П.Д. Варбанец О.В. Савастру

ЛИНЕЙНАЯ АЛГЕБРА
часть 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ОДЕССКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
имени И.И.МЕЧНИКОВА
ИНСТИТУТ МАТЕМАТИКИ, ЭКОНОМИКИ И МЕХАНИКИ

П.Д. Варбанец О.В. Савастру

ЛИНЕЙНАЯ АЛГЕБРА
часть 1

Одеса - 2013

Линейная Алгебра, часть 1: учебное пособие для студентов 1 курса специальностей "прикладная математика"и "компьютерная инженерия".– Одесса, 2013.– 130 стр.

Составители:
Варбанец П.Д., д.ф.-м.н., профессор кафедры компьютерной алгебры и дискретной математики ИМЭМ
Савастру О.В., к.ф.-м.н., доцент кафедры компьютерной алгебры и дискретной математики ИМЭМ

Рецензенты:
Евтухов В.М., д.ф.-м.н., профессор кафедры дифференциальных уравнений ИМЭМ
Кореновский А.А., д.ф.-м.н., профессор кафедры математического анализа ИМЭМ

Рекомендовано к печати Ученым советом Института математики, экономики и механики Одесского национального университета им. И. И. Мечникова, протокол № 4 от 18 мая 2011 года

Оглавление

1 Основные алгебраические образования

1.1 Отображения

Одним из самых основных понятий современной математики является понятие *отображение* множества U во множество W.

Определение. *Отображением f множества U во множество V называется правило, сопоставляющее каждому элементу $u \in U$ определенный (единственный) элемент $v \in V$. (Иногда пишут $v = f(u)$ или fu). Термины «преобразование », «функция», «функционал» будут использоваться нами как синонимы слова «отображение» (это в каждой конкретной обстановке — дань традиции).*

Часто символически отображение мы будем записывать в виде

$$f : U \mapsto V \text{ или } f : U \xrightarrow{f} V.$$

Определение. *Образом отображения называется множество всех элементов $f(u)$, когда u пробегает все множество U , и обозначается $\mathfrak{Im} f$ или $\mathfrak{Im} U$.*

Ясно, что

$$\mathfrak{Im} f = \{f(u) | u \in U\} = f(U) \in V.$$

($\mathfrak{Im} f$ - сокращение от $\mathfrak{Image}$).

Определение. *Отображение f называется **отображением на** (или сюръективным (surjective) отображением), если $\mathfrak{Im} f = V$.*

Определение. *Отображение f называется **инъективным** (injective), если из $u \neq u'$ следует $f(u) \neq f(u')$.*

Определение. *Отображение f называется **взаимно-однозначным** (биективным (bijective) отображением), если оно сюръективно и инъективно.*

Пусть заданы три множества U, V, W и два отображения $f : U \mapsto V$ и $\varphi : V \mapsto W$. Мы можем построить третье отображение ψ множества U во множество W по следующему правилу : если $v = f(u)$, а $w = \varphi(v)$, то полагаем $\psi(u) = w$.

Определение. *Отображение ψ называется* ***произведением (композицией)*** *отображений f и φ, и обозначается $\psi = \varphi \circ f$. (****Обратите внимание на порядок записи****.)*

Заметим, что если задано отображение $\psi = \varphi \circ f$, то отображение f указывает множество, являющееся прообразом отображения ψ, а отображение φ определяет множество (в наших обозначениях это будет W), где находится образ отображения ψ. Важное свойство композиции (произведения) отображений выражает следующая теорема.

Теорема 1.1.1. *Произведение отображений ассоциативно, т.е. если f, φ, ψ — три отображения $f : U \mapsto V$, $\varphi : V \mapsto W$, $\psi : W \mapsto X$, то для любого $u \in U$:*

$$(\psi \circ (\varphi \circ f))(u) = ((\psi \circ \varphi) \circ f)(u).$$

Доказательство. Прежде всего заметим, что каждое отображение $(\psi \circ (\varphi \circ f))$ $((\psi \circ \varphi) \circ f)$ отображает U в X. Поэтому достаточно показать, что образы произвольного элемента $u \in U$ при этих отображениях совпадают. Мы имеем

$$(\psi \circ (\varphi \circ f))(u) = \psi(\varphi \circ f)(u) = \psi(\varphi(f(u))$$

$$((\psi \circ \varphi) \circ f)(u) = (\psi \circ \varphi)(f(u)) = \psi(\varphi(f(u)).$$

□

В случае , когда $U = V$, говорят, что отображение f является отображением множества U в себя (или **на** себя, если f — сюръективно).

Определение. *Два отображения f и φ множества U в себя называются* ***перестановочными*** *(****коммутирующими****), если для любого $u \in U$*

$$(\varphi \circ f)(u) = (f \circ \varphi)(u).$$

Существуют отображения множества U в себя, которые не коммутируют. Так, например, если U состоит из двух элементов a и b, то отображения

$$f : a \longrightarrow b; b \longrightarrow a \text{ и } \varphi : a \longrightarrow a; b \longrightarrow b,$$

не коммутируют.

Среди всех отображений множества U в себя выделяют **тождественное (единичное)** отображение $e : U \mapsto U$. Очевидно, для любого отображения f множества U в себя

$$f \circ e = e \circ f = f.$$

Определение. *Пусть f — отображение множества U в себя. Отображение φ множества U в себя называется* ***левым*** *(соответственно* ***правым****)* ***обратным*** *к отображению f, если $\varphi \circ f = e$ (соответственно $(f \circ \varphi = e)$. Если $\varphi \circ f = f \circ \varphi = e$, то φ называется обратным к f и обозначается f^{-1}.*

Замечание. Из существования левого обратного не следует существование правого обратного, и наоборот. Например, пусть $U = \mathbb{N}$. Определим отображение:

$$f : n \mapsto 2n; \qquad \varphi : n \mapsto \begin{cases} \frac{n+1}{2} & \text{если } n\text{- четное} \\ \frac{n}{2} & \text{если } n\text{- нечетное} \end{cases}$$

Тогда для любого $n \in \mathbb{N}$ имеем $(\varphi \circ f)(n) = \varphi(2n) = n$, т.е. $\varphi \circ f = e$. Значит, φ — левое обратное отображение к f. Но правого обратного f не имеет, так как каково бы ни было отображение ψ множества $\mathbb{N}$ в себя, всегда $(f \circ \psi)(n) = f(\psi(n))$ — четное число, и ,значит, для нечетных n $(f \circ \psi)(n) \neq n$.

Упражнение 1. Если для f существует двустороннее обратное отображение, то оно единственно.

Теорема 1.1.2. *Отображение f множества U в себя тогда и только тогда имеет обратное, когда оно взаимно-однозначно (биективно).*

Доказательство. Пусть φ — обратное для f отображение. Тогда для любого $u \in U$ имеем

$$u = e(u) = (f \circ \varphi)(u) = f(\varphi(u)),$$

то есть u является образом некоторого элемента $\varphi(u) \in U$, а потому f сюръективно.
Кроме того, если $f(u_1) = f(u_2) = u$, то

$$\varphi(u) = \varphi(f(u_1) = (\varphi \circ f)(u_1) = e(u_1) = u_1,$$

$$\varphi(u) = \varphi(f(u_2) = (\varphi \circ f)(u_2) = e(u_2) = u_2,$$

отсюда следует, что $u_1 = u_2$.
Таким образом, f - инъективно, а потому f - биективно.

И наоборот, если f — биективно, то в силу его сюръективности, для каждого $u \in U$ найдется $u' \in U$ такой что $u = f(u')$, а ввиду инъективности этот элемент u' единственный, так что соответствие $u \mapsto u'$ является отображением U в себя, которое мы обозначим через φ.
Кроме того,

$$(f \circ \varphi)(u) = f(\varphi(u)) = f(u') = u,$$
$$(\varphi \circ f)(u) = \varphi(f(u')) = \varphi(u) = u',$$

То есть отображения $f \circ \varphi$ и $\varphi \circ f$ оставляют на месте элементы из U, а потому они тождественные. □

Замечание. Пусть f — отображение множества U на V, а φ — отображение множества V на U. Мы говорим, что φ является **левым обратным** к отображению f, если для любого $u \in U$ $(\varphi \circ f)(u) = u$. Отображение φ является

правым обратным к отображению f, если для любого $v \in V\,(f \circ \varphi)(v) = v$. Если отображение φ является одновременно левым и правым обратным к f, то оно называется обратным отображением к f и обозначается как и выше через f^{-1}.

Теорема 1.1.3. *Отображение f множества U на V имеет обратное отображение $\Leftrightarrow$ когда f — биективное отображение.*

Доказательство. Доказательство проходит аналогично доказательству теоремы 1.1.2. □

1.2 Алгебраические операции

Оперируя с рациональными и вещественными числами мы пользуемся двумя основными арифметическими действиями — сложением и умножением.

Внесение подобных действий во множества элементов произвольной природы в каком-то смысле "оживляет"эти множества.

Определение. *Пусть $\mathfrak{M}$ — непустое произвольное множество. Говорят, что на $\mathfrak{M}$ задана **n-арная алгебраическая операция** (или определен **закон композиции**), если указано правило, сопоставляющее любым n элементам $a_1, \ldots, a_n$ из $\mathfrak{M}$, взятым в определенном порядке, однозначно определенный элемент $n \in \mathfrak{M}$.*

Если $n = 1$, то мы имеем **унарную** операцию, которая есть ничто иное, как отображение $\mathfrak{M}$ в себя.
При $n = 2$ алгебраическая операция называется **бинарной**. В дальнейшем мы в основном рассматриваем бинарные алгебраические операции, а потому, если не указано особо, алгебраическая операция считается бинарной.

Отметим 3 основных момента в определении n–арной алгебраической операции:

1. операция определена на любом упорядоченном наборе из n элементов множества $\mathfrak{M}$. Поэтому говорят, что алгебраическая операция **определена всюду на $\mathfrak{M}$**;

2. сопоставляемый элемент «b» обязательно принадлежит $\mathfrak{M}$. В этом случае говорят, что алгебраическая операция **замкнута** на $\mathfrak{M}$;

3. элемент «b» единственный для набора $(a_1, \ldots, a_n)$.

Для обозначения бинарных алгебраических операций обычно используются значки: $+$, $\cdot$, $\times$, $-$, $:$, $\otimes, \perp$ и т.д.

Изучим ряд свойств бинарных алгебраических операций.

Определение. *Алгебраическая операция называется* ***ассоциативной****, если для любых* $a, b, c \in \mathfrak{M}$ $\quad (a * b) * c = a * (b * c)$.

Определение. *Алгебраическая операция называется* ***коммутативной****, если для любых* $a, b \in \mathfrak{M}$ $\quad a * b = b * a$.

Определение. *Множество* $\mathfrak{M}$ *с заданной на нем бинарной ассоциативной алгебраической операцией называется полугруппой.*

Пример 1. Множество натуральных чисел $\mathbb{N}$ относительно обычного умножения есть полугруппа.

Теорема 1.2.1. *Если бинарная операция ассоциативна, то результат ее применения к* n *элементам не зависит от расстановки скобок.*

Доказательство. Воспользуемся методом индукции по числу n. Для $n = 3$ теорема верна. Пусть $n > 3$ и предположим ее справедливость для числа элементов $< n$. Пусть мы имеем двоякое распределение скобок:

$$(a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n)$$

и

$$(a_1 * \ldots * a_l) * (a_{l+1} * \ldots * a_n).$$

Мы имеем

$$\begin{aligned}(a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n) = (a_1 * \ldots * a_k) * ((a_{k+1} * \ldots * a_{n-1}) * a_n) = \\ = ((a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_{n-1})) * a_n = a_1 * \ldots * a_{n-1}) * a_n.\end{aligned}$$

И аналогично,

$$(a_1 * \ldots * a_l) * (a_{l+1} * \ldots * a_n) = (a_1 * \ldots * a_l) * a_n.$$

□

Определение. *Элемент* $e \in \mathfrak{M}$ *называется* ***единичным (нейтральным)*** *относительно операции* $*$*, если* $a * e = e * a = a$ *для всех* $a \in \mathfrak{M}$.

Определение. *Пусть в* $\mathfrak{M}$ *существует единичный элемент* e*. Элемент* $\bar{a}$ *называется* ***обратным*** *к* $\bar{a}$*, если* $a * \bar{a} = \bar{a} * a = e$.

Теорема 1.2.2. *Во множестве $\mathfrak{M}$ с ассоциативной операцией $*$, если единичный элемент существует, то только один; если элемент a из $\mathfrak{M}$ имеет обратный, то только один.*

Доказательство. Пусть e и e' — два единичных элемента в $\mathfrak{M}$. В силу ассоциативности

$$e * e' * e = e * (e' * e) = e * e = e,$$
$$e * e' * e = e * (e' * e) = e * e' = e'.$$

Пусть

$$a * \bar{a} = e = \bar{a} * a \qquad \text{и} \qquad a * b = e = b * a.$$

Тогда

$$\bar{a} * a * b = (\bar{a} * a) * b = e * b = b,$$
$$\bar{a} * a * b = \bar{a} * (a * b) = \bar{a} * e = \bar{a}.$$

□

Чаще всего мы будем алгебраическую операцию обозначать через $*$ (или $\cdot$) и называть ее умножением, или через $+$ и называть сложением. (При сложении единичный элемент обычно называют **нулем** и обозначают через 0). Обратный к a элемент при умножении обозначают через a^{-1}.

На одном и том же множестве можно задавать несколько алгебраических операций. Наибольший интерес представляет случай, когда эти операции связаны между собой. Одной из таких связей является свойство левой (правой) дистрибутивности. Пусть на $\mathfrak{M}$ заданы две операции $+$ (сложение) и $*$ (умножение). Тогда говорят, что умножение дистрибутивно слева (справа) относительно сложения, если

$$a * (b + c) = a * b + a * c$$
(или соответственно, $(b + c) * a = b * a + c * a$).

1.3 Группы

Определение. *Множество $\mathfrak{M}$ с операцией $*$ называется группой, если выполняются следующие требования:*

1. *операция $*$ ассоциативна;*
2. *в $\mathfrak{M}$ существует единичный элемент;*
3. *каждый элемент из $\mathfrak{M}$ имеет обратный.*

Если на $\mathfrak{M}$ задана операция умножения, то $\mathfrak{M}$ называется ***мультипликативной*** *группой, а если сложение, то мы имеем* ***аддитивную*** *группу.*

Если операция, заданная на группе коммутативна, то сама группа называется **коммутативной**, или **абелевой** (в честь норвежского математика Г.Абеля). Если в $\mathfrak{M}$ содержится конечное число элементов, то группа $\mathfrak{M}$ называется **конечной**, а число элементов в ней — порядком группы (обозначается **порядок** $\mathfrak{M}$ или *Card* $\mathfrak{M}$). Если в $\mathfrak{M}$ имеется бесконечное число элементов, то $\mathfrak{M}$ — бесконечная группа.

Теорема 1.3.1. *Совокупность G всех взаимно-однозначных отображений множества U на себя вместе с определенной операцией умножения (композиции) отображений образует группу.*

Доказательство. Ранее мы убедились, что умножение отображений множества U на себя ассоциативно, и кроме того, в G имеется единственный элемент — тождественное отображение. Каждое отображение $f \in G$ обратимо (в силу взаимной однозначности). Поэтому утверждение теоремы будет завершено, если мы покажем, что умножение отображений является алгебраической операцией. А для этого осталось доказать, что для любых f и φ из G всегда $f \circ \varphi \in G$. Положим $\psi = f \circ \varphi$. В силу сюръективности f и φ для любого $u \in U$ существуют w и v такие, что $f(w) = u$, $\varphi(v) = w$. Поэтому $\psi(v) = f(\varphi(v)) = u$, то есть ψ — сюръективно. Инъктивность ψ доказывается также просто: равенство $\psi(v) = u$ может выполняться только для одного $v \in U$, ибо $\psi(v) = f(\varphi(v)) = u$, $f(w) = u$ — только для одного w (в силу инъективности f), а $\varphi(v) = w$ — только для одного v (в силу инъективности φ). □

Результат доказанной теоремы применим ко множеству U, состоящему из n элементов. (Поскольку природа элементов для нас несущественна, то будем считать, что $U = \{1, 2, \ldots, n\}$ на себя называется **симметрической группой подстановок** степени n и обозначается $\mathbf{S}_n$. Ее элементы обычно называются подстановками.

Если $\sigma \in \mathbf{S}_n$ — какая-либо подстановка, сопоставляющая элементу i элемент a_i, то мы будем писать

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ a_1 & a_2 & \ldots & a_i & \ldots & a_n \end{pmatrix}$$

Перемножить две подстановки σ_1 и σ_2 – это значит найти нижнюю строку результирующей подстановки.

Пример 2. Пусть $\sigma_1 = \left(\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right)$, $\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right)$. Тогда

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\4&3&2&1\\ \downarrow&\downarrow&\downarrow&\downarrow\\1&4&3&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

Легко видеть, что $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$, так что симметрическая группа $\mathbf{S}_n$ не является абелевой (кроме случая $n \leq 2$).

Лемма 1.3.1. *Порядок группы $\mathbf{S}_n$ равен $n!$*

Доказательство. Проведем индукцию по числу $n!$. Для $n = 1$ мы имеем единственную тождественную подстановку. Пусть утверждение леммы верно для всех симметрических групп степени $\leq n-1$. Пусть в некоторой подстановке из $\mathbf{S}_n$ на i–ом месте второй строки стоит n, это значит, что выбранная подстановка осуществляет отображение множества $\{1, 2, \ldots, n\}$ в себя таким образом, что $i \to n$. Для оставшихся $(n-1)$ элементов нижней строки имеется $(n-1)$ мест. И согласно предположению индукции они могут распределиться на этих местах $(n-1)!$ способами. Итак, имеется $(n-1)!$ подстановок степени n, у которых $i \to n$. Но i может быть любым из чисел $1, 2, \ldots, n$. Поэтому всего различных подстановок степени n :

$$\underbrace{(n-1)! + \ldots + (n-1)!}_{n \text{ раз}} = n \cdot (n-1)! = n!$$

□

Группы $\mathbf{S}_n$ естественным образом возникают не только в алгебре. Исключительно велика их роль в геометрии, квантовой механике, теоретической химии и т.д. Вот почему мы подробнее изучим эту группу.

Определение. *Подстановка $\sigma \in \mathbf{S}_n$ называется **транспозицией**, если она меняет местами только два элемента. Иначе говоря, подстановка σ есть транспозиция, если для каждого числа верхней строки (кроме двух чисел i и j) соответствующее ему число нижней строки совпадает с верхним числом, а для элементов i и j имеем $i \to j$, $j \to i$.*

Пример 3. Например,

$$\sigma = \begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix}.$$

Определение. *Транспозиция σ называется **транспозицией соседних**, если она меняет местами i и j, причем $j = i + 1$.*

Подстановки из $\mathbf{S}_n$, являющиеся транспозициями, мы обозначаем через τ, а если она к тому же является транспозицией соседних (с номерами i и $i+1$), то через $\tau(i)$.

Определение. *Пусть дана подстановка*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_i & \dots & a_j & \dots & a_n \end{pmatrix}.$$

Говорят,что пара (i,j) образует ***инверсию****, если $i<j$, но $a_i > a_j$. Количество инверсий, образуемых всевозможными парами чисел $1,2,\dots,n$ называется числом инверсий подстановки σ и обозначается через $\nu(\sigma)$.*

Определение. *Подстановка σ называется* ***четной****, если $\nu(\sigma)$ – четное. В противном случае, σ –* ***нечетная*** *подстановка. Положим*

$$\rho(\sigma) = \begin{cases} 1, & \text{если } \sigma\text{- четная подстановка,} \\ -1, & \text{если } \sigma\text{- нечетная подстановка.} \end{cases}$$

Очевидно, что $\rho(\sigma) = (-1)^{\nu(\sigma)}$.

Лемма 1.3.2. *Каждую подстановку можно разложить в произведение транспозиций соседних.*

Доказательство. Проведем индукцию по числу инверсий в подстановке. Если $\nu(\sigma) = 0$, то σ — единичная подстановка (она не меняет никакие элементы множества $\{1,2,\dots,n\}$). Но для любой транспозиции соседних $\tau(i)$ имеем

$$\tau^2(i) = \tau(i)\tau(i) = e \qquad (e - \text{единичная подстановка}). \tag{1.1}$$

То есть, для e разложение получено. Предположим теперь утверждение леммы справедливо для любой подстановки степени n с числом инверсий $< k$. И рассмотрим подстановку σ с числом инверсий $\nu(\sigma) = k > 0$. Подстановка σ не является тождественной, а потому найдется номер i, что пара $(i, i+1)$ образует инверсию. Рассмотрим транспозицию $\tau(i)$. Тогда подстановка $\sigma \circ \tau(i)$ отличается от σ только в местах $i, i+1$, причем теперь пара $(i, i+1)$ уже не образует инверсию (ибо $i \to i+1 \to a_{i+1}$, $i+1 \to i \to a_i$ и $a_{i+1} < a_i$). Поэтому $\nu(\sigma \circ \tau(i)) = \nu(\sigma) - 1 < k$.
И значит, к подстановке $\sigma \circ \tau(i)$ можно применить предположение индукции. Имеем:

$$\sigma \circ \tau(i) = \tau(i_1) \dots \tau(i_l).$$

А в силу (1.1):

$$\sigma = \tau(i_1) \dots \tau(i_l)\tau(i).$$

□

Следствие 1. *Если* $\sigma = \tau(i_1)\dots\tau(i_m)$, *то* $\rho(\sigma) = (-1)^m$.

Доказательство. В самом деле,сначала заметим, что умножение любой подстановки на транспозицию соседних изменяет четность подстановки:

$$\nu(\sigma \circ \tau(i)) = \nu(\sigma) \pm 1$$

(ибо транспозиция $\tau(i)$ либо ликвидирует инверсию пары $(i, i+1)$, если такая была в σ, либо образует инверсию, если ее не было в σ). Из равенства

$$\sigma = \tau(i_1)\dots\tau(i_m) \tag{1.2}$$

имеем

$$\sigma \circ \tau(i_1) \circ \dots \circ \tau(i_m) = e. \tag{1.3}$$

В силу $\nu(e) = 0$ и предыдущего замечания, получаем, что при переходе от (1.2) к (1.3) мы m раз изменим четность числа инверсий, то есть от $(-1)^0$ мы придем к $(-1)^m$. □

Следствие 2. $\rho(\sigma \circ \tau(i_1)) = -\rho(\sigma)$.

Следствие 3. *Для любых подстановок* σ_1 *и* σ_2

$$\rho(\sigma_1 \circ \sigma_2) = \rho(\sigma_1)\rho(\sigma_2).$$

Доказательство. В самом деле, если $\sigma_1 = \tau(i_1) \circ \dots \circ \tau(i_m)$, $\sigma = \tau(j_1) \circ \dots \circ \tau(j_k)$, то в силу ассоциативности умножения подстановок

$$\sigma_1 \circ \sigma_2 = \tau(i_1) \circ \dots \circ \tau(i_m) \circ \tau(j_1) \circ \dots \circ \tau(j_k).$$

Таким образом

$$\rho(\sigma_1 \circ \sigma_2) = (-1)^{m+k} = \rho(\sigma_1)\rho(\sigma_2).$$

□

Следствие 4. *Произведение подстановок одинаковой четности есть четная подстановка, а разной четности — нечетная подстановка.*

Доказательство. Непосредственно следует из предыдущего следствия. □

Следствие 5. *Если* σ^{-1} *— подстановка, обратная к* σ, *то*

$$\rho(\sigma) = \rho(\sigma^{-1}),$$

то есть σ *и* σ^{-1} *имеют одинаковую четность.*

Доказательство. Действительно,

$$1 = \rho(e) = \rho(\sigma \circ \sigma^{-1}) = \rho(\sigma)\rho(\sigma^{-1}) \Rightarrow \rho(\sigma) = \rho(\sigma^{-1}).$$

□

Следствие 6. *Все четные подстановки степени n образуют группу. Она называется* ***знакопеременной группой*** *и обозначается через* $\mathbf{A}_n$*. Порядок* $\mathbf{A}_n$ *равен* $\frac{1}{2}n!$ *(для* $n > 1$*).*

Доказательство. Действительно, из следствия 4 следует, что множество четных подстановок замкнуто относительно операции умножения. Эта операция ассоциативна. Кроме того, единичная подстановка e – четная, а для каждой четной подстановки σ обратная ей σ_{-1} также четная. Поэтому выполнены все аксиомы группы. Таким образом доказано, что $\mathbf{A}_n$ — группа.

Пусть $n > 1$. Обозначим через $\mathbf{B}_n$ — множество нечетных подстановок. Тогда совокупности $\mathbf{A}_n$ и $\mathbf{B}_n$ не пересекаются, а в объединении дают $\mathbf{S}_n$. Обозначим через *Card* $\mathbf{A}_n$ и *Card* $\mathbf{B}_n$ — количества элементов в $\mathbf{A}_n$ и $\mathbf{B}_n$. Возьмем теперь некоторую нечетную подстановку σ и умножим на нее каждую подстановку из $\mathbf{S}_n$. По следствию 4 нечетные подстановки после этого умножения сделаются четными, а четные нечетными, то есть мы получим взаимно однозначное отображение $\mathbf{A}_n$ на $\mathbf{B}_n$, а потому *Card* $\mathbf{A}_n$ = *Card* $\mathbf{B}_n$. Но *Card* $\mathbf{A}_n$ + *Card* $\mathbf{B}_n$ = *Card* $\mathbf{S}_n = n!$ Поэтому *Card* $\mathbf{A}_n = \frac{1}{2}n!$ $(n > 1)$. Очевидно, что при $n = 1$ $\mathbf{S}_n = \mathbf{A}_n$. □

Предыдущее следствие наводит на мысль дать следующее определение.

Определение. *Подмножество H группы G называется* ***подгруппой*** *в G, если оно само является группой относительно операции, заданной на G. Подгруппа, состоящая только из одного элемента e, называется* ***единичной****. Подгруппа G, отличная от G и от единичной подгруппы, называется* ***собственной*** *подгруппой.*

Лемма 1.3.3. ***Критерий подгруппы.*** *Подмножество* $H \subset G$ *будет подгруппой в группе G тогда и только тогда, когда для любых* $h_1, h_2 \in H$ *имеем* $h_1 h_2^{-1} \in H$*.*

Доказательство. Необходимость очевидна. Поэтому докажем достаточность. Пусть $h \in H$. Возьмем $h_1 = h_2 = h$, тогда из $h_1 h_2^{-1} \in H$ следует, что $hh^{-1} = e \in H$, то есть в H содержится единичный элемент. Если $h \in H$, то положив $h_1 = e,\ h_2 = h$ получим $h_1 h_2^{-1} = eh^{-1} = h^{-1} \in H$, то есть с каждым $h \in H$ имеем $h^{-1} \in H$. Умножение в H ассоциативно, так как оно ассоциативно в G. Наконец, если $h_1, h_2 \in H$, то $h_1, h_2^{-1} \in H$, то есть умножение замкнуто в H. Выполнены все аксиомы группы. □

Пример 4. Пусть $\mathbb{Z}$ — множество целых чисел. Относительно операции обычного сложения $\mathbb{Z}$ — аддитивная абелева группа. Обозначим через $m\mathbb{Z}$ — совокупность целых чисел, кратных m. $m\mathbb{Z}$ — подгруппа в $\mathbb{Z}$. Действительно, применим критерий, пусть $k_1, k_2 \in m\mathbb{Z}$, тогда $k_1 = q_1 m$, $k_2 = q_2 m$, а $k^{-1} = -q_2 m$ (в силу того что мы имеем аддитивную группу). Поэтому $k_1 \cdot k_2^{-1} = (q_1 - q_2)m = qm \in \mathbb{Z}$.

Упражнение 2. Доказать, что подгруппами $m\mathbb{Z}$, m — натуральное или 0, исчерпываются все подгруппы в $\mathbb{Z}$.

Пусть G — группа по умножению. Тогда вместе с элементом $g \in G$ в этой группе содержатся и элементы

$$g \cdot g, \qquad g \cdot g \cdot g, \qquad \dots \qquad , \underbrace{g \cdot g \cdot \ldots \cdot g}_{k}.$$

Подобные произведения естественно назвать **степенями** g и обозначать $g^2,\ g^3,\ \dots\ , g^k$. Естественно также положить $(g^{-1})^k = g^{-k}$. И как легко видеть, $(g^k)^{-1} = g^{-k}$. Под g^0 мы будем понимать элемент $e = g \cdot g^{-1}$.

Лемма 1.3.4. *Для любых m, $n \in \mathbb{Z}$ и любого $g \in G$*

$$g^m \cdot g^n = g^{m+n}, \qquad (g^m)^n = g^{mn}.$$

Доказательство предоставляется читателю.

Следствие 1. $g^m \cdot g^n = g^n \cdot g^m = g^{m+n}$.

Следствие 2. *Пусть $< g >$ означает множество всех степеней элемента g. Тогда из определения степеней, леммы и следствия 1 следует, что $< g >$ — подгруппа в G, причем –абелевая. Она называется **циклической** подгруппой, порожденной элементом g. А элемент g — **образующий** группы $< g >$.*

Могут встретиться две возможности:

1. Все степени g различны, т.е. при $m \neq n$ $\ g^m \neq g^n$. Тогда говорят, что элемент g имеет бесконечный порядок.

2. Для некоторой пары m, n $\ (m \neq n)$ $\ g^m = g^n$. Тогда, предполагая, что $m > n$ получим $g^{m-n} = e$. Пусть k — наименьший натуральный показатель, для которого $g^k = e$ (по принципу наименьшего натурального числа такое k обязательно имеется). Тогда говорят, что g – элемент **конечного порядка** k.

Упражнение 3. Если G — конечная группа порядка h, то все её элементы имеют конечный порядок $\leq h$.

Теорема 1.3.2. *Если g — элемент конечного порядка, то порядок g равен* $\mathrm{Card} < g >$.

Доказательство. Пусть порядок g равен k. Тогда все элементы

$$g^0 = e,\ g,\ g^2,\ \ldots\ , g^{k-1} \tag{1.4}$$

различны, а всякая другая степень g совпадает с одним из элементов (1.4).

Действительно, рассмотрим элемент $g^l,\ l \geq 0$. Если $0 \leq l \leq k-1$, то g^l есть одно из чисел в (1.4). Если же $l > k-1$, то представим l в виде $l = kq+r,\ 0 \leq r \leq k-1$ (такое представление существует по известной теореме о делении с остатком). Но тогда $g^l = g^{kq+r} = g^{kq} \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r$, и g^r есть одно из чисел в (1.4). Наконец, если $l < 0$, то обозначим $l' = -l,\ l' > 0$. И в силу $g^{k-1} \cdot g = g^k = e \ \Rightarrow\ g^{k-1} = g^{-1}$, имеем

$$g^l = g^{-l'} = (g^{-1})^{l'} = g^{(k-1)l^{l'} = g^{l''}},$$

где $l'' = (k-1)l' > 0$ и мы приходим к предыдущему случаю. Подгруппа $< g >$ состоит из всех **различных** степеней g, и в силу доказанного совпадает с множеством элементов (1.4), число которых равно $k =$ порядок g. □

Упражнение 4. Если $< g >$ — элемент порядка k, то $g^m = e \ \Leftrightarrow\ m = kq,\ q \in \mathbb{Z}$.

Из теоремы 1.3.2 следует, что если G — группа конечного порядка, то порядок элемента не превосходит порядка группы. Следующая теорема уточняет этот факт.

Теорема 1.3.3. *Если G — конечная группа, H — ее подгруппа, то порядок G делится на порядок H.*

Доказательство. Пусть порядок $Card\, G = n$, порядок $Card\, H = m$, и $h_1, \ldots, h_m$ — все элементы подгруппы H (неограничивая общности, можно считать, что $h_1 = e$ — единичный элемент группы G). Если $m = n$, то утверждение теоремы доказано. Пусть $m < n$, тогда в G найдется элемент g_1 такой, что $g_1 \bar{\in} H$. Очевидно, что элементы $g_1h_1,\ g_1h_2,\ \ldots,\ g_1h_m$ все различны между собой и не принадлежат H. Если вместе с H они исчерпывают группу G, то порядок G равен $2n$. В противном случае, найдется $g_2 \in G$, которое отлично от элементов $h_1, \ldots, h_m,\ g_1h_1,\ \ldots,\ g_1h_m$ и такое, что $g_2h_1,\ \ldots,\ g_2h_m$ все различны между собой и от h_i и $g_1h_j,\ i = 1, 2, \ldots m;\ j = 1, 2, \ldots m$. Через конечное число шагов мы найдем элементы $g_1,\ g_2,\ \ldots,\ g_{k-1}$ такие, что совокупность

$$h_1, \ldots, h_m, g_1h_1, \ldots,\ g_1h_m,\ \ldots,\ g_{k-1}h_1,\ \ldots,\ g_{k-1}h_m$$

исчерпывает собой всю группу G, а потому $Card\, G = k \cdot Card\, H$. □

Следствие. *Порядок элемента конечной группы является делителем порядка группы.*

В самом деле, порядок g равен порядку $< g >$, где $< g >$ — подгруппа в G, порожденная элементом g.

1.4 Кольца

Определение. *Пусть K — множество, на котором заданы две бинарные алгебраические операции $+$ и $\cdot$, называемые сложением и умножением. Пусть при этом выполняются следующие 3 условия (аксиомы):*

1. *относительно операции сложения K является абелевой группой (с нулевым элементом 0);*
2. *операция умножение ассоциативна (то есть по умножению K — полугруппа);*
3. *умножение дистрибутивно относительно сложения, то есть*

$$a(b+c) = ab + ac, \qquad (b+c)a = ba + ca.$$

Тогда K называется ***кольцом****.*

Кольцо K называется **коммутативным**, если операция умножения — коммутативна. Если в K содержится 1 (по умножению), то K называется **кольцом с единицей**.

Пример 5. Примерами колец являются $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, не считая **тривиального** кольца, состоящего только из 0.

В различных разделах математики широко используется следующий важный пример.

Пример 6. Кольцо функций. Пусть X — произвольное множество, K — произвольное кольцо. Пусть F — множество всех отображений (функций) $f : X \to K$, рассматриваемое вместе с двумя бинарными операциями: **поточечной суммой** $f + g$ и **поточечным произведением** $f \cdot g$, что означает следующее:

$$(f+g)(x) = f(x) \oplus g(x), \qquad (f \cdot g)(x) = f(x) \odot g(x)$$

($\oplus$, $\odot$ — операции сложения и умножения в K).

(Заметим, что введенная операция умножения не является композицией (умножением) отображений, рассмотренной ранее). Так, например, если $X = \mathbb{R}$, $K = \mathbb{R}$, то произведением двух функций (отображений) tg и sin будет:

$$\operatorname{tg} \cdot \sin : \; x \to \operatorname{tg} \cdot \sin x$$

(а не tg(sin)). Без труда проверяется, что множество F удовлетворяет всем аксиомам кольца. Проверим только дистрибутивную аксиому:

$$(f + g) \cdot h : \; (f(x) \oplus g(x)) \odot h(x) = f(x) \odot h(x) \oplus g(x) \odot h(x),$$

но $fh+gh : \; f(x) \odot h(x) \oplus g(x) \odot h(x)$, (здесь мы воспользовались дистрибутивностью в K). Аналогично проверяется второе равенство дистрибутивности.

Если 0 и 1 — нулевой и единичный элементы в K, то отображения

$$\mathrm{O}_X : \; x \to 0; \qquad 1_X : \; x \to 1$$

— **постоянные** функции, играющие роль 0 и 1 в F. Кольцо F коммутативно $\Leftrightarrow$ когда коммутативно кольцо K.

Некоторые свойства кольца являются переформулировкой свойств абелевых групп и множеств с ассоциативной операцией (в частности, если единичный элемент существует, то он единственный).

Перечислим некоторые специфические свойства кольца, вытекающие из наличия двух операций в K.

1. $a \cdot 0 = 0 \cdot a = 0$ для любого $a \in K$.

   Действительно, $a+0 = a \Rightarrow a(a+0) = a \cdot a \Rightarrow a^2 + a \cdot 0 = a^2 \Rightarrow a^2 + a \cdot 0 = = a^2 + 0 \Rightarrow a \cdot 0 = 0$. (Аналогично $0 \cdot a = 0$).

2. Пусть K — нетривиальное кольцо (т.е. $K \neq 0$), и пусть 1 — единица в K. Покажем, что $1 \neq 0$.

   Действительно, если бы $1 = 0$, то мы имели бы $a = a \cdot 1 = a \cdot 0 = 0$ для всех $a \in K$, т.е. K — тривиальное кольцо.

3. $(-a) \cdot b = a \cdot (-b) = -(ab)$.

   Действительно, $0 = a \cdot 0 = a(b - b) = ab + a(-b) \Rightarrow -(ab) = a(-b)$ (и аналогично, $-(ab) = (-a) \cdot b$).

4. По индукции можно доказать **общий закон дистрибутивности**

$$(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.$$

   А потому из предыдущих свойств:

$$n(a \cdot b) = (na) \cdot b = a \cdot (nb) \qquad \text{для любого } n \in \mathbb{Z}.$$

Определение. *Подмножество K_1 кольца K называется* ***подкольцом*** *кольца K, если K_1 замкнуто относительно операций кольца K, то есть если $a, b \in K_1$, то $-a, a+b, ab \in K_1$.*

Пример 7. Например, $\mathbb{Z}$ подкольцо в $\mathbb{Q}$, а $\mathbb{Q}$ в $\mathbb{R}$.

