Р. А. Попков

АЛГЕБРА

§1. Алгебраические операции и алгебраические системы

...главная трудность для начинающего заключается в овладении разумным словарным запасом за короткое время. Ни одно из новых понятий само по себе не является трудным, но их последовательное накопление может иногда показаться тяжким.

Серж Ленг

Опр. 1.1. n***-арная*** (n***-местная***) ***алгебраическая операция*** — отображение $X_1 \times X_2 \times \ldots \times X_n \to Y$, где $X_1, X_2, \ldots, X_n, Y$ — непустые множества.

Опр. 1.2. Если $X_1 = X_2 = \ldots = X_n = Y$, то алгебраическая операция называется ***внутренней***.

$n = 0$ (нульарная): $\{\varnothing\} = X^0 \to X$ — выбор элемента в X.
$n = 1$ (унарная): $X = X^1 \to X$ — функция из X в X.
$n = 2$ (бинарная): $X^2 \to X$.
$n = 3$ (тернарная): $X^3 \to X$.

Замечание. В дальнейшем, если не оговорено иное, будем рассматривать внутренние бинарные операции, которые ещё называются ***внутренним законом композиции***.

Замечание. Обычно для записи бинарной операции используется ***инфиксная*** нотация, когда знак операции пишется ***между*** операндами: $x * y$, $x \circ y$, $x \circledcirc y$. Чаще всего мы будем использовать мультипликативную запись $(x \cdot y, xy)$ и называть операнды ***сомножителями***, а результат операции — ***произведением***. Аддитивную запись $(x+y)$ будем чаще всего использовать в контексте разговора об абелевых группах.

Опр. 1.3. ***Алгебраическая система*** $\mathscr{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$ — объект, являющийся совокупностью непустого множества A и непустого набора алгебраических операций, заданных на A. Множество A называется ***носителем*** алгебраической системы.

Опр. 1.4. Говорят, что множество $B \subseteq A$ ***замкнуто относительно операции*** $*$, если $\forall x, y \in B \; x * y \in B$.

Опр. 1.5. Система $\mathscr{B} = \langle B, f_1, f_2, \ldots, f_k, \ldots \rangle$ называется ***подсистемой*** системы $\mathscr{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$, если $B \subseteq A$ и B замкнуто относительно всех операций f_i.

Опр. 1.6. Алгебраическая система $\langle X, \cdot \rangle$ с одной бинарной операцией называется ***группоидом*** или ***магмой***.

Опр. 1.7. Элемент x группоида называется ***идемпотентом***, если $x^2 = x$.

Опр. 1.8. Элемент e_L группоида $\langle X, \cdot \rangle$ называется ***левым нейтральным***, если $\forall x \in X \ e_L x = x$. Элемент e_R группоида называется ***правым нейтральным***, если $\forall x \in X \ x e_R = x$. Элемент e группоида называется ***нейтральным***, если $\forall x \in X \ ex = xe = x$.

Лемма 1.1. *Если в группоиде есть левый нейтральный и правый нейтральный, то они совпадают.*

Опр. 1.9. Элемент x группоида $\langle X, \cdot \rangle$ называется ***регулярным слева***, если на него можно сокращать слева: $\forall y, z \in X \ xy = xz \Rightarrow y = z$. Элемент x моноида X называется ***регулярным справа***, если на него можно сокращать справа.

Опр. 1.10. Элемент y группоида $\langle X, \cdot \rangle$ с нейтральным элементом e называется ***левым обратным*** к x, если $yx = e$. Элемент y группоида $\langle X, \cdot \rangle$ с нейтральным элементом e называется ***правым обратным*** к x, если $xy = e$. Элемент y группоида $\langle X, \cdot \rangle$ с нейтральным элементом e называется ***обратным*** к x, если $xy = yx = e$. Если элемент имеет обратный, то он называется ***обратимым***.

Замечание. При использовании аддитивной записи обратный часто называется ***противоположным***.

Опр. 1.11. Операция $*$ на множестве X называется ***ассоциативной***, если $\forall x, y, x \in X \ (x * y) * z = x * (y * z)$.

Опр. 1.12. Операция $*$ на множестве X называется ***коммутативной***, если $\forall x, y \in X \ x * y = y * x$.

Теорема 1.1. (***об обобщённой ассоциативности***) *Если на X задана ассоциативная операция $*$, то она обладает обобщённой ассоциативностью: результат $x_1 * x_2 * \ldots * x_n$ не зависит от расстановки скобок.*

Опр. 1.13. Группоид с ассоциативной операцией называется ***полугруппой***.

Опр. 1.14. Полугруппа с нейтральным элементов называется ***моноидом***.

Лемма 5.2. *Если характеристика поля больше нуля, то стым числом.*

Опр. 1.15. Элемент x моноида X называется ***обратимым***, если $x^{-1} = e$.

Лемма 1.2. *Пусть $\langle X, \cdot \rangle$ — моноид. Тогда если у элемента $x \in X$ есть правый обратный и левый обратный, то они совпадают.*

Лемма 1.3. *Элемент x моноида X, обратимый слева/справа, является регулярным слева/справа.*

Лемма 1.4. *Если операция ассоциативна, то обратный элемент единственен.*

§2. Группы

...понятие группы является древнейшим математическим понятием, не только более древним, чем алгебраические уравнения, но даже более древним, чем само понятие числа, и неотделимым от человеческой цивилизации.

Н. А. Вавилов

Опр. 2.1. ***Группа*** — моноид, в котором все элементы обратимы.

Лемма 2.1. *G — группа. $\forall g, h \in G\ \exists!\, x \in G\ hx = g$; $\forall g, h \in G\ \exists!\, x \in G\ xh = g$.*

Опр. 2.2. Группа с коммутативной операцией называется ***абелевой группой***.

