Оглавление

§ 3. Кольца и поля

3.1. Определения и примеры. В школьном курсе вы уже встречались со множествами, на которых определены операции сложения и умножения. Таковыми, в частности, являются целые, рациональные, вещественные числа. Это и есть примеры колец и полей. В этом параграфе мы дадим формальные определения и приведём примеры.

О п р е д е л е н и е. *Кольцом* называется алгебраическая система $\langle K; +, \cdot \rangle$ с двумя бинарными операциями ($+$ — сложение, $\cdot$ — умножение), которые удовлетворяют следующим аксиомам:

С1. Сложение *ассоциативно*, т. е. $(a+b)+c = a+(b+c)$ для любых a, b, c из K.

С2. Сложение *коммутативно*, т. е. $a + b = b + a$ для любых a, b из K.

С3. Существование нулевого элемента, т. е. в K существует такой элемент 0 — он называется *нулем*, что $a + 0 = a$ для любого a из K.

С4. Существование противоположного элемента, т. е. для любого a из K существует в K такой элемент x — он называется *противоположным* к a, что $a + x = 0$.

У1. Умножение *ассоциативно*, т. е. $a(bc) = (ab)c$ для любых a, b, c из K.

СУ1. Сложение и умножение удовлетворяют правой дистрибутивности, т. е. $(a + b)c = ac + bc$ для любых a, b, c из K.

СУ2. Сложение и умножение удовлетворяют левой дистрибутивности, т. е. $c(a + b) = ca + cb$ для любых a, b, c из K.

Иными словами, по сложению K является абелевой группой (выполнены аксиомы С1–С4); по умножению K является полугруппой (напомним, что полугруппа — алгебраическая система с одной бинарной ассоциативной операцией) и операции сложения и умножения связаны аксиомами дистрибутивности.

Так же, как и для групп, можно показать, что нулевой элемент единственный и для всякого элемента a из K существует единственный противоположный, который будем обозначать символом $-a$.

П р и м е р ы колец.

1. Множество целых (рациональных, вещественных) чисел с операциями сложения и умножения является кольцом.

2. Множество натуральных чисел с этими же операциями кольцом не является.

3. Рассмотрим множество функций

$$f\colon \mathbb{R} \longrightarrow \mathbb{R},$$

определённых для всех вещественных чисел и принимающих вещественные значения. Если определить операции сложения и умножения функций по правилу

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x), \quad x \in \mathbb{R},$$

то множество функций с этими операциями является кольцом.

Укажем некоторые следствия из аксиом кольца.

С л е д с т в и е. *Во всяком кольце произведение любого элемента на нулевой элемент есть нулевой элемент.*

Действительно,

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0.$$

Прибавляя к обеим частям этого равенства по элементу $-(a \cdot 0)$, получим $a \cdot 0 = 0$. Аналогично доказывается, что $0 \cdot a = 0$.

О п р е д е л е н и е. *Полем* называется алгебраическая система $\langle P; +, \cdot \rangle$ с двумя бинарными операциями ($+$ — сложение, $\cdot$ — умножение), которые удовлетворяют следующим аксиомам:

С1. Сложение *ассоциативно*, т. е. $(a+b)+c = a+(b+c)$ для любых a, b, c из P.

С2. Сложение *коммутативно*, т. е. $a + b = b + a$ для любых a, b из P.

С3. Существование нулевого элемента, т. е. в P существует такой элемент 0 — он называется *нулём*, что $a + 0 = a$ для любого a из P.

С4. Существование противоположного элемента, т. е. для любого a из P существует в P такой элемент x — он называется *противоположным* к a, что $a + x = 0$.

У1. Умножение *ассоциативно*, т. е. $a(bc) = (ab)c$ для любых a, b, c из P.

У2. Умножение *коммутативно*, т. е. $ab = ba$ для любых a, b из P.

У3. Существование единичного элемента, т. е. в P существует такой элемент $1 \neq 0$ — он называется *единицей*, что $1a = a$ для любого a из P.

У4. Существование обратного элемента, т. е. для любого a из P, отличного от нуля, существует в P такой элемент y — он называется *обратным* к a, что $ay = 1$.

СУ. Дистрибутивность, т. е. $(a+b)c = ac+bc$ для любых a, b, c из P.

Нетрудно показать, что в поле существует единственный нулевой элемент и единственный единичный элемент; противоположный и обратный к a определяются единственным образом и обозначаются соответственно $-a$ и a^{-1}.

Каждое поле является кольцом. С другой стороны, поле можно определить как кольцо, в котором выполнены аксиомы У2–У4. Если положить $P^* = P \setminus \{0\}$, то $\langle P^*; \cdot\rangle$ – группа. Она называется *мультипликативной группой поля.* Из аксиомы У3 следует, что поле содержит, по крайней мере, два элемента. В силу коммутативности умножения в поле правая дистрибутивность равносильна левой дистрибутивности.

П р и м е р ы полей.

1. Множество рациональных (вещественных) чисел с операциями сложения и умножения образует поле.

2. Кольцо целых чисел не является полем.

3.2. Кольца вычетов. Существуют кольца, состоящие из конечного числа элементов.

П р и м е р. Рассмотрим алгебраическую систему $\langle\{\overline{0}, \overline{1}, \overline{2}\}; +, \cdot\rangle$, где операции сложения и умножения определены правилами

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

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

Нетрудно проверить, что полученная алгебраическая система является кольцом и полем.

П р и м е р. Алгебраическая система $\langle\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}; +, \cdot\rangle$, в которой операции сложения и умножения определены правилами

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

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

является кольцом, но не полем (не выполняется аксиома У4).

Разобранные примеры являются частными случаями общего семейства *колец вычетов по модулю* n. Будем обозначать символом $\mathbb{Z}_n$ множество остатков от деления целых чисел на n. Для произвольного целого числа a символом $\overline{a}$ будем обозначать остаток от деления a на n. Определим на множестве $\mathbb{Z}_n$ операции сложения и умножения по правилу

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

У п р а ж н е н и е. Алгебраическая система

$$\mathbb{Z}_n = \langle \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}; +, \cdot \rangle$$

всегда является кольцом, но полем является тогда и только тогда, когда n — простое число. При простом $n = p$ поле $\mathbb{Z}_p$ называется *полем Галуа* и часто обозначается $GF(p)$.

У п р а ж н е н и е. Пусть $n \in \mathbb{N}$. Существует поле из n элементов тогда и только тогда, когда n — степень простого числа.

3.3. Делители нуля. Рассматривая кольцо вычетов $\mathbb{Z}_4$, видим, что $\overline{2} \cdot \overline{2} = \overline{0}$, т. е. произведение двух ненулевых элементов равно нулю.

О п р е д е л е н и е. Ненулевые элементы a и b кольца K такие, что $a \cdot b = 0$ называются *делителями нуля.*

Приведём примеры колец с делителями нуля.

П р и м е р ы.

1) Если число n не является простым, то кольцо $\mathbb{Z}_n$ обладает делителями нуля. Действительно, пусть $n = kl$, $1 < k, l < n$. Элементы $\overline{k}$ и $\overline{l}$ лежат в $\mathbb{Z}_n$. Их произведение

$$\overline{k} \cdot \overline{l} = \overline{k \cdot l} = \overline{n} = \overline{0}.$$

Следовательно, $\overline{k}$ и $\overline{l}$ — делители нуля.

2) Покажем, что кольцо вещественных функций обладает делителями нуля. Действительно, полагая

$$f(x) = \begin{cases} 0 & \text{при} \quad x \le 0, \\ x & \text{при} \quad x > 0, \end{cases} \qquad g(x) = \begin{cases} x & \text{при} \quad x \le 0, \\ 0 & \text{при} \quad x > 0, \end{cases}$$

видим, что обе эти функции отличны от нуля, а их произведение равно нулю, т. е. функции, которая при любом x принимает значение 0.

Легко показать, что никакое поле не содержит делителей нуля. Действительно, если в поле P справедливо равенство $ab = 0$ и $a \neq 0$, то, домножая обе части на a^{-1}, получим $b = 0$.

Именно это свойство вещественных чисел и имелось в виду, когда в школе вас учили, что если произведение двух выражений равно нулю, то хотя бы одно из них равно нулю.

Из отсутствия делителей нуля в кольце K вытекает, что любое равенство можно сократить на ненулевой общий множитель. Действительно, если $c\,a = c\,b$, $a, b, c \in K$, и $c \neq 0$, то $c\,(a - b) = 0$, откуда заключаем, что $a - b = 0$, т. е. $a = b$.

3.4. Характеристика поля. Если P — поле, то в нём есть единица 1. Возьмем её и будем складывать с собой. Возможно, что на некотором шаге получим 0. Если впервые 0 получим на m–м шаге:

$$\underbrace{1 + 1 + \ldots + 1}_{m} = 0,$$

то говорим, что *характеристика поля* P равна m.

Как мы знаем, в числовых полях (т. е. подполях поля комплексных чисел) такое невозможно. В этом случае говорим, что поле имеет характеристику 0. Примерами полей ненулевой характеристики служат все конечные поля; существуют, впрочем, и бесконечные поля, имеющие ненулевую характеристику.

Если поле имеет характеристику 2, то $1 + 1 = 0$, а потому и для любого элемента $a \in P$ сумма $a + a = 0$, т. е. каждый элемент есть противоположный к себе.

У п р а ж н е н и е. Характеристика поля — либо 0, либо простое число.

3.5. Гомоморфизмы и изоморфизмы колец и полей. Пусть $\langle K;\, +,\, \cdot \rangle$ и $\langle K';\, \oplus,\, \odot \rangle$ — два кольца. Отображение

$$\varphi\colon K \longrightarrow K'$$

кольца K в кольцо K' называется *гомоморфизмом колец,* если для всех $a, b \in K$ справедливы равенства:

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b),$$

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b).$$

Биективный гомоморфизм φ называется *изоморфизмом.* Изоморфные кольца обозначаем $K \cong K'$.

Заметим, что всякий гомоморфизм полей является изоморфизмом. Позже мы вернемся к этому вопросу.

П р и м е р. Рассмотрим кольцо вычетов $\mathbb{Z}_2 = \langle\{\overline{0}, \overline{1}\}; +, \cdot\rangle$, состоящее из двух элементов с операциями сложения и умножения, заданными таблицами

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

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

и другое кольцо $\langle\{$ н, ч $\}; \oplus, \odot\rangle$, для которого

$\oplus$	ч	н
ч	ч	н
н	н	ч

$\odot$	ч	н
ч	ч	ч
н	ч	н

Нетрудно проверить, что эти два кольца изоморфны, если установить соответствие:

$$\overline{0} \longmapsto \text{ч}, \quad \overline{1} \longmapsto \text{н}.$$

Сравните этот пример с примером, разобранным в конце первого параграфа.

Для гомоморфизмов колец справедлива

Л е м м а 1. *При гомоморфизме колец нулевой элемент переходит в нулевой, противоположный — в противоположный, единичный (если есть) — в единичный, обратный (если есть) — в обратный.*

Д о к а з а т е л ь с т в о. Аналогично доказательству соответствующей леммы для групповых гомоморфизмов.

3.6. Подкольцо, подполе. Подмножество кольца (поля) называется *подкольцом* (*подполем*), если оно замкнуто относительно сложения и умножения и само является кольцом (полем) относительно этих индуцированных операций.