Пример 8. Пусть F — кольцо отображений $X = [0,1]$ в кольцо $\mathbb{R}$ (то есть F — кольцо всех вещественно-значных функций на $X = [0,1]$). Тогда $F_{\text{непр}}$ — множество всех непрерывных вещественных на $[0,1]$ функций — подкольцо в F.

Поскольку подкольцо в K это прежде всего подгруппа аддитивной группы кольца K, то легко убедиться, что $m\mathbb{Z}$, $m = 0, 1, 2, \ldots$, исчерпывают собой все подкольца в $\mathbb{Z}$. С помощью кольца $\mathbb{Z}$ мы построим новое кольцо, которое не является подкольцом в $\mathbb{Z}$, но с ним связано. С этой целью введем следующее определение.

Определение. *Два целых числа a и b называются* ***сравнимыми*** *по* $\mod m$, *($m \geq 1$ — целое), если $(a-b)$ — делится на m. И обозначают $a \equiv b(\mod m)$. Число m называется* ***модулем сравнения****.*

Упражнение 5. $a \equiv b(\mod m) \Leftrightarrow$ когда a и b имеют одинаковые остатки от деления на m.

Все числа, сравнимые между собой по $\mod m$, объединяются в классы. Поскольку каждое число сравнимо со своим остатком от деления на m, а всех различных остатков ровно m : $\{0, 1, \ldots m-1\}$, то мы имеем точно m различных классов, называемых **классами вычетов** по $\mod m$. Каждый класс вычетов состоит из чисел $C_r = \{r + mk | \, k \in \mathbb{Z}\}$, r — фиксировано, $0 \leq r \leq m-1$. Классы $C_0, C_1, \ldots, C_{m-1}$ не имеют общих элементов и

$$\mathbb{Z} = C_0 \bigcup C_1 \bigcup \ldots \bigcup C_{m-1}.$$

На совокупности классов введем две операции: сложение и умножение.
Суммой двух классов $C_i + C_j$ назовем класс, в котором содержится $i + j$ (это будет класс C_{i+j}, если $i + j \leq m-1$). Произведением классов $C_i \cdot C_j$ назовем класс, в котором содержится число $i \cdot j$.
Относительно введенных операций совокупность классов образует кольцо, называемое **кольцом классов вычетов** по $\mod m$, и обозначаемое через $\mathbb{Z}_m$ (иногда пишут $\mathbb{Z}/_{(m)}$).

Таким образом мы построили пример кольца, состоящего из конечного числа элементов.

Рассмотрим кольцо $\mathbb{Z}_m$ и условимся вместо обозначения класса C_i писать просто i. Так в кольце $\mathbb{Z}_5$ мы имеем элементы $0, 1, 2, 3, 4$. Составим для них таблицы сложения и умножения.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Такие же таблицы мы можем составить для любого кольца $\mathbb{Z}_m$. Рассмотрим подробнее таблицу умножения для $\mathbb{Z}_4$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Из этой таблицы видно, что $2 \cdot 2 = 0$, вопреки общеизвестной истине « дважды два — четыре ». Мы привыкли к тому, что в хорошо известных числовых кольцах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ из $a \cdot b = 0$ обязательно хотя бы одно из чисел a или b равно 0. Но в кольце $\mathbb{Z}_4$ это уже не так. Оказывается, что столь необычное для нас явление не такое уже и редкое. Приведем еще один пример.

Пример 9. Пусть K есть множество пар (a, b), где $a, b \in \mathbb{Z}$ с покомпонентным сложением и умножением:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Легко проверить, что K — коммутативное кольцо, нулем которого служит пара $(0, 0)$, а единицей — $(1, 1)$. Тогда имеем $(a, 0) \cdot (0, b) = (0, 0)$.

Определение. *Если $ab = 0$ при $a \neq 0, b \neq 0$, то a называется* ***левым делителем нуля****, а b —* ***правым делителем нуля****. В коммутативном кольце говорят просто о делителях нуля.*

Определение. *Коммутативное кольцо с единицей и без делителей нуля называется* ***областью целостности****.*

Теорема 1.4.1. *Нетривиальное коммутативное кольцо K с единицей является областью целостности $\Leftrightarrow$ когда в нем выполнен* ***закон сокращения***

$$ab = ac,\ a \neq 0 \ \Rightarrow\ b = c,\ \textit{для всех}\, a, b, c \in K.$$

Доказательство оставляем читателю.

1.5 Поля

Пусть K — кольцо с единицей. Элемент $a \in K$ называется **обратимым** (или делителем единицы), если существует в K элемент b, для которого $ab = ba = 1$. Обычно элемент b обозначают через a^{-1}.

Теорема 1.5.1. *Все обратимые элементы кольца K с единицей образуют группу $K^\star$ по умножению.*

Доказательство. Поскольку множество $K^\star$ содержит 1, ассоциативно по умножению, каждый его элемент обратим, то нам достаточно проверить, что $K^\star$ замкнуто по умножению. Пусть $a, b \in K^\star$, тогда $a^{-1}, b^{-1} \in K^\star$, и мы имеем

$$(ab) \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1,$$

то есть ab — обратим и обратный ему равен $b^{-1}a^{-1}$, а потому $ab \in K^\star$. □

Естественно ожидать, что кольцо, все ненулевые элементы которого образуют группу по умножению, обладает более содержательной структурой. Такое кольцо называют **кольцом с делением**, или **телом**.
В кольце с делением нет делителей нуля, а если еще потребовать коммутативности умножения, то получим новое алгебраическое образование — **поле**. Итак

Определение. *Поле F — это коммутативное кольцо с единицей, $1 \neq 0$, в котором каждый элемент $a \neq 0$ обратим.*

Определение. *Подполем H поля F называется подкольцо в F, само являющееся полем.*

Пример 10. Примерами полей служат множества $\mathbb{Q}$, $\mathbb{R}$, причем $\mathbb{Q}$ подполе в $\mathbb{R}$.

Если $H \subset F$ — подполе в F, то F называется **расширением** своего подполя H.

Пример 11. Обозначим через $\mathbb{Q}(\sqrt{2})$ совокупность чисел вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Q}$. Относительно операций сложения и умножения эта совокупность замкнута (мы учитываем, что $(\sqrt{2})^2 = 2$). Нулем служит $0 + 0\sqrt{2}$, а единицей $1 + 0\sqrt{2} = 1$. Поэтому обратным по сложению к $a + b\sqrt{2}$ будет $-a - b\sqrt{2}$, а по умножению

$$\frac{1}{-a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$

правда, нужно убедиться, что для $a + b\sqrt{2} \neq 0$ обязательно $a^2 - 2b^2 \neq 0$. Но в противном случае мы имели бы $2 = \dfrac{a^2}{b^2} \Rightarrow \sqrt{2} = \pm\dfrac{a}{b}$, что противоречит иррациональности $\sqrt{2}$. Таким образом мы построили поле $\mathbb{Q}(\sqrt{2})$, являющееся

расширением поля $\mathbb{Q}$. Заметим, что в поле $\mathbb{Q}$ уравнение $x^2 - 2 = 0$ не имеет решений, а в $\mathbb{Q}(\sqrt{2})$ это уравнение уже разрешимо. Однако, линейное уравнение $ax + b = 0$ при $a \neq 0$ разрешимо в любом поле.

Лемма 1.5.1. *В поле F однозначно разрешимо уравнение*

$$ax + b = 0, \qquad a \neq 0. \tag{1.5}$$

Доказательство. Поскольку $a \neq 0$, то в F найдется единственный обратный (по умножению) элемент a^{-1}. И тогда $x = -a^{-1}b$ является решением уравнения. Ибо

$$a(-a^{-1}b) + b = -(aa^{-1})b + b = -b + b = 0.$$

Если бы уравнение 1.5 обладало двумя решениями c и d, то мы имели бы

$$\begin{matrix} ac + b = 0 \\ ad + b = 0 \end{matrix} \qquad \Rightarrow \qquad ac = ad \qquad \Rightarrow \qquad a(c - d) = 0 \qquad \Rightarrow \qquad c = d.$$

□

Итак, мы видим, что линейные уравнения всегда разрешимы в поле, а более сложные уравнения (например, квадратные) в данном поле могут быть неразрешимыми. Но пример с уравнением $x^2 - 2 = 0$ показывает, что можно ожидать, что для данного уравнения $f(x) = 0$ ($f(x) = 0$ — многочлен с коэффициентами из данного поля F) найдется расширение поля F, в котором это уравнение разрешится. Как мы убедимся позже важнейшим этапом в развитии математики послужило поле, являющееся расширением поля $\mathbb{R}$, и в котором разрешимо уравнение $x^2 + 1 = 0$.

Здесь мы сталкиваемся с двумя проблемами:

1. Как построить такое расширение $\mathbb{R}$, если это возможножно;
2. Если такие расширения существуют, то сколько их и какое из них следует использовать.

Чтобы был ясен смысл второй проблемы, объясним понятие **минимальности** на следующих примерах.

Пример 12. Поле $\mathbb{Q}$ не содержит никаких подполей кроме самого себя.
В самом деле, пусть $F \subset \mathbb{Q}$, тогда в F обязательно содержатся 0 и 1, а значит и суммы вида

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ раз}},$$

то есть в F содержатся все натуральные числа, а в силу обратимости сложения, и все целые числа. Но в поле F разрешимо уравнение

$$ax - b = 0, \qquad a, b \in \mathbb{Z} \subset F, \qquad a \neq 0,$$

решением которого служит рациональное число $\frac{b}{a}$, поэтому $\mathbb{Q} \subset F$. Откуда $F = \mathbb{Q}$.

Пример 13. $\mathbb{Q}(\sqrt{2})$ является минимальным среди всех полей, являющихся расширением поля $\mathbb{Q}$ и в которых разрешимо уравнение $x^2 - 2 = 0$.
Действительно, пусть P одно из таких полей. Тогда $\mathbb{Q} \subset P$ и $\sqrt{2} \in P$, а значит все числа вида $a + b\sqrt{2} \in P$, где $a, b \in \mathbb{Q}$. Но именно такими числами исчерпывается поле $\mathbb{Q}(\sqrt{2})$, так что $\mathbb{Q}(\sqrt{2}) \subset P$.

Эти примеры наталкивают нас на мысль искать поле, являющееся расширением поля $\mathbb{R}$, и в котором разрешимо уравнение $x^2 + 1 = 0$. Причем это поле должно быть минимальным среди всех полей, удовлетворяющих этим требованиям. Заметим, что мы ищем расширение поля $\mathbb{R}$, а не только $\mathbb{Q}$, ибо мы знаем, что в $\mathbb{R}$ нет решений уравнения $x^2 + 1 = 0$.

1.6 Комплексные числа

Обозначим через $\mathfrak{M}$ множество пар (a, b), где $a, b \in \mathbb{R}$.
Две пары (a_1, b_1) и (a_2, b_2) считаются равными $\Leftrightarrow$ когда $a_1 = a_2$, $b_1 = b_2$.
И введем на этом множестве операции сложения и умножения:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2,\ a_1 b_2 + a_2 b_1).$$

Из определения операций следует, что они замкнуты на $\mathfrak{M}$. Пара $(0, 0)$ играет роль нуля по сложению, а пара $(1, 0)$ — роль 1 по умножению. Обратной к паре (a, b) по сложению будет пара $(-a, -b)$. И теперь без труда убеждаемся, что относительно сложения $\mathfrak{M}$ — абелева группа.
Коммутативность умножения очевидна. Проверим ассоциативность.

$$((a, b) \cdot (c, d))\,(e, f) = (ac - bd, ad + bc)(e, f) =$$
$$= (ace - bde - adf - bcf, acf - bdf + ade + bce);$$
$$(a, b)\,((c, d) \cdot (e, f)) = (a, b)(ce - df, cf + de) =$$
$$= (ace - adf - bcf - bde, acf + ade + bce - bdf).$$

Правые части рассматриваемых равенств совпали. Поэтому, чтобы убедиться, что $\mathfrak{M}$ — поле, осталось показать, что каждая пара $(a, b) \neq (0, 0)$ обратима. Для этого рассмотрим произведение

$$(a, b) \cdot (x, y) = (ax - by, ay + bx)$$

и выясним, существуют ли $x, y \in \mathbb{R}$, для которых

$$\begin{cases} ax - by = 1, \\ ay + bx = 0. \end{cases}$$

Решая эту систему методом исключения, получим:

$$x = \frac{a}{a^2 + b^2}, \qquad y = \frac{-b}{a^2 + b^2} \qquad \left(\text{ибо } a^2 + b^2 \neq 0\right).$$

Но тогда

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}; \frac{-b}{a^2 + b^2}\right).$$

Итак, каждый ненулевой элемент из $\mathfrak{M}$ обратим.
Дистрибутивность умножения по сложению проверяется непосредственно. А потому выполнены все аксиомы поля, значит $\mathfrak{M}$ — поле.

Выясним теперь, удовлетворяет ли поле $\mathfrak{M}$ нашим запросам. Обозначим через D — множество пар вида $(a, 0)$, $a \in \mathbb{R}$. Относительно операций, определенных на $\mathfrak{M}$, множество D — поле. В частности,

$$(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0),$$
$$(a_1, 0) \cdot (a_2, 0) = (a_1 a_2 - b_1 b_2, 0),$$
$$(0, 0) \in D,\ (1, 0) \in D.$$

Это показывает, что относительно операций сложения и умножения, определенных на $\mathfrak{M}$, поле D «похоже» на $\mathbb{R}$. Если мы установим отображение D в $\mathbb{R}$: $(a, 0) \to a$, то это отображение будет взаимно однозначным отображением D в $\mathbb{R}$, сохраняющимся при операциях, определенных на этих полях. А потому естественно отождествить D и $\mathbb{R}$, и поскольку D — поле в $\mathfrak{M}$, то мы можем говорить, что $\mathbb{R}$ подполе в $\mathfrak{M}$, то есть $\mathfrak{M}$ — расширение поля $\mathbb{R}$ (с точностью до обозначений). Покажем, что в $\mathfrak{M}$ разрешимо уравнение

$$x^2 + 1 = 0,$$

то есть покажем, что найдется пара (a, b), такая, что

$$(a, b)^2 + (1, 0) = (0, 0).$$

Или

$$(a^2 - b^2, 2ab) + (1, 0) = (0, 0),$$
$$(a^2 - b^2 + 1, 2ab) = (0, 0).$$

Для определения a и b имеем систему уравнений:

$$\begin{cases} a^2 - b^2 + 1 = 0, \\ 2ab = 0, \end{cases}$$

(мы пользуемся тем, что две пары считаются равными $\Leftrightarrow$ когда соответственно равны их компоненты). Из второго равенства заключаем, что либо a, либо b равны нулю.

1. если $b = 0$, то $a^2 + 1 = 0$, что для $a \in \mathbb{R}$ невозможно;

2. если $a = 0$, то $-b^2 + 1 = 0$, то есть $b = \pm 1$.

Итак, пары $(0, 1)$ и $(0, -1)$ являются решениями уравнения $x^2 + 1 = 0$ в поле $\mathfrak{M}$. Поэтому выполнено и второе требование на искомое поле.

Чтобы доказать минимальность $\mathfrak{M}$, мы воспользуемся новой записью элементов из $\mathfrak{M}$. Мы уже заметили, что пары вида $(a, 0)$ могут быть отождествлены с элементами a. Поэтому обозначим $(a, 0)$ через a, в частности $(0, 0)$ через 0, а $(1, 0)$ через 1. Кроме того обозначим $(0, 1)$ через i. Для пары (a, b) имеем

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1).$$

А потому естественно обозначить пару (a, b) через $a + b \cdot i$. Если еще вспомнить, что $(0, 1)^2 = (-1, 0)$, то получим $i^2 = -1$, а это дает возможность естественно производить операции сложения и умножения:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i,$$
$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.$$

Условимся теперь множество $\mathfrak{M}$ обозначать через $\mathbb{C}$, элементами которого служат $a + b \cdot i$.

Поле $\mathbb{C}$ называется **полем комплексных чисел**.

Теперь мы покажем, что $\mathbb{C}$ удовлетворяет условию минимальности. Пусть P — произвольное расширение $\mathbb{R}$, в котором разрешимо уравнение $x^2 + 1 = 0$. Не ограничивая общности, можно считать, что решение этого уравнения обозначено через i, так что $(i)^2 = -1$. Поскольку $\mathbb{R} \subset \mathrm{P}$, то для любого $b \in \mathbb{R}$ имеем $b \cdot i \in \mathrm{P}$, а значит и $a + bi \in \mathbb{R}$ $(a, b \in \mathbb{R})$. Но тогда $\mathbb{C} \subset \mathrm{P}$, ибо $\mathbb{C}$ исчерпывается элементами вида $a + bi$, $a, b \in \mathbb{R}$. Таким образом минимальность доказана. Этим также показано, что **единственное** поле (с точностью до обозначения его элементов), удовлетворяющее поставленным выше трем условиям.

При изучении чисел в школе мы постепенно расширяли числовое множество. При этом основное ударение делалось на тот факт, что такие расширения позволяют нам более свободно оперировать с числами. Так, при переходе от натуральных чисел к целым становится возможным вычитать любые числа, при

переходе к рациональным становится возможным делить любые числа и т.д. На самом деле более важным результатом таких расширений оказывается тот факт, что свойства расширенной системы часто позволяют получать новые результаты об исходной системе. Так, например, многие сложные классические задачи теории чисел, касающиеся только натуральных чисел, были решены с использованием действительных и даже комплексных чисел.

Исторически комплексные числа появились именно как средство решения некоторых задач о действительных числах. Так, итальянский математик Кардано (XVI в.) при решении кубических уравнений находил правильные действительные корни, используя в промежуточных вычислениях «несуществующие» квадратные корни из отрицательных чисел.

Со временем комплексные числа занимали все более важное место в математике и ее приложениях. Поэтому и нам не мешает их подробнее изучить.

Комплексные числа обычно обозначаются буквой z, т.е. $z = a + bi$, и, следуя историческим традициям, принято a называть **действительной частью** комплексного числа z , b — **мнимой частью**. Часто еще пишут $a = Rez\,, b = Imz$. Операции над комплексными числами нами уже изучены как операции над парами, поэтому только перечислим их:

1. $(a + bi) + (c + di) = (a + c) + (b + d)i$,
2. $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$,
3. $(a + bi)^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{-b}{a^2 + b^2}i$.

Так что решением уравнения

$$(a + bi)x = c + di$$

$$\text{будет} \qquad x = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}i.$$

Комплексное число $a - bi$ называется **сопряженным** (**комплексно сопряженным**) к $z = a + bi$, и обозначается через $\bar{z}$.

Свойства операции комплексного сопряжения

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,
3. Пусть $z = a + bi$, тогда $z\bar{z} = a^2 + b^2$,
4. $\overline{z_1} + \overline{z_2} = 2Rez,\ z - \bar{z} = 2Imz$.

5. Комплексное число $z = a$ будет вещественным (т.е. $Imz = 0$) $\Leftrightarrow$ когда $z = \overline{z}$.

В поле $\mathbb{R}$ любых два различных числа могут быть соединены знаком $>$. Оказывается, что в поле $\mathbb{C}$ это свойство сохранить нельзя. Точнее говоря, в поле $\mathbb{R}$ из $a > b$ и $c > d \Rightarrow ac > bd$ для всех a, b, c, d. Если бы и в $\mathbb{C}$ можно было сравнивать числа с указанным выше свойством знака $>$, то мы имели бы, что числа i и 0 удовлетворяли бы одному из соотношений

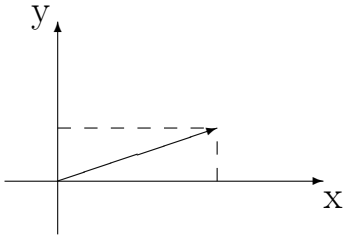
$$1)\, i > 0; \qquad 2)\, i < 0.$$

В случае 1) мы имели бы тогда $-1 = i^2 > 0$, что невозможно. А во втором случае, из $-i > 0 \Rightarrow (-i)^2 = -1 > 0$, что снова нелепо.
Вот почему в поле $\mathbb{C}$ сравнение чисел не проводится.

До появления комплексных чисел каждое вещественное число имело геометрическую интерпретацию. А потому естественно наше желание дать геометрическую интерпретацию и комплексным числам. Но на вещественной прямой свободных мест нет. Пришлось подумать о плоскости. Этому способствовало наше первоначальное определение комплексных чисел как пар чисел (a, b). Но именно так задаются точки на плоскости. Итак

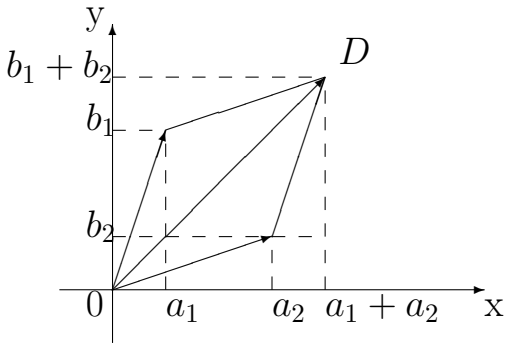
Геометрическая интерпретация комплексных чисел

Введем на плоскости прямоугольную систему координат XOY и поставим в соответствие каждому комплексному числу $z = a + bi$ точку плоскости с координатами (a, b). Это соответствие взаимно однозначное. Поэтому саму плоскость часто называют **комплексной плоскостью**.
Поскольку каждая точка плоскости XOY



однозначно определяет вектор, исходящий из начала и с концом в данной точке, то между такими **векторами и комплексными числами установлено взаимно однозначное соответствие**. Это вторая форма геометрической интерпретации комплексных чисел. Она позволяет дать геометрическое изображение суммы двух комплексных чисел.

Действительно, пусть $z_1 = a_1 + b_1 i$ и $z_2 = a_2 + b_2 i$. Рассмотрим на плоскости соответствующие им векторы



Из рисунка видно, что координаты точки D равны $a_1 + a_2$ и $b_1 + b_2$. Но в точке D находится конец вектора, являющегося суммой векторов, соответствующих числам z_1 и z_2.

Заметим еще, что для того чтобы найти вектор, соответствующий разности комплексных чисел $z_1 - z_2$, надо сложить векторы, соответствующие числам z_1 и $-z_2$.

Геометрическая интерпретация комплексных чисел, однако, не позволяет интерпретировать произведение комплексных чисел. Но на помощь приходит

Тригонометрическая форма комплексных чисел.

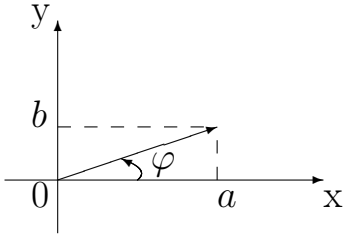
Определение. ***Аргументом*** *комплексного числа z называется угол между положительным направлением оси OX и вектором, соответствующим числу z на комплексной плоскости. При этом углу приписывается знак плюс,если отсчет идет против часовой стрелки, и знак минус, если — по часовой стрелке. Угол определяется неоднозначно, а с точностью до слагаемого $2k\pi$, k — любое целое.*

Аргумент z обозначается *$arg\, z$ (и как сказано выше определяется с точностью до слагаемого $2k\pi, k = 0, \pm 1, \pm 2, \ldots$). Запись $arg\, z = \varphi$ означает, что φ — одно из значений аргумента z.*

Определение. ***Модулем*** *комплексного числа z называется длина соответствующего ему вектора, обозначается $|z|$. Очевидно, если $z = a + bi$, то $|z| = \sqrt{a^2 + b^2}$.*

Ранее мы видели, что $z \cdot \bar{z} = a^2 + b^2$, так что $|z|^2 = z \cdot \bar{z}$.

Пусть $z = a + bi$, $|z| = r$, $arg\, z = \varphi$, тогда из рисунка



видно

$$\cos\varphi = \frac{a}{r},\ \sin\varphi = \frac{b}{r}.$$

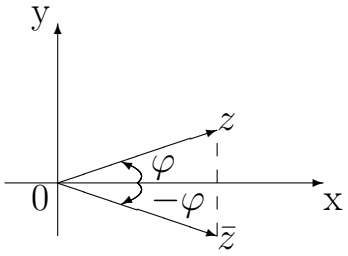
А потому

$$z = a + bi = r\left(\cos\varphi + i\sin\varphi\right).$$

Правая часть полученного равенства называется **тригонометрической формой** комплексного числа z.

Для комплексного числа $z = 0$ значение аргумента не определяется, а его модуль равен 0.

Из рисунка



видно, что **комплексно сопряженные числа имеют равные модули, а их аргументы различаются знаком, то есть** $arg\, z = -arg\, \bar{z}$.

Понятие аргумента комплексного числа обобщает понятие знака вещественного числа, так знаку «+» соответствует $arg\, z = 0$, а знаку «−» соответствут $arg\, z = \pi$.

Тригонометрическая форма комплексного числа позволяет интерпретировать произведение двух комплексных чисел:

$$z_1 = a_1 + b_1 i = |z_1|\left(\cos\varphi_1 + i\sin\varphi_1\right),$$
$$z_2 = a_2 + b_2 i = |z_2|\left(\cos\varphi_2 + i\sin\varphi_2\right).$$

Откуда, после несложных вычислений

$$\begin{aligned} z_1 z_2 = |z_1|\cdot|z_2|[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + \\ + i(\sin\varphi_1\cos\varphi_2 - \sin\varphi_2\cos\varphi_1)] = \\ = |z_1|\cdot|z_2|\left(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\right). \end{aligned}$$

Поэтому заключаем, что **произведением двух комплексных чисел будет комплексное число, модуль которого равен произведению модулей сомножителей, а аргумент равен сумме аргументов сомножителей**.

Это свойство остается справедливым при умножении любого конечного числа комплексных чисел. А потому, если все множители равны между собой, то получаем следующую формулу.

Формула Муавра.

Если $z = |z|(\cos\varphi + i\sin\varphi)$, *то* $z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$, $n \geq 0$ — *целое.*

Далее, поскольку

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{1}{|z|^2}\bar{z} = \frac{1}{|z|}(\cos(-\varphi) + i\sin(-\varphi)),$$

то получаем, если

$$z_1 = a_1 + b_1 i = |z_1|(\cos\varphi_1 + i\sin\varphi_1),$$
$$z_2 = a_2 + b_2 i = |z_2|(\cos\varphi_2 + i\sin\varphi_2),$$

$z_2 \neq 0$, то

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Таким образом, чтобы **разделить два комплексных числа, заданных в тригонометрической форме, необходимо разделить модули этих чисел, а аргументом дроби будет разность аргументов числителя и знаменателя**.

Из полученных результатов мы можем высказать общий принцип: обычная (алгебраическая) форма комплексных чисел приспособлена для выражения аддитивных свойств комплексных чисел, а тригонометрическая форма — для выражения мультипликативных свойств. Нарушение этого принципа приводит к чрезвычайно сложным формулам, затуманивающим суть дела. Подтверждением этой мысли является изучение операции

Извлечение корня.

Пусть задано $z = a + bi$. Всегда ли можно найти комплексное число z', такое, чтобы

$$z' = \sqrt[n]{z},\ n \geq 2 — \text{натуральное}.$$

Пусть сначала $n = 2$. Будем искать z' в виде $z' = x + iy$ так, чтобы

$$\sqrt{a + bi} = x + iy.$$

Это значит

$$a + bi = (x + iy)^2.$$

А потому имеем

$$x^2 - y^2 + i2xy = a + bi.$$

Или

$$\begin{cases} x^2 - y^2 = a, \\ 2xy = b, \end{cases} \quad \Rightarrow \quad \begin{cases} x^2 - y^2 = a, \\ (x^2 + y^2)^2 = a^2 + b^2, \end{cases} \quad \Rightarrow$$

$$\Rightarrow \qquad \begin{cases} x^2 - y^2 = a, \\ x^2 + y^2 = +\sqrt{a^2 + b^2}. \end{cases}$$

Таким образом

$$x^2 = \frac{a}{2} + \frac{\sqrt{a^2 + b^2}}{2}, \qquad y^2 = -\frac{a}{2} + \frac{\sqrt{a^2 + b^2}}{2}.$$

Мы видим, что правые части выражений для x^2 и y^2 неотрицательны, это означает, что мы можем найти **вещественные** значения x и y (а только такие значения нас устраивают) такие что $\sqrt{a + bi} = x + iy$.
Мы имеем

$$x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}, \qquad y = \pm\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}.$$

Знаки при корнях следует выбрать так, чтобы $sign(xy) = sign\, b$
Итак, мы показали, что **всегда** можно извлечь квадратный корень (причем получаем ровно два значения) из комплексного числа. При этом мы использовали алгебраическую форму комплексного числа. Но метод построения этих корней показывает, что при извлечении корня $n^{\text{ой}}$ степени из комплексного числа, вообще говоря, приходится решать систему $n^{\text{ой}}$ степени с двумя неизвестными, что весьма трудно. Однако тригонометрическая форма комплексного числа легко обходит эту трудность.

Пусть $z = a + bi = r\left(\cos\varphi + i\sin\varphi\right)$, $r = |z|$.
Чтобы извлечь корень $n^{\text{ой}}$ степени из z, положим

$$\sqrt[n]{r\left(\cos\varphi + i\sin\varphi\right)} = \rho\left(\cos\psi + i\sin\psi\right).$$

Отсюда

$$r\left(\cos\varphi + i\sin\varphi\right) = \rho^n\left(\cos n\psi + i\sin n\psi\right).$$

Мы имеем равенство двух комплексных чисел, а потому равны их модули и аргументы (причем аргументы с точностью до слагаемого $2k\pi, k = 0, \pm1, \pm2, \ldots$).
Поэтому

$$r = \rho^n \;\Rightarrow\; \rho = \sqrt[n]{r},$$
$$\varphi = n\psi - 2k\pi \;\Rightarrow\; \psi = \frac{\varphi + 2k\pi}{n},\ k = 0, \pm1, \pm2, \ldots.$$

Из выражения для ψ мы видим, что при $k = 0, 1, \ldots, n-1$ мы получаем существенно различные значения (т.е. отличающиеся между собой на числа не кратные 2π), а все остальные значения ψ совпадают с ними с точностью до слагаемых, кратных 2π. Это означает, что мы получили ровно n различных

комплексных чисел, являющихся корнями $n^{\text{ой}}$ степени из заданного z. Эти значения суть:

$$\sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n}+i\sin\frac{\varphi+2k\pi}{n}\right),\ k=0,1,\ldots,n-1.$$

В частности, имеем

$$\sqrt[n]{1}=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\ k=0,1,\ldots,n-1.$$

О значении корней $n^{\text{ой}}$ степени из 1 говорит следующая

Теорема 1.6.1. *Чтобы получить все корни $n^{ой}$ степени из комплексного числа z, достаточно один из таких корней последовательно умножать на все различные корни $n^{ой}$ степени из 1. Иначе говоря, если z_0 — один из корней $\sqrt[n]{z}$ и $\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{n-1}$ — все корни $\sqrt[n]{1}$, то все корни $n^{ой}$ степени из комплексного числа z суть $z_0\varepsilon_0, z_0\varepsilon_1,\ldots,z_0\varepsilon_{n-1}$.*

Доказательство. Так как $\varepsilon_i^n=1$, $i=0,1,\ldots,n-1$, и $z_0^n=z$, то каждое из чисел $z_0\varepsilon_i$, $i=0,1,\ldots,n-1$, является корнем $n^{\text{ой}}$ степени из комплексного числа z. Поэтому утверждение теоремы будет доказано, если мы покажем, что $z_0\varepsilon_i\neq z_0\varepsilon_j$ при $i\neq j$. Но равенство $z_0\varepsilon_i=z_0\varepsilon_j\ \Rightarrow\ \varepsilon_i=\varepsilon_j\ \Rightarrow\ i=j$. □

Поэтому подробнее изучим

Корни $n^{\text{ой}}$ степени из 1.

Обозначим

$$\varepsilon_k=\left(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\right),\ k=0,1,\ldots,n-1.$$

Ясно, ε_k — корень $n^{\text{ой}}$ степени из 1.
Зафиксируем k и рассмотрим числа

$$\varepsilon_k,\ \varepsilon_k^2,\ \ldots\ ,\varepsilon_k^n. \tag{1.6}$$

Все ли числа в 1.6 различны между собой? Прежде всего замечаем, что каждое из чисел в 1.6 является корнем $n^{\text{ой}}$ степени из 1:

$$\left(\varepsilon_k^l\right)^n=\left(\varepsilon_k^n\right)^l,\ l=1,2,\ldots,n.$$

Прежде чем ответить на поставленный вопрос, рассмотрим

Пример 14. Пусть $n=4$. Тогда

$$\varepsilon_0=1,\ \varepsilon_1=i,\ \varepsilon_2=-1,\ \varepsilon_3=-i.$$

Отсюда видно, что все числа ε_0, ε_0^2, ε_0^3, ε_0^4 совпадают между собой; а числа ε_1, ε_1^2, ε_1^3, ε_1^4 — суть числа i, -1, $-i$, 1 — все различны между собой. Такая же картина будет для ε_3, а в случае ε_2 имеем -1, 1, -1, 1, т.е. хотя они и не все совпали между собой, но встречаются равные

Определение. *Корень ε $n^{ой}$ степени из 1 называется* ***первообразным****, если все числа ε, ε^2, ..., ε^n различны между собой.*

Рассмотренный выше пример показывает, что, вообще говоря, первообразные корни существуют. Значение их состоит в том, что последовательные n степеней первообразного корня ε, например, ε^l, ε^{l+1}, ..., ε^{l+n-1}, порождают все корни $n^{\text{ой}}$ степени из 1 (ибо их n штук, все они различны и являются корнями $n^{\text{ой}}$ степени из 1).
На существование первообразных корней $n^{\text{ой}}$ степени из 1 для любого $n \geq 1$ указывает следующая

Теорема 1.6.2. ***Критерий первообразности корня.***
Корень $\varepsilon_k = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)$ будет первообразным корнем $n^{ой}$ степени из 1 $\Leftrightarrow$ когда $(k,\, n) = 1$.

Доказательство. **Необходимость.** Пусть ε_k — первообразный корень и пусть $d = (k,\, 1)$. Нам нужно показать, что $d = 1$. Но если бы $d > 1$, то среди чисел

$$\varepsilon_k,\ \varepsilon_k^2,\ \ldots\ ,\varepsilon_k^{\frac{n}{d}},\ \ldots\ ,\varepsilon_k^n$$

имелось бы, по крайней мере, два равных, а именно

$$\varepsilon_k^{\frac{n}{d}} = \left(\cos\frac{2k\pi\frac{n}{d}}{n} + i\sin\frac{2k\pi\frac{n}{d}}{n}\right) =$$
$$= \left(\cos 2\pi\frac{k}{d} + i\sin 2\pi\frac{kn}{d}\right) = 1 =$$
$$= \left(\cos 2\pi\frac{kn}{n} + i\sin 2\pi\frac{kn}{n}\right) = \varepsilon_k^n.$$

Достаточность. Пусть $(k,\, n) = 1$ и пусть $1 \leq l_1 < l_2 \leq n$. Из предположения $\varepsilon_k^{l_1} = \varepsilon_k^{l_2}$ следует, что аргументы этих чисел отличаются между собой на число, кратное 2π, т.е.

$$\frac{2kl_1\pi}{n} = \frac{2kl_2\pi}{n} + 2m\pi.$$

Откуда

$$\frac{k(l_1 - l_2)}{n} = m \ \text{— целое число.}$$

А в силу $(k,\, n) = 1 \Rightarrow (l_1 - l_2) \vdots n$, что невозможно, т.к. $0 < |l_1 - l_2| < n$. $\square$

Совокупность всех корней $n^{\text{ой}}$ степени из 1 образует группу по умножению. (**Проверить**). Порядок этой группы равен n. Из определения первообразного корня следует, что эта группа циклическая, так как совпадает с множеством

всех различных степеней первообразного корня. Таким образом всякий первообразный корень $n^{\text{ой}}$ степени из 1 является образующим циклической группы всех корней $n^{\text{ой}}$ степени из 1. Число различных первообразных корней $n^{\text{ой}}$ степени из 1 обозначают через $\varphi(n)$.

Упражнение 6. Доказать, что если $n = p_1^{a_1} \dots p_s^{a_s}$ — каноническое разложение n, то $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$.

2 Пространство n–мерных векторов

2.1 Линейная зависимость

Пусть $\mathbb{R}$ — множество вещественных чисел.

Определение. *Упорядоченный набор n чисел $a_1, \ldots, a_n$ из $\mathbb{R}$ называется n–**мерным вектором** над $\mathbb{R}$.*

n-мерные векторы будем обозначать через $\bar{a}$, $\bar{b}, \ldots$ Элементы $a_1, \ldots, a_n$ называются компонентами вектора $\bar{a}$. Таким образом $\bar{a} = (a_1, \ldots, a_n)$. Совокупность всех n–мерных векторов будем обозначать через $\mathbb{R}^n$.

Два вектора $\bar{a}$ и $\bar{b}$ считаются равными $\Leftrightarrow$ когда $a_i = b_i,\ i = 1, \ldots, n$.

