Начала теории групп и колец

П.А. Кожевников

12 января 2018 г.

Оглавление

Глава 1

Абстрактные отображения.

§ 1. Понятие отображения и преобразования. Терминология. Примеры.

ВАЖНО ЗНАТЬ ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ПРАВИЛЬНО ИХ ПОНИМАТЬ!!

Бинарные операции на множестве.

§ 2. Отношение эквивалентности.

Отношение эквивалентности. Множество классов эквивалентности (фактор-множество).

С отображением $\varphi : X \to Y$ связано отношение эквивалентности: $a \sim b$, если $\varphi(a) = \varphi(b)$.

ПРИМЕРЫ:

1)свободные векторы — классы эквивалентности направленных отрезков с отношением равенства.

2) классы вычетов по модулю n,

3) $\mathbb{C}$, $z_1 \sim z_2$, если $|z_1| = |z_2|$

4) Подобные матрицы: $A, B \in \mathbb{M}_{n\times n}$ подобны, если существует невырожденная матрица S такая, что $B = S^{-1}AS$.

Глава 2

Группы.

§ 1. Определение и некоторые конструкции.

Определение и его следствия.

Рассмотрим $(G, \cdot)$ — множество G с бинарной операцией, для которой используем *мультипликативную запись*. Рассмотрим следующие аксиомы.

G1. $(ab)c = a(bc) \quad (\forall\ a, b, c \in G)$;
G2. $\exists\ e \in G \quad \forall\ a \in G$: $\quad ae = ea = a$;
G3. $\forall\ a \in G \quad \exists\ x \in G$: $\quad xa = ax = e$;
G4. $ab = ba \quad (\forall\ a, b \in G)$.

G1 — аксиома ассоциативности. Если $(G, \cdot)$ удовлетворяет G1, то G называется *полугруппой*. Из G1 следует обобщенная ассоциативность:

Предложение 1.1. *Пусть $(G, \cdot)$ удовлетворяет аксиоме G1. Тогда значения произведения $a_1 a_2 \dots a_k$ не зависит от расстановки скобок.*

▷ ... индукция □

В частности, однозначно определены *степени* элемента a^n, $n \in \mathbb{N}$. Для степеней выполнены привычные правила $a^{m+n} = a^m a^n$, $a^{mn} = (a^m)^n$.

В аксиоме G2 элемент e называется *нейтральным элементом* или *единицей*. Иногда для него используется обозначение 1. Если $(G, \cdot)$ удовлетворяет аксиомам G1 и G2, то G называют *полугруппой с единицей* или *моноидом*.

Предложение 1.2. *Пусть $(G, \cdot)$ удовлетворяет аксиоме G2. Тогда нейтральный элемент единственный.*

▷ Пусть e и e' — нейтральные элементы. Тогда $e = ee' = e'$. □

Элемент x такой, что $xa = ax = e$ (как в аксиоме G3) называется *обратным* элементом для элемента a.

Предложение 1.3. *Пусть $(G, \cdot)$ — полугруппа с единицей (т.е. выполнены аксиомы G1 и G2). Если для элемента $a \in G$ существует обратный элемент, то он единственный.*

▷ Пусть x и y — обратные элементы для a. Тогда $x = xe = x(ay) = (xa)y = ey = y$. □

Если для элемента a существует обратный элемент, то a называется *обратимым*. Обратный элемент обозначается a^{-1}. Очевидно, $e^{-1} = e$, $(a^{-1})^{-1} = a$ (если a^{-1} существует).

Предложение 1.4. *Пусть $(G, \cdot)$ — полугруппа с единицей. Если $a, b \in G$ — обратимые элементы, то ab — обратимый элемент, причем $(ab)^{-1} = b^{-1}a^{-1}$.*

▷ Перемножим ab и $b^{-1}a^{-1}$: $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Аналогично убеждаемся, что $(b^{-1}a^{-1})(ab) = e$. □

Следствие. *Если $a_1, a_2, \ldots, a_k$ — обратимые элементы полугруппы с единицей $(G, \cdot)$, то $a_1a_2 \ldots a_k$ — обратимый элемент, причем $(a_1a_2 \ldots a_k)^{-1} = a_k^{-1}a_{k-1}^{-1} \ldots a_1^{-1}$.*

Если обратимого элемнета a можно определить *степени* a^n для всех $n \in \mathbb{Z}$, полагая $a^0 = e$, $a^n = (a^{-1})^{-n}$ при $n < 0$. Для степеней выполнены привычные правила:

Предложение 1.5. *(степени) Пусть a — обратимый элемент полугруппы $(G, \cdot)$. Тогда $\forall\ m, n \in \mathbb{Z}$ выполнено*
1) $a^{m+n} = a^m a^n$;
2) $a^{mn} = (a^m)^n$.

▷ ... □

Дадим основное определение:

|| $(G, \cdot)$ называется *группой*, если удовлетворяет аксиомам G1, G2 и G3.

Если хотят уточнить, о какой бинарной операции идет речь, говорят «G — группа относительно операции $\cdot$». Если ясно, о какой бинарной операции идет речь, группу иногда будем обозначать просто G.

Согласно предложениям 1.1, 1.2, 1.3, в группе выполнена обобщенная ассоциативность, существует единственный нейтральный элемент, и для любого элемента существует единственный обратный элемент.

Предложение 1.6. *(закон сокращения) Пусть $(G, \cdot)$ — группа. Тогда $\forall\ a, b, c \in G$ выполнено $ab = ac \Leftrightarrow b = c \Leftrightarrow ba = ca$.*

▷ $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow b = c$. Следствие $b = c \Rightarrow ab = ac$ очевидно. Аналогично показывается, что $ba = ca \Leftrightarrow b = c$. □

Предложение 1.7. *(уравнения в группе) Пусть $(G, \cdot)$ — группа, $a, b \in G$. Тогда 1) уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$; 2) уравнение $xa = b$ имеет единственное решение $x = ba^{-1}$.*

▷ ... □

Если в группе $(G, \cdot)$ элементы a и b таковы, что $ab = ba$, такие элементы называются *перестановочными* или *коммутирующими*. G4 — аксиома коммутативности. Пусть группа $(G, \cdot)$ удовлетворяет еще и аксиоме G4 (тем самым, $(G, \cdot)$ удовлетворяет всем аксиомам G1 — G4). Такая группа называется *коммутативной*, или *абелевой*.

Упражнение. Если в группе $(G, \cdot)$ элементы a и b коммутируют, то a^m и b^n коммутируют $\forall\ m, n \in \mathbb{Z}$.

Упражнение. В группе $(G, \cdot)$ выполнено $(ab)^2 = a^2b^2 \Leftrightarrow$ элементы a и b коммутируют.

|| Количество элементов в группе G называется *порядком* группы.

Порядок группы обозначается $|G|$. Соответственно, группа называется *бесконечной*, если $|G| = \infty$, и *конечной* в противном случае.

Аддитивная форма записи.

Для обозначения операции иногда используется знак «+» (аддитивная запись). Как правило, это делается только для абелевой группы, чтобы результат взятия суммы $\sum\limits_{i=1}^{k} a_i = a_1 + a_2 + \ldots + a_k$ не зависел от порядка действий. Аксиомы G1 — G4 для $(G, +)$ принимают следующий вид.

G1. $(a + b) + c = a + (b + c) \quad (\forall\ a, b, c \in G)$;
G2. $\exists\ 0 \in G \quad \forall\ a \in G$: $\quad a + 0 = 0 + a = a$;
G3. $\forall\ a \in G \quad \exists\ x \in G$: $\quad x + a = a + x = 0$;
G4. $a + b = b + a \quad (\forall\ a, b \in G)$.