Опр. 2.3. Пусть G — группа. Её подсистема H называется ***подгруппой***, если она является группой относительно той же групповой операции. Другими словами,

1) H замкнуто относительно групповой операции;
2) $x \in H \Rightarrow x^{-1} \in H$;
3) $e \in H$.

Опр. 2.4. ***Порядок группы***— мощность носителя группы. Обозначается $|G|$.

Опр. 2.5. ***Порядок элемента*** g ***группы*** G — наименьшее натуральное n такое, что $g^n = e$, если такое существует. Если такого натурального числа нет, то порядок равен ∞. Обозначение $|g|$, $\mathrm{ord}(g)$, $o(g)$.

Опр. 2.6. Группы $\langle G, * \rangle$ и $\langle H, \star \rangle$ называются ***изоморфными***, если существует такая биекция $\varphi\colon G \to H$, что $\forall x, y \in G\ \varphi(x * y) = \varphi(x) \star \varphi(y)$. Обозначение $G \simeq H$. Изоморфизм группы на себя называется ***автоморфизмом***.

Опр. 2.7. Пусть $\langle G, * \rangle$ и $\langle H, \star \rangle$ — группы. Отображение $\varphi\colon G \to H$ называются ***гомоморфизмом***, если $\forall x, y \in G\ \varphi(x * y) = \varphi(x) \star \varphi(y)$. Гомоморфизм группы в себя называется ***эндоморфизмом***.

Замечание. Можно аналогично определить изоморфизм и гомоморфизм произвольных группоидов.

Лемма 2.2. *Образом нейтрального элемента при гомоморфизме групп является нейтральный. Образом обратного к x — обратный к образу x.*

Лемма 2.3. *$(x^{-1})^{-1} = x$, $(xy)^{-1} = y^{-1}x^{-1}$. Другими словами, взятие обратного является* ***антиавтоморфизмом групп порядка 2***.

§3. Группа перестановок

Свойства перестановок настолько красивы, что представляют и самостоятельный интерес.

Дональд Кнут

...вместилище всех вообще конечных групп, рассматриваемых с точностью до изоморфизма.

А. И. Кострикин

Опр. 3.1. ***Группой*** S_n ***перестановок на*** n ***точках*** называется группа всех биекций на множестве $\{1, 2, \ldots, n\}$ относительно операции композиции.

Опр. 3.2. ***Полная запись перестановки*** — запись перестановки σ в виде $\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$.

Замечание. В контексте разговора о перестановках операция композиции часто называется умножением.

Теорема 3.1. $|S_n| = n!$

Опр. 3.3. Перестановка $\sigma \in S_n$ называется ***циклом*** длины k, если для некоторых различных $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, …, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$, а для всех остальных $i \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$ $\sigma(i) = i$. Цикл длины 1 будем называть ***тривиальным циклом***. Цикл длины n называется ***длинным циклом***.

Лемма 3.1. *Порядок цикла длины k равен k.*

Опр. 3.4. Циклы называются ***независимыми***, если множества перемещаемых ими элементов не пересекаются.

Опр. 3.5. Пусть $\sigma \in S_n$. Определим отношение $\sim$ на $\{1, 2, \ldots, n\}$ так: $i \sim j \Leftrightarrow j = \sigma^k(i)$ для некоторого $k \in \mathbb{Z}$. Это отношение является эквивалентностью. Её классы эквивалентности называются ***орбитами*** σ.

Теорема 3.2.
1) *Любая перестановка раскладывается в произведение независимых циклов. Такое разложение единственно с точностью до порядка множителей.*
2) *Независимые циклы коммутируют.*

Опр. 3.6. ***Цикленная запись перестановки*** — запись перестановки в виде произведения независимых циклов.

Замечание. Зависимые циклы в общем случае не коммутируют.

Опр. 3.7. ***Транспозиция*** — цикл длины 2, то есть перестановка двух элементов. ***Фундаментальная транспозиция*** — перестановка двух соседних элементов.

Лемма 3.2. *Любая перестановка раскладываться в произведение транспозиций.*

Опр. 3.8. Говорят, что пара элементов $\sigma(i)$ и $\sigma(j)$ образуют ***инверсию***, если $\sigma(i) > \sigma(j)$ при $i < j$.

Опр. 3.9. ***Чётность перестановки*** σ — чётность числа инверсий $\mathrm{inv}(\sigma)$ в ней. Соответственно, перестановки делятся на ***чётные*** и ***нечётные***.

Опр. 3.10. ***Знак перестановки*** σ: $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$.

Лемма 3.3. *Фундаментальная транспозиция является нечётной перестановкой.*

Лемма 3.4. *Пусть $(i\,j)$ — произвольная транспозиция. Тогда для любой $\sigma \in S_n$ чётности перестановок σ и $\sigma(i\,j)$ различны.*

Следствие 3.2.1. *Любая перестановка раскладывается в произведение фундаментальных транспозиций.*

Теорема 3.3. *В S_n число чётных перестановок равно числу нечётных перестановок и равно $\dfrac{n!}{2}$ $(n > 1)$.*

Теорема 3.4. $\mathrm{sgn}(\sigma\pi) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi)$. *Другими словам, знак перестановки является гомоморфизмом.*

Следствие 3.4.1. $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$.

Следствие 3.4.2. *Чётность числа транспозиций, на которые раскладывается перестановка, всегда одинакова.*

Следствие 3.4.3. *Все чётные перестановки A_n образуют подгруппу в группе S_n. A_n называется* ***знакопеременной группой***.

Теорема 3.5. *Всякую перестановку из S_n можно разложить на $n - s$ транспозиций, где s — числов независимых циклов, на которые раскладывается перестановка, включая тривиальные.*

Опр. 3.11. Число $d(\sigma) = n - s$ из предыдущей теоремы называется ***декрементом*** перестановки σ. Легко заметить, что он равен разности между числом перемещаемых элементов и нетривиальных циклов.

