которой закон композиции определяется операцией умножения в полугруппах $S_a = S$ для всех $a \in A$. Этот закон композиции часто называется *поточечным умножением* или *покоординатным умножением*.

Для каждого элемента $a \in A$ определено отображение $p_a : \Pi \{S_a : a \in A\} \to S_a$, которое называют проекцией $p_a(f) = f(a)$, проекция представляет собой эпиморфизм. В случае, когда $A = \{1, ..., k\}$, перепишем произведение $\Pi \{S_a : a \in \{1, ..., k\}\}$ в виде $S_1 \times ... \times S_k$, каждый элемент $f \in S_1 \times ... \times S_k$ представляется как $[f(1), ..., f(k)]$. Для проекции справедливо соотношение $p_j(s_1, ..., s_k) = s_j$.

13. Предположим, что A и B - непустые множества, а G — группа. Пусть $C: B \times A \to G^0$ — некоторое отображение.

Полугруппа $[(G \times A \times B) \cup \{0\}, \cdot]$, где символ 0 обозначает нулевой элемент, с операцией

$$(g_1, a_1, b_1) \cdot (g_2, a_2, b_2) = \begin{cases} (g_1 C(b_1, a_2) g_2, a_1, b_2), \text{ если } C(b_1, a_2) \neq 0, \\ 0, \text{ если } C(b_1, a_2) = 0 \end{cases}$$

иазивається *рисовской полугруппой матричного типа из сендвич-матрицей C над группой с нулем* G^0 и обозначается как $\mathcal{M}^0(G; A, B; C)$. Следовательно , $(g_1, a_1, b_1)(g_2, a_2, b_2) = 0$ тогда и только тогда, когда $C(b_1, a_2) = 0$. Из этого следует, что для $m_1, ..., m_k \in \mathcal{M}^0(G; A, B; C)$ $m_1 ... m_k = 0$ тогда и только тогда, когда $m_i m_{i+1} = 0$ для некоторого $i = 1, ..., k - 1$.

Иногда удобно представлять элемент (g, a, b) как $|A| \times |B|$ матрицу над полугруппой G^0, у которой элемент с номером (a, b) равен g, а все остальные элементы — нули. Элемент 0 описанной полугруппы

следует представлять как нулевую матрицу порядка $|A| \times |B|$. Тогда, если C представить как $|B| \times |A|$ матрицу над группой с нулем G^0, произведение матриц $(g_1, a_1, b_1)\ C\ (g_2, a_2, b_2)$ имеет смысл (операция в полугруппе G^0 определяется операцией сложения в группе G и соотношениями $x + 0 = x = 0 + x$ для всех $x \in (G^0)$ и легко проверить, что это дает в точности ранее определенное произведение $(g_1, a_1, b_1) \bullet (g_2, a_2, b_2)$. Часто элемент (g,a,b) будет обозначаться нами как $(g)_{ab}$, а полугруппа $\mathcal{M}^0(G; A, B; C)$ - как $S_{mn}(G, C)$, где $m = |A|$ и $n = |B|$.

Следовательно, полугруппа $S_{mn}(G, C)$ состоит из всех $m \times n$ матриц с коэффициентами в группе с нулем G^0, содержащими не более одного ненулевого элемента. Операция умножения в полугруппе $S_{mn}(G, C)$ определяется соотношением

$$(g)_{ab} \bullet (g')_{a'b'} = (g)_{ab}\ C\ (g')_{a'b'},$$

где $m = |A|$ и $n = |B|$. Очевидно, полугруппы $S_{mn}(G, C)$ и $\mathcal{M}^0(G; A, B; C)$ изоморфны.

Множество $\mathcal{M}^0(G; A, B; C) - \{0\}$ представляет собой подполугруппу в $\mathcal{M}^0(G; A, B; C)$ тогда и только тогда, когда матрица C не содержит нулевых элементов, т.е. $0 \notin C(B \times A)$. В этом случае обозначим подполугруппу $\mathcal{M}^0(G; A, B; C) - \{0\}$ как $\mathcal{M}(G; A, B; C)$. Тогда $[\mathcal{M}(G; A, B; C)]^0 = \mathcal{M}^0(G; A, B; C)$.

Рисовская полугруппа матричного типа со структурной матрицей C над группой с нулем *регулярна* тогда и только тогда, если каждая строка и каждый столбец матрицы C содержит ненулевой элемент. Регулярные рисовские матричные полугруппы играют важную роль в структурной теории конечных полугрупп (см. микромодуль 8).

14. Пусть $E(S)$ обозначает множество идемпотентов полугруппы S, положим $IG(S) = \langle E(S) \rangle$. Очевидно, что $IG(S) = E(S)$, если S — коммутативная полугруппа. Пусть элементы $e_1\ e_2 \in E(S)$, будем писать: $e_1 \le e_2$ в том и только в том случае, когда $e_1e_2 = e_1 = e_2e_1$. Полугруппа S называется *связкой* тогда и только тогда, когда $E(S) = S$. Полугруппы A^l и A^r являются связями. Полугруппа $(2^X, \square)$ — коммутативная связка. Рассмотрим полугруппу $S_{22}(\{1\}, G)$, где $C(2, 2) = 0$ и $C(a, b) = 1$ для $(a, b) \neq (2, 2)$ (см. 13), очевидно, что $IG(S) \neq E(S)$.

15. Пусть G - группа. Обозначим через $\mathcal{FM}(n, G)$ множество всех $n \times n$ матриц над G^0, каждый столбец которых содержит не более одного ненулевого элемента. Такие матрицы называются *мономиальными по столбцам*. Множество $\mathcal{FM}(n, G)$ всех $n \times n$ мономиальных по столбцам матриц над G^0 образует полугруппу относительно обычной операции умножения матриц при условии, что $x + 0 = x = 0 + x$ для всех

элементов $x \in G^0$. Аналогично, полугруппа $\mathcal{RM}(n, G)$ всех *n×n мономиальных по строкам матриц* над G^0 состоит из всех матриц над G^0, каждая строка которых содержит не более одного ненулевого элемента полугруппы G^0. Заметим, что полугруппа $\mathcal{RM}(n, G)$ действует точно справа на $S_{mn}(G, C)$ при любых m, n, G, C; действие определяется справа на элементы полугруппы $\mathcal{RM}(n, G)$. Полугруппа $\mathcal{FM}(m, G)$ действует точно слева на $S_{mn}(G, C)$; действие определяется по помощи обычного матричного умножения слева на элементы полугруппы $\mathcal{FM}(m, G)$.

Мы введем понятие идеала полугруппы и опишем некоторые его свойства. Более подробно идеалы изучаются в микромодуле 8.

5. Определение. Пусть S — полугруппа. Непустое подмножество $I \subseteq S$ называется *идеалом,* если для всех $i \in I$ и $s \in S$ справедливы соотношения $is \in I$ и $si \in I$. Следовательно, I будет идеалом тогда и только тогда, когда $IS \subseteq I$ и $SI \subseteq I$. Множество I называется *левым* или *правым идеалом,* если соответственно имеет место первое или второе из этих соотношений. Заметим, что идеалы, левые идеалы и правые идеалы представляют собой полугруппы.

Идеал полугруппы S называется *минимальным,* если он не содержит не равных себе идеалов полугруппы S. Идеал I полугруппы S называется 0-*минимальным,* если $I \neq \{0\}$ и I не содержит отличных от I и 0 идеалов полугруппы S. Заметим, что минимальный идеал есть 0-минимальным, кроме случая $I=\{0\}$. Следовательно, в общем случае минимальность не влечет 0-минимальность. Минимальные и 0-минимальные левые и правые идеалы определяются аналогично.

Полугруппа S называется *нулевой,* если $S^2 = \{0\}$.

Полугруппа S называется *простой,* если она не содержит собственных простых идеалов. Полугруппа S с нулем называется 0-простоя, если $S^2 \neq 0$ и $\{0\}$ есть единственный собственный идеал из S. Заметим, что простая полугруппа — 0-простая, исключая случай $S=\{0\}$. Следовательно, в общем случае из того, что полугруппа простая, не следует, что она 0-простая. Простая слева, 0-простая слева простая справа и 0-простая справа полугруппы определяются аналогично.

Замечание. Множество идеалов, левых идеалов и правых идеалов полугруппы S замкнуты относительно операций объединения и непустого пересечения. Если I_1 и I_2 — идеалы полугруппы S, то $I_1 I_2$ — идеал в S и $I_1 I_2 \subseteq I_1 \square I_2$. Далее, если $I_{1,\ldots}, I_n$ — множество всех идеалов полугруппы S, то $I_1 \ldots I_n = I_1 \text{ I } \ldots I_n$, и этот идеал называется *ядром*

полугруппы S. Ядро обозначается $K(S)$. Так как $K(S)$ содержится в любом идеале полугруппы S, то это единственный минимальный идеал полугруппы S. $K(S) = \{0\}$ тогда и только тогда, когда S — полугруппа с нулем.

Утверждение 1. Пусть S — полугруппа.

а) S — простая тогда и только тогда, когда $SaS = S$ для всех $a \in S$.

б) S — 0-простая тогда и только тогда, когда $S \neq \{0\}$ и $Sa\ S = S$ для всех $a \in S$, $a \neq 0$.

Доказательство. Пусть S — 0-простая полугруппа. Тогда S^2 будет ненулевым идеалом из S. Следовательно, $S^2 = S$ и $S^n = S$ для любого целого $n > 0$. Для любого $a \in S$ множество SaS — идеал в полугруппе S, поэтому $SaS = S$ или $SaS = \{0\}$. Пусть $I = \{a \in S: SaS = \{0\}\}$. Очевидно, что множество I является идеалом, поэтому $I = \{0\}$. Но так как $S^3 = S$, то $I \neq S$. Следовательно, если $0 \neq a \in S$, то $SaS = S$.

И наоборот, если $SaS = S$ для $0 \neq a \in S$, обозначим через I ненулевой идеал полугруппы S, причем пусть $0 \neq a \in I$. Тогда $S = SaS \subseteq SIS \subseteq I$, следовательно, $S = I$, т.е. полугруппа S 0-простая.

в) Пусть I — минимальный идеал полугруппы S. Тогда I — простая полугруппа. В частности, $K(S)$ — простая полугруппа.

г) Пусть I — 0-минимальный идеал полугруппы S. Тогда I — или полугруппа с нулевым умножением, или 0-простая полугруппа.

Доказательство. Пусть I — 0-минимальный идеал полугруппы S. Если $I^2 = \{0\}$, то I — полугруппа с нулевым умножением. Если $I^2 \neq \{0\}$, то $I^2 = I$, так как I^2 — ненулевой идеал полугруппы S, содержащийся в I. Следовательно, $I^n = I$ для любого $n > 0$. Пусть $0 \neq a \in I$. Тогда S^1aS^1 — ненулевой идеал полугруппы S, содержащийся в идеале I, следовательно, он равен I. Таким образом, $IaI = (IS^1)a(S^1I) = I^3 = I$ и поэтому I — 0-простая полутрупа в силу б.

Замечание. 0-минимальный левый идеал или правый идеал 0-простой подгруппы не обязательно будет 0-простым. Рассмотрим, например, полугруппу $S = S_{22}(\{1\}, I)$, где I — 2×2 единичная матрица (см. пример 9). Тогда $L = \{(1)_{11}, (1)_{21}, 0\}$ — 0-минимальный левый идеал полугруппы S и $\{(1)_{21}, 0\}$ — идеал для L. Заметим, что $L^2 \neq \{0\}$.

Будем говорить, что подполугруппа T полугруппы S *расщепляет* S тогда и только тогда, когда S—T — подполугруппа для S. Предыдущий пример показывает, что $\{0\}$ не обязательно расщепляет в случае 0-простой полугруппы. Однако, если полугруппа S 0-простая слева или 0-простая справа, легко проверить, что $\{0\}$ расщепляет S и $S = T^0$, где T - соответственно простая слева или простая справа полугруппа.

Утверждение 2. Пусть заданы полугруппы S_1 и S_2 и дано отображения $\varphi : S_1 \to\to S_2$, представляющее собой эпиморфизм.

а) Пусть S_1 — подполугруппа, подгруппа, идеал, левый идеал, правый идеал, простая подполугруппа, простая слева подполугруппа, простая справа подполугруппа, минимальный идеал, минимальный левый идеал, минимальный правый идеал, ядро или подполугруппа с нулевым умножением в полугруппе S_1. Тогда множество $\varphi(S'_1)$ обладает тем же свойством в полугруппе S_2. Если S'_1 — 0-минимальный идеал (следовательно, и 0-простой), то $\varphi(S'_1) = \{0\}$ или $\varphi(S'_1)$ является 0-минимальным идеалом (следовательно, и 0-простым). Если e— единица (соответственно нуль) полугруппы S_1, то $\varphi(e)$ — единица (соответственно нуль) полугруппы S_2.

б) Пусть S'_2 — подполугруппа, идеал, левый идеал или правый идеал полугруппы S_2. Тогда $\varphi^{-1}(S'_2)$ обладает таким же свойство в полугруппе S_1. Отображение $T \to \varphi^{-1}(T)$ является взаимно однозначным, «сохраняющим включение» отображением множеств левых, правых и двусторонних идеалов полугруппы S'_2 в соответствующие множества полугруппы S_1.

в) Пусть S'_2— простая, простая справа, простая слева или простая слева и справа (т.е. группа) подполугруппа в S_2. Тогда существует подполугруппа S'_1 в S_1, обладающая таким же свойством, что и подполугруппа S'_2, причем выполнено соотношения $\varphi(S'_1)=S'_2$. В действительности в качестве полугруппы S'_1 может быть выбрана любая минимальная по включению подполугруппа $T \subseteq S_1$, обладающая свойством $\varphi(T) = S'_2$.

В заключение микромодуля докажем несколько основополагающих утверждений о полугруппах.

Утверждение 3 (классификация циклических полугрупп). Пусть $S = \langle s \rangle$ — циклическая полугруппа, порожденная элементом $s \in S$. Тогда или

1) $S \cong (Z^+,+)$, причем изоморфизм задается отображением $n \to s^n$, или

2) S представляет собой конечную полугруппу и существуют два единственных положительных целых числа r и m *индекс* и *период* полугруппы S, такие, что $S=\{s, s^2, ..., s^{m+r-1}\}$. Множество $K_s = \{s^r, ..., s^{m+r-1}\}$ — циклическая подгруппа порядка m полугруппы S.

Для любых двух заведомо заданных целых чисел r и m можно построить единственную (с точностью до изоморфизма) конечную циклическую полугруппу индекса r и периода m.

Доказательство. Если все степени элемента s различны между собой, то, очевидно, справедлив первый случай. Если это не так,

обозначим через r наименьшее целое положительное число, такое, что $s^r=s^{r+x}$ при некоторому положительном целом x. Пусть m — наименьшее такое x. Тогда элементы $s, s^2, ..., s^r$ различны и не равны элементам $s^{r+1}, ..., s^{r+m-1}$. Если $k \geq m$, то $s^{r+k}=s^{r+jm+n}=s^{r+n}$, где $0 \leq n < m$. Следовательно, $S = \{s, s^2, ..., s^{r+m-1}\}$. Наконец, отображение $s^{r+p} \rightarrow (r + p) \pmod m$ — изоморфизм множества $\{s^r, ..., s^{r+m-1}\}$ с группой $(Z_m, +)$, следовательно, имеет место случай 2.

Пусть r и m заданы, рассмотрим $f \in F_L$ ($\{0,..., r + m—1\}$), определяемую соотношениями $f(i) = i + 1$ для $i= 0,1, ... , r+m—2$ и $f(r + m—1) =r$. Тогда $<f> \subseteq F_{L_2}$ ($\{0, .., r+ m—1\}$) имеет индекс r и период m. Утверждение о единственности очевидно.

Полугруппа S называется *периодической*, если для любого элемента $s \in S$ справедливо неравенство $|<s>| < \infty$. *Периодическая группа - это* периодическая полугруппа, являющаяся группой. Каждая конечная полугруппа представляет собой периодическую полугруппу. Хотя в этой работе мы будем иметь дело только с конечными полугруппами, доказательства некоторых важных утверждений справедливы для более широкого класса периодических полугрупп.

Выведем некоторые полезные следствия из утверждения 3.

Утверждение 4. а) Пусть S — периодическая полугруппа и элемент $s \in S$. Тогда среди всевозможных степеней элемента s существует единственный идемпотент.

б) Полугруппа G - периодическая группа тогда и только тогда, когда каждая подполугруппа в G является подгруппой в G. В частности, подполугруппы конечных групп представляют собой подгруппы.

Доказательство, а) Единица циклической подгруппы полугруппы $<s>$ — единственный идемпотент.

б) Если G не является периодической группой, то она содержит циклическую полугруппу, изоморфную полугруппе $(Z^+, +)$, которая не может быть группой. Следовательно, если множество S есть подполугруппа периодической группы G, обозначим через r и m индекс и период соответственно элемента $s \in S$. Тогда $s^r s^m = s^r$ и поэтому $1=s^m \in S$. Если m — 1, то $s^{-1}=s \in S$, а если $m > 1$, то $s^{-1}= s^{m-1} \in S$. Следовательно, полугруппа является группой.

Утверждение 5. Пусть S_1 — периодическая полугруппа, а отображение $\varphi: S_1 \rightarrow\rightarrow S_2$ — эпиморфизм. Тогда S_2 - периодическая полугруппа, а отображение φ отображает $E(S_1)$ на $E(S_2)$ и сохраняет введенное в этих множествах отношение упорядоченности (см. пример 14).

Доказательство. Если $s \in S_1$, то $\varphi(\langle s\rangle)=\langle\varphi(s)\rangle$, следовательно, полугруппа S_2 периодическая. Очевидно, $\varphi[E(S_1]\ s \subseteq (S_2)$. И наоборот, если $e \in E(S_2)$, выберем $x \in S_1$ такой, что $\varphi(x)=e$, и обозначим через f единственный идемпотент, такой, что $x^n = f$ при некотором n. Тогда $\varphi(f) = e^n = e$, следовательно, $\varphi[E(S_1)] = E(S_2)$. Наконец, если $e_1e_2 = e_1 = e_2e_1$, то $\varphi(e_1)\varphi(e_2)=\varphi(e_1)=\varphi(e_2)\varphi(e_1)$, поэтому отображение сохраняет отношение упорядоченности.

Микромодуль 7.
Примеры решения типовых задач

1. Пусть S — полугруппа, обладающая следующим свойством. Существует элемент $x \in S$, что «делит» каждый элемент полугруппы S, т.е. для каждого элемента $s \in S$ найдутся элементы $l, r \in S$, такие, что $lx = s = xr$. Тогда S — моноид.

2. а) Пусть $\psi : A \to S$ — отображение множества A в полугруппу S. Тогда ψ можно единственным образом продолжить до гомоморфизма $\psi^{\Gamma}: \sum A \to S$, причем $\psi^{\Gamma}(\sum A) = \langle \psi(A)\rangle$.

б) Пусть T — некоторая полугруппа вида $T = \langle A \rangle$ и такая, что для любой полугруппы S и любого отображения θ: $A \to S$ существует единственное продолжение θ док гомоморфизма θ^{Γ}: $T \to S$. Тогда полугруппа T изоморфна полугруппе $\sum A$, а отображение, осуществляющее этот изоморфизм, фиксированно на множестве A.

3. Пусть S — полугруппа в $e \in E(S)$. Положим

$$H_e = \{s \in S: es = s = se \text{ и } sr = e = rs \text{ для некоторого } r \in S\}.$$

Тогда H_e — максимальная подгруппа в S, содержащая элемент e. В действительности, если G — подгруппа в S и $G \cap H_e \neq \varnothing$, то $G \subseteq H_e$. Следовательно, для $f \neq e$ $H_f \cap H_e = \varnothing$ и $\{H_e: e \in E(S)\}$ — множество максимальных подгрупп полугруппы S.

4. Пусть T — периодическая полугруппа и пусть $s_1, \ldots, s_m \in T$. Тогда для любого целого $N \geq 1$ существует $n \geq N$, такой, что $s_j^n \in E(S)$ при $j = 1, \ldots, m$.

Микромодуль 7.
Идивидуальные тестовые задачи

1. Если S — моноид и $xy = 1$ для $x, y \in S$, то элемент x называется *левым обратным* для элемента y, а элемент y — *правым обратным* для элемента x.

Постройте полугруппу, которая имеет n левых единиц и не имеет правых единиц. Если элемент моноида имеет левый и правый обратные элементы, то эти элементы равны.

2. Пусть S — конечная циклическая полугруппа. Найдите все гомоморфные образы и все подполугруппы полугруппы S. Будут ли они циклическими полугруппами?

3. Пусть S — конечная полугруппа и $t_1, t_2 \in S$. Пусть t_1, t_2, m_1, m_2 — соответственно индексы и периоды полугрупп $< t_1\ t_2 >$ и $< t_2 t_1 >$ [т.е. r_1, r_2, m_1, m_2 - наименьшие целые числа, такие, что $(t_1t_2)^{r_1} = (t_1t_2)^{r_1+m_1}$ и $(t_2t_1)^{r_2+m_2} = (t_2t_1)^{r_2}$]. Тогда $m_1 = m_2$ и $|r_2 — r_1| \leq 1$. Существует ли более тонкое утверждение относительно элементов r_1 и r_2?

4. Для полугрупп из примеров 1, 2, 9, 10 определить следующее:

а) максимальные подгруппы (с точностью до изоморфизма);

б) *IG (S);*

в) максимальные подполугруппы.

5. При условии, которое рисовская полугруппа матричного типа $S=\mathcal{M}^0(G;A;B;C)$ регулярна, докажите следующее:

а) если элементы $s, t \in S$ и $x \in S^1$ такие, что $sx=t$, то $t = 0$, или существует элемент $y \in S^1$, такой, что $ty = s$;

б) если элементы $s, t \in S$ и $x \in S^1$ такие, что $xs = t$, то $t = 0$ или существует элемент $y \in S^1$, такой, что $yt = s$;

в) если элементы $s, t \in S — \{0\}$, то существуют элементы $x, y \in S^1$, такие что $xsy = t$.

Микромодуль 8
Локальное построение конечных полугрупп

3.3. Локальные координаты: теорема Риса

В этом микромодуле развиваются два важных подхода к изучению конечных полугрупп. Первый из них основывается на отношениях Грина, а второй — на теореме Риса. Вместе они позволяют выяснить локальное строение конечных полугрупп.

Предполагается, что все полугруппы, рассматриваемые в этом микромодуле, имеют конечный порядок, если противное специально не оговорено.

Перед тем как приступать к изучению материала этого микромодуля, читатель может просмотреть материал микромодуля 7, связанный с понятием идеала.

Определение 1. Если $I \subseteq$ E — идеал полугруппы S, *фактор-полугруппа* S/I определяется как $((S - I) \cup \{0\}, \bullet)$, где $0 \notin S - I$ и

$$s_1 \cdot s_2 = \begin{cases} s_1 s_2, & \text{если } s_1 s_2 \in S - I, \\ 0 & \text{в противном случае.} \end{cases}$$

Ассоциативность умножения следует из того, что I — идеал полугруппы S.

Естественный (или канонический) эпиморфизм η_I: $S \to\to S/I$ определяется соотношениями

$$\eta_I(s) = \begin{cases} s, & \text{если } s_1 s_2 \in S - I, \\ 0, & \text{если } s \in I. \end{cases}$$

Следовательно, $S/S = \{0\}$. Положим по определению $S/\varnothing = S^0$.

Утверждение 1. а) Пусть S_1— полугруппа, I — идеал полугруппы S_1, положим $S_2 = S_1/I$. Если $\varphi = \eta_I$ — естественный эпиморфизм, то соответствие $T \to \varphi^{-1}(T)$ будет взаимно однозначным отображением множеств левых, правых и двусторонних идеалов полугруппы S_2 на соответствующие множества идеалов полугруппы S_1, содержащих I. Обратным отображением к $T \to \varphi^{1}(T)$ является $J \to \varphi(J)$.

б) Если множества A и B — подполугруппы полугруппы S, то $A \cup B$ — подполугруппа в S тогда и только тогда, когда

$AB \cap BA \subseteq A \cup B$. В частности, это включение имеет место, если A и B оба — левые идеалы, или A и B оба правые идеала, а также если либо A, либо B представляет собой идеал.

в) Пусть J — идеал и T — подполугруппа полугруппы S. Тогда $J \cap T = \varnothing$ или $J \cap T$ есть идеал в T и $J \cup T$ есть подполугруппа полугруппы S, содержащая J в качестве идеал. Следовательно, $(J \cup T)/J = T/(J \cap T)$.

г) Пусть $I_1 \subseteq I_2 \subseteq S$, где I_1 и I_2 — идеалы полугруппы S. Тогда I_2/I_1 — идеал полугруппы S / I_1 и $(S / I_1)/(I_2/ I_1) = S / I_2$.

д) Пусть $I_1 \subseteq I_2 \subseteq S$, где I_2 — идеал полугруппы S и I_1 — идеал в I_2 (т.е. I_1 — идеал I_2, рассматриваемого как полугруппа). Если $I^2_1 = I_1$, то I_1 есть идеал полугруппы S. (В замечании 1 покзано, что если $I^2_1 \neq I_1$, то I_1 может не быть идеалом полугруппы S.)

Доказательство. Проверку пунктов а)-г) оставляем читателю в качестве упражнения. Перейдем к пункту д). Так как $I^2_1 = I_1$, имеем $I^3_1 = I_1$.

Следовательно,

$$S I_1 S = S I^3_1 S = (S I_1) I_1 (I_1 S) \subseteq I_2 I_1 I_2 \subseteq I_1.$$

Поэтому I_1 будет идеалом полугруппы S.

Определение 2. Пусть $n>1$ и N_n обозначает полугруппу $(\{0, 1,..., n— 1\}, \bullet)$, где $\alpha \bullet \beta = 0$ для $\alpha, \beta \in \{0, 1, ..., n— 1\}$. N_n называется *стандартной полугруппой с нулевым умножением* порядка n.

Замечание 1. Пусть $n>1$ и N_{n+1} есть полугруппа вида $(N_n \cup \{e\},*)$, где N_n и $\{e\}$ — подполугруппы, $e*0 = 0 = 0*e$ и $e*\alpha = 1 = a*e$ для всех элементов $\alpha \in N_n$ — $\{0\}$. Пусть $I = N_n — \{1\}$. Тогда I есть идеал подполугруппы N_n и N_n есть идеал полугруппы S_{n+1}, но I не является идеалом полугруппы S_{n+1}. Отметим, что $I^2 = \{0\} \neq I$. Следовательно, этот пример показывает необходимость условия $I^2_1 = I_1$ в пункте д) утверждения 1.

Напомним, что ядром $K(S)$ полугруппы S называется ее минимальный идеал.

Определение 3. Пусть S — полугруппа. Рядом главных идеалов (или просто рядом) полугруппы S называется последовательность $S = I_0 \supset I_1 \supset \ldots \supset I_n = K(S)$, такая, что I_j - есть идеал полугруппы S при $j= 1, 2, ..., n$, и не существует идеала в полугруппе S, содержащего I_j и являющегося собственным подмножеством идеала I_{j-1} при некотором j. Отметим, что S есть объединение непересекающихся множеств $(I_0 — I_1)$, $(I_1— I_2),...,(I_{n-1}— I_n), I_n$. Факторами главного ряда называют фактор-полугруппы Риса

$F_j = I_{j-1}/I_j$ при j= 1, ... n и $F_{n+1}= I_n / \varnothing = K(S)^0$.

Замечание 2. Мы хотим разложить полугруппу на меньшие куски, или «основные блоки», и исследовать эти куски для определения локального построения. Сначала представляется разумным исследовать факторы главного ряда. В следующем утверждении будет показано, что эти факторы являются 0-простыми полугруппами, или полугруппами с нулевым умножением. Потом мы покажем, что для всех главных рядов полугруппы факторы будут одинаковы. Поскольку строение (т.е. закон умножения) полугрупп с нулевым умножением известен *(ab* = 0 для всех элементов *a*, *b*∈ *S),* остается только определить строение 0-простых полугрупп, чтобы уже стало известным локальное строение самой полугруппы. С помощью теоремы Риса и отношений Грина можно выяснить строение 0-простых полугрупп. Поэтому наша цель состоит теперь в доказательстве этой теоремы,

Утверждение 2. Факторы главного ряда являются или 0-простыми полугруппами, или полугруппами с нулевым умножением.

Доказательство. Так как *K (S)* — всегда простая полугруппа, полугруппа $F_{n+k} = K(S)^0$ будет 0-простоя. Пусть для j = 1, ..., n K есть ненулевой идеал полугруппы S/I_j, содержщийся в $F_j = I_{j-1}/I_j$, и пусть η*:* $S \to\to S/I_j$ — канонический эпиморфизм. Тогда $\eta^{-1}(K)$-идеал полугруппы S, содержщийся в I_{i-1} и I_i - собственное подмножество идеала K. Следовательно, $\eta^{-1}(K)= I_{i-1}$ и $K = F_i$. Поэтому F_i не содержит собственных идеалов полугруппы S/I_j, отличных от {0}. Но тогда F_i будет 0-минимальным в S/I_j, откуда следует, что F_j — или 0-простая полугруппа, или полугруппа с нулевым умножением.

Определение 4 (Грина). Пусть S — полугруппа. Для элемента $s \in S$ равенства $L(s) = S^1s$, $R(s) = sS^1$ и $J(s) = S^1sS^1$ являются соответственно *главным левым идеалом, главным правым идеалом и главным идеалом,* порожденными s.

Определим бинарные отношения $\mathcal{F}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ и $\mathcal{D}$ на S следующим образом:

1) $s_1 \mathcal{F} s_2$ тогда и только тогда, когда $J(s_1) = J(s_2)$,

2) $s_1 \mathcal{L} s_2$ тогда и только тогда, когда $L(s_1) = L(s_2)$,

3) $s_1 \mathcal{R} s_2$ тогда и только тогда, когда $R(s_1) = R(s_2)$,

4) $s_1 \mathcal{H} s_2$ тогда и только тогда, когда $s_1 \mathcal{L} s_2$ и $s_1 \mathcal{R} s_2$,

5) $s_1 \mathcal{D} s_2$ тогда и только тогда, когда существует $s \in S$, такой, что $s_1 \mathcal{L} s$ и $s \mathcal{R} s_2$ или, что является эквивалентным (см. пункт з) утверждения 3), тогда и только тогда, когда существует элемент $t \in S$, такой, что $s_1 \mathcal{R} t$ и $t \mathcal{L} s_2$.

Утверждение 3. а) $\mathcal{L}$, $\mathcal{R}$, $\mathcal{F}$ и $\mathcal{H}$ — отношения эквивалентности на полугруппе S. Мы обозначим через L_s, R_s, J_s и H_s соответственно $\mathcal{L}$, $\mathcal{R}$, $\mathcal{F}$ и $\mathcal{H}$ классы эквивалентности, которые содержат элемент s.

б) $\mathcal{L}$ — правоинвариантное отношение;

в) $\mathcal{R}$ — левоинвариантное отношение;

г) $s_1 \mathcal{F} s_2$ тогда и только тогда, когда существуют элементы $x, y, z, w \in S^1$, такие, что $xs_1y = s_2$ и $zs_2w = s_1$;

д) $s_1 \mathcal{L}\, s_2$ тогда и только тогда, когда существуют элементы $x, y \in S^1$, такие, что $xs_1 = s_2$ и $ys_2 = s_1$;

е) $s_1 \mathcal{R}\, s_2$ тогда и только тогда, когда существуют элементы $x, y \in S^1$, такие, что $s_1x = s_2$ и $s_2y = s_1$;

ж) $s_1 \mathcal{D} s_2$ тогда и только тогда, когда существуют элемент $s \in S$ и элементы $x, y, z, w \in S^1$, такие, что $xs_1 = s$, $ys = s_1$, $sz = s_2$, $s_2w = s$.

з) $\mathcal{D} = \mathcal{L} \bullet \mathcal{R} = \mathcal{R} \bullet \mathcal{L}$, поэтому $\mathcal{D}$ = LUB $(\mathcal{L}, \mathcal{R})$ (см. пример 4 из микромодуля 7).

Доказательство. Утверждения пунктов а)-ж) проверяются легко. Для доказательства пункта з) достаточно показать, что $\mathcal{L} \bullet \mathcal{R} \subseteq \mathcal{R} \bullet \mathcal{L}$, так как тогда $\mathcal{R} \bullet \mathcal{L} = \mathcal{R}^{-1} \bullet \mathcal{L}^{-1} = (\mathcal{L} \bullet \mathcal{R})^{-1} \subseteq (\mathcal{R} \bullet \mathcal{L})^{-1} = \mathcal{L}^{-1} \bullet \mathcal{R}^{-1} = \mathcal{L} \bullet \mathcal{R}$ и поэтому $\mathcal{L} \bullet \mathcal{R} = \mathcal{R} \bullet \mathcal{L}$. Для того чтобы доказать, что $\mathcal{L} \bullet \mathcal{R} \subseteq \mathcal{R} \bullet \mathcal{L}$, выберем элементы $s_1 s_2 \in S$, такие, что $s_1 (\mathcal{R} \bullet \mathcal{L}) s_2$.

Тогда для некоторого элемента $s \in S$ $s_1 \mathcal{L} s$ и $s \mathcal{R}\, s_2$, поэтому существуют элементы $w, x, y, z \in S^1$, такие, что $ws_1 = s$, $xs = s_1$, $sy = s_2$ и $s_2z = s$. Пусть $a = s_1y = xsy = xs_2$. Но поскольку отношения $\mathcal{L}$ и $\mathcal{R}$ правоинвариантно и левоинвариантно соответственно, из $s_1 \mathcal{L} s$ вытекает, что $a = s_1y \,\mathcal{L}\, sy = s_2$ и из $s \,\mathcal{R}\, s_2$ вытекает, что $s_1 = xs \,\mathcal{R}\, xs_2 = a$. Значит, $s_1 (\mathcal{R} \bullet \mathcal{L})\, s_2$.

Определение 5. Пусть S — полугруппа. Определим следующие отношения порядка на $\mathcal{F}$, $\mathcal{R}$ и $\mathcal{L}$ классах полугруппы S:

а) $J_a \le J_b$ тогда и только тогда, когда $J(a) \subseteq J(b)$;

б) $R_a \le R_b$ тогда и только тогда, когда $R(a) \subseteq R(b)$;

в) $L_a \le L_b$ тогда и только тогда, когда $L(a) \subseteq L(b)$.

Эти отношения порядка рефлексивны, антисимметричны и транзитивны.

Замечание 3. Отметим, что идеал I представляет собой объединение главных идеалов и объединение непересекающихся $\mathcal{F}$ классов J. Действительно, если $a \in J \cap I$ и $b \in J$, то существуют элементы $x, y \in S^1$, такие, что $b = xay \in S^1 I S^1 = I$. Следовательно, $J \subseteq I$. Если $J \subseteq I$, то идеал, порождаемый J, содержится в I. Следовательно, $\mathcal{F}$ класс J

порождает идеал I тогда и только тогда, когда $J \geq J'$ для всех $\mathcal{F}$ классов $J' \subseteq I$.

С каждым $\mathcal{F}$ классом J полугруппы S можно, естественно, связать полугруппу J^0, реализуемую следующим образом. Определим $B(J)$ как объединение всех $\mathcal{F}$ классов, строго меньших, чем J. Или $B(J) = \varnothing$, или $B(J)$ есть идеал полугруппы S. В обеих случаях $S^1JS^1 — B(J) = J$, поэтому определена фактор-полугруппа $J^0 == S^1JS^1 / B(J)$. [В случае, когда $B(J) = \varnothing$, имеем $J = R(S)$, поэтому $J^0 = R(S)^0$ есть полугруппа.] Следовательно, $J^0 = (J \cup \{0\}, \circ)$, где

$$x \circ y = \begin{cases} xy, \ \textit{если } xy \in J, \\ 0 \ \textit{в противном случае.} \end{cases}$$

Утверждение 4. а) Пусть I_1 и I_2 - идеалы полугруппы S и I_2 является максимальным идеалом, который содержится в I_1. Тогда множество $I_1 — I_2$ есть в точности один $\mathcal{F}$ класс полугруппы S. Следовательно, $I_1/I_2 = J^0$.

б) Факторы каждого главного ряда полугруппы S являются в точности полугруппами вида $\{ J^0 : J$ есть $\mathcal{F}$ класс полугруппы $S\}$.

в) Если J есть $\mathcal{F}$ класс полугруппы S, то полугруппа J^0 будет или 0-простоя, или полугруппой с нулевым умножением.

Доказательство. а) Очевидно, что $I_1 — I_2$ есть объединение $\mathcal{F}$ -классов. Пусть J — минимальный из них в $I_1 — I_2$. Покажем, что $J \cup I_2$ есть идеал полугруппы S.

Имеем $S^1JS^1 = J \cup B(J)$ и $B(J) \subseteq I_2$, так как J — минимальный в $I_1 — I_2$. Следовательно, $S^1JS^1 = J \cup B(J) \subseteq J \cup I_2$, поэтому множество $J \cup I_2$ представляет собой идеал полугруппы S, который содержится в I_1 и который включает как собственное подмножество идеал I_2. Следовательно, $I_1 = I_2 \cup J$. Пункт а) полностью доказан.

б) Воспользовавшись результатом пункта а), мы видим, что каждый главный ряд получается следующим образом. Выбираем любой максимальный $\mathcal{F}$ класс J_1 в полугруппе S. Обозначим $I_1 = S — J_1$. Выбираем любой максимальный $\mathcal{F}$ класс J_2 полугруппы S, содержащийся в I_1. Положим $I_2 = I_1 — J_2$ и т.д. Каждый $\mathcal{F}$ класс полугруппы S будет при соответствующих обстоятельствах выбран таким способом. Это доказывает пункт б).

Доказательство пункта в) вытекает из пункта б) и утверждения 2.

Определение 6. Пусть J некоторый $\mathcal{F}$ класс полугруппы S. Назовем J *регулярным $\mathcal{F}$ классом* полугруппы S тогда и только тогда, когда полугруппа J^0 является 0-простой. Назовем J *нулевым $\mathcal{F}$ классом* тогда и только тогда, когда J^0 есть полугруппа с нулевым умножением.

Замечание 4. Так как факторы главного ряда полугруппы S оказываются в точности полугруппами вида J^0, получающимися из $\mathcal{F}$ классов полугруппы S, было бы полезным исследовать строение $\mathcal{F}$ классов полугруппы S.

Из определений $\mathcal{H}$, $\mathcal{L}$, $\mathcal{R}$, и $\mathcal{F}$ сразу же вытекает, что:

1) $\mathcal{R}$, и $\mathcal{L}$ классы — непересекающиеся объединения $\mathcal{H}$ классов;

2) $\mathcal{F}$ классы — непересекающиеся объединения $\mathcal{L}$ классов;

3) $\mathcal{F}$ классы — непересекающиеся объединения $\mathcal{R}$ классов;

4) следовательно, $\mathcal{F}$ классы — непересекающиеся объединения $\mathcal{H}$ классов;

5) каждый $\mathcal{H}$ класс— пересечение $\mathcal{R}$ и $\mathcal{L}$ классов;

6) пересечение $\mathcal{L}$ и $\mathcal{R}$ классов есть или пустое множество, или $\mathcal{H}$ класс.

Следующий факт устанавливает (для конечных полугрупп), что внутри $\mathcal{F}$ класса пересечения $\mathcal{R}$ и $\mathcal{L}$ классов никогда не будет пустым и что все $\mathcal{H}$ классы из $\mathcal{F}$ класса находятся во взаимно однозначном соответствии.

Утверждение 5 (Грин). Пусть S — полугруппа. Тогда справедливы следующие факты.

а) $\mathcal{F} = \mathcal{D}$. (Напомним, что мы рассматриваем только конечные полугруппы, если только противное не оговорено. Существуют бесконечные полугруппы, для которых $\mathcal{F} \neq \mathcal{D}$. В действительности $\mathcal{F} = \mathcal{D}$, если каждый элемент полугруппы S, возведенный в некоторую степень, будет идемпотентом).

б) Пусть J - некоторый $\mathcal{F}$ класс полугруппы S. Тогда $L \cap R \neq \varnothing$ для всех $\mathcal{L}$ классов L из J и всех $\mathcal{R}$ классов R из J.

в) $h\mathcal{F}hx$ тогда и только тогда, когда $h\mathcal{R}hx$ для всех элементов x, $h \in S$.

г) $h\mathcal{F}xh$ тогда и только тогда, когда $h\mathcal{L}xh$ для всех элементов x, $h \in S$.

д) Пусть элементы s_1, $s_2 \in S$ и $s_1\mathcal{L}s_2$; x, $y \in S^1$ — такие элементы, что $xs_1=s_2$ и $ys_2=s_1$; отображения φ: $R_{s_1} \to R_{s_2}$ и θ: $R_{s_2} \to R_{s_1}$ определяются соотношениями $\varphi(s) = xs$ и $\theta(t) = yt$. Тогда оба отображения φ и θ будут взаимно однозначными и эпиморфными и $\varphi^{-1} = \theta$. Для a, $b \in R_{s_1}$ из $a \mathcal{L} b$ вытекает, что $\varphi(a) \mathcal{L} \varphi(b)$. Следовательно, $a\mathcal{H}b$, тогда и только

тогда, когда φ *(a)* $\mathcal{H}$ φ *(b),* т.е. отображение φ и θ переводят $\mathcal{H}$ классы на $\mathcal{H}$ классы. Дуальное предложение также справедливо.

е) Пусть элементы s_1, $s_2 \in S$ и $s_1 \mathcal{F} s_2$; $s \in S^1$, $w, x, y, z \in S^1$ — такие элементы, что $ws_1 = s$, $xs = s_1$, $sy = s_2$ и $s_2 z = s$; отображение $\alpha : H_{s_1} \to H_{s_2}$ и $\beta : H_{s_2} \to H_{s_1}$ определяются соотношениями $\alpha(t) = wty$ и $\beta(u) = xuz$. Тогда оба отображения α и β будут взаимно однозначными и эпиморфными и $\alpha^{-1} = \beta$. Следовательно, любые два $\mathcal{H}$ класса полугруппы S, содержащиеся в одном и том же $\mathcal{F}$ классе, находятся во взаимно однозначном соответствии.

Доказательство. а) Если $s_1 \mathcal{D} s_2$, то существует элемент $s \in S$, такой, что $s_1 \mathcal{L} s$ и $s \mathcal{R} s_2$. Следовательно, $s_1 \mathcal{F} s \mathcal{F} s_2$, так что из $s_1 \mathcal{D} s_2$ вытекает $s_1 \mathcal{F} s_2$.

Предположим, что $s_1 \mathcal{F} s_2$. Тогда существуют элементы $w, x, y, z \in S^1$, такие, что $ws_1 x = s_2$ и $ys_2 z = s_1$. Следовательно, $yws_1 xz = s_1$, поэтому $(yw)^n s_1 (xz)^n = s_1$ для $n \geq 1$. Для некоторого $N > 2$ элементы $(yw)^N = e_2$ и $(xz)^N = e_2$ являются идемпотентами. Следовательно, $e_1 s_1 = e_1 (e_1 s_1 e_2) = e_1 s_1 e_2 = s_1$, так что $[(yw)^{N-1} y]ws_1 = s_1$ и поэтому $ws_1 \mathcal{L} s_1$. Аналогично $s_1 x \mathcal{R} s_1$. Следовательно, $s_2 = ws_1 x \mathcal{R} ws_1 \mathcal{L} s_1$, но, поскольку отношение $\mathcal{R}$ левоинвариантно, $s_1 \mathcal{D} s_2$. Следовательно, $\mathcal{F} = \mathcal{D}$.

б) Пусть L и R будут соответственно $\mathcal{L}$ и $\mathcal{R}$ классами, которые принадлежат J. Пусть $a \in L$, $b \in R$. Тогда $a \mathcal{F} b$, так что $a \mathcal{D} b$, т.е. существует элемент $c \in S$, такой, что $a \mathcal{L} c \mathcal{R} b$. Следовательно, $c \in L \cap R$.

в, г) Пусть элементы $x, h \in S$. Если $h \mathcal{R} hx$, то $h \mathcal{F} hx$. Обратно, если $h \mathcal{F} hx$, то существуют элементы $a, b \in S^1$, такие, что $h = ahxb = a^n h (xb)^n$ для всех $n > 0$, поэтому, рассуждая так же, как в пункте а), получаем $h \mathcal{R} hx$.

Доказательство пункта г) дуально к доказательству пункта в).

д) Отображения φ и θ имеют требуемые области значений, поскольку отношение $\mathcal{R}$ левоинвариантно. Если $s \in R_{s_2}$, положим $s = s_2 z$ для некоторого элемента $z \in S^1$. Тогда $\varphi\theta(s) = xys_2 z = s_2 z = s$. Аналогичные рассуждения приводят к тому, что $\theta\varphi(t) = t$ для элементов $t \in R_{s_1}$. Следовательно, отображения θ и φ взаимно однозначные и эпиморфные и $\theta^{-1} = \varphi$. Так как для элемента $s \in R_{s_1}$, $\varphi(s) = xs$ и $y\varphi(s) = s$, получаем, что $s \mathcal{L} \varphi(s)$ для всех $s \in R_{s_1}$, поэтому, в частности, из отношения $s_1 \mathcal{L} s_2$ вытекает, что $\varphi(s_1) \mathcal{L} \varphi(s_2)$.

е) Рассматривая композицию отображений $a \to wa$ и $c \to cy$ и применяя рассуждения, которые дуальны к рассуждениям при доказательстве пункта д), получаем требуемое.

Замечание 5. Из пункта е) утверждения 5 немедленно следует, что если φ — гомоморфизм на полугруппе S, ограничение которого на $\mathcal{H}$ класс H взаимно однозначно, то φ будет взаимно однозначным на каждом $\mathcal{H}$ классе F, эквивалентном классу H. В самом деле, пусть $H_1 \mathcal{F} H$ и $h_1, h_2 \in H_1$ — такие элементы, что $\varphi(h_1) = \varphi(h_2)$. Тогда, как мы знаем, существуют элементы $x, y \in S^1$, такие, что $xH_1y = H$. Теперь $xh_1y, xh_2y \in H$ и $\varphi(xh_1y) = \varphi(xh_2y)$, так что $xh_1y = xh_2y$. Но так как отображение $h \to xhy$ взаимно однозначно, получаем $h_1 = h_2$.

Замечание 6. Далее будет показано, что для каждого $\mathcal{F}$ класса J полугруппы S можно так ввести систему координат, что закон умножения полугруппы J^0 относительно этой системы будет иметь некоторый естественный вид.

Предположим, что J — $\mathcal{F}$ класс полугруппы S. Пусть $R_1, ..., R_m$ есть $\mathcal{R}$ классами в J и $L_1, ..., L_n$ есть $\mathcal{L}$ классы из J. Тогда по утверждению 5 $\mathcal{H}$ классы, которые принадлежат J, описываются как $\{H_{ij} = R_i \square L_j : i = 1, ..., m; j = 1, ..., n\}$. Следовательно, мы получаем для J наглядный образ, называемый «eggbox»-картинкой. Она представляет собой прямоугольную таблицу, строки которой соответствуют $\mathcal{R}$ классам, а столбцы — $\mathcal{L}$ классам (содержащимся в J), и пересечение каждого столбца с каждой строкой определяет (внутри клеточки таблицы) некоторый $\mathcal{H}$ класс (см. рис. 3.1). Из пункта е) утверждения 5 следует, что любые $\mathcal{H}$ классы из этой таблицы находятся во взаимно однозначном соответствии, там же описаны отображения, которые переводят один $\mathcal{H}$ класс на другие.

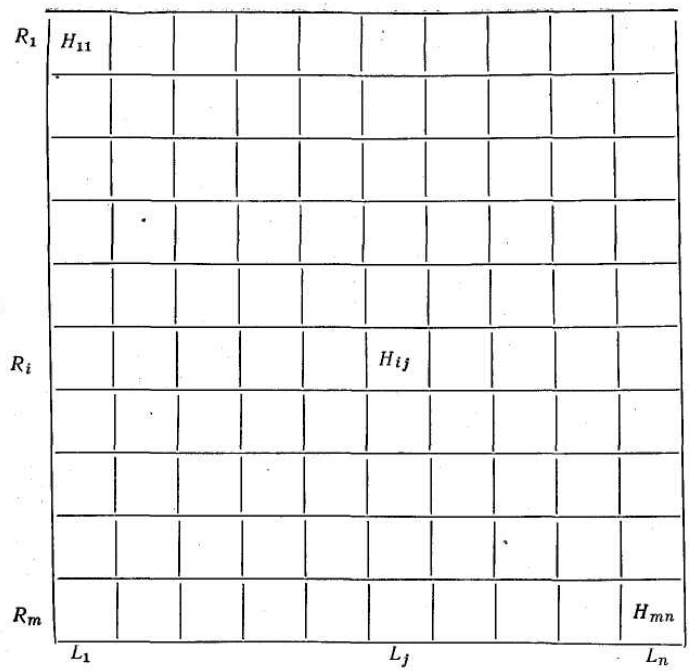


Рис. 3.1

Здесь изображена «eggbox»-картинка для $\mathcal{F}$ класса J. Строки соответствуют $\mathcal{R}$ классам полугруппы S, содержащимся в J. Столбцы соответствуют $\mathcal{L}$ классам полугруппы S, содержащимся в J. На пересечении строки и столбца получается $\mathcal{H}$ класс полугруппы S, содержащийся в J. Класс J нулевой или регулярный. Если J — регулярный, эти классы совпадают с неравными нулю классами из J^0 и умножение определяется с помощью теоремы Риса.

Утверждение 6 (Грин). Пусть S — полугруппа.

а) Каждая подгруппа из S содержится в некоторому $\mathcal{H}$ классе полугруппы S. $\mathcal{H}$ класс H полугруппы S будет подгруппой тогда и только тогда, когда существуют элементы s_1, $s_2 \in H$, такие, что $s_1 s_2 \in H$. Таким образом, H есть подгруппа в S тогда и только тогда, когда H содержит идемпотент. Следовательно, максимальные подгруппы полугруппы S — это в точности $\mathcal{H}$ классы полугруппы S, содержащие идемпотенты.

б) Пусть S есть 0-простой полугруппой, тогда каждый $\mathcal{R}$ и каждый $\mathcal{L}$ класс полугруппы S содержит идемпотент.

Доказательство. Очевидно, что каждая подгруппа из S содержится в $\mathcal{H}$ классе. Перейдем к проверке второго утверждения: если $s_1, s_2, s_1s_2 \in H$, то $s \to ss_2$ и $s \to ss_2$ являются взаимно однозначными отображениями H на себя (согласно утверждению 5). Следовательно, $s_1H = H = Hs_2$, так что, если $x_1, x_2 \in H$, то $x_1H = H = Hx_2$. Так как это имеет место для всех элементов $x_1, x_2 \in H$, то H будет подполугруппой полугруппы S, причем эта подполугруппа простая слева и справа. Следовательно, H есть группа (см. упражнение 6 из настоящего микромодуля). Оставшаяся часть пункта а) доказывается очень легко.

б) Пусть полугруппа S будет 0-простоя. Тогда S — {0} является $\mathcal{F}$ классом полугруппы S. Из утверждения 5 следует, что для всех ненулевых элементов $a \in S$ $R(a) = R_a \cup \{0\}$ и $L(a) = L_a \cup \{0\}$, т.е. правый идеал, порожденный элементом a, есть просто $\mathcal{R}$ класс, который содержит a с нулем.

Пусть теперь $a \in S$ — {0}. Тогда $SaS = S$, поэтому существуют ненулевые элементы $x, y \in S$, такие, что $xay = a$, тогда $x^n a y^n = a$ для всех $n \geq 1$ и поэтому существуют ненулевые идемпотенты e_1, e_2, такие, что $e_1 ae_2 = a$. Тогда $e_1 a = a$ и $ae_2 = a$. Из равенства $e_1 a = a$ вытекает, что $a \in R(e_1)$. Так как $a \neq 0$, имеем $a \in R_{e_1}$, поэтому $R_a = R_{e_1}$ и $e_1 \in R_a$. Аналогично $e_2 \in L_a$.

Утверждение 7. Если J-регулярный $\mathcal{F}$ класс полугруппы S, то $\mathcal{R}$, $\mathcal{L}$, и $\mathcal{H}$ классы полугруппы, содержащиеся в J, будут соответственно ненулевыми $\mathcal{R}$, $\mathcal{L}$, и $\mathcal{H}$ классами 0-простой полугруппы J^0.

Доказательство. Мы докажем утверждение для $\mathcal{L}$ классов; для $\mathcal{R}$ классов доказательство проводится аналогично. Поскольку $\mathcal{H}$ классы представляют собой пересечения $\mathcal{L}$ и $\mathcal{R}$ классов, утверждение будет справедливо и для $\mathcal{H}$ классов.

Пусть $\mathcal{L}(S)$ и $\mathcal{L}(J)$ обозначают отношения эквивалентности $\mathcal{L}$ для полугрупп S и J^0 соответственно. Очевидно, если L' — ненулевой $\mathcal{L}$ класс полугруппы J^0, то L' содержится в $\mathcal{L}$ классе J полугруппы S.

Обратно: пусть элементы $a, b \in J$. Предположим, что $a(S)b$. Тогда в силу утверждения 7 существуют идемпотенты $e_a, e_b \in J^0$, такие, что $e_a \mathcal{L}(J) a$ и $e_b \mathcal{L}(J) b$. Так как $\mathcal{L}(J)$ эквивалентность влечет $\mathcal{L}(S)$ эквивалентность, имеем $e_a \mathcal{L}(S) a \mathcal{L}(S) b \mathcal{L}(S) e_b$, т.е. $e_a \mathcal{L}(S) e_b$. Тогда существуют элементы $x, y \in S^1$, такие, что $xe_a = e_b$ и $ye_b = e_a$. Поэтому

$e_a e_b = y e_b e_b = y e_b = e_a$ и аналогично $e_b e_a = e_b$. Следовательно, $e_a \mathcal{L}(J) e_b$, поэтому $a \mathcal{L}(J) e_a \mathcal{L}(J) e_b \mathcal{L}(J) b$.

Замечание 7. Теперь мы знаем, что если J является регулярным $\mathcal{F}$ - классом, то картинка, которую мы ввели для J (см. рис. 3.1), в точности совпадает с картинкой для ненулевого $\mathcal{F}$ класса полугруппы J^0. Дальше мы сформулируем и докажем теорему Риса, которая полностью определяет строение 0-простых полугрупп при помощи «eggbox»-картинки. Тогда в силу утверждения 7 мы будем знать строение регулярных $\mathcal{F}$ - классов.

Теорема Риса. Если S — 0-простая полугруппа, то полугруппа S^0 изоморфная регулярной рисовской полугруппе матричного типа. Наоборот, регулярная рисовская полугруппа матричного типа есть 0-простоя.

Доказательство. Пусть S — 0-простая полугруппа и J — ее (единственный) ненулевой $\mathcal{F}$ класс. Как и в замечании, предшествующем утверждению 6, пусть $R_1, ..., R_m$ и $L_1..., L_n$ обозначают $\mathcal{R}$ и $\mathcal{L}$ классы полугруппы S, содержащиеся в J. Тогда $H_{ij} = R_i \square L_j$ есть $\mathcal{H}$ классы полугруппы S, содержащиеся в J. В силу утверждения 6 по крайней мере один $\mathcal{H}$ класс, который принадлежит J, является подгруппой полугруппы S. Предположим, что $\mathcal{R}$ и $\mathcal{L}$ классы занумерованы так, что $H_{11} = R_1 \cap L_1$ есть подгруппа. Пусть e — единичный элемент подгруппы H_{11}. Для номеров $i = 1, ..., m$ и $j = 1, ..., n$ выберем элементы $l_i \in H_{i1}$ и $r_j \in H_{1j}$. Теперь $e \mathcal{L} l_i$, поэтому существует элемент $x \in S^1$, такой, что $xe = l_i$. Тогда $l_i e = xee = xe = l_i$. Аналогично $er_i = r_i$. Тогда в силу утверждения 5 соответствие $g \to l_i g r_j$ будет взаимно однозначным отображением класса H_{11} на класс H_{ij} для $i = 1, ..., m$ и $j = 1, ..., n$. Следовательно, при заданных l_i -м и r_j-м элементах каждый элемент $s \in J$ однозначно представляется в виде $s = l_i g r_i$, где $g \in H_{11}$.

Пусть теперь $A = \{1, ..., m\}$, $B = \{1, ..., n\}$ и $G = H_{11}$. Определим отображение $\psi: S^0 \to \mathcal{M}^0 (G; A, B; C)$, полагая $\psi(l_i g r_j) = (g, i, j)$ и $\psi(0) = 0$. Из предыдущих рассуждений вытекает, что отображение ψ взаимно однозначное и эпиморфное. Определим отображение $C: B \times A \to G^0$, полагая $C(j, i) = r_j l_i$. Теперь $r_j \in R_1 \cup \{0\}$— правый идеал полугруппы S и $l_i \in L_1 \cup \{0\}$ — левый идеал полугруппы S. Следовательно, $r_j l_i \in (R_1 \cap L_1) \cup \{0\} = G^0$, легко видеть, что отображение ψ есть изоморфизм.

Для того чтобы завершить доказательство, остается показать, что рисовская полугруппа матричного типа 0-простая тогда и только тогда,

когда она регулярная. Мы оставляем это читателю как упражнение (см. упражнение 3 в этом микромодуле).

Резюме. Все приведенные соображения дают возможность узнать, как локально устроено умножение в полугруппе S. Термин «локально» означает, что рассматривается произведение элементов из одного $\mathcal{F}$ класса. Если произведение двух элементов из $\mathcal{F}$ класса J снова принадлежит J, то мы знаем, чему это произведение равно. Если же произведение не принадлежит J, оно переходит, или «спускается», в $\mathcal{F}$ класс, меньший, чем класс J (в смысле отношения порядка, введенного на множестве $\mathcal{F}$ классов). Этот факт нам известен, однако чему равно произведение или в какой конкретно $\mathcal{F}$ класс оно попадает, мы не знаем.

Нам известно «локальное умножение» потому, что $\mathcal{F}$ класс J является или регулярным, или нулевым. Если класс J нулевой, произведение двух элементов всегда спускается в меньший $\mathcal{F}$ класс. Если класс J регулярный, то рисовская полугруппа матричного типа, изоморфная J^0, позволяет определить, или спускается или нет произведение, и если оно не спускается, то чему оно равно.

Такая характеристика регулярных $\mathcal{F}$ классов с помощью регулярных рисовских полугрупп матричного типа исключительно полезна и мы рекомендуем читателю как можно лучше ознакомиться с этим специальным классом полугрупп. Далее, начиная с этого места, *большинство доказательств будет проводиться при помощи теоремы Риса и рисовских полугрупп матричного типа.*

Замечание 8. Изоморфизм $\psi : S^0 \to\to \mathcal{M}^0(G; A, B; C)$, определенный в доказательстве теоремы Риса, целиком зависел от выбора элементов $l_i \in H_{i1}$ и $r_j \in H_{1j}$. Так как внутри соответствующих $\mathcal{H}$ классов эти элементы можно выбирать произвольно, для полугруппы S^0 существует, вообще говоря, много таких изоморфизмов. Любой изоморфизм полугруппы S^0, определенный таким образом, называется *координатным отображением для (0-простой) полугруппы* S. Следующее утверждение дает полезную характеристику всех координатных отображений S.

Утверждение 8. Пусть S есть 0-простая полугруппа. Предположим, что

$$\psi : S^0 \to\to \mathcal{M}^0(G; A, B; C) \text{ и } \psi' : S^0 \to\to \mathcal{M}^0(G; A, B; P)$$

представляют собой два координатных отображения для полугруппы S. Пусть $l_i \in H_{i1}$, $r_j \in H_{1i}$ и $l_{i'} \in H_{i1}$, $r_{j'} \in H_{1j}$, $i = 1, ..., n$, $j = 1, ..., m$, будут соответствующими наборами элементов, которые определяют

отображения ψ и ψ'. Тогда существуют отображения $\lambda: A \to G$ и $\delta: B \to G$, такие, что $P(j, i) = \delta(j) C(j, i)\, \lambda(i)$ и отображение
$\theta : \mathcal{M}^0(G; A, B; C) \to\to \mathcal{M}^0(G; A, B; P)$, определяемое соотношением $\theta(g,i,j)=(\lambda(i)^{-1} g \delta(j)^{-1}, i, j)$, будет изоморфизмом, причем $\psi'=\theta\psi$. Наоборот, если для любых заданных отображений $\lambda : A \to G$ и $\delta: B \to G$ структурная матрица $P: B \times A \to G^0$ определяется соотношением $P(j, i)=\delta(j)\, C(j, i)\, \lambda(i)$, то отображение θ, введенное раньше, устанавливает изоморфизм из $\mathcal{M}^0(G; A, B; C)$ на $\mathcal{M}^0(G; A, B; P)$ и изоморфизм $\psi'=\theta\psi$ есть координатное отображение для полугруппы S.

Доказательство. Пусть ψ и ψ' — два координатных отображения для полугруппы S, определенные ранее. Так как умножение слева на элемент l_i есть взаимно однозначное отображение из $H_{11} = G$ в H_{i1}, то существует единственный элемент $g_j \in G$, такой, что $l_i g_i = l_{i'}$. Аналогично существует единственный элемент $g_j \in G$, такой, что $g_j r_j = r_{j'}$. Определим λ и δ, полагая $\delta(i) = g_i$ и $\delta(j) = g_i$. Тогда $P(j, i) = r_{j'} l_{i'} = \delta(j) C(j, i)\, \lambda(i)$ и θ - такой изоморфизм, что $\psi'=\theta\psi$.

Наоборот, очевидно, что θ является изоморфизмом. Определим $l_{i'} = l_i \lambda(i) \in H_{i1}$, $r_{j'} = \delta(j)\, r_j \in H_{1i}$. Легко видеть, что элементы $l_{i'}$ и $r_{j'}$ определяют отображение $\psi'=\theta\psi$, так что ψ' есть координатное отображение для полугруппы S.

Замечание 9. Из изложенного следует, что могут существовать два различных координатных отображения для полугруппы S, переводящие S^0 в одну и ту же регулярную рисовскую полугруппу матричного типа $\mathcal{M}^0(G; A, B; C)$. Предположим, например, что G - не абелева группа и $C(B \times A)$ содержится в центре группы G. Пусть $g_0 \in G$ — произвольный элемент, не принадлежащий центру, для всех i, j, положим $\lambda(i) = g_0$, $\delta(j) = g_0^{-1}$. Тогда $P(j, i) = C(j, i)$, но отображение $(g, i, j) \to [\lambda(i)^{-1} g \delta(j)^{-1}, i, j]$ не является тождественным.

Утверждение 9. Пусть S — 0-простая полугруппа. Тогда существует такое координатное отображение для полугруппы S, что все элементы в данном столбце и данной строке соответствующей структурной матрицы равны нулю или единице (единице группы G).

Доказательство. Это утверждение следует из утверждения 8, если соответствующим образом выбрать отображение $\lambda : A \to G$ и $\delta: B \to G$.

Утверждение 10. Пусть S — полугруппа.

а) Если S — простая слева, то $S \cong G \times A^l$, где G — группа и A — конечное множество.

б) Если S— простая справа, то $S \cong G \times B^r$, где G— группа и B — конечное множество.

Мы оставляем читателю доказательство этого утверждения как простое упражнение на применение теоремы Риса. *(Указание.* Воспользуйтесь утверждением 9.)

3.4. Приложения теоремы Риса и группа Щютценберже.

В этом пункте вводится группа Щютценберже - важный инструмент для исследования конечных полугрупп. Вместе с теоремой Риса эта группа используется для определения вида и строения локальных гомоморфизмов и переносов конечных полугрупп, а также для описания различных локальных свойств полугрупп.

Под термином «локальный гомоморфизм» мы имеем в виду ограничение эпиморфизма $\varphi : S_1 \to\to S_2$ на $\mathcal{F}$ класс полугруппы S_1. Мы определим вид всех таких ограничений с помощью координатной картинки Грина-Риса для $\mathcal{F}$ классов.

Утверждение 11. Пусть отображение $\varphi : S_1 \to\to S_2$ есть эпиморфизм. Пусть символ $\alpha(S_i)$ обозначает любое из отношений $\mathcal{F}$, $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$ на полугруппе S_i, i =1,2.

а) Если $s\alpha(S_1)t$, то $\varphi(s)\alpha(S_2)\varphi(t)$. Следовательно, эпиморфизм φ переводит α классы полугруппы S_1 в α классы полугруппы S_2.

б) Пусть A_2 есть α класс полугруппы S_2. Тогда $\varphi^{-1}(A_2)$ есть объединения α классов полугруппы S_1.

в) Пусть J_2 есть $\mathcal{F}$ класс полугруппы S_2, а J_1— минимальный $\mathcal{F}$ класс (см. определение 5) полугруппы S_1, содержащийся в $\varphi^{-1}(J_2)$. Тогда $\varphi(J_1) = J_2$ и φ индуцирует эпиморфизм $\varphi^{-1} : J^0{}_1 \to\to J^0{}_2$.

г) Каждый $\mathcal{R}$ и $\mathcal{L}$ классы полугруппы S_1, которые содержатся в J_1, переводятся отображением φ на $\mathcal{R}$ и $\mathcal{L}$ классы соответственно полугруппы S_2, содержащиеся в J_2. (Если класс J_2 не регулярный, то утверждение для $\mathcal{H}$ классов, вообще говоря, не верное; см. предложение 1 и замечание 12, где приводится контрпример.)

д) Класс J_1 регулярный тогда и только тогда, когда регулярный класс J_2. Если класс J_2 нулевой, то каждый $\mathcal{F}$ класс, который содержится в $\varphi^{-1}(J_2)$, нулевой. Когда класс J_2 регулярный, J_1 - единственный минимальный $\mathcal{F}$ класс прообраза $\varphi^{-1}(J_2)$.

Доказательство. В случае пункта а) доказательство тривиально, а пункт б) следует из а).

в) Пусть класс J_1 удовлетворяет условию пункта в). Тогда множество $\varphi(S|\ J_1S|)$ есть идеал полугруппы S_2, пересекающийся с J_2 и, следовательно, содержащий класс J_2. Кроме того, множество $B(J_1)=S^1J_1S^1—J_1$ есть идеал полугруппы S_1 и $B\ (J_1) \square \varphi^{-1}\ (J_2) = \varnothing$ в силу минимальности класса J_1. Следовательно, $\varphi\ [B\ (J_1)]\ \mathrm{I}\ \ (J_2) = \varnothing$ и $\varphi(J_1) = J_2$. Отображение φ': $J^0{}_1 \rightarrow J^0{}_2$ определено корректно, поскольку класс J_1 минимальный в $\varphi^{-1}\ (J_2)$.

г) Так как J_1 минимальный, каждый $\mathcal{R}$ и $\mathcal{L}$ класс полугруппы S_1, содержащийся в J_1, будет минимальным относительно соответствующего упорядочения $\mathcal{R}$ и $\mathcal{L}$ классов. Пусть L_1 есть $\mathcal{L}$ класс полугруппы S_1, содержащийся в J_1 Предположим, что $\varphi\ (L_1) \subseteq L_2$— $\mathcal{L}$ класс полугруппы S_2, содержащийся в J_2. Тогда L_1 является минимальным в $\varphi^{-1}(L_2)$, последнее множество есть объединения $\mathcal{L}$ классов. Теперь пункт г) доказывается с помощью рассуждений, аналогичных пункту в).

д) Если J_2 есть регулярный класс, он содержит идемпотент e. Пусть элемент $s \in J_1$, такой, что $\varphi(s)=e$. Для некоторого n элемент s^n будет идемпотентом и $\varphi\ (s^n) = e^n = e$. Следовательно, $s^n = J_1$ и класс J_1 регулярный. Если J_2 — нулевой класс, то J_2 не содержит идемпотентов. Пусть e — идемпотент некоторого $\mathcal{F}$ класса в прообразе $\varphi^{-1}(J_2)$. Тогда элемент $\varphi(e) \in J_2$ будет идемпотентом. Следовательно, каждый $\mathcal{F}$ - класс, который содержится в множестве $\varphi^{-1}(J_2)$, будет нулевым, если нулевой класс J_2.

Перейдем к доказательству последнего пункта. Пусть J_2-регулярный $\mathcal{F}$ класс. Предположим, что J_1 и J'_1 — два минимальных $\mathcal{F}$ классы, которые содержатся в множестве $\varphi^{-1}\ (J_1)$. Тогда $\varphi\ (J_1) = \varphi\ (J'_{1)} = J_2$. Так как класс J_2 регулярный, имеем в силу теоремы Риса включение $J_2 \subseteq J^2{}_2$. Тогда $J_2 \subseteq J_2\ J_2 = \varphi\ (J_1)\ \varphi\ (J'_{1)} = \varphi\ (J_1\ J'_{1)}$. Если классы J_1 и J'_1 различные, то множество $J_1 \cdot J'_1$, которое принадлежит пересечению $S|J_1S|\ \mathrm{I}\ \ S|J'_1S|$, не пересекается с множеством $\varphi^{-1}\ (J_2)$. Следовательно, $J_1 = J'_1$.

Определение 7. Пусть S' — подмножество полугруппы S. Пусть φ — отображение из S' в полугруппу T. Отображение φ называется *частичным гомоморфизмом* тогда и только тогда, когда для всех элементов $s_1, s_2 \in S'$, таких, что $s_1s_2 \in S'$ выполняется соотношение $\varphi(s_1)\varphi\ (s_2) = \varphi\ (s_1s_2)$. Если $s_1s_2 \notin S'$, то никаких условий на элемент $\varphi(s_1)\varphi\ (s_2)$ не накладывается.

Замечание 10. Пусть отображение $\varphi : S_1 \rightarrow\rightarrow S_2$ является эпиморфизмом. Ограничение φ на любой $\mathcal{F}$ класс полугруппы S_1 будет

частичным гомоморфизмом. Отметим, что любая функция, которая определена на нулевом $\mathcal{F}$ классе, является частичным гомоморфизмом. Следующее предложение дает простое описание всех частичных гомоморфизмов регулярных $\mathcal{F}$ классов при помощи картинки Грин-Риса для $\mathcal{F}$ классов.

Определение 8. Понятие координатного отображения для 0-простых полугрупп можно очевидным образом распространить на регулярные $\mathcal{F}$ классы. *Координатными отображениями для регулярного $\mathcal{F}$ класса* J будут ограничения координатных отображений $C: J^0 \to\to \mathcal{M}^0 (G; A, B; P)$ на класс J, переводящие J на $\mathcal{M}^0 (G; A, B; P) — \{0\}$. Следовательно, координатное отображение для J дает описание класса J как ненулевой части регулярной рисовской полугруппы матричного типа.

Предложение 1. Пусть J_1 — регулярный $\mathcal{F}$ класс полугруппы S_1. Предположим, что отображение $\varphi: J_1 \to S_2$ является частичным гомоморфизмом. Тогда справедливы следующие утверждения.

а) Множество $\varphi (J_1)$ содержится в регулярному $\mathcal{F}$ классе (обозначим его как J_2) полугруппы S_2 и $\mathcal{R}$, $\mathcal{L}$, и $\mathcal{H}$ классы полугруппы S_1, приналежащие классу J_1, переводятся в $\mathcal{R}$, $\mathcal{L}$, и $\mathcal{H}$ классы соответственно полугруппы S_2, принадлежащие J_2.

б) Занумеруем для удобства $\mathcal{R}$ и $\mathcal{L}$ классы, которые содержатся в J_2, так, что группа H_{11}, которая принадлежит классу J_1, переходит в группу $\overline{H}_{11}$ из J_2. Пусть теперь

$$C'_1: J_1 \to\to \mathcal{M}^0 (G; A, B; P') — \{0\}$$

и

$$C'_2: J_2 \to\to \mathcal{M}^0 (H; C, D; Q') — \{0\}$$

представляют собой любые координатные отображения для классов J_1 и J_2. Тогда существуют гомоморфизм $\omega : G \to H$ и отображения $\psi_L: A \to C$, $\psi_R: B \to D$, $\lambda : A \to H$, $\delta : B \to H$, такие, что частичный гомоморфизм

$$\theta = C'_2 \varphi C'_1 : \mathcal{M}^0 (G; A, B; P') — \{0\} \to \mathcal{M}^0 (H; C, D; Q') — \{0\}$$

задается соотношением

$$\theta (g,a,b) = (\lambda (a)^{-1} \omega (g) \delta (b)^{-1}, \psi_L (a), \psi_R (b)). \qquad (3.1)$$

Кроме того, если $P' (b, a) \neq 0$, то

$$\theta [\psi_L (a), \psi_R (b)] = \delta (b) \omega [P' (b, a)] \lambda (a). \qquad (3.2)$$

Наоборот, любые функции, которые удовлетворяют соотношениям (3.1) и (3.2), определяют частичный гомоморфизм регулярного $\mathcal{F}$ класса.

в) Пусть J_1— минимальный $\mathcal{F}$ класс, который содержится в $\varphi^{-1}(J_2)$. Тогда $\varphi(J_1) = J_2$ и отображение $\varphi' : J^0{}_1 \to J^0{}_2$ есть эпиморфизм (см. утверждение 11). В этом случае существуют координатные отображения $C_1 : J^0{}_1 \to\to \mathcal{M}^0(G; A, B; P)$ и $C_2 : J^0{}_2 \to\to \mathcal{M}^0(H; C, D; Q')$ для $J^0{}_1$ и $J^0{}_2$, такие, что эпиморфизм $\theta' = C_2 \varphi' C^{-1}{}_1$ задается соотношением

$$\theta'(g,a,b) = (\omega(g), \psi_L(a), \psi_R(b)),$$
$$\theta'(0) = 0, \qquad (3.3)$$

где ω, ψ_L, ψ_R определены в пункте б) и есть эпиморфными отображениями. Кроме того,

$$Q[\psi_L(a), \psi_R(b)] = \begin{cases} \omega[P(b,a)], & \text{если } P(b,a) \neq 0, \\ 0, & \text{если } P(b,a) = 0. \end{cases} \qquad (3.4)$$

Наоборот, любые функции, которые удовлетворяют соотношениям (3.3) и (3.4), определяют эпиморфизм регулярной рисовской полугруппы матричного типа.

Доказательство. а) Пусть элементы $s_1, s_2 \in J_1$. Предположим, что класс J_1 регулярный, тогда по теореме Риса мы можем найти такие элементы $x, y, z, w \in J_1$, что $xs_1y = s_2$ и $zs_2w = s_1$. Так как φ — частичный гомоморфизм, имеем $\varphi(x)\varphi(s_1)\varphi(y) = \varphi(s_2)$ и $\varphi(z)\varphi(s_2)\varphi(w) = \varphi(s_1)$, поэтому $\varphi(s_1)\mathcal{F}\varphi(s_2)$ и все элементы множества $\varphi(J_1)$ будут $\mathcal{F}$-эквивалентны.

Доказательство пункта а) завершается точно такими же рассуждениями.

б) Пусть θ — частичный гомоморфизм. Определим отображение ψ_L и ψ_R, полагая $\varphi(H_{ab}) \subseteq \overbrace{H}_{\psi_L(a)\varphi_R(b)}$. В силу пункта а) они определены корректно. Определим отображение

$$\gamma : \mathcal{M}^0(G; A, B; P') — \{0\} \to H$$

с помощью соотношения

$$\theta(g,a,b) = (\gamma(g\,a,b), \psi_L(a), \psi_R(b)).$$

$\mathcal{H}$ класс H_{ab} рисовской полугруппы матричного типа содержит идемпотент тогда и только тогда, когда $P'(b, a) \neq 0$, и так как $\mathcal{H}$ класс имеет самое большее один идемпотент, все ненулевые идемпотенты рисовской полугруппы матричного типа записываются в виде $(P'(b,a)^{-1}, a, b)$.

Пусть теперь элемент $(g_0, a_0, b_0) \in \mathcal{M}^0(G; A, B; P') — \{0\}$ будет идемпотентом [он существует, так как полугруппа $\mathcal{M}^0(G; A, B; P')$ регулярна]. Следовательно, $g_0 = P'(b_0,a_0)^{-1}$. Пусть $(g, a, b) \in \mathcal{M}^0(G; A, B; P') — \{0\}$. Тогда элемент (g, a, b) можно

представить в виде $(g, a, b) = (g_0, a, b_0)\ (gg_0, a_0, b_0)\ (1, a_0, b)$. Поскольку φ - гомоморфизм, получаем соотношение

$$\gamma\ (g, a, b) = \gamma\ (g_0, a, b_0)\ h_0\ \gamma\ (gg_0, a_0, b_0)\ h_0\ \gamma\ (1, a_0, b),$$

где элемент $h_0 = Q'[\psi_R(b_0), \psi_L\ (a_0)]$ не равен нулю, так как θ - частичный гомоморфизм.

Положим

$\omega(g) = h_0\ \gamma\ (gg_0, a_0, b_0)$, $\lambda\ (a)^{-1} = \gamma\ (g_0, a, b_0)$ и $\delta\ (b)^{-1}$— $h_0\ \gamma\ (1, a_0, b)$.

Легко проверить, что ω — гомоморфизм. Следовательно, соотношение (3.1) выполняется. Для того чтобы проверить соотношение (3.2), предположим, что $P'\ (b, a) \neq 0$, и рассмотрим идемпотент $\theta(P'\ (b, a)^{-1}, a, b)$:

$$\theta(P'\ (b, a)^{-1}, a, b) = (\gamma\ (P'\ (b, a)^{-1}, a, b),\ \psi_L\ (a),\ \psi_R(b)) =$$
$$= (\lambda\ (a)^{-1}\ \omega\ [P'(b, a)^{-1}],\ \delta\ (b)^{-1},\ \psi_L\ (a),\ \psi_R(b)).$$

Но поскольку образом идемпотента относительно частичного гомоморфизма снова будет идемпотент, мы получим

$$\gamma\ (P'\ (b, a)^{-1}, a, b) = Q'[\psi_R(b), \psi_L(a)]^{-1}.$$

Следовательно, соотношение (3.2) выполняется.

Обратное утверждение очевидно и поэтому пункт б) доказан полностью.

в) Пусть класс J_1 удовлетворяет условию пункта в) и все отображения выбраны, как в пункте б). Тогда отображение

$$\theta = C'_2 \varphi C'^{-1}_1 : \mathcal{M}^0\ (G; A, B; P') \rightarrow\rightarrow \mathcal{M}^0\ (H; C, D; Q')$$

представляет собой гомоморфизм, который удовлетворяет соотношению (3.1), а также соотношению (3.2) даже в том случае, когда $P'(b, a)=0$, т.е.

$$Q'\ (\psi_L\ (a),\ \psi_R\ (b)) = \begin{cases} \delta(b)\omega[P'(b,a)]\lambda(a), & \text{если } P'(b,a) \neq 0, \\ 0, & \text{если } P'(b,a) = 0. \end{cases}$$

Для того чтобы убедиться в этом, вычислим обе части соотношения

$$\theta\ [(1, 1, b) \bullet (1, a, 1)] = [\theta\ (1, 1, b)] \bullet [\theta\ (1, a, 1)]$$

при помощи выражения (3.1).

Для каждого элемента $c \in \psi_L(A)$ и $d \in \psi_R(B)$ выберем представителя $\bar{c} \in \psi_L^{-1}(c) \subseteq A$ и $d' \in \psi_R^{-1}(d) \subseteq B$ соответственно. Кроме того, для $a \in A$, $b \in B$ пусть $\bar{a} = \overline{\psi_L(a)}$ и $\bar{b} = \overline{\psi_R(b)}$) соответственно.

Докажем теперь, что для каждого элемента $a \in A$ существует элемент $g_a \in G$, такой, что $\lambda\ (a)\omega$ с $(g_a)\ \lambda\ (\bar{a})$. Для каждого элемента $a \in A$ существует элемент $b \in B$, такой, что $P'(b, a) \neq 0$ в силу регулярности. Теперь $\psi_L\ (a) = \psi_L\ (\bar{a})$, так что

$\omega\,[P'(b, a)]\,\lambda(a) = \delta(b)^{-1}\,Q'\,[\psi_R(b), \psi_L(a)] = \delta(b)^{-1}\,Q'\,[\psi_R(b), \psi_L(\bar{a})] =$
$= \omega\,[P'(b, \bar{a})]\,\lambda(\bar{a})$. (3.5)

Следовательно,

$$\lambda(a) = \omega\,[P'(b, a)^{-1}\,P'(b, \bar{a})]\,\lambda(\bar{a}).$$

и потому положим $g_a = P'(b, a)^{-1}\,P'(b, \bar{a})$.

Аналогичным образом для каждого элемента $b \in B$ существует элемент $g_b \in G$, такой, что $\delta(b) = \delta(\bar{b})\,\omega(g_b)$.

Определим теперь изоморфизм i: $\mathcal{M}^0(G; A, B; P') \to\to \mathcal{M}^0(G; A, B; P)$ с помощью соотношений $i(0) = 0$, $i(g, a, b) = (g_a^{-1} g g_b^{-1}, a, b)$ и полагая $P(b, a) = g_b P'(b, a)\,g_a$ (см. утверждение 8). Тогда $C_1 \equiv iC'_1$ есть координатное отображение для полугруппы S.

Определим изоморфизм $j : \mathcal{M}^0(H; C, D; Q') \to\to \mathcal{M}^0(H; C, D; Q)$ с помощью соотношений $j(0) = 0$, $j(h, c, d) = (\lambda(\bar{c})\,h\,\delta(\bar{d}), c, d)$ и полагая $Q(d, c) = \delta(\bar{d})^{-1} Q'(d, c)\,\lambda(\bar{c})^{-1}$. Тогда $C_2 = jC'_2$ будет координатным отображением для T.

Легко проверить, что $\theta' = C'_2 \varphi C'^{-1}_1$ удовлетворяет соотношениям (3.3) и (3.4). Обратное утверждение очевидно.

Замечание 11. Из упрощения, полученного в пункте в) предыдущего предложения, следует, что $\mathcal{H}$ классы, которые принадлежат J_1, должны отображаться на $\mathcal{H}$ классы, которые принадлежат J_2, всякий раз, когда класс J_2 регулярный и класс J_1 — единственный минимальный член для $\varphi^{-1}(J_2)$. Тем самым дополнен пункт г) утверждения 11.

Было бы очень хорошо, если бы такое же утверждение удалось получить для частичных гомоморфизмов регулярных $\mathcal{F}$ классов. Доказательство пункта в) не переносится на частичные гомоморфизмы, поскольку не удается воспользоваться соотношением (3.5). Если бы упрощение было возможно, из него бы следовало, что два различных $\mathcal{H}$ класса из J_1, которые отображаются в один и тот же $\mathcal{H}$ класс из J_2, должны иметь одинаковые образы. Следующий пример показывает, что это может не выполняться.

Пусть $Z_2 = \{1, -1\}$ — мультипликативная группа второго порядка.

$$\text{Пусть } J_1 = \mathcal{M}^0\left(Z_1;\ \{1, 2\}, \{1, 2\}; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) — \{0\}.$$

Определим ω: $Z_2 \to Z_2$, полагая $\omega(z) = 1$ для всех $x \in Z_2$. Определим ψ_L, ψ_R,, λ, δ следующим образом:

$$\psi_L(1) = 1,\ \psi_L(2) = 2,\ \psi_R(1) = \psi_R(2) = 1,\ \lambda(1) = -1,$$
$$\lambda(2) = -1 \text{ и } \delta(1) = 1,\ \delta(2) = -1.$$

Теперь $P(1, 1) = P(2, 2) = 1$ и $P(1, 2) = P(2, 1) = 0$.
Определим

$$Q(1, 1) = \delta(1)\omega[P(1, 1)]\lambda(1) = -1$$

и

$$Q(1, 2) = \delta(2)\omega[P(2, 2)]\lambda(2) = 1.$$

Тогда пункт б) предложения 1 утверждает, что соотношение

$$\varphi(z, i, j) = (\lambda(i)^{-1}\omega(z)\delta(j)^{-1}, \psi_L(i), \psi_R(j))$$

определяет частичный гомоморфизм класса J_1 на $\mathcal{M}^0(Z_2;\{1,2\},\{1\}:Q)-\{0\}$.
Теперь $\varphi(H_{11}) \subseteq \overline{H}_{11}$ и $\varphi(H_{12}) \subseteq \overline{H}_{11}$, но $\varphi(H_{11}) = \{(-1, 1, 1)\}$ и $\varphi(H_{12}) = \{(1, 1, 1)\}$. Следовательно, $\varphi(H_{11}) \neq \varphi(H_{12})$. Таким образом, частичные гомоморфизмы нельзя в общем случае свести к виду, определяемлму соотношением (3.3).

Далее мы вводим важный объект, группу Щютценберже, которая позволит нам (помимо всего прочего) распространить идею координатного отображения на нулевые $\mathcal{F}$ классы и, следовательно, на все $\mathcal{F}$ классы. Тогда мы получим описание гомоморфних образов нулевых $\mathcal{F}$ классов в форме, аналогичной предложению 1.

Пусть H представляет собой $\mathcal{H}$ класс полугруппы S. Тогда мы сделаем следующее:

1) сопоставим классу H группу $\mathcal{G}(H)$, называемую группой Щютценберже класса H;

2) $\mathcal{G}(H)$ зависит в действительности только от $\mathcal{F}$ класса, которому принадлежит H;

3) если H — группа, то $H \cong \mathcal{G}(H)$.

Определение 9. Пусть S — полугруппа, а X и T — непустые подмножества моноида S^1. Тогда *правый идеализатор, левый идеализатор и идеализатор* множества X в T определяются соответственно как

$$RI_T(X) = \{t \in T^1 : Xt \subseteq X\},$$
$$LI_T(X) = \{t \in T^1 : tX \subseteq X\},$$
$$I_T(X) = RI_T(X) \cap LI_T(X).$$

Мы будем писать $RI(X)$, $LI(X)$ и $I(X)$, если $T = S$. Множества $RI(X)$, $LI(X)$ и $I(X)$ есть подполугруппы полугруппы S.

Определим гомоморфизмы $M^R_X : RI(X) \to F_R(X)$ и $M^L_X : LI(X) \to F_L(X)$, переводящие t в $(x \to xt)$ и в $(x \to tx)$ соответственно.

Предложение 2 (Щютценберже). Пусть H представляет собой $\mathcal{H}$ класс полугруппы S.

а) Множество $M^R_H\,[RI\,(H)] = P$ является регулярной транзитивной группой подстановок множества H [т.е. для всех элементов $h, h' \in H$ существует *единственный* элемент $\pi \in P$, такой, что $(h)\pi = h'$]. Дуальный результат: $M^L_H\,[LI\,(H)] = P'$ есть регулярная транзитивная группа подстановок множества H. Элементы из P и P' коммутируют, т.е. если $\pi \in P$, $\pi' \in P'$, $h \in H$, то $(\pi' h)\pi = \pi'(h\pi)$. Кроме того, если h_0 — фиксированный элемент множества H, то отображение $\pi \to \pi'$ определяет изоморфизм между P и P'. Здесь π' — единственный элемент множества P', такой, что $(h_0)\,\pi = \pi'(h_0)$.

б) Мы можем определить на множестве H строение группы следующим образом. Выберем фиксированную базисную точку $h_0 \in H$ и для элементов $h_1, h_2 \in H$ пусть π_1, π_2 — такие единственные элементы из P, что $(h_0)\,\pi_1 = h_1$ и $(h_0)\,\pi_1 = h_2$. Положим $h_1 * h_2 = (h_0)\pi_1\pi_2$. Тогда $(H, *)$ будет группой, которая не зависит (с точностью до изоморфизма) от выбора элемента (h_0). Множество P как подгруппа полугруппы $F_R(H)$ будет изоморфна правому регулярному представлению группы $(H, *)$.

в) Можно определить групповую структуру $(H, \odot)$ на H двойственным образом, используя P'. Тогда P' как подгруппа полугруппы $F_L(H)$ будет изоморфна левому регулярному представлению $(H, \odot)$.

г) Если H — группа (в полугруппе), то $H \cong (H, *) \cong (H, \odot)$, где базисная точка выбирается как единица в H.

д) Обозначим абстрактную группу $(H, *) \cong P \cong P' \cong (H, \odot)$ как $\mathcal{G}(H)$ и назовем ее *группой Шютценберже класса* H. Если H и H' — два $\mathcal{H}$ класса, которые принадлежат одному $\mathcal{F}$ классу J, то $\mathcal{G}(H) \cong \mathcal{G}(H')$. Следовательно, мы также обозначаем эту группу как $\mathcal{G}(J)$.

Доказательство. а) Множество P есть подполугруппа в $F'(H)$, так как P емть образ относительно гомоморфизма полугруппы $RI(H)$. Из пункта д) утверждения 5 следует, что каждый элемент из P является подстановкой класса H, поэтому $P \subseteq SYM_R(H)$ и, следовательно, согласно пункту б) утверждения 10 из микромодуля 7 является подгруппой. То, что P транзитивна, следует из определения отношения $\mathcal{H}$. Перейдем к доказательству единичности. Предположим, что для некоторого элемента $h \in H$ $h\pi_1 = h\pi_2$. Пусть h' — произвольный элемент из H. Тогда существует элемент $s \in S^1$, такой, что $h' = sh$. Следовательно, $h'\pi_1 = sh\pi_1 = sh\pi_2 = h'\pi_2$, поэтому $\pi_1 = \pi_2$.

К множеству $M^L_H[LI(H)] = P'$ применяются двойственные (дуальные) рассуждения. Для того чтобы показать, что P и P' коммутируют, предположим, что $\pi \in P$ и $\pi' \in P'$. Пусть $s \in RI\,(H)$, $s' \in (H)$, такие,

что M^R_H $(s)=\pi$ и M^L_H $\pi(s')=\pi'$ соответственно. Тогда в силу ассоциативности полугруппового умножения получаем

$$(\pi' h)\,\pi = (s' h)\,s = s'\,(hs) = \pi'\,(h\pi).$$

Наконец, отображение $\pi \rightarrow \pi'$ является взаимно однозначным и эпиморфным. Пусть $\pi_1, \pi_2 \in \Gamma$. Тогда

$$(\pi_1\pi_2)'h_0 = h_0\,(\pi_1\pi_2) = (h_0\,\pi_1)\,\pi_2 = (\pi'_1\,h_0)\,\pi_2 = \pi'_1\,(h_0\pi_2) = (\pi'_1\,\pi'_2)\,h_0.$$

Следовательно, отображение является изоморфизмом.

Пункты б)-г) оставляем читателю как упражнения.

д) Предположим, что $a \mathcal{L} b$. Тогда $RI(Ha)=RI(H_b)$. Определим отображение $\psi : \mathcal{G}(Ha) \rightarrow\rightarrow \mathcal{G}(H_b)$, полагая $\psi(\pi) = M^R{}_{H_b}(\overline{\pi})$, где $\overline{\pi}$ есть представитель из $M^{R^{-1}}{}_{H_a}(\pi) \subseteq RI(H_a)$. Легко проверить, что отображение ψ — изоморфизм, поэтому $\mathcal{G}(H_a) \cong \mathcal{G}(H_b)$. Дуальное соотношение — bRc, тогда $\mathcal{G}(H_b) \cong \mathcal{G}(H_c)$. Следовательно, если $a \mathcal{F} c$, то $\mathcal{G}(H_a) \cong \mathcal{G}(H_c)$. Доказательство закончено.

Определение 10. Пусть множество J является $\mathcal{F}$ классом полугруппы S. Как и раньше, $R_1, \ldots, R_m$ и $L_1, \ldots, L_n$ обозначают соответственно $\mathcal{R}$ и $\mathcal{L}$ классы полугруппы S, принадлежащие классу J. Пусть $\{H_{ij} = R_i \square L_j\}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$ есть $\mathcal{H}$ классы полугруппы S, которые принадлежат J. Предположим, что h_0 — фиксированный элемент из класса H_{11}. Для номеров $i = 1,\ldots,m$; $j = 1,\ldots,n$ выберем элементы $l_i, r_i \in S^1$, такие, что $h_0 r_i \in H_{1i}$ и $l_i\, h_0 \in H_{i1}$ (элементы l_i и r_i могут не принадлежать множеству J). Для удобства будем считать, что $l_1=r_1=1$. Тогда согласно утверждению 5 соответствие $h \rightarrow l_i h r_j$ определяет взаимно однозначное соответствие H_{11} в H_{ij}. Но для каждого элемента $h \in H_{11}$ существует единственный элемент $\pi \in P \cong \mathcal{G}(J)$, такой, что $h=h_0\pi$. Следовательно, при заданных элементах l_i и r_j каждый элемент $s \in J$ единственным образом представляется в виде $s= l_i\,(h_0\pi)\,r_j \in H_{ij}$. Взаимно однозначное эпиморфное отображение

$$C: J \rightarrow\rightarrow \mathcal{G}(J) \times \{1,\ldots,m\} \times \{1,\ldots,n\},$$

определеняемое как $C\,[l_i\,(h_0\pi)\,r_j] = (\pi, i, j)$, называется *координатным отображением для J*. Каждый выбор элементов l_i и r_j определяет координатное отображение для J.

Если класс J регулярный, выбранный класс H_{11} будет группой и выбранный элемент h_0 будет единицей группы H_{11}, то данное здесь определение координатных отображений совпадает с введенными ранее определениями.

Координатные отображения для J распространяются на J^0, если считать, что нуль переходит в нуль, добавленный к области значений.

Если класс J регулярный, то эти расширения будут, конечно, координатными отображениями для 0-простой полугруппы J^0. Если класс J нулевой, то образы расширений можно рассматривать как (нерегулярную) рисовскую полугруппу матричного типа, $\mathcal{M}^0$ ($\mathcal{G}$ (J); {1, ..., m}; P), где $P(j, i) = 0$ для всех i, j.

Мы вернемся теперь к ситуации, которая описана в утверждении 11.

Утверждение 12. а) Пусть J_1 — нулевой $\mathcal{F}$ класс полугруппы S_1, содержийся в прообразе $\varphi^{-1}(J_2)$. Тогда существуют координатные отображения $C_1 : J_1 \to\to \mathcal{G}(J_1) \times A \times B$ и $C_2 : J_2 \to\to \mathcal{G}(J_2) \times C \times D$, такие, что $\theta = C_2 \varphi C_1^{-1}$ задается соотношением

$$\theta(g,a,b) = (\lambda(a)\omega(g)\delta(b), \psi_L(a), \psi_R(b)) \qquad (3.6)$$

где ω: $\mathcal{G}(J_1) \to \mathcal{G}(J_1)$ есть гомоморфизм, а $\psi_L : A \to C$, ψ_R: $B \to D$, $\lambda : A \to \mathcal{G}(J_2)$ и $\delta : B \to \mathcal{G}(J_2)$ — отображения.

б) Пусть J_1 — минимальный класс в $\varphi^{-1}(J_2)$. Тогда $\varphi(J_1) = J_2$ и каждый $\mathcal{L}$ и $\mathcal{R}$ классы, которые принадлежат J_1, отображаются на $\mathcal{L}$ и $\mathcal{R}$ классы соответственно, принадлежащие классу J_2 (утверждение 11). Следовательно, для каждого $c \in C$ имеем

$$\mathcal{G}(J_2) = \lambda[\psi_L^{-1}(c)]\,\omega[\mathcal{G}(J_1)]$$

и для каждого $d \in D$ имеем

$$\mathcal{G}(J_2) = \omega[\mathcal{G}(J_1)]\,\delta[\psi_R^{-1}(d)]$$

Доказательство. а) Как и в предложении 1, перенумеруем $\mathcal{R}$ и $\mathcal{L}$ классы, которые принадлежат J_2, так, что $\varphi(H_{11}) \subseteq \overline{H}_{11}$. Выберем базисный элемент $h_0 \in H_{11}$, пусть C_1 — любое координатное отображение для класса J_1, которое определяется соотношением $C_1[l_a (h_0\pi) r_b] = (\pi, a, b)$, где $\pi \in P \cong \mathcal{G}(J_1)$. Пусть C_2 — любое координатное отображение для класса J_2, которое определяется соотношением $C_2(x_c[\varphi(h_0) q] y_d) = (q, c, d)$, где $q \in Q \cong \mathcal{G}(J_2)$.

Обозначение. Пусть $\pi' \in P' \subseteq F_L(H_{11})$ — такой единственный элемент, что $\pi'(h_0) = (h_0)\pi$, $\pi \in P \subseteq F_R(H_{11})$ [см. пункт а) предложения 2]. Аналогично пусть q' — такой единственный элемент в Q', что $q'\varphi(h_0) = \varphi(h_0) q$. Пусть $\overline{\pi}$ — любой элемент из $RI(H_{11})$, такой, что $M^R{}_{H_{11}}(\overline{\pi}) = \pi$, т.е. $(h_0)\pi = h_0\overline{\pi}$. Аналогичные обозначения используются для π', q, q'.

Определим отображение $\omega : P \to Q$ следующим образом. Пусть $\pi \in P$, тогда определим $\omega(\pi)$ как такой единственный элемент из Q, что $\varphi(h_0\pi) = \varphi(h_0)\,\omega(\pi)$. Покажем, что ω — гомоморфизм, пусть $\pi_1, \pi_2 \in \Gamma$. Тогда

$$\varphi(h_0)\,\omega(\pi_1\pi_2)=\varphi[h_0(\pi_1\pi_2)]=\varphi[(h_0\pi_1)\pi_2]=$$
$$\varphi[\pi_1'(h_0\pi_2)]=\varphi(\overline{\pi}_1')\,\varphi(h_0\pi_2)=\varphi(\overline{\pi}_1')\,\varphi(h_0)\,\omega(\pi_2)=$$
$$\varphi(\pi_1' h_0)\,\omega(\pi_2)=\varphi(h_0\pi_1)\,\omega(\pi_2)=\varphi(h_0)\,[\omega(\pi_1)\,\omega(\pi_2)].$$

Учитывая единственноть представления, получаем, что отображение ω является гомоморфизмом.

Определим ψ_L и ψ_R, полагая, как и в предложении 1, $\varphi(H_{ab})\subseteq \overline{H}_{\psi_L(a)\psi_R(b)}$. Определим отображение λ: $A\to Q$, полагая, что оно описывает $\varphi(l_a h_0)$ для каждого элемента $a\in A$, т.е. $\varphi(l_a h_0)\in \overline{H}_{\psi_L(a)1}$, пусть тогда $\lambda(a)\in Q$ — единственный элемент, такой, что $\varphi(l_a h_0)= x_{\psi_L(a)}[\varphi(h_0)\,\lambda(a)]$. (Напомним, что согласно выбору $l_1,r_1,x_1,y_1=1$). Аналогично определяем отображение $\delta: B\to Q$, полагая $\varphi(h_0 r_b)=[\varphi(h_0)\,\delta(b)]\,y_{\psi_R(b)}$.

Пусть $s=l_a(h_0\pi)\,r_b\in J_1$. Тогда

$$\varphi(s)=\varphi(l_a)\,\varphi(h_0\pi)\,\varphi(r_b)=\varphi(l_a)\,[\varphi(h_0)\,\omega(\pi)]\,\varphi(r_b)$$
$$=\varphi(l_a h_0)\,\overline{\omega(\pi)}\,\varphi(r_b)=x_{\psi_L(a)}[\varphi(h_0)\,\lambda(a)]\,\overline{\omega(\pi)}\,\varphi(r_b)$$
$$=x_{\psi_L(a)}(\varphi(h_0)\,[\lambda(a)\,\omega(\pi)])\,\varphi(r_b)=x_{\omega_L(a)}([\lambda(a)\,\omega(\pi)]'\,\varphi(h_0))\,\varphi(r_b)$$
$$=x_{\psi_L(a)}\,\overline{[\lambda(a)\,\omega(\pi)]'}\,[\varphi(h_0)\,\delta(b)]\,y_{\psi_R(b)}$$
$$=x_{\psi_L(a)}(\varphi(h_0)\,[\lambda(a)\,\omega(\pi)\,\delta(b)])\,y_{\psi_R(b)}.$$

Следовательно, отображение $\theta=C_2\,\varphi\,C_1^{-1}$ имеет требуемый вид.

б) Так как каждый $\mathcal{R}$ класс, который принадлежит J_1, отображается на $\mathcal{R}$ класс, который принадлежит J_2, имеем $\varphi(R_1)=\overline{R}_1$. Рассмотрим в R_1 прообраз произвольного $\mathcal{H}$ класса, который принадлежит $\overline{R}_1$, например $\overline{H}_{1d}$. Этот прообраз является объединением $\mathcal{H}$ классов, которые принадлежат R_1, пусть он имеет вид $\square\{H_{1b}: b\in \psi_R^{-1}(d)\}$. Образ каждого $\mathcal{H}$ класса в этом множестве есть

$$\varphi(H_{1b})=\varphi[\mathcal{G}(J_1),\ 1,\ b]$$
$$=(\lambda(1)\,\omega[\mathcal{G}(J_1)]\,\delta(b),\ 1,\ d)$$

для всех $b\in \psi_R^{-1}(d)$. Но по предположению $\lambda(1)=1$- единица группы

$\mathcal{G}(J_2)$. Тогда, поскольку множество $\square\{H_{1b} : b \in \psi_R^{-1}(d)\}$ отображается на $\overline{H}_{1d}$, получаем, что

$$\cup\{\omega[\mathcal{G}(J_1)]\,\delta(b) : b \in \psi_R^{-1}(d)\} = \mathcal{G}(J_2).$$

Так как $\mathcal{G}(J_2)$ есть группа, это эквивалентно соотношению

$$\mathcal{G}(J_2) = \omega[\mathcal{G}(J_1)]\,\delta[\psi_R^{-1}(d)].$$

Посредством аналогичных рассуждений в дуальном случае доказывают оставшуюся часть утверждения.

Замечание 12. Следующий пример показывает, что в общем случае, если J_1 — минимальный класс в $\varphi^{-1}(J_2)$ (ситуация, которая описана в утверждении 11), то $\mathcal{H}$ классы полугруппы S_1, принадлежащие J_1, не обязательно отображаются на $\mathcal{H}$ классы полугруппы S_2, принадлежщие J_2.

Пусть G — группа, H — подгруппа, $\overline{x}_1,\ldots,\overline{x}_n$ — множество представителей смежных классов $\{gH : g \in G\}$ и $\overline{y}_1,\ldots,\overline{y}_n$ — множество представителей смежных классов $\{Hg : g \in G\}$. Пусть A и B — конечные множества. Символ R обозначает множество вида $\{0\} \cup (A \times \{\overline{x}_1,\ldots,\overline{x}_n\} \times H \times \{\overline{y}_1,\ldots,\overline{y}_n\} \times B)$ и V — множество вида $(A \times G \times B) \cup \{0\}$. Символ T обозначает группу $\mathrm{SYM}_L(A) \times G \times \mathrm{SYM}_R(B)$. Пусть S_1 — полугруппа, которая состоит из элементов дизъюнктивного объединения $T \cup R$, где T — подгруппа, R — нулевая подполугруппа, 0 — элемент из S_1. Если $(f_1, g, f_2) \in T$ и $(a, \overline{x}_k, h, \overline{y}_j, b) \in R - \{0\}$, то

$$(f_1, g, f_2)\cdot(a, \overline{x}_k, h, \overline{y}_j, b) = (f_1(a), \overline{x}_{k'}, h'h, \overline{y}_j, b)$$

и

$$(a, \overline{x}_k, h, \overline{y}_j, b)\cdot(f_1, g, f_2) = (a, \overline{x}_k, hh^*, \overline{y}_{j'}, f_2(b)),$$

где элементы h', h^*, $\overline{x}_k$, $\overline{y}_j$ определяются соотношениями $g\,\overline{x}_k = \overline{x}_{k'}h'$ и $\overline{y}_j g = h^*\overline{y}_{j'}$. Пусть S_2 — полугруппа, которая состоит из элементов дизъюнктивного объединения $T \cup V$, где T — подгруппа, V — нулевая подполугруппа, 0 — нулевой элемент из S_2. Если $(f_1, g, f_2) \in T$ и $(a, g') \in V - \{0\}$, то

$$(f_1, g, f_2)\cdot(a, g', b) = (f_1(a), gg', b)$$

и

$$(a, g', b)\cdot(f_1, g, f_2) = (a, g'g, f_2(b)).$$

Два элемента из R (соответственно из V) будут H-эквивалентны в S_1 (соответственно в S_2) тогда и только тогда, когда все их координаты, кроме центральной, т.е. H (соответственно G), согласуются. Пусть φ: $S_1 \longrightarrow S_2$ определяется следующим образом: на T отображение φ является тождественным, $\varphi(0) = 0$ и $\varphi(a, \overline{x}_k, h, \overline{y}_j, b) = (a, \overline{x}_k\, h\, \overline{y}_j, b)$. Очевидно, что отображение φ — эпиморфизм, но φ переводит каждый $\mathcal{H}$ класс полугруппы S_1, на $\mathcal{H}$ класс полугруппы S_2 тогда и только тогда, когда $H = G$.

Отметим, что законы умножения для только что определенных полугрупп S_1 и S_2 должны быть проверены на ассоциативность. Далее в замечании 14 предлагается общий способ построения новых полугрупп из имеющихся полугрупп, обобщающий построение, которое проведено для S_1 и S_2.

Мы введем теперь важное множество преобразований полугруппы — переносы.

Определение 11. Пусть S — полугруппа, элемент $\alpha \in F_R(S)$ называется *правым переносом* полугруппы S тогда и только тогда, когда для всех элементов $s_1, s_2 \in S$, $(s_1 s_2)\,\alpha = s_1\,[(s_2)\,\alpha]$. Аналогично элемент $\beta \in F_L(S)$ называется *левым переносом* полугрупп S тогда и только тогда, когда для всех элементов $s_1, s_2 \in S$, $\beta\,(s_1 s_2) = [\beta\,(s_1)]s_2$.

Левый перенос α и правый перенос β называются связанными тогда и только тогда, когда для всех элементов $s_1, s_2 \in S$ существует равенство $(s_1\alpha)\, s_2 = s_1\,(\beta s_2)$.

Легко проверить, что множество правых переносов полугруппы S будет подполугруппой в $F_R(S)$; обозначим полугруппу правых переносов как $RT(S)$. По аналогии полугруппа левых переносов будет обозначаться как $LT(S)$.

Замечание 13. Пусть $s \in S$. Тогда умножение полугруппы S на элемент s справа определяет правый перенос S. В действительности правое регулярное представление $R(S)$ полугруппы S является подполугруппой в $RT(S^1)$. Аналогично $L(S) \subseteq LT(S^1)$.

Если $s \in S$, обозначим определяемые им переносы как $R(s) \in RT(S)$ и $L(s) \in LT(S)$. Эти переносы связаны.

Аналогично тому, как мы изучали вид локальных гомоморфизмов, попробуем теперь определить вид всех правых и левых переносов регулярной рисовской полугруппы матричного типа с помощью картинки Грин-Риса. Для удобства мы обозначим множество, на котором основывается определение рисовской полугруппы матричного типа $\mathcal{M}^0(G; A, B; C)$ как $G^0 \times A^0 \times B^0$ (вместо $(G \times A \times B) \cup \{0\}$) и

отождествим тройку элементов, в которой есть один или более нулей, с нулем множества $(G \times A \times B) \square \{0\}$. Умножение остается согласованным с расширениями $C : B \times A \to G^0$ на $C : B^0 \times A^0 \to G^0$, где

$$C(0, 0) = C(b, 0) = C(0, a) = 0.$$

Утверждение 13. Пусть $M = \mathcal{M}^0(G; A, B; C)$ — регулярная рисовская полугруппа матричного типа.

а) Пусть $\alpha \in RT(M)$. Тогда существуют функции $\psi_R(\alpha) : B^0 \to B^0$ и $\delta(\alpha) : B^0 \to G^0$, такие, что для всех элементов $(g, a, b) \in M$

$$(g, a, b)\,\alpha = (g\delta(\alpha)(b), a, \psi_R(\alpha)(b)). \qquad (3.7)$$

Кроме того, $\psi_R(\alpha)(b) = 0$ тогда и только тогда, когда $\delta(\alpha)(b) = 0$ и $\psi(\alpha)(0)=0$. Наоборот, с помощью любых функций с такими свойствами, основываясь на соотношении (3.7), легко определить правый перенос.

б) Пусть $\beta \in LT(M)$. Тогда существуют функции $\psi_L(\beta) : A^0 \to A^0$ и $\lambda(\beta): A^0 \to G^0$, такие, что для всех элементов $(g, a, b) \in M$

$$\beta(g, a, b) = (\lambda(\beta)(a)\, g, \psi_L(\beta)(a), b). \qquad (3.8)$$

Кроме того, $\psi_L(\beta)(a)=0$ тогда и только тогда, когда $\lambda(\beta)(a)=0$ и $\psi_L(\beta)(0)=0$. Наоборот, с помощью любых функций с такими свойствами, основываясь на соотношении (3.8), легко определить левый перенос.

в) $RT(M)$ и $LT(M)$ коммутируют, т.е. для всех $m \in M$, $\alpha \in RT(M)$ и $\beta \in LT(M)$ выполняется равенство $(\beta m)\,\alpha = \beta(m\alpha)$.

г) Пусть $\alpha \in RT(M)$ и $\beta \in LT(M)$. Переносы α и β будут связаны тогда и только тогда, когда для всех $a \in A$, $b \in B$ выполняется следующее соотношение:

$$\delta(\alpha)(b)\, C[\psi_R(\alpha)(b), a] = C[b, \psi_L(\beta)(a)]\,\lambda(\beta)(a). \qquad (3.9)$$

Доказательство:

а) Пусть $\alpha \in RT(M)$, предположим, что $(g, a, b) \in M$ — ненулевой элемент. Так как M — регулярная подгруппа, существует идемпотент $(g_0, a_0, b) \in M$, такой, что $(g, a, b)(g_0, a_0, b) = (g, a, b)$. Рассмотрим действие переноса α на идемпотент. Или $(g_0, a_0, b)\,\alpha = 0$, или

$$(g'_0, a'_0, b') \equiv (g_0, a_0, b)\,\alpha = (g_0, a_0, b)[(g_0, a_0, b)\,\alpha].$$

Следовательно, $a'_0 = a_0$. Теперь

$$(g, a, b)\,\alpha = (g, a, b)[(g_0, a_0, b)\,\alpha] = \begin{cases} 0 \\ (gg^{-1}{}_0 g'_0, a, b') \end{cases}$$

Определим функцию $\psi_R(\alpha) : B^0 \to B^0$, полагая

$$\psi_R(\alpha)(b) = \begin{cases} 0, & \text{если } (g, a, b)\alpha = 0, \\ b' & \text{в противном случае.} \end{cases}$$

Определим функцию $\delta(\alpha) : B^0 \to G^0$, где

$$\delta(\alpha)(b)=\begin{cases}0, & \text{если } \psi_R(\alpha)(b)=0,\\ g_0^{-1}g_0' & \text{в противном случае.}\end{cases}$$

Легко проверить, что эти функции определены коротко и удовлетворяют соотношению (3.7). Обратное утверждение очевидно.

б) Этот пункт является дуальным к а) и доказывается с помощью двойственных рассуждений.

в) Справедливость утверждения этого пункта вытекает из вида соотношений (3.7) и (3.8).

г) Пусть переносы α и β связаны. Рассмотрим

$$[(g, c, b)\ \alpha]\ (h, a, d) = (g, c, b)\ [\beta\ (h, a, d)].$$

Из левой части соотношения получаем, что

$$[(g, c, b)\ \alpha]\ (h, a, d) = (g\delta\ (\alpha)\ (b)\ C\ [\psi_R(\alpha)\ (b), a]\ h, c, d),$$

в то время как правая часть равна $(g\ C[b,\ \psi_L(\beta)\ (a)]\ \lambda(\beta)(a)h, c, d)$. Следовательно, α и β связаны тогда и только тогда, когда

$$\delta\ (\alpha)\ (b)\ C\ [\psi_R\ (\alpha)\ (b),\ a] = C\ [b,\ \psi_L\ (\beta)\ (a)]\ \lambda\ (\beta)\ (a).$$

Полугруппы *RT (M)* и *LT (M)* можно представить двумя специальными способами. Первый из них представляет *RT (M)* и *LT (M)* как матрицы, мономиальные по строкам, и матрицы, мономиальные по столбцам

Утверждение 14. Пусть $M = \mathcal{M}^0\ (G; A, B; C)$ — регулярная рисовская полугруппа матричного типа и предположим, что $|A| = m$ и $|B| = n$. Тогда:

а) $RT\ (M) \cong \mathcal{RM}(n, G)$ — $n \times n$ матрицы, над G^0 мономиальные по строкам;

б) $LT\ (M) \cong \mathcal{LM}\ (m, G)$ — $m \times m$ матрицы, над G^0 мономиальные по столбцам.

Доказательство. а) Представим каждый ненулевой элемент $(g, a, b) \in M$ как $m \times n$ матрицу с элементом g на пересечении строки a и столбца b и с нулями на всех других местах. Элемент $0 \in M$ представим $m \times n$ матрицей, которая целиком состоит из нулей. Тогда каждый элемент из *RT (M)* легко записать как матрицу, мономиальную по строкам. Действительно пусть $\alpha \in RT\ (M)$, предположим, что $\psi_R\ (\alpha)$ и $\delta(\alpha)$ — функции, определенные в утверждении 13.

Определим $n \times n$ матрицу, мономиальную по строкам, α^*: $B \times B \to G^0$, полагая

$$\alpha^*(b,b') = \begin{cases}\delta(\alpha)(b), & \text{если } b' = \psi_R(\alpha)(b),\\ 0 & \text{в противном случае.}\end{cases}$$

Отображение $\alpha \to \alpha^*$ является изоморфизмом. Пункт б) доказывается с помощью дуальных соображений.

Пусть $\alpha \in RT(M)$. Из соотношения (3.7) вытекает, что действие α на $G^0 \times A^0 \times B^0$ приводится к треугольной форме. Это позволяет надеяться, что $RT(M)$ можно представить в виде узлового произведения.

Утверждение 15. Определим две подполугруппы

$$S = \{f \in F_R(B^0) : f(0) = 0\},$$
$$S' = \{f \in F_L(A^0) : f(0) = 0\}.$$

а) $RT(M)$ изоморфна подполугруппе узлового произведения $(G^0, R(G^0))\mathrm{w}(B^0, S)$;

б) $LT(M)$ изоморфна подполугруппе узлового произведения $(S^r, A^0)\mathrm{w}^*(L(G^0), G^0)$, где символ w* обозначает узловое произведение для полугрупп *левых* преобразований (дуальное понятие к узловому произведению). Отметим, что действие также приводится к треугольному виду для операции w*.

Доказательство. а) $(G^0, R(G^0))\mathrm{w}(B^0, S) \cong (B^0, G^0) \times_Y S$, где $Y : S \to \mathrm{End}_L[F(B^0, G^0)]$ есть гомоморфизм, определяемый следующим образом: пусть $f \in F(B^0, G^0)$, $s \in S$ и $b \in B^0$, тогда $[Y(s)f](b) = f(bs)$.

Пусть $a \in RT(M)$. Тогда отображение

$$\alpha \to (\delta(\alpha), \psi_R(\alpha)) \in F(B^0, G^0) \times_Y S$$

будет взаимно однозначным гомоморфизмом. Проверим это. Пусть $\alpha, \beta \in RT(M)$, тогда

$$(g, a, b)\alpha\beta = (g\delta(\alpha)(b), a, (b)\psi_R(\alpha))\beta$$
$$= (g\delta(\alpha)(b)\delta(\beta)((b)\psi_R(\alpha)), a, (b)\psi_R(\alpha)\psi_R(\beta)).$$

Следовательно, $\alpha\beta \to (\delta(\alpha)Y(\psi_R(\alpha))\delta(\beta), \psi_R(\alpha)\psi_R(\beta))$ и отображение является гомоморфизмом. Так как задание отображений δ и ψ_R полностью определяет правый перенос, отображение будет взаимно однозначным. Пункт б) доказывается посредством дуальных рассуждений.

Замечание 14. В замечании 12 был предложен способ построения из заданных полугрупп некоторых новых полугрупп. Использованный прием оказывается довольно удобным для построения примеров. Пусть T (вершина), B (основание) — две полугруппы и мы хотим сформировать новую полугруппу $(T \square B, \bullet) = S$ (дизъюнктивное объединение), где $t \bullet b \in B$ і $b \bullet t \in B$ для всех элементов $t \in T$, $b \in B$ (следовательно, имеется некоторое описание) и множества T и B— подполугруппы S. Закон умножения в новой полугруппе должен быть ассоциативным, поэтому он должен выполняться для следующих

восьми множеств: 1) *TTT,2) BOB,* 3) *TTB,* 4) *BTT,* 5) *BBT,* 6) *TBB,* 7) *BT B* и 8) *TBT.*

Так как мы требуем, чтобы T и B были подполугруппами полугруппы S, пункты 1 и 2 выполняются. Так как $t \bullet b \in B$ и $b \bullet t \in B$, можно определить функции φ_L: $T \to F_L(B)$ и $\varphi_R : T \to F_R(B)$. Определим тогда $t \bullet b = \varphi_L(t)\, b$ и $b \bullet t = b\, \varphi_R(t)$. Для того чтобы выполнялись пункты 3 и 4, функции φ_L и φ_R должны быть гомоморфизмами. Для выполнения пунктов 5 и 6 мы должны потребовать, чтобы $\varphi_L(T) \subseteq LT(B)$ и $\varphi_R(T) \subseteq RT(B)$. Для выполнения пункта 7 $\varphi_L(t)$ и $\varphi_R(t)$ должны быть связаны при всех $t \in T$, а для выполнения пункта 8 $\varphi_L(T)$ и $\varphi_R(T)$ должны коммутировать.

Если B — полугруппа с нулевым умножением (как в замечании 12), то пункты 5—7 выполняются автоматически. Один со способов удовлетворить пункту 8 заключается в том, чтобы для всех $b \in B$ существовало равенство $\varphi_L(t)b = b\varphi_R(t)$ при всех $t \in T$. Отметим, что в этом случае полугруппы $\varphi_L(T)$ и $\varphi_R(T)$ будут коммутативными.

Определение 12. Совокупность $\mathcal{P}$ конечных полугрупп называется *свойством* конечных полугрупп тогда и только тогда, когда из соотношений $S \in \mathcal{P}$ и $T \cong S$ вытекает, что $T \in \mathcal{P}$. Мы будем говорить, что полугруппа S имеет свойство $\mathcal{P}$, если $S \in \mathcal{P}$. $\mathcal{P}$ называется *локальным* свойством конечных полугрупп тогда и только тогда, когда из условия, что T — конечная полугруппа, каждый главный фактор J^0 которой изоморфен некоторой полугруппе $S \in \mathcal{P}$, вытекает, что $T \in \mathcal{P}$. Например, в силу определения 14 полугруппа S регулярна тогда и только тогда, когда каждый $\mathcal{F}$ класс полугрупп S регулярный. Следовательно, регулярность — локальное свойство.

Конец этого раздела будет посвящен определению и характеристике нескольких важных локальных свойств конечных полугрупп.

Определение 13. Элемент a полугруппы S называется *регулярным.* тогда и только тогда, когда $a \in aSa$, т.е. когда существует такой элемент $b \in S$, что

$$a = aba$$

Утверждение 16. Пусть $a, b \in S$ — регулярные элементы.

а) $L_a \leq L_b$ тогда и только тогда, когда существуют (идемпотентные) элементы $a_1 \in L_a$ и $b_1 \in L_b$, такие, что $a_1 b_1 = a_1$.

б) $R_a \leq R_b$ тогда и только тогда, когда существуют (идемпотентные) элементы $a_1 \in R_a$ и $b_x \in R_b$, такие, что $b_1 a_1 = a_1$.

в) $J_a \leq J_b$ тогда и только тогда, когда существуют (идемпотентные) элементы $a_1 \in J_a$ и $b_1 \in J_b$, такие, что $a_1 b_1 = a_1 = b_1 a_1$ (т.е. $a_1 \leq b_1$, если a_1 и b_1 — идемпотенты).

Доказательство. а) Предположим, что $L_a \le L_b$. Так как элементы a и b регулярные, существуют элементы $x, y \in S^1$, такие, что $a = axa$ и $b = byb$. Отметим, что $xa £ a$ и $yb £ b$. Но поскольку $xa \in L_a \le L_b$, мы получим $xa \in S^1b$.

Положим $xa = sb$. Тогда $(xa)(yb) = sbyb = sb = xa$. (Отметим, что xa и yb — идемпотенты.)

Обратно: если существуют элементы $a_1 \in L_a$ и $b_1 \in L_b$, такие, что $a_1b_1 = a_1$, то $S^1a = S^1a_1 = S^1a_1b_1 \subseteq S^1b_1 = S^1b$, т.е. $L_a \le L_b$. К пункту б) применяем дуальные рассуждения.

в) Предположим, что существуют элементы $a_1 \in J_a$, $b_1 \in J_b$, такие, что $a_1b_1 = a_1 = b_1a_1$. Тогда $S^1a_1S^1 = S^1a_1b_1S^1 \subseteq S^1b_1S^1$, т.е. $J_a \le J_b$. Наоборот, если $J_a \le J_b$, предположим, что $x \in J_a$, $y \in J_b$ — такие элементы, которые $a = axa$ и $b = byb$. Пусть $b_1 = yb$ и $a_2 = xa$. Тогда b_1 и a_2 идемпотенты. Кроме того, $b_1 \in J_b$, $a_2 \in J_a$, т.е. в частности, $a_2 \in J(a) \subseteq J(b) = J(b_1) = S^1b_1S^1$. Пусть $s_1, s_2 \in S^1$ — такие элементы, что $s_1b_1s_2 = a_2$.

Положим $a_1 = b_1s_2a_2s_1b_1$. Тогда a_1 является идемпотентом и $a_2 = s_1a_1s_2$, т.е. $J_a = J_{a_1}$. Наконец, $a_1b_1 = a_1 = b_1a_1$. Утверждение полностью доказано.

Определение 14. Полугруппа S называется *регулярной*, если каждый $\mathcal{F}$ класс J полугруппы S регулярный.

Утверждение 17. а) Полугруппа S регулярна тогда и только тогда, когда регулярен каждый ее элемент.

б) Полугруппа S регулярна тогда и только тогда, когда для всех элементов $a \in S$ класс L_a или (R_a) содержит идемпотент.

в) Полугруппа S регулярна тогда и только тогда, когда $J \subseteq J^2$ для каждого $\mathcal{F}$ класса J из S.

г) Полугруппа S регулярна тогда и только тогда, когда для каждого правого идеала A и левого идеала B $AB = A \cap B$.

д) Если S и T — регулярные полугруппы, то полугруппа $S \times T$ и образ при гомоморфизме полугруппы S будут регулярны. Идеалы полугруппы S — регулярные полугруппы, но правые или левые идеалы (следовательно, и подполугруппы) могут не быть регулярными.

е) Если S — регулярная полугруппа, то каждый ее композиционный ряд является главным рядом.

ж) Каждая полугруппа представляет собой подполугруппу регулярной полугруппы.

Доказательство. а, б) Пусть S — регулярная полугруппа, тогда по теореме Риса каждый элемент полугруппы S будет регулярным. Пусть

$a \in S$, тогда полугруппа J^0_a изоморфна регулярной рисовской полугруппе матричного типа $\mathcal{M}^0(G; A, B; C)$.

Пусть $a = (g)_{ij}$, $i \in A$, $j \in B$, $g \in G$. Существуют элементы $k \in B$ и $l \in A$, такие, что $C(j, k) \neq 0$ и $C(l, i) \neq 0$. Тогда $b = (C(j, k)^{-1} g^{-1} C(l, i)^{-1})_{kl}$ есть такой элемент полугруппы S, что $a = aba$ (и $b = bab$).

Если элемент a регулярный, т.е. $a = aba$ для некоторого элемента b, то $ba \in L_a$ и $ab \in R_a$ — идемпотенты.

Если каждый $\mathcal{L}$ класс и, следовательно, каждый $\mathcal{F}$ класс содержит идемпотент, то не существует нулевых $\mathcal{F}$ классов в полугруппе S. Следовательно, S регулярная. Это доказывают пункты а) и б).

в) Предположим, что S — регулярная полугруппа и $a \in S$. Тогда $a = aba$ для некоторого элемента b. Так как $a \mathcal{F} ba$, мы имеем $a = aba \in J^2_a$. Следовательно, $J \subseteq J^2$ для всех классов J в полугруппе S. Наоборот, из включение $J \subseteq J^2$ вытекает $(J^0)^2 \neq \{0\}$. Поэтому каждый класс J регулярный.

г) Пусть S — регулярная полугруппа и $x \in A \square B$. Тогда существует элемент $y \in S$, такой, что $xyx = x$. Но из включения $x \in B$ вытекает, что $yx \in B$, т.е. $x = xyx \in AB$ и $AB = A \cap B$. Обратно, если $AB = A \cap B$ для каждого правого идеала A и левого идеала B, то для любого элемента $x \in S$ $x \in x S^1 \cap S^1 x = x S^1 x$, т.е. $x \in xSx$, или $x = x1x = x^2 = x^3 \in xSx$. Это доказывает данный пункт.

д) Свойство $a \in aSa$ сохраняется при гомоморфизмах и взятии конечных прямых произведений. Пусть I — идеал полугруппы S и $a \in I$. Так как S — регулярная полугруппа, существует элемент $b \in S$, такой, что $a = aba$ и $b = bab$. Но тогда $b \in I$, т.е. I — регулярная подполугруппа.

Для того чтобы завершить доказательство данного пункта, заметим, что $B = \{(1, 1, 1), (1, 1, 2), 0\}$ — правый идеал полугруппы $S = S_{22}(\{1\}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$, но последовательность $B \supseteq \{(1, 1, 2), 0\} \supseteq \{0\}$ является главным рядом для B с нулевым вторым фактором, в то время как S — регулярная полугруппа.

е) Пусть I_2 - идеал в I_1 и I_1 — идеал в S. Тогда I_2 - объединение $\mathcal{F}$ классов для I_1, все из которых регулярны согласно пункту д). Тогда согласно пункту в) $I^2_2 = I_2$, т.е. I_2 есть идеал полугруппы S согласно пункту д) утверждения 11.

ж) Полугруппа S изоморфна своему правому регулярному представлению $R(S)$, которое преставляє собой подполугруппу регулярной полугруппы $F_R(S^1)$. Утверждение доказано полностью.

Теперь рассмотрим полугруппы, являющиеся объединением групп.

Определение 15. Говорят, что полугруппа S представляет собой *объединение групп,* если каждый элемент из S принадлежит подгруппе полугруппы S.

Предложение (Клиффорд). Пусть S — полугруппа.

а) Полугруппа S является объединением групп тогда и только тогда, когда каждый $\mathcal{H}$ класс есть группа. Следовательно, S — дизъюнктивное объединение своих максимальных подгрупп.

б) S — объединение групп тогда и только тогда, когда для каждого $\mathcal{F}$ класса J полугруппы S J^0 имеет вид $\mathcal{M}^0$ $(G; A, B; C)$, где C не содержит нулевых элементов. Это эквивалентно свойству, что каждый $\mathcal{F}$ класс полугруппы S — (простая) подполугруппа.

в) S — объединение групп тогда и только тогда, когда для каждых элементов $a, b \in S$, $J(ab) = J(a) \square J(b) = J(ba)$. Следовательно, S — объединение групп, если отображение $s \to J(s)$ является гомоморфизмом S на коммутативную связку $\{J(s) : s \in S\} = B \subseteq (2^S, \cap)$. Прообраз любого $J(s) \in B$ будет простой полугруппой J_s.

г) S — объединение групп тогда и только тогда, когда $\mathcal{F}$ есть конгруэнтность и полугруппа S регулярна.

д) Образы при гомоморфизмах, подполугруппы и конечные прямые произведения полугрупп, являющихся объединением групп, снова будут объединениями групп.

Доказательство. а) Так как каждый элемент $a \in S$ представляет собой элемент подгруппы, то H_a — подгруппа.

б) Доказательство следует из теоремы Риса.

в) Предположим, что S есть объединения групп и $a, b \in S$. Тогда $ab \mathcal{H} (ab)^2 \in SbaS \subseteq J(ba)$, т.е. $ab \in J(ba)$. Следовательно, $J(ab) = J(ba)$. Теперь очевидно, что $J(ab) \subseteq J(a) \cap J(b)$. Пусть $c \in J(a) \cap J(b)$, т.е. для некоторых $u, v, x, y \in S^1$ $c = uav = xby$. Тогда

$$c \mathcal{H} c^2 = xbyuav \in J(byua) — J(uaby) \subseteq J(ab),$$

т.е.

$$c \in J(ab) \text{ и } J(ab) = J(a) \cap J(b).$$

Наоборот, если S удовлетворяет $J(ab) = J(a) \cap J(b)$ для всех элементов $a, b \in S$, то для всех $a, b \in S$ из соотношения $a \mathcal{F} b$ вытекает, что $J(ab) = J(a) \cap J(b) = J(a) = J(b)$, т.е. $\mathcal{F}$ классы полугруппы S — простые полугруппы и S есть объединение групп.

г) Предположим, что S есть объединение групп. Тогда полугруппа S регулярна. Пусть $ab, x \in S$, где $a \mathcal{F} b$. Тогда $J(a) = J(b)$, поэтому

$$J(xa) = J(ax) = J(a) \square J(x) = J(b) \text{ I } J(x) = J(bx) = J(xb),$$

т.е. $ax \mathcal{F} bx$ и $xa \mathcal{F} xb$. Следовательно, $\mathcal{F}$ - отношение конгруэнтности.

Наоборот, предположим, что S — регулярная полугруппа, для которой отношение $\mathcal{F}$ является конгруэнтностью. Пусть $a \in S$ и $e \in J_a$ - такой идемпотент, что $ae = a$. Пусть теперь $b \in S$ — такой элемент, что $b \mathcal{F} a$. Тогда из отношения $b \mathcal{F} e$ вытекает, что $ab \mathcal{F} a$, поскольку $\mathcal{F}$ — конгруэнтность. Следовательно, $\mathcal{F}$ классы полугруппы S — подполугруппы, поэтому S есть объединение групп.

д) Очевидно, что образ гомоморфизма объединения групп снова будет объединением групп.

Перейдем к подполугруппам.

Пусть $T \subseteq S$ — подполугруппа S. Пусть $t \in T$. Тогда t принадлежит подгруппе полугруппы S, поэтому циклическая группа, порожденная элементом t, принадлежит подполугруппе T. Следовательно, T есть объединения групп.

Пусть S и T — объединение групп. Пусть $(a, b) \in S \times T$. Так как a и b принадлежат подгруппам G_a и G_b полугрупп S и T соответственно, то $(a, b) \in G_a \times G_b$ есть подгруппа $S \times T$.

Определение 16. Элемент b полугруппы S называется *инверсным к* элементу $a \in S$, если $a = aba$ и $b = bab$. Отметим, что тогда $d \mathcal{F} b$.

Утверждение 18. а) Из соотношений $a = aba$ и $a \mathcal{F} b$ вытекает, что $b = bab$.

б) Полугруппа S регулярна тогда и только тогда, когда для каждого элемента в S имеется инверсный.

Доказательство. а) Так как $aba = a$ элемент ba будет идемпотентом и $ba \mathcal{F} a$. Но по условию $a \mathcal{F} b$, поэтому $ba \mathcal{F} b$. Тогда согласно пункту в) утверждение 5 $ba \mathcal{R} b$. Теперь если $e \mathcal{R} x$, где e — идемпотент, то $ex = x$. Следовательно, $(ba)\, b = b$.

б) Этот пункт вытекает из теоремы Риса.

Определение 17. Полугруппа S называется *инверсной*, если для каждого элемента $s \in S$ существует единственный инверсный элемент, он обозначается как s^{-1}. T называется *инверсной подполугруппой* полугруппы S, если T — подполугруппа и из включения $x \in T$ вытекает, что $x^{-1} \in T$.

Утверждение 19. а) Полугруппа S будет инверсной тогда и только тогда, когда S регулярна и множество ее идемпотентов $E(S)$ есть коммутативная полугруппа.

б) Полугруппа S инверсна тогда и только тогда, когда ее ядро $K(S)$ является группой и для любого другого $\mathcal{F}$ класса J полугруппы S J^0 имеет вид $\mathcal{M}^0\ (G;\ A,\ A;\ \Delta)$, где Δ есть $|A| \times |A|$ единичная матрица.

в) Гомоморфные образы, инверсные подполугруппы, идеалы и конечные прямые произведения инверсных полугрупп представляют собой инверсные полугруппы. Левые или правые идеалы (следовательно, и подполугруппы) инверсных полугрупп могут не быть инверсными полугруппами.

Доказательство. а) Пусть S — инверсная полугруппа. Тогда S регулярная. Предположим, что $e_1,\ e_2 \in E\ (S)$ и что a — инверсный элемент для e_1e_2. Тогда ae_1 и e_2a также инверсные для $e_1\ e_2$, т.е. $a = ae_1 = e_2a$. Тогда $a^2 = (ae_1)\ (e_2a) = a$, т.е. $a \in E\ (S)$. Следовательно, $a^{-1} = e_1e_2 \in E\ (S)$. Тогда e_2e_1 также будет инверсным для e_1e_2, поэтому $e_1e_2 = e_2e_1$

Наоборот, пусть $x \in S$, где S — регулярная полугруппа. Пусть $y,\ z$ инверсные для элемента x. Тогда, поскольку $E\ (S)$ коммутативная полугруппа,

$$xz,\ xy,\ zx,\ yx \in E\ (S),$$
$$y = yxy = y(xzxzx)y = yxz\ (xz)\ (xy) = yxz\ (xy)\ (xz) =$$
$$= (yx)\ (zx)\ yxz = (zx)\ (yx)\ yxz = zxz = z.$$

Следовательно, инверсный элемент будет единственным.

б) Очевидно, что полугруппа, локальное построение которой удовлетворяет условиям пункта б), инверсная. Наоборот, если J есть $\mathcal{F}$ класс инверсной полугруппы и $J^0 = \mathcal{M}^\circ\ (G;\ A,\ B;\ C)$, то C имеет в точности один ненулевой элемент в каждой строке и в каждом столбце, так как элемент $(g,\ a,\ b)$ имеет в точности один инверсный элемент вида $(g^1,\ a_1,\ b_1)$ для каждой пары ненулевых матричных элементов $C\ (b,\ a_1)$ и $C\ (b_1,\ a)$. Так как $K\ (S)$ — простая полугруппа, из этих условий следует, что $K\ (S)$ имеет только один $\mathcal{H}$ класс и, следовательно, $K\ (S)$ есть группа. Теперь пункт б) следует из утверждения 8.

в) Доказательство этого пункта оставляем читателю как упражнение.

Определение 18. Пусть S — полугруппа, S называется *нильпотентной*, если S содержит нулевой элемент и $S^n = \{0.\}$ для некоторого целого n. Наименьшее такое целое число $cl(S)$ называется *нильпотентным классом* полугруппы S.

Утверждение 20. а) Следующие высказывания эквивалентны:

1) S — нильпотентная полугруппа;

2) S содержит нулевой элемент и каждый, не равный нулю, $\mathcal{F}$ класс полугруппы S — нулевой;

3) $E\ (S) = \{0\}$;

4) для каждого элемента $x \in S$ существует целое число $n(x)$, такое, что $x^{n(x)} = 0$;

5) для каждого идеала I полугруппы S, I и S/I есть нильпотентными.

6) Гомоморфные образы, подполугруппы и конечные прямые произведения нильпотентных полугрупп — нильпотентнные.

в) Пусть S — полугруппа и n — наименьшее целое положительное число, такое, что $S^n=S^{n+1}$. Тогда $S\to\to S/S^n$ есть максимальный нильпотентный гомоморфный образ полугруппы S и $cl\,(S/S^n) = n$.

Доказательство. Пункт б) проверяется очень легко.

а) Легко видеть, что из (1) вытекает (3), из (3) вытекает (4) и из (4) вытекает (3). Для того чтобы доказать, что из (3) вытекает (2), предположим, что $E(S) = \{0\}$ и пусть J будет $\mathcal{F}$ класс, который не равный нулю. Тогда J не содержит идемпотентов, поэтому J^0 не содержит ненулевых идемпотентов. Следовательно, J^0 не является 0-простой, т.е. J — нулевой $\mathcal{F}$ класс.

Для того чтобы доказать, что из (2) вытекает (1), предположим, что каждый не равный нулю $\mathcal{F}$ класс полугруппы S, нулевой. Пусть $0 \in S$. Кроме того, пусть $S = I_0 \supseteq I_1 \supseteq \ldots \supseteq I_n = \{0\}$ есть главный ряд для полугруппы S. Тогда S/I_1— полугруппа с нулевым умножением, поэтому $S^2 \subseteq I_1$. Далее I_1/I_2 — полугруппа с нулевым умножением, поэтому $S^4 \subseteq I_1^2 \subseteq I_2$. Продолжая дальше, мы получим, что $S^{2_n} \subseteq I_n = \{0\}$, поэтому S нильпотентна.

Тот факт, что из (1) вытекает (5), следует из пункта б). Для того чтобы доказать, что из (5) следует (1), предположим, что I и S/I нильпотенты с $n_1 = cl\,(S/I)$ и $n_2 = cl\,(I)$. Тогда $S^{n_1} \subseteq I$, поэтому $S^{n_1 n_2} \subseteq \{0\}$, т.е. S — нильпотентная полугруппа.

в) Для того чтобы показать, что $\eta : S \to\to S/S^n$ есть максимальный нильпотентный образ полугруппы S, положим $\varphi : S \to\to N$, где $N^k = \{0\}$. Пусть $m = \max(n, k)$, тогда $\varphi(S^n)=\varphi(S^m)=N^m=\{0\}$. Пусть отображение $\varphi^* : S/S^n \to\to N$ определяется соотношениями $\varphi^*(0)=0$ и $\varphi^*(s)= \varphi(s)$ для $s \in S — S^n$. Тогда равенство $\varphi^*\eta= \varphi$ доказывает максимальность, $cl\,(S/S^n) = n$ по определению n и cl.

Напомним следующее определение.

Определение 19. Полугруппа S называется *комбинаторной*, если каждая подгруппа полугруппы S имеет порядок 1.

Утверждение 21. а) Полугруппа S комбинаторная тогда и только тогда, когда каждый $\mathcal{H}$ класс полугруппы S содержит в точности один элемент.

б) Гомоморфные образы, подполугруппы, конечные прямые произведения и узловые произведения комбинаторных полугрупп — также комбинаторные полугруппы.

Доказателство. а) Так как любая подгруппа из S содержится в $\mathcal{H}$ классе, из условия на $\mathcal{H}$ классы вытекает комбинаторность полугруппы S. Обратно, если H есть $\mathcal{H}$ класс полугруппы S и $|H| \geq 2$, то группа Щютценберже $\mathcal{G}(H)$ имеет порядок ≥ 2. Но $\mathcal{G}(H)$ есть гомоморфный образ $RI(H) \subseteq S^1$ и в силу пункта в) утверждения 7 существует группа $G \subseteq RI(H)$, такая, что $G \rightarrow\rightarrow \mathcal{G}(H))$. Следовательно, $|G| \geq 2$ и $G \subseteq S^1$. Однако, если $S^1 \neq S$, то подгруппа, которая содержит 1, имеет только один элемент, поэтому в любом случае S содержит нетривиальную подгруппу; получено противоречие.

б) Доказательство этого пункта оставляем читателю как упражнение.

3.5. Подполугруппы

В этом разделе развитый выше аппарат применяется для доказательства некоторых фактов о подполугруппах конечных полугрупп. Все рассматриваемые далее полугруппы предполагаются конечными.

Определение 20. Множество M называется *максимальной собственной подполугруппой* полугруппы S, если M — такая собственная подполугруппа в S, что всякий раз, как $M \subseteq T \subseteq S$ для некоторой подполугруппы T в S, или $M = T$, или $T=S$. M называется *максимальной комбинаторной подполугруппой* полугруппы S, если M — такая комбинаторная подполугруппа, что, когда T является комбинаторной подполугруппой, содержащей M, $T = M$.

Утверждение 22. Пусть C — максимальная комбинаторная подполугруппа полугруппы S. Тогда $I(C)—LI(C)=RI(C)=C$ (см. определение 9).

Доказательство. Из соображений двойственности следует, что достаточно доказать равенство $LI(C)=C$. Предположим, что оно неверно. Тогда в S существует подполугруппа T, минимальная по отношению к свойству $C \subset T \subseteq LI(C)$. Тогда подполугруппа T не будет комбинаторной и C есть максимальный левый идеал полугруппы T.

Пусть $L = T\text{-}C$ будет $\mathcal{L}$ классом полугруппы T. Поскольку T не комбинаторная, L содержит нетривиальную группу. Следовательно,

$\mathcal{F}$ класс полугруппы T, которому принадлежит L, регулярен. Тогда этим $\mathcal{F}$ классом должно быть множество L, так как в противном случае полугруппа C содержала бы нетривиальную группу. Следовательно, L — регулярный $\mathcal{F}$ класс, который содержит единственный $\mathcal{L}$ класс. В силу теоремы Риса L — простая слева полугруппа и $L^2 = L$. Пусть $e \in L$ — идемпотентный элемент. Покажем теперь, что $C \square \{e\}$ — комбинаторная подполугруппа полугруппы T, тем самым будет получено противоречие, так как C — максимальная комбинаторная подполугруппа.

Для того чтобы доказать, что $C \cup \{e\}$ — подполугруппа, достаточно показать (поскольку C есть левый идеал), что $Ce \subseteq C$. Предположим, что $l \in L$, $c \in C$ и что $ce \in L$. Тогда $lce \in L^2 = L$ и мы получаем соотношение

$$S^1LS^1 = S^1lce\,S^1 \subseteq S^1lc\,S^1 \subseteq S^1lS^1 = S^1LS^1.$$

Следовательно, $lc \in L$ это противоречие, так как C — левый идеал. Поэтому $Ce \subseteq C$. Утверждение доказано.

Следующее предложение дает полную классификацию максимальных подполугрупп. Каждая максимальная подполугруппа полугруппы S имеет некоторое естественное представление в координатах Грина — Риса.

Предложение. Пусть M — максимальная подполугруппа конечной полугруппы S. Тогда справедливы следующие утверждения:

а) для некоторого $\mathcal{F}$ - класса $J(M)$ полугруппы S $S — M \subseteq (M)$;

б) M пересекает (пересечение нетривиальное) каждый $\mathcal{H}$ класс полугруппы S или M является объединением $\mathcal{H}$ классов полугруппы S;

в) если класс $J(M)$ нулевой, то $J(M) \cap M = \varnothing$, поэтому $M = S — J(M)$;

г) если $M \cap J(M) \neq \varnothing$ [тогда в силу пункта в) класс $J(M)$ регулярный и полугруппа $J(M)^0$ изоморфна регулярной рисовской полугруппе матричного типа], то в силу пункта б) возможны два случая.

Случай 1. Если M пересекает каждый $\mathcal{H}$ класс полугруппы S, то изоморфизм $j : J(M)^0 \to \mathcal{M}^0(G; A, B; C)$ может быть выбран так, что $j[M \cap J(M)] = G_1 \times A \times B$, где G_1 — максимальная полугруппа группы G. В этом случае $[M \cap J(M)]^0$ будет максимальной подполугруппой полугруппы J^0.

Случай 2. Если M есть объединение $\mathcal{H}$ классов полугруппы $\mathcal{H}$, то изоморфизм $j : J(M)^0 \to \mathcal{M}^0(G; A, B; C)$ может быть выбран так, что $j[M \square J(M)]$ есть дополнение «прямоугольника» $\mathcal{H}$ классов полугруппы $\mathcal{M}^0(G; A, B; C)$. $j[M \cap J(M)]$ представляется только одним из следующих трех выражений:

1) $G \times (A — A') \times B$, A' — собственное непустое подмножество множества A;

2) $G \times A \times (B — B')$, B' — собственное непустое подмножество множества B;

3) $(G \times A \times B) — (G \times A' \times B')$, A', B' - собственные непустые подмножества множества A и B соответственно.

В случае 2 $[M \cap J(M)]^0$ есть максимальная подполугруппа полугруппы $J(M)^0$ тогда и только тогда, когда $j[M \cap J(M)]$ представляется выражением 3.

Доказательство. Начнем из пункта а). Пусть J минимальный среди $\mathcal{F}$ - классов полугруппы S, не содержащихся в M [в обычной упорядоченности $J_1 \le J_2$ тогда и только тогда, когда $S^1 J_1 S^1 \subseteq S^1 J_2 S^1$].

Тогда $M \cup J$ есть подполугруппа в S, содержащая M как собственное подмножество, так что $M \cup J = S$. Следовательно, $S — M \subseteq J \equiv J(M)$.

Рассмотрим пункт б). Пусть $J=J(M)$. Определим M' как объединение всех $\mathcal{H}$ классов, которые пересекают M. Покажем, что M' будет подполугруппой S, содержащей M, и тогда в силу максимальности M или $M' = M$, или $M' = S$. Из первого соотношения следует, что M есть объединение $\mathcal{H}$ классов, второе показывает, что M пересекает каждый $\mathcal{H}$ класс полугруппы S.

Докажем, что M' — подполугруппа. Пусть $h_1, h_2 \in M'$. Если $h_1 h_2 \in M \subseteq M'$, то все сделано, поэтому предположим противное. Тогда $h_1 h_2 \in J$ и по крайней мере один из элементов h_1 или h_2 принадлежит J. По определению множества M' существуют элементы $m_1, m_2 \in M$, такие, что $h_i \mathcal{H} m_i$, $i = 1, 2$. Возможны два случая.

Случай А. Предположим $h_1 \in M$, $h_2 \in J$. Так как (по предположению) $h_1 h_2 \in J'$, умножение слева на элемент h_1 переводит $\mathcal{H}$ класс, который содержит элемент h_2, на $\mathcal{H}$ класс, который содержит элемент $h_1 h_2$. Следовательно, из отношения $h_2 \mathcal{H} m_2$ вытекает, что $h_1 h_2 \mathcal{H} h_1 m_2 \in M$, поэтому $h_1 h_2 \in M'$. (Ситуация, при которой $h_1 \in J$, $h_2 \in M$ доказывается с помощью дуальных рассуждений.)

Случай В. Предположим, что $f_1, h_2 \in J$. Тогда при помощи теоремы Риса получаем, что из $h_i \mathcal{H} m_i$, $i = 1, 2$, вытекает $h_1 h_2 \mathcal{H} m_1 m_2 \in M$, поэтому $h_1 h_2 \in M'$.

Теперь все возможные случаи исследованы и можно сделать вывод, что множество M' есть полугруппа. Пункт б) доказан.

Перейдем к пункту в). Пусть $J = J(M)$, J — нулевой класс и $n_1, n_2 \in J$. Тогда $n_1 = s_1 n_2 s_2$ для некоторых элементов $s_1, s_2 \in S^1$ (по определению отношения $\mathcal{F}$) и $s_1, s_2 \notin J$, так как по определению нулевого класса, произведение двух или более элементов из J принадлежит $S^1 J S^1 — J$. Итак, $s_1, s_2 \in M^1$, поскольку из $n_2 \in M$ вытекает, что $n_1 \in M$. Следовательно, $J \square M = \varnothing$.

В случае 1 (см. пункт г)) предположим, что M пересекает каждый $\mathcal{H}$ класс полугруппы S. Пусть j' обозначает изоморфизм полугруппы J^0 на полугруппу $T = \mathcal{M}^0(G; A, B; C)$. Тогда $T_1 = j'(M \text{ I } J)$ есть подполугруппой в T, пересекающа каждый $\mathcal{H}$ класс

$$H(a, b) = (G, a, b) = \{(g, a, b) : g \in G\}.$$

Пусть

$$T_1 \cap H(a, b) = M(a, b) = (X(a, b), a, b) = \{(x, a, b) : x \in X(a, b) \subseteq G\}.$$

Предположим теперь, что $H(a_0, b_0)$ — фиксированный не равный нулю $\mathcal{H}$ класс в T, для которого $g_0 = C(b_0, a_0) \neq 0$, т.е. $H(a_0, b_0)$ есть подполугруппа в T, которая изоморфна G. Изоморфизм устанавливается отображением $(g, a_0, b_0) \to g_0 g$. Тогда $X(a_0, b_0) = \{g_0^{-1} g : g \in G_1\} = g_0^{-1} G_1$ для некоторой подгруппы G_1 группы G, так как $M(a_0, b_0)$ есть подгруппа из T, содержащаяся в $H(a_0, b_0)$. Пусть для каждого $a \in A$, g_a— фиксированный элемент из $X(a, b_0)$, а для каждого $b \in B$, y_b— фиксированный элемент из $X(a_0, b)$. Тогда

$$(g_a, a, b_0) M(a_0, b_0) (y_b, a_0, b) = (g_a G_1 g_0 y_b, a, b) \subseteq M(a, b) = (X(a, b), a, b).$$

Но согласно аналогичным рассуждениям существуют элементы $t_1, t_2 \in T_1$, такие, что

$$t_1 M(a, b) t_2 \subseteq M(a_0, b_0) = (X(a_0, b_0), a_0, b_0),$$

поэтому

$$|X(a, b)| = |X(a_0, b_0)| = |G_1| = |g_a G_1 g_0 y_b|.$$

Для каждого $b \in B$ пусть $h_b = g_a y_b$. Тогда $X(a, b) = g_a G_1 h_b$. Пусть матрица $C : B \times A \to G^0$ задается соотношением

$$C(b,\ a) = h_b\, C'(b,\ a)\, g_a.$$

Тогда полугруппа $\mathcal{M}^0(G;\ A,\ B;\ C')$ изоморфна полугруппе $\mathcal{M}^0(G;A,B;\ C)$. Изоморфизм определяется как отображение

$$j_1 : \mathcal{M}^0\ (G;\ A,\ B;\ C \to \mathcal{M}^0\ (G;\ A,\ B;\ C),$$

для которого

$$j_1(g,\ a,\ b) = (g_a^{-1}\, g h_b^{-1},\ a,\ b), \quad j_1(0) = 0.$$

Следовательно, $j_1\ (T_1 — \{0\}) = G_1 \times A \times B$ принадлежит полугруппе $\mathcal{M}^0\ (G;\ A,\ B;\ C)$, поэтому, полагая $j = j_1 j'$, получим $j\ (M \square J) = G_1 \times A \times B$.

Наконец, покажем, что G_1 — максимальная подгруппа G, так что $(M \cap J)^0$ будет максимальной подполугруппой в J^0. Пусть G'_1 — такая подгруппа группы G, что $G_1 \subseteq G'_1 \subseteq G$. Предположим, что $T = j^{-1}(G'_1 \times A \times B)$. Определим $M' = M \cup T$. Мы докажем, что M' есть подполугруппой и тогда в силу максимальности M требуемое утверждение будет получено.

Так как $C\ (b,\ a) \in G^0_1$, $\mathcal{M}^0\ (G'_1;\ A,\ B;\ C)$ — полугруппа, поэтому $T \cup \{0\} = j^{-1}[(G'_1 \times A \times B) \cup \{0\}]$ — подполугруппа полугруппы J^0. Поскольку T^0 есть подполугруппа в J^0, мы должны показать только, что для элементов $m \in M$ и $x \in T$ имеет место $mx \in M'$ и $xm \in M'$. Если $mx,\ xm \in M \subset M'$, то требемое получено, поэтому предположим, что $mx,\ xm \in J$. Так как J — регулярный класс, существуют идемпотенты e_1 $e_2 \in J$, такие, что $e_1 x = x$, $xe_2 = x$. К тому же $e_1,\ e_2 \in M$, так как M пересекает каждый H класс полугруппы S, поэтому $me_1,\ e_2 m \in M$. Кроме того, $me_1,\ e_2 m \in J$, так как $mx = (me_1)x \in J$ и $xm = x\ (e_2 m) \in J$. Следовательно, $me_1 e_2 m \in J \cap M \subset T$, откуда вытекает, что $(me_1)x = mx \in M'$ и $x(e_2 m) = xm \in M'$. Следовательно, M'' есть подполугруппа полугруппы S и утверждение доказано.

В случае 2 (см. пункт г)) M является объединением $\mathcal{H}$ классов и $M \cap J \neq 0$. Пусть $J = J(M)$ и предположим, что $\{R\ (a) : a \in A\}$, $\{L(b) : b \in B\}$ и $\{H(a,\ b) = R\ (a) \cap L\ (b)\}$ будут $\mathcal{R}$, $\mathcal{L}$ и $\mathcal{H}$ классами соответственно полугруппы S, содержащимися в J. Пусть

$$A' = \{a \in A : R(a) \not\subseteq M\} \quad \text{и} \quad B' = \{b \in B : L(b) \not\subseteq M\}.$$

Очевидно, что A' и B' - непустые множества, но тогда получаем противоречие $J \subseteq M$.

Пусть $a_1 \in A'$. Тогда $T = M^1\ R\ (a_1) \cup M$ есть подполугруппа в S, содержащая в качестве собственного подмножествоа M. Для того чтобы доказать это, воспользуемся тем фактом, который

$R(a_1)M \subseteq R(a_1)$ $\square M \subset$ Т. [Действительно, пусть $r \in R(a_1)$, $m \in M$ и предположим $rm \notin M$. Тогда $rm \in J$, так что $rm \mathcal{F} r$, откуда вытекает $rm \mathcal{R} r$, т.е. $rm \in R(a_1)$.] Следовательно, $T = S$. Пусть $a_2 \in A'$, поэтому $R(a_2) \not\subset M$. Тогда $M^1R(a_1)$ I $R(a_2) \neq \varnothing$, т.е. существует такой элемент $m \in M^1$, что $mR(a_1)$ I $R(a_2) \neq \varnothing$. Но в силу утверждения $mR(a_1)=R(a_2)$ и, в частности, для всех $b \in B mH(a_1, b)=H(a_2, b)$. Аналогично (при помощи $\mathcal{L}$ классов) легко устанавливается существование такого элемента $m \in M^1$, что для $b_1, b_2 \in B' H(a, b_1)m = H(a, b_2)$ при всех $a \in A$.

Теперь для того чтобы показать, что $\mathcal{H}$ классы из J не принадлежат M, докажем лемму.

Лемма. *$H(a, b)$* I $M = \varnothing$ тогда и только тогда, когда $a \in A'$ и $b \in B'$.

Пусть $a \in A'$ и $b \in B'$ и предположим, что $H(a, b) \subseteq M$. Тогда для каждого $a_i \in A'$ существует элемент $m_i \in M^1$, такой, что $m_iH(a,b)=H(a_i,b)$. Следовательно, для всех $a \in AH(a_i\ b) \subseteq M$, откуда вытекает, что $L(b) \subseteq M$, это противоречие. Обратное очевидно.

Следовательно, если $B' = B$, то легко видеть, что j (M I J) представляется выражением 3.1. Аналогично, если $A'=A$, $j(M$ I $J)$ должно быть представлено выражением 3.2. A' и B' - собственные подмножества A и B, тогда j (M I J) представляется выражением 3.3.

Так как легко построить примеры, в которых j (M I J) представлено выражением 3.1 или 3.2, но $(M$ I $J)^0$ не является максимальной подполугруппой в J^0 (см. замечание 16), мы завершим доказательство, показав, что $(M$ I $J)^0$ будет максимальной в J^0, если $j(M$ I $J)$ представляется выражением 3.3. Принимая к вниманию предыдущие рассуждения, достаточно показать, что для каждых $a_1, a_2 \in A'$ существует элемент $m \in M$ I J (а не просто $m \in M^1$ как ранее), такой, что $mR(a_1) = R(a_2)$ и что для каждых $b_1, b_2 \in B'$ существует элемент $m' \in M$ I J, такой, что $L(b_1)m' = L(b_2)$. Кроме того, согласно определению упорядочения на $\mathcal{F}$ классах, это эквивалентно тому, что такие m, m' можно выбрать в M I J^*, где $J^* = \bigcup \{ J' : J'$ есть $\mathcal{F}$ класс полугруппы S и $J' \leq J\}$, так как J^* — J есть идеал полугруппы S.

Пусть $R(A') = \bigcup \{R(a) : a \in A'\}$. Теперь для всех $a \in A'$ мы показали, что $R(A') \subseteq M^1R(a)$. К тому же по определению J^* имеем

$(M \square J^*)\ M^1 = M \cap J^* = M^1(M \cap J^*)$. Пусть теперь для любого $a \in A'\ R(A') \subseteq (M \cap J^*)\ R(a)$ или $R(A') \cap (M \cap J^*)\ R(a) = \varnothing$, так как если $m\ R(a) \cap R(a') \neq \varnothing$ для некоторого $a' \in A'$ и $m \in M$, то $m\ R(a) = R(a')$, поэтому

$$R(a') \subseteq (M \cap J^*)\ R(a)$$

и

$$R(A') \subseteq M^1 R(a') \subseteq M^1(M \cap J^*) R(a) = (M \cap J^*) R(a).$$

Если

$$R(A') \cap (M \cap J^*) R(a) = \varnothing,$$

тогда

$$(M \cap J^*) R(A') \cap R(A') \subseteq (M \cap J^*) M^1 R(a) \cap R(A') = (M \cap J^*) R(a) \cap R(A') = \varnothing.$$

Теперь

$$j(J^0) = \mathcal{M}^0(G;\ A,\ B;\ C)$$

и

$$j(M \cap J)^0 = [(G \times A \times B) - (G \times A' \times B')] \cup \{0\}$$

есть подполугруппа, поэтому

$C(b, a) = 0$ для всех $(a, b) \in (A - A') \times (B - B')$.

Если для $a \in A'$ мы имеем $R(A') \cap (M \cap J^*) R(a) = \varnothing$, то в силу изложенного ранее $R(A') \cap (M \cap J^*) R(A') = \varnothing$, поэтому, в частности, равенство $[G \times A' \times (B - B')]\ (G \times A' \times B) = \{0\}$, показывая, что $C(b, a) = 0$ при всех $(a, b) \in A \times (B - B')$, противоречит регулярности класса J. Из этого следует, что $R(A') \subseteq (M \cap J^*) R(a)$ для любого элемента $a \in A'$, т.е. для всех элементов $a_1, a_2 \in A'$ существует $m \in M \cap J$, такой, что $m\ R(a_1) = R(a_2)$ (мы заменяем J^* на J, так как не существует элементов из $J^* - J$, которые могли бы удовлетворять условию). Доказательство для $\mathcal{L}$ классов аналогично.

Замечание 15. Пусть $S = \mathcal{M}^0(G; A, B; C)$ — регулярная рисовская полугруппа матричного типа. Если M — максимальная подполугруппа полугруппы S, то $J(M) = \{0\}$ или $J(M) = S - \{0\}$. В первом случае $S - \{0\}$ есть подполугруппа и $M = S - \{0\}$. Во втором случае $M \cap J(M) = \varnothing$ тогда и только тогда, когда $S - \{0\}$ есть простая абелева группа [т.е. $(Z_p, +)$ для некоторого простого числа p]. В противном

случае $M \square J(M)$ имеет один из следующих трех видов в некоторой системе координат:

1) $(G' \times A \times B)$, G' — максимальная подгруппа группы G;

2) $(G \times A \times B')$, где $B' = B — \{b\}$ для некоторого $b \in B$ и матрица C, ограниченная на $B' \times A$, является регулярной (т.е. имеет по крайней мере один ненулевой элемент в каждом строке и в каждом столбце);

3) $(G \times A' \times B)$, где $A' = A — \{a\}$ для некоторого элемента $a \in A$ и матрица C, ограниченная на $B \times A'$, будет регулярной;

4) $(G \times A \times B) — (G \times A' \times B')$, где $A' = A — Y$ и $B' = B — X$ и $X \times Y$ представляет собой *максимальный* «прямоугольник», на котором матрица C тождественно равна нулю.

Кроме того, каждая подполугруппа M полугруппы S, содержащая все, кроме одного $\mathcal{F}$ класса, и такая, что $M \cap J(M)$ имеет один из приведенных ранее видов, будет максимальной подполугруппой в S.

Замечание 16. Контрпример, показывающий, что полугруппа $(M \cap J)^0$ не обязательно будет максимальной в полугруппе J^0, когда $j(M \cap J)$ представляется выражением 3.1 (см. случай 2, пункт г)), можно построить следующим образом.

Пусть $F(X_n)$, $n \geq 2$ есть полугруппа всех функций на последовательности $x_1, \ldots, x_n$ длины n с обычным законом композиции. Пусть $\{x_1 \ldots, x_n, z\}^1$ — полугруппа, определяемая соотношениям $xy = x$ для всех $x, y \in \{x_1 \ldots, x_n, z\}$. Построим полугруппу $S = F(X_n) \cup \{x_1, \ldots, x_n, z\}$, определяя умножение следующим образом. Пусть $F(X_n)$ и $\{x_1, \ldots, x_n, z\}$ — подполугруппы и для всех $f \in F(X_n)$

$$f \circ x_i = f(x_i) \text{ для всех } x_i \in X_n,$$

$$x_i \circ f = x_i \text{ для всех } x_i \in X_n,$$

$$f \circ z = z \circ f = z.$$

Тогда $M = F(X_n) \cup \{ z \}$ есть максимальная подполугруппа полугруппы S и $J(M) = \{x_1 \ldots, x_n, z\}$. Так как каждый элемент из $J(M)$ является $\mathcal{R}$ классом, $J[M \cap J(M)]$ представляется выражением 3.1. Но согласно замечанию 15 $j[M \cap J(M)]^0$ не является максимальной подполугруппой в $j[J(M)^0]$. Контрпример для выражения (3.2) конструируется дуальным способом.

Микромодуль 8.
Идивидуальные тестовые задачи

1. Покажите, что пересечение левых, правых или двусторонних идеалов (когда оно непустое) будет левым, правым или двусторонним идеалом соответственно. Докажите, что $S^1 \cdot s$ есть пересечение всех левых идеалов, которые содержат элемент s и, следовательно, является наименьшим (относительно включения) левым идеалом, который содержит элемент s. Сделайте то же самое для правых идеалов $(s \cdot S^1)$ и двусторонних идеалов $(S^1 s S^1)$.

2. Проверьте недоказанные пункты утверждения 1.

3. Покажите, что рисовская полугруппа матричного типа является 0-простой тогда и только тогда, когда она регулярна (т.е. ее структурная матрица содержит ненулевой элемент в каждом строке и в каждом столбце). При каких условиях относительно структурной матрицы $\{0\}$ расщепляет рисовскую полугруппу матричного типа S? Покажите, что в этом случае полугруппа S — $\{0\}$ — простая (см. замечание 2 микромодуля 7).

4. Вычислите левые, праве, двусторонние идеалы и ядра

а) для $F_r(X_n)$,где X_n — $\{1, ..., n\}$;

б) для $(2^{X_n}, \square)$.

5. Докажите, что конечная полугруппа S — простая справа тогда и только тогда, когда она имеет вид $G \times B^r$, где G - некоторая группа и B - некоторое конечное множество. Докажите дуальное утверждение.

6. Докажите, что полугруппа G (быть может, бесконечная) является группой тогда и только тогда, когда она простая справа и справа.

7. Какие результаты утверждения 7 микромодуля 7 неверны для бесконечных полугрупп? Постройте контрпримеры.

8. Определите 0-простые слева полугруппы. Докажите, что $T \neq \{0\}$ будет 0-простоя слева тогда и только тогда, когда T является простой слева или $T = L^0$, где L — простая слева полугруппа.

9. Докажите, что утверждение 3 и пункты д) и е) утверждения 5 справедливы для любых полугрупп. Докажите, что пункты а)-г) утверждения 5 справедливы для любых периодических полугрупп.

10. Вычислите $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ и $\mathcal{F} = \mathcal{D}$ классы для полугрупп:

а) $F_R(X_n)$, где $X_n = \{1.....n\}$;

б) $\mathcal{M}^\circ(G; A, B; C)$, где C — регулярная матрица (т.е. каждая ее строка и каждый столбец содержат ненулевые элементы);

в) $(2^{X_n}, \square)$;

г) для конечной циклической полугруппы.

11. Пусть S— конечная абелева полугруппа, тогда $\mathcal{H} = \mathcal{L} = \mathcal{R} = \mathcal{F}$. Верно ли обратное утверждение?

12. Пусть символ $\mathcal{T}$ обозначает одно из отношений $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ или $\mathcal{F}$. Если T подполугруппа полугруппы S и $t_1, t_2 \in T$, то отношение $t_1 \mathcal{T} t_2$ в T влечет $t_1 \mathcal{T} t_2$ в S. Постройте конечную полугруппу S и подполугруппу T с элементами $t_1, t_2 \in T$, для которых $t_1 \mathcal{T} t_2$ в S, но не в T. Покажите, что из отношения $t_1 \mathcal{T} t_2$ в S вытекает $t_1 \mathcal{T} t_2$ в T, если t_1 и t_2 являются $\mathcal{T}$-эквивалентными в T с некоторыми идемпотентами и $\mathcal{T}$ не является отношением $\mathcal{F}$.

13. Пусть полугруппа S 0-простая и $0 \neq a \in S$. Покажите, что существуют идемпотенты $e_1, e_2 \in S$ — $\{0\}$, такие что $e_1 \mathcal{L} a$ и $a \mathcal{R} e_2$.

14. Пусть S — конечная полугруппа. Последовательность $K(S) = I_n \subset I_{n-1} \subset \ldots \subset I_0 = S$ называется *композиционным рядом для полугруппы S,* если для $j = 1 \ldots .. n$ I_j есть максимальный идеал в I_{j-1}. Для $j = 1, \ldots, n$ $F_j = I_{j-1}/I_j$ и $F_{n+1} = I^0_n = K(S)^0$. $F_1, \ldots, F_{n+1}$ называются *факторами* композиционного ряда. Покажите, что факторы каждого композиционного ряда представляют собой полугруппы $\{J^\circ: J$ - регулярный $\mathcal{F}$ класс полугруппы $S\}$ и совокупность двухэлементных полугрупп с нулевым умножением (N_2; см. определение 2), появляющихся как композиционные факторы из нулевых $\mathcal{F}$ классов полугруппы S. Что можно сказать в случае, когда полугруппа S будет бесконечной?

15. Для каждого $\mathcal{F}$ класса J полугруппы $F_R(X_n)$, где $X_n = (1, \ldots, n)$, найдите изоморфизм между J° и регулярной рисовской полугруппой матричного типа.

16. а) Определите с точностью до изоморфизма все простые полугруппы порядка p, где p — простое число.

б) Определите с точностью до изоморфизма все полугруппы порядка 3.

17. Пусть $S = \mathcal{M}(G; A, B; C)$ яаляется простой полугруппой, т.е. для всех элементов $a \in A, b \in B$ $C(b, a) \neq 0$. Предположим, что T — подполугруппа в S и что $(g_1, a_1, b_1), (g_2, a_2, b_2) \in T$. Пусть G_1 — подгруппа в G, рожденная элементами g_1, g_2 и $C(\{b_1, b_2\} \times \{a_1, a_2\})$. Покажите, что множество $G_1 \times \{a_1, a_2\} \times \{b_1, b_2\}$ есть подполугруппа полугруппы T.

18. Докажите, что любая подполугруппа простой полугруппы простая.

19. Если соотношения $\varnothing \neq A' \subset A$ и $\varnothing \neq B' \subset B$ имеют место, сформулируйте необходимые и достаточные условия для того, чтобы

множество $\mathcal{M}^\circ$ $(G; A, B; C) — G \times A' \times B'$ было подполугруппой полугруппы $\mathcal{M}^\circ (G; A, B; C)$. (Что можно сказать о C?)

20. Если S — полугруппа и $X \subseteq S$, то $\mathrm{Perm}_R(X)$ — *правым преобразователем множества* X — называется полугруппа $\{s \in S^1 : Xs = X\}$. $\mathrm{Perm}_R(X) \subseteq RI(X)$. $\mathrm{Perm}_L(X)$ определяется дуально и

$$\mathrm{Perm}(X) = \mathrm{Perm}_R(X) \cap \mathrm{Perm}_L(X).$$

Подполугруппа U полугруппы S называется *унитарной справа*, если для всех элементов $x \in S$ — U имеем $Ux \cap U = \varnothing$. U называется *унитарной слева*, если для всех элементов $x \in S$ — U имеем $xU \cap U = \varnothing$.

Если $1 \in S$ и U — унитарная подполугруппа в S, то $1 \in U$.

Подполугруппа U полугруппы S унитарная справа тогда и только тогда, когда для некоторого действия полугруппы S на некоторое множество X и для некоторого $x \in X$ $U = \{s \in S : xs = x\}$. Легко проверить, что подполугруппа U, удовлетворяющая этому условию, унитарна справа. Проверим обратное. Пусть S действует на совокупность классов эквивалентности элементов полугруппы S^1, определяемых отношением $s_1 \equiv s_2$, тогда и только тогда, когда для всех $x \in S^1$ s_1x и s_2x или оба вместе принадлежат U, или оба не принадлежат U. Множество U есть $(\equiv)$ класс и U — множество элементов из S, оставляющих U на месте.

Если H является $\mathcal{H}$ классом полугруппы S, то $\mathrm{Perm}_R(H) = RI(H)$ и $\mathrm{Perm}_R(H)$ унитарна справа. (*Указание.* Пусть S действует справа на 2^S, далее воспользуйтесь изложенным ранее). Если H — группа, то существует гомоморфизм из $\mathrm{Perm}_R(H)$ на H, фиксирующий H. Следовательно, для любой максимальной подгруппы H полугруппы S существует унитарная подполугруппа U в S, для которой H — ретракт, т.е. $H \subseteq U \subseteq S$. U унитарная и существует гомоморфизм $\varphi : U \to\!\!\!\to H$, ограничение которого на H будет тождественным отображением.

21. Пусть A — множество. Для элементов $a, b \in A$ пусть $T(a, b) \in F_R(A)$ обозначает функцию, переводящая a в b и оставляющую все другие элементы множества A на месте. Если $|A| \geq 2$, то подполугруппа полугруппы $F_R(A)$, порождаемая множеством элементов $\{T(a, b) : a, b \in A\}$, есть $F_R(A) — \mathrm{SYM}_R(A)) \cup \{1\}$. Следовательно, $F_R(A)$ порождается тремя элементами, и если $|A| \geq 3$, то меньшего числа образующих будет недостаточно.

[*Указание.* Покажите, что $\mathrm{SYM}_R(A)$ порождается двумя элементами и что для порождения любой $T(a, b)$ достаточно группы $\mathrm{SYN}_R(A)$ и

любого элемента, область значения которого содержит $|A|$ — 1 элементов.]

22. Пусть J — простой $\mathcal{F}$ класс полугруппы S. Пусть $x \in S$. Докажите, что если $j \in J$ и $jx \in J$, то $xJ \subseteq J$. Затем, применяя дуальный результат, докажите, что $Jx \subseteq J$.

23. Пусть I — непустое подмножество полугруппы S • I будет идеалом, если I является объединением $\mathcal{F}$ классов полугруппы S, таких, что как только J_1 и J_2 представляют собой два $\mathcal{F}$ классы S, причем $J_1 \leq J_2$ и $J_2 \subseteq I$, то $J_1 \subseteq I$. I будет левым (соответственно правым) идеалом тогда и только тогда, когда I — объединение $\mathcal{L}$ классов (соответственно $\mathcal{R}$, классов), удовлетворяющих сформулированному ранее условию упорядоченности.

Если I есть максимальный идеал, то S — I есть единственный $\mathcal{F}$ класс. Соответствующий факт справедлив для максимальных левых или правых идеалов. Если I есть максимальный левый идеал, требуется ли, чтобы $\mathcal{F}$ класс, который содержит S — I, был максимальным?

24. а) Для $x, y \in S$ доказать, что $L_x R_y \subseteq J_{xy}$.

б) Пусть h_1, h_2, h'_1, h'_2 — элементы полугруппы S и $h_i \mathcal{H} h'_i$ при i = 1; 2. Тогда $h_1 h_2 \mathcal{F} h'_1 h'_2$, и если $h_1 \mathcal{F} h_2$ и $h_1 \mathcal{F} h_1 h_2$, то $h_1 h_2 \mathcal{F} h'_1 h'_2$.

25. Пусть S — конечная нильпотентная полугруппа. Тогда каждый $\mathcal{F}$, $\mathcal{L}$, $\mathcal{R}$ и $\mathcal{H}$ классы полугруппы S состоят из одного элемента. [*Указание.* Если $s_1 \neq 0 \neq s_2$ $xs_1 = s_2$, $ys_2 = s_1$, то $(yx)^n s_1 = s_1$ для всех n, поэтому некоторая степень элемента (yx) будет ненулевым идемпотентом.].

26. Пусть T — подполугруппа полугруппы S. Предположим, что $\alpha(T)$ и $\alpha(S)$ обозначают одно из отношений $\mathcal{H}$, $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{F}$ на T или S соответственно. Тогда из соотношения $s_1 \alpha(S) s_2$ вытекает $s_1 \alpha(T) s_2$, если справедливо одно из следующих условий:

а) T — циклическая полугруппа;

б) T — регулярная и $\alpha \neq \mathcal{F}$;

в) S есть нильпотентное расширение объединения групп (т.е. M — объединение групп и идеал полугруппы S, полугруппа S/M нильпотентная). В частности, если S — циклическая или нильпотентная полугруппа или S есть объединение групп, результат справедлив.

27. Найдите все подполугруппы инверсной 0-простой полугруппы.

28. Охарактеризуйте инверсные, комбинаторные полугруппы, являющиеся объединением групп.

29. Пусть C_1 и C_2 — комбинаторные полугруппы и $\varphi : C_1 \to \mathrm{End}(C_2)$ — гомоморфизм. Докажите, что $C_2 \times_{\varphi} C_1$ — комбинаторная полугруппа.

30. а) Полугруппа S регулярна тогда и только тогда, когда для каждого $x \in S$ существуют $e_1, e_2 \in E(S)$, такие, что $e_1 \mathcal{L} x$ и $e_2 \mathcal{R} x$.
б) S регулярна тогда и только тогда, когда каждый элемент полугруппы S имеет по крайней мере один инверсный элемент.
в) $x, y \in S$ будут инверсный в групповом смысле тогда и только тогда, когда x будет инверсным в полугрупповом смысле для y, y в полугрупповом смысле инверсный для x и $xy = yx$.
г) Если $X_n=\{1, ...,n\}$, то $F_R(X_n)$ регулярна.
д) Если A и B — конечные непустые множества, то любые два элемента из $A^l \times B^r$ инверсны друг к другу.
е) S регулярна тогда и только тогда, когда $r(S)$ регулярна.
31. а) S будет инверсной полугруппой тогда и только тогда, когда каждого элемента $x \in S$ существуют единственные элементы $e_1, e_2 \in E(S)$, такие, что $S^1x = Se_1$ и $x S^1 = e_2S$.
б) Если S — инверсная полугруппа, то $(a^{-1})^{-1} = a$ и $(a\ b)^{-l} = b^{-l}a^{-1}$ для всех $a, b \in S$. Следовательно, отображение $a \to a^{-1}$ есть изоморфизм S с $r(S)$.
в) Пусть G — конечная группа и $S=(2^G, \bullet)$, где $H_1 \bullet H_2=\{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}$. Тогда $E(S)$ есть совокупность подгрупп группы G. В общем случае $E(S)$ не является коммутативной, однако каждый регулярный фактор полугруппы S будет инверсной полугруппой.
32. Пусть $A = \{a_1, ..., a_n\}$ и I — идеал в полугруппе $\sum A$, состоящей из цепочек $(x_1, ..., x_k)$, таких, что $k \geq c$ для некоторого фиксированного целого c. Тогда $(\sum A)/I$ есть *свободная нильпотентная полугруппа* $FN(n, c)$ класса c з n образующими. S есть нильпотентная полугруппа с самое большее n образующими и с $cl(S) \leq c$ тогда и только тогда, когда существует гомоморфизм $\varphi : FN(n, c) \to\to S$.
33.Пусть J есть $\mathcal{F}$ класс полугруппы S. Определим

$F(J) = \square\{J' : J'$ есть $\mathcal{F}$ класс в S и $J \not\leq J'\}$.

а) $F(J) = \varnothing$ или $F(J)$ есть идеал полугруппы S.

б) $F(J) = \varnothing$ тогда и только тогда, когда $J = K(S)$.

в) Если $F(J) \neq \varnothing$, то J° есть единственный 0-минимальный идеал полугруппы $S/F(J)$.
34. Пусть $M = \mathcal{M}^\circ(G; A, B; C)$ — регулярная рисовская полугруппа матричного типа. Пусть $\alpha \in RT(M)$ и $\beta \in LT(M)$ связаны. Тогда докажите, рассмотрев α, β и C как матрицы, которые $\alpha C = C\beta$. Это матричная форма для определения 10.

Микромодуль 9.
Гомоморфизмы и полулокальная теория

3.6. Гомоморфизмы

В этом микромодуле будет показано, что если $\theta : S \to\to T$ есть максимальный собственный эпиморфизм—MPE (Maximal proper epimorphism, см. определение 1.12), то или θ, ограниченный на H классы будет взаимно однозначным [$\gamma(\theta)$ эпиморфизм], или θ разделяет H классы (H эпиморфизм). Из этого следует, что каждый эпиморфизм между двумя конечными полугруппами можно разложить в γ(H) и H эпиморфизмы. Кроме того, если θ есть MPE, то будет доказано, что существует такой F класс J, что θ является взаимно однозначным на множестве S — J. Следовательно, дальнейший анализ эпиморфизма θ при помощи теорем Грина—Риса можно проводить на классе J.

1.1. Определение. Пусть S — заданная полугруппа. *Свойством гомоморфизмов* полугруппы S называется совокупность P пар (φ, T), где φ: $S \to\to T$, причем если

$$(\varphi_1, T_1) \in \mathcal{P} \text{ и } j : T_1 \to\to T_2$$

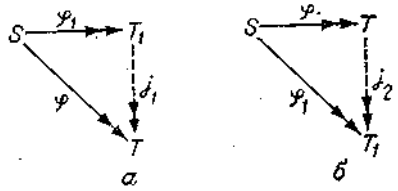
есть изоморфизм, то $(j\varphi_1, T_2) \in \mathcal{P}$.

Мы будем писать $(\varphi_1, T_1) \leqslant (\varphi_2, T_2)$ тогда и только тогда, когда существует эпиморфизм: $j : T_2 \to\to T_1$, такой, что $\varphi_1 = j\varphi_2$. Если

$$(\varphi_1, T_1) \leqslant (\varphi_2, T_2) \text{ и } (\varphi_2, T_2) \leqslant (\varphi_1, T_1),$$

то T_1 и T_2 изоморфны. Тогда мы говорим, что (φ_1, T_1) и (φ_2, T_2) также изоморфны.

1.2. Определение. Пусть P —свойство гомоморфизмов полугруппы S. Назовем $(\varphi, T) \in$ P *минимальным* (соответственно *максимальным) гомоморфным образом полугруппы S по отношению к* P, если (φ, T) является единственным (с точностью до изоморфизма) минимальным (соответственно максимальным) элементом из P в упорядочении $\leq$. Следовательно, утверждение, что (φ, T) есть минимальный (соответственно максимальный), означает, что если $(\varphi_1, T_1) \in$ P, то существует гомоморфизм f_1: $T_1 \to\to T$ (соответственно f_2: $T \to\to T_1$), который делает приведенную диаграмму *а* (соответственно диаграмму *б)* коммутативной.



а б

1.3. Замечание. P не обязательно имеет максимальный или минимальный гомоморфный образ. Например, если $|A| \geq 3$, то A^r не имеет ни максимального, ни минимального гомоморфного образа по отношению к P, где P есть совокупность таких пар (φ, T), что $\varphi : A^1 \to\to T$, где $|T| = 2$.

1.4. Утверждение. Пусть P ' — свойство полугруппы, замкнутое относительно прямых произведений и подполугрупп (т. е. если $S_1, S_2 \in \mathcal{P}'$, то $S_1 \times S_2 \in \mathcal{P}'$, и если T — подполугруппа полугруппы $S \in$ P ', то $T \in$ P '). Тогда пусть S — полугруппа и предположим, что P — свойство гомоморфизмов полугруппы S, определяемое следующим образом: $(\varphi, T) \in$ P тогда и только тогда, когда $T \in$ P '. В этом случае S «имеет максимальный гомоморфный образ по отношению к P.

Доказательство. Пусть $\mathcal{P} = \{(\varphi_i, T_i) : i = 1, \ldots, n\}$, поскольку ясно, что P может иметь только конечное число неизоморфных членов, Тогда $T_1 \times \ldots \times T_n \in \mathcal{P}'$. Рассмотрим гомоморфизм

$$\varphi = (\varphi_1 \times \ldots \times \varphi_n)\,\Delta : S \to T_1 \times \ldots \times T_n$$

(не обязательно эпиморфизм), где $\Delta : S \to S \times \ldots \times S$ (n раз) определяется соотношением $\Delta(s) = (s, \ldots, s)$. Тогда $\varphi(S)$ есть подполугруппа в $T_1 \times \ldots \times T_n$, поэтому $\varphi(S) \in$ P ' и $(\varphi, \varphi(S)) \in \mathcal{P}$. Очевидно, что $(\varphi, \varphi(S))$ есть максимальный гомоморфный образ полугруппы S по отношению к P.

1.5. Замечание. Примерами совокупностей полугрупп, замкнутых относительно прямых произведений и подполугрупп служат: 1) группы (конечные), 2) комбинаторные полугруппы, 3) полугруппы, представляющие собой объединения групп, 4) абелевы полугруппы, 5) связки и т. п.

В качестве примера построим максимальный групповой гомоморфный образ конечной полугруппы. Прежде всего докажем следующую лемму.

1.6. Лемма. Пусть S — полугруппа с идеалом I и $\varphi : I \to\to T^1$ — эпиморфизм. Тогда существует единственное расширение φ на S.

Доказательство. Пусть $x \in \varphi^{-1}(1)$. Определим отображение $\hat{\varphi} : S \to\!\!\!\to T^1$, полагая $\hat{\varphi}(s) = \varphi(xsx)$. Зная, что $\varphi(x) = 1$, нетрудно проверить, что $\hat{\varphi}$ является эпиморфизмом. Пусть $s \in I$. Тогда $\hat{\varphi}(s) = \varphi(xsx) = \varphi(s)$, поэтому $\hat{\varphi}$ есть расширение φ.

Пусть $\bar{\varphi}$ — другое расширение φ на S, предположим, что $s \in S$. Тогда $\hat{\varphi}(s) = \varphi(xsx) = \bar{\varphi}(xsx)$, поскольку $xsx \in I$. Но $\bar{\varphi}(xsx) = \bar{\varphi}(x)\,\bar{\varphi}(s)\,\bar{\varphi}(x) = \bar{\varphi}(s)$, так как $\bar{\varphi}(x) = \varphi(x) = 1$, следовательно $\bar{\varphi} = \varphi$.

1.7. Пример. Мы построим теперь максимальный групповой гомоморфный образ конечной полугруппы *S*. Если $\varphi : S \to\!\!\!\to H$ и H — группа, то $\varphi[K(S)] = H$, так как эпиморфизм отображает ядро на ядро и группа является своим собственным ядром. Давайте исследуем строение эпиморфизма φ на $K(S)$. Так как $K(S)$ есть регулярный $\mathcal{F}$ класс, мы можем воспользоваться свойствами локальных гомоморфизмов из п. 3.4.

Пусть $K(S) \cong \mathcal{M}(G; A, B; C)$, где C выбрана так, чтобы гомоморфизм φ можно было описать в нормализованной форме, т. е.

$$\varphi(g, a, b) = (\omega(g), \psi_L(a), \psi_R(b)).$$

Но областью значений (образом) φ будет группа, поэтому $\psi_L(a) = 1$ для всех $a \in A$, $\psi_R(b) = 1$ для всех $b \in B$ и $\omega[C(b, a)] = 1$ для всех $a \in A$, $b \in B$. [Напомним, что $C(b, a) \neq 0$ для всех $a \in A$, $b \in B$, так как $K(S)$—простая полугруппа.] Тогда $C(B \times A)$ должна принадлежать ядру ω.

Построим теперь следующий гомоморфизм на $K(S)$. Пусть N — нормальный делитель группы G, порожденный $C(B \times A)$. Пусть $\nu : G \to\!\!\!\to G/N$ — канонический гомоморфизм. Пусть тогда $\psi_L(a) = \{1\}$ и $\psi_R(b) = \{1\}$. Определим $\theta : K(S) \to\!\!\!\to \nu(G)$, полагая

$$\theta(g, a, b) = (\nu(g), 1, 1) = \nu(g).$$

Мы утверждаем, что θ, расширяемый единственным образом на *S*, в силу леммы 1.6 будет максимальным групповым гомоморфизмом полугруппы *S*. [Термин *групповой гомоморфизм* означает, что образом этого гомоморфизма является группа.] Если φ есть такой гомоморфизм, что $\varphi(S)$ — группа, то гомоморфизм ω на G, ассоциированный с φ, будет содержать N как подмножество своего ядра. Следовательно, существует гомоморфизм $\mu : \nu(G) \to\!\!\!\to \omega(G)$, т. е. $\omega = \mu\nu$. Но $\theta(S) = \nu(G)$ и $\varphi(S) = \omega(G)$, поэтому $\mu : \theta(S) \to\!\!\!\to \varphi(S)$ и $\varphi = \mu\theta$.

1.8. Определение. Пусть P — разбиение на полугруппе S, а $\mathrm{P}(S, P)$ — совокупность пар (φ, T), $\varphi : S \to\to T$, таких, что $\varphi(s_1) = \varphi(s_2)$ влечет $s_1 \equiv s_2 \pmod{P}$. Если $(\varphi, T) \in \mathrm{P}(S, P)$, мы пишем $\varphi : S \to\to T$ и φ называем *P гомоморфизмом полугруппы S.*

1.9. Утверждение. Пусть P — любое разбиение на полугруппе S. Тогда $\mathrm{P}(S, P)$ имеет минимальный гомоморфный образ, обозначаемый как S^P.

Доказательство. Пусть Q будет отношением конгруэнтности, порожденным P, т. е. $s_1 \equiv s_2 \pmod{Q}$, тогда и только тогда, когда $\alpha s_1 \beta \equiv \alpha s_2 \beta \pmod{P}$ для всех элементов $\alpha, \beta \in S^1$. Пусть $\eta : S \to\to S/Q$ — канонический гомоморфизм. Тогда легко доказать, что $(\eta, S/Q)$ будет минимальным гомоморфным образом полугруппы S по отношению к $\mathrm{P}(S, P)$.

1.10. Замечание. а) Важный пример минимального гомоморфного образа по отношению к разбиению был приведен ранее. Если дан автомат $f : \sum A \to$, то полугруппа f^S автомата f будет в точности минимальным гомоморфным образом для $\mathrm{P}(\sum A, \pmod{f})$, где $\pmod{f}$ есть разбиение, которое f индуцирует на $\sum A$. Другими словами, $f^S = \sum A^{(\mathrm{mod}\, f)}$.

б) Пусть $\varphi: S \to\to T$ — эпиморфизм. Тогда (φ, T) представляет собой минимальный гомоморфный образ по отношению к $\mathrm{P}(S, \mathrm{mod}\ \varphi)$. Таким образом, если $\theta : S \to\to T_1$ —такой эпиморфизм, что из равенства $\theta(s_1) \equiv \theta(s_2)$ вытекает отношение $s_1 \equiv s_2 \pmod{\varphi}$ для всех $s_1, s_2 \in S$, то $(\theta, T_1) \in \mathrm{P}(S, \mathrm{mod}\ \varphi)$. Следовательно, существует эпиморфизм $j : T_1 \to\to T$, такой, что $\varphi = j\theta$.

1.11. Обозначения. Пусть α— любое из отношений F, R, L или H на полугруппе S. Тогда α является разбиением на S и $\mathrm{P}(S, \alpha)$ имеет минимальный гомоморфный образ S^{α}. Отображение $\theta : S \to\to T$ есть α *гомоморфизм* (или *эпиморфизм),* если $(\theta, T) \in \mathrm{P}(S, \alpha)$. Например, θ будет H эпиморфизмом тогда и только тогда, когда для всех элементов $s_1, s_2 \in S$, таких, что $\theta(s_1) = \theta(s_2)$, необходимо s_1 H s_2.

1.12. Определение. Пусть $\theta : S \to\to T$, θ называется γ *эпиморфизмом,* если ограничение θ на любую подгруппу полугруппы S взаимно однозначное. Пусть α — одно из отношений F, R, L или H. Тогда θ называется $\gamma(\alpha)$ *эпиморфизмом,* если ограничение θ на любой α класс есть взаимно однозначное отображение. В частности, $\gamma(\alpha)$ эпиморфизм представляет собой γ эпиморфизм.

1.13. Утверждение. Пусть α — любое из отношений F, R, L или H. Тогда

а) композиция двух α эпиморфизмов будет α эпиморфизмом;

б) композиция двух $\gamma(\alpha)$ эпиморфизмов (соответственно γ эпиморфизмов) будет $\gamma(\alpha)$ эпиморфизмом (соответственно γ эпиморфизмом).

Доказательство, а) Докажем, что если φ: $S \to\to T$ есть α эпиморфизм, то каждый α класс полугруппы S отображается на α класс полугруппы T. Следовательно, α классы полугруппы S и α классы полугруппы T находятся во взаимно однозначном соответствии, из этого легко вытекает требуемый результат.

Предположим, что $\alpha = \mathsf{F}$ и $\varphi(j_1)\ \mathrm{F}\ \varphi(j_2)$. Пусть $s, t, u, v \in S$ — такие любые элементы, что $\varphi(s)\ \varphi(j_1)\ \varphi(t) = \varphi(j_2)$ и $\varphi(u)\ \varphi(j_2)\ \varphi(v) = \varphi(j_1)$. Тогда поскольку φ есть F эпиморфизм, имеем $sj_1t\mathrm{F}\ j_2$ и $uj_2v\mathrm{F}\ j_1$. Из этого следует, что $j_1\mathrm{F}\ j_2$, следовательно, $j_1\mathrm{F}\ j_2$ тогда и только тогда, когда $\varphi(j_1)\ \mathrm{F}\ \varphi(j_2)$.

Для отношений α = R, L и H доказательство проводится аналогично.

б) Оставляем доказательство читателю в качестве упражнения.

Мы докажем теперь основной результат этого пункта, а именно, что каждый эпиморфизм между двумя конечными полугруппами можно разложить в γ(H) и H эпиморфизмы.

1.14. Теорема. Пусть $\theta : S \to\to T$ — эпиморфизм. Тогда θ можно записать как $\theta = \theta_n \ldots \theta_1$ где $\theta_1, \theta_3, \theta_5, \ldots$ будут γ(H) эпиморфизмами и $\theta_2, \theta_4, \theta_6, \ldots$ будут H эпиморфизмами (или наоборот).

Прежде чем приступить к доказательству теоремы, введем следующее определение.

1.15. Определение. Пусть $\theta : S \to\to T$ —эпиморфизм. Тогда θ называется *максимальным собственным эпиморфизмом* (МРЕ), если из соотношения $\theta = \theta_2\theta_1$ где θ_1 и θ_2 — эпиморфизмы, следует, что одно и только одно из отображений θ_1, θ_2 взаимно однозначное.

Очевидно, что любой эпиморфизм θ будет изоморфизмом или может быть записан как $\theta = \theta_n \ldots \theta_1$, где каждый θ_k есть МРЕ. Поэтому из утверждения 1.13 легко следует, что теорема 1.14 эквивалентна следующему результату.

1.16. Теорема. Пусть $\theta : S \to\to T$ есть МРЕ. Тогда θ является или γ(H), или H эпиморфизмом.

Для того чтобы доказать предыдущие теоремы, нам потребуются следующие определения и лемма.

1.17. Определение. Пусть $\theta : S \to\to T$ —эпиморфизм. Тогда F класс J полугруппы S называется θ-*сингулярным,* если отображение θ взаимно однозначно на S — J.

1.18. Лемма. Пусть отображение $\theta : S \to\to T$ есть МРЕ. Тогда существует θ -сингулярный F - класс полугруппы S.

Доказательство. Пусть I_1 — максимальный (по включению) член из $\mathsf{F} = \{ I : I$ есть идеал полугруппы S и ограничение θ на I— взаимно однозначное отображение$\}$. $I_1 \neq S$, поскольку θ не является взаимно однозначным на полугруппе S. (F может быть пустым, но по соглашению мы будем рассматривать пустое множество $\varnothing$ как идеал.) Пусть J_1 будет ≤-минимальным элементом из $\{J : J$ есть F класс полугруппы S и $J \mid I_1 = \varnothing\}$. Пусть $I_2 = I_1 \cup J_1$. Тогда I_2— идеал полугруппы S, содержащий I_1 как собственное подмножество. Следовательно, по определению $I_1\theta$, ограниченный на I_2, не является взаимно однозначным.

Пусть (mod θ) будет отношением конгруэнтности на S, задаваемым как $s_1 \equiv s_2$ (mod θ), тогда и только тогда, когда $\theta(s_1) = \theta(s_2)$.

Определим отношение эквивалентности ≡ на S, полагая $s_1 \equiv s_2$ тогда только тогда, когда имеем $s_1 = s_2$ или $s_1, s_2 \in I_2$ и $\theta(s_1) = \theta(s_2)$. Легко проверить, что отношение ≡ является конгруэнтностью. Пусть $\theta_1 : S \to\to S/\equiv$ есть канонический гомоморфизм. Тогда очевидно, что равенство $\theta_1(s_1) = \theta_1(s_2)$ влечет $s_1 \equiv s_2$ (mod θ), поэтому в силу пункта б) замечания 1.10 существует такой эпиморфизм $\theta_2 : S/\equiv \to\to T$, что $\theta = \theta_2 \theta_1$. Но поскольку $\theta = \theta_1$ на I_2 и θ не взаимно однозначный на I_2, θ не является взаимно однозначным. Следовательно, θ_2 будет взаимно однозначным, так как θ есть МРЕ. Следовательюю, отношения ≡ и (mod θ) равны и J_1 есть θ -сингулярный F класс.

Доказательство теоремы 1.16. Эпиморфизм, представляющий собой $\gamma(\mathrm{H})$ и H эпиморфизм, есть изоморфизм. Пусть $\theta : S \to\to T$ есть МРЕ с θ-сингулярным F классом J. Если θ является $\gamma(\mathrm{H})$ эпиморфизмом, то требуемый результат получен, поэтому предположим противное.

Определим отношение эквивалентности ≡ на полугруппе S, полагая $s_1 \equiv s_2$ тогда и только тогда, когда s_1 H s_2 и $\theta(s_1) = \theta(s_2)$. Поскольку класс J θ-сингулярный, ограничивая это отношение на S — J, получаем $s_1 \equiv s_2$ тогда и только тогда, когда $s_1 = s_2$.

Проверим теперь, что ≡ представляет собой отношение конгруэнтности на S. Очевидно,что ≡ есть отношение конгруэнтности на S — J. Пусть $s_1 \equiv s_2$, s_1 и $s_2 \in J$. Пусть $x, y \in S^1$. Так как s_1 H s_2, то из результата Грина (см. утверждение 5 предыдушего микромодуля) известно, что или оба элемента xs_1y и xs_2y не принадлежат J, или xs_1yHxs_2y. В каждом случае $\theta(xs_1y) = \theta(xs_2y)$. Так как класс J θ-сингулярный, то если $xs_1y, xs_2y \in$ S—J, получим $xs_1y \equiv xs_2y$. Следовательно, ≡ есть отношение конгруэнтности. Поскольку θ не есть $\gamma(\mathrm{H})$ эпиморфизм, отношение ≡ не является тождественным.

Пусть теперь θ_1: $S \to\to S/\equiv$ будет каноническим эпиморфизмом. θ_1 есть H эпиморфизм, который не является взаимно однозначным. Кроме того, равенство $\theta_1(s_1) = \theta_1(s_2)$ влечет соотношение $s_1 \equiv s_2 \pmod{\theta}$. Поэтому так же, как и в доказательстве леммы 1.18, поскольку θ есть MPE, получаем равенство отношений $\equiv$ и $(\mathrm{mod}\ \theta)$. Тогда θ есть H эпиморфизм. Это доказывает теорему 1.16, а следовательно, и теорему 1.14.

1.19. Замечание. Предшествующая классификация MPE исключительно полезна для доказательства (и открытия) утверждений, справедливых для конечных полугрупп, методом рассмотрения «минимального контрпримера» (т. е. по индукции).

По индукции утверждение будет справедливо для каждого образа MPE, поэтому необходимо только «протащить утверждение через MPE» при помощи классифицирующей теоремы (опровергая, таким образом, существование контрпримера).

3.7. Полулокальная теория

В этом пункте произвольная конечная полугруппа разлагается в подпрямые произведения полугрупп, обладающих некоторыми важными свойствами; предлагаются методы построения гомоморфизмов полугрупп посредством действия на идеалы или F классы умножением слева или справа. Это дает переход к гомоморфным образам в терминах левых или правых переносов.

2.1. Определение. Пусть S, T_1, ..., T_n — полугруппы. S называется *подпрямым произведением* полугрупп T_1, ..., T_n (обозначается $S \leqslant\leqslant T_1 \times \ldots \times T_n$), если S есть (с точностью до изоморфизма) подполугруппа в $T_1 \times \ldots \times T_n$, такая, что $p_i(S) = T_i$, где p_i — отображение проекции на T_i, $i = 1, \ldots, n$.

2.2. Обозначения. Пусть $\varphi_i : S_i \to\to T$—эпиморфизм для $i = 1, \ldots, n$. Тогда отображение

$$\varphi_1 \times \ldots \times \varphi_n : S_1 \times \ldots \times S_n \to\to T_1 \times \ldots \times T_n$$

определяется с помощью соотношения

$$\varphi_1 \times \ldots \times \varphi_n (s_1, \ldots, s_n) = (\varphi_1(s_1), \ldots, \varphi_n(s_n)).$$

Пусть $\Delta : S \to S \times \ldots \times S$ (n раз) — мономорфизм, определяемый как $\Delta(s) = (s, \ldots, s)$. Пусть $\varphi_i : S \to\to T_i$ — эпиморфизм для $i = 1, \ldots, n$. Тогда отображение $\prod \varphi_i : S \to T_1 \times \ldots \times T_n$ есть гомоморфизм, определяемый как $\prod \varphi_i = (\varphi_1 \times \ldots \times \varphi_n)\,\Delta$.

Отметим, что $\Pi \varphi_i (S) \leqslant\leqslant T_1 \times \ldots \times T_n$. Тогда S будет подпрямым произведением полугрупп $T_1, \ldots, T_n$, если отображение $\Pi \varphi_i$ взаимно однозначное. Следовательно, можно разложить полугруппу S в подпрямое произведение, найдя совокупность гомоморфизмов $\{ \varphi_i \}$ на S, таких, что отображения $\Pi \varphi_i$ взаимно однозначны.

Следующий факт позволяет получить критерий для нахождения такой совокупности гомоморфизмов на S с помощью F классов полугруппы. Мы напомним определение идеала *F (J)* F класса *J* полугруппы 5 и определение идеала *B (J)*:

$$F(J) = \bigcup \{J' : J' \text{ есть } \mathcal{Y} \text{ класс для } S \text{ и } J \trianglelefteq J'\};$$
$$B(J) = \bigcup \{J' : J' \text{ есть } \mathcal{Y} \text{ класс для } S \text{ и } J' \not\trianglelefteq J\}.$$

2.3. Утверждение. Пусть $J_1, \ldots, J_n$— набор F классов полугруппы *S*, а $\{ \varphi_i : i = 1, \ldots, n)$ — гомоморфизмы на *S*, удовлетворяющие условиям:

1) отображения ϕ_r взаимно однозначные и ненулевые на J_i;

2) $\varphi_i [F(J_i)] = 0$, $i = 1, \ldots, n$.

Тогда отображения $\Pi \varphi_i$ взаимно однозначные и, следовательно,

$$S \leqslant\leqslant \varphi_1(S) \times \ldots \times \varphi_n (S).$$

Доказательство. Мы покажем, что отображение $\Pi\varphi_i$ взаимно однозначное. Пусть $s_i \in J_i$, $s_j \in J_j$ и предположим, что $s_i \neq s_i$. Если $i = j$, то $\varphi_i (s_i) \neq \varphi_i (s_i)$, так как φ_i является однозначным на J_i. Следовательно, $\Pi\varphi_i (s_i) \neq \Pi\varphi_i (s_j)$. Если $i \neq j$, то или $J_i \subseteq (J_j)$, или $J_j \subseteq (J_i)$ (возможно, оба включения выполняются одновременно). Без ограничения общности можно предположить, что выполняется первое включение. Тогда $\varphi_j (s_i) = 0$ и $\varphi_j (s_j) \neq 0$ и поэтому снова $\Pi\varphi_i (s_i) \neq \Pi\varphi_i (s_j)$.

Далее приведено одно из простых следствий утверждения 2.3.

2.4. Следствие. $S \leqslant\leqslant S/F (J_1) \times \ldots \times S/F (J_n)$.

Доказательство. Результат получается немедленно, поскольку канонические эпиморфизмы $\{\eta_i : S \twoheadrightarrow S/F (J_i) : i = 1, \ldots, n\}$ удовлетворяют условиям 1 и 2 из утверждения 2.3. Перейдем теперь к нахождению совокупности гомоморфизмов полугруппы S, которые будут минимальны по отношению к этим условиям.

2.5.Определение. Напомним определения гомоморфизмов $M_X^R: RI(X) \to F_R(X)$ и $M_X^L : LI(X) \to F_L(X)$. Гомоморфизм M_X^R переводит элемент *t*, такой, что $Xt \subseteq X$, и отображение $(x \to xt)$, а гомоморфизм M_X^L переводит элемент *t*, такой, что $tX \subseteq X$, в отображение $(x \to tx)$. Пусть *J* будет F классом полугруппы S и $\eta_J : S \twoheadrightarrow S/F(J)$— каноническим эпиморфизмом.

Отметим, что J^0 является единственным 0-минимальным идеалом полугруппы *S/F (J).* Определим

$$RM_J : S \to F_R(J^0), \text{ где } RM_J = M_J^{R_0} \eta_J$$

и

$$LM_J : S \to F_L(J^0), \text{ где } LM_J = M_J^{L_0} \eta_J.$$

Тогда, например,

$$LM_J(s)(j) = \begin{cases} sj, & \text{если } sj \in J, \\ 0, & \text{если } sj \notin J \end{cases} \quad \text{для всех } j \in J,$$

$$LM_J(s)(0) = 0.$$

Пусть J — нулевой F класс полугруппы S. Определим отображение $\psi_J : S \to\!\!\!\to J^0$, полагая

$$\psi_J(s) = \begin{cases} s, & \text{если } s \in J, \\ 0, & \text{если } s \notin J. \end{cases}$$

Пусть P_i обозначает разбиение, индуцированное на S, отображением ψ_i. Тогда согласно утверждению 1.7 P *(S, P_i)* имеет минимальный гомоморфный образ *(N_i, S/Q_i)*, где N_i (s_1) = N_i (s_2) тогда и только тогда, когда $\psi_J(\alpha s_1 \beta) = \psi_J(\alpha s_2 \beta)$ для всех $\alpha, \beta \in S^1$, N_J — единственный минимальный гомоморфизм на S, взаимно однозначный на J, разделяет J и $S - J$, а N_i *(F (J))* = {0}.

2.6. Предложение, а) Пусть J — регулярный F класс полугруппы S. Тогда $(LM_J \times RM_J)\,\Delta$. — единственный минимальный гомоморфизм полугруппы S, который является взаимно однозначным ненулевым на J и нулевым на *F (J).*

б) Пусть $J_1, ..., J_k$ — регулярные F классы и

$$J_{k+1}, \ \ldots, \ J_n$$

— нулевые F классы полугруппы S. Тогда

$$S \leqslant\!\!\leqslant LM_{J_1}(S) \times \ldots \times LM_{J_k}(S) \times RM_{J_1}(S) \times \ldots \times RM_{J_k}(S) \times$$
$$\times N_{J_{k+1}}(S) \times \ldots \times N_{J_n}(S).$$

в) (Щютценберже—Престон). Пусть S — регулярная полугруппа. Тогда S может быть представлена как подпрямое произведение полугрупп матриц, мономиальных по строкам и по столбцам. В частности, пусть $J_1, ..., J_n$ будут F классы полугруппы S и $J_i^0 \cong M_i^0$ *(G_i; A_i, B_i; C_i)*, $i = 1, ... n$. Тогда

$$S \leqslant\!\!\leqslant T_1 \times \ldots \times T_n \times T_1' \times \ldots \times T_n',$$

где T_i есть подполугруппа в $\mathscr{R}\mathscr{M}(|B_i|, G_i)$ и T_i' — подполугруппа в $\mathscr{C}\mathscr{M}(|A_i|, G_i)$, $i = 1, \ldots, n$. Или эквивалентно:

$$S \leqslant\leqslant W_1 \times \ldots \times W_n \times W_1' \times \ldots \times W_n'.$$

где W_i есть подполугруппа полугруппы—

$$(G_i^0, R(G_i^0)) \text{ w } (B_i^0, S_i) \text{ и } W_i'$$

подполугруппа полугруппы

$$(S_i', A_i^0) \text{ w}^* (L(G_i^0), G_i^0), i = 1, \ldots, n.$$

Доказательство, а) Пусть $\theta = (LM_J \times RM_J)\Delta$. Сперва покажем, что θ является взаимно однозначным ненулевым на J и $\theta[F(J)] = 0$. Пусть $a, b \in J$ и предположим, что $\theta(a) = \theta(b)$. Из этого следует, что для всех $j \in J$: 1) $ja = jb$ и 2) $aj = bj$ в $S/F(J)$. Тогда в силу равенства 1 aLb, и по регулярности класса J для a и b существует общая правая единица $e \in J$. Но в силу равенства (2) $a = ae = be = b$. Следовательно, θ взаимно однозначный на J и отображение θ ненулевое на J и нулевое на $F(J)$.

Пусть теперь Q_L и Q_R будут отношениями конгруэнтности, ассоциированными с LM_j и RM_j соответственно. Тогда $Q_L \mid Q_R$ — отношение конгруэнтности, ассоциированное с θ. Пусть φ—любой гомоморфизм на S, взаимно однозначный ненулевой на J и такой, что $\varphi[F(J)] = 0$. Мыдолжны показать, что отношение $s_1 \not\equiv s_2 \pmod{Q_L \cap Q_R}$ влечет $\varphi(s_1) \neq \varphi(s_2)$.

Предположим, что $s_1 \not\equiv s_2 \pmod{Q_L}$. Тогда существует элемент $j \in J$, такой, что $s_1 j \neq s_2 j$ в $S/F(J)$.

Но $s_1 j, s_2 j \in J^0$, где J^0 есть 0-минимальный идеал полугруппы $S/F(J)$ и φ является взаимно однозначным на J^0. Следовательно, $\varphi(s_1 j) \neq \varphi(s_2 j)$, откуда следует, что $\varphi(s_1) \neq \varphi(s_2)$. Аналогично $s_1 \not\equiv s_2 \pmod{Q_R}$ влечет $\varphi(s_1) \neq \varphi(s_2)$, поэтому $s_1 \not\equiv s_2 \pmod{Q_L \mid Q_R}$ влечет $\varphi(s_1) \neq \varphi(s_2)$.

б) Этот пункт следует из пункта а).

в) Заметим, что $RM_j(S)$ есть подполугруппа правых сдвигов на J^0, $RT(J^0)$ и $LM_J(S) \subseteq LT(J^0)$. Результат теперь следует из утверждений 5 и 6, приведенных в предыдущем модуле, и из пункта б).

2.7. Замечание. Предположим теперь, что для J задано фиксированное матричное представление, т. е. имеется изоморфизм $J^0 \cong \mathscr{M}^0(G; A, B; C)$. Заметим, что два элемента эквивалентны относительно $Q_L \mid Q_R$ тогда и только тогда, когда они действуют одинаково слева и справа на J. Пользуясь обозначениями, применявшимися для описания

левых и правых переносов регулярных рисовских полугрупп матричного типа (см. утверждение 4 из предыдущего модуля), и рассматривая умножение на s_1 и s_2 как переносы, найдем, что

$$s_1 \equiv s_2 \pmod{Q_L \cap Q_R}$$

тогда и только тогда, когда

$$\psi_R(s_1) = \psi_R(s_2),\ \psi_L(s_1) = \psi_L(s_2),\ \delta(s_1) = \delta(s_2)$$

и

$$\lambda(s_1) = \lambda(s_2).$$

Однако $RM_J(s)$ и $LM_J(s)$ связаны для всех элементов $s \in S$. Опираясь на пункт г) утверждения 4 из предыдущего модуля, мы получим, что если ψ_R, ψ_L и δ совпадают на элементах s_1 и s_2, то λ совпадает на элементах s_1 и s_2. Это наводит на мысль, что имеется некоторое удваивание информации при описании $(LM_J \times RM_J)\Delta$ как гомоморфизма, ассоциированного с $Q_L \cap Q_R$. Исследуем это подробно и дадим явное определение.

2.8. Определение. Пусть S — полугруппа с регулярным F классом *J*.

а) Определим $LLM_J : S \to [S/F(J)]/\equiv_L$, где для всех элементов $s_1, s_2 \in S/F(J)$ $s_1 \equiv_L s_2$ тогда и только тогда, когда $s_1 x R s_2 x$ в *S/F(J)* для всех элементов $x \in J$. Следовательно, $s_1 \equiv {}_L s_2$ тогда и только тогда, когда они действуют одинаково на левые символы, т. е. тогда и только тогда, когда $\psi_L(s_1) = \psi_L(s_2)$. Легко показать, что $\equiv_L$ есть отношение конгруэнтности.

б) Аналогично определим $RLM_J : S \to [S/F(J)]/\equiv_R$, где для всех элементов $s_1, s_2 \in S/F(J)$ $s_1 \equiv {}_R s_2$. тогда и только тогда, когда $x s_1 L x s_2$ в *S/F (J)* для всех $x \in J$. Следовательно, $s_1 \equiv {}_R s_2$ тогда и только тогда, когда $\psi_R(s_1) = \psi_R(s_2)$.

2.9. Утверждение. а) $(LLM_j \times RM_j)\Delta$. индуцирует $Q_L \cap Q_R$.

б) $(LM_i \times RLM_i)\Delta$ индуцирует $Q_L \cap Q_R$.

Доказательство. Очевидно, что отношение $s_1 \equiv s_2 \bmod (Q_L \cap Q_R)$ влечет

$$[LLM_J(s_1), RM_J(s_1)] = [LLM_J(s_2), RM_J(s_2)].$$

Наоборот, предположим, что $(LLM_J \times RM_J)\Delta(s_1) = (LLM_J \times RM_J)\Delta(s_2)$. Тогда ψ_L, ψ_R и δ согласуются на s_1 и s_2. Предположим, что $\lambda(s_1)(a) = 0$. Из этого следует, $\psi_L(s_1)(a) = 0$, последнее в свою очередь влечет $\psi_L(s_2)(a) = 0$. Следовательно, $\lambda(s_2)(a) = 0$. Предположим,

что $\lambda(s_1)(a) \neq 0$. Тогда $\psi_L(s_1)(a) \neq 0$ и в силу связывающего уравнения [см. пункт г) утверждения 4 из предыдущего модуля и регулярности класса J существует такой элемент $b \in B$, что

$$\lambda(s_1)(a) = C[b, \psi_L(s_1)(a)]^{-1} \delta(s_1)(b) C[\psi_R(s_1)(b), a] = C[b, \psi_L(s_2)(a)]^{-1}$$

$$\delta(s_2)(b) C[\psi_R(s_2)(b), a] = \lambda(s_2)(a).$$

Следовательно, $s_1 \equiv s_2 \bmod (Q_L \cap Q_R)$.

б) Доказательство аналогично пункту а).

2.10. Замечание. Таким образом, мы получили на полугруппе S/F (J) отношения конгруэнтности, которые отождествляют два элемента, если они одинаково действуют на левые и правые символы. Соответственно и отношение $Q_L \cap Q_R$ содержится в обоих из них. Мы хотели бы найти третий гомоморфизм полугруппы S, такой, что его комбинация с LLM_j и с RLM_j давала бы $Q_L \cap Q_R$. Этот новый гомоморфизм обязательно говорил бы что-нибудь о том, как два элемента действуют на групповую координату.

2.11. Определение. Пусть J — регулярный F класс полугруппы S. Определим гомоморфизм $GGM_J : S \to\!\!\!\!\to [S/F(J)]/\equiv$, полагая $s_1 \equiv s_2$ тогда и только тогда, когда $x_1 s_1 x_2 = x_1 s_2 x_2$ в $S/F(J)$ для всех элементов $x_1, x_2 \in J$. Очевидно, $\equiv$ есть отношение конгруэнтности.

Мы назовем F класс *комбинаторным* тогда и только тогда, когда он не содержит нетривиальных групп. В противном случае F класс называется некомбинаторным (т. е. F класс будет некомбинаторным тогда и только тогда, когда он содержит нетривиальную группу). Следовательно, комбинаторные F классы являются нулевыми или регулярными с одноэлементными H классами.

Эквивалентно: F класс J комбинаторный тогда и только тогда, когда полугруппа J^0 комбинаторная, и J некомбинаторный тогда и только тогда, когда полугруппа J^0 не является комбинаторной.

Определим гомоморфизм GM_j полугруппы S, полагая

$$GM_J(S) = \begin{cases} GGM_J(S), & \text{если } J \text{ некомбинаторный}, \\ \{0\}, & \text{если } J \text{ комбинаторный}. \end{cases}$$

2.12. Предложение. а) $(LLM_J \times GM_J \times RLM_J)\Delta$ индуцирует

$$Q_L \cap Q_R.$$

б) Пусть $J_1, \ldots, J_k$ — регулярные F классы полугруппы S и $J_{k+1}, \ldots, J_n$ — нулевые F классы полугруппы S. Тогда

$$S \leqslant\leqslant \Pi\{LLM_{J_i}(S) : i = 1, \ldots, k\} \times \Pi\{GM_{J_i}(S) : i = 1, \ldots, k\}$$
$$\times \Pi\{RLM_{J_i}(S) : i = 1, \ldots, k\} \times \Pi\{N_{J_i}(S) : i = k+1, \ldots, n\}.$$

Доказательство, а) Предположим, что регулярный F класс J комбинаторный, т. е. H классы, принадлежащие J, состоят из одного элемента. Тогда по определению $GM_J(S) = \{0\}$. Поэтому равенство влечет

$$(LLM_J \times GM_J \times RLM_J)\Delta(s_1) = (LLM_J \times GM_J \times RLM_J)\Delta(s_2)$$

только $\psi_R(s_1) = \psi_R(s_2)$ и $\psi_L(s_1) = \psi_L(s_2)$. Но этого ужедостаточно. Предположим, что $\psi_R(s_1)(b) = 0 = \psi_R(s_2)(b)$. Тогда $\delta(s_1)(b) = \delta(s_2)(b) = 0$. Если $\psi_R(s_1)(b) = \psi_R(s_2)(b) \neq 0$, то $\delta(s_1)(b) = \delta(s_2)(b) = 1$, так как J комбинаторный. Аналогично: из равенства $\psi_L(s_1) = \psi_L(s_2)$ следует, что $\lambda(s_1) = \lambda(s_2)$. Поэтому если Q есть конгруэнтность, индуцированная $(LLM_J \times GM_J \times RLM_J)\Delta$ на S, то $Q \subseteq Q_L \cap Q_R$. Очевидно, что $Q_L \cap Q_R \subseteq Q$.

Тепеоь предположим, что класс J некомбинаторный, так что $GM_J(S) = GGM_J(S)$. Пусть $s_1, s_2 \in S$ и предположим, что $GM_i(s_1) = GM_i(s_2)$. Пусть $(g, a, b), (h, c, d) \in J$. Тогда, поскольку $(g, a, b)s_1(h, c, d) = (g, a, b)s_2(h, c, d)$, мы имеем

$$\delta(s_1)(b)\, C[\psi_R(s_1)(b), c] = \delta(s_2)(b)\, C[\psi_R(s_2)(b), c] \qquad (1)$$

и

$$C[b, \psi_L(s_1)(c)]\,\lambda(s_1)(c) = C[b, \psi_L(s_2)(c)]\,\lambda(s_2)(c). \qquad (2)$$

Если теперь $RLM_J(s_1) = RLM_J(s_2)$, то $\psi_R(s_1) = \psi_R(s_2)$. Если $\psi_R(s_1)(b) = 0$, то оба элемента $\delta(s_1)(b)$ и $\delta(s_2)(b)$ будут равны нулю.

Если $\psi_R(s_1)(b) \neq 0$, то существует элемент $c \in A$, такой, что $C[\psi_R(s_1)(b), c] \neq 0$, и в силу соотношения (1) $\delta(s_1)(b) = \delta(s_2)(b)$. Аналогично из равенства $LLM_J(s_1) = LLM_J(s_2)$ вытекает $\lambda(s_1) = \lambda(s_2)$. Следовательно, $Q \subseteq Q_L \cap Q_R$. С другой стороны, нетрудно показать, что $Q_L \cap Q_R \subseteq Q$, таким образом, пункт а) доказан.

б) Этот пункт следует из предложения 2.6 и пункта а), так как для регулярного класса J конгруэнтности $(LLM_J \times GM_J \times RLM_J)\Delta$ и $(LM_J \times RM_J)\Delta$ равны.

Исследуем теперь природу полугрупп

$$RM_J(S),\ LM_J(S),\ RLM_J(S),$$
$$LLM_J(S),\ GGM_J(S) \text{ и } GM_J(S).$$

2.13. Утверждение. Пусть $J \neq \{0\}$ — регулярный F класс полугруппы S.

а) Ограничение гомоморфизма RM_J на подгруппы (следовательно, H классы) класса J взаимно однозначно. $RM_J(S)$ имеет единственный 0-минимальный регулярный идеал I, который представляет собой образ $J \cup F(J)$, и каждый элемент из $RM_J(S)$ есть отдельный правый перенос идеала J. Таким образом, гомоморфизм M^R_I будет взаимно однозначным на $RM_J(S)$.

б) Ограничение гомоморфизма LM_J на подгруппы (следовательно, H классы), принадлежащие классу J, взаимно однозначно. $LM_J(S)$ имеет единственный 0-минимальный регулярный идеал I, представляющий собой образ $J \cup F(J)$, и M^L_I — взаимно однозначный гомоморфизм на $LM_J(S)$.

в) $RLM_J(S)$ содержит единственный 0-минимальный регулярный комбинаторный идеал I, являющийся образом $J \cup F(J)$, и M^R_I — взаимно однозначный гомоморфизм на $RLM_J(S)$.

г) $LLM_J(S)$ содержит единственный 0-минимальный регулярный комбинаторный идеал I, являющийся образом $J \cup F(J)$, и M^L_I — взаимно однозначный гомоморфизм на $LLM_J(S)$.

д) Ограничение гомоморфизма GGM_J на подгруппы (следовательно, H классы), принадлежащие классу J, взаимно однозначно. $GGM_J(S)$ содержит единственный 0-минимальный регулярный идеал I, который представляет собой образ $J \cup F(J)$, M^L_I и M^R_I — взаимно однозначные гомоморфизмы на $GGM_J(S)$.

е) Полугруппа $GM_J(S)$ или совпадает с $\{0\}$, или равна $GGM_J(S)$. Если $GM_J(S) = GGM_J(S)$, то I —не комбинаторный идеал.

Доказательство. Мы будем доказывать, что M^R_I — взаимно однозначный гомоморфизм на $RM_J(S)$. Другие утверждения следуют из определения RM_J.

Пусть $RM_J(s_1)$ и $RM_J(s_2)$ таковы, что $(i)RM_J(s_1) = (i)RM_J(s_2)$ для всех $i \in I - \{0\}$. Так как J отображается на $I = \{0\}$, это эквивалентно тому, что $RM_J(js_1) = RM_J(js_2)$ для всех $j \in J$. Следовательно, для всех $j_1 \in J$ мы имеем $j_1(js_1) = j_1(js_2)$ в $S/F(J)$. Так как класс J регулярный, для каждого элемента j существует левая единица, например e_j. Тогда $e_j js_1 = e_j js_2$ в $S/F(J)$, поэтому $js_1 = js_2$ в $S/F(J)$ для всех $j \in J$. Следовательно, $RM_J(s_1) = RM_J(s_2)$ и M^R_I — взаимно однозначный гомоморфизм на $RM_J(S)$.

Доказательство пунктов б) — е) основывается на доказательстве пункта а).

Теперь дадим наименования полугруппам, обладающим рассмотренными свойствами.

2.14. Определение. а) S называется *отображающей справа* полугруппой *(RM),* если она содержит минимальный или 0-минимальный идеал I, для которого M_I^R — взаимно однозначный гомоморфизм.

б) S называется *отображающей слева* полугруппой *(LM),* если она содержит минимальный или 0-минимальный идеал, для которого M_I^L — взаимно однозначный гомоморфизм.

в) S называется *отображающей справа символьной* полугруппой *(RLM),* если S есть *RM* полугруппа, идеал I которой будет комбинаторным (см. пункт в) утверждения 2.15).

г) S называется *отображающей слева символьной* полугруппой *(LLM),* если S есть *LM* полугруппа, идеал I которой будет комбинаторным.

д) *S* называется *обобщенной групповой отображающей* полугруппой *(GGM),* если S есть *RM* и *LM* полугруппа.

е) S называется *групповой отображающей* полугруппой *(GM),* если *S* есть *GGM* полугруппа, идеал I которой будет некомбинаторным.

2.15. Утверждение. а) Пусть J — регулярный F класс полугруппы *S*. Тогда

$RM_J(S)$, $LM_J(S)$, $RLM_J(S)$, $LLM_J(S)$, $GGM_J(S)$ и $GM_J(S)$— соответственно *RM, LM, RLM, LLM, GGM* и *GM* полугруппы. Кроме того, *GM, GGM* и *LLM* полугруппы будут *LM* полугруппами и *GM, GGM* и *RLM* полугруппы будут *RM* полугруппами. Если S есть *GGM* полугруппа, не являющаяся *GM* полугруппой, то *S* есть и *RLM* и *LLM* полугруппа.

б) Если $S\neq\{0\}$, то идеал I, упоминающийся в каждом пункте определения 2.14, необходимо будет регулярным и ненулевым.

в) Пусть I — минимальный или 0-минимальный идеал полугруппы $S\neq\{0\}$, для которого M_I^R или M_I^L — взаимно однозначный гомоморфизм. Тогда I будет единственным (кроме, быть может, 0) минимальным или 0-минимальным идеалом полугруппы *S*. Следовательно, идеал I в каждом пункте определения 2.14 будет единственным.

Доказательство, а) Этот пункт следует из утверждения 2,13,

б) Предположим, что не равный нулю F класс в I является нулевым. Тогда $M_I^R(I) = 0$ и $M_I^L = 0$. В каждом пункте определения 2.14 одно из отображений M_I^R или M_I^L было взаимно однозначным. Таким образом, $I=\{0\}$ противоречит сделанному предположению.

в) Предположим $S \neq \{0\}$ и M_I^R является взаимно однозначным на *S*, $I \neq \{0\}$, Пусть *I* — другой 0-минимальный идеал полугруппы *S*. Так как $I \neq \{0\}$, то $M_I^R(J) \neq \{0\}$ и поэтому идеал $IJ \neq \{0\}$. Но $I \supseteq IJ$ и $J \supseteq IJ$, так что $I = IJ = J$ в силу минимальности. Аналогично проводится доказательство, когда взаимно однозначно отображение M^L.

2.16. Обозначения. а) Пусть S — полугруппа. Определим $S^\# = S^0 - \{0\}$. Другими словами, $S^\#$ — ненулевая часть полугруппы S.

Единственный регулярный минимальный или 0-минимальный идеал *I* в *RM, LM, RLM, LLM, GM* или *GGM* полугруппе называется *отмеченным идеалом,* и $I^\#$ называется *отмеченным* F *классом.*

б) Часто в тех случаях, когда нет неясности, на каком F классе определяется гомоморфизм, *J* индексирует гомоморфизмы. Например, $RLM[GM_J(S)]$ означает взятие *RLM* для *GMj (S)* по отношению к отмеченному F классу.

2.17. Предложение. а) Пусть *S* — регулярная полугруппа. Тогда *S* может быть записана как подпрямое произведение *GM, RLM* и *LLM* полугрупп.

б) Пусть *T* будет *RM* полугруппой с отмеченным F классом *J*. Пусть *G* — максимальная подгруппа в *J* и *B* — множество *L* классов в *J*. Тогда

$$T \subseteq (G^0, R(G^0))\mathrm{w}(B^0, RLM_J(T)).$$

в) Пусть *T* будет *LM* полугруппой с отмеченным F классом *J*. Пусть *G* — максимальная подгруппа в *J* и *A* — множество R классов в *J*. Тогда

$$T \subseteq (LLM_J(T), A^0)\mathrm{w}^*(L(G^0), G^0).$$

г) Полугруппа S является *RM* полугруппой тогда и только тогда, когда *r(S)* есть *LM* полугруппа. В общем случае, однако, $RM_J(T)$ не будет антиизоморфна $LM_J(T)$.

Доказательство, а) Этот пункт следует из утверждения 2.15 и предложения 2.12.

б) Пусть $I = J \cup \{0\}$.Так как гомоморфизм M_I^R взаимно однозначный на *T,* каждый элемент из *T* будет отдельным правым переносом на *I*. Следовательно, в силу утверждения 2.16 из гл. 7

$$T \subseteq (G^0, R(G^0))\,\mathrm{w}\,(B^0, S),$$

где

$$S = \{f \in F_R(B^0) : f(0) = 0\}.$$

Рассматривая теперь каждый элемент полугруппы T как элемент узлового произведения, легко видеть, что два элемента имеют одинаковую первую координату тогда и только тогда, когда они одинаково действуют на правые символы. Но это есть определение RLM_J. Очевидно, что $RLM_J(T) \subseteq S$, поэтому легко видеть, что

$$T \subseteq (G^\circ, R(G^0)) \mathrm{w} (B^0, RLM_J(T)).$$

в) С помощью рассуждений, дуальных пункту б), доказывают пункт в).

г) Первое утверждение очевидно. Рассмотрим следующий контрпример, показывающий, что $RM_J(T)$ и $LM_J(T)$ могут не быть антиизоморфны. Пусть

$$T = \mathcal{M}^0(\{1\}; A, B; C),$$

где

$$A = \{a_1, a_2, a_3\}, B = \{b_1, b_2\}$$

и

$$C = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Тогда легко проверить, что $LM(T) = T$, в то время как $RM(T) \cong \mathcal{M}^0(\{1\}; \{1, 2\}; \{1, 2\}; I)$, где I есть единичная матрица порядка 2×2. Следовательно, $|LM(T)| \neq |RM(T)|$.

Мы предлагаем теперь другой пример, в котором S есть GM полугруппа, представляющая собой объединение групп с отмеченным F классом T. Покажем, что $RLM_T(S)$ не будет антиизоморфна $LLM_T(S)$.

Пусть $\mathbf{Z}_2$—группа из двух элементов $\{1, -1\}$ по умножению. Пусть $T = \mathcal{S}_{22}(\mathbf{Z}_2, C)$, где

$$C = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Пусть $S = \mathbf{Z}_2 \cup T$ — новая полугруппа со следующим законом умножения: $\mathbf{Z}_2$ и T— подполугруппы в S; $1 \in \mathbf{Z}_2$ есть единица S и

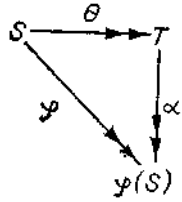
$$RM_T(-1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{RM}(2, \mathbf{Z}_2),$$

$$LM_T(-1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{CM}(2, \mathbf{Z}_2).$$

Теперь можно проверить, что S есть GM полугруппа, являющаяся объединением групп с отмеченным идеалом T. Однако некоторые вы-

численния показывают, что $|RLM_T(S)| = 4$, в то время как $|LLM_T(S)|=3$. Следовательно, $RLM_T(S)$ и $LLM_T(S)$ не будут антиизоморфны.

2.18. Определение. а) Напомним определение максимального собственного эпиморфизма (MPE) полугруппы S (см. определение 1.15). Мы говорим, что *S* имеет единственный максимальный собственный эпиморфизм (UMPE) (Unique maximal proper epimorphism) $\theta : S \to\to T$, если для всех собственных (т. е. не взаимно однозначных) эпиморфизмов $\varphi : S \to\to \varphi(S)$ существует эпиморфизм $\alpha : T \to\to \varphi(S)$, такой, что $\varphi = \alpha\theta$, т. е. представленная диаграмма коммутативна.



б) Полугруппа S называется *неразложимой относительно подпрямого произведения,* если из соотношения $S \leqslant\leqslant S_1 \times \ldots \times S_n$ вытекает $S \cong S_i$ для некоторого $i = 1, ..., n$.

2.19. Лемма. а) *S* имеет UMPE тогда и только тогда, когда 5 неразложима относительно подпрямого произведения. Следовательно, S может быть записана как под-прямое произведение UMPE полугрупп.

б) Пусть *S* неразложима относительно подпрямого произведения, или *S* содержит ненулевой комбинаторный идеал *I*, так что $| S/I | < | S |$, или *S* есть *GM* полугруппа.

Доказательство, а) Пусть S имеет UMPE, скажем θ. Пусть $S \leq S_1 \times ... \times S_n$ и p_i — гомоморфизм, являющийся *i*-й проекцией. Тогда $p_i(S) = S_i$ и отображение $\Pi p_i = (p_1 \times \ldots \times p_n)\Delta$ взаимно однозначно на S. Предположим, что каждый p_i является собственным гомоморфизмом. Тогда существуют q_i, такие, что $p_i = q_i\theta$ для всех $i = 1, ..., n$.

Тогда

$$(p_1 \times \ldots \times p_n)\Delta = (q_1\theta \times \ldots \times q_n\theta)\Delta = (q_1 \times \ldots \times q_n)\Delta\theta.$$

Πp_i не является взаимно однозначным, так как θ — не взаимно однозначное отображение. Это противоречие. Следовательно, для некоторого $i = 1, ..., n$ p_i будет изоморфизмом и $S \cong S$. Наоборот,

предположим, что S неразложима относительно подпрямого произведения. Пусть $\{\varphi_i : i = 1, ..., n)$ — множество всех собственных гомоморфизмов на S. По предложению $\Pi\varphi_i$ не является взаимно однозначным на S, если бы это имело место, то $\varphi_i(S) \cong S$ для некоторого i=1, ..., n. Легко проверить, что $\Pi\varphi_i = (\varphi_1 \times \ldots \times \varphi_n)\Delta$ есть UMPE полугруппы S.

б) В силу предложения 2.12 и пункта а) S представляется как *Nj(S)* для некоторого нулевого F класса *J* или S есть *RLM, LLM* или *GM* полугруппа. В первых трех случаях *S* содержит нулевой комбинаторный идеал. Лемма доказана.

Продолжим описание полугрупп с помощью единственного максимального собственного эпиморфизма.

2.20. Лемма. Пусть полугруппа S имеет единственный максимальный собственный эпиморфизм, например θ.

а) S содержит единственный 0-минимальный идеал I и θ является взаимно однозначным на S— $I^{\#}$. Нет собственного эпиморфизма полугруппы S, взаимно однозначного на $I^{\#}$.

б) Пусть S—регулярная полугруппа. Тогда или $S \cong RLM_{I^{\#}}(S)$, $S \cong LLM_{I^{\#}}(S)$, или $S \cong GM_{I^{\#}}(S)$.

Доказательство, а) Пусть Q* — отношение конгруэнтности, ассоциированное с θ. Если Q — любое другое отношение конгруэнтности, ассоциированное с собственным гомоморфизмом φ на *S*, то $Q^* \subseteq Q$. Теперь, поскольку $Q^*=Q^* \cap Q$, мы имеем $(\theta \times \varphi)\Delta = \theta$ для всех собственных гомоморфизмов φ на *S*.

Пусть $I \neq \{0\}$ — любой собственный идеал полугруппы S и $\eta : S \to\to S/I$. Предположим что θ является взаимно однозначным на *I*. Тогда $(\theta \times \eta)\Delta$ будет взаимно однозначным на S. Но $(\theta \times \eta)\Delta = \theta$ и θ не является взаимно однозначным на S. Это противоречие. Следовательно, θ не будет взаимно однозначным на любом собственном идеале полугруппы S.

Пусть I есть 0-минимальный идеал. Тогда, поскольку θ не является взаимно однозначным на I в соответствии с леммой 1.18, θ будет взаимно однозначным на S— $I^{\#}$. Следовательно, если бы полугруппа S содержала другой 0-минимальный идеал, отображение θ было бы взаимно однозначным на нем. Это противоречие. Следовательно, I единственный.

Если φ — собственный гомоморфизм, взаимно однозначный на *I*, то $(\theta \times \varphi)\Delta = \theta$ будет взаимно однозначным отображением на *I*.

Это противоречие. Пункт а) полностью доказан.

б) Пусть S — регулярная полугруппа. Тогда ее единственный 0-минимальный идеал I будет регулярным. Тогда отображение $(LLM_{I\#} \times \times GM_{I\#} \times RLM_{I\#})\Delta$ взаимно однозначно на I и, следовательно, в силу пункта а) взаимно однозначно на S, т. е.

$$S \leqslant\leqslant LLM_{I\#}(S) \times GM_{I\#}(S) \times RLM_{I\#}(S).$$

Следовательно, по лемме 2.19 (пункта)) доказано все, что требовалось. Теперь более внимательно рассмотрим *RM* и *LM* полугруппы.

2.21. Определение. Пусть $C : B \times A \to G^0$ есть структурная матрица для рисовской полугруппы матричного типа. Две строки матрицы C называются *пропорциональными (слева),* если существует элемент $g \in G$, такой, что $gC(b_1, a) = C(b_2, a)$ для всех $a \in A$. Два столбца матрицы C называются *пропорциональными (справа),* если существует элемент $g \in G$, такой, что $C(b, a_1)g = C(b, a_2)$ для всех $b \in B$.

2.22. Утверждение. а) Пусть S есть LM полугруппа с отмеченным идеалом I. Предположим, что $I^0 \cong \mathcal{M}^0(G; A, B; C)$. Тогда двух пропорциональных (слева) строк структурной матрицы C не существует.

б) Пусть S — полугруппа и I — регулярный F класс полугруппы S с $J^0 \cong \mathcal{M}^0(G; A, B; C)$. Тогда LM_J отождествляет L классы, принадлежащие J, если ассоциированные строки матрицы C пропорциональны.

в) Пусть S есть RM полугруппа с отмеченным идеалом I. Предположим, что $I^0 \cong \mathcal{M}^0(G; A, B; C)$. Тогда двух пропорциональных (справа) столбцов структурной матрицы C не существует.

г) Предположим ситуацию пункта б). RM_J отождествляет R классы, принадлежащие J, если соответствующие столбцы матрицы C пропорциональны.

д) Пусть S есть GGM полугруппа с отмеченным идеалом I. Предположим, что $I^0 \cong \mathcal{M}^0(G; A, B; C)$. Тогда двух пропорциональных (слева) строк и двух пропорциональных (справа) столбцов матрицы C не существует.

е) Предположим ситуацию пункта б). GGM_J отождествляет R классы, принадлежащие J, если соответствующие столбцы матрицы C пропорциональны, и отождествляет L классы, принадлежащие J, если соответствующие строки матрицы C также пропорциональны.

Доказательство, а) Предположим, что две строки матрицы C пропорциональны, т. е. для некоторых b_1, b_2, $b_1 \neq b_2$ существует элемент $g_1 \in G$, такой, что $g_1C(b_1, a) = C(b_2, a)$ для всех a d A. Тогда для всех

$(g, a, b) \in I$ $(g_1, a, b_1)(g, a, b) = (1, a, b_2)(g, a, b)$, т. е. $M_I^L(g_1, a, b_1) = M_I^L(1, a, b_2)$. Но $M^L{}_I$ является взаимно однозначным. Это противоречие.

б) Заметим, что если две строки матрицы C пропорциональны, то такие же две строки любой другой структурной матрицы для J^0 будут также пропорциональны. Далее в силу утверждения 8 из предыдущего микромодуля все новые структурные матрицы P для J^0 задаются соотношением

$$P(b, a) = \delta(b) C(b, a) \lambda(a).$$

Поэтому если $C(b_1, a) = gC(b_2, a)$ для всех $a \in A$, то

$$P(b_1, a) = \delta(b_1) C(b_1, a) \lambda(a) = \delta(b_1) g C(b_2, a) \lambda(a) =$$
$$= \delta(b_1) g \delta(b_2)^{-1} \delta(b_2) C(b_2, a) \lambda(a) = \delta(b_1) g \delta(b_2)^{-1} P(b_2, a) =$$
$$= g' P(b_2, a) \text{ для всех } a \in A.$$

Пусть I —отмеченный идеал в $LM_J(S)$. Тогда $LM_J(J) = I^\#$. Нормализуем структурные матрицы для J^0 и I так, чтобы гомоморфизм LM_J на $J0$ описывался в нормализованной форме, определяемой соотношениями (3.3) и (3.4) из предложения 1 предыдущего микромодуля. Если тогда $J^0 \cong \mathcal{M}^\circ(G; A, B; C)$, то мы имеем

$$I \cong \mathcal{M}^0(\omega(G); \psi_L(A), \psi_R(B); Q).$$

Предположим теперь, что $C(b_1, a) = gC(b_2, a)$ для всех $a \in A$. Тогда, поскольку $\omega[C(b, a)] = Q[\psi_R(b), \psi_L(a)]$, мы имеем $Q[\psi_R(b_1), \psi_L(a)] = \omega(g) Q[\psi_R(b_2), \psi_L(a)]$ для всех $\psi_L(a) \in \psi_L(A)$. В силу пункта а) из этой формулы вытекает, что $\psi_R(b_1) = \psi_R(b_2)$ (и $g \in \ker\omega$), из последнего соотношения в свою очередь следует, что L классы L_{b1} и L_{b2} из J отождествляются при LM_J.