Теперь *степени* элемента a записываются как *кратные*: na, $n \in \mathbb{Z}$. При этом (см. предложение 1.5) выполнены правила $(m + n)a = ma + na$, $(mn)a = m(na)$.

В аксиоме G2 нейтральнй элемент теперь обозначен 0. Иногда его так и называют *нуль*.

Элемент x из аксиомы G3 уместно теперь называть *противоположным* элементом для элемента a и обозначать $-a$. Легко видеть, что $-(ma) = (-m)a = m(-a)$ (для $m \in \mathbb{Z}$).

Для элементов $(G, +)$ можно определить *вычитание* по правилу $a - b = a + (-b)$. При этом легко видеть, что $m(a - b) = ma - mb$, $(m - n)a = ma - na$ (для $m, n \in \mathbb{Z}$).

Следствия аксиом G1 — G4 для абелевой группы $(G, +)$ принимают вид: 0 — единственный; $\forall\ a \in G$ элемент $-a$ единственный; $\forall\ a_i \in G$ выполнено: $-(a_1 + a_2 + \ldots + a_k) = -a_k - a_{k-1} - \ldots - a_1$; $\forall\ a, b, c \in G$ выполнено $a + b = a + c \Leftrightarrow b = c$; уравнение $x + a = b$ имеет единственное решение $x = b - a$.

Изоморфизм, гомоморфизм.

Пусть даны две группы, или более общо, два множества, на которых определены бинарные операции $(G, \cdot)$ и $(\widetilde{G}, *)$.

Отображение $\varphi : G \to \widetilde{G}$ называется *гомоморфизмом*, если $\forall\ a, b \in G$ выполнено $\varphi(ab) = \varphi(a) * \varphi(b)$.

Иначе говоря, гомоморфизм — отображение, которое сохраняет («уважает») бинарную операцию. Для любых групп $(G, \cdot)$ и $(\widetilde{G}, *)$ есть тривиальный гомоморфизм, отображающий каждый элемент из G в нейтральный элемент группы $\widetilde{G}$.

Предложение 1.8. *Пусть $(G, \cdot)$ и $(\widetilde{G}, \cdot)$ — группы, а $\varphi : G \to \widetilde{G}$ — гомоморфизм. Тогда*
1) $\varphi(e) = \widetilde{e}$ (где e и $\widetilde{e}$ — нейтральные элементы групп G и $\widetilde{G}$).
2) $\forall\ a \in G$ выполнено $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

▷ ... □

Отображение $\varphi : G \to \widetilde{G}$ называется *изоморфизмом*, если φ — гомоморфизм, являющийся биекцией.

Группы $(G, \cdot)$ и $(\widetilde{G}, *)$ называются *изоморфными*, если существует изоморфизм $\varphi : G \to \widetilde{G}$.

Тот факт, что $(G, \cdot)$ и $(\widetilde{G}, *)$ изоморфны, обозначаем $(G, \cdot) \cong (\widetilde{G}, *)$ (или $G \cong \widetilde{G}$).

Предложение 1.9. *Пусть даны* $(G,\cdot)$, $(\widetilde{G},*)$, $(\widetilde{\widetilde{G}},\circ)$ *и* $\varphi: G\to\widetilde{G}$ *и* $\psi:\widetilde{G}\to\widetilde{\widetilde{G}}$ *— гомоморфизмы. Тогда 1)* $\psi\varphi: G\to\widetilde{\widetilde{G}}$ *— гомоморфизм.*
2) Если кроме того φ *и* ψ *— изоморфизмы, то* $\psi\varphi$ *— также изоморфизм.*
3) Если $\varphi: G\to\widetilde{G}$ *— изоморфизм, то* φ^{-1} *— также изоморфизм.*

$\triangleright$ ... $\square$

Как видим, отношение «быть изоморфными» рефлексивно (очевидно $G\cong G$, так как тождественное преобразование является изоморфизмом), симметрично и транзитивно. Оно формализует понятие «одинаковости» групп с точки зрения бинарной операции. Тем самым, класс всех группы можно мыслить себе разбитым на классы изоморных групп.

Прямое произведение (прямая сумма).

Пусть даны две группы, или более общо, два множества, на которых определены бинарные операции $(G,\cdot)$ и $(\widetilde{G},\cdot)$.

Прямым произведением $(G,\cdot)$ и $(\widetilde{G},\cdot)$ называется множество $G\times\widetilde{G}$, на котором операция задана правилом $(a,\widetilde{a})(b,\widetilde{b})=(ab,\widetilde{a}\widetilde{b})$.

Используется то же обозначение, что и для обычного декартового произведения множеств: $G\times\widetilde{G}$. Итак, в прямом произведении операция выполняется *покомпонентно*. Аналогичным образом определяется прямое произведение нескольких групп. В том случае, когда используется аддитивная запись (т.е. даны $(G,+)$ и $(\widetilde{G},+)$), прямое произведение называют также *прямой суммой* и обозначают $G\oplus\widetilde{G}$.

Предложение 1.10. *Прямое произведение нескольких групп является группой.*

$\triangleright$ ... $\square$

Упражнение. Пусть $G\times\widetilde{G}$ — прямое произведение групп. Тогда *проектирование* $\varphi: G\times\widetilde{G}\to G$, определенное правилом $\varphi((a,\widetilde{a}))=a$ является гомоморфизмом.

Обратимые элементы полугруппы.

Пусть $(G,\cdot)$ — моноид (полугруппа с единицей) с нейтральным элементом e. Выделим в G подмножество G^* обратимых элементов: $G^*=\{a\in G\,|\,\exists\, x\in G\, ax=xa=e\}$.

Предложение 1.11. *Пусть* $(G,\cdot)$ *— моноид. Тогда* $(G^*,\cdot)$ *— группа.*

$\triangleright$ ... $\square$

Упражнение. Если $G\times\widetilde{G}$ — прямое произведение моноидов, то $(G\times\widetilde{G})^*=G^*\times\widetilde{G}^*$.

Подгруппы. Порождающие множества.

Непустое подмножество H группы $(G,\cdot)$ называется *подгруппой*, если $\forall\ a,b\in H$ выполнено:
П1. $ab\in H$;
П2. $a^{-1}\in H$.

Тот факт, что H является подгруппой группы G, будем обозначать $H\leqslant G$.

Предложение 1.12. *Пусть* $(G,\cdot)$ *— группа,* $H\leqslant G$. *Тогда* $e\in H$.

▷ Пусть $a \in H$, тогда, согласно П2 и П1, $e = (a^{-1})a \in H$. □

Свойства П1 и П2 означают, что подгруппа является подмножеством, замкнутым относительно операций умножения и взятия обратного, тем самым, подгруппа сама является группой относительно операций в объемлющей группе G. Любая группа G содержит *тривиальные* подгруппы G и $\{e\}$ (*единичная* подгруппа).

Упражнение. Укажите в прямом произведении $G \times \widetilde{G}$ подгруппу, изоморфную G.

В аддитивной записи (для группы $(G, +)$ условия П1 и П2 будут выглядеть как $a+b \in H$, $-a \in H$.

Предложение 1.13. *Пересечение подгрупп является подгруппой.*

▷ Пусть $H_i \leqslant G$ для $i \in I$ (где I — некоторое множество индексов); $H = \bigcap\limits_{i \in I} H_i$. Проверим П1 для множества H (П2 проверяется аналогично).

Пусть $a, b \in H$, тогда $a, b \in H_i$ $(\forall\ i \in I)$. Так как H_i — подгруппа, то $ab \in H_i$ $(\forall\ i \in I)$, тем самым $ab \in H$, что и требовалось. □

Упражнение. Пусть $H_1 \leqslant G$, $H_2 \leqslant G$. Докажите, что объединение $H_1 \cup H_2$ является подгруппой $\Leftrightarrow H_1 \subset H_2$ или $H_2 \subset H_1$.