Теорема 3.6. (***смысл декремента***) *Декремент — наименьшее число транспозиций, на которые можно разложить перестановку.*

Теорема 3.7. (***теорема Кэли***) *Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.*

§4. Разбиение на смежные классы и факторгруппы

Переход от уровня абстракции, который ассоциируется со школьной алгеброй, к тому уровню абстракции, который ассоциируется с алгеброй университетской, связан ровно с одной конструкцией — рассмотрением фактор-объектов.

Н. А. Вавилов

Гомоморфный образ группы
До победы коммунизма
Изоморфен факторгруппе
По ядру гомоморфизма

Математический фольклор

Опр. 4.1. Пусть G — группа, $H \leqslant G$. Будем говорить, что $g_1, g_2 \in G$ ***сравнимы по модулю*** H, если $g_1^{-1} g_2 \in H$, то есть $g_2 = g_1 H$. Это отношение является эквивалентностью. Классы этой эквивалентности называются ***левыми смежными классами***.

Левый смежный класс, содержащий элемент g, имеет вид $gH = \{gh \mid h \in H\}$.

Замечание. Иногда смежные классы gH называют правыми смежными классами.

Лемма 4.1. (***свойства смежных классов***)
1) *Образуют разбиение множества G на попарно непересекающиеся подмножества;*
2) *Существует биекция между H и gH $(H \ni h \mapsto gh \in H)$ и, следовательно, $|H| = |gH|$.*

Теорема 4.1. (***теорема Лагранжа***)
Пусть G — конечная группа, $H \leqslant G$, тогда $|G| = |H||G/H|$.

Следствие 4.1.1.
1) *Порядок любой подгруппы конечной группы делит порядок группы;*
2) *Порядок любого элемента конечной группы делит порядок группы;*
3) *Всякая конечная группа простого порядка является циклической;*
4) *Если $|G| = n$, то $g^n = e$ $\forall g \in G$.*

Опр. 4.2. ***Циклической*** называется группа G, состоящая из степеней одного элемента $g \in G$. Обозначение $G = \langle g \rangle$.

Опр. 4.3. Число смежных классов G по подгруппе H называется ***индексом подгруппы*** H и обозначается $|G : H|$, $[G : H]$ или просто $|G/H|$.

Замечание. Можно рассмотреть смежность справа по подгруппе H, тогда получатся ***правые смежные классы*** $Hg = \{hg \,|\, h \in H\}$. Отображение $g \mapsto g^{-1}$ устанавливает биекцию $(gH)^{-1} = Hg^{-1}$ и вся теория переносится на правые смежные классы.

Опр. 4.4. Подгруппа $H \leqslant G$ называется ***нормальной***, если $\forall g \in G\ gH = Hg$. Обозначается $H \trianglelefteqslant G$.

Замечание. Если группа абелева, то в ней любая подгруппа нормальна.

Лемма 4.2. *Следующие условия эквивалентны:*
1) $H \trianglelefteqslant G$;
2) $gHg^{-1} = H\ \forall g \in G$;
3) $gHg^{-1} \in H\ \forall h \in H,\ \forall g \in G$.

Опр. 4.5. Элемент ghg^{-1} называется ***сопряжённым*** к h с помощью ***сопрягающего*** элемента g. ***Отношение сопряжённости*** является эквивалентностью.

Замечание. Условие 3 обычно проще всего проверить: нормальная подгруппа замкнута относительно сопряжения.

Теорема 4.2. (***описание сопряжённости в группе*** S_n)
Две перестановки сопряжены тогда и только тогда, когда они имеют одинаковое цикленное строение.

Опр. 4.6. ***Факторгруппа***[1] группы G по нормальной подгруппе H — это множество смежных классов G/H с операцией умножения смежных классов как подмножеств в G: $AB = \{ab \,|\, a \in A, b \in B\}$.

Лемма 4.3. *Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Тогда:*
1) $\operatorname{Im}\varphi = \{\varphi(g) \,|\, g \in G\} \leqslant H$;
2) $\operatorname{Ker}\varphi = \{g \in G \,|\, \varphi(g) = e\} \trianglelefteqslant G$.

Опр. 4.7. В абелевой группе можно рассмотреть факторгруппу $G/\operatorname{Im}\varphi$, которая называется ***коядром*** гомоморфизма φ.

Пусть $H \trianglelefteqslant G$. ***Каноническая проекция*** π — отображение $\pi\colon G \to G/H$, $g \mapsto gH$. Она является гомоморфизмом и $\operatorname{Im}\pi = G/H$, $\operatorname{Ker}\pi = H$. Любая нормальная подгруппа является ядром некоторого гомоморфизма и наоборот, ядро гомоморфизма — нормальная подгруппа. То есть нормальные подгруппы — это в точности ядра гомоморфизмов.

Теорема 4.3. (***о гомоморфизме групп***)
Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Тогда существует изоморфизм

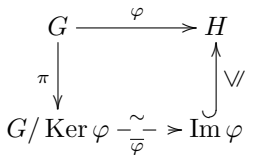
$$\overline{\varphi}\colon G/\operatorname{Ker}\varphi \xrightarrow{\sim} \operatorname{Im}\varphi,$$

для которого $\varphi = \overline{\varphi} \circ \pi$, где $\pi\colon G \to G/\operatorname{Ker}\varphi$ — каноническая проекция. Другими словами, $\varphi(g) = \overline{\varphi}(g \operatorname{Ker}\varphi)$.

[1] Иногда через дефис: ***фактор-группа***.

Следствие 4.3.1. *Для любого гомоморфизма конечных групп* $\varphi\colon G \to H$ *верно, что* $|G| = |\operatorname{Im}\varphi||\operatorname{Ker}\varphi|$.