Пункты в) и г) доказываются посредством рассуждений, дуальных к пунктам а) и б) соответственно.

Пункт д) следует из пунктов а) и в), так как GGM полугруппа является и RM и LM полугруппой.

Опираясь на доказательство пункта д), доказываем пункт е) точно так же, как пункты б) и г). Для другого доказательства можно воспользоваться фактом, что

$GGM_J(S) \cong RM[LM_J(S)] \cong LM[RM_J(S)]$ (см. 2.3).

Пусть S будет GGM полугруппой с отмеченным идеалом I. Тогда, если известно, как элемент полугруппы S действует справа на I, это

полностью определяет, как он действует на I слева. Если $0 \in I$ и $I^{\#}$ — простая полугруппа, то 0 выключается из S, т. е. S — {0} будет подполугруппой полугруппы S. Эти факты доказываются далее.

2.23. Утверждение. Пусть S есть *GM* полугруппа с отмеченным идеалом I. Тогда справедливы следующие положения:

а) пусть элемент $s \in S$. В этом случае xs известен для всех элементов $x \in I$ тогда и только тогда, когда sx известен для всех $x \in I$;

б) если $0 \in S$ и $I^{\#}$ — простая полугруппа, то S — {0} есть подполугруппа полугруппы S,

Доказательство, а) Пусть $s \in S$, $s \neq 0$ и $\psi_R(s)$, $\psi_L(s)$, $\delta(s)$ и $\lambda(s)$ — функции, описывающие действие умножения справа и слева на $I \cong M^0(G; A,B; C)$. Так как умножения слева и справа на элемент s связаны, мы имеем

$$\delta(b)C[\psi_R(b), a] = C[b, \psi_L(a)]\lambda(a) \tag{3}$$

для всех $a \in A$, $b \in B$,

где элемент s для удобства опущен из обозначений $[$т. е. $\psi_R(b) \equiv \psi_R(s)(b)]$.

Предположим теперь, что мы знаем, как s действует справа на I, т. е. $\psi_R(b)$ и $\delta(b)$ известны для всех $b \in B$. Нужно показать, что это полностью определяет $\psi_L(a)$ и $\lambda(a)$ для всех $a \in A$. Предположим, что ψ_L, λ и ψ_L', λ' — два возможных множества функций, описывающих действие s слева на I, удовлетворяющее соотношению (2.3). Фиксируя элемент $a \in A$ из (3), мы получаем

$$f(b) = C[b, \psi_L(a)]\lambda(a) = C[b, \psi_L'(a)]\lambda'(a) \text{ для всех } b \in B. \tag{4}$$

Если $f(b)$ равно нулю для всех элементов $b \in B$, то $\psi_L(a) = 0$ в силу регулярности C. Из этого следует, что $\psi_L'(a) = 0$, $\lambda(a) = 0$ и $\lambda'(a) = 0$. Поэтому $\psi_L(a) = \psi_L'(a) = 0$ и $\lambda(a) = \lambda'(a) = 0$ в этом случае. Если существует элемент $b \in B$, такой, что $I(b)$ не равно нулю, то $\psi_L(a)$, $\psi_L'(a)$, $\lambda(a)$ и $\lambda'(a)$ также не равны нулю. Тогда

$$C[b, \psi_L(a)] = C[b, \psi_L'(a)]\lambda'(a)\lambda(a)^{-1}. \tag{5}$$

Следовательно, столбцы $\psi_L(a)$ и $\psi_L'(a)$ матрицы C пропорциональны справа. Но S есть *GGM* полугруппа, поэтому в силу утверждения 2.22 $\psi_L(a) = \psi_L'(a)$ и, следовательно, $\lambda(a) = \lambda'(a)$. Таким образом, существует только одно решение. Для определения значений $\psi_L(a)$ и $\lambda(a)$ рассмотрим известную величину $f(b)$. Согласно (4) $f(b)$ пропорционален справа столбцу $\psi_L(a)$ матрицы C. Так как S есть *GGM* полугруппа, столбец $\psi_L(a)$ может быть найден с помощью матрицы C

и коэффициент пропорциональности между $f(b)$ и $C(b, \psi_L(a))$ есть $\lambda(a)$. Следовательно, ψ_L и λ полностью определены. Доказательство обратного утверждения проводится на основе дуальных рассуждений, б) Мы должны показать, что для всех $s_1, s_2 \in S - \{0\}$, $s_1 s_2 \neq 0$. Так как полугруппа $I^{\#}$ простая, мы имеем $I^{\#} \cong \mathcal{M}(G; A, B; C)$, где $C(b,a) \neq 0$ для всех $a \in A$, $b \in B$. Покажем, что не существует элемента $s \in S - \{0\}$, переводящего любой элемент из $I^{\#}$ в нуль.

Так как $s \neq 0$ и M^R_I точный, существует элемент $b \in B$, такой, что $\psi_R(b) \neq 0$. Из этого следует, что $\delta(b) \neq 0$; так как $C(b, a) \neq 0$ для всех $a \in A$, $b \in B$. то получаем, что $C[\psi_R(b), a] \neq 0$. Следовательно, в силу (2.3) $C[b, \psi_L(a)]\lambda(a) \neq 0$ для всех $a \in A$, откуда в свою очередь следует $C[b, \psi_L(a)] \neq 0$, из этого вытекает, что $\psi_L(a) \neq 0$ для всех $a \in A$. Обращая эти рассуждения, мы приходим к выводу, что $\psi_R(b) \neq 0$ для всех $b \in B$.

Мы видели, что никакой элемент из $S - \{0\}$ не переводит элемент из $I^{\#}$ в нуль. Поэтому остается только показать, что если $s_1, s_2 \in S - I$, то $s_1 s_2 \neq 0$. Пусть $x \in I^{\#}$. Тогда $s_2 x \neq 0$ и $s_2 x \in I^{\#}$, так что $s_1(s_2 x) \neq 0$. Из этого следует, что $s_1 s_2 \neq 0$.

2.24. Замечание. Предполагая ситуацию, описанную в пункте б) утверждения 2.23, нормализуем структурную матрицу идеала I так, что все элементы одного столбца и одной строки будут равны единице. Это можно сделать согласно утверждению 9 из предыдущего микромодуля. Предположим, что мы выбрали $C(1, a) = 1$ для всех $a \in A$ и $C(b, 1) = 1$ для всех $b \in B$.

Покажем теперь, как действие любого элемента полугруппы S на I связано со структурной матрицей для I. Рассмотрим, например,

$$\delta(b)\, C[\psi_R(b), 1] = C[b, \psi_L(1)]\, \lambda(1).$$

Тогда, поскольку $C[\psi_R(b), 1] = 1$, получаем

$$\delta(b) = C[b, \psi_L(1)]\lambda(1)$$

для всех $b \in B$. Поэтому $\delta(b)$ будет прямо пропорционален некоторому столбцу матрицы C. Аналогично $\lambda(a) = \delta(1) C[\psi_R(1), a]$, поэтому λ, и некоторая строка матрицы C пропорциональны. Эта связь между структурной матрицей и действием существенно зависит от того факта, что $C(b, a) \neq 0$ для всех $a \in A$ и для всех $b \in B$. В тех случаях, когда C имеет нулевые элементы, связь существенно ослабляется.

3.8. Разложение гомоморфизмов

Этот пункт посвящен различным разложениям гомоморфизмов конечных полугрупп. Мы докажем, что полугруппа имеет функториально минимальный γ гомоморфный образ, а также минимальные гомоморфные образы по отношению к другим свойствам гомоморфизмов. Мы докажем, что если *G* — группа и S — моноид, то гомоморфизм проекций $GwS \to\!\!\!\to S$ будет L гомоморфизмом; кроме того, если *C* — комбинаторная полугруппа и *S* — любая конечная полугруппа, то $CwS \to\!\!\!\to S$ есть γ(H) гомоморфизм.

Эти вычисления гомоморфизмов представляют самостоятельный интерес.

Пусть *P* — разбиение на полугруппе *S.* Вспомним определение *P* гомоморфизма и теорему о существовании S^p — минимального гомоморфного образа по отношению к P *(S, P).*

3.1. Замечание, а) Пусть P — свойство гомоморфизмов полугруппы S. Если *Q* — конгруэнтность на *S,* пусть $(\eta Q) : S \to\!\!\!\to S/Q$ — канонический гомоморфизм. Пусть $Q' = \operatorname{lub}\{Q : Q$ есть конгруэнтность на S и $((\eta Q),\ S/Q) \in \mathcal{P}\}$. Тогда *S* имеет минимальный гомоморфный образ по отношению к P тогда и только тогда, когда $((\eta\, Q'),\ S/Q) \in \mathcal{P}$. В этом случае $((\eta Q'),\ S/Q')$ представляет собой минимальный гомоморфный образ. Следовательно, если P непусто, то S имеет минимальный гомоморфный образ по отношению к P, когда включение $((\eta Q_1),\ S/Q_1),\ ((\eta Q_2),\ S/Q_2) \in \mathcal{P}$ влечет включение

$$((\eta Q),\ S/Q) \in \mathcal{P},\ \text{где } Q = \operatorname{lub}\{Q_1,\ Q_2\} \equiv Q_1 \vee Q_2.$$

б) Пусть *P* — разбиение на S. Пусть φ — гомоморфизм полугруппы *S* и *Q* — отношение конгруэнтности, индуцированное φ. В этом случае φ будет *P* гомоморфизмом тогда и только тогда, когда $Q \in P$.

в) Если φ есть *P* гомоморфизм, то φ разделяет *P* классы полугруппы S [т. е. $\varphi(P_i) \cap \varphi(P_j) = \emptyset$]. Следовательно, φ индуцирует разбиение *P′* на φ *(S),* определяемое отношением

$$\varphi(s_1) \equiv \varphi(s_2) \pmod{P'},$$

тогда и только тогда, когда $s_1 \equiv s_2 \pmod{P}$. *P* классы полугруппы *S* и *P′* классы полугруппы φ*(S)* находятся во взаимно однозначном соответствии, осуществляемом отображением φ. Следовательно, если x ≡ *y* (mod *P′),* то $\varphi^{-1}(x) \cup \varphi^{-1}(y)$ содержатся в одном *P* классе полугруппы *S*. Если *P*— отношение конгруэнтности, то и *P′* — отношение конгруэнтности.

3.2. Предложение. а) Пусть S — полугруппа с разбиением *P.*

Пусть заданы эпиморфизмы $S \xrightarrow{\varphi_1} T \xrightarrow{\varphi_2} U$. В этом случае $\varphi_2\varphi_1$ будет P гомоморфизмом тогда и только тогда, когда φ_1 будет P гомоморфизмом и φ_2 будет P' гомоморфизмом,

б) Пусть α обозначает одно из отношений $\mathcal{Y}$, $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$. Пусть $\varphi : S \twoheadrightarrow T$. Тогда для каждого α $S^\alpha \twoheadrightarrow T^\alpha$ и следующая диаграмма коммутативна:

$$\begin{array}{ccc} S & \twoheadrightarrow & T \\ \downarrow & & \downarrow \\ S^\alpha & \twoheadrightarrow & T^\alpha \end{array}$$

Доказательство, а) Пусть φ_1 будет P гомоморфизмом, а φ_2 есть P' гомоморфизм. Пусть $x, y \in S$ — такие элементы, что $x \not\equiv y \pmod{P}$. Тогда $\varphi_1(x) \not\equiv \varphi_1(y) \pmod{P'}$. Так как φ_2 есть P' гомоморфизм, $\varphi_2\varphi_1(x) \neq \varphi_2\varphi_1(y)$, так что $\varphi_2\varphi_1$ есть P гомоморфизм. Наоборот, пусть $\varphi_2\varphi_1$ есть P гомоморфизм и $x \not\equiv y \pmod{P}$. Тогда $\varphi_2\varphi_1(x) \neq \varphi_2\varphi_1(y)$, так что $\varphi_1(x) \neq \varphi_1(y)$ и φ_1 есть P гомоморфизм. Следовательно, P' индуцируется на T. Предположим, что $\varphi_1(a) \not\equiv \varphi_1(b) \pmod{P'}$. Тогда

$$a \not\equiv b \pmod{P} \text{ и } \varphi_2\varphi_1(a) \neq \varphi_2\varphi_1(b),$$

поэтому φ_2 есть P' гомоморфизм.

б) Доказательство основывается на том факте, что гомоморфизмы переводят α классы в α классы. Пусть $\alpha = \mathsf{F}$. Предположим, что Q и Q_J есть конгруэнтности на S, такие, что $S/Q \cong T$ и $S/Q_J \cong S^{\mathcal{F}}$. Пусть $J_1, \ldots, J_n$ будут F классы полугруппы T. Множества $\varphi^{-1}(J_i)$, $i = 1, \ldots, n$, не пересекаются и определяют разбиение S. Обозначим это разбиение P. Тогда $Q \subseteq P$ и $Q_J \subseteq P$, так что $Q \vee Q_J \subseteq P$. Заметим, что $s_1 \equiv s_2 \pmod{P}$ тогда и только тогда, когда $\varphi(s_1) \mathcal{Y} \varphi(s_2)$.

Рассмотрим коммутативную диаграмму:

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & T = S/Q \\ \downarrow & & \downarrow \theta \\ S/Q_J = S^{\mathcal{F}} & \xrightarrow{\eta} & S/(Q \vee Q_J) \end{array}$$

Предположим, что $\theta\varphi(s_1) = \theta\varphi(s_2)$. Тогда $s_1 \equiv s_2 \pmod{(Q \vee Q_J)}$, поэтому $s_1 \equiv s_2 \pmod{P}$. Из этого следует, что $\varphi(s_1) \mathcal{Y} \varphi(s_2)$ в T. Следовательно, θ есть F гомоморфизм и существует

гомоморфизм $\psi : S/Q \vee Q_J \to\to T^{\mathcal{J}}$. Тогда $\psi\eta : S^{\mathcal{J}} \to\to T^{\mathcal{J}}$. Доказательства для $\mathcal{R}$, $\mathcal{L}$ и $\mathcal{H}$ аналогичны.

3.3. Утверждение. Пусть T — подполугруппа полугруппы S. Пусть $\alpha(S)$ и $\alpha(T)$ — любые из отношений $\mathcal{J}$, $\mathcal{R}$, $\mathcal{L}$ и $\mathcal{H}$ на S и T соответственно.

а) Если $t_1, t_2 \in T$— регулярные элементы полугруппы T и α — любое из отношений $\mathcal{R}$, $\mathcal{L}$ или $\mathcal{H}$, то $t_1\alpha(T)t_2$ тогда и только тогда, когда $t_1\alpha(S)t_2$.

б) Если S — полугруппа, представляющая собой объединение групп, то результат пункта а) справедлив также для $\alpha = \mathcal{J}$.

в) Пусть

$$\varphi : S \xrightarrow[\alpha(S)]{} S'.$$

Тогда ограничение φ на T будет $\alpha(T)$ гомоморфизмомв следующих случаях: 1) S есть объединение групп и α есть одно из отношений $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$; 2) T регулярна и α есть одно из отношений $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$.

Доказательство, а) Отсылаем к доказательству утверждения 7 из предыдущего микромодуля.

б) Пусть $t_1 \mathcal{J}(S) t_2$ и J есть F класс полугруппы S, содержащий элементы t_1 и t_2. J есть простая полугруппа, так что $T \cap J$ — также простая полугруппа. Поскольку простая полугруппа содержит только один F классе, из $t_1 \mathcal{J}(T \cap J) t_2$ вытекает, что $t_1 \mathcal{J}(T) t_2$. Очевидно, что обратное также справедливо.

в) Этот пункт следует из пунктов а) и б).

3.4. Предложение. Пусть $\varphi : S \to\to T$, предположим, что T есть *RLM, LLM, GGM* или *GM* полугруппа с отмеченным идеалом *I*. Пусть J — минимальный F класс полугруппы *S*, такой, что $\varphi(J) = I^{\#}$. Тогда

$RLM_J(S) \to\to T$, $LLM_J(S) \to\to T$, $GGM_J(S) \to\to T$ или $GM_J(S) \to\to T$ соответственно.

Доказательство. Пусть T будет *RLM* полугруппой. Пусть $s_1, s_2 \in S$ и предположим, что $RLM_J(s_1) = RLM_J(s_2)$. Мы должны показать, что $\varphi(s_1) = \varphi(s_2)$. Для каждого элемента $x \in J$ или $xs_1 \mathcal{L} xs_2$ в J, или оба xs_1 и $xs_2 \in B(J)$. В последнем случае в силу минимальности класса J мы имеем $\varphi(xs_1) = \varphi(xs_2) = 0$. Если $xs_1 L xs_2$, то $xs_1 \mathcal{H} xs_2$. Следовательно, $\varphi(xs_1) \mathcal{H} \varphi(xs_2)$, а так как $I^{\#}$ комбинаторная, получаем, что $\varphi(xs_1) = \varphi(xs_2)$. Таким образом, для всех $i \in I$ мы имеем

$i\varphi(s_1) = i\varphi(s_2)$. Следовательно, $\varphi(s_1) = \varphi(s_2)$, так как T есть *RLM* полугруппа. Посредством дуальных рассуждений доказывают требуемый результат, когда T есть *LLM* полугруппа.

Пусть T есть *GGM* полугруппа. Пусть элементы $s_1, s_2 \in S$, такие, что $GGM_J(s_1) = GGM_J(s_2)$. Для всех $x_1, x_2 \in I$ или $x_1s_1x_2 = x_1s_2x_2$ в J, или оба элемента $x_1s_1x_2$ и $x_1s_2x_2 \in B(J)$. Следовательно,

$$\varphi(x_1s_1x_2) = \varphi(x_1s_2x_2)$$

для всех $x_1, x_2 \in J$ или

$$i_1\varphi(s_1)i_2 = i_1\varphi(s_2)i_2$$

для всех $i_1, i_2 \in I$. Так как T есть *GGM* полугруппа, получаем, что $i_1\varphi(s_1) = i_1\varphi(s_2)$ для всех $i_1 \in I$, из этого следует, что $\varphi(s_1) = \varphi(s_2)$. Пусть T есть *GW* полугруппа. Если $T = \{0\}$, то утверждение тривиально. Предположим, что $T \neq \{0\}$. Тогда $I^{\#}$ будет регулярной некомбинаторной. Далее доказательство ведется так же, как в случае, когда T есть *GGM* полугруппа.

3.5. Определение. Пусть S — полугруппа.

а) Положим $Q(GM) = glb\{Q' : Q'$ есть отношение конгруэнтности на S и S/Q' есть *GM* полугруппа$\}$. По определению $S^{GM} = S/Q(GM)$. Отметим, что S^{GM} не обязательно является *GM* полугруппой.

б) Положим $Q(GGM) = glb\{Q' : Q'$ есть отношение конгруэнтности и S/Q' есть *GGM* полугруппа$\}$. По определению $S^{GGM} = S/Q(GGM)$. Отметим, что S^{GGM} не обязательно является *GGM* полугруппой.

в) Положим $Q(RLM) = glb\{Q' : Q'$ есть отношение конгруэнтности и S/Q' есть *RLM* полугруппа$\}$. По определению $S^{RLM} = S/Q(RLM)$. Отметим, что S^{RLM} не является в общем случае *RLM* полугруппой.

г) Дуальным образом определяем $S^{LLM} = S/Q(LLM)$.

3.6. Утверждение. Пусть $J_1, \ldots, J_n$ — регулярные F классы полугруппы S.

а) $S^{GM} \cong (GM_{J_1} \times \ldots \times GM_{J_n})\Delta(S)$;

б) $S^{GGM} \cong (GGM_{J_1} \times \ldots \times GGM_{J_n})\Delta(S)$;

в) $S^{RLM} \cong (RLM_{J_1} \times \ldots \times RLM_{J_n})\Delta(S)$;

г) $S^{LLM} \cong (LLM_{J_1} \times \ldots \times LLM_{J_n})\Delta(S)$.

Доказательство, а) Пусть Q, есть отношение конгруэнтности на S, индуцированное

$$GM_{J_i}, \quad i = 1, \ldots, n.$$

Тогда предложение 3.4 утверждает, что для каждого отношения конгруэнтности Q, где S/Q есть GM, существует i, такое, что $Q_i \subseteq Q$. Таким образом, легко видеть, что $Q(GM) = Q_1 \cap \ldots \cap Q_n$, так что $S^{GM} \cong (GM_{J_1} \times \ldots \times GM_{J_n})\Delta(S)$.

Доказательства пунктов б)—г) примерно такие же.

3.7. Утверждение. Пусть α будет любым из следующих символов: *CM, GGM, RLM* или *LLM*.

а) Если $S \xrightarrow{\psi} T$, то $S^\alpha \twoheadrightarrow T^\alpha$ и следующая диаграмма коммутативна

$$\begin{array}{ccc} S & \xrightarrow{\psi} & T \\ \downarrow & & \downarrow \\ S^\alpha & \twoheadrightarrow & T^\alpha \end{array}$$

б) Если T — подполугруппа полугруппы S, то $T^\alpha \mid S^\alpha$.

в) Если $T \mid S$, то $T^\alpha \mid S^\alpha$.

Доказательство, а) Будем доказывать пункт а) для α = *GM*. Остальные случаи разбираются аналогично. Пусть $K_1, \ldots, K_m$ есть регулярные некомбинаторные F классы полугруппы T. Тогда

$$T^{GM} = (GM_{K_1} \times \ldots \times GM_{K_m})\,\Delta\,(T).$$

В силу предложения 3.4 существует отдельный некомбинаторный регулярный F класс J_i полугруппы S, такой, что

$$GM_{J_i}(S) \xrightarrow{\varphi_i} GM_{K_i}(T)$$

для каждого i = 1, ..., m. Поэтому для каждого i = 1, ..., m получаем равенство $\varphi_i GM_{J_i} = GM_{K_i}\psi_i$. Пусть $J_1, \ldots, J_m, \ldots, J_n$ — регулярные некомбинаторные F классы полугруппы S. Тогда

$$S^{GM} = (GM_{J_1} \times \ldots \times GM_{J_n})\Delta(S).$$

Пусть П — прямое произведение первых m отображений проекции для

$$GM_{J_1}(S) \times \ldots \times GM_{J_n}(S).$$

Тогда

$$(\varphi_1 \times \ldots \times \varphi_m)\,\Pi : S^{GM} \twoheadrightarrow (\varphi_1 GM_{J_1} \times \ldots \times \varphi_m GM_{J_m})\Delta(S) =$$
$$= (GM_{K_1}\psi \times \ldots \times GM_{K_m}\psi)\Delta(S) =$$
$$= (GM_{K_1} \times \ldots \times GM_{K_m})\Delta\psi(S) = T^{GM},$$
$$\text{так как } \psi(S) = T.$$

Очевидно, что приведенная диаграмма коммутативна.

б) Покажем теперь, что если T — подполугруппа полугруппы S, то $T^{GM} \mid S^{GM}$. Пусть $\psi : S \to\!\!\!\to S^{GM}$. Мы должны показать, что $\psi(T) \to\!\!\!\to T^{GM}$. Пусть $S^{GM} = S/Q_S(GM)$ и $T^{GM} = T/Q_T(GM)$. Тогда достаточнопоказать, что для $t_1, t_2 \in T$ и $t_1 \not\equiv t_2 \pmod{Q_T(GM)}$ справедливо соотношение $t_1 \not\equiv t_2 \pmod{Q_S(GM)}$. Предположим, что $t_1 \not\equiv t_2 \pmod{Q_T(GM)}$. Тогда существуют F класс J полугруппы T и элементы $x_1, x_2 \in J$, такие, что или

1) $x_1t_1x_2,\ x_1t_2x_2 \in J$ и $x_1t_1x_2 \neq x_1t_2x_2$,

или

2) $x_1t_1x_2 \in J$ и $x_1t_2x_2 \notin J'$, где J' есть F класс полугруппы S, содержащий J,

или

3) $x_1t_1x_2 \in J'$ и $x_1t_2x_2 \in J' - J$.

В случаях 1 и 3

$$x_1t_1x_2,\quad x_1t_2x_2 \in J' \text{ и } x_1t_1x_2 \neq x_1t_2x_2,$$

так что

$$t_1 \not\equiv t_2 \pmod{Q_S(GM)}$$

Вслучае 2 $x_1t_1x_2 \in J'$ и $x_1t_2x_2 \notin J'$ и снова получается, что $t_1 \not\equiv t_2 \pmod{Q_S(GM)}$.

Следовательно, если $T \subseteq S$, то $T^{GM} \mid S^{GM}$. Доказательство для $\alpha = GGM$ проводится точно так же, а аналогичные доказательства с использованием пункта а) утверждения 3.3 проводятся в случаях, когда $\alpha = RLM$ и LLM.

в) Этот пункт следует из пунктов а) и б).

3.8. Определение. Пусть α — одно из отношений $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$. Будем говорить, что $\varphi : S \to\!\!\!\to T$ есть α' гомоморфизм (и писать $\varphi : S \xrightarrow[\alpha']{} T$), если для всех регулярных элементов $s_1, s_2 \in S$ из равенства $\varphi(s_1) = \varphi(s_2)$ вытекает, что $s_1 \alpha s_2$.

Пусть $\mathcal{P}(S, \alpha')$ — совокупность пар (φ, T), таких, что φ есть α' гомоморфизм. Отметим, что если S регулярна, то $\mathcal{P}(S, \alpha') = \mathcal{P}(S, \alpha)$.

3.9. Утверждение. а) Если $\varphi : S \xrightarrow[\alpha]{} T$, то $\varphi : S \xrightarrow[\alpha']{} T$ для $\alpha = \mathcal{R}, \mathcal{L}, \mathcal{H}$ или $\mathcal{J}$. Если

$$\varphi : S \xrightarrow[\alpha']{} T \text{ и } S_1$$

— подполугруппа полугруппы *S*, то ограничение φ на S_1 будет α′ отображением для α = L, R или H^1 (этот результат верен также для α =F).

б) Пусть $\varphi : S \xrightarrow[\alpha']{} T$ и предположим, что *J* — регулярный F класс полугруппы *S*. Тогда φ (*J*) будет F классом полугруппы *T* и *J* — единственный регулярный и единственный минимальный F класс полугруппы *S*, содержащийся в $\varphi^{-1}[\varphi(J)]$.

в) *S* имеет минимальный гомоморфный образ относительно P *(S, α′)* [это обозначается как $S \to\!\!\!\to S^{\alpha'}$] для $\alpha = \mathcal{R}, \mathcal{L}$ и $\mathcal{H}$. $(S^{\alpha'})^{\alpha'} = S^{\alpha'}$ В действительности 1) $S^{\mathcal{L}} \cong S^{RLM}$, 2) $S^{\mathcal{R}'} \cong$ $\cong S^{LLM}$ и 3) $S^{\mathcal{H}'}$ индуцируется $Q(LLM) \cap Q(RLM)$.

Следовательно, если S есть *RLM* полугруппа, то $S = S^{\mathcal{L}}$, и если S есть *LLM* полугруппа, то $S = S^{\mathcal{R}'}$.

г) $\varphi : S \xrightarrow[\alpha']{} T$ тогда и только тогда, когда из условия, что s_1 и s_2 — регулярные элементы полугруппы S, такие, что $\varphi(s_1)\alpha\varphi(s_2)$, вытекает соотношение $s_1 \alpha s_2$, где $\alpha = \mathcal{L}, \mathcal{R}, \mathcal{H}$ или $\mathcal{J}$. Следовательно, φψ будет α′ гомоморфизмом тогда и только тогда, когда φ и ψ будут α′ гомоморфизмами.

д) Если $S \mid T$, то $S^{\alpha'} \mid T^{\alpha'}$ для $\alpha = \mathcal{L}$ или $\mathcal{R}$.

Доказательство, а) Первое утверждение пункта а) очевидно. Перейдем ко второму утверждению. Пусть s_1, s_2 — такие регулярные элементы полугруппы *S*, что $\varphi(s_1) = \varphi(s_2)$. Так как φ является α′ гомоморфизмом, $s_1 \alpha s_2$ в *S*. Но в силу пункта а) утверждения 3.3 $s_1 \alpha s_2$ в S_1. Следовательно, ограничение φ на S_1 будет α′ гомоморфизмом.

б) Так как φ есть гомоморфизм, существует такой F класс $J_1 \subseteq T$, что $\varphi(J) \subseteq J_1$, и так как класс *J* регулярный, то класс J_1 также регулярный. Тогда в силу утверждения 11 из предыдущего микромодуля $\varphi^{-1}(J_1)$ является объединением F классов полугруппы S с единственным минимальным классом *J′* и $\varphi(J')=J_1$. Класс *J′* регулярен, так как J_1 регулярен и, следовательно, существуют элементы $x \in J$ и $x' \in J'$, такие, что $\varphi(x) = \varphi(x')$. Так как φ есть α′ отображение, получаем, что $x \alpha x'$, откуда в свою очередь вытекает, что $x F x'$. Следовательно, $J = J'$. Если *J″*— произвольный регулярный F класс полугруппы *S*, содержащийся $\varphi^{-1}[\varphi(J)]$, то из тех же самых рассуждений вытекает, что $J = J''$. Следовательно, *J* — единственный регулярный F класс, содержащийся в $\varphi^{-1}[\varphi(J)]$.

в) Пусть $J_1, \ldots, J_n$— регулярные F классы полугруппы *S*. Мы покажем, что отображение $\Pi RLM_{J_i} : S \to\!\!\!\to S^{RLM}$ будет $\mathcal{L}'$

гомоморфизмом. Пусть $s_1, s_2 \in S$ — регулярные элементы и предположим, что $\Pi RLM_{J_i}(s_1) = \Pi RLM_{J_i}(s_2)$. Тогда $RLM_{J_i}(s_1) = RLM_{J_i}(s_2)$ для каждого $i = 1, ..., n$, из этого следует, что $s_1 F s_2$ и поэтому $s_1 L s_2$.

Покажем теперь, что $S^{RLM} \cong S^{\mathscr{L}'}$. Пусть отображение $\varphi : S \twoheadrightarrow T$ есть $\mathscr{L}'$ гомоморфизм и предположим, что $\varphi(s_1) = \varphi(s_2)$, а элементы s_1, s_2 регулярные. Нужно доказать, что $RLM_{J_i}(s_1) = RLM_{J_i}(s_2)$ для всех $i = 1.....n$, т. е. для каждого J_i и всех $x \in J_i$ или 1) $xs_1, xs_2 \in J_i$ и $xs_1 \mathscr{L} xs_2$, или 2) $xs_1, xs_2 \in B(J_i)$.

Предположим, что $xs_1 \in J_i$ и $xs_2 \in J_i$. Тогда $xs_2 \in B(J_i)$ и поскольку

$$\varphi(xs_1) = \varphi(xs_2),$$

то $\varphi(J_i) \cap \varphi[B(J_i)] \neq \varnothing$. Но это противоречие, так как J_i — единственный минимальный F класс в $\varphi^{-1}[\varphi(J_i)]$ согласно пункту б). Таким образом, для каждого $i = 1, ..., n$ $RLM_{J_i}(s_1) = RLM_{J_i}(s_2)$. Доказательство для отношения M проводится аналогично и из этого легко получается доказательство для отношения H.

г) Пусть $\varphi : S \xrightarrow[\alpha']{} T$, предположим, что $s_1, s_2 \in S$ — регулярные элементы и $\varphi(s_1) \alpha \varphi(s_2)$. Тогда согласно пункту б) $s_1 F s_2$. Пусть $s_1, s_2 \in J$. Тогда, поскольку φ является α' гомоморфизмом и J регулярен, φ действует как α гомоморфизм на J. Согласно утверждению 1.13 α классы S α J находятся во взаимно однозначном соответствии с α классами полугруппы T, принадлежащими $\varphi(J)$. Следовательно, $s_1 \alpha s_2$. Обратное очевидно. Оставшаяся часть утверждения проверяется легко.

д) Этот пункт следует из пункта в) и утверждения 3.7,

3.10. Определение. Пусть S — полугруппа и, $\mathscr{P}(S, \gamma)$ — совокупность пар (φ, T), таких, что $\varphi : S \twoheadrightarrow T$ и φ есть γ гомоморфизм, т. е. ограничение φ на любую подгруппу является взаимно однозначным отображением (определение 1.12). Если $\varphi \in \mathscr{P}(S, \gamma)$, то будем писать $\varphi : S \xrightarrow[\gamma]{} T$.

Приступим теперь к доказательству того, что S имеет минимальный гомоморфный образ относительно $\mathscr{P}(S, \gamma)$.

3.11. Лемма. Пусть I — максимальный собственный идеал полугруппы S и предположим, что существует $\varphi \in \mathscr{P}(S, \gamma)$, такой, что $\varphi(S) = \varphi(I)$. Пусть ψ— любой гомоморфизм полугруппы S. В этом случае ψ будет γ гомоморфизмом тогда и только тогда, когда ограничение ψ на I есть γ гомоморфизм.

Доказательство. Предположим, что ограничение ψ на I является γ гомоморфизмом. Пусть G — нетривиальная группа, принадлежащая S —I (если такой не существует, то все сделано). Пусть $H = \varphi(G)$ и S_1 — подполугруппа в $\varphi^{-1}(H)$. Тогда $\varphi(S_1) = H$ и поскольку $\varphi(I) = \varphi(S)$, то имеем $\varphi(S_1 \cap I) = H$. $S_1 \cap I$ — непустой идеал полугруппы S_1. Теперь φ будет обозначать ограничение φ на S_1 Пусть $K(S_1)$ — ядро полугруппы S_1. $K(S_1) \subseteq I$ и поскольку при эпиморфизмах ядра переходят в ядра и группа представляет собой свое собственное ядро, то $\varphi[K(S_1)] = H$. Но из предложения 1 из предыдущего микромодуля мы знаем, что каждая максимальная подгруппа из $K(S_1)$ переводится отображением φ на H. Поскольку φ взаимно однозначно на подгруппах, H изоморфна каждой максимальной подгруппе из $K(S_1)$.

Пусть G_1 — одна из максимальных подгрупп, принадлежащих $K(S_1)$ и e — единица группы G_1. Определим отображение из G в $K(S_1)$, полагая $g \to ege$. По теореме Риса в силу свойств переносов 0-простых полугрупп $ege \in G_1$. Кроме того, это отображение взаимно однозначно, так как если $ege = ehe$, то $\varphi(g) = \varphi(h)$, откуда следует, что $g = h$.

Теперь $G_1 \subseteq I$, поэтому ψ по предложению будет взаимно однозначным на G_1. Пусть $g_1 \neq g_2 \in G$. Тогда $eg_1e \neq eg_2e \in G_1$. Следовательно, $\psi(eg_1e) \neq \psi(eg_2e)$, из этого вытекает, что $\psi(g_1) \neq \psi(g_2)$. Следовательно, $\psi \in \mathcal{P}(S, \gamma)$. Обратное утверждение очевидно.

3.12. Предложение. Полугруппа S имеет минимальный гомоморфный образ относительно $\mathcal{P}(S, \gamma)$., который обозначается S^γ и строится следующим образом. Если S — комбинаторная полугруппа, то $S^\gamma = \{0\}$. Если S — не комбинаторная, пусть $J_1, \ldots, J_k$ есть k различных $\mathcal{F}$ классов полугруппы S, упорядоченных так, что, если $i<j$, то $J_j \not\leq J_i$. Гомоморфизм ψ полугруппы S определяется по индукции. Пусть $\psi_1 = GM_{J_1}$. Предположим теперь, что ψ_j уже определен. Если ψ_j будет взаимно однозначным на подгруппах из J_{j+1}, положим $\psi_{j+1} = \psi_j$. Впротивном случае, пусть $\psi_{j+1} = (\psi_j \times GM_{J_{j+1}})\Delta$ и $\psi = \psi_k$. Тогда

$$\psi(S) = S^\gamma.$$

Доказательство. Так как GM_{J_1} является взаимно однозначным на подгруппах из J_i, $i = 1, \ldots, k$, нетрудно проверить, что $(\psi, \psi(S)) \in \mathcal{P}(S, \gamma)$. Если теперь

$$\varphi : S \xrightarrow[\nu]{} T,$$

мы должны показать, что из равенства $\varphi(s_1) = \varphi(s_2)$ вытекает равенство $\psi(s_1) = \psi(s_2)$. По индукции докажем эквивалентный результат. Если $\varphi(s_1) = \varphi(s_2)$, то для $1 \leq j \leq k$ справедливы равенства $\psi_j(s_1) = \psi_j(s_2)$.

Предположим, что $\varphi(s_1) = \varphi(s_2)$. Пусть $x_1, x_2 \in J_1$. Докажем, что $x_1 s_1 x_2 \in J_1$ тогда и только тогда, когда $x_1 s_2 x_2 \in J_1$. Если $x_1 s_1 x_2 \in J_1$ и $x_1 s_2 x_2 \notin J_1$, то и $x_1 s_2 x_2 \in B(J_1)$, так как $\varphi(x_1 s_1 x_2) = \varphi(x_1 s_2 x_2)$, из этого вытекает, что $\varphi(J_1) \subseteq \varphi[B(J_1)]$, т. е. $\varphi[J_1 \cup B(J_1)] = \varphi[B(J_1)]$.

Но тогда по лемме 3.11 гомоморфизм, являющийся γ гомоморфизмом на $B(J_1)$, будет γ гомоморфизмом и на $J_1 \cup B(J_1)$. $B(J_1)$ комбинаторна, поэтому нулевой гомоморфизм будет γ гомоморфизмом на $B(J_1)$ и, следовательно, он взаимно однозначен на подгруппах из J_1. Это противоречие. Таким образом, $x_1 s_1 x_2 \in J_1$ тогда и только тогда, когда $x_1 s_2 x_2 \in J_1$ для всех $x_1, x_2 \in J_1$. Покажем теперь, что если $x_1 s_1 x_2 \in J_1$ (и $x_1 s_2 x_2 \in J_1$), то $x_1 s_1 x_2 = x_1 s_2 x_2$.

По теореме Риса в силу свойств переносов 0-простых полугрупп (см. утверждение 13 из предыдущего микромодуля) $x_1 s_1 x_2 \mathcal{H} x_1 s_2 x_2$ и существуют $z_1, z_2, a_1, a_2 \in J_1$, такие, что $b_1 = z_1 x_1 s_1 x_2 z_2$ и $b_2 = z_1 x_1 s_2 x_2 z_2$ лежат в одной максимальной подгруппе из J_1 и $a_1 b_1 a_2 = x_1 s_1 x_2$, $a_1 b_2 a_2 = x_1 s_2 x_2$. Так как φ будет взаимно однозначным на подгруппах и $\varphi(b_1) = \varphi(b_2)$, имеем $b_1 = b_2$, так что $x_1 s_1 x_2 = x_1 s_2 x_2$. Следовательно, для всех $x_1, x_2 \in J_1$ или $x_1 s_1 x_2$ и $x_1 s_2 x_2$ лежат в $B(J_1)$, или $x_1 s_1 x_2 = x_1 s_2 x_2 \in J_1$. Таким образом, $\psi_1(s_1) = \psi_1(s_2)$.

Пусть теперь по предложению индукции из равенства $\varphi(s_1) = \varphi(s_2)$ вытекает, что $\psi_i(s_1) = \psi_i(s_2)$ для всех таких i, что $1 \leq i \leq j < k$. Мы должны показать, что из равенства $\varphi(s_1) = \varphi(s_2)$ вытекает $\psi_{j+1}(s_1) = \psi_{j+1}(s_2)$. Если ψ_j будет взаимно однозначным на подгруппах из J_{j+1}, то,

$$\psi_j = \psi_{j+1},$$

и в этом случае переход по индукции к следующему номеру получается тривиально. Следовательно, $\psi_{j+1} = (\psi_j \times GM_{J_{j+1}})\Delta$. Пусть $x_1, x_2 \in J_{j+1}$. Мы покажем сейчас, что $x_1 s_1 x_2 \in J_{j+1}$ тогда и только тогда, когда $x_1 s_2 x_2 \in J_{j+1}$. Предположим, что

$x_1s_1x_2 \in J_{j+1}$ и $x_1s_2x_2 \notin J_{j+1}$. Тогда $x_1s_2x_2 \in B(J_{j+1})$ и $B(J_{j+1})$ — максимальный идеал в $B(J_{j+1}) \cup J_{j+1}$, поэтому

$$\varphi[B(J_{j+1})] = \varphi[B(J_{j+1}) \cup J_{j+1}].$$

В силу леммы 3.11, поскольку φ_j является взаимно однозначным на подгруппах из $B(J_{j+1})$, ψ_j будет взаимно однозначным на подгруппах из J_{j+1}. Это противоречие. Но тогда действуя так же, как раньше, получаем, что $\psi_{j+1}(s_1) = \psi_{j+1}(s_2)$. Предложение доказано.

3.13. Замечание. а) Если $S \xrightarrow[\nu]{} T$, то

$$S \xrightarrow[\nu]{} T \xrightarrow[\nu]{} S^\nu.$$

б) Пусть

$$\varphi : S \xrightarrow[\nu]{} T$$

и предположим, что J — регулярный F класс полугруппы S. Тогда ограничение φ на любой H класс полугруппы S, принадлежащий J, будет взаимно однозначным отображением. Следовательно, если S — регулярная полугруппа, то φ будет γ гомоморфизмом тогда и только тогда, когда φ будет $\gamma(H)$ гомоморфизмом. Это следует из замечания 5 предыдущего микромодуля.

в) Пусть S — 0-простая полугруппа. Тогда $S^\nu = GM(S)$.

г) Пусть R — подполугруппа полугруппы S и $\varphi : S \xrightarrow[\nu]{} T$. Тогда ограничение φ на R будет γ гомоморфизмом. Следовательно, $R \xrightarrow[\nu]{} \varphi(R) \xrightarrow[\nu]{} R^\nu$ и поэтому $R^\nu | S^\nu$.

д) Неверно, что если S | T, то $S^\nu | T^\nu$. Это объясняется тем, что из $T \to\to S$ не следует, что $S^\nu | T^\nu$. Пусть $G \neq \{1\}$ — группа и $U_2 = \{0\}^1$. Пусть $S = G \times U_2$. Тогда задается $S \to S^\nu$ соотношением $(g, x) \to (g, 0)$, поэтому $S^\nu \cong G$. Множество $G \times \{0\}$ будет идеалом полугруппы S и $S / (G \times \{0\}) \cong G^0$, так что полугруппа $(G^0)^\nu = G^0$ не делит группу $S^\nu = G$.

3.14. Определение. Пусть P (S, γ, F) обозначает совокупность таких пар (φ, T), что φ есть γ гомоморфизм и F гомоморфизм, φ мы назовем $(\gamma + F)$ гомоморфизмом.

3.15. Предложение. Полугруппа S имеет минимальный гомоморфный образ относительно P (S, γ, F), обозначаемый как $S \to\to S^{\gamma+F}$. Для $S^{\gamma+F}$ имеются две формулы.

а) Пусть $\varphi : S \to\!\!\!\!\to S^{\gamma}$ и $\psi : S \to\!\!\!\!\to S^{\mathcal{F}}$. Положим $(\varphi\times\psi)\Delta: S \to S^{\gamma}\times S^{\mathrm{F}}$.

Тогда $(\varphi \times \psi)\Delta : S \to\!\!\!\!\to S^{\gamma+\mathcal{F}}$. Следовательно, $S^{\gamma+\mathcal{F}} \leqslant\!\!\leqslant S^{\gamma}\times \times S^{\mathcal{F}}$.

б) Пусть S — регулярная полугруппа. Тогда $S^{\gamma+\mathrm{F}} = S^{GGM}$.

в) Пусть S — регулярная полугруппа. Если $S \to\!\!\!\!\to T$, то $S^{\gamma+\mathcal{F}} \to\!\!\!\!\to \to\!\!\!\!\to T^{\gamma+\mathcal{F}}$ и следующая диаграмма коммутативна:

$$\begin{array}{ccc} S & \to\!\!\!\!\to & T \\ \downarrow & & \downarrow \\ S^{\gamma+\mathcal{F}} & \to\!\!\!\!\to & T^{\gamma+\mathcal{F}} \end{array}$$

г) Пусть S и T — регулярные полугруппы. Тогда если $T|S$, то $T^{\gamma+\mathcal{F}}|S^{\gamma+\mathcal{F}}$.

Доказательство, а) Очевидно, что $(\varphi \times \psi)\Delta$ есть $(\gamma + \mathcal{F})$, гомоморфизм. Наоборот, пусть Q_2 и Q_2 — отношения конгруэнтности на S, индуцированные φ и ψ соответственно. Тогда $Q_1 \cap Q_2$ индуцируется отображением $(\varphi \times \psi)\Delta$. Если $\theta : S \to\!\!\!\!\to S/Q$ есть любой (γ+F) гомоморфизм, то $Q \subseteq Q_1$ и $Q \subseteq Q_2$, так что $Q \subseteq Q_1 \cap Q_2$. Следовательно, $(\varphi \times \psi)\Delta\,(S)$ будет минимальным гомоморфным образом относительно $\mathcal{P}\,(S,\ \gamma,\ \mathcal{F})$.

б) Пусть $J_1, \ldots, J_n$ будут F классами полугруппы S. Так как GGM_{J_i} — взаимно однозначное отображение на подгруппах из J_i, i =1, ... n, ПGGM_{J_i} будет у гомоморфизмом. Пользуясь определением GGM_J, легко показать, что $nGGM_{J_i}$ будет F гомоморфизмом. Следовательно, ПGGM_{J_i} есть $(\gamma + \mathcal{F})$ гомоморфизм.

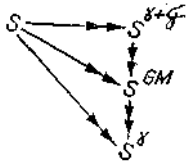
Пусть $(\varphi,\ T) \in \mathcal{P}(S,\ \gamma,\ \mathcal{F})$. Мы должны доказать, что если $nGGM_{J_i}(s_1) \neq nGGM_{J_i}(s_2)$, то $\varphi\,(s_1) \neq \varphi\,(s_2)$. Но

$$nGGM_{J_i}\,(s_1) \neq nGGM_{J_i}\,(s_2)$$

тогда и только тогда, когда существует F класс J полугруппы S и элементы $x_1, x_2 \in J$, такие, что или 1) $x_1s_1x_2 \in J$ и $x_1s_2x_2 \in J$, или 2) оба элемента $x_1s_1x_2$ и $x_1s_2x_2$ лежат в J и $x_1s_1x_2 \neq x_1s_2x_2$. В первом случае, поскольку отображение φ есть F гомоморфизм, мы имеем $\varphi\,(x_1s_1x_2) \neq \varphi\,(x_1s_2x_2)$, поэтому $\varphi\,(s_1) \neq \varphi\,(s_2)$.

Во втором случае $x_1 s_1 x_2 \mathrel{H} x_1 s_2 x_2$, поэтому $\varphi(x_1 s_1 x_2) \neq \varphi(x_1 s_2 x_2)$, так как φ есть γ (H) гомоморфизм согласно пункту б) замечания 3.13. Следовательно, $\varphi(s_1) \neq \varphi(s_2)$. Пункты в) и г) вытекают из утверждения 3.7.

3.16. Замечание. Отметим, что если S — регулярная полугруппа, то и приведенная диаграмма коммутативна.



Это следует из того факта, что $S^{\gamma+\mathcal{F}} \cong S^{\mathcal{GGM}} \twoheadrightarrow S^{\mathcal{GM}}$, и из способа, которым определялась полугруппа S^{γ}.

Следующее предложение будет очень важным при изучении материала микромодуля 10.

3.17. Предложение. Пусть S и T_1, ..., T_n — полугруппы, представляющие собой объединение групп, и α есть γ + F, R или L. Тогда если $S \leq\leq T_1 \times \ldots \times T_n$ и $\theta_i : T_i \twoheadrightarrow T^{\alpha}_i$, так, что $\theta_i = \theta_1 \times \ldots \times \theta_n$: $T_1 \times \ldots \times T_n \twoheadrightarrow T^{\alpha}_1 \times \ldots \times T^{\alpha}_n$, то $\theta(S) = S^{\alpha}$ и $S^{\alpha} \leq\leq T^{\alpha}_1 \times \ldots \times T^{\alpha}_n$.

Доказательство. Ограничение θ на S будет α гомоморфизмом, поскольку α гомоморфизм сохраняется при взятии прямого произведения и ограничения. Следовательно, $\theta(S) \twoheadrightarrow S^{\alpha}$. С другой стороны, положим $p_i : S \twoheadrightarrow T_i$, тогда $\theta_i p_i : S \twoheadrightarrow T^{\alpha}_i$. Так как $S \twoheadrightarrow T_i$, мы имеем $S^{\alpha} \xrightarrow{\varphi_i} T^{\alpha}_i$, поэтому если $\psi : S \twoheadrightarrow S^{\alpha}$, то $\varphi_i \psi = \theta_i p_i$. Теперь

$$\begin{aligned}\theta(S) &= (\theta_1 p_1 \times \ldots \times \theta_n p_n)\,\Delta(S) \\ &= (\varphi_1 \psi \times \ldots \times \varphi_n \psi)\,\Delta(S) \\ &= (\varphi_1 \times \ldots \times \varphi_n)\,\Delta\psi(S) \\ &= (\varphi_1 \times \ldots \times \varphi_n)\,\Delta S^{\alpha}.\end{aligned}$$

Следовательно, $S^{\alpha} \twoheadrightarrow \theta(S)$, поэтому $\theta(S) = S^{\alpha} \leq\leq T^{\alpha}_1 \times \ldots \times T^{\alpha}_n$.

3.18. Лемма. а) Пусть $\varphi_i : S_i \twoheadrightarrow T_i$ для i = 1, 2 будет γ (соответственно α') гомоморфизмом, где $\alpha = \mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$. Тогда $\varphi = (\varphi_1 \times \varphi_2) : S_1 \times S_2 \twoheadrightarrow T_1 \times T_2$ будет γ (соответственно α') гомоморфизмом.

б) Пусть $S = S^{\gamma}$ и $S = S^{\alpha'}$, где $\alpha = \mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$. Тогда S = {0}.

Доказательство, а) Доказательство утверждения для α' гомоморфизмов проводится легко. Пусть φ_i будет γ гомоморфизмом для $i = 1, 2$ и G — подгруппа в $S_1 \times S_2$, такая, что $\varphi(G) = \{e\}$, где $e = (e_1, e_2)$ — идемпотент в $T_1 \times T_2$. Тогда $S_1' = \varphi_1^{-1}(e_1)$ и $S_2' = \varphi_1^{-1}(e_2)$ — комбинаторные подполугруппы полугрупп S_1 и S_2 соответственно, так как φ_i есть γ отображение и $G \subseteq S_1' \times S_2'$. Следовательно, $|G| = 1$.

б) Если $S = S^{\gamma}$, то S = {0} или полугруппа S содержит ненулевые комбинаторные идеалы. Если I—комбинаторный идеал, то $S \to\to S/I$ должно быть γ отображением. Следовательно, предположим, что I является 0-минимальным идеалом полугруппы S. Тогда I — {0} будет регулярным F классом полугруппы S, порядок H классов которого ≥2. Рассмотрим теперь на S отношение конгруэнтности, определяемое следующим образом:

$s_1 \equiv s_2$ тогда и только тогда, когда $\begin{cases} s_1 = s_2 \text{ для всех } s_1, s_2 \in S, \\ s_1 \mathcal{H} s_2, \text{ если } s_1, s_2 \in I. \end{cases}$

Тогда гомоморфизм $S \to\to S/\equiv$ будет собственным α' гомоморфизмом для $\alpha = \mathcal{R}, \mathcal{L}$ или $\mathcal{H}$. Это противоречит тому, что $S = S^{\alpha'}$. Следовательно, $S = \{0\}$.

Следующее предложение приводит к ослабленной форме теоремы 1.14. Мы включили его сюда потому, что метод доказательства, рассмотренный здесь, существенно отличается от метода, применявшегося для теоремы 1.14.

3.19. Предложение. Пусть $\varphi : S \to\to T$ и α будет одним из $\mathcal{L}$, $\mathcal{R}$ или $\mathcal{H}$. Тогда $\varphi = \varphi_n \dots \varphi_1$, где φ_1, φ_3, ... есть γ гомоморфизмы и φ_2, φ_4, ... есть α′ гомоморфизмы.

Доказательство. Рассмотрим последовательность

$$S \to\to S^{\gamma} \to\to (S^{\gamma})^{\alpha'} \to\to (S^{\gamma\alpha'})^{\gamma} \to\to \dots \to\to \{0\}. \quad (1)$$

Лемма 3.18 (пункт б) утверждает, что эта последовательность достигает {0}. Пусть отображение $\tilde{\Delta} : S \to S \times T$ задается соотношением $\tilde{\Delta}(s) = (s, \varphi(s))$. Рассмотрим последовательность

$$S \xrightarrow{\tilde{\Delta}} S \times T \underset{\gamma}{\to\to} S^{\gamma} \times T \underset{\alpha'}{\to\to} (S^{\gamma})^{\alpha'} \times T \underset{\gamma}{\to\to} \dots \to\to \{0\} \times T \cong T, \quad (2)$$

где отображения на T тождественные, а отображения на первом сомножителе задаются отображениями последовательности (1). То, что эти гомоморфизмы будут попеременно γ и α′ гомоморфизмами, следует из пункта а) леммы 3.18. Тогда ограничение последовательности (2) на образы полугруппы S даст

$$S \twoheadrightarrow S \underset{\gamma}{\twoheadrightarrow} S_1 \underset{\alpha'}{\twoheadrightarrow} S_2 \underset{\gamma}{\twoheadrightarrow} \ldots \twoheadrightarrow T, \qquad (3)$$

поскольку ограничение γ отображения есть γ отображение, а ограничение α′ отображения есть α′ отображение. Композицией гомоморфизмов последовательности (3) будет : S $\twoheadrightarrow$ *T*.

3.20. Следствие. Пусть $\varphi : S \twoheadrightarrow T$ будет МРЕ. Тогда φ есть или γ гомоморфизм или H′ гомоморфизм. [В действительности мы знаем, что φ будет γ (H) гомоморфизмом или H гомоморфизмом.]

3.21. Определение. Пусть $\varphi : S \twoheadrightarrow T$. Предположим, что $\{T_i : i = 1, \ldots, n\}$ есть множество всех таких полугрупп, что $S \overset{\alpha_i}{\twoheadrightarrow} T_i$ и $T_i \underset{\gamma}{\overset{\beta_i}{\twoheadrightarrow}} T$, где $\beta_i \alpha_i = \varphi$. Определим полугруппу $T^{\gamma-1}$, полагая

$$T^{\gamma^{-1}} = (\alpha_1 \times \ldots \times \alpha_n)\,\Delta\,(S).$$

3.22. Утверждение. а) Отображение $T^{\gamma^{-1}} \twoheadrightarrow T$ есть γ гомоморфизм.

б) Пусть *T′* — произвольная полугруппа и

$$\varphi : S \twoheadrightarrow T' \underset{\gamma}{\twoheadrightarrow} T.$$

Тогда $T^{\gamma^{-1}} \underset{\gamma}{\twoheadrightarrow} T' \underset{\gamma}{\twoheadrightarrow} T$.

Доказательство, а) Воспользуемся обозначением, принятым в определении, и введем отображение

$$\theta : T_1 \times \ldots \times T_n \twoheadrightarrow T \times \ldots \times T,$$

полагая $\theta = \beta_1 \times \ldots \times \beta_n$. По лемме 3.18 отображение θ будет γ гомоморфизмом, поскольку им является каждое β_i. Мы докажем, что $\theta\,(T^{\gamma^{-1}}) \cong T$, тем самым будет установлена справедливость пункта а), так как ограничение γ гомоморфизма снова есть γ гомоморфизм. Любой элемент из $T^{\gamma^{-1}}$ имеет вид $[\alpha_1(s), \ldots, \alpha_n(s)]$, поэтому

$$\theta\,[\alpha_1(s), \ldots, \alpha_n(s)] = [\beta_1\alpha_1(s), \ldots, \beta_n\alpha_n(s)] = [\varphi(s), \ldots, \varphi(s)].$$

Отождествим тогда $(t, \ldots, t)$ с $t \in T$. Следовательно,

$$\theta : T^{\gamma^{-1}} \underset{\gamma}{\twoheadrightarrow} T.$$

б) Утверждение этого пункта, очевидно, следует из определения полугруппы $T^{\gamma^{-1}}$.

3.23. Замечание. Пусть $\alpha = \mathcal{R}$, $\mathcal{L}$ или $\mathcal{H}$. Тогда если $\varphi : S \twoheadrightarrow T$, то полугруппа $T^{\alpha'-1}$ определяется точно так же (с соответствующими модификациями), как $T^{\gamma^{-1}}$, и она будет обладать примерно

теми же свойствами. Справедливость этого вытекает из сохранения α' при ограничении (см. пункт а) утверждения 3.9), из того, что элемент прямого произведения полугрупп будет регулярным тогда и только тогда, когда регулярна каждая компонента, а также из того, что два элемента прямого произведения будут α эквивалентны тогда и только тогда, когда их компоненты α эквивалентны. Этими понятиями мы будем пользоваться далее. Отметим, что $T^{\gamma^{-1}}$ и $T^{\alpha'^{-1}}$ имеют смысл только при наличии полугруппы S и гомоморфизма $\varphi : S \to\!\!\!\to T$,

Следующее предложение дает важный способ построения $\mathcal{L}$, γ $(\mathcal{H})$ и γ гомоморфизмов.

3.24.Предложение. а) Рассмотрим узловое произведение $(X_2, G)\mathrm{w}(X_1, S)$, где C — простая слева полугруппа (например, группа) и S — моноид. Пусть $p_1 : (X_2, G)\mathrm{w}(X_1, S) \to\!\!\!\to S$ — естественная проекция, легко видеть, что p_1 — гомоморфизм. Тогда p_1 будет L гомоморфизмом.

б) Рассмотрим узловое произведение $(X_2, C)\mathrm{w}(X_1, S)$, где C— комбинаторная полугруппа и S — произвольная конечная полугруппа. Тогда отображение

$$p_1 : (X_2, C)\mathrm{w}\,(X_1, S) \to\!\!\!\to S$$

будет γ $(\mathcal{H})$ гомоморфизмом.

Доказательство. а) $(X_2, G)\mathrm{w}(X_1, C) \cong F\,(X_1, G) \times {}_{\Upsilon}S$, где $\Upsilon(1)$ есть тождественный эндоморфизм полугруппы G. Так как $F\,(X_1, G) \cong G \times \ldots \times G$ ($|X_1|$ раз), полугруппа $F(X_1, G)$ простая слева, поскольку это свойство сохраняется при взятии прямого произведения.

Следовательно, утверждение достаточно доказать для $G \times {}_{\nu}S \to\!\!\!\to S$, где $\Upsilon(1)$ — тождественный эндоморфизм полугруппы G.

Пусть $p_1\,(s_2, s_1) = p_1\,(t_2, t_1)$ (т. е. $s_1 = t_1$). Мы должны показать, что для всех элементов $s_2, t_2 \in G$, $(s_2, s_1)\,\mathcal{L}\,(t_2, s_1)$. Так как полугруппа G простая слева, $s_2 G = t_2 G$, поэтому если $s_2 \neq t_2$, то существуют такие элементы $x, y \in G$, что $xs_2 = t_2$ и $yt_2 = s_2$.

Тогда $(x, 1)(s_2, s_1) = (x^1 s_2, s_1) =$
$= (t_2, s_1)$ и $(y, 1)(t_2, s_1) = (s_2, s_1)$, т. е. $(s_2, s_1)\mathcal{L}(t_2, s_1)$.

б) Сперва мы покажем, что отображение $(X_2, C)\mathrm{w}(X_1, S) \xrightarrow{p_1} S$ будет у гомоморфизмом. Имеем

$$(X_2, C)\mathrm{w}(X_1, S) \cong F\,(X_1, C) \times {}_{\Upsilon}S$$

и $F(X_1, C) \cong C \times \ldots \times C$ (|X_1| раз), поэтому $F(X_1, C)$ — комбинаторная полугруппа. Следовательно, достаточно доказать утверждение для $C \times_\gamma S$. Пусть G — подгруппа полугруппы $C \times_\gamma S$ и $G_1 = p_1(G)$ — подгруппа полугруппы S. Известно, что существует подгруппа $G_2 \subseteq C$, такая, что G представляет собой расширение G_2 при помощи G_1. Но $G_2=\{1\}$, так как C — комбинаторная полугруппа, поэтому $G \cong G_1$. Следовательно, p_1 будет γ гомоморфизмом.

Теперь для того чтобы доказать, что p_1 является $\gamma(\mathcal{H})$ гомоморфизмом, достаточно показать, что всякий раз, когда $(c_1, s)\mathcal{H}(c_2, s)$, справедливо равенство $c_1 = c_2$. Пусть H есть H класс, содержащий (c_1, s) и (c_2, s), и предположим, что $\mathcal{G}(H)$ — группа Щютценберже (правая) класса H. Тогда действие $\mathcal{G}(H)$ на H представляется в треугольной форме. Далее пусть $\pi \in \mathcal{G}(H)$ и $\bar{\pi} = (d_1, s_1)$ — представитель элемента π в $C \times_\gamma S$. Тогда для $(c, s) \in H$ имеем

$$(c, s)\pi = (c, s)(d_1, s_1) = (c^s d_1, ss_1).$$

Таким образом, легко видеть, что $\pi \in C^1 \mathrm{w} S^1$, поэтому $\mathcal{G}(H) \subseteq \subseteq C^1 \mathrm{w} S^1$. Но C^1 — комбинаторная полугруппа, поэтому отображение проекции $q_1: C^1 \mathrm{w} S^1 \to\!\!\!\to S^1$ будет γ гомоморфизмом. Следовательно, $q_1[\mathcal{G}(H)] \cong \mathcal{G}(H)$ и поэтому ядро ограничения q_1 на $\mathcal{G}(H)$ есть в точности единица группы $\mathcal{G}(H)$.

Пусть теперь π — такой элемент группы $\mathcal{G}(H)$, что $(c_1, s)\pi = (c_2, s)$.

На первую координату π действует как единица, поэтому $\pi \in \ker q_1$. Следовательно, π есть единица группы

$$\mathcal{G}(H) \text{ и } c_1 = c_2.$$

Предложение доказано.

3.25. Утверждение. а) Если S — комбинаторная полугруппа, то $S^\gamma=\{0\}$ и $S^{GM} = \{0\}$. Следовательно, если S^γ — комбинаторная полугруппа, то $S^\gamma = \{0\}$, и если S^{GM} — комбинаторная полугруппа, то $S^{GM} = \{0\}$.

б) Пусть S будет *GGM* полугруппой с отмеченным F классом J. Пусть φ — гомоморфизм полугруппы S, взаимно однозначный на максимальной подгруппе в J. Тогда φ будет взаимно однозначным на S.

в) Если S есть *GM* полугруппа, то $S^\gamma = S$

г) Если S есть *GGM* полугруппа, то $RLM(S) = S^{RLM} = S^{\mathcal{L}'}$.

д) Если S есть *GM* и *RLM* полугруппы, то $S = \{0\}$.

Доказательство, а) $S^{GM} = \{0\}$, когда S — комбинаторная полугруппа, поскольку $GM_J(S) = \{0\}$ всякий раз, когда J будет комбинаторным F классом. Следовательно, $S^{GM} = \{0\}$. Последнее утверждение вытекает из того, что $(S^{\nu})^{\nu} = S^{\nu}$ и $(S^{GM})^{GM} = S^{GM}$.

б) Заметим, что ограничение φ на J будет $\gamma(\mathcal{H})$ гомоморфизмом.

Пусть $s_1 \neq s_2 \in S$. Так как S есть GM полугруппа, существуют элементы $j_1, j_2 \in J$, такие, что $j_1 s_1 j_2 \neq j_1 s_2 j_2$. Тогда или

1) $j_1 s_1 j_2 = 0 \neq j_1 s_2 j_2$,

или

2) $j_1 s_1 j_2 \mathcal{H} j_1 s_2 j_2$

в J.

В первом случае, поскольку $\varphi(J) \neq \{0\}$, мы имеем

$$\varphi(j_1 s_1 j_2) \neq \varphi(j_1 s_2 j_2).$$

Во втором случае, так как φ на J есть γ(H) гомоморфизм, имеем $\varphi(j_1 s_1 j_2) \neq \varphi(j_1 s_2 j_2)$. В обоих случаях, таким образом, $\varphi(s_1) \neq \varphi(s_2)$ и φ взаимно однозначно на S.

в) Этот пункт доказывается с помощью пункта б) и построения полугруппы S^{γ}.

г) $RLM(S) = RLM(S)^{RLM} = RLM(S)^{\mathcal{L}'}$.

Следовательно, достаточно доказать, что $S \to\to RLM(S)$ есть L ′ гомоморфизм, и если $S \xrightarrow[\mathcal{L}']{} T$, то $S^{\mathcal{L}'} = T^{\mathcal{L}'}$.

Из доказательства предложения 2.17 имеем

$$S \subseteq (G^0, G^0) \mathrm{w} (B^0, S') \cong F(B^0, G^0) \times {}_{\gamma}S',$$

где $S' = \{f \in F_R(B^0) : f(0) = 0\}$ и ограничение

$p_1 : F(B^0, G^0) \times {}_{\gamma}S' \to\to S'$ на S приводит к $p_1 : S \to\to RLM(S)$.

Определим подполугруппу

$$T = \{(f_2, f_1) \in F(B^0, G^0) \times {}_{\gamma}S' : (b)f_1 = 0$$

тогда и только тогда, когда $f_2(b) = 0\}$. Покажем, что ограничение p_1 на T будет $\mathcal{L}'$ гомоморфизмом, так что $p_1 : S \to\to RLM(S)$ есть $\mathcal{L}'$ гомоморфизм, поскольку $S \subseteq T$.

Мы должны показать, что любые два элемента из T с одинаковыми первыми координатами будут $\mathcal{L}'$ эквивалентны. Пусть $(f_2, f_1), (g_2, f_1) \in T$. Положим $B_1 = \{b \in B^0 : (b) f_1 \neq 0\}$. Определим $(h_1, 1)$ и $(h_2, 1) \in T$, полагая

$$(b)\,\bar{1} = \begin{cases} b, & \text{если } b \in B_1, \\ 0, & \text{если } b \notin B_1; \end{cases}$$

$$h_1(b) = \begin{cases} g_2(b) f_2(b)^{-1}, & \text{если } b \in B_1, \\ 0, & \text{если } b \notin B_1, \end{cases}$$

$$h_2(b) = \begin{cases} f_2(b) g_2(b)^{-1}, & \text{если } b \in B_1, \\ 0, & \text{если } b \notin B_1. \end{cases}$$

Тогда

$$(h_1,\ \bar{1})(f_2,\ f_1) = (g_2,\ f_1) \quad \text{и} \quad (h_2,\ \bar{1})(g_2,\ f_1) = (f_2,\ f_1),$$

поэтому

$$(f_2,\ f_1)\ \mathcal{L}\ (g_2,\ f_1) \text{ в } T.$$

д) Поскольку *S* есть *GM* полугруппа, то ее отмеченный F класс будет некомбинаторным или $S = \{0\}$. Но так как S есть *RLM* полугруппа, она не может иметь некомбинаторный отмеченный F класс. Следовательно, $S = \{0\}$.

3.26. Обозначения. Условимся, что для полугруппы *S* тройка *(J, G, N)* обозначает, что *J* есть F класс полугруппы *S*, *G* — максимальная подгруппа в *J* и *N* — нормальная подгруппа группы *G* (записывается как $N \lhd G$).

3.27. Определение. а) Пусть S — полугруппа и пусть *(J, G, N)* принадлежит *S*. Представим J^0 с помощью рисовской полугруппы $M^0(G; A,B; C)$. Определим полугруппу *S/(J,* G, *N),* полагая *S/(J, G, N)*=[*S/F(J)*]/≡, где ≡ есть тождественное отношение конгруэнтности на [*SIF(J)*]—*J* и задается гомоморфизмом $(g,a,b)\to(\omega(g),a,b)$ на *J* , где $\omega: G\to\to G/N$ — канонический гомоморфизм групп. Легко проверить, что если для полугруппы J^0 выбрана другая система координат M^0 (*G*; *A, B; P)* (с группой *G*), то отношение конгруэнтности ≡ останется неизменным, т. е. *S/(J, G, N)* не зависит от выбора системы координат (с группой *G*). *S/(J, G, N)* содержит единственный регулярный 0-минимальный идеал, а именно образ $J \cup F(J)$.

б) Пусть S — полугруппа и тройка (*J, G, N)* принадлежит *S*. Определим полугруппу *GM* (*J, G, N)* как *GM [S/(J, G, N)]*.

в) Пусть *T*—полугруппа с единственным регулярным 0-минимальным идеалом *I*. Пусть задан эпиморфизм $\varphi : S\to\to T$. Определим тогда ядро φ как тройку (*J, G, N),* где *J* — единственный минимальный регулярный F класс полугруппы *S,* содержащийся в $\varphi^{-1}(I^{\#})$, *G* — любая

максимальная подгруппа класса *J, N* — (групповое) ядро ограничения φ на *G* (т. е. если 1 — единичный элемент группы *G*, то
N = {*g* ∈ *G*: φ (*g*) = φ (l)}).

3.28. Предложение. Пусть φ — гомоморфизм полугруппы S на *GM* полугруппу и (*J, G, N)* — ядро гомоморфизма φ. Пусть P — свойство гомоморфизмов полугруппы S. определяемое следующим образом:

$$\mathcal{P} = \{(\psi,\ T) : \psi(J) \cap \psi[F(J)] = \varnothing$$

и групповое ядро ограничения ψ на *G* содержится в *N}*. Тогда $(\varphi,\ \varphi(S))$ будет минимальным гомоморфным образом *S* относительно P.

Доказательство. Заметим, что $(\varphi,\ \varphi(S)) \in \mathcal{P}$. Теперь мы должны показать, что если $\varphi(s_1) \neq \varphi(s_2)$ для некоторых элементов $s_1, s_2 \in S$, то $\psi(s_1) \neq \psi(s_2)$ для всех $\psi \in \mathcal{P}$. Так как φ(S) есть *GM* полугруппа по отношению к отмеченному идеалу $\varphi[J \cup F(J)]$, из соотношения $\varphi(s_1) \neq \varphi(s_2)$ вытекает существование таких элементов $j_1, j_2 \in J$, что $\varphi(j_1 s_1 j_2) \neq \varphi(j_1 s_2 j_2)$. Если один из этих элементов, например $\varphi(j_1 s_1 j_2)$, равен нулю, то

$$j_1 s_1 j_2 \in F(J),$$

тогда как $j_1 s_2 j_2 \in J$, так что $\psi(j_1 s_1 j_2) \neq \psi(j_1 s_2 j_2)$ для всехгр $\psi \in P$, откуда следует, что $\psi(s_1) \neq \psi(s_2)$.

Поэтому предположим, что $\varphi(j_1 s_1 j_2),\ \varphi(j_1 s_2 j_2) \in \varphi(J)$. Тогда $j_1 s_1 j_2\ \mathcal{H}\ j_1 s_2 j_2$ и, следовательно, существуют такие элементы $x, y \in S^1$, что

$$x j_1 s_1 j_2 y,\ x j_1 s_2 j_2 y \in G \text{ и } \varphi(x j_1 s_1 j_2 y) \neq \varphi(x j_1 s_2 j_2 y).$$

Пусть $j_1' = x j_1,\ j_2' = j_2 y$. Тогда $(j_1' s_1 j_2') N \neq (j_1' s_2 j_2') N$. Пусть *K* — ядро ограничения ψ на *G*. Так как $K \subseteq N$, имеем

$$(j_1' s_1 j_2') K \neq (j_1' s_2 j_2') K, \text{ т. е. } \psi(j_1' s_1 j_2') \neq \psi(j_1' s_2 j_2'),$$

поэтому $\psi(s_1) \neq \psi(s_2)$.

3.29. Замечание. Непосредственным следствием предложения 3.28 является результат: если тройка (*J, G, N)* есть ядро гомоморфизма φ : S→→*T,* где *T* есть *GM* полугруппа, то $GM(J, G, N) \cong T$.

Следовательно, для каждого *GM* гомоморфного образа полугруппы S существует внутреннее кодирование, а именно одно из ядер *(J, G, N)* гомоморфизма, и не имеет значения, какое ядро выбирается, *GM* полугруппа может быть восстановлена, так как она изоморфна *GM* (*J, G, N).*

3.30 Утверждение, а) Пусть S — полугруппа и G_1, G_3 — две максимальные подгруппы в S. Пусть e_1 и e_2 — единицы групп G_1 и G_2 соответственно. Если $G_1 \mathcal{L} G_2$, то $G_1 = e_1 G_2$ и $G_2 = e_2 G_1$, а

отображение $G_i \to e_i G_i = G_i$, $i, j = 1, 2$, будет изоморфизмом. Если $G_1 \mathcal{H} G_2$, то $G_1 = G_2 e_1$ и $G_2 = G_1 e_2$, а отображение

$$G_i \to\!\!\!\to G_i e_j = G_j, i, j = 1, 2,$$

будет изоморфизмом.

б) Пусть (J, G_1, N_1) принадлежит S. Рассмотрим гомоморфизм φ: $S \to\!\!\!\to GM(J, G_1, N_1)$. Пусть $G_2 \mathrm{F} G_1$. Выберем ядро гомоморфизма φ относительно G_2, (J, G_2, N_2). Тогда $N_1 \cong N_2$. Если $G_1 \mathcal{H} G_2$, то $N_1 = N_2 e_1$ и $N_2 = N_1 e_2$. Если $G_1 \mathcal{L} G_2$, то $N_1 = e_1 N_2$ и $N_2 = e_2 N_1$.

Доказательство, а) Здесь все очевидно.

б) $N_1 = \{g_1 \in G_1 : \varphi(g_1) = \varphi(e_1)\}$ и $N_2 = \{g_2 \in G_2 : \varphi(g_2) = \varphi(e_2)\}$.

Предположим, что $G_1 \mathcal{R} G_2$. Тогда $e_1 e_2 = e_2$ и $e_2 e_1 = e_1$.

Рассмотрим $N_1 e_2$. Пусть $h \in N_1 e_2$; $h = g e_2$, где $g \in N_1$. $\varphi(h) = \varphi(g e_2) = \varphi(e_1)\varphi(e_2) = \varphi(e_2)$ и поэтому $N_1 e_2 \subseteq N_2$. Аналогично $N_2 e_1 \subseteq N_1$; поэтому $N_1 e_2 = N_2$ и $N_2 e_1 = N_1$. В случае, когда $G_1 \mathrm{L} G_2$, доказательство проводится аналогично.

3.31. Определение. Пусть задана тройка (J_1, G_1, N_1) для полугруппы S и $\theta : S \to\!\!\!\to RLM\,[GM(J_1, G_1, N_1)]$.

Предположим, что J_2 — регулярный F класс полугруппы S и G_2 — максимальная подгруппа в J_2. Пусть $1 \in G_2$ есть единица группы G_2. Определим

$$\ker[(J_1, G_1, N_1), (J_2, G_2)] \equiv \{g \in G_2 : \theta(g) = \theta(1)\} = \text{групповое ядро ограничения } \theta \text{ на } G_2.$$

Очевидно, что $\ker[(J_1, G_1, N_1), (J_2, G_2)] \lhd G_2$.

3.32. Замечание. Можно дать иное описание для $N_2 = \ker[(J_1, G_1, N_1), (J_2, G_2)]$. Пусть X равно множеству L классов, принадлежащих образу $J_1 \cup F(J_1)$ в полугруппе $GM(J_1, G_1, N_1)$. Тогда G_2 будет группой операторов множества X, т. е. $X \cdot G_2 \subseteq X$, если положить по определению

$$x \cdot g = x\theta(g) \quad \text{и} \quad x \cdot (g_1 g_2) = (x \cdot g_1) \cdot g_2.$$

Пусть $R = X \cdot 1$ (заметим, что $X \cdot g = K$ для всех элементов $g \in G_2$). G_2 переставляет R, т. е. пара (R, G_2) есть (не обязательно точная) группа преобразований. R называется *областью определения* для G_2.

Теперь X будет множеством отождествленных [при отображении $S \to\!\!\!\to S/(J_1, G_1, N_1) \to\!\!\!\to GM(J_1, G_1, N_1)]\mathcal{L}$ классов из $J^0{}_1$ и R есть подмножество таких L классов, которые G_2 переставляет.

Рассмотрим гомоморфизм φ группы G_2, который делает действие G_2 на R точным. Легко видеть, что $\varphi(G_2) = G_2/N_2$.

Следовательно, $N_2 = \ker[(J_1, G_1, N_1), (J_2, G_2)]$ есть такая часть группы G_2, при исключении которой все еще известно, как G_2 действует на свою область определения R в множестве отождествленных L классов из J^0_1.

Эти понятия будут применяться далее.

3.33. Утверждение. Пусть J^0 — 0-простая полугруппа и X—множество. Предположим, что (X, J^0) есть (не обязательно точная) полугруппа преобразований. Пусть G_1 и G_2 —максимальные подгруппы в J. Тогда G_1 и G_2 действуют на X. Пусть $R_1 = R_{11} \cup \ldots \cup R_{1n}$ и $R_2 = R_{21} \cup \ldots \cup R_{2m}$ — области определения и транзитивные компоненты групп G_1 и G_2 соответственно. Пусть $e_1 \in G_1$ и $e_2 \in G_2$ — единицы G_1 и G_2.

а) Если $G_1 \mathcal{L} G_2$, то группы G_1 и G_2 имеют одинаковые области определения и транзитивные компоненты. Пусть R — область определения (или транзитивная компонента) группы G_1, пусть $N_1 < G_1$, такой, что фактор-группа G_1/N_1 действует точно на R. Тогда G_2/e_2N_1 действует точно на R, и наоборот.

б) Если $G_1 \mathcal{R} G_2$, то области определения и транзитивные компоненты групп G_1 и G_2 находятся во взаимно однозначном соответствии. На самом, деле,

$$R_2 = R_1e_2 = R_{11}e_2 \cup \ldots \cup R_{1n}e_2 \quad \text{и} \quad R_1 = R_2e_1 = R_{21}e_1 \cup \ldots \cup R_{2n}e_1.$$

Пусть R — область определения (или транзитивная компонента) группы G_1 и $N_1 \lhd G_1$, такой, что G_1/N_1 действует точно на R. Тогда G_2/N_1e_2 действует точно на Re_2, и наоборот.

Доказательство. а) $R_1 = XG_1 = Xe_1G_2 \subseteq XG_2 = R_2$. Аналогично $R_2 \subseteq R_1$, так что $R_1 = R_2$. Пусть R_{1i} — транзитивная компонента группы G_1. Тогда существует элемент $x \in R_{1i}$, такой, что $R_{1i} = xG_1$. Но $xG_1 = xe_1G_2$ и $xe_1 \in R_{1i}$, поэтому $R_{1i} = (xe_1)G_2$. Следовательно, каждая транзитивная компонента группы G_1 будет также транзитивной компонентой группы G_2, и наоборот.

Пусть N_2 — нормальный делитель группы G_2, делающий действие G_2 на R точным. Теперь $N_i = \{g \in G_i : rg = r$ для всех $r \in R\}$, $i = 1,2$. Пусть $h \in e_2N_1 \subseteq G_2$.