Суммой двух векторов $\bar{a} = (a_1, \ldots, a_n)$ и $\bar{b} = (b_1, \ldots, b_n)$ называем n-мерный вектор $\bar{c} = (c_1, \ldots, c_n)$, где $c_i = a_i + b_i,\ i = 1, \ldots, n$.

Вектор $\bar{0} = (0, \ldots, 0)$ называем нулевым.

Пусть $\alpha \in \mathbb{R}$, то $\alpha\bar{a}$ обозначает вектор, получаемый из $\bar{a} = (a_1, \ldots, a_n)$ по правилу:

$$\alpha\bar{a} = (\alpha a_1, \ldots, \alpha a_n).$$

Справедливы следующие свойства:

1. Для α и$\beta \in \mathbb{R}$ и $\bar{a} \in \mathbb{R}^n$ имеем

$$(\alpha + \beta)\bar{a} = \alpha\bar{a} + \beta\bar{a}.$$

2. Для $\alpha \in \mathbb{R}$ и $\bar{a}$, $\bar{b} \in \mathbb{R}^n$ имеем

$$(\alpha(\bar{a} + \bar{b}) = \alpha\bar{a} + \alpha\bar{b}.$$

3. $0 \cdot \bar{a} = \bar{0}$.

4. $\alpha\bar{a} = \bar{0} \Leftrightarrow$ когда либо $\alpha = 0$, либо $\bar{a} = \bar{0}$.

5. $1 \cdot \bar{a} = \bar{a}$.

Множество $\mathbb{R}^n$ вместе с определенными на нем операциями сложения векторов и умножения их на элементы из $\mathbb{R}$ мы будем называть **пространством n–мерных векторов**.

Определение. *Говорят, что два вектора $\bar{a}$ и $\bar{b}$ пропорциональны, если существует такое $\alpha \in \mathbb{R}$, что либо $\bar{a} = \alpha \cdot \bar{b}$, либо $\bar{b} = \alpha \cdot \bar{a}$.*

Пример 15. Например, векторы $\bar{a} = (1, 1, -2)$ и $\bar{b} = (2, 2, -4)$ — пропорциональны. Векторы $\bar{0}$ и $\bar{a}$ всегда пропорциональны.

Пусть выбрано r векторов $\bar{a}_1, \ldots, \bar{a}_r$ и r элементов из $\mathbb{R}$, тогда сумма

$$c_1\bar{a}_1 + \ldots + c_r\bar{a}_r$$

называется **линейной комбинацией** векторов $\bar{a}_1, \ldots, \bar{a}_r$. Элементы $c_1, \ldots, c_r$ называются **коэффициентами** линейной комбинации.

Определение. *Система векторов (т.е. совокупность векторов) $\bar{a}_1, \ldots, \bar{a}_r \in \mathbb{R}^n$ называется **линейно зависимой**, если найдутся элементы $c_1, \ldots, c_r \in \mathbb{R}$, причем хотя бы одно $c_i \neq 0$, так что линейная комбинация $c_1\bar{a}_1 + \ldots + c_r\bar{a}_r$ равна $\bar{0}$.*

Определение. *Система векторов (т.е. совокупность векторов) $\bar{a}_1, \ldots, \bar{a}_r \in \mathbb{R}^n$ называется **линейно независимой**, если не существует ни одной линейной комбинации этих векторов равной $\bar{0}$, когда хотя бы одно из чисел c_i отлично от нуля, т.е.линейно независимая система векторов $\bar{a}_1, \ldots, \bar{a}_r$ имеет нулевую линейную комбинацию только в одном случае — все коэффициенты c_i этой линейной комбинации равны 0.*

Таким образом, всякая конечная система векторов является либо линейно зависимой, либо линейно независимой.

Определение. *Бесконечная система (совокупность) векторов называется **линейно зависимой**, если линейно зависима хотя бы одна ее конечная подсистема. В противном случае **бесконечная система векторов** называется **линейно независимой**.*

В дальнейшем, если не оговорено, под системой векторов всегда будет пониматься конечная система векторов.

Лемма 2.1.1. *Система векторов $\bar{a}_1, \ldots, \bar{a}_r$ будет линейно зависима $\Leftrightarrow$ когда хотя бы один из векторов $\bar{a}_i\,(i = 1, \ldots, r)$ является линейной комбинацией остальных.*

Доказательство. Пусть $c_1\bar{a}_1+\ldots+c_r\bar{a}_r=\bar{0}$ и хотя бы одно из чисел $c_1,\ldots,c_r$, например, c_i, не равно 0. Тогда, $\bar{a}_i=-\dfrac{c_1}{c_i}\bar{a}_1+\ldots+\left(-\dfrac{c_r}{c_i}\right)\bar{a}_r$.
И наоборот, если $\bar{a}_i=\alpha_1\bar{a}_1+\ldots+\alpha_{i-1}\bar{a}_{i-1}+\alpha_{i+1}\bar{a}_{i+1}+\ldots+\alpha_r\bar{a}_r$, то $c_1\bar{a}_1+\ldots+c_r\bar{a}_r=\bar{0}$, где $c_j=\alpha_j$ при $j\neq i$, $c_i=-1\neq 0$. □

Пример 16. Примером линейно зависимой системы векторов является система, содержащая $\bar{0}$.
Любые два непропорциональных вектора линейно независимы.

Лемма 2.1.2. *Пусть S' — система векторов, а $T\subset S'$ — ее подсистема. Тогда:*

(i) *Из линейной зависимости $T\Rightarrow$ линейная зависимость S'.*

(ii) *Из линейной независимости $S'\Rightarrow$ линейная независимость T .*

(iii) *Утверждения (i) и (ii) необратимы.*

Доказательство этой леммы оставляем читателю.

2.2 Ранг системы векторов

Из рассмотрения векторов из $\mathbb{R}^n$ видно, что чем больше n, тем сложнее структура вектора, например, условия пропорциональности двух векторов необходимо проверять для n чисел. Поэтому естественно возникает вопрос: влияет ли значение n на линейную зависимость системы векторов? Ответ на этот вопрос дает следующая

Теорема 2.2.1. *Любые $n+1$ векторов пространства $\mathbb{R}^n$ линейно зависимы.*

Доказательство. Теорему доказываем методом математической индукции.
Пусть $n=1$. Тогда одномерные векторы — суть элементы из $\mathbb{R}$, а потому для любых α, $\beta\in\mathbb{R}$ имеем 4 возможности:

1. $\alpha=\beta=0\Rightarrow 1\cdot\alpha+1\cdot\beta=1\cdot 0+1\cdot 0=0\Rightarrow$ α, β — линейно зависимы;
2. $\alpha=0$, $\beta\neq 0\Rightarrow 1\cdot\alpha+0\cdot\beta=0\Rightarrow$ α, β — линейно зависимы;
3. $\alpha\neq 0$, $\beta=0\Rightarrow 0\cdot\alpha+1\cdot\beta=0\Rightarrow$ α, β — линейно зависимы;
4. $\alpha\neq 0$, $\beta\neq 0\Rightarrow \beta\cdot\alpha+(-\alpha)\cdot\beta=0\Rightarrow$ α, β — линейно зависимы;

Предположим теперь, что утверждение теоремы верно, для всех пространств $\mathbb{R}^k$, $1 \le k \le n-1$.
Пусть теперь $\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}$ — любые векторы из $\mathbb{R}^n$. Положим

$$\bar{a}_i = (a_1^{(i)}, \ldots, a_n^{(i)}),\ i = 1, \ldots, n, n+1.$$

Обозначим теперь через

$$\bar{b}_i = (a_1^{(i)}, \ldots, a_{n-1}^{(i)}),\ i = 1, \ldots, n, n+1.$$

Векторы $\bar{b}_i$ принадлежат пространству $\mathbb{R}^{n-1}$. Рассмотрим первые n из них $\bar{b}_1, \ldots, \bar{b}_n$. В силу предположения индукции, эти векторы линейно зависимы, а потому найдутся элементы $c_1, \ldots, c_n \in \mathbb{R}$, не все равные 0, например, $c_i \neq 0$, такие, что

$$c_1\bar{b}_1 + \ldots + c_n\bar{b}_n = \bar{0}. \tag{2.1}$$

Теперь составим линейную комбинацию векторов $\bar{a}_1, \ldots, \bar{a}_n$ (это уже векторы из $\mathbb{R}^n$) с тем же набором коэффициентов $c_1, \ldots, c_n$:

$$c_1\bar{a}_1 + \ldots + c_n\bar{a}_n.$$

Результирующий вектор обозначим через $\bar{c}$. Мы замечаем, что первые $n-1$ компонент вектора $\bar{c}$ равны 0 (в силу (2.1)), а последнюю обозначим через c. Таким образом

$$c_1\bar{a}_1 + \ldots + c_n\bar{a}_n = \bar{c} = (0, \ldots, 0, c). \tag{2.2}$$

Ясно, что

$$c = c_1a_1^{(1)} + \ldots + c_na_n^{(n)}.$$

Если $c = 0$, то в силу (2.2) $\Rightarrow$ $\bar{a}_1, \ldots, \bar{a}_n$ — линейно зависимы, а значит, линейно зависимы и $\bar{a}_1, \ldots, \bar{a}_n$, $\bar{a}_{n+1}$ (и теорема доказана).
Если же $c \neq 0$, то из (2.2) имеем

$$\frac{c_1}{c}\bar{a}_1 + \ldots + \frac{c_n}{c}\bar{a}_n = (0, 0, \ldots, 0, 1). \tag{2.3}$$

Мы предположили, что $c \neq 0$. Поэтому рассмотрим еще систему n векторов

$$\bar{a}_1,\ \ldots,\ \bar{a}_{i-1},\ \bar{a}_{i+1},\ \ldots,\ \bar{a}_n,\ \bar{a}_{n+1}$$

и соответствующую ей систему «урезанных» векторов

$$\bar{b}_1,\ \ldots,\ \bar{b}_{i-1},\ \bar{b}_{i+1},\ \ldots,\ \bar{b}_n,\ \bar{b}_{n+1}.$$

Как и раньше, в силу предположения индукции векторы $\bar{b}$ линейно зависимы, как векторы из $\mathbb{R}^{n-1}$ в количестве n. А потому найдутся числа $d_1,\ \ldots,\ d_{i-1},\ d_{i+1},\ \ldots,\ d_n$, не все равные нулю, такие что

$$d_1\bar{b}_1 + \ldots + d_{i-1}\bar{b}_{i-1} + d_{i+1}\bar{b}_{i+1} + \ldots + d_n\bar{b}_n + d_{n+1}\bar{b}_{n+1} = \bar{0}.$$

А потому

$$d_1\bar{a}_1+\ldots+d_{i-1}\bar{a}_{i-1}+d_{i+1}\bar{a}_{i+1}+\ldots+d_n\bar{a}_n+d_{n+1}\bar{a}_{n+1}=\bar{d}=(0,0,\ldots,0,d). \quad (2.4)$$

Если $d=0$, то есть $\bar{d}=\bar{0}$, то система векторов $\bar{a}_1$, $\ldots$, $\bar{a}_{i-1}$, $\bar{a}_{i+1}$, $\ldots$, $\bar{a}_n$, $\bar{a}_{n+1}$, а значит и исходная система векторов $\bar{a}_1$, $\ldots$, $\bar{a}_{n+1}$, линейно зависима.
Если же $d\neq 0$, то подобно 2.3 имеем

$$\frac{d_1}{d}\bar{a}_1+\ldots+\frac{d_{i-1}}{d}\bar{a}_{i-1}+\frac{d_{i+1}}{d}\bar{a}_{i+1}+\ldots+\frac{d_n}{d}\bar{a}_n+\frac{d_{n+1}}{d}\bar{a}_{n+1}=(0,0,\ldots,0,1). \quad (2.5)$$

Вычитая теперь из (2.3) соотношение (2.5) получаем:

$$\left(\frac{c_1}{c}-\frac{d_1}{d}\right)\bar{a}_1+\ldots+\left(\frac{c_{i-1}}{c}-\frac{d_{i-1}}{d}\right)\bar{a}_{i-1}+\left(\frac{c_{i+1}}{c}-\frac{d_{i+1}}{d}\right)\bar{a}_{i+1}+\ldots+$$
$$+\left(\frac{c_n}{c}-\frac{d_n}{d}\right)\bar{a}_n+\left(\frac{c_{n+1}}{c}-\frac{d_{n+1}}{d}\right)\bar{a}_{n+1}=\bar{0}.$$

Итак, мы имеем линейную комбинацию векторов $\bar{a}_1$, $\ldots$, $\bar{a}_n$, $\bar{a}_{n+1}$, равную $\bar{0}$, не все коэффициенты которой, например, $\dfrac{c_i}{c}\neq 0$, равны нулю, а потому эти векторы линейно зависимы. □

Следствие 1. *В пространстве $\mathbb{R}^n$ нет бесконечных линейно независимых систем векторов.*

Следствие 2. *Из доказанной теоремы следует, что всякая система векторов из $\mathbb{R}^n$ содержит не более n – линейно независимых. А потому оправдано следующее*

Определение. ***Рангом*** *системы векторов S называется* ***максимальное число линейно независимых векторов системы.***

Пусть S' состоит из всех векторов пространства $\mathbb{R}^n$ и рассмотрим векторы

$$\bar{e}_1=(1,\,0,\,0,\,\ldots,\,0,\,0),$$
$$\bar{e}_2=(0,\,1,\,0,\,\ldots,\,0,\,0),$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$\bar{e}_n=(0,\,0,\,0,\,\ldots,\,0,\,1).$$

Эти векторы линейно независимые, так как из

$$c_1\bar{e}_1+\ldots+c_n\bar{e}_n=(c_1,\,\ldots,\,c_n)=\bar{0}$$

следует $c_1=c_1=\ldots=c_n=0$.
Таким образом, в S' **имеется** n **– линейно независимых векторов**, а более чем n их быть не может, поэтому **ранг** S **равен** n.

Определение. *Пусть S произвольная система векторов, а $T \subset S$ — ее подсистема. Подсистема T называется* ***максимальной подсистемой*** *векторов системы S, если она линейно независима, но присоединение к ней любого вектора из S превращает ее в линейно зависимую систему векторов.*

Из этого определения ясно, как определять ранг системы S. Достаточно рассмотреть все ее максимальные подсистемы, и тогда, та из них, которая содержит максимальное число векторов, определяет ранг системы. Но практически мы не всегда в состоянии обозреть все максимальные подсистемы. К счастью, как мы увидим позже, этого делать и не нужно.

Теорема 2.2.2. *Пусть T — подсистема системы S векторов из $\mathbb{R}^n$. Тогда ранг T будет равен рангу S $\Leftrightarrow$ когда каждый вектор из S является линейной комбинацией векторов из T.*

Доказательство. **Необходимость.** Пусть ранг S =ранг $T = r$ и пусть $\bar{a}_1, \ldots, \bar{a}_r$ — r-линейно независимых векторов из T (такие векторы обязательно имеются в T). Обозначим через

$$S_i = \{\bar{a}_1, \ldots, \bar{a}_r, b_i\},$$

где b_i — выбранный вектор из S (то есть для каждого $b_i \in S$ мы рассматриваем свою подсистему S_i).

Количество векторов в подсистеме S_i равно $r + 1$, а потому эти векторы линейно зависимы. Пусть

$$c_1\bar{a}_1 + \ldots + c_r\bar{a}_r + d_i\bar{b}_i = \bar{0}$$

— линейная комбинация, не все коэффициенты которой равны 0. В частности $d_i \neq 0$ (ибо иначе мы имели бы нулевую комбинацию

$$c_1\bar{a}_1 + \ldots + c_r\bar{a}_r = \bar{0}$$

не все коэффициенты которой равны 0, что противоречит линейной независимости $a_1, \ldots, a_r$).
Отсюда

$$\bar{b}_i = -\frac{c_1}{d_i}\bar{a}_1 + \ldots + \left(-\frac{c_r}{d_i}\right)\bar{a}_r.$$

В силу произвола в выборе вектора $\bar{b}_i$ необходимость доказана.
Достаточность. Пусть ранг $T = r$, ранг $S = r'$, $r' \geq r$, и пусть каждый вектор из S является линейной комбинацией векторов из T. Пусть $a_1, \ldots, a_r$ — линейно независимые векторы из T. Обозначим эту совокупность через R и заметим, что ее ранг равен r. Поскольку $R \subset T$, то по только что доказанному каждый вектор из T является линейной комбинацией векторов из R, а потому

и каждый вектор из S является линейной комбинацией векторов из R. Итак, для каждого $b_i \in S$ имеем

$$\bar{b}_i = \alpha_1^{(i)}\bar{a}_1 + \ldots + \alpha_r^{(i)}\bar{a}_r. \tag{2.6}$$

Обозначим через $\bar{\alpha}_i$ вектор $(\alpha_1^{(i)}, \ldots, \alpha_r^{(i)})$. Это вектор пространства $\mathbb{R}^r$. В силу теоремы 2.2.1 любые $(r+1)$ векторов этого пространства линейно зависимы. Пусть $\bar{b}_1, \ldots, \bar{b}_r, \bar{b}_{r+1}$ — любые $(r+1)$ векторов из S, а $\bar{\alpha}_1, \ldots, \bar{\alpha}_{r+1}$ — соответствующие им векторы из пространства $\mathbb{R}^r$. Но тогда найдутся элементы $c_1, \ldots, c_{r+1} \in \mathbb{R}$ такие, что

$$c_1\bar{\alpha}_1 + \ldots + c_{r+1}\bar{\alpha}_{r+1} = \bar{0} \in \mathbb{R}^r.$$

Поэтому мы имеем r равенств (из сравнения r компонент векторов в последнем равенстве):

$$\begin{cases} c_1\alpha_1^{(1)} + c_2\alpha_1^{(2)} + \ldots + c_{r+1}\alpha_1^{(r+1)} = 0, \\ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ c_1\alpha_r^{(1)} + c_2\alpha_r^{(2)} + \ldots + c_{r+1}\alpha_r^{(r+1)} = 0. \end{cases} \tag{2.7}$$

Рассмотрим теперь линейную комбинацию векторов $\bar{b}_1, \ldots, \bar{b}_{r+1}$ с коэффициентами $c_1, \ldots, c_{r+1}$:

$$c_1\bar{b}_1 + \ldots + c_{r+1}\bar{b}_{r+1},$$

или подставляя вместо $\bar{b}_i$ их выражения из (2.6) получаем

$$\begin{aligned} c_1\bar{b}_1 + \ldots + c_{r+1}\bar{b}_{r+1} &= c_1(\alpha_1^{(1)}\bar{a}_1 + \ldots + \alpha_r^{(1)}\bar{a}_r) + \ldots + \\ &\quad + c_{r+1}(\alpha_1^{(r+1)}\bar{a}_1 + \ldots + \alpha_r^{(r+1)}\bar{a}_r) = \\ &= (c_1\alpha_1^{(1)} + \ldots + c_{r+1}\alpha_1^{(r+1)})\bar{a}_1 + \ldots + (c_1\alpha_r^{(1)} + \ldots + c_{r+1}\alpha_r^{(r+1)})\bar{a}_r. \end{aligned}$$

Но в силу равенств (2.7) коэффициенты при $a_1, \ldots, a_r$ в последнем равенстве равны 0. Поэтому

$$c_1\bar{b}_1 + \ldots + c_{r+1}\bar{b}_{r+1} = \bar{0}.$$

Итак, любые $(r+1)$ векторов из S линейно зависимы, а потому $r' < r+1$, что в силу неравенства $r \leq r' \Rightarrow r = r'$. □

Следствие 1. *Если к системе S векторов из $\mathbb{R}^n$ добавить вектор, являющийся линейной комбинацией векторов из S, то он не изменит ранга системы S.*

Следствие 2. *Любые две максимальные подсистемы T_1 и T_2 векторов системы S содержат одинаковое число векторов.*

Доказательство. В самом деле, ранги этих подсистем совпадают с числом векторов в них. Обозначим через $T = T_1 \bigcup T_2$. Ясно, что $T \subset S$, $T_1 \subset T$, $T_2 \subset T$. Каждый вектор из T можно представить линейной комбинацией векторов только из T_1 (и аналогично, линейной комбинацией векторов только изT_2). Это следует из того, что каждый вектор $\bar{a}$ из T либо принадлежит T_1, и тогда $\bar{a} = \bar{a}$, либо $\bar{a} \in T_2$, но в силу максимальности системы T_1 в S, обязательно система векторов $T_1 \bigcup \bar{a}$ линейно зависима, и тогда $\bar{a}$ представляется линейной комбинацией векторов из T_1 (почему?). Аналогично и для T_2. Таким образом согласно предыдущей теореме

$$\text{ранг}\, T_1 = \text{ранг}\, T = \text{ранг}\, T_2.$$

□

Следствие 3. *Ранг системы S векторов из $\mathbb{R}^n$ равен числу векторов в* ***любой*** *ее максимальной подсистеме.*

Определение. *Любая максимальная подсистема T системы S называется* ***базой системы*** *S.*

Определение. *База пространства $\mathbb{R}^n$ называется* ***базисом*** *этого пространства.*

Теорема 2.2.3. *Пусть $\bar{a}_1, \ldots, \bar{a}_n$ — базис пространства $\mathbb{R}^n$. Тогда представление любого вектора $\bar{a} \in \mathbb{R}^n$ через базис однозначно.*

Доказательство. Для каждого $\bar{a} \in \mathbb{R}^n$ хотя бы одно представление существует, ибо система $S = \mathbb{R}^n$ и подсистема $T = \{\bar{a}_1, \ldots, \bar{a}_n\}$ удовлетворяют необходимому условию теоремы 2.2.2. Предположим, что имеют место два представления $\bar{a}$:

$$\bar{a} = c_1\bar{a}_1 + \ldots + c_n\bar{a}_n,$$
$$\bar{a} = d_1\bar{a}_1 + \ldots + d_n\bar{a}_n.$$

Тогда

$$\bar{0} = \bar{a} - \bar{a} = (c_1 - d_1)\bar{a}_1 + \ldots + (c_n - d_n)\bar{a}_n \;\Rightarrow$$

в силу линейной независимости $\bar{a}_1, \ldots, \bar{a}_n$ обязательно $c_1 = d_1, \ldots, c_n = d_n$. □

Для эффективного представления векторов системы S через ее базу, а также для исследования системы векторов на линейную зависимость удобно использовать следующий метод Штифеля.

2.3 Метод Штифеля

Пусть $\bar{a}_1, \ldots, \bar{a}_r$ - база системы векторов S.
Как найти коэффициенты представления любого вектора $\bar{a} \in S$ через эту базу? Нам известны только компоненты $(a_1, \ldots, a_n)$ вектора $\bar{a}$. Какую они несут в себе информацию?

Рассмотрим систему векторов $\bar{e}_i = (0, \ldots, 1, 0, \ldots, 0, \ldots, 0), 1$ стоит на $i^{\text{ом}}$ месте, $i = 1, \ldots, n$. Как мы видели ранее эти векторы составляют базис пространства $\mathbb{R}^n$. Если $\bar{a} = (a_1, \ldots, a_n)$, то имеем

$$\bar{a} = a_1\bar{e}_1 + \ldots + a_n\bar{e}_n,$$

то есть компоненты вектора $\bar{a}$ представляют собой коэффициенты представления этого вектора через вполне определенный базис пространства $\mathbb{R}^n$. А как быть в общем случае?

Пусть $\bar{x}_1, \ldots, \bar{x}_n$ — произвольный базис пространства $\mathbb{R}^n$. Пусть $\bar{y}_1, \ldots, \bar{y}_m$ — произвольная система векторов из $\mathbb{R}^n$. Пусть мы знаем представление этих векторов через базис $\bar{x}_1, \ldots, \bar{x}_n$:

$$\bar{y}_i = a_{i1}\bar{x}_1 + \ldots + a_{in}\bar{x}_n, \qquad i = 1, \ldots, m. \tag{2.8}$$

Равенства (2.8) запишем в виде таблицы (2.9)

	$\bar{x}_1$	$\bar{x}_2$	$\ldots$	$\bar{x}_s$	$\ldots$	$\bar{x}_n$
$\bar{y}_1$	a_{11}	a_{12}	$\ldots$	a_{1s}	$\ldots$	a_{1n}
$\bar{y}_2$	a_{21}	a_{22}	$\ldots$	a_{2s}	$\ldots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$\bar{y}_r$	a_{r1}	a_{r2}	$\ldots$	$\boxed{a_{rs}}$	$\ldots$	a_{rn}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$\bar{y}_m$	a_{m1}	a_{m2}	$\ldots$	a_{ms}	$\ldots$	a_{mn}

(2.9)

Пусть $a_{rs} \neq 0$. Тогда из $r^{\text{го}}$ равенства системы (2.8)(равно как и из $r^{\text{го}}$ равенства таблицы (2.9)) мы можем выразить $\bar{x}_s$ через $\bar{x}_1, \ldots, \bar{x}_{s-1}, \bar{x}_{s+1}, \ldots, \bar{x}_n$ и $\bar{y}_r$:

$$\bar{x}_s = \frac{1}{a_{rs}}(-a_{r,1}\bar{x}_1 - \ldots - a_{r,s-1}\bar{x}_{s-1} + \bar{y}_r - a_{r,s+1}\bar{x}_{s+1} - \ldots - a_{r,n}\bar{x}_n).$$

Но тогда и все векторы $\bar{y}_1, \ldots, \bar{y}_{r-1}, \bar{y}_{r+1}, \ldots, \bar{y}_m$ могут быть выражены через $\bar{x}_1, \ldots, \bar{x}_{s-1}, \bar{y}_r, \bar{x}_{s+1}, \ldots, \bar{x}_n$. Это дает таблицу (2.10):

	$\bar{x}_1$	$\ldots$	$\bar{y}_r$	$\ldots$	$\bar{x}_n$
$\bar{y}_1$	b'_{11}	$\ldots$	b'_{1s}	$\ldots$	b'_{1n}
$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$\bar{x}_s$	b'_{r1}	$\ldots$	b'_{rs}	$\ldots$	b'_{rn}
$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$\bar{y}_m$	b'_{m1}	$\ldots$	b'_{ms}	$\ldots$	b'_{mn}

(2.10)

Заметим, что индексы при «b'» задаются номерами строк и столбцов матрицы, где находятся элементы b', а не индексами соответствующих $\bar{x}$ и $\bar{y}$.
Простые вычисления показывают, что

$$b'_{ij} = \frac{a_{ij}a_{rs} - a_{is}a_{rj}}{a_{rs}}, \qquad \text{если } i \neq r;\ j \neq s;$$
$$b'_{rj} = -\frac{a_{rj}}{a_{rs}}, \qquad \text{если } j \neq s;$$
$$b'_{is} = \frac{a_{is}}{a_{rs}}, \qquad \text{если } i \neq r;$$
$$b'_{rs} = \frac{1}{a_{rs}}.$$

Для удобства дальнейших вычислений мы заменим таблицу (2.10) таблицей (2.11), которая получается из таблицы (2.10) умножением всех ее элементов b' на число a_{rs}:

	$\bar{x}_1$	$\dots$	$\bar{y}_r$	$\dots$	$\bar{x}_n$
$\bar{y}_1$	b_{11}	$\dots$	a_{1s}	$\dots$	b_{1n}
$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$	$\vdots$
$\bar{x}_s$	$-a_{r1}$	$\dots$	1	$\dots$	$-a_{rn}$
$\vdots$	$\vdots$	$\dots$	$\vdots$	$\dots$	$\vdots$
$\bar{y}_m$	b_{m1}	$\dots$	a_{ms}	$\dots$	b_{mn}

$\div\, a_{rs}.$ (2.11)

(Мы справа указали, что элементы таблицы необходимо разделить на a_{rs} — его обычно называют **разрешающим элементом**).
Записывать таблицу (2.11) более удобно, так как у нее легко выписываются элементы $r^{\text{ой}}$ строки и $s^{\text{го}}$ столбца.

Теперь заметим, что векторы $\bar{x}_1, \dots, \bar{y}_r, \dots, \bar{x}_n$ (т.е. векторы, лежащие вверху таблицы) линейно независимы. Действительно, если бы

$$c_1\bar{x}_1 + \dots + c_{s-1}\bar{x}_{s-1} + c_s\bar{y}_r + c_{s+1}\bar{x}_{s+1} + \dots + c_n\bar{x}_n = \bar{0}$$

и не все $c_i = 0$, то обязательно $c_s \neq 0$ (иначе векторы $\bar{x}_1, \dots, \bar{x}_{s-1}, \bar{x}_{s+1}, \dots, \bar{x}_n$ были бы линейно зависимыми). Но тогда для вектора $\bar{y}_r$ имелось бы два представления через базис $\bar{x}_1, \dots, \bar{x}_n$, а именно в одном представлении коэффициент при $\bar{x}_s$ равен $a_{rs} \neq 0$ а во втором представлении коэффициент при $\bar{x}_s$ равен 0. Полученное противоречие доказывает линейную независимость $\bar{x}_1, \dots, \bar{x}_{s-1}, \bar{y}_r, \bar{x}_{s+1}, \dots, \bar{x}_n$. Этот процесс продолжаем далее, т.е. находим строку для $\bar{y}$ и столбец для $\bar{x}$, на пересечении которых лежит ненулевой коэффициент , а затем осуществляем переброс $\bar{y}$ на место $\bar{x}$, и т.д. Возможны два исхода:

1. все $\bar{y}_i$, $i = 1, \dots, n$, переброшены наверх, а потому они являются линейно независимыми векторами;

2. не все $\bar{y}_i$, $i = 1, \ldots, n$, переброшены, но дальнейший переброс невозможен, ибо мы перешли к таблице вида (с точностью до переобозначения индексов):

	$\bar{y}_1$	$\ldots$	$\bar{y}_k$	$\bar{x}_{k+1}$	$\ldots$	$\bar{x}_n$
$\bar{x}_1$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\bar{x}_k$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\bar{y}_{k+1}$	$\cdot$	$\cdot$	$\cdot$	0	$\ldots$	0
$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\vdots$	$\ldots$	$\vdots$
$\bar{y}_m$	$\cdot$	$\cdot$	$\cdot$	0	$\ldots$	0

(2.12)

В этом случае векторы $\bar{y}_{k+1}, \ldots, \bar{y}_m$ являются линейными комбинациями векторов $\bar{y}_1, \ldots, \bar{y}_k$, причем в таблице (2.12) даже найдены коэффициенты этих линейных комбинаций, если только предварительно разделить коэффициенты таблицы на все разрешающие элементы a_{rs} промежуточных шагов.

таким образом, мы описали эффективный алгоритм исследования на линейную зависимость произвольной системы векторов из $\mathbb{R}^n$. Этот алгоритм есть частный случай общего метода, разработанного **Штифелем**.

А теперь мы в состоянии ответить на вопрос, поставленный выше: как найти коэффициенты линейного представления вектора $\bar{a}$ (или даже совокупности векторов) из некоторой системы S через базу этой системы? Для этого выписываем вектор $\bar{a}$ (или данный набор векторов) и базу системы в таблицу вида (2.9), где в качестве $\bar{x}_1, \ldots, \bar{x}_n$ взяты базисные векторы пространства $\bar{e}_1, \ldots, \bar{e}_n$. Роль коэффициентов a_{ij} играют компоненты вектора $\bar{a}$ и базы системы S. А затем последовательно перебрасываем векторы базы системы S (это всегда можно сделать в силу линейной независимости векторов базы). После переброса всей базы процесс обязательно оборвется (почему?), а из полученной таблицы найдем коэффициенты представления вектора $\bar{a}$ (или набора векторов) в новой базе.

Пример 17. Пусть в пространстве $\mathbb{R}^4$ выбрана система S с базой $\bar{a}_1 = (1, -1, 2, 1)$, $\bar{a}_2 = (0, 2, 1, 4)$, $\bar{a}_3 = (2, 2, 5, -1)$. Узнать, принадлежат ли векторы $\bar{a} = (0, -6, -2, -1)$, $\bar{b} = (-1, -1, -2, 3)$ системе S.

	$\bar{e}_1$	$\bar{e}_2$	$\bar{e}_3$	$\bar{e}_4$
$\bar{a}_1$	$\boxed{1}$	-1	2	1
$\bar{a}_2$	0	2	1	4
$\bar{a}_3$	2	2	5	-1
$\bar{a}$	0	-6	-2	-1
$\bar{b}$	-1	-1	-2	3

$\Rightarrow$

	$\bar{a}_1$	$\bar{e}_2$	$\bar{e}_3$	$\bar{e}_4$
$\bar{e}_1$	1	1	-2	-1
$\bar{a}_2$	0	2	$\boxed{1}$	4
$\bar{a}_3$	2	4	1	-3
$\bar{a}$	0	-6	-2	-1
$\bar{b}$	-1	-2	0	4

$\Rightarrow$

	$\bar{a}_1$	$\bar{e}_2$	$\bar{a}_2$	$\bar{e}_4$
$\bar{e}_1$	1	5	-2	7
$\bar{e}_3$	0	-2	1	-4
$\bar{a}_3$	2	$\boxed{2}$	1	-7
$\bar{a}$	0	-2	-2	7
$\bar{b}$	1	-2	0	4

$\Rightarrow$

	$\bar{e}_1$	$\bar{a}_3$	$\bar{a}_2$	$\bar{e}_4$
$\bar{e}_1$	-8	5	-9	49
$\bar{e}_3$	4	-2	4	6
$\bar{e}_2$	-2	1	-1	7
$\bar{a}$	4	-2	-2	0
$\bar{b}$	6	-2	2	-6

$\div 2$

Из таблицы заключаем, что вектор $\bar{a} \in S$, причем $\bar{a} = 2\bar{a}_1 - \bar{a}_2 - \bar{a}_3$, а вектор $\bar{b} \bar{\in} S$, ибо он не представляется через базу этой системы.

3 Матрицы и определители

3.1 Линейные отображения и матрицы

Пусть $L_1 = \mathbb{P}^m$ и $L_2 = \mathbb{P}^n$ два подпространства n–мерных векторов над полем $\mathbb{P}$. Пусть f — отображение L_1 в L_2.

Определение. *Отображение $f : L_1 \to L_2$ называется* ***линейным отображением****, если выполняются следующие условия:*

1. *для любых $\bar{a}$ и $\bar{b}$ из L_1*

$$f(\bar{a} + \bar{b}) = f(\bar{a}) + f(\bar{b})$$

(заметим, что сумма $(\bar{a} + \bar{b})$ вычисляется в L_1, а $f(\bar{a}) + f(\bar{b})$ в L_2);

2. *для любого $\alpha \in \mathbb{P}$ и $\bar{a} \in L_1$*

$$f(\alpha\bar{a}) = \alpha f(\bar{a}).$$

Если для удобства условиться нулевой вектор из L_1 обозначать через $\bar{0}_1$, а из L_2 — через $\bar{0}_2$, то для линейного отображения имеем

$$f(\bar{0}_1) = \bar{0}_2.$$

В самом деле, возьмем $\alpha = 0 \in \mathbb{P}$, тогда $\bar{0}_1 = 0 \cdot \bar{a}$, $\bar{a} \in L_1$, а потому

$$f(\bar{0}_1) = f(0 \cdot \bar{a}) = 0 \cdot f(\bar{a}) = \bar{0}_2.$$

Вектор $f(\bar{a}) \in L_2$ называем образом вектора $\bar{a} \in L_1$, а сам вектор $\bar{a}$ его прообразом.
В пространствах $L_1 = \mathbb{P}^m$ и $L_2 = \mathbb{P}^n$ зафиксируем базисы

$$X = \{\bar{x}_1, \ldots, \bar{x}_m\} \subset L_1,\ Y = \{\bar{y}_1, \ldots, \bar{y}_n\} \subset L_2.$$

Выразим образы векторов $f(\bar{x}_i)$ через базис Y:

$$f(\bar{x}_1) = \sum_{j=1}^{n} a_{1j}\bar{y}_j,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$f(\bar{x}_i) = \sum_{j=1}^{n} a_{ij}\bar{y}_j,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$f(\bar{x}_m) = \sum_{j=1}^{n} a_{mj}\bar{y}_j.$$

Коэффициенты a_{ij} определяются однозначно, ибо представление вектора через базис однозначно.

Определение. *Таблица, составленная из чисел* a_{ij}

$$A_f = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

называется ***матрицей линейного отображения*** $f : \mathbb{P}^m \to \mathbb{P}^n$ *относительно базисов* X *и* Y.

Замечание 1. Матрица отображения f существенно зависит от выбора базисов X и Y.

Замечание 2. Число строк матрицы A_f равно m, а число столбцов — n. Иногда говорят, что A_f — матрица размера $m \times n$.