Теорему о гомоморфизме можно проиллюстрировать следующей диаграммой (движение по стрелкам приводит к одинаковому результату, стрелка $\hookrightarrow$ означает изоморфное вложение (в данном случае абсолютно естественное), пунктирная стрелка означает утверждение о существовании гомоморфизма, знак $\sim$ говорит о том, что гомоморфизм является изоморфизмом):



§5. Кольца и поля

Опр. 5.1. ***Кольцом*** называется алгебраическая система $\langle R, +, \cdot\rangle$ с двумя бинарными операциями — сложением и умножением, если выполняются следующие условия (аксиомы кольца):

1) R является абелевой группой по сложению;
2) $\forall x, y, z \in R\ (x+y)z = xz + yz,\ x(y+z) = xy + xz$.

Следствие 5.0.2. (*из аксиом кольца*)

1) $\forall x \in R\ x0 = 0x = 0$;
2) $\forall x, y \in R\ x(-y) = (-x)y = -xy$;
3) $\forall x, y, z \in R\ x(y-z) = xy - xz,\ (x-y)z = xz - yz$.

Опр. 5.2. Подмножество $L \subseteq R$ называется ***подкольцом*** ($L \leqslant R$), если:

1) L является подгруппой аддитивной группы кольца R;
2) L замкнуто относительно умножения.

Опр. 5.3. Кольцо называется ***ассоциативным***, если операция умножения ассоциативна, и ***коммутативным*** — если операция умножения коммутативна. Кольцо называется ***кольцом с единицей***, если существует нейтральный элемент по умножению.

Замечание. Если $1 = 0$, то $\forall x \in R\ x = 1x = 0x = 0$, и такое кольцо называется ***нулевым***.

Замечание. При наличии коммутативности из двух аксиом дистрибутивности можно оставить только одну.

Опр. 5.4. Элемент x^{-1} называется ***обратным*** к x, если $xx^{-1} = x^{-1}x = 1$. Сам элемент x при этом называется ***обратимым***. ***Множество всех обратимых элементов*** кольца R обозначается R^*.

Опр. 5.5. Ненулевые элементы $x, y \in R$, для которых $xy = 0$ называются ***делителями нуля***. Кольцо в котором нет делителей нуля, называется ***кольцом без делителей нуля***.

Опр. 5.6. Ассоциативное коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется ***полем***.

Лемма 5.1. *В поле нет делителей нуля.*

Замечание. Ненулевые элементы поля F образуют абелеву групп по умножению, которая называется ***мультипликативной группой поля*** F и обозначается F^*.

Опр. 5.7. Подмножество K поля F называется ***подполем***, если:
1) K является подкольцом F;
2) $x \in K$, $x \neq 0 \Rightarrow x^{-1} \in K$;
3) $1 \in K$.

Опр. 5.8. ***Порядок*** кольца — мощность его носителя.

Опр. 5.9. Отображение $\varphi\colon R \to Q$ называется ***гомоморфизмом колец***, если:
1) $\forall x, y \in R\ \varphi(x + y) = \varphi(x) + \varphi(y)$;
2) $\forall x, y \in R\ \varphi(xy) = \varphi(x)\varphi(y)$;

Замечание. При гомоморфизме колец единица кольца R не обязана переходить в единицу кольца Q (её может вообще не быть).

Опр. 5.10. Пусть F — произвольное поле. Наименьшее натуральное число n такое, что $\underbrace{1 + 1 + \ldots + 1}_{n} = 0$ называется ***характеристикой*** этого поля ($\operatorname{char} F = n$). Если такого натурального числа нет, что $\operatorname{char} F = 0$.

Лемма 5.2. *Если характеристика поля больше нуля, то она является простым числом.*

§6. Кольцо вычетов

Рассмотрим группу $\langle \mathbb{Z}_n, + \rangle$ и введём на её элементах операцию умножения: $\overline{x}\,\overline{y} = \overline{xy}$. Операция введена корректно, так как $a \equiv b \pmod n$ и $c \equiv d \pmod n$ влечёт $ac \equiv bd \pmod n$.

Теорема 6.1. $\langle \mathbb{Z}_n, +, \cdot \rangle$ *является ассоциативным коммутативным кольцом с единицей.*

Теорема 6.2. $\langle \mathbb{Z}_n, +, \cdot \rangle$ *является полем тогда и только тогда, когда* n *— простое число.*

Замечание. Говоря о поле, будем писать $\mathbb{Z}_p$. Легко понять, что $\operatorname{char} \mathbb{Z}_p = p$.

Лемма 6.1. (***бином Ньютона в поле*** $\mathbb{Z}_p$) $\forall x, y \in \mathbb{Z}_p\ (a+b)^p = a^p + b^p$.

Следствие 6.2.1. (***малая теорема Ферма***)
1) $\forall a \in \mathbb{Z}, \forall p \in \mathbb{P}\ a^p \equiv a \pmod{p}$.
2) $\forall a \in \mathbb{Z}, \forall p \in \mathbb{P}\ a^{p-1} \equiv 1 \pmod{p}$, *если* a *взаимно просто с* p.

Опр. 6.1. $\varphi\colon \mathbb{N} \to \mathbb{N}_0$, $\varphi(n)$ — количество натуральных чисел, меньших n, и взаимно простых с ним.

Теорема 6.3. (***теорема Эйлера***)
Если a *взаимно просто с* n, *то* $a^{\varphi}(n) \equiv 1 \pmod{n}$.

Теорема 6.4. (***теорема Вильсона***)
$p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.