Запишем $h = e_2g$, $g \in N_1$, $rh = re_2g = rg = r$ для всех $r \in R$, поэтому $e_2N_1 \subseteq N_2$. Аналогично $e_1N_2 \subseteq N_1$, так что

$$e_2N_1 = N_2 \text{ и } e_1N_2 = N_1.$$

б) В этом случае

$$R_1 = XG_1 = XG_2e_1 = R_2e_1 \text{ и } R_2 = XG_2 = XG_1e_2 = R_1e_2.$$

Пусть R_{2i} — транзитивная компонента группы G_2. Пусть $x \in R_1$. Тогда $xe_2 \in R_2$. Определим $R_{1i} = xG_1$ и $R_{2i} = (xe_2)G_2$. Теперь

$$R_{1i} = xG_1 = xe_1G_1 = xe_2e_1G_1 = (xe_2)G_1 = (xe_2)G_2e_1 = R_{2i}e_1.$$

Аналогично $R_{2i}=R_{1i}e_2$. Пусть $N_1 = \{g \in G_1 : rg = r$ для всех $r \in R\}$ и $N_2 = \{h \in G_2 : (re_2)h = re_2$ для всех $r \in R\}$. Положим тогда $h \in N_1e_2$, так что $h=ge_2$, где $g \in N_1$.

Тогда $(re_2)h = rh = rge_2 = re_2$, поэтому $N_1e_2 \subseteq N_2$. Аналогично $N_2e_1 \subseteq N_1$, поэтому $N_1e_2 = N_2$ и $N_2e_1 = N_1$.

Микромодуль 9.
Идивидуальные тестовые задачи

1. Пусть J — нулевой F класс полугруппы S. Докажите, что $N_J(S)$ содержит нетривиальный комбинаторный идеал.
2. Пусть J — регулярный F класс полугруппы S.

а) Определим на S отношение эквивалентности ≡ следующим образом:

$$s_1 \equiv s_2, \text{ если } \begin{cases} s_1, s_2 \in F(J), \\ s_1, s_2 \in J \text{ и } s_1 \mathcal{H} s_2, \\ s_1, s_2 \in S - (J \cup F(J)) \text{ и } s_1 = s_2. \end{cases}$$

Докажите, что ≡ есть отношение конгруэнтности.

б) Пусть φ — гомоморфизм, ассоциированный с ≡, и $J' = \varphi(J)$ — F класс в $\varphi(S)$. Докажите, что

$$RM_{J'}[\varphi(S)] \cong RLM_J(S) \text{ и } LM_{J'}[\varphi(S)] \cong LLM_J(S).$$

3. Пусть J — регулярный F класс полугруппы S. Докажите, что

$$GGM_J(S) \cong RM[LM_J(S)] \cong LM[RM_J(S)].$$

Микромодуль 10.
Методы вычисления сложности конечных полугрупп

Цель настоящего микромодуля состоит в том, чтобы разработать методы вычисления (групповой) сложности заданной конечной полугруппы или заданного приведенного конечного автомата M. В

основном представленные здесь результаты доказаны только для тех автоматов, полугруппы которых представляют собой объединение групп. Однако многие методы, видимо, можно распространить на произвольные конечные полугруппы.

Приводится набор аксиом и доказывается, что им может удовлетворять только одна функция. Показывается, что функция $\#_G$, рассматриваемая для полугрупп, являющихся объединением групп, удовлетворяет этим аксиомам. Используются аксиомы для развития нескольких подходов к вычислению $\#_G$.

1. Аксиомы

1.1. Обозначения. Предполагается, что все рассматриваемые полугруппы имеют конечный порядок. Символ $T \leq S$ указывает, что T есть подполугруппа полугруппы S, в частности $S \leq S$. Символ N обозначает множество неотрицательных целых чисел, а L есть непустая совокупность конечных полугрупп, причем образы гомоморфизмов полугрупп из S снова принадлежат P, т. е. если $S \in \mathsf{L}$ и $S \to\to T$, то $T \in \mathsf{L}$.

Заметим, что если полугруппы S и S_1 — изоморфны, то $S \in \mathsf{L}$ тогда и только тогда, когда $S_1 \in \mathsf{L}$. Далее $\{0\} \in \mathsf{L}$, так как для любой полугруппы S существует гомоморфизм $S \to\to \{0\}$ и по предположению P — непустое множество. Наконец, если $S \leqslant\leqslant S_1 \times \ldots \times S_n$ и $S \in \mathsf{L}$, то $S_i \in \mathsf{P}$ для $j = 1, \ldots, n$.

Примерами совокупностей полугрупп, удовлетворяющих сформулированным требованиям, служат все конечные полугруппы, все регулярные конечные полугруппы, все конечные полугруппы, представляющие собой объединение групп, и все абелевы конечные полугруппы.

1.2. Определение (P аксиомы для сложности). Пусть P — свойство полугрупп и L —совокупность полугрупп, замкнутая относительно взятия образов гомоморфизмов полугрупп из L. В этом случае отображение θ: $L \to N$ называется *G сложностью для* L *относительно* P, если θ удовлетворяет следующим трем аксиомам.

Аксиома 1. Пусть $S \leqslant\leqslant S_1 \times \ldots \times S_n$. Тогда

$$\theta(S) = \max\{\theta(S_i) : i = 1, \ldots, n\}.$$

Аксиома 2. (Основная лемма для сложности). Пусть I — комбинаторный идеал полугруппы S.

Тогда $\theta(S) = \theta(S/I)$; $\theta(\{0\}) = 0$.,

Аксиома 3. Пусть $S \neq \{0\}$ есть *GM* полугруппа. Тогда

$$\theta(S) = \begin{cases} 0\,[RLM(S)] + 1, & \text{если } S \in \mathcal{P}, \\ \theta\,[RLM(S)], & \text{если } S \notin \mathcal{P}. \end{cases}$$

1.3. Предложение. Пусть L и P — такие, как в определении 1.2. Тогда существует самое большее одно отображение, являющееся *G* сложностью для L относительно P.

Доказательство. Предположим, что θ_1 и θ_2 — два отображения, являющиеся *G* сложностью для L относительно P. Пусть S — полугруппа в L наименьшего порядка, такая, что

$$\theta_1(S) \neq \theta_2(S).$$

По аксиоме 2 $S \neq \{0\}$. Но тогда по лемме 2.19 из микромодуля 9 или 1) *S* имеет UMPE, или 2) $S \lessdot\lessdot S_1 \times \ldots \times S_n$, где $|S_k| < |S|$ для $k = 1, \ldots, n$. Случай 3 невозможен, так как по аксиоме 1

$$\theta_j(S) = \max\{\theta_j(S_i) : i = 1, \ldots, n\} \text{ для } j = 1, 2,$$

и, учитывая то, как была выбрана полугруппа *S*, $\theta_1(S_i) = \theta_2(S_i)$ для $i = 1, \ldots, n$. Следовательно, S имеет UMPE и тогда по лемме 2.19 из микромодуля 9 или S есть *GM* полугруппа, или S содержит ненулевой комбинаторный идеал *I*. Последнее невозможно, так как по аксиоме 2 $\theta_j(S) = \theta_j(S/I)$ для $j = 1, 2$ и $\theta_1(S/I) = \theta_2(S/I)$ по определению полугруппы S.

Следовательно, S будет *GM* полугруппой. Отметим, что $|RLM(S)| < |S|$, когда S есть *GM* полугруппа. Следовательно, $\theta_1[RLM(S)] = \theta_2[RLM(S)]$ и тогда по аксиоме 3 в обоих случаях получаем, что $\theta_1(S) = \theta_2(S)$. Это противоречие. Таким образом, предложение доказано.

2. Теорема

Единственность функции, могущей быть *G* сложностью, установлен на в предыдущем пункте. Теперь рассмотрим вопросы, связанные с существованием сложности. Основная теорема этого пункта характеризует различными способами *G* сложность для L относительно P, где L есть совокупность всех полугрупп, представляющих собой объединение групп, и P есть совокупность всех *GM* полугрупп.

Начнем с небольшого обзора теории полугрупп, являющихся объединением групп. *Предполагается, что все рассматриваемые в этом параграфе полугруппы представляют собой объединения групп.* Определение и некоторые результаты можно найти в определении 15 и в предложении 1 из микромодуля 7.

2.1. Краткое изложение результатов п. 3.8 микромодуля 9 для полугрупп, являющихся объединением групп.

а) $\alpha = \alpha'$ для $\alpha = \mathcal{Y}, \mathcal{R}, \mathcal{L}, \mathcal{H}$ и все они сохраняются при ограничениях.

б) $S^{\mathcal{L}} = S^{RLM}$, $S^{\gamma+\mathcal{J}} = S^{GGM}$.

в) Предложение 3.17 из микромодуля 9 справедливо для $\gamma + \mathcal{J}$ и $\mathcal{L}$. (важный результат).

г) $S^{\mathcal{J}}$ есть комбинаторная полугруппа, так как F есть отношение конгруэнтности, когда S представляет собой объединение групп.

2.2. Определение. Говорят, что последовательность $S_1 \to\to S_2 \to\to S_3 \to\to$ ... отображается на последовательность $T_1 \to\to T_2 \to\to T_3 \to\to$ ..., если для всех i = 1,2,3, ... существуют эпиморфизмы $S_i \to\to T_i$.

2.3. Замечание. Пусть α и β — два оператора на полугруппе *S*, такие, что $(S^{\alpha})^{\alpha} = S^{\alpha}$ и $(S^{\beta})^{\beta} = S^{\beta}$ (например, γ, $\gamma + \mathcal{J}$, $\mathcal{L}$, $\mathcal{J}$, *GGM* и т. п.). Рассмотрим последовательность с чередованием α и β для *S*,

$$S \to\to S^{\alpha} \to\to (S^{\alpha})^{\beta} \to\to S^{\alpha\beta\alpha} \to\to \ldots$$

Если некоторый эпиморфизм в последовательности не будет собственным (эпиморфизм собственный, если он не взаимно однозначный), то с этого места последовательность становится постоянной. Предположим, например,что

$$(T^{\alpha})^{\beta} = T^{\alpha}.$$

Тогда

$$T^{\alpha} = (T^{\alpha})^{\alpha} = T^{\alpha\beta\alpha} \text{ и } T^{\alpha} = T^{\alpha\beta} = (T^{\alpha\beta\alpha})^{\beta} \text{ и т. д.}$$

Теперь введем несколько функций, определенных на совокупности полугрупп, являющихся объединением групп. Эти функции принимают целые значения. Основная теорема этого пункта доказывает, что все функции равны между собой.

2.4. Определение. Пусть $S \in \mathcal{S}$, где $\mathcal{S}$ — совокупность полугрупп, представляющих собой объединение групп.

а) Рассмотрим $\theta_a : \mathcal{S} \to N$, где $\theta_a(S) = \#\, c(S)$, *G* сложность полугруппы S.

б) Рассмотрим последовательность

$$\{0\} \leftarrow\leftarrow \{0\}^{\gamma^{-1}} \leftarrow\leftarrow (\{0\}^{\gamma^{-1}})^{\mathcal{L}^{-1}} \leftarrow\leftarrow [(\{0\}^{\gamma^{-1}})^{\mathcal{L}^{-1}}]^{\gamma^{-1}} \leftarrow\leftarrow \ldots \leftarrow\leftarrow S. \quad (б)$$

Определим $\theta_b : \mathcal{S} \to N$, полагая $\theta_b(S)$ = числу собственных гомоморфизмов вида $T^{\mathcal{L}^{-1}} \to\to T$ в последовательности.

в) Рассмотрим последовательность

$$S \to\to S^{\gamma+\mathcal{J}} \to\to (S^{\gamma+\mathcal{J}})^{\mathcal{L}} = S^{(\gamma+\mathcal{J})\mathcal{L}} \to\to S^{(\gamma+\mathcal{J})\mathcal{L}(\gamma+\mathcal{J})} \to\to \ldots \quad (в)$$

Определим $\theta_c : \mathcal{S} \to N$, полагая $\theta_c(S)$ = числу собственных $\mathcal{S}$ гомоморфизмов в последовательности.

г) Рассмотрим последовательность

$$S \to\to S^{GM} \to\to (S^{GM})^{RLM} = S^{GM(RLM)} \to\to S^{GM(RLM)GM} \to\to \dots \quad (г)$$

Определим $\theta_d : \mathcal{S} \to N$, полагая $\theta_d(S)$= числу собственных гомоморфизмов вида $T \to\to T^{RLM}$ в последовательности.

д) Рассмотрим последовательность

$$S \to\to S^{\mathcal{V}} \to\to (S^{\mathcal{V}})^{\mathcal{L}} = S^{\mathcal{V}\mathcal{L}} \to\to S^{\mathcal{V}\mathcal{L}\mathcal{V}} \to\to \dots \quad (д)$$

Определим $\theta_e : \mathcal{S} \to N$, полагая $\theta_e(S)$= числу собственных $\mathcal{S}$ гомоморфизмов в последовательности.

е) Пусть $(GM)_i$ и $(RLM)_i$ обозначают *GM* и *RLM* полугруппы соответственно. Рассмотрим все последовательности вида

$$S \to\to (GM)_1 \to\to (RLM)_1 \to\to (GM)_2 \to\to \dots \quad (е)$$

Назовем нормой каждой последовательности наибольшее целое число *n,* такое, что $(GM)_n \neq \{0\}$. Определим $\theta_f : \mathcal{S} \to N$, полагая $\theta_f(S)$= максимуму норм всех таких последовательностей.

ж) Определим $\theta_g : \mathcal{S} \to N$, полагая $\theta_g(S)$= наибольшему целому *n,* такому, что существует последовательность троек $(J_1, G_1, N_1), \dots, (J_n, G_n, N_n)$ для *S,* удовлетворяющая следующим трем условиям

1) $J_1 < J_2 < \dots < J_n$;
2) $N_i \neq G_i$, $i = 1, \dots, n$;
3) $\ker[(J_i, G_i, N_i), (J_{i+1}, G_{i+1})] \leqslant N_{i+1}$, $i = 1, \dots, n-1$.

з) *Разложением* E для полугруппы S называется функция, которая ставит в соответствие каждому набору

$$[(J_1, G_1, N_1), (J_2, G_2)] \subset J_1 < J_2$$

непустое множество наборов:

$$\left\{ N_{21}^{(\alpha)}, N_{22}^{(\alpha)}, \dots, N_{2\alpha(2)}^{(\alpha)} : \alpha \in A — \text{непустое множество} \right\},$$

где

$$N_{2j}^{(\alpha)} \lhd G_2$$

и

$$N_{21}^{(\alpha)} \cap \dots \cap N_{2\alpha(2)}^{(\alpha)} = N_2 \equiv \ker[(J_1, G_1, N_1), (J_2, G_2)]$$

для каждого $\alpha \in A$. Мы будем писать $N_2 \xrightarrow{(\mathscr{C}, \alpha)} (N_{21}^{(\alpha)}, \ldots, N_{2\alpha(2)}^{\alpha})$ (см. замечание 2.27, где имеются примеры разложений).

Пусть E —разложение полугруппы S. Определим $\theta_h^{(\mathscr{E})} : \mathscr{S} \to N$, полагая $\theta_h^{(\mathscr{E})}(S) =$ наибольшему целому n, такому, что существует последовательность $(J_1, G_1, N_1), \ldots, (J_n, G_n, N_n)$, удовлетворяющая следующим

1) $J_1 < J_2 < \ldots < J_n$;

2) пусть $K_{i+1} = \ker [(J_i, G_i, N_i), (J_{i+1}, G_{i+1})], \quad i = 1, \ldots, n-1.$

трем условиям:

Тогда N_{i+1}, $i = 1, \ldots, n-1$, есть член некоторого набора разложения E:

$$K_{i+1} \xrightarrow{(\mathscr{E}, \alpha)} (K_{(i+1)1}^{(\alpha)}, \ldots, K_{(i+1)\alpha(i+1)}^{(\alpha)}),$$

Определяемого

$$[(J_i, G_i, N_i), (J_{i+1}, G_{i+1})], \text{ т. е. } N_{i+1} = K_{(i+1)j}^{(\alpha)}$$

для некоторого $\alpha \in A$ и некоторого j, такого, что $1 \leq j \leq \alpha (i+1)$;

3) $N_i \neq G_i$, $i = 1, \ldots, n$.

и) Говорят, что полугруппа S имеет тип I, если $U_1 = \{r_0, r_1\}^r$ не делит S^C—максимальный комбинаторный образ полугруппы S. Определим $\theta_i : \mathscr{S} \to N$, полагая $\theta_i(S)$= длине наибольшей (в смысле числа членов) последовательности подполугрупп

$$(T_1, \ldots, T_n)$$

полугруппы S, удовлетворяющей следующим условиям:

1) T_1 — некомбинаторная полугруппа типа I;

2) T_i— некомбинаторная подполугруппа типа I полугруппы $IG(T_{i-1})$ для $j = 2, \ldots, n$;

3) $IG(T_n)$ — комбинаторная полугруппа.

к) Пусть $S \in \mathscr{S}$. Пусть $\mathscr{C}(S)$ обозначает кольцо характеров полугруппы S ад полем комплексных чисел **C**. Все рассматриваемые представления конечномерные. Пусть $\mathscr{R}_1, \ldots, \mathscr{R}_n$ обозначает полное множество неэквивалентных ненулевых неприводимых комплексных представлений полугруппы S. Пусть $\chi_j = \chi(\mathscr{R}_j)$, $j = 1, \ldots, n$, — соответствующий характер. Тогда, как известно, определено взаимно однозначное соответствие

$$\chi_j \leftrightarrow \mathscr{R}_j \quad \text{и } \chi_1, \ldots, \chi_n$$

образуют базис векторного пространства:

$$\mathscr{C}(S) = \left\{ \sum_{i=1}^{n} a_i \chi_i : a_i \in \mathbf{C} \right\}.$$

Роудз доказал, что $\mathscr{R}_j(S)$ есть *GGM* полугруппа и, следовательно, можно рассмотреть гомоморфизм $RLM\mathsf{R}_j$, или $S \to\to \mathscr{R}_j(S) \to\to \to\to RLM[\mathscr{R}_j(S)]$. Пусть $L_1, \ldots L_n$ — совокупность L классов, содержащихся в отмеченном F классе полугруппы $\mathscr{R}_j(S)$. Для элемента $s \in S$ пусть M (s) обозначает $n \times n$ матрицу с коэффициентами из множества {0,1}, определяемую следующим образом:

$$M(s)(i, j) = \begin{cases} 1, & \text{если } L_i s \subseteq L_j, \\ 0 & \text{в противном случае.} \end{cases}$$

Очевидно, что $RLM\mathscr{R}_j(s_1) = RLM\mathscr{R}_j(s_2)$ тогда и только тогда, когда $M(s_1) = M(s_2)$. Определим $\chi(RLM\mathscr{R}_j)$, полагая $\chi(RLM\mathscr{R}_j)(s) = \chi[M(s)]$, что равно числу различных L_i, так что $L_i s \subseteq L_i$. $\chi(RLM\mathscr{R}_j)$ есть характер матричного представления M и, следовательно,

$$\chi(RLM\mathscr{R}_j) = \sum_{i=1}^{n} m_{ji} \chi_i,$$

где m_{ij} — целые неотрицательные числа.

Пусть $A : \mathscr{C}(S) \to \mathscr{C}(S)$ — линейное преобразование, определяемое формулой

$$A(\chi_j) = \chi(RLM\mathscr{R}_j) = \sum_{i=1}^{n} m_{ji} \chi_i.$$

Положим $\mathscr{C}(S)^A = \{\chi \in \mathscr{C}(S) : A(\chi) = \chi\}$. Пусть $B : \mathscr{C}(S)/\mathscr{C}(S)^A \to \to \mathscr{C}(S)/\mathscr{C}(S)^A$ — линейное преобразование, индуцированное A. Роудз показал, что B нильпотентно.

Определим $\theta_j : \mathscr{S} \to N$, полагая $\theta_j(S)$ = индексу B при обычном условии, что индекс равен нулю тогда и только тогда, когда $\mathscr{C}(S) = \mathscr{C}(S)^A$ и наименьшему положительному целому числу n, такому, что $B^n = 0$ в противном случае.

2.5. Теорема. Пусть L — совокупность всех конечных полугрупп, являющихся объединением групп, а $\mathscr{P}$ — совокупность всех *GM* полугрупп. Тогда групповая сложность $\#G$ есть (единственная)

функция, представляющая собой G сложность для L относительно $\mathcal{P}$. Обозначая $\#_G$ как G, получаем

$$0 = \theta_a = 0_b = \ldots = 0_j.$$

Доказательство. Мы должны доказать, что $\#_G$ удовлетворяет аксиомам 1, 2 и 3 (определение 1.2). Ранее было показано, что сложность $\#_G$ удовлетворяет аксиоме 1.

Сейчас с помощью нескольких лемм мы докажем, что функция $\#_G$ удовлетворяет аксиоме 3.

2.6. Обозначения. Напомним определение сложности полугруппы S. В принятой системе обозначений из равенства C (S) = *(n,* **G**), например, следовало, что все минимальные разложения S в узловые произведения имели длину *n,* причем первая координата (справа) была групповой. Предположим, что *n* — четное число. Тогда эквивалентное обозначение для C *(S)* должно быть (**C**, *n);* если *n* нечетное, то $C(S) = (\mathbf{G}, n)$. Таким образом, мы вводим

$$(\mathbf{C}, n),\ (\mathbf{G}, n) \text{ и } (\mathbf{C} \vee \mathbf{G}, n),$$

а именно:

$$(\mathbf{C} \vee \mathbf{G}, n) \equiv (n, \mathbf{C} \vee \mathbf{G}) \text{ для всех } n \geqslant 1;$$

$$(\mathbf{C}, n) \equiv \begin{cases} (n, \mathbf{G}), & \text{если } n \text{ четное}, \\ (n, \mathbf{C}), & \text{если } n \text{ нечетное}, \end{cases}$$

$$(\mathbf{G}, n) \equiv \begin{cases} (n, \mathbf{C}), & \text{если } n \text{ четное}, \\ (n, \mathbf{G}), & \text{если } n \text{ нечетное}. \end{cases}$$

Изменение обозначений вызвано ранее определенной частичной упорядоченностью.

Наконец, мы переходим к новым обозначениям для операции сложения сложностей. Например,

$$(\mathbf{C}, 1) \oplus (\mathbf{G}, n) = (\mathbf{C}, n+1);$$
$$(\mathbf{C}, 1) \oplus (\mathbf{C}, n) = (\mathbf{C}, 1) \oplus (\mathbf{C} \vee \mathbf{G}, n) = (\mathbf{C}, n);$$
$$(\mathbf{G}, 1) \oplus (\mathbf{C}, n) = (\mathbf{G}, n+1);$$
$$(\mathbf{G}, 1) \oplus (\mathbf{G}, n) = (\mathbf{G}, 1) \oplus (\mathbf{C} \vee \mathbf{G}, n) = (\mathbf{G}, n).$$

2.7. Лемма. Пусть $S \neq \{0\}$ будет *GM* полугруппой, отмеченный F класс которой есть объединение групп.. Если $S \neq G^0$ для некоторой группы *G*, то *C (S)* = (**G**, *n)* для некоторого *n.* Конечно, $C(G^0) = (\mathbf{C} \vee \mathbf{G}, 2)$.

Доказательство. Пусть *J* —отмеченный F класс полугруппы S. По условию *J* есть объединение групп, тогда согласно пункту б) утверждения 2.23 из микромодуля 9, если S содержит нуль, то *S*— {0} будет подполугруппой полугруппы S. Следовательно, вообще $S^{\#} = S^0$—{0} будет подполугруппой полугруппы *S*. Заметим, что $S^{\#}$ есть *GM* полугруппа с отмеченным идеалом *J,* являющимся ядром полугруппы $S^{\#}$.

Сначала докажем, что если $S \mid (X_2, C)\mathrm{w}\,(X_1, T)$ и C — комбинаторная полугруппа, то $S^{\#}|T$. Можно считать, что $S|C \times {}_{\gamma}T$. Теперь $S^{\#}| C \times {}_{\gamma}T$, пусть тогда $C \times {}_{\gamma}T \supseteq S' \xrightarrow{\varphi} S^{\#}$

Можно утверждать, что $S^{\#} = (S^{\#})^{\gamma}|(S')^{\gamma}$, это следует из построения минимального γ гомоморфного образа (см. предложение 3.12 и предложение 3.4 из микромодуля 9). Из замечания 3.13 в микромодулт 9 известно, что если $R \subseteq S$, то $R^{\gamma} | S^{\gamma}$. Учитывая все эти факты, мы видим, что $S^{\#} | (C \times {}_{\gamma}T)^{\gamma}$. Но отображение проекции $p_1 : C \times {}_{\gamma}T \twoheadrightarrow T$ будет γ гомоморфизмом, поэтому $(C \times {}_{\gamma}T)^{\gamma} = T^{\gamma}$ и $S^{\#} | T^{\gamma} | T$.

Теперь легко видеть, что $C(S^{\#})$ должна оканчиваться группой, т. е. $C(S^{\#}) = (\mathbf{G}, n)$ для некоторого $n \geq 1$. В противном случае мы получим противоречие. Теперь или $S = (S^{\#})^0$, или $S = S^{\#}$. Но $C(S^{\#}) = C[(S^{\#})^0] = C(S)$, если $S^{\#}$ не является группой.

2.8. Лемма. Пусть S ≠{0} будет *RLM* полугруппой. Тогда *C*(S)=(**C**, *n)* для некоторого $n \geq 1$, т. е. *RLM* полугруппа оканчивается комбинаторной полугруппой.

Доказательство. Предположим, что $C(S) = (\mathbf{G}, n)$ или $(\mathbf{C} \bigvee \mathbf{G}, n)$ Тогда существуют группа преобразований (X_2, *G*) и моноид *T,* такие, что $S| (X_2, G)\ \mathrm{w}\ (X_1, T)$, где $C(T) = (\mathbf{C}, n - 1)$. Тогда отображение $p_1 : (X_2, G)\mathrm{w}\,(X_1, T) \twoheadrightarrow T$ будет L гомоморфизмом и, следовательно, L ' гомоморфизмом (см. предложение 3.24 из микромодуля 9). Тогда $T \twoheadrightarrow [(X_2, G)\mathrm{w}(X_1, T)]^{\mathscr{L}'}$ и, $S^{\mathscr{L}'} | [(X_2, G)\mathrm{w}\,(X_1, T)]^{\mathscr{L}'}$, поэтому $S^{\mathscr{L}'}| T$. Но $S^{\mathscr{L}'} = S^{RLM} = S$, так как S есть *RLM* полугруппа. Следовательно, $S|T$, поэтому, предполагая, что $C(S) \neq (\mathbf{G}, n)$ для некоторого $n \geq 1$, мы приходим к противоречию. Лемма доказана.

2.9. Лемма. Пусть S ≠ {0} и S есть *GM* полугруппа, представляющая собой объединение групп. Тогда $\#_G(S) = 1 + \#_G[RLM(S)]$.

Доказательство. По лемме 2.7 или S будет группой с нулем, или $C(S) = (\mathbf{G}, n)$ для некоторого $n \geq 1$. Предположим, что $S = G^0$ для

некоторой нетривиальной группы *G*. Тогда $C(S) = (\mathbf{C} \vee \mathbf{G}, 2)$ и $\#_G(S) = 1$. $RLM(S) = \{0\}^I$, поэтому $\#_G[RLM(S)] = 0$ и в этом случае утверждение доказано.

Предположим теперь, что $C(S) = (\mathbf{G}, n)$ для некоторого $n \geq 1$.

Пусть I — отмеченный идеал полугруппы S и $I^0 = \mathcal{M}^0(G; A, B; C)$. Тогда в соответствии с пунктом б) предложения 2.17 из микромодуля $S|(G^0, G^0)w(B^0, RLM(S))$, поэтому $C(S) \leqslant (\mathbf{C} \vee \mathbf{G}, 2) \oplus C[RLM(S)]$. Так как *RLM*(S) оканчивается комбинаторной полугруппой, мы можем получить неравенство:

$$C[RLM(S)] \leqslant C(S) \leqslant (\mathbf{G}, 1) \oplus C[RLM(S)].$$

Далее, поскольку $C(S) = (\mathbf{G}, n)$ для некоторого $n \geq 1$, легко видеть, что $C(S) = (\mathbf{G}, 1) \oplus C[RLM(S)]$. Тогда

$$\#_G(S) = 1 + \#_G[RLM(S)].$$

Лемма доказана.

Следовательно, функция $\#_G$ удовлетворяет аксиоме 3. Теперь докажем, что $\#_G$ удовлетворяет аксиоме 2 (основной лемме для сложности).

Основная лемма для сложности (критическая точка всей теории сложности) утверждает, что если I — комбинаторный идеал полугруппы S, то $\#_G(S/I) = \#_G(S)$. Мы доказываем здесь этот факт для полугрупп, являющихся объединением групп, и наше доказательство существенно опирается на свойства этого класса полугрупп.

Представляется естественным получить эту теорему, доказав тот факт, что если I — идеал полугруппы S, то $S|(X_2, I)\ w\ (X_1, S/I)$.

Теорема из этого результата следовала бы немедленно; в действительности и основная теорема декомпозиции была бы тогда тривиальной. Однако сформулированное утверждение неверно. В самом деле, если I — комбинаторный, то соотношение $S|(X_2, C)w(X_1, S/I)$, где C — некоторая комбинаторная полугруппа, в общем случае неверно. Приступая к доказательству теоремы, мы исследуем вид и сложность полугруппы частичного произведения PP $(S^I)^S$ автомата S^I с помощью полугруппы S.

2.10. Замечание. Пусть $S_2 \times_\gamma S_1$ — полупрямое произведение полугрупп S_1 и S_2. Напомним, что имеем

$$(S_2 \times_\gamma S_1)^I = (S_2^I \times S_1^{rI})\, h^\Gamma 2^\sigma_{S_2 \times S_1} (S_2^{rI} \times S_1^I)^\sigma,$$

где

$$h[*, (s_2, s_1)] = (s_2, s_1)$$

и

$$h\,[(s_2, s_1), (t_2, t_1)] = (Y(s_1)t_2, t_1).$$

Автомат $PP\,[(S_2 \times {}_Y S_1)^f]$ можно записать в аналогичной форме, а именно

$$PP\,[(S_2 \times {}_Y S_1)^f] = h_3 (PP(S_2^f) \times S_1'^{rf}) h_2^{\Gamma} 2^{\sigma}_{S_2' \times S_1'} (S_2'^{rf} \times PP(S_1^f))^{\sigma} h_1^{\Gamma}, \quad (1)$$

где $S_i' = S_i \cup \{c\}$, $i = 1, 2$, и где

1) h_t является тождественным на $S_2 \times {}_Y S_1$ и $h_1(c) = (c, c)$;

2) $h_2[*, (s_2, s_1)] = (s_2, s_1)$, $s_i \in S_i'$, $i = 1, 2$,

и

$$h_2[(s_2, s_1), (t_2, t_1)] = \begin{cases} (c, c), \text{ если } (t_2, t_1) = (c, c), \\ (t_2, t_1), \text{ если } (s_2, s_1) = (c, c), \\ (Y(s_1)t_2, t_1) \text{ в противном случае;} \end{cases}$$

3) h_3 является тождественным на $S_2 \times {}_Y S_1$ и $h_3(c, c) = c$. Отметим, что элементы c всегда встречаются в паре.

2.11. Лемма. Пусть S— полугруппа. Тогда

$$C[PP(S^f)^S] \leqslant (1, \mathbf{C}) \oplus C(S).$$

Доказательство. Будем вести доказательство по индукции относительно $\#(S)$ $(\equiv \#(S^1, S))$. Если $\#(S) = 1$, то S — или группа, или комбинаторная полугруппа. Если S — группа, то

$$C[PP(S^f)^S] \leqslant (2, \mathbf{G}) = (1, \mathbf{C}) \oplus C(S).$$

Если S — комбинаторная полугруппа, то S делит узловое произведение полугрупп U_3. Мы покажем, что $PP(S^f)^S$ есть комбинаторная полугруппа. Пусть U_3 (длина полугруппы S) есть наименьшее целое n, такое, что $S|U_3 \mathrm{w} \ldots \mathrm{w} U_3$ (n раз). Предположим, что U_3 (длина полугруппы S) равна 1. Тогда $S|U_3$, поэтому $PP(S^1)^S \mid PP(U_3^1)^S$. Далее $PP(U_3^1)^S$ есть комбинаторная полугруппа, поэтому $PP(S^1)^S$ будет также комбинаторной полугруппой. Тогда основываясь на изложенном ранее и пользуясь соотношением (1) и методом индукции относительно U_3 — длины, нетрудно доказать, что полугруппа $PP(S^1)^S$ будет комбинаторной тогда и только тогда, когда комбинаторной будет полугруппа S. Следовательно,

$C[PP(S^1)^S] = (1, \mathbf{C}) = (1, \mathbf{C}) \oplus C(S)$ и для $\#(S) = 1$ утверждение справедливо.

Предположим, что утверждение справедливо для $\#(S) < n$. Пусть

теперь $\#(S) = n$. Тогда существуют полугруппы S_1 и S_2, такие, что

$$S|(X_2,\ S_2)\mathrm{w}(X_1,\ S_1) = F\ (X_1,\ S_2) \times_Y (S_1)$$

и

$$\#\ (S_1) = 1,\ \#(S_2) = n - 1.$$

Пусть $T = F\ (X_1,\ S_2)$, напомним, что $C\ (T) = C\ (S_2)$. Теперь

$PP\ (S^I)^S | PP\ [(T \times_Y S_1)^I]^S$ и из соотношения (1) получаем, что $PP\ [(T \times_Y S_1)^I]^S | C_2 \mathrm{w} PP\ (T^I)^S\ \mathrm{w} C_1 \mathrm{w} PP\ (S_1^I)^S$, где C_1 и C_2 — комбинаторные полугруппы. По предположению индукции имеем

$$C\ [PP\ (S^I)^S] \leqslant (1,\ \mathbf{C}) \oplus C\ (T) \oplus (1,\ \mathbf{C}) \oplus C\ (S_1).$$

Тогда или $C\ (S_1) = (1,\ \mathbf{C})$, или

$$C\ (S_1) = (1,\ \mathbf{G}) \text{ и } C\ (T) = (n - 1,\ \mathbf{C}).$$

В обоих случаях

$$C\ [PP\ (S^I)^S] \leqslant (1,\ \mathbf{C}) \oplus C\ (T) \oplus C\ (S_1) = (1,\ \mathbf{C}) \oplus C\ (S).$$

2.12. Следствие. $\#_G\ [PP\ (S^I)^S] = \#_G\ (S)$

Доказательство. Так как $S^I \mid PP\ (S^I)$, имеем $\#_G\ (S) \leqslant \#_G [PP\ (S^I)^S]$.

Неравенство в другую сторону получено согласно лемме 2.11.

2.13. Замечание. Вспомним некоторые важные свойства полугрупп, представляющих собой объединение групп (см. предложение 2.24 из микромодуля 8). Пусть S — такая полугруппа. Каждый класс полугруппы S будет простой полугруппой и отношение эквивалентности F будет конгруэнтностью. Если $J_1, \ldots, J_n$ являются F классами полугруппы *S*, эпиморфизм, ассоциированный с конгруэнтностью F, можно представить как эпиморфизм θ из S на $M = (\{1, \ldots, n\}, *)$, где операция * определяется следующим образом: если $a \in J_i$ и $b \in J_k$, то $ab \in J_{i*k}$. есть коммутативная связка.

2.14. Определение. *Комбинаторным идеалом* полугруппы будем называть идеал, максимальные подгруппы которого тривиальны.

2.15. Теорема (основная лемма для сложности**).** Пусть S— полугруппа, являющаяся объединением групп с комбинаторным идеалом *I*. Тогда

$$\#_G\ (S) = \#_G\ (S/I).$$

Доказательство. Для того чтобы сделать более ясными обозначения, предположим, что комбинаторный идеал обозначается символом *K,* вместо *I*. *S — K* есть объединение F классов полугруппы S; занумеруем эти F классы $J_1, \ldots, J_{n-1}$ так, что неравенство $J_i > J_j$ влечет $i<j$. Тогда, поскольку каждый F класс полугруппы *S* есть подполугруппа,

легко видеть, что упорядоченный набор из n членов $(J_1, ..., ..., J_{n-1}, K)$ будет системой для S.

Введем автоматы F_n :

$\Sigma S \to K^I$ и $F_i : \Sigma S \to J_i^I$, $i = 1, \ldots, n-1$, следующим образом. Пусть $\alpha = (s_1, \ldots, s_r) \in \Sigma S$. Тогда

$$(F_n(\alpha), F_{n-1}(\alpha), \ldots, F_1(\alpha)) \equiv (I, \ldots, I)\hat{s}_1\hat{s}_2 \ldots \hat{s}_r.$$

Для большей прозрачности дадим явное индуктивное определение. Если $\alpha \in \Sigma S$ имеет длину 1, т. е., например, $\alpha = s_1$ то для $i = 1, ..., n$

$$F_i(\alpha) = \begin{cases} s_1, & \text{если } s_1 \in J_i \text{ (случай 2),} \\ I & \text{в противном случае (случаи 1 и 3).} \end{cases} \tag{2а}$$

Пусть теперь $\alpha_r = (s_1, \ldots, s_r)$ и $\alpha_{r-1} = (s_1, \ldots, s_{r-1})$. Тогда для $i = 1, ..., n$

$$F_i(\alpha_r) = \begin{cases} F_i(\alpha_{r-1}), & \text{если } s_r \in J_1, \text{ или } F_1(\alpha_{r-1})s_r \in J_2, \\ & \text{или ..., или } F_{i-2}(\alpha_{r-1})F_{i-3}(\alpha_{r-1}) \\ & \ldots F_1(\alpha_{r-1})s_r \in J_{i-1} \text{ (случай 1),} \\ F_i(\alpha_{r-1})F_{i-1}(\alpha_{r-1}) \ldots F_1(\alpha_{r-1})s_r, & \text{если не справедливо ни} \\ & \text{одно из приведенных условий, и } F_{i-1}(\alpha_{r-1}) \ldots \\ & F_1(\alpha_{r-1})s_r \in J_i \text{ (случай 2),} \\ I & \text{в противном случае (случай 3).} \end{cases} \tag{2б}$$

Заметим, что для $F_n(\alpha)$ случай 3 не может возникнуть.

Теперь легко проверить следующее соотношение для автоматов:

$$S^I = h(F_n \times \ldots \times F_1)\Delta_n^\Gamma, \tag{2.3}$$

где $\Delta_n : S \to S \times \ldots \times S$ (n раз) — диагональное отображение, т. е. $\Delta(s) = (s, \ldots, s)$, и отображение $h : S \times \ldots \times S \to\!\!\!\!\to S$ задается соотношением $h(s_1, \ldots, s_n) = s_1 \ldots s_n$.

Из равенства (3) следует, что

$$C(S) \leqslant LUB\{C(F_i^S) : i = 1, \ldots, n\}. \tag{2.4}$$

Теперь запишем для F_n соотношение, включающее идеал K и автоматы $F_1, \ldots, F_{n-1}$, а именно

$$F_n = K^{If} h^\Gamma 2_X [S^{rf} \times (F_{n-1} \times \ldots \times F_1)]^\sigma \Delta_n^\Gamma. \tag{2.5а}$$

Эторавенство легко проверить. Здесь $X = S \times (J_{n-1}^I \times \ldots \times J_1^I)$ и для

$$\alpha, \alpha_{r-1}, \alpha_r \in J_{n-1}^I \times \ldots \times J_1^I$$

$$h(*, (s_1, \alpha)) = \begin{cases} s_1, & \text{если } s_1 \in K, \\ I & \text{в противном случае} \end{cases}$$

и

$$h[(s_{r-1}, \alpha_{r-1}), (s_r, \alpha_r)] = \begin{cases} S^{If}(\alpha_{r-1})\, s_r, & \text{если } \alpha_r = (I, \ldots, I), \\ I & \text{в противном случае.} \end{cases}$$

Тогда

$$F_n^S \mid K^I \text{ w } 2_X^S \text{ w } (S^r \times F_{n-1}^S \times \ldots \times F_1^S),$$

и, так как K^I, 2_X^S и S^r—комбинаторные полугруппы, имеем

$$\#_G(F_n^S) \leqslant \max\{\#_G(F_i^S) : i = 1, \ldots, n-1\}.$$

Поэтому в силу соотношения (4) получаем

$$\#_G(S) \leqslant \max\{\#_G(F_i^S) : i = 1, \ldots, n-1\}. \qquad (2.5б)$$

Теперь приступим к основному этапу доказательства теоремы и покажем, что

$$\#_G(F_i^S) \leqslant \#_G(S/K) \text{ для всех } i = 1, \ldots, n-1. \qquad (2.6)$$

Применяя соотношение (6) к формуле (5б), получим теорему.

Сейчас будет построен комбинаторный автомат M_i, $i = 1, \ldots, n$, который содержит след состояния автомата F_i. Более точно, M_i: $\sum S \to \{i, \ldots, n, 1\}$ — комбинаторный автомат, который будет по значению $M_i(\alpha)$ определять, какой случай соотношения (2) для $F_i(\alpha)$ выполняется ($\alpha \in \sum S$).

2.16. Определение. Пусть $M_i = \{i, i+1, \ldots, n, I\}$ для $i = 1, \ldots, n$.

Определим автомат

$$\beta_i : \Sigma M_i \to M_{i+1}, \quad i = 1, \ldots, n-1$$

следующим образом:

$$\beta_i = h_{i3}([h_{i2}\, 2_{M_i}\{i, \ldots, n\}^{rI^{\sigma}}] \times M_i^{rI}) h_{i1}^{\Gamma},$$

где

1) $h_{i1} : M_i \to M_i \times M_i$ с $h_{i1}(x) = (x, x)$;

2) $h_{i2} : (M_i \cup \{\mp\}) \times M_i \to M_{i+1}$, где

$$h_{i2}(\mp, j) = \begin{cases} I, & \text{если } j = i, \\ j, & \text{в противном случае} \end{cases}$$

и

$$h_{i2}(j_1, j_2) = \begin{cases} I, & \text{если } j_2 = i, \\ j_1 * j_2, & \text{если } j_1 = i \text{ и } j_2 \neq i \text{ или } I, \\ j_2 & \text{в противном случае,} \end{cases}$$

где операция * есть операция, взятая из замечания 2.13;

3) $h_{i3} : M_{i+1} \times M_i \to M_{i+1}$, где

$$h_{i3}(j_1, j_2) = \begin{cases} I, & \text{если } j_2 = I, \\ j_1 & \text{в противном случае.} \end{cases}$$

Очевидно, что β_i, — комбинаторный автомат, т. е. β_i^S — комбинаторная полугруппа.

Определим теперь автомат M_i. Пусть отображение $i : S \to \{1, ..., n\}$ задается соотношением $i(s) = k$, $1 \leqslant k \leqslant n - 1$ тогда и только тогда, когда $s \in J_k$, и соотношением $i(s) = n$ тогда и только тогда, когда $s \in K$, где K — идеал. Тогда положим

$$\mathcal{M}_1 = \{1, ..., n\}^{r_1 i^r}$$

и по определению

$$\mathcal{M}_i = \beta_{i-1} \cdot \beta_{i-2}^{\sigma} \ldots \beta_i^{\sigma i^r}, \quad i = 2, ..., n.$$

Это эквивалентно равенству

$$\mathcal{M}_i = \beta_{i-1} \mathcal{M}_{i-1}^{\sigma}, \quad i = 2, ..., n.$$

(Отметим, что β_i не участвует в определении M_i). Автомат M_i является комбинаторным.

2.17. Лемма.

Пусть $\alpha_1 = s_1$, $\alpha_2 = (s_1, s_2)$, ..., $\alpha_r = (s_1, ..., s_r) \in \Sigma S$.

Тогда автомат M_i обладает следующими свойствами (положим для удобства обозначений $K = J_n$):

а) $\mathcal{M}_1(\alpha_r) = k$ тогда и только тогда, когда $s_r \in J_k$, $1 \leqslant k \leqslant n$;

б) если $\mathcal{M}_i(\alpha_r) = I$ при $i = 2, ..., n$, то $F_{k-1}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \in J_k$ для некоторого k, $1 \leqslant k < i$;

в) если $\mathcal{M}_i(\alpha_r) = k \in \{i, ..., n\}$ для $i = 2, ..., n$, то $s_r \notin J_1$, $F_1(\alpha_{r-1}) s_r \notin J_2$, ..., $F_{i-2}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \notin J_{i-1}$ и

$$F_{i-1}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \in J_k.$$

Если, в частности, $\mathcal{M}_i(\alpha_r) = I$ для $i = 1, ..., n$, то $F_i(\alpha_r)$ удовлетворяет случаю 1 (см. уравнение 2). Если $\mathcal{M}_i(\alpha_r) = i$, то $F_i(\alpha_r)$ удовлетворяет случаю 2. Если $\mathcal{M}_i(\alpha_r) \in \{i + 1, ..., n\}$, то $F_i(\alpha_r)$ удовлет-

воряет случаю 3.

Доказательство.

а) Этот пункт вытекает из определения автомата M_i.

Сперва исследуем $\mathcal{M}_i(\alpha_r)$, $2 \leqslant i \leqslant n$. Пусть j_i — такое наибольшее целое число, что $\mathcal{M}_i(\alpha_{j_i}) \neq I$ в последовательности $(M_i(\alpha_1), \mathcal{M}_i(\alpha_2), \ldots, \mathcal{M}_i(\alpha_{r-1})) = \mathcal{M}_i^{\sigma}(\alpha_{r-1})$, т. е. $\mathcal{M}_i(\alpha_{j_i})$ — последний членв последовательности $\mathcal{M}_i^{\sigma}(\alpha_{r-1})$ (нет члена $\mathcal{M}_i^{\sigma}(\alpha_r)$), не совпадающий с I. Условимся считать $j_i = 0$, если такой автомат не существует. Тогда, рассмотрев определение автомата M_i $i = 2, \ldots, n$, приходим к следующей формуле:

$$\mathcal{M}_i(\alpha_r) = \begin{cases} I, & \text{если } \mathcal{M}_{i-1}(\alpha_r) = i-1 \text{ или } I, \\ \mathcal{M}_{i-1}(\alpha_r), & \text{если предыдущее не выполняется} \\ & \text{и } j_{i-1} = 0 \text{ или} \\ & \mathcal{M}_{i-1}(\alpha_{j_{i-1}}) \neq i-1, \\ (i-1) * \mathcal{M}_{i-1}(\alpha_r), & \text{если верхние условия не выполняются,} \\ & \text{т. е. если } \mathcal{M}_{i-1}(\alpha_{j_{i-1}}) = i-1 \\ & \text{и } \mathcal{M}_{i-1}(\alpha_r) \neq i-1. \end{cases}$$

Заметим, что пункты б) и в) легко доказываются, когда α_r есть последовательность длины 1. Поэтому предположим, что $r \geq 2$. Будем вести доказательство по индукции относительно i, где i — индекс для M_i, доказав сперва пункты б) и в) для $M_2(\alpha_r)$.

б) Если $\mathcal{M}_2(\alpha_r) = I$, то $\mathcal{M}_1(\alpha_r) = 1$, поскольку $\mathcal{M}_1(\alpha_r)$ не может быть равен I. Следовательно, $s_r \in J_1$.

в) Если $\mathcal{M}_2(\alpha_r) = k \in \{2, \ldots, n\}$, то $\mathcal{M}_1(\alpha_r) \in \{2, \ldots, n\}$. Положим $\mathcal{M}_1(\alpha_r) = k'$. Поскольку $j_1 = n-1$, имеем два случая:

1) $\mathcal{M}_1(\alpha_{r-1}) \neq 1$ и $\mathcal{M}_1(\alpha_r) = k = k'$;

2) $\mathcal{M}_1(\alpha_{r-1}) = 1$ и $1 * k' = k$.

Случай 1. $s_r \in J_k$, поэтому $s_r \notin J_1$, $F_1(\alpha_{r-1}) = I$; так как $\mathcal{M}_1(\alpha_{r-1}) \neq 1$, поэтому $F_1(\alpha_{r-1}) s_r \in J_k$.

Случай 2. $s_r \in J_{k'}$, поэтому $s_r \notin J_1$, $F_1(\alpha_{r-1}) \in J$; так как $\mathcal{M}_1(\alpha_{r-1}) = 1$, поэтому $F_1(\alpha_{r-1}) s_r \in J_{1*k'} = J_k$.

Следовательно, утверждения пунктов б) и в) справедливы для $\mathcal{M}_2(\alpha_r)$.

Предположим, что утверждения пунктов б) и в) верны для целых чисел, меньших i, и рассмотрим , $M_i(\alpha_r)$.

б) Если $\mathcal{M}_i(\alpha_r) = I$, то $\mathcal{M}_{i-1}(\alpha_r) = i-1$ или I. По предположению индукции из равенства $M_{i-1}(\alpha_r) = i-1$ следует, что

$$F_{i-2}(\alpha_{r-1}) \ldots F_1(\alpha_{r-1}) s_r \in J_{i-1},$$

и из равенства $\mathcal{M}_{i-1}(\alpha_r) = I$ вытекает,что $F_{k-1}(\alpha_r) \ldots F_1(\alpha_r) \in J_k$ для некоторого $k < i$— 1. В обоих случаях утверждение для $\mathcal{M}_i(\alpha_r)$ доказано.

в) Если $\mathcal{M}_i(\alpha_r) = k \in \{i, \ldots, n\}$, то $\mathcal{M}_{i-1}(\alpha_r) \in \{i, \ldots, n\}$. Пусть $\mathcal{M}_{i-1}(\alpha_r) = k'$. Теперь имеются три возможности:

1) $j_{i-1} = 0$;

2) $\mathcal{M}_{i-1}(\alpha_{j_{i-1}}) \neq i-1$;

3) $\mathcal{M}_{i-1}(\alpha_{j_{i-1}}) = i-1$.

Случай 1. Если $j_{i-1} = 0$, то $k = k'$ и $\mathcal{M}_{i-1}(\alpha_m) = I$ для каждого $m \leqslant r$ — 1. По предположению индукции из этого следует, что $F_{i-1}(\alpha_m)$ удовлетворяет случаю 1 для каждого $m \leqslant r-1$, откуда в свою очередь следует, что $F_{i-1}(\alpha_{r-1}) = I$. Теперь по предположению индукции из равенства $\mathcal{M}_{i-1}(\alpha_r) = k$ вытекает, что $s_r \notin J_1$,

$F_1(\alpha_{r-1}) s_r \notin J_2$, …, $F_{i-3}(\alpha_{r-1}) \ldots F_1(\alpha_{r-1}) s_r \notin J_{i-2}$ и $F_{i-2}(\alpha_{r-1}) \ldots F_1(\alpha_{r-1}) s_r \in J_k \neq J_{i-1}$. Но тогда

$$F_{i-1}(\alpha_{r-1}) \ldots F_1(\alpha_{r-1}) s_r \in J_k$$

и пункт в) в этом случае выполняется.

Случай 2. Если $\mathcal{M}_{i-1}(\alpha_{j_{i-1}}) \neq i-1$, то $k = k'$ и $F_{i-1}(\alpha_{j_{i-1}}) = I$, откуда следует равенство $F_{i-1}(\alpha_{r-1}) = I$. Тогда мы находимся в ситуации случая 1. Поскольку

$$\mathcal{M}_{i-1}(\alpha_r) = k,$$

поэтому снова пункт в) выполняется.

Случай 3. Если $\mathcal{M}_{i-1}(\alpha_{j_{i-1}}) = i-1$, то $(i-1) * k' = k$. По предположению индукции $F_{i-1}(\alpha_{j_{i-1}}) \in J_{i-1}$, поэтому $F_{i-1}(\alpha_{r-1}) \in J_{i-1}$. Так как $\mathcal{M}_{i-1}(\alpha_r) = k' \in \{i, \ldots, n\}$, мы имеем

$$s_r \notin J_1, \quad F_1(\alpha_{r-1}) s_r \notin J_2, \ldots,$$

$$F_{i-3}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \notin J_{i-2}$$

и по индукции $F_{i-2}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \in J_{k'} \neq J_{i-1}$. Тогда

$$F_{i-1}(\alpha_{r-1}) \cdots F_1(\alpha_{r-1}) s_r \in J_{(i-1)*k'} = J_k.$$

Теперь продолжим доказательство теоремы. Если $F_i(\alpha_r)$ будет таким, как в случае 1, мы знаем, что изменений не произошло, т. е. $F_i(\alpha_r) = F_i(\alpha_{r-1})$. Если $F_i(\alpha_r)$ будет таким, как в случае 2, то мы

знаем, что $F_i(\alpha_r) = F_i(\alpha_{r-1})F_{i-1}(\alpha_{r-1})\ldots s_r$. Если же $F_i(\alpha_r)$ будет таким, как в случае 3, то мы знаем, что $F_i(\alpha_r)$ возвращается в I и, чтобы ни случилось перед этим, $(F_i(\alpha_{r-1}))$ полностью забывается.

Эти свойства позволяют построить последующий автомат.

2.18. Замечание. Пусть J будет F классом полугруппы S. Вспомним определение идеала $F(J)$ (см. обозначения 2.2 из микромодуля 9). В случае полугруппы, представляющей собой объединение групп, нуль разделяет $S/F(J)$, поэтому $S - F(J)$ будет подполугруппой полугруппы S. J есть ядро полугруппы $S - F(J)$.

Из этого следует, что для $i = 1, \ldots, n-1$ имеется включение $S - F(J_i) \subseteq S - K$, так как $K \subseteq F(J_i)$, то $S - F(J_i) \subseteq (S-K) \cup \{0\} \cong S/K$. Положим $S_i = S - F(J_i)$, $i = 1, \ldots, n-1$, тогда $S_i | S/K$. Отметим, что любой элемент последовательности $\alpha \in \Sigma S$, принадлежащий $F(J_i)$, не влияет на выход автомата F_i.

Теперь с помощью имеющихся у нас сведений, включая лемму 2.17, нетрудно проверить следующие соотношения для автоматов при $i = 1, 2, \ldots, n$-1:

$$F_i = j_{i4}(J_i \cup \{c\})^{r_{II}} j_{i3}^{\Gamma}[M_i^I \times PP(S_i^I)]^{\sigma} j_{i2}^{\Gamma}[\mathcal{M}_i \times (S_i \cup \{c\})^{r_I}]^{\sigma} j_{i1}^{\Gamma}, \quad (2.7)$$

где 1) $j_{i1}: S \to S \times (S_i \cup \{c\})$, где

$$j_{i1}(s) = \begin{cases} (s, s), & \text{если } s \in S - F(J_i), \\ (s, c), & \text{если } s \in F(J_i); \end{cases}$$

2) $j_{i2}: M_i \times (S_i \cup \{c\}) \to M_i \times (S_i \cup \{c\})$, где

$$j_{i2}(l, x) = \begin{cases} (l, x), & \text{если } l = i \text{ или } I, \\ (l, c), & \text{если } l \neq i \text{ или } I; \end{cases}$$

3) $j_{i3}: M_i \times (S_i \cup \{c\}) \to J_i^I \cup \{c\}$, где

$$j_{i3}(l, x) = \begin{cases} I, & \text{если } l = I, \\ x & \text{в противном случае;} \end{cases}$$

4) $j_{i4}: J_i^I \cup \{c\} \to J_i^I$, где

$$j_{i4}(x) = \begin{cases} I, & \text{если } x = c, \\ x & \text{в противном случае.} \end{cases}$$

Из соотношения (7) получаем

$$C(F_i^S) \leqslant (1, \mathbf{C}) \oplus C[PP(S_i^I)^S] \oplus (1, \mathbf{C}), \quad i = 1, \ldots, n-1.$$

Тогда согласно следствию 2.12 имеем:

$$\#_G(F_i^S) \leqslant \#_G(S_i),\ i=1, \ldots, n-1.$$

Но поскольку $S_i \backslash SIK$, i — 1, ..., n—1, то справедливо соотношение

$$\#_G(F_i^S) \leqslant \#_G(S/K), \quad i=1, \ldots, n-1. \tag{6}$$

Теперь, применяя неравенства (2.5б) и (6), получаем

$$\#_G(S) \leqslant \#_G(S/K).$$

Но S/K есть образ гомоморфизма полугруппы S, поэтому

$$\#_G(S) = \#_G(S/K).$$

Тем самым фундаментальная лемма для сложности доказана (т. е. теорема 2.15).

Таким образом, мы доказали, что $\theta = \theta_\alpha = \#_G$. Оставшаяся часть доказательства теоремы 2.5 основывается на нескольких леммах.

2.19. Лемма. $\theta_b = \theta_c = \theta_d = \theta_e$.

Доказательство. Сначала рассмотрим последовательность (б) определения 2.4. Пусть $S_{-1} = \{0\}^{\gamma^{-1}}$, $S_{-2} = (\{0\}^{\gamma^{-1}})^{\mathscr{L}^{-1}}$ и т. д.

Заметим, что в силу теоремы 1.14 из микромодуля 9 (или предложения 3.19 из микромодуля 9) последовательность должна достигать полугруппы S.

Можно утверждать, что $S_{-1} = (\Pi\theta_j^{(1)})(S)$, где j пробегает совокупность всех таких эпиморфизмов, что

$$\theta_j^{(1)} : S \twoheadrightarrow T_j,\ T_j \xrightarrow[\gamma]{} \{0\},$$

и $S_{-2} = (\Pi\theta_j^{(2)})(S)$, где j пробегает совокупность всех таких эпиморфизмов, что $\theta_j^{(2)} : S \twoheadrightarrow T_j$, и существуют такие эпиморфизмы, что $T_j \xrightarrow[\mathscr{L}]{} T_j' \xrightarrow[\gamma]{} \{0\}$ и т. д. Для того чтобы доказать это, положим $U_{-k} = (\Pi\theta_j^{(k)})(S)$. По определению полугруппы S_{-1} имеем $U_{-1} = S_{-1} = S^C$, где S^C — максимальный гомоморфный комбинаторный образ полугруппы S. Теперь $S \twoheadrightarrow U_{-2} \xrightarrow[\mathscr{L}]{} U_{-1} \xrightarrow[\gamma]{} \{0\}$, поскольку прямые суммы и ограничения L и γ гомоморфизмов являются L и γ гомоморфизмами соответственно. Так как $S_{-2} = (S_{-1})^{\mathscr{L}^{-1}}$, имеем $S_{-2} \twoheadrightarrow U_{-2}$.

С другой стороны, $S \twoheadrightarrow S_{-2} \xrightarrow[\mathscr{L}]{} S_{-1} \xrightarrow[\gamma]{} \{0\}$, поэтому

$U_{-2} \twoheadrightarrow S_{-2}$. Следовательно, $U_{-2} = S_{-2}$. Продолжая эти рассуждения, мы докажем, что $U_{-i} = S_{-i}$ для всех $i = 1, 2, \ldots$ Пусть k — такое наименьшее целое число, что $S_{-k} = S$.

Сейчас мы докажем, что число собственных L гомоморфизмов в последовательности

$$S = S_{-k} \twoheadrightarrow S_{-k+1} \twoheadrightarrow \cdots \twoheadrightarrow S_{-2} \underset{\mathscr{L}}{\twoheadrightarrow} S_{-1} \underset{\gamma}{\twoheadrightarrow} \{0\}, \quad (б)$$

[т. е. θ_b (S)] не превосходит числа собственных L гомоморфизмов в *любой* последовательности, состоящей из чередующихся γ и L гомоморфизмов полугруппы и начинающейся с γ гомоморфизма.

Пусть k — четное число. Тогда последовательность (б) начинается с L гомоморфизма. Предположим, что последовательность, состоящая из чередующихся L и γ гомоморфизмов полугруппы S и начинающаяся с γ гомоморфизма, достигает {0} за k— 1 шагов. Тогда из имеющихся результатов для $S_{-(k-1)}$ мы получаем, что $S = S_{-(k-1)}$. Это противоречие. Если в последовательности, с которой мы имеем дело, {0} получается на k— 2 шаге, то, добавляя тривиальное отображение $\{0\} \underset{\gamma}{\twoheadrightarrow} \{0\}$ к концу последовательности, мы получаем последовательность длины k — 1 и снова приходим к противоречию. Следовательно, длина последовательности должна быть не меньше k и утверждение для случая, когда k —четное число, доказано.

Пусть число k— нечетное, так что последовательность (б) начинается с γ гомоморфизма. Если длина последовательности чередующихся гомоморфизмов не превосходит числа k — 2, то снова возникает противоречие. Поэтому в рассматриваемом случае длина последовательности должна быть равна самое меньшее k— 1. Но легко видеть, что для L гомоморфизмов утверждение справедливо, поэтому все доказано.

Теперь мы применим аппарат, развитый в п. 3.8 микромодуля 9, для того, чтобы получить коммутативную диаграмму (см. рис. 3.2).

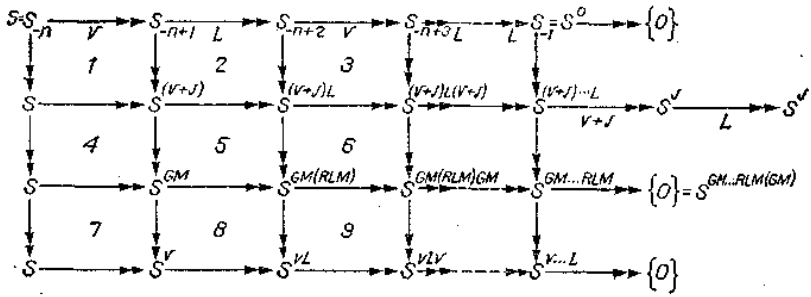


Рис. 3.2

Если последовательность (б) начинается с L гомоморфизма, добавим в начале тождественное отображение, чтобы она начиналась с γ гомоморфизма. Тогда заметим, что $S_{-1} = S^{C} \to\!\!\to S^{\mathcal{F}}$, так как для полугруппы, являющейся объединением группы, S^{F} будет комбинаторной полугруппой. Тогда каждое γ отображение, исключая последнее, будет γ+F отображением. Следовательно, квадрат 1 коммутативен.

Так как $S_{-n+1} \xrightarrow[\mathcal{L}]{} S_{-n+2}$, мы имеем последовательность $S_{-n+1} \to\!\!\to S_{-n+2} \to\!\!\to S\mathcal{L}_{-n+1}$. Коммутативность квадрата 2 следует из пункта б) предложения 3.2 из микромодуля 9.

Так как имеется последовательность

$$S_{-n+2} \xrightarrow[\nu+\mathcal{F}]{} S_{-n+3} \to\!\!\to S^{(\nu+\mathcal{F})}_{-n+2},$$

квадрат 3 коммутативен в силу утверждения 3.15 из микромодуля 9. Продолжаем действовать таким же способом на соединении последовательностей (б) и (в).

Из замечания 3.16 в микромодуле 9 теперь следует коммутативность квадратов 4 и 7. Так как $S^{\mathcal{L}} = S^{RLM}$, то квадраты 5 и 8 коммутативны. Для квадрата 6 имеем:

$$\begin{array}{ccc} S^{(\nu+\mathcal{F})\mathcal{L}} & \to\!\!\to & S^{(\nu+\mathcal{F})\mathcal{L}\,(\nu+\mathcal{F})} \\ \downarrow & & \downarrow \\ S^{GM\,(RLM)} & \to\!\!\to & S^{GM\,(RLM)\,(\nu+\mathcal{F})} \to\!\!\to S^{GM\,(RLM)\,GM} \end{array}$$

Для квадрата 9 в силу утверждения 3.7 из микромодуля 9 имеем:

$$\begin{array}{ccc} S^{GM\,(RLM)} & \to\!\!\to & S^{GM\,(RLM)\,GM} \\ \downarrow & & \downarrow \\ S^{\nu\mathcal{L}} & \to\!\!\to & S^{\nu\mathcal{L}GM} \to\!\!\to S^{\nu\mathcal{L}\nu} \end{array}$$

Продолжая далее эти рассуждения, получим коммутативность всей диаграммы.

Так как S_{-1} — комбинаторная полугруппа, полугруппы $S^{(\nu+\mathcal{F})\ldots\mathcal{L}}$, $S^{GM\ldots RLM}$ и $S^{\nu\ldots\mathcal{L}}$ также комбинаторные. Покажем, что если T — комбинаторная полугруппа, то

$$T^{(\nu+\mathcal{F})} = T^{\mathcal{F}},\ T^{GM} = \{0\} \text{ и } T\nu = \{0\}.$$

Последние два равенства следуют из пункта а) утверждения 3.25 из микромодуля 9. Для доказательства первого напомним, что $T^{\gamma+\mathscr{F}} \leqslant\leqslant T^{\gamma} \times T^{\mathscr{F}}$. Но $T^{\gamma} = \{0\}$. Следовательно, справедливы соотношения $T^{(\gamma+\mathscr{F})} \leqslant T^{\mathscr{F}}$ и $T^{(\gamma+\mathscr{F})} \to\to T^{\mathscr{F}}$, поэтому они изоморфны.

Теперь нетрудно убедиться, что полугруппа $S^{(\gamma+\mathscr{F})} \ldots \mathscr{L}^{(\gamma+\mathscr{F})} = S^{(\gamma+\mathscr{F})} \ldots \mathscr{L}^{\mathscr{F}}$ изоморфна S^{F}, так как каждое отображение в последовательности (в) является F гомоморфизмом. Очевидно, что $S^{\mathscr{F}\mathscr{L}} = S^{\mathscr{F}}$. Следовательно, мы объяснили диаграмму (см. рис. 3.2). Совершенно ясно, что число собственных L гомоморфизмов в последовательности (б) не меньше соответствующего числа в последовательностях (в), (г) или (д), т. е.

$$\theta_b(S) \geqslant \theta_c(S) \geqslant \theta_d(S) \geqslant \theta_e(S).$$

Но мы показали, что $\theta_b(S) \leqslant$ числа собственных L гомоморфизмов в последовательности чередующихся γ и L гомоморфизмов для S, начинающейся с γ гомоморфизма и заканчивающейся $\{0\}$. [Конец последовательности (в) будет нулем, так как $S^{\mathscr{F}} \xrightarrow[\gamma]{} \{0\}$.] Следовательно,

$$\theta_b(S) = \theta_c(S) = \theta_d(S) = \theta_e(S)$$

для всех полугрупп $S \in$ L. Лемма доказана.

2.20. Лемма. $\theta = \theta_b = \theta_c = \theta_d = \theta_e$.

Доказательство. Покажем сначала, что θ_c удовлетворяет аксиоме 1. Пусть $S \leqslant\leqslant S_1 \times \ldots \times S_n$. Для каждого числа k = 1, ..., n рассмотрим последовательность

$$S_k \to\to S^{\gamma}_k + \mathscr{F} \to\to S^{(\gamma_k+\mathscr{F})}\mathscr{L} \to\to \ldots \to\to S^{\mathscr{F}}_k.$$

Прямая сумма этих последовательностей (k = 1, ..., n) сводится к ограничению на диагональ и взятию последовательных образов. Тогда по предложению 3.17 из микромодуля 9 результирующей последовательностью будет последовательность (в). Из этого сразу следует, что θ_c удовлетворяет аксиоме 1.

Теперь докажем, что θ_c удовлетворяет аксиоме 2. S$\to\to$*S/I* тогда и только тогда, когда идеал *I* комбинаторный. Из $S \xrightarrow[\gamma]{} S/I$ получаем, что $S \to\to S/I \to\to S^{\gamma} = (S/I)^{\gamma}$, поэтому последовательности (д) для S и для *S/I* различаются только первым членом и имеют одинаковую длину. Это доказывает, что θ_c удовлетворяет аксиоме 2.

Наконец, мы покажем, что θ_c удовлетворяет аксиоме 3. Пусть S $\neq \{0\}$ есть *GM* полугруппа. Тогда в силу пункта г) утверждения 3.25 из микромодуля 9 *S*$\to\to$*RLM (S)* равно S$\to\to S^{L}$. Далее S есть *GGM* полу-

группа и поэтому $S = S^{GGM} = S^{\mathfrak{N}+\mathfrak{F}}$. Таким образом, последовательность (в) для S имеет вид

$$S \to\to S^{\mathfrak{N}+\mathfrak{F}} = S \to\to RLM\,(S) = S^{\mathfrak{L}} \to\to \to\to S^{\mathfrak{L}\,(\mathfrak{N}+\mathfrak{F})} \to\to \ldots$$

и, следовательно, $\theta_c\,(S) = \theta_c\,[RLM\,(S)] + 1$.

2.21. Лемма. Если $S \in \mathfrak{S}$ и $T \mid S$, то $0\,(T) \leqslant \theta\,(S)$.

Доказательство. $T|S$ влечет $T^{GM}|S^{GM}$ влечет $T^{GM(RLM)}|S^{GM(RLM)}$ влечет ... и т. д. Поэтому когда последовательность для S достигает $\{0\}$, последовательность для T должна достичь $\{0\}$ по крайней мере на члене того же номера. Следовательно, $\theta_d\,(T) \leqslant \theta_d\,(S)$. Но $\theta = \theta_d$.

2.22. Лемма. $\theta_j = \theta$.

Доказательство. Заметим, что если полугруппа S является объединением групп и есть *GGM,* но не *GM* полугруппа, то $S = \{0\}^I$. Действительно, отмеченный идеал I полугруппы S должен быть комбинаторным и поэтому $I^{\#} = A^I \times B^I$. Но требование, чтобы S действовала точно слева и справа на I, заставляет $I^{\#}$ быть одноэлементным множеством. Следовательно, $S = \{0\}^I$.

Теперь, если мы заменим *GM* полугруппы в последовательности (е) *GGM* полугруппами и определим норму последовательности как наибольшее целое число *n,* такое, что $(GGM)_n$ будет некомбинаторной, то, очевидно, максимум норм всех этих последовательностей равен $\theta_f\,(S)$.

Рассмотрим все последовательности этого вида и добавим к каждой из них тривиальное отображение $\{0\}^I \to\to \{0\}^I \to\to \ldots \to\to \{0\}^I$ с тем, чтобы все они имели максимальную длину. Затем возьмем прямую сумму всех этих последовательностей. Число членов прямого произведения вида *GGM,* которые некомбинаторны, равно $\theta_f\,(S)$. Тогда ограничим эту последовательность на диагональ и рассмотрим первый образ. Очевидно, что $S^{GGM} = S^{(\mathfrak{N}+\mathfrak{F})}$ и S^{GGM} есть подпрямое произведение всех GGM_1 полугрупп всех этих последовательностей. Запишем это как

$$S^{(\mathfrak{N}+\mathfrak{F})} = S^{GGM} \leqslant\leqslant GGM_1^{(1)} \times \cdots \times GGM_1^{(k)}.$$

Применим теперь предложение 3.17 из микромодуля 9 для того, чтобы получить соотношение

$$S^{(\mathfrak{N}+\mathfrak{F})\,\mathfrak{L}} \leqslant\leqslant (GGM_1^{(1)})^{RLM} \times \cdots \times (GGM_1^{(k)})^{RLM}.$$

Однако по транзитивности подпрямых произведений $S^{(\mathfrak{N}+\mathfrak{F})\mathfrak{L}}$ есть подпрямое произведение второго члена прямой суммы всех последовательностей, поскольку им является

$$(GGM_1^{(1)})^{RLM} \times \ldots \times (GGM_1^{(k)})^{RLM}.$$

Запишем второй член $RLM_1^{(1)} \times \cdots \times RLM_1^{(k)}$. Тогда снова в соответствии с предложением 3.17 из микромодуля 9 получаем $S^{(\nu+\mathscr{J})}\mathscr{L}^{(\nu+\mathscr{J})} \leqslant\leqslant RLM_1^{(1)\,GGM} \times \ldots \times RLM_1^{(k)\,GGM}$,

так что $S^{(\nu+\mathscr{J})}\mathscr{L}^{(\nu+\mathscr{J})} \leqslant\leqslant GGM_2^{(1)} \times \cdots \times GGM_2^{(k)}$. Далее продолжаем рассуждать аналогично.

Воспользуемся теперь следующим, легко доказываемым фактом. Пусть $S \leqslant\leqslant S_1 \times \ldots \times S_n$. В этом случае полугруппа S будет комбинаторной тогда и только тогда, когда каждая полугруппа S_i комбинаторна, где $i = 1, \ldots, n$.

Если $\theta_f(S) = n$, то первый член последовательности (в), который мог бы быть комбинаторным, будет подпрямым произведением

$$RLM_n^{(1)} \times \ldots \times RLM_n^{(k)}.$$

В этом случае последовательность (в) оканчивается самое худшее после одного шага, так как если C — комбинаторная полугруппа и

$$S \xrightarrow[\mathscr{J}]{} C, \text{ то } C^{\nu+\mathscr{J}} = S^{\mathscr{J}}.$$

В любом случае следующий член последовательности (в) будет комбинаторным, так как он представляет собой подпрямое произведение для $\{0\}^I \times \ldots \times \{0\}^I$. Если теперь

$$S \xrightarrow[\mathscr{J}]{} T \xrightarrow[\mathscr{J}]{} C = T^{(\nu+\mathscr{J})}$$

и C—комбинаторная полугруппа, то $C = S^{\mathsf{F}}$.

Поэтому подсчет последовательности (в) доставит нам n собственных L гомоморфизмов. Следовательно, $\theta_f(S) = \theta_c(S)$ для всех $S \in \mathrm{L}$.

Рассматриваемое далее утверждение представляет собой следствие только что изложенного доказательства. Пусть $S^{(\nu_n+\mathscr{J})} \ldots \mathscr{L}$ обозначает n-й член такого вида в последовательности (в) для полугруппы S. Пусть $\theta(S)=n$. Рассмотрим все самые длинные *GGM — RLM* последовательности для S. Тогда мы знаем, что каждая GGM_n есть последняя *GGM* полугруппа в последовательности, которая не будет $\leqslant\{0\}^I$. Для члена RLM_n не обязательно выполняется соотношение $\leqslant\{0\}^I$.

Мы укажем необходимые и достаточные условия для того, чтобы каждая полугруппа $RLM_n \leqslant \{0\}^I$. Этот результат окажется полезным в доказательстве равенства $\theta_i = \theta$.

2.23. Утверждение. Пусть имеется описанная ранее ситуация.

В этом случае $RLM_n \preceq \{0\}^I$ тогда и только тогда, когда $U_1 \mid S_{(n)}^{(\gamma+\mathscr{F})\ldots\mathscr{L}}$

Доказательство. Напомним, что $U_1 \mid S$ тогда и только тогда, когда $U_1 \leq S$. Отмеченный F класс *RLM* полугруппы имеет вид A^r.

Если $|A| > 2$, то, $U_1 \leq A^r$. Если $|A| = 1$, то *RLM* полугруппа должна иметь вид $\{0\}^I$ или $\{0\}$. Следовательно, $RLM_n \preceq \{0\}^I$ тогда и только тогда, когда $U_1 \mid RLM_n$.

Из доказательства леммы 2.22 известно, что $S_{(n)}^{(\gamma+\mathscr{F})\ldots\mathscr{L}}$ есть подпрямое произведение всех *RLM* полугрупп, стоящих на n-м месте в *GGM— RLM* последовательностях для S. Если некоторая полугруппа $RLM_{(n)} \preceq \{0\}^I$, то, так как $S_{(n)}^{(\gamma+\mathscr{F})\ldots\mathscr{L}} \twoheadrightarrow RLM_{(n)}$, мы имеем $U_1 \mid RLM_n \mid S_{(n)}^{(\gamma+\mathscr{F})\ldots\mathscr{L}}$. Наоборот, предположим, что $U_1 \mid S_{(n)}^{(\gamma+\mathscr{F})\ldots\mathscr{L}}$. Тогда U_1 делит прямую сумму всех упомянутых *RLM* полугрупп. Но полугруппа U_1 принадлежит классу *IRR*, поэтому U_1 делит некоторую RLM_n полугруппу. Следовательно, $RLM_n \preceq \{0\}^I$.

2.24. Лемма. $\theta = \theta_g$.

Доказательство. Пусть

$$S \twoheadrightarrow GM_1 \twoheadrightarrow RLM_1 \twoheadrightarrow GM_2 \twoheadrightarrow \ldots$$

есть последовательность типа (е) наибольшей длины. Если для нее GM_n — последняя ненулевая *GM* полугруппа, то $n = \theta$ (S). Заменим эту последовательность следующей последовательностью *равной длины*

$$S \twoheadrightarrow GM_1 \twoheadrightarrow RLM(GM_1) \twoheadrightarrow GM_2 \twoheadrightarrow \ldots$$

[Этоможно сделать, так как согласно утверждению 3.25 из микромодуля 9

$$RLM(GM_j) = GM_j^{\mathscr{L}} = GM_j^{RLM} \twoheadrightarrow RLM_1.]$$

Пусть (J_i, G_i, N_i) — ядро отображения $S \twoheadrightarrow GM_i$ (см. пункт в) определения 3.27 из микромодуля 9). Тогда мы имеем последовательность троек (J_1, G_1, N_1), ..., (J_n, G_n, N_n), удовлетворяющую соотношениям $J_1 < < J_2 < \ldots < J_n$. Легко видеть, что если $i < j$, то отображение $S \twoheadrightarrow GM_j$ переводит J_i в $\{0\}$. Кроме того, $N_i \neq G_i$ для $i = 1, \ldots, n$, так как максимальные подгруппы в отмеченных F классах полугрупп GM_i изоморфны G_i/N_i и по предположению эти отмеченные F классы некомбинаторны, т. е. для фактор-групп G_i/N_i справедливы неравенства $|G_i/N_i| > 1$ для $i = 1, \ldots, n$.

Пусть $K_{i+1} = \ker [(J_i, G_i, N_i), (J_{i+1}, G_{i+1})]$ (см. определение 3.31 из микромодуля 9). Тогда K_{i+1} есть ядро ограничения на группу G_{i+1} гомоморфизма $S \to\!\!\!\to RLM\ (GM_i)$ и N_{i+1} есть ядро ограничения на группу G_{i+1} гомоморфизма $S \to\!\!\!\to RLM\ (GM_i) \to GM_{i+1}$. Из элементарных фактов теории групп следует, что $K_{i+1} \leqslant N_{i+1}$. Следовательно, последовательность троек $(J_1, G_1, N_1), \ldots, (J_n, G_n, N_n)$ удовлетворяет условиям 1—3 определения θ_q. Таким образом, $\theta_q\ (S) \geq \theta\ (S)$ для всех полугрупп $S \in \mathsf{L}$.

Наоборот, пусть последовательность $(J_1, G_1, N_1), \ldots, (J_n, G_n, N_n)$ удовлетворяет условиям 1—3, где $n = \theta_g\ (S)$. Положим $S' = J_1 \cup \ldots \cup J_n$, так что S' есть подполугруппа полугруппы S, $J_1, \ldots, J_n$ являются F классами полугруппы S' и $(J_1, G_1, N_1), \ldots, (J_n, G_n, N_n)$ есть последовательность для S', удовлетворяющая условиям 1—3.

Рассмотрим гомоморфизмы

$$\varphi_1 : S' \to GM\ (J_1, G_1, N_1) \to\!\!\!\to RLM\ [GM\ (J_1, G_1, N_1)].$$

Заметим, что K_2 есть группа, являющаяся ядром ограничения на G_2 гомоморфизма φ_1 и по предположению $K_2 \leq N_2$. Предположим, что $\varphi_1\ (J_2) \subseteq \varphi_1\ (J_1)$. $\varphi_1\ (J_1)$ будет комбинаторным, тогда $\varphi_1\ (G_2) = G_2/K_2 = \{1\}$, но это противоречие. Следовательно, имеем $\varphi_1\ (J_2) \cap \varphi_1\ [F\ (J_2)] = \varnothing$, так как $J_1 = F\ (J_2)$. По предложению 3.28 из микромодуля 9 получаем гомоморфизмы

$$S' \xrightarrow{\varphi_1} RLM\ [GM\ (J_1, G_1, N_1)] \to\!\!\!\to GM\ (J_2, G_2, N_2) \to\!\!\!\to RLM\ [GM\ (J_2, G_2, N_2)].$$

Дальше действуем аналогично для того, чтобы построить последовательность типа (е). $GM\ (J_n, G_n, N_n) \neq \{0\}$, поскольку $N_n \neq G_n$. Следовательно, $\theta_g\ (S) = n \leqslant \theta_f\ (S') = \theta\ (S') \leqslant \theta\ (S)$. Таким образом,

$$\theta_g\ (S) = \theta\ (S)$$

для всех полугрупп $S \in \mathsf{L}$.

2.25. Утверждение. а) Пусть задана тройка (J, G, N). Предположим, что $G/N \lessdot\!\!\lessdot G_1 \times \ldots \times G_n$ (т. е. существуют $N_i \lhd G$, $i = 1, 2, \ldots, n$, где $G_i = G/N_i$ и $N_1 \cap \ldots \cap N_n = N$). Тогда

$$GM\ (J, G, N) \lessdot\!\!\lessdot GM\ (J, G, N_1) \times \ldots \times GM\ (J, G, N_n).$$

б) $\theta\ [GM\ (J, G, N)] = \theta\ [GM\ (J, G, N_i)]$ для некоторого $i = 1, \ldots, n$.

Доказательство, а) Так как $N \leq N_i$, существуют гомоморфизмы

$$\varphi_i : GM\ (J,\ G,\ N) \to\to GM\ (J,\ G,\ N_i),\ i = 1,\ \ldots,\ n.$$

Ограничение гомоморфизма φ_i на максимальную подгруппу *G/N* отмеченного F класса из *GM (J, G, N)* есть отображение $G/N \to\to G/N_i = G_i$, поэтому отображение $(\varphi_1 \times \ldots \times \varphi_n)\Delta$ будет взаимно однозначным на *G/N*. Тогда отображение $(\varphi_1 \times \ldots \times \varphi_n)\Delta$ взаимно однозначно на *GM (J, G, N)* согласно пункту б) утверждения 3.25 из микромодуля 9.

б) Этот пункт следует из аксиомы 1 (определение 1.2).

2.26. Лемма. Пусть E — разложение полугруппы S. Тогда

$$\theta_h^{(\mathscr{E})} = \theta.$$

Следовательно, θ_h не зависит от E.

Доказательство. Пусть $(J_1,\ G_1,\ H_1),\ \ldots,\ (J_n,\ G_n,\ H_n)$ — последовательность наибольшей длины для полугруппы *S*, удовлетворяющая условию определения θ_q. Тогда $n = \theta(S)$. Пусть полугруппа $S' = J_1 \cup \ldots \cup J_n$ выбирается так же, как в доказательстве леммы 2.24.

Положим $K_2 = \ker [(J_1,\ G_1,\ H_1),\ (J_2,\ G_2)]$. В силу предложения 3.28 из микромодуля 9 имеется следующая последовательность:

$$S' \to\to GM\ (J_1, G_1, H_1) \to\to RLM\ [GM\ (J_1, G_1, H_1)] \to\to GM\ (J_2, G_2, K_2) \to\to GM\ (J_2, G_2, H_2) \to\to \ldots$$

Поэтому мы получаем, что

$$\theta\ [GM\ (J_2,\ G_2,\ K_2)] = n - 1.$$

Рассмотрим разложение для K_2:

$$K_2 \overset{(\mathscr{E},\ \alpha)}{\to\to} K_{21}^{(\alpha)}, \ldots, K_{2\alpha(2)}^{(\alpha)}.$$

Тогда, поскольку $K_2 = K_{21}^{(\alpha)} \cap \ldots \cap K_{2\alpha(2)}^{(\alpha)}$, существует целое число $j, 1 \leq j \leq \alpha$ (2), такое, что $\theta\ [GM\ (J_2,\ G_2,\ K_{2j}^{(\alpha)})] = n - 1$ (см. утверждение 2.25). Кроме того, мы имеем гомоморфизм $GM\ (J_2,\ G_2,\ K_2) \to\to GM\ (J_2, G_2, K_{2j}^{(\alpha)})$. Пусть $N_2 = K_{2j}^{(\alpha)}$. Тогда существует последовательность

$$S' \to\to GM\ (J_2,\ G_2,\ N_2) \to\to RLM\ [GM\ (J_2,\ G_2,\ N_2)] \to\to \ldots,$$

$n - 1$ членов которой представляют собой *GM* полугруппы. Следовательно, выбирая ядро каждого гомоморфизма $S \to\to GM$ в последовательности, мы получим новую последовательность $(J_1,\ G_1,\ N_1 = H_1),\ (J_2,\ G_2,\ N_2),\ (J_3,\ G_3,\ H_3'),\ \ldots,\ (J_n,\ G_n,\ H_n')$ для полугруппы *S'*, удовлетворяющую условиям определения θ_g.

Действуя далее таким же образом, можно получить последовательность длины n, удовлетворяющую условиям 1—3 определения θ_h. Следовательно, $\theta_h^{(\mathscr{E})}(S) \geqslant \theta(S)$. Очевидно, по лемме 2.24, что $\theta_h^{(\mathscr{E})}(S) \leqslant \theta(S)$, поэтом

$$\theta_h^{(\mathscr{E})}(S) = \theta(S)$$

для каждого разложения E полугруппы S.

2.27. Замечание. а) Пусть $N_2 = \ker [(J_1, G_1, N_1), (J_2, G_2)]$. Тогда разложение E для набора $[(J_1, G_1, N_1), (J_2, G_2)]$, задаваемое как $N_2 \xrightarrow{\mathscr{E}} N_2$, называется *тривиальным разложением.*

б) Следующее разложение является очень важным. Пусть задан набор $[(J_1, G_1, N_1), (J_2, G_2)]$, положим

$$N_2 = \ker [(J_1, G_1, N_1), (J_2, G_2)].$$

Обратимся к замечанию 3.32 из микромодуля 9. Нам известно, что G_2 действует на отождествленные L классы из J_1. Пусть R — область определения G_2 и $R = R_1 \cup \ldots \cup R_n$ — разложение в объединение непересекающихся компонент, где (R_i, G_2), $i = 1, \ldots, n$, — транзитивные компоненты группы преобразований (R, G_2). Пусть ядро группы G_2, действующее на R_i есть N_{2i}. Тогда легко видеть, что $N_2 = N_{21} \cap \ldots \cap N_{2n}$. Мы определяем

$$N_2 \to N_{21}, \ldots, N_{2n}$$

как единственное разложение, ассоциированное с $[(J_1, G_1, N_1), (J_2, G_2)]$. Будем называть его разложением транзитивных компонент для полугруппы S.

2.28. Лемма. $\theta_i = 0$.

Доказательство. Из определения θ_i легко вытекает, что если $T \leq S$, то $\theta_i(T) \leqslant \theta_i(S)$. Кроме того, справедливы следующие два утверждения:

а) пусть $S \in \mathscr{S}$. Тогда

$\theta_i(S) = \max \{\theta_i(T) : T \leqslant S$ и N— полугруппа типа $I\}$, где по определению max для пустого множества равен нулю;

б) пусть S — некомбинаторная полугруппа типа I. Тогда

$$\theta_i(S) = \theta_i[IG(S)] + 1.$$

Для доказательства пункта а) положим $\theta_i(S) = n$, пусть $(T_1, \ldots, T_n)$

— максимальная последовательность для полугруппы .*S*, удовлетворяющая условиям пункта и) определения 2.4. Тогда $(T_1, ..., T_n)$ есть последовательность и для T_1 так что

$$\theta_i (T_1) \geqslant n = \theta_i (S).$$

Но $T_1 \leq S$, поэтому $\theta_i (T_1) = \theta_i(S)$.

Перейдем к доказательству пункта б). Пусть $\theta_i(S) = n$ и $(T_1, ..., T_n)$ — максимальная последовательность для полугруппы *S*. Тогда $S \supseteq T_1 \supseteq IG (T_1) \supseteq T_2 \supseteq \ldots$, так что $IG (S) \supseteq IG (T_1)$ и поэтому (S, T_2, T_3, ..., T_n) — другая максимальная последовательность для S, так как S — полугруппа типа *I*. В этом случае очевидно, что $\theta_i [IG (S)] \geq n$— 1, так как она имеет последовательность $(T_2, ..., T_n)$. Однако если $\theta_i [IG (S)] > n - 1$, то $\theta_i (S) > n$. Это противоречие. Следова тельно, $\theta_i [IG (S)] + 1 = \theta_i (S)$.

Допустим теперь, что утверждения а) и б) справедливы также для θ. Мы заявляем тогда, что $\theta = \theta_i$. Докажем это равенство индукцией по $|S|$. Предположим, что $\theta = \theta_i$, для всех полугрупп *S*, таких, что $| S | \leq n$ —1. Пусть S — полугруппа порядка *n*.

Предположим, что S не есть полугруппа типа *I*. Тогда каждая полугруппа из множества $\{T : T \leqslant S$ и *T*—полугруппа типа *I*$\}$ будет собственной подполугруппой в *S*, следовательно, по предположению индукции $\theta_i (T) = \theta (T)$ для каждой такой полугруппы *T*. Но тогда в силу пункта а) $\theta (S) = \theta_i (S)$. Теперь предположим, что *S* — некомбинаторная полугруппа типа *I*. Тогда $IG (S) < S$, поскольку для θ_i справедлив пункт б). Следовательно, $\theta_i [IG (S)] = \theta [IG (S)]$, поэтому согласно пункту б) $\theta_i (S) = \theta (S)$.

Таким образом, достаточно доказать справедливость пунктов а) и б) для θ. Мы сделаем это с помощью следующих двух лемм.

2.29. Лемма. Пусть $S \in \mathscr{S}$. Тогда

$$\theta (S) = \max \{\theta (T) : T \leqslant S \text{ и } T\text{—полугруппа типа } I\},$$

где по определению max пустого множества равен нулю.

Доказательство. Мы построим такую подполугруппу *T* в *S*, что $\theta (T) = \theta (S)$ и *T* имеет тип *I*.

Возьмем разложение транзитивных компонент E для полугруппы S. Пусть $\theta (S) = n$ и $(J_1, G'_1, N'_1), \ldots, (J_n, G'_n, N'_n)$ — максимальная последовательность, удовлетворяющая условиям 1—3 определения $\theta_h^{\mathscr{E}}$. Сперва мы построим новую последовательность $(J_1, G_1, N_1), \ldots, (J_n, G_n, N_n)$, которая также удовлетворяет этим условиям. Пусть $G_n = G'_n$, $N_n = N'_n$ и Y_{n-1} — транзитивная компонента

группы G_n, определяемая N_n. Y_{n-1} есть объединение L классов из J_{n-1}. Пусть G_{n-1} — максимальная подгруппа, принадлежащая классу J_{n-1}, которая R эквивалентна G'_{n-1} и которая содержится в Y_{n-1}. Тогда пусть $(J_{n-1},\ G_{n-1},\ N_{n-1})$ — ядро отображения

$$S \to\to GM\ (J_{n-1}, G'_{n-1},\ N'_{n-1}).$$

Согласно утверждению 3.30 из микромодуля 9, если элемент e_{n-1} есть единица группы G_{n-1}, то $N_{n-1} = N'_{n-1}\ e_{n-1}$. Так как

$$GM\ (J_{n-1},\ G_{n-1},\ \ N_{n-1}) \cong GM\ (J_{n-1},\ \ G'_{n-1},\ \ N'_{n-1}),$$

то N_n есть элемент разложения транзитивных компонент для $[(J_{n-1},\ G_{n-1},\ N_{n-1}),\ (J_n,\ G_n)]$.

Поскольку N'_{n-1} кодирует транзитивную компоненту группы G'_{n-1} в J_{n-1}, согласно утверждению 3.33 из микромодуля 9 $N_{n-1} = N'_{n-1}\ e_{n-1}$ кодирует транзитивную компоненту для G_{n-1} в J_{n-2}. Назовем ее Y_{n-2}. Выберем такую максимальную подгруппу $G_{n-2} \leqslant Y_{n-2}$, что $G_{n-2}\ \mathcal{R}\ G'_{n-2}$. Пусть тогда $(J_{n-2},\ G_{n-2},\ N_{n-2})$ — ядро гомоморфизма $S \to\to GM\ (J_{n-2},\ G'_{n-2},\ N'_{n-2})$. Как и ранее, пусть N_{n-1} есть элемент разложения для $[(J_{n-2},\ G_{n-2},\ N_{n-2}),\ (J_{n-1},\ G_{n-1})]$. Продолжая эти рассуждения, получаем искомую последовательность.

Предположим, что Y_i, i = 1, ..., n— 1, — только что описанные транзитивные компоненты для G_{i+1}. Пусть $y_i \in Y_i$. Тогда $J_i y_i$ есть L класс, содержащий y_i и $Y_i = J_i y_i G_{i+1}$.

Построение подполугруппы T проводится по индукции. Положим $T_1 = G_n \equiv X_n$. Очевидно, что T_1 — полугруппа типа I.

Пусть $X_{n-1} = Y_{n-1}$ и $T_2 = X_n \cup X_{n-1}$. Множество T_2 является полугруппой,так как $G_n J_{n-1} \subseteq J_{n-1}$ и T_2 содержит два F класса X_n и X_{n-1}, причем $X_{n-1} < X_n$. Легко видеть, что

$$\ker\ [(X_{n-1}, G_{n-1},\ N_{n-1}),\ (X_n,\ \hat{G}_n)] \leqslant N_n$$

и последовательность $(X_{n-1},\ G_{n-1}, N_{n-1}),\ (X_n,\ G_n,\ N_n)$ для T_2 удовлетворяет условиям определения θ_q, поэтому $\theta\ (T_2) = 2$.

Теперь для того чтобы доказать, что T_2 — полугруппа типа I, мы должны показать, что $U_1 \preceq T_2^C$, или, что эквивалентно, мы должны показать, что любое отношение конгруэнтности на T_2, которое содержит H классы (т. е. стягивает их в точку), должно стягивать R классы полугруппы T_2 в множества, состоящие из одного элемента. Тогда каждый F класс из $T^C{}_2$ должен иметь вид A^l и $U_1 \preceq T_2^C$. Пусть φ будет

гомоморфизмом, ассоциированным с таким отношением конгруэнтности. Тогда $\varphi(X_n)$ состоит из одного элемента и $\varphi(X_{n-1}) = \varphi(J_{n-1}y_{n-1})\varphi(G_n)$. $J_{n-1}y_{n-1}$ является L классом и поэтому $\varphi(J_{n-1}y_{n-1})$ имеет вид A^l. Но так как $\varphi(G_n)$ состоит из одного элемента, $\varphi(X_{n-1})$ имеет вид A^l. Следовательно, T_2 есть полугруппа типа *I*.

Теперь построим T_3. Пусть $X_{n-2} = J_{n-2}y_{n-2}X_{n-1}$. Так как $G_{n-1} \subseteq X_{n-1}$, имеем $Y_{n-2} \subseteq X_{n-2}$. Положим $T_3 = X_n \cup X_{n-1} \cup X_{n-2}$. Очевидно, что множество T_3—это полугруппа с тремя F классами $X_{n-2} < X_{n-1} < X_n$. По тем же причинам, что и раньше,

$$\ker[(X_{n-2},\ G_{n-2},\ N_{n-2}),\ (X_{n-1},\ G_{n-1})] \leqslant N_{n-1}.$$

Следовательно, для полугруппы T_3 мы имеем последовательность длины три, удовлетворяющую определению θ_q, поэтому $\theta(T_3) = 3$. Как и ранее, пусть φ — любой гомоморфизм полугруппы T_3, стягивающий H классы в точку. Мы должны показать, что

$$\varphi(X_{n-2}) = \varphi(J_{n-2}y_{n-2})\ \varphi(X_{n-1})$$

имеет вид A^l. Так как множество $J_{n-2}y_{n-2}$ является L классом, $\varphi(J_{n-2}y_{n-2})$ имеет такой вид, и мы уже знаем, что $\varphi(X_{n-1})$ также имеет такой вид. Нам известно, что $J_{n-2}y_{n-2}$ содержится в области определения для G_{n-1} и согласно утверждению 3.33 из микромодуля 9 содержится в области определения каждой максимальной подгруппы, которая L эквивалентна G_{n-1}. Это означает, что каждый идемпотент из L класса, содержащего G_{n-1}, фиксирует $J_{n-2}y_{n-2}$. Пусть это множество идемпотентов обозначено $\{e_i\}$. Тогда легко видеть, что $\varphi(X_{n-1}) = \varphi(\{e_i\})$. Следовательно,

$$\varphi(X_{n-2}) = \varphi(J_{n-2}y_{n-2})\varphi(\{e_i\}) = \varphi(J_{n-2}y_{n-2}),$$

так что

$$\varphi(X_{n-2})$$

имеет вид A^l и T_3 есть полугруппа типа *I*.

Продолжая эту процедуру далее, мы построим множество $T \equiv T_n$, которое будет подполугруппой типа *I* полугруппы *S*, такой, что $\theta(T) = n$.

2.30. Лемма. Пусть $S \in \mathscr{S}$ — некомбинаторная полугруппа типа *I*. Тогда

$$\theta(S) = \theta[IG(S)] + 1.$$

Для доказательства этой леммы нам потребуются следующие утверждения.

2.31. Утверждение, а) Пусть $S \in \mathcal{S}$ будет *GGM, RLM* или *LLM* полугруппой. Тогда *IG (S)* будет *GGM, RLM* или *LLM* полугруппой соответственно. Если S есть *GM* полугруппа, то *IG (S)* будет *GM* полугруппой тогда и только тогда, когда *S* не будет группой с нулем.

б) Пусть $S \in \mathcal{S}$ — полугруппа типа *I*. Рассмотрим для S самую длинную последовательность чередующихся *GGM* и *RLM* полугрупп. Эта последовательность оканчивается $\{0\}^I$ или $\{0\}$. Последний член этой последовательности, который $\not\leq \{0\}^I$, есть *GGM* полугруппа, являющаяся или группой, или группой с нулем.

в) Пусть $S \in \mathcal{S}$ и предположим, что *IG (S) = S*. Рассмотрим для *S* последовательность максимальной длины с чередующимися *GGM* и *RLM* полугруппами. Последний член этой последовательности, который $\not\leq \{0\}^I$, есть (комбинаторная) *RLM* полугруппа.

Доказательство, а) Пусть S будет *GGM* полугруппой с отмеченным F классом *J*. Так как S есть объединение групп, $J \bigcap IG(S)$ есть F класс полугруппы *IG (S)*. Назовем его *J'*. Тогда *J'* — единственный минимальный ненулевой F класс в *IG (S)*. Пусть $js_1 \neq js_2 \in IG\ (S)$. Так как *S* является *GGM* полугруппой, существует такой элемент $j \in J$, что $js_1 \neq js_2$. Пусть *e*— единица для *j*. Тогда $jes_1 \neq jes_2$, откуда следует, что $es_1 \neq es_2$. Так как $e \in J'$, мы видим, что *IG (S)* действует точно справа на *J'*. Аналогично *IG (S)* действует точно слева на *J'*. Следовательно, *IG(S)* представляет собой *GGM* полугруппу. Для *RLM* и *LLM* полугрупп доказательства идентичны.

Пусть S — группа с нулем. Тогда $IG\ (S) = \{0\}^I$ и, следовательно, не есть *GM* полугруппа. Наоборот, пусть *S* является *GM* полугруппой. Предположим, что *IG (S)* не есть *GM* полугруппа. Из изложенного ясно, что если S есть *GM* полугруппа, то *IG (S)* будет *GM* полугруппой тогда и только тогда, когда класс *J'* некомбинаторный или $IG\ (S) = \{0\}$.

Следовательно, *J'* —- комбинаторный класс. Это значит, что *J' =E (J)* = {единицы максимальных подгрупп класса *J*}. Таким образом, существует рисовское матричное представление $\mathcal{M}\ (G;\ A,\ B;\ C)$ для *J* с *C(b, a)*=1 для всех элементов $(b,\ a) \in B \times A$. Но так как *S* есть *GM* полугруппа, структурная матрица *C* не может иметь пропорциональных строк или столбцов (см. утверждение 2.22 из микромодуля 9), так что *J=G*. Но согласно представлению Щютценберже для *GM* полугрупп имеем *S = G* или G^0 (см. пункт б) леммы 2.17 из микромодуля 9). Так как $IG\ (S) \neq \{0\}$, то S = G^0.

б) *RLM* полугруппа, идущая вслед за последней некомбинаторной *GGM* полугруппой, должна быть комбинаторной. Обозначим ее

символом T. Тогда $S \twoheadrightarrow S^C \twoheadrightarrow T$. Если $T \not\leq \{0\}^I$, то $U_1 \mid T \mid S^C$. Это противоречие. Следовательно, последний член $\not\leq \{0\}^I$ есть *GGM* полугруппа, а следовательно, и *GM* полугруппа. Обозначим ее символом S_1. Пусть J — отмеченный F класс полугруппы S_1. Мы утверждаем, что J — простой слева. Если же это не так, то $U_1 \leqslant RLM_J(S_1)$. Это противоречие. Но представление Щютценберже для *UM* полугрупп показывает, что если S_1— простая слева полугруппа, то $S=G$ или G^0.

в) Предположим, что утверждение этого пункта неверно. Тогда из доказательства пункта б) следует, что последний член $T = G$ или G^0. Но если $IG(S) = S$ и $S \twoheadrightarrow T$, то $IG(T) = T$. Так как $IG(G) = \{0\}$ и $IG(G^0) = \{0\}^I$, мы получаем противоречие. Тем самым утверждение полностью доказано.

Доказательство леммы 2.30. Пусть $\theta(s) = n$. Тогда для S существует *GGM — RLM* последовательность:

$$S \twoheadrightarrow GGM_1 \twoheadrightarrow RLM_1 \twoheadrightarrow \ldots \twoheadrightarrow GGM_n \twoheadrightarrow \{0\}^I \text{ или } \{0\}, \quad (2.8)$$

где $GGM_n = G$ или $GGM_n = G^0$ (согласно пункту б) утверждения 2.31). Если $\varphi : S \twoheadrightarrow T$, то $\varphi[IG(S)] = IG(T)$. Следовательно, ограничение последовательности (8) приводит к

$$IG(S) \twoheadrightarrow IG(GGM_1) \twoheadrightarrow \ldots \twoheadrightarrow IG(GGM_{n-1}) \twoheadrightarrow IG(RLM_{n-1}) \twoheadrightarrow \{0\}^I \text{ или } \{0\}$$

и каждый член $IG(GGM_i)$, $i = 1, \ldots, n$—1, является *GM* полугруппой (см. пункт а) утверждения 2.31). Следовательно,

$$\theta[IG(S)] \geqslant \theta(S) - 1$$

Предположим теперь, что $\theta[IG(S)] = n$. Тогда для $IG(S)$ существует последовательность с n *GGM* полугруппами, оканчивающаяся членом $RLM_n \leq \{0\}^I$ (см. пункт в) утвеожления 2.31). В силу утверждения 2.23 $U_1 \mid [IG(S)]_{(n)}^{(\nu+\mathscr{J})} \ldots \mathscr{L}$.

Но

$$[IG(S)]_{(n)}^{(\nu+\mathscr{J})} \ldots \mathscr{L} \mid S_{(n)}^{(\nu+\mathscr{J})} \ldots \mathscr{L},$$

из этого следует существование для полугруппы S последовательности, n-й *RLM* член которой $\not\leq \{0\}^I$. Это противоречие, так как $\theta(S) = n$ и все максимальные последовательности для S должны оканчиваться *GGM* полугруппой. Следовательно,

$$\theta[IG(S)] \neq n \text{ и } \theta(S) = \theta[IG(S)] + 1.$$

2.32. Лемма. $\theta_j = \theta$.

Доказательство. Пусть $X \subseteq \mathscr{C}(S)$. Положим $p(X) = \{\chi_i : \text{су-}$

ществует элемент $x \in X$, такой, что $x = \sum_{i=1}^{n} a_i \chi_j$, где $a_i \neq 0$}. Пусть отображение $H(X) : S \longrightarrow\!\!\!\!\rightarrow T = H(X)(S)$ определяется соотношением

$$H(X) = \Pi \{\mathcal{R}_i : \chi_i \in p(X)\}.$$

Положим $RLM(X) = \Pi\{RLM\,\mathcal{R}_j : \chi_j \in p(X)\}$.

Теперь $RLM\mathcal{R}_j(S) = \mathcal{R}_j(S)^{\mathscr{L}} = \mathcal{R}_j(S)^{RLM}$, и, следовательно, по предложению 3.17 из гл. микромодуля 9.

$$\varphi H(X) = RLM(X), \tag{2.9}$$

где $\varphi : H(X)(S) \rightarrow\!\!\!\!\rightarrow [H(X)(S)]^{\mathscr{L}}$.

Роудзом было доказано, что

$$H[\mathscr{C}(S)](S) = S^{\nu+\mathscr{J}}. \tag{2.10}$$

Пусть M— матричное представление полугруппы S (не обязательно вполне приводимое). Роудз доказал, что $H[\chi(\mathcal{R})](S) = [\mathcal{R}(S)]^{\nu+\mathscr{J}}$.

Тогда из предложения 3.17 в микромодуле 9 следует, что если {R}— совокупность матричных представлений полугруппы S и $\chi\{\mathcal{R}\} = \{\chi(\mathcal{R})\}$, то

$$H(\chi\{\mathcal{R}\})(S) = (\Pi\{\mathcal{R}\}](S))^{\nu+\mathscr{J}}. \tag{2.11}$$

Роудзом получен также результат: $\mathscr{C}(S)^A$ является линейной оболочкой для $p[\mathscr{C}(S)^A]$ и

$$H[\mathscr{C}(S)^A](S) = S^{\mathscr{J}}. \tag{12}$$

Кроме того, если $X \subseteq \mathscr{C}(S)$, так что $X \supseteq \mathscr{C}(S)^A$, то $H(X)$ есть F гомоморфизм и

$H(X) : S \longrightarrow\!\!\!\!\rightarrow S^{\mathscr{J}}$ тогда и только тогда, когда $X = \mathscr{C}(S)^A$. (2.13)

Из определения отображения $A : \mathscr{C}(S) \rightarrow \mathscr{C}(S)$ следует, что для $X \subseteq \mathscr{C}(S)$

$$p[A(X)] = p(\chi[RLM(X)]). \tag{2.14}$$

Докажем теперь, что $\theta_j = \theta_e$. В силу соотношения (10) $H[\mathscr{C}[(S)]$: $S \longrightarrow\!\!\!\!\rightarrow S^{\nu+\mathscr{J}}$ и в силу соотношения (2.9)

$$RLM[\mathscr{C}(S)] = S \longrightarrow\!\!\!\!\rightarrow S^{\nu+\mathscr{J}} \longrightarrow\!\!\!\!\rightarrow S^{(\nu+\mathscr{J})\mathscr{L}}.$$

Кроме того, согласно равенству (2.11)

$$H(\chi RLM[\mathscr{C}(S)]) : S \rightarrow\!\!\!\!\rightarrow S^{\nu+\mathscr{J}} \rightarrow\!\!\!\!\rightarrow S^{(\nu+\mathscr{J})\mathscr{L}} \rightarrow\!\!\!\!\rightarrow S^{(\nu+\mathscr{J})\mathscr{L}(\nu+\mathscr{J})}.$$

Но из (2.14) получаем $p(A[\mathscr{C}(X)]) = p(\chi RLM[\mathscr{C}(S)])$ и, следовательно,

$$H(\chi RLM[\mathscr{C}(S)]) = H(A[\mathscr{C}(S)]) \quad \text{или} \quad H(A[\mathscr{C}(S)]) : S \twoheadrightarrow S^{\nu+\mathscr{J}} \twoheadrightarrow S^{(\nu+\mathscr{J})\mathscr{L}} \twoheadrightarrow S^{(\nu+\mathscr{J})\mathscr{L}(\nu+\mathscr{J})}.$$

Продолжая теперь действовать таким же образом для вычисления $H(A^k[\mathscr{C}(S)])$ и применяя формулы (2.12)—(2. 14), мы находим, что первое целое число n, для которого справедливо соотношение $H(A^n[\mathscr{C}(S)])(S) = S^{\mathscr{J}}$ (т. е. $\theta_c(S) = n$), равно первому целому числу n, для которого справедливо включение $A^n[\mathscr{C}(S)] \subseteq \mathscr{C}(S)^A$. Но это последнее число равно индексу B. Следовательно, $\theta_j(S) = \theta_c(S)$. Это доказывает лемму 2.32 и завершает доказательство основной теоремы 2.5.

3. Следствие теоремы

Мы обозначим единственную функцию G сложности для полугрупп, являющихся объединением групп, относительно GM полугрупп как $\#_G : \mathscr{S} \to N$. В этом пункте снова рассматриваются только полугруппы, являющиеся объединением групп, если противное не оговорено.

3.1. Следствие (непрерывность сложности по отношению к гомоморфизмам).

а) Если $\varphi : S \underset{\nu}{\twoheadrightarrow} T$, то $\#_G(S) = \#_G(T)$.

б) Если $\varphi : S \underset{\mathscr{L}}{\twoheadrightarrow} T$, то $\#_G(T) \leqslant \#_G(S) \leqslant \#_G(T) + 1$.

в) Пусть $\varphi : S \twoheadrightarrow T$ — некоторый эпиморфизм, $\#_G(S) = n$ и $\#_G(T) = k$. Тогда существуют такие эпиморфизмы $S = S_n \twoheadrightarrow S_{n-1} \twoheadrightarrow \cdots \twoheadrightarrow S_k = T$, что φ есть их композиция и $\#_G(S_j) = j$

для $j = k,\ldots,n$.

Доказательство, а) Если $S \underset{\nu}{\twoheadrightarrow} T$, то $S^\nu = T^\nu$. Следовательно последовательность (д) для T идентична после первого γ отображения последовательности для S. Следовательно, $\theta_e(S) = \theta_e(T)$.

б) Пусть

$$S \twoheadrightarrow GM_1 \twoheadrightarrow RLM_1 \twoheadrightarrow GM_2 \twoheadrightarrow \dots$$

есть последовательность максимальной длины этого типа для полугруппы *S*. Теперь поскольку $S \xrightarrow[\mathscr{L}]{} T$, имеем

$$T \twoheadrightarrow T^{\mathscr{L}} = S^{\mathscr{L}} = S^{RLM} \twoheadrightarrow RLM_1,$$

так что

$$T \twoheadrightarrow RLM_1 \twoheadrightarrow GM_2 \twoheadrightarrow \cdots$$

есть последовательность типа (e) для *T*. Тогда $\# G(T) = \theta_1(T) \geqslant \geqslant \# G(S) - 1$. С другой стороны, $\# G(T) \leqslant \# G(S)$.

в) Так как эпиморфизм $\varphi : S \twoheadrightarrow T$ можно разложить в последовательность чередующихся *y* гомоморфизмов и *X* гомоморфизмов (см. теорему 1.14 в микромодуле 9), требуемый результат следует из пунктов а) и б).

3.2. Следствие (непрерывность сложности по отношению к подполугруппам).

а) Если *T* — максимальная собственная подполугруппа полугруппы *S*, то $\# G(T) \leqslant \# G(S) \leqslant \# G(T) + 1$.

б) Пусть $T \leqslant S$, где $k = \# G(T) \leqslant \# G(S) = n$;

тогда существуют подполугруппы

$$T = S_k \leqslant S_{k+1} \leqslant \dots \leqslant S_n = S,$$

такие, что $\# G(S_j) = j$ для $j = k, \dots, n$.

Доказательство, а) Рассмотрим для полугруппы S последовательность максимальной длины вида

$$S \twoheadrightarrow GM_1 \twoheadrightarrow RLM_1 \twoheadrightarrow GM_2 \twoheadrightarrow \cdots \twoheadrightarrow \{0\}.$$

Так как $RLM(GM_k) = GM_k^{RLM} \twoheadrightarrow RLM_k$, заменим каждую полугруппу RLM_k на $RLM(GM_k)$. Новая последовательность будет иметь ту же длину, т. е. существуют $\# G(S)$ ненулевых *GM* полугрупп в последовательности. Рассмотрим ограничение на *T* и возьмем последовательные образы, тогда получим

$$\begin{array}{ccccccccc} S & \twoheadrightarrow & GM_1 & \twoheadrightarrow & RLM(GM_1) & \twoheadrightarrow & GM_2 & \twoheadrightarrow \cdots \twoheadrightarrow & \{0\}, \\ \cup & & \cup & & \cup & & \cup & & \end{array} \qquad (1)$$

$$T \twoheadrightarrow T_{11} \twoheadrightarrow T_{12} \twoheadrightarrow T_{21} \twoheadrightarrow \cdots \twoheadrightarrow \{0\}. \qquad (2)$$

Так как *T*—максимальная собственная подполугруппа полугруппы *S*, T_{k1} и T_{k2} будут максимальными подполугруппами полугрупп GM_k и

RLM (GM_k) соответственно. По предложению 3.3 из микромодуля 8 максимальная подполугруппа содержит все, кроме, быть может, одного, F классы полугруппы. Пусть I_{k1} и I_{k2} — отмеченные F классы (по отношению к *GM* и *RLM* полугруппам) полугрупп GM_k и *RLM* (GM_k) соответственно.

Если I_{11} содержится в T_{11}, то он представляет собой единственный минимальный ненулевой F класс полугруппы T_{11} и T_{11} действует на него слева и справа. Другими словами, T_{11} есть *GM* полугруппа $\neq\{0\}$. Так как I_{12} является образом I_{11}, I_{12} содержится в T_{12} и T_{12} будет *RLM* полугруппой. Продолжим эти рассуждения. Если $I_{k1} \subseteq T_{k1}$ для каждого *k*, то последовательность (2) имеет такое же число ненулевых *GM* полугрупп, как и последовательность (1). Так как (2) — это последовательность вида (е), имеем $\#_G(T) = \#_G(S)$. Предположим тогда, что

$$I_{j1} \subsetneq T_{j1}$$

для некоторого j, $1 \leqslant j \leqslant \#_G(S)$. Выберем такое наименьшее *j*. Тогда $GM_j — I_{j1} \subseteq T_{j1}$. Пусть $\varphi\colon GM_j \twoheadrightarrow GM_{j+1}$. Тогда $GM_{j+1} — \varphi(I_{j1}) \subseteq T_{(j+1)1}$. Но мы утверждаем, что $\varphi(I_{j1})=\{0\}$. Действительно, его образ в *RLM* (*GMj*) является комбинаторным и 0-минимальным. Несмотря на это, $I_{(j+1)1}$ — некомбинаторный, поэтому $\varphi(I_{j1})=\{0\}$. Следовательно, $T_{(j+1)1} = GM_{j+1}$ или $GM_{j+1} — \{0\}$. Таким образом, остаток ряда (2) идентичен последовательности (1), за исключением, быть может, нуля. Поэтому последовательность (2) может быть записана в виде (е) как

$$T \twoheadrightarrow \cdots \twoheadrightarrow T_{(j-1)2} \twoheadrightarrow T_{(j+1)1} \twoheadrightarrow \cdots \twoheadrightarrow \{0\}.$$

Таким образом, в этом случае $\#_G(T) \geqslant \#_G(S) — 1$.

б) Этот пункт вытекает из справедливости пункта а).

3.3. Следствие (непрерывность сложности относительно делимости).

Пусть *T\S*, где $k = \#_G(T) \leqslant \#_G(S) = n$. Тогда существует последовательность полугрупп $T = T_k \mid T_{k+1} \mid \ldots \mid T_n = S$, таких, что $\#_G(T_j) = j$ для $j = k, \ldots, n$.

Доказательство. Результат вытекает из следствий 3.1 и 3.2.

3.4 Следствие. Аксиомы 1 и 2 определения 1.2 эквивалентны аксиоме 1 и следующей аксиоме.

Аксиома 2'. Если $S \xrightarrow{\gamma} T$, то $\#_G(S) = \#_G(T)$, где *S* — про-

извольная конечная группа.

Доказательство. Очевидно, что из аксиом 1 и 2' следуют аксиомы 1 и 2. Докажем обратное. Пусть у нас имеются аксиомы 1 и 2. Пусть $\varphi : S \longrightarrow\!\!\!\!\rightarrow T$ будет у гомоморфизмом, положим $\varphi = \varphi_n \varphi_{n-1} \cdots \varphi_1$, где φ_i, $i = 1, ..., n$, есть *MPE*. Очевидно, каждое отображение φ_i есть γ гомоморфизм и поэтому достаточно доказать, что

$$\#_G(S) = \#_G[\varphi(S)],$$

где φ есть γ *MPE*.

По лемме 1.18 из микромодуля 9 существует F класс J полугруппы S, такой, что φ взаимно однозначно на $S - J$, φ разделяет $(J \cup F(J))$ и его дополнение в S. Если J регулярен, то φ является $\gamma(\mathcal{H})$ гомоморфизмом на J.

Если J нулевой, положим $\psi : S \longrightarrow\!\!\!\!\rightarrow S/F(J)$. Тогда отображение $(\varphi \times \psi)\,\Delta$ будет взаимно однозначным на S.

Если класс J регулярен, то определим отображение $\psi : S \dashrightarrow \dashrightarrow [S/F(J)]/\equiv$, где $\equiv$ есть отношение конгруэнтности на $S/F(J)$, задаваемое как $s_1 \equiv s_2$, тогда и только тогда, когда $s_1 = s_2$, или если $s_1, s_2 \in J$, то $s_1 H s_2$. Тогда ψ будет H гомоморфизмом на $S/F(J)$. Легко проверить, что в этом случае $(\varphi \times \psi)\,\Delta$ будет взаимно однозначным на S.

Мы остановимся здесь, чтобы заметить, что из одной аксиомы 1, когда $\varphi : S \longrightarrow\!\!\!\!\rightarrow T$, вытекает неравенство

$$\#_G(S) \geqslant \#_G(T).$$

Действительно, отображение $(\varphi \times Id)\,\Delta$ взаимнооднозначно на S и поэтому по аксиоме 1 $\#_G(S) = \max[\#_G(S), \#_G(T)]$. Следовательно,

$$\#_G(S) \geqslant \#_G(T).$$

Теперь вернемся к доказательству. Так как отображение $(\psi\times\varphi)\Delta$ взаимно однозначно на S, по аксиоме 1 имеем

$$\#_G(S) = \max(\#_G[\varphi(S)], \#_G[\psi(S)]). \qquad (3)$$

Отображение φ взаимно однозначно на $S - J$, поэтому существует отображение $\varphi(S) \longrightarrow\!\!\!\!\rightarrow S/[J \cup F(J)]$. Кроме того $S/[J \cup F(J)] \longrightarrow\!\!\!\!\rightarrow \psi(S)/\psi[J \cup F(J)]$, поэтому

$$\varphi(S) \longrightarrow\!\!\!\!\rightarrow \psi(S)/\psi[J \cup F(J)].$$

Тогда

$$\#_G[\varphi(S)] \geqslant \#_G(\psi(S)/\psi[J \cup F(J)]).$$

Но $\psi\,[J \cup F\,(J)]$— комби наторный идеал полугруппы ψ(S), поэтому $\#_G\,[\psi\,(S)] = \#_G\,(\psi\,(S)/\psi\,|J \cup F\,(J)])$ по аксиоме 2. Следовательно, $\#_G\,|\varphi\,(S)| \geqslant \#_G\,|\psi\,(S)|$ и из следствия 3.1 вытекает, что $\#_G\,(S) = \#_G\,[\varphi\,(S)]$.

Микромодуль 10.
Идивидуальные тестовые задачи

1. Покажите, что полугруппа $F_R\,(X_3)$ *никогда* не делит полугруппу $C\mathrm{w}\,[F_R\,(X_3)/K]$, где K — комбинаторное ядро полугруппы $F_R\,(X_3)$, состоящеена грех постоянных функций, а С — любая комбинаторная полугруппа.

[Указание. Докажите сначала, что $F_R\,(X_3)$ — регулярная полугруппа с тремя F классами

$$J_3 = SYM_R\,(X_3),\ J_2 \cong \mathscr{M}^0\,(Z_2;\ X_3,\ X_3;\ C) - \{0\},$$

где $Z_2 = \{1, —1\}$ есть циклическая группа второго порядка и где

$$C = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

и $J_1 = K \cong X_3^t$. Затем допустим, что

$$F_R\,(X_3) \leftarrow\!\!\leftarrow T \leqslant C' \times_Y [F_R\,(X_3)/K],$$

где С' — комбинаторная полугруппа. Пусть $K\,(T)$ — ядро полугруппы T и p_1 — гомоморфизм проекции на полупрямое произведение. Рассмотрим $p_1\,[K\,(\mathrm{T})]$.

Тогда

1) $p_1\,[K\,(T)] = \{0\}$; 2) $p_1\,[K\,(T)] \leqslant J_2$ или 3) $p_1\,[K\,(T)] = \{0\}$.

Если имеет место случай 1, то

$$F_R\,(X_3)\,|\,C' \times_Y J_3,$$

откуда следует, что

$$IG\,[F_R\,(X_3)]\,|\,IG\,[C' \times_Y J_3].$$

Но $IG[C' \times {}_Y J_3]$ будет комбинаторной, так как J_3 — группа, поэтому

$$IG[F_R(X_3)]$$

будет комбинаторной. Это противоречие. Если справедлив случай 3, то отображение $(t, x) \to Y(0)t$ будет гомоморфизмом полугруппы T на $T' \leq C'$, который разделяет L классы ядра $K(T)$. Следовательно, $F_R(X_3) \mid T' \mid C'$. Это противоречие. В случае 2 предлагаем читателю, используя структуру матрицы C, доказать, что $p_1[K(T)]$ является подполугруппой в $Z_2 \times \{1, 2\}^r$ или $Z_2 \times \{1, 2\}^l$. Следовательно, заключаем, что $p_1(T)$ представляет собой подполугруппу полугруппы, которая есть объединение групп, с двумя F классами D_1 и D_2, где $D_2 < J_3$ и $D_1 = p_1[K(T)]$. Затем покажите, что $p_1(T) \mid C_1 w G_1$, где C_1 — комбинаторная полугруппа, а G_1 — группа. Таким образом, полугруппа $F_R(X_3) \mid C_2 w C_1 w G_1$, поэтому $IG(F_R(X_3))$ является комбинаторной. Это противоречие.]

2. Пусть Z^+ — полугруппа целых положительных чисел по сложению. Покажите, что существует такой гомоморфизм $Y : Z+ \to \mathrm{End}_L(Z+)$, что любая конечно порожденная полугруппа делит $Z+ \times {}_Y Z+$.

[*Указание.* Покажите сначала, что полугруппа $\sum\{0, 1, ..., n\}$ изоморфна подполугруппе $\sum\{0, 1\}$ для всех $n = 1,2.....$так что каждая конечно порожденная полугруппа делит $\sum\{0, 1\}$. Определите Y, положив $Y(k)(z) = 2^k \cdot z$, проверьте, что отображение $t \to [n_2(t), n_1(t)] \in Z+ \times {}_Y Z+$ есть заимно однозначный гомоморфизм, где $t \in \sum\{0, 1\}$, $t = (t_1, ..., t_k)$, $n_1(t) = k$ и $n_2(t)$ — целые положительные числа с двоичным разложением $t_k, ... t_1$.]

Микромодуль 11.
Топологические полугруппы

3.12. Начальные определения

Начало изучения топологических полугрупп следует отнести к 1950г. Первые работы по этому вопросу принадлежат профессору Л. Д. Уоллесу, который внес большой вклад в развитие теории

топологических полугрупп и очертил основные направления дальнейших исследований.

Цель этого микромодуля заключается в том, чтобы познакомить читателя с некоторыми результатами и техническими средствами теории топологических полугрупп. Мы не ставили перед собой задачи дать детальный или даже подробный обзор состояния этой теории по современной литературе.

Мы включаем в изложение, возможно в несколько укороченном варианте, те доказательства, технический аппарат которых представляет практический интерес.

Много теорем, которые относятся к полугруппам, основываются на ***свойствах компактности, локальной компактности или дискретности***.

Отметим, что всякая алгебраическая полугруппа оказывается топологической, если ввести на ней дискретную топологию (любое множество открыто). В этой топологии все функции непрерывные. В частности, конечная полугруппа будет компактной топологической полугруппой.

Поскольку при дальнейшем изложении используются некоторые факты из топологии, мы будем применять обозначение A^*, $A\backslash B$ и $\square$ для замыкания множества, разности двух множеств и пустого множества соответственно. Элемент x и точечное множество $\{x\}$ мы не будем различать. Терминам топологии отдается преимущество перед терминами алгебры там, где из контекста не возникает недоразумений. Все рассматриваемые в этом микромодуле полугруппы будут топологическими. Многие ранее полученные результаты для конечных полугрупп распространяются на топологические полугруппы.

Когда мы говорим, что множество *замкнуто,* это значит, что оно замкнуто в топологическом пространстве и это не означает, что оно замкнуто относительно полугрупповой операции (т.е. есть подполугруппой).

Определение. *Полугруппой* называется непустое, хаусдорфовое топологическое пространство S с заданным на нем непрерывным ассоциативным законом умножения

$$S \times S > S,$$

который обычно не обозначается никаким символом и записывается просто с помощью последовательного размещения элементов. S называется *пространством полугруппы,* и если из контекста не следует двусмысленности, связанной с законом умножения, мы говорим, что S является полугруппой.

Для подмножеств A, $B \subset S$ AB обозначает множество $\{ab | a \in A, b \in B\}$ и A^2 обозначает множество $\{aa' | a, a' \in A\}$. Два факта из общей топологии будут очень важны для нас в дальнейшем. Первый из них заключается в том, что произведение компактных пространств компактно, а второй — в том, что образ при непрерывном отображении компактного пространства тоже будет компактным. Так как A и B — компактные подмножества полугруппы S, то AB — также компактное подмножество, и, в частности, если множество A компактно, то для любого элемента $x \in S$ xA и Ax тоже компактны.

В топологии *гомеоморфизмом* называется взаимно однозначное сюръективное непрерывное отображение, обратное к которому также неспрерывно. Для полугрупп *изеоморфизмом* будем называть отображение, что является гомеоморфизмом пространств и изоморфизмом соответствующих алгебраических полугрупп.

Минимальный идеал полугруппы S, как правило, обозначается символом $K(S)$. Для компактной полугруппы S $K(S)$ существует и его построение полностью известно. На языке алгебраических полугрупп $K(S)$ есть полностью простым. В частности, $K(S)$ компактен и представляет собой дизъюнктивное объединение семейства компактных групп (см. теорему 8).

Множество всех идемпотентов полугруппы S, как правило, обозначается символом $E(S)$. *Подгруппой* полугруппы S называется подмножество G в S, которое является группой (в алгебраическом смысле) с операцией, унаследованной от полугруппы S. Закон умножения в подгруппе G, очевидно, будет непрерывным, и если G локально компактна, то операция взятия обратного элемента также будет непрерывной, поэтому G окажется топологической группой. Для каждого идемпотента $e \in E(S)$ существует максимальная группа в S, единицей которой является элемент e (см. лемму 1).

Бингом называется компактная связная полугруппа, *кланом* называется компактная связная полугруппа (бинг) с единицей. На рис. 3.3 показанные некоторые простые примеры полугрупп с обычным для каждого примера законом умножения: действительный отрезок [0, 1], единичный круг D в комплексной плоскости и для фиксированного $n \geq 1$ выпуклое подмножество в D, содержащее корни n-й степени из единицы $\{\alpha_1, ..., \alpha_m\}$ (все это изображено для случая $n = 3$).

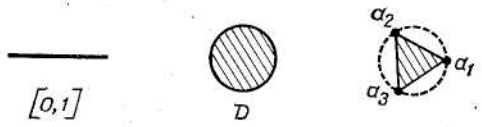


Рис. 3.3.

Заметим, что каждая из этих полугрупп действительно представляет собой клан.

3.13. Дуги и полугруппы

Нитью называется полугруппа, пространство которой является *дугой,* т.е. хаусдорфовым множеством мощности континуум, каждая точка которого разрезает само множество, а две точки, которые не разрезают множество, концевые. (Замкнутый действительный интервал [*a, b*] с $a < b$ представляет собой дугу с концевыми точками *a* и *b.) Стандартной нитью* или *I полугруппой* называется нить, одна концевая точка которой является нулем (т.е. нулевым элементом полугруппы), а другая — единицей.

Строение нитей интересно само по себе, а также потому, что многие из известных сейчас нитей (особенно это относится к *I* полугруппам) лежат в бóльших полугруппах. Фосе доказад, что *I* полугруппа, которая не имеет внутренних (не концевых) идемпотентов, должна быть гомеоморфна действительному интервалу [0, 1]. (Однако в общем случае *I* полугруппа не обязательно должна быть метрической; она может быть «слишком длинной».) Фосе получил дальнейшие результаты в направлении характеристики *I* полугрупп, эта работа была завершена Мостертом и Шайлдзом, когда они воспользовались результатами своего исследования некоторых кланов на компактных поверхностях с границей (см. теорему 5). Клиффорд получил более общие результаты о нитях, которые полностью описывают построение нитей с идемпотентными концами, а Коэн и Вэйд охарактеризовали метризуемые нити с нулем и единицей. Одним из наиболее важных результатов относительно *I* полугрупп является то, что все они абелевы. Мы опишем их строение, но сперва необходимо дать некоторые определения.

Определение 1. 1) *Единичной нитью* называется полугруппа, изеоморфная полугруппе [0, 1] с обычным законом умножения.

2) *Ниль-нитью* называется полугруппа, которая изеоморфна полугруппе [1/2,1] с законом умножения, определенным соотношением $xy = \max\{1/2,$ обычное произведение элементов *x* и *y*$\}$ [см. пример 2 (1)].

3) *Мин-нитью* называется дуга, для которой задано упорядочение разделяющих точек, а закон умножения определяется соотношением

$xy=\min\{x,y\}$. (На дуге A упорядочение разделяющих точек определяется следующим образом: выбирается одна концевая точка a и для $x, y \in A$ кладется $x \le y$ тогда и только тогда, когда $x = a$ или $x = y$, или x разделяет точки a и y в A. Доказано, что этот порядок линеен.)

Теорема 1. Пусть S является I полугруппой. Зададим упорядочение розбивающих точек, выбрав в качестве минимального элемента нуль. Тогда $E(S)$ замкнуто и для $x, y \in E(S)$ $xy = \min\{x, y\}$. Дополнение $E(S)$ будет объединением не имеющих общих элементов открытых интервалов и если P — один из них, то P^* будет подполугруппой в S, являющейся единичной нитью или ниль-нитью. И наконец, если $x \in P$ и $y \notin P$, то $xy = \min\{x, y\}$. В частности, S — абелева полугруппа.

Не все нити являются абелевыми полугруппами, неабелевыми могут быть даже те из них, концевые точки которых идемпотентны. Это показывает следующий пример.

Пример 1. Пусть S — подмножество в плоскости, определяемое соотношением

$$S = ([0, 1] \times 0) \cup (0 \times [0, 1])$$ (см. рис. 3.4).

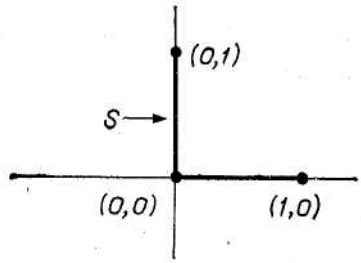


Рис.3.4

Определим умножение в S, полагая

$$(x, y)(x', y') = (xx', xy' + y).$$

Мы получили неабелеву нить с единицей, но без нуля. Однако каждый элемент p, принадлежащий вертикальному сегменту, *будет левым нулем,* т.е. $pS=p$. Заметим, что горизонтальный сегмент является единичной нитью.

В соответствии с теоремой 1 нить только с двумя идемпотентами — концевыми точками (т.е. I полугруппа, которая не имеет внутренних идемпотентов), является или единичной нитью или ниль-нитью. Уоллес изучал клетки более высокой размерности, однако для этого случая практически ничего не известно.

Рассмотрим, какова структура полугруппы, если ее пространство есть произвольная n клетка для $n>1$ и если потребовать, чтобы

множество идемпотентов совпадало с границей? В частности, обладает ли 2-клетка строением соответствующей полугруппы?

В примере 3(3) будет представлена полугруппа, пространство которой есть 2-клетка и идемпотентами которой являются граничные точки и еще одна внутренняя точка. Однако нет стандартной процедуры, которая бы исключила внутренний идемпотент из этой полугруппы. В общем случае определить построение полугруппы с необходимыми геометрическими свойствами на пространстве S очень трудно, как правило, несколько легче подобрать непрерывную функцию $S \times S \to S$ с этими свойствами, но получить еще при этом закон ассоциативности тяжело. Поэтому новые примеры обычно строятся с помощью уже известных полугрупп; приемы построения этих примеров описаны в разделе 3.13.

Заодно упомянем, что из теоремы Коэна и Круля следует, что нетривиальный гомоморфизм из действительной I полугруппы сохраняет размерность, хотя в общем случае мало что можно сказать об изменении размерности при гомоморфизмах полугрупп. Существуют примеры гомоморфизмов из компактных полугрупп на полугруппы более высокой размерности. Это, конечно, невозможно для групп (как следует из результатов Монтгомери и Зиппина).

Под размерностью мы понимаем индуктивную или топологическую размерность.

Определение 2. *Однопараметрической полугруппой в S* называется функция σ: $[0, 1] \to S$, которая непрерывна, взаимно однозначна и удовлетворяет соотношению $\sigma(x + y) = \sigma(x)\,\sigma(y)$ всякий раз, когда $x, y, x + y \in [0,1]$. $\sigma([0,1])$ есть дуга как подпространство в S, поскольку $[0,1]$ компактен, S хаусдорфово, а σ непрерывна и взаимно однозначна, откуда следует, что σ-гомеоморфизм $[0, 1]$ в S. Как правило, мы будем называть *образ отрезка* $[0,1]$ относительно отображения σ *однопараметрической полугруппой*. Отметим, что этот образ не обязан быть подполугруппой в S, так как отрезок $[0,1]$ не замкнут относительно сложения. В качестве примера однопараметрической полугруппы, которая не является подполугруппой, возьмем интервал $[1/2, 1]$ действительной оси, где S есть единичный комплексный круг с обычным комплексным умножением (см. рис. 3.5).

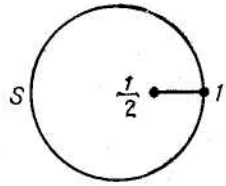


Рис. 3.5

Лемма 1. Если $e \in E(S)$, то существует максимальная подгруппа $H(e)$ полугруппы S, содержащая e, и $H(e)=\{x \in eSe | xx'=e=x'x$ для некоторого $x' \in Se\} = \{x \in S | x \square x = e \cup eS$ и $x \cup Sx = e \cup Se\}$.

В 1960 г. Мостерт и Шайлдз опубликовали следующую теорему, которая все еще является основным инструментом для изучения полугрупп. Первый вариант теоремы, в котором требуется, чтобы $H(1)$ была группой Ли, появился в 1957 г. Скажем, что дуга A в S *выходит из идемпотента* $e \in S$ тогда и только тогда, когда $A \cap H(e) = e$. Пример однопараметрической полугруппы, данный в определении 2 служит также примером дуги, которая выходит из идемпотента.

Теорема 2. Пусть S — локально компактная полугруппа с единицей 1. Предположим, что существует компактная подгруппа G в $H(1)$, открытая в $H(1)$, но не являющаяся открытой в S. Предположим, что существует окрестность 1, не содержащая других идемпотентов. Тогда S содержит однопараметрическую полугруппу, которая выходит из 1.

Несмотря на то, что с момента появления первого варианта этой теоремы прошло десятки лет, доказательство ее все еще встречает трудности. Мостерт и Шайлдз отмечают, что если им не нужны выздодящие однопараметрические полугруппы, то они могут использовать теорему Глисона, гарантирущую существование однопараметрических групп в локально компактных группах и которая доуазывается легче. В результате теоремы Мостерта и Шайлдза естественно возникает вопрос, существует ли дуга или однопараметрическая полугруппа, которая выходит из неизолированного идемпотента, и является ли однопараметрическая полугруппа в S подмножеством нити, которая принадлежит S. Как показывают примеры, приведенные далее, ответы на эти вопросы отрицательны, хотя справедливо, что бинг должен вести себя достаточно хорошо около идемпотента вне $K(S)$, так как Кох доказал, что каждая окрестность такого идемпотента содержит дугу. Однако эти

дуги могут не содержать идемпотент, они не обязаны быть подполугруппами в S или даже однопараметрическими полугруппами.

Определение 3. *Произведением полугрупп* S и W называется декартово произведение пространств $S \times W$ с покоординатным законом умножения, т.е. $(x, y)(x^1, y') = (xx^1, yy')$.

Примеры 2. Пусть I=[0,1] — действительный отрезок с обычным умножением, C — единичная окружнсть, а D — единичный круг в комплексной плоскости с обычным комплексным умножением.

1) $I \times C$ — полугруппа, пространство которой есть боковая поверхность цилиндра, с единицей (1,1) и минимальным идеалом $0 \times C$. Положим

$$S = (0 \times C) \cup \{(e^{-t}, e^{2\pi it}) | 0 \le t < \infty\},$$

так что S есть базисная окружность $0 \times C$ вместе с бесконечной спиральной обмоткой вокруг нее (см. рис. 3.6).

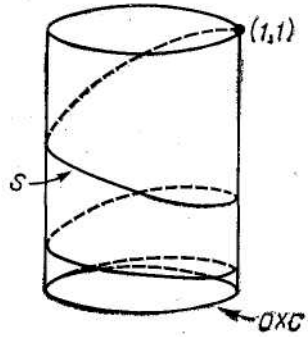


Рис. 3.6

Заметим, что S является кланом с единицей (1,1) и $K(S) = 0 \times C$. Любая дуга в S, что выходит из (1,1), есть однопараметрическая полугруппа, но наименьший подбинг, содержащий такую дугу, есть вся полугруппа S. Следовательно, не существует такой дуги, которую можно было бы продолжить до нити в S. Мы будем называть полугруппу S единичной спиральной полугруппой.

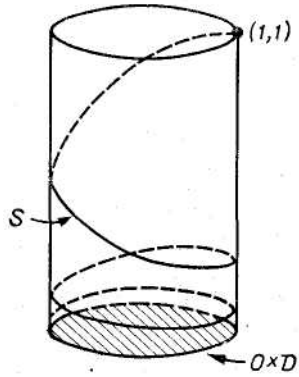


Рис. 3.7

2) $I\times D$ есть полугруппа, пространство которой — цилиндр, с единицей (1,1) и минимальным идеалом (0,0) (см. рис.3.7). Спиральная полугруппа S, определенная в пункте 1, будет подполугруппой в $I\times D$; $T=S\cup(0\times D)$ также будет подполугруппой. T есть объединения спиральной обмотки, которая начинается с нижнего основания цилиндра плюс это основание. Заметим, что T является кланом с единицей (1,1) и нулем, $K(T)$=(0,0). Таким образом, мы опять получаем, что любая дуга, выходящая из точки (1,1), является однопараметрической полугруппой, но ее нельзя продолжить до нити в T.

3) Этот пример принадлежит Хантеру. Мы получим клан T', в котором нет дуг, выходящих из единицы, и вообще единица не лежит в дуге. И дуга, конечно, не будет открытой в $E(T')$. В пространстве E^3 рассмотрим круг D_i, определяемый соотношениями $x^2 + y^2 \le (1/i)$ и $z=1-(1/i)$, где $i = 1, 2, 3,...$, так что круги D_i сходятся к точке $u= (0, 0, 1)$. Из центра круга D_{i+1} проводим криволинейный луч A_i, который остается в пределах конуса, определяемого центром круга D_{i+1} и границей круга D_i и обматывается над границей D, как в примере 2. Положим $T_i = A_i \cup D_i$ и для каждого $i = 1, 2, 3,...$ зададим в T_i умножение так же, как оно определялось для T в примере 2. Тогда центр круга D_i будет нулем для T_i. Пусть $T_\infty = u$ и $T' \cup \{T_i \mid i =\infty, 1, 2, ...\}$. Дополним определение умножения в T' следующим образом: будем считать, что ∞ больше любого целого числа и если $x\in T_i$, $y\in T_j$ и $i < j$, то положим $xy = yx = x$. Тогда T' будет кланом с нулем

$K(T) = (0, 0, 0)$ и единицей u и в T' нет дуги, содержащей точку u (см. рис. 3.8).

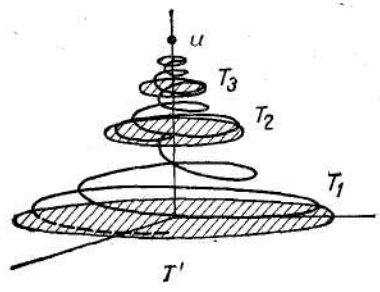


Рис. 3.8

Следует, конечно, проверить непрерывность умножения для каждого i на $T_i \square T_{i+1}$, а также ассоциативность умножения в T'. Это умножение не было бы непрерывным, если бы начало спирали полугруппы T_i находилось бы в единице круга D_{i+1}, а не в его нуле. Заметим, что T' строится из однотипных спиралей по аналогии с тем, как I полугруппы строятся с единичных, ниль- и мин-нитей (см. теорему 1 и определение 4). Заметим также, что в каждой окрестности точки u имеются невырожденные связные группы (границы кругов D_i при достаточно большом i), и интуитивно ясно, что их наличие препятствует построению дуги, которая выходит из u. Это действительно так и следует из теоремы, которая принадлежит Коху.

Теорема 3. Если S есть бинг, в котором каждая подгруппа вполне несвязна, то для каждого идемпотента $e \in S \backslash K(S)$ существует подполугруппа I в S, которая содержит e в качестве единицы, пересекает $K(S)$ и является I полугруппой.

Основным инструментом, которым пользовался Кох в доказательстве этой теоремы, была теорема Мостерта-Шайлдза об однопараметрической полугруппе (см. теорему 2).

Определение 4. *Неприводимой полугруппой* называется *клан* T, в котором нет собственного континуального подмножества, содержащего единицу полугруппы T, пересекающего $K(T)$ и являющегося также подполугруппой.

Возможная ситуация, когда неприводимая полугруппа не будет *топологически неприводимым* пространством, для ее единицы и минимального идеала, т.е. может существовать собственное континуальное подмножество, которое соединяет единицу и

минимальный идеал, хотя соединяющей их собственной континуальной подгруппы нет. Например, *S, T* и *T′* в примерах 2 — неприводимые полугруппы, но *T* и *T′* тем не менее не является топологически неприводимыми. Смысл этого различия стал ясен довольно давно, была выдвинута гипотеза, что неприводимые полугруппы должны быть абелевыми. После многочисленных попыток доказать справедливость этого предположения Кох и Уоллес показали, что топологически неприводимый клан является абелевым. И только Хофманн и Мостерт сумели доказать, что неприводимая полугруппа абелева, их доказательство не элементарно. Формулировка основной теоремы приводится далее.

Пример полугруппы *T′* в примерах 2(3) показывает, что неприводимые полугруппы могут быть значительно более сложными, чем нити или просто одна спираль; в действительности, они строятся из базисных блоков (которые Хофманн и Мостерт назвали *цилиндрическими полугруппами),* вводимых вместе способом, более сложным, но похожим на способ, которым *I* полугруппы строятся из единичных ниль- и мин-нитей.

Строение неприводимых полугрупп имеет особое значение, так как большинство бингов содержит их согласно следующему результату.

Лемма 2. Если *S* — бинг и $e \in S \backslash K(S)$, то *S* содержит неприводимую полугруппу, которая пересекает *K(S*) и имеет единицей элемент *e.*

Доказательство этой леммы простое. Заметим, что {*eSe*} есть семейство кланов, которые содержат *e* и пересекают *K(S).* Это семейство линейно упорядочено по включению (семейство имеет только один член). По лемме Цорна такое семейство имеет максимальный элемент и тогда его пересечение — неприводимая полугруппа, что и требовалось доказать.

Следующая теорема — центральный аспект в исследовании Хофманна и Мостерта о неприводимых полугруппах.

Теорема 4. Неприводимая полугруппа будет абелевой и неприводимые полугруппы представляют собой кланы, для которых *S/*$\mathcal{H}$ обладает естественным строением *I* полугруппы, где $\mathcal{H}$ - отношение эквивалентности на *S,* которое определяется соотношением

$$\mathcal{H} = \{(x, y) \in S \times S \mid x \cup Sx = y \cup Sy \text{ и } x \cup xS = y \cup yS\}.$$

Отношение $\mathcal{H}$, определенное здесь, есть одно из *отношений Грина* на *S* (см. п. 3.10) и согласно определению 3 максимальная подгруппа *H(e),* содержащая элемент *e,* является $\mathcal{H}$ классом для *e. S/*$\mathcal{H}$ есть пространство, получаемое в результате отождествления точек в

каждом $\mathcal{H}$ классе и, в частности, при этом подгруппы из S стягиваются в точки, поэтому $S/\mathcal{H}$ не содержит невырожденных связных групп.

Рассмотрим, например, единичную спираль S из примеров 2 (1). $\mathcal{H}$ классом каждого элемента $x \in S\setminus(0 \times C)$ будет сам x и единственным другим $\mathcal{H}$ классом будет базисная окружность. Следовательно, $S/\mathcal{H}$ есть S, у которой базисная окружность стянута в точку. Очевидно, что мы получили дугу. Аналогично для T из примеров 2 (2): $\mathcal{H}$ классами являются множества, которые были описаны раньше, кроме того, каждая окружность в круге $0 \times D$ радиуса r, $0 \le r \le 1$, с центром в (0, 0) тоже будет $\mathcal{H}$ классом (см. рис. 3.9).

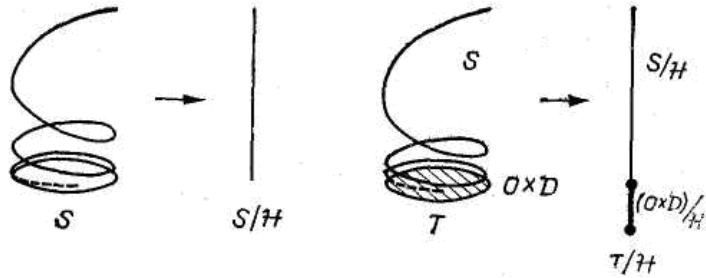


Рис. 3.9

Ясно, что отношение $\mathcal{H}$ можно определить для любой полугруппы S и оно будет отношением эквивалентности, так что пространство $S/\mathcal{H}$ определено корректно, и если S — компактная, то $S/\mathcal{H}$ — хаусдорфово пространство (можно пользоваться несколько более слабыми условиями, чем компактность, чтобы пространство $S/\mathcal{H}$ было хаусдорфовым). Однако в общем случае $S/\mathcal{H}$ не обладает естественной структурой полугруппы, т.е. произведение (в S) двух $\mathcal{H}$ классов может не содержаться в другом $\mathcal{H}$ классе. Это можно выразить, сказав, что $\mathcal{H}$ может не быть отношением *конгруэнтности* (относительно формального определения см. теорему 6). Если полугруппа S *нормальна,* т.е. $xS = Sx$ для каждого $x \in S$, то $S/\mathcal{H}$ будет обладать естественной структурой полугруппы. Очевидно, если S — абелева, то S нормальна, и это одна из причин, по которой очень важно знать, является ли полугруппа абелевой. Например, в 1960 г. Хантер доказал, что если S - нормальная неприводимая полугруппа, то $S/\mathcal{H}$ будет I полугруппой. Но это не было известно для произвольных неприводимых полугрупп, пока Мостерт и Хофманн не доказали их абелевость.

3.13. Построение новых полугрупп

Определение произведения полугрупп (см. определение 3) представляет один из основных способов построения новых полугрупп из имеющихся. Другая основополагающая идея состоит в замене части заданной полугруппы на что-то другое. Этот метод описан в определении 5 и в пункте ”Склеивание Барсука”, посвященном методу склеивания.

5. Определение фактор-полугруппы Риса. Пусть S — компактная полугруппа и I — *замкнутый* идеал. Пусть S/I обозначает обычное фактор-пространство, получаемое в результате отождествления всех точек из I, а ϕ: $S \to S/I$- каноническое отображение. Тогда S/I есть полугруппа с умножением, определяемым равенством $\phi(x)\,\phi(y)=\phi(xy)$, такая фактор-полугруппа называется *фактор-полугруппой Риса.*

Поскольку I — идеал, умножение в S/I определено корректно. Компактность S и замкнутость I применяются для доказательства непрерывности умножения и хаусдорфовости пространства S/I (см. теорему 6).

3. Примеры фактор-полугрупп Риса 1) Ниль-нитка является фактор-полугруппой Риса единичной нити. Действительно, из пункта 2 определения 1 видно, что ниль-нитка есть [0, 1] / [0,1/2], где в [0,1] рассматривается обычное умножение действительных чисел.

2) Несвязная полугруппа может быть преобразована в связную, если существует замкнутый идеал, который пересекает все ее компоненты. Пусть, например, W— конечная полугруппа с n элементами и I =[0, 1] — обычный единичный отрезок. Тогда $W \times I$ — компактная полугруппа с n компонентами; множество $W \times 0$ будет замкнутым идеалом, который пересекает все компоненты, поэтому $W \times I/W \times 0$ будет связным веером. На рис. 3.10 изображен случай для n = 2.

Рис. 3.10

3) Пусть S^1— полугруппа на одномерной сфере, а I = [0, 1] будет I полугруппа. Обозначим через $T = S^1 \times I$ произведение полугрупп.

Очевидно T представляет собой пустой цилиндр. Множество $I_r = S^1 \times [0, r]$ является идеалом полугруппы T для $r \in [0, 1)$ и фактор-полугруппа Риса T/I_r топологически есть 2-клетка, граничная сфера которой будет подполугруппой (см. рис. 3.11).

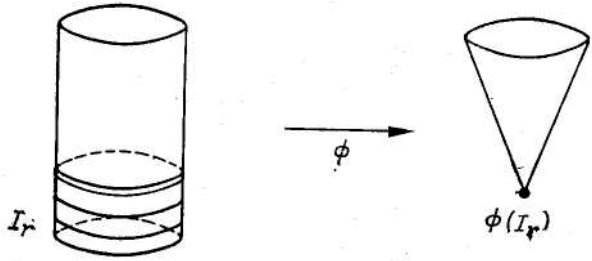


Рис. 3.11

Описанная в пункте 3 ситуация подлается обобщению, если вместо S^1 рассмотреть S^{n-1}, где $n \geq 2$. Мы получим строение полугруппы на n клетке, которая содержит граничную (n—1) сферу как полугруппу. Существует теорема, которая приналежит Мостерту и Шайлдзу, из которой следует, что клан на n-клетке с нулем, граница которой есть подполугруппа, должен быть фактор-полугруппой Риса цилиндра. Эта теорема приводится далее. Она является более общей, поскольку формулируется для L полугрупп. По определению L *полугруппой* называется клан на компактной поверхности, такой, что граница этой поверхности есть подбинг. Для доказательства теоремы о L полугруппах Мостерт и Шайлдз дополнили работу Фосе об I полугруппах и доказали первый вариант своей теоремы об однопараметрической полугруппе. Оба эти результата были упомянуты ранее.

5. Теорема Если S есть L полугруппа с границей B, то B будет компактной группой Ли; B действует на S с помощью левых переносов; пространство орбит S' является I полугруппой и в S существует I полугруппа J, которая будет также сечением для S', следовательно, $S = JB$. Если S содержит нуль, то полугруппа S изеоморфна $(J \times B)/K$, где K — идеал $J \times B$. Умножение в S дифференцируемо тогда и только тогда, когда S' — единичная нить. Например, нетрудно показать, что единичный комплексный круг имеет вид $(I \times C)/K$, где I — стандартная единичная нить, C — группа вращений окружности и $K = (0 \times C)$ (см. рис. 3.6).

Эта теорема частично отвечает на вопросы о топологических полугруппах, поставленные Уоллесом.

Задачи. Предположим, что S — полугруппа на компактной поверхности, граница B которой есть подполугруппой. Насколько умножение в S определяется умножением в B? Когда это умножение дифференцируемо?

Относительно строения таких полугрупп, если они не имеют единицы, известно очень мало. К известным фактам следует отнести результат Хадсона, показавшего, что в случае, когда S есть замкнутая n клетка и ограничивающая сфера B есть левотривиальная подполугруппа в S ($xB = x$ для любого $x \in B$), то или S левотривиальная, или $(S \setminus K(S))^* = BT$ для некоторой I полугруппы T, содержащейся в S.

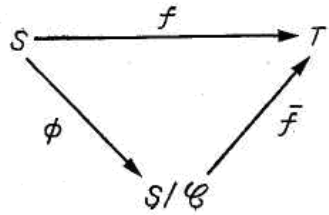
Ранее мы указали, почему хорошо сжимать замкнутый идеал в точку, или, что то же самое, почему фактор-пространство Риса оказывается полугруппой. Формально фактор-полугруппа Риса компактной полугруппы представляет собой специальный случай общего приема выделений замкнутой конгруэнтности, которая приводит к полугруппе в соответствии со следующей теоремой. Большое значение при этом имеет связь между конгруэнтностями и гомоморфизмами, поэтому мы формулируем предложение в полной общности. Отметим, что оно остается справедливым, если прилагательные «компактный» и «компактный хаусдорфовый» заменить на прилагательное «дискретный».

6. Теорема. Предположим, что S — компактная (дискретная) полугруппа и $\mathscr{C}$ — замкнутое отношение эквивалентности на S. Пусть $\phi : S \to S/\mathscr{C}$ — каноническое отображение. Тогда множество $S/\mathscr{C}$ будет компактным и хаусдорфовым (дискретным) в фактор-топологии, множество U в которой открыто по определению тогда и только тогда, когда открыто множество $\phi^{-1}(U)$.

Если $\mathscr{C}$ есть еще и конгруэнтностью, то множество $S/\mathscr{C}$ обладает естественным строением полугруппы, причем отображение ϕ будет гомоморфизмом. Следовательно, замкнутое отношение конгруэнтности на S индуцирует гомоморфизм полугруппы S на другую полугруппу. Наоборот, если $f : S \to T$ есть гомоморфизм из S на T, то отношение

$$\mathscr{C} = f\{(s,s') \in \mathcal{B}S \times S \mid f(s) = f(s')\}$$

будет замкнутой конгруэнтностью на S и полугруппа $S/\mathscr{C}$ изеоморфна T, изеоморфизм $\overline{f} : S/\mathscr{C} \to T$ определяется равенством $\overline{f}\,\phi = f$:



Следующая конструкция, как и фактор-полугруппа Риса, получается в результате применения теоремы 6, но другим способом. Фактор-полугруппа Риса заменяет идеалы на точки, тогда как метод склеивания Борсука описывает условия, при которых подполугруппа может быть заменена другой полугруппой. Эта простая вариация хорошо известного метода склеивания с помощью непрерывной функции, предложенного К. Борсуком.

7. Теорема. Склеивание Борсука. Пусть S — компактная полугруппа и A — замкнутая подполугруппа в S. Предположим, что $f{:}A\to T$ — сюръективный гомоморфизм. Обозначим как $\Delta(S)=\{(x, x)|x\in S\}$ диагональ полугруппы S. Положим

$$\mathcal{E} = \Delta(S) \cup \{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}.$$

Тогда $\mathcal{E}$ есть замкнутое отношение эквивалентности на S, и если $\mathcal{E}$ — конгруэнтность, то и $S/\mathcal{E}$ будет полугруппой и ее можно рассматривать как полугруппу S, у которой вырезана подполугруппа A и разрез заклеен полугруппой T, причем правила склеивания определяются отображением f. Если A — идеал полугруппы S, то $\mathcal{E}$ будет отношением конгруэнтности, когда $f(xa_1) = f(xa_2)$ и $f(a_1x) = f(a_2x)$ для каждого $x\in S$.

4. Примеры 1) Фактор-полугруппа Риса. Пусть A — замкнутый идеал компактной полугруппы S и T — одноточечная полугруппа, а f — отображение A в T.

2) Клан на листе Мебиуса. Пусть C и I такие, как в примере 2. Положим

$$S = I\times C,\ A=0\times C \text{ и } T = C.$$

Определим отображение $f : A\to T$, полагая $f(0, z) = z^2$. Легко видеть, что в результате склеивания отождествляются только противоположные точки на базисной окружности полугруппы S, а остальная часть S остается без изменения. Для того чтобы представить себе геометрически, что пространство, полученное в результате склеивания, действительно является листом Мебиуса, можно: 1) разрезать вертикально S пополам и спустить переднюю половину вниз; 2) повернуть переднюю половину на 180°; 3) склеить два ссмежных

края вместе, это даст нам 2-клетку с отождествленными противоположными точками на базисной окружности полугруппы *S*, исключая угловые точек; 4) снова соединить края разреза так, как они были первоначально, что завершит отождествление противоположных точек базисной окружности полугруппы *S*.

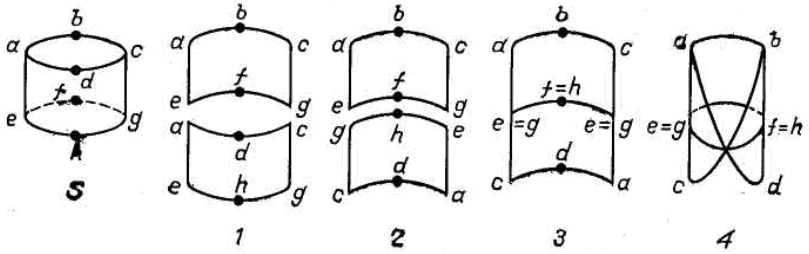


Рис. 3.12

Теперь получится пространство склейки, в то же время процесс построения этого пространства есть стандартный способ получения листа Мебиуса из клетки (см. рис. 3.12).

3) Клан на зонтике. Пусть множество *D* такое же, как в примере 2, $A=\{z\in D>|\ |z|\le 1/2\}$, $T=[0,\ ½]$ с действительным умножением. Определим $f\colon A\to T$, полагая $f(z)=|z|$ (см. рис. 3.13).

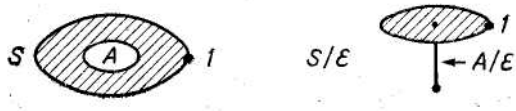


Рис. 3.13

4) Пусть *S* — единичная спираль примера 2 (1) и $\{a, b\}$ — полугруппа, которая состоит из двух элементов. [Например, умножение может быть тривиальным слева, или $\{a, b\}$ может быть циклической группой из двух элементов.] Пусть *T*— базисная окружность полугруппы *S*, а $W=\{a, b\}\times S$ — обычное произведение полугрупп (см. определение 7). Полугруппа *W* компактна, поскольку таковыми являются полугруппы $\{a, b\}$ и *S*. Пусть $A=\{a, b\}\times T\subset W$, определим отображение $f\colon A\to T$ просто как проекцию. Тогда условия теоремы 7 выполняются и в результате склеивания получаем двойную спираль (см. рис. 3.14).