Пусть дано некоторое подмножество $A = \{a, b, c, \ldots\}$ в группе $(G, \cdot)$. Определим множество $\langle a, b, c, \ldots\ldots\rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} \mid k \in \mathbb{N}, x_i \in A, \varepsilon_i \in \{-1, 1\}\}$.

Например, $\langle a\rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\}$, так как в любом «слове» $a^{\varepsilon_1} a^{\varepsilon_2} \ldots a^{\varepsilon_k}$ произведения aa^{-1} и $a^{-1}a$ сокращаются.

Предложение 1.14. *Пусть дано подмножество $A = \{a, b, c, \ldots\}$ в группе $(G, \cdot)$. Тогда $\langle a, b, c, \ldots\rangle$ — подгруппа.*

▷ Проверим П1 и П2. .... □

Пусть $A = \{a, b, c, \ldots\} \subset H \leqslant G$. Многократно используя П1 и П2, получаем, любой элемент из $\langle a, b, c, \ldots\rangle$ также принадлежит подгруппе H. Таким образом, $\langle a, b, c, \ldots\rangle$ является минимальной (по включению) подгруппой, содержащей множество A, она называется *подгруппой, порожденной множеством A*. Если $\langle a, b, c, \ldots\rangle = G$, то множество A называется *порождающим* множеством элементов группы G. (Конечно, в данной группе G может быть много различных порождающих множеств.)

Примеры.

I. Числа и матрицы по сложению:

$(\mathbb{Z}, +)$ — группа по сложению. Отметим, что $(\mathbb{Z}, +) = \langle 1\rangle$.

Цепочка вложенных абелевых групп $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C} \cong \mathbb{R}^2 \leqslant \mathbb{R}^3 \leqslant \ldots$.

Для $n \in \mathbb{N}$: $n\mathbb{Z} \leqslant \mathbb{Z}$. Имеется изоморфизм $\mathbb{Z} \to n\mathbb{Z}$, задаваемый правилом $t \mapsto nt$.

$\mathbb{M}_{m\times n}(\mathbb{R}) \cong \mathbb{R}^{mn}$.

II. Числа и матрицы по умножению:

Полугруппы (моноиды) по умножению $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$. Вложения $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$ порождают цепочку вложенных (абелевых) групп по умножению:
$\mathbb{Z}^* \leqslant \mathbb{Q}^* \leqslant \mathbb{R}^* \leqslant \mathbb{C}^*$. (Здесь $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.)

$\mathbb{M}_{n\times n}(\mathbb{R})$, $\mathbb{M}_{n\times n}(\mathbb{Z})$, и т.д. — моноиды по умножению. $\mathbb{M}_{n\times n}(\mathbb{R})^*$ обозначается также $GL_n(\mathbb{R})$ (общая линейная группа) — группа всех невырожденных матриц размера $n \times n$. При $n \geqslant 2$ это неабелева группа.

Упражнение. Покажите, что $GL_n(\mathbb{R}) = \langle S \rangle$, где S — множество *элементарных матриц* $n \times n$.

$GL_n(\mathbb{R}) \geqslant UT_n(\mathbb{R})$ — подгруппа верхнеунитреугольных матриц с единицами на главной диагонали.

$GL_n(\mathbb{R}) \geqslant SL_n(\mathbb{R}) = \{A \in \mathbb{M}_{n\times n}(\mathbb{R}) \mid \det A = 1\}$ — специальная линейная группа.

III. Вычеты по модулю n.

Пусть $\overline{k}$ обозначает класс эквивалентности числа $k \in \mathbb{Z}$ относительно отношения эквивалентности $k \sim l \Leftrightarrow k - l \vdots n$. $\overline{k}$ называют *вычетом* по модулю n. (Возможен и другой вариант определения $\overline{k}$ как остатка числа $k \in \mathbb{Z}$ при делении на n.)

Обозначим $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ (так, $|\mathbb{Z}_n| = n$). Операции сложения и умножения вводятся как $\overline{k} + \overline{l} = \overline{k+l}$, $\overline{k} \cdot \overline{l} = \overline{kl}$. (Необходима проверка корректности(!) т.е. того, что результат операции на классах не зависит от выбора представителя.)

$(\mathbb{Z}_n, +)$ — абелева группа. Отметим, что $(\mathbb{Z}_n, +) = \langle \overline{1} \rangle$.

$(\mathbb{Z}_n, \cdot)$ — моноид. На самом деле правило $k \mapsto \overline{k}$ дает естественные сюръективные гомоморфизмы групп $(\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ и моноидов $(\mathbb{Z}, \cdot) \to (\mathbb{Z}_n, \cdot)$. (Т.е., см. ниже, это кольцевой гомоморфизм $\mathbb{Z} \to \mathbb{Z}_n$).

Предложение 1.15. *(Критерий обратимости в $\mathbb{Z}_n$). Элемент $\overline{k} \in \mathbb{Z}_n$ обратим в моноиде $(\mathbb{Z}_n, \cdot) \Leftrightarrow (k, n) = 1$.*

$\triangleright$ 1) Пусть $(k, n) = d > 1$ и пусть $m = n/d$. Тогда $km \vdots n$, поэтому $\overline{k}\overline{m} = \overline{0}$. Предположим, что есть $\overline{k}^{-1} = \overline{l}$. Но отсюда $\overline{0} = \overline{k}\overline{m} = \overline{lk}\overline{m} = \overline{1}\overline{m} = \overline{m}$.
2) Следует из *леммы*: Для $(k, n) = 1$ числа $0 \cdot k, 1 \cdot k, \ldots, (n-1)k$ дают различные остатки при делении на n. (Иначе говоря, $\{\overline{0 \cdot k}, \overline{1 \cdot k}, \ldots, \overline{(n-1)k}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.)
Док-во леммы....
$\square$

Таким образом, мы получили, что $\mathbb{Z}_n^* = \{\overline{k} \mid 1 \leqslant k \leqslant n, (k, n) = 1\}$.

Функцией Эйлера от натурального числа n называется количество чисел, взаимно-простых с n среди чисел $\{1, 2, \ldots, n\}$.

Обозначение для функции Эйлера: $\varphi(n)$. Таким образом, $|\mathbb{Z}_n^*| = \varphi(n)$.

IV. Группы преобразований.

Пусть X — произвольное множество, $S(X)$ — множество всех биекций $X \to X$. На множестве $S(X)$ есть естественная операция композиции. $S(X)$, наделенное этой операцией, превращается в группу. При $|X| \geqslant 3$ группа $S(X)$ неабелева.

Для $|X| < \infty$ элементы группы $S(X)$ называют *перестановками* или *подстановками*, а саму группу — *группой перестановок* или *симметрической группой*. Вместо $S(\{1, 2, \ldots, n\})$ используется стандартное более короткое обозначение S_n.

Упражнение. $|S_n| = n!$.

Любая подгруппа $G \leqslant S(X)$ является *группой преобразований*. В этом случае возникает естественное *действие* группы G на множестве X: $\forall\ a, b \in G$, $\forall\ x \in X$ выполнено $(ab)(x) = a(b(x))$.

Более общо, *действием* группы G на множестве X называют гомоморфизм $\alpha : G \to S(X)$. Таким образом, $\forall\ a, b \in G$, $\forall\ x \in X$ выполнено $(\alpha(a)\alpha(b))(x) = \alpha(a)(\alpha(b)(x))$ или, опуская символ гомоморфизма, $(ab)(x) = a(b(x))$.