Пример 6.1. (конечные геометрии) Будем говорить, что ***прямая*** — это множество точек, удовлетворяющих уравнению $ax + by = c$, $a, b, c \in F$ и хотя бы один из коэффициентов a и b отличен от нуля. Либо, что эквивалентно, прямая — траектория точки (x_0, y_0), движущейся со скоростью (v, u), то есть множество точек $(x_0 + tv, y_0 + tu) \in F^2$, параметр t пробегает поле F. Тогда на плоскости $\mathbb{Z}^2 \times \mathbb{Z}^2$, состоящей из точек $A(0,0), B(0,1), C(1,0), D(1,1)$, ровно 6 прямых:
1) $AB\colon x = 0$;
2) $BC\colon x + y = 1$;
3) $CD\colon x = 1$;
4) $AC\colon y = 0$;
5) $AD\colon x + y = 0$;
6) $BD\colon y = 1$.
Всего на этой плоскости 3 пары параллельных прямых: $AB \| CD$, $AD \| BC$, $AC \| BD$.

§7. Поле комплексных чисел

Рассмотрим пары $(x, y) \in \mathbb{R}^2$ и введём операции над ними:
$(a, b) + (c, d) = (a + c, b + d)$;
$(a, b)(c, d) = (ac - bd, ad + bc)$.

Теорема 7.1. *Множество* $\mathbb{R}^2$ *с введёнными выше операциями сложения и умножения является полем.*

Это поле называется ***полем комплексных чисел*** и обозначается $\mathbb{C}$. Вещественные числа естественным образом вкладываются в комплексные: $\mathbb{R} \hookrightarrow \mathbb{C}$, $x \mapsto (x, 0)$. Числа $\mathbb{C} \setminus \mathbb{R}$ называются ***мнимыми***. Числа вида $(0, y)$ называются ***чисто мнимыми***. Элемент $(0, 1)$ называется ***мнимой единицей***. Легко проверить, что $(0, 1)^2 = (-1, 0)$. Обозначим мнимую единицу i, тогда $i^2 = -1$. Комплексные числа можно изобразить точками на плоскости, ось Ox называется ***вещественной осью***, Oy — ***мнимой осью***.

Опр. 7.1. Форма записи комплексного числа $\boldsymbol{x + yi} = x(1,0) + y(0,1) = (x, y)$ называется ***алгебраической формой*** записи.

Опр. 7.2. Отображение $^- : \mathbb{C} \to \mathbb{C}$, $x + yi \mapsto x - yi = \overline{x + yi}$ называется ***сопряжением*** комплексного числа.

Лемма 7.1. *Сопряжение — автоморфизм поля* $\mathbb{C}$*, то есть* $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

Опр. 7.3. Пусть $z = x + yi \in C$. Тогда:
$x = \mathrm{Re}(z)$ — ***вещественная часть*** z;
$y = \mathrm{Im}(z)$ — ***мнимая часть*** z;
$|z| = \sqrt{x^2 + y^2}$ — ***модуль*** z;
$|z|^2$ — ***норма*** z;
Угол между радиус-вектором точки z и положительным направлением вещественной оси — ***аргумент*** $\arg(z) \in \mathbb{T}$ числа z.

Опр. 7.4. Форма записи $\rho(\cos\varphi + i\sin\varphi) = |z|\left(\dfrac{x}{|z|} + i\dfrac{y}{|z|}\right)$ называется ***тригонометрической формой*** записи.

Опр. 7.5. Форма записи $\rho e^{i\varphi}$ называется ***показательной формой*** записи.

Теорема 7.2. $\mathbb{C}^* \simeq \mathbb{R}_{>0} \times \mathbb{T}$.

Теорема 7.3. $\rho e^{i\varphi} = \rho(\cos\varphi + i\sin\varphi)$.

Следствие 7.3.1. $e^{i\pi} = -1$.

Следствие 7.3.2. *Пусть* $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2)$, *тогда:*
1) $z_1 z_2 = \rho_1\rho_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$;
2) $\dfrac{\rho_1}{\rho_2} = \dfrac{z_1}{z_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$, *если* $z_2 \neq 0$;
3) $(\rho(\cos\varphi + i\sin\varphi))^n = \rho^n(\cos n\varphi + i\sin n\varphi)$ (***формула Муавра***).

Теорема 7.4. (*извлечение корней из комплексного числа*) *Корней степени* n *из комплексного числа* z *существует ровно* n *штук и они находятся по формуле*

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

где $\varphi = \arg(z)$, $\rho = |z|$.

Следствие 7.4.1. *Корни* n*-ной степени располагаются в вершинах правильного* n*-угольника.*

Следствие 7.4.2. *Множество корней* n*-ой степени из 1 относительно умножения образует группу* μ_n *и* $\mu_n \simeq \mathbb{Z}_n$.

Замечание. Все комплексные числа с модулем 1 образуют мультипликативную группу, изоморфную группе углов $\mathbb{T}$. Иногда это принимают за определение группы углов.

§8. Кольцо многочленов

Пусть R — кольцо. Построим новое кольцо $R[x]$, состоящее из последовательностей $(a_0, a_1, a_2, \ldots)$, где $a_i \in R$, в которых лишь конечное число элементов отлично от нуля (***почти все*** равны нулю). Если $a = (a_0, a_1, a_2, \ldots)$, $b = (b_0, b_1, b_2, \ldots)$, то определим сумму $a + b$ как последовательность с элементами $a_i + b_i$ и произведение $c = ab$ как

$$c_i = \sum_{k=0}^{i} a_k b_{i-k}.$$

Теорема 8.1. *Если R — ассоциативное коммутативное кольцо с единицей, то $R[x]$ — ассоциативное коммутативное кольцо с единицей.*

Введём сокращения: $x^0 = (1, 0, 0, 0, \ldots)$, $x = x^1 = (0, 1, 0, 0, \ldots)$. Тогда $x^2 = x \cdot x = (0, 0, 1, 0, \ldots)$, $x^3 = x^2 \cdot x = (0, 0, 0, 1, \ldots)$ и т.д. Кольцо R естественным образом вкладывается в $R[x]$: $R \ni r \mapsto (r, 0, 0, 0, \ldots) \in R[x]$. Тогда любой многочлен можно записать в стандартном виде $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$.