Л е м м а 2. *Подмножество L кольца K тогда и только тогда является подкольцом, когда оно замкнуто относительно сложения, умножения и взятия противоположного элемента, т. е. когда выполняются следующие условия*:

а) *для любых $a, b \in L$ сумма $a + b \in L$*;

б) *для любых $a, b \in L$ произведение $ab \in L$*;

в) *для любого $a \in L$ противоположный $-a \in L$.*

Подмножество L поля P тогда и только тогда является подполем, когда оно замкнуто относительно сложения, умножения, взятия противоположного элемента и взятия обратного элемента. Последнее означает:

г) *для любого* $a \in L, a \neq 0$ *обратный элемент* $a^{-1} \in L$.

Доказательство. Рассмотрим множество L с операцией сложения. Так как выполнены условия а) и в), то ввиду леммы 1 из § 2 $\langle L; + \rangle$ является подгруппой группы $\langle K; + \rangle$, а так как выполнено условие б), то $\langle L; +, \cdot \rangle$ — подкольцо. Для доказательства второго утверждения достаточно заметить, что в силу условий б) и г) $\langle L \setminus \{0\}; \cdot \rangle$ является подгруппой группы $\langle P \setminus \{0\}; \cdot \rangle$, а потому $\langle L; +, \cdot \rangle$ является подполем.

Лемма доказана.

Условия а) – в) леммы символически записывают так:

$$L + L \subseteq L, \quad LL \subseteq L, \quad -L \subseteq L.$$

Лемма 3. *Пересечение любого семейства подколец* (*подполей*) *снова является подкольцом* (*подполем*).

Доказательство. Пусть K — некоторое кольцо, L_α, $\alpha \in J$ – семейство подколец и $L = \bigcap_{\alpha \in J} L_\alpha$ — их пересечение. Чтобы доказать, что L — подкольцо, надо доказать, что L замкнуто относительно сложения, умножения и взятия противоположного, т. е.

а) если $a, b \in L$, то $a + b \in L$;

б) если $a, b \in L$, то $ab \in L$;

в) если $a \in L$, то $-a \in L$.

Для доказательства а) заметим, что если $a, b \in L$, то $a, b \in L_\alpha$ для любого $\alpha \in J$. Следовательно, $a + b \in L_\alpha$ для любого $\alpha \in J$, но это и означает, что $a + b \in L$.

б) Если $a, b \in L$, то $a, b \in L_\alpha$ для любого $\alpha \in J$. Следовательно, $ab \in L_\alpha$ для любого $\alpha \in J$, т. е. $ab \in L$.

в) Пусть $a \in L$. Тогда $a \in L_\alpha$ для любого $\alpha \in J$, но тогда $-a \in L_\alpha$ для любого $\alpha \in J$ и, следовательно, $-a \in L$.

Если теперь K — поле, а L_α — семейство подполей, то мы должны установить следующее утверждение:

г) если $a \in L$, $a \neq 0$, то $a^{-1} \in L$.

Заметим, что если $a \in L$, то $a \in L_\alpha$ для любого $\alpha \in J$ и $a^{-1} \in L_\alpha$ для любого $\alpha \in J$, но это и означает, что $a^{-1} \in L$.

Лемма доказана.

Подкольцом кольца K*, порождённым множеством* M, называется пересечение всех подколец, содержащих M, т. е.

$$(M) = \bigcap L_\alpha, \quad L_\alpha \text{ — подкольцо в } K, \quad L_\alpha \supseteq M.$$

Подполем поля P, порождённым множеством M, называется пересечение всех подполей, содержащих M.

П р и м е р ы. 1) Кольцо $\langle \mathbb{Z};\, +,\, \cdot \rangle$ порождается 1. Аналогично поле $\langle \mathbb{Q};\, +,\, \cdot \rangle$ порождается 1.

2) В поле $\langle \mathbb{R};\, +,\, \cdot \rangle$ рассмотрим подкольцо, порождённое элементами 1 и $\sqrt{n}$, где n — натуральное число, свободное от квадратов. Нетрудно заметить, что это подкольцо состоит из чисел

$$L_n = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}.$$

3.7. Ядро и образ гомоморфизма. Идеал. Так же как и в случае групп, для гомоморфизма колец определено понятие ядра и образа. Пусть $\langle K;\, +,\, \cdot \rangle$ и $\langle K';\, \oplus,\, \odot \rangle$ — кольца,

$$\varphi\colon K \longrightarrow K'$$

— кольцевой гомоморфизм. Сопоставим ему два множества: *ядро гомоморфизма φ*:

$$\operatorname{Ker}(\varphi) = \{a \in K \mid \varphi(a) = 0\} \subseteq K$$

и *образ гомоморфизма φ*:

$$\operatorname{Im}(\varphi) = \{\varphi(g) \mid g \in K\} \subseteq K'.$$

Покажем, что на самом деле, ядро $\operatorname{Ker}(\varphi)$ является подкольцом кольца K, а образ $\operatorname{Im}(\varphi)$ — подкольцом кольца K'. Более того, $\operatorname{Ker}(\varphi)$ является идеалом.

О п р е д е л е н и е. Подмножество I кольца K называется *идеалом* (обозначение: $I \trianglelefteq K$), если выполнены следующие три условия:

а) если $a, b \in I$, то $a + b \in I$;

б) если $a \in I$, то $-a \in I$;

в) если $a \in I$, $c \in K$, то $a \cdot c \in I$, $c \cdot a \in I$.

Из этого определения, в частности, следует, что идеал является подкольцом. С другой стороны, кольцо целых чисел является подкольцом поля рациональных чисел, но не является идеалом.

Введенный нами идеал часто называют двусторонним. Если кольцо K некоммутативно и его подкольцо I выдерживает умножение слева (справа) на элементы кольца K, то I называется левосторонним (правосторонним) идеалом.

П р и м е р. Пусть $\mathbb{Z}$ — кольцо целых чисел. Тогда множество

$$n\mathbb{Z} = \{\text{целые числа, делящиеся на } n\}$$

является идеалом для любого целого неотрицательного n.

У п р а ж н е н и е. Докажите, что идеалы $n\mathbb{Z}$ исчерпывают все идеалы в $\mathbb{Z}$.

Л е м м а 4. *Если $\varphi\colon K \longrightarrow K'$ — гомоморфизм колец, то*
1) $\mathrm{Ker}(\varphi)$ — *идеал кольца K*;
2) $\mathrm{Im}(\varphi)$ — *подкольцо кольца K'*.

Д о к а з а т е л ь с т в о. 1) Пусть $a, b \in \mathrm{Ker}(\varphi)$. Тогда

$$\varphi(a+b) = \varphi(a) \oplus \varphi(b) = 0 \oplus 0 = 0.$$

Учитывая, что при гомоморфизме колец противоположный элемент переходит в противоположный, заключаем

$$\varphi(-a) = -\varphi(a) = -0 = 0.$$

Следовательно, ввиду леммы 2 из § 2, множество $\mathrm{Ker}(\varphi)$ является аддитивной подгруппой группы $\langle K; + \rangle$.

Пусть теперь $c \in K$. Тогда

$$\varphi(a \cdot c) = \varphi(a) \odot \varphi(c) = 0 \odot \varphi(c) = 0,$$

$$\varphi(c \cdot a) = \varphi(c) \odot \varphi(a) = \varphi(c) \odot 0 = 0,$$

откуда следует, что $\mathrm{Ker}(\varphi)$ является идеалом.

2) Выберем два элемента $\varphi(a)$ и $\varphi(b)$ из $\mathrm{Im}(\varphi)$. Тогда

$$\varphi(a) \oplus \varphi(b) = \varphi(a+b),$$

$$\varphi(a) \odot \varphi(b) = \varphi(a \cdot b)$$

т. е. их сумма и произведение лежат в $\mathrm{Im}(\varphi)$. Далее, $-\varphi(a) = \varphi(-a)$, т. е. противоположный элемент тоже лежит в образе гомоморфизма φ. Ввиду леммы 2, $\mathrm{Im}(\varphi)$ является подкольцом.

Лемма доказана.

У п р а ж н е н и е. *Во всяком поле P существует только два идеала: нулевой и само P.*

Р е ш е н и е. Действительно, пусть I — идеал в P и $I \neq 0$. Возьмем элемент $a \in I$, $a \neq 0$. Тогда $1 = a \cdot a^{-1} \in I$, но по определению идеала отсюда следует, что $1 \cdot b$ для любого элемента $b \in P$. Следовательно, $I = P$.

Именно из этого факта и следует, что всякий гомоморфизм полей является изоморфизмом.

Покажем, что кольцо целых чисел $\mathbb{Z}$ гомоморфно отображается на кольцо вычетов $\mathbb{Z}_n$, $n > 1$.

Л е м м а 5. *Отображение* $^-\colon \mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto \overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, *сопоставляющее каждому целому числу его остаток от деления на* n, *является гомоморфизмом. Его ядро* $\mathrm{Ker}(^-) = n\mathbb{Z}$ — *множество целых чисел, кратных* n.

Д о к а з а т е л ь с т в о. Чтобы проверить, что $^-$ — гомоморфизм, возьмем $a, b \in \mathbb{Z}$. Надо показать, что справедливы равенства

$$\overline{a+b} = \overline{a} + \overline{b}, \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Заметим, что в правой части рассматриваются операции в $\mathbb{Z}_n$. Как мы знаем из определения этих операций :

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

что и означает: $^-$ — гомоморфизм.

Для описания ядра, возьмем произвольное целое число a и, используя операцию деления с остатком, представим его в виде $a = nq + r$, где q, r — целые числа и $0 \leq r < n$. Применяя гомоморфизм $^-$, получим

$$\overline{a} = \overline{nq + r} = \overline{r}.$$

Следовательно, a лежит в ядре $\mathrm{Ker}(^-)$ тогда и только тогда, когда $r = 0$, т. е. $a \in n\mathbb{Z}$.

Лемма доказана.

3.8. Порождающее множество идеала. Так же, как и в случае колец (см. лемму 3 настоящего параграфа), доказывается

Л е м м а 6. *Пересечение любого семейства идеалов является идеалом.*

Если M — некоторое подмножество кольца K, то символом ид(M) или просто (M) обозначим пересечение всех идеалов в K, содержащих M, иными словами, (M) — наименьший идеал, содержащий множество M. Если $I = (M)$, то говорим, что I *порождается множеством* M или что M является *базой* идеала I.

Более конструктивное описание идеала (M) дает

Л е м м а 7. *Пусть* K — *коммутативное кольцо с единицей и* $M \subseteq K$. *Тогда*

$$(M) = \left\{ \sum m_i b_i \mid m_i \in M, \quad b_i \in K \right\},$$

где в каждой сумме лишь конечное число b_i отлично от нуля. В частности, если $M = \{m_1, m_2, \ldots, m_n\}$ — конечно, то

$$(m_1, m_2, \ldots, m_n) = \left\{ \sum_{i=1}^{n} m_i\, b_i \;\middle|\; b_i \in K \right\}.$$

Д о к а з а т е л ь с т в о. Обозначим множество сумм, стоящих в правой части, символом L. Включение $(M) \supseteq L$ очевидно. Проверим, что множество L действительно образуют идеал:

а) так как $\sum m_i\, b_i + \sum m_i\, b'_i = \sum m_i\, (b_i + b'_i)$, то множество L замкнуто относительно сложения;

б) так как $-\sum m_i\, b_i = \sum m_i\, (-b_i)$, то множество L замкнуто относительно взятия противоположного элемента;

в) так как $(\sum m_i\, b_i) \cdot c = \sum m_i\, (b_i c)$, то умножение на c переводит сумму из L в аналогичную сумму из L.