Стабилизатор, или *подгруппа симметрий* подмножества $X' \subset X$ при действии $\alpha : G \to S(X)$ — это $Sym(X') = \{a \in G \mid a(X') = X'\}$. Легко видеть, что $Sym(X') \leqslant G$.

Орбита подмножества $X' \subset X$ при действии $\alpha : G \to S(X)$ — это множество $G(X') = \{a(X') \,|\, a \in G\}$ (т.е. орбита состоит из подмножеств, в которые может перейти X' под действием элементов из G).

Можно ввести отношение $X' \sim X'' \Leftrightarrow \exists\, a \in G\ a(X') = X''$. Это отношение является отношением эквивалентности, а классы эквивалентности — это орбиты.

ПРИМЕРЫ действий.

1) Естественные примеры действий возникают в геометрии (под этот формализм попадают задачи нахождения групп симметрий фигур и задача классификации фигур относительно той или иной группы преобразований).

Пусть $X = \mathbb{R}^2$ — плоскость, G — группа движений ($G \leqslant S(X)$). Пусть $X' \subset X$ — некоторая фигура, скажем, правильный n-угольник. Тогда орбита $G(X')$ — множество всех фигур, равных (конгруэнтных) X'. $Sym(X')$ — группа «самосовмещений» X' (для n-угольника получается так называемая *группа диэдра*).

Для того же случая $X = \mathbb{R}^2$ можно взять, скажем, более широкую группу так называемых *аффинных* преобразований, которую можно определить как $A = \langle G \cup S \rangle$, где G — множество движений, S — множество сжатий и растяжений относительно прямых.

2) Любая подгруппа $G \leqslant S_n$ естественно действует на конечном множестве $\{1, 2, \ldots, n\}$.

3) Пусть $X = \mathbb{M}_{n\times 1}(\mathbb{R})$ (множество векторов-столбцов), $G = GL_n(\mathbb{R})$. Тогда каждая матрица $A \in G$ задает биекцию $x \mapsto Ax$ (умножение на A слева), при этом $(AB)x = A(Bx)$, тем самым G действует на X. (Этому действию позже придадим «бескоординатную» интерпретацию: действие группы биективных линейных преобразований (автоморфизмов) на n-мерном векторном пространстве.)

Матричным представлением группы G называется гомоморфизм $G \to GL_n(\mathbb{R})$. При этом возникает естественное действие G на $X = \mathbb{M}_{n\times 1}(\mathbb{R})$.

§ 2. Порядок элемента. Циклические группы.

Порядок элемента.

Пусть $(G, \cdot)$ — группа, e — ее нейтральный элемент.

Натуральное n называют *порядком* элемента $a \in G$, если $a^n = e$ и $a^k \neq e$ при $k = 1, 2, \ldots, n-1$.
В случае, когда такого n не существует, полагаем порядок элемента равным ∞.

Порядок элемента a обозначаем $\operatorname{ord} a$ или $|a|$.

Предложение 2.1. *Пусть $a \in G$, $k, l \in \mathbb{Z}$.*

1) Пусть $\operatorname{ord} a = n < \infty$. Тогда $a^k = a^l \Leftrightarrow k - l \vdots n$, в частности, $a^k = e \Leftrightarrow k \vdots n$;
2) Пусть $\operatorname{ord} a = \infty$. Тогда $a^k = a^l \Leftrightarrow k = l$.

▷ Пусть для определенности $k > l$. Тогда $a^k = a^l \Leftrightarrow a^{k-l} = e$. В случае $\operatorname{ord} a = \infty$ это противоречие. В случае $\operatorname{ord} a = n$ рассуждаем далее: разделим $k - l$ на n с остатком: $k - l = qn + r$, $r \in \{0, 1, \ldots, n-1\}$. Тогда $a^{k-l} = a^{qn+r} = (a^n)^q a^r = a^r$ и $a^{k-l} = e \Leftrightarrow a^r = e$, что верно при $r = 0$ и противоречит определению порядка элемента a при $r \in \{1, 2, \ldots, n-1\}$. □

Упражнение. Пусть $(a, \widetilde{a}) \in G \times \widetilde{G}$, причем $\operatorname{ord} a = n$, $\operatorname{ord} \widetilde{a} = m$. Тогда $\operatorname{ord}(a, \widetilde{a}) = \text{НОК}(m, n)$.

Упражнение. Пусть a, b — элементы группы $(G, \cdot)$. Покажите, что $\operatorname{ord} a = \operatorname{ord}(bab^{-1})$.

Циклические группы и их классификация.

Как мы видели, любое подмножество элементов группы порождает некоторую подгруппу, в частности, любой элемент порождает некоторую подгруппу.

Циклической группой называется группа, порожденная некоторым своим одним элементом.

Если группа $(G, \cdot)$ — циклическая, то $\exists\, a \in G$: $G = \langle a \rangle$. Такой элемент a называется *порождающим* элементом циклической группы (в согласии с общим определением порождающего множества). Как мы видели, полный список (возможно, с повторениями) элементов группы G имеет вид $G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$.

Примеры циклических групп мы видели ранее: $(\mathbb{Z}, +) = \langle 1 \rangle$ и $(\mathbb{Z}_n, +) = \langle \overline{1} \rangle$.

Теорема 2.1. *(классификация циклических групп) Пусть $(G, \cdot)$ — циклическая группа. Если $|G| = n$, то $G \cong (\mathbb{Z}_n, +)$. Если $|G| = \infty$, то $G \cong (\mathbb{Z}, +)$.*

▷ Итак, пусть $G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$. Рассмотрим две возможности.
1) $\operatorname{ord} a = \infty$. Тогда, по предложению 2.1, в этом списке нет повторений. Тогда отображение $\varphi : G \to \mathbb{Z}$, такое, что $\varphi(a^k) = k$ является биекцией. Более того, это изоморфизм. Проверка:....
2) $\operatorname{ord} a = n < \infty$. Тогда, по предложению 2.1, $G = \{e, a, a^2, \ldots, a^{n-1}\}$, и в этом списке нет повторений. Тогда отображение $\varphi : G \to \mathbb{Z}_n$, такое, что $\varphi(a^k) = \overline{k}$ является биекцией. Более того, это изоморфизм. Проверка:.... □

Следствие. $\operatorname{ord} a = |\langle a \rangle|$.

Предложение 2.2. *Пусть $\overline{k} \in \mathbb{Z}_n$. Тогда $\operatorname{ord} \overline{k}$ (в группе $(\mathbb{Z}_n, +)$) равен $\dfrac{n}{(n,k)}$.*

▷ Пусть $m \in \mathbb{N}$. Тогда $m \cdot \overline{k} = \overline{0} \Leftrightarrow mk \vdots n \Leftrightarrow m \vdots \dfrac{n}{(n,k)}$. □

Мы видим, что в $(\mathbb{Z}_n, +)$ есть элементы только порядков, равных делителям n (это согласуется с теоремой Лагранжа, см. ниже). Укажем количество элементов фиксированного порядка.

Предложение 2.3. *Пусть d — делитель числа n. Тогда в группе $(\mathbb{Z}_n, +)$) количество элементов порядка d равно $\varphi(d)$. В частности, количество порождающих элементов равно $\varphi(n)$.*

▷ Пусть $k \in \{1, 2, \ldots, n\}$. Имеем $\operatorname{ord} \overline{k} = d \Leftrightarrow \dfrac{n}{(n,k)} = d \Leftrightarrow (n,k) = \dfrac{n}{d} \Leftrightarrow k = \dfrac{nt}{d}$, где $(t,d) = 1$, $1 \leqslant t \leqslant d$. □

Подгруппы циклические групп.