Опр. 8.1. Построенное выше кольцо $R[x]$ называется ***кольцом многочленов от одной переменной*** над кольцом R.

Опр. 8.2. Номер n наибольшего ненулевого элемента a_n называется ***степенью*** многочлена и обозначается deg. Будем считать, что $\deg(0, 0, 0, \ldots) = -\infty$, то есть $\deg\colon R[x] \to \mathbb{N}_0 \cup \{-\infty\}$.

Лемма 8.1.
1) $\forall f, g \in R[x]\ \deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}$;
2) $\forall f, g \in R[x]\ \deg(fg) \leqslant \deg(f) + \deg(g)$.

Лемма 8.2. (*О делении с остатком в кольце многочленов*) *Пусть F — поле, $f, g \in F[x]$, $g \neq 0$. Тогда существуют единственные многочлены $q, r \in R[x]$ такие, что $f = dq + r$, $\deg r < \deg g$.*

Определим ***значение*** $f(c)$ многочлена $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ в точке c как отображение $\mathrm{ev}_c\colon R[x] \to R$, $f \mapsto a_n c^n + a_{n-1} c^{n-1} + \ldots a_1 c + a_0$.

Лемма 8.3. *Отображение ev_c является гомоморфизмом колец, то есть*
1) $\mathrm{ev}_c(f + g) = \mathrm{ev}_c(f) + \mathrm{ev}_c(g)$;
2) $\mathrm{ev}_c(fg) = \mathrm{ev}_c(f)\,\mathrm{ev}_c(g)$.

Опр. 8.3. Пусть $f \in R[x]$, $c \in R$. Говорят, что c является ***корнем*** многочлена, если $f(c) = 0$.

Лемма 8.4. *Пусть $f \in \mathbb{R}[x]$. Если $f(c) = 0$, то $f(\overline{c}) = 0$.*

Опр. 8.4. Поле F называется ***алгебраически замкнутым***, если у любого многочлена из $F[x]$ положительной степени есть корень в F.

Теорема 8.2. (***«основная теорема алгебры»***) *Поле* $\mathbb{C}$ *алгебраически замкнуто.*

Следствие 8.2.1.
1) *Любой многочлен из* $\mathbb{R}[x]$ *нечётной степени имеет как минимум один вещественный корень;*
2) *Любой многочлен из* $\mathbb{R}[x]$ *раскладывается на линейные многочлены и квадратичные с отрицательным дискриминантом.*

§9. Кольцо квадратных матриц

Опр. 9.1. Пусть F — поле. Отображение $\mathscr{A}\colon I \times J \to F$ называется ***матрицей*** над полем F. Если $I = \{1, 2, \ldots, m\}$, $J = \{1, 2, \ldots, n\}$, то матрицу $\mathscr{A}$ можно записать в виде таблицы $A = (a_{ij})$, где i — номер строки, j — номер столбца. Обозначим все матрицы $F^{\{1,2,\ldots,m\}\times\{1,2,\ldots,n\}}$ как $M_{m\times n}(F)$. Если $m = n$, то матрицы называются ***квадратными*** и пишется $M_n(F)$.

Определим операции над матрицами:
1) $A, B \in M_{m\times n}(F)$, $M_{m\times n}(F) \ni C = A + B$, если $c_{ij} = a_{ij} + b_{ij}$.
2) $A \in M_{m\times k}, B \in M_{k\times n}(F)$, $M_{m\times n}(F) \ni C = AB$, если $c_{ij} = \sum\limits_{l=1}^{k} a_{il}b_{lj}$.

Теорема 9.1. *Множество* $M_n(F)$ *с введёнными выше операциями является ассоциативным кольцом с единицей* E.

«Негативные» свойства кольца матриц:
1) Не коммутативно;
2) Есть делители нуля;
3) Не всякое уравнение $AX = E$, где $A \neq 0$ имеет решение.

Опр. 9.2. Список $(a_{11}, a_{22}, \ldots, a_{nn})$ называется главной диагональю матрицы $A \in M_n(F)$. Сумма $a_{11} + a_{22} + \ldots + a_{nn} = \operatorname{tr} A$ называется ***следом*** матрицы A.

Лемма 9.1. *Пусть* $A, B \in M_n(F)$, *тогда:*
1) $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$;
2) $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Отображение ***транспонирования*** $^{\mathrm{T}}\colon M_n(F) \to M_n(F)$, $(a_{ij}) \mapsto (a_{ji})$. Легко понять, что оно биективно.

Лемма 9.2. *Пусть* $A, B \in M_n(F)$, *тогда:*
1) $(A^{\mathrm{T}})^{\mathrm{T}} = A$;
2) $(A + B)^{\mathrm{T}} = A^{\mathrm{T}} + B^{\mathrm{T}}$;
3) $(AB)^{\mathrm{T}} = B^{\mathrm{T}}A^{\mathrm{T}}$;
Другими словами, транспонирование является ***антиавтоморфизмом колец порядка 2****.*

Матрицы E_{ij}, в которых на позиции (i,j) стоит 1, а на остальных позициях — 0, называются ***стандартными матричными единицами***. Можно убедиться, что $E_{ij}E_{kl} = \delta_{jk}E_{il}$, где $\delta_{jk} = \begin{cases}1, \text{ если } j = k\\ 0, \text{ если } j \neq k\end{cases}$ — ***символ Кронекера***.