Следовательно, множество L является идеалом и содержит M, т. е. имеет место включение $(M) \subseteq L$.

Таким образом, мы установили, что множество сумм

$$\left\{ \sum m_i\, b_i \;\middle|\; m_i \in M, b_i \in K \right\}$$

является наименьшим идеалом, содержащим M. Лемма доказана.

У п р а ж н е н и е. Где в этой лемме используется наличие единицы в K?

У п р а ж н е н и е. Что изменится, если кольцо K не коммутативно?

О п р е д е л е н и е. Идеал, порожденный одним элементом, называется *главным.*

П р и м е р. Очевидно, $n\mathbb{Z} = (n)$, n — порождающий идеала $n\mathbb{Z}$. При этом

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}.$$

3.9. Фактор–кольца. В этом пункте мы рассмотрим понятие конгруэнции для колец и определим фактор–кольцо. Рассмотрим кольцо K и его подкольцо L. Так же как для групп введем отношение левой смежности на множестве K, полагая по определению:

$$a \sim b \;\Leftrightarrow\; a - b \in L$$

и, аналогично, отношение правой смежности:

$$a \sim b \;\Leftrightarrow\; -a + b \in L.$$

Учитывая, что из включения $a-b \in L$ следует включение $-(a-b) = b-a = -a+b \in L$, заключаем, что для колец отношение левой смежности совпадает с отношением правой смежности. Поэтому далее будем говорить просто про отношение смежности. Покажем, что это отношение является отношением эквивалентности. Имеем

1) $a \sim a$ так как $a-a \in L$;

2) если $a \sim b$, т. е. $a-b \in L$, то, учитывая, что L — подкольцо, заключаем

$$-(a-b) = b-a \in L,$$

а потому $b \sim a$;

3) если $a \sim b$, т. е. $a-b \in L$ и $b \sim c$, т. е. $b-c \in L$, то, учитывая, что L — подкольцо, заключаем

$$(a-b)+(b-c) = a-c \in L,$$

а потому $a \sim c$.

Каждому элементу $a \in K$ отвечает класс эквивалентности

$$K_a = \{x \in K \mid x \sim a\}$$

— множество элементов, эквивалентных a. Покажем, что этот класс эквивалентности равен

$$a+L = \{a+l \mid l \in L\}.$$

Действительно, если $x \in K_a$, то $x \sim a \Leftrightarrow x-a = l \in L$, а потому $x = a+l \in a+L$. Обратно, если $x = a+l \in a+L$, то $x-a = l \in L$, что означает $x \sim a$, т. е. $x \in K_a$. Будем называть класс эквивалентности $K_a = a+L$ *смежным классом* кольца K по подкольцу L.

Число смежных классов $a+L$ называется *индексом* подкольца L в кольце K и обозначается $|K:L|$.

Таким образом, мы имеем разложение кольца K:

$$K = \bigcup_{a \in K} (a+L).$$

По теореме о разбиении, в каждом классе эквивалентности можно выбрать по одному представителю и представить K в виде независимого объединения смежных классов:

$$K = \coprod_{a_i \in J} (a_i + L),$$

где мощность множества J равна индексу $|K : L|$.

Таким образом, мы научились по всякому подкольцу L кольца K строить фактор–множества, состоящие из смежных классов. Возникает естественный вопрос: можно ли на этом фактор–множестве определить структуру кольца? Для этого, как мы знаем из теории алгебраических систем, отношение эквивалентности, разбивающее множество K на классы, должно быть конгруэнцией на кольце K, т. е. быть стабильным относительно операций сложения и умножения: если $a \sim a'$ и $b \sim b'$, то $a + b \sim a' + b'$ и $ab \sim a'b'$. Это означает, что если $a' = a + l_1$ и $b' = b + l_2$, то $a' + b' = a + b + l_3$ и $a'b' = ab + l_4$ для некоторых $l_1, l_2, l_3, l_4 \in H$. Для доказательства заметим, что

$$a' + b' = (a + l_1) + (b + l_2) = (a + b) + (l_1 + l_2).$$

Полагая $l_3 = l_1 + l_2$, видим, что $a + b \sim a' + b'$.

Рассмотрим произведение:

$$a'b' = (a + l_1) \cdot (b + l_2) = ab + al_2 + l_1b + l_1l_2.$$

Положим $l_4 = al_2 + l_1b + l_1l_2$. Видим, что этот элемент лежит в L, если для любых $a, b \in K$ справедливо включение

$$aL \subseteq L, \quad Lb \subseteq L,$$

которое, как мы знаем, выполняется если подкольцо L является идеалом. Таким образом, множество смежных классов

$$K/L = \{a + L \mid a \in K\}$$

относительно введенных операций сложения и умножения является алгебраической системой. Более того, справедлива

Т е о р е м а. *Пусть I — идеал кольца K. На множестве смежных классов K/I определим сумму и произведение смежных классов равенствами*

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = ab + I, \quad a, b \in K.$$

Тогда алгебраическая система $\langle K/I; +, \cdot \rangle$ является кольцом и существует кольцевой гомоморфизм $K \to K/I$, переводящий элемент a из K в смежный класс, которому принадлежит a. Этот гомоморфизм называется естественным гомоморфизмом.

Д о к а з а т е л ь с т в о. Выше мы показали, что для идеала I отношение смежности является конгруэнцией и из теоремы о

фактор–системах (см. § 1) следует, что $\langle K/I; +, \cdot\rangle$ является алгебраической системой. Покажем, что эта алгебраическая система является кольцом. Заметим, что $\langle K; +\rangle$ — абелева группа, а потому I – её нормальная подгруппа. По теореме о фактор–группах из § 2, алгебраическая система $\langle K/I; +\rangle$ является абелевой группой. При этом смежный класс $0 + I = I$ является нулевым элементом, а противоположным к классу $a + I$ является класс $-(a + I) = (-a) + I$.

Покажем, что операция умножения на множестве смежных классов K/I ассоциативна. Действительно,

$$(a + I) \cdot ((b + I) \cdot (c + I)) = (a + I) \cdot (bc + I) = a(bc) + I = (ab)c + I =$$

$$= (ab + I) \cdot (c + I) = ((a + I) \cdot (b + I)) \cdot (c + I).$$

Проверим левую дистрибутивность:

$$(a+I)\cdot((b+I)+(c+I)) = (a+I)\cdot(b+c+I) = a(b+c)+I = (ab+ac)+I =$$

$$= (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I).$$

Правая дистрибутивность проверяется аналогично. Таким образом, мы показали, что $\langle K/I; +, \cdot\rangle$ является кольцом.

Если K — кольцо с единице 1, то смежный класс $1 + K$ является единицей кольца K/I. Если кольцо K — коммутативно, то и K/I — коммутативно.

Рассмотрим отображение $\varphi\colon K \to K/I$, переводящее a в класс $a + I$. Покажем, что это отображение является гомоморфизмом. Действительно, выберем $a, b \in K$ и, по определению, найдем

$$\varphi(a + b) = (a + b) + I, \quad \varphi(ab) = (ab) + I.$$

С другой стороны, по определению операций на смежных классах, имеем

$$\varphi(a) + \varphi(b) = (a + I) + (b + I) = (a + b) + I,$$

$$\varphi(a) \cdot \varphi(b) = (a + I) \cdot (b + I) = ab + I.$$

Следовательно, $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Теорема доказана.

П р и м е р. Пусть $K = \mathbb{Z}$ – кольцо целых чисел, $I = n\mathbb{Z}$ — идеал в $\mathbb{Z}$. Тогда

$$K = \coprod_{a\in\{0,1,\ldots,n-1\}} (a + I)$$

— разбиение множества K. По доказанной теореме, K/I является кольцом. Заметим, что это кольцо изоморфно кольцу вычетов $\mathbb{Z}_n$ по модулю n. Изоморфизм задается отображением

$$a + I \mapsto \bar{a}, \quad a \in \{0, 1, \ldots, n-1\}.$$

Как мы видели ранее, существует эпиморфизм $\mathbb{Z} \to \mathbb{Z}_n$. Его ядро $I = n\mathbb{Z}$ является идеалом и фактор–кольцо $\mathbb{Z}/n\mathbb{Z}$ изоморфно $\mathbb{Z}_n$.

На самом деле, это общий факт, который гласит, что если $\varphi\colon K \to K'$ — эпиморфизм колец, то имеет место изоморфизм $K/\operatorname{Ker}\varphi \cong K'$ (теорема о гомоморфизме колец).

3.10. *Задачи по кольцам и полям.*

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций. (Если операции не указаны, то подразумеваются сложение и умножение чисел.)

1) (П, 1709) Целые числа.

2) (П, 1710) Четные числа.

3) (П, 1711) Целые числа, кратные данному числу n (рассмотреть, в частности, случай $n = 0$).

4) (П, 1712) Рациональные числа.

5) (П, 1713) Действительные числа.

6) (П, 1714) Комплексные числа.

7) (П, 1715) Числа вида $a + b\sqrt{2}$ с целыми a и b.

8) (П, 1716) Числа вида $a + b\sqrt{3}$ с рациональными a и b.

9) (П, 1721) Функции с действительными значениями, непрерывные на отрезке $[-1, +1]$ относительно обычных сложения и умножения функций.

10) (П, 1722) Многочлены от одного неизвестного x с целыми коэффициентами относительно обычных операций сложения и умножения.

11) (П, 1723) Многочлены от одного неизвестного x с действительными коэффициентами относительно обычных операций.

12) (П, 1734) Показать, что пары (a, b) целых чисел с операциями, заданными равенствами

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2),$$

образуют кольцо, и найти все делители нуля этого кольца.

13) (П, 1735) Доказать, что поле не имеет делителей нуля.

14) (П, 1741) Пусть дано целое число $n \geq 0$. Два целых числа a и b называются *сравнимыми по модулю* n, что записывается так: $a \equiv b \pmod{n}$, если их разность $a - b$ делится на n (при $n = 0$ это означает, что $a = b$; при $n > 0$ — что a и b при делении на n дают один и тот же остаток — вычет по модулю n). Показать, что совокупность всех целых чисел $\mathbb{Z}$ разбивается на классы сравнимых между собой чисел, не имеющие общих элементов. Определим сложение и умножение классов через соответствующие операции над их представителями, т. е. если числа a, b, $a+b$ и ab принадлежат соответственно классам A, B, C и D, то положим $A + B = C$ и $AB = D$.

Доказать, что при таких операциях множество классов является кольцом (кольцо вычетов $\mathbb{Z}_n$ по модулю n).

15) (П, 1742*) Доказать, что конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем.

16) (П, 1743*) Показать, что кольцо вычетов по модулю n будет полем тогда и только тогда, когда n — число простое.

17) (П, 1751*) Доказать, что при любом изоморфизме числовых полей подполе рациональных чисел отображается тождественно.