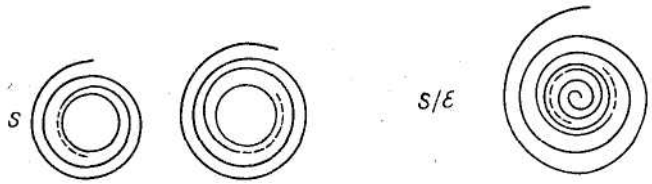


Рис. 3.14

Так как для любой конечной (или более обще, компактной) полугруппы X, $X\times S$ — компактная полугруппа, можно таким же способом склеить множество спиралей, мощность которого есть мощность множества X. Сравните этот пример с примером 3 (2).

Во всех предыдущих примерах отображение f должно было выбираться каждый раз так, чтобы индуцированное им отношение эквивалентности оказывалось замкнутой конгруэнтностью.

3.14. Некоторые соображения о компактных группах

В этом разделе предметом обсуждения будут элементарные, но в тот же время наиболее часто применяемые факты о компактных полугруппах. Предварительно мы приведем без доказательства несколько простых, однако достаточно важных результатов из топологии, которая нам понадобятся в дальнейшем.

Замечания по общей топологии. Пусть X, Y и Z обозначают хаусдорфовы топологические пространства.

1) Если A, $U\subset X$ и U - *открытое* множество, то из $A^*\ \square U\neq\square$ следует, что $A\ \mathrm{I}\ U\neq\square$.

В пунктах 2 и 3 символ $\mathcal{A}$ будет обозначать непустое семейство подмножеств из X, которое является *башней*, т.е. для каждых $A, B\in\mathcal{A}$ или $A\subset B$ или $B\subset A$. Условимся что символ $\mathrm{I}\ \mathcal{A}$ обозначает множество $\mathrm{I}\ \{A\mid A\in\mathcal{A}\}$.

2) Если каждый элемент $A\in\mathcal{A}$ семейства $\mathcal{A}$ есть компактное, непустое множество, то $\mathrm{I}\ \mathcal{A}$ также компактно и непусто.

3) Пусть $f: X\to Y$ - *непрерывное* отображение, тогда $f(\mathrm{I}\ \mathcal{A})\subset\mathrm{I}\ \{f(A)\mid A\in\mathcal{A}\}$, и если каждое $A\in\mathcal{A}$ компактно, то

$f(\square\, \mathcal{A}) = \mathrm{I}\ \{f(A) | A \in \mathcal{A}\}$. Следовательно, если X - полугруппа и $\mathcal{A}$ — башня компактных подмножеств из X, то $x(\mathrm{I}\ \mathcal{A}) = \mathrm{I}\ \{xA | \in \mathcal{A}\}$ для каждого элемента $x \in X$.

4) Для любого непрерывного отображения $f: X \to Y$ и множества $A \subset X$ имеется включение $f(A^*) \subset f(A)^*$, и если множество A компактно в X, то $f(A^*) = f(A)^*$. Следовательно, если A и B — подмножества полугруппы, то $A^* B^* \subset (AB)^*$, и если A^* и B^* еще и компактны, то $A^*B^* = (AB)^*$.

5) Если $A \subset X$, A компактно и $z \notin A$, то существует такое открытое множество W, что $A \subset W$ и $z \notin W$.

6) Если A и B компактны, $A \times B \subset X \times Y$, $f: X \times Y \to Z$ - неспрерывное отображение и $f(A \times B) \subset W$, где W- открытое множество, то существуют открытые множества U и V, такие, что $A \subset U$, $B \subset V$ и $f(U \times V) \subset W$. Следовательно, если $X = Y = Z$ есть полугруппа и $AB \subset W$, где W— открытое множество, то существуют открытые множества U и V, такие, что $A \subset U$, $B \subset V$ и $UV \subset W$.

6. Определение Для элемента $x \in S$ положим $\Gamma_n(x) = \{x^p | p \geq n\}^*$,

$$\Gamma(x) = \Gamma_1(x) \text{ и } N(x) = \mathrm{I}\ \{\Gamma_n(x) | n \geq 1\}.$$

Следующая теорема была сформулирована Кохом и Намакурой.

8. Теорема Если $x \in S$ и $\Gamma(x)$ — компактное множество, то $N(x)$ будет идеалом $\Gamma(x)$ и $N(x)$ — группа. Следовательно, для элемента x в компактной полугруппе степени x скапливаются к некоторому идемпотенту, в частности компактная полугруппа содержит идемпотент.

Доказательство. Замкнутое подмножество компактного пространства само компактно, поэтому $N(x)$ есть пересечение непустой башни непустых *компактных* множеств. Тогда, в соответствии с пунктом 2 вышеприведенных замечаний, множество $N(x)$ компактно и непусто. Непустое пересечение подполугрупп полугруппы снова будет полугруппой, поэтому $N(x)$ — полугруппа.

Для того чтобы доказать, что $N(x)$ является идеалом $\Gamma(x)$, мы покажем, что $x^r N(x) = N(x)$ для каждого $r \geq 1$. Следовательно, $\{x^r | r \geq 1\}\ N(x) \subset N(x)$. Тогда согласно пунктам 1 и 4 вышеприведенных замечаний $\Gamma(x)N(x) \subset N(x)$. Имеется дуальное включение: $N(x)\Gamma(x) \subset N(x)$. Пусть поэтому $r \geq 1$. Проделаем некоторые вычисления: $x^r N(x) = x^r(\mathrm{I}\ \{\Gamma_n(x) | n \geq 1\})$ и в соответствии с пунктом 3 вышеприведенных замечаний это равно $\mathrm{I}\ \{x^r \Gamma_n(x) | n \geq 1\}$; согласно пункту 4 вышеприведенных замечаний $x^r \Gamma_n(x) = (x^r\{x^p | p \geq n\})^*$, что равно $\{x^{r+p} | p \geq n\}^* = \Gamma_{r+n}$. Следовательно,

$$x^r N(x) = \bigcap \{\Gamma_{r+n}(x) \mid n \geqslant 1\} = \bigcap \{\Gamma_n(x) \mid n \geqslant r+1\},$$

что равно $N(x)$, так как $\Gamma_{r+1}(x) \subset \ldots \subset \Gamma_1(x)$.

Поскольку $N(x)$ — полугруппа, для того чтобы доказать, что она является группой, достаточно показать, что $y(x) = N(x)y = N(x)$ для каждого элемента $y \in N(x)$. Мы показали предварительно, что для каждого $r \geq 1$ $x^r N(x) = N(x)x^r = N(x)$, интуитивно ясно, что последовательности x^r сходятся к точкам множества $N(x)$ и из этого должны бы следовать нужные нам равенства. Для справедливости этих рассуждений необходима компактность. Перейдем к доказательству. Положим $A = \{a \in \Gamma(x) \mid aN(x) = N(x)\}$. Если бы мы знали, что $A^* \subset A$, то, поскольку $\{x^r \mid r \geq 1\} \subset A$, мы должны были бы иметь $\Gamma(x) \subset A^* \subset A$ и, в частности, $N(x) \subset A$, что и требуется. Для того чтобы доказать, что $A^* \subset A$, положим $в \in A^*$ и предположим методом от противного, что $y \notin A$. Тогда $yN(x) \not\subseteq N(x)$, поэтому существует $z \in N(x) \setminus yN(x)$. Так как y и $N(x)$ компактны, $yN(x)$ — также компактное множество, следовательно, из пункта 5 вышеприведенных замечаний вытекает, что существует открытое множество W, такое, что $z \notin W$ и $yN(x) \subset W$. [Отметим, что $N(x) \not\subset W$]. Согласно пункту 6 вышеприведенных замечаний существуют открытые множества U и V, такие, что $y \in U$, $N(x) \subset V$ и $UV \subset W$. Но в соответствии с пунктом 1 вышеприведенных замечаний, поскольку $y \in U \square A^*$, существует некоторый элемент $a \in U \cap A$; если $a \in U$, то $aN(x) \subset UV \subset W$, если $a \in A$, то $a\,N(x) = N(x)$, но $a \in A \cap U$, т.е. $a \in U$ и $a \in A$. Мы получили противоречие. Поэтому предположения, что $y \notin A$, неверно, следовательно, $A^* \subset A$.

Из дуальных рассуждений вытекает, что множество $A' = \{a \in \Gamma(x) \mid N(x)\, a = N(x)\}$ замкнуто и, следовательно, $\Gamma(x) \subset A'$, поэтому $\Gamma(x) \subseteq A \cap A' = \{a \in \Gamma(x) \mid aN(x) = N(x)\, a = N(x)\}$, в частичности $N(x) \subset A \cap A'$. Теорема доказана.

Прежде чем идти дальше, отметим, что доказательство замкнутости A зависело только от компактности $N(x)$, и точно таким же способом можно доказать, что для любого компактного подмножества $N(x)$ полугруппы S множества $\{x \in S \mid xN \supset N\}$, $\{x \in S \mid xN \subset N\}$, $\{x \in S \mid Nx \subset N\}$ и $\{x \in S \mid Nx \supset N\}$ замкнуты.

7. Определение. *Действием* называется полугруппа S, пространство X и непрерывное отображение

$$S \times X \to X,$$

которое, как правило, не обозначается никаким символом (образ пары элементов s и x обозначается просто как sx) и удовлетворяющее соотношению

$$t_1 (t_2 x) = (t_1 t_2) x$$

для любых $t_1, t_2 \in S$ и любого $x \in X$.

Читатель, знакомый с теорией автоматов, сразу обнаружит, что действие есть в точности непрерывный автомат. Действия играли ранее вспомогательную роль в различных результатах, таких, как лемма 3, и только позднее они стали предметом детального изучения. Следующая лемма представляет собой исключительно полезный инструмент для изучения строения топологических полугрупп и принадлежит Уоллесу. Она носит нескольео неестественное, на наш взгляд, название - лемма об опухоли (опухолевой леммы).

Лемма 3. Предположим, что S действует на X, $x \in S$ и $\Gamma(x)$ компактно. Пусть A — такое компактное подмножество в X, что $x \supset A$. Тогда $xA = A$ и для каждого элемента $y \in \Gamma(x)$ отображение $a \to ya$ является гомеоморфизмом A на A. Следовательно, идемпотент в $\Gamma(x)$ есть элемент, действующий как единица на A.

Доказательство. Так как $xA \supset A$, то $x^2A \supset xA \supset A$, и по индукции $x^nA \supset A$ для всех $n \geq 1$. Следовательно, $\{x^n \mid n \geq 1\} \subset \{y \in S \mid y \supset A\}$ и последнее множество замкнуто (см. замечание после доказательства теоремы 8), поэтому $\Gamma(x) \subset \{y \in S \mid y \supset A\}$. Так как $\Gamma(x)$ — компактное множество, то по теореме 8 существует идемпотент $e \in N(x)$ и согласно предыдущему предложению $eA \supset A$. Из этого следует, что для каждого $a \in A$ выполняется равенство $ea=a$ (так как если $a \in eA$, то $a=eb$ для некоторого $b \in A$ и, следовательно, $ea=e^2b=eb=a$). Поэтому $a \to ea$ — тождественное отображение множества A и, в частности, $eA = A$.

Для того чтобы убедиться, что $yA = A$ для любого элемента $y \in \Gamma(x)$, мы должны еще доказать, что $yA \subset A$. Для этого заметим, что $yA = yeA$, $ye \in N(x)$, так как $N(x)$ — идеал в $\Gamma(x)$ и $N(x)$ — группа. Тогда существует элемент $(ye)^{-1} \in N(x)$, такой, что $(ye)(ye)^{-1} = e$. Нам известно, что $(ye)^{-1}A \supset A$, следовательно, $(ye)(ye)^{-1}A \supset yeA$, т.е. $A \supset yA$. Таким образом, $yA = A$. Наконец, $a \to ya$ такое же отображение, что и $a \to yea$, это отображение является гомеоморфизмом, так как оно отображает A на A и обратное ему отображение $a \to (ye)^{-1}a$ непрерывно.

3. Приложения леммы. 1) Предположим, что S — компактная полугруппа, $T=S \times S$ — обычное декартово произведение и умножение в T определяется соотношением

$$(x,y)(x',y')=(xx',y'y).$$

(Заметим, что умножение, определенное в полугруппе T, не совпадает с законом умножения в умножении полугрупп, введенном в определении

3, т.е. T не является произведением (умножением) полугрупп S. Полугруппа T нужна нам для того, чтобы определить некоторое действие.) Очевидно, что T — компактная полугруппа и с учетом умножения, определенного в T, она действует на S, а именно

$$[(x, y), s] \to xsy.$$

Если A и S компактны, $A \subset S$, и если $xAy \supset A$ для некоторых элементов $x, y \in S$, то $x'Ay' = A$ для всех элементов $(x', y') \in \Gamma(x, y)$ [здесь $\Gamma(x, y)$ — это $\Gamma((x, y))$ для элемента (x, y) полугруппы T], в частности, S содержит левую и правую единицы для подмножества A.

Доказательство. Полугруппа T компактна, так как компактна полугруппа S. Тогда по лемме 3 $(x', y')\, A = A$ для каждого элемента $(x', y') \in \Gamma(x, y)$, т.е. $x'Ay' = A$. Если (e, f) — идемпотент в $\Gamma(x, y)$, то $eAf = A$, откуда получаем $eA = A = Af$, так что e и f— левая и правая единицы соответственно для множества A. [Здесь существенно используется тот факт, что e и f — идемпотенты, так как, вообще говоря, из равенства $xAy = A$ не следует, что $xA = A$ или $Ay = A$. Кроме того, $\Gamma(x, y)$ — всего лишь подмножество в $\Gamma(x) \times \Gamma(y)$, поэтому нельзя утверждать, что $x'Ay' = A$ для каждых $x' \in \Gamma(x)$ и $y' \in \Gamma(y)$.]

2) Компактная полугруппа S является *устойчивой*, т.е. из условий $baS \supset aS$ для любых $a, b \in S$ следует, что $baS = aS$, и из условий $Sab \supset Sa$ для любых $a, b \in S$ следует, что $Sab = Sa$. (Устойчивость означает, что отношение Грина $\mathcal{D}$ и $\mathcal{F}$ на полугруппе S равны).

3) Если S — компактная полугруппа и $xS = S$ для некоторого элемента $x \in S$, то S содержит левую единицу— идемпотент в $\Gamma(x)$.

4) Если S— компактная полугруппа, $x \in A = A^* \subset S$ и $xA \supset A$, то $\Gamma(x)$ есть группа, которая содержится в A. Наиболее важная сторона этого результата заключается в том, что *A не обязательно будет подполугруппой*.

Доказательство. Если $x \in A$, то $x^2 \in xA$ и $xA = A$ по лемме 3. Следовательно, $x^2 \in A$. По индукции доказывается, что $x^n \in A$ для всех $n \geq 1$. По условию множество A замкнуто, следовательно, $\Gamma(x) \subset A$. Тогда по лемме 3 $e\Gamma(x) = \Gamma(x)$, где e — идемпотент в $\Gamma(x)$. Но имеется включение $e\Gamma(x) \subset N(x)$, поскольку $N(x)$ — идеал в $\Gamma(x)$. Из этого вытекает, что $\Gamma(x) = N(x)$, следовательно, $\Gamma(x)$ — группа.

Следующая лемма дает нам удобное техническое средство для изучения компактных полугрупп с разделяющими точками, а также компактных полугрупповых действий на континуумы с разделяющими точками.

5. Лемма. Предположим, что S - компактная полугруппа и S действует на континуальное множество X. Если H — подмножество в S

с непустой границей $F(H)$ и H^* содержит такую точку x, что $Sx \subset H^*$, то для некоторой точки $p \in F(H)$ имеется включение $Sp \subset H^*$.

На интуитивном уровне строгости формулировка этой леммы означает, что если некоторая точка из множества H^* переводится всей полугруппой S внутрь H^*, но эта точка лежит в H^* достаточно глубоко, то ее можно вытянуть из внутренности H^*, т.е. имеется граничная точка множества H, переводимая всей полугруппой S также в H^*. Ясно, что эта лемма оказывается очень полезной, когда H имеет только одну граничную точку, она существенно применяется в доказательстве свойств (1) и (2) в применении леммы 5.

5. Применение леммы. 1) Пусть имеется действие $S \times X \to X$, где S и X — компактные множества. Пусть J — максимальное множество относительно свойств $\square \neq J \subset X$ и $SJ \subset J$. Если $C \subset X \setminus J$ и C есть пересечения континуальных множеств с одноточечной границей, то C содержит самое большее одну точку.

Это предложение — одно из важнейших вспомогательных средств в роботах Дэй и Уоллеса, где рассматриваются действия $S \times X \to X$, для которых X является *континуальным множеством с открытой плотной полупрямой,* т.е. X содержит гомеоморфный образ интервала (0, 1], который плотен в X (т.е. его замыкание равно X), но который открыт в X. Каждая точка в образе (0, 1) является разделяющей. Единичная спираль из примера 2 (1) представляет собой континуальное множество с открытой плотной полупрямой.

2) Пусть S — компактная полугруппа, которая действует на отрезок $I = [0, 1]$ так, что $S0 = 0$. Тогда множество нулей этого действия $\{x \in I \mid Sx = x\}$ имеет вид $[0, c]$ для некоторого $c \in [0, 1]$.

Доказательство. Пусть $Z = \{x \in I \mid Sx = x\}$ и z есть верхняя грань множества Z, z существует, так как $Z \neq \square (0 \in Z)$ и так как Z ограничено, например, числом 1. Поскольку S — компактная полугруппа, нетрудно доказать, что множество Z замкнуто (см. доказательство леммы 3), следовательно, $z \in Z$. Итак, $Z \subset [0, z]$, и $0, z \in Z$. Предположим, что $x \in (0, z)$, тогда x— граничная точка в I как множества $[0, x]$, так и множества $[x, 1]$. Положим $H = [0, x]$ и применим лемму 5. Мы получим, что $Sx \subset [0, x]$, так как $S0=0$. Пусть теперь $H=[x, 1]$, тогда снова из леммы 3 вытекает, что $Sx \subset [x, 1]$, так как $z \in [x, 1]$ и $Sz = z$. Следовательно, $Sx = x$ и поэтому $x \in Z$. Отсюда следует что $(0, z) \subset Z$. Таким образом, получаем $[0, z] = Z$.

Информация, которая содержится в следующей теореме, применяется очень часто. На языке алгебраических полугрупп она утверждает, что минимальный идеал компактной полугруппы вполне

простой. Доказательство этого факта, по существу, алгебраическое, компактность необходимая для того, чтобы установить существование минимального левого, правого и двустороннего идеалов. Дальше топологические свойства не играют никакой роли и то, что идеал вполне простой, показывается так же, как в алгебраической полугруппе.

9. Теорема. Если S — компактная полугруппа, то S имеет компактный минимальный идеал $K(S)$, и если $\hat{L}$ и $\hat{R}$ — семейства всех минимальных левых и минимальных правых идеалов полугруппы S соответственно, то $K(S) = \bigcap \hat{L} = \bigcup \hat{R}$. Кроме того, если $L \in \hat{L}$ и $R \in \hat{R}$, то $LR = K(S)$ и $L \cap R = H(e)$ для некоторого идемпотента e. Следовательно, $K(S)$ является объединением непересекающихся групп которые непересекаются. Если $x \in K(S)$, то минимальный левый идеал, который содержит x, имеет вид Sx и минимальный правый идеал, который содержит x, имеет вид xS.

Доказательство. Сама полугруппа S есть компактный идеал в S, поэтому по лемме Цорна существует непустая максимальная башня $\mathcal{T}$ компактных идеалов. Согласно пункту 2 вышеприведенных замечаний $K = \bigcap \mathcal{T}$ — компактное непустое множество, поэтому K будет минимальным компактным идеалом полугруппы S. В то же время K - минимальный идеал, так как для любого элемента $x \in K$ множество SxS компактно, оно является идеалом и подмножеством любого идеала, содержащего x. Аналогично S содержит минимальный левый и правый идеалы. K— единственное подмножество в S с перечисленными ранее свойствами. Действительно, если K'— другой минимальный идеал, то $\square \neq KK' \subset K \cap K'$. Следовательно, $K \cap K'$ является идеалом, но тогда $K \cap K' = K = K'$. $\bigcup \hat{L} \subset K$, так как если $L \in \hat{L}$, то L будет левым идеалом. В то же время K — идеал и мы получаем, что $K\hat{L} \subset L \cap K$ и KL — левый идеал. Следовательно, $KL = L \subset K$. Очевидно, объединение $\bigcup \hat{L}$ есть левый идеал, поэтому если мы докажем, что он является еще и правым идеалом, то получим, что $\bigcup \hat{L} = K$. Для того чтобы сделать это, отметим, что $Lx \in \hat{L}$ для каждого $L \in \hat{L}$ и $x \in S$. (В самом деле Lx — левый идеал и если бы M был левым идеалом, содержащимся в Lx, то множество $\{y \in L \mid yx \in M\}$ была бы левым идеалом, содержащимся в L и, следовательно, равным L, но тогда M равен Lx.) Поэтому

$$(\square \hat{L}) = \bigcup \{LS | L \in \hat{L}\} = \bigcup \{Lx | L \in \hat{L}, x \in S\} \subset \bigcup \hat{L},$$

так что $\bigcup \hat{L}$ есть правый идеал и $K = \bigcup \hat{L}$. Дуальные рассуждения доказывают, что $K = \bigcup \hat{R}$.

Пусть $L \in \hat{L}$ и $R \in \hat{R}$. Очевидно, что множество LR будет идеалом и $LR \subset K$. Следовательно, $LR = K$. Далее заметим, что если $x \in L$, то $Lx \subset L^2 \subset L$, и из $Lx \in L$ следует, что $Lx = L$. Дуальное утверждение также верно, т.е. если $x \in R$, то $x = R$. Тот факт, что множество $R \cap L$ будет группой, доказывается следующим образом. Очевидно, $\square \neq RL \subset R \cap L$ и RL— полугруппа. Если $x \in RL$, то $Lx = L$ и $x = R$ согласно доказанному ранее. Следовательно, $xRL = RLx = RL$, так что RL — группа. Наконец, $R \cap L = (R \cap L)e \subset RL$, где e — идемпотент в RL. Следовательно, $R \cap L = RL$ и поэтому $R \cap L$ есть группа.

Пусть $x \in K$, выберем $L \in \hat{L}$ так, что $x \in L$. Очевидно, Sx - левый идеал, а также $Sx \subset SL \subset L$. Следовательно, $Sx = L$. Дуальные рассуждения доказывают, что $x \in xS \in R$.

3.15. Индуцированные отношения Грина

Введение. Обычные отношения Грина определяются для топологической полугруппы точно так же, как для алгебраической полугруппы. Они являются отношениями эквивалентности и будут замкнуты, если полугруппа S компактна. В случае топологических полугрупп эти отношения, как и для алгебраических полугрупп, служат одним из фундаментальных средств изучения строения полугруппы. Укажем, например, теорему Хофманна — Мостерта (теорема 4), результаты о построении минимального идеала компактной полугруппы, полученные в результате изучения $\mathcal{D}$ класса (см. теоремы 11, 12), теорему Щютценберже об $\mathcal{H}$ классах, принадлежащих общему $\mathcal{D}$ классу (см. теорему 13). Уоллес определил *относительные идеалы и индуцированные отношения Грина* и обобщил на них в топологическом случае многие из имеющихся результатов.

Пусть S — полугруппа и $T \subset S$ обозначает подмножество. Отметим, что, вообще говоря, T не является подполугруппой полугруппы S.

8. Определение. Для элементов $x, y \in S$ определим $(x,y) \in \mathcal{L}_T$ тогда и только тогда, когда $T^1x = T^1y$; $(x, y) \in \mathcal{R}_T$ тогда и только тогда, когда $xT^1 = yT^1$; $(x, y) \in \mathcal{F}_T$ тогда и только тогда, когда $T^1xT^1 = T^1yT^1$; $\mathcal{H}_T = \mathcal{L}_T \cap \mathcal{R}_T$ и $\mathcal{D}_T = \mathcal{L}_T \circ \mathcal{R}_T$. Определенные здесь отношения $\mathcal{L}_T$, $\mathcal{R}_T$, $\mathcal{H}_T$, $\mathcal{F}_T$ и $\mathcal{D}_T$ называются *индуцированными отношениями Грина* полугруппы S. Если $T=S$, мы получим обычные отношения Грина, определенные Клиффордом и Престоном. Нижний индекс писать не обязательно, мы используем его здесь, чтобы подчеркнуть, что рассматриваются индуцированные отношения. Для элемента $x \in S$ символы R_x, L_x, D_x и H_x обозначают $\mathcal{R}_T$ класс, $\mathcal{L}_T$ класс, $\mathcal{D}_T$ класс и $\mathcal{H}_T$ класс соответственно, что содержит x.

Согласно следующей лемме классы индуцированного отношения обеспечивают разложение классов обычного отношения Грина. Это указывает одну из причин, по которой следует считать полезным введение индуцированных отношений, но, кроме того, они являются достаточно мощным техническим инструментом. Многие теоремы об обычных отношениях Грина обобщаются на индуцированные отношения, если T выбирается таким, что $T = T^*$, а также в случае, когда $T^2 \subset T$.

6. Лемма. Для любого подмножества $T \subset S$ каждый класс эквивалентности обычного отношения Грина $\mathcal{L}_S$ является объединением $\mathcal{L}_T$ классов, т.е. $\mathcal{L}_T \subset \mathcal{L}_S$. Аналогично

$$\mathcal{R}_T \subset \mathcal{R}_S, \mathcal{F}_T \subset \mathcal{F}_S, \mathcal{H}_T \subset \mathcal{H}_S, \mathcal{D}_T \subset \mathcal{D}_S.$$

11. Теорема. Если $x, y \in S$ и $xy \in R_x \cap L_y$, то $R_y \cap L_x = H_e$ для некоторого $e \in E$ и H_e является подгруппой в S. К томк же $H_xH_y = H_{xy} = R_x \cap L_y$.

Если еще $T^2 \subset T$ и $xT \cup Ty \subset T$, то имеет место диаграмма egg-box Клиффорда, которая изображена на рис. 3.15.

$L_e = Ly' = L_x$

$R_e = R_{x'} = R_y$

e	x'	y
y'	$y'x'$	$y'y$
x	xx'	xy

Рис. 3.15.

Ее строки обозначают $\mathcal{R}_T$ классы, столбцы обозначают $\mathcal{L}_T$ классы и все они принадлежат $\mathcal{D}_T$ классу. Если $e \in E$, $x \in L_e$ и $y \in R_e$, то $xy \in R_x \cap L_y$. Здесь никакие допущения о множестве T не делаются.

12. Теорема. Пусть S — компактная полугруппа и T— замкнутое подмножество. Пространство $Z=S\times S\times S$ с законом умножения, определенным из равенства $(x, y, z)\ (x', y', z') = (x, yzx'y', z')$, является полугруппой, отображение $f : Z\to S$, где $f(x, y, z)=xyz$, есть гомоморфизм. Если

$$e \in E(S) \text{ и } Z_e = (L_e \cap E) \times H_e \times (R_e \cap E),$$

то $f|Z_e$ будет гомеоморфизмом в S. Следовательно, $f|Z_e$ будет изеоморфизмом в S.

Положим $H = \bigcup H_f | f \in E(S)\}$ и $M_e = \{x \in S | ex, xe \in H\}$. Определим $u : H \to E$, полагая $u(x)$ единицей для H_f, где H_f есть $\mathcal{H}_T$ класс, который содержит x. Отображение u непрерывно, следовательно, отображение $g:M_e\to Z$, задаваемое соотношением $g(x)=[u(xe),exe,$и $(ex)]$, непрерывно и отображение $g|f(Z_e)$ является обратным для f.

Если Z_e - подполугруппа (а это так, когда $D_e \subset H$), то отображение $f|Z_e$ — изеоморфизм.

13. Следствие: теорема Риса — Сушкевича. Если S - компактная полугруппа и $e \in E \cap K$, то K изеоморфен $(Se \cap E) \times eSe \times (eS \cap E)$ с умножением, определяемым соотношениям

$(x, y, z)\ (x', y', z') = (x, yzx'y', z')$, и K будет ретрактом S, как и $K \cap E$, $eS \cap E$, и eSe, и $Se \cap E$.

Доказательство. По теореме 9 $eS \cup Se \subset K$, $K \subset H$, следовательно, $M_e = S$. К томуже по теореме 9, так как $e \in K$, имеем $L_e = Se$ и $R_e = e$, поэтому согласно определению $\mathcal{H}$ $He=eS \cap Se$. Так как $e = e^2$, $eS \cap Se = eSe$, и тогда в силу теоремы 12 получаем, что $Z_e=(Se \cap E)\times eSe \times(eS \cap E)$. Z_e имеет требуемое умножение и $f|Z_e$ является изеоморфизмом на $(Se \cap E)\ eSe(eS \cap E)$, последнее множество равно K согласно следующим рассуждениям. Так как $eS = eSeS = eSe^2S$, $e(eS \cap E) = eS \cap E$ и $(Se \cap E)e = Se \cap E$, мы видим, что

$(Se \cap E)\ eSe\ (eS \cap E) =(Se \cap E)\ (Se)\ (eS)\ (eS \cap E) =(L \cap E)\ LR\ (R \cap E)$,

где $L \in \hat{L}$, $R \in \hat{R}$. По теореме 9 $(L \cap E)\ L = L$, $R\ (R \cap E) = R$ и $LR = K$.

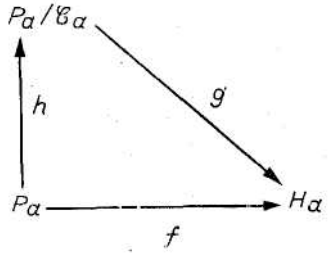
Отображение $fg : S \to K$ есть ретракция S на K и ufg: $S \to E \cap K$ есть ретракция S на $E \cap K$.

Рассматривая композиции g с проекциями на соответствующие сомножители Z_e, получаем ретракции S на $Se \cap E$, eSe и $eS \cap E$.

14. Теорема (Щютценберже). Пусть S — компактная полугруппа, $T = T^*$ и для элемента $a \in S$ положим

$$P_a = \{x \in S \mid xH_a = H_a\} \text{ и } \mathscr{C}_a = \{(x, y) \in P_a \times P_a \mid xa = ya\}.$$

Если мощность множества H_a больше 1, то P_a будет замкнутой подполугруппой, $\mathscr{C}_a$ - замкнутое отношение конгруэнтности на P_a и существует следующая коммутативная диаграмма:



где h — каноническая проекция, $f(x) = xa$, g — гомеоморфизм и $P_a/\mathscr{C}_a$ — компактная группа. Если $a^2 = a$, то f есть гомоморфизм и g будет изеоморфизмом. Независимо от того, верно или нет равенство $a^2 = a$, существует единственная группа G, гомеоморфная H_b для каждого $b \in D_a$ и изеоморфная H_b, если H_b содержит идемпотент.

Приведем еще одну структурную теорему, которая представляет определенный интерес.

Для множества $T \subset S$ J называется *максимальным собственным T идеалом,* если $\square \neq J \neq S$,

$$T^1 J T^1 \subset J$$

и J есть максимальным по включению подмножеством полугруппы S, обладающим этими свойствами. Следующий результат, который принадлежит Уоллесу, обобщает на T идеалы (в случае, когда $T^2 \subset T$) теорему о строении дополнения максимального собственного идеала. Было бы очень хорошо, если бы существовал аналог этой теоремы в случае, когда T не является подполугруппой.

15. Теорема. Пусть S — компактная полугруппа и T — ее замкнутая подполугруппа. Пусть J — максимальный собственный T идеал, положим $A = S \setminus J$. Допустим, что мощность множества A больше 1.

1) Если $TST \subset J$, то или $S = J \cup T_a$ и $A = L_a$ для каждого элемента $a \in A$, или $S = J \cup aT$ и $A = R_a$ для каждого элемента $a \in A$.

2) Если $TST \not\subset J$, то $S = J \square TaT$, $J_a = A$, $L_a = Ta \cap A$ и $R_a = aT \cup A$ для каждого $a \in A$.

3) Если $T \cap A \neq \square$, то или $T \cap J$ — максимальный собственный идеал полугруппы T, или T — простая полугруппа.

Микромодуль 12.
Моноиды и регулярные события

В этом микромодуле представлен основной аппарат и связаные с ним понятия по применению монотдов и полугрупп для исследования свойств дискретных систем, как объектных, так и процессных. Мы начнем с того, что приведем определение полугруппы и моноида.

Полугруппой называется множество элементов S вместе с бинарной операцией произведения на этом множестве (произведение элементов a и b обозначается как ab), удовлетворяющей следующим условиям:

1) если $a, b \in S$, то $ab \in S$;

2) $(ab)c = a(bc)$ для всех элементов $a, b, c \in S$.

Если в дополнение к этому в S имеется единица (или нейтральный элемент) e, такая, что

3) $ea = ae = a$ для всех элементов $a \in S$, то S называется *моноидом*.

Раличие между моноидами и полугруппами тривиально и, казалось бы, можно не повторять, что они почти одинаковы. Однако для изучения событий такой объект, как моноид, более удобный, и дальше, как правило, мы будем иметь дело с моноидами, а не с полугруппами. Условимся о некоторых обозначениях для множества элементов моноида и для самого моноида. Так, когда мы говорим «пусть M — моноид», то одновременно M обозначает множество элементов этого моноида. Это общепринятая двусмысленность, которая никогда не причиняет неприятностей в работе.

Напомним, что согласно принятой терминологии *группой* называется такой моноид, каждый элемент которого имеет обратный a^{-1}, т.е. a^{-1} — такой элемент, который $a^{-1}a = aa^{-1} = e$. Оказывается, важные результаты алгебраической теории систем связаны с рассмотрением подгрупп данного моноида, т.е. тех подмоноидов, которые представляют собой группы.

Множеством $\sum^*$ всех слов над алфавитом $\sum$ называется свободный моноид, единица которого (нейтральный элемент) есть пустое слово λ, а произведение слов моноида есть просто их

последовательное приписывание. Очевидно, что эта операция ассоциативна.

Событием (или языком) над алфавитом $\sum$ мы будем называть любое подмножество из $\sum^*$. Особый интерес представляют *регулярные* события — события, которве связанны с конечными автоматами и могут быть охарактеризованы с помощью гомоморфизмов $\sum^*$ на некоторые конечные моноиды.

Скажем несколько слов об обозначениях. Пусть γ — такое отображение, что для любого слова $W \in \sum^*$ $\gamma(W)$ будет элементом моноида M. Говорят, что отображение γ есть гомоморфизм, если для всех слов W и $V \in \sum^*$ выполняется соотношение $\gamma(WV) = \gamma(W)\gamma(V)$. Для любого множества A слов из $\sum^*$ $\gamma(A)$ есть в точности множество всех таких элементов m из M, что для некоторого слова $W \in A$ имеем $\gamma(W)=m$. $\gamma^{-1}(m)$ есть множество всех слов, которые переходят в m при отображении γ. И для любого подмножества S моноида M $\gamma^{-1}(S)$ есть в точности такое множество слов из $\sum^*$, которые переводятся в элементы множества S отображением γ.

Заметим, что если γ — гомоморфизм моноида $\sum^*$ на некоторый моноид, то необходимо $\gamma(\lambda)=e$. Так как пустое слово λ играет большую роль в наших рассмотрениях, существенно, чтобы любая применявшаяся полугруппа была моноидом. Разумеется, теория регулярных событий могла бы быть развита без специального упоминания пустого слова, но включение этого слова делает все результаты более естественными. По этой причине удобно при изучении событий исключить из рассмотрения те полугруппы, которые не является моноидами.

Обычно, если имеется некоторое событие E, мы интересуемся только теми гомоморфизмами γ, для которых E *замкнуто* относительно $\gamma^{-1}\gamma$, т.е. такими гомоморфизмами γ, что $E = \gamma^{-1}\gamma(E)$.

Для любого отображения γ моноида $\sum^*$ назовем слово W_1 *конгруэнтным* слову W_2 *по модулю* γ [или $W_1 \equiv W_2 \pmod{\gamma}$], если $\gamma(W_1) = \gamma(W_2)$. Будем также говорить, что W_1 *конгруэнтно* W_2 по модулю E [или $W_1 \equiv W_2 \pmod{E}$], если для любых слов V и X $VW_1X \in E$ тогда и только тогда, когда $VW_2X \in Э$. Читатель должен четко понимать, что это есть два различных вида конгруэнтности. Но хотя они и различны, существующая между ними связь, определяет появление моноидов в изучении событий.

Мы используем разбиение $\sum^*$ на конгруэнтные множества и укажем зависимость между этими разбиениями для раздичных отношений конгруэнтности. *Множеством конгруэнтных* слов (по модулю γ или по модулю E) называется непустое множество, которое содержит

вместе с некоторым элементом все те и только те слова, которые конгруэнтны этому элементу. Множества конгруэнтности (множества конгруэнтных слов) чаще называются классами конгруэнтности, но мы предпочитаем употреблять термин «множество» для обозначения множества слов, а термин «класс» — для класса множеств.

Среди всех гомоморфних отображений моноида $\sum^*$ существует одно наиболее важное для изучение события E, а именно отображение в *синтаксический моноид* события E или в $S(E)$. Элементами моноида $S(E)$ являются множества конгруэнтности по модулю E. Гомоморфизм просто отображает слово из $\sum^*$ на множестве конгруэнтности по модулю E, какое это слово содержит. Отображение определено корректно, поскольку каждое слово над алфавитом $\sum$ принадлежит одному и только одному множеству конгруэнтности по модулю E.

Для того чтобы сделать множество $S(E)$ моноидом, мы должны ввести операцию умножения и установить ее ассоциативность. Для этого заметим, что если A и B — множества конгруэнтности, то для некоторого множества конгруэнтности C $AB \subseteq C$, т.е. множество конгруэнтности C содержит все слова вида WW', где $W \in A$ и $W' \in B$. (Однако ввиду того, что в C могут быть слова, не представляемые в таком виде, мы не можем в общем случае утверждать, что $C=AB$.) Это замечание дает нам операцию умножения, а именно, произведением двух множеств конгруэнтности A и B называется такое множество конгруэнтности C, что $AB \subseteq C$. Ассоциативность этой операции немедленно следует из ассоциативности умножения слов в $\sum^*$. (Фактически это указывает, как следует проверять последнее предложение. Несколько сложнее доказывается корректность введенной операции умножения. Здесь надо установить, что все слова из AB содержатся в одном и только в одном множестве конгруэнтности).

Название «синтаксический моноид» вызвано тем, что его определение дается в сроках понятия конгруэнтности слов по модулю события.

1. Теорема. Если γ есть гомоморфизм $\sum^*$ в $S(E)$, то E замкнуто относительно $\gamma^{-1}\gamma$, более того, для любых слов W и W' $W \equiv W' \pmod{\gamma}$ тогда и только тогда, когда $W \equiv W' \pmod{E}$.

Доказательство. Для того чтобы установить первое утверждение, достаточно доказать, что любые два слова W и W', отображающиеся при гомоморфизме γ в один и тот же элемент, или оба принадлежат E, или оба находятся вне E. Но если W и W' отображаются в один и тот же элемент, они должны быть конгруэнтны по модулю E,

следовательно, $W = \lambda W \lambda \in E$ тогда и только тогда, когда $W' = \lambda W' \lambda \in E$. Второе утверждение теоремы 1 представляет собой просто переформулировку определения синтаксического моноида.

Однако существуют и другие гомоморфизмы γ моноида $\sum^*$, при которых событие E замкнуто относительно $\gamma^{-1}\gamma$. Связь между моноидами, являющимися образами этих гомоморфизмов и синтаксическим моноидом, исключительно важна. Следующий результат представляет собой обобщение теоремы 1.

2. Теорема. Для того чтобы событие E было замкнуто относительно $\gamma^{-1}\gamma$, где γ — гомоморфизм, необходимо и достаточно, чтобы для всех слов W и W' из соотношения $W \equiv W' \pmod{\gamma}$ следовало $W \equiv W' \pmod{E}$.

Доказательство. *Достаточность.* Предположим, что условие выполнено. Пусть для любого слова $W \in \sum^*$ A_W обозначает множество слов, конгруэнтных W по модулю γ. Тогда для любого W $\gamma^{-1}\gamma(A_W) = A_W$. Из этого следует, что для $B = \bigcup_{W \in E} A_W$ $\gamma^{-1}\gamma(B) = B$. Требуемое равенство $\gamma^{-1}[\gamma(E)] = E$ будет доказано, если мы покажем, что $E = B$. Перейдем к проверке последнего равенства.

Включение $E \subseteq B$ немедленно следует из определения множества B. Предположим теперь, что W — произвольное слово из B. Существует слово $W' \in E$, такое, что $W' \equiv W \pmod{\gamma}$, тогда по условию $W' \equiv W \pmod{E}$. Следовательно, W также принадлежит E (действительно, $W' = \lambda W' \lambda \in E$, откуда по определению конгруэнтности следует, что $\lambda W \lambda = W \in E$).

Необходимость. Предположим, что $\gamma^{-1}[\gamma(E)] = E$. Необходимо доказать, что если слова W и W' удовлетворяют соотношению $W \equiv W' \pmod{\gamma}$, то $W \equiv W' \pmod{E}$. Предположим, что $W \equiv W' \pmod{\gamma}$. Это значит, что $\gamma(W) \equiv \gamma(W')$. Для того чтобы показать, что $W \equiv W' \pmod{E}$, мы должны проверить, что для всех V и X $VWX \in E$ тогда и только тогда, когда $VW' \in E$. Но заметим, что $\gamma(VWX) = \gamma(V)\gamma(W)\gamma(X)$ и $\gamma(VW'X) = \gamma(V)\gamma(W')\gamma(X)$, так как отображение γ есть гомоморфизм; поскольку $\gamma(W) = \gamma(W')$, то $\gamma(VWX) = \gamma(VW')$. Из этого следует, что $VWX \in \gamma^{-1}[\gamma(VW')]$ и $VW' \in \gamma^{-1}[\gamma(VWX)]$. Так как $\gamma^{-1}[\gamma(E)] = E$, то $VWX \in E$ тогда и только тогда, когда $VW'X \in E$. Теорема доказана полностью.

Подумаем о значении теоремы 2. Гомоморфизм и событие E определяют разбиение моноїда $\sum^*$ на множества конгруэнтности. Теорема 2 утверждает, что для замкнутости E относительно $\gamma^{-1}\gamma$ необходимо и достаточно, чтобы разбиение, определяемое гомоморфизмом γ, было мельче (или равно) разбиения, определяемого событием E. Другими словами, необходимо и достаточно, чтобы

каждое множество конгруэнтности по модулю γ было подмножеством некоторого множества конгруэнтности по модулю *E*. Таким образом, разбиение, соответствующее гомоморфизму на синтаксический моноид, самае грубое среди всех разбиений, соответствующих гомоморфизмам γ, таким, что $\gamma^{-1}\gamma(E)=E$. Теорема 3 устанавливает фундаментальное отношение между моноидами, являющимися образами таких гомоморфизмов, и синтаксическим моноидом. Читателя, возможно, заинтересует сравнительная роль синтаксического моноида в классе всех моноидов, для которых $\gamma^{-1}\gamma(E)=E$ (где γ — гомоморфизм на соответствующий моноид), и роль (редуцированного) приведенного графа состояния в классе графов состояния для данного события. Как известно, произвольный граф состояния для события гомоморфен приведенному графу состояния.

Действительно, мы можем рассматривать граф состояния как разбиение $\sum^*$ на множества слов. Каждое множество соответствует одному из состояний и является в точности множеством слов, образующих путь, который выходит из начального состояния и заканчивается в заданном состоянии. Рабин и Скотт дали математическую характеристику таких множеств, а именно: они являются множествами эквивалентности правоинвариантного отношение эквивалентности; отношение эквивалентности rel (сокращенно от relation (англ.) — отношение) над множеством слов называется *правоинвариантным*, если из соотношение *W* rel *W′* вытекает, что *WU* rel *W′U*. Рассматривая очевидное аналогичное определение левоинвариантного отношение, Рабин и Скотт определили отношение конгруэнтности как отношение эквивалентности, которое левоинвариантно и правоинвариантно.

3. Теорема. Если γ - гомоморфизм и $\gamma^{-1}\gamma\ (E) = E$, то моноид $M=\gamma(\sum^*)$ может быть гомоморфно отображен на синтаксический моноид *S (E)*.

Доказательство. Напомним, что элементами *S(E)* есть множества конгруэнтности слов по модулю *E*. По теореме 2 каждое множество конгруэнтности по модулю γ будет подмножеством некоторого множества конгруэнтности по модулю *E*. Пусть η — такое отображение моноида *M* на *S(E),* что для каждого $s \in M$ $\eta(s)$ есть такое множество конгруэнтности по модулю *E,* подмножеством которого будет $\gamma^{-1}(s)$ (множество конгруэнтности по модулю γ*)*. Очевидно, что η отображает *M* на *S(E)*. Нам необходимо только доказать, что η представляет собой гомоморфизм, т.е. что для каждых элементов $s_1, s_2 \in M$ $\eta(s_1s_2) =\eta(s_1)\eta(s_2)$. Но так как каждый элемент из *M* является

образом при гомоморфизме γ некоторого слова из ∑*, достаточно показать, что для всех слов W_1 и W_2

$$\eta [\gamma(W_1)\, \gamma(W_2)]=\eta [\gamma(W_1)]\eta [\gamma(W_2)]. \qquad (*)$$

Так как γ — гомоморфизм, $\gamma (W_1W_2) = \gamma (W_1)\, \gamma (W_2)$, поэтому для проверки справедливости соотношения (*) достаточно доказать, что

$$\eta [\gamma(W_1W_2)]=\eta [\gamma(W_1)]\eta [\gamma(W_2)]. \qquad (**)$$

или, другими словами, надо доказать, что отображение ηγ есть гомоморфизм.

Но ηγ отображает каждое слово в его множество конгруэнтности. Читатель может без труда установить это, рассмотрев определение отображения γ. То, что это отображение есть гомоморфизм, было уже показано при обсуждении построения синтаксического моноида события.

Все изложенное справедливо независимо от того, конечен или бесконечен моноид γ(∑*). Здесь нас интересуют только регулярные события, и последующие теоремы подскажут нам, что можно ограничиться рассмотрением только таких γ, для которых моноид γ(∑*) конечен.

Конечный граф состояния над алфавитом ∑ имеет конечное число вершин или состояний, обозначенных окружностями. Из каждого кружочка выходит стрелка, соответствующая каждой букве из ∑, наконечник стрелки достигает некоторого состояния. Одно состояние избрано в качестве начального, другие могут быть названы терминальными состояниями. На рис. 3.16 ∑={0, 1} и имеется три состояния.

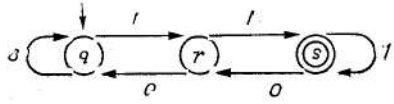


Рис. 3.16

Терминальные состояния — это двойные окружности, и единственная, никак не обозначенная точка указывает начальное состояние. Такой граф можно рассматривать как граф, соответствующий отображению переходов конечного автомата с входным алфавитом ∑.

В таком графе *G* пусть *G (s, W)* обозначает состояние — конечную точку пути, начинающегося в *s* и прочитывающего слово *W*. Состояние *G (s, W)* существует и однозначно определено в графе состояния. Пусть *G (W)* обозначает состояние *G* (s_0, *W)*, где s_0 — начальное состояние. Так, *G (λ)* есть само начальное состояние. Мы полагаем, что

использование буквы G для обозначения графа и описанной функциональной зависимости не вызовет путаницы.

Говорят, что событие E, содержщееся в $\sum^*$, является *регулярным событием,* если существует конечный граф состояний G с начальным состоянием s_0 и множество терминальных состояний, такие, что

$$E = \{W \in \sum^* | G(W) \in T\}.$$

Известно, что регулярные события — это в точности те события, которые можно получить с помощью *регулярных выражений*, последние представляют события через конечное число операций об′единения, умножения ($A \bullet B = \{ab \mid a \in A$ й $b \in B\}$) и операции итерации ($A^* = \{a_1 .. a_n \mid n \geq 0$ каждое $a \in A\}$).

Приведенным (или редуцированным) графом состояния G для релярного события E называется граф, в котором:

1) для каждого состояния s из G существует слово W, такое, что $s = G(W)$,

2) для каждой пары состояний s и s', где $s \neq s'$, существует W, такое, что или $G(s, W)$ — терминальное состояние, а $G(s', W)$ — нетерминальное, или наоборот.

4. Теорема. Каждому регулярному событию E соответствует единственный с точностью до изоморфизма приведенный граф состояний, имеющий меньше состояний, чем любой другой граф для E, и вычисляющийся алгоритмически одним из обычных способов, если событие задано (как, например, произвольный граф состояний или регулятное выражение).

Даказывать эту теорему не будем.

5. Теорема. Два слова W и W' содержатся в одном и том же множестве конгруэнтности по модулю регулярного события E тогда и только тогда, когда для каждого состояния приведенного графа состояния события E справедливо равенство $G(s, W) = G(s, W')$.

Доказательство. Предположим сперва, что W и W' приналежат одному и тому же множеству конгруэнтности по модулю E, т.е. для всех слов V и X $VWX \in E$ тогда и только тогда, когда $VW' \in E$. Пусть s - любое состояние. Существует путь из начального состояния в s, пусть этот путь прочитывает (или расшифровывает) слово V. Предположим, что $s_0 = G(s, W) \neq G(s, W) = s_v$. Тогда существует такое X, что или $G(s_0, X)$ является терминальным состоянием и $G(s_1, X)$ не является терминальным состоянием, или наоборот. Тогда $VWX \in E$, но $VW' \notin E$, или наоборот. Но эти соотношения противоречат допущению, что $W \equiv W' (\mathrm{mod}\ E)$. Из этого следует, что $G(s, W) = G(s, W')$.

Предположим теперь, что для каждого s из G выполняется равенство $G(s, W) = G(s, W')$. Тогда для каждого слова V

$G(VW) = G(VW')$ и, следовательно, для каждого слова X $G(VWX) = G(VW'X)$. Поэтому мы получаем, что $VWX \in E$ тогда и только тогда когда $VW' \in E$.

Если задан граф G и выбрано слово W, то имеется отображение на множестве состояний графа G, переводящее состояние s в $G(s, W)$.

Тогда из теоремы 5 следует, что конгруэнтными по модулю E будут такие слова, которые индуцируют одинаковые функции на приведенном графе состояния G события E. Заметим, что если G имеет n состояний, то существуют самое больше n^n отображений на множестве состояний графа G. Вспомнив теперь теорему 3, мы получаем следующий важный результат.

Следствие. Событие E на алфавите $\sum$ регулярно тогда и только тогда, когда синтаксический моноид $S(E)$ конечен, и, следовательно, E регулярно тогда и только тогда, когда существует гомоморфизм моноида $\sum^*$ на конечный моноид S, такой, что $E = \gamma^{-1}\gamma(S)$.

Теорема 5 дает нам удобный вычислительный метод для получения синтаксического моноида; приведем соответствующий пример. Рассмотрим граф G, изображенный на рис. 3.16. Очевидно, что G приведенный. Для того чтобы следить за множествами конгруэнтности слов, мы должны знать, что происходит при выборе произвольного слова и произвольного состояния. Построим новый граф состояния G', начальное состояние которого обозначено как qrs, и такой, что для каждого слова W $G'(W) = G(q, W)\, G(r, W)\, G(s, W)$. Граф G' строится последовательно шаг за шагом, а именно $G'(0) = qqr$, $G'(1) = rss$, $G'(00) = qqq$, $G'(01) = rrs$ и т.д. Результат представлен на рис. 3.17.

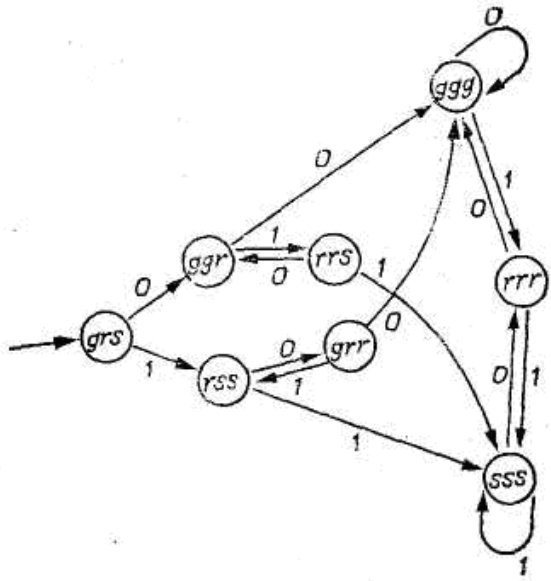


Рис. 3.17

Каждое состояние графа G' представляет множество конгруэнтных слов события, которое задается графом G. Для любого состояния соответствующее множество конруэнтности есть множество всех таких слов W, что $G'(W) = s'$. Следовательно, множество, соответствующее состоянию qrs, состоит из пустого слова λ, состоянию qqr соответствует множество 0 (10)* и т.д. Из метода построения и теоремы 5 очевидно следует, что $G'(W) = G'(W')$ тогда и только тогда, когда $W = W' (\mathrm{mod} E)$. Следовательно, G' представляет синтаксический моноид графа G. Если слова — представители множества конгруэнтности будут по соглашению именовать классы (за исключением m для rrr), то таблица умножения этого моноида будет иметь следующий вид:

	λ	0	1	01	10	00	11	*m*
λ	λ	0	1	01	10	00	11	*m*
0	0	00	01	*m*	0	00	11	*m*
1	1	10	11	1	*m*	00	11	*m*
01	01	0	11	01	*m*	00	11	*m*
10	10	00	1	*m*	10	00	11	*m*
00	00	00	*m*	*m*	00	00	11	*m*
11	11	*m*	11	11	*m*	00	11	*m*
m	*m*	00	11	*m*	*m*	00	11	*m*

Эту таблицу умножения можно отождествить с самим моноидом, Отметим, что любая небольшая полугруппа может быть практически преставлена в таком виде. Отметим также, что граф состояния на рис. 3.17 включает в себя такую же информацию; умножение любых двух элементов может быть получено на рисунке почти так же легко, как и с помощью таблицы. Например, если требуется найти произведение элемента (10) с *(m),* мы заметим, что *m* = 110 и затем выведем 10110 из начального состояния и приведем к окружности, обозначенной как *rrr*. Теперь мы вспомним, что *rrr* представляет 110=*m,* и получим результат умножения. Для того чтобы сделать этот процесс более ясным, заменим граф состояния, изображенный на рис. 3.17, графом, представленным на рис. 3.18, который станем называть моноидным графом.

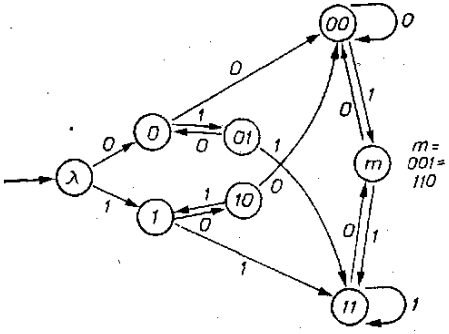


Рис. 3.18.

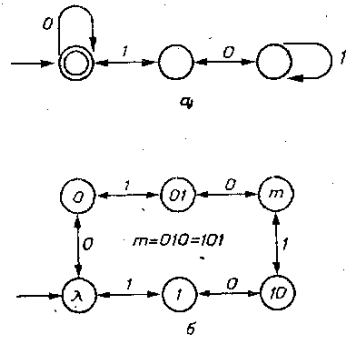


Рис. 3.19

Мы будем рассматривать его как удобное представление синтаксического моноида регулярного события. Далее предполагается, что читатель знает, как из приведенного графа состояния строится моноидный граф и как он используется в качестве представления синтаксического моноида. (Следует отметить, что ряд специалистов по

современной теории групп добились успехов в применении таких графов для представления групп.)

Рассмотрим еще два примера. На рис. 3.19а и 3.20а изображены приведенные графы состояния двух событий, а на рис. 3.19б и 3.20б — соответствующие им синтаксические моноиды. Стрелки с двумя концами, помеченные 1 (или 0), означают, что 1 (или 0) переходит из одного состояния в другое, и наоборот.

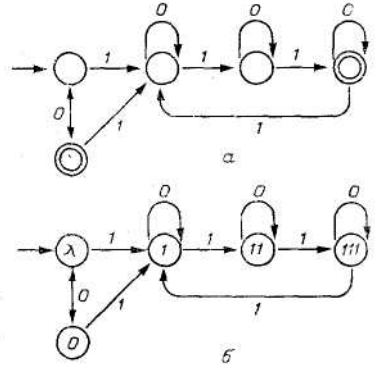


Рис. 3.20

Многие задачи о конечном автомате могут быть решены, если известно, из каких подгрупп состоит синтаксический моноид автомата и какую роль в строении моноида играют его подгруппы. Читатель, знакомый с работами Крона и Роудза по теории декомпозиции, уже знает, какое значение в декомпозиции имеют подгруппы моноида и его негрупповая часть, а также как они связаны друг с другом. В исследованиях событий было открыто (результат следует из работы Щютценберже), что если синтаксический моноид события не имеет нетривиальных подгрупп, то для события могут быть получены многие факты даже без применения алгебры. Например, такое событие представляется как разновидность регулярного события, выражаемая в терминах операций объединения, пересечения, дополнения (над множеством всех слов, порожденных алфавитом) и умножения, но без использования итерационной операции (или звездочки*). Кроме того, как доказал Щютценберже, это в точности те события, которые могут быть описаны в некоторой системе символической логики. Из этого результата видно, какое большое значение имеют относительно замкнутые системы символической логики. С 1962 г. (с появлением теории Крона и Роудза) все большее значение стали играть алгебраические достижения в теории автоматов. И здесь особое значение приобретает

исследование группового строения автомата. Поэтому заключительная часть данного пункта посвящается изложению алгоритма для нахождения максимальных подгрупп конечного моноида.

Подгруппой моноида называется подполугруппа, которая в свою очередь является группой. Другими словами, это множество элементов, которое: 1) замкнуто относительно операции произведения элементов, 2) содержит единичный элемент, 3) вместе с любым принадлежащим ему элементом содержит обратный элемент. Единичный элемент i подгруппы вовсе не обязан быть единицей основного моноида. Существенно то, что он должен удовлетворять соотношению $i^2 = i$, т. е. быть идемпотентом моноида. Наоборот, каждый идемпотент моноида является единицей некоторой подгруппы моноида, она может быть даже тривиальной группой (т. е. группой порядка 1), состоящей олько из самого идемпотента.

Если задана подгруппа G с единицей i, то мы будем говорить, что G будет подгруппой *вокруг* идемпотента i. Оказывается, что каждый идемпотент моноида имеет вокруг себя максимальную подгруппу, точный результат дается теоремой 11. Проблема, которой мы будем заниматься, состоит в нахождении этих максимальных подгрупп, так как все другие подгруппы моноида представляют собой подмножества (и, разумеется, подгруппы) максимальных подгрупп. Заметим, что в моноиде, изображенном на рис. 3.18, все элементы, кроме 0 и 1, являются идемпотентами. Моноид из рис. 3.20 имеет два идемпотента λ и 111, в то время как у моноида, приведенного на рисунке 3.19б, только один идемпотент λ — единица моноида. Мы увидим вскоре, что изобилие идемпотентов в примере, представленном на рис. 3.18, отражает тот факт, что моноид в этом случае имеет только тривиальные подгруппы. С другой стороны, моноид на рис. 3.19б является группой. Где-то между этими двумя крайними случаями находится моноид, изображенный на рис. 3.20б, он содержит нетривиальные подгруппы, но в то же время не является группой. Для того чтобы у читателя не возникло ложное впечатление, мы должны отметить, чю существуют моноиды, у которых мало идемпотентов, но которые имеют только тривиальные подгруппы. Пример такого моноида представлен на рис. 3.21.

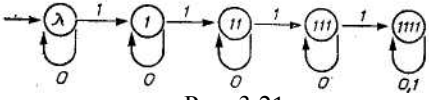


Рис. 3.21

Этот моноид имеет только два идемпотента и не содержит (как мы увидим) нетривиальных подгрупп. (Мы предоставляем читателю проверить, что на рис. 3.21 изображен граф моноида. Один из методов проверки того, что граф состояния является графом моноида, заключается в том, чтобы представить его как приведенный граф состояния для события и построить для него граф синтаксического моноида. Теперь первоначальный граф является графом моноида тогда и только тогда, когда он изоморфен графу, полученному в результате предложенного построения. Доказательство последнего утверждения мы оставляем читателю в качестве самостоятельного упражнения.)

Каждый элемент a конечного моноида M определяет последовательность степеней $a, a^2, a^3, \ldots$ Так как моноид M конечен, в этой последовательности степеней имеется только конечное число различных элементов. Пусть $n(a)$, $q(a)$ и $m(a)$ — положительные целые числа, определяемые следующим образом: $n(a)$ — наименьшее целое положительное число, такое, что для некоторого $y>n(a)$, $a^{n(a)} = a^y$; затем $q(a)$ есть наименьшее целое положительное число, такое, что $a^{n(a)} = a^{n(a)+q(a)}$, наконец, $m(a)$ есть такое кратное $q(a)$, что $n(a) \le m(a) \le n(a) + q(a) - 1$. Три построенных целых числа определяют степени элемента a, играющие исключительно важную роль в нахождении максимальных подгрупп моноида. Докажем некоторые результаты для этих чисел.

Лемма. Элементы $a^{n(a)}, a^{n(a)+1}, \ldots, a^{n(a)+q(a)-1}$ попарно различны.

Доказательство. Предположим, что $a^{n(a)+l} = a^{n(a)+j}$, $0 \le i < j \le q(a)-1$. Так как из равенства $ax = a^y$ следует, что для любого z $a^{x+z} = a^{y+z}$, мы получаем соотношение $a^{n(a)+i+q(a)-1} = a^{n(a)+q(a)} = a^{n(a)}$, которое противоречит определению числа $q(a)$, так как $i + q(a) - j < q(a)$.

7. Теорема. Элемент $a^{m(a)}$ есть идемпотентом и это единственный идемпотент среди степеней a.

Доказательство. Заметим, что из равенства $a^{n(a)} = a^{n(a)+q(a)}$ следует, что для всех $x \ge n(a)$

$$a^x = a^{x+q(a)} \qquad (***)$$

Так как $m(a)$ есть кратное числа $q(a)$, то

$$a^{m(a)} = a^{m(a)+q(a)} = a^{m(a)+2q(a)} = \ldots = a^{2m(a)}$$

Это доказывает, что элемент $a^{m(a)}$ является идемпотентом.

Предположим теперь, что a^x также идемпотент, т.е. что $a^{2x} = a^x$. Число x не может быть меньше, чем $n(a)$, так как $a^{n(a)}$ есть по определению наименьшая степень элемента a, равная большей степени того же элемента. Предположим, что $x - n(a) \equiv i_1 [\mathrm{mod}\ q(a)]$ и

$2x - n(a) \equiv i_2 \pmod{q(a)}$, где $0 \le i_1 \le q(a) - 1$ и $0 \le i_2 \le q(a) - 1$. В силу равенства (***) $a^x = a^{n(a)+i_1}$ и $a^{2x}=a^{n(a)+i_2}$. В силу леммы a^x и a^{2x} будут равны, только если числа i_1 и i_2 равны, откуда следует, что $x=2x \pmod{q(a)}$. Это последнее соотношение справедливо только тогда, когда число x кратно $q(a)$. Но тогда $a^x = a^{m(a)}$. Тем самым показано, что $a^{m(a)}$ — единствнный идемпотент среди степеней элемента a. Теорема доказана полностью.

8. Теорема. Множество $\{a^{n(a)}, a^{n(a)+1},\ldots,a^{n(a)+q(a)-1}\}$ является циклической подгруппой с единицей $a^{m(a)}$ и порождается элементом $a^{m(a)+1}$.

Доказательство. Заметим, что так как $m(a)$ есть кратное числа $q(a)$, то $a^{m(a)+1}a^{m(a)+1}=a^{m(a)+2}$. В самом деле, для любого $i(a^{m(a)+1})^i=a^{m(a)+i}$, к тому же, если $m(a)+i>n(a)+q(a)-1$, то $a^{m(a)+1}=a^{m(a)+i-q(a)}$. Следовательно, множество, порождаемое элементом $a^{m(a)+1}$ совпадает с множеством $\{a^{n(a)}, a^{n(a)+1},\ldots,a^{n(a)+q(a)-1}\}$. В частности, $(a^{m(a)+1})^{q(a)}=a^{m(a)}$ и $(a^{m(a)+1})^{q(a)+1}=a^{m(a)+1}$ и потому в силу элементарных фактов теории групп последнее множество будет циклической группой порядка $q(a)$ с единицей $a^{m(a)}$.

9. Теорема. Произвольная степень a^x элемента a принадлежит подгруппе моноида тогда и только тогда, когда $x \ge n(a)$.

Доказательство. Половина теоремы 9 уже доказана в теореме 8 Поэтому предположим, что $x<n(a)$. Из основ теории групп известно, что если элемент a^x принадлежит конечной группе, то a^x порождает циклическую подгруппу этой группы и для некоторого $y>1$ $a^x = (a^x)^y = a^{xy}$. Но это противоречит условию, что $a^{n(a)}$ есть наименьшая степень элемента a, равная одной из него более высоких степеней. Следовательно, элемент a^x не может принадлежать никакой подгруппе моноида.

Значение теоремы 9 заключается в том, что, определив числа $n(a)$ и $q(a)$, мы знаем, какие степени элемента a принадлежат подгруппам и какие не принадлежат, а также сколько имеется таких элементов.

10. Теорема. Теоретико-множественное объединение всех циклических групп, расположенных вокруг идемпотента, является группой и содержит в качестве подгруппы каждую подгруппу моноида, расположенную вокруг этого идемпотента,

Доказательство. Пусть G_u — замыкание относительно операции произведения теоретико-множественного объединения всех циклических групп, расположенных вокруг идемпотента u. В силу своего определения G_u является подмоноидом и для любого элемента $a \in G_u$

$a = c_1c_2...c_n$, где c_i есть элемент соответствующей циклической группы, расположенной вокруг идемпотента *u*. Очевидно, что $a^2=c_1c_2... c_nc_1c_2...c_n$ и так же, как и все степени элемента *a,* принадлежит G_u (этих степеней, разумеется, конечное число).

Для каждого *i* существует элемент $c_i^{-1} \in G_u$, такой, что $c_i^{-1}c_i = c_i c_i^{-1} = u$. Тогда элемент $a^{-1} = c_i^{-1}c_{n-1}^{-1}\dots c_1^{-1}$, как и все его степени, которых имеется конечное число, принадлежит G_u. Очевидно, что $aa^{-1} = a^{-1}a = u$. Множество, состоящее из элемента *u,* всех степеней элемента *a* и всех степеней элемента a^{-1}, является, следовательно, конечной группой с единичным элементом *u,* так как оно удовлетворяет всем необходимым аксиомам; эта группа должна совпадать со своей циклической подгруппой, порожденной элементом *a.* Поэтому мы доказали, что каждый элемент из G_u принадлежит циклической группе, единицей которой является *u.* Следовательно, G_u есть теоретико-множественное объединение циклических групп. То, что G_u есть группа, проверяется непосредственно.

Рассмотрим теперь произвольную подгруппу *G,* расположенную вокруг идемпотента *u.* Для каждого элемента $a \in G$ циклическая подгруппа в *G,* порожденная *a,* содержит *u* в качестве единицы и должна, следовательно, быть подгруппой в G_u. Но так как группа *G* есть объединение таких циклических подгрупп, *G* представляет собой подгруппу группы G_u.

Теорема 11. Подгруппы, которые расположены вокруг различных идемпотентов, не пересекаются.

Доказательство. Предположим, что G_1 и G_2 — группы, расположенные вокруг идемпотентов u_1 и u_2, причем $u_1 \neq u_2$. Пусть $a \in G_1$ и $a \in G_2$. Это предположение приводит к противоречию сразу по нескольким причинам. Одна из них заключается в том, что u_1 и u_2, оба должны быть степенями элемента *a,* но это невозможно по теореме 7. (Теорема 11 остается верной и для бесконечных моноидов. Доказательство этого случая оставляем читателю.)

Теперь мы изложим вычислительную процедуру для получения всех максимальных подгрупп моноида, основывающуюся на теоремах 7—11. Начнем с произвольного элемента *a* моноида. Определим числа *n (a), q (a)* и *m (a),* которые дают нам информацию о том, что $a^{n(a)},\dots,a^{n(a)+q(a)-1}$ — попарно различные элементы, принадлежащие максимальной подгруппе, расположенной вокруг идемпотента $a^{m(a)}$ и что элементы $a, a^2, \dots, a^{n(a)-1}$ вообще не принадлежат никакой подгруппе.

Затем выберем произвольный элемент *b,* не являющийся степенью *a,* и проделаем то же самое для *b,* найдя циклическую группу, распо-

ложенную вокруг идемпотента, являющегося степенью *b*. Этот идемпотент может совпадать с найденным ранее идемпотентом, и тогда все элементы построенной циклической группы будут элементами построенной ранее циклической подгруппы. Если же новый идемпотент не совпадает с построенным ранее, то циклические группы этих двух идемпотентов не пересекаются.

Построение проводится до тех пор, пока не будут исчерпаны все элементы моноида, т. е. пока каждый элемент не будет включен в какую-либо циклическую полугруппу. Таким способом будут получены все максимальные группы в моноиде. Результат проделанной операции заключается в делении моноида на его максимальные подгруппы и на смешанный набор элементов, которые не принадлежат никакой группе.

Применяя описанную процедуру к моноиду, изображенному на рис. 3.20,б, берем a=0. Мы получаем последовательность степеней 0, 0^2, 0^3=0; следовательно, $n(0)$=1, $q(0)$=2, идемпотентом оказывается элемент 0^2=λ, а циклической группой, которая расположена вокруг λ, будет множество {0, λ}. Затем выбираем b=1, последовательность степеней элемента b имеет вид $1,1^2,1^3,1^4$=1, поэтому $n(1)$ = 1, $q(1)$= 3. Циклической группой, которая расположена вокруг идемпотента 111, будет множество {1, 11, 111}. Больше элементов в моноиде нет, следовательно, он состоит из двух максимальных подгрупп, обе они циклические и любой элемент моноида принадлежит одной из них Заметим, что если нашу процедуру применить к моноиду, который изображен на рис. 3.19,*б*, то каждый раз будет появляться один и тот же идемопотент λ. Существуют четыре различные циклические группы { λ, 0}, { λ, 1}, { λ, *m*}, { λ, 01, 10}. В моноиде нет элементов, лежащих вне единственной максимальной подгруппы, расположенной вокруг λ, т. е. моноид является группой. Читатель, знакомый с теорией групп, не должен, конечно, применять вычислительную процедуру для установления этого факта. Из рис. 3.19,*б* ему должно быть сразу ясно, что здесь имеется симметрическая группа перестановок трех элементов.

Применим нашу процедуру к моноиду, изображенному на рис. 3.19. Мы можем начать с 0, получим 0, 0^2, 0^3 = 0^2, с n (0) = 2, q (0) = 1. Следовательно, 0 не является элементом никакой подгруппы и вокруг идемпотента 0^2 расположена тривиальная подгруппа. Аналогично 1 не является элементом никакой подгруппы, но она порождает тривиальную подгруппу, расположенную вокруг 11. Продолжая вычисле-

ния, мы найдем, что каждый из оставшихся элементов будет идемпотентом и нетривиальных подгрупп не существует.

Микромодуль 13.
Нечеткие композиции

В этом микромодуле предлагаем читателю познакомиться с законами нечеткой композиции. Среди этих законов наиболее общими и полезными являются те, которые образовуют моноид (полугруппу), т.е. имеют единичный элемент и ассоциативны. Кроме того, покажем, что структура группы не подходит для основных операций, рассмотренных в теории нечетких подмножеств, - понятие симметрии нечетких подмножеств не определяется для операторов этой теории.

Известно, что подлинная важность теории моноидов или полугрупп проявляется там, где есть связь с теорией информации, кодами, системами команд и т.д.

3.16. Основные понятия закона композиции

Вспомним несколько классических понятий теории обычных множеств.

Закон внутренней композиции. *Законом внутренней композиции на множестве* E называется отображение из E×E в E. Иначе говоря, каждой упорядоченной паре $(x, y) \in$ E×E ставится в соответствие один и только один элемент $z \in$ E.

На практике этот закон изображают символом, который, располагаясь между x и y, служит для обозначения элемента, соответствующего упорядоченной паре (x, y). Часто используют символ *. Таким образом,

$$x * y = z;$$

на практике для разновидностей законов используют подходящие общепринятые символы такие как: $+, \cdot, \times, \oplus, \otimes$ и. т.

Отображение E × E в E часто удобно изображать условным знаком, связанным с элементами E:

$$(x, y) \sim\!\!\!\rightarrow z, \; x, y, z \in \text{E}.$$

Закон внешней композиции. Пусть $x \in \text{E}_1$; $y \in \text{E}_2$ и $z \in \text{E}_3$. Отображение $\text{E}_1 \times \text{E}_2$ в E_3 называется *законом внешней композиции.*

Другими словами, каждой упорядоченной паре *(x, y)* ставится в соответствие элемент $z \in E_3$ и только один такой элемент.

Закон композиции будет внешним тогда и только тогда, когда

$$E_1 = E_2 = E_3$$

Примеры.

1. Пусть $E_1 = E_2 = R$ (множество действительных чисел); если в качестве закона выбрано обычное сложение +, то этот закон внутренний, так как сумма двух действительных чисел — всегда действительное число; действительно, имеем $E_3 = R$

2. Пусть P (E) — обычное множество всех подмножеств некоторого множества; тогда операции пересечения, объединения, разности и дизъюнктивной суммы определяют внутренние законы.

3. Если $E_1 = E_2 = R^+$ (множество неотрицательных чисел) и если закон состоит в вычислении разности $x — y = z$, $x, y \in R^+$, то получаем внешний закон, так как возможно, что $z \notin R^+$.

4. Если $E_1 = E_2$ — множество свободных векторов в плоскости и если символ × определяет векторное произведение (прямое произведение) двух векторов, то имеем закон внешней композиции.

Группоид. Упорядоченная пара, которая состоит из множества E и внутреннего закона композиции *, определенного на этом множестве всюду, называется *группомдом* и обозначается (E, *).

Примеры.

1. Закон композиции, представленный на рис. 3.22, задает группоид.

E \ E	A	B	C	D	E
A	B	A	D	D	C
B	C	B	B	A	E
C	A	A	A	B	C
D	C	A	B	B	C
E	E	C	A	A	D

Рис. 3.22

2. Примеры 1 и 2, которые приведены выше для иллюстрации понятия внутреннего закона композиции, определяют группоид.

3. Наибольший общий делитель и наименьшее общее кратное положительных целых чисел определяют внутренние законы композиции на множестве N_0 положительных целых чисел. Если $*_1$

обозначает наибольший общий делитель и $*_2$ — наименьшее общее кратное, то $(N_0, *_1)$ и $(N_0, *_2)$ являются группоидами.

3.17. Закон нечеткой внутренней композиции. Нечеткий группоид

Рассмотренные понятия можно в обобщенном виде перенести на нечеткие подмножества следующим образом.

Пусть E — универсальное множество и $A_{0\swarrow} \subset$ E. Обозначим множество нечетких подмножеств множества E через P (E). Тогда можно записать $A_{0\swarrow} \subset$ P (E). Мы уже видели, что если n = card E и m = card M конечные, то и P (E) конечно.

Теперь можно определить закон внутренней композиции на P (E), т.е. определить отображение из P (E) ×P (E) в P (E). Другими словами, каждой упорядоченной паре ($A_{0\swarrow}$, $B_{0\swarrow}$), где $A_{0\swarrow} \subset$ E, $B_{0\swarrow} \subset$ E, поставить в соответствие единственное нечеткое подмножество $C_{0\swarrow} \subset$ E. Если m и n конечные, то посредством этих условий описывают конечный группоид (и бесконечный группоид, если m или (и) n не конечные).

Определенные таким образом законы внутренней композиции и группоиды будут называться *законами нечеткой внутренней композиции* или нечеткими внутренними законами и *нечеткими группоидами*, Рассмотрим несколько примеров.

Пример 1. Пусть

$$E = \{A, B\} \tag{3.10}$$

и

$$M = \{0, 1/2, 1\}. \tag{3.11}$$

Обратившись к рис. 3.23, получим

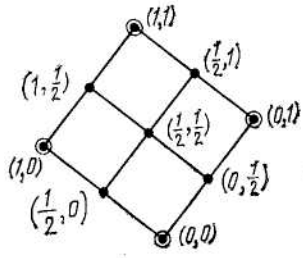


Рис. 3.23.

$$\mathcal{P}(\mathbf{E}) = \Big\{\{(A\,|\,0),\ (B\,|\,0)\},\ \Big\{(A\,|\,0),\Big(B\ \Big|\ \frac{1}{2}\Big)\Big\},\ \Big\{\Big(A\,\Big|\,\frac{1}{2}\Big),\ (B\,|\,0)\Big\},$$
$$\Big\{\Big(A\,\Big|\,\frac{1}{2}\Big),\ \Big(B\,\Big|\,\frac{1}{2}\Big)\Big\},\ \{(A\,|\,0),\ (B\,|\,1)\},\ \{(A\,|\,1),\ (B\,|\,0)\},$$
$$\Big\{\Big(A\,\Big|\,\frac{1}{2}\Big),\ (B\,|\,1)\Big\},\ \Big\{(A\,|\,1),\ \Big(B\,\Big|\,\frac{1}{2}\Big)\Big\},\ \{(A\,|\,1),\ (B\,|\,1)\}.$$

Для упрощения записи для $\underset{0\mathcal{L}}{X} \subset E$ вместо

$$\{(A\mid \mu_{\underset{0\mathcal{L}}{X}}(A)),\ (B\mid \mu_{\underset{0\mathcal{L}}{X}}(B))\}$$

будем писать

$$(\mu_{\underset{0\mathcal{L}}{X}}(A),\ \mu_{\underset{0\mathcal{L}}{X}}(B)).$$

Таким образом, {(A | 1/2), (B | 0)} будем записывать (1/2, 0). При этом обозначении таблица на рис. 3.24 представляет нечеткий группоид.

$\mathcal{P}(E)$ / $\mathcal{P}(E)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,0)$	$(0,1)$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(1,\frac{1}{2})$	$(0,1)$	$(0,1)$	$(1,\frac{1}{2})$	$(1,1)$	$(1,\frac{1}{2})$
$(0,\frac{1}{2})$	$(1,0)$	$(0,\frac{1}{2})$	$\frac{1}{2},0$	$(\frac{1}{2},1)$	$(0,0)$	$(1,0)$	$(0,1)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(\frac{1}{2},0)$	$(0,0)$	$(1,\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,1)$	$(1,\frac{1}{2})$	$(1,1)$	$(1,1)$	$(1,1)$	$(\frac{1}{2},\frac{1}{2})$
$(\frac{1}{2},\frac{1}{2})$	$(1,1)$	$(0,0)$	$(1,1)$	$(\frac{1}{2},1)$	$(1,0)$	$(1,0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,0)$
$(0,1)$	$(\frac{1}{2},\frac{1}{2})$	$(0,\frac{1}{2})$	$(1,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(1,0)$	$(\frac{1}{2},0)$	$(1,\frac{1}{2})$	$(\frac{1}{2},1)$
$(1,0)$	$(\frac{1}{2},0)$	$(0,0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(0,1)$	$(1,1)$	$(1,\frac{1}{2})$
$(\frac{1}{2},1)$	$(0,0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(0,\frac{1}{2})$	$(1,0)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(1,\frac{1}{2})$	$(0,0)$	$(\frac{1}{2},1)$	$(0,\frac{1}{2})$	$(0,0)$	$(1,\frac{1}{2})$	$(\frac{1}{2},1)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$
$(1,1)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,0)$	$(1,0)$	$(\frac{1}{2},1)$	$(0,\frac{1}{2})$	$(1,\frac{1}{2})$

Рис. 3.24

Пример 2. Если рассматриваемая операция * есть пересечение I и если $\underset{0\nearrow}{A} \subset$ E и $\underset{0\nearrow}{B} \subset$ E, то можно образовать группоид с нечеткими подмножествами $\underset{0\nearrow}{A}$ I $\underset{0\nearrow}{B}$ в качестве результата применения этой операции. То же справедливо для операций U и $\oplus$.