Пусть $X \in M_{m\times n}(F)$ и $m = m_1 + m_2 + \ldots + m_r$, $n = n_1 + n_2 + \ldots + n_s$. Рассмотрим ***блочную матрицу*** $r \times s$, элементами которой являются матрицы $X_{ij} \in M_{m_i \times n_j}(F)$, называемые ***блоками***:

$$\left(\begin{array}{c|c|c|c} X_{11} & X_{12} & \ldots & X_{1s} \\ \hline X_{21} & X_{22} & \ldots & X_{2s} \\ \hline \ldots & \ldots & \ldots & \ldots \\ \hline X_{r1} & X_{r2} & \ldots & X_{rs} \end{array}\right).$$

Теорема 9.2. *Если разбиения и размеры блоков согласованны, то сложение и умножение блочных матриц происходят по обычным правилам.*

Следующие матрицы из $M_n(F)$ называются ***элементарными***:
а) $T_{ij}(\lambda) = E + \lambda E_{ij}$ — ***элементарная трансвекция***;
б) $R_{ij} = E - (E_{ii} + E_{jj}) + (E_{ij} + E_{ji})$ — ***элементарное отражение***;
в) $D_i(\lambda) = E + (\lambda - 1)E_{ii}$ — ***элементарное псевдоотражение***.

Опр. 9.3. Матрица $A \in M_n(F)$ называется ***симметрической***, если $A = A^{\mathrm{T}}$ и ***кососимметрической***, если $A = -A^{\mathrm{T}}$. Матрицы A и B называются ***коммутирующими*** или ***перестановочными***, если $AB = BA$.

§10. Евклидовы кольца

Опр. 10.1. Ассоциативное коммутативное кольцо с единицей и без делителей нуля называется ***целостным кольцом*** или ***областью целостности***.

Опр. 10.2. Пусть R — целостное кольцо. Элемент $y \in R$ ***делит*** $x \in R$ $(y \,|\, x)$ если существует такой $z \in R$, что $x = yz$. Элементы x и y называются ***ассоциированными*** $(x \sim y)$, если $x \,|\, y$ и $y \,|\, x$.

Опр. 10.3. Целостное кольцо R, не являющееся полем, называется ***евклидовым***, если существует такая функция $N\colon R \setminus \{0\} \to \mathbb{N}_0$, называемая ***нормой***, которая удовлетворяет следующим условиям:
1) $N(fg) \geqslant N(f)$, причём $N(fg) = N(f) \Leftrightarrow g$ обратим;
2) $\forall f, 0 \neq g \in R$, $\exists\, q, r \in R$, что $f = gq + r$ и либо $r = 0$, либо $N(r) < N(g)$.

Опр. 10.4. ***Наибольший общий делитель*** элементов a и b целостного кольца — их общий делитель, который делится на все их общие делители.

Теорема 10.1. *В евклидовом кольце R для любых элементов a и b существует наибольший общий делитель d и он может быть представлен в виде $d = au + bv$, где $u, v \in R$.*

Процедура нахождения НОДа, используемая в доказательстве этой теоремы, называется ***алгоритмом Евклида***. Элементы $a, b \in R$ называются ***взаимно простыми***, если НОД$(a, b) = 1$.

Опр. 10.5. Необратимый ненулевой элемент p целостного кольца называется ***простым***, если он не может быть представлен в виде $p = xy$, где x, y — необратимые элементы.

Теорема 10.2. *Если простой элемент p евклидова кольца делит произведение $x_1 x_2 \dots x_n$, то он делит хотя бы один из сомножителей $x_1, x_2, \dots, x_n$.*

Теорема 10.3. *В евклидовом кольце всякий необратимый ненулевой элемент может быть разложен на простые множители, причём это разложение единственного с точностью до порядка сомножителей и умножения на обратимые элементы.*

Замечание. Свойство, описанное в предыдущей теореме, называется ***факториальностью***. То есть каждое евклидово кольцо факториально.

Опр. 10.6. ***Наименьшим общим кратным*** элементов a и b целостного кольца называется их общее кратное, делящее все их общие кратные.

Лемма 10.1. НОК$(x, y)\cdot$НОД$(x, y) \sim xy$.

Замечание. Простые элементы кольца $\mathbb{Z}$ — простые числа и противоположные к ним, кольца $F[x]$ — ***неприводимые*** над F (то есть не раскладывающиеся на многочлены с коэффициентами из F меньших, но положительных степеней) многочлены.

Лемма 10.2. (***лемма Гаусса***) *Приводимость многочлена из $\mathbb{Z}[x]$ в кольце $\mathbb{Q}[x]$ равносильна его приводимости в $\mathbb{Z}[x]$.*

Теорема 10.4. (***признак Эйзенштейна***) $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$. *Если существует такое простое число p, что $p \nmid a_n$, $p \mid a_i$ для всех i от 0 до $n-1$, $p^2 \nmid a_0$, то f неприводим над $\mathbb{Q}$.*

§11. Идеалы и факторкольца

Ах, какое блаженство,
Ах, какое блаженство,
Знать, что я совершенство,
Знать, что я идеал.

Опр. 11.1. Нормальная подгруппа I аддитивной группы кольца R называется ***левосторонним идеалом***, если $\forall x \in I\ \forall \in R\ ax \in I$ и ***правосторонним идеалом***, если $\forall x \in I\ \forall \in R\ xa \in I$. Если выполняются оба этих условия, то I называется идеалом кольца R и обозначается $I \trianglelefteqslant R$.

Лемма 11.1. *Отношение сравнимости по модулю I согласованно с умножением тогда и только тогда, когда I — идеал.*

Опр. 11.2. Пусть $I \trianglelefteqslant R$, тогда на факторгруппе R/I можно определить умножение по правилу $(x+I)(y+I) = xy+I$ и получить ***факторкольцо*** кольца R по идеалу I.