В частности, поле рациональных чисел допускает лишь тождественное изоморфное отображение в себя.

18) (П, 1754) Доказать, что минимальное подполе любого поля характеристики нуль изоморфно полю рациональных чисел.

19) (П, 1755) Доказать, что минимальное подполе любого поля характеристики p изоморфно полю вычетов по модулю p.

20) На множестве многочленов $\mathbb{Q}[x]$ определим композицию многочленов $f, g \in \mathbb{Q}[x]$ равенством $(f \circ g)(x) = g(f(x))$. Будет ли алгебраическая система $\langle \mathbb{Q}[x]; +, \circ \rangle$ кольцом? Если да, то изоморфно ли оно кольцу многочленов $\langle \mathbb{Q}[x]; +, \cdot \rangle$ с обычной операцией умножения?

21) При каких натуральных n, множество

$$L_n = \{a + \sqrt{n}b \mid a, b \in \mathbb{Q}\}$$

с операциями сложения и умножения будет полем? Будет ли поле L_2 изоморфно полю L_3? При каких натуральных p и q имеет место изоморфизм $L_p \cong L_q$?

22) Пусть $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \ldots, \bar{5}\}$ — множество классов вычетов по модулю 6. Для каждого $k = 0, 1, \ldots, 5$ определим на множестве $\mathbb{Z}_6$ унар-

ную алгебраическую операцию f_k правилом $f_k(\bar{a}) = \bar{a} + \bar{k}$. Будет ли алгебраическая система $A_1 = \langle \mathbb{Z}_6, f_1 \rangle$ изоморфна алгебраической системе $A_3 = \langle \mathbb{Z}_6, f_3 \rangle$?

23) Изоморфны ли группа $\mathbb{Z}_4$ по сложению и группа $\mathbb{Z}_5 \setminus \{0\}$ по умножению?

3.11. *Задачи для любознательных.*

1) (BMO, 1923) Доказать, что все члены арифметической прогрессии, образованной из целых положительных чисел, не могут быть простыми числами (за исключением вырожденного случая — арифметической прогрессии с нулевой разностью, все члены которой равны одному и тому же простому числу).

2) (BMO, 1938) Доказать, что целое число представимо в виде суммы двух квадратов тогда и только тогда, когда вдвое большее число обладает тем же свойством.

3) (BMO, 1940) Пусть m и n — два различных целых положительных числа. Доказать, что

$$2^{2^m} + 1 \text{ и } 2^{2^n} + 1$$

не имеют ни одного общего делителя, большего 1.

3.12. *Мозаика: замощение прямоугольника, сумма двух простых чисел.*

Замощение прямоугольника. Сколькими способами можно замостить прямоугольник $2 \times n$, $n \in \mathbb{N}$ прямоугольниками 2×1? Представьте ответ в виде функции от n. Замостить означает выложить прямоугольниками без наложений и пустых клеток.

Натуральные числа как сумма двух простых. Развлекаясь с натуральными числами, натыкаемся на такие равенства

$$3 + 7 = 10,$$

$$3 + 17 = 20,$$

$$13 + 17 = 30.$$

Попытаемся продолжить эту последовательность, увеличивая слагаемые на 10. Получим

$$13 + 27 = 40,$$

$$23 + 27 = 50.$$

Теперь закономерность ясна и мы можем написать ещё 2 равенства:

$$23 + 37 = 60,$$

$$33 + 37 = 70.$$

Что можно извлечь из этих равенств? Мы представили числа, кратные 10 в виде суммы двух чисел. Здесь нет ничего необычного, но давайте посмотрим на первые три равенства. Заметим, что все числа, стоящие в левой части: 3, 7, 13 являются простыми, т. е. мы представили 10, 20 и 30 в виде суммы двух простых. В четвёртом и пятом равенствах число $27 = 3^3$ не является простым. В шестом равенстве опять оба числа, стоящие в левой части — простые, но в седьмом равенстве число $33 = 3 \cdot 11$ не является простым. А что можно сказать про другие чётные числа? Будем представлять их в виде суммы натуральных чисел, больших 1. Получим

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5, \quad 10 = 3 + 7,$$

$$12 = 5 + 7, \quad 14 = 3 + 11, \quad 16 = 3 + 13 = 5 + 11, \ldots$$

Видим, что нам удалось представить четные числа, не превосходящие 16, а также числа 20, 30 и 60 в виде суммы двух простых чисел, но не удалось это сделать для 40, 50 и 70. Немного повозившись, найдем такие равенства:

$$3 + 37 = 40, \quad 3 + 47 = 50, \quad 3 + 67 = 70,$$

в которых числа 3, 37, 47 и 67 являются простыми. Можно найти и другие разложения в сумму простых:

$$11 + 29 = 17 + 23 = 40,$$

$$7 + 43 = 13 + 37 = 19 + 31 = 50,$$

$$11 + 59 = 17 + 53 = 23 + 47 = 29 + 41 = 70.$$

Анализируя полученные результаты, кажется справедливой

Гипотеза. Любое четное число, большее 4, представимо в виде суммы двух нечётных простых чисел.

Сможете доказать? Первым троим, доказавшим или опровергнувшим эту гипотезу, готов поставить оценку «отлично» за экзамен.

Если мы рассмотрим простые числа, то некоторые из них, являются суммой двойки и другого простого числа. Например,

$$5 = 2+3,\ \ 7 = 2+5,\ \ 13 = 2+11,\ \ 19 = 2+17,\ \ 31 = 2+29,\ \ 43 = 2+41,$$

$$61 = 2+59,\ \ 73 = 2+71,\ \ 103 = 2+101,\ \ 109 = 2+107,\ \ 139 = 2+137,$$

$$151 = 2+149,\ \ 181 = 2+179.$$

Возникает естественный

Вопросы. 1) Верно ли, что таких простых чисел бесконечно много?

2) Верно ли, что таких пар простых чисел, у которых одно оканчивается на 1, а второе на 9 также бесконечно много?

Кольцо Маяковского. Как писал В. В. Маяковский в поэме «Единица — ноль, единица — вздор, ...». Это значит, что в кольце Маяковского единица равна нулю. Нетрудно показать, что в таком кольце всякий элемент равен нулю. Следовательно, кольцо Маяковского не является полем.

§ 4. Группы подстановок

В этом параграфе мы познакомимся с одним из важнейших примеров групп — группами подстановок. Это первый нетривиальный пример групп, которые изучал Э. Галуа, занимаясь задачей о разрешимости уравнения в радикалах. С другой стороны, группы подстановок — это универсальное хранилище всех групп, т. е. всякая группа может быть вложена в группу подстановок некоторого множества. Мы, в основном, будем рассматривать подстановки конечных множеств, но многие результаты без труда переносятся на счетные и даже на произвольные множества.

4.1. Определения и примеры. Пусть

$$M_n = \{1, 2, 3, \ldots, n\}$$

— конечное множество. *Подстановкой* множества M_n называется взаимно однозначное отображение этого множества на себя. Всякую подстановку можно записать в виде

$$a = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix},$$

где в верхней строке перечислены все элементы из M_n, а в нижней строке — под каждым элементом подставлен его образ из M_n при отображении a. Именно, благодаря этой форме записи, используется термин *подстановка*. Очевидно, одна и та же подстановка может быть записана несколькими способами, например,

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

На множестве подстановок определим умножение.

Произведением двух подстановок называется третья, равная последовательному выполнению первой, а затем второй.

П р и м е р. Если

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$$

то их произведения

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad ba = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Из этого примера видим, что операция умножения подстановок некоммутативна.

Обозначим

$$S_n = \{\text{подстановки множества } M_n\}$$

и будем называть *множеством подстановок степени* n. Нетрудно проверить, что $|S_n| = n!$, где символом $|A|$ обозначается число элементов множества A.

Справедлива

Т е о р е м а 1. *Множество S_n с операцией умножения образует группу. При $n \geq 3$ она неабелева.*

Д о к а з а т е л ь с т в о. То, что $\langle S_n; \cdot \rangle$ является алгебраической системой, следует из определения произведения подстановок. Проверим аксиомы группы.

1) Ассоциативность: проверим, что для любых подстановок a, b, c из S_n справедливо равенство

$$(ab)c = a(bc).$$

Для этого обозначим $ab = d$, $dc = f$ — левая часть равенства; $bc = g$, $ag = h$ — правая часть равенства. Выберем некоторый символ i из $M_n = \{1, 2, \ldots, n\}$ и подействуем на него подстановкой f. Получим

$$if = (id)c = ((ia)b)c.$$

Действуя подстановкой h, получим

$$ih = (ia)g = ((ia)b)c.$$

Следовательно, на каждый символ $i \in M_n$ подстановки f и h действуют одинаково, но это означает, что они равны, т. е. ассоциативность умножения выполняется.

2) Легко проверить, что единичным элементом является подстановка

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

оставляющая все символы на месте.

3) Пусть

$$a = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

— произвольная подстановка. Нетрудно убедиться, что обратной является подстановка

$$a^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Покажем, что при $n \geq 3$ группа S_n неабелева. Положим

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 3 & 2 & 1 & 4 & \ldots & n \end{pmatrix}.$$

Тогда $1(ab) = 2$, т. е. подстановка ab переводит символ 1 в символ 2, а $1(ba) = 3$, т. е. подстановка ba переводит символ 1 в символ 3. Следовательно, $ab \neq ba$. Теорема доказана.

Из этой теоремы, в частности, следует, что группа S_3 порядка 6 неабелева.

У п р а ж н е н и е. Существует ли неабелева группа порядка меньше 6?

4.2. Разложение подстановки в произведение независимых циклов. Рассмотрим подстановку

$$\begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_s & \dots & i_1 & \dots \end{pmatrix},$$

где все невыписанные символы остаются на месте. Тогда эту подстаноку будем записывать в виде $(i_1 i_2 \dots i_{s-1} i_s)$ и называть *циклической подстановкой*, или *циклом.*

П р и м е р. Подстановка

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 4 & 7 & 6 & 2 \end{pmatrix}$$

имеет следующее представление в виде цикла $a = (257)$. Заметим, что этот цикл можно записать несколькими способами:

$$(257) = (572) = (725).$$

Две циклические подстановки, или короче, два цикла называются *независимыми*, если их множества действительно перемещаемых символов не пересекаются. Легко заметить, что независимые циклы перестановочны.

П р и м е р. Пара зависимых циклов:

$$(123),\ (257)$$

(оба содержат символ 2); пара независимых циклов:

$$(134),\ (257).$$

Т е о р е м а 2. *Всякая нетождественная подстановка может быть разложена в произведение независимых циклов. Это разложение единственно с точностью до порядка множителей.*

Д о к а з а т е л ь с т в о. Пусть a — некоторая подстановка из S_n и t — число действительно перемещаемых символов. Проведём доказательство индукцией по t. Очевидно, что $t \geq 2$. При $t = 2$ имеем

$$a = \begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix} = (ij)$$

— цикл, и утверждение теоремы справедливо.