Если в $\mathbb{P}^m$ и $\mathbb{P}^n$ выбрать стандартные базисы $\{\bar{e}_1, \dots, \bar{e}_m\}$ и $\{\bar{e}'_1, \dots, \bar{e}'_n\}$,

$$\bar{e}_i = \underbrace{(0, \dots, 1, 0, \dots, 0)}_{m},\ \bar{e}'_j = \underbrace{(0, \dots, 1, 0, \dots, 0)}_{n}$$

(1 стоит на $i^{\text{ом}}$, соответственно, $j^{\text{ом}}$, месте), то коэффициенты матрицы A_f определяются совсем просто: $i^{\text{ая}}$ строка матрицы A_f состоит из компонент вектора $f(\bar{e}_i)$. Действительно,

$$f(\bar{e}_i) = \sum_{j=1}^{n} a_{ij}\bar{e}'_j = \sum_{j=1}^{n} a_{ij}(0, \dots, 1, 0, \dots, 0) = (a_{i1}, a_{i2}, \dots, a_{in}).$$

Пример 18. Пусть $m \geq n$ и пусть $f : \mathbb{P}^m \to \mathbb{P}^n$ — линейное отображение вида: для $\bar{a} = (a_1, \ldots, a_m)$ полагаем $f(\bar{a}) = \bar{a}' = (a_1, \ldots, a_n)$.
(Проверить линейность отображения f).
Вычислим матрицу A_f в стандартных базисах:

$$\begin{gathered} f(\bar{e}_1) = (1, 0, 0, \ldots, 0), \\ f(\bar{e}_2) = (0, 1, 0, \ldots, 0), \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f(\bar{e}_n) = (0, 0, 0, \ldots, 1), \\ f(\bar{e}_{n+1}) = (0, 0, 0, \ldots, 0), \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f(\bar{e}_m) = \underbrace{(0, 0, 0, \ldots, 0)}_{n}. \end{gathered}$$

Поэтому

$$A_f = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

С частным случаем такого отображения мы уже встречались, когда доказывали теорему о линейной зависимости $(n+1)$ векторов в $\mathbb{P}^n$. У нас было отображение $f : \mathbb{P}^n \to \mathbb{P}^{n-1}$ ($\mathbb{P}^{n-1}$ — пространство «усеченных» векторов).
Если $n = 1$, то матрица A_f есть **столбец чисел** $f(\bar{e}_i)$:

$$A_f = \begin{pmatrix} f(\bar{e}_1) \\ \vdots \\ f(\bar{e}_m) \end{pmatrix}$$

Теорема 3.1.1. *Пусть $\mathbb{P}^m$ и $\mathbb{P}^n$ — пространства векторов с фиксированными в них базисами $X = \{\bar{x}_1, \ldots, \bar{x}_m\}$ и $Y = \{\bar{y}_1, \ldots, \bar{y}_n$. Тогда, сопоставляя каждому линейному отображению $f : \mathbb{P}^m \to \mathbb{P}^n$ его матрицу A_f относительно базисов X и Y, мы получаем взаимно-однозначное соответствие между множеством всех линейных отображений f и множеством всех матриц с m строками и n столбцами.*

Доказательство. Покажем сначала, что для любой матрицы $A = (a_{ij})$ с m строками и n столбцами можно построить отображение $f : \mathbb{P}^m \to \mathbb{P}^n$, причем $A_f = A$. Именно, определим f, положив

$$f\Big(\sum_{i=1}^{m} \alpha_i \bar{x}_i\Big) = \sum_{i=1}^{m} \alpha_i \sum_{j=1}^{n} a_{ij} \bar{y}_j \qquad \text{для любых } \alpha_i \in \mathbb{P}.$$

Проверка линейности f предоставляется читателю.
Покажем, что $A_f = A$. Мы имеем

$$f(\bar{x}_i) = \sum_{j=1}^{n} a_{ij}\bar{y}_j \qquad \Rightarrow \qquad A = (a_{ij}).$$

Остается проверить, что если двум отображениям f_1 и f_2 соответствуют одна и та же матрица, то $f_1 = f_2$. Действительно, из $A_{f_1} = A_{f_2} \Rightarrow f_1(\bar{x}_i) = f_2(\bar{x}_i)$, а поскольку любой вектор из $\mathbb{P}^m$ однозначно представляется через базис и f_1, f_2 — линейные отображения $f_1(\bar{x}) = f_2(\bar{x})$ для всех $\bar{x} \in \mathbb{P}^m$, а значит $f_1 = f_2$. $\square$

Матрицы A и B называются равными, если равны соответствующие линейные отображения, а это будет $\Leftrightarrow$ когда $a_{ij} = b_{ij}$.

Пусть $f_1 : \mathbb{P}^m \to \mathbb{P}^n$; $f_2 : \mathbb{P}^n \to \mathbb{P}^l$. Тогда отображение $f : \mathbb{P}^m \to \mathbb{P}^l$ называется **произведением** линейных отображений f_1 и f_2 (обозначается $f = f_2 f_1$), если для любого $\bar{x} \in \mathbb{P}^m$ имеем:

$$f(\bar{x}) = f_2(f_1(\bar{x})).$$

Это определение уже давалось нами для произвольных отображений. Легко убедиться, что f — линейное отображение $\mathbb{P}^m$ в $\mathbb{P}^l$.

Определение. *Пусть $f : \mathbb{P}^m \to \mathbb{P}^n$ — линейное отображение,$\alpha \in \mathbb{P}$ — произвольное число, тогда **отображение** αf определяется так:*

$$\alpha f : \mathbb{P}^m \to \mathbb{P}^n$$
$$(\alpha f)(\bar{x}) = \alpha \cdot f(\bar{x}).$$

Определение. *Пусть f_1 и f_2 — два линейных отображения $\mathbb{P}^m \to \mathbb{P}^n$. Тогда отображение $f : \mathbb{P}^m \to \mathbb{P}^n$, задаваемое так:*

$$\forall \bar{x} \in \mathbb{P}^m \; f(\bar{x}) = f_1(\bar{x}) + f_2(\bar{x})$$

*называется **суммой** отображений f_1 и f_2 и обозначается $f = f_1 + f_2$.*

Отображения αf и $f_1 + f_2$ — линейные.
Введенные действия над линейными отображениями автоматически (в силу взаимно однозначного соответствия) определяют действия над матрицами (соответствующих размеров).

- **Умножение на число.**
  Если $A_f = (a_{ij})$ — матрица, соответствующая отображению $f : \mathbb{P}^m \to \mathbb{P}^n$,

то имеем

$$f(\bar{x}_i) = \sum_{j=1}^{n} a_{ij}\bar{y}_j,\ i = 1, \ldots, m;\ j = 1, \ldots, n$$

$$\alpha \cdot f(\bar{x}_i) = \sum_{j=1}^{n} \alpha a_{ij}\bar{y}_j.$$

Поэтому $A_{\alpha f} = (\alpha a_{ij})$.

По определению полагаем $\alpha A_f = A_{\alpha f}$. Так что для любой матрицы $A = (a_{ij})$ имеем $\alpha A = (\alpha a_{ij})$.

- **Сложение матриц.**
Пусть

$$\begin{aligned} f_1 : \mathbb{P}^m \to \mathbb{P}^n \quad &\sim \quad A_{f_1}, \\ f_2 : \mathbb{P}^m \to \mathbb{P}^n \quad &\sim \quad A_{f_2}, \end{aligned}$$

матрицы A_{f_1}, A_{f_2} — в одних и тех же базисах.
Это значит,

$$f_1(\bar{x}_i) = \sum_{j=1}^{n} a'_{ij}\bar{y}_j,$$

$$f_2(\bar{x}_i) = \sum_{j=1}^{n} a''_{ij}\bar{y}_j.$$

А потому

$$(f_1 + f_2)(\bar{x}_i) = f_1(\bar{x}_i) + f_2(\bar{x}_i) = \sum_{j=1}^{n} (a'_{ij} + a''_{ij})\bar{y}_j.$$

Так, что для сохранения взаимно однозначного соответствия между матрицами и линейными отображениями при сложении, полагаем

$$A_{f_1} + A_{f_2} = A_{f_1+f_2} \qquad \text{или} \qquad (a'_{ij}) + (a''_{ij}) = (a'_{ij} + a''_{ij}).$$

Итак, **суммой двух матриц** $A = (a_{ij})$ **и** $B = (b_{ij})$ называется матрица $C = (c_{ij})$, где $c_{ij} = a_{ij} + b_{ij}$, причем размеры всех трех матриц одинаковы: $m \times n$.
Обычно пишут $A + B = C$.

- **Умножение матриц.**
  Пусть $X = \{\bar{x}_1, \ldots, \bar{x}_m\}$, $Y = \{\bar{y}_1, \ldots, \bar{y}_n\}$, $Z = \{\bar{z}_1, \ldots, \bar{z}_l\}$ — фиксированные базисы пространств $\mathbb{P}^m$, $\mathbb{P}^m$ и $\mathbb{P}^l$. Пусть $f_1 : \mathbb{P}^m \to \mathbb{P}^n$, $f_2 : \mathbb{P}^n \to \mathbb{P}^l$ — линейные отображения, которым соответствуют матрицы $A_{f_1} = (a_{ij})$ и $A_{f_2} = (b_{jk})$. Вычислим $A_{f_2 f_1}$.
  Имеем:

$$f_2(f_1(\bar{x}_i)) = f_2(\sum_{j=1}^{n} a_{ij}\bar{y}_j) = \sum_{j=1}^{n} a_{ij} f_2(\bar{y}_j) =$$

$$= \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{l} b_{jk}\bar{z}_k = \sum_{k=1}^{l} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) \bar{z}_k.$$

  Поскольку i принимает значения от 1 до m, а k от 1 до l, то получаем, что $A_{f_2 f_1}$ есть матрица размера $m \times l$, элемент c_{ik}, который вычисляется по формуле

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

  Поэтому имеет место

  Определение. *Пусть даны две матрицы $A = (a_{ij})$ и $B = (b_{ij})$, причем число столбцов матрицы A равно числу строк матрицы B (и равно n). Тогда произведением матриц A и B (обозначается AB) называется матрица размера $m \times l$, для которой элемент из $i^{ой}$ строки и $k^{ого}$ столбца равен сумме попарных произведений элементов $i^{ой}$ строки матрицы A на элементы $k^{ого}$ столбца матрицы B. При этом число строк AB равно числу строк A, а число столбцов AB равно числу столбцов B.*

  Итак, $A_{f_1 f_2} = A_{f_1} A_{f_2}$.

(Обратите **внимание** на порядок, в котором пишутся перемножаемые матрицы и соответствующие им линейные отображения).
Следует заметить, что не всякие две матрицы можно перемножать — имеется серьезное ограничение на размеры матриц.

Матрица A размера $m \times n$ называется квадратной матрицей порядка n, если $m = n$. Квадратные матрицы одного и того же порядка всегда можно премножать.

Свойства действий над матрицами.

1. **Совокупность матриц по сложению образует абелеву группу.**

2. **Умножение матриц ассоциативно**
   (ибо умножение соответствующих отображений ассоциативно).

3. **Умножение матриц не коммутативно.**
Во-первых, если A — размера $m \times n$, а B — размера $n \times k$, причем $k \neq m$, то AB — существует, а BA — не определено. Но даже если $k = m$, то не обязательно $AB = BA$.
Например, пусть

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix}.$$

Тогда

$$AB = \begin{pmatrix} 2 & -1 \\ 6 & -1 \end{pmatrix}, \qquad BA = \begin{pmatrix} 5 & 6 \\ -3 & -4 \end{pmatrix}.$$

4. **Квадратные матрицы порядка n образуют кольцо.** Его обозначают через M_n.
Роль нуля играет нулевая матрица $\begin{pmatrix} 0 & \dots & 0 \\ . & . & . \\ 0 & \dots & 0 \end{pmatrix}$, которая соответствует нулевому отображению, то есть отображению, при котором любому вектору из $\mathbb{P}^n$ соответствует нулевой вектор из $\mathbb{P}^n$.
В M_n есть единица, роль которой играет единичная матрица

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

(такая матрица соответствует тождественному (единичному) отображению $\mathbb{P}^n$ в себя).

С матрицей можно связать некоторые числовые характеристики, важнейшей из которых является **определитель**.

3.2 Определители

Пусть имеется квадратная матрица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

и пусть σ — какая-либо подстановка на множестве $\{1, 2, \dots, n\}$, то есть

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_n \end{pmatrix}.$$

Членом определителя матрицы A, соответствующим подстановке σ называется выражение

$$\rho(\sigma)a_{1\alpha_1}a_{2\alpha_2}\dots a_{n\alpha_n},$$

где $\rho(\sigma)$ — знак подстановки σ.

Определение. *Определителем матрицы A (обозначается $|A|$ или $\det A$) называется сумма*

$$\sum_{\sigma\in S_n}\rho(\sigma)a_{1\alpha_1}a_{2\alpha_2}\dots a_{n\alpha_n},$$

то есть сумма членов определителя, распространенная на все подстановки симметрической группы подстановок S_n.

Иногда, определитель матрицы A записывают так

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Итак, определитель матрицы порядка n есть сумма $n!$ своих членов.
В дальнейшем определитель матрицы порядка n будем называть определителем порядка n. В определителе порядка n мы естественно определяем строки и столбцы определителя. Так что определитель порядка n имеет м строк и n столбцов. Нумерация строк идет сверху вниз, а столбцов — слева направо. Например, $i^{\text{ая}}$ строка состоит из элементов

$$a_{i1}, a_{i2}, \dots, a_{in},$$

а $j^{\text{ый}}$ столбец состоит из элементов

$$a_{1j}, a_{2j}, \dots, a_{nj}.$$

Из определения члена определителя видно, что член определителя равен произведению n элементов определителя, взятых из разных строк и разных столбцов его, причем этому произведению приписывается знак соответствующей подстановки.

Свойства определителей.

1. Пусть $A = (a_{ij})$ — матрица порядка n. Обозначим через $A' = (a'_{ij})$ — матрицу, для которой $a'_{ij} = a_{ji}$. Матрица A' называется **транспонированной** по отоношению к A. Тогда

$$|A| = |A'|,$$

то есть **определитель матрицы не изменяется при транспонировании**.
В самом деле,

$$|A'| = \sum_{\sigma\in S_n} \rho(\sigma) a'_{1\alpha_1} \dots a'_{n\alpha_n} = \sum_{\sigma\in S_n} \rho(\sigma) a_{\alpha_1 1} \dots a_{\alpha_n n}.$$

Подстановки $\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_n \end{pmatrix}$
и $\sigma^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_n \\ 1 & 2 & \dots & i & \dots & n \end{pmatrix}$ взаимно обратны, то есть $\sigma\sigma^{-1} = e$, и, значит, $\rho(\sigma) = \rho(\sigma^{-1})$. Кроме того, когда σ пробегает всю группу S_n, подстановка σ^{-1} также пробегает всю группу S_n. А потому

$$|A'| = \sum_{\sigma^{-1}\in S_n} \rho(\sigma^{-1}) a_{\alpha_1 1} \dots a_{\alpha_n n} = |A|.$$

Следствие. *Всякое утверждение, доказанное для строк определителя, является верным и для столбцов.*
Поэтому в дальнейшем свойства определителя формулируются в терминах строк.

2. **Если в определителе одна строка нулевая, то определитель равен** 0**.**
Это следует из того, что каждый член определителя содержит в качестве множителя элемент из этой нулевой строки.

3. **Если в определителе поменять местами две строки, то он изменит свой знак.**
В самом деле, пусть

$$|A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{j1} & \dots & a_{jn} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}, \qquad |B| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{j1} & \dots & a_{jn} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Тогда имеем

$$|B| = \sum \rho \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_j & \dots & \alpha_n \end{pmatrix} a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{j\alpha_j} \dots a_{n\alpha_n} =$$
$$= -\sum \rho \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_j & \dots & \alpha_i & \dots & \alpha_n \end{pmatrix} a_{1\alpha_1} \dots a_{i\alpha_j} \dots a_{j\alpha_i} \dots a_{n\alpha_n} = -|A|.$$

Мы учли, что подстановки

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_j & \dots & \alpha_n \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_j & \dots & \alpha_i & \dots & \alpha_n \end{pmatrix}$$

переходят одна в другую с помощью одной транспозиции (i, j), а потому имеют разные знаки.

4. **Если в определителе имеются две равные строки, то он равен нулю.**
Действительно, поменяв местами равные строки, мы не изменим вида определителя, а потому и его значения. Но по предыдущему свойству он обязан изменить свой знак. Поэтому

$$|A| = -|A| \quad \Rightarrow \quad |A| = 0.$$

Свойство 4 доказано не вполне корректно, ибо из $2|A| = 0$ еще не следует $|A| = 0$ (если основное поле $\mathbb{P}$ имеет характеристику 2).
Поэтому приведем другое доказательство этого свойства:

Пусть в определителе $|A|$ равны $i^{\text{ая}}$ и $j^{\text{ая}}$ строки. Это значит, что $a_{ik} = a_{jk}$, $k = 1, \dots, n$.
Пусть дан произвольный член определителя $|A|$,

$$\rho(\sigma) a_{1\alpha_1} \dots a_{i\alpha_i} \dots a_{j\alpha_j} \dots a_{n\alpha_n},$$

где $\rho(\sigma)$ — знак подстановки

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_j & \dots & \alpha_n \end{pmatrix}.$$

В этом же определителе имеется член

$$\rho(\tau) a_{1\alpha_1} \dots a_{i\alpha_j} \dots a_{j\alpha_i} \dots a_{n\alpha_n},$$

где

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_j & \dots & \alpha_i & \dots & \alpha_n \end{pmatrix}.$$

Знаки подстановок σ и τ различны, а в силу $a_{i\alpha_i} = a_{j\alpha_i}, a_{i\alpha_j} = a_{j\alpha_j}$, следует, что эти два члена определителя погашают друг друга, а потому определитель $|A|$ равен сумме пар взаимно погашающих друг друга слагаемых, и значит $|A|$ равен 0.

5. **Если в определителе элементы какой-либо строки умножить на одно и то же число C, то значение определителя умножится на это число**, то есть если

$$|A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}, \qquad \text{то} \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ ca_{i1} & \dots & ca_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = c|A|.$$

   Доказательство непосредственно следует из определения членов определителя.

6. **Если матрицы A, B, C порядка n таковы, что элементы всех строк, кроме одной, $i^{\text{ой}}$, равны, а $i^{\text{ые}}$ строки связаны соотношением**

$$a_{ij} + b_{ij} = c_{ij}, \quad j = 1, 2, \dots, n,$$

   тогда

$$|A| + |B| = |C|.$$

7. **Если в определителе имеются две пропорциональные строки, то он равен нулю.**

8. **Если одна из строк определителя является линейной комбинацией других его строк, то определитель равен нулю.**
   (Здесь строки рассматриваются как n–мерные векторы).
   Это свойство следует из свойств 6 и 7.

9. **Определитель не изменит своего значения, если к какой-либо строке прибавить линейную комбинацию других строк.**
   Это свойство следует из свойств 8 и 6.

3.3 Элементарные преобразования и элементарные матрицы

Пусть A — произвольная матрица размера $m \times n$.
Элементарным преобразованием матрицы A называется одно из преобразований вида:

I. Умножение какой-либо строки (столбца) матрицы на число C.

II. Прибавление к какой-либо строке (столбцу) другой строки (столбца), умноженной на некоторое число.

III. Перестановка 2^{x} строк (столбцов) матрицы.

Из свойств определителя матрицы следует, что при преобразовании $\texttt{I}^{\text{го}}$ типа определитель умножается на число , при преобразовании $\texttt{II}^{\text{го}}$ определитель не меняется, а при преобразовании $\texttt{III}^{\text{го}}$ типа он изменяет свой знак.

Определение. *Матрица A размера $m \times n$ называется диагональной, если для ее элементов справедливы условия*

$$a_{ij} = 0 \quad \textit{при} \quad i \neq j, \quad i = 1, \ldots, m; \quad j = 1, \ldots, n.$$

Так, при $m = n$ диагональная матрица имеет вид

$$A = \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & 0 \\ . & . & . & . \\ 0 & 0 & \ldots & a_{nn} \end{pmatrix},$$

при $m > n$ имеем

$$A = \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & 0 \\ . & . & . & . \\ 0 & 0 & \ldots & a_{nn} \\ 0 & 0 & \ldots & 0 \\ . & . & . & . \\ 0 & 0 & \ldots & 0 \end{pmatrix},$$

при $m < n$ имеем

$$A = \begin{pmatrix} a_{11} & 0 & \ldots & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & 0 & \ldots & 0 \\ . & . & . & . & . & . \\ 0 & 0 & \ldots & a_{nn} & \ldots & 0 \end{pmatrix}.$$

Диагональную матрицу порядка n, на диагонали которой стоят элементы $a_1, a_2, \ldots, a_n$, часто обозначают через $D(a_1, a_2, \ldots, a_n)$, или $diag(a_1, a_2, \ldots, a_n)$.

Лемма 3.3.1. *Если $A = D(a_1, a_2, \ldots, a_n)$, то $|A| = a_1 a_2 \ldots a_n$.*

Доказательство. Действительно, произведение $a_1 a_2 \ldots a_n$ является единственным членом определителя, отличным от нуля (по крайней мере формально). □

Имея ввиду предыдущую лемму, легко понять стремление с помощью элементарных преобразований привести любую матрицу к диагональному виду. На следующем примере видна реальность этих стремлений.

Пример 19. Пусть дана матрица

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 0 & 4 & 2 \\ -1 & 3 & 2 \end{pmatrix}.$$

Для удобства будем обозначать строки матрицы A через C_1, C_2, C_3, а столбцы — через K_1, K_2, K_3. Будем считать, что запись $2K_2$ означает, что к соответствующему столбцу прибавлен $2^{\text{ой}}$, умноженный на 2.
Тогда имеем:

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 0 & 4 & 2 \\ -1 & 3 & 2 \end{pmatrix} \xrightarrow[|A|\to -|A|]{\text{переставим местами } K_1 \text{ и } K_2} \begin{pmatrix} 1 & 2 & -3 \\ 4 & 0 & 2 \\ 3 & -1 & 2 \end{pmatrix} \xrightarrow{-2K_1} \to$$

$$\xrightarrow[-|A|\to -|A|]{} \begin{pmatrix} 1 & 0 & -3 \\ 4 & -8 & 2 \\ 3 & -7 & 2 \end{pmatrix} \xrightarrow[-|A|\to -|A|]{+3K_1} \begin{matrix} \\ -4C_1 \\ -3C_1 \end{matrix} \begin{pmatrix} 1 & 0 & 0 \\ 4 & -8 & 14 \\ 3 & -7 & 11 \end{pmatrix} \to$$

$$\xrightarrow[-|A|\to -|A|]{} -C_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & -8 & 14 \\ 0 & -7 & 11 \end{pmatrix} \xrightarrow[-|A|\to -|A|]{+3K_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 3 \\ 0 & -7 & 11 \end{pmatrix} \to$$

$$\xrightarrow[-|A|\to -|A|]{} -7C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -7 & -10 \end{pmatrix} \xrightarrow[-|A|\to -|A|]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -10 \end{pmatrix}.$$

Поэтому

$$-|A| = |diag(1, -1, \ldots, -10)| = 10 \Rightarrow |A| = -10.$$

В рассмотренном примере преобразованиями $\texttt{II}^{\text{го}}$ и $\texttt{III}^{\text{го}}$ типов мы привели матрицу к диагональному виду. А что будет в общем случае? Ответ дает следующая

Теорема 3.3.1. *Элементарными преобразованиями $\texttt{II}^{\text{го}}$ типа матрицу A можно привести к диагональному виду.*

С элементарными преобразованиями матриц связаны элементарные матрицы.

Определение. ***Элементарной матрицей I типа*** *называется матрица, у которой элементы главной диагонали равны 1, а все остальные элементы, кроме возможно только одного, равны нулю.*

Если отличный от нуля элемент вне главной диагонали равен $\boldsymbol{c}$ *и стоит на* (i,j) *— месте, то элементарную матрицу* $I^{го}$ *типа обозначаем через* $\varepsilon_{ij}(c)$.

Определение. ***Элементарной матрицей II типа*** *называется матрица, у которой элементы вне главной диагонали равны нулю, а на диагонали все элементы, кроме возможно только одного, равны 1.*
Элементарную матрицу II типа с отличным от 1 элементом главной диагонали, стоящим на (i,i) *— месте и равным* $\boldsymbol{c}$ *обозначаем через* $\varepsilon^{(i)}(c)$.

Непосредственной проверкой убеждаемся, что $\varepsilon_{ij}(c)A$ есть матрица, получаемая из A прибавлением к $i^{\text{ой}}$ строке $j^{\text{ой}}$ строки, умноженной на c. Аналогично, $A\varepsilon_{ij}(c)$ — матрица, получаемая из A прибавлением к $j^{\text{ому}}$ столбцу $i^{\text{го}}$ столбца, умноженного на c.
Кроме того,

$$diag(c_1, c_2, \ldots, c_n) = \varepsilon^{(1)}(c_1) \cdot \varepsilon^{(2)}(c_2) \cdot \ldots \cdot \varepsilon^{(n)}(c_n).$$

Элементарная матрица $\varepsilon^{(i)}(c)$ второго типа является частным случаем диагональной матрицы, а потому ее определитель $|\varepsilon^{(i)}(c)| = 1$ (**почему?**)

3.4 Делители нуля и единицы в кольце матриц M_n

Рассмотрим произведение двух матриц

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Итак, в M_2 имеются делители нуля.
Оказывается в кольце M_n для любого $n > 2$ существуют делители нуля. Например, $E_{ij}E_{ki} = O$ при $j \neq k$, хотя, конечно, $E_{ij} \neq O$, $E_{ki} \neq O$.
Заметим, что $E_{ki}E_{ij} = E_{kj} \neq O$.
В силу отсутствия коммутативности в M_n естественно говорить о левых и правых делителях нуля.

Определение. *Матрица* A *называется* ***левым делителем единицы (обратима справа)****, если найдется такая матрица* $A_p^{-1} \in M_n$, *что*

$$AA_p^{-1} = E.$$

*Аналогично, A — **правый делитель единицы (обратима слева)**, если найдется матрица $A_l^{-1} \in M_n$, такая, что*

$$A_l^{-1}A = E.$$

Лемма 3.4.1. *Если матрица A обратима слева и справа, то $A_l^{-1} = A_p^{-1}$.*

Доказательство. Действительно, из ассоциативности умножения матриц имеем:

$$A_l^{-1} = A_l^{-1}\left(AA_p^{-1}\right) = \left(A_l^{-1}A\right)A_p^{-1} = A_p^{-1}.$$

□

Определение. *Матрица A , обратимая слева и справа,называется **обратимой матрицей**, а $A_l^{-1} = A_p^{-1} = A^{-1}$ **называется обратной к** A.*

Позже мы увидим, что каждая матрица из M_n либо является делителем единицы, либо является делителем нуля (как слева, так и справа).

Лемма 3.4.2. *Матрица $\varepsilon^{(i)}(c)$ является делителем нуля, если $c = 0$, и является делителем единицы, если $c \neq 0$.*

Доказательство. Если $c = 0$, то $\varepsilon^{(i)}(0) \cdot E_{ij} = O$ — нуль-матрица из M_n (здесь как обычно E_{ij} — матрица, у которой на (i, j)–месте стоит 1, а на остальных местах нули).
Если же $c \neq 0$, то $\varepsilon^{(i)}(c)\varepsilon^{(i)}(c^{-1}) = \varepsilon^{(i)}(c^{-1})\varepsilon^{(i)}(c) = E$ — единичная матрица из M_n. Таким образом, обратной к матрице $\varepsilon^{(i)}(c)$, $c \neq 0$ будет $\varepsilon^{(i)}(c^{-1})$. □

Лемма 3.4.3. *Элементарная матрица $\mathtt{I}^{zo}$ типа обратима.*

Доказательство. Рассмотри произведение матриц

$$\varepsilon_{ij}(c) \cdot \varepsilon_{ij}(-c).$$

Каждая из перемножаемых матриц является элементарной матрицей $\mathtt{I}^{\text{го}}$ типа. Рассматриваемое произведение — матрица, получаемая из $\varepsilon_{ij}(-c)$ прибавлением к $i^{\text{ой}}$ строке $j^{\text{ой}}$ строки, умноженной на c. Но мы имеем

$i^{\text{ая}}$ строка $\quad (0, 0, \ldots, \overset{(i)}{1}, \ldots, \overset{(j)}{-c}, 0, \ldots, 0),$
$j^{\text{ая}}$ строка $\quad (0, 0, \ldots, 0, \ldots, 1, 0, \ldots, 0).$

Поэтому $\quad C_i + c \cdot C_j = (0, 0, \ldots, \overset{(i)}{1}, 0, \ldots, \overset{(j)}{0}, 0, \ldots, 0).$
Отсюда имеем

$$\varepsilon_{ij}(c) \cdot \varepsilon_{ij}(-c) = E.$$

Аналогично,

$$\varepsilon_{ij}(-c) \cdot \varepsilon_{ij}(c) = E.$$

□

Следствием предыдущих лемм является

Теорема 3.4.1. *Всякая матрица из M_n может быть разложена в произведение элементарных матриц.*

Доказательство. Поскольку элементарное преобразование II типа эквивалентно умножению слева или справа исходной матрицы A на элементарную матрицу $\mathtt{I}^{\text{го}}$ типа, то в силу теоремы (3.3.1) предыдущего параграфа, имеем

$$\varepsilon_{i_1,j_1}(c_1)\cdot\ldots\cdot\varepsilon_{i_k,j_k}(c_k)\cdot A\cdot\varepsilon_{i_{k+1},j_{k+1}}(c_{k+1})\cdot\ldots\cdot\varepsilon_{i_m,j_m}(c_m)=D(a_1,\ldots,a_n).$$

В силу, $D(a_1,\ldots,a_n)=\varepsilon^{(1)}(a_1)\ldots\varepsilon^{(n)}(a_n)$.
А потому применяя Лемму (3.4.3), получим

$$A=\varepsilon_{i_k,j_k}(-c_k)\cdot\ldots\cdot\varepsilon_{i_1,j_1}(-c_1)\cdot\varepsilon^{(1)}(a_1)\ldots\varepsilon^{(n)}(a_n)\cdot\varepsilon_{i_m,j_m}(-c_m)\cdot\ldots\cdot\varepsilon_{i_{k+1},j_{k+1}}(-c_{k+1}).$$

□

Теорема 3.4.2. *Пусть A и B — две квадратные матрицы порядка n. Тогда*

$$|A\cdot B|=|A|\cdot|B|.$$

Доказательство. Предположим сначала, что одна из матриц, например, A — элементарная. Если A — элементарная матрица $\mathtt{I}^{\text{го}}$ типа, то ее умножение на B не изменяет определитель B, то есть $|A\cdot B|=|B|$. Но определитель элементарной матрицы $\mathtt{I}^{\text{го}}$ типа равен 1, а потому $|A|=1$, и значит, $|A\cdot B|=|A|\cdot|B|$.
Если же A — элементарная матрица $\mathtt{II}^{\text{го}}$ типа, то $A=\varepsilon^{(i)}(c)$, то легко убедиться, что $A\cdot B$ получается из B умножением $i^{\text{ой}}$ строки на c, а потому $|A\cdot B|=c|B|=|A|\cdot|B|$, та как $|A|=|\varepsilon^{(i)}(c)|=c$.
В общем случае, мы представляем A в виде произведения элементарных матриц $A=\varepsilon_1\cdot\ldots\cdot\varepsilon_k$. Тогда пользуясь ассоциативностью умножения матриц и рассмотренным выше частным случаем, получаем

$$|A\cdot B|=|\varepsilon_1\cdot\ldots\cdot\varepsilon_k\cdot B|=|\varepsilon_1|\cdot|\varepsilon_2\ldots\cdot\varepsilon_k\cdot B|=|\varepsilon_1|\cdot|\varepsilon_2|\cdot\ldots\cdot|\varepsilon_k|\cdot|B|=$$

$$=|\varepsilon_1\cdot\ldots\cdot\varepsilon_k|\cdot|B|=|A|\cdot|B|.$$

□

Определение. *Квадратная матрица называется* ***невырожденной****, если ее определитель $\neq 0$. В противном случае, матрица называется* ***вырожденной****.*

Теорема 3.4.3. *Произведение матриц $A_1\ldots A_k$ будет невырожденной матрицей $\Leftrightarrow$ когда каждая из матриц $A_1,\ldots,A_k$ — невырожденная матрица.*

Доказательство. Доказательство следует непосредственно из определения невырожденности и теоремы об определителе произведения матриц. □

Теорема 3.4.4. ***(Критерий невырожденности.)***
Квадратная матрица невырождена ⇔ когда она обратима.

Доказательство. **Достаточность.** Пусть A — обратима. Тогда из $A \cdot A^{-1} = E \Rightarrow |A| \cdot |A^{-1}| = 1 \Rightarrow |A| \neq 0$.
Необходимость. Пусть A — невырожденная матрица. Приведем A к диагональному виду с помощью элементарных преобразований $\mathtt{II}^{\text{ro}}$ типа. Это значит, что найдутся элементарные матрицы $\mathtt{I}^{\text{ro}}$ типа такие, что

$$\varepsilon_{i_1,j_1}(c_1) \cdot \ldots \cdot \varepsilon_{i_k,j_k}(c_k) \cdot A \cdot \varepsilon_{i_{k+1},j_{k+1}}(c_{k+1}) \cdot \ldots \cdot \varepsilon_{i_m,j_m}(c_m) = D(a_1, \ldots, a_n).$$

Отсюда,

$$|A| = |D| = a_1 \ldots a_n.$$

Но A — невырождена, а потому $|A| \neq 0 \Rightarrow a_i \neq 0$, $i = 1, 2, \ldots, n$, и значит, в представлении D через произведение элементарных матриц второго типа $D(a_1, \ldots, a_n) = \varepsilon^{(1)}(a_1) \cdot \ldots \cdot \varepsilon^{(n)}(a_n)$ каждая из матриц $\varepsilon^{(i)}(a_i)$ обратима. Но тогда в представлении A через элементарные

$$A = \varepsilon_1 \ldots \varepsilon_l,$$

каждая матрица обратима, а потому

$$A^{-1} = \varepsilon_l^{-1} \ldots \varepsilon_1^{-1}$$

является обратной к A. □

Теорема 3.4.5. ***(2-й критерий невырожденности.)***
Матрица $A \in M_n$ невырождена ⇔ когда строки A, как n-мерные векторы, линейно независимы.

Доказательство. **Необходимость.** Если A — невырожденная матрица, то ее строки (также как и столбцы) как n-мерные векторы обязательно линейно независимы (по свойству 8 определителей).
Достаточность. Пусть строки матрицы A, как n-мерные векторы, линейно независимы. И предположим, что A — вырожденная матрица, то есть $|A| = 0$. Тогда в представлении

$$\varepsilon_{i_1,j_1}(c_1) \cdot \ldots \cdot \varepsilon_{i_k,j_k}(c_k) \cdot A \cdot \varepsilon_{i_{k+1},j_{k+1}}(c_{k+1}) \cdot \ldots \cdot \varepsilon_{i_m,j_m}(c_m) = diag(a_1, \ldots, a_n) \quad (3.1)$$

хотя бы одно из чисел $a_1, \ldots, a_n$, например, a_l, равно нулю.
Из (3.1) имеем

$$\varepsilon_{i_1,j_1}(c_1) \cdot \ldots \cdot \varepsilon_{i_k,j_k}(c_k) \cdot A = diag(a_1, \ldots, a_n) \cdot \varepsilon_{i_m,j_m}(-c_m) \cdot \ldots \cdot \varepsilon_{i_{k+1},j_{k+1}}(-c_{k+1}). \quad (3.2)$$

Матрица $diag(a_1, \ldots, a_n)$ имеет $l^{\text{ую}}$ строку — нулевую, умножение ее справа на элементарные матрицы $\mathtt{I}^{\text{го}}$ типа не изменит эту строку, так что в (3.2) справа стоит матрица, $l^{\text{ая}}$ строка которой — нулевая.
Отсюда следует, что $l^{\text{ая}}$ строка матрицы

$$\varepsilon_{i_1,j_1}(c_1) \cdot \ldots \cdot \varepsilon_{i_k,j_k}(c_k) \cdot A \tag{3.3}$$

равна нулю, то есть строки этой матрицы линейно зависимы.
Однако, мы сейчас покажем, что всякая матрица B с линейно независимыми строками после умножения ее слева на $\varepsilon_{i,j}(c)$ переходит в матрицу с линейно независимыми строками. Действительно, пусть $C_1, \ldots, C_n$ — строки матрицы B. После умножения B на $\varepsilon_{i,j}(c)$ получим строки

$$C_1, \ldots, C_{i-1}, C_i + c \cdot C_j, C_{i+1}, \ldots, C_n.$$

И теперь, из

$$\begin{aligned} \alpha_1 C_1 + \ldots + \alpha_{i-1} C_{i-1} + \alpha_i (C_i + c \cdot C_j) + \alpha_{i+1} C_{i+1} + \ldots + \alpha_n C_n = 0 \Rightarrow \\ \Rightarrow \alpha_1 = \ldots = \alpha_{i-1} = \alpha_i = \ldots = c\alpha_i + \alpha_j = \ldots = \alpha_n = 0 \Rightarrow \\ \Rightarrow \alpha_1 = 0, \ldots, \alpha_i = 0, \ldots, \alpha_j = 0, \ldots, \alpha_n = 0. \end{aligned}$$

Таким образом, если строки матрицы A — линейно независимы, то и стоки матрицы (3.3) линейно независимы. Полученное противоречие доказывает неверность предположения о вырожденности A. □

Следствие 1. *Поскольку определитель матрицы не меняется при транспонировании, то матрица A невырождена $\Leftrightarrow$ когда ее столбцы линейно независимы.*

Следствие 2. ***Критерий равенства нулю определителя.***
Определитель равен 0 $\Leftrightarrow$ когда его строки (столбцы) линейно зависимы, то есть какая-либо строка (столбец) является линейной комбинацией других строк (столбцов).

Следствие 3. *Каждая матрица порядка n является либо делителем нуля, либо делителем единицы.*

Доказательство. Если $|A| \neq 0$, то A — обратима, то есть является делителем единицы.
Пусть $|A| = 0$, тогда столбцы A линейно зависимы, то есть

$$\alpha_1 K_1 + \ldots + \alpha_n K_n = 0.$$

А потому

$$\begin{cases} \alpha_1 a_{11} + \alpha_2 a_{12} + \ldots + \alpha_n a_{1n} = 0, \\ \alpha_1 a_{21} + \alpha_2 a_{22} + \ldots + \alpha_n a_{2n} = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \alpha_1 a_{n1} + \alpha_2 a_{n2} + \ldots + \alpha_n a_{nn} = 0. \end{cases}$$

Положим

$$B = \begin{pmatrix} \alpha_1 & \alpha_1 & \ldots & \alpha_1 \\ \alpha_2 & \alpha_2 & \ldots & \alpha_2 \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_n & \alpha_n & \ldots & \alpha_n \end{pmatrix}.$$

Тогда $AB = 0$.
Аналогично строится матрица C, для которой $CA = 0$. □

3.5 Вычисление определителей

Пусть A — определитель порядка n. Зафиксируем в A k строк с номерами $i_1, \ldots, i_k$ и k столбцов с номерами $j_1, \ldots, j_k$. На пересечении этих строк и столбцов находится k^2 элементов, из которых можно составить определитель $k^{\text{го}}$ порядка

$$\begin{vmatrix} a_{i_1 j_1} & \ldots & a_{i_1 j_k} \\ \ldots & \ldots & \ldots \\ a_{i_k j_1} & \ldots & a_{i_k j_k} \end{vmatrix}.$$

Этот определитель называется **минором $k^{\text{го}}$ порядка определителя** A, соответствующим выбранным строкам и столбцам.
Если $k = 1$, то получаем минор $1^{\text{го}}$ порядка $|a_{ij}| = a_{ij}$, где i и j номера зафиксированных строки и столбца.
Если выделен минор $k^{\text{го}}$ порядка M, то из оставшихся строк и столбцов определителя можно составить другой определитель порядка $n-k$, который называется **дополнительным минором для M и обозначается M^c**.
Например, в определителе

$$\begin{vmatrix} 1 & -1 & 2 & 4 & 5 \\ 6 & 0 & 2 & 1 & 3 \\ 1 & -2 & 0 & 3 & 4 \\ 4 & 1 & 7 & 2 & -1 \\ 3 & 0 & -10 & 1 & 1 \end{vmatrix}$$

строкам с номерами 2,4,5 и столбцам с номерами 1,2,4 соответствует минор

$$M = \begin{vmatrix} 6 & 0 & 1 \\ 4 & 1 & 2 \\ 3 & 0 & 1 \end{vmatrix},$$

а дополнительный минор равен

$$M^c = \begin{vmatrix} 2 & 5 \\ 0 & 4 \end{vmatrix}.$$

Если дополнительному минору M^c приписать знак $(-1)^{S_M}$, где $S_M = i_1 + \ldots + i_k + j_1 + \ldots + j^k$, то есть S_M есть сумма номеров выделенных строк и столбцов, то $(-1)^{S_M} M^c$ называется **алгебраическим дополнением минора** M.

Для элемента a_{ij} как минора $I^{\text{го}}$ порядка алгебраическим дополнением будет определитель

$$(-1)^{i+j} \begin{vmatrix} a_{11} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{i-1,n} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{i+1,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{n,n} \end{vmatrix}.$$

Алгебраическое дополнение элемента a_{ij} будем обозначать A_{ij}.

В предыдущем параграфе мы указали способ вычисления определителя, приведением его к диагональному виду. Однако, при больших n этот способ требует много вычислений. Поэтому естественно стремление найти метод вычисления определителя порядка n через определители меньших порядков. Сначала мы займемся вычислением определителей, близких к диагональным.

Определитель A называется **определителем верхнего треугольного вида**, если все его элементы, лежащих под главной диагональю, равны 0.

Определитель A называется **определителем нижнего треугольного вида**, если все его элементы, лежащих над главной диагональю, равны 0.

Легко видеть, что при транспонировании определитель верхнего треугольного вида переходит в определитель нижнего треугольного вида, и наоборот. Поэтому достаточно уметь вычислять определитель верхнего треугольного вида:

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_{n,n} \end{vmatrix}.$$

Из определения членов определителя следует, что только один член — произведение элементов главной диагонали — не содержит элементов, лежащих под главной диагональю (которые равны нулю). Поэтому значение такого определителя равно произведению элементов главной диагонали.

Квадратная матрица вида

$$\begin{pmatrix} a_{11} & \dots & a_{1,k} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} & 0 & \dots & 0 \\ a_{k+1,1} & \dots & a_{k+1,k} & a_{k+1,k+1} & \dots & a_{k+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,k} & a_{n,k+1} & \dots & a_{n,n} \end{pmatrix}$$

называется **ступенчатой матрицей**.
Очевидно, ее можно представить в виде

$$\begin{pmatrix} A & O \\ B & C \end{pmatrix},$$

где A — квадратная матрица порядка k,
C — квадратная матрица порядка $n-k$,
B и O — прямоугольные матрицы соответственно размеров $(n-k)\times k$ и $k\times(n-k)$.

Лемма. *Для ступенчатой матрицы*

$$\begin{pmatrix} A & O \\ B & C \end{pmatrix}$$

имеем

$$\begin{vmatrix} A & O \\ B & C \end{vmatrix} = |A|\cdot|C|.$$

Доказательство. Элементарные преобразования $II^{\text{го}}$ типа приводят матрицу A к диагональному виду, не меняя элементов матрицы C, а элементарные преобразования $II^{\text{го}}$ типа, приводящие C к диагональному виду не меняют матрицу A. Поэтому имеем:

$$\begin{vmatrix} A & O \\ B & C \end{vmatrix} = \begin{vmatrix} a_1 & 0 & \dots & 0 & & & & \\ 0 & a_2 & \dots & 0 & & \bigcirc & & \\ \dots & \dots & \dots & \dots & & & & \\ 0 & 0 & \dots & a_k & & & & \\ b'_{11} & b'_{12} & \dots & b'_{1k} & c_1 & 0 & \dots & 0 \\ b'_{21} & b'_{22} & \dots & b'_{2k} & 0 & c_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b'_{n-k,1} & b'_{n-k,2} & \dots & b'_{n-k,k} & 0 & 0 & \dots & c_{n-k} \end{vmatrix}.$$

Мы пришли к определителю нижнего треугольного вида, который равен $a_1\dots a_k c_1\dots c_{n-k}$.
Но $|A| = a_1\dots a_k$, $|C| = c_1\dots c_{n-k}$. □

Теорема 3.5.1. *Если в определителе все элементы какой-либо строки, кроме одного, равны* 0*, то этот определитель равен произведению ненулевого элемента строки на его алгебраическое дополнение.*

Доказательство. Пусть сначала в определителе A первая строка такова, что $a_{12} = \ldots = a_{1n} = 0$. Тогда A имеет вид

$$\left|\begin{array}{c|ccc} a_{11} & a_{12} & \ldots & a_{1n} \\ \hline a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{array}\right|.$$

Тогда этот определитель является определителем ступенчатой матрицы, причем $k = 1$. Согласно предыдущей лемме имеем

$$|A| = a_{11} \cdot \begin{vmatrix} a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot \\ a_{n2} & \ldots & a_{nn} \end{vmatrix} = a_{11} \cdot A_{11},$$

(ибо в этом случае знак дополнительного минора для элемента a_{11} равен $(-1)^{1+1} = 1$).
В общем случае, $|A|$ имеет вид:

$$|A| = \begin{vmatrix} a_{11} & \ldots & a_{1,j} & \ldots & a_{1,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{i-1,1} & \ldots & a_{i-1,j} & \ldots & a_{i-1,n} \\ 0 & \ldots & a_{i,j} & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \ldots & a_{n,j} & \ldots & a_{n,n} \end{vmatrix}.$$

Мы будем последовательно менять местами столбцы справа налево, начиная с $j^{\text{го}}$, пока не выведем $j^{\text{ый}}$ столбец на $I^{\text{ое}}$ место. Аналогично поступаем с $i^{\text{ой}}$ строкой. Поскольку каждое такое перемещение меняет знак определителя, то определитель $|A|$ будет отличаться от полученного определителя множителем $(-1)^s$,
$s = (j-1) + (i-1) = (i+j) - 2$. Итак,

$$|A| = (-1)^{i+j-2} \begin{vmatrix} a_{ij} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ a_{1j} & a_{11} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{nj} & a_{n1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{n,n} \end{vmatrix}.$$

Используя предыдущий случай:

$$|A| = (-1)^{-2} \cdot a_{ij} \cdot A_{ij} = a_{ij} \cdot A_{ij}.$$

□

Теорема 3.5.2. *Определитель порядка n равен сумме попарных произведений элементов какой-либо строки на их алгебраические дополнения.*

Доказательство. Зафиксируем $i^{\text{ую}}$ строку определителя A и представим элемент этой строки в виде

$$\begin{aligned} a_{i1} &= a_{i1} + 0, \\ a_{i2} &= 0 + a_{i2}, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{in} &= 0 + a_{in}. \end{aligned}$$

Тогда $i^{\text{ую}}$ строку определителя $|A|$ можно рассматривать как сумму двух строк. А потому по свойству 6 определителей имеем

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & 0 & \dots & a_{i-1,n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Со вторым определителем справа в полученном равенстве поступаем аналогичным образом, и т.д. Через n шагов получим

$$\begin{aligned} |A| = &\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{i2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \dots + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \\ &= a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}. \end{aligned}$$

□

Теорема 3.5.3. *При* $i \neq k$

$$\sum_{j=1}^{n} a_{ij}A_{kj} = 0,$$

т.е. сумма попарных произведений элементов какой-либо строки на алгебраические дополнения элементов другой строки равна 0.

Доказательство. Пусть дан определитель

$$|A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

и рассмотрим определитель

$$|B| = \begin{vmatrix} b_{11} & \dots & b_{1n} \\ . & . & . \\ b_{n1} & \dots & b_{nn} \end{vmatrix}$$

элементы которого удовлетворяют условиям:

$$\begin{aligned} b_{ml} &= a_{ml}, \qquad (l = 1, 2, \dots, n), \qquad \text{если } m \neq k \\ b_{kl} &= a_{il}, \qquad (l = 1, 2, \dots, n), \end{aligned}$$

т.е. определители $|A|$ и $|B|$ имеют одинаковые строки, кроме $k^{\text{ой}}$, а именно $k^{\text{ая}}$ строка определителя $|B|$ совпадает с $i^{\text{ой}}$ определителя $|A|$, а значит и со своей $i^{\text{ой}}$ строкой. Но тогда по 4 свойству определителей $|B| = 0$. Применим к определителю $|B|$ предыдущую теорему для $k^{\text{ой}}$ строки, тогда

$$0 = |B| = \sum_{j=1}^{n} b_{ij} B_{kj}.$$

Поскольку все строки определителей $|A|$ и $|B|$ кроме $k^{\text{ой}}$, совпадают, то алгебраические дополнения элементов $k^{\text{ых}}$ строк этих определителей равны, так что $A_{kj} = B_{kj}$. Если еще вспомнить, что $b_{kj} = a_{ij}$, $j = 1, \dots, n$, то получим

$$0 = \sum_{j=1}^{n} a_{ij} A_{kj}.$$

□

Следствие. ***(Формулы элементов обратной матрицы)*** *Пусть A — невырожденная матрица порядка n, так что $|A| \neq 0$. Мы знаем, что существует A^{-1} . Но как ее определить по элементам матрицы A? Образуем матрицу $\widetilde{A}$, элементы которой $\widetilde{a}_{ij}$ удовлетворяют равенствам*

$$\widetilde{a}_{ij} = \widetilde{A}_{ji},$$

где $\widetilde{A}_{ji}$ — алгебраическое дополнение в $|A|$ элемента $\widetilde{a}_{ji}$. Матрица $\widetilde{A}$ называется ***присоединенной*** *к A. Рассмотрим произведение*

$$A\widetilde{A} = \begin{vmatrix} b_{11} & \dots & b_{1n} \\ . & . & . \\ b_{n1} & \dots & b_{nn} \end{vmatrix},$$

где

$$b_{ij} = \sum_{k=1}^{n} a_{ik}\widetilde{a}_{kj} = \sum_{k=1}^{n} a_{ik}A_{kj} = \begin{cases} 0 & \text{если } i \neq j, \\ |A| & \text{если } i = j. \end{cases}$$

Поэтому

$$A\widetilde{A} = \begin{vmatrix} |A| & 0 & \dots & 0 \\ 0 & |A| & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & |A| \end{vmatrix} = |A| \cdot E.$$

Отсюда следует, что матрица

$$\frac{1}{A} \cdot \widetilde{A} = \begin{vmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \dots & \frac{A_{n1}}{|A|} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \dots & \frac{A_{nn}}{|A|} \end{vmatrix}$$

является правой обратной к A, а в силу обратимости A обязательно $\frac{1}{A} \cdot \widetilde{A} = A^{-1}$.

Чтобы завершить рассмотрение обратных матриц перечислим несколько свойств:

1. Если A и B — квадратные невырожденные матрицы, то
$$(AB)^{-1} = B^{-1}A^{-1}.$$
2. Если A— невырожденная, то $(A^k)^{-1} = (A^{-1})^k$.
3. $(A^{-1})' = (A')^{-1}$ — следует из формулы для A^{-1}.
4. Если A, B, C— матрица порядка n, причем $|A| \neq 0$, то существуют матрицы, X и Y определяемые однозначно, такие что
$$AX = B \qquad \text{и} \qquad YA = C,$$
а именно, $X = A^{-1}B$, $Y = CA^{-1}$.

Теперь мы завершаем рассмотрение методов вычисления определителей.

Лемма 3.5.1. *Пусть M— минор порядка k в определителе $|A|$ порядка n, и пусть A_M— алгебраическое дополнение минора M. Тогда произведение любого члена минора M на любой член из его алгебраического дополнения является членом определителя $|A|$.*

Доказательство. Предположим сначала, что минор M расположен в левом верхнем углу определителя $|A|$

$$|A| = \begin{vmatrix} M & C \\ B & M^c \end{vmatrix}.$$

Поскольку, $A_M = (-1)^{S_M} M^c$, где $S_M = (1 + \ldots + k) + (1 + \ldots + k)$— четное, то $A_M = M^c$.
Выберем произвольный член минора M:

$$\rho(\sigma) a_{1,\alpha_1} \ldots a_{k,\alpha_k},$$

где $\rho(\sigma)$ — знак подстановки

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & k \\ \alpha_1 & \alpha_2 & \ldots & \alpha_k \end{pmatrix}.$$

Выпишем теперь произвольный член A_M:

$$\rho(\tau) a_{k+1,\alpha_{k+1}} \ldots a_{n,\alpha_n},$$

где $\rho(\tau)$ — знак подстановки

$$\tau = \begin{pmatrix} k+1 & \ldots & n \\ \alpha_{k+1} & \ldots & \alpha_n \end{pmatrix}.$$

Произведение $a_{1,\alpha_1} \ldots a_{k,\alpha_k} a_{k+1,\alpha_{k+1}} \ldots a_{n,\alpha_n}$ представляет собой произведение элементов определителя $|A|$, взятых из разных строк и разных столбцов. В определителе $|A|$ это произведение имеет знак, равный знаку подстановки γ

$$\gamma = \begin{pmatrix} 1 & 2 & \ldots & k & k+1 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_k & \alpha_{k+1} & \ldots & \alpha_n \end{pmatrix}.$$

Поскольку $\alpha_1, \ldots, \alpha_k \leq k$, а $\alpha_{k+1}, \ldots, \alpha_n > k$, то пара (α_i, α_j), $i \leq k$, $j > k$, не образует инверсию, а потому число инверсий подстановки γ равно сумме числа инверсий подстановок σ и τ, и значит

$$\rho(\gamma) = \rho(\sigma) \cdot \rho(\tau).$$

Так, что в рассматриваемом случае утверждение леммы доказано.
Пусть теперь минор M расположен на пересечении строк с номерами $i_1, \ldots, i_k$ и столбцов с номерами $j_1, \ldots, j_k$. Перестановками строк и столбцов мы выведем его в левый верхний угол. При этом определитель $|A|$ перейдет в определитель $|B|$, отличающийся от него расположением строк и столбцов, а потому и знаком. Этот знак равен $(-1)^d$, где

$$d = (i_1 - 1) + (i_2 - 2) + \ldots + (i_k - k) + (j_1 - 1) + (j_2 - 2) + \ldots + (j_k - k) =$$
$$= (i_1 + i_2 + \ldots + i_k) + (j_1 + j_2 + \ldots + j_k) - 2(1 + 2 + \ldots + k) = S_M - 2(1 + 2 + \ldots + k).$$

Поэтому $(-1)^d = (-1)^{S_M}$.
Алгебраическое дополнение минора M в $|A|$ равно $(-1)^{S_M}$, умноженной на дополнительный минор M^c, который в определителе $|B|$ является алгебраическим дополнением для M.
В определителе $|B|$ мы имеем дело с разобранным уже случаем, так что произведение любого члена минора M на любой член M^c является членом определителя $|B|$, а с учетом знака $(-1)^d$ это произведение будет членом определителя и будет являться произведением члена минора M в $|A|$ на член алгебраического дополнения M в $|A|$. □

Теорема (**Лапласа**). *Пусть $|A|$ — определитель порядка n. Зафиксируем в нем k строк. Из n столбцов определителя $|A|$ и выбранных k строк можно образовать $\dfrac{n!}{k!(n-k)!}$ миноров $k^{ого}$ порядка. Тогда сумма всех попарных произведений этих миноров на их алгебраические дополнения равна определителю $|A|$.*

Доказательство. Из комбинаторики известно, что из n элементов можно составить точно $\dfrac{n!}{k!(n-k)!}$ различных наборов по k элементов в каждом. Так, что мы действительно из выбранных k строк можем составить ровно $\dfrac{n!}{k!(n-k)!}$ миноров $k^{\text{ого}}$ порядка. Попарные произведения членов этих миноров и их алгебраических дополнений для разных миноров дают разные члены определителя $|A|$ (**почему?**). Если теперь учесть, что в миноре порядка k имеется $k!$ членов, а в его алгебраическом дополнении (порядка $n-k$) имеется $(n-k)!$ членов, то каждое произведение минора на его алгебраическое дополнение дает $k!(n-k)!$ членов определителя $|A|$, но всех различных произведений миноров и их алгебраических дополнений имеется ровно $\dfrac{n!}{k!(n-k)!}$, поэтому такие произведения породят

$$k!(n-k)! \cdot \frac{n!}{k!(n-k)!} = n!$$

членов определителя $|A|$, то есть все его члены. □

Пример 20. Вычислить определитель

$$\begin{vmatrix} 1 & 0 & -2 & 1 \\ 3 & -1 & 2 & 1 \\ 3 & 0 & -1 & 0 \\ 1 & 2 & -2 & 0 \end{vmatrix}.$$

Выделим I и III строки и будем по ним образовывать миноры $2^{\text{ого}}$ порядка и их алгебраические дополнения:

Миноры	**Алгебраические дополнения**
$\begin{vmatrix} 1 & 0 \\ 3 & 0 \end{vmatrix} = 0$	$(-1)^{1+3+1+2} \cdot \begin{vmatrix} 2 & 1 \\ -2 & 0 \end{vmatrix} = -2$
$\begin{vmatrix} 1 & -2 \\ 3 & -1 \end{vmatrix} = 5$	$(-1)^{1+3+1+3} \cdot \begin{vmatrix} -1 & 1 \\ 2 & 0 \end{vmatrix} = -2$
$\begin{vmatrix} 1 & 1 \\ 3 & 0 \end{vmatrix} = -3$	$(-1)^{1+3+1+4} \cdot \begin{vmatrix} -1 & 2 \\ 2 & -2 \end{vmatrix} = 2$
$\begin{vmatrix} 0 & -2 \\ 0 & -1 \end{vmatrix} = 0$	$(-1)^{1+3+2+3} \cdot \begin{vmatrix} 3 & 1 \\ 1 & 0 \end{vmatrix} = 1$
$\begin{vmatrix} 0 & 1 \\ 0 & 0 \end{vmatrix} = 0$	$(-1)^{1+3+2+4} \cdot \begin{vmatrix} 3 & 2 \\ 1 & -2 \end{vmatrix} = -8$
$\begin{vmatrix} -2 & 1 \\ -1 & 0 \end{vmatrix} = 1$	$(-1)^{1+3+3+4} \cdot \begin{vmatrix} 3 & -1 \\ 1 & 2 \end{vmatrix} = -7$

$$|A| = 0 \cdot (-2) + 5 \cdot (-2) + (-3) \cdot (2) + 0 \cdot (1) + 0 \cdot (-8) + 1 \cdot (-7) = -23.$$

4 Общая теория систем линейных уравнений

4.1 Условия совместности системы линейных уравнений

Линейным уравнением от n неизвестных над полем P называется выражение вида

$$a_1x_1 + \ldots + a_nx_n = b,$$

где a_i, $i = 1, \ldots, n$, b — элементы поля P, называемые **коэффициентами уравнения**, а $x_1, \ldots, x_n$ называются **неизвестными**.
Системой линейных уравнений от n неизвестных называется совокупность линейных уравнений вида:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + \ldots + a_{2n}x_n = b_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{4.1}$$

Решением системы (4.1) называется всякий упорядоченный набор $x_1^0, \ldots, x_n^0$ элементов из P, такой что имеет место следующий ряд числовых равенств

$$\begin{cases} a_{11}x_1^0 + \ldots + a_{1n}x_n^0 = b_1, \\ a_{21}x_1^0 + \ldots + a_{2n}x_n^0 = b_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1^0 + \ldots + a_{mn}x_n^0 = b_m. \end{cases} \tag{4.2}$$

Система (4.1) называется **однородной**, если $b_1 = b_2 = \ldots = b_m = 0$.
Система

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases} \tag{4.3}$$

называется однородной системой, соответствующей системе (4.1).
Система линейных уравнений называется **совместной**, если она имеет хотя бы одно решение $x_1^0, \ldots, x_n^0$. В противном случае она называется **несовместной**. Совместная система называется **определенной**, если она имеет единственное решение. Если система линейных уравнений имеет более одного решения, то система называется **неопределенной**.

Теорема 4.1.1. *Если система (4.1) неопределенная, то она имеет бесконечное число решений.*

Доказательство. В силу неопределенности системы (4.1) существуют два набора элементов из P:

$$(c_1, \ldots, c_n) \qquad \text{и} \qquad (d_1, \ldots, d_n),$$

являющиеся решениями системы (4.1).
Покажем, что для каждого $t \in P$ набор элементов

$$(h_1(t), \ldots, h_n(t)), \text{ где } h_i(t) = t \cdot c_i + (1-t) \cdot d_i,$$

является решением системы (4.1).
Подставим в i^{oe} уравнение системы (4.1):

$$\begin{aligned} a_{i1}h_1(t) + \ldots + a_{in}h_n(t) = a_{i1}(t \cdot c_1 + (1-t) \cdot d_1) + \ldots + a_{in}(t \cdot c_n + (1-t) \cdot d_n) = \\ = t(a_{i1}c_1 + \ldots + a_{in}c_n) - t(a_{i1}d_1 + \ldots + a_{in}d_n) + (a_{i1}d_1 + \ldots + a_{in}d_n) = \\ = tb_i - tb_i + b_i = b_i. \end{aligned}$$

Итак, удовлетворяется каждое уравнение системы (4.1) (в силу произвола в выборе i), а потому мы построили решение системы (4.1). Покажем еще, что при различных t мы получаем различные решения.
Действительно, пусть $t_1 \neq t_2$, но для всех $i = 1, \ldots, n$:

$$h_i(t_1) = h_i(t_2).$$

Тогда имеем:

$$\begin{array}{l} (t_1 - t_2)c_1 = (t_1 - t_2)d_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ (t_1 - t_2)c_n = (t_1 - t_2)d_n \end{array} \Longrightarrow c_i = d_i,\ i = 1, \ldots, n,$$

что противоречит тому, что решение $(_1, \ldots, c_n)$ и $(d_1, \ldots, d_n)$ — различны. $\square$

С системой линейных уравнений (4.1) связаны две матрицы

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix}.$$

Матрица A называется **основной матрицей** системы (4.1), а матрица B называется **расширенной матрицей системы** (4.1).
Обозначим еще через $\overline{x}$ столбцевую матрицу

$$\overline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

а через $\overline{b}$ столбцевую матрицу

$$\overline{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ - столбец свободных членов.}$$

Поскольку матрица A имеет размер $m \times n$, то возможно произведение матриц $A \cdot \overline{x}$, а результатом будет матрица размера $m \times 1$, то есть столбцевая матрица. Мы имеем

$$A \cdot \overline{x} = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \ldots\ldots\ldots\ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix}.$$

Поэтому система (4.1) допускает матричную запись

$$A \cdot \overline{x} = \overline{b}. \tag{4.4}$$

Решить систему (4.1) это значит найти такую столбцевую матрицу $\overline{x}$, которая удовлетворяет матричному уравнению (4.4).
Рассмотрим пространство m–мерных векторов P^m, то векторы из P^m будем записывать в виде столбцов длины m.

Обозначим через $\overline{a}_1, \ldots, \overline{a}_n$ столбцы основной матрицы A системы (1). Тогда $\overline{a}_i \in P^m, i = 1, \ldots, n$. И теперь систему (1) можно записывать в виде

$$x_1\overline{a}_1 + \ldots + x_n\overline{a}_n = \overline{b}. \tag{4.5}$$

Итак, для системы (4.1) мы нашли матричную и векторную формы записи. Каждая из форм записи позволить информацию о характере совместности системы (4.1).
Обозначим через T систему векторов $\{\overline{a}_1, \ldots, \overline{a}_n\}$, а через S — систему векторов $\{\overline{a}_1, \ldots, \overline{a}_n, \overline{b}\}$. Ясно, что T подсистема в S.

Теорема (**Кронекера-Капелли**). *Система линейных уравнений (4.1) совместна* $\Longleftrightarrow$ *когда ранг* $T =$ *ранг* S.

Доказательство. **Необходимость.** Если система (4.1) совместна и $(c_1, \ldots, c_n)$ — одно из ее решений, то для вектора $\overline{b} \in S$ имеем представление

$$\overline{b} = c_1\overline{a}_1 + \ldots + c_n\overline{a}_n,$$

а значит и каждый вектор из S является линейной комбинацией векторов из T. А это, как известно из теории пространства P^m, означает, что ранг T = ранг S.
Достаточность. Если ранг T = ранг S, то каждый вектор из S, в частности вектор $\overline{b}$, является линейной комбинацией векторов из T. Так что

$$\overline{b} = c_1\overline{a}_1 + \ldots + c_n\overline{a}_n.$$

Но тогда $(c_1, \ldots, c_n)$ — решение системы (4.1). □

Теорема (**Критерий определенности**). *Система (4.1) определена* $\Longleftrightarrow$ *когда ранг* T = *ранг* $S = n$.

Доказательство. **Необходимость.** Пусть система (4.1) определенная, и $(c_1, c_2, \ldots, c_n)$ — ее единственное решение. Из определенности системы (4.1) следует что она совместна, а тогда по теореме Кронекера-Капелли ранг T = ранг $S = r$. Покажем, что $n = r$. А поскольку число векторов в T равно n, то нам достаточно показать, что векторы в T линейно независимы. Но из предположения о линейной зависимости векторов $\overline{a}_1, \ldots, \overline{a}_n$ следует

$$d_1\overline{a}_1 + \ldots + d_n\overline{a}_n = 0, \tag{4.6}$$

причем не все d_i равны 0.
Поскольку $(c_1, \ldots, c_n)$ — решение системы (4.1), то

$$c_1\overline{a}_1 + \ldots + c_n\overline{a}_n = \overline{b}. \tag{4.7}$$

Откуда

$$(c_1 - d_1)\overline{a}_1 + \ldots + (c_n - d_n)\overline{a}_n = \overline{b}.$$

То есть $(c_1 - d_1, \ldots, c_n - d_n)$ — еще одно решение системы (4.1), что противоречит определенности системы (4.1).
Достаточность. Пусть ранг S = ранг $T = n$. Тогда в силу теоремы Кронекера-Капелли, система (4.1) совместна. И если бы она имела два решения $(c_1, \ldots, c_n)$ и $(d_1, \ldots, d_n)$, то

$$c_1\overline{a}_1 + \ldots + c_n\overline{a}_n = \overline{b},$$
$$d_1\overline{a}_1 + \ldots + d_n\overline{a}_n = \overline{b}.$$

Откуда

$$(c_1 - d_1)\overline{a}_1 + \ldots + (c_n - d_n)\overline{a}_n = 0,$$

причем не все величины $c_i - d_i$ равны 0. Но это противоречит линейной независимости векторов из T. □

Теорема (Крамера 1). *Система n–линейных уравнений с n неизвестными определена $\Longleftrightarrow$ когда векторы $\overline{a}_1, \ldots, \overline{a}_n$ — линейно независимы.*

Доказательство. **Необходимость.** Если данная система (4.1) определенная,то согласно предыдущей теореме ранг T = ранг $S = n$. Но это означает, что векторы $\overline{a}_1, \ldots, \overline{a}_n$ — линейно независимы.
Достаточность. Из линейной независимости векторов $\overline{a}_1, \ldots, \overline{a}_n$ следует, что ранг $T = n$. Ранг $S \geqslant$ ранг T, и так как $\overline{a}_i$ — векторы из P^n, то ранг $S \leqslant n$. Откуда ранг S = ранг $T = n$, а потому система (4.1) определенная. $\square$

Следствие. *Из критерия равенства нулю определителя порядка n и теоремы Крамера следует:*

Теорема (Крамера 2). *Система (4.1) n–линейных уравнений с n неизвестными определена (имеет единственное решение) $\Longleftrightarrow$ когда определитель основной матрицы A отличен от нуля.*

Правило Крамера

Пусть система (4.1) удовлетворяет условиям Теоремы Крамера 2. Запишем ее в матричном виде

$$A \cdot \overline{x} = \overline{b}.$$

Матрица A невырождена, а потому

$$\overline{x} = A^{-1} \cdot \overline{b}$$

(заметим, что произведение $A^{-1} \cdot \overline{b}$ имеет смысл, так как A^{-1} имеет размер $n \times n$, а $\overline{b}$ — размер $n \times 1$).
Поскольку $A^{-1} = \dfrac{1}{|A|} \cdot \widetilde{A}$, то

$$\overline{x} = \frac{1}{|A|} \cdot \widetilde{A} \cdot \overline{b}.$$

Если правую часть последнего равенства обозначить столбцом $\begin{pmatrix} \delta_1 \\ \vdots \\ \delta_2 \end{pmatrix}$, то имеем $\delta_i = \frac{1}{|A|} \sum_{j=1}^{n} A_{ji} b_j$, где A_{ji} — алгебраическое дополнение элемента a_{ji} в матрице A.
Обозначим

$$|A_i| = \begin{vmatrix} a_{11} & \ldots & a_{1,i-1} & b_1 & a_{1,i+1} & \ldots & a_{1n} \\ . & . & . & . & . & . & . \\ a_{n1} & \ldots & a_{n,i-1} & b_n & a_{n,i+1} & \ldots & a_{n,n} \end{vmatrix}$$

($|A_i|$ получается из $|A|$ заменой $i^{\text{ого}}$ столбца $\overline{a}_i$ столбцом $\overline{b}$).
Вычислим $|A_i|$, разложив его по элементам $i^{\text{ого}}$ столбца

$$|A_i| = \sum_{j=1}^{n} b_j A_{ji}.$$

Таким образом, для определения решения системы n–линейных уравнений с n неизвестными и определителем $|A| \neq 0$, нами получено следующее **правило Крамера**:
Система имеет единственное решение $(x_1^0, \ldots, x_n^0)$, где

$$x_i^0 = \frac{|A_i|}{|A|}.$$

Доказанные выше условия совместности и определенности системы линейных уравнений становятся емкими и практически более удобными, если пользоваться матричным языком.

Определение. *Пусть A — произвольная матрица размера $m \times n$. **Строчным рангом** матрицы A называется ранг системы строк этой матрицы как n-мерных векторов. (**Обозначается** $r_C(A)$).*

Определение. ***Столбцевым рангом** матрицы A называется ранг системы столбцов этой матрицы как m-мерных векторов. (**Обозначается** $r_K(A)$).*

Определение. ***Минорным рангом** матрицы A называется максимальный порядок минора этой матрицы,отличного от нуля. (**Обозначается** $r_M(A)$).*

Теорема 4.1.2. *Для всякой матрицы A :*

$$r_C(A) = r_K(A) = r_M(A) = r.$$

Доказательство. Обозначим $r_M(A)$ через r. Тогда в матрице A рассмотрим минор $r^{\text{ого}}$ порядка, отличный от нуля. Для удобства записи (и только для этого) будем считать, что этот минор M расположен в левом верхнем углу матрицы A:

$$A = \left(\begin{array}{ccc|ccc} a_{11} & \ldots & a_{1,r} & a_{1,r+1} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{r,1} & \ldots & a_{r,r} & a_{r,r+1} & \ldots & a_{r,n} \\ \hline a_{r+1,1} & \ldots & a_{r+1,r} & a_{r+1,r+1} & \ldots & a_{r+1,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \ldots & a_{n,r} & a_{n,r+1} & \ldots & a_{n,n} \end{array}\right).$$

Из условия, $M \neq 0 \implies$ строки и столбцы M — линейно независимы, а потому линейно независимы первые r строк и первые r столбцов матрицы A (пояснить

почему?)
Отсюда

$$r_M(A) = r \leqslant r_C(A),$$
$$r_M(A) = r \leqslant r_K(A).$$

Если мы покажем справедливость противоположных неравенств, то утверждение теоремы будет доказано. Для этого докажем. что каждый столбец матрицы A (и аналогично каждая строка) с номером $> r$ является линейной комбинацией первых r столбцов (соответственно, строк) этой матрицы.
Возьмем $l^{\text{ый}}$ столбец K_l матрицы A. Мы имеем

$$K_l = c_1K_1 + \ldots + c_rK_r \iff a_{il} = c_1a_{i1} + \ldots + c_ra_{ir},$$

где $c_1, \ldots, c_r$ не зависят от i, $i = 1, \ldots, m$. Рассмотрим определитель

$$M_{r+1} = \begin{pmatrix} a_{11} & \ldots & a_{1r} & a_{1l} \\ \cdot & \cdot & \cdot & \cdot \\ a_{r1} & \ldots & a_{rr} & a_{rl} \\ a_{i1} & \ldots & a_{ir} & a_{il} \end{pmatrix},$$

здесь i — любое из чисел $1, 2, \ldots, m$.
Имеем $M_{r+1} = 0$.
Действительно, если $1 \leqslant i \leqslant r$, то $M_{r+1} = 0$, как определитель с равными строками: $i^{\text{ой}}$ и последней. Если же $i > r$, то $M_{r+1} = 0$, как минор $r + 1$ порядка матрицы A.
Разложим M_{r+1} по элементам $(r + 1)$ строки.
Тогда

$$0 = M_{r+1} = a_{i1}c'_1 + \ldots + a_{ir}c'_r + a_{il}c'_l,$$

где $c'_1, \ldots, c'_r, c'_l$ — алгебраические дополнения в M_{r+1} элементов последней строки, а потому не зависят от i. Кроме того,

$$c'_l = M_r \neq 0.$$

А потому имеем

$$a_{il} = c_1a_1 + \ldots + c_ra_r,$$

где $c_j = \dfrac{c'_j}{c'_l}$ — не зависят от i.
Этим показано, что l столбец, $l = r+1, \ldots, n$, является линейной комбинацией первых r столбцов матрицы A, а потому $r_K(A) \leqslant r$. Аналогично доказывается, что $r_C(A) \leqslant r$. □

Определение. *Общее значение строчного, столбцевого и минорного рангов матрицы A называется* ***рангом*** *A. (****Обозначается*** *$r(A)$).*

И тогда имеем:

Теорема (**Кронекера-Капелли**). *Система линейных уравнений (4.1) совместна $\Longleftrightarrow$ когда $r(A) = r(B)$, то есть когда ранги основной и расширенной матриц совпадают.*

Теорема (**Крамера**). *Система линейных уравнений (4.1) будет определенной $\Longleftrightarrow$ когда $r(A) = r(B) = n$, то есть когда ранги основной и расширенной матриц равны числу неизвестных.*

Теорема (**о ранге произведения матриц**). *Пусть матрицы A и B таковы, что AB — существует. Тогда*

$$r(AB) \leqslant \min(r(A), r(B)).$$

Доказательство. Пусть $A = (a_{ij})$ — матрица размера $m \times n$, $B = (b_{ij})$ — матрица размера $n \times l$, тогда $C = (c_{ij})$ — матрица размера $m \times l$ и кроме того $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Отсюда видно, что $j^{\text{ый}}$ столбец матрицы C равен линейной комбинации столбцов матрицы A (с коэффициентами линейной комбинации $b_{1j}, b_{2j}, \ldots, b_{nj}$). Аналогично $i^{\text{ая}}$ строка матрицы C является линейной комбинации строк матрицы B с коэффициентами линейной комбинации $a_{i1}, a_{i2}, \ldots, a_{in}$. Но тогда ранг системы столбцов матрицы C не превосходит ранга системы столбцов матрицы A, то есть $\leqslant r(A)$. Итак, $r(C) \leqslant r(A)$, и аналогично $r(C) \leqslant r(B)$. А потому $r(AB) \leqslant \min(r(A), r(B))$. □

Следствие. *Ранг матрицы не изменится, если умножить ее слева или справа на квадратную невырожденную матрицу.*

Доказательство. В самом деле, пусть A — квадратная невырожденная, такая что AB — существует. Тогда $r(AB) \leqslant r(B)$,

$$r(B) = r(A^{-1} \cdot AB) \leqslant \min(r(A^{-1}), r(AB)) \leqslant r(AB).$$

А значит, $r(AB) = r(B)$.
Аналогично рассматривается случай умножения справа на квадратную невырожденную. □

4.2 Строение решений системы линейных уравнений

Пусть L — система n-мерных векторов из P^n (вообще говоря, бесконечная).