Лемма 11.2. *Если R ассоциативно, коммутативно или кольцо с единицей, то R/I тоже ассоциативно, коммутативно и кольцо с единицей соответственно.*

Лемма 11.3. *$\varphi\colon R \to Q$ — гомоморфизм колец. Тогда:*
1) $\operatorname{Im}\varphi = \{y \mid y = \varphi(x), x \in R\} \leqslant Q$;
2) $\operatorname{Ker}\varphi = \{x \mid \varphi(x) = 0\} \trianglelefteqslant R$.

Опр. 11.3. $\pi\colon R \to R/I$, $x \mapsto x + I$ — ***каноническая проекция***.

Замечание. $\operatorname{Im}\pi = R/I$, $\operatorname{Ker}\pi = I$. Таким образом, идеалы — это в точности ядра гомоморфизмом колец.

Теорема 11.1. *Пусть $\varphi\colon R \to Q$ — гомоморфизм колец. Тогда существует изоморфизм*

$$\overline{\varphi}\colon R/\operatorname{Ker}\varphi \xrightarrow{\sim} \operatorname{Im}\varphi,$$

для которого $\varphi = \overline{\varphi}\circ\pi$, где $\pi\colon R \to R/\operatorname{Ker}\varphi$ — каноническая проекция. Другими словами, $\varphi(x) = \overline{\varphi}(x + \operatorname{Ker}\varphi)$.

Опр. 11.4. $(a) = aR = Ra$ — идеал, порождённый одним элементом $a \in R$, — ***главный идеал***. Кольцо, в котором все идеалы главные, называется ***кольцом главных идеалов***.

Теорема 11.2. *Пусть $f \in F[x]$. $F[x]/(f)$ является полем тогда и только тогда, когда f неприводим в $F[x]$.*

Следствие 11.2.1. $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

§12. Определители и их приложения

Определим функцию $\det\colon \underbrace{F^n \times F^n \times \ldots \times F^n}_{n} \to F$, которая удовлетворяет следующим условиям:

1) ***Полилинейность***: линейна по каждом аргументу;
2) ***Антисимметричность***: если два аргумента равны, то она равна нулю;
3) ***Нормированность***: $\det(e_1, e_2, \ldots, e_n) = 1$,
$e_1 = (1,0,0,\ldots,0)^{\mathrm{T}}$, $e_2 = (0,1,0,\ldots,0)^{\mathrm{T}}$, $\ldots$, $e_n = (0,0,0,\ldots,1)^{\mathrm{T}} \in F^n$.

Замечание. Из антисимметричности следует ***кососимметричность***: det меняет знак при перестановке двух аргументов. Обратное в общем случае неверно.

Замечание. Можно проинтерпретировать аргументы функции det как столбцы матрицы $A \in M_n(F)$ и говорить о функции $\det\colon M_n(F) \to F$. Тогда, например, $\det E = 1$.

Следствие 12.0.2. (*непосредственно из условий*)
1) $\det(AT_{ij}(\lambda)) = \det A$;
2) $\det(AD_i(\lambda)) = \lambda \det A$;
3) $\det(AP_{ij}) = -\det A$.

Теорема 12.1. *Существует единственная функция* det, *удовлетворяющая описанным условиям*:

$$\det A = \det(a_1, a_2, \dots a_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \dots a_{\sigma(n),n}.$$

Эта функция называется ***определителем*** *матрицы* A.

Следствие 12.1.1.
1) $\det A = \det A^{\mathrm{T}}$;
2) *Определитель треугольной матрицы равен произведению её элементов на главной диагонали.*

Опр. 12.1. Определитель матрицы, которая получается при вычёркивании из матрицы A i-той строки и j-того столбца, называется i-тым j-тым ***минором*** M_{ij}. $A_{ij} = (-1)^{i+j} M_{ij}$ называется ***алгебраическом дополнением*** элемента a_{ij}.

Теорема 12.2. (***разложение определителя по строке/столбцу***)

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij} = \sum_{i=1}^{n} a_{ij} A_{ij}.$$

Лемма 12.1. *Сумма произведение элементов строки/столбца на соответствующие алгебраические дополнения элементов другой строки/столбца равна нулю.*

Лемма 12.2. $\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \det B.$

Теорема 12.3. $\det(AB) = \det A \det B$.

Опр. 12.2. Матрица называется ***невырожденной***, если её определитель не равен нулю.

Замечание. Все невырожденные матрицы из $M_n(F)$ образуют (мультипликативную) ***общую линейную группу*** $\mathrm{GL}_n(F)$. Определитель является гомоморфизмом групп: $\mathrm{GL}_n(F) \to F^*$, $A \mapsto \det A$. Все матрицы из $M_n(F)$ с определителем единица образуют ***специальную линейную группу*** $\mathrm{SL}_n(F) \leqslant \mathrm{GL}_n(F)$.

Рассмотрим отображение $L\colon S_n \to \mathrm{GL}_n(F)$, $\sigma \mapsto E_{\sigma(1),1}+E_{\sigma(2),2}+\ldots+E_{\sigma(n),n}$. Можно показать, что L — гомоморфизм групп. Это пример ***матричного представления*** группы над полем F.

Теорема 12.4. *Если* $\det A \neq 0$*, то квадратная система* $Ax = b$ *линейных алгебраических уравнений имеет единственное решение, которое может быть найдено по* ***формулам Крамера*** $x_i = \dfrac{\det A_i}{\det A}$*, где* A_i *— матрица, полученная из матрицы* A *заменой* i*-того столбца на столбец* b *свободных коэффициентов.*

Опр. 12.3. Матрица A^{-1} называется ***обратной*** к матрице A, если $A^{-1}A = AA^{-1} = E$.

Теорема 12.5. *Пусть* $\det A \neq 0$*. Тогда*

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1n} \\ A_{21} & A_{22} & \ldots & A_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ A_{n1} & A_{n2} & \ldots & A_{nn} \end{pmatrix}^{\mathrm{T}}.$$