При $t > 2$ представим нашу подстановку в таком виде:

$$a = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \bullet\bullet\bullet & i_2 & \bullet\bullet\bullet & i_3 & \bullet\bullet\bullet & i_s & \bullet\bullet\bullet & i_1 & \bullet\bullet\bullet \end{pmatrix}.$$

Здесь мы выбрали некоторый символ i_1 и следим за тем, куда он переходит. Начиная с некоторого момента символы будут повторяться, и первым повтором будет символ i_1. Пропущенные символы отмечены разными типами точек в верхней и нижней строках, что означает, что эти символы тоже могут перемещаться.

Определим подстановку

$$b = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_s & \dots & i_1 & \dots \end{pmatrix},$$

в которой невыписанные символы остаются на месте, и подстановку

$$c = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \bullet\bullet\bullet & i_1 & \bullet\bullet\bullet & i_2 & \bullet\bullet\bullet & i_{s-1} & \bullet\bullet\bullet & i_s & \bullet\bullet\bullet \end{pmatrix},$$

в которой невыписанные символы переходят в те, в которые переходят символы подстановки a, а выписанные остаются на месте.

Заметим, что $bc = a$. При этом b — цикл длины s, в b и c нет общих перемещаемых символов и в c число перемещаемых символов равно $t - s$, т. е. на s меньше, чем в a. По предположению индукции

$$c = c_1\, c_2\, \dots\, c_p$$

— произведение независимых циклов. Следовательно,

$$a = b\, c_1\, c_2\, \dots\, c_p$$

— произведение независимых циклов. Таким образом, мы представили всякую подстановку $a \in S_n$ в виде произведения независимых циклов.

Докажем единственность. Пусть

$$a = c_1\, c_2\, \dots\, c_k = d_1\, d_2\, \dots\, d_l$$

— два разложения подстановки a в произведения независимых циклов. Заметим, что если какой–то символ встречается в одной записи, то он встречается и в другой (если символ перемещается, это указывается в любой записи). Возьмем некоторый перемещаемый символ i

и передвинем его в начало соответствующего цикла, а также поставим этот цикл на первое место. Будем иметь

$$c_1 = (i\,\alpha\,\beta\,\ldots\,\delta), \qquad d_1 = (i\,\alpha'\,\beta'\,\ldots\,\delta').$$

Это означает, что подстановка a содержит, с одной стороны, фрагмент

$$\begin{pmatrix} \ldots & i & \ldots \\ \bullet\bullet\bullet & \alpha & \bullet\bullet\bullet \end{pmatrix},$$

а с другой — фрагмент

$$\begin{pmatrix} \ldots & i & \ldots \\ \bullet\bullet\bullet & \alpha' & \bullet\bullet\bullet \end{pmatrix},$$

(учесть, что циклы независимы). Следовательно, $\alpha = \alpha'$. Теорема доказана.

4.3. Декремент. Чётность подстановки. *Декрементом* подстановки называется разность между числом действительно перемещаемых символов и числом независимых циклов.

П р и м е р. Пусть

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 7 & 2 & 3 & 5 & 8 \end{pmatrix} = (163)(2475).$$

Тогда декремент d равен $7 - 2 = 5$.

Если декремент подстановки — чётное число, то подстановка называется *чётной*. Если декремент — нечётное число, то подстановка называется *нечётной*. Подстановка, переставляющая только два символа, называется *транспозицией*. Очевидно, транспозиция — нечётная подстановка.

Т е о р е м а 3. *При умножении произвольной подстановки на транспозицию её чётность меняется.*

Д о к а з а т е л ь с т в о. Пусть

$$a = (i_1\,i_2\,\ldots\,i_r)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$$

— разложение подстановки a в произведение независимых циклов. Пусть при этом k — число действительно перемещаемых символов и l — число независимых циклов, декремент $d = k - l$. Рассмотрим транспозицию $b = (p\,q)$. При этом символы p и q могут либо входить, либо не входить в независимые циклы подстановки a. Разберем все эти случаи и результаты поместим в таблицу:

	Случаи	a
1	p и q не входят в a	$(i_1\, i_2\, \ldots\, i_r)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$
2	p входит, q не входит в a	$(p\, i_2\, \ldots\, i_r)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$
3	p не входит, q входит в a	$(q\, i_2\, \ldots\, i_r)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$
4	p и q входят в один цикл	$(p\,\ldots\,q\,\ldots)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$
5	p и q входят в разные циклы	$(p\,\ldots)\,(q\,\ldots)\,(j_1\,\ldots\, j_s)\,\ldots$

ab	k'	l'	d'
$(i_1\, i_2\, \ldots\, i_r)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots\,(p\, q)$	$k+2$	$l+1$	$d+1$
$(p\, i_2\, \ldots\, i_r\, q)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$	$k+1$	l	$d+1$
$(q\, i_2\, \ldots\, i_r\, p)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$	$k+1$	l	$d+1$
$(p\,\ldots)\,(q\,\ldots)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$	k	$l+1$	$d-1$
$(p\,\ldots\,q\,\ldots)\,(j_1\, j_2\, \ldots\, j_s)\,\ldots$	k	$l-1$	$d+1$

где k' — число действительно перемещаемых символов подстановки ab, l' — число её независимых циклов, а $d' = k' - l'$ — декремент. Анализируя последний столбец полученной таблицы, получаем требуемое утверждение.

Мы разобрали случай, когда подстановка a умножается на транспозицию $b = (pq)$ справа. Учитывая, что чётность подстановки и обратной к ней совпадают, ввиду равенства $(ab)^{-1} = ba^{-1}$ получаем нужное утверждение и при умножении подстановки слева на транспозицию.

Теорема доказана.

Т е о р е м а 4. *В группе S_n число чётных и нечётных подстановок одно и то же и равно $\frac{1}{2}n!$.*

Д о к а з а т е л ь с т в о. Пусть

$$P = \{a_1,\, a_2,\, \ldots,\, a_s\}$$

— множество всех чётных подстановок из S_n. Возьмём транспозицию $t = (1\,2)$ и рассмотрим множество подстановок:

$$Pt = \{a_1t,\, a_2t,\, \ldots,\, a_st\}.$$

По теореме 3 все эти подстановки нечётные. Чтобы доказать теорему, надо установить, что

1) в Pt все подстановки различны;

2) всякая нечётная подстановка из S_n содержится в множестве Pt.

Докажем 1). Предположим, что $a_it = a_jt$. Умножая обе части этого равенства справа на t, получим $a_it^2 = a_jt^2$. Учитывая, что t^2 —

тождественная подстановка, получим $a_i = a_j$, но так как в P все подстановки различны, то $a_i \neq a_j$.

Для доказательства 2) возьмём некоторую нечётную подстановку b и найдём $a = bt$. По теореме 3, подстановка a — чётная, а все чётные подстановки содержатся в множестве P. Следовательно, $a = a_i$ для некоторого i. Тогда в множестве Pt находим $a_i t = bt^2 = b$. Пункт 2) установлен.

Следовательно, число чётных и нечётных подстановок в S_n одно и то же, а так как в S_n содержится $n!$ элементов, то это число равно $\frac{1}{2}n!$.

Теорема доказана.

4.4. Порождающие множества. Транспозиции являются простейшими подстановками. Как показывает следующая теорема, множество транспозиций является порождающим множеством группы подстановок.

Т е о р е м а 5. *Всякая подстановка разлагается в произведение транспозиций. Это разложение не является единственным, но чётность числа транспозиций всегда одна и та же и совпадает с чётностью самой подстановки.*

Следующее равенство показывает, что одна и та же подстановка может иметь различные разложения в произведение транспозиций:

$$(2\,3) = (1\,2)\,(1\,3)\,(1\,2).$$

Д о к а з а т е л ь с т в о т е о р е м ы. Рассмотрим некоторую подстановку a и представим её в виде произведения независимых циклов:

$$a = c_1\, c_2\, \ldots\, c_s.$$

Легко проверить, что каждый цикл разлагается в произведение транспозиций:

$$(i_1\, i_2\, \ldots\, i_t) = (i_1\, i_2)\,(i_1\, i_3)\, \ldots\, (i_1\, i_t).$$

Следовательно, и сама подстановка a разлагается в произведение транспозиций:

$$a = t_1\, t_2\, \ldots\, t_k.$$

Так как транспозиция — нечётная подстановка, а при умножении её на транспозицию получаем чётную подстановку, то по теореме 3 чётность k равна четности a. Теорема доказана.

У п р а ж н е н и е. Докажите, что наименьшее число транспозиций, в произведение которых можно разложить данную подстановку, равно её декременту.

Отметим, что найденное в теореме множество порождающих группы S_n при $n > 2$ не является минимальным ($S_2 = \text{гр}((1\,2))$ — циклическая группа порядка 2).

У п р а ж н е н и е. Группа S_n порождается множеством транспозиций $(1\,2)$, $(1\,3)$, $\ldots$, $(1\,n)$.

Оказывается, что и это множество не является минимальным.

У п р а ж н е н и е. Группа S_n, $n > 2$, порождается транспозицией $(1\,2)$ и циклом $(1\,2\,\ldots\,n)$.

Чётные подстановки образуют подгруппу группы S_n, которая называется *знакопеременной группой* и обозначается символом A_n.

У п р а ж н е н и е. Найдите собственные нормальные подгруппы группы A_4.

Оказывается, что при $n \geq 5$, группа A_n является простой, т. е. не содержит собственных нормальных подгрупп. Отметим, что именно этот факт лежит в основе доказательства неразрешимости в радикалах общего уравнения пятой степени.

4.5. Гомоморфизм группы S_n на группу $\mathbb{Z}_2$. Из теорем 3, 4 и 5 легко выводится

П р е д л о ж е н и е 1. *Группа A_n является нормальной подгруппой группы S_n и фактор–группа S_n/A_n — циклическая группа порядка 2.*

Д о к а з а т е л ь с т в о. При $n = 2$ группа S_2 — циклическая группа порядка 2 и A_2 — единичная группа. В этом случае теорема очевидна. Будем считать, что $n > 2$ и возьмем элемент $a \in A_n$, а также элемент $b \in S_n$. Надо показать, что $b^{-1}ab \in A_n$. Для этого представим b в виде произведения транспозиций. Если таких транспозиций k, то подстановка $b^{-1}ab$ получается из a умножением на $2k$ транспозиций (k транспозиций слева и k транспозиций справа), а потому $b^{-1}ab \in A_n$.

Далее, из теоремы 4 вытекает, что S_n является независимым объединением смежных классов $S_n = A_n \sqcup (12)A_n$. По теореме о фактор–группах, эти смежные классы образуют группу относительно умножения

$$A_n \cdot A_n = A_n, \;\; A_n \cdot (12)A_n = (12)A_n \cdot A_n = (12)A_n, \;\; (12)A_n \cdot (12)A_n = A_n.$$

Очевидно, это циклическа группа порядка 2.

Предложение доказано.