Определение. *L называется подпространством пространства P^n, если для любых $\overline{a}$ и $\overline{b} \in L$ и любых α и $\beta \in P$ обязательно $\alpha\overline{a} + \beta\overline{b} \in L$.*

Определение. *Пусть $\overline{c} \in P^n$, L — подпространство пространства P^n. Тогда совокупность векторов $\overline{c}+\overline{a}$, где $\overline{a}$ пробегает все L, называется линейным многообразием пространства P^n, и обозначается $\overline{c} + L$.*

Упражнение. Линейное многообразие $\overline{c} + L$ является подпространством пространства P^n (и тогда совпадает с L) $\Longleftrightarrow$ когда $\overline{c} \in L$.

Рассмотрим однородную систему линейных уравнений

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases} \tag{4.8}$$

Ее матрицу обозначим через A, а через $\overline{x}$ — столбец $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Тогда система (4.8) в матричном виде запишется так:

$$A \cdot \overline{x} = \overline{0}, \tag{4.9}$$

где $\overline{0}$ — нулевой вектор-столбец из P^m.

Теорема 4.2.1. *Решения системы (4.8) образуют подпространство пространства P^n.*

Доказательство. Каждое решение системы (4.8) является n-мерным вектором, а потому принадлежит P^n. Совокупность всех решений обозначим через L. Тогда если $\overline{a}$ и $\overline{b}$ — два решения, то есть два вектора из L, то имеем

$$A \cdot \overline{a} = \overline{0}, \qquad A \cdot \overline{b} = \overline{0}.$$

Если теперь α и β — произвольные элементы из P, то

$$A(\alpha\overline{a}) = \alpha A\overline{a} = \overline{0}, \qquad A(\beta\overline{b}) = \beta A\overline{b} = \overline{0}.$$

А потому, в силу дистрибутивности умножения матриц

$$A(\alpha\overline{a} + \beta\overline{b}) = \overline{0},$$

то есть $\alpha\overline{a} + \beta\overline{b} \in L$, и значит L — подпространство. $\square$

Рассмотрим теперь неоднородную систему, для которой система (4.8)является соответствующей однородной:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{4.10}$$

Или в матричном виде

$$A \cdot \overline{x} = \overline{b}, \qquad \overline{b} \in P^m. \tag{4.11}$$

Теорема 4.2.2. *Если система (4.10) совместна и $\overline{c}$ — одно из ее решений, то совокупность решений системы (4.10) образует линейное многообразие $\overline{c} + L$, где L — подпространство решений системы (4.8).*

Доказательство. Вектор $\overline{c}$ принадлежит линейному многообразию $\overline{c} + L$, ибо имеет место представление $\overline{c} = \overline{c} + \overline{0}$, где $\overline{0} \in L$.
Кроме того, каждый вектор из $\overline{c} + L$ является решением системы (4.10) (или, что все равно, уравнения (4.11)). Действительно, пусть $\overline{c} + \overline{a} \in \overline{c} + L$. Тогда $A\overline{a} = \overline{0}$, и значит

$$A(\overline{c} + \overline{a}) = A\overline{c} + A\overline{a} = \overline{b} + \overline{0} = \overline{b}.$$

Пусть теперь, $\overline{c}_1$ — произвольное решение системы (4.10), тогда из равенств

$$A\overline{c} = \overline{b},$$
$$A\overline{c}_1 = \overline{b},$$

следует, $A(\overline{c}_1 - \overline{c}) = \overline{0}$, то есть $\overline{c}_1 - \overline{c} \in L$, а значит, $\overline{c}_1 - \overline{c} = \overline{a} \in L$. Откуда

$$\overline{c}_1 = \overline{c} + \overline{a} \in \overline{c} + L.$$

□

Замечание. Из доказательства теоремы 4.2.2 следует, что разность двух решений линейной системы уравнений является решением соответствующей однородной системы.

Определение. *Пусть L — подпространство пространства P^n. Ранг системы векторов из L, называется* ***размерностью*** *L.*

Определение. *Пусть $\overline{c} + L$ — линейное многообразие. Ранг системы векторов из $\overline{c} + L$ называется* ***рангом многообразия****.*

Теорема 4.2.3. *Пусть L — подпространство решений системы (4.8), а $\overline{c} + L$ — линейное многообразие решений системы (4.10), причем $\overline{c} \notin L$ (то есть система (4.10) строго неоднородная).Тогда если размерность L равна k, то ранг $\overline{c} + L$ равен $k + 1$.*

Доказательство. Пусть $\overline{a}_1, \ldots, \overline{a}_k$ — линейно независимые векторы из L, так что каждый вектор из L является их линейной комбинацией. Покажем, что векторы $\overline{c}, \overline{c}+\overline{a}_1, \ldots, \overline{c}+\overline{a}_k \in \overline{c}+L$ — линейно независимы. Действительно, пусть

$$\alpha_0\overline{c} + \alpha_1(\overline{c}+\overline{a}_1) + \ldots + \alpha_k(\overline{c}+\overline{a}_k) = \overline{0}.$$

Тогда

$$(\alpha_0 + \alpha_1 + \ldots + \alpha_k)\overline{c} + \alpha_1\overline{a}_1 + \ldots + \alpha_k\overline{a}_k = \overline{0}.$$

Или

$$(\alpha_0 + \alpha_1 + \ldots + \alpha_k)\overline{c} = -(\alpha_1\overline{a}_1 + \ldots + \alpha_k\overline{a}_k) \in L,$$

что в силу $\overline{c} \notin L$, означает

$$\alpha_0 + \alpha_1 + \ldots + \alpha_k = 0.$$

Но тогда

$$\alpha_1\overline{a}_1 + \ldots + \alpha_k\overline{a}_k = \overline{0}$$

и ввиду линейной независимости $\overline{a}_1, \ldots, \overline{a}_k$, следует $\alpha_1 = \ldots = \alpha_k = 0$. А потому и $\alpha_0 = 0$.
Более чем $(k+1)$ линейно независимых векторов в $\overline{c}+L$ быть не может, ибо, если бы $\overline{c}_1, \ldots, \overline{c}_{k+1}, \overline{c}_{k+2}$ были бы такими векторами, то векторы $\overline{c}_1 - \overline{c}_{k+2}, \ldots, \overline{c}_{k+1} - \overline{c}_{k+2}$ принадлежали бы L и были бы там линейно независимы, что невозможно. □

Из доказанных выше теорем следует, что для определения всех решений системы неоднородных линейных уравнений (4.10), достаточно определить подпространство решений соответствующей однородной системы (4.8) и какое-либо решение исходной неоднородной системы (4.10).
Итак, решаем две задачи:

а) Нахождение частного решения.

Мы считаем, что условия теоремы Кронекера-Капелли для системы (4.10) выполнены — иначе система (4.10) несовместна и нечего искать решения.
Итак, пусть $r(A) = r(B) = r$.
Это значит, что в системе строк матрицы B имеется r линейно независимых. Выделим их. (Вопрос об эффективном вычислении линейно независимых строк будет рассмотрен позже). Будем считать, что это первые r строк матрицы B. Это значит, что каждая другая строка матрицы B является линейной комбинацией ее первых строк. Переводя на язык уравнений системы (4.10), мы получаем, что первые r уравнений системы (4.10) обладают тем свойством, что каждое последующее уравнение системы получается из первых как линейная

комбинация их. Но тогда каждое решение системы первых r уравнений будет решением и остальных уравнений, так что система (4.10) эквивалентна системе

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1}x_1 + \ldots + a_{rn}x_n = b_r. \end{cases} \tag{4.12}$$

Итак, ищем решения системы (4.12).
Поскольку ранг матрицы A также равен r, то среди ее столбцов, а значит, и среди столбцов матрицы коэффициентов системы (4.12) имеется r линейно независимых. Пусть это будут первые r (это делается только с целью упрощения записи) столбцов.
Перепишем систему (4.12) в виде

$$\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \ldots - a_{1n}x_n, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1}x_1 + \ldots + a_{rr}x_r = b_r - a_{r,r+1}x_{r+1} - \ldots - a_{rn}x_n. \end{cases} \tag{4.13}$$

Определитель

$$\begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \cdot & \cdot & \cdot \\ a_{r1} & \ldots & a_{rr} \end{vmatrix}$$

отличен от нуля, ибо его столбцы линейно независимы. Поэтому, если неизвестным $x_{r+1}, \ldots, x_n$ придать какие-либо числовые значения, то остальные неизвестные системы (4.13) определятся однозначно (по правилу Крамера). Обычно, неизвестные $x_{r+1}, \ldots, x_n$ принято называть **свободными неизвестными**. Итак, придавая определенные значения свободным неизвестным, мы с помощью правила Крамера находим значения остальных неизвестных, а потому определяем решения системы (4.12), а значит и системы (4.10).
Поскольку нас интересует только одно решение системы (4.10) (**одно частное решение**), то достаточно ограничиться только одним набором свободных неизвестных $x_{r+1}, \ldots, x_n$, например, $x_{r+1} = \ldots = x_n = 0$. Таким образом, мы описали способ нахождения одного решения системы (4.10).

Для построения **общего решения** системы (4.10) найдем общее решение системы (4.8).

b) Нахождение подпространства решений L.

Теперь мы рассматриваем систему (4.8), которая получается из (4.10), если положить $\overline{b} = \overline{0}$. Тогда повторяя все рассуждения предыдущего пункта, мы от системы (4.8) перейдем к системе

$$\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r = -a_{1,r+1}x_{r+1} - \ldots - a_{1n}x_n, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1}x_1 + \ldots + a_{rr}x_r = -a_{r,r+1}x_{r+1} - \ldots - a_{rn}x_n. \end{cases} \tag{4.14}$$

Теперь нас интересует не одно частное решение этой системы, а всё подпространство L, которое можно построить, если определить максимальную линейно независимую подсистему векторов из L (ибо тогда L состоит из всевозможных линейных комбинаций векторов этой подсистемы).

Определение. *Максимальная подсистема линейно независимых векторов подпространства L называется* ***фундаментальной системой решений однородной линейной системы (4.8)***.

Теорема 4.2.4. *Если ранг матрицы A системы однородных линейных уравнений (4.8) равен r, то фундаментальная система решений системы (4.8) содержит $(n - r)$ решений.*

Доказательство. Возможны два случая:

1. $r = n$. Тогда система (4.14) принимает вид:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{n1}x_1 + \ldots + a_{nn}x_n = 0. \end{cases} \tag{4.15}$$

   И мы имеем квадратную систему с определителем $|A| \neq 0$, а потому по теореме Крамера эта система имеет единственное решение. Но одно решение этой системы мы знаем: $x_1 = 0, \ldots, x_n = 0$. Таким образом, L состоит из одного $\overline{0}$, то есть в L нет линейно независимых решений, значит нет фундаментальных решений, что согласуется с условием $(n - r) = 0$.

2. $r < n$. Тогда в системе (4.14) имеется $n - r$ свободных неизвестных

$$\begin{array}{llll} x_{r+1} = 1, & x_{r+2} = 0, & \ldots & x_n = 0, \\ x_{r+1} = 0, & x_{r+2} = 1, & \ldots & x_n = 0, \\ \ldots & \ldots & \ldots & \ldots \\ x_{r+1} = 0, & x_{r+2} = 0, & \ldots & x_n = 1. \end{array}$$

Каждый из наборов определяет (однозначно) решение системы (4.14). Таким образом, мы построили $(n-r)$ решений $\overline{f}_1, \ldots, \overline{f}_{n-r}$ системы (4.8). Покажем, что $\overline{f}_1, \ldots, \overline{f}_{n-r}$ как векторы из L линейно независимы.
В самом деле, если бы они были бы линейно зависимыми, то матрица, составленная из них как из строк, имела бы ранг $< (n-r)$. Но минорный ранг этой матрицы равен $n-r$, так как она имеет минор порядка $(n-r)$

$$\begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1$$

отличный от нуля. Противоречие означает, что векторы $\overline{f}_1, \ldots, \overline{f}_{n-r}$ линейно независимые.
Кроме того, пусть $\overline{f} \in L$ — произвольное решение системы (4.8)

$$\overline{f} = (k_1, \ldots, k_r, k_{r+1}, \ldots, k_n).$$

Рассмотрим вектор

$$\overline{f}_0 = k_{r+1}\overline{f}_1 + \ldots + k_n\overline{f}_{n-r}.$$

Каждый из векторов $\overline{f}$ и $\overline{f}_0$ удовлетворяет системе (4.8), а значит и системе (4.14). Но тогда и $\overline{f}-\overline{f}_0$ удовлетворяет системе (4.14). Вектор $\overline{f}-\overline{f}_0$ имеет последние $(n-r)$ компонент равными нулю, то есть для него значения свободных неизвестных равны 0. И так как значения свободных неизвестных **однозначно** определяют значения остальных неизвестных, то получаем, что первые r компонент вектора $\overline{f}-\overline{f}_0$ являются решениями системы уравнений

$$\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r = 0, \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{r1}x_1 + \ldots + a_{rr}x_r = 0. \end{cases}$$

Но это квадратная система однородных линейных уравнений с определителем, отличным от нуля. Поэтому по теореме Крамера она имеет единственное — нулевое решение.
Этим показано, что $\overline{f} = \overline{f}_0$, то есть $\overline{f}$ есть линейная комбинация $\overline{f}_1, \ldots, \overline{f}_{n-r}$, а потому $\overline{f}_1, \ldots, \overline{f}_{n-r}$ образуют фундаментальную систему решений.

□

Замечание. Если мы нашли частное решение системы (4.10) $\overline{c}$ и фундаментальную систему решений системы (4.8) $\overline{f}_1, \ldots, \overline{f}_{n-r}$, то общее решение системы (4.10) обычно записывают в виде

$$\overline{c} + c_1\overline{f}_1 + \ldots + c_{n-r}\overline{f}_{n-r},$$

где $c_1 \ldots, c_{n-r}$ — произвольные постоянные из поля P.

4.3 Эффективные методы вычисления ранга матриц и нахождения решений

В предыдущем параграфе мы видели, что вопрос о совместности системы линейных уравнений и о числе решений такой системы решается просто, если известны ранги матриц системы. Мы рассмотрим два метода вычисления рангов матриц. первый метод основан на следующей лемме:

Лемма 4.3.1. *Элементарные преобразования не меняют ранга матрицы.*

Доказательство. Для элементарных преобразований $\mathtt{I}^{\text{го}}$ и $\mathtt{III}^{\text{го}}$ типов это очевидно. Поэтому рассмотрим преобразование $\mathtt{II}^{\text{го}}$ типа.
Пусть к строке C_i прибавлена строка C_j, умноженная на число α. Покажем, что системы строк

$$T_1 = \{C_1, C_2, \ldots, C_i, \ldots, C_m\}$$

и

$$T_2 = \{C_1, C_2, \ldots, C_i' = C_i + \alpha C_j, \ldots, C_m\}$$

имеют одинаковые ранги. Но это следует из того, что каждая строка из T_2 является линейной комбинацией строк из T_1, и наоборот (ибо $C_i = C_i' - \alpha C_j$). Аналогичные рассуждения можно провести и для столбцов. □

Следствие. *Пусть A — заданная матрица, тогда элементарными преобразованиями ее можно привести к диагональному виду $D(a_1, \ldots, a_k)$, где $k = \min(m, n)$. Ранги матриц A и $D(a_1, \ldots, a_k)$ равны, но ранг диагональной матрицы равен числу ненулевых элементов ее главной диагонали (как минорный ранг матрицы).*

Пример 21. Найти ранг матрицы

$$A = \begin{pmatrix} -2 & 1 & 4 & 3 \\ 1 & 2 & -1 & 0 \\ 3 & -6 & 5 & 1 \end{pmatrix}.$$

Имеем

$$A \Longrightarrow \begin{pmatrix} 0 & 5 & 2 & 3 \\ 1 & 2 & -1 & 0 \\ 0 & -12 & 8 & 1 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 2 & 3 \\ 0 & -12 & 8 & 1 \end{pmatrix} \Longrightarrow$$

$$\Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 5 & 2 \\ 0 & 1 & -12 & 8 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & 2 \\ 0 & 1 & -12 & 8 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & 2 \\ 0 & 0 & -17 & 6 \end{pmatrix} \Longrightarrow$$

$$\Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -17 & 6 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -17 & 0 \end{pmatrix}; \qquad \rho(A) = 3.$$

При фактическом построении решений системы линейных уравнений важно знать не только ранги основной и расширенной матриц A и B, но и линейно независимые строки и столбцы этих матриц. Можно было бы предположить, что те строки и столбцы, где расположены ненулевые диагональные элементы как раз являются линейно независимыми. Но в общем случае это не так. Рассмотрим пример.

Пример 22.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Вычтем $4^{\text{ую}}$ строку из $2^{\text{ой}}$, а $5^{\text{ую}}$ строку из $3^{\text{ой}}$, и продолжим далее приведение A к диагональному виду с помощью элементарных преобразований:

$$A \Longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Но отсюда, конечно, не следует, что в матрице A первые три строки линейно независимы.

Однако с помощью метода Штифеля мы в состоянии вычленить в A линейно независимые строки и столбцы.

Пусть дана матрица A размера $m \times n$. Тогда ее строки представляют собой n-мерные векторы, а столбцы — m-мерные векторы.
Поэтому для системы строк и соответственно для системы столбцов A мы имеем две схемы Штифеля:

Строки

	$\bar{e}_1$	$\bar{e}_2$	$\dots$	$\bar{e}_n$
C_1	a_{11}	a_{12}	$\dots$	a_{1n}
C_2	a_{21}	a_{22}	$\dots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
C_m	a_{m1}	a_{m2}	$\dots$	a_{mn}

Столбцы

	$\bar{e}'_1$	$\bar{e}'_2$	$\dots$	$\bar{e}'_m$
K_1	a_{11}	a_{21}	$\dots$	a_{m1}
K_2	a_{12}	a_{22}	$\dots$	a_{m2}
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
K_n	a_{1n}	a_{2n}	$\dots$	a_{mn}

Мы видим, что исходные схемы метода Штифеля для строк и столбцов транспонированы друг к другу. Если в этих схемах выбирать одни и те же

разрешающие элементы, то различие будет наблюдаться только в разрешающих строчках и столбцах, а именно, в разрешающей строке $\mathtt{I}^{\text{ой}}$ таблицы элементы изменяют знак, но эти же элементы, находясь в разрешающем столбце $\mathtt{II}^{\text{ой}}$ таблицы не изменят своего знака. Аналогично и для разрешающей строки $\mathtt{II}^{\text{ой}}$ таблицы и разрешающего столбца $\mathtt{I}^{\text{ой}}$ таблицы. Итак, после первого шага преобразования схемы Штифеля мы получаем, что коэффициенты, соответствующие клеточкам $(C_i, \bar{e}_j)$ и $(\bar{e}'_i, K_j)$ равны между собой как по величине, так и по знаку. А коэффициенты, лежащие соответственно в клетках (C_i, C_r) и (K_s, K_i) (у нас наверх перебросились C_r и $\bar{e}_s$, K_s и $\bar{e}'_r$) равны по абсолютной величине, но различны по знаку. Такая же картинка для пар (C_s, C_j) и (K_j, K_r).

По индуктивному рассуждению получаем, что в клетках типа $(C_i, \bar{e}_j)$ и $(\bar{e}'_i, K_j)$ (и аналогично, в клетках $(\bar{e}_i, C_j)$ и $(K_i, \bar{e}'_j)$) расположены равные величины, а в клетках типа (C_i, C_j) и (K_j, K_i) коэффициенты равны по величине, но противоположны по знаку.

Далее, так как в матрице столбцевой и минорной ранги равны, то число переброшенных наверх строк C_i будет равно числу переброшенных наверх столбцов K_j. Так что процесс остановится одновременно в двух схемах Штифеля.

Предыдущие рассуждения показывают, что достаточно работать только с одной схемой Штифеля, ибо если $\mathtt{I}$ схема приведена к виду

	C_{i_1}	C_{i_2}	$\dots$	C_{i_k}	$\bar{e}_{j_{k+1}}$	$\dots$	$\bar{e}_{j_n}$
$\bar{e}_{j_1}$	$b_{j_1 i_1}$	$b_{j_1 i_2}$	$\dots$	$b_{j_1 i_k}$	$b_{j_1 i_{k+1}}$	$\dots$	$b_{j_1 i_n}$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$\bar{e}_{j_k}$	$b_{j_k i_1}$	$b_{j_k i_2}$	$\dots$	$b_{j_k i_k}$	$b_{j_k i_{k+1}}$	$\dots$	$b_{j_k i_n}$
$C_{i_{k+1}}$	$b_{i_{k+1} i_1}$	$b_{i_{k+1} i_2}$	$\dots$	$b_{i_{k+1} i_k}$	0	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
C_{i_m}	$b_{i_m i_1}$	$b_{i_m i_2}$	$\dots$	$b_{i_m i_k}$	0	$\dots$	0

то $\mathtt{II}$ схема приведется к виду

	K_{j_1}	K_{j_2}	$\dots$	K_{j_k}	$\bar{e}'_{i_{k+1}}$	$\dots$	$\bar{e}'_{i_m}$
$\bar{e}'_{i_1}$	$b_{j_1 i_1}$	$b_{j_2 i_1}$	$\dots$	$b_{j_k i_1}$	$-b_{i_{k+1} i_1}$	$\dots$	$-b_{i_m i_1}$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$\bar{e}'_{i_k}$	$b_{j_1 i_k}$	$b_{j_2 i_k}$	$\dots$	$b_{j_k i_k}$	$-b_{i_{k+1} i_k}$	$\dots$	$-b_{i_m i_k}$
$K_{j_{k+1}}$	$-b_{j_1 j_{k+1}}$	$-b_{j_2 j_{k+1}}$	$\dots$	$-b_{j_k j_{k+1}}$	0	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
K_{j_n}	$-b_{j_1 j_n}$	$-b_{j_2 j_n}$	$\dots$	$-b_{j_k j_n}$	0	$\dots$	0

Таким образом, мы заключаем, что строки $C_{i_1}, \dots, C_{i_k}$ и столбцы $K_{j_1}, \dots, K_{j_k}$ линейно независимы.

К тому же мы получили коэффициенты линейных представлений других строк (столбцов) через выделенные базы строк (столбцов) матрицы A.
Заметим, что номера $i_1, \ldots, i_k$ обозначают номера переброшенных наверх (а значит линейно независимых) строк, а номера $j_1, \ldots, j_k$ означают номера верхнего ряда, которые заняли переброшенные строки, и эти номера означают номера линейно независимых столбцов матрицы A.

Пример 23. Определить линейно независимые строки и столбцы матрицы

$$\begin{pmatrix} -1 & 4 & 3 & -2 & 1 \\ 2 & -1 & 1 & 4 & 2 \\ 1 & -2 & 4 & 8 & -3 \\ 1 & 5 & 11 & 8 & 1 \end{pmatrix}.$$

Имеем

	$\bar{e}_1$	$\bar{e}_2$	$\bar{e}_3$	$\bar{e}_4$	$\bar{e}_5$
C_1	-1	4	3	-2	1
C_2	2	-1	1	4	2
C_3	$\boxed{1}$	-2	4	8	-3
C_4	1	5	11	8	1

$\Longrightarrow$

	C_3	$\bar{e}_2$	$\bar{e}_3$	$\bar{e}_4$	$\bar{e}_5$
C_1	-1	$\boxed{2}$	7	6	-2
C_2	2	3	-7	-12	8
$\bar{e}_1$	1	2	-4	-8	3
C_4	1	7	7	0	4

$\Longrightarrow$

	C_3	C_1	$\bar{e}_3$	$\bar{e}_4$	$\bar{e}_5$
$2\bar{e}_2$	1	1	-7	-6	2
$2C_2$	7	3	-35	-42	$\boxed{22}$
$2\bar{e}_1$	4	2	-22	-28	10
$2C_4$	9	7	-35	-42	22

$\Longrightarrow$

	C_3	C_1	$\bar{e}_3$	$\bar{e}_4$	$2C_2$
$2\bar{e}_2$	8	16	-84	-48	2
$\bar{e}_5$	-7	-3	35	42	1
$2\bar{e}_1$	18	14	-134	-196	10
$2C_4$	44	88	0	0	22

$\div 22$

Строка C_4 не может быть переброшена, а потому процесс окончен. И мы имеем: в матрице A имеется 3 линейно независимые строки — C_1, C_2, C_3 и 3 линейно независимых столбца — K_1, K_2, K_5, причем

$$C_4 = 2C_1 + C_2 + C_3$$
$$K_3 = \frac{134}{11}K_1 + \frac{84}{11}K_2 - \frac{35}{22}K_5$$
$$K_4 = \frac{196}{11}K_1 + \frac{48}{11}K_2 - \frac{21}{11}K_5$$

Переходим к рассмотрению методов определения решений совместной системы (4.10).
Предположим, что рассмотренными выше методами мы привели систему (4.10)

к виду (4.13). Для построения частного решения системы (4.13) придаем свободным неизвестным какие-либо значения, например, нулевые. Получим систему

$$\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r = d_1, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1}x_1 + \ldots + a_{rr}x_r = d_r. \end{cases} \tag{4.16}$$

Элементарными преобразованиями строк матрицы

$$\begin{pmatrix} a_{11} & \ldots & a_{1r} & d_1 \\ \cdot & \cdot & \cdot & \cdot \\ a_{r1} & \ldots & a_{rr} & d_r \end{pmatrix}$$

приводим ее к треугольному виду

$$\begin{pmatrix} a'_{11} & a'_{12} & \ldots & a'_{1r} & d'_1 \\ 0 & a'_{22} & \ldots & a'_{2r} & d'_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a'_{rr} & d'_r \end{pmatrix}.$$

Ее диагональные элементы $a'_{11}, \ldots, a'_{rr}$ не равны нулю (почему?). Эта матрица соответствует системе линейных уравнений

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \ldots + a'_{1r}x_r = d'_1, \\ a'_{22}x_1 + \ldots + a'_{2r}x_r = d'_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a'_{rr}x_r = d'_r, \end{cases}$$

решение которой находится снизу вверх без особого труда.

Этот метод решения системы (4.16) связан с именем К.Гаусса (и называется методом исключений Гаусса).

Систему (4.16) можно, конечно, решить и по правилу Крамера. Но практически для больших r (уже при $r > 3$) этот метод весьма трудоемкий.

Достаточно простым для вычислений является метод, основанный на использовании схемы Штифеля. Но мы его здесь не рассматриваем.

4.4 Матричные уравнения

Пусть даны две матрицы A и B соответственно размеров $m \times n$ и $k \times l$. Возникает вопрос: существуют ли матрицы X и Y такие, что

$$AX = B, \tag{4.17}$$
$$YA = B. \tag{4.18}$$

Необходимым условием матричного уравнения (4.17) является условие $m = k$, а для уравнения (4.18) необходимо, чтобы $n = l$.
Если эти условия выполнены, то матрица X должна иметь размер $n \times l$, а матрица Y — $k \times m$. Но эти условия не являются достаточными. Так, если A и B – квадратные матрицы порядка n, причем A — вырождена, а B — невырождена, то искомые матрицы X и Y не существуют.

Исследуем только матричное уравнение (4.17), ибо уравнение (4.18) может быть изучено аналогично.
Итак, пусть A — матрица размера $m \times n$, а B — матрица размера $m \times k$. Ищем матрицу X размера $n \times k$ в виде

$$X = \begin{pmatrix} x_1 & y_1 & \dots & z_1 \\ \vdots & \vdots & \dots & \vdots \\ x_n & y_n & \dots & z_n \end{pmatrix}.$$

По-элементарным сравнением элементов матриц AX и B получаем следующие k систем линейных уравнений

$$\left\{ \begin{array}{rcl} a_{11}u_1 + \ldots + a_{1n}u_n = & \begin{array}{c|c|c|c} x & y & \dots & z \end{array} \\ a_{11}u_1 + \ldots + a_{1n}u_n = & \begin{array}{c|c|c|c} b_{11} & b_{12} & \dots & b_{1k} \end{array} \\ a_{11}u_1 + \ldots + a_{1n}u_n = & \begin{array}{c|c|c|c} b_{21} & b_{22} & \dots & b_{2k} \end{array} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \begin{array}{c|c|c|c} \vdots & \vdots & \dots & \vdots \end{array} \\ a_{m1}u_1 + \ldots + a_{mn}u_n = & \begin{array}{c|c|c|c} b_{m1} & b_{m2} & \dots & b_{mk} \end{array} \end{array} \right.$$

Системы линейных уравнений для определения $x_1, \ldots, x_n; y_1, \ldots, y_n; z_1, \ldots, z_n$ имеют одну и ту же матрицу коэффициентов — матрица A, а столбцами свободных членов будут соответственно, $\mathtt{I}, \mathtt{II}^{\text{ой}}, \ldots, k^{\text{ый}}$ столбцы матрицы B.

Матрица X будет определена, если будут определены решения каждой из k систем. А для этого необходимо и достаточно, чтобы каждый столбец матрицы B был линейной комбинацией столбцов матрицы A и мы приходим к следующему обобщению теоремы Кронекера-Капелли:

Теорема 4.4.1. *Пусть A — матрица размера $m \times n$, а B — матрица размера $m \times k$. Для того чтобы матричное уравнение $AX = B$ было разрешимо, необходимо и достаточно, чтобы ранг A = ранг $(A \cup B)$ (здесь $A \cup B$ — матрица, составленная из столбцов матриц A и B).*

Решение рассмотренных выше систем можно находить одновременно, используя указанную выше процедуру схемы Штифеля, или же метод исключения неизвестных Гаусса.

5 Кольцо многочленов

5.1 Основные определения

Определение. ***Многочленом*** *от переменной x над полем $\mathbf{P}$ называется выражение вида*

$$a_n x^n + \ldots + a_0,$$

где $a_0, \ldots, a_n \in P$, $n \geqslant 0$ — целое.

Совокупность всех многочленов над $\mathbf{P}$ обозначается через $\mathbf{P}[x]$. Многочлены обычно будем обозначать через $f(x)$, $g(x)$, $h(x)$ и т.д.

Слагаемые $a_n x^n$, $a_{n-1}x^{n-1}$, $\ldots$, $a_1 x$, a_0 будем называть **членами многочлена**, а числа a_n, a_{n-1}, $\ldots$, a_0 — **коэффициентами многочлена**.

Определение. *Пусть дан многочлен $f(x) = a_n x^n + \ldots + a_0$. Наибольший индекс k, $0 \leqslant k \leqslant n$, для которого $a_k \neq 0$, называется* ***степенью многочлена****, а число a_k — **старшим коэффициентом многочлена**; коэффициент a_0 называется свободным членом.*

Определение. *Если в многочлене $f(x) = a_n x^n + \ldots + a_0$ все коэффициенты равны 0, то многочлен $f(x)$ называется* ***нулевым многочленом****, и обозначается через 0.*

Для многочлена 0 степень не определяется.

Определение. *Два многочлена $f(x)$ и $g(x)$ называются* ***равными****, если соответственные* ***ненулевые коэффициенты их равны между собой****.*

Определение. *Пусть даны два многочлена*

$$f(x) = a_n x^n + \ldots + a_0$$
$$g(x) = b_m x^m + \ldots + b_0$$

соответственно степеней n и m (то есть $a_n \neq 0$, $b_m \neq 0$) и пусть для определенности $n \geqslant m$. Тогда ***суммой*** *двух многочленов (обозначается $f(x) + g(x)$) называется многочлен*

$$h(x) = c_n x^n + \ldots + c_0,$$

где

$$c_i = a_i + b_i, \qquad i = 0, 1, \ldots, m;$$
$$c_i = a_i, \qquad i = m+1, \ldots, n.$$

Отсюда видно, что при $n \neq m$ **степень суммы** двух многочленов $f(x)$ и $g(x)$ **равна максимальной из степеней** $f(x)$ и $g(x)$. Если же $n = m$, то степень суммы может быть меньше n, ибо $c_n = a_n + b_n$ может обращаться в нуль.

Если условиться обозначать степень многочлена $f(x)$ через $grad\, f(x)$, то

$$grad\,(f(x) + g(x)) \leqslant \max(grad\, f(x), grad\, g(x)). \tag{5.1}$$

Определение. *Произведением двух ненулевых многочленов $f(x)$ и $g(x)$ (обозначается $f(x) \cdot g(x)$) называется многочлен*

$$f(x) \cdot g(x) = c_{n+m}x^{n+m} + \ldots + c_0,$$

где

$$c_i = \sum_{\substack{i+j=k \\ 0 \leqslant i \leqslant n,\, 0 \leqslant j \leqslant n}} a_i b_j, \qquad k = 0, 1, \ldots, n+m.$$

Отсюда замечаем, что $c_{n+m} = a_n b_{m \neq 0}$, так что степень произведения двух многочленов равна сумме степеней перемножаемых многочленов:

$$grad\,(f(x) \cdot g(x)) = grad\, f(x) + grad\, g(x). \tag{5.2}$$

По определению полагаем: $f(x) \cdot 0 = 0 \cdot f(x) = 0$.

Из формул, определяющих коэффициенты суммы и произведения двух многочленов, заключаем, что **операции «+» и «·»** на множестве многочленов **коммутативны**.

Также легко проверяется, что эти операции **ассоциативны**, а умножение **дистрибутивно** относительно сложения.

Многочлен $f(x) = 1$ играет роль единицы по умножению, а $f(x) = 0$ — роль нуля по сложению.

И наконец, сложение обратимо, то есть для любого многочлена $f(x) = a_n x^n + \ldots + a_0$ существует многочлен (обозначается $-f(x)$)

$$-f(x) = (-a_n)x^n + \ldots + (-a_0),$$

такой что

$$f(x) + (-f(x)) = 0.$$

Но тогда мы получаем, что $\mathbf{P}[x]$ есть коммутативное кольцо с единицей. В этом кольце нет делителей нуля (это следует из того, что произведение двух ненулевых многочленов, а потому имеющих степень, есть многочлен со степенью, и значит ненулевой). Итак, $\mathbf{P}[x]$ — область целостности.

Заметим еще, что множество многочленов нулевой степени из $\mathbf{P}[x]$ совпадает с полем $\mathbf{P}$, то есть $\mathbf{P} \subset \mathbf{P}[x]$. Многочлены нулевой степени будем называть **константами**.

5.2 Идеалы кольца

Поскольку $\mathbf{P}[x]$ — коммутативное кольцо, то изучим подробнее структуру таких колец.

Определение. *Пусть K — коммутативное кольцо. Подмножество $\mathfrak{I} \subset K$ называется **идеалом** в K, если выполняются следующие требования:*

1. *для любых a, $b \in \mathfrak{I} \Longrightarrow a - b \in \mathfrak{I}$;*
2. *для любого $a \in \mathfrak{I}$ и любого $r \in K \Longrightarrow ar \in \mathfrak{I}$.*

Из первого требования для идеала следует, что **идеал кольца является подгруппой аддитивной группы кольца**.

Пример 24. 1. Пусть $\mathfrak{I}$ состоит из одного нуля кольца, $\mathfrak{I} = \{0\}$.
$\mathfrak{I}$ называется **нулевым идеалом** и обозначается $\mathfrak{I}(0)$.

2. Само кольцо K является идеалом и называется **единичным идеалом**.

3. Пусть a — произвольный элемент из K. Обозначим через $\mathfrak{I}(a)$ множество элементов вида $ar + na$, где r — любой элемент из K, а $na = \underbrace{a + \ldots + a}_{n}$, если $n \geqslant 0$ — целое, $na = \underbrace{(-a) + \ldots + (-a)}_{-n}$, если $n < 0$ — целое.

   Непосредственная проверка показывает, что $\mathfrak{I}(a)$ — идеал в K.
   $\mathfrak{I}(a)$ называется **главным идеалом**, порожденным элементом a.

   Если в кольце K имеется единица (обозначаемая через 1), то элемент

   $$na = n(ea) = ne \cdot a = a \cdot ne,$$

   так что $ne \in K$, а потому na имеет вид ar' и тогда $\mathfrak{I}(a)$ есть совокупность элементов вида ar, где r — пробегает всё кольцо K.

4. Если $a_1, \ldots, a_m$ — элементы из K, то множество $\mathfrak{I}(a_1, \ldots, a_m)$ элементов кольца K вида

$$a_1 r_1 + \ldots + a_m r_m + n_1 a_1 + \ldots + n_m a_m,$$

где $r_i \in K$, $n_i \in \mathbb{Z}$, есть идеал в K, называемый **идеалом, порожденным** $a_1, \ldots, a_m$.