Построение нечеткого группоида. Для построения нечеткого группоида достаточно задать универсальное множество E, конечное или нет, образовать P (E) явно или нет и определить закон *, который каждой упорядоченной паре нечетких подмножеств ($\underset{0\nearrow}{A}, \underset{0\nearrow}{B}$) ставит в соответствие одно и только одно нечеткое подмножество $\underset{0\nearrow}{C}$ ($\underset{0\nearrow}{A}, \underset{0\nearrow}{B}, \underset{0\nearrow}{C} \subset \underset{0\nearrow}{E}$).

Рассмотрим несколько примеров.

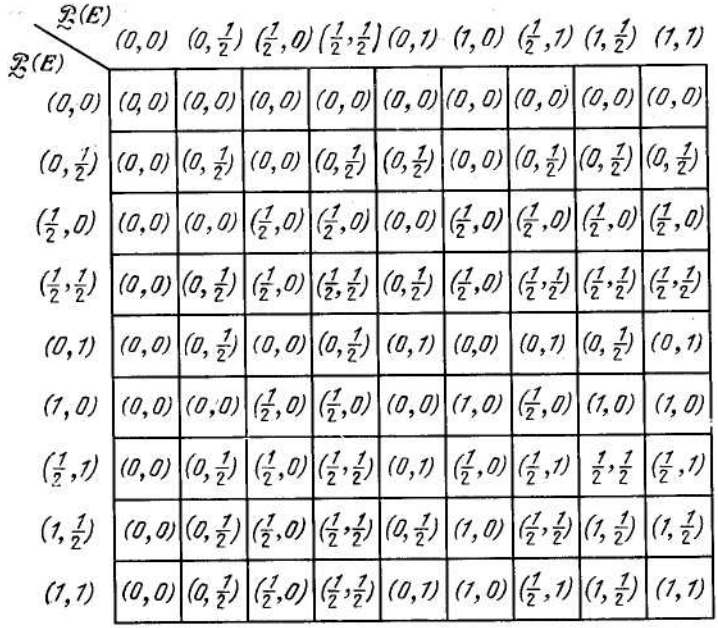
Пример 1. Рассмотрим еще раз (3.10) и (3.11) с законом

$$\underset{0\nearrow}{A} * \underset{0\nearrow}{B} = \underset{0\nearrow}{A} \text{ I } \underset{0\nearrow}{B}, \tag{3.13}$$

т.е.

$$\mu_{\underset{0\nearrow}{A} \text{I } \underset{0\nearrow}{B}} = \text{MIN} (\mu_{\underset{0\nearrow}{A}} (x), \ \mu_{\underset{0\nearrow}{B}} (x)) = \mu_{\underset{0\nearrow}{A}} (x) \wedge \mu_{\underset{0\nearrow}{B}} (x) . \tag{3.14}$$

Таким образом, мы построили группоид, представленный на рис. 3.25.



$\mathcal{P}(E)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,\frac{1}{2})$
$(\frac{1}{2},0)$	$(0,0)$	$(0,0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(0,0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$
$(\frac{1}{2},\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$
$(0,1)$	$(0,0)$	$(0,\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(0,1)$	$(0,0)$	$(0,1)$	$(0,\frac{1}{2})$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(0,0)$	$(1,0)$	$(\frac{1}{2},0)$	$(1,0)$	$(1,0)$
$(\frac{1}{2},1)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(\frac{1}{2},0)$	$(\frac{1}{2},1)$	$\frac{1}{2},\frac{1}{2}$	$(\frac{1}{2},1)$
$(1,\frac{1}{2})$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,\frac{1}{2})$	$(1,0)$	$(\frac{1}{2},\frac{1}{2})$	$(1,\frac{1}{2})$	$(1,\frac{1}{2})$
$(1,1)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$

Рис. 3.25

Пример 2. Попробуем определить «нечеткие положительные целые числа». Начнем из определения нечеткого числа $\underset{0}{1}$ с функцией принадлежности $\mu_{\underset{0}{1}}(n)$, произвольной, но такой, что

$$\sum_{n=0}^{\infty} \mu_{\underset{0}{1}}(n) = 1, \quad n = 0, 1,2,3,... \tag{3.15}$$

Например,

$$\underset{0}{1} = \{(0|0,1), (11\ 0,8), (2|0,l),...(N>2|0)\}. \tag{3.16}$$

Построим $\underset{0}{2}$ следующим образом:

$$\mu_{\underset{0}{2}}(0) = \mu_{\underset{0}{1}}(0) \cdot \mu_{\underset{0}{1}}(0) = (0,1) \cdot (0,1) = 0,01,$$

$$\mu_{\underset{0}{2}}(l) = \mu_{\underset{0}{1}}(0) \cdot \mu_{\underset{0}{1}}(l) + \mu_{\underset{0}{1}}(l) \cdot \mu_{\underset{0}{1}}(0) = (0,l) \cdot (0,8) + (0,8) \cdot (0,l) = 0,16,$$

$$\mu_{\underset{0}{2}}(2) = \mu_{\underset{0}{1}}(0) \cdot \mu_{\underset{0}{1}}(2) + \mu_{\underset{0}{1}}(l) \cdot \mu_{\underset{0}{1}}(l) + \mu_{\underset{0}{1}}(2) \cdot \mu_{\underset{0}{1}}(0) =$$

$$= (0,1) \cdot (0,1) + (0.8) \cdot (0,8) + (0,1) \cdot (0,1) = 0,66, \tag{3.17}$$

$\mu_{\underset{\sim}{2}}(3) = \mu_{\underset{\sim}{1}}(1) \cdot \mu_{\underset{\sim}{1}}(2) + \mu_{\underset{\sim}{1}}(2) \cdot \mu_{\underset{\sim}{1}}(1) = (0{,}8) \cdot (0{,}1) + (0{,}1) \cdot (0{,}8) = 0{,}16,$

$\mu_{\underset{\sim}{2}}(4) = \mu_{\underset{\sim}{1}}(2) \cdot \mu_{\underset{\sim}{1}}(2) = (0{,}1) \cdot (0{,}1) = 0{,}01,$

$\mu_{\underset{\sim}{2}}(N>4) = 0.$

Таким образом,

$$\underset{\sim}{2} = \{(0 \mid 0{,}01),\ (1 \mid 0{,}16),\ (2 \mid 0{,}66),\ (3 \mid 0{,}16),\ (4 \mid 0{,}01),\ ...,(N>4|0)\}. \quad (3.18)$$

Закончим построения на числе $\underset{\sim}{3}$, используя формулу, которая обобщает (3.17):

$$\mu_{A \underset{\sim}{*} B}(N) = \sum_{r=0}^{N} \mu_{A}(r) \cdot \mu_{B}(N-r) = \sum_{r=0}^{N} \mu_{B}(r) \cdot \mu_{A}(N-r). \quad (3.19)$$

В этом выражении можно узнать преобразование свертки, используемое в теории вероятностей и в преобразованиях линейных функций.

Для $\underset{\sim}{3}$ имеем

$$\mu_{\underset{\sim}{3}}(N) = \mu_{\underset{\sim}{2}} * \mu_{\underset{\sim}{1}}(N) = \sum_{r=0}^{N} \mu_{\underset{\sim}{2}}(r) \cdot \mu_{\underset{\sim}{1}}(N-r),\ N \leqslant 6. \quad (3.20)$$

Таким образом,

$$\underset{\sim}{3} = \{(0 \mid 0{,}001),\ (1 \mid 0{,}024),\ (2 \mid 0{,}195),\ (3 \mid 0{,}560),\ (4 \mid 0{,}195),$$
$$(5 \mid 0{,}024),\ (6 \mid 0{,}001).....(N > 6 \mid 0)\}. \quad (3.21)$$

Таким путем процесс построения продолжается далее. Отметим, что нечеткий характер построенных чисел проявляется все сильнее с ростом их значений.

Позднее мы познакомимся с некоторыми частными свойствами группоидов. Здесь же отметим, что построенные нами группоиды имеют следующие свойства:

$$(A * B) * C = A * (B * C) \text{ -ассоциативность}, \quad (3.22)$$

$$A * B = B * A \text{ - коммутативность}. \quad (3.23)$$

При этом $\mu_{\underset{\sim}{1}}(n)$ нужно выбирать такими, чтобы

$$\sum_{n=0}^{\infty} \mu_{\underset{\sim}{1}}(r) = 1.$$

Это условие отвечает использованию произведения - свертки (3.19).

Пример 3. Возьмем функцию принадлежности, которую можно рассматривать как закон распределения вероятностей. Рассмотрим два

нечетких подмножества $\underset{0/}{A} \subset \mathrm{R}$ и $\underset{0/}{B} \subset \mathrm{R}$, с помощью которых получим другие нечеткие подмножества (таким образом мы рассматриваем $\underset{0/}{A}$ и $\underset{0/}{B}$ как нечеткие множества, которые порождают бесконечное число других нечетких подмножеств). Пусть

$$\mu_{\underset{\sim}{A}}(x) = \frac{1}{\sqrt{2\pi\sigma_1^2}} e^{-\frac{(x-a)^2}{2\sigma_1^2}}, \quad a, \sigma_1 \in \mathbf{R}^+,$$

$$\mu_{\underset{\sim}{B}}(x) = \frac{1}{\sqrt{2\pi\sigma_2^2}} e^{-\frac{(x-b)^2}{2\sigma_2^2}}, \quad b, \sigma_2 \in \mathbf{R}^+.$$

Теперь рассмотрим следующий закон композиции:

$$\mu_{\underset{\sim}{A}*\underset{\sim}{B}}(x) = \int_{-\infty}^{\infty} \mu_{\underset{\sim}{A}}(t) \cdot \mu_{\underset{\sim}{B}}(x-t) \cdot dt = \int_{-\infty}^{\infty} \mu_{\underset{\sim}{B}}(t) \cdot \mu_{\underset{\sim}{A}}(x-t) \cdot dt =$$

$$= \frac{1}{\sqrt{2\pi(\sigma_1^2+\sigma_2^2)}} e^{-\frac{(x-a-b)^2}{2(\sigma_1^2+\sigma_2^2)}}. \tag{3.24}$$

Он определяет нечеткое число $\underset{0/}{A} * \underset{0/}{B}$.

Аналогично порождаются другие нечеткие числа:

$$\underset{0/}{A} * \underset{0/}{A}, \ \underset{0/}{B} * \underset{0/}{B}, \ \underset{0/}{A} * \underset{0/}{A} * \underset{0/}{A}, \ \underset{0/}{A} * \underset{0/}{A} * \underset{0/}{B}, ..., \ \underset{0/}{A}^r * \underset{0/}{B}^s, ...,$$

где верхние индексы указывают на то, что проведено r — 1 композиций нечеткого числа $\underset{0/}{A}$ и s — 1 композиций нечеткого числа $\underset{0/}{B}$.

Из двух нечетких чисел $\underset{0/}{A}$ и $\underset{0/}{B}$ можно образовать композиции

$$\underset{0/}{A}, \ \underset{0/}{B}, \ \underset{0/}{A} * \underset{0/}{A}, \ \underset{0/}{A} * \underset{0/}{B}, \ \underset{0/}{B} * \underset{0/}{B}, ..., \ \underset{0/}{A}^r * \underset{0/}{B}^s, ...$$

и множество

$$Q = \{ \underset{0/}{A}, \ \underset{0/}{B}, \ \underset{0/}{A} * \underset{0/}{A}, \ \underset{0/}{A} * \underset{0/}{B}, \ \underset{0/}{B} * \underset{0/}{B}, ..., \ \underset{0/}{A}^r * \underset{0/}{B}^s, ... \},$$

наделенное структурой группоида, который к тому же обладает свойствами ассоциативности и коммутативности, присущими закону (3.24).

3.18. Основные свойства нечетких группоидов

Пусть * есть закон внутренней композиции нечеткого группоида; определим несколько свойств группоидов. Группоид будет обозначаться
(P (E), *).

Коммутативность. Если для всех упорядоченных пар
$(A_{0/}, B_{0/}) \in$ P (E) × P (E) выполняется условие

$$A_{0/} * B_{0/} = B_{0/} * A_{0/},$$

то говорят, что закон внутренней композиции коммутативен; также говорят, что группоид коммутативен. Например, группоид на рис. 3.25 коммутативен, в то время как на рис. 3.24 - нет. Для примера на рис. 3.25 можно проверить, что
{(A|l/2), (B|1)} ∧ {(A|1), (B|0)}= {(A|1/2), (B|0)},
{(A|l), (B|0)} ∧ {(A|1/2), (B|1)} = {(A|l/2), (B|0)}.

Исходя из данного определения закона * для нечетких подмножеств, можно заключить, что если

$$\mu_{\underset{\sim}{A} * \underset{\sim}{B}}(x) = \mu_{\underset{\sim}{A}}(x) \odot \mu_{\underset{\sim}{B}}(x),$$

это из коммутативности для ⊙ следует коммутативность для * и наоборот. Очевидным примером служат выражения (3.13) и (3.14).

Ассоциативность. Если

$$\forall\ A_{0/}, B_{0/}, C_{0/} \subset E_{0/} : (A_{0/} * B_{0/}) * C_{0/} = A_{0/} * (B_{0/} * C_{0/}),$$

то говорят, что закон ассоциативный; говорят также, что группоид ассоциативен.

Так, группоид на рис. 3.25 ассоциативен, а на рис. 3.24 - нет. Можем это проверить, например, для группоида на рис. 3.25, используя сокращенное обозначение

((1/2, 1/2) ∧ (1, 0)) ∧ (1/2, 1) = (1/2, 0) ∧ (1/2, 1) = (1/2, 0),
(1/2, 1/2) ∧ ((1, 0) ∧ (1/2, 1)) = (1/2, 1/2) ∧ (1/2, 0) = (1/2, 0).

Исходя из данного определения закона для нечетких подмножеств, можно заключить, что если

$$(\mu_{A_{0/}}(x) \odot \mu_{B_{0/}}(x)) \odot (\mu_{C_{0/}}(x) = \mu_{A_{0/}}(x) \odot (\mu_{B_{0/}}(x) \odot \mu_{C_{0/}}(x)),$$

это из ассоциативности для ⊙ следует ассоциативность для * и наоборот.

Единичный элемент. В теории обычных множеств для рассматриваемого закона * выделяют особый элемент $e \in$ E, если он существует, такой, что

$$\forall\, a \in \mathrm{E} : e * a = a.$$

Этот элемент называют левой единицей. Аналогично элемент $e' \in \mathrm{E}$, если он существует, такой, что

$$\forall\, a \in \mathrm{E}: a*e' = a,$$

называется правой единицей.

Элемент, который есть одновременно и левой и правой единицей, называется *единицей.*

Если единичный элемент существует, то он единственный. Действительно, если бы существовал другой такой элемент ε, то мы имели бы

$$\varepsilon * e = e * \varepsilon = \varepsilon = e.$$

Аналогично можно определить единичный элемент в нечетком группоиде. Покажем сначала на примере, что это действительно возможно, а затем перейдем к общему определению. Рассмотрим пример на рис. 3.25. Очевидно, что элемент (1,1) будет одновременно как левой, так и правой единицей, т.е. просто единицей. Действительно, $\forall x \in \{0, 1/2, 1\}$ и $\forall y \in \{0, 1/2, 1\}$,

$$(1, 1) \wedge (x, y) = (x, y) \wedge (1, 1) = (x, y).$$

Будем говорить, что нечеткий группоид с законом композиции * обладает левой единицей $U_{0'}$, если

$$\forall\, A_{0'} \subset \mathrm{E}: U_{0'} * A_{0'} = A_{0'} \qquad (3.25)$$

и правой единицей $U_{0'}$', если

$$\forall\, A_{0'} \subset \mathrm{E}: A_{0'} * U_{0'}' = A_{0'}, \qquad (3.26)$$

и обладает единицей $U_{0'}$, если

$$\forall\, A_{0'} \subset \mathrm{E}: U_{0'} * A_{0'} = A_{0'} * U_{0'} = A_{0'}. \qquad (3.27)$$

В примере на рис. 3.25 представлен случай, когда нечеткий группоид обладает единицей. Теперь рассмотрим другой случай, когда нечеткий группоид не обладает единицей. Такая ситуация возникает в примере, рассматриваемом в (3.15)-(3.23). С помощью элемента $1_{0'}$ невозможно генерировать ни четкое подмножество, обладающее свойством (3.27), ни нечеткое подмножество, обладающее свойством (3.25) или (3.26).

Обратные элементы. Напомним, что понимается под обратным элементом в теории обычных множеств.

Рассмотрим закон, для которого существует единичный элемент *e*. Теперь пусть a и $\overline{a} \in \underline{E}$ - два элемента. Если

$$\overline{a} * a = e,$$

то говорят, что элемент $\overline{a}$ есть левый обратный элемент для *a.* Аналогично, если

$$a*\overline{a}\ ' = e,$$

то говорят, что $\overline{a}\ '$ есть правый обратный элемент для *a.* Наконец, если $\overline{a}\ ' = a$, то

$$\overline{a}\ *a = a*\overline{a}\ = e,$$

и говорят, что $\overline{a}$ есть обратный элемент для *a.*

В нечетком группоиде для каждого элемента можно попытаться определить обратный.

Обратимся опять к примеру на рис. 3.25. Мы уже видели, что здесь существует единица, а именно пара (1, 1). Очевидно, что имеется только один элемент, который в композиции с самим собой дает (1, 1); это элемент (1, 1).

Для всех остальных элементов, таких, что *(a, b)* ρ (1, 1) и (*a', b')* ρ (1, 1), имеем

$$(a, b) \wedge (a', b')\ \rho\ (1, 1).$$

Следовательно, в группоиде на рис. 3.25 каждый элемент не имеет обратного.

В более общем случае, когда в качестве закона * используется $\cup$ или $\cap$, обратный элемент не существует.

В случае $\cup$ существует единица, определямая условием $\forall x \in$ E, $\mu_{\underset{\sim}{A}_{0/}}(x)$=0; в случае $\cap$ существует единица, определямая условием $\forall x \in$ E, $\mu_{\underset{\sim}{A}_{0/}}(x)$=1. Но ни в одном из этих случаев, независимо от того, каково нечеткое подмножество $\underset{\sim}{A}_{0/}$, нельзя определить обратный элемент. Известно, что

$$(\text{условие } \forall x \in \text{E: } \mu_{\underset{\sim}{A}_{0/}}(x)=0 \Leftrightarrow (\underset{\sim}{A}_{0/} = \varnothing),$$

$$(\text{условие } \forall x \in \text{E: } \mu_{\underset{\sim}{A}_{0/}}(x)=1 \Leftrightarrow (\underset{\sim}{A}_{0/} = \text{E}).$$

Однако если $\varnothing$ принять за единицу для $\cup$, а E- в качестве единица для $\cap$, то это все равно не позволит определить обратные элементы; никакой элемент, скажем B, не может дать

$\underset{\sim}{A}_{0/} \cup \underset{\sim}{B}_{0/} = \varnothing$, за исключением случая $\underset{\sim}{B}_{0/} = \varnothing$ и $\underset{\sim}{A}_{0/} = \varnothing$;

$\underset{\sim}{A}_{0/} \cap \underset{\sim}{B}_{0/} = \text{E}$, за исключением случая $\underset{\sim}{B}_{0/} = \text{E}$ и $\underset{\sim}{A}_{0/} = \text{E}$.

Аналогично можно проверить, что для законов*

$$\underset{\sim}{\mathbf{A}} \oplus \underset{\sim}{\mathbf{B}} = (\overline{\underset{\sim}{\mathbf{A}}} \cap \underset{\sim}{\mathbf{B}}) \cup (\underset{\sim}{\mathbf{A}} \cap \overline{\underset{\sim}{\mathbf{B}}}),$$

$$\underset{\sim}{\mathbf{A}} \overline{\oplus} \underset{\sim}{\mathbf{B}} = (\overline{\underset{\sim}{\mathbf{A}}} \cup \underset{\sim}{\mathbf{B}}) \cap (\underset{\sim}{\mathbf{A}} \cup \overline{\underset{\sim}{\mathbf{B}}})$$

также нельзя определить обратные элементы.

(Для закона композиции $\underset{0\nearrow}{A} \oplus \underset{0\nearrow}{B}$ единицей является $\varnothing$. Если положить

$a = \mu_{\underset{0\nearrow}{A}}(x))$ и $b = \mu_{\underset{0\nearrow}{B}}(x)$ при $0<a<b<1$, то $a*b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$.

и мы никогда не получим $a * b = 0$; следовательно, не существует числа b, которое можно было бы поставить в соответствие числу a в качестве обратного, то же справедливо и для $\underset{0\nearrow}{A} \overline{\oplus} \underset{0\nearrow}{B}$).

Можно проверить, что это справедливо также для закона * :

$\underset{0\nearrow}{A} * \underset{0\nearrow}{B}$, определенного с помощью

$$\mu_{\underset{0\nearrow}{A}*\underset{0\nearrow}{B}}(x) = \mu_{\underset{0\nearrow}{A}}(x) \cdot \mu_{\underset{0\nearrow}{B}}(x)$$

или закона *:

$\underset{0\nearrow}{A} * \underset{0\nearrow}{B}$, определенного с помощью

$$\mu_{\underset{\%\%}{A*B}}(x) = \int_{-\infty}^{\infty} \mu_{\underset{\%\%}{A*B}}(x) = \mu_{\underset{\%}{A}}(x) \cdot \mu_{\underset{\%}{B}}(x) \cdot dt$$

Дистрибутивность. Пусть * и *' представляют собой два закона внутренней композиции, определенных на том же самом множестве E. Если

$$\forall \underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}}, \underset{\sim}{\mathbf{C}} \subset \mathbf{E} : \underset{\sim}{\mathbf{A}} * (\underset{\sim}{\mathbf{B}} *' \underset{\sim}{\mathbf{C}}) = (\underset{\sim}{\mathbf{A}} * \underset{\sim}{\mathbf{B}}) *' (\underset{\sim}{\mathbf{A}} * \underset{\sim}{\mathbf{C}}),$$

то говорят, что закон * *дистрибутивен слева* относительно закона *'. Аналогично, если

$$\forall \underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}}, \underset{\sim}{\mathbf{C}} \subset \mathbf{E} : (\underset{\sim}{\mathbf{A}} *' \underset{\sim}{\mathbf{B}}) * \underset{\sim}{\mathbf{C}} = (\underset{\sim}{\mathbf{A}} *' \underset{\sim}{\mathbf{C}}) * (\underset{\sim}{\mathbf{B}} *' \underset{\sim}{\mathbf{C}}),$$

то говорят, что закон * *дистрибутивен справа* относительно закона *'. Если закон * дистрибутивен относительно другого закона *' и слева и справа, то говорят, что он *дистрибутивен относительно* *'. Тогда можно записать

$$(\underset{\sim}{\mathbf{A}} *' \underset{\sim}{\mathbf{B}}) * (\underset{\sim}{\mathbf{C}} *' \underset{\sim}{\mathbf{D}}) = (\underset{\sim}{\mathbf{A}} * \underset{\sim}{\mathbf{C}}) *' (\underset{\sim}{\mathbf{A}} * \underset{\sim}{\mathbf{D}}) *' (\underset{\sim}{\mathbf{B}} * \underset{\sim}{\mathbf{C}}) *' (\underset{\sim}{\mathbf{B}} * \underset{\sim}{\mathbf{D}}).$$

Можно, например, проверить, что закон I дистрибутивен относительно U и, наоборот, закон U дистрибутивен относительно I. Для закона $\oplus$

$$\underset{\sim}{\mathbf{A}} \oplus \underset{\sim}{\mathbf{B}} = (\underset{\sim}{\mathbf{A}} \cap \overline{\underset{\sim}{\mathbf{B}}}) \cup (\overline{\underset{\sim}{\mathbf{A}}} \cap \underset{\sim}{\mathbf{B}})$$

относительно I или U свойство дистрибутивности не имеет места.

Обычное подмножество нечеткого множества, замкнутое относительно закона композиции. (Напомним, что нечеткие подмножества универсума E образуют множество, которое обозначается $\mathsf{P}_{0\swarrow}(E)$; поэтому, имея в виду нечеткие подмножества, сказать, что множество E наделено законом * или что этим законом наделено множество $\mathsf{P}_{0\swarrow}(E)$, значит, сказать одно и то же).

Пусть $\Delta \subset P(E)$, причем P (E) наделено законом *. Если для каждой упорядоченной пары $(A_{0\swarrow}, B_{0\swarrow}) \in \Delta \times \Delta$

$$A_{0\swarrow} * B_{0\swarrow} \in \Delta,$$

это говорят, что Δ замкнуто относительно *.

Рассмотрим, например, группоид, представленный на рис. 3.25. Можно проверить, что группоид

$\Delta_1 = \{ (0, 0), (0, 1/2), (1/2, 0)\}$ замкнутый,

$\Delta_2 = \{ (1/2, 1), (1, 1/2)\}$ незамкнутый.

$\mathfrak{P}(E)$ \ $\mathfrak{P}(E)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(0,1)$	$(1,\frac{1}{2})$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$	$(1,0)$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(\frac{1}{2},1)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(0,1)$	$(1,1)$	$(\frac{1}{2},1)$	$(1,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,\frac{1}{2})$	$(1,0)$	$(1,\frac{1}{2})$	$(1,1)$	$(1,0)$	$(1,1)$	$(1,\frac{1}{2})$	$(1,1)$
$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(1,1)$	$(\frac{1}{2},1)$	$(1,1)$	$(1,1)$
$(1,\frac{1}{2})$	$(1,\frac{1}{2})$	$(1,\frac{1}{2})$	$(1,\frac{1}{2})$	$(1,\frac{1}{2})$	$(1,1)$	$(1,\frac{1}{2})$	$(1,1)$	$(1,\frac{1}{2})$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$

Рис. 3.26

На рис. 3.26 представлен тот же группоид, что и на рис. 3.25, но наделенный законом $\cup$: группоид

$\Delta_1 = \{ (0, 0), (0, 1/2), (1/2, 0)\}$ незамкнутый,

$\Delta_2 = \{ (1/2, 1), (1, 1/2)\}$ незамкнутый,

$\Delta_3 = \{ (1/2, 1), (1, 1/2)(1, 1)\}$ замкнутый.

Интересно проследить, как получить замкнутые подмножества для примеров на рис. 3.25 и 3.26 с помощью диаграммы Хассе векторной решетки, представляющей P (E) (см. рис. 3.27).

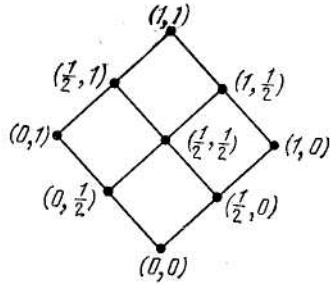


Рис. 3.27

Правило заключается в следующем. Чтобы некоторое подмножество из $P_{0\nu}$ (E) было замкнуто, оно должно содержать нижнюю грань любой пары ($A_{0\nu}$, $B_{0\nu}$), $A_{0\nu}, B_{0\nu} \in \Delta$. Например, подмножество { (0, 0), (0,1/2), (1/2, 0), (1,0)} замкнуто относительно $\cap$. Это можно видеть на рис. 3.27. С другой стороны, подмножество {(0, 1/2), (1/2, 0), (1/2, 1), (1, 1/2)} незамкнуто относительно $\cap$. Такое же правило применяют и для операции $\cup$, но только рассматривают верхние границы. Например, подмножество {(0, 0), (0, 1/2), (1/2, 0), (1, 0)} незамкнуто относительно $\cup$, а подмножество {(0, 1/2), (1, 0), (1, 1/2), (1,1)} - замкнуто.

Это свойство — общее для любого $P_{0\nu}$ (E), коким бы не было E, поскольку, как мы видели, $P_{0\nu}$ (E) всегда образует векторные решетки по отношению включения $A_{0\nu} \subset B_{0\nu}$ [т.е. $\mu_{A_{0\nu}}(x) \leq \mu_{B_{0\nu}}(x)$], для которого можно всегда рассматривать $A_{0\nu} \cap B_{0\nu}$ и $A_{0\nu} \cup B_{0\nu}$.

Подгруппоиды. Любое подмножество $\Delta \subset P_{0\not}(E)$, которое замкнуто относительно закона *, называется *подгруппотдом* группоида (E, *) и обозначается ($\Delta \subset$ E, *) или (Δ , *), если не возникает путаницы.

3.19. Нечеткие моноиды

Нечетким моноидом называется любой ассоциативный нечеткий группоид, имеющий единицу. Отметим, что много авторов не требуют в этом определении обязательного наличия единицы, но мы будем полагать это требование выполненным во всем, что будет рассматриваться ниже.

Если моноид к тому же имеет свойство коммутативности, его называют *коммутативным моноидом.*

Все следующие ниже нечеткие группоиды, которые определены с помощью их функций принадлежности, внутренние законы которых также определены и указаны ниже, являются моноидами и при том коммутативными.

1. $(\underset{\sim}{\mathcal{P}}(\mathbf{E}),\ \cap)$, где $\mu_{\underset{\sim}{A}\cap\underset{\sim}{B}}(x) = \mu_{\underset{\sim}{A}}(x) \wedge \mu_{\underset{\sim}{B}}(x),\ \underset{\sim}{A}, \underset{\sim}{B} \subset \mathbf{E}.$ (3.28)

Ассоциативность группоида ($P_{0\not}$ (E), I) очевидна. Единицей служит универсальное множество E.

2. $(\underset{\sim}{\mathcal{P}}(\mathbf{E}),\ \cup)$, где $\mu_{\underset{\sim}{A}\cup\underset{\sim}{B}}(x) = \mu_{\underset{\sim}{A}}(x) \vee \mu_{\underset{\sim}{B}}(x),\ \underset{\sim}{A}, \underset{\sim}{B} \subset \mathbf{E}.$ (3.29)

Ассоциативность группоида ($P_{0\not}$ (E), U) очевидна. Единицей служит $\varnothing$. Группоид

3. $(\underset{\sim}{\mathcal{P}}(\mathbf{E}),\ \cdot)$, где $\mu_{\underset{\sim}{A}\,.\,\underset{\sim}{B}}(x) = \mu_{\underset{\sim}{A}}(x) \cdot \mu_{\underset{\sim}{B}}(x),\ \underset{\sim}{A}, \underset{\sim}{B} \subset \mathbf{E},$ (3.30)

ассоциативный, с единицей E.

Группоид

4. $(\underset{\sim}{\mathcal{P}}(\mathbf{E}),\ \hat{+})$, где $\mu_{\underset{\sim}{A}\,\hat{+}\,\underset{\sim}{B}}(x) = \mu_{\underset{\sim}{A}}(x) + \mu_{\underset{\sim}{B}}(x) - \mu_{\underset{\sim}{A}}(x) \cdot \mu_{\underset{\sim}{B}}(x),$

$\underset{\sim}{A}, \underset{\sim}{B} \subset \mathbf{E},$ (3.31)

ассоциативный, с единицей $\varnothing$.

Уравнения (3.30) и (3.31) будут определять внутренние законы при условии, что M = [0, 1] или M = {0, 1}. Однако эти уравнения могут и не задавать внутреннего закона, например, для M = {0, 1/2, 1}, так как

(1/2) (1/2) = 1/4 $\notin$ M.

Группоид

$$5. \quad (\mathcal{P}(\mathbf{E}), \oplus), \text{ где } \mu_{\underset{\sim}{A} \oplus \underset{\sim}{B}}(x) = [\mu_{\underset{\sim}{A}}(x) \wedge (1 - \mu_{\underset{\sim}{B}}(x))] \vee \vee [\mu_{\underset{\sim}{B}}(x) \wedge (1 - \mu_{\underset{\sim}{A}}(x))], \quad \underset{\sim}{A}, \underset{\sim}{B} \subset \mathbf{E}, \tag{3.32}$$

ассоциативный, с единицей $\varnothing$.

Нечеткий моноид обозначается (E,*) или, что предпочтительнее, ($P_{0\nu}$(E), *).

Рассмотрим несколько нечетких группоидов, которые не является моноидами.

Пример 1. Пусть $A *_{0\nu} B$ определяется соотношением

$$\mu_{\underset{\sim}{A} * \underset{\sim}{B}}(x) = |\mu_{\underset{\sim}{A}}(x) - \mu_{\underset{\sim}{B}}(x)|.$$

Положим

$$a = \mu_{\underset{\sim}{A}}(x), \quad b = \mu_{\underset{\sim}{B}}(x), \quad c = \mu_{\underset{\sim}{C}}(x) \tag{3.33}$$

и обозначим

$$a \odot b = |a - b|.$$

Легко показать, что

$$(a \odot b) \odot c \neq a \odot (b \odot c),$$

т.е.

$$||a - b| - c| \neq |a - |b - c||.$$

Например, если

$$a = 0{,}3, \quad b = 0{,}5, \quad c = 0{,}9,$$

то имеем

$$|| a\text{-}b \text{ }|\text{-}c \text{ }| = || 0{,}3\text{-}0{,}5| - 0{,}9| = |0{,}2 - 0{,}9| = 0{,}7,$$
$$| a - | b\text{-}c \text{ }|| = | 0{,}3 - | 0{,}5 - 0{,}9|| = | 0{,}3 - 0{,}4 | = 0{,}1.$$

Этот коммутативный группоид не моноид, поскольку не обладает свойством ассоциативности.

Пример 2. Используя обозначение (3.33), положим

$$a \odot b = a + kb - ab, \quad k \in [0, 1].$$

Имеем

$(a \text{ e } b) \text{ e } c = (a + kb - ab) + kc - (a + kb - ab)c =$
$= a + kb + kc - ab - ac - kbc + abc,$
$a \text{ e } (b \text{ e } c) = a + k(b + kc\text{-}bc) - a(b + kc\text{-}bc) =$
$= a + kb + k^2c - ab - kac - kbc + abc,$

$(a \circ b) \circ c - a \circ (b \circ c) = kc - k^2c - ac + kac =$
$= c(1 - k)(k - a).$

Таким образом, свойство ассоциативности не выполняется, за исключением случая $k = 1$.

Нечеткий подмоноид. Пусть $(P_{0\nu}(E), *)$ — нечеткий моноид и $\Delta \subset P_{0\nu}(E)$ замкнуто относительно закона *, тогда Δ будет называться *нечетким подмоноидом* моноида и обозначаться $(\Delta, *)$.

Пример. Рассмотрим моноид $(P_{0\nu}(E), \cup)$ (рис. 3.28). На рис. 3.28 - 3.30 представлены подмоноиды этого моноида:

$\Delta = \{(0, 0), (1/2, 1)\}$,

$\Delta' = \{(0, 0), (0, 1/2), (1, 1/2)\}$,

$\Delta'' = \{(0, 0), (0, 1/2), (1/2, 0), (1/2, 1/2), (1/2, 1)\}$.

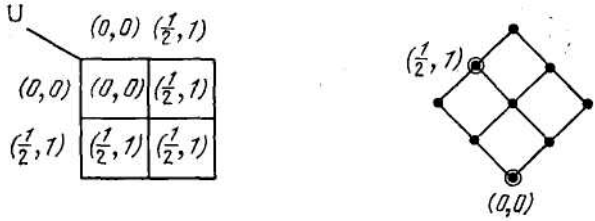


Рис. 3.28

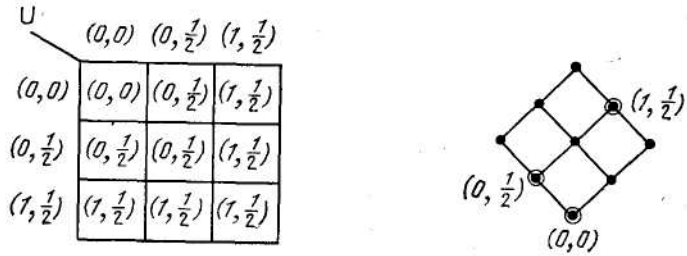


Рис. 3.29

∪	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(0,0)$	$(0,0)$	$(0,\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(0,\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(\frac{1}{2},0)$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$
$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$	$(\frac{1}{2},1)$

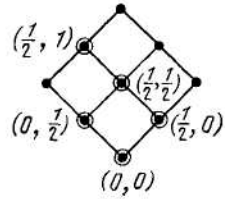


Рис. 3.30

Существует несколько других таких подмоноидов, которые читатель может сам перечислить как упражнения.

Конечно, все эти моноиды должны включать единицу (0, 0) [см. (3.29)].

Теорема. Если (Δ, *) и (Δ', *) — подмоноиды моноида ($P_{0\infty}$(E), *), то ($\Delta \cap \Delta'$, *) — подмоноид моноида ($P_{0\infty}$(E), *).

Доказательство. Очевидно, что для пересечения моноидов сохраняется единица и выполняется свойство ассоциативности. Теперь покажем, что $\Delta \cap \Delta'$ замкнуто относительно операции *.

Пусть $(A_{0\infty}, B_{0\infty}) \in \Delta \cap \Delta'$. Тогда $A_{0\infty} * B_{0\infty}$ по предположению принадлежит Δ и Δ' (поскольку в противном случае Δ или (и) Δ' не будут замкнутыми относительно *); но тогда $A_{0\infty} * B_{0\infty}$ принадлежит $\Delta \cap \Delta'$ и, значит, $\Delta \cap \Delta'$ замкнуто относительно *.

Для объединения $\cup$ моноидов свойство замкнутости относительно операции * в общем случае не выполняется.

Нечеткие группы. Можно задать следующий вопрос: существуют ли реально группы, которые являются нечеткими (необычными), если рассматривать операции $\cap$, $\cup, \cdot, \text{€}$, $\oplus$?

Известно, что группа представляет собой моноид, в котором для каждого элемента существует и при том единственный обратный элемент.

Дальше мы покажем, что необходимое условие для того, чтобы моноид ($P_{0\infty}$(E), *) имел групповую структуру, состоит в том, чтобы

M =[0, 1] было наделено групповой структурой для операции, соответствующей *. Более того, мы увидим, что в любом случае M=[0, 1] можно наделить групповой структурой с помощью некоторой операции °.

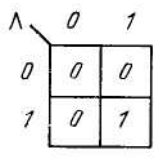
M = [0, 1] можно рассматривать как векторную решетку, которая состоит из единственной цепи, образующей полный порядок. Рассмотрим операции $\wedge$ (минимум), $\vee$ (максимум), • (произведение), € (алгебраическая сумма), $\oplus$ (дизъюнктивная сумма). Каждая из этих операций ассоциативна и для каждой существует единица, роль которой, в зависимости от случая, играет 0 или 1; однако почти одинаково для каждого случая легко доказать, что для каждой из этих операций не существует обратных элементов. Мы сделаем это для операції $\wedge$. Рассмотрим пару $(a, b) \in M \times M$, где M = [0, 1] и $0 < a < b < 1$. Единицей для операции $\wedge$ служит 1. Существует ли такое a или b, что

$$a \wedge b = 1?$$

Нет, не существуют, поскольку

$$a \wedge b = a < 1.$$

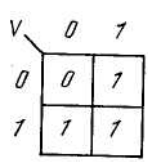
С другой стороны, если мы возьмем M={0, 1} , то обнаружим, что групповая структура возможна.



Это не группа. Есть единичный элемент 1, но 0 не имеет обратного элемента:

$0 \wedge 0 = 0$,
$0 \wedge 1 = 0$,
$1 \wedge 0 = 0$,
$1 \wedge 1 = 1$.

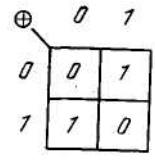
Рис. 3.31.



Это не группа. Есть единичный элемент 0, но 1 не имеет обратного элемента:

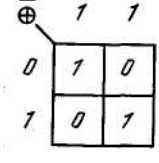
$0 \vee 0 = 0$,
$0 \vee 0 = 1$,
$1 \vee 0 = 1$,
$1 \vee 1 = 1$.

Рис. 3.32.



Это группа. Есть единичный элемент 0, 0 есть обратный элемент 0, 1 есть обратный элемент 1.

Рис. 3.33.



Это группа. Есть единичный элемент 1, 0 есть обратный элемент 0, 1 есть обратный элемент 1.

Так, на рис. 3.33 мы показали, что относительно операций $\wedge$ или $\vee$ группа не получается (и, следовательно, не получается группа относительно каждой из операций • и €, которые в булевом случая дают эквивалентные операции). И, наоборот, получаем группу, если берем операцию $\oplus$. Группа получится и в том случае, когда рассматривается операция $\overline{\oplus}$ (инверсная дизъюнктивная сумма). Отметим, что две группы $\oplus$ и $\overline{\oplus}$ оказываются изоморфными в результате перестановки элементов 0 и 1. Эти группы различаются по фактической реализации, но как абстрактные группы они одинаковы.

Отсюда следует, что если рассматривать каждую из операций I , U,·,€ , $\oplus$ и M= [0, 1], то на ($P_{0\not}$ (E), *) нельзя определить групповую структуру.

Для M = {0, 1} группу можно образовать только с операцией $\oplus$ (или, что то же, с $\overline{\oplus}$). В качестве примера рассмотрим обычную группу, образованнуь таким образом на

$$E = \{x_1, x_2, x_3\}.$$

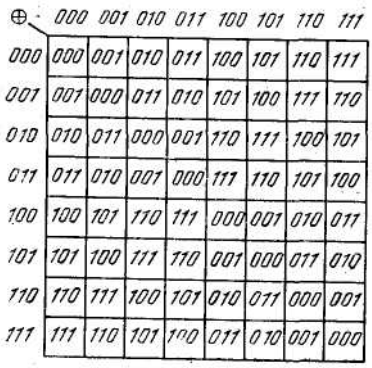
Если для упрощения записи положим

$$abc = \{ (x_2|a), (x_2|b), (x_3|c)\}$$

и при этом

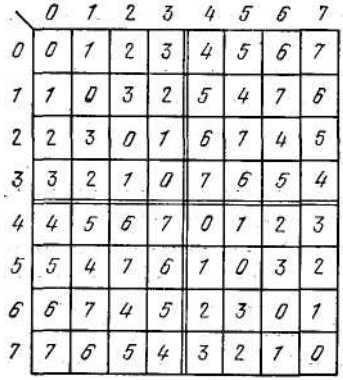
$$a,b,c \in \{0, 1\},$$

то получим группу, представленную на рис. 3.34. Единицей здесь служит элемент 000, и каждый элемент *abc* сам себе служит обратным. Эта группа изображена на рис. 3.35, где бинарные переменные *abc* заменены соответствующими им десятичными числами. На рисунке отчетливо видны некоторые свойства (подгруппоидов, латинских квадратов и т.д.), общие для этих групп, построенных с дизъюнктивной суммой $\oplus$.



⊕	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Рис. 3.34.



	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

Рис. 3.34.

Позже мы возвратимся к тому, что связано со структурами или конфигурациями множеств приналежностей М, какие мы обобщим, изучая другие вполне упорядоченные конфигурации для М.

3.20. Нечеткая внешняя композиция

Пусть E_1, E_2 и E_3— три множеств. Если каждой упорядоченной паре ($\underset{\sim}{A}_1$, $\underset{\sim}{A}_2$), $\underset{\sim}{A}_1 \subset E_1$, $\underset{\sim}{A}_2 \subset E_2$ можно поставить в соответствие одно и только одно подмножество $\underset{\sim}{A}_3 \subset E_3$, то это соответствие называется законом нечеткой внешней композиции при условии, что $E_3 \neq E_1$ или (и) $E_3 \neq E_2$. Если $E_3 = E_2 = E_2$, то закон внутренний.

Пример 1 — чисто дискретный. Пусть

$E_1 = \{A, B, C\}$, card $E_1 = 3$;
$M_1 = \{0, 1/4, 1/2, 3/4, 1\}$, card $M_1 = 5$;
$E_2 = \{a, b, c, d\}$, card $E_2 = 4$;
$M_2 = \{0, 1/2, 1\}$, card $M_2 = 3$;
$E_3 = \{\alpha, \beta\}$, card $E_2 = 2$;
$M_3 = \{0, 1/3, 2/3, 1\}$, card $M_3 = 4$.

Пусть $\underset{\sim}{A}_1 \subset E_1$ и $\underset{\sim}{A}_2 \subset E_2$; каждой упорядоченной паре ($\underset{\sim}{A}_1$, $\underset{\sim}{A}_2$) поставим в соответствие одно и только одно подмножество $\underset{\sim}{A}_3 \subset E_3$ с помощью таблицы. А именно, пусть

$\underset{\sim}{A}_1 = \{ (A|1/4), (B|1/2), (C|1)\}$ обозначается (1/4, 1/2, 1), (3.34)

$A_{\underset{\sim}{02}}$ ={(*a*|0), (*b*|1/2), (*c*|0), (*d*|l)} обозначается (0, 1/2, 0, 1). (3.35)
Предположим, что таблица этим двум подмножествам ставит в соответствие третье подмножество

$$A_{\underset{\sim}{03}} = \{ (\alpha\,|1/3), (\beta\,|1)\} \text{ обозначается } (1/3, 1).$$

Таблица будет содержать $5^3 \times 3^4 = 125 \times 81$ случаев. На рис. 3.36. приведен небольшой фрагмент этой таблицы.

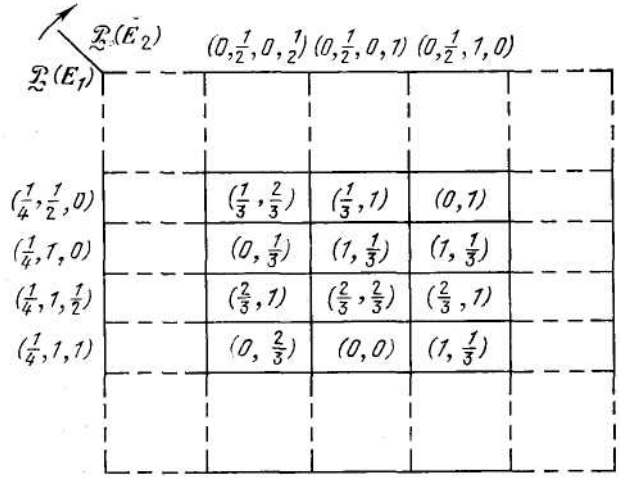


Рис. 3.36

Пример 2. Рассмотрим предыдущий пример для закона

$$\mu_{A_{\underset{\sim}{03}}}(\alpha) = \bigwedge_x \bigwedge_y [\, \mu_{A_{\underset{\sim}{01}}}(x) \vee \mu_{A_{\underset{\sim}{02}}}(y)] \tag{3.36}$$

$$\mu_{A_{\underset{\sim}{03}}}(\beta) = \bigvee_x \bigvee_y [\, \mu_{A_{\underset{\sim}{01}}}(x) \wedge \mu_{A_{\underset{\sim}{02}}}(y)]. \tag{3.37}$$

Получим другую композиционную таблицу, на основе которой вычислим элемент $P_{\underset{\sim}{04}}(E_1) \times P_{\underset{\sim}{04}}(E_2)$. Пусть $A_{\underset{\sim}{01}}$ задано соотношениям (3.34), а $A_{\underset{\sim}{02}}$ — соотношением (3.35). Имеем

$$\mu_{A_{\underset{\sim}{03}}}(\alpha) = \bigwedge_x [\bigwedge_y (1/4 \vee 0, 1/4 \vee 1/2, 1/4 \vee 0, 1/4 \vee 1), \bigwedge_y (1/2 \vee 0, 1/2 \vee$$

$$\vee\ 1/2, 1/2 \vee 0, 1/2 \vee 1), \bigwedge_y (1 \vee 0, 1 \vee 1/2, 1 \vee 0, 1 \vee 1)] =$$

$$= \bigwedge_x [\bigwedge_y (1/4, 1/2, 1/4, 1), \bigwedge_y (1/2, 1/2, 1/2, 1), \bigwedge_y (0, 1, 1, 1)1 =$$

$= \bigwedge_x (1/4, 1/2, 1)= 1/4,$

$\mu_{A_2}(\beta) = \bigvee_x [\bigvee_y (1/4 \wedge 0, 1/4 \wedge 1/2, 1/4 \wedge 0, 1/4 \wedge 1),$

$\bigvee_y (1/2 \wedge 0, 1/2 \wedge 1/2, 1/2 \wedge 0, 1/2 \wedge 1),$

$\bigvee_y (1 \wedge 0, 1 \wedge 1/2, 1 \wedge 0, 1 \wedge 1)] = \bigvee_x [\bigvee_y (0,1/4, 0, 1/4),$

$\bigvee_y (0, 1/2, 0, 1/2), \bigvee_y (0, 1/2, 0, 1) = \bigvee_x (1/4, 1/2, 1)=1.$

Таким образом,

$$\mu_{A_2}(\alpha)= 1/4 \text{ и } \mu_{A_2}(\beta)=1.$$

Подмножествам

$$A_1 = (A|1/4),(B|1/2), (C|1)$$

и

$$A_2 = (a|0),(b|1/2),(c|0),(d|1)$$

соответствует

$$A_2 = (\alpha\ |1/4), (\beta\ |1).$$

Замечание. Пусть в общем случае M_1 связано с E_1; M_2 связано с E_2, M_3 связано с E_3.

Если $P(E_3)$ формируется из $P(E_1)$ и $P(E_2)$ посредством закона *, определяемого условием

$$\mu_{A_3}(x,y) = \mu_{A_1}(x) \ e \ \mu_{A_2}(y) \qquad (3.38)$$

то M_3 будет выведено из M_1 и M_2 посредством формулы композиции (3.38). Так, для примера (3.36) и (3.37) очевидно, что

$$M_3=M_1 \cup M_{i!} = M_1= \{0, 1/4, 1/2, 3/4, 1\}.$$

Разумеется, (3.38) не может рассматриваться как общая формула. Ранее мы показали, как компонуются интервалы для операций $\wedge$ и $\vee$. Аналогичные процедуры можно применить для других случаев.

Пример 3. Построим нечеткий граф, вершины которого - нечеткие подмножества; этим будет определен закон внешней композиции.

Пусть

$$A \subset E,\ B \subset E.$$

Каждой упорядоченной паре $(A, B) \in P(E) \times P(E)$ будет поставлен в соответствие элемент, обозначенный

$$A * B = c(A, B).$$

Элемент *c* принимает свои значения во множестве Q, определенном операцией *.

Предположим, например, что

$$E = \{a,b\},$$

и

$$M= \{0,1/2,1\}.$$

Предположим также, что

$$c(\underset{\sim}{A}, \underset{\sim}{B}) = [\mu_{\underset{\sim}{A}}(a) \wedge \mu_{\underset{\sim}{B}}(a)] \vee [\mu_{\underset{\sim}{A}}(b) \wedge \mu_{\underset{\sim}{B}}(b)].$$

Эта функция определяет значение *c* в

$$Q=M= \{0, 1/2, 1\}.$$

Полученный нечеткий граф представлен на рис. 3.37.

*	(0,0)	(0,1/2)	(0,1)	(1/2,0)	(1/2,1/2)	(1/2,1)	(1,0)	(1,1/2)	(1,1)
(0,0)	0	0	0	0	0	0	0	0	0
(0,1/2)	0	1/2	1/2	0	1/2	1/2	0	1/2	1/2
(0,1)	0	1/2	1	0	1/2	1	0	1/2	1
(1/2,0)	0	0	0	1/2	1/2	1/2	1/2	1/2	1/2
(1/2,1/2)	0	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2
(1/2,1)	0	1/2	1	1/2	1/2	1	1/2	1/2	1
(1,0)	0	0	0	1/2	1/2	1/2	1	1	1
(1,1/2)	0	1/2	1/2	1/2	1/2	1/2	1	1	1
(1,1)	0	1/2	1	1/2	1/2	1	1	1	1

Рис. 3.37

Таким способом можно строить нечеткие графы, которые обладают специфическими свойствами, обусловленные их построением.

Достоинство представления внешнего закона композиции в виде нечеткого графа заключается в том, что элементы (вершины графа) — нечеткие подмножества одного и того же универсального множества.

Если расширить эту тему, то можно дать конкретные приложения, например, когда операцию * используют при оценке расстояния.

Пример 4. Вернемся к примеру 3 и предположим теперь, что $c(\underset{\sim}{A}, \underset{\sim}{B})$ - это относительное обобщенное расстояние Хемминга, которое определяется выражением

$$\delta(\underset{\sim}{A}, \underset{\sim}{B}) = 1/2\,(|\mu_{\underset{\sim}{A}}(a) - \mu_{\underset{\sim}{B}}(a)| + |\mu_{\underset{\sim}{A}}(b) - \mu_{\underset{\sim}{B}}(b)|).$$

Очевидно, что им задается закон внешней композиции (рис. 3.38).

*	$(0,0)$	$(0,\frac{1}{2})$	$(0,1)$	$(\frac{1}{2},0)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},1)$	$(1,0)$	$(1,\frac{1}{2})$	$(1,1)$
$(0,0)$	0	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	1
$(0,\frac{1}{2})$	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{3}{4}$
$(0,1)$	$\frac{1}{2}$	$\frac{1}{4}$	0	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	1	$\frac{3}{4}$	$\frac{1}{2}$
$(\frac{1}{2},0)$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	0	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{3}{4}$
$(\frac{1}{2},\frac{1}{2})$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$
$(\frac{1}{2},1)$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$
$(1,0)$	$\frac{1}{2}$	$\frac{3}{4}$	1	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	0	$\frac{1}{4}$	$\frac{1}{2}$
$(1,\frac{1}{2})$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0	$\frac{1}{4}$
$(1,1)$	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0

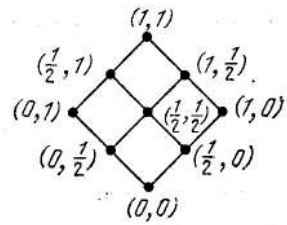


Рис. 3.38

Важность понятия закона внешней композиции нечетких подмножеств. Закон внешней композиции - очень важное понятие: им характеризуется любая система оценки отношений между нечеткими подмножествами одного и того же универсального множества, а фактически и между нечеткими подмножествами разных универсальных множеств. Множество, в котором $P_{0\mathcal{A}}(E_1) \times P_{0\mathcal{A}}(E_2)$ принимает свои значения, может быть обычным множеством или обычным множеством всех подмножеств, а в общем случае — множеством нечетких подмножеств (рис. 3.39).

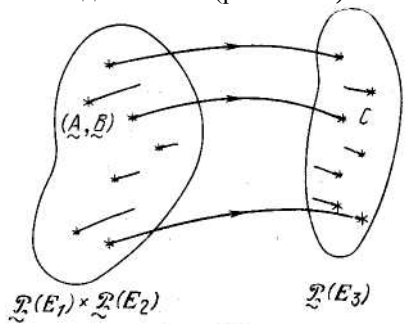


Рис. 3.39

Расстояние между сообщениями или нечеткими подмножествами одного и того же универсального множества — пример (и при том один из наиболее тривиальных), иллюстрирующий это общее понятие.

Отметим, что процедуры для предсказания или разработки открытий и изобретений, называемые биассоциацией, в значительной степени опираются на законы внешней композиции. Такие процедуры состоят в потому, что выбирают понятие А, которое характеризуется обычным или нечетким подмножеством семейства понятий E_1, и другое понятие *B,* которое характеризуется обычным или нечетким подмножеством другого (а в частности, и того же самого) семейства. Биассоциация А и В представляет собой внешний закон *, который позволяет получить новое понятие С, характеризующееся обычным или нечетким подмножеством третьего семейства (не исключается и случай совпадения этого семейства с одним из предыдущих) (рис. 3.40).

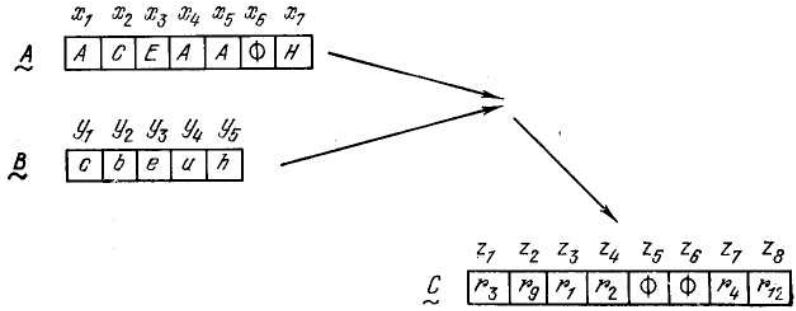


Рис. 3.40. Биассоциация

3.21. Операции на нечетких числах

Рассмотрим различные виды нечетких чисел.

Экспоненциальные нечеткие целые числа. Рассмотрим универсальное множество

$$E = R^+$$

и нечеткое подмножество $\underset{0}{\tilde{I}}_1$, такое, что

$$\mu_{\underset{\sim}{I}_1}(x) = \lambda\, e^{-\lambda x},\ x \in \mathbf{R}+.$$

Теперь определим $\underset{0}{\tilde{I}}_2$:

$$\mu_{\underset{\sim}{I}_2}(x) = \mu_{\underset{\sim}{I}_1}(x) * \mu_{\underset{\sim}{I}_1}(x) = \int_0^x \mu_{\underset{\sim}{I}_1}(t)\cdot\mu_{\underset{\sim}{I}_1}(x-t)\,dt =$$

$$= \int_0^x \lambda\, e^{-\lambda t}.\lambda\, e^{-\lambda(x-t)}\,dt = \lambda^2 x\, e^{-\lambda x}. \tag{3.39}$$

Далее определим $\underset{0}{\tilde{I}}_3$:

$$\mu_{\underset{\sim}{I}_3}(x) = \mu_{\underset{\sim}{I}_2}(x) * \mu_{\underset{\sim}{I}_1}(x) = \mu_{\underset{\sim}{I}_1}(x) * \mu_{\underset{\sim}{I}_2}(x) =$$

$$= \int_0^x \lambda^2 t\, e^{-\lambda t}.\lambda\, e^{-\lambda(x-t)}\,dt = \frac{\lambda^3 x^2 e^{-\lambda x}}{2}$$

и вообще $\underset{0}{\tilde{I}}_n$:

$$\mu_{\underset{\sim}{I}_n}(x) = \mu_{\underset{\sim}{I}_{n-1}}(x) * \mu_{\underset{\sim}{I}_1}(x) = \mu_{\underset{\sim}{I}_1}(x) * \mu_{\underset{\sim}{I}_{n-1}}(x) = \frac{\lambda^n x^{n-1} e^{-\lambda x}}{n!}.$$

Отметим, что

$$\underset{x}{\mathrm{MAX}}\, \mu_{\underset{\sim}{I}_n}(x) = \underset{x}{\mathrm{MAX}} \frac{\lambda^n x^{n-1} e^{-\lambda x}}{(n-1)!} = \lambda \frac{(n-1)^{(n-1)} e^{-(n-1)}}{(n-1)!},$$

и максимум достигается при

$$x = \frac{n-1}{\lambda}.$$

Таким образом, можно получить значения, которые приведено в табл. 3.1.

Нечеткие подмножества

$$\underset{\sim}{I}_0, \underset{\sim}{I}_1, \underset{\sim}{I}_2, \underset{\sim}{I}_3, \ldots, \underset{\sim}{I}_n, \ldots\ldots$$

называются *экспоненциальными нечеткими целыми числами*, $\underset{\sim}{I}_0$ — экспоненциальной нечеткой единицей, $\underset{\sim}{I}_1$ — экспоненциальной нечеткой двойкой и т.д.

Таблица 3.1

$\underset{\sim}{I}_i$	$\mu_{\underset{\sim}{I}_i}(x)$	Абсцисса максимума	Ордината максимума
$\underset{\sim}{I}_1$	$\lambda e^{-\lambda x}$	$x=0$	λ
$\underset{\sim}{I}_2$	$\lambda^2 x e^{-\lambda x}$	$x=\frac{1}{\lambda}$	λe^{-1}
$\underset{\sim}{I}_3$	$\frac{\lambda^3 x^2 e^{-\lambda x}}{2}$	$x=\frac{2}{\lambda}$	$\frac{\lambda 2^2 e^{-2}}{2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\underset{\sim}{I}_n$	$\frac{\lambda^n x^{n-1} e^{-\lambda x}}{(n-1)!}$	$x=\frac{n-1}{\lambda}$	$\lambda \frac{(n-1)^{(n-1)} e^{-(n-1)}}{(n-1)!}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

(3.40)

Операция композиции, определенная соотношением (3.39), ассоциативна и коммутативна; следовательно, множество нечетких подмножеств

$$\underset{\sim}{I}_0, \underset{\sim}{I}_1, \underset{\sim}{I}_2, \underset{\sim}{I}_3, \ldots, \underset{\sim}{I}_n, \ldots\ldots$$

образует ассоциативный и коммутативный группоид.

Кроме того, этот группоид имеет единицу, которую обозначим $\underset{\sim}{I}_0$ и которая определяется функцией принадлежности

$$\mu_{\underset{\sim}{I}_0}(x) = \delta(x),$$

где $\delta(x)$ — функция Дирака, для которой

$$\lim_{\varepsilon \to 0} \int_0^{\varepsilon} \delta(x)\, dx = 1.$$

Действительно, для $I_{0\sim}$ имеем

$$\mu_{\tilde{I}_r}(x) * \mu_{\tilde{I}_0}(x) = \mu_{\tilde{I}_0}(x) * \mu_{\tilde{I}_r}(x) = \int_0^r \mu_{\tilde{I}_r}(x) \cdot \delta(x-t)\, dt = \mu_{\tilde{I}_r}(x).$$

Будем считать, что построенное множество нечетких подмножеств пополнено $I_{0\sim}$.

Моноид

$$I_{0\sim},\ I_{1\sim}, I_{2\sim}, I_{3\sim}, \ldots, I_{n\sim}, \ldots$$

изоморфен моноиду натуральных чисел

$$0, 1, 2, \ldots, n, \ldots$$

Относительно (3.40) заметим также, что абсциссы максимумов каждого из экспоненциальных нечетких целых чисел следуют друг за другом с интервалом, равным $1/\lambda$.

Геометрические нечеткие целые числа. Рассмотрим универсальное множество

$$E = N$$

и нечеткое подмножество $J_{1\sim}$, такое, что

$$\mu_{\tilde{J}_1}(x) = a(1-a)^{x-1},\ a \in \mathbf{R}^+;\ 0 < |a| < 1;\ x = 1, 2, 3, \ldots$$

Затем определим $J_{2\sim}$ следующим образом:

$$\mu_{\tilde{J}_2}(x) = \mu_{\tilde{J}_1}(x) * \mu_{\tilde{J}_1}(x) = \sum_{t=1}^{x-1} \mu_{\tilde{J}_1}(t) \cdot \mu_{\tilde{J}_1}(x-t) = \sum_{t=1}^{x-1} a(1-a)^{t-1} \times$$

$$\times\, a(1-a)^{x-t-1} = a^2(1-a)^{x-2} \sum_{t=1}^{x-1} 1 = (x-1)\, a^2 (1-a)^{x-2},\ x = 2,3,4,\ldots$$

Теперь определим $J_{3\sim}$:

$$\mu_{\tilde{I}_3}(x) = \mu_{\tilde{J}_2}(x) * \mu_{\tilde{J}_1}(x) = \mu_{\tilde{J}_1}(x) * \mu_{\tilde{J}_2} =$$

$$= \sum_{t=2}^{x-1} \mu_{\tilde{J}_2}(t) \cdot \mu_{\tilde{J}_1}(x-t) = \sum_{t=2}^{x-1} (t-1)\, a^2 (1-a)^{t-2} \cdot a(1-a)^{x-t-1} =$$

$$= a^3 (1-a)^{x-3} \sum_{t=2}^{x-1} (t-1) =$$

$$= \frac{(x-2)(x-1)}{2}\, a^3 (1-a)^{x-3},\ x = 3,4,5,\ldots$$

Аналогично в общем случае получаем

$$\mu_{\underset{\sim}{J}_r}(x) = C_{x-1}^{x-r} \cdot a^r \cdot (1-a)^{x-r}.$$

Абсциссы максимумов — это $x = r, r+1, \ldots$ (табл. 3.2).

Таблица 3.2

$\underset{\sim}{J}_i$	$\mu_{\underset{\sim}{J}_i}(x)$	Абсцисса максимума
$\underset{\sim}{J}_1$	$a(1-a)^{x-1}$	$x=1$
$\underset{\sim}{J}_2$	$(x-1)\,a^2(1-a)^{x-2}$	$\frac{1}{a} \leqslant x \leqslant 1+\frac{1}{a}$
$\underset{\sim}{J}_3$	$\frac{(x-2)(x-1)}{2}\,a^3(1-a)^{x-3}$	$\frac{2}{a} \leqslant x \leqslant 1+\frac{2}{a}$
$\vdots$	$\vdots$	$\vdots$
$\underset{\sim}{J}_n$	$C_{x-1}^{x-n}\,a^n(1-a)^{x-n}$	$\frac{n-1}{a} \leqslant x \leqslant 1+\frac{n-1}{a}$
$\vdots$	$\vdots$	$\vdots$

(3.42)

Отметим, что максимум $J_{0\underset{\sim}{2}}$ может достигаться не только на одной точке, а точка x максимума не обязательно равна n — все зависит от значения параметра a.

Нечеткие подмножества

$$J_{0\underset{\sim}{1}}, J_{0\underset{\sim}{2}}, J_{0\underset{\sim}{3}}, \ldots, J_{0\underset{\sim}{n}}, \ldots (3...41)$$

называются *геометрическими нечеткими целыми числами.*

$J_{0\underset{\sim}{1}}$ называется геометрической единицей (1) и т.д.

Множество нечетких подмножеств (3.41) также образуют коммутативный моноид. Это моноид с единицей, которую мы обозначим $J_{0\underset{\sim}{0}}$, и для нее

$$\mu_{J_0}(x)=1, \; x=0,$$
$$= 0, \; x= 1,2,3,...$$

Можно проверить справедливость соотношения

$$\mu_{\underset{\sim}{J}_r}(x) * \mu_{\underset{\sim}{J}_0}(x) = \mu_{\underset{\sim}{J}_0}(x) * \mu_{\underset{\sim}{J}_r}(x) = \mu_{\underset{\sim}{J}_r}(x).$$

Между $J_{0\underset{\sim}{0}}, J_{0\underset{\sim}{1}}, J_{0\underset{\sim}{2}}, J_{0\underset{\sim}{3}}, \ldots, J_{0\underset{\sim}{n}}, \ldots$ и множеством N натуральных чисел также существует изоморфизм.

Относительно выражения (3.42) заметим, что абсциссы максимумов всех этих геометрических нечетких целых чисел следуют друн за лругом с интервалом, который зависит от *a*.

С помощью подобных процедур можно определить другие нечеткие натуральные числа, которые рассматриваются в вероятностных законах, например, в биномиальных законах, законах Пуассона, отрицательных биномиальных или прямоугольных распределениях, нормальных, эйлерових (гамма) распределениях и т.д.

Здесь мы ограничимся гауссовыми натуральными числами (нормальный закон).

Гауссовы нечеткие целые числа. Рассмотрим универсальное множество

$$E = R$$

и нечеткое подмножество $\underset{\sim}{K}_1$, такое, что

$$\mu_{\underset{\sim}{K}_1}(x) = \frac{1}{\sqrt{2\pi\sigma_1^2}} e^{-\frac{(x-1)^2}{2\sigma_1^2}}.$$

Определим $\underset{\sim}{K}_2$

$$\mu_{\underset{\sim}{K}_2}(x) = \mu_{\underset{\sim}{K}_1}(x) * \mu_{\underset{\sim}{K}_1}(x) = \int_0^x \mu_{\underset{\sim}{K}_1}(t) \cdot \mu_{\underset{\sim}{K}_1}(x-t)\, dt =$$

$$= \frac{1}{\sqrt{4\pi\sigma_1^2}} \cdot e^{-\frac{(x-2)^2}{4\sigma_1^2}},$$

и, продолжая этот процесс выписывания $\mu_{\underset{\sim}{K}_r}$ для $\underset{\sim}{K}_2, \underset{\sim}{K}_4$,…, $\underset{\sim}{K}_r$ получим

$$\mu_{\underset{\sim}{K}_r}(x) = \frac{1}{\sqrt{2\pi r\sigma_1^2}} \cdot e^{-\frac{(x-r)^2}{2r\sigma_1^2}}.$$

Тогда можно составить табл. 3.3.

Нечеткие подмножества

$$\underset{\sim}{K}_1, \underset{\sim}{K}_2, \underset{\sim}{K}_3, \ldots, \underset{\sim}{K}_r, \ldots$$

называются *гауссовыми нечеткими целыми числами.*

В действительности мы здесь также имеем дело с коммутативным моноидом с единицей $\underset{\sim}{K}_0$, которая определена условием

$$\mu_{\underset{\sim}{K}_0}(x) = \delta(x),$$

где $\delta(x)$ - симметричная функция Дирака, т.е. такая функция, что

$$\lim_{\varepsilon \to 0} \int_{x=-\varepsilon}^{\varepsilon} \delta(x)\, dx = 1.$$

Таким образом, мы опять имеем изоморфизм из N, но на этот раз абсциссы максимумов $\mu_{K_{0\Gamma}}(x)$ соответственно равны значениям рассмотренного целого числа *r*.

Таблица 3.3

$\underset{\sim}{K}_i$	$\mu_{\underset{\sim}{K}_i}(x)$	Абсцисса максимума	Ордината максимума
$\underset{\sim}{K}_1$	$\frac{1}{\sqrt{2\pi\sigma_1^2}} \cdot e^{-\frac{(x-1)^2}{2\sigma_1^2}}$	1	$\frac{1}{\sqrt{2\pi\sigma_1^2}}$
$\underset{\sim}{K}_2$	$\frac{1}{\sqrt{4\pi\sigma_1^2}} \cdot e^{-\frac{(x-2)^2}{4\sigma_1^2}}$	2	$\frac{1}{\sqrt{4\pi\sigma_1^2}}$
$\underset{\sim}{K}_3$	$\frac{1}{\sqrt{6\pi\sigma_1^2}} \cdot e^{-\frac{(x-3)^2}{6\sigma_1^2}}$	3	$\frac{1}{\sqrt{6\pi\sigma_1^2}}$
⋮	⋮	⋮	⋮
$\underset{\sim}{K}_r$	$\frac{1}{\sqrt{2\pi r\sigma_1}} \cdot e^{-\frac{(x-r)^2}{2r\sigma_1^2}}$	r	$\frac{1}{\sqrt{2\pi r\sigma_1^2}}$
⋮	⋮	⋮	⋮

Гауссовы нечеткие целые числа имеют следующее важное свойство: зависимость абсциссы максимума, которая является также средним значением от дисперсии, постоянна:

$$\frac{r}{r\sigma_1^2} = \frac{1}{\sigma_1^2} = C.$$

(Средним заначенням случайной величины ξ_r с плотностью распределения, равной $\mu_{K_{0\Gamma}}(x)$).

Таким образом, чем большее нечеткое число $K_{0\Gamma}$ (т.е. чем больше *r)*, тем большая его дисперсия, т.е. больше его нечеткость, но что касается *r*, то относительная нечеткость постоянна.

Микромодуль 13.
Идивидуальные тестовые задачи

1. Составьте таблицу, которая представляет собой нечеткий группоид, такой, что

$$\mathbf{E}=\{a,\ b\},\quad \mathbf{M}=\left\{0,\ \frac{1}{3},\ \frac{2}{3},\ 1\right\},$$

$$\mu_{\underset{\sim}{A*B}}(x)=\mu_{\underset{\sim}{A}}(x)\ \vee\ \mu_{\underset{\sim}{B}}(x).$$

2. Нечеткий группоид определен таблицей

*	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,1)	(0,0)
(1,0)	(1,1)	(1,0)	(0,0)	(0,1)

задающей операцию * относительно

E= {A, B} и M= {0, 1}.

В таблице {(A|α), (B|β)} записано как (α, β).

1. Ассоциативный ли этот группоид?
2. Имеет ли он единицу?
3. Если ответ положительный, т.е. группоид есть моноид, то каковы его подмоноиды?
4. Для каждой ли упорядоченной пары (α, β) существует обратная ей, и если ответ положительный, т.е. группоид есть группа, то каковы ее подгруппы?

3. Таблица

*	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

определяет групповую операцию *. Выразите эту операцию * только с помощью символов $\cap$ (пересечение), $\cup$ (объединение) и $^-$ (дополнение). В таблице пара {(A|α), (B|β)} представлена как (α, β).

Для этой операции * опишите группу, которая соответстует семейству множеств

$$E = \{A, B, C\}$$

(вместо E = {A, B}).

4. Заданы нечеткие группоиды ($P_{0/}$ (E), *), где M = [0, 1] - функция принадлежности универсального множества E:

1. $\mu_{\underset{\sim}{A}*\underset{\sim}{B}}(x) = (1-\mu_{\underset{\sim}{A}}(x)) \wedge (1-\mu_{\underset{\sim}{B}}(x))$,
2. $\mu_{\underset{\sim}{A}*\underset{\sim}{B}}(x) = (\mu_{\underset{\sim}{A}}(x)\cdot\mu_{\underset{\sim}{B}}(x)) \wedge [(1-\mu_{\underset{\sim}{A}}(x))\cdot(1-\mu_{\underset{\sim}{B}}(x))]$,
3. $\mu_{\underset{\sim}{A}*\underset{\sim}{B}}(x) = [(1-\mu_{\underset{\sim}{A}}(x))\cdot\mu_{\underset{\sim}{B}}(x)] \hat{+} [(1-\mu_{\underset{\sim}{B}}(x))\cdot\mu_{\underset{\sim}{A}}(x)]$,

где операция $\hat{+}$ такая, что $a \hat{+} b = a + b - a\cdot b$. Какие из этих нечетких группоидов а) коммутативные, б) ассоциативные, в) обладают единицей, и если она существует, то определите ее; г) какие из них таковы, что каждое нечеткое подмножество имеет себе обратное?

5. Определите следующие законы внешней композиции, где

$$\mathbf{E} = \{a, b\},\ \mathbf{M} = \{0, 1/2, 1\},$$
$$(\underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}}) \in \underset{\sim}{\mathscr{P}}(\mathbf{E}) \times \underset{\sim}{\mathscr{P}}(\mathbf{E}),\ x, y \in \mathbf{E},$$

и составьте таблицы этих законов

а) $c(\underset{\sim}{\mathbf{A}}, \underset{\sim}{\mathbf{B}}) = 1/2 \sqrt{(\mu_{\underset{\sim}{A}}(a)-\mu_{\underset{\sim}{B}}(a))^2+(\mu_A(b)-\mu_{\underset{\sim}{B}}(b))^2}$,

б) $\underset{\sim}{\mathbf{C}} \subset \mathbf{E}' = \{X, Y\}$, $\underset{\sim}{\mathbf{C}} = \underset{\sim}{\mathbf{A}} * \underset{\sim}{\mathbf{B}}$,

$\mu_{\underset{\sim}{C}}(X) = \mu_{\underset{\sim}{A}}(x) \wedge \mu_{\underset{\sim}{B}}(y)$, $\mu_{\underset{\sim}{C}}(Y) = \mu_{\underset{\sim}{A}}(x) \vee \mu_{\underset{\sim}{B}}(y)$.

Список литературы

1. Горбатов В.А. Основы дискретной математики. – М.: Высшая школа, 1986.
2. Коршунов Ю.М. Математические основы кибернетики. – М.:Энергия, 1980.
3. Кузнецов О.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. – М.:Энергия, 1980.
4. Кук Д., Бейз Г. Компьютерная математика.– М.: Наука, 1990.
5. Сигорский В.П. Математический аппарат инженера.-К.: Техніка, 1977.
6. Кузичев А.С. Диаграммы Венна.– М.: Наука, 1968.
7. Кононюк А.Ю. Вища математика. У 2 ч. Ч.1, - К:Кольори, 2007.
8. Аверкин А.Н., Батыршин И.З. и др. Нечеткие множества в моделях управления и икусственного интелекта.– М.: Наука, 1986.
9. Кофман А. Введение в теорию нечетких множеств.– М.: Радио и связь, 1982.
10. Кофман А. Введение в прикладную комбинаторику.– М.: Наука, 1975.
11. Згуровский М.З. Интегрированные системы оптимального управления и проектирования.- К.: Вища школа, 1990.
13. Минский М. Фреймы для представления знаний. – М.:Энергия, 1979.
14. Вильсон А. Дж. Энтропийные методы моделирования сложных систем.– М.: Наука, 1978.
15. В.Ю. Юрков, О.В. Лукина /Прикладная геометрия, вып. 8, N 18 (2006), стр. 9-36.
16. И.И. Ежев, А.В. Скороход, М.И. Ядренко. Элементы комбинаторики.-М.: Наука, 1977.
17. Алгебраическая теория автоматов, языков и полугрупп. Под ред. М.А. Арбиба. – М.: Статистика, 1975.
18. Минк Х. Перманенты. М.: Мир, 1982.
19. Холл. М. М.: Мир, 1970.
20. Борисов А. Н. Некоторые обучающиеся алгоритмы диагностики систем с размытыми классами состояний. — Техническая кибернетика. — Рига, 1970.
21. Борисов А. Н., Алексеев А. В. Нечеткие алгоритмы в ситуационных моделях управления организационными системами. —

В кн.: Методика построения систем ситуационного управления /Науч. совет АН СССР по комплексной проблеме «Кибернетика». — М., 1978, с. 3—10.

22. Борисов А. Н., Аппен Е. П. Оценка возможных характеристик при анализе альтернатив. — В кн.: Методы принятия решений в условиях неопределенности. — Рига: РПИ, 1980, с. 94—100.

23. Борисов А. Н., Голендер В. Е. Оптимальное разделение размытых образов — Методы и средства технической кибернетики. — Рига: РПИ, 1969, вып. 5, с. 32—38.

24. Борисов А. Н., Корнеева Г. В. Лингвистический подход к построению моделей принятия решений в условиях неопределенности. — В кн.: Методы принятия решений в условиях неопределенности. — Рига: РПИ, 1980, с. 4—12.

24. Борисов А. Н., Крумберг О. А. Анализ решений при выборе технологических объектов. — Там же, с. 127—134.

Научно-практическое издание

Кононюк Анатолий Ефимович

Дискретная математика

Книга 4
Алгебры
Часть 1

Авторская редакция

Подписано в печать 21.01.2011 г.
Формат 60х84/16.
Усл. печ. л. 16,5. Тираж 300 экз.

Издатель и изготовитель:
Издательство «Освита Украины»
04214, г. Киев, ул. Героев Днепра, 63, к. 40
Свидетельство о внесении в Государственный реестр
издателей ДК №1957 от 23.04.2009 г.
Тел./факс (044) 411-4397; 237-5992
E-mail: osvita2005@ukr.net, www.rambook.ru