О п р е д е л е н и е. *Знаком подстановки a* назовём следующее

число:

$$\operatorname{sgn} a = \begin{cases} +1 & \text{если } a \text{ четная,} \\ -1 & \text{если } a \text{ нечетная.} \end{cases}$$

Л е м м а. *Для любых подстановок a и b из S_n справедливы равенства*:

$$\operatorname{sgn}(a \cdot b) = \operatorname{sgn} a \cdot \operatorname{sgn} b,$$

$$\operatorname{sgn}(a^{-1}) = \operatorname{sgn} a.$$

Д о к а з а т е л ь с т в о. Представим подстановки a и b в виде произведения транспозиций:

$$a = a_1\, a_2\, \ldots\, a_s, \quad b = b_1\, b_2\, \ldots\, b_t.$$

Тогда

$$a\, b = a_1\, a_2\, \ldots\, a_s\, b_1\, b_2\, \ldots\, b_t,$$

$$a^{-1} = a_s\, \ldots\, a_2\, a_1.$$

По теореме 5

$$\operatorname{sgn} a = (-1)^s, \quad \operatorname{sgn} b = (-1)^t, \quad \operatorname{sgn}(a\, b) = (-1)^{s+t}, \quad \operatorname{sgn}(a^{-1}) = (-1)^s.$$

Лемма доказана.

П р е д л о ж е н и е 2. *Отображение*

$$sgn\colon S_n \to \langle \{-1, 1\}; \cdot \rangle \cong \mathbb{Z}_2$$

является гомоморфизмом групп, ядро которого — группа четных подстановок A_n и фактор–группа $S_n/\operatorname{Ker}(sgn)$ изоморфна $\mathbb{Z}_2$.

Д о к а з а т е л ь с т в о. То, что отображение sgn — гомоморфизм, следует из предыдущей леммы. Кроме того, очевидно, что $a \in \operatorname{Ker}(sgn)$ тогда и только тогда, когда a — четна, т. е. лежит в A_n. Ввиду предложения 1, отображение

$$A_n \mapsto 1, \quad (12)A_n \mapsto -1$$

даёт нужный изоморфизм. Предложение доказано.

Отметим, что так же как для колец, для групп справедлива теорема о гомоморфизме, утверждающая, что если $\varphi\colon G \to G'$ — эпиморфизм группы G на группу G', то имеет место изоморфизм $G/\operatorname{Ker}\varphi \cong G'$.

4.6. Теорема Кэли. Докажем теорему, о которой упоминали в начале параграфа, о том, что группы подстановок являются вместилищем всех конечных групп.

Т е о р е м а (Кэли). *Всякая конечная группа порядка n изоморфна некоторой подгруппе группы подстановок степени n.*

Д о к а з а т е л ь с т в о. Пусть

$$G = \{g_1, g_2, \ldots, g_n\}$$

— некоторая конечная группа. Хотим представить её подстановками некоторого конечного множества. В качестве этого множества возьмём саму G, так как ничего другого у нас нет. Сопоставим элементу g из G подстановку $\widehat{g}$, первая строка которой — элементы из G. Умножим эти элементы справа на g и запишем полученные элементы во вторую строчку:

$$\widehat{g} = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_1 g & g_2 g & \ldots & g_n g \end{pmatrix}.$$

Из аксиом группы следует, что элементы второй строки попарно различны, а потому $\widehat{g}$ является подстановкой. Надо проверить, что отображение $\widehat{\ }$ является изоморфизмом. Вначале заметим, что это гомоморфизм

$$\widehat{a\,b} = \widehat{a}\,\widehat{b} \quad \text{для всех } a, b \in G.$$

Действительно, на каждый элемент $x \in G$ обе части равенства действуют одинаково:

$$x\widehat{a\,b} = x(ab) = (xa)b = (x\widehat{a})\,\widehat{b} = x(\widehat{a}\,\widehat{b}).$$

Далее, ядро отображения $\widehat{\ }$ тривиально: если $\widehat{g} = e$ — тождественная подстановка, то подстановка $\widehat{g}$ переводит единичный элемент 1, с одной стороны, в g, а с другой — оставляет на месте, поэтому $g = 1$.

Теорема доказана.

4.7. *Задачи по подстановкам.*

Следующие подстановки разложить в произведение независимых циклов и по декременту (т. е. разности между числом действительно перемещаемых элементов и числом циклов) определить их чётность. Для удобства подсчёта декремента можно для чисел, остающихся на месте, ввести в разложение одночленные циклы.

1) (П. 151) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$.

2) (П. 152) $\begin{pmatrix}1&2&3&4&5&6\\6&5&1&4&2&3\end{pmatrix}$.

3) (П. 153) $\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&3&6&5&7&4&2\end{pmatrix}$.

4) (П. 154) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\5&8&9&2&1&4&3&6&7\end{pmatrix}$.

В следующих подстановках перейти от записи в циклах к записи двумя строками:

5) (П. 163) (15)(234).

6) (П. 164) (13)(25)(4).

7) (П. 174) Доказать, что если некоторая степень цикла равна единице, то показатель степени делится на длину цикла. (Длиной цикла называется число его элементов.)

8) (П. 174) Доказать, что среди всех степеней подстановки, равных единице, наименьший показатель равен наименьшему общему кратному длин циклов, входящих в разложение подстановки.

9) (П. 176*) Найти A^{100}, где $A = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&5&4&1&7&10&2&6&9&8\end{pmatrix}$.

10) (П. 177) Найти A^{150}, где $A = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&5&4&6&9&7&1&10&8&2\end{pmatrix}$.

11) (П. 178) Найти подстановку X из равенства $AXB = C$, где

$$A = \begin{pmatrix}1&2&3&4&5&6&7\\7&3&2&1&6&5&4\end{pmatrix}, \quad B = \begin{pmatrix}1&2&3&4&5&6&7\\3&1&2&7&4&5&6\end{pmatrix},$$

$$C = \begin{pmatrix}1&2&3&4&5&6&7\\5&1&3&6&4&7&2\end{pmatrix}.$$

12) (П. 184*) Найти все подстановки чисел 1, 2, 3, 4, перестановочные с подстановкой

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

13 (П. 185) Найти все подстановки чисел 1, 2, 3, 4, 5, перестановочные с подстановкой

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

14) (П, 1658*) Доказать утверждения:

а) симметрическая группа S_n при $n > 1$ порождается множеством всех транспозиций (i, j);

б) симметрическая группа S_n при $n > 1$ порождается транспозициями: $(1,2),(1,3),\ldots,(1,n)$;

в) знакопеременная группа A_n при $n > 2$ порождается множеством всех тройных циклов (ijk);

г) знакопеременная группа A_n при $n > 2$ порождается тройными циклами: $(123),(124),\ldots,(12n)$.

4.8. *Задачи для любознательных.*

1) (ВМО, 1906) Пусть $a_1, a_2, \ldots, a_n$ — некая перестановка чисел $1, 2, \ldots, n$. Доказать, что произведение

$$(a_1 - 1)(a_2 - 2)(a_3 - 3) \cdot \ldots \cdot (a_n - n)$$

равно чётному числу, если n нечётно.

4.9. *Мозаика: чётные и нечётные латинские квадраты.*

Под *латинским квадратом* понимается квадратная $n\times n$–таблица, заполненная n символами так, что в каждой строке и в каждом столбце все символы различны.

Сформулируем более серьезную задачу, связанную с латинскими квадратами (см. Кострикин А. И. Введение в алгебру: в 3-х ч. М.: Физматлит, 2000. Часть 2, с. 343). Пусть L — латинский квадрат $n\times n$, заполненный символами $\{0,1,\ldots,n-1\}$. Знаком строки или столбца квадрата L называется знак перестановки на множестве $\{0,1,\ldots,n-1\}$, отвечающий данной строке или данному столбцу. Произведение всех $2n$ знаков строк и столбцов называется знаком $\varepsilon(L)$ квадрата L. Квадрат L называется чётным, если $\varepsilon(L) = +1$, и нечётным, если $\varepsilon(L) = -1$. При нечётном n число чётных и нечётных латинских квадратов порядка n одинаково, но уже при $n = 2, 4, 6$ это не так. В 1986 г. Алон–Тарси предложил следующую гипотезу.

Гипотеза. Пусть n — чётное натуральное число. Тогда $\sum \varepsilon(L) \neq 0$, где сумма берётся по всем латинским квадратам L порядка n.

В 1997 г. было доказано, что если $n = p + 1$, где p — нечётное простое число, то гипотеза верна. Верна ли гипотеза для $n = p^k + 1$?

§ 5. Кольца матриц

5.1. Матрицы. Сложение и умножение матриц. *Матрицей*

размера $m \times n$ над кольцом K называется таблица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad a_{ij} \in K.$$

В дальнейшем будем записывать такие матрицы как $A = (a_{ij})_{i,j=1}^{m,n}$ или, если размеры матрицы ясны, просто как $A = (a_{ij})$. Матрицу A можно представлять либо как набор m строк:

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_m \end{pmatrix}, \quad \text{где } A_i = (a_{i1}, a_{i2}, \dots, a_{in}), \quad i = 1, 2, \dots, m,$$

либо как набор n столбцов:

$$A = \begin{pmatrix} A^1 & A^2 & \dots & A^n \end{pmatrix}, \quad \text{где } A_j = \begin{pmatrix} a_{j1} \\ a_{j2} \\ \dots \\ a_{jm} \end{pmatrix}, \quad j = 1, 2, \dots, n.$$

Множество всех матриц размера $m \times n$ над кольцом K будем обозначать $M_{m\times n}(K)$.

Пусть заданы две матрицы, имеющие одинаковые размеры с элементами из одного кольца:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots\dots\dots\dots\dots\dots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}.$$

Тогда их *суммой* называется матрица

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

Если матрицы

$$F = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots\dots\dots\dots\dots\dots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{pmatrix}$$

и

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1k} \\ g_{21} & g_{22} & \dots & g_{2k} \\ \dots\dots\dots\dots\dots\dots \\ g_{n1} & g_{n2} & \dots & g_{nk} \end{pmatrix}$$

таковы, что число столбцов в F совпадает с числом строк в G, то мы можем определить *произведение*

$$F \cdot G = H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1k} \\ h_{21} & h_{22} & \dots & h_{2k} \\ \dots\dots\dots\dots\dots\dots \\ h_{m1} & h_{m2} & \dots & h_{mk} \end{pmatrix},$$

где

$$h_{ij} = f_{i1}\, g_{1j} + f_{i2}\, g_{2j} + \dots + f_{in}\, g_{nj} = \sum_{s=1}^{n} f_{is}\, g_{sj}.$$

П р и м е р. Произведение двух матриц равно

$$\begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 & 3 \\ -1 & 0 & 5 \\ 4 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 12 \\ 11 & 4 & 21 \end{pmatrix}.$$

Вы можете спросить: что за странное произведение? Ответ можно найти в следующем пункте.