Предложение 2.4. *0) Подгруппа циклической группы является циклической группой.*
1) Все подгруппы $(\mathbb{Z}, +)$ — в точности $m\mathbb{Z}$, $m \in \mathbb{N}$.
2) Для каждого делителя d числа n в $(\mathbb{Z}_n, +)$ имеется ровно одна подгруппа порядка d. Она состоит из элементов $\{\overline{mt} \,|\, t = 0, 1, \ldots, d-1\}$, где $m = \dfrac{n}{d}$.

▷ 1) Пусть $H \leqslant \mathbb{Z}$, $H \neq \{0\}$, а $m \in \mathbb{N}$ — наименьшее такое, что $m \in H$ (если нашлось $m < 0$ такое, что $m \in H$, то и $-m \in H$). Тогда $m\mathbb{Z} \leqslant H$. Предположим, что $t \in H \setminus m\mathbb{Z}$. Разделим t на m с сотатком: $t = qm + r$, $r \in \{1, 2, \ldots, m-1\}$. Тогда $r = t - mq \in H$. Но $0 < r < m$ — противоречие. Значит, $H = m\mathbb{Z}$. (Как ранее отмечалось, $m\mathbb{Z}$ — действительно подгруппа.)
2) Пусть $H \leqslant \mathbb{Z}_n$, а $m \in \{1, 2, \ldots, n-1\}$ — наименьшее такое, что $\overline{m} \in H$ (если такого m нет, то $H = \{\overline{0}\}$). Разделим n на m с остатком: $n = qm + r$, $r \in \{0, 1, 2, \ldots, m-1\}$. Тогда $\overline{r} \in H$. Если $r > 0$, то получаем противоречие с выбором m. Значит, $n \vdots m$. Далее.... □

§ 3. Симметрическая группа.

Умножение перестановок. Циклы. Порождающие множества.

Изучим более детально группу перестановок S_n.

Перестановку $\sigma \in S_n$ можно записать в виде таблицы $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$. При этому перемножение перестановок происходит «справа налево»: $\sigma\eta = \begin{pmatrix} \ldots & \eta(i) & \ldots \\ \ldots & \sigma(\eta(i)) & \ldots \end{pmatrix} \begin{pmatrix} \ldots & i & \ldots \\ \ldots & \eta(i) & \ldots \end{pmatrix} = \begin{pmatrix} \ldots & i & \ldots \\ \ldots & \sigma(\eta(i)) & \ldots \end{pmatrix}$. Чтобы построить таблицу для обратной перестановки, нужно поменять строки местами и переставить столбцы так, чтобы в первой строке числа шли в порядке возрастания: $\sigma^{-1} = \begin{pmatrix} \ldots & \sigma(i) & \ldots \\ \ldots & i & \ldots \end{pmatrix}$

Другой способ задать перестановку — построить *ориентированный граф* («диаграмму со стрелками»), в котором n вершин занумерованы $1, 2, \ldots, n$, и из вершины i идет стрелка в $\sigma(i)$, $i = 1, 2, \ldots .n$. Переход к обратной перестановке соответствует изменению направления на всех стрелках. Пусть две перестановки $\sigma, \eta \in S_n$ заданы своими диаграммами со стрелками на одной и том же множестве вершин $\{1, 2, \ldots, n\}$. Чтобы найти $(\sigma\eta)(i)$, надо пройти из вершины i пусть по двум стрелкам: сначала по стрелке из диаграммы η, далее по стрелке из диаграммы σ.

Поскольку в каждую вершину идет ровно одна стрелка и из каждой вершины выходит ровно одна стрелка, граф представляет собой объединение ориентированных циклов (докажите это), при этом некоторые циклы могут быть *тривиальными*, т.е. представлять собой петлю.

Слово «цикл» относят и к перестановкам специального вида. Перестановка $\sigma \in S_n$ называется *циклом длины* d, если ей сооответствует ориентированный граф в виде одного нетривиального цикла длины d (т.е. имеющего d ребер) и $n - d$ тривиальных циклов. Формально, цикл длины d — перестановка, для которой имеется подмножество $\{i_1, \ldots, i_d\} \subset \{1, 2, \ldots, n\}$ такое, что $\sigma(i_t) = i_{t+1}$ для $i = 1, \ldots, d$ (здесь полагаем $i_{d+1} = i_1$) и $\sigma(k) = k$ при $k \notin \{i_1, \ldots, i_d\}$. Такой цикл обозначаем коротко $(i_1 i_2 \ldots i_d)$. Очевидно, $(i_1 i_2 \ldots i_d) = (i_2 \ldots i_d i_1) = \ldots = (i_d i_1 \ldots i_{d-1})$, $(i_1 i_2 \ldots i_d)^{-1} = (i_d \ldots i_2 i_1)$ Цикл длины 2 называют также *транспозицией*. Отметим, что транспозиция является обратной к самой себе. Два цикла (перестановки) называем *независимыми*, если в их диаграммах нетрививальные циклы не имеют общих вершин.

Предложение 3.1. *Любая перестановка раскладывается в произведение (попарно) независимых циклов.*

▷ Следует из структуры соответствующего ориентированного графа. □

Следствие. *S_n порождается циклами.*

Упражнение. Пусть перестановка σ раскладывается в произведение (попарно) независимых циклов длин $d_1, d_2, \ldots, d_t$. Покажите, что $\operatorname{ord}\sigma = \text{НОК}(d_1, d_2, \ldots, d_t)$.

Предложение 3.2. *Цикл длины d представляется в виде произведения $d-1$ транспозиций.*

▷ Непосредственно проверяется, что $(i_1 i_2 \ldots i_d) = (i_1 i_d)(i_1 i_{d-1}) \ldots (i_1 i_2)$. □

Следствие. *S_n порождается транспозициями.*

▷ Следует из предложения с учетом следствия из предложения 3.1. □

Предложение 3.3. *Транспозиция (kl), $k < l$, представляется в виде произведения $2(l-k)+1$ транспозиций вида $(i\ i+1)$.*

▷ Имеем $(kl) = (k\ k+1)(k+1\ k+2)\ldots(l-2\ l-1)(l-1\ 1)(l-2\ l-1)\ldots(k\ k+1)$. Это равенство можно проверить непосредственно. □

Следствие. $S_n = \langle (12), (23), \ldots, (n-1\ n) \rangle$.

▷ Следует из предложения с учетом следствия из предложения 3.2. □

Упражнение. Покажите, что $S_n = \langle (12), (12\ldots n) \rangle$.

Четность перестановки.

Для $\sigma \in S_n$ *инверсией* назовем каждую пару (i, j), $1 \leqslant i < j \leqslant n$, для которой $\sigma(i) > \sigma(j)$. Через $N(\sigma)$ обозначим количество инверсий в перестановке σ. Также введем *знак* перестановки $\varepsilon(\sigma) = (-1)^{N(\sigma)}$. Перестановки, для которых $\varepsilon(\sigma) = 1$ называются *четными*, а для которых $\varepsilon(\sigma) = -1$ — *нечетными*.

Упражнение. Покажите, указав подходящую биекцию, что при $n \geqslant 2$ количества четных и нечетным перестановок равны.

Предложение 3.4. *Пусть $\sigma \in S_n$.*
1) Пусть $\tau \in S_n$ — транспозиция вида $(i\ i+1)$. Тогда $N(\sigma\tau) = N(\sigma) \pm 1$.
2) Пусть $\tau \in S_n$ — произвольная транспозиция. Тогда $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$.