Пусть $\mathfrak{I}$ — произвольный идеал кольца K. Множество элементов кольца K разобьем на классы так, что два элемента a, $b \in K$ принадлежат одному и тому же классу $\mathbb{C} \iff$ когда $(a - b) \in \mathfrak{I}$.

Упражнение. Два класса C_1 и C_2 либо совпадают, либо не имеют общих элементов.

На множестве классов введем операции сложения и умножения:

- **суммой** двух классов $C_1 + C_2$ называется класс C_3, получаемый следующим образом: если $a_1 \in C_1$, $a_2 \in C_2$, то класс C_3 — это класс, в котором содержится элемент $a_1 + a_2$;
- **произведением** двух классов $C_1 \cdot C_2$ называется класс C_3, в котором содержится элемент $a_1 \cdot a_2$.

Такое разбиение кольца K на классы напоминает разбиение $\mathbb{Z}$ на классы вычетов по модулю натурального m. И также как и там легко показать, что построенная совокупность классов есть коммутативное кольцо, причем если в K есть 1, то и этом кольце имеется единица — класс, содержащий 1. Это кольцо называется **кольцом классов вычетов по модулю идеала** $\mathfrak{I}$. (Иногда говорят, **фактор-кольцо кольца** K **по идеалу** $\mathfrak{I}$). Обозначается $K/\mathfrak{I}$.

Рассмотрим кольцо $\mathbb{Z}$ с обычными операциями сложения и умножения.
$\mathbb{Z}$ — кольцо с 1 и без делителей нуля. Ранее было показано, что подгруппы аддитивной группы кольца $\mathbb{Z}$ имеют вид $a\mathbb{Z} = \{an \,|\, n \in \mathbb{Z}\}$. Но тогда и каждый идеал в $\mathbb{Z}$ (будучи к тому же подгруппой аддитивной группы) имеет вид $\mathfrak{I}(a)$, то есть в $\mathbb{Z}$ каждый идеал — главный.

Определение. *Коммутативное кольцо без делителей нуля, в котором каждый идеал — главный, называется* ***кольцом главных идеалов****.*

Итак, $\mathbb{Z}$ — кольцо главных идеалов.

В дальнейшем, если не оговорено особо, рассматриваются коммутативные кольца с 1, являющиеся кольцами главных идеалов.

Пусть K — такое кольцо, и пусть a и b — произвольные элементы из K. Тогда идеал $\mathfrak{I}(a, b)$ — главный и состоит из элементов вида $ax + by$, где $x, y \in K$.

Так как $\mathfrak{I}(a, b)$ — главный идеал, то найдется $d \in K$, такое, что $\mathfrak{I}(a, b) = \mathfrak{I}(d)$.

Определение. *Пусть a, $b \in K$. Говорят, что a* ***делится на*** *b (обозначается $a \vdots b$), если $a \in \mathfrak{I}(b)$.*

Из этого определения следует, что поскольку $a \in \mathfrak{I}(d)$ и $b \in \mathfrak{I}(d)$, то a и b делятся на d. Но поскольку $d \in \mathfrak{I}(d) = \mathfrak{I}(a, b)$, то d представимо в виде

$$d = ax_0 + by_0,$$

с некоторыми x_0, $y_0 \in K$.
Из определения делимости $a \vdots b \implies a = br$, $r \in K$, а потому из равенства

$$d = ax_0 + by_0,$$

следует, что для всякого d', на которое одновременно делятся a и $b (a = d'r_1, b = d'r_2)$, обязательно следует $d = d'r_1x_0 + d'r_2y_0 = d'(r_1x_0 + r_2y_0) = d'r \in \mathfrak{I}(d')$, то есть $d \vdots d'$. Поэтому естественно назвать d **общим наибольшим делителем** a **и** b, и обозначается $d = (a, b)$.

Итак, доказана

Лемма 5.2.1. *В кольце главных идеалов с* 1 *любые два элемента имеют общий наибольший делитель*

Определение. *Элемент $a \in K$ называется* ***делителем единицы****, если в K есть элемент a^{-1} такой, что $a \cdot a^{-1} = 1$.*

Определение. *Два элемента a и b из K называются* ***взаимно простыми****, если любой их общий делитель является делителем* 1.

Лемма 5.2.2. *Элементы a и b из K будут взаимно простыми $\iff$ когда найдутся элементы x и y из K, такие что $ax + by = 1$.*

Доказательство. **Необходимость.** Пусть a и b взаимно простые и пусть d их ОНД. Тогда найдутся такие x и y из K, что

$$d = ax + by.$$

Но d — делитель единицы. Поэтому $d^{-1} \in K$ и мы имеем:

$$1 = d \cdot d^{-1} = a(xd^{-1}) + b(yd^{-1}).$$

Достаточность. Пусть $ax_1 + by_1 = 1$, и пусть d — их ОНД. Тогда для любых x и y из K

$$ax + by \in \mathfrak{I}(d).$$

Так что $1 = ax_1 + by_1 \in \mathfrak{I}(d) \implies 1 = dr$, $r \in K$, то есть d — делитель единицы. □

Определение. *Элемент $p \in K$ называется* ***простым*** *(иногда говорят* ***неприводимым****), если он делится только на себя и на делитель единицы, но не является делителем единицы.*

Теорема 5.2.1. *Пусть K — кольцо главных идеалов с единицей и пусть p — простой элемент из K. Тогда фактор-кольцо $K/\mathfrak{I}(p)$ есть поле.*

Доказательство. Фактор-кольцо $K/\mathfrak{I}(p)$ является коммутативным кольцом с 1. Поэтому утверждение теоремы будет доказано, если мы покажем, что каждый ненулевой класс из фактор-кольцо $K/\mathfrak{I}(p)$ обратим. Роль нулевого класса играет идеал $\mathfrak{I}(p)$. Поэтому элементы из ненулевого класса C могут быть записаны в виде

$$a + \mathfrak{I}(p), \qquad \text{где} \quad a \in C,\ a \notin \mathfrak{I}(p).$$

Но тогда a не делится на p, и в силу простоты p, элементы a и p — взаимно простые. Так что для некоторых $u, v \in K$

$$au + bv = 1$$

или $\qquad au = 1 + b(-v)$.
Таким образом, элемент au принадлежит классу, содержащему 1, а потому au находится в единичном классе фактор-кольца $K/\mathfrak{I}(p)$. Если теперь C' — класс, в котором лежит u, то имеем

$$C \cdot C' \text{ — единичный класс,}$$

то есть C' — обратный для C. □

Следствие. *В кольце $\mathbb{Z}$ рассмотрим идеал $\mathfrak{I}(p) = p\mathbb{Z}$ (совокупность целых чисел, делящихся на простое число p). Все условия теоремы выполнены, поэтому*

$$\mathbb{Z}/p\mathbb{Z} \text{ — поле.}$$

Но $\mathbb{Z}/p\mathbb{Z}$ — это кольцо классов вычетов по $\mod p$, состоящее из p классов. Таким образом, мы имеем пример поля, содержащего конечное число элементов.
Поле, содержащее конечное число элементов, называется **конечным**, или **полем Галуа**.
Конечные поля обладают одной особенностью:
пусть F — конечное поле, содержащее q элементов, и пусть $e \in F$ — единица поля. Рассмотрим суммы:

$$e, \quad e + e = 2e, \quad e + e + e = 3e, \quad \ldots, \quad e + e + \ldots + e = ne, \quad \ldots$$

Ясно, $ne \in F$ для любого натурального n. Но не все ne различны между собой (ибо в F только конечное число элементов). Значит найдутся натуральные n_1 и n_2, $n_1 < n_2$, такие, что $n_1 e = n_2 e \implies (n_2 - n_1)e = 0$, а значит найдется наименьшее натуральное n_0, такое, что $n_0 e = 0$. С таким явлением мы не встречались в полях $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Оказывается, что существуют и бесконечные поля (отличные, конечно, от $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), обладающие свойством $ne = 0$, для некоторых натуральных n и единицы e поля.

Определение. *Пусть* $\mathbf{P}$ *— произвольное поле. Поле* $\mathbf{P}$ *называется полем* ***конечной характеристики****, если для единицы* $e \in \mathbf{P}$ *существует наименьшее натуральное* p *такое, что* $pe = 0$*. При этом* p *называется* ***характеристикой поля****. Если такого* p *не существует, то поле* $\mathbf{P}$ *называется полем* ***нулевой характеристики****.*

Например, поле $\mathbb{Z}/7\mathbb{Z}$ — поле характеристики 7, а поле $\mathbb{R}$ имеет нулевую характеристику.

Упражнение. Доказать, что если $\mathbf{P}$ — поле конечной характеристики p, то p — простое число.

5.3 Кольцо главных идеалов $\mathbf{P}[x]$

Мы приступаем к подробному исследованию кольца многочленов $\mathbf{P}[x]$.

Теорема (о делении с остатком). *Для любых ненулевых многочленов* $f(x)$ *и* $g(x) \in \mathbf{P}[x]$ *найдутся многочлены* $q(x)$ *и* $r(x) \in \mathbf{P}[x]$*, такие что либо* $grad\, r(x) < grad\, g(x)$*, либо* $r(x) = 0$*, и*

$$f(x) = g(x)q(x) + r(x).$$

Доказательство. Пусть $grad\, f(x) = n$, $grad\, g(x) = m$ и a_n, b_m — соответственно старшие коэффициенты этих многочленов.
Если $n < m$, то полагаем $g(x) = 0$, $r(x) = f(x)$ и

$$f(x) = g(x) \cdot 0 + r(x), \quad grad\, r(x) < grad\, g(x).$$

Поэтому пусть $n \geqslant m$. Тогда степень многочлена $f(x) - a_n b_m^{-1} x^{n-m} g(x)$ меньше n, и его мы обозначим через $f_1(x)$. Имеем $grad\, f_1(x) = n_1 < n$.
И теперь, если $n_1 < m$, то представление получено

$$f(x) = g(x)a_n b_m^{-1} x^{n-m} + f_1(x),$$

с $q(x) = a_n b_m^{-1} x^{n-m}$, $r(x) = f_1(x)$.
Если же $n_1 \geqslant m$, то с многочленами $f_1(x)$ и $g(x)$ поступаем подобно тому, как

мы делали с $f(x)$ и $g(x)$. Этот процесс обязательно оборвется, так как степени получающихся многочленов $f_1(x)$, $f_2(x)$, ... убывают, и значит найдется такое k, что либо $f_k(x) = 0$, либо $grad\, f_k(x) < m$. В обоих случаях

$$f_k(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) - a'_{n_1} b_m^{-1} x^{n_1-m} g(x) - \ldots - a_{n_{k-1}}^{(k-1)} b_m^{-1} x^{n_{k-1}-m} g(x).$$

Полагая

$$q(x) = a_n b_m^{-1} x^{n-m} + a'_{n_1} b_m^{-1} x^{n_1-m} + \ldots + a_{n_{k-1}}^{(k-1)} b_m^{-1} x^{n_{k-1}-m},$$
$$r(x) = f_k(x),$$

получаем утверждение теоремы. □

Теорема 5.3.1. *Кольцо* $\mathbf{P}[x]$ *есть кольцо главных идеалов.*

Доказательство. Пусть $\mathfrak{I}$ — произвольный ненулевой идеал кольца $\mathbf{P}[x]$. Обозначим через $\mathfrak{M}$ — множество степеней многочленов из $\mathfrak{I}$. Это непустое множество неотрицательных целых чисел и по принципу наименьшего числа ограниченного снизу множества целых чисел в $\mathfrak{M}$ имеется наименьший элемент n_0. Пусть $g(x)$ — многочлен из $\mathfrak{I}$, имеющий эту наименьшую степень n_0, и пусть $f(x)$ — произвольный многочлен из $\mathfrak{I}$. На основании предыдущей теоремы имеем

$$f(x) = g(x)q(x) + r(x).$$

Многочлен $r(x) \in \mathfrak{I}$ и если бы $r(x) \neq 0$, то мы имели бы

$$grad\, r(x) < grad\, g(x) = n_0,$$

что противоречит минимальности n_0.
Итак, $r(x) = 0$, а значит $\mathfrak{I} = \mathfrak{I}(g(x))$, то есть каждый идеал $\mathfrak{I}$ в $\mathbf{P}[x]$ — главный. □

В кольце $\mathbf{P}[x]$ делителями единицы будут все ненулевые константы из $\mathbf{P}$ и только они. Ибо если $grad\, f(x) \geqslant 1$, то каков бы ни был ненулевой многочлен $g(x)$, всегда $grad\,(f(x) \cdot g(x)) \geqslant 1$, то есть произведение $f(x) \cdot g(x)$ никогда не может стать единицей.
Отсюда следует, что неприводимыми (простыми) многочленами из $\mathbf{P}[x]$ будут те и только те многочлены степени $\geqslant 1$, которые не делятся ни на какие неконстантные многочлены меньших степеней. Так что многочлены $ax + b$, $a \neq 0$, — неприводимые.

Теорема 5.3.2. *Всякий ненулевой многочлен* $f(x) \in \mathbf{P}[x]$ *допускает разложение в произведение неприводимых многочленов, и с точностью до множителей — делителей единицы и порядка следования неприводимых многочленов это разложение однозначно.*

Доказательство. Многочлены первой степени — сами неприводимые многочлены, а потому для них существование разложения доказано. Для многочленов степени > 1 доказательство сразу следует по индукции.
Поэтому докажем единственность.
Пусть мы имеем

$$f(x) = p_1(x) \cdot \ldots \cdot p_r(x) = q_1(x) \cdot \ldots \cdot q_s(x). \tag{5.3}$$

Мы считаем, что все $p_i(x)$ и $q_j(x)$ — неприводимые многочлены (то есть делители единицы уже включены в качестве множителей в эти неприводимые многочлены).

Если $r = 0$, то утверждение очевидно — все $q_j(x)$ — константы.

Если $r = 1$, то в первом разложении имеется только один неприводимый многочлен, а тогда и $s = 1$, то есть и во втором разложении есть только один неприводимый многочлен (иначе мы имели бы противоречие с неприводимостью $p_1(x)$).

Для $r > 1$ доказательство мы проведем индукцией по r. Итак, предполагаем, что если в одном из разложений меньше, чем r неприводимых многочленов, то разложение единственно.
Пусть теперь $f(x)$ — многочлен, содержащий одном из своих разложений r неприводимых многочленов, а в другом не менее r.
Рассмотрим фактор-кольцо $\mathbf{P}[x]/\mathfrak{I}(p_1(x))$. Это фактор-кольцо — поле. Обозначим через $C_{g(x)}$ класс вычетов этого фактор-кольца, содержащий многочлен $g(x)$. Ясно, что $C_{p_1(x)}$ — нулевой класс. Вообще, если $g(x) \vdots p_1(x)$, то $C_{g(x)}$ — также нулевой класс. На основании определения операции умножения классов имеем

$$C_{q_1(x)\ldots q_s(x)} = C_{q_1(x)} \ldots C_{q_s(x)}.$$

С другой стороны, $q_1(x) \cdot \ldots \cdot q_s(x) = f(x)$ и $f(x) \vdots p_1(x)$. Поэтому

$$0 = C_{f(x)} = C_{q_1(x)} \ldots C_{q_s(x)}.$$

Но классы $C_{q_i(x)}$ являются элементами поля, а в поле нет делителей нуля, значит хотя бы один из классов $C_{q_i(x)}$, например, $C_{q_1(x)}$, равен 0. Итак, $C_{q_1(x)} = 0$, а значит $q_1(x) \in \mathfrak{I}(p_1(x))$, то есть $q_1(x) \vdots p_1(x)$. А в силу неприводимости $q_1(x)$ следует, что $q_1(x)$ и $p_1(x)$ отличаются между собой только множителем — делитель единицы. Сокращая обе части разложения (5.3) на $p_1(x)$, мы оказываемся в условиях предположения индукции. □

Применим теперь теорему о делении с остатком к построению алгоритма Евклида для двух многочленов. Поскольку кольцо $\mathbf{P}[x]$ есть кольцо главных идеалов, то любые два многочлена $f(x)$ и $g(x)$ имеют ОНД. Наиболее удобный способ нахождения ОНД $(f(x), g(x))$ дает алгоритм Евклида:

$$f(x) = g(x)q_1(x) + r_1(x),$$

где либо $grad\, r_1(x) < grad\, g(x)$, либо $r_1(x) = 0$.
Если $r_1(x) = 0$, то ОНД $(f(x), g(x)) = g(x)$.
В противном случае:

$$g(x) = r_1(x)q_2(x) + r_2(x),$$

где либо $grad\, r_2(x) < grad\, r_1(x)$, либо $r_2(x) = 0$.
Этот процесс продолжаем далее. Поскольку степени многочленов целые числа $\geqslant 0$, то мы обязательно прийдем к остатку $r_{k+1}(x) = 0$. Поэтому мы имеем цепочку равенств:

$$\begin{cases} f(x) = g(x)q_1(x) + r_1(x), \\ g(x) = r_1(x)q_2(x) + r_2(x), \\ r_1(x) = r_2q_3(x) + r_3(x), \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), \\ r_{k-1}(x) = r_k(x)q_{k+1}(x). \end{cases} \tag{5.4}$$

Откуда легко получаем представление

$$r_k(x) = f(x)u(x) + g(x)v(x), \tag{5.5}$$

где $u(x)$ и $v(x)$ — многочлены.
Кроме того из равенств (5.4) следует, что $r_k(x)$ — ОНД $(f(x), g(x))$. Многочлены $u(x)$ и $v(x)$, дающие равенство (5.5), могут определяться неоднозначно, но всегда можно их выбрать так, чтобы $grad\, u(x) < grad\, g(x)$, $grad\, v(x) < grad\, f(x)$, и в этих условиях $u(x)$ и $v(x)$ определяются однозначно.

Пусть $f(x) \in \mathbf{P}[x]$ и $a \in \mathbf{P}$, тогда подставляя в выражение для $f(x)$ вместо x элемент a, получим некоторый элемент из $\mathbf{P}$, обозначаемый через $f(a)$ и называемый **значением многочлена** при $x = a$. Если $\mathbf{L}$ — некоторое расширение поля $\mathbf{P}$ и $\alpha \in \mathbf{L}$, то мы можем рассматривать $f(\alpha)$, которое, вообще говоря, принадлежит полю $\mathbf{L}$.

Элемент α из $\mathbf{P}$ или из некоторого расширения $\mathbf{L}$ поля $\mathbf{P}$ называется **корнем многочлена $f(x)$, если $f(\alpha) = 0$.**

Возникает вопрос: всякий ли многочлен, отличный от константы, имеет корни?
Так, например, раньше мы считали, что многочлен $x^2 + 1$ не имеет корней, но расширив $\mathbb{R}$ до $\mathbb{C}$, мы обнаружили корни.
Чтобы ответить на поставленный вопрос, изучим подробнее поле классов вычетов $\mathbf{P}[x]/\mathfrak{I}(p(x))$, где $p(x)$ — неприводимый многочлен из $\mathbf{P}[x]$. Каждый класс вычетов характеризуется остатком от деления многочленов этого класса на $p(x)$. Поэтому классы вычетов находятся во взаимно однозначном соответствии с многочленами

$$a_{n-1}x^{n-1} + \ldots + a_0, \qquad a_i \in \mathbf{P}[x], \qquad n = grad\, p(x).$$

Сумма двух таких многочленов определяется естественным образом, а чтобы получить произведение, надо сначала перемножить эти многочлены как обычно и заменить это произведение остатком от деления на $p(x)$.
Например, в кольце $\mathbb{Q}[x]$ многочлен x^2+3 неприводим. Поэтому классы вычетов поля $\mathbb{Q}[x]/\mathfrak{I}(x^2+3)$ характеризуются многочленами $ax+b$. И мы имеем $(2x+4)(-3x+2) = -6x^2-8x+8$, этот многочлен заменяем остатком от деления на x^2+3, а именно многочленом $10x+8$.
Обратный элемент в $\mathbf{P}[x]/\mathfrak{I}(p(x))$ находится так:
пусть $g(x)$ — остаток, отличный от нуля. Тогда $p(x)$ и $g(x)$ взаимно просты, а потому найдутся $u(x)$ и $v(x)$, степени которых меньше степени $p(x)$, такие

$$p(x)u(x) + v(x)g(x) = 1.$$

Но $p(x)v(x)$ как элемент поля $\mathbf{P}[x]/\mathfrak{I}(p(x))$ равен 0. Поэтому $g(x)v(x) = 1$ в поле $\mathbf{P}[x]/\mathfrak{I}(p(x))$, то есть $v(x)$ — обратный элемент для $g(x)$.

Теперь мы в состоянии доказать очень важную теорему Кронекера.

Теорема (Кронекера). *Для любого многочлена $f(x) \in \mathbf{P}[x]$, $grad\, f(x) \geqslant 1$, существует расширение $\mathbf{L}$ поля $\mathbf{P}$, в котором содержится корень этого многочлена.*

Доказательство. Поскольку $grad\, f(x) \geqslant 1$, то $f(x)$ допускает разложение в произведение простых, а потому найдется неприводимый многочлен $p(x)$, такой что

$$f(x) = p(x)f_1(x). \tag{5.6}$$

Обозначим через $\mathbf{L}$ фактор-кольцо $\mathbf{L} = \mathbf{P}[x]/\mathfrak{I}(p(x))$. Мы видели, $\mathbf{L}$ — поле, являющееся расширением поля $\mathbf{P}[x]$. Обозначим через $\bar{x}$ — класс вычетов поля $\mathbf{L}$, в котором содержится x. Рассмотрим значения многочленов $f(x)$, $p(x)$ и $f_1(x)$ при $x = \bar{x}$. Из соотношения (5.6) имеем:

$$f(\bar{x}) = p(\bar{x})f_1(\bar{x}) = 0 \qquad (\text{ибо} \quad p(\bar{x}) - \text{нулевой класс}).$$

Таким образом, $\bar{x} \in \mathbf{L}$ является корнем многочлена $f(x)$. □

Пример 25. Рассмотрим неприводимый многочлен $x^2+1 \in \mathbb{R}[x]$. Элементами поля $\mathbb{R}[x]/\mathfrak{I}(x^2+1)$ будут $a+b\bar{x}$, где a, $b \in \mathbb{R}$, а $\bar{x}$ — класс вычетов в котором содержится x. Если $a+b\bar{x}$ и $c+d\bar{x}$ — два элемента из $\mathbb{R}[x]/\mathfrak{I}(x^2+1)$, то суммой будет $(a+c)+(b+d)\bar{x}$, а произведением — остаток от деления $(a+b\bar{x})(c+d\bar{x})$ на x^2+1. Таким образом, $(a+b\bar{x})(c+d\bar{x}) = (ac-bd)+(ad+bc)\bar{x}$. Сравнивая эти значения суммы и произведения с результатами суммы и произведения двух комплексных чисел $a+bi$ и $c+di$, видим, что они идентичны. Поэтому поле $\mathbb{R}[x]/\mathfrak{I}(x^2+1)$ можно отождествить с полем комплексных чисел $\mathbb{C}$.
В поле $\mathbb{R}[x]/\mathfrak{I}(x^2+1)$ элемент $\bar{x}$ является корнем многочлена x^2+1, подобно тому как в поле $\mathbb{C}$ таким элементом является комплексное число i.

Следующая теорема устанавливает зависимость между корнями многочлена $f(x)$ и его линейными делителями (то есть делители — многочлены I$^{\text{ой}}$ степени).

Теорема (Безу). *Пусть$f(x) \in \mathbf{P}[x]$ и $grad\, f(x) \geqslant 1$. Элемент $\alpha \in \mathbf{P}$ является корнем $f(x) \iff$ когда $f(x)$ делится на $x - \alpha$.*

Доказательство. Разделим $f(x)$ на $(x - \alpha)$, тогда в силу алгоритма деления имеем

$$f(x) = (x - \alpha)g(x) + r(x), \quad grad\, r(x) < 1. \tag{5.7}$$

Поэтому, либо $r(x) = 0$, либо $r(x) = const = r$. Из равенства (5.7) видно, что

$$f(\alpha) = r.$$

А потому α — корень $f(x) \iff$ когда $r = 0$, то есть когда $f(x)$ делится на $(x - \alpha)$. □

Следствие 1. *Пусть $f(x) \in \mathbf{P}[x]$, а $\mathbf{L}$ — некоторое расширение поля $\mathbf{P}$, $\alpha_1, \ldots, \alpha_k$ — различные элементы из $\mathbf{L}$, являющиеся корнями $f(x)$. Тогда $f(x)$ делится на $(x - \alpha_1) \ldots (x - \alpha_k)$ в кольце $\mathbf{L}[x]$.*

Это утверждение следует непосредственно из теоремы Безу, если только еще учесть, что $(x - \alpha_1), \ldots, (x - \alpha_k)$ — различные неприводимые многочлены из $\mathbf{L}[x]$.

Следствие 2. *Если $f(x) \in \mathbf{P}[x]$ и $grad\, f(x) = n \geqslant 1$, то ни в каком расширении поля $\mathbf{P}$ многочлен $f(x)$ не может иметь более n различных корней.*

В самом деле, предположим, что в некотором расширении $\mathbf{L}$ $f(x)$ имеет $(n + 1)$ корней. По предыдущему следствию имеем

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_{n+1})g(x).$$

Но $grad\, f(x) = n$, $grad\, [(x - \alpha_1) \ldots (x - \alpha_{n+1})g(x)] \geqslant n + 1$, что нелепо.

Следствие 3. *Если два многочлена $f(x)$ и $g(x)$ из $\mathbf{P}[x]$ степеней не выше n, принимают одинаковые значения для $(n + 1)$ элементов из $\mathbf{P}$, то эти многочлены равны между собой.*

Действительно, разность этих многочленов либо равна нулю (и тогда утверждение доказано), либо есть многочлен степени $\geqslant 1$. Во втором случае, мы имеем многочлен степени $n \geqslant 1$, имеющий, по крайней мере, $(n + 1)$ корней, что невозможно.

Следствие 4. *Неприводимый многочлен из $\mathbf{P}[x]$ степени > 1 не имеет корней в $\mathbf{P}$.*

Действительно, иначе этот многочлен делился бы на $x - \alpha$ (α — корень многочлена), что противоречит неприводимости.

Следствие 5. *Для всякого многочлена положительной степени из кольца* $\mathbf{P}[x]$ *существует расширение* $\mathbf{L}$ *поля* $\mathbf{P}$, *в котором многочлен* $f(x)$ *имеет все свои корни.*

Это утверждение следует из теоремы Кронекера и следствия 1 теоремы Безу.

Из следствия 2 следует, что для всякого многочлена $f(x) \in \mathbf{P}[x]$ существует расширение $\mathbf{L}$ поля $\mathbf{P}$, в котором $f(x)$ разлагается в произведение линейных множителей.

Определение. *Минимальное поле* $\mathbf{L}$, *являющееся расширением поля* $\mathbf{P}$, *в котором многочлен* $f(x) \in \mathbf{P}[x]$ *разлагается на линейные множители, называется* ***полем разложения многочлена*** $f(x)$.

Пусть многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbf{P}[x]$ в некотором расширении $\mathbf{L}$ поля $\mathbf{P}$ имеет все свои корни $\alpha_1, \ldots, \alpha_n$ (не все α_i обязательно различные). Мы имеем

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_n).$$

Сравнивая теперь коэффициенты в двух представлениях $f(x)$, получаем **формулы Виета**:

$$\begin{aligned}
a_{n-1} &= -(\alpha_1 + \ldots + \alpha_n), \\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \ldots + \alpha_{n-1}\alpha_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
a_{n-k} &= (-1)^k \sum \alpha_{i_1} \ldots \alpha_{i_k}, \text{ (суммирование ведется по всем} \\
&\qquad \text{неупорядоченным наборам из } k \text{ элементов)} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
a_0 &= (-1)^n \alpha_1 \ldots \alpha_n.
\end{aligned}$$

5.4 Симметрические многочлены

Пусть $\mathbf{P}$ — некоторое поле и пусть $x_1, \ldots, x_n$ — выбранное множество символов, которые будем называть переменными или неизвестными.

Определение. *Многочленом от* $x_1, \ldots, x_n$ *над полем* $\mathbf{P}$ *называется формальная сумма конечного числа слагаемых вида*

$$ax_1^{k_1} \ldots x_n^{k_n}, \qquad a \in \mathbf{P}, \qquad k_1, \ldots, k_n \geqslant 0 — \text{ целые.}$$

Иначе говоря, многочлен от n переменных $x_1, \ldots, x_n$ есть

$$f(x) = \sum a_{k_1 \ldots k_n} x_1^{k_1} \ldots x_n^{k_n},$$

где сумма содержит лишь конечное число слагаемых.

Если на множестве многочленов от $x_1, \ldots, x_n$ естественным образом ввести операции «+» и «·», то это множество превращается в кольцо многочленов $\mathbf{P}[x_1, \ldots, x_n]$.

Степенью одночлена $ax_1^{k_1} \ldots x_n^{k_n}$ называется число, равное $k_1 + \ldots + k_n$.

Степенью многочлена называется максимальная из степеней, входящих в него одночленов.

Как и для многочленов от одной переменной справедливо утверждение: степень произведения многочленов из $\mathbf{P}[x_1, \ldots, x_n]$ равна сумме степеней сомножителей.

В кольце $\mathbf{P}[x_1, \ldots, x_n]$ нет делителей нуля, но оно не является кольцом главных идеалов при $n \geqslant 2$.

Упражнение. Доказать, что идеал $\mathfrak{I}(x_1, x_2)$ не является главным в $\mathbf{P}(x_1, x_2)$.

В многочлене от нескольких переменных не всегда можно добиться расположения его членов по убывающим или возрастающим степеням.

Так, например, как поступить с многочленом

$$f(x_1, x_2) = 2x_1^3 + x_1x_2^2 + 3x_1^2x_2 - 4x_2^2 + 2x_1 - 9.$$

Для удобства (и единообразия) записи используют **лексико-графическую (или словарную)** запись многочлена.

Для этого с каждым одночленом $ax_1^{k_1} \ldots x_n^{k_n}$ связывают его **цену** — вектор $(k_1, \ldots, k_n)$, и говорят, что одночлен $ax_1^{k_1} \ldots x_n^{k_n}$ **выше**, чем одночлен $bx_1^{l_1} \ldots x_n^{l_n}$, если первая ненулевая разность среди $k_1 - l_1, k_2 - l_2, \ldots, k_n - l_n$ положительна. Иногда говорят, что цена I члена выше цены второго члена. Так в приведенном выше примере одночлен $2x_1$ имеет цену $(1, 0)$, а одночлен $-4x_2^2$ — цену $(0, 2)$, поэтому $2x_1$, выше, чем $-4x_2^2$.

Если теперь члены многочлена расположить так, чтобы предыдущий член был выше любого последующего, то получим лексико-графическую (словарную) запись многочлена, которая характеризуется свойством однозначности.

Член многочлена с ненулевым коэффициентом м высшей ценой называется **высшим членом многочлена**.

Упражнение. Доказать, что высший член произведения многочленов равен произведению их высших членов, а цена высшего члена равна сумме цен высших членов сомножителей.

Определение. *Многочлен $f(x_1, \ldots, x_n)$ называется* ***симметрическим****, если он не меняется (то есть переходит в себя) при любой подстановке, примененной к переменным $x_1, \ldots, x_n$.*

Теорема 5.4.1. *Совокупность симметрических многочленов от $x_1, \ldots, x_n$ образует подкольцо в $\mathbf{P}[x_1, \ldots, x_n]$.*

Это утверждение есть несложное упражнение на проверку свойств подкольца.
Из формул Виета следует, что коэффициенты многочлена $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ могут быть выражены как симметрические функции его n корней $x_1, \ldots, x_n$.

Оказывается, что симметрические многочлены, участвующие в образовании формул Виета играют замечательную роль в теории алгебраических многочленов. Выпишем их

$$\begin{aligned}
\sigma_1 &= \sigma_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n, \\
\sigma_2 &= \sigma_2(x_1, \ldots, x_n) = x_1x_2 + \ldots + x_1x_n + \ldots + x_{n-1}x_n, \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\sigma_n &= \sigma_n(x_1, \ldots, x_n) = x_1x_2 \ldots x_n.
\end{aligned}$$

Многочлены $\sigma_1, \ldots, \sigma_n$ называются **элементарными симметрическими многочленами**.

Теорема (основная). *Для всякого симметрического многочлена $f(x_1, \ldots, x_n) \in \mathbf{P}[x_1, \ldots, x_n]$ найдется многочлен $\varphi(y_1, \ldots, y_n)$ с коэффициентами из $\mathbf{P}$, такой, что тождественно по $x_1, \ldots, x_n$*

$$f(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n).$$

Доказательство. Рассмотрим высший член $ax_1^{k_1} \ldots x_n^{k_n}$ многочлена $f(x_1, \ldots, x_n)$. Его цена $(k_1, \ldots, k_n)$ обладает свойством $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$.
Действительно, если бы, например, $k_{i+1} > k_i$ для некоторого i, то подстановка, задаваемая транспозицией $x_i \rightleftarrows x_{i+1}$ привела бы к члену, содержащемуся в $f(x_1, \ldots, x_n)$ с ненулевым коэффициентом, но цена этого члена была бы выше цены высшего члена, что невозможно.
Обозначим теперь через

$$\varphi_1(\sigma_1, \ldots, \sigma_n) = \varphi_1 = a\sigma_1^{k_1-k_2} \ldots \sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}.$$

Ясно, что φ_1 — симметрический многочлен, а его высший член (как произведение высших членов элементарных симметрических функций) равен

$$ax_1^{k_1-k_2}(x_1x_2)^{k_2-k_3} \ldots (x_1 \ldots x_{n-1})^{k_{n-1}-k_n}(x_1 \ldots x_n)^{k_n} = ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}.$$

Но тогда разность $f - \varphi_1$, являясь симметрическим многочленом, имеет высший член, цена которого ниже $(k_1 \dots k_n)$.
С многочленом $f_1 = f - \varphi_1$ поступаем аналогично предыдущему. Тогда получим последовательность симметрических многочленов $f, f_1, f_2, \dots, f_s, \dots$, обладающих тем свойством, что высший член предыдущего члена многочлена этой последовательности выше высших членов каждого из последующих многочленов последовательности.

Если учесть, что для цены $(l_1, \dots, l_n)$ любого члена последовательности справедливы неравенства $l_1 \geqslant l_2 \geqslant \dots \geqslant l_n \geqslant 0$, то получим, что существует только конечное число цен $(l_1, \dots, l_n)$, низших чем цена $(k_1, \dots, k_n)$, а значит, рассматриваемая последовательность $f, f_1, f_2, \dots, f_s, \dots$ конечна, то есть наступит такой момент, что $f_r(x_1, \dots, x_n) = 0$.

Итак, мы имеем

$$\begin{cases} f_1 = f - \varphi_1, \\ f_2 = f_1 - \varphi_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_r = f_{r-1} - \varphi_r = 0. \end{cases} \tag{5.8}$$

Откуда, $f = \varphi_1 + \varphi_2 + \dots + \varphi_r$.
Но каждое φ_i есть одночлен вида

$$\varphi_i = a_i \sigma_1^{k_1^{(i)} - k_2^{(i)}} \dots \sigma_n^{k_n^{(i)}}.$$

А потому сумма $\varphi = \varphi_1 + \varphi_2 + \dots + \varphi_r$ — есть искомый многочлен. □

Теорема (единственности). *Многочлен $\varphi(\sigma_1, \dots, \sigma_n)$ из предыдущей теоремы определяется однозначно, то есть представление симметрического многочлена через элементарные симметрические многочлены — единственно.*

Доказательство. Предположим, что для некоторого многочлена $f(x_1, \dots, x_n)$ имеются два представления

$$f(x_1, \dots, x_n) = \varphi_1(\sigma_1, \dots, \sigma_n),$$
$$f(x_1, \dots, x_n) = \varphi_2(\sigma_1, \dots, \sigma_n).$$

Но тогда разность $\varphi_1 - \varphi_2$ представляет нулевой многочлен. И наше утверждение будет доказано, если мы покажем, что ненулевой многочлен $\varphi(\sigma_1, \dots, \sigma_n)$ обязательно представляет ненулевой многочлен от $x_1, \dots, x_n$.
Если $a\sigma_1^{l_1} \dots \sigma_n^{l_n}$ — какой-либо член многочлена $\varphi(\sigma_1, \dots, \sigma_n)$, то ему соответствует высший член

$$a x_1^{k_1} \dots x_n^{k_n},$$

где

$$\begin{cases} k_1 = l_1 + l_2 + \ldots + l_n, \\ k_2 = \quad l_2 + \ldots + l_n, \\ \ldots \quad \ldots \\ k_n = \quad l_n. \end{cases} \tag{5.9}$$

Из этих равенств видно, что двум различным членам $a\sigma_1^{l_1'} \ldots \sigma_n^{l_n'}$ и $b\sigma_1^{l_1''} \ldots \sigma_n^{l_n''}$ соответствуют различные высшие члены:

$$ax_1^{k_1'} \ldots x_n^{k_n'} \qquad \text{и} \qquad bx_1^{k_1''} \ldots x_n^{k_n''}$$

(ибо если i наивысший индекс из $1, 2, \ldots, n$, для которого $l_i' \neq l_i''$, то обязательно $k_n' = k_n'', \ldots, k_{i+1}' = k_{i+1}''$, но $k_i' \neq k_i''$).