5.2. Суперпозиция линейных замен. Рассмотрим две линейные замены переменных с коэффициентами из кольца K:

$$\begin{cases} x_1 = f_{11}\, y_1 + \dots + f_{1n}\, y_n, \\ x_2 = f_{21}\, y_1 + \dots + f_{2n}\, y_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_m = f_{m1}\, y_1 + \dots + f_{mn}\, y_n, \end{cases} \qquad f_{ij} \in K,$$

$$\begin{cases} y_1 = g_{11}\, z_1 + \dots + g_{1k}\, z_k, \\ y_2 = g_{21}\, z_1 + \dots + g_{2k}\, z_k, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ y_n = g_{n1}\, z_1 + \dots + g_{nk}\, z_k, \end{cases} \qquad g_{pq} \in K.$$

Если подставить вторую замену в первую, то получим

$$x_i = f_{i1}\,y_1 + \ldots + f_{in}\,y_n = f_{i1}(g_{11}\,z_1 + \ldots + g_{1k}\,z_k) + \ldots + f_{in}(g_{n1}\,z_1 + \ldots + g_{nk}\,z_k) =$$

$$= (f_{i1}\,g_{11} + f_{i2}\,g_{21} + \ldots + f_{in}\,g_{n1})\,z_1 + \ldots + (f_{i1}\,g_{1k} + f_{i2}\,g_{2k} + \ldots + f_{in}\,g_{nk})\,z_k =$$

$$= h_{i1}\,z_1 \,+\, h_{i2}\,z_2 \,+ \ldots +\, h_{is}\,z_k, \quad i = 1, 2, \ldots, m,$$

где

$$h_{ij} = f_{i1}\,g_{1j} \,+\, f_{i2}\,g_{2j} \,+ \ldots +\, f_{in}\,g_{nj} = \sum_{s=1}^{n} f_{is}\,g_{sj}.$$

Такая замена переменных, когда в одну подставляется другая, называется *суперпозицией линейных замен*. Получается опять линейная замена:

$$\begin{cases} x_1 = h_{11}\,z_1 \,+\, \ldots \,+ h_{1k}\,z_k, \\ x_2 = h_{21}\,z_1 \,+\, \ldots \,+ h_{2k}\,z_k, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_m = h_{m1}\,z_1 \,+\, \ldots \,+ h_{mk}\,z_k, \end{cases} \qquad c_{pq} \in K.$$

Если для переменных ввести матриц–столбцы

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_m \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix}, \quad Z = \begin{pmatrix} z_1 \\ z_2 \\ \cdots \\ z_k \end{pmatrix},$$

то формулы замен можно записать в таком виде

$$X = FY, \;\; Y = GZ \Rightarrow X = F(GZ) = (FG)Z = HZ.$$

5.3. Кольцо матриц. Как мы знаем, если матрицы квадратные, т. е. имеют размеры $n \times n$, то их можно складывать и умножать. Будем называть такие матрицы *матрицами степени* n. Определим множество

$$M_n(K) = \{\text{матрицы степени } n \text{ над } K\} = M_{n\times n}(K).$$

Т е о р е м а 1. *Если K — кольцо, то $\langle M_n(K);\, +,\, \cdot\,\rangle$ — кольцо. Если K — кольцо с единицей, то $\langle M_n(K);\, +,\, \cdot\,\rangle$ — кольцо с единицей.*

Д о к а з а т е л ь с т в о. То, что операции сложения и умножения матриц являются алгебраическими, следует из определения. Проверим аксиомы кольца.

С1. Рассмотрим матрицы $A, B, C \in M_n(K)$. Нам надо доказать, что

$$(A + B) + C = A + (B + C).$$

Рассмотрим элемент, стоящий на месте (i, j) в матрице $(A + B) + C$. Он равен $(a_{ij} + b_{ij}) + c_{ij}$. Так как K — кольцо, то

$$(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}).$$

Следовательно, сложение матриц ассоциативно.

С2. Устанавливается аналогичным образом, при этом учитывается тот факт, что сложение в кольце K коммутативно.

С3. В качестве нулевого элемента надо взять матрицу, у которой на всех местах стоят нули.

С4. Легко проверить, что если матрица $A \in M_n(K)$ имеет вид

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

то противоположная

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

Для проверки ассоциативности умножения (аксиома У1) $(AB)C = A(BC)$, введем обозначения:

$$AB = D, \quad DC = F, \quad BC = G, \quad AG = H.$$

Нужно доказать, что $F = H$. Имеем:

$$f_{ij} = \sum_{k=1}^{n} d_{ik}\, c_{kj} = \sum_{k=1}^{n} \left(\sum_{l=1}^{n} a_{il}\, b_{lk} \right) c_{kj} = \sum_{k=1}^{n} \sum_{l=1}^{n} (a_{il}\, b_{lk})\, c_{kj}.$$

С другой стороны,

$$h_{ij} = \sum_{p=1}^{n} a_{ip}\, g_{pj} = \sum_{p=1}^{n} a_{ip} \left(\sum_{q=1}^{n} b_{pq}\, c_{qj} \right) =$$

$$= \sum_{p=1}^{n} \sum_{q=1}^{n} a_{ip} \, (b_{pq} \, c_{qj}) = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{il} \, (b_{lk} \, c_{kj}),$$

где последнее равенство вытекает из следующего равенства:

$$\sum_{i=1}^{n} a_i = \sum_{p=1}^{n} a_p = a_1 + \ldots + a_n,$$

которое показывает, что индекс суммирования можно обозначить любой буквой.

Далее нам потребуется

Л е м м а 1. *Если* α_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$ — *элементы кольца* K, *то*

$$\sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij} = \sum_{j=1}^{s} \sum_{i=1}^{r} \alpha_{ij}.$$

Д о к а з а т е л ь с т в о. Построим матрицу

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1s} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2s} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{r1} & \alpha_{r2} & \ldots & \alpha_{rs} \end{pmatrix}.$$

Сначала складываем элементы в каждой строке, а затем складываем полученные элементы:

$$(\alpha_{11} + \alpha_{12} + \ldots + \alpha_{1s}) + \ldots + (\alpha_{r1} + \alpha_{r2} + \ldots + \alpha_{rs}) = \sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij};$$

затем складываем элементы в каждом столбце и находим сумму полученных элементов:

$$(\alpha_{11} + \alpha_{21} + \ldots + \alpha_{r1}) + \ldots + (\alpha_{1s} + \alpha_{2s} + \ldots + \alpha_{rs}) = \sum_{j=1}^{s} \sum_{i=1}^{r} \alpha_{ij}.$$

Из коммутативности сложения в K следует, что эти две суммы совпадают. Лемма доказана.

Воспользовавшись этой леммой, получим:

$$\sum_{l=1}^{n} \sum_{k=1}^{n} a_{il} \, (b_{lk} \, c_{kj}) = \sum_{k=1}^{n} \sum_{l=1}^{n} (a_{il} \, b_{lk}) \, c_{kj}.$$

Следовательно, аксиома У1 установлена.

Для доказательства СУ1, $(A+B)C = AC+BC$, введем обозначения

$$A+B=D, \quad DC=F, \quad AC=G, \quad BC=H, \quad G+H=U.$$

Нам надо доказать, что $F=U$. Для этого вычислим элемент, стоящий на месте (i,j) в матрице F. Имеем:

$$f_{ij} = \sum_{k=1}^{n} d_{ik}\, c_{kj} = \sum_{k=1}^{n} (a_{ik}+b_{ik})\, c_{kj}.$$

С другой стороны,

$$u_{ij} = g_{ij} + h_{ij} = \sum_{k=1}^{n} a_{ik}\, c_{kj} + \sum_{k=1}^{n} b_{ik}\, c_{kj} = \sum_{k=1}^{n} (a_{ik}+b_{ik}) c_{kj},$$

где в последнем равенстве мы воспользовались коммутативностью сложения и правой дистрибутивностью в кольце K.

Аксиома СУ2 проверяется аналогично.

Если K — кольцо с единицей 1, то единицей кольца $M_n(K)$ является единичная матрица E, у которой на главной диагонали стоят 1, а на всех остальных местах — нули. Теорема доказана.

5.4. Диагональные матрицы и трансвекции. В кольце $M_n(K)$ введем два класса матриц.

О п р е д е л е н и е. *Диагональной матрицей* называется матрица, у которой все элементы вне главной диагонали равны нулю:

$$\operatorname{diag}(\alpha_1, \ldots, \alpha_n) = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}.$$

О п р е д е л е н и е. *Трансвекцией* $T_{ij}(\beta)$, $1 \le i \ne j \le n$ называется матрица, у которой на главной диагонали стоят 1, на месте (i,j) – элемент $\beta \in K$, а на всех остальных местах – нули.

Посмотрим, что происходит при умножении произвольной матрицы на диагональную. Если матрицу умножить на диагональную

справа, то получим

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}\alpha_1 & a_{12}\alpha_2 & \dots & a_{1n}\alpha_n \\ a_{21}\alpha_1 & a_{22}\alpha_2 & \dots & a_{2n}\alpha_n \\ \dots & \dots & \dots & \dots \\ a_{n1}\alpha_1 & a_{n2}\alpha_2 & \dots & a_{nn}\alpha_n \end{pmatrix}.$$

Если матрицу умножить на диагональную слева, то получим

$$\begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1 a_{11} & \alpha_1 a_{12} & \dots & \alpha_1 a_{1n} \\ \alpha_2 a_{21} & \alpha_2 a_{22} & \dots & \alpha_2 a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_n a_{n1} & \alpha_n a_{n2} & \dots & \alpha_n a_{nn} \end{pmatrix}.$$

Таким образом, справедлива

Л е м м а 2. *При умножении произвольной матрицы на диагональную матрицу* $\operatorname{diag}(\alpha_1, \dots, \alpha_n)$ *справа первый столбец умножается на* α_1, *второй — на* α_2 *и т. д. При умножении произвольной матрицы на диагональную матрицу* $\operatorname{diag}(\alpha_1, \dots, \alpha_n)$ *слева первая строка умножается на* α_1, *вторая — на* α_2 *и т. д.*

Пусть дана трансвекция $T_{ij}(\beta)$. При умножении её на произвольную матрицу справа получим

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot T_{ij}(\beta) =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1,j-1} & a_{1i}\beta + a_{1j} & a_{1,j+1} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2,j-1} & a_{2i}\beta + a_{2j} & a_{2,j+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{n,j-1} & a_{ni}\beta + a_{nj} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix},$$

где сумма стоит в j–м столбце.

При умножении слева получим матрицу

$$T_{ij}(\beta)\cdot\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{i-1,1} & a_{i-1,2} & \dots & a_{i-1,n} \\ a_{i1}+\beta a_{j1} & a_{i2}+\beta a_{j2} & \dots & a_{in}+\beta a_{jn} \\ a_{i+1,1} & a_{i+1,2} & \dots & a_{i+1,n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

где сумма стоит в i–й строке.

Справедлива

Л е м м а 3. *При умножении произвольной матрицы на трансвекцию $T_{ij}(\beta)$ справа к ее j–му столбцу прибавляется i–й столбец, умноженный на β. При умножении произвольной матрицы на трансвекцию $T_{ij}(\beta)$ слева к ее i–й строке прибавляется j–я строка, умноженная на β.*

Отметим также следующие свойства трансвекций.

Л е м м а 4. 1) *Для произведения трансвекций справедливо равенство*

$$T_{ij}(\beta)\cdot T_{ij}(\gamma) = T_{ij}(\beta+\gamma).$$

2) *Обратной к трансвекции $T_{ij}(\beta)$ является трансвекция $T_{ij}(-\beta)$.*

Д о к а з а т е л ь с т в о. 1) По лемме 3 умножение $T_{ij}(\beta)$ справа на трансвекцию $T_{ij}(\gamma)$ соответствует тому, что мы к j–му столбцу матрицы $T_{ij}(\beta)$ прибавляем i–й столбец, умноженный на γ. В результате получим трансвекцию $T_{ij}(\beta+\gamma)$.

2) По пункту 1 имеем

$$T_{ij}(\beta)\cdot T_{ij}(-\beta) = T_{ij}(0),$$

а $T_{ij}(0)$ — единичная матрица.

5.5. Разложение матрицы в произведение диагональной и трансвекций. Основным результатом настоящего пункта является доказательство следующего утверждения.

Т е о р е м а 2. *Пусть P — поле. Всякая матрица $A \in M_n(P)$ разлагается в произведение*

$$A = T_1\, T_2\, \dots\, T_r\, D\, T_{r+1}\, T_{r+2}\, \dots\, T_s,$$

где D — диагональная матрица, T_i, $i = 1, 2, \ldots, s$, — трансвекции.

Доказательство. Назовем *элементарными преобразованиями матрицы* следующие преобразования:

1) прибавление к одной строке матрицы другой ее строки, умноженной на ненулевой элемент из P;

2) прибавление к одному столбцу матрицы другого ее столбца, умноженного на ненулевой элемент из P.

Используя индукцию по n, докажем, что при помощи этих элементарных преобразований всякую матрицу можно привести к диагональной матрице.

При $n = 1$ матрица A диагональная.

Предположим, что матрицы порядка $n - 1$ мы умеем приводить к диагональному виду. Рассмотрим матрицу $A = (a_{ij}) \in M_n(P)$ степени n. В зависимости от вида этой матрицы рассмотрим несколько случаев.

Случай 1: $a_{11} \neq 0$. Так как P — поле, то существует элемент a_{11}^{-1}, обратный к элементу a_{11}. Умножим первый столбец матрицы A на $-a_{1j}a_{11}^{-1}$ и прибавим к j–му столбцу, где $j = 2, 3, \ldots, n$. Получим матрицу, у которой все элементы, стоящие в первой строке, за исключением первого элемента, равны нулю:

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & a'_{22} & \ldots & a'_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a'_{n2} & \ldots & a'_{nn} \end{pmatrix}.$$

Умножим первую строку на $-a_{i1}a_{11}^{-1}$ и прибавим к i–ой строке для всех $i = 2, 3, \ldots, n$. Получим матрицу

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \ldots & 0 \\ \hline 0 & * & \ldots & * \\ \vdots & \multicolumn{3}{c}{\ldots\ldots\ldots} \\ 0 & * & \ldots & * \end{array}\right).$$

Применяя предположение индукции, приведем эту матрицу при помощи элементарных преобразований к диагональному виду:

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_n \end{pmatrix}.$$

Случай 2: $a_{11} = 0$, но какой–то элемент, a_{1j} или a_{i1}, $i, j \in \{2, 3, \ldots, n\}$, отличен от нуля. Если $a_{1j} \neq 0$, то умножим j-й столбец на единицу и прибавим к первому столбцу. Если $a_{i1} \neq 0$, то умножим i-ую строку на 1 и прибавим к первой строке. В обоих случаях приходим к разобранному выше случаю 1.

Случай 3: весь первый столбец и вся первая строка матрицы A состоят из нулей. В этом случае, воспользовавшись предположением индукции, приведем ее к диагональному виду.

Возвращаемся к доказательству теоремы. Как следует из леммы 3, умножение матрицы на трансвекцию справа соответствует элементарному преобразованию столбцов матрицы, а умножение матрицы на трансвекцию слева соответствует элементарному преобразованию строк матрицы. Таким образом, мы установили, что найдутся трансвекции $U_1, U_2, \ldots, U_r, U_{r+1}, \ldots, U_s$ такие, что

$$U_1 U_2 \ldots U_r A U_{r+1} \ldots U_s = D,$$

где D — некоторая диагональная матрица.

Воспользовавшись далее леммой 4, получим

$$A = U_r^{-1} U_{r-1}^{-1} \ldots U_1^{-1} D U_s^{-1} \ldots U_{r+1}^{-1},$$

где каждая U_i^{-1}, $i = 1, 2, \ldots, s$, как следует из леммы 4, является трансвекцией. Теорема доказана.

5.6. *Задачи на кольца матриц.*

Вычислить произведения матриц:

1) (П, 788)

$$\begin{pmatrix} 3 & -2 \\ 5 & -4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}.$$

2) (П, 789)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

3) (П, 790)

$$\begin{pmatrix} 1 & -3 & 2 \\ 3 & -4 & 1 \\ 2 & -5 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 5 & 6 \\ 1 & 2 & 5 \\ 1 & 3 & 2 \end{pmatrix}.$$

4) (П, 791)

$$\begin{pmatrix} 5 & 8 & -4 \\ 6 & 9 & -5 \\ 4 & 7 & -3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 & 5 \\ 4 & -1 & 3 \\ 9 & 6 & 5 \end{pmatrix}.$$

Вычислить выражения:

5) (П, 801)

$$\begin{pmatrix} 2 & -1 \\ 3 & -2 \end{pmatrix}^n.$$

6) (П, 802)

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^n.$$

7) (П, 803)

$$\begin{pmatrix} \lambda_1 & & & \mathbf{0} \\ & \lambda_2 & & \\ & & \ddots & \\ \mathbf{0} & & & \lambda_n \end{pmatrix}^k,$$

где нули обозначают, что все элементы матрицы, стоящие вне главной диагонали, равны нулю.

8) (П, 804)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n.$$

9) (П, 805)

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}^n.$$

10) (П, 811) Как изменится произведение AB матриц A и B, если:

а) переставить i–ю и j–ю строки матрицы A?

б) к i–й строке матрицы A прибавить j–ю строку, умноженную на число c?

в) переставить i–й и j–й столбцы матрицы B?

г) к i–му столбцу матрицы B прибавить j–й столбец, умноженный на число c?

11) (П, 814) Следом квадратной матрицы называется сумма элементов, стоящих на главной диагонали. Доказать, что след AB равен следу BA.

12) (П, 818) Матрицы A и B называются *перестановочными*, если $AB = BA$. Квадратная матрица A называется *скалярной*, если все её

элементы главной диагонали равны между собой, т. е. если $A = cE$, где c — число, а E — единичная матрица. Доказать утверждение: для того чтобы квадратная матрица A была перестановочна со всеми квадратными матрицами того же порядка, необходимо и достаточно, чтобы матрица A была скалярной.

12) (П, 827) Найти значение многочлена $f(x) = 3x^2 - 2x + 5$ от матрицы

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

13) (П, 828) Найти значение многочлена $f(x) = x^3 - 7x^2 + 13x - 5$ от матрицы

$$\begin{pmatrix} 5 & 2 & -3 \\ 1 & 3 & -1 \\ 2 & 2 & -1 \end{pmatrix}.$$

14) (П, 829) Доказать, что матрица $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ удовлетворяет уравнению

$$x^3 - (a + d)x + ad - bc = 0.$$

15) Разложить матрицу в произведение диагональной и трансвекций:

$$\text{а)} \begin{pmatrix} 1 & -3 & 2 \\ 3 & -4 & 1 \\ 2 & -5 & 3 \end{pmatrix}, \quad \text{б)} \begin{pmatrix} 2 & 5 & 6 \\ 1 & 2 & 5 \\ 1 & 3 & 2 \end{pmatrix}.$$

5.7. *Задачи для любознательных.*

1) (ОК, 99–3) Найти все вещественные матрицы A размерности 2×2, такие, что $A^n = E$, если а) $n = 2$; б) $n = 3$.

Замечание. Вернитесь к этой задаче после того как изучите форму Жордана.

2) (ОК, 03–2) Пусть квадратная матрица A — невырожденная, а матрица X удовлетворяет уравнению

$$AX + XA = 0.$$

Доказать, что след матрицы X равен 0.

3) (ОК, 03–3) Пусть A — квадратная матрица порядка n. Доказать, что если $A^2 = E$, то сумма рангов матриц $A + E$ и $A - E$ равна n.

4) (ОК, 04–9) Пусть A и B — квадратная матрица порядка n, причем матрица A обратима. Возможно ли равенство $AB - BA = A$?

5) (ОК, 06–4) Пусть M — множество квадратных матриц $n \times n$, элементами которых являются 0 и 1. Произведение $D = (d_{ij})$ матриц $A = (a_{ij})$ и $B = (b_{ij})$ из M находится по формуле

$$d_{ij} = max_k min(a_{ik}, b_{kj}).$$

а) Пусть

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

Найдите A^2, A^3, ...

б) Будет ли это умножение ассоциативным?

6) (ОК, 08–3) Найти все квадратные матрицы второго порядка, удовлетворяющие условию

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

7) (ОК, 11–1) Матрицы A и B не коммутируют между собой т. е. $AB \neq BA$. Может ли оказаться, что матрицы A^2 и B^2 коммутируют?

8) (ОК, 14–4) Квадратная матрица A размера 20×20 невырождена. Какое наименьшее значение может иметь ранг подматрицы 12×13 матрицы A?

9) (ОК, 14–9) В каждой строке невырожденной квадратной $n \times n$ матрицы A стоит только одно, отличное от 0 число, равное + 1 или -1. Докажите, что найдется такое m, при котором m–я степень матрицы совпадает с матрицей, транспонированной к A, т. е. $A^m = A^T$.

10) (ОК, 17–3) Решить матричное уравнение $AX + X + A = 0$, где квадратная матрица A нильпотентна (некоторая степень A является нулевой матрицей).

11) (ОК, 19–9) Доказать, что для любой вещественной матрицы A размера 2×2 с нулевым следом существуют такие вещественные матрицы B и C, что $A = BC - CB$.

Комментарии. Операция $[B, C] = BC - CB$ называется коммутатором B и C. Следовательно, матрица 2×2 имеет нулевой след тогда и только тогда, когда она является коммутатором.

12) (СМО, Задача 334) Найти матрицу

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}^{100}.$$

5.8. *Мозаика: Математики шутят.*

Многомерная абстрактная чепуха. Каждое лето в НГУ проводится Большая математическая мастерская (БММ). Руководители предлагают темы для исследований, студенты выбирают понравившуюся, набирается команда и в течении нескольких недель эта тема активно изучается. Одна из предложенных тем на БММ-24 звучала так: "Многомерная абстрактная чепуха". Никого из математиков такое название не удивило, представители команды были весьма довольны и активно обсуждали вопрос о том как их называть: "Чепухасты", "Чепухисты" или "Чепушисты"? Сложности возникли при оплате выполненной работы. В бухгалтерии никак не могли понять, как можно платить деньги за чепуху?

Метод. Три математика из Института математики и три физика из Института ядерной физики поехали в город на конгресс ученых. Встретились на Сеятеле. При этом физики купили три билета на электричку до горда, а математики — только один. На вопрос физиков: "Почему?" — Математики важно ответили: "Мы знаем метод." Во время поездки в вагон вошел контролёр. Математики потихоньку встали, прошли в туалет, где и закрылись. На стук контролёра, дверь приоткрылась, высунулась рука и показала билет. Наблюдавшие за этим физики были в полном восторге.

После окончания конгресса, наша веселая шестёрка встретилась на вокзале Новосибирск–главный у пригородных касс. На этот раз физики купили всего один билет. На вопрос: "Почему?" — Физики, подражая математикам, важно ответили: "Мы знаем метод." Математики вообще не стали покупать билеты. Во время поездки в вагон вошел контролёр. Физики проследовали в туалет, где и закрылись. На стук дверь отворилась и рука протянула билет. Довольные математики схватили билет и убежали в туалет другого вагона.

Мораль. Мало знать метод, надо уметь эффективно его использовать.