АЛГЕБРА-3

МОДУЛЬ 1. ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП

МОДУЛЬ 2. ЭЛЕМЕНТЫ ТЕОРИИ КОЛЕЦ

МОДУЛЬ-1

ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП

§1. Группа. Примеры и простейшие свойства элементов группы.

О.1. Пусть M – множество. Говорят, что на M задана *бинарная алгебраическая операция* φ, если задано отображение $\varphi: M \times M \to M$, т. е. любой упорядоченной паре (a,b) элементов из M соответствует однозначно определенный элемент $c = \varphi(a,b) = a\varphi b \in M$.

О.2. Непустое множество G, с заданной на нем бинарной операцией $\circ$, называется *группой*, если выполняются следующие условия (аксиомы):

1) операция $\circ$ ассоциативна на множестве G, т. е.

$$\forall a, b, c \in G: (a \circ b) \circ c = a \circ (b \circ c);$$

2) в G существует нейтральный элемент e, т. е.

$$\exists e \in G \ \forall a \in G: e \circ a = a \circ e = a;$$

3) каждый элемент в G обладает симметричным элементом в G, т. е.

$$\forall a \in G \ \ \exists a' \in G: a' \circ a = a \circ a' = e.$$

Вместо общей формы записи операции $\circ$ в теории групп принято использовать обозначения операций:

$+$ – сложение (аддитивная форма записи) и

$\cdot$ – умножение (мультипликативная форма записи).

$(G,+)$	$(G,\cdot)$
1) ассоциативность: $\forall a,b,c \in G$: $(a+b)+c=a+(b+c)$;	1) ассоциативность: $\forall a,b,c \in G$: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;
2) нейтральный элемент обозначают 0 и называют *нулевым* (*нулем*): $\exists 0 \in G\ \forall a \in G$: $0+a=a+0=a$;	2) нейтральный элемент обозначают 1 и называют *единичным* (*единицей*): $\exists 1 \in G\ \forall a \in G$: $1\cdot a=a\cdot 1=a$;

3) симметричный элемент обозначают $-a$ и называют *противоположным*:

$$\forall a \in G \ \exists -a \in G:$$

$$-a + a = a + (-a) = 0.$$

В этом случае множество G называют *аддитивной* группой.

3) симметричный элемент обозначают a^{-1} и называют *обратным*:

$$\forall a \in G \ \exists a^{-1} \in G:$$

$$a^{-1} \cdot a = a \cdot a^{-1} = 1.$$

В этом случае множество G называют *мультипликативной* группой.

О.3. Если бинарная операция $\circ$ коммутативна на G, т.е.

$$a \circ b = b \circ a, \forall a, b \in G,$$

то группу $(G, \circ)$ называют *абелевой*.

О.4. Если множество G состоит из конечного числа элементов, то группа G называется *конечной*. Число элементов конечной группы G будет обозначать $|G|$ и называть *порядком* этой группы. Если множество G бесконечно, то группу G называют *бесконечной*.

Рассмотрим некоторые примеры групп

Пр.1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – бесконечные аддитивные абелевы группы.

Пр.2. Множество $\mathbb{Z}_n$ классов вычетов по модулю n – конечная аддитивная абелева группа порядка n.

Пр.3. $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}, \mathbb{C}^* = \mathbb{C}\backslash\{0\}$ – бесконечные мультипликативные абелевы группы.

Пр.4. Множество S_n подстановок степени n – конечная группа порядка $n!$. Группа S_n при $n > 2$ неабелева.

Пр.5. Множества матриц

$$M_{m\times n}(P)=\left\{\left.\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}\right| a_{ij}\in P-\text{поле}\right\}-$$

аддитивная абелева группа.

$GL_n(P)=\{A\in M_{n\times n}(P)||A|\neq 0\}-$ мультипликативная группа

$SL_n(P)=\{A\in M_{n\times n}(P)||A|=1\}-$ мультипликативная группа

В дальнейшем, если не оговорено противное, будем рассматривать мультипликативную форму записи и обозначение · опускать.

Отметим некоторые свойства элементов группы.

Св-во 1. В группе имеется единственный единичный элемент и для каждого элемента существует единственный обратный.

Св-во 2. $(a^{-1})^{-1} = a$ и $(ab)^{-1} = b^{-1}a^{-1}, \forall a, b \in G$.

Пусть $a \in G$. Обозначим $\underbrace{aa \dots a}_{n} = a^n$, $a^{-n} = (a^n)^{-1}$.

Несложно доказать, что $\forall m, n \in \mathbb{Z}$:

$$(a^n)^{-1} = (a^{-1})^n = a^{-n},$$

$$a^m a^n = a^{m+n} \text{ и } (a^m)^n = a^{mn}.$$

Св-во 3. В группе уравнение $ax = b$ и $yc = d$ имеет единственное решение.

§2. Подгруппа. Критерий подгруппы.

О.1. Пусть G – группа и $\emptyset \neq H \subseteq G$. Если H является группой относительно той же операции, которая задана на G, то H называется *подгруппой* группы G и пишут $H \leq G$.

Если $H \neq G$, то подгруппу H называют *собственной* и пишут $H < G$.

3.1. Очевидно, что не всякое подмножество элементов группы является группой. Например,

$\mathbb{Z}-$ аддитивная абелева группа,

$H_1 = 2\mathbb{Z}-$ собственная подгруппы $\mathbb{Z}$,

$H_2 = 2\mathbb{Z} + 1 -$ не является подгруппой в $\mathbb{Z}$.

Т.1 (критерий подгруппы). Пусть G – группа и $\emptyset \neq H \subseteq G$. Тогда H является подгруппой группы $G \Leftrightarrow$ когда выполнены следующие условия:

(1) $\forall h_1, h_2 \in H: h_1 h_2 \in H$;

(2) $\forall h \in H: h^{-1} \in H$.

Пр.1. $SL_n(P) \leq GL_n(P)$.

§3. Порядок элемента группы. Циклическая группа.

О.1. Пусть $G -$ группа, $a \in G$. Если $\exists n \in \mathbb{N}$, что

$$\underbrace{aa \dots a}_{n} = a^n = 1,$$

причем n является наименьшим натуральным числом с таким свойством, то n называют *порядком* элемента a и обозначают: $|a| = n$. Если такого $n \in \mathbb{N}$ не существует, то a называют элементом бесконечного порядка и обозначают: $|a| = \infty$. Полагаем, что $a^0 = 1$.

Пр.1. Найти порядок:

1) элемента $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ в группе $GL_2(\mathbb{Z}_2) =$

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\}.$$

2) элемента $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 5 & 3 & 8 & 1 & 6 \end{pmatrix}$

в группе S_8.

О.2. Элементы второго порядка в группах называют *инволюциями*.

З.1. Сама группа может быть бесконечной, но в ней могут существовать неединичные элементы конечных порядков. Например, $GL_2(\mathbb{Q})$ – бесконечная группа, хотя

$$C^3 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = E,$$

т. е. $o(C) = 3$.

О.3. Пусть G – группа, $a \in G$. Если любой другой элемент этой группы можно записать в виде $a^k, k \in \mathbb{Z}$ то говорят, что данная группа является циклической группой, порожденной элементом a и записывают

$$G =< a >= \{a^k \big| k \in \mathbb{Z}\}.$$

Сам элемент a называется *порождающим элементом* группы G.

Пр.2. Рассмотрим примеры циклических групп.

(1) $G_1 = \{-1, 1\} = \langle -1 \rangle$ – мультипликативная циклическая группа порядка 2.

(2) $G_2 = \{-1, 1, i, -i\} = \langle i \rangle = \langle -i \rangle$ – мультипликативная циклическая группа порядка 4.

(3) $G_3 = \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix} \middle| \, k \in \mathbb{Z} \right\}$ – мультипликативная бесконечная циклическая группа.

3.2. Мы дали определение циклической группы для мультипликативных групп. Однако, его можