Министерство образования Республики Беларусь

Учреждение образования
“Гомельский государственный университет им. Ф. Скорины”

Кафедра алгебры и геометрии

Краткий конспект лекций по курсу “Алгебра и теория чисел”

для студентов первого курса математического факультета

Гомель, 2005

Авторы: Бузланов А.В., Близнец И.В.

Рецензент — Семенчук В.Н., доктор физико-математических наук

Рекомендовано к печати научно-методическим советом Гомельского государственного университета им. Ф. Скорины

Содержание

Тема 1. Основные алгебраические структуры

§1. Множества с алгебраическими операциями

(1) Понятие множества принадлежит к основным понятиям современной математики. Будем понимать под *множеством* любую совокупность объектов. Эти объекты будем называть *элементами* данного множества. Если a есть элемент множества A, то пишут $a \in A$ (a *принадлежит множеству* A). Запись $a \notin A$ означает, что a не является элементом множества A (a *не принадлежит* A).

Для некоторых важных множеств приняты стандартные обозначения:

$\mathbb{N}$ — множество всех натуральных чисел,

$\mathbb{Z}$ — множество всех целых чисел,

$\mathbb{Q}$ — множество всех рациональных чисел,

$\mathbb{R}$ — множество всех действительных чисел.

Если множество A выделяется некоторым свойством $\mathscr{P}$, присущим только элементам множества A, то множество A удобно записывать в виде

$$A = \{a \mid a \text{ удовлетворяет } \mathscr{P}\}.$$

Так, если A — множество целых чисел, делящихся на 6, то $A = \{a \mid a = 6k, \text{ где } k \in \mathbb{Z}\}$.

Множество, состоящее из конечного числа элементов, может быть задано перечислением элементов: $A = \{a_1, a_2, \ldots, a_k\}$. Если A — конечное множество, то через $|A|$ будем обозначать число всех элементов множества A.

(2) *Пустое множество* $\varnothing$ — это множество, не содержащее ни одного элемента. Если каждый элемент множества A принадлежит множеству B, то говорят, что A есть *подмножество* множества B или A содержится в B и пишут $A \subseteq B$. Два множества A и B *равны*, если $A \subseteq B$ и $B \subseteq A$, т.е. у них одни и те же элементы.

Пусть A и B — непустые множества. *Декартово произведение* $A \times B$ этих множеств есть множество всех упорядоченных пар (a, b), где $a \in A$, $b \in B$, т.е.

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Элементы (a_1, b_1), $(a_2, b_2) \in A \times B$ называются *равными* (пишут: $(a_1, b_1) = (a_2, b_2)$), если $a_1 = a_2$, $b_1 = b_2$. Декартово произведение $A \times$

$\times A$ называют *декартовым квадратом* множества A и обозначают A^2.

(3) Пусть A — произвольное множество. *Бинарной алгебраической операцией* на A называется произвольное отображение $f : A^2 \to A$, которое любой упорядоченной паре $(a, b) \in A^2$ ставит в соответствие однозначно определенный элемент $c = f((a, b))$ из множества A. Бинарную операцию на A часто обозначают каким-либо специальным символом: $*$, $\circ$, $\cdot$, $+$ и вместо $f((a, b)) = c$ пишут $a * b = c$ или $a \circ b = c$, или $a \cdot b = c$, или $a + b = c$. Операцию $\cdot$ называют *произведением*, а $+$ *суммой*. *Алгебраической системой* $(A, *)$ будем называть множество A с заданной на нем бинарной алгебраической операцией $*$.

(4) Бинарная алгебраическая операция $*$ на множестве A называется *ассоциативной*, если $(a * b) * c = a * (b * c)$ для всех a, b, $c \in A$. Если же для любых a, $b \in A$ имеет место $a * b = b * a$, то операция $*$ называется *коммутативной*. Такие же названия присваиваются соответствующей алгебраической системе $(A, *)$. Так, $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ — ассоциативные и коммутативные алгебраические системы.

(5) Элемент $n \in A$ называется *нейтральным* в алгебраической системе $(A, *)$, если $n * a = a * n = a$ для всех $a \in A$. В алгебраической системе $(A, *)$ не может быть более одного нейтрального элемента. При умножении нейтральный элемент называется *единичным*, а при сложении — *нулевым элементом*, и обозначается 1 или 0, соответственно.

Ассоциативная алгебраическая система называется *полугруппой*. Полугруппа с нейтральным элементом называется *моноидом*. Моноид $(A, \cdot, 1)$ называют *мультипликативным моноидом*, а моноид $(A, +, 0)$ — *аддитивным*.

(6) Элемент a моноида $(A, *, n)$ называется *симметричным* элементу $b \in A$, если $a * b = b * a = n$. В моноиде для каждого элемента существует не более одного симметричного элемента. В мультипликативном моноиде элемент, симметричный элементу a, называется *обратным* и обозначается a^{-1}; элемент a в этом случае называется *обратимым*. В аддитивном моноиде элемент, симметричный элементу a, называется *противоположным* и обозначается $-a$.

§2. Группы

(1) **Определение 2.1.** Непустое множество G с бинарной алгебраической операцией $*$ называется *группой*, если выполняются следующие условия:

1) операция $*$ ассоциативна;

2) в $(G, *)$ существует нейтральный элемент;

3) для каждого элемента множества G существует симметричный элемент.

Если алгебраическая система $(G, *)$ — группа, то $*$ называется *групповой операцией*. В случае коммутативности групповой операции группу называют *абелевой*. Группа с конечным числом элементов называется *конечной группой*. Число элементов конечной группы G называется *порядком группы* и обозначается $|G|$.

(2) Наиболее употребительны мультипликативная и аддитивная группы.

Определение 2.2. Непустое множество G с бинарной алгебраической операцией умножения называется *мультипликативной группой*, если выполнены следующие условия:

1) операция умножения ассоциативна, т.е. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для любых a, b, $c \in G$;

2) в $(G, \cdot)$ существует единичный элемент 1, т.е. такой элемент, что $a \cdot 1 = 1 \cdot a = a$ для всех $a \in G$;

3) для каждого элемента $a \in G$ существует в G обратный элемент a^{-1}, т.е. такой элемент, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Так, $\mathbb{Q}^{\#}$ и $\mathbb{R}^{\#}$ — мультипликативные абелевы группы ($\mathbb{Q}^{\#} = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^{\#} = \mathbb{R} \setminus \{0\}$).

Определение 2.3. Непустое множество G с бинарной алгебраической операцией сложения называется *аддитивной группой*, если выполнены следующие условия:

1) операция сложения ассоциативна, т.е. $a + (b + c) = (a + b) + c$ для любых a, b, $c \in G$;

2) в $(G, +)$ существует нулевой элемент 0, т.е. такой элемент, что $a + 0 = 0 + a = a$ для всех $a \in G$;

3) для каждого элемента $a \in G$ существует в G противоположный элемент $-a$, т.е. такой элемент, что $a + (-a) = (-a) + a = 0$.

Так, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ — аддитивные абелевы группы.

(3) **Определение 2.4.** Подмножество H группы G называется *подгруппой группы* G, если множество H является группой относительно групповой операции в G. Если H — подгруппа группы G, то пишут $H \leqslant G$.

Например, $\mathbb{Q}^{\#} \leqslant \mathbb{R}^{\#}$ с групповой операцией умножения; $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R}$ с групповой операцией сложения.

§3. Кольца и их простейшие свойства

① **Определение 3.1.** *Кольцом* называется непустое множество K с двумя бинарными алгебраическими операциями сложения и умножения, которые удовлетворяют следующим условиям:

1) $(K, +)$ — абелева группа;

2) $(K, \cdot)$ — полугруппа;

3) операции связаны законами дистрибутивности $(a+b)\cdot c = a\cdot c + b\cdot c$ и $c\cdot(a+b) = c\cdot a + c\cdot b$ для всех a, b, $c \in K$.

Система $(K, +)$ называется *аддитивной группой кольца*, $(K, \cdot)$ — *мультипликативной полугруппой кольца*. Если $(K, \cdot)$ — моноид, то говорят, что K — *кольцо с единицей* 1. Если $(K, \cdot)$ — коммутативная полугруппа, то K называют *коммутативным кольцом*. Так, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ — коммутативные кольца с единицей.

② Простейшие свойства кольца K.

1. Пусть $x_1, x_2, \ldots, x_n \in K$, $n \in \mathbb{N}$. Результат сложения (умножения) элементов $x_1, x_2, \ldots, x_n$ не зависит от расстановки скобок, указывающих порядок действий.

Это свойство позволяет ввести следующие обозначения: $x_1 + x_2 + \ldots + x_n = \sum\limits_{i=1}^{n} x_i$; $\quad x_1 \cdot x_2 \cdot \ldots \cdot x_n = \prod\limits_{i=1}^{n} x_i$.

2. **Определение 3.2.** Пусть $x \in K$. Произведение $\underbrace{x \cdot x \cdot \ldots \cdot x}_{n}$, где $n \in \mathbb{N}$, обозначают x^n и называют *степенью элемента* x. Сумму $\underbrace{x + x + \ldots + x}_{n}$ обозначают nx и называют *кратным элемента* x.

Для любых m, $n \in \mathbb{N}$, $x \in K$ справедливы равенства: $x^m \cdot x^n = x^{m+n}$; $\quad (x^m)^n = x^{mn}$; $\quad mx + nx = (m+n)x$; $\quad m(nx) = (mn)x$.

3. Пусть x, $y \in K$, $n \in \mathbb{N}$. Тогда $n(x+y) = nx + ny$, а если кольцо K коммутативно, то $(x\cdot y)^n = x^n \cdot y^n$.

4. Для любого $x \in K$ верны равенства $x \cdot 0 = 0 \cdot x = 0$.

5. Для элементов кольца верно равенство

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_i x_j = \sum_{j=1}^{m}\sum_{i=1}^{n} x_i x_j.$$

§4. Поле и его простейшие свойства

① **Определение 4.1.** *Полем* называется непустое множество P с двумя бинарными алгебраическими операциями сложения и умножения, которые удовлетворяют следующим условиям:

1) $(P, +)$ — абелева группа;

2) $(P^{\#}, \cdot)$ — абелева группа;

3) операции связаны законом дистрибутивности: $(a+b)\cdot c = a\cdot c + b\cdot c$ для всех a, b, $c \in P$.

Так, $\mathbb{Q}$ и $\mathbb{R}$ — поля. Полем является множество $P = \{0, 1\}$ с операциями сложения и умножения, заданными следующими таблицами, которые заполняются по правилу $\rightarrow +(\cdot) \downarrow = \rightarrow \overset{\downarrow}{\square}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

② Простейшие свойства поля.

1. Поле содержит не менее двух элементов, так как $1 \neq 0$.

2. Всякое поле является кольцом. Поэтому все свойства колец справедливы и для полей.

3. **Определение 4.2.** Если x и y — ненулевые элементы кольца K, но произведение $x \cdot y = 0$, то элементы x и y называются *делителями нуля.*

Лемма 1. *В поле нет делителей нуля.*

③ Будем говорить, что поле P имеет *нулевую характеристику*, если все кратные единицы отличны от нуля, т.е. $m1 = \underbrace{1 + \ldots + 1}_{m} \neq 0$ для всех $m \in \mathbb{N}$.

Так, поля $\mathbb{Q}$ и $\mathbb{R}$ являются полями нулевой характеристики.

Если в поле P существуют кратные единицы, отличные от нуля, то P называется *полем положительной характеристики.* Наименьшее натуральное число n со свойством $n1 = 0$ называется *характеристикой поля* P.

Лемма 2. *Характеристика поля является простым числом.*

Так, поле $P = \{0, 1\}$, рассмотренное выше, имеет характеристику 2.

Тема 2. Основы теории чисел

§1. Теорема о делении с остатком

(1) **Определение 1.1.** Пусть $a,\ b \in \mathbb{Z}$. Говорят, что b *делит* a (пишут $b \mid a$) или что a *делится на* b (пишут $a \vdots b$), если существует целое число c такое, что $a = b \cdot c$. В этом случае b называют *делителем* числа a, число a — *кратным* числа b.

Из определения делимости целых чисел следует, что число нуль делится на любое целое число, в том числе и на нуль. Однако, ни одно целое число, отличное от нуля, на нуль не делится. Очевидно, что любое целое число a делится на a, $-a$, 1, -1. Эти числа называют *несобственными* (или *тривиальными*) делителями числа a. Остальные делители числа a, если они есть, называются *собственными* (или *нетривиальными*).

Лемма 1. *Для любых целых чисел a, b и c справедливы следующие утверждения:*

1) *если $a \mid b$ и $b \mid c$, то $a \mid c$;*

2) *если $a \mid b$, то $a \mid bc$;*

3) *если $a \mid b$ и $a \mid c$, то $a \mid (b \cdot k + c \cdot m)$ для любых целых чисел k и m;*

4) *если $a \mid b$ и $b \neq 0$, то $|a| \leqslant |b|$.*

(2) **Теорема 1 (о делении с остатком).** *Пусть $a,\ b \in \mathbb{Z}$ и $b \neq 0$. Существуют и притом единственные целые числа q и r такие, что $a = bq + r$, где $0 \leqslant r < |b|$. Число q называют* неполным частным, *а r* — остатком при делении a на b.

§2. Наибольший общий делитель. Алгоритм Евклида

(1) Пусть $a_1, a_2, \ldots, a_k$ — целые числа, не все равные нулю. Всякое целое число d, которое делит каждое из чисел $a_1, a_2, \ldots, a_k$, называется их *общим делителем*. Так как не все числа $a_1, a_2, \ldots, a_k$ равны нулю, то они имеют лишь конечное число общих делителей. Наибольший среди общих делителей называется *наибольшим общим делителем* чисел $a_1, a_2, \ldots, a_k$ и обозначается НОД$(a_1, a_2, \ldots, a_k)$.

Если $d_2 = \text{НОД}(a_1, a_2)$, $d_3 = \text{НОД}(d_2, a_3), \ldots$, $d_k = \text{НОД}(d_{k-1}, a_k)$, то НОД$(a_1, a_2, \ldots, a_k) = d_k$. Таким образом, задача нахождения НОД нескольких чисел сводится к задаче нахождения НОД двух чисел.

(2) Из определения НОД очевидны следующие свойства:

1) НОД$(0,0)$ не существует;

2) НОД$(0,a) = |a|$, если $a \neq 0$;

3) НОД$(a,b) =$ НОД$(|a|,|b|)$;

4) если $b \mid a$, то НОД$(a,b) = |b|$.

Свойство 3) позволяет при изучении НОД(a,b) рассматривать только неотрицательные числа a и b.

Лемма 1. *Если $a = bq + c$ для целых чисел a, b, q, c и $d =$ = НОД(a,b), то* НОД$(b,c) = d$.

(3) Пусть $a > b$ — положительные целые числа. По теореме о делении с остатком существуют целые числа q и r такие, что $a = bq + r$, где $0 \leqslant r < b$. По лемме 1 НОД$(a,b) =$ НОД(b,r). Таким образом, задача нахождения НОД (a,b) сводится к задаче нахождения НОД меньших чисел b и r. Это простое наблюдение лежит в основе общего метода отыскания НОД двух чисел, предложенного Евклидом и названного в его честь *алгоритмом Евклида.*

Пусть $a > b$ — положительные целые числа и b не делит a. Применяя теорему о делении с остатком, получим ряд равенств

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\ldots\ldots\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_nq_{n+1}, \end{aligned} \qquad (*)$$

где

$$b > r_1 > r_2 > \ldots > r_{n-1} > r_n > 0. \qquad (**)$$

Цепочка равенств $(*)$ называется алгоритмом Евклида для чисел a и b. Ввиду неравенств $(**)$ алгоритм Евклида $(*)$ обязательно закончится.

(4) Следующая теорема дает способ нахождения НОД двух целых чисел.

Теорема 1. *Пусть $a > b$ — положительные целые числа и b не делит a. Тогда* НОД(a,b) *равен последнему ненулевому остатку в алгоритме Евклида.*

Приведем важное свойств НОД целых чисел.

Теорема 2 (о линейном выражении НОД через исходные числа). *Пусть $a \geqslant b$ — положительные целые числа. Существуют целые числа k и m такие, что* НОД$(a,b) = a \cdot k + b \cdot m$.

Следствие 1. *Пусть a и b — целые числа и $d = \text{НОД}(a, b)$. Если t — общий делитель чисел a и b, то $t \mid d$.*

§3. Взаимно простые числа

(1) Два целых числа называются *взаимно простыми*, если их наибольший общий делитель равен 1.

Очевидно, что если $d = \text{НОД}(a, b)$, то числа $\frac{a}{d}$ и $\frac{b}{d}$ взаимно просты.

Критерий взаимной простоты двух целых чисел дает следующая

Лемма 1. *Два целых числа a и b взаимно просты тогда и только тогда, когда существуют целые числа k и m такие, что $ak + bm = 1$.*

(2) Свойства взаимно простых чисел.

Лемма 2. *Справедливы следующие утверждения:*

1) *если целые числа a_1 и a_2 взаимно просты с целым числом b, то их произведение a_1a_2 также взаимно просто с b;*

2) *если произведение двух целых чисел a и b делится на целое число c и числа b и c взаимно просты, то a делится на c;*

3) *если целое число a делится на взаимно простые числа b_1 и b_2, то a делится и на их произведение b_1b_2;*

4) *если каждое из целых чисел $a_1, a_2, \ldots, a_k$ взаимно просто с числом b, то произведение $a_1a_2 \ldots a_k$ взаимно просто с числом b;*

5) *если каждое из целых чисел $a_1, \ldots, a_k$ взаимно просто с каждым из чисел $b_1, b_2, \ldots, b_m$, то их произведения $a_1a_2 \ldots a_k$ и $b_1b_2 \ldots b_m$ взаимно просты;*

6) *если целые числа a и b взаимно просты, то для любых натуральных чисел k и n числа a^k и b^n взаимно просты.*

§4. Простые числа и их свойства

(1) Натуральное число, большее 1, называется *простым числом*, если оно не имеет других натуральных делителей кроме себя и единицы. Так, 2, 3, 5, 7, 11 — простые числа. Натуральные числа, отличные от 1 и простых чисел, называются *составными числами*. Составное число всегда можно представить в виде произведения двух натуральных чисел, отличных от 1.

(2) Свойства простых чисел.

Лемма 1. *Справедливы следующие утверждения:*

1) *всякое натуральное число, отличное от* 1, *делится по крайней мере на одно простое число;*

2) *множество всех простых чисел бесконечно;*

3) *если целое число* n *не делится на простое число* p, *то* n *и* p *взаимно просты;*

4) *если* p_1 *и* p_2 — *различные простые числа, то они взаимно просты;*

5) *если произведение нескольких натуральных чисел делится на простое число* p, *то хотя бы один из сомножителей делится на* p.

§5. Основная теорема арифметики

(1) **Теорема 1.** *Всякое натуральное число, большее* 1, *либо является простым, либо может быть представлено в виде произведения простых чисел и притом единственным образом.*

(2) По основной теореме арифметики всякое ненулевое целое число $a \neq \pm 1$ можно единственным образом представить в виде $a = \pm p_1 \dots p_n$, где $n \in \mathbb{N}$, $p_1 \leqslant \dots \leqslant p_n$. Простые числа в таком разложении могут повторяться. Пусть простое число p_1 встречается α_1 раз,..., p_k — α_k раз, где $p_1, \dots, p_k$ — различные простые числа, $k \in \mathbb{N}$. Разложение числа a в виде

$$a = \pm p_1^{\alpha_1} \dots p_k^{\alpha_k},$$

где $k \in \mathbb{N}$, $p_1 < \dots < p_k$ — простые числа, называется *каноническим разложением* целого числа a.

§6. Наименьшее общее кратное целых чисел и его свойства

(1) Пусть $a_1, a_2, \dots, a_k$ — целые числа, отличные от нуля. Всякое целое число, кратное каждому a_i, $i = 1, \dots, k$, называется их *общим кратным*. Наименьшее положительное из общих кратных чисел $a_1, a_2, \dots, a_k$ называется их *наименьшим общим кратным* и обозначается $\text{НОК}(a_1, a_2, \dots, a_k)$.

Если $m_2 = \text{НОК}(a_1, a_2), m_3 = \text{НОК}(m_2, a_3), \dots, m_k = \text{НОК}(m_{k-1}, a_k)$, то $\text{НОК}(a_1, \dots, a_k) = m_k$. Таким образом, задача нахождения НОК нескольких целых чисел сводится к аналогичной задаче нахождения НОК двух целых чисел.

(2) Из определения НОК очевидны следующие свойства:

1) $\text{НОК}(a_1, a_2)$ не определено, если хотя бы одно из чисел a_1, a_2 равно нулю;

2) $\text{НОК}(a_1, a_2) = \text{НОК}(|a_1|, |a_2|)$;

3) если $a_1 \mid a_2$, то $\text{НОК}(a_1, a_2) = |a_2|$.

Свойство 2) позволяет при изучении $\text{НОК}(a, b)$ рассматривать только натуральные числа a, b.

Теорема 1. *Если a и b — натуральные числа, то $a \cdot b = \text{НОД}(a, b) \cdot \text{НОК}(a, b)$.*

Если в каноническом разложении числа допустить существование простого числа с нулевым показателем, то нетрудно доказать следующее утверждение.

Теорема 2. *Пусть $a_1, \ldots, a_k$ — целые числа, отличные от нуля,*

$$\begin{aligned} a_1 &= \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \\ a_2 &= \pm p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}, \\ &\ldots\ldots\ldots\ldots\ldots \\ a_k &= \pm p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n} \end{aligned}$$

— их канонические разложения. Тогда

$$\text{НОД} = (a_1, \ldots, a_k) = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_n^{\lambda_n},$$

где $\lambda_i = \min\{\alpha_i, \beta_i, \ldots, \gamma_i\}$, $i = 1, \ldots, n$, а

$$\text{НОК}(a_1, \ldots, a_n) = p_1^{\mu_1} p_2^{\mu_2} \ldots p_n^{\mu_n},$$

где $\mu_i = \max\{\alpha_i, \beta_i, \ldots, \gamma_i\}$, $i = 1, \ldots, n$.

§7. Сравнения и их свойства

(1) Пусть m — фиксированное натуральное число, a и b — произвольные целые числа. Говорят, что число a *сравнимо с b по модулю m*, и пишут $a \equiv b \pmod m$, если $(a - b) \vdots m$.

Теорема 1. *Два целых числа a и b сравнимы по модулю m тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m.*

(2) Свойства сравнений, не связанные с модулем.

Из теоремы 1 легко следует

Лемма 1. *Пусть $m \in \mathbb{N}$, a, b, $c \in \mathbb{Z}$. Справедливы следующие утверждения:*

1) $a \equiv a \pmod m$;

2) *если* $a \equiv b \pmod m$, *то* $b \equiv a \pmod m$;

3) *если* $a \equiv b \pmod m$, $b \equiv c \pmod m$, *то* $a \equiv c \pmod m$.

Важные свойства дает

Лемма 2. *Сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать.*

Из леммы 2 следует ряд новых свойств сравнений.

Лемма 3. *Пусть* $m \in \mathbb{N}$, a, b, $c \in \mathbb{Z}$. *Справедливы следующие утверждения:*

1) *если* $a \equiv b \pmod m$, *то* $a^n \equiv b^n \pmod m$ *для любого* $n \in \mathbb{N}$;

2) *если* $a \equiv b \pmod m$, *то* $a+c \equiv b+c \pmod m$, $ac \equiv bc \pmod m$;

3) *если* $a + c \equiv b \pmod m$, *то* $a \equiv b - c \pmod m$.

(3) Свойства сравнений, связанные с модулем.

Лемма 4. *Пусть* $m \in \mathbb{N}$, a, b, $c \in \mathbb{Z}$. *Если* $ac \equiv bc \pmod m$ *и* $d = \text{НОД}(c, m)$, *то* $a \equiv b \pmod{\frac{m}{d}}$.

При $d = c$ из леммы 4 получаем

Следствие 1. *Обе части сравнения и модуль можно разделить на любой их натуральный общий делитель.*

При $d = 1$ из леммы 4 получим

Следствие 2. *Обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.*

§8. Кольцо классов вычетов

(1) **Лемма 1.** *Пусть* $m \in \mathbb{N}$. *Каждое целое число сравнимо по модулю* m *точно с одним из чисел ряда* $0, 1, \ldots, m-1$, *а именно, с остатком от деления этого числа на* m.

(2) Пусть m — натуральное число. Все целые числа по отношению к m можно разбить на m классов, если отнести к одному классу числа, дающие один и тот же остаток при делении на m. По лемме 1 каждое целое число попадет точно в один такой класс. Эти классы называют *классами вычетов по модулю* m. Класс вычетов по модулю m, содержащий число a, обозначим $\overline{a}$.

По теореме 1 из §7 класс вычетов состоит из целых чисел, сравнимых между собой по модулю m. В связи с этим равенство классов $\overline{a} = \overline{b}$ равносильно сравнению $a \equiv b \pmod m$. Так как остатки при делении целых чисел на m есть числа ряда $0, 1, \ldots, m-1$, то классы вычетов по модулю m удобнее записывать в виде $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. Множество всех

классов вычетов по модулю m принято обозначать символом $\mathbb{Z}_m$, т.е.

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

(3) Определим на $\mathbb{Z}_m$ сложение и умножение классов вычетов следующим образом:

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}. \qquad (*)$$

Теорема 1. *Пусть $m \in \mathbb{N}$. Множество $\mathbb{Z}_m$ классов вычетов по модулю m с операциями сложения и умножения $(*)$ является коммутативным кольцом с единицей.*

Кольцо $\mathbb{Z}_m$ называют *кольцом классов вычетов по модулю m.*

(4) Составим таблицы сложения и умножения для кольца $\mathbb{Z}_4$. Так как $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, то

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

На пересечении строки $\overline{a}$ и столбца $\overline{b}$ в таблицах стоят сумма $\overline{a} + \overline{b}$ и произведение $\overline{a} \cdot \overline{b}$ классов вычетов.

Обратим внимание на то, что $\overline{2} \cdot \overline{2} = \overline{0}$, т. е. в кольце $\mathbb{Z}_4$ имеются делители нуля, а значит, $\mathbb{Z}_4$ не является полем. Возникает вопрос: может ли кольцо $\mathbb{Z}_m$ быть полем и при каких условиях?

(5) **Лемма 2.** *Элемент $\overline{a}$ кольца $\mathbb{Z}_m$ имеет в $\mathbb{Z}_m$ обратный элемент тогда и только тогда, когда числа a и m взаимно просты.*

Следующая теорема дает ответ на вопрос, поставленный выше.

Теорема 2. *Кольцо классов вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число.*

§9. Функция Эйлера

(1) *Функция Эйлера $\varphi(n)$* определена на множестве $\mathbb{N}$ всех натуральных чисел и представляет собой число чисел ряда $0, 1, \ldots, n-1$, взаимно простых с числом n.

Например, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

(2) **Лемма 1.** *Если $n \in \mathbb{N}$ и p — простое число, то $\varphi(p^n) = p^n - p^{n-1}$.*

Следствие. *Если p — простое число, то $\varphi(p) = p - 1$.*

Функция Эйлера обладает *свойством мультипликативности*: если натуральные числа a и b взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$. Это свойство позволяет получить правило вычисления значений функции Эйлера.

Теорема 1. *Если $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение натурального числа a, то*

$$\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

или

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

(3) Одно из приложений функции Эйлера, важное для теории сравнений, дает

Теорема Эйлера. *Если a и m — взаимно простые натуральные числа, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Следствие (теорема Ферма). *Если a — натуральное число, p — простое число, то $a^p \equiv a \pmod{p}$.*

Тема 3. Комплексные числа

§1. Построение поля комплексных чисел

(1) Рассмотрим множество упорядоченных пар действительных чисел

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Пары (a, b) и (c, d) считаются *равными* (пишут $(a, b) = (c, d)$), если $a = c$ и $b = d$.

Введем на множестве $\mathbb{C}$ операцию сложения

$$(a, b) + (c, d) = (a + c, b + d).$$

Лемма 1. *Множество $\mathbb{C}$ — аддитивная абелева группа.*

(2) Операцию умножения на множестве $\mathbb{C}$ введем следующим образом:

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Лемма 2. *Множество $\mathbb{C}^{\#} = \mathbb{C} \setminus \{(0, 0)\}$ — мультипликативная абелева группа.*

(3) **Лемма 3.** *Для элементов множества* $\mathbb{C}$ *выполняются законы дистрибутивности, т. е. для любых* (a,b), (c,d), $(f,h) \in \mathbb{C}$ *справедливы равенства*

$$\big((a,b)+(c,d)\big)(f,h) = (a,b)(f,h) + (c,d)(f,h)$$

и

$$(f,h)\big((a,b)+(c,d)\big) = (f,h)(a,b) + (f,h)(c,d).$$

Из лемм 1, 2 и 3 следует

Теорема 1. *Множество* $\mathbb{C}$ *с операциями сложения и умножения пар*

$$(a,b)+(c,d) = (a+c, b+d),$$
$$(a,b)\cdot(c,d) = (ac-bd, ad+bc)$$

является полем.

Построенное поле $\mathbb{C}$ называют *полем комплексных чисел*, а пары $(a,b) \in \mathbb{C}$, — комплексными числами.

§2. Комплексные числа в алгебраической форме

(1) Так как пары $(a,0)$ из поля $\mathbb{C}$, $a \in \mathbb{R}$, складываются и умножаются как действительные числа, то положим $(a,0) = a$. Пару $(0,1)$ обозначим через i и назовем *мнимой единицей*. Ее основное свойство: $i^2 = -1$. Нетрудно проверить, что пара $(0,b) = (b,0)\cdot(0,1) = bi$ для любого $b \in \mathbb{R}$.

В таких обозначениях любое комплексное число $(a,b) = (a,0) + (0,b) = a + bi$. Запись комплексного числа (a,b) в виде $a+bi$ будем называть его *алгебраической формой*. Число a называют *действительной частью* комплексного числа $z = a+bi$, а bi — его *мнимой частью*. Комплексное число $z = bi$ называют *чисто мнимым комплексным числом.*

(2) Таким образом, поле комплексных чисел

$$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R},\ i^2 = -1\}.$$

Согласно с действиями над комплексными числами в виде пар определяются и действия над комплексными числами в алгебраической форме: Для любых чисел $z_1 = a+bi$ и $z_2 = c+di$:

2.1) $z_1 = z_2$, если $a = c$ и $b = d$;

2.2) $z_1 + z_2 = (a + c) + (b + d)i$;

2.3) $z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$.

Нетрудно заметить, что для вычисления произведения $z_1 \cdot z_2$ надо перемножить их как двучлены, заменить i^2 на -1 и выделить действительную и мнимую части.

(3) Для комплексного числа $z = a + bi$ число $a - bi$ называется *сопряженным* и обозначается $\overline{z}$. Очевидно, что $\overline{z} = z$ тогда и только тогда, когда число $z \in \mathbb{R}$.

Лемма 1. *Сумма и произведение двух сопряженных комплексных чисел являются действительными числами.*

Свойства умножения сопряженных комплексных чисел лежит в основе деления комплексных чисел в алгебраической форме:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

(4) Существует формула извлечения квадратного корня из комплексного числа $z = a + bi$

$$\sqrt{a + bi} = \pm \left(\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i \operatorname{sign} b \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \right),$$

где

$$\operatorname{sign} b = \begin{cases} 1, & \text{если } b \geqslant 0, \\ -1, & \text{если } b < 0. \end{cases}$$

В частности, из этой формулы следует:

4.1) если $a > 0$, $b = 0$, то $\sqrt{a} = \pm\sqrt{a}$;

4.2) если $a < 0$, $b = 0$, то $\sqrt{a} = \pm i\sqrt{-a}$;

4.3) если $a = 0$, $b \neq 0$, то $\sqrt{bi} = \pm\sqrt{\frac{|b|}{2}}\,(1 + i \operatorname{sign} b)$.

(5) Если $ax^2 + bx + c = 0$ — квадратное уравнение над полем $\mathbb{C}$, т. е. a, b, $c \in \mathbb{C}$ и $a \neq 0$, то, повторяя вывод формулы корней квадратного уравнения, который известен из школьного курса математики, получим ту же формулу

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

§3. Тригонометрическая форма комплексного числа

(1) В связи с геометрической интерпретацией действительных чисел естественно комплексное число $z = a + bi$ изображать точкой на плоскости, приняв числа a и b за координаты точки. При этом каждому комплексному числу соответствует точка на плоскости и каждой точке на плоскости соответствует некоторое комплексное число.

Плоскость, на которой изображаются комплексные числа, называется *комплексной плоскостью*. Ось абсцисс называется *действительной осью*, ось ординат — *мнимой осью*.

(2) Положение комплексного числа $z = a + bi$ на плоскости вполне определяется полярными координатами r и φ соответствующей точки на плоскости, где r — расстояние от начала координат до точки z, а φ — угол между положительным направлением оси Ox и вектором $\overline{Oz}$. Число r называется *модулем комплексного числа* z и обозначается $|z|$. Очевидно, что $r = |z| \geqslant 0$, причем $|z| = 0$ лишь для комплексного числа $z = 0$. Угол φ называется *аргументом комплексного числа* z и обозначается $\arg z$. Единственное число, для которого аргумент не определен, — число $z = 0$. Принято считать, что аргументом числа $z = 0$ может быть любое действительное число. Для других комплексных чисел аргумент определяется с точностью до целых кратных числа 2π и может принимать как положительные, так и отрицательные действительные значения. При этом положительные углы отсчитываются против часовой стрелки.

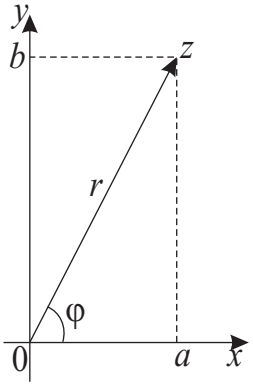


Рис. 1:

Поскольку полярные координаты точки, соответствующей комплексному числу $z = a + bi$, связаны с ее прямоугольными координатами известными формулами

$$a = r\cos\varphi, \qquad b = r\sin\varphi, \tag{$*$}$$

то $z = a + bi = r\cos\varphi + ir\sin\varphi = r(\cos\varphi + i\sin\varphi)$. Запись комплексного числа $z = r(\cos\varphi + i\sin\varphi)$, где $r = |z|$, $\varphi = \arg z$, называется *тригонометрической формой комплексного числа* z.

Для перехода от алгебраической формы комплексного числа $z = a + bi$ к тригонометрической форме используют формулы: $r = |z| =$

$= \sqrt{a^2 + b^2}$, а $\varphi = \arg z$ определяют из системы

$$\begin{cases} \cos\varphi = \frac{a}{|z|}, \\ \sin\varphi = \frac{b}{|z|}. \end{cases}$$

На практике для нахождения одного из значений аргумента комплексного числа $z = a + bi$ часто удобно изобразить комплексное число на плоскости и использовать следующие правила:

1) если число z изображается на действительной или мнимой оси, то в качестве $\arg z$ можно взять одно из значений 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ в соответствии с расположением числа z;

2) если число z изображается не на осях, то

$$\arg z = \begin{cases} \operatorname{arctg}\frac{b}{a}, & \text{если } z \in \text{I или IV четвертям;} \\ \pi + \operatorname{arctg}\frac{b}{a}, & \text{если } z \in \text{II или III четвертям.} \end{cases}$$

(3) Тригонометрическая форма комплексных чисел удобна для их умножения и деления.

Теорема 1. *При умножении комплексных чисел в тригонометрической форме их модули перемножаются, а аргументы складываются.*

Теорема 2. *При делении комплексных чисел в тригонометрической форме их модули делятся, а аргументы вычитаются.*

Следствие 1. *Для ненулевого комплексного числа* z

$$z^{-1} = \frac{1}{|z|}\big(\cos(-\arg z) + i\sin(-\arg z)\big).$$

(4) С помощью тригонометрической формы легко вычислить любую целую степень комплексного числа.

Теорема 3. *При возведении комплексного числа* $z = |z|(\cos\varphi + i\sin\varphi)$ *в степень с целым показателем* n *его модуль возводится в эту степень, а аргумент умножается на показатель:*

$$\big(|z|(\cos\varphi + i\sin\varphi)\big)^n = |z|^n(\cos n\varphi + i\sin n\varphi).$$

Это равенство называется *формулой Муавра.*

При $|z| = 1$ из формулы Муавра имеем равенство

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi,$$

которое позволяет вычислять косинусы и синусы кратных углов $n\varphi$ через синусы и косинусы угла φ.

(5) Пусть n — натуральное число, большее 1. *Корнем n-ой степени* из комплексного числа z называется такое комплексное число c, что $c^n = z$. Корень n-ой степени из комплексного числа z будем обозначать $\sqrt[n]{z}$.

Теорема 4. *Пусть n — натуральное число, большее 1, и $z = |z|(\cos\varphi + i\sin\varphi)$ — комплексное число. В поле комплексных чисел корень n-ой степени из z при $z = 0$ имеет единственное значение $\sqrt[n]{z} = 0$, а при $z \neq 0$ — n различных значений*

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right),$$

где $k = 0, 1, \ldots, n-1$.

(6) Так как $1 = \cos 0 + i\sin 0$, то из теоремы 4 получаем

Следствие 1. *В поле комплексных чисел имеется n различных значений корня n-ой степени из единицы, которые вычисляются по формуле*

$$\varepsilon_k = \sqrt[n]{1} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n},$$

где $k = 0, 1, \ldots, n-1$.

Теорема 5. *Корни n-ой степени из единицы образуют конечную мультипликативную группу порядка n, каждый элемент которой есть степень корня $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.*

(7) Теорема 4 показывает, что любое уравнение вида $x^n - z = 0$, где z — произвольное комплексное число, имеет в поле $\mathbb{C}$ n различных решений. Еще удивительнее то, что в $\mathbb{C}$ имеет решение любое алгебраическое уравнение с комплексными коэффициентами.

Теорема 6 (основная теорема алгебры комплексных чисел). *Всякое алгебраическое уравнение*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

где $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, имеет в поле $\mathbb{C}$ хотя бы одно решение.

Эта теорема является одним из крупнейших достижений в истории развития алгебры. Раньше ее называли основной теоремой алгебры, так как решение алгебраических уравнений долгое время было в центре внимания алгебраистов. Первое доказательство этой теоремы было дано Гауссом в 1799 году.

Тема 4. Матрицы и определители

§1. Матрицы и действия над ними

① Пусть P — произвольное поле, k и n — натуральные числа. Прямоугольная таблица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kj} & \dots & a_{kn} \end{pmatrix},$$

составленная из элементов поля P, называется *матрицей размера* $k \times n$ *над полем* P. Для обозначения матрицы A будем употреблять также запись $A = (a_{ij})$, $i = 1, \dots, k$, $j = 1, \dots, n$. Элементы a_{ij}, из которых составлена матрица, называются *элементами матрицы*. Элементы $a_{i1}, a_{i2}, \dots, a_{in}$ имеют первым индексом число i и составляют в матрице A i-ю строку. Элементы $a_{1j}, a_{2j}, \dots, a_{kj}$ имеют вторым индексом число j и составляют в матрице A j-й столбец. Таким образом, размер матрицы $k \times n$ указывает число строк и число столбцов матрицы. Если $k \neq n$, то говорят о *прямоугольной матрице*. Если $k = 1$, то матрицу называют *матрицей-строкой*, а если $n = 1$, — то *матрицей-столбцом*. Матрица размера $k \times n$, все элементы которой нулевые, называется *нулевой матрицей* и обозначается $O_{k,n}$. Если же $k = n$, т. е. число строк матрицы равно числу ее столбцов, то матрица называется *квадратной матрицей порядка* n, а множество всех таких матриц обозначается $M_n(P)$.

Пусть $A = (a_{ij})$ — квадратная матрица порядка n над полем P. Элементы $a_{11}, a_{22}, \dots, a_{nn}$ в такой матрице составляют *главную диагональ*, другая диагональ квадратной матрицы называется *побочной диагональю*. Если в квадратной матрице все элементы, кроме элементов главной диагонали, равны нулю, то матрицу называют *диагональной* и обозначают $\operatorname{diag}(a_{11}, a_{22}, \dots, a_{nn})$. Диагональная матрица называется *единичной матрицей порядка* n, если она имеет вид

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

Две матрицы $A = (a_{ij})$ и $B = (b_{ij})$ над полем P называются *равными*, если они имеют одинаковый размер и равны элементы, стоящие на одинаковых местах, т.е. $a_{ij} = b_{ij}$ для всех i, j.

(2) Если $A = (a_{ij})$ и $B = (b_{ij})$ — матрицы размера $k \times n$ над полем P, то их *суммой* будем называть матрицу $C = (c_{ij})$ размера $k \times n$ над полем P, у которой элементы $c_{ij} = a_{ij} + b_{ij}$ для $i = 1, \ldots, k$, $j = 1, \ldots, n$. Пишут: $C = A + B$.

Пример. $\begin{pmatrix} 2 & -1 & 3 \\ 0 & -2 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 4 & -3 \\ 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 0 \\ 2 & -1 & 6 \end{pmatrix}$.

Свойства сложения матриц сформулируем в следующей лемме

Лемма 1. *Пусть A, B и C — матрицы размера $k \times n$ над полем P. Справедливы следующие утверждения:*

1) $A + (B + C) = (A + B) + C$;

2) $A + B = B + A$;

3) $A + O_{k,n} = O_{k,n} + A = A$.

(3) Если $A = (a_{ij})$ — матрица размера $k \times n$ над полем P и α — элемент поля P, то *произведением матрицы A на элемент α* называется матрица $B = (b_{ij})$ размера $k \times n$ над полем P, у которой $b_{ij} = \alpha a_{ij}$ для $i = 1, \ldots, k$, $j = 1, \ldots, n$. Пишут: $B = \alpha A$.

Пример. $4\begin{pmatrix} -1 & 2 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} -4 & 8 \\ 0 & -8 \end{pmatrix}$.

Матрица $(-1)A$ обозначается $(-A)$ и называется *противоположной матрице* A. Таким образом, можно определить вычитание матриц одинакового размера: $A - B = A + (-B)$.

Лемма 2. *Пусть A и B — матрицы размера $k \times n$ над полем P, α и β — элементы поля P. Справедливы следующие утверждения:*

1) $A + (-A) = (-A) + A = O_{k,n}$;

2) $(\alpha\beta)A = \alpha(\beta A) = \beta(\alpha A)$;

3) $\alpha(A + B) = \alpha A + \alpha B$;

4) $(\alpha + \beta)A = \alpha A + \beta A$.

(4) Пусть $A = (a_{ij})$ — матрица размера $k \times n$ над полем P, $B = (b_{ij})$ — матрица размера $n \times m$ над полем P. *Произведением матриц* A и B называется матрица $C = (c_{ij})$ размера $k \times m$ над полем P, у которой $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj} = \prod\limits_{t=1}^{n} a_{it}b_{tj}$ для $i = 1, \ldots, k$, $j = 1, \ldots, m$. Пишут: $C = AB$.

Пример. Пусть

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

Так как A — матрица размера 2×2, B — матрица размера 2×3, то произведение AB определено, а произведение BA не определено.

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

$$= \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 & 1 \cdot 4 + 2 \cdot 3 & 1 \cdot (-1) + 2 \cdot 0 \\ 1 \cdot 1 + 0 \cdot 2 & 1 \cdot 4 + 0 \cdot 3 & 1 \cdot (-1) + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 5 & 10 & -1 \\ 1 & 4 & -1 \end{pmatrix}$$

Лемма 3. *Справедливы следующие утверждения:*

1) *умножение матриц некоммутативно, т.е.* $AB \neq BA$;

2) *если определено одно из произведений* $A(BC)$, $(AB)C$, *то определено и другое, причем* $A(BC) = (AB)C$;

3) *если* A *— матрица размера* $k \times n$, *то* $AE_n = E_k A = A$.

Лемма 4. *Справедливы следующие утверждения:*

1) *если определена матрица* $A(B+C)$, *то* $A(B+C) = AB + AC$;

2) *если определена матрица* $(A+B)C$, *то* $(A+B)C = AC + BC$.

(5) Нетрудно заметить, что если A, B, $C \in M_n(P)$, то матрицы $A(BC)$, $(AB)C$, $A(B+C)$, $(A+B)C$ определены и также являются квадратными порядка n.

Из лемм 1, 2, 3 и 4 следует

Теорема 1. *Пусть* P *— поле,* $n \in \mathbb{N}$. *Множество* $M_n(P)$ *образует кольцо с единицей, которое называется* полным матричным кольцом над полем P.

(6) Если в матрице A строки сделать столбцами, то получится матрица, которую называют *транспонированной к матрице* A и обозначают A^T. Так, если

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}, \qquad \text{то} \qquad A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{k1} \\ a_{12} & a_{22} & \dots & a_{k2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{kn} \end{pmatrix}.$$

Свойства транспонирования матриц, сформулируем в следующей лемме

Лемма 5. *Справедливы следующие утверждения:*

1) $(A^T)^T = A$;

2) $(\alpha A)^T = \alpha A^T$ *для любого элемента* α *из поля* P;

3) $(A+B)^T = A^T + B^T$;

4) $(AB)^T = B^T \cdot A^T$.

(7) Пусть A — произвольная матрица над полем P.

Элементарными преобразованиями строк матрицы A называют следующие преобразования:

1) умножение всех элементов какой-либо строки матрицы A на ненулевой элемент поля;

2) прибавление ко всем элементам какой-либо строки соответствующих элементов другой строки, умноженных на один и тот же элемент поля.

Если матрица B получена из матрицы A в результате одного или нескольких элементарных преобразований строк, то говорят, что матрица A *эквивалентна* матрице B и пишут: $A \sim B$.

Лемма 6. *С помощью элементарных преобразований строк можно поменять местами любые две строки матрицы.*

Лемма 7. *Если* $A \sim B$, *то* $B \sim A$.

(8) *Ступенчатой* называется матрица, обладающая следующими свойствами:

1) если i-я строка матрицы нулевая, т. е. состоит из одних нулей, то $(i+1)$-я строка также нулевая;

2) если первые ненулевые элементы i-й и $(i+1)$-й строк расположены в столбцах с номерами k и l, то $k < l$.

Теорема 2. *Всякую матрицу с помощью элементарных преобразований строк можно привести к ступенчатой матрице.*

§2. Перестановки

(1) Пусть $X = \{1, 2, \ldots, n\}$. Взаимно однозначное отображение множества X на себя называется *перестановкой степени* n. Множество всех перестановок степени n обозначается S_n. Перестановки удобно изображать двухстрочной таблицей

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix},$$

указывая во второй строке образы всех элементов, причем $\{\tau(1), \tau(2), \ldots$ $\ldots, \tau(n)\} = X$. Тождественное отображение

$$\varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

называют *тождественной* (или *единичной*) перестановкой.

Определим на множестве S_n умножение перестановок следующим правилом: для любых $\sigma, \tau \in S_n$

$$(\sigma\tau)(i) = \sigma(\tau(i))$$

для $i = 1, 2, \ldots, n$.

Например,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

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

В частности, этот пример показывает, что $\sigma\tau \neq \tau\sigma$, т. е. умножение перестановок некоммутативно.

(2) **Теорема 1.** *Пусть $n \in \mathbb{N}$. Множество S_n с операцией умножения перестановок является конечной группой порядка $n!$. Эту группу называют* симметрической группой степени n.

Пример. $S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \varepsilon \right\}$. $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \varepsilon, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.
$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$.

(3) Перестановка из группы S_n вида

$$\tau = \begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k & a_{k+1} & \ldots & a_n \\ a_2 & a_3 & \ldots & a_k & a_1 & a_{k+1} & \ldots & a_n \end{pmatrix}$$

называется *циклом длины k* и кратко записывается $\tau = (a_1 a_2 \ldots \ldots a_k)(a_{k+1}) \ldots (a_n) = (a_1 a_2 \ldots a_k)$. Циклы без общих символов называются *независимыми*. Циклы с общими символами называются *зависимыми*. Любую перестановку можно записать в виде произведения независимых циклов. Например,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 1 & 4 & 8 & 7 & 6 \end{pmatrix} = (154)(23)(68)(7).$$

Заметим, что произведение независимых циклов коммутативно, а произ-

ведение зависимых циклов некоммутативно. Например,

$$(12)(13) = (132), \qquad \text{а} \qquad (13)(12) = (123).$$

Цикл длины 2 называется *транспозицией*. Непосредственной проверкой нетрудно убедиться, что цикл длины k можно записать в виде произведения $(k-1)$ транспозиций по правилу:

$$(a_1 a_2 \dots a_{k-1} a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2).$$

Теорема 2. *Всякую перестановку из группы S_n можно записать в виде произведения $(n-c)$ транспозиций, где c — число независимых циклов.*

(4) Для введения знака перестановки нам понадобится функция

$$\operatorname{sign} a = \begin{cases} 1, & \text{если } a \geqslant 0, \\ -1, & \text{если } a < 0 \end{cases}$$

для всех $a \in \mathbb{R}$. Отметим одно из свойств этой функции: для всех $a, b \in \mathbb{R}$ $\operatorname{sign}(ab) = \operatorname{sign} a \cdot \operatorname{sign} b$.

Рассмотрим отображение $\operatorname{sgn} : S_n \to \{-1, 1\}$, считая

$$\operatorname{sgn} \tau = \begin{cases} 1, & \text{если } \tau \in S_1; \\ \prod\limits_{\substack{\{i,k\} \subseteq X \\ i \neq k}} \operatorname{sign} \frac{i-k}{\tau(i)-\tau(k)}, & \text{если } \tau \in S_n,\ n \geqslant 2. \end{cases}$$

Поскольку τ — взаимно однозначное отображение, то $\tau(i) \neq \tau(k)$ при $i \neq k$. Следовательно каждая дробь $\frac{i-k}{\tau(i)-\tau(k)}$ в формуле существует. Так как $\{i, k\} = \{k, i\}$, то дробь $\frac{i-k}{\tau(i)-\tau(k)} = \frac{k-i}{\tau(k)-\tau(i)}$ встречается в произведении только один раз и поэтому можно рассматривать только $\{i, k\}$, где $i > k$. Тогда

$$\operatorname{sign} \frac{i-k}{\tau(i)-\tau(k)} = \operatorname{sign} (\tau(i) - \tau(k))$$

и формулу для знака перестановки можно записать в виде

$$\operatorname{sgn} \tau = \begin{cases} 1, & \text{если } \tau \in S_1, \\ \prod\limits_{1 \leqslant k < i \leqslant n} \operatorname{sign} (\tau(i) - \tau(k)), & \text{если } n \geqslant 2. \end{cases}$$

Перестановку τ назовем *четной*, если $\operatorname{sgn} \tau = 1$, и *нечетной*, если $\operatorname{sgn} \tau = -1$.

(5) **Лемма 1.** *Единичная перестановка четная.*

Теорема 3. *Знак произведения перестановок равен произведению*

их знаков, т. е. для любых $\tau, \sigma \in S_n$ *имеет место равенство* $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma$.

Следствие 1. *Произведение двух четных или двух нечетных перестановок есть перестановка четная.*

Следствие 2. *Произведение четной и нечетной перестановок есть перестановка нечетная.*

Следствие 3. *Обратная перестановка* τ^{-1} *имеет ту же четность, что и перестановка* τ.

(6) **Теорема 4.** *Любая транспозиция нечетна.*

Удобный практический способ вычисления знака перестановки дает следующая теорема.

Теорема 5. *Если перестановка* τ *из группы* S_n *имеет* c *независимых циклов, то* $\operatorname{sgn}\tau = (-1)^{n-c}$.

(7) Множество всех четных перестановок из группы S_n обозначим A_n, т. е.

$$A_n = \{\tau \in S_n \mid \operatorname{sgn}\tau = 1\}.$$

Теорема 6. *Множество* A_n *относительно умножения перестановок образует группу, которую называют* знакопеременной группой степени n. *При* $n \geqslant 2$ *группа* A_n *имеет* $n!/2$ *перестановок.*

Пример. $A_1 = \left\{\begin{pmatrix}1\\1\end{pmatrix} = \varepsilon\right\}$. $A_2 = \left\{\begin{pmatrix}1&2\\1&2\end{pmatrix} = \varepsilon\right\}$. $A_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \varepsilon,\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123),\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132)\right\}$.

§3. Определители

Будем рассматривать только квадратные матрицы над числовым полем P.

(1) Пусть $n \in \mathbb{N}$ и $A = (a_{ij})$ — квадратная матрица порядка n. *Определителем* или (*детерминантом*) матрицы A называется число, которое обозначается $|A|$ или $\det A$ и вычисляется по формуле

$$|A| = \sum_{\tau \in S_n} \operatorname{sgn}\tau \; a_{1\tau(1)} a_{2\tau(2)} \ldots a_{n\tau(n)}. \qquad (*)$$

Определитель $|A|$ будем называть также *определителем* n*-го порядка.*

Из определения $|A|$ непосредственно следует:

1) в правой части равенства $(*)$ $n!$ слагаемых, так как суммирование ведется по всем элементам симметрической группы S_n;

2) в зависимости от четности перестановки τ каждое слагаемое имеет знак "+" или "−". Если $n \geqslant 2$, то число слагаемых со знаком "+" равно числу слагаемых со знаком "−";

3) каждое слагаемое $\operatorname{sgn}\tau\ a_{1\tau(1)}a_{2\tau(2)}\dots a_{n\tau(n)}$ содержит произведение n элементов матрицы A. Так как первые индексы элементов различны, то элементы взяты по одному из каждой строки матрицы. Поскольку вторые индексы $\tau(1), \tau(2), \dots, \tau(n)$ различны, то элементы взяты по одному из каждого столбца матрицы.

(2) Вычисление определителей малых порядков.

2.1) $n = 1$. $A = (a_{11})$ — квадратная матрица $1^{\underline{\text{го}}}$ порядка. $|A| = |a_{11}| = a_{11}$.

2.2) $n = 2$. $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ — квадратная матрица $2^{\underline{\text{го}}}$ порядка.

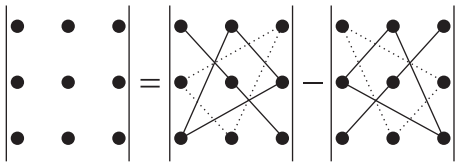
$$|A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

2.3) $n = 3$.

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} +$$

$$+a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Схема вычисления определителя третьего порядка называется "правилом треугольников"



(3) Свойства определителей.

Треугольной называется квадратная матрица, у которой все элементы ниже или выше главной диагонали равны нулю.

Свойство 1. *Определитель треугольной матрицы равен произведению элементов главной диагонали. В частности,* $|E_n| = 1$.

Свойство 2. *Определитель матрицы с нулевой строкой или нулевым столбцом равен нулю.*

Свойство 3. *При транспонировании матрицы определитель не изменяется, т.е.* $\det(A^T) = \det A$.

Свойство 4. *Общий множитель элементов строки (столбца) можно выносить за знак определителя.*

Следствие 1. *Если A — квадратная матрица порядка n и α — элемент поля, то* $\det(\alpha A) = \alpha^n \det A$.

Свойство 5. *Если каждый элемент k-й строки матрицы A есть сумма двух слагаемых $a_{kj} + \overline{a}_{kj}$, $j = 1, \ldots, n$, то определитель матрицы A равен сумме определителей двух матриц, у которых все строки, кроме k-ой, прежние, k-я строка первой матрицы состоит из первых слагаемых a_{kj}, а k-я строка второй матрицы — из вторых слагаемых $\overline{a}_{kj}$.*

Свойство 6. *Если матрица B получена из матрицы A с помощью перестановки двух строк (столбцов), то* $\det B = -\det A$.

Свойство 7. *Определитель матрицы с двумя одинаковыми строками (столбцами) равен нулю.*

Следствие 1. *Определитель матрицы с пропорциональными строками (столбцами) равен нулю.*

Свойство 8. *Определитель матрицы не изменится, если к элементам одной строки (одного столбца) матрицы прибавить соответствующие элементы другой строки (другого столбца), умноженные на один и тот же элемент поля.*

Свойства определителей используются для вычисления определителей.

Пример. Вычислить определитель

$$\Delta = \begin{vmatrix} -2 & 1 & 3 & 4 \\ 1 & -2 & 0 & 2 \\ -1 & 0 & 3 & -4 \\ 3 & 4 & -5 & 1 \end{vmatrix}.$$

Решение. С помощью свойств определителя приведем его к треугольному виду.

$$\Delta = \begin{vmatrix} -2 & 1 & 3 & 4 \\ 1 & -2 & 0 & 2 \\ -1 & 0 & 3 & -4 \\ 3 & 4 & -5 & 1 \end{vmatrix} \overset{\text{I ст} \leftrightarrows \text{II ст}}{=} - \begin{vmatrix} 1 & -2 & 3 & 4 \\ -2 & 1 & 0 & 2 \\ 0 & -1 & 3 & -4 \\ 4 & 3 & -5 & 1 \end{vmatrix} \overset{\substack{\text{II}+\text{I}\cdot 2 \\ \text{IV}+\text{I}\cdot(-4)}}{=}$$

$$= - \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -3 & 6 & 10 \\ 0 & -1 & 3 & -4 \\ 0 & 11 & -17 & -15 \end{vmatrix} \overset{\text{II} \leftrightarrows \text{III}}{=} \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -1 & 3 & -4 \\ 0 & -3 & 6 & 10 \\ 0 & 11 & -17 & -15 \end{vmatrix} \overset{\substack{\text{III}+\text{II}\cdot(-3) \\ \text{IV}+\text{II}\cdot 11}}{=}$$

$$= \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -1 & 3 & -4 \\ 0 & 0 & -3 & 22 \\ 0 & 0 & 16 & -59 \end{vmatrix} \overset{\text{IV}+\text{III}\cdot 5}{=} \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -1 & 3 & -4 \\ 0 & 0 & -3 & 22 \\ 0 & 0 & 1 & 51 \end{vmatrix} \overset{\text{III}\rightleftharpoons\text{IV}}{=}$$

$$= - \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -1 & 3 & -4 \\ 0 & 0 & 1 & 51 \\ 0 & 0 & -3 & 22 \end{vmatrix} \overset{\text{IV}+\text{III}\cdot 3}{=} - \begin{vmatrix} 1 & -2 & 3 & 4 \\ 0 & -1 & 3 & -4 \\ 0 & 0 & 1 & 51 \\ 0 & 0 & 0 & 175 \end{vmatrix} = 175.$$

(4) Клеточные матрицы и их определители.

Пусть $A = (a_{ij})$ — квадратная матрица порядка n, $B = (b_{ij})$ — квадратная матрица порядка m. Обозначим через

$$\begin{pmatrix} A & C \\ O & B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & c_{11} & \dots & c_{1m} \\ \dots\dots & & \dots\dots & \dots\dots & & \dots\dots \\ a_{n1} & \dots & a_{nn} & c_{n1} & \dots & c_{nm} \\ 0 & \dots & 0 & b_{11} & \dots & b_{1m} \\ \dots\dots & & \dots\dots & \dots\dots & & \dots\dots \\ 0 & \dots & 0 & b_{m1} & \dots & b_{mm} \end{pmatrix},$$

где $C = (c_{ij})$ — матрица размера $n \times m$, O — нулевая матрица размера $m \times n$. Аналогично можно построить матрицы

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

Все эти матрицы будем называть *клеточными*.

Правила вычисления определителей клеточных матриц дают следующие теоремы.

Теорема 1. $\det \begin{pmatrix} A & C \\ O & B \end{pmatrix} = \det \begin{pmatrix} A & O \\ C & B \end{pmatrix} = \det A \cdot \det B.$

Теорема 2. $\det \begin{pmatrix} O & A \\ B & C \end{pmatrix} = \det \begin{pmatrix} C & A \\ B & O \end{pmatrix} = (-1)^{nm} \det A \cdot \det B.$

(5) Важное свойство определителей дает следующая теорема.

Теорема 3. *Если A и B — квадратные матрицы порядка n, то* $\det(AB) = \det A \cdot \det B$.

(6) Миноры и алгебраические дополнения.

Пусть $A = (a_{ij})$ — квадратная матрица порядка n. *Минором* M_{kl} элемента a_{kl} матрицы A называется определитель матрицы, полученной из A вычеркиванием k-ой строки и l-го столбца. Произведение $A_{kl} = (-1)^{k+l} M_{kl}$ называется *алгебраическим дополнением* элемента a_{kl}. На-

пример, если

$$A = \begin{pmatrix} -1 & 3 & -2 \\ 0 & 1 & 4 \\ -2 & 5 & 0 \end{pmatrix}, \text{ то } M_{23} = \begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix} = 1, \ A_{23} = (-1)^{2+3} M_{23} = -1.$$

Лемма 1. *Если равны нулю все элементы некоторой строки (столбца) квадратной матрицы, кроме одного, то определитель матрицы равен произведению этого ненулевого элемента на его алгебраическое дополнение.*

Эта лемма позволяет доказать следующую теорему, дающую еще один способ вычисления определителей порядка $n \geqslant 2$.

Теорема 4. *Определитель квадратной матрицы равен сумме произведений элементов какой-либо строки (столбца) матрицы на их алгебраические дополнения.*

Таким образом, если $A = (a_{ij})$ — квадратная матрица порядка n, то

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}, \ i = 1, 2, \ldots, n;$$

или

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj}, \ j = 1, 2, \ldots, n.$$

Такой способ вычисления определителя называется *разложением по элементам i-й строки или j-го столбца.*

Теорема 5. *Сумма произведений элементов какой-либо строки (столбца) квадратной матрицы на алгебраические дополнения соответствующих элементов другой строки (столбца) равна нулю.*

§4. Обратная матрица

Продолжаем рассматривать только квадратные матрицы над числовым полем P.

(1) Квадратная матрица A порядка n называется *обратимой*, если существует матрица B такая, что $AB = BA = E_n$. В этом случае матрица B называется *обратной* матрице A и обозначается A^{-1}.

Из определения нетрудно заметить, что:

1) обратная матрица A^{-1} является квадратной матрицей порядка n;

2) матрица A является обратной матрице A^{-1}, т. е. $(A^{-1})^{-1} = A$.

Другие свойства обратимых матриц приведем в следующей лемме.

Лемма 1. *Справедливы следующие утверждения:*

1) *если матрица A обратима, то существует точно одна ей обратная матрица;*

2) *обратимая матрица невырождена, т. е. ее определитель отличен от нуля;*

3) *если A и B — обратимые матрицы порядка n, то матрица AB также обратима, причем $(AB)^{-1} = B^{-1}A^{-1}$.*

(2) Пусть $A = (a_{ij})$ — квадратная матрица порядка n. Матрица

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

называется *присоединенной* (или *взаимной*) матрицей к матрице A.

Критерий обратимости матрицы и способ вычисления обратной матрицы дает следующая теорема.

Теорема 1. *Квадратная матрица обратима тогда и только тогда, когда она невырождена. Если A — невырожденная матрица, то $A^{-1} = \frac{1}{|A|} \cdot A^{\vee}$.*

Пример. Найти матрицу, обратную матрице

$$A = \begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}$$

Решение. Вычислим $\det A = \begin{vmatrix} -1 & 2 \\ 1 & 1 \end{vmatrix} = -1 - 2 = -3$. Так как матрица A невырождена, то существует обратная матрица

$$A^{-1} = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}.$$

Нетрудно вычислить $A_{11} = 1$, $A_{12} = -1$, $A_{21} = -2$, $A_{22} = -1$. Следовательно,

$$A^{-1} = -\frac{1}{3} \begin{pmatrix} 1 & -2 \\ -1 & -1 \end{pmatrix}.$$

(3) Вычислить обратную матрицу можно также с помощью элементарных преобразований. Этот способ основан на следующей теореме.

Теорема 2. *Обратимую матрицу с помощью элементарных преобразований строк можно превратить в единичную матрицу. Применяя те же элементарные преобразования в том же порядке к единичной матрице, получим матрицу, обратную данной.*

Пример. С помощью элементарных преобразований строк найти матрицу, обратную матрице

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

Решение.

$$\left(\begin{array}{ccc|ccc} -1 & 1 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \overset{\substack{\text{II}+\text{I}\cdot 1 \\ \text{III}+\text{I}\cdot 2}}{\sim} \left(\begin{array}{ccc|ccc} -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 & 1 \end{array}\right) \sim$$

$$\overset{\text{II}\rightleftharpoons\text{III}}{\sim} \left(\begin{array}{ccc|ccc} -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \overset{\substack{\text{I}\cdot(-1) \\ \text{II}\cdot\frac{1}{2}}}{\sim} \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \overset{\text{II}+\text{III}\cdot\left(-\frac{1}{2}\right)}{\sim}$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \overset{\text{I}+\text{II}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right).$$

Таким образом,

$$A^{-1} = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 1 & 1 & 0 \end{pmatrix}.$$

④ Обозначим через $GL(n, P)$ множество всех невырожденных квадратных матриц порядка n с элементами из поля P.

Теорема 3. *Пусть n — натуральное число. Множество $GL(n, P)$ образует мультипликативную группу.*

Тема 5. Системы линейных уравнений

§1. Основные понятия

Рассмотрим совокупность k уравнений вида

$$(*) \qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kn}x_n = b_k, \end{cases}$$

где a_{ij}, b_i — элементы числового поля P, $x_1, x_2, \ldots, x_n$ — неизвестные. Совокупность уравнений $(*)$ называют *системой линейных уравнений* над

полем P с n неизвестными $x_1, x_2, \ldots, x_n$. Элементы a_{ij} называют *коэффициентами системы* $(*)$, b_j — *свободными коэффициентами*. Последовательность $(c_1, \ldots, c_n)$ чисел поля P называется *решением системы* $(*)$, если после подстановки их вместо неизвестных $x_1, \ldots, x_n$, соответственно, каждое уравнение системы обращается в верное числовое равенство. Система линейных уравнений $(*)$ называется *совместной*, если она имеет хотя бы одно решение, и *несовместной* — в противном случае. Две системы линейных уравнений с n неизвестными $x_1, x_2, \ldots, x_n$ называются *равносильными*, если множества их решений совпадают.

Матрица

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \end{pmatrix},$$

составленная из коэффициентов системы $(*)$, называется *матрицей системы*. Матрица

$$C = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} & b_k \end{array}\right)$$

называется *расширенной матрицей системы* $(*)$. Если обозначим через

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_k \end{pmatrix},$$

то систему $(*)$ можно записать в виде матричного уравнения $AX = B$.

§2. Метод Гаусса решения систем линейных уравнений

Метод Гаусса или *метод последовательного исключения неизвестных* до настоящего времени остается одним из лучших методов решения систем линейных уравнений.

В основе метода Гаусса лежат следующие два факта: 1) всякая система линейных уравнений равносильна некоторой *ступенчатой системе линейных уравнений*, т. е. системе линейных уравнений, у которой

расширенная матрица системы ступенчатая; 2) ступенчатая система линейных уравнений довольно просто решается.

(1) Пусть дана система k линейных уравнений с n неизвестными $x_1, x_2, \ldots, x_n$, коэффициенты которой принадлежат числовому полю P.

Элементарными преобразованиями системы линейных уравнений $(*)$ будем называть следующие преобразования:

1) умножение какого-либо уравнения на число, отличное от нуля;

2) прибавление к одному уравнению другого уравнения, умноженного на произвольное число.

Очевидно, что каждому элементарному преобразованию системы линейных уравнений соответствует аналогичное элементарное преобразование строк расширенной матрицы системы. Ввиду этого, утверждения, справедливые для элементарных преобразований строк матрицы, могут быть переформулированы и являются справедливыми для элементарных преобразований системы линейных уравнений. Таким образом, справедливы следующие леммы.

Лемма 1. *С помощью элементарных преобразований можно поменять местами любые два уравнения системы.*

Лемма 2. *Всякую систему линейных уравнений с помощью элементарных преобразований можно привести к ступенчатой системе.*

Лемма 3. *Элементарные преобразования системы линейных уравнений обратимы, т. е. если в результате элементарных преобразований из системы* $(*)$ *получилась система* $(**)$*, то из системы* $(**)$ *можно получить систему* $(*)$ *также в результате элементарных преобразований.*

Важную роль играет следующая теорема.

Теорема 1. *При элементарных преобразованиях система линейных уравнений переходит в равносильную систему.*

(2) Таким образом, ввиду леммы 2 и теоремы 1 всякую систему линейных уравнений с помощью элементарных преобразований можно привести к равносильной ступенчатой системе. Отметим, что вместо элементарных преобразований системы линейных уравнений можно выполнять элементарные преобразования строк расширенной матрицы. А приведя расширенную матрицу системы к ступенчатому виду, можно перейти к соответствующей ступенчатой системе.

Пусть расширенная матрица системы $(*)$ с помощью элементарных преобразований строк приведена к ступенчатой матрице A. Возможны следующие случаи:

2.1) Матрица

$$A = \left(\begin{array}{cccc|c} c_{11} & c_{12} & \dots & c_{1n} & d_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & d_l \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \end{array}\right).$$

Соответствующая ступенчатая система имеет вид

$$(**) \qquad \begin{cases} c_{11}x_1 + c_{12}x_2 + \ldots + c_{1n}x_n = d_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = d_l. \end{cases}$$

Очевидно, что последнее уравнение не имеет решений, поэтому система $(**)$, а значит, и система $(*)$ несовместна.

2.2) Матрица

$$A = \left(\begin{array}{ccccc|c} c_{11} & c_{12} & \dots & c_{1n-1} & c_{1n} & d_1 \\ 0 & c_{22} & \dots & c_{2n-1} & c_{2n} & d_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_{n-1n-1} & c_{n-1n} & d_{n-1} \\ 0 & 0 & \dots & 0 & c_{nn} & d_n \\ 0 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 \end{array}\right).$$

Соответствующая ступенчатая система имеет вид

$$(**) \qquad \begin{cases} c_{11}x_1 + c_{12}x_2 + \ldots + c_{1n-1}x_{n-1} + c_{1n}x_n = d_1, \\ \qquad\quad c_{22}x_2 + \ldots + c_{2n-1}x_{n-1} + c_{2n}x_n = d_2, \\ \qquad\qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad\qquad c_{n-1n-1}x_{n-1} + c_{n-1n}x_n = d_{n-1}, \\ \qquad\qquad\qquad\qquad\qquad c_{nn}x_n = d_n. \end{cases}$$

Из последнего уравнения находим x_n. Подставляя его в предпоследнее уравнение, найдем x_{n-1} и т. д. Таким образом, в этом случае система $(**)$, а значит, и система $(*)$ имеет единственное решение.

2.3) Матрица

$$A = \left(\begin{array}{cccccc|c} c_{11} & \dots & c_{1j-1} & c_{1j} & \dots & c_{1n} & d_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & c_{ij} & \dots & c_{in} & d_i \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{array}\right).$$

Соответствующая ступенчатая система имеет вид

$$(**)\qquad \begin{cases} c_{11}x_1 + \ldots c_{1j}x_j + \ldots + c_{1n}x_n = d_1, \\ \qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad c_{ij}x_j + \ldots + c_{in}x_n = d_i. \end{cases}$$

Неизвестные $x_1, \ldots, x_j$, которые первыми встречаются в уравнениях системы $(**)$, назовем *главными неизвестными*, а остальные — *свободными*. Перенося свободные неизвестные в правую часть равенств, получим следующую систему

$$\begin{cases} c_{11}x_1 + \ldots + c_{1j}x_j = d_1 - \ldots - c_{1n}x_n, \\ \qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad c_{ij}x_j = d_i - \ldots - c_{in}x_n. \end{cases}$$

Пусть свободным неизвестным даны некоторые значения из поля P. Тогда (как и в 2.2)), двигаясь в системе снизу вверх, мы получим значения для главных неизвестных. Таким образом, мы получим решение системы $(**)$, а значит, и системы $(*)$. Придавая свободным неизвестным различные значения из поля P, можно получить все решения системы $(*)$.

Замечание. *Очевидно, что если числовое поле P бесконечно, то система $(*)$ будет иметь бесконечно много решений.*

(3) Итак, чтобы решить систему линейных уравнений методом Гаусса, следует:

1) выписать расширенную матрицу системы и привести ее к ступенчатой матрице A с помощью элементарных преобразований строк;

2) записать соответствующую ступенчатую систему линейных уравнений и в зависимости от вида матрицы A найти решения системы.

Пример. Решить систему линейных уравнений методом Гаусса.

$$\begin{cases} -x_1 + 2x_2 - x_3 + x_4 = 1, \\ -3x_1 + x_2 + 2x_3 = 2, \\ 4x_1 - 3x_2 - x_3 - x_4 = -3. \end{cases}$$

Решение.

$$\left(\begin{array}{cccc|c} -1 & 2 & -1 & 1 & 1 \\ -3 & 1 & 2 & 0 & 2 \\ 4 & -3 & -1 & -1 & -3 \end{array}\right) \overset{\substack{\text{II+I}\cdot(-3) \\ \text{III+I}\cdot 4}}{\sim} \left(\begin{array}{cccc|c} -1 & 2 & -1 & 1 & 1 \\ 0 & -5 & 5 & -3 & -1 \\ 0 & 5 & -5 & 3 & 1 \end{array}\right) \overset{\text{III+II}\cdot 1}{\sim}$$

$$\sim \left(\begin{array}{cccc|c} -1 & 2 & -1 & 1 & 1 \\ 0 & -5 & 5 & -3 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Соответствующая ступенчатая система имеет вид

$$\begin{cases} -x_1 + 2x_2 - x_3 + x_4 = 1, \\ \quad - 5x_2 + 5x_3 - 3x_4 = -1. \end{cases}$$

Неизвестные x_1 и x_2 будут главными, а x_3 и x_4 — свободными. Перенесем свободные неизвестные в правую часть уравнений

$$\begin{cases} -x_1 + 2x_2 = 1 + x_3 - x_4, \\ \quad - 5x_2 = -1 - 5x_3 + 3x_4. \end{cases}$$

Придадим свободными неизвестным произвольные числовые значения. Пусть $x_3 = \alpha$, $x_4 = \beta$, где $\alpha, \beta \in P$. Тогда

$$\begin{cases} -x_1 + 2x_2 = 1 + \alpha - \beta, \\ \quad - 5x_2 = -1 - 5\alpha + 3\beta, \end{cases}$$

откуда

$$\begin{aligned} x_2 &= \tfrac{1}{5} + \alpha - \tfrac{3}{5}\beta, \\ x_1 &= -\tfrac{3}{5} + \alpha - \tfrac{1}{5}\beta. \end{aligned}$$

Ответ:

$$\begin{aligned} x_1 &= -\tfrac{3}{5} + \alpha - \tfrac{1}{5}\beta, \\ x_2 &= \tfrac{1}{5} + \alpha - \tfrac{3}{5}\beta, \\ x_3 &= \alpha, \\ x_4 &= \beta, \text{ где } \alpha, \beta \in P. \end{aligned}$$

§3. Правило Крамера и матричный метод решения систем линейных уравнений

(1) Габриэль Крамер (1704–1752) — швейцарский математик.

Система линейных уравнений называется *крамеровской*, если выполняются два условия:

1) число уравнений системы равно числу неизвестных;

2) определитель матрицы системы отличен от нуля.

Как и прежде, будем рассматривать системы линейных уравнений над числовым полем P.

Теорема 1 (правило Крамера). *Крамеровская система линей-*

ных уравнений

$$(*)\qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= b_n \end{cases}$$

имеет единственное решение

$$x_1 = \frac{\Delta_1}{\Delta},\ x_2 = \frac{\Delta_2}{\Delta}, \ldots,\ x_n = \frac{\Delta_n}{\Delta},$$

где Δ — определитель матрицы системы $(*)$, а Δ_i — определитель, полученный из Δ заменой столбца коэффициентов при x_i столбцом свободных коэффициентов, $i = 1, 2, \ldots, n$.

(2) Доказательство правила Крамера дает еще один способ решения крамеровской системы, который называют *матричным методом.* Он основан на использовании следующего матричного равенства: $X = A^{-1}B$, где X — матрица-столбец неизвестных, A — матрица системы $(*)$, B — матрица-столбец свободных коэффициентов.

Пример. Решить систему линейных уравнений

$$\begin{cases} x_1 - 2x_2 = -1, \\ 2x_1 - 3x_2 = -1. \end{cases}$$

а) по правилу Крамера; б) матричным методом.

Решение. Так как число уравнений системы равно числу неизвестных и

$$\Delta = \begin{vmatrix} 1 & -2 \\ 2 & -3 \end{vmatrix} = -3 + 4 = 1 \neq 0,$$

то данная система уравнений является крамеровской.

а) Решим систему по правилу Крамера:

$$\Delta_1 = \begin{vmatrix} -1 & -2 \\ -1 & -3 \end{vmatrix} = 3 - 2 = 1,\ x_1 = \frac{\Delta_1}{\Delta} = 1,$$

$$\Delta_2 = \begin{vmatrix} 1 & -1 \\ 2 & -1 \end{vmatrix} = -1 + 2 = 1,\ x_1 = \frac{\Delta_1}{\Delta} = 1.$$

б) Применим для решения матричный метод. Находим

$$A^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}^{-1} = \frac{1}{\Delta}\begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix} = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix}.$$

Тогда

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = A^{-1}B = \begin{pmatrix} -3 & 2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

откуда $x_1 = 1$, $x_2 = 1$.

Ответ: $x_1 = x_2 = 1$.

§4. Ранг матрицы

(1) Пусть $A = (a_{ij})$ — матрица размера $n \times k$ над числовым полем P. Зафиксируем натуральное число $r \leqslant \min\{n, k\}$. Выделим в матрице A произвольно r строк с номерами $i_1 < i_2 < \ldots < i_r$ и r столбцов с номерами $j_1 < j_2 < \ldots < j_r$. Из элементов матрицы A, стоящих на пересечении выбранных строк и столбцов, составим определитель r-го порядка

$$\begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \ldots & a_{i_1 j_r} \\ a_{i_2 j_1} & a_{i_2 j_2} & \ldots & a_{i_2 j_r} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{i_r j_1} & a_{i_r j_2} & \ldots & a_{i_r j_r} \end{vmatrix}.$$

Этот определитель называют *минором r-го порядка* матрицы A.

В пункте (6) §3 темы 4 мы определили минор M_{kl} элемента a_{kl} квадратной матрицы A порядка n. Очевидно, что M_{kl} является минором $(n-1)$-го порядка матрицы A.

Важное свойство миноров дает следующая

Лемма 1. *Если в матрице A все миноры r-го порядка равны нулю, то равны нулю и все миноры более высокого порядка, если их можно составить.*

(2) *Рангом ненулевой матрицы A* называется такое натуральное число r, что среди миноров r-го порядка есть отличные от нуля, а все миноры $(r+1)$-го порядка, если их можно составить, равны нулю. *Ранг нулевой матрицы* считают равным нулю. Ранг матрицы A обозначают $r(A)$.

Ввиду леммы 1 ранг ненулевой матрицы A — это наивысший порядок минора матрицы A, отличного от нуля.

Замечание. *Так как при транспонировании определитель не изменяется, то очевидно, что миноры матрицы A и миноры матрицы A^T будут иметь одни и те же значения. Следовательно, $r(A) = r(A^T)$.*

(3) Практический способ вычисления ранга матрицы основан на следующих двух теоремах.

Теорема 1. *При элементарных преобразованиях строк матрицы ее ранг не изменяется.*

Следствие 1. *При элементарных преобразованиях строк невырожденная квадратная матрица остается невырожденной.*

Теорема 2. *Ранг ступенчатой матрицы равен числу ее ненулевых строк.*

Из теорем 1 и 2 следует простой способ вычисления ранга матрицы A:

1) привести матрицу A к ступенчатому виду с помощью элементарных преобразований строк;

2) число ненулевых строк получившейся ступенчатой матрицы будет рангом матрицы A.

§5. Теорема Кронекера-Капелли

(1) Эта теорема дает критерий совместности системы линейных уравнений.

Теорема Кронекера-Капелли. *Система линейных уравнений совместна тогда и только тогда, когда ранг матрицы этой системы равен рангу расширенной матрицы системы.*

(2) **Замечание 1.** *Из доказательства теоремы Кронекера-Капелли следует, что при решении системы линейных уравнений возможен один из трех случаев:*

1) *ранг матрицы системы $r(A)$ не равен рангу $r(B)$ расширенной матрицы системы. В этом случае система несовместна;*

2) *$r(A) = r(B) = n$, где n — число неизвестных. В этом случае система имеет единственное решение;*

3) *$r(A) = r(B) < n$. В этом случае система имеет более одного решения. Если числовое поле P бесконечно, то и решений системы будет бесконечно много.*

Замечание 2. *Доказательство теоремы Кронекера-Капелли показывает, что если $r(A) = r(B) = r < n$, то неизвестные разделяются на две группы: те, которым придаются произвольные значения (в методе Гаусса мы их назвали свободными неизвестными), и те, которые выражаются через свободные (в методе Гаусса — главные неизвестные). Причем, главными неизвестными могут быть любые r неизвестных, коэффициенты которых в матрице системы составляют ненулевой минор r-го порядка.*

Пример. Исследовать систему на совместность. Совместную систему решить по правилу Крамера.

$$\begin{cases} x_1 + 3x_2 + 2x_3 = 1, \\ 2x_1 + 2x_2 - 3x_3 = 9, \\ -x_1 + x_2 + 5x_3 = -8. \end{cases}$$

Решение. Исследуем систему на совместность:

$$\left(\begin{array}{ccc|c} 1 & 3 & 2 & 1 \\ 2 & 2 & -3 & 9 \\ -1 & 1 & 5 & -8 \end{array}\right) \overset{\text{II+I}\cdot(-2)}{\underset{\text{III+I}}{\sim}} \left(\begin{array}{ccc|c} 1 & 3 & 2 & 1 \\ 0 & -4 & -7 & 7 \\ 0 & 4 & 7 & -7 \end{array}\right) \overset{\text{III+II}\cdot 1}{\sim}$$

$$\sim \left(\begin{array}{ccc|c} 1 & 3 & 2 & 1 \\ 0 & -4 & -7 & 7 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

В расширенной матрице системы до черты записана матрица системы. Мы привели эти матрицы к ступенчатому виду одновременно. Так как ранг матрицы равен числу ненулевых строк в ступенчатом виде матрицы, то ранг $r(A)$ матрицы системы равен 2, и ранг $r(B)$ расширенной матрицы системы также равен 2. Поскольку $r(A) = r(B)$, то по теореме Кронекера-Капелли система совместна.

Так как $r(A) = 2$, то $|A| = 0$, а значит, данная система крамеровской не является.

Поскольку $r(A) = r(B)$ меньше числа неизвестных, то система имеет бесконечно много решений над числовым полем $\mathbb{R}$. Так как определитель из коэффициентов при x_2 и x_3 во втором и третьем уравнениях отличен от нуля

$$\Delta = \begin{vmatrix} 2 & -3 \\ 1 & 5 \end{vmatrix} = 10 + 3 = 13 \neq 0,$$

то в качестве главных неизвестных можно взять x_2 и x_3, а в системе оставить соответствующие определителю Δ уравнения

$$\begin{cases} 2x_1 + 2x_2 - 3x_3 = 9, \\ -x_1 + x_2 + 5x_3 = -8. \end{cases}$$

Пусть свободная неизвестная $x_1 = \alpha$ — произвольное число. Тогда система

$$(*) \qquad \begin{cases} 2x_2 - 3x_3 = 9 - 2\alpha, \\ x_2 + 5x_3 = -8 + \alpha \end{cases}$$

будет крамеровской относительно главных неизвестных x_2 и x_3,

Находим

$$\Delta_2 = \begin{vmatrix} 9-2\alpha & -3 \\ -8+\alpha & 5 \end{vmatrix} = 5(9-2\alpha) + 3(-8+\alpha) = 21 - 7\alpha,$$

$$\Delta_3 = \begin{vmatrix} 2 & 9-2\alpha \\ 1 & -8+\alpha \end{vmatrix} = 2(-8+\alpha) - (9-2\alpha) = -25 + 4\alpha.$$

Тогда

$$x_2 = \frac{\Delta_2}{\Delta} = \frac{21-7\alpha}{13} = \frac{21}{13} - \frac{7}{13}\alpha,$$

$$x_3 = \frac{\Delta_3}{\Delta} = \frac{-25+4\alpha}{13} = -\frac{25}{13} + \frac{4}{13}\alpha.$$

Ответ: система совместна и имеет бесконечно много решений над $\mathbb{R}$:
$x_2 = \frac{21}{13} - \frac{7}{13}\alpha$,
$x_3 = -\frac{25}{13} + \frac{4}{13}\alpha$,
$x_1 = \alpha$ — любое число из $\mathbb{R}$.

§6. Однородные системы линейных уравнений

Система линейных уравнений называется *однородной*, если все свободные коэффициенты системы равны нулю.

Пусть дана однородная система линейных уравнений

$$(*) \qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kn}x_n = 0. \end{cases}$$

Очевидно, что однородная система $(*)$ всегда совместна, так как она имеет *нулевое решение* $x_1 = 0$, $x_2 = 0, \ldots, x_n = 0$. Ввиду этого для однородных систем линейных уравнений интерес представляет вопрос о существовании ненулевых решений. Следующая теорема дает необходимые и достаточные условия для решения этого вопроса.

Теорема 1. *Однородная система линейных уравнений имеет ненулевое решение тогда и только тогда, когда ранг матрицы системы меньше числа неизвестных.*

Следствие 1. *Если в однородной системе линейных уравнений число уравнений меньше числа неизвестных, то система имеет ненулевое решение.*

Следствие 2. *Однородная система n линейных уравнений с n*

неизвестными имеет ненулевое решение тогда и только тогда, когда определитель матрицы системы равен нулю.

Тема 6. Многочлены от одной переменной

§1. Построение кольца многочленов

(1) Пусть A — произвольное кольцо с единицей 1. Обозначим через B множество, элементами которого являются бесконечные упорядоченные последовательности

$$f = (f_0, f_1, \ldots, f_n, \ldots), \quad f_i \in A,$$

с конечным числом ненулевых элементов. В каждой такой последовательности, начиная с некоторого номера, все члены последовательности равны нулевому элементу 0 кольца A. Две последовательности $f = (f_0, f_1, \ldots)$ и $g = (g_0, g_1, \ldots)$ будем считать *равными* и писать $f = g$ тогда и только тогда, когда $f_i = g_i$ для $i = 0, 1, \ldots$.

Введем на множестве B операции сложения и умножения:

1) $f + g = (f_0, f_1, \ldots) + (g_0, g_1, \ldots) = (f_0 + g_0, f_1 + g_1, \ldots)$;

2) $f \cdot g = (f_0, f_1, \ldots)(g_0, g_1, \ldots) = (h_0, h_1, \ldots)$, где $h_k = \sum\limits_{i+j=k} f_i \cdot g_j$, $k = 0, 1, \ldots$. В частности, $h_0 = f_0 g_0$, $h_1 = f_0 g_1 + f_1 g_0$, $h_2 = f_0 g_2 + f_1 g_1 + f_2 g_0$ и т. д.

(2) **Лемма 1.** *Множество B с операцией сложения является абелевой группой.*

(3) **Лемма 2.** *Множество B с операцией умножения является полугруппой с единицей.*

(4) **Теорема 1.** *Множество B с операциями сложения и умножения является кольцом с единицей.*

(5) Заметим, что если кольцо A коммутативное, то кольцо B также является коммутативным. В частности, если A — поле, то кольцо B коммутативно.

(6) Последовательности вида $(a, 0, 0, \ldots)$, $a \in A$, складываются и умножаются так же, как элементы кольца A:

$$(a, 0, \ldots) + (b, 0, \ldots) = (a + b, 0, \ldots);$$
$$(a, 0, \ldots)(b, 0, \ldots) = (ab, 0, \ldots).$$

Это позволяет отождествить такие последовательности с соответствующими элементами из A. Положим $(a, 0, \ldots) = a \in A$. Тем самым элементы кольца A становятся элементами кольца B.

Обозначим последовательность $(0, 1, 0, \ldots) = x$ и назовем x *переменной над кольцом* A. Тогда нетрудно проверить, что

$$\begin{aligned} x^2 &= (0, 0, 1, 0, \ldots), \\ x^3 &= (0, 0, 0, 1, 0, \ldots), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x^n &= (\underbrace{0, \ldots, 0}_{n}, 1, 0, \ldots). \end{aligned}$$

Кроме того $a_k x^k = (a_k, 0, \ldots) \cdot (\underbrace{0, \ldots, 0}_{k}, 1, 0, \ldots) = (\underbrace{0, \ldots, 0}_{k}, a_k, 0, \ldots)$.

Таким образом, если $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$, где a_n — последний ненулевой элемент в последовательности f, то

$$f = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, 0, \ldots) + \ldots$$
$$\ldots + (0, \ldots, 0, a_n, 0, \ldots) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

Итак, кольцо

$$B = \{f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in A,\ n \in \mathbb{Z},\ n \geqslant 0\}.$$

Это кольцо называют *кольцом многочленов над кольцом* A *от одной переменной* x и обозначают $A[x]$. Элементы $f(x) \in A[x]$ называют *многочленами* или *полиномами*. Более привычной является запись многочлена по убывающим степеням x, т. е. в виде

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Элементы $a_0, a_1, \ldots, a_n$ называют *коэффициентами* многочлена $f(x)$. Коэффициент a_0 называют *свободным коэффициентом*, a_n — *старшим коэффициентом*, а число n — *степенью многочлена* $f(x)$, которую обозначают $\deg f$.

Нулевым многочленом называют многочлен $f(x)$, у которого все коэффициенты равны нулевому элементу кольца A. Степень нулевого многочлена считают равной $(-\infty)$, причем степень $-\infty < n$ для любого $n = 0, 1, \ldots$. Если многочлен $f(x) = a_0$, где $a_0 \neq 0$, то $\deg f(x) = 0$. Многочлены степени 1, т. е. $f(x) = a_1 x + a_0$ называются *линейными многочленами*, а многочлены степени 2 — *квадратными*.

(7) На основании определений равенства, суммы и произведения последовательностей, которые даны в (1), можно сказать, что:

1) два многочлена $f(x)$ и $g(x)$ из кольца $A[x]$ равны тогда и только тогда, когда равны их коэффициенты при одинаковых степенях x;

2) при сложении многочленов складываются коэффициенты при одинаковых степенях x;

3) при умножении многочленов их перемножают, раскрывая скобки и приводя подобные.

Очевидны следующие свойства степеней:

$$\deg(f(x)+g(x)) \leqslant \max\{\deg f(x),\ \deg g(x)\},$$
$$\deg(f(x)\cdot g(x)) \leqslant \deg f(x)+\deg g(x),$$

причем, если в кольце A нет делителей нуля, то

$$(*) \qquad \deg(f(x)\cdot g(x)) = \deg f(x)+\deg g(x).$$

Итак, если P — поле, то кольцо $P[x]$ — коммутативное кольцо с единицей, в котором выполняется равенство $(*)$.

§2. Делимость многочленов

Так как многочлены от одной переменной x образуют кольцо, то многие их свойства похожи на свойства целых чисел в кольце $\mathbb{Z}$.

Пусть P — поле. Всюду в этом параграфе будем рассматривать многочлены из кольца $P[x]$.

(1) **Определение 2.1.** Будем говорить, что многочлен $g(x)$ *делит многочлен* $f(x)$, если в кольце $P[x]$ существует такой многочлен $h(x)$, что $f(x)=g(x)h(x)$. В этом случае пишут: $g(x) \mid f(x)$. Многочлен $g(x)$ называют *делителем* многочлена $f(x)$, а $h(x)$ — *частным* при делении $f(x)$ на $g(x)$. Если $g(x) \mid f(x)$, то говорят также, что $f(x)$ *делится* на $g(x)$ и пишут $f(x) \vdots g(x)$.

Свойства делимости многочленов сформулируем в следующей лемме.

Лемма 1. *Для многочленов из кольца $P[x]$ справедливы следующие свойства:*

1) $f(x) \vdots f(x)$;

2) *если* $f(x) \vdots g(x)$, $g(x) \vdots h(x)$, *то* $f(x) \vdots h(x)$;

3) *если* $h(x) \mid f(x)$ *и* $h(x) \mid g(x)$, *то для любых* $u(x)$, $v(x) \in P[x]$ *верно* $h(x) \mid (u(x)f(x)+v(x)g(x))$;

4) $f(x) \vdots a$, *для всех* $a \in P^{\#}$;

5) *если* $f(x) \vdots g(x)$, *то* $f(x) \vdots ag(x)$ *для всех* $a \in P^{\#}$;

6) *если* $f(x) \vdots g(x)$ *и* $g(x) \vdots f(x)$, *то* $f(x) = ag(x)$ *для некоторого* $a \in P^{\#}$;

7) $f(x) \vdots g(x)$ *тогда и только тогда, когда* $af(x) \vdots g(x)$ *для любого* $a \in P^{\#}$.

(2) Для многочленов, как и для целых чисел, справедлива теорема о делении с остатком.

Теорема (о делении с остатком для многочленов). *Для данных многочленов* $f(x) \in P[x]$ *и* $g(x) \in P[x]^{\#}$ *существуют и притом единственные многочлены* $q(x)$ *и* $r(x)$ *из кольца* $P[x]$ *такие, что* $f(x) = g(x)q(x) + r(x)$, *где* $\deg r(x) < \deg g(x)$.

Многочлен $q(x)$ называют *неполным частным*, а $r(x)$ — *остатком* при делении $f(x)$ на $g(x)$.

(3) **Определение 2.2.** Если многочлен $d(x)$ делит многочлены $f(x)$ и $g(x)$, то $d(x)$ называется *общим делителем* многочленов $f(x)$ и $g(x)$. *Наибольшим общим делителем* многочленов $f(x)$ и $g(x)$ называется общий делитель $d(x)$ этих многочленов, который делится на любой общий делитель многочленов $f(x)$ и $g(x)$. Обозначается: НОД$(f(x), g(x))$.

В отличие от целых чисел НОД$(f(x), g(x))$ определяется неоднозначно. Действительно, если НОД$(f(x), g(x)) = d(x)$, то ввиду свойства 7) леммы 1 многочлен $ad(x)$ также будет НОД$(f(x), g(x))$ для любого $a \in P^{\#}$. Следующая лемма определяет множество всех НОД$(f(x), g(x))$.

Лемма 2. *Если* $d(x) =$ НОД$(f(x), g(x))$, *то* $\{ad(x) \mid a \in P^{\#}\}$ *есть множество всех наибольших общих делителей многочленов* $f(x)$ *и* $g(x)$.

Среди всех НОД$(f(x), g(x))$ выделим тот, у которого старший коэффициент равен 1. Обозначим его НОД$^1(f(x), g(x))$. Ввиду леммы 2 очевидно, что НОД$^1(f(x), g(x))$ определяется для $f(x)$ и $g(x)$ однозначно.

Лемма 3. *Если* $f(x) = g(x)q(x) + r(x)$, *то* НОД$^1(f(x), g(x)) =$ НОД$^1(g(x), r(x))$.

(4) Рассмотрим вопрос о существовании и нахождении НОД двух многочленов.

Из определения 2.2 нетрудно заметить:

1) если $g(x)$ — нулевой многочлен, то НОД$(g(x), g(x))$ не существует;

2) если $g(x)$ — нулевой многочлен, а $f(x)$ — ненулевой многочлен из кольца $P[x]$, то НОД$(f(x), g(x)) = f(x)$;

3) НОД$(f(x), g(x)) = g(x)$ тогда и только тогда, когда $g(x) \mid f(x)$.

Пусть теперь $g(x) \in P[x]^{\#}$ и $g(x)$ не делит $f(x)$. Используя теорему о делении с остатком, мы можем составить последовательность равенств

$$(*)\qquad \begin{aligned} f(x) &= g(x)q_1(x) + r_1(x),\\ g(x) &= r_1(x)q_2(x) + r_2(x),\\ r_1(x) &= r_2(x)q_3(x) + r_3(x),\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x),\\ r_{n-1}(x) &= r_n(x)q_{n+1}(x), \end{aligned}$$

где

$$(**)\qquad \deg g(x) > \deg r_1(x) > \deg r_2(x) > \ldots$$

$$\ldots > \deg r_{n-1}(x) > \deg r_n(x) > 0.$$

Неравенства $(**)$ показывают, что равенства $(*)$ обязательно закончатся, т.е. на каком-то шаге остаток при делении станет равным нулю. Последовательность равенств $(*)$ называется *алгоритмом Евклида для многочленов* $f(x)$ *и* $g(x)$.

Теорема (о нахождении НОД многочленов). *Наибольший общий делитель любых двух ненулевых многочленов* $f(x)$ *и* $g(x)$ *существует. Если* $g(x) \mid f(x)$, *то* НОД$(f(x), g(x)) = g(x)$. *Если же* $g(x)$ *не делит* $f(x)$, *то* НОД$(f(x), g(x))$ *равен последнему ненулевому остатку в алгоритме Евклида многочленов* $f(x)$ *и* $g(x)$.

(5) Наибольший общий делитель всегда можно выразить через исходные многочлены.

Теорема (о линейном выражении НОД двух многочленов). *Если* $d(x) =$ НОД$(f(x), g(x))$, *то в кольце* $P[x]$ *существуют многочлены* $u(x)$ *и* $v(x)$ *такие, что* $d(x) = u(x)f(x) + v(x)g(x)$.

(6) **Определение 2.3.** Многочлены $f(x)$ и $g(x)$ называются *взаимно простыми*, если НОД$^1(f(x), g(x)) = 1$.

Свойства взаимно простых многочленов дает следующая лемма.

Лемма 4. *Для многочленов из кольца* $P[x]$ *справедливы следующие утверждения:*

1) *многочлены* $f(x)$ *и* $g(x)$ *взаимно просты тогда и только тогда, когда существуют многочлены* $u(x)$ *и* $v(x)$ *из кольца* $P[x]$ *такие, что* $u(x)f(x) + v(x)g(x) = 1$;

2) *если произведение многочленов* $f(x)\cdot g(x)$ *делится на многочлен* $h(x)$, *причем* $f(x)$ *и* $h(x)$ *взаимно просты, то* $g(x) \vdots h(x)$.

§3. Неприводимые многочлены

(1) **Определение 3.1.** Пусть P — поле, $f(x)$ — многочлен из кольца $P[x]$, степень которого больше или равна 1. По лемме 1 из §2 $f(x)$ делится на a и на $af(x)$, где a — ненулевой элемент поля P. Если $f(x)$ не имеет в кольце $P[x]$ других делителей, то он называется *неприводимым над полем* P. Многочлен, который не является неприводимым над полем P, называется *приводимым над полем* P.

По определению, если $f(x)$ — неприводим над полем P, то его нельзя представить в виде произведения $f(x) = f_1(x)f_2(x)$, где $1 \leqslant \leqslant \deg f_1(x) < \deg f(x)$ и $1 \leqslant \deg f_2(x) < \deg f(x)$.

Приводимость многочлена зависит от поля, над которым рассматривается многочлен. Например, многочлен $f(x) = x^2+1$ неприводим над полем $\mathbb{R}$, но приводим над полем $\mathbb{C}$, так как $f(x) = (x+i)(x-i)$.

(2) Свойства неприводимых многочленов приведем в следующей лемме.

Лемма 1. *Для многочленов над полем P справедливы следующие утверждения:*

1) *любой многочлен первой степени неприводим над полем P;*

2) *если многочлен $f(x)$ неприводим над полем P, то многочлен $af(x)$ неприводим над полем P для любого $a \in P^{\#}$;*

3) *если $f(x)$ — неприводимый над P многочлен, то для любого многочлена $g(x)$ либо $f(x) \mid g(x)$, либо $f(x)$ и $g(x)$ взаимно просты;*

4) *если произведение многочленов $g(x)h(x)$ делится на неприводимый многочлен $f(x)$, то либо $g(x) \vdots f(x)$, либо $h(x) \vdots f(x)$.*

(3) Следующая теорема является аналогом основной теоремы арифметики в кольце целых чисел $\mathbb{Z}$.

Теорема 1. *Всякий многочлен $f(x)$ над полем P степени большей или равной 1 либо неприводим над P, либо может быть представлен в виде произведения неприводимых над полем P многочленов. Если имеются два таких разложения $f(x) = \varphi_1(x) \dots \varphi_s(x) = h_1(x) \dots \dots h_t(x)$, то $s = t$ и при подходящей нумерации $h_i(x) = a_i\varphi_i(x)$, где $a_i \in P^{\#}$, $i = 1, 2 \dots, t$.*

(4) Мы добьемся полной однозначности разложения многочлена $f(x)$ из кольца $P[x]$ на неприводимые над полем P множители, если из каждого такого множителя вынесем его старший коэффициент. В ре-

зультате получим разложение

$$f(x) = ap_1(x) \dots p_s(x),$$

где $a \in P^{\#}$, $p_1(x), \dots, p_s(x)$ — неприводимые над P многочлены со старшим коэффициентом 1.

Определение 3.2. Многочлен со старшим коэффициентом 1 называют *унитарным многочленом.*

Определение 3.3. Пусть $p(x)$ — неприводимый над полем P многочлен, $f(x)$ — многочлен из кольца $P[x]$. Если $p^k(x) \mid f(x)$, а $p^{k+1}(x)$ не делит $f(x)$, то $p(x)$ называют *k-кратным неприводимым множителем многочлена* $f(x)$. Если $k = 0$, то как и в числах $p^0(x) = 1$ и $p(x)$ называется *0-кратным неприводимым множителем* многочлена $f(x)$. Если $k = 1$, то $p(x)$ называется *простым неприводимым множителем* $f(x)$.

Теперь в разложении $f(x) = ap_1(x) \dots p_s(x)$, где $a \in P^{\#}$, $p_1(x), \dots$ $\dots, p_s(x)$ — унитарные неприводимые над P многочлены, соберем одинаковые множители. Получим каноническое разложение многочлена $f(x)$ над полем P:

$$f(x) = ap_1^{\alpha_1}(x) \dots p_k^{\alpha_k}(x).$$

Так же как и в целых числах наибольший общий делитель многочленов можно найти, используя их канонические разложения.

Теорема 2. *Наибольший общий делитель многочленов $f(x)$ и $g(x)$ из кольца $P[x]$, степень которых больше или равна 1, равен произведению унитарных неприводимых над полем P многочленов, одновременно входящих в канонические разложения $f(x)$ и $g(x)$ над полем P. Каждый такой неприводимый многочлен берется с показателем степени, равным меньшей из его кратностей в $f(x)$ и $g(x)$.*

§4. Производная многочлена

(1) Теорема 1 из §3 имеет в основном теоретическое значение, так как не дает общего метода разложения многочлена на неприводимые множители. Более того, даже на вопрос о неприводимости данного многочлена над данным полем в настоящее время нет исчерпывающего ответа. Общее решение этой задачи мы укажем лишь для полей $\mathbb{R}$ и $\mathbb{C}$.

Тем не менее существует метод, позволяющий выяснить, имеет ли данный многочлен $f(x)$ кратные неприводимые множители и в случае положительного ответа сводящий задачу разложения $f(x)$ на неприводи-

мые множители к аналогичной задаче для некоторого многочлена меньшей степени.

(2) Пусть P — поле нулевой характеристики. Для многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ из кольца $P[x]$ определим его *производную* как многочлен

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1.$$

Так как P — поле нулевой характеристики, то старший коэффициент $na_n \neq 0$. Поэтому, если $f(x)$ — многочлен степени n, то производная $f'(x)$ имеет степень $(n-1)$.

При таком определении производной многочлена сохраняются все правила дифференцирования:

1) $(cf(x))' = c \cdot f'(x)$ для любого $c \in P$;

2) $(f(x) + g(x))' = f'(x) + g'(x)$;

3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;

4) $((f(x))^k)' = kf^{k-1}(x) \cdot f'(x)$.

Лемма 1. *Если P — поле нулевой характеристики, $f(x) \in P[x]$ и $p(x)$ — k-кратный неприводимый множитель многочлена $f(x)$, то он является $(k-1)$-кратным множителем производной $f'(x)$ для $k \geqslant \geqslant 1$. В частности, если $p(x)$ — простой неприводимый множитель многочлена $f(x)$, то $p(x)$ не входит в разложение на неприводимые множители над P многочлена $f'(x)$.*

Из теоремы 2 §3 и леммы 1 следует

Теорема 1. *Пусть P — поле нулевой характеристики, $f(x) \in \in P[x]$. Если $f(x) = ap_1^{\alpha_1}(x) \ldots p_n^{\alpha_n}(x)$ — каноническое разложение многочлена $f(x)$ над полем P , то*

$$\text{НОД}(f(x), f'(x)) = p_1^{\alpha_1 - 1}(x) \ldots p_n^{\alpha_n - 1}(x).$$

В частности, $f(x)$ не содержит кратных неприводимых множителей тогда и только тогда, когда он взаимно прост со своей производной.

Таким образом, если $d(x) = \text{НОД}(f(x), f'(x)) \neq 1$, то многочлен $f(x)$ обладает кратными неприводимыми множителями. Разделив $f(x)$ на $d(x)$, получим многочлен $g(x) = ap_1(x) \ldots p_n(x)$, который имеет точно такие же неприводимые множители как многочлен $f(x)$. Так как $f(x)$ имеет кратные неприводимые множители, то $\deg g(x) < \deg f(x)$. Если неприводимые множители многочлена $g(x)$ удается найти, то можно найти каноническое разложение и многочлена $f(x)$.

§5. Корни многочлена

(1) Пусть P — поле и многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ принадлежит кольцу $P[x]$. Если c — элемент поля P, то элемент $f(c) = a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0$ поля P называется *значением многочлена* $f(x)$ *при* $x = c$. Элемент $c \in P$ называют *корнем многочлена* $f(x)$, если $f(c) = 0$.

Теорема (Безу). *Элемент* $c \in P$ *является корнем многочлена* $f(x) \in P[x]$ *тогда и только тогда, когда* $f(x) \vdots (x - c)$.

(2) Теорема Безу связывает понятие корня x_0 многочлена $f(x)$ с неприводимым множителем $(x - x_0)$ этого многочлена: элемент x_0 является корнем многочлена $f(x)$ тогда и только тогда, когда $(x - x_0)$ является множителем многочлена $f(x)$.

В связи с этим естественно следующее определение.

Определение 5.1. Элемент $x_0 \in P$ называется *k-кратным корнем* многочлена $f(x) \in P[x]$, если $(x - x_0)$ является k-кратным неприводимым множителем многочлена $f(x)$, т. е. если $(x - x_0)^k$ делит $f(x)$, а $(x - x_0)^{k+1}$ не делит $f(x)$. Если $k = 1$, то x_0 называют *простым корнем* многочлена $f(x)$.

Тогда ввиду леммы 1 и теоремы 1 из §4 справедливы следующие утверждения, которые устанавливают связь кратностей корня многочлена и его производной.

Теорема 1. *Пусть* P *— поле нулевой характеристики, многочлен* $f(x) \in P[x]$ *и* $x_0 \in P$ *— k-кратный корень многочлена* $f(x)$, *где* $k \in \mathbb{N}$. *Тогда* x_0 *— $(k-1)$-кратный корень производной* $f'(x)$. *В частности, если* x_0 *— простой корень многочлена* $f(x)$, *то* $f'(x_0) \neq 0$.

Теорема 2. *Пусть* P *— поле нулевой характеристики и многочлен* $f(x) \in P[x]$. *Многочлен* $f(x)$ *не имеет в поле* P *кратных корней тогда и только тогда, когда он взаимно прост со своей производной.*

(3) Пусть $c_1, \ldots, c_n$ — все корни ненулевого многочлена $f(x) \in \in P[x]$, принадлежащие полю P и имеющие кратности $\alpha_1, \alpha_2, \ldots, \alpha_n$ соответственно. Тогда ввиду теоремы Безу

$$f(x) = (x - c_1)^{\alpha_1} \ldots (x - c_n)^{\alpha_n} g(x)$$

для некоторого многочлена $g(x) \in P[x]$, и нетрудно доказать следующую теорему.

Теорема 3. *Число всех корней ненулевого многочлена, учитывая их кратности, не превосходит степени многочлена.*

④ В случае, когда многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ из кольца $P[x]$ имеет в поле P ровно n корней $c_1, c_2, \ldots, c_n$, то справедливы *формулы Виета*, устанавливающие связь корней многочлена с его коэффициентами

$$\begin{aligned}
a_{n-1} &= -(c_1 + c_2 + \ldots + c_n);\\
a_{n-2} &= c_1c_2 + \ldots + c_1c_n + c_2c_3 + \ldots c_2c_n + \ldots +\\
&\quad + c_{n-1}c_n = \sum_{1\leqslant i_1<i_2\leqslant n} c_{i_1}c_{i_2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{n-k} &= (-1)^k \sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n} c_{i_1}c_{i_2}\ldots c_{i_k},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_0 &= (-1)^n c_1c_2\ldots c_n.
\end{aligned}$$

В частности, если $n = 2$ и $P = \mathbb{R}$, получаем известные формулы Виета, которые рассматривались в школьном курсе математики: два числа c_1 и $c_2 \in \mathbb{R}$ являются корнями квадратного трехчлена $f(x) = x^2 + px + q$ тогда и только тогда, когда $c_1 + c_2 = -p$, $c_1 \cdot c_2 = q$.

§6. Схема Горнера

Схема Горнера представляет собой удобный способ деления многочлена $f(x)$ из кольца $P[x]$ на линейный многочлен $(x - c)$, где c — элемент поля P.

① Пусть многочлен $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ при делении на $(x - c)$ имеет неполное частное $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ и остаток $r(x)$, т. е. $f(x) = (x-c)q(x)+r(x)$. Представляя правую часть равенства в виде многочлена по убывающим степеням x и учитывая, что $r(x) = f(c) \in P$, нетрудно установить следующие формулы:

$$\begin{aligned}
b_{n-1} &= a_n,\\
b_{n-2} &= c \cdot b_{n-1} + a_{n-1},\\
b_{n-3} &= c \cdot b_{n-2} + a_{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\\
b_1 &= c \cdot b_2 + a_2,\\
b_0 &= c \cdot b_1 + a_1,\\
f(c) &= c \cdot b_0 + a_0.
\end{aligned}$$

Эти равенства удобно записывать в виде таблицы, заполняя клетки нижней строки по схемам

1) $\boxed{a_n}$ $\downarrow$ $\boxed{b_{n-1}}$

2) $\boxed{b_{k-1}} = c \cdot b_k + \boxed{a_k}\downarrow$, $k = n-2, \ldots, 1$.

3) $\boxed{f(c)} = c \cdot b_0 + \boxed{a_0}\downarrow$.

Таблица схемы Горнера

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_2	a_1	a_0
c	b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_1	b_0	$f(c)$

(2) **Пример.** В кольце $\mathbb{Q}(x)$ разделить многочлен $f(x) = -3x^4 + 2x^2 - 3x + 1$ на $(x+1)$ с остатком.

Решение. Применим схему Горнера.

	-3	0	2	-3	1
-1	-3	3	-1	-2	3

Таким образом, $q(x) = -3x^3+3x^2-x-2$ — неполное частное, а $f(-1) = 3$ — остаток при делении $f(x)$ на $(x+1)$.

§7. Многочлены над полем комплексных чисел

(1) Напомним, что в §3 темы 3 мы уже встречались с основной теоремой алгебры комплексных чисел. Сформулируем эту теорему несколько иначе.

Теорема 1 (основная теорема алгебры комплексных чисел). *Всякий многочлен $f(x)$ степени большей или равной 1 из кольца $\mathbb{C}[x]$ имеет в поле $\mathbb{C}$ хотя бы один корень.*

Определение 7.1. Поле P называется *алгебраически замкнутым*, если каждый многочлен $f(x) \in P[x]$ степени большей или равной 1 имеет в этом поле хотя бы один корень.

Ввиду этого определения основную теорему алгебры комплексных чисел можно сформулировать следующим образом:

Теорема 2 (основная теорема алгебры комплексных чисел). *Поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.*

(2) Остановимся на некоторых важных следствиях основной теоремы алгебры комплексных чисел.

Следствие 1. *Всякий многочлен степени $n \geqslant 1$ из кольца $\mathbb{C}[x]$ имеет в поле $\mathbb{C}$ ровно n корней.*

Следствие 2. *Неприводимыми над полем $\mathbb{C}$ комплексных чисел являются только многочлены первой степени.*

Итак, каждый многочлен $f(x) \in \mathbb{C}[x]$ степени $n \geqslant 1$ можно представить в виде произведения неприводимых над полем $\mathbb{C}$ многочленов

$$f(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n),$$

где a_n — старший коэффициент многочлена $f(x)$; $c_1, \dots, c_n$ — корни $f(x)$ из поля $\mathbb{C}$.

Пример. Разложить многочлен $f(x) = x^4 + x^3 - x - 1$ на неприводимые множители над полем $\mathbb{C}$.

Решение. $f(x) = (x^4 + x^3) - (x + 1) = x^3(x + 1) - (x + 1) = (x + 1)(x^3 - 1) = (x + 1)(x - 1)(x^2 + x + 1)$. Найдем корни многочлена $x^2 + x + 1$ в поле $\mathbb{C}$:

$$x_1 = \frac{-1 - i\sqrt{3}}{2}, \quad x_1 = \frac{-1 + i\sqrt{3}}{2}.$$

Тогда $x^2 + x + 1 = (x + \frac{1+i\sqrt{3}}{2})(x + \frac{1-i\sqrt{3}}{2})$.

Ответ: $f(x) = (x + 1)(x - 1)(x + \frac{1+i\sqrt{3}}{2})(x + \frac{1-i\sqrt{3}}{2})$.

§8. Многочлены над полем действительных чисел

(1) Прежде всего отметим, что поле $\mathbb{R}$ не является алгебраически замкнутым. Действительно, например, многочлен $f(x) = x^2 + 1 \in \mathbb{R}[x]$ не имеет корней в поле $\mathbb{R}$. Однако поле $\mathbb{R}$ содержится в поле $\mathbb{C}$, поэтому всякий многочлен с действительными коэффициентами можно рассматривать как многочлен из кольца $\mathbb{C}[x]$. По следствию 1 §7 такой многочлен имеет в поле $\mathbb{C}$ столько корней, какова его степень. Следующая теорема показывает особенность комплексных корней такого многочлена.

Теорема 1. *Если комплексное число $z = a + bi$ является корнем многочлена с действительными коэффициентами, то число $\overline{z} = a - bi$ также является корнем этого многочлена.*

Следствие 1. *Многочлен нечетной степени с действительными коэффициентами имеет хотя бы один действительный корень.*

Таким образом, у многочлена с действительными коэффициентами комплексные недействительные корни попарно сопряжены, т. е. их четное число.

(2) Рассмотрим вопрос о неприводимых многочленах над полем $\mathbb{R}$.

Теорема 2. *Неприводимыми над полем $\mathbb{R}$ действительных чисел являются многочлены первой степени и многочлены второй степени с отрицательным дискриминантом.*

Итак, всякий многочлен $f(x) \in \mathbb{R}[x]$ степени $n \geqslant 1$ можно представить в виде произведения $m \leqslant n$ многочленов первой степени, соответствующих действительным корням, и $(n-m)/2$ многочленов второй степени с отрицательным дискриминантом, соответствующих парам комплексных недействительных сопряженных корней.

Пример. Разложить многочлен $f(x) = x^4 + 4x^2 + 9$ на неприводимые множители над $\mathbb{R}$.

Решение. Преобразуем многочлен $f(x)$, выделяя разность квадратов:

$$f(x) = (x^2)^2 + 6x^2 + 9 - 2x^2 = (x^2+3)^2 - \left(\sqrt{2}x\right)^2 =$$
$$= (x^2 - \sqrt{2}x + 3)(x^2 + \sqrt{2}x + 3).$$

Так как полученные квадратные трехчлены имеют отрицательные дискриминанты, то они неприводимы над $\mathbb{R}$.

Ответ: $f(x) = (x^2 - \sqrt{2}x + 3)(x^2 + \sqrt{2}x + 3)$.

§9. Интерполяция многочленов

(1) *Интерполяция многочлена* — это конструктивное восстановление многочлена по известным его значениям.

Задачу об интерполяции многочлена можно сформулировать следующим образом: дана таблица, в которой значениям переменной соответствуют значения многочлена. Требуется найти многочлен с такой таблицей значений.

(2) Поставленная задача над числовым полем P решается однозначно следующей теоремой.

Теорема 1. *Пусть P — числовое поле. Для данного натурального числа n существует и притом единственный многочлен $f(x) \in P[x]$ степени меньшей или равной n, который принимает любые наперед заданные значения $b_1, b_2, \ldots, b_{n+1}$ при различных значениях $a_1, a_2, \ldots, a_{n+1}$ переменной x, взятых из поля P. Этот многочлен вычисляется с по-*

мощью интерполяционной формулы Лагранжа

$$f(x) = \sum_{i=1}^{n+1} b_i \varphi_i(x),$$

где

$$\varphi_i(x) = \frac{(x-a_1)\dots(x-a_{i-1})(x-a_{i+1})\dots(x-a_{n+1})}{(a_i-a_1)\dots(a_i-a_{i-1})(a_i-a_{i+1})\dots(a_i-a_{n+1})}.$$

Пример. В кольце $\mathbb{R}[x]$ найти многочлен $f(x)$ степени, не превосходящей 3, со следующей таблицей значений

x	-2	0	1	2
$f(x)$	-25	-1	-1	-1

Решение. Воспользуемся интерполяционной формулой Лагранжа

$$f(x) = b_1\varphi_1(x) + b_2\varphi_2(x) + b_3\varphi_3(x) + b_4\varphi_4(x).$$

$$\varphi_1(x) = \frac{x(x-1)(x-2)}{(-2)(-3)(-4)} = -\frac{1}{24}(x^3 - 3x^2 + 2x);$$

$$\varphi_2(x) = \frac{(x+2)(x-1)(x-2)}{2\cdot(-1)(-2)} = \frac{1}{4}(x^3 - x^2 - 4x + 4);$$

$$\varphi_3(x) = \frac{(x+2)x(x-2)}{3\cdot 1\cdot(-1)} = -\frac{1}{3}(x^3 - 4x);$$

$$\varphi_4(x) = \frac{(x+2)x(x-1)}{4\cdot 2\cdot 1} = \frac{1}{8}(x^3 + x^2 - 2x).$$

Тогда

$$f(x) = \frac{25}{24}(x^3 - 3x^2 + 2x) - \frac{1}{4}(x^3 - x^2 - 4x + 4) +$$
$$+ \frac{1}{3}(x^3 - 4x) - \frac{1}{8}(x^3 + x^2 - 2x) = x^3 - 3x^2 + 2x - 1.$$

Ответ: $f(x) = x^3 - 3x^2 + 2x - 1$.

(3) В §1 мы определили многочлены над кольцом A как бесконечные последовательности с конечным числом ненулевых элементов. Эти последовательности складываются и умножаются по определенным правилам. Такой взгляд на многочлены называется *формально алгебраическим.*

С другой стороны, любой многочлен $f(x)$ над кольцом A определяет функцию $\overline{f} : a \mapsto f(a)$, где $a \in A$. Такой взгляд на многочлен называется *функциональным.*

Пример. Пусть $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ — конечное поле, $f(x) = \overline{1}x + \overline{1}$ и $g(x) = \overline{1}x^2 + \overline{1}$ — многочлены из кольца $\mathbb{Z}_2[x]$. С формально алгебраической точки зрения эти многочлены различны. Однако с функциональной точки зрения они одинаковы, так как определяют одну и ту же функцию. Действительно, функция $\overline{f} : \overline{0} \to \overline{1}$, $\overline{f} : \overline{1} \to \overline{0}$ и $\overline{g} : \overline{0} \to \overline{1}$, $\overline{g} : \overline{1} \to \overline{0}$.

Этот пример показывает, что над конечными полями формально алгебраический и функциональный взгляды на многочлен различны. Однако над бесконечными полями они совпадают.

Теорема 2. *Пусть P — бесконечное поле. Многочлены $f(x)$ и $g(x)$ из кольца $P[x]$ равны тогда и только тогда, когда равны определяемые ими функции.*

§10. Рациональные дроби

Среди элементарных функций, изучаемых в курсе математического анализа, важное место занимают рациональные функции. При интегрировании рациональную функцию часто приходится преобразовывать к виду, удобному для интегрирования. Описание неприводимых многочленов над полем P позволяет обосновать этот процесс преобразований. Пусть $P = \mathbb{C}$ или $P = \mathbb{R}$.

(1) **Определение 10.1.** *Рациональная дробь над полем P* — это функция вида

$$\varphi(x) = \frac{f(x)}{g(x)},$$

где $f(x)$ и $g(x)$ — многочлены из кольца $P[x]$, причем $g(x)$ — ненулевой многочлен. *Областью определения рациональной дроби $\varphi(x)$* является множество элементов x_0 из поля P, для которых $g(x_0) \neq 0$.

Определение 10.2. Две рациональные дроби $\varphi_1(x) = \frac{f_1(x)}{g_1(x)}$ и $\varphi_2(x) = \frac{f_2(x)}{g_2(x)}$ называются *равными*, если их области определения совпадают и для любого элемента x_0 из области определения $\varphi_1(x_0) = \varphi_2(x_0)$, т. е.

$$\frac{f_1(x_0)}{g_1(x_0)} = \frac{f_2(x_0)}{g_2(x_0)}$$

или

$$(*) \qquad f_1(x_0)g_2(x_0) = f_2(x_0)g_1(x_0).$$

(2) Следует отметить, что так как поле P бесконечно, то x_0 может принимать бесконечно много различных значений из области определе-

ния дробей $\varphi_1(x)$ и $\varphi_2(x)$. Тогда по теореме 1 из §9 из условия $(*)$ следует равенство многочленов

$$(**) \qquad f_1(x)g_2(x) = f_2(x)g_1(x).$$

Обратно. Если выполняется равенство $(**)$, то для любого x_0 из области определения $\varphi_1(x)$ и $\varphi_2(x)$ выполняется равенство $(*)$, т. е. рациональные дроби $\varphi_1(x)$ и $\varphi_2(x)$ равны.

Таким образом, рациональные дроби

$$\varphi_1(x) = \frac{f_1(x)}{g_1(x)} \quad \text{и} \quad \varphi_2(x) = \frac{f_2(x)}{g_2(x)}$$

над полем P равны, если равны их области определения и $f_1(x)g_2(x) = f_2(x)g_1(x)$.

(3) Обозначим через $P(x)$ множество всех рациональных дробей над полем P. Определим на множестве $P(x)$ операции сложения и умножения следующими равенствами:

1) $\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)}$;

2) $\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}$.

Нетрудно проверить, что эти операции являются бинарными алгебраическими операциями на $P(x)$.

Теорема 1. *Множество $P(x)$ всех рациональных дробей над полем P с операциями сложения и умножения является полем.*

Также легко заметить, что любой многочлен $f(x) \in P[x]$, является рациональной дробью $\frac{f(x)}{1}$ над полем P. Это означает, что кольцо $P[x] \subseteq \subseteq P(x)$.

(4) **Определение 10.3.** Рациональная дробь называется *правильной*, если степень числителя дроби меньше степени знаменателя.

Лемма 1. *Любую рациональную дробь можно представить в виде суммы многочлена и правильной рациональной дроби.*

Лемма 2. *Сумма, разность и произведение правильных рациональных дробей есть правильная рациональная дробь.*

Обозначим множество всех правильных рациональных дробей над полем P через $\Pi(x)$. По лемме 2 операции сложения и умножения являются бинарными алгебраическими операциями на $\Pi(x)$. Ввиду теоремы 1 нетрудно заметить, что $\Pi(x)$ — кольцо.

(5) **Определение 10.4.** Правильная рациональная дробь $\frac{f(x)}{g(x)}$ называется *простейшей над полем P*, если она удовлетворяет двум условиям:

1) $g(x) = (p(x))^k$, где $p(x)$ — неприводимый над полем P многочлен;
2) $\deg f(x) < \deg p(x)$.

Поскольку неприводимыми над полем $\mathbb{C}$ являются только многочлены первой степени, то простейшими над полем $\mathbb{C}$ являются дроби вида

$$\frac{a}{(bx+c)^k}, \text{ где } k \in \mathbb{N},\ a, b, c \in \mathbb{C}.$$

Неприводимыми над полем $\mathbb{R}$ являются многочлены первой степени и второй степени с отрицательным дискриминантом. Поэтому простейшими над полем $\mathbb{R}$ являются дроби двух видов

$$\frac{a}{(bx+c)^k} \quad \text{и} \quad \frac{ax+b}{(cx^2+px+q)^k},$$

где $k \in \mathbb{N}$, $a, b, c, p, q \in \mathbb{R}$ и $p^2 - 4cq < 0$.

(6) Ввиду леммы 1 рациональная дробь представима в виде суммы многочлена и правильной рациональной дроби. Следующие леммы показывают, что любая правильная рациональная дробь может быть представлена в виде суммы простейших над полем P дробей.

Лемма 3. *Если знаменатель $g(x)$ правильной рациональной дроби над полем P представим в виде произведения двух взаимно простых многочленов $g_1(x)$ и $g_2(x)$ из кольца $P[x]$, то рациональная дробь может быть записана в виде суммы двух правильных рациональных дробей над P со знаменателями $g_1(x)$ и $g_2(x)$.*

Лемма 4. *Всякая правильная рациональная дробь над полем P представима в виде суммы нескольких правильных рациональных дробей, каждая из которых имеет своим знаменателем степень некоторого неприводимого над полем P многочлена.*

Лемма 5. *Всякая правильная рациональная дробь над полем P, знаменатель которой есть степень неприводимого над полем P многочлена, представима в виде суммы простейших над полем P дробей.*

Из лемм 1, 3, 4, 5 непосредственно следует

Теорема (о разложении рациональной дроби). *Всякую рациональную дробь над полем P можно представить в виде суммы многочлена и простейших дробей над полем P.*

Пример. Разложить в сумму многочлена и простейших дробей над полями $\mathbb{R}$ и $\mathbb{C}$ рациональную дробь

$$\varphi(x) = \frac{x^5 + 3x^4 + 4x^3 + 3x^2 + 3x - 1}{x^4 + 3x^3 + 4x^2 + 3x + 1}.$$

Решение. Так как дробь $\varphi(x)$ не являются правильной, то по лемме 1 ее можно представить в виде суммы многочлена и правильной рациональной дроби

$$\begin{array}{r|l} x^5+3x^4+4x^3+3x^2+3x-1 & x^4+3x^3+4x^2+3x+1 \\ \hline x^5+3x^4+4x^3+3x^2+x & x \\ \hline 2x-1 & \end{array}$$

Итак,

$$\varphi(x) = x + \frac{2x-1}{x^4+3x^3+4x^2+3x+1}.$$

Разложим знаменатель дроби на неприводимые над полем $\mathbb{R}$ множители:

$$x^4+3x^3+4x^2+3x+1 = (x^4+x^3)+(2x^3+2x^2)+$$
$$+(2x^2+2x)+(x+1) = x^3(x+1)+2x^2(x+1)+$$
$$+2x(x+1)+(x+1) = (x+1)(x^3+2x^2+2x+1) =$$
$$= (x+1)((x^3+x^2)+(x^2+x)+(x+1)) = (x+1)(x+1)\cdot$$
$$\cdot(x^2+x+1) = (x+1)^2(x+x+1).$$

Многочлен x^2+x+1 неприводим над полем $\mathbb{R}$, так как его дискриминант $D = 1-4 < 0$.

Разложим правильную рациональную дробь $\frac{2x-1}{(x+1)^2(x^2+x+1)}$ на простейшие дроби, используя метод неопределенных коэффициентов.

$$\frac{2x-1}{(x+1)^2(x^2+x+1)} = \frac{A}{(x+1)^2} + \frac{B}{x+1} + \frac{Cx+D}{x^2+x+1} =$$
$$= \frac{A(x^2+x+1)+B(x+1)(x^2+x+1)+(Cx+D)(x+1)^2}{(x+1)^2(x^2+x+1)}.$$

Приравнивая числители, получим

$$2x-1 = (B+C)x^3+(A+2B+2C+D)x^2+$$
$$(A+2B+C+2D)x+(A+B+D),$$

откуда

$$\begin{cases} B + C = 0, \\ A + 2B + 2C + D = 0, \\ A + 2B + C + 2D = 2, \\ A + B + D = -1. \end{cases}$$

Решая эту систему методом Гаусса, получим $A = -3$, $B = -1$, $C = 1$, $D = 3$.

Искомое разложение над полем $\mathbb{R}$ имеет вид:

$$\varphi(x) = x + \frac{-3}{(x+1)^2} + \frac{-1}{x+1} + \frac{x+3}{x^2+x+1}.$$

Чтобы получить разложение над полем $\mathbb{C}$, достаточно представить последнюю дробь в виде суммы простейших над полем $\mathbb{C}$.

Разложим $x^2 + x + 1$ в произведение неприводимых множителей над $\mathbb{C}$. Находим корни многочлена и получаем

$$x^2 + x + 1 = \left(x - \frac{-1 - i\sqrt{3}}{2}\right)\left(x - \frac{-1 + i\sqrt{3}}{2}\right).$$

Тогда

$$\frac{x+3}{x^2+x+1} = \frac{A}{x - \frac{-1-i\sqrt{3}}{2}} + \frac{B}{x - \frac{-1+i\sqrt{3}}{2}} = \\ = \frac{A\left(x - \frac{-1+i\sqrt{3}}{2}\right) + B\left(x - \frac{-1-i\sqrt{3}}{2}\right)}{x^2+x+1}.$$

Приравнивая числители, имеем

$$x + 3 = (A+B)x + \left(A \cdot \frac{1 - i\sqrt{3}}{2} + B \cdot \frac{1 + i\sqrt{3}}{2}\right),$$

откуда

$$\begin{cases} A + B &= 1, \\ A \cdot \frac{1-i\sqrt{3}}{2} + B \cdot \frac{1+i\sqrt{3}}{2} &= 3. \end{cases}$$

Решая эту систему, получим $A = \frac{1}{2} + \frac{5\sqrt{3}}{6}i$, $B = \frac{1}{2} - \frac{5\sqrt{3}}{6}i$.

Таким образом, искомое разложение над $\mathbb{C}$ имеет вид

$$\varphi(x) = x + \frac{-3}{(x+1)^2} + \frac{-1}{x+1} + \frac{\frac{1}{2} + \frac{5\sqrt{3}}{6}i}{x + \frac{1+i\sqrt{3}}{2}} + \frac{\frac{1}{2} - \frac{5\sqrt{3}}{6}i}{x + \frac{1-i\sqrt{3}}{2}}.$$

Ответ: разложение над $\mathbb{R}$:

$$\varphi(x) = x + \frac{-3}{(x+1)^2} + \frac{-1}{x+1} + \frac{x+3}{x^2+x+1};$$

разложение над $\mathbb{C}$:

$$\varphi(x) = x + \frac{-3}{(x+1)^2} + \frac{-1}{x+1} + \frac{\frac{1}{2} + \frac{5\sqrt{3}}{6}i}{x + \frac{1+i\sqrt{3}}{2}} + \frac{\frac{1}{2} - \frac{5\sqrt{3}}{6}i}{x + \frac{1-i\sqrt{3}}{2}}.$$

ВОПРОСЫ
к экзамену по курсу “Алгебра и теория чисел”

1. Множества с алгебраическими операциями.

2. Группы.

3. Кольца и их простейшие свойства.

4. Поле и его простейшие свойства.

5. Определение и свойства делимости целых чисел. Теорема о делении с остатком.

6. Наибольший общий делитель целых чисел и его свойства. Алгоритм Евклида. Теорема о нахождении НОД двух целых чисел.

7. Теорема о линейном выражении НОД двух целых чисел.

8. Взаимно простые числа и их свойства.

9. Простые числа и их свойства.

10. Основная теорема арифметики. Каноническое разложение натурального числа.

11. Наименьшее общее кратное целых чисел. Формула связи НОД и НОК двух чисел. Нахождение НОД и НОК с помощью канонического разложения чисел.

12. Сравнения и их свойства.

13. Кольцо классов вычетов.

14. Условие существования обратного элемента в кольце классов вычетов. Поле классов вычетов.

15. Функция Эйлера и ее свойства и вычисление.

16. Теорема Эйлера и теорема Ферма о сравнениях.

17. Построение поля комплексных чисел.

18. Комплексные числа в алгебраической форме.

19. Тригонометрическая форма комплексного числа. Умножение и деление.

20. Формула Муавра.

21. Извлечение корня n-й степени из комплексного числа.

22. Группа корней n-й степени из единицы.

23. Матрицы и действия над ними. Полное матричное кольцо. Транспонирование матрицы.

24. Элементарные преобразования строк матрицы. Ступенчатая матрица.

25. Перестановка. Умножение перестановок. Симметрическая группа степени n.

26. Циклы. Транспозиция. Разложение перестановки в произведение транспозиций. Знак перестановки.

27. Знак единичной перестановки. Теорема о знаке произведения перестановок.

28. Теорема о знаке транспозиции. Практический способ вычисления знака перестановки.

29. Знакопеременная группа степени n.

30. Определитель, его простейшие свойства. Определители малых порядков.

31. Свойства определителей.

32. Клеточные матрицы и их вычисление.

33. Теорема об определителе произведения матриц.

34. Миноры и алгебраические дополнения. Вычисление определителя разложением по элементам строки или столбца.

35. Обратная матрица, ее свойства и вычисление.

36. Мультипликативная группа невырожденных матриц порядка n над полем.

37. Системы линейных уравнений: основные понятия. Метод Гаусса решения систем линейных уравнений.

38. Правило Крамера и матричный метод решения систем линейных уравнений.

39. Ранг матрицы и его вычисление.

40. Критерий совместности системы линейных уравнений. Однородные системы линейных уравнений.

41. Построение кольца многочленов.

42. Переход к обычной форме записи многочленов. Действия над многочленами. Свойства степеней.

43. Делимость многочленов. Свойства делимости. Теорема о делении с остатком.

44. Наибольший общий делитель многочленов, его неоднозначность. Алгоритм Евклида.

45. Вычисление НОД двух многочленов с помощью алгоритма Евклида. Линейное выражение НОД двух многочленов через исходные многочлены.

46. Взаимно простые многочлены и их свойства.

47. Неприводимые многочлены и их свойства.

48. Аналог основной теоремы арифметики.

49. Унитарные многочлены. Кратные неприводимые множители

многочлена. Каноническое разложение многочлена и вычисление НОД многочленов с его помощью.

50. Производная многочлена. Понижение кратности неприводимого множителя в производной многочлена. Теорема о НОД многочлена и его производной.

51. Корни многочлена. Теорема Безу.

52. Кратные корни многочлена. Понижение кратности корня в производной многочлена. Теорема о числе корней ненулевого многочлена.

53. Формулы Виета.

54. Схема Горнера.

55. Многочлены над полем комплексных чисел.

56. Многочлены над полем действительных чисел. Неприводимые многочлены над полем действительных чисел.

57. Интерполяция. Формально алгебраический и функциональный взгляды на многочлен.

58. Рациональные дроби. Поле рациональных дробей.

59. Правильная рациональная дробь. Разложение многочлена в сумму многочлена и правильной рациональной дроби. Лемма о сумме, разности и произведении двух правильных рациональных дробей. Кольцо правильных рациональных дробей.

60. Простейшая дробь над полем. Простейшие дроби над полями действительных и комплексных чисел. Теорема о разложении рациональной дроби.

61. Лемма о разложении правильной рациональной дроби, знаменатель которой есть произведение двух взаимно простых многочленов.

62. Лемма о разложении правильной рациональной дроби в сумму правильных рациональных дробей, знаменатель каждой из которых есть степень неприводимого над полем многочлена.

63. Лемма о разложении в сумму простейших дробей правильной рациональной дроби, у которой знаменатель есть степень неприводимого над полем многочлена.

Литература

Основная

1. Кострикин А. И. Введение в алгебру. М.: Наука, 1977.

2. Милованов М. В., Тышкевич Р. И., Феденко А. С. Алгебра и аналитическая геометрия. Часть I. Мн.: Вышэйшая школа, 1984.

3. Фаддеев Д. К. Лекции по алгебре. М.: Наука, 1984.

4. Монахов В. С. Числа и многочлены. Тексты лекций. Гомель, 1992.

5. Монахов В. С. Перестановки и определители. Учебное пособие. Гомель, 1987.

6. Монахов В. С. Определители и системы линейных уравнений. Тексты лекций. Гомель, 1991.

7. Сборник задач по алгебре. Под редакцией А. И. Кострикина. М.: Наука, 1987.

8. Шнеперман Л. Б. Курс алгебры и теории чисел в задачах и упражнениях. Мн.: Вышэйшая школа. Часть I, 1986. Часть II, 1987.

9. Бузланов А. В., Монахов В. С. Лабораторные работы по курсу "Алгебра и теория чисел". Гомель, 1991.

Дополнительная

1. Ван дер Варден. Алгебра. М.: Наука, 1979.

2. Курош А. Г. Лекции по общей алгебре. М.: Наука, 1973.

3. Виноградов И. М. Основы теории чисел. М.: Наука, 1981.

Учебно-методическое пособие

Авторы: Бузланов Александр Васильевич
Близнец Игорь Васильевич

Подписано в печать ___.___.2005 г. Формат 60 × 84 1/16.
Бумага офсетная. Печать офсетная.
Усл. п. л. ___,___ Уч.-изд. л. ___.___
Тираж ___ экз. Заказ №___

Отпечатано на полиграфической технике ГГУ им. Ф.Скорины
Лицензия № 02330/0056611 от 16 февраля 2004.
246019 г.Гомель, ул.Советская 104