▷ 1) Таблица, задающая $\sigma(i\ i+1)$, получается из таблицы, задающей σ, обменом двух соседних чисел в нижней строке.
2) Согласно предложению 3.3, τ представляется в виде произведения нечетного количества транспозиций вида $(i\ i+1$. Тогда из 1) следует, что при домножении справа на τ знак перестановки меняется нечетное количество раз. □

Теорема 3.1. *Пусть $\sigma \in S_n$. Тогда σ — четная (нечетная) $\Leftrightarrow$ σ представляется в виде произведения четного (нечетного) количества транспозиций.*

▷ По следствию из предложения 3.2, каждая перестановка представляется в виде $\sigma = \mathrm{Id}\,\tau_1\tau_2\ldots\tau_k$, где Id — тождественная перестановка, а τ_i — транспозиции. Так как $\varepsilon(\mathrm{Id}) = 1$, четность перестановки σ совпадает с четностью k. □

Следствие. *Если $\sigma \in S_n$ — цикл длины d, то $\varepsilon(\sigma) = (-1)d - 1$.*

▷ Следует из теоремы с учетом предложения 3.2. □

Теорема 3.2. *Пусть $\sigma, \eta \in S_n$. Тогда:*
1) $\varepsilon(\sigma\eta) = \varepsilon(\sigma)\varepsilon(\eta)$.
2) $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

▷ Следует из теоремы 3.1. □

Следствие. *Множество четных перестановок является подгруппой в S_n.*

Подгруппа всех четных перестановок называется *знакопеременной*, ее обозначают A_n. Утверждение теоремы 3.2 означает, что отображение $\sigma \mapsto \varepsilon(\sigma)$ является гомоморфизмом из S_n в группу (по умножению) из двух элементов ± 1.

§ 4. Смежные классы. Теорема Лагранжа.

Пусть в группе $(G, \cdot)$ зафиксирована подгруппа $H \leqslant G$. Введем на G отношение $\sim$: положим $a \sim b \Leftrightarrow a^{-1}b \in H$.

Предложение 4.1. *Введенное отношение является отношением эквивалентности.*

▷ ... □

Заметим, что $a^{-1}b = h \in H \Leftrightarrow b = ah$, где $h \in H$. Значит, класс эквивалентности элемента a равен aH (по определению, $aH = \{ah \mid h \in H\}$) и называется *левым смежном классом* по подгруппе H. Таким образом, введенное отношение порождает разбиение G на левые смежные классы. Одним из классов является сама подгруппа $H = eH$.

Предложение 4.2. *Любые два левых смежных класса равномощны.*

▷ Отображение $h \mapsto ah$ задает биекцию $H \to aH$. □

Теорема 4.1. *(теорема Лагранжа). Пусть $(G, \cdot)$ — группа. Пусть $|G| < \infty$ и $H \leqslant G$. Тогда $|G| \vdots |H|$.*

▷ G разбивается на равномощные левые смежные классы, один из которых совпадает с H, значит $|G| = s \cdot |H|$, где s — количество левых смежных классов. (Иногда теоремой Лагранжа называют последнее утверждение.) □

Следствие 1. *Пусть $(G, \cdot)$ — группа. Пусть $|G| < \infty$ и $a \in G$. Тогда $|G| \vdots \operatorname{ord} a$.*

▷ Достаточно взять $H = \langle a \rangle$ (с учетом следствия из теоремы 2.1). □

Следствие 2. *Пусть $(G, \cdot)$ — группа. Пусть $|G| < \infty$ и $a \in G$. Тогда $a^{|G|} = e$.*

▷ Вытекает из предыдущего следствия и предложения 2.1. □

Следствие 3. *(теорема Эйлера) Пусть $k \in \mathbb{Z}$, $n \in \mathbb{N}$, $(k, n) = 1$. Тогда $k^{\varphi(n)} - 1 \vdots n$.*

▷ В $\mathbb{Z}_n^*$ выполнено: $|\mathbb{Z}_n^*| = \varphi(n)$, значит, по предыдущему следствию, $\overline{k}^{\varphi(n)} = \overline{1}$. □

В случае простого $n = p$ предыдущая теорема превращается в малую теорему Ферма (так как $\varphi(p) = p - 1$).

Следствие 4. *(классификация групп простого порядка) Пусть $(G, \cdot)$ — группа, $|G| = p$ — простое число. Тогда G — циклическая группа.*

$\triangleright$ Возьмем $a \in G$, $a \neq e$ и возьмем подгруппу $H = \langle a \rangle$. Тогда $|H| \geqslant 2$, а в силу теоремы Лагранжа, $p \vdots |H|$. Отсюда $|H| = p$, т.е. $H = G$, значит $H = \langle a \rangle$. $\square$

ПРИМЕРЫ.

Гомоморфизм.

Пусть $\varphi : G \to \widetilde{G}$ — гомоморфизм. *Ядром* гомоморзизма называется полный прообраз нейтрального элемента, т.е. множество $H = \{a \in G \,|\, \varphi(a) = e\}$. Тогда классы эквивалентности относительно отношения эквивалентности $a \sim b \Leftrightarrow \varphi(a) = \varphi(b)$ — это левые смежные классы по подгруппе H. (В этом примере каждый левый смежный класс совпадает с правым. Подгруппы H с таким свойством наызваются *нормальными*. Только нормальная подгруппа может являться ядром гомоморфизма. На фактор-множестве можно ввести операцию по правилу $aH \cdot bH = abH$, превращающую фактор-множество в группу — это *фактор-группа*.)

Например, смежный классы $GL_n(\mathbb{R})$ по $SL_n(\mathbb{R})$ — множество матриц с фиксированным определителем. Это можно увидеть из гомоморфизма $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$.

Действия.

Пусть группа $(G, \cdot)$ действует на множестве X, и $a(X') = X''$ (где $a \in G$, $X', X'' \subset X$, подразумевается, что X' и X'' — из одной орбиты). Тогда множество $\{b \in G \,|\, b(X') = X''\}$ равно смежному классу aH, где H — стабилизатор $Sym(X')$. Имеется биекция между смежными классами по стабилизатору $Sym(X')$ и элементами орбиты $G(X')$.

Глава 3

Кольца и поля.

§ 1. Определения и примеры.

Рассмотрим $(K, +, \cdot)$ — множество K с двумя бинарными операциями. Рассмотрим следующие аксиомы.

К I. $(K, +, \cdot)$ — абелева группа.

К II.1. $a(b + c) = ab + ac \qquad (\forall\ a, b, c \in K)$;
К II.2. $(a + b)c = ac + bc \qquad (\forall\ a, b, c \in K)$.

К III.1. $(ab)c = a(bc) \qquad (\forall\ a, b, c \in K)$;
К III.2. $\exists\ 1 \in K \quad \forall\ a \in K: \quad a \cdot 1 = 1 \cdot a = a$;
К III.3. $\forall\ a \in K \setminus \{0\} \quad \exists\ a^{-1}$.
К III.4. $ab = ba \qquad (\forall\ a, b \in K)$.

К II — аксиомы дистрибутивности, они связывают две операции в K.

Докажем некоторые следствия аксиом.

Предложение 1.1. *Пусть $(K, +)$ удовлетворяет аксиомам К I и К II. Тогда $\forall\ a, b, c \in K$ выполнено:*
1) $\forall\ a \in K\ \ a \cdot 0 = 0 \cdot a = 0$.
2) $a(-b) = (-a)b = -(ab)$.
3) $a(b - c) = ab - ac$; $(a - b)c = ac - bc$.

$\triangleright$ ... $\square$

Дадим основное определение:

|| $(K, +, \cdot)$ называем *кольцом*, если удовлетворяет аксиомам К I, К II и К III.1.