Но тогда мы получаем, что наивысший член среди высших членов ненулевых членов многочлена $\varphi(\sigma_1, \ldots, \sigma_n)$ будет единственным, а потому будет иметь ненулевой коэффициент. □

Из доказательства основной теоремы о симметрических многочленах следует, что если коэффициенты симметрического многочлена $f(x_1, \ldots, x_n)$ принадлежат некоторому кольцу $\mathbf{K}$ поля $\mathbf{P}$, то и коэффициенты соответствующего многочлена $\varphi(\sigma_1, \ldots, \sigma_n)$ принадлежат этому же кольцу $\mathbf{K}$. Например, если $\mathbf{P} = \mathbb{R}$ и коэффициенты $f(x_1, \ldots, x_n)$ — целые числа из $\mathbb{Z}$, то такими же будут и коэффициенты $\varphi(\sigma_1, \ldots, \sigma_n)$.

В некоторых прикладных вопросах алгебры встречаются симметрические многочлены

$$s_i = x_1^i + \ldots + x_n^i, \qquad i = 1, 2, \ldots$$

Эти многочлены часто называют **степенными суммами**. Установим связь между степенными суммами и элементарными симметрическими многочленами. Ясно, что $s_1 = \sigma_1$. Далее, при $k \leqslant n$ и $1 \leqslant i \leqslant k-2$ имеем

$$\begin{aligned} s_{k-i}\sigma_i = \left(x_1^{k-i} + \ldots + x_n^{k-i}\right)\left(x_1 \ldots x_i + x_1 \ldots x_{i-1}x_{i+1} + \ldots + x_{n-i+1} \ldots x_n\right) = \\ = \left(x_1^{k+1-i}x_2 \ldots x_i + x_1^{k+1-i}x_3 \ldots x_{i+1} + \ldots + x_1 \ldots x_{i-1}x_i^{k+1-i} + \ldots + \right. \\ \left. + x_{n+1-i} \ldots x_n^{k+1-i}\right) + \left(x_1^{k-i}x_2 \ldots x_i x_{i+1} + \ldots + x_{n-i}x_{n-i+1} \ldots x_n^{k-i}\right) = \\ = S(x_1^{k+1-i}x_2 \ldots x_i) + S(x_1^{k-i}x_2 \ldots x_i x_{i+1}). \end{aligned} \tag{5.10}$$

Здесь $S(x_1^{k+1-i}x_2 \ldots x_i)$ и $S(x_1^{k-i}x_2 \ldots x_i x_{i+1})$ — моногенные многочлены. Кроме того,

$$\begin{aligned} s_1\sigma_{k-1} = (x_1 + \ldots + x_n)\left(x_1 \ldots x_{k-1} + \ldots + x_{n-k+2} \ldots x_n\right) = \\ = S(x_1^2 x_2 \ldots x_{k-1}) + k\sigma_k. \end{aligned} \tag{5.11}$$

Если равенства (5.10) умножить на $(-1)^i$, $i = 1, \ldots, k-2$, а соотношение (5.11) на $(-1)^k$, и сложить, то получим

$$-s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \ldots + (-1)^{k-1}s_1\sigma_{k-1} = -S(x_1^k) + (-1)^{k-1}k\sigma_n,$$

а потому при $k \leqslant n$:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \ldots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_n = 0, \qquad (k \leqslant n). \quad (5.12)$$

При $k > n$ равенства (5.10) сохраняются для всех $i = 1, \ldots, n-1$ а вместо (5.11) имеем

$$s_{k-n}\sigma_n = S(x_1^{k-n+1}x_2 \ldots x_n).$$

Поэтому

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \ldots + (-1)^n s_{k-n}\sigma_n = 0, \qquad (k > n). \quad (5.13)$$

Из формулы (5.12) следует, что элементарные симметрические функции $\sigma_1, \ldots, \sigma_n$ выражаются в виде многочленов от степенных сумм $s_1, \ldots, s_k$ с коэффициентами из поля $\mathbf{P}$, если только $\mathbf{P}$ имеет характеристику нуль.(Почему?)

5.5 Основная теорема алгебры

Определение. *Поле* $\mathbf{P}$ *называется* ***алгебраически замкнутым****, если любой многочлен* $f(x) \in \mathbf{P}[x]$ *имеет в* $\mathbf{P}$ *все свои корни.*

Существуют ли такие поля? Основная цель настоящего параграфа состоит в том, чтобы показать, что поле комплексных чисел $\mathbb{C}$ является алгебраически замкнутым. Но для этого мы подробнее изучим многочлены с вещественными коэффициентами.

Лемма 5.5.1. *Пусть* $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{R}[x]$ *— многочлен нечетной степени* n*. Тогда* $f(x)$ *имеет хотя бы один вещественный корень.*

Доказательство. Поскольку $a_k \in \mathbb{R}$, то $f(x)$ является непрерывной функцией на всей вещественной прямой как конечная сумма непрерывных функций вида $a_k x^k$. Кроме того,

$$f(x) = x^n \left(a_n + \frac{a_{n-1}}{x^n} + \ldots + \frac{a_0}{x^n}\right).$$

Выражение в скобках в последнем равенстве при $x \longrightarrow \infty$ стремится к $a_n \neq 0$. А потому найдется такое $N > 0$, что при $|x| > N$ значение в скобках будет

заключено между $\frac{1}{2}a_n$ и $\frac{3}{2}a_n$, то есть при $x = -N$ и $x = N$ значение в скобках сохраняет знак a_n. Поэтому (в силу нечетности n)

$$sign\, f(-N) = -sign\, a_n,$$
$$sign\, f(N) = sign\, a_n,$$

то есть на концах промежутка $[-N, N]$ непрерывная функция $f(x)$ принимает значения разных знаков, а потому внутри промежутка найдется точка, где $f(x)$ обращается в 0. □

Лемма 5.5.2. *Всякий многочлен $f(x)$ с вещественными коэффициентами имеет хотя бы один комплексный корень.*

Доказательство. Пусть $grad\, f(x) = n$. Представим n в виде $n = 2^m n_1$, n_1 — нечетное. Утверждение теоремы при $m = 0$ доказано в лемме 5.5.1. Поэтому естественно провести доказательство леммы при $m \geqslant 1$ методом индукции.
Итак, считаем утверждение леммы верным, для всех многочленов из $\mathbb{R}[x]$, степени которых $n' = 2^{m'} n_1'$, где $(n_1', 2) = 1$ и $m' < m$.
Многочлен $f(x)$ рассматриваем как многочлен из $\mathbb{C}[x]$. Тогда, согласно теореме Кронекера в некотором расширении $\mathbf{L}$ поля $\mathbb{C}$ многочлен имеет все свои корни. Выпишем эти корни

$$x_1, x_2, \ldots, x_n \qquad (\text{не все} \quad x_i \quad \text{обязательно различны}).$$

Для каждого вещественного $a \in \mathbb{R}$ полагаем

$$u_{i,j} = u_{i,j}(a) = x_i + x_j + a x_i x_j, \qquad u_{i,j}(a) \in \mathbf{L}.$$

Рассмотрим многочлен

$$F(x) = \prod_{1 \leqslant i < j \leqslant n} (x - u_{i,j}).$$

Степень этого многочлена равна

$$\sum_{j=2}^{n} (j-1) = \sum_{k=1}^{n-1} k = \frac{(n-1)n}{2} = 2^{m-1} n_2, \qquad n_2 - \text{нечетное}.$$

Коэффициенты $F(x)$ являются симметрическими многочленами его корней $u_{i,j}$, $1 \leqslant i < j \leqslant n$ (формулы Виета). Но всякий симметрический многочлен от чисел $u_{i,j}$ является симметрическим многочленом и от корней $x_1, x_2, \ldots, x_n$. Чтобы в этом убедиться, достаточно проверить неизменяемость такого многочлена лишь для произвольной транспозиции (ибо каждая подстановка равна произведению транспозиций). Но если (i, j) — данная транспозиция, то она

переводит элементы x_i в x_j и наоборот и не трогает других корней многочлена $f(x)$. И тогда $u_{i,k} \longrightarrow u_{j,k}$, а $u_{j,k} \longrightarrow u_{i,k}$, а остальные элементы u останутся на месте, но в силу симметричности коэффициентов многочлена $F(x)$ от элементов $u_{i,j}$, получаем что $F(x)$ не изменяется при подстановках корней x_1, x_2, $\ldots$, x_n, то есть коэффициенты $F(x)$ — симметрические многочлены элементов x_1, x_2, $\ldots$, x_n, а потому — выражаются как многочлены (с целыми рациональными коэффициентами) от коэффициентов многочлена $f(x)$ и числа a, и значит являются действительными числами.

Итак, $F(x)$ — многочлен степени $2^{m-1}n_2$ с действительными коэффициентами, и, в силу предположения индукции, имеет комплексный корень. То есть, для некоторой пары (i,j) число

$$u_{i,j}(a) = x_i + x_j + ax_ix_j = \alpha, \quad - \quad \text{комплексное.}$$

Заставляя a пробегать множество вещественных чисел, мы каждый раз будем получать хотя бы одно соответствующее комплексное число $u_{i,j}$, то есть для выбранного значения a' найдется пара (i',j') так, что $u_{i',j'}(a') = x_{i'}+x_{j'}+a'x_{i'}x_{j'}$ — комплексное.

Но пар (i,j) — конечное число, а вещественных числе бесконечно много, и значит найдутся два вещественных числа a и b, которым будет соответствовать одна и та же пара (i,j).

Иначе говоря

$$\begin{aligned} x_i + x_j + ax_ix_j &= \alpha, \\ x_i + x_j + bx_ix_j &= \beta, \end{aligned}$$

где $\alpha, \beta \in \mathbb{C}$.

Из последних равенств имеем:

$$\begin{aligned} x_ix_j &= \frac{\alpha - \beta}{a - b} = q, \\ x_i + x_j &= \alpha - aq = -p, \end{aligned}$$

p и q — комплексные числа.

Рассмотрим уравнение (с комплексными коэффициентами)

$$z^2 + pz + q = 0 \tag{5.14}$$

или

$$\left(z + \frac{p}{2}\right)^2 + \left(q - \frac{p^2}{4}\right) = 0.$$

Отсюда

$$z = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q},$$

но $\sqrt{\frac{p^2}{4}-q}$ — комплексное число (как квадратный корень из комплексного числа).

Но в силу теоремы Виета числа x_i и x_j — корни уравнения (5.14), а потому (как только что было доказано) являются комплексными числами. Таким образом, мы нашли комплексный корень (даже два) для многочлена $f(x)$. $\square$

Теорема (**основная теорема алгебры**). *Всякий многочлен с комплексными коэффициентами степени* $\geqslant 1$ *имеет комплексный корень.*

Доказательство. Пусть $f(x) = a_n x^n + \ldots + a_0$, где $a_k \in \mathbb{C}$. Обозначим

$$\bar{f}(x) = \bar{a}_n x^n + \ldots + \bar{a}_0,$$

здесь черта означает взятие комплексного сопряжения. Ясно, что $\bar{f}(x) \in \mathbb{C}[x]$.

Покажем, что

$$f(x) \cdot \bar{f}(x) \in \mathbb{R}[x].$$

В самом деле, пусть

$$f(x) \cdot \bar{f}(x) = b_{2n} x^{2n} + \ldots + b_0,$$

тогда

$$\begin{aligned} b_k &= a_k\bar{a}_0 + a_{k-1}\bar{a}_1 + \ldots + \bar{a}_0\bar{a}_k, && k = 0, 1, \ldots, n; \\ b_n &= a_{k-n}\bar{a}_n + a_{k-n+1}\bar{a}_{n-1} + \ldots + a_n\bar{a}_{k-n}, && n < k \leqslant 2n. \end{aligned}$$

В обоих случаях, $b_n = \bar{b}_k$, а значит, $f(x) \cdot \bar{f}(x) \in \mathbb{R}[x]$.

По лемме 5.5.2 найдется комплексное α, такое что

$$f(\alpha) \cdot \bar{f}(\alpha) = 0.$$

Если $f(\alpha) = 0$, то α — корень $f(x)$ и теорема доказана.
Поэтому, пусть $\bar{f}(\alpha) = 0$, то есть

$$\bar{a}_n\alpha^n + \ldots + \bar{a}_0 = 0.$$

Но тогда

$$\overline{\bar{f}(\alpha)} = \overline{\bar{a}_n\alpha^n + \ldots + \bar{a}_0} = a_n(\bar{\alpha})^n + \ldots + a_0 = 0.$$

Отсюда следует, что $\bar{\alpha}$ — корень $f(x)$. $\square$

Следствие 1. *Поле комплексных чисел* $\mathbb{C}$ *алгебраически замкнуто.*

В самом деле, если $f(x) \in \mathbb{C}[x]$, то найдется в $\mathbb{C}$ корень α, так что по теореме Безу $f(x) = (x-\alpha)f_1(x)$. Но $f_1(x) \in \mathbb{C}[x]$ и степень $f_1(x)$ на 1 меньше степени $f(x)$. Продолжая этот процесс далее, мы через n шагов ($n = grad\, f(x)$) прийдем к разложению

$$f(x) = (x-\alpha_1)\dots(x-\alpha_n)f_n(x),$$

где $grad\, f_n(x) = 0$, а потому $f_n(x) = a_n$ — старший коэффициент $f(x)$. Из полученного разложения следует утверждение следствия.

Следствие 2. *Неприводимыми многочленами в кольце $\mathbb{C}[x]$ являются многочлены первой степени $x-\alpha$, $\alpha \in \mathbb{C}$, и только они.*

Рассмотренные утверждения справедливы для каждого многочлена из $\mathbb{C}[x]$, а значит и для многочленов из $\mathbb{R}[x]$, но эти утверждения не могут быть сужены до поля $\mathbb{R}$ для кольца $\mathbb{R}[x]$. В частности, над полем $\mathbb{R}$ существует бесконечно много многочленов, не имеющих в $\mathbb{R}$ корней. (Например, многочлен вида $x^{2n}+1$). Сложнее структура и неприводимых многочленов над $\mathbb{R}$. Поэтому подробнее изучим кольцо $\mathbb{R}[x]$.

Пусть $f(x) \in \mathbb{R}[x]$, $grad\, f(x) \geqslant 1$. Тогда по основной теореме алгебры $f(x)$ имеет в $\mathbb{C}$ все свои корни. Пусть α — один из корней $f(x)$. Если $\alpha = \bar{\alpha}$, то есть α — вещественное, то заключаем, что $\bar{\alpha}$ корень $f(x)$. Но это тавтология. Однако, это утверждение не становится тривиальным, если α — комплексное. Итак, покажем, что если $\alpha \notin \mathbb{R}$, — корень $f(x)$, то и $\bar{\alpha}$ — корень $f(x)$. Мы имеем

$$a_n\alpha^n + \dots + a_0 = 0.$$

Или беря от обеих частей этого числового равенства комплексно сопряженные, получим

$$a_n\bar{\alpha}^n + \dots + a_0 = 0,$$

то есть $f(\bar{\alpha}) = 0$.

Определение. *Пусть $f(x) = a_nx^n+\dots+a_0 \in \mathbf{P}[x]$ и $f(x) = a_n(x-\alpha_1)\dots(x-\alpha_n)$ — разложение $f(x)$ на линейные множители в поле разложения этого многочлена. Корень α многочлена $f(x)$ называется k-* ***кратным****, если в указанном разложении множитель $(x-\alpha)$ встречается k раз.*

Корень α называется ***простым****, если его кратность k равна 1. При $k > 1$ корень α называется* ***кратным****.*

Пусть комплексное α является корнем $f(x)$ кратности k, мы показали, что и $\bar{\alpha}$ — корень $f(x)$, обозначим его кратность через l, $l \geqslant 1$. Мы покажем, что $k = l$. Пусть для определенности $k > l$ (если $k < l$, то мы обозначаем $\bar{\alpha} = \beta$, и тогда $\bar{\beta} = \bar{\bar{\alpha}} = \alpha$, и проводим рассуждения относительно β). Имеем

$$f(x) = (x-\alpha)^k(x-\bar{\alpha})^l\psi(x), \qquad \psi(x) \in \mathbb{C}[x],$$

причем $\psi(\alpha) \neq 0$, $\psi(\bar{\alpha}) \neq 0$.

Поскольку $(x-\alpha)\cdot(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$ — многочлен с вещественными коэффициентами, то получаем, что

$$f_1(x) = \frac{f_1(x)}{((x-\alpha)(x-\bar{\alpha}))^l} = (x-\alpha)^{k-l}\psi(x)$$

— многочлен с вещественными коэффициентами, который имеет комплексное число α своим корнем, но $\bar{\alpha}$ не является его корнем. А это невозможно. Итак, обязательно $k = l$ и нами доказана

Лемма 5.5.3. *Многочлен $f(x) \in \mathbb{R}[x]$ с каждым комплексным корнем α кратности k имеет своим корнем и $\bar{\alpha}$ той же кратности k.*

Следующая теорема характеризует многочлены из $\mathbb{R}[x]$:

Теорема (неприводимые многочлены над $\mathbb{R}$). *Неприводимыми многочленами кольца $\mathbb{R}[x]$ являются многочлены вида*

$$\begin{aligned} x-a, &\qquad a \in \mathbb{R}, \\ x^2+ax+b, &\qquad a,b \in \mathbb{R},\ a^2-4b<0, \end{aligned}$$

и только они.

Доказательство. В силу следствия 2 нам необходимо рассмотреть только многочлены x^2+ax+b, $a,b \in \mathbb{R}$, $a^2-4b<0$. Эти многочлены неприводимы над $\mathbb{R}$, ибо иначе они разлагались бы на линейные множители, а потому имели бы в $\mathbb{R}$ корни (но это не так). Если же в квадратном трехчлене x^2+ax+b, $a,b \in \mathbb{R}$ выполняется соотношение $a^2-4b \geqslant 0$, то этот многочлен имеет вещественные корни, а потому приводим. Наконец, если $f(x) \in \mathbb{R}[x]$ имеет степень > 2, то либо $f(x)$ имеет вещественный корень α, а потому делится на $x-\alpha$, либо α — комплексное, а тогда $f(x)$ делится на $(x-\alpha)\cdot(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$, то есть $f(x)$ снова приводим над $\mathbb{R}$. □

5.6 Вычисление корней многочлена

Основная теорема алгебры устанавливает место, где лежат корни многочлена $f(x)$ — поле $\mathbb{C}$. Но как их там обнаружить?

Этот вопрос интересовал математиков во все времена. По теореме Виета коэффициенты многочлена выражаются через корни уравнения, естественно, что имеет место и обратная связь. Но как ее выразить. Наиболее простые способы выражения математической связи — это использование операций сложения,

вычитания, умножения, деления, возведение в натуральную степень и извлечение натурального корня.
И действительно, корни квадратного многочлена

$$f(x) = x^2 + ax + b$$

выражаются через коэффициенты многочлена так

$$x_1 = -\frac{a}{2} + \sqrt{\frac{a^2}{4} - b},$$
$$x_2 = -\frac{a}{2} - \sqrt{\frac{a^2}{4} - b}.$$

Из этих формул, кстати, видно, что лишь при $\frac{a^2}{4} - b = 0$ многочлен имеет равные корни.
Долгое время не удавалось найти подходящие формулы для определения корней многочлена $3^{\text{ей}}$ степени

$$f(x) = x^3 + ax^2 + bx + c.$$

Завершение усилий в этом направлении связывают с именем итальянского математика Дж. Кардано (1501-1576). Вот вывод его формул.
В уравнении

$$x^3 + ax^2 + bx + c = 0 \tag{5.15}$$

сделаем замену неизвестного $x = y - \frac{a}{3}$, тогда мы прийдем к уравнению вида

$$y^3 + py + q = 0, \tag{5.16}$$

где $p = -\frac{a^2}{3} + b, \quad q = -\frac{2a^3}{27} - \frac{ab}{3} + c$. По основной теореме алгебры уравнение (5.16) имеет решение — корни многолена $y^3 + py + q$. Пусть y_0 один из них. Положим $y_0 = \alpha + \beta$, где комплексные числа α и β нам пока неизвестны. Подставляя $y_0 = \alpha + \beta$ в уравнение (5.16) получим

$$\alpha^3 + \beta^3 + (\alpha + \beta)(3\alpha\beta + p) + q = 0. \tag{5.17}$$

Будем теперь находить α и β из условий

$$\begin{cases} \alpha \cdot \beta = -\frac{p}{3}, \\ \alpha + \beta = y_0. \end{cases} \tag{5.18}$$

Из теоремы Виета (школьный курс) следует, что α и β являются корнями уравнения (относительно z)

$$z^2 - y_0 z - \frac{p}{3} = 0.$$

Если α и β уже выбраны именно таким образом, то соотношение (5.17) приводится к виду

$$\alpha^3 + \beta^3 + q = 0. \tag{5.19}$$

Используя первое в (5.18) и соотношение (5.19), имеем:

$$\begin{cases} \alpha^3 + \beta^3 = -q, \\ \alpha^3 \cdot \beta^3 = -\dfrac{p^3}{27}. \end{cases}$$

Откуда по теореме Виета α^3 и β^3 совпадают с корнями уравнения

$$z^2 + qz - \frac{p^3}{27} = 0.$$

Таким образом,

$$\alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad \beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

где под $\sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}$ в выражениях для $\alpha^3 + \beta^3$ понимается одно и тоже значение квадратного корня.

Теперь имеем

$$y_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{5.20}$$

Здесь каждый кубический корень имеет 3 значения, поэтому, вообще говоря, мы получаем 6 значений y_0, но не все являются допустимыми, так как эти кубические корни, являясь значениями для α и β подчинены дополнительному условию

$$\alpha\beta = -\frac{p}{3}.$$

Это условие выделяет только три значения для y_0, которые являются значениями корней многочлена $y^3 + py + q$.

Полученная формула (5.20) носит название **формулы Кардано**.

Уравнение $4^{\text{ой}}$ степени

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

заменой $x = y - \dfrac{a}{4}$ приводится к виду

$$y^4 + py^2 + qy^2 + r = 0.$$

Итальянский математик Л. Феррари (1522-1565) построил метод решения такого уравнения, в основе которого лежит использование формул Кардано. Суть этого метода состоит в том, что с помощью вспомогательного уравнения $3^{\text{ей}}$ степени уравнение $4^{\text{ой}}$ степени сводится к решению двух уравнений $2^{\text{ой}}$ степени. Такую же цепь рассуждений можно проследить и при выводе формул Кардано. Мы не будем проводить здесь эти выкладки, ввиду их громоздкости (и малой практической полезности). Индуктивно напрашивается предложение: свести уравнение $5^{\text{ой}}$ степени к решению уравнений низших степеней и т.д. То есть, возникает предположение, что для многочленов любой степени существуют формулы (возможно громоздкие), позволяющие с помощью операций сложения, вычитания, умножения, деления, возведение в натуральную степень и извлечение натурального корня, определить по коэффициентам многочлена все его корни. Увы, это не так.

В 1824 году норвежский математик Н. Абель (1802-1829) доказал следующую теорему.

Теорема (**Абеля**). *Общее уравнение с одним неизвестным степени выше $4^{ой}$ неразрешимо в радикалах, то есть не существует формулы, выражающей корни общего уравнения степени выше $4^{ой}$ через коэффициенты этого уравнения с помощью операций сложения, умножения, вычитания, деления, возведение в натуральную степень и извлечение натуральной степени.*

Окончательную точку в этом вопросе поставил французский математик Э. Галуа (1811-1832).

Он показал, что даже не для всякого конкретного уравнения степени выше $4^{\text{ой}}$ (то есть с числовыми коэффициентами) существует представление корней через радикалы. Так, для уравнения

$$x^5 + 5x - 15 = 0$$

не существует выражение корней уравнения через радикалы.

Но доказательства теоремы Абеля и результатов Галуа требуют большой информации по теории групп и полей, а потому в нашем курсе проведены не будут.

В настоящее время создано достаточно большое число методов приближенного вычисления корней многочлена. Некоторые из них будут изучаться позднее в курсах «Вычислительные методы алгебры» и «Приближенные вычисления».

Завершаем мы эту главу следующим параграфом.

5.7 Результант. Дискриминант

Пусть $f(x) = a_n x^n + \ldots + a_0 \in \mathbf{P}[x]$.

Определение. *Многочлен* $f'(x) = na_n x^{n-1} + \ldots + a_1$ *называется* ***производной многочлена*** $f(x)$.

Из определения непосредственно следуют свойства:

1. $(f(x) \pm g(x))' = f'(x) \pm g'(x)$
2. $(f(x) \cdot g(x))' = f'(x)g(x) + f(x)g'(x)$

Теорема 5.7.1. *Корень* α *многочлена* $f(x) \in \mathbf{P}[x]$ *будет* k*- кратным корнем этого многочлена только тогда, когда* α *— корень кратности не менее* $(k-1)$ *для производной* $f'(x)$.

Доказательство. Пусть α — корень кратности k для многочлена $f(x)$. Тогда

$$f(x) = (x-\alpha)^k f_1(x), \qquad f_1(\alpha) \neq 0.$$

Поэтому

$$f'(x) = k(x-\alpha)^{k-1} f_1(x) + (x-\alpha)^k f_1'(x) = (x-\alpha)^{k-1}\left(kf_1(x) + (x-\alpha)f_1'(x)\right)$$

и значит, α корень, по крайней мере, кратности $(k-1)$ для производной $f'(x)$. □

Замечание. Если поле $\mathbf{P}$ — есть поле нулевой характеристики, то при $x = \alpha$ сумма $kf_1(x) + (x-\alpha)f_1'(x)$ в нуль не обращается, а потому для $f'(x)$ элемент α является корнем в точности кратности $(k-1)$. Так что в этом случае утверждение теоремы обратимо.

Следствие 1 (**отделение кратных корней**). *Пусть* $\mathbf{P}$ *— поле нулевой характеристики, тогда для многочлена* $f(x) \in \mathbf{P}[x]$ *элемент* α *является корнем кратности* $k \iff$ *когда* $f(\alpha) = 0$ *и* α *— корень кратности* $(k-1)$ *для производной* $f'(x)$.

Поэтому , если $d(x)$ — ОНД$(f(x), f'(x))$, то каждый корень α многочлена $f(x)$ является корнем $d(x)$, но кратности на 1 меньше, и других корней многочлен $d(x)$ не имеет. Кроме того, $d(x) \in \mathbf{P}[x]$, как это следует из алгоритма Евклида построения ОНД двух многочленов. Но тогда многочлен $f_1(x) = \dfrac{f(x)}{d(x)} \in \mathbf{P}[x]$ и его корнями являются все различные корни $f(x)$, но с кратностью 1.

Описанная процедура назыается **отделением кратных корней**.

Следствие 2. *Многочлен $f(x) \in \mathbf{P}[x]$, где $\mathbf{P}$ — поле характеристики 0, имеет кратные корни $\Longleftrightarrow$ когда ОНД$(f(x), f'(x))$ отличен от const.*

Действительно, каждый корень $d(x)$ =ОНД$(f(x), f'(x))$ является общим корнем $f(x)$ и $f'(x)$ и значит является корнем $f(x)$, по крайней мере, второй кратности.

Замечание. Если поле $\mathbf{P}$ — поле характеристики $p \neq 0$, то это утверждение уже ошибочно. Например, многочлен $f(x) = x^{2p} - x^p - 2$ имеет производную, равную нулю. Так что ОНД$(f(x), f'(x)) \neq const$, но в силу $f(x) = (x^p - 2)(x^p + 1)$ видно, что все корни $f(x)$ — простые.

Предыдущее следствие показывает, что вопрос о существовании кратных корней многочлена $f(x)$ сводится к вопросу о существовании общих корней двух многочленов $f(x)$ и $f'(x)$.

Решим этот вопрос в общем случае. Итак, даны два многочлена $f(x)$ и $g(x)$ из $\mathbf{P}$. Как узнать имеют ли они общие корни.

Пусть

$$f(x) = a_n x^n + \ldots + a_0$$

и $x_1, \ldots, x_n$ — корни $f(x)$.
Аналогично,

$$g(x) = b_m x^m + \ldots + b_0$$

и $y_1, \ldots, y_m$ — корни $g(x)$.
Рассмотрим произведение

$$\Pi = \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

Очевидно, многочлены $f(x)$ и $g(x)$ имеют общие корни $\Longleftrightarrow$ когда $\Pi = 0$.

Вместо величины Π более удобно рассматривать величину

$$S = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j). \tag{5.21}$$

Так что $f(x)$ и $g(x)$ имеют общие корни $\Longleftrightarrow$ когда $S = 0$.

Из разложений

$$f(x) = a_n(x - x_1) \ldots (x - x_n) = a_n \prod_{i=1}^{n} (x - x_i),$$

$$g(x) = b_m(x - y_1) \ldots (x - y_m) = b_m \prod_{j=1}^{m} (x - y_j),$$

получаем

$$S = a_n^m \prod_{i=1}^{n} g(x_i) == (-1)^{mn} b_m^n \prod_{j=1}^{m} f(y_j). \tag{5.22}$$

Откуда видно, что для ответа на вопрос имеют ли многочлены $f(x)$ и $g(x)$ общие корни достаточно знать корни хотя бы одного из этих многочленов. Но и это слишком большая роскошь.

Рассмотрение выражения (5.21) для S показывает, что S при фиксированных $y_1, \ldots, y_m$ является симметрической функцией от $x_1, \ldots, x_n$.

Аналогично, при фиксированных $x_1, \ldots, x_n$ величина S является симметрической функцией от $y_1, \ldots, y_m$. Так что можно ожидать, что S может быть выражена через элементарные симметрические функции соответственно от $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$. Но мы имеем:

$$\begin{aligned}
\sigma_1(x_1, \ldots, x_n) &= -\frac{a_{n-1}}{a_n}, \\
\sigma_2(x_1, \ldots, x_n) &= \frac{a_{n-2}}{a_n}, \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\sigma_k(x_1, \ldots, x_n) &= (-1)^k \cdot \frac{a_{n-k}}{a_n}, \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\sigma_n(x_1, \ldots, x_n) &= (-1)^n \cdot \frac{a_0}{a_n}.
\end{aligned}$$

И аналогично,

$$\sigma_k(y_1, \ldots, y_m) = (-1)^k \cdot \frac{b_{m-k}}{b_m}, \qquad k = 1, \ldots, m.$$

Таким образом, можно ожидать, что существует некоторое выражение для S в виде многочлена с коэффициентами из $\mathbf{P}$ от переменных $a_0, \ldots, a_n, b_0, \ldots, b_m$.

Чтобы найти это выражение, рассмотрим ряд вспомогательных утверждений.

Лемма 5.7.1. *Два многочлена $f(x)$ и $g(x)$ имеют общий делитель, отличный от const $\iff$ когда существуют ненулевые многочлены $u(x)$ и $v(x)$, удовлетворяющие условиям:*

$$\begin{gathered}
f(x)u(x) + g(x)v(x) = 0, \\
grad\, u(x) < grad\, g(x), \qquad grad\, v(x) < grad\, f(x).
\end{gathered} \tag{5.23}$$

Доказательство. Пусть $\varphi(x) \neq const$ — общий делитель $f(x)$ и $g(x)$.

$$\begin{aligned}
f(x) &= \varphi(x) f_1(x), & grad\, f_1(x) &< grad\, f(x), \\
g(x) &= \varphi(x) g_1(x), & grad\, g_1(x) &< grad\, g(x).
\end{aligned}$$

Положив $u(x) = g_1(x),\ v(x) = -f_1(x)$, получим соотношение (5.23). И наоборот, если соотношение (5.23) имеет место, то

$$f(x)u(x) = -g(x)v(x).$$

Пусть $x_1, \ldots, x_n$ — корни многочлена $f(x)$ (возможно с повторениями). Поскольку $grad\, v(x) < grad\, f(x) = n$, то не все $x_1, \ldots, x_n$ с учетом кратности являются корнями $v(x)$. Это значит, что $f(x)$ и $g(x)$ имеют хотя бы один общий корень (который является и корнем их ОНД), а потому их ОНД$\neq const$. $\square$

Обозначим

$$u(x) = c_{m-1}x^{m-1} + \ldots + c_0,$$
$$v(x) = d_{n-1}x^{n-1} + \ldots + d_0$$

и выясним, каким условиям должны удовлетворять коэффициенты многочленов $f(x)$ и $g(x)$, чтобы существовали коэффициенты c_i, d_j так, что

$$f(x)u(x) + g(x)v(x) = 0$$

(то есть при каких условиях на коэффициенты $f(x)$ и $g(x)$ эти многочлены имеют общие корни).

Предыдущее равенство приводит к следующей системе равенств:

$$\begin{array}{c|l} x^{n+m-1} & a_nc_{m-1} + b_md_{n-1} = 0 \\ x^{n+m-2} & a_{n-1}c_{m-1} + a_nc_{m-2} + b_{m-1}d_{n-1} + b_md_{n-2} = 0 \\ \vdots & \qquad . \quad . \quad . \quad . \quad . \quad . \\ x^0 & a_0c_0 + b_0d_0 = 0 \end{array}$$

Полученную систему равенств рассматриваем как систему уравнений (линейных однородных) относительно неизвестных $c_{m-1}, \ldots, c_0, d_{n-1}, \ldots, d_0$. Мы имеем систему $n + m$ уравнений относительно $n + m$ неизвестных. По теореме Крамера эта система имеет ненулевое решение (а только такие решения нас интересуют) $\Longleftrightarrow$ когда определитель системы равен нулю. Обозначим этот определитель (точнее говоря, транспонированный определитель) через $\mathrm{R}(f, g)$. Имеем

$$\mathrm{R}(f,g) = \begin{vmatrix} a_n & a_{n-1} & \ldots & & a_0 & 0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & & a_1 & a_0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & & 0 & 0 & a_n & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_0 & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & & 0 & 0 & 0 & \ldots & b_0 \end{vmatrix}.$$

Таким образом, многочлены $f(x)$ и $g(x)$ имеют общие корни $\Longleftrightarrow$ когда $\mathrm{R}(f, g) = 0$.

Определение. *Определитель* $\mathrm{R}(f,g)$ *называется* ***результантом многочленов*** $f(x)$ *и* $g(x)$.

Из приведенных выше рассуждений следует, что

$$\mathrm{R}(f,g)=0 \qquad \Longleftrightarrow \qquad S=0.$$

На самом деле имеет место равенство $\mathrm{R}(f,g)=S$, но поскольку нас интересует только факт обращения в нуль результанта, то мы не будем тратить усилия на доказательство равенство $\mathrm{R}(f,g)=S$.

Пример 26. Пусть $f(x)=x^2-3x+2$, $g(x)=x^3-4x+3$.

$$\mathrm{R}(f,g)=\begin{vmatrix}1&-3&2&0&0\\0&1&-3&2&0\\0&0&1&-3&2\\1&0&-4&3&0\\0&1&0&-4&3\end{vmatrix}=\begin{vmatrix}1&0&0&0&0\\0&1&-3&2&0\\0&0&1&-3&2\\0&3&-6&3&0\\0&1&0&-4&3\end{vmatrix}=\begin{vmatrix}1&0&0&0\\0&1&-3&2\\0&3&-3&0\\0&3&-6&3\end{vmatrix}=0.$$

Теперь мы в состоянии ответить на вопрос о существовании кратных корней для многочлена $f(x)$. А именно:

Многочлен $f(x)$ имеет кратные корни $\Longleftrightarrow$ когда $\mathrm{R}(f,f')=0$.

Но

$$\mathrm{R}(f,f')=S=a_n^{n-1}\prod_{i=1}^{n}f'(x_i)$$

и если

$$f(x)=a_n\prod_{j=1}^{n}(x-x_j),$$

то

$$f'(x)=a_n\sum_{k=1}^{n}\prod_{\substack{j=1\\j\neq k}}^{n}(x-x_j).$$

Так что

$$f'(x_i)=a_n\prod_{\substack{j=1\\j\neq i}}^{n}(x_i-x_j).$$

А потому

$$\mathrm{R}(f,f')=a_n^{2n-1}\prod_{i=1}^{n}\prod_{\substack{j=1\\j\neq i}}^{n}(x_i-x_j)=(-1)^{\frac{n(n-1)}{2}}a_n^{2n-1}\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)^2.$$

(Мы учли, что в произведение

$$\prod_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (x_i - x_j)$$

входят два множителя $(x_i - x_j)$ и таких пар множителей ровно $\frac{1}{2}n(n-1)$).

Обозначим

$$D(f) = a_n^{2n-1} \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2$$

и назовем $D(f)$ **дискриминантом** многочлена $f(x)$.

Ясно, что $f(x)$ имеет кратные корни $\Longleftrightarrow$ когда $D(f) = 0$.

Замечание. Полученные нами результаты имеют место только в предположении, что поле $\mathbf{P}$ имеет характеристику 0.

Литература

[1] **Завало С.Т.** Алгебра и теория чисел, ч.1 / Завало С.Т., Костарчук В.Н., Хацет Б.И. – К.: Вища школа, 1980.

[2] **Кострикин А.И.** Введение в алгебру / Кострикин А.И. – М.: Наука, 1977.

[3] **Курош А.Г.** Курс высшей алгебры /Курош А.Г. – М.: Наука, 1975.