(Иногда кольцом называют $(K, +, \cdot)$, удовлетворяющие только аксиомам К I, К II, а кольцо, удовлетворяющее также К III.1, называют *ассоциативным кольцом*.)

Кольцо $(K, +, \cdot)$, удовлетворяющее К III.2, называют *кольцом с единицей*. Нетрудно показать, что если в кольце с единицей $1 = 0$, то $K = \{0\}$. Далее считаем, что $1 \neq 0$.

Кольцо $(K, +, \cdot)$, удовлетворяющее также К III.4, называют *коммутативным кольцом*.

Кольцо $(K, +, \cdot)$, удовлетворяющее К III.2 и К III.3, называют *телом*.

Кольцо $(K, +, \cdot)$, удовлетворяющее К III.2, К III.3 и К III.4, называют *полем*.

Подмножество $L \subset K$ называется *подкольцом*, если L — подгруппа в $(K, +)$ и K замкнуто относительно операции умножения.

Имея кольца K_i $(i = 1, \ldots, t)$, можно определить их прямую сумму $K_1 \oplus K_2 \oplus \ldots \oplus K_t$ (операции производятся покомпонентно).

В коммутативном кольце K элемент $a \in K$ называется *делителем нуля*, если $\exists\, b \in K$, $b \neq 0$: $ab = 0$.

Предложение 1.2. *Пусть $(K, +, \cdot)$ — коммутативное кольцо с единицей. Если a — обратимый элемент (в полугруппе K), то a не является делитем нуля.*

$\triangleright$ Пусть $ab = 0$. Тогда $a^{-1}ab = 0 \Rightarrow b = 0$. $\square$

Примеры.

I. Числа:
$(\mathbb{Z}, +, \cdot)$ — коммутативное кольцо с единицей без делителей нуля.
$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ — поля.

II. Кольца вычетов:
$(\mathbb{Z}_n, +, \cdot)$ — коммутативное кольцо с единицей. Если n составное, то в $\mathbb{Z}_n$ есть делители нуля. Если $n = p$ — простое, то $(\mathbb{Z}_p, +, \cdot)$ — поле (см. ниже).

III. Матрицы:
$(\mathbb{M}_{n\times n}(\mathbb{F}), +, \cdot)$ — кольцо с единицей (где $\mathbb{F}$ — поле, или более общо, коммутативное кольцо с единицей). При $n \geqslant 2$ это кольцо некоммутативное.

Упражнение. Опишите делители нуля в $\mathbb{M}_{n\times n}(\mathbb{R})$.

IV. Многочлены:
$(\mathbb{F}[X], +, \cdot)$ — коммутативное кольцо, (где $\mathbb{F}$ — поле, или более общо, коммутативное кольцо).

Упражнение. Покажите, что если F не имеет делителей нуля, то $\mathbb{F}[X]$ — тоже.

§ 2. Начала теории делимости в кольцах.

В этом параграфе K обозначает коммутативное кольцо с единицей без делителей нуля.

Пусть $a, b \in K$, $b \neq 0$. Скажем, что a делится на b, если найдется элемент $c \in K$ такой, что $a = bc$. Испольуем обычное обозначение $a \vdots b$ или $b \mid a$.

Очевидно, если $a \vdots c$, $b \vdots c \Rightarrow a \pm b \vdots c$. Отношение делимости рефлексивно и транзитивно, т.е. $a \vdots b$, $b \vdots c \Rightarrow a \vdots c$.

Упражнение. Пусть $b \in K$, $b \neq 0$. Покажите, что $b \in K^* \Leftrightarrow \forall\, a \in K\ a \vdots b$ (здесь как обычно, K^* обозначает множество обратимых элементов кольца K.)

Введем отношение *ассоциировнности*: $a \sim b$, если $\exists\, t \in K^*$: $a = tb$.

Предложение 2.1. *Это отношение — эквивалентность.*

$\triangleright$ ... $\square$

Покажем, что замена элемента на эквивалентный (ассоциированный) не меняет делимости (Т.е. на самом деле можно говорить не о делимости элементов, а о делимости классов ассоциированных элементов.)

Предложение 2.2. *Пусть $a \sim a'$, $b \sim b'$. Тогда $a \vdots b \Leftrightarrow a' \vdots b'$.*

$\triangleright$ ... $\square$

Упражнение. $a \sim b \Leftrightarrow a \vdots b$ и $b \vdots a$. (в доказательстве здесь использвуется отсутствие делителей нуля).

Скажем, что элемент $c \in K$ является общим делителем (ОД) элементов a и b, если $a \vdots c$ и $b \vdots c$. Скажем, что элемент $d \in K$ равен НОД элементов a и b, если d является ОД и для любого ОД c выполнено $d \vdots c$. (Конечно, для произвольного K НОД (a, b) не обязан существовать.) Обозначение для НОД: (a, b). Если $(a, b) = 1$, то a и b называются взаимно-простыми.

Предложение 2.3. *Пусть для некоторых $a, b \in K$ $\exists\ (a, b)$. Тогда (a, b) определен однозначно с точностью до ассоциированности.*

$\triangleright$ ... $\square$

Предложение 2.4. *Пусть $a, b, q \in K$. Множество общих делителей a и b совпадает с множеством общих делителей $a + qb$ и b. В частности, если существует (a, b), то существует и $(a + qb, b)$, и он равен (a, b).*

$\triangleright$ ... $\square$

Элемент $p \notin K^*$ называется *неразложимым*, если из равенства $p = ab$ следует, что хотя бы один из элементов a, b принадлежит K^*.

(Имеется понятие *простого элемента* кольца, но оно несколько отличается от понятия неразложимого элемента.) Иными словами, у неразложимого элемента делителями являются только 1, p и ассоциированные с ними элементы.

§ 3. Кольцо $\mathbb{Z}$.

Алгоритм Евклида. Линейное представление НОД.

Так как $\mathbb{Z}^* = \{-1, 1\}$, в кольце $\mathbb{Z}$ ассоциированные элементы могут отличаться только знаком. Понятие НОД согласуется с общем понятием НОД из предыдущего параграфа. Понятие простого числа согласуется с понятием неразложимого элемента кольца.

Пусть $a, b \in \mathbb{N}$. Положим $r_0 = a$, $r_1 = b$, произведем многократное деление с остатком (это и есть алгоритм Евклида):

$r_0 = q_1 r_1 + r_2$,
$r_1 = q_2 r_2 + r_3$,
$\dots$,
$r_{n-1} = q_n r_n + 0$.

Поскольку $r_1 > r_2 > r_3 > \ldots \geqslant 0$, процедура закончится тем, что очередной остаток $r_{n+1} = 0$. Согласно предложению 2.4, $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_n, 0) = r_n$.

Теорема 3.1. *(О линейном предсталении НОД) Пусть $a, b \in \mathbb{Z}$, $b \neq 0$, $d = (a, b)$. Тогда $\exists\ x, y \in \mathbb{Z}$: $d = xa + yb$.*

$\triangleright$ ... Пусть $a, b \in \mathbb{N}$ (другие случаи легко сводятся к этому). Из формул алгоритма Евклида последовательно для $k = 1, 2, \ldots$ находим $x_k, y_k \in \mathbb{Z}$: $x_k a + y_k b = r_k$... $\square$

Упражнение. Докажите, что в линейном представлении НОД $d = xa + yb$ для $a, b \in \mathbb{N}$ можно выбрать $|x| < b$, $|y| < a$.

Разложение на простые множители и его единственность.

Лемма. *Пусть $a, b, p \in\in \mathbb{Z}$, причем p — простое число и $ab \vdots p$. Тогда $a \vdots p$ или $b \vdots p$.*

$\triangleright$ Если b не делится на p, то $(b, p) = 1$. По теореме о линейном представлении НОД тогда найдутся $x, y \in \mathbb{Z}$ такие, что $1 = bx + py$. Умножим равенство на a, получим $a = abx + apy$. Так как $abx \vdots p$ и $apy \vdots p$, получаем, что $a \vdots p$. $\square$

Теорема 3.2. *(Основная теорема арифметики) 1)* $\forall\ a \in \mathbb{N}$, $a > 1$, *существует разложение* $a = p_1 p_2 \dots p_k$, *где* p_i — *простые числа.*
2) В указанном разложении набор простых множителей определен однозначно.

$\triangleright$ 1)...
2) Рассуждаем от противного. Пусть a — минимальное натуральное число, для которого имеются два различных разложения: $a = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$. Так как $p_1(p_2 \dots p_k) \vdots q_1$, то по лемме либо $p_1 \vdots q_1$ (и значит, $p_1 = q_1$, ибо оба числа простые), либо $p_2 \dots p_k \vdots q_1$. Продолжая далее: $p_2(p_3 \dots p_k) \vdots q_1$ и т.д., в конце концов находим $p_i = q_1$. Сокращая равенство $p_1 p_2 \dots p_k = q_1 q_2 \dots q_k$ на q_1, получаем противоречие с выбором a. $\square$

Китайская теорема об остатках.

Теорема 3.3. *(Китайская теорема об остатках) Пусть даны* $a_1, \dots, a_k \in \mathbb{N}$ — *попарно взаимно простые числа,* $r_1, \dots, r_k \in \mathbb{Z}$. *Тогда* $\exists\ x \in \mathbb{Z}$: $x \equiv r_i \pmod{a_i}$, $i = 1, \dots, k$.

$\triangleright$ Применим теорему о линейной представлении НОД к a_1 и $A_1 = a_2 \dots a_k$: $\exists\ t, s \in \mathbb{Z}$: $ta_1 + sA_1 = 1$. Положим $x_1 = sA_1$. Тогда $x_1 \equiv 1 \pmod{a_1}$ и $x_1 \equiv 0 \pmod{a_i}$ $i = 2, \dots, k$.
Аналогично найдем $x_2, \dots, x_k$ так, что $x_m \equiv 1 \pmod{a_m}$ и $x_m \equiv 0 \pmod{a_i}$ при $i \neq m$.
Искомое x зададим как $x = r_1 x_1 + r_2 x_2 + \dots + r_k x_k$. $\square$

Упражнение. Покажите, что в условиях Китайской теоремы об остатках x можно выбрать из множества $\{0, 1, \dots, a_1 a_2 \dots a_k - 1\}$.

§ 4. Арифметика по модулю n (кольцо $\mathbb{Z}_n$).

Структура $\mathbb{Z}_n$.

Теорема 4.1. *Пусть* $m, n \in \mathbb{N}$, $(m, n) = 1$. *Тогда* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.

$\triangleright$ Для числа $k \in \mathbb{Z}$ пусть $\overline{k}_{(s)}$ означает соответствующий вычет в $\mathbb{Z}_s$. Рассмотрим отображение $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$, заданное правилом $\overline{k}_{(mn)} \mapsto (\overline{k}_{(m)}, \overline{k}_{(n)})$. Это отображение корректно и гомоморфно (док-во...). А из Китайской теоремы об остатках следует, что оно сюръективно, и значит, биективно, ввиду $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$. $\square$

Следствие 1. *Пусть* $n \in \mathbb{N}$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *где* p_i — *попарно различные простые числа, а* $\alpha_i \in \mathbb{N}$. *Тогда* $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$.

Следствие 2. *(Формула для функции Эйлера) Пусть* $n \in \mathbb{N}$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *где* p_i — *попарно различные простые числа, а* $\alpha_i \in \mathbb{N}$. *Тогда* $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$.

$\triangleright$ Из предыдущего следствия получаем, что $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}^*$. Приравнивая порядки групп, получаем мультипликативность функции Эйлера: $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k})$.
Но $\varphi(p^\alpha)$ находится непосредственно: чтобы в множестве $\{1, 2, \dots, p^\alpha\}$ остались только числа, взаимно простые с p^α, надо вычеркнуть числа, кратные p, отсюда $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. $\square$

Делители нуля и обратимые элементы. Поле $\mathbb{Z}_p$.

Как мы видели ранее, в кольце $\mathbb{Z}_n$ обратимые элементы — в точности элементы вида $\overline{k}$, где $(k, n) = 1$. Остальные элементы — делители нуля. Действительно, если $(k, n) = d > 1$, положим $m = n/d$. Тогда $mk \vdots n$, т.е. $\overline{m}\overline{k} = \overline{0}$, но $\overline{m} \neq \overline{0}$. Отсюда, в частности, мы получаем:

Теорема 4.2. *Кольцо* $\mathbb{Z}_n$ — *поле* $\Leftrightarrow$ n — *простое число.*

Характеристика поля.

Пусть $\mathbb{F}$ — произвольное поле. Пусть $p = \operatorname{ord} 1$ (порядок единицы поля в абелевой группе $(\mathbb{F}, +)$. Если $p < \infty$, говорят, что поле имеет *характеристику* p. Иначе говорят, что поле имеет характеристику 0. Характеристику поля $\mathbb{F}$ обозначаем $\operatorname{Char}\mathbb{F}$.

Теорема 4.3. *Пусть $\mathbb{F}$ — поле, $\operatorname{Char}\mathbb{F} = p < \infty$. Тогда p — простое число.*

$\triangleright$ Предположим противное, $p = kl$, где $k, l \in \mathbb{N}$, $k > 1$, $l > 1$. Тогда в абелевой группе $(\mathbb{F}, +)$ выполнено $(kl) \cdot 1 = 0$, но $k \cdot 1 \neq 0$, $l \cdot 1 \neq 0$. С другой стороны, из дистрибутивности в $\mathbb{F}$ выполнено $(kl) \cdot 1 = (k \cdot 1)(l \cdot 1)$ — в поле нашлись делители нуля — противоречие. $\square$

Можно показать, что в поле $\mathbb{F}$ характеристики p элементы $\{k \cdot 1 \,|\, k = 0, 1, \ldots, p-1\}$, образуют подполе. Это подполе является минимальным подполем (так называемое *простое подполе*) в $\mathbb{F}$, оно изоморфно полю $\mathbb{Z}_p$. Если же $\operatorname{Char}\mathbb{F} = 0$, то элементы вида $(k \cdot 1)(l \cdot 1)^{-1}$, $k \in \mathbb{Z}$, $l \in \mathbb{N}$, простое подполе, изоморфное $\mathbb{Q}$.

§ 5. Поле комплексных чисел.

Операции в $\mathbb{C}$.

Сопряжение. Модуль и аргумент комплексного числа, тригонометрическая запись. Умножение, возведение в степень, обращение. Извлечение корней.

Примеры подполей в $\mathbb{C}$, подгруппы в $\mathbb{C}^*$.

Матрицы с комплексными коэффициентами.

Гауссовы числа.

Делимость. Деление с остатком. Разложение на простые.

Кватернионы.

Определение. Обратимость.

§ 6. Кольцо многочленов от одной переменной.

Делимость в $\mathbb{F}[X]$.

Пусть $\mathbb{F}$ — поле. Тогда $\mathbb{F}[X]$ — коммутативное кольцо с единицей без делителей нуля.

Делимость. НОД. Алгоритм Евклида. Разложение на неприводимые сомножители (неразложимые элементы кольца) и его единственность. (Аналогично $\mathbb{Z}$).

Неприводимые многочлены над $\mathbb{R}$, $\mathbb{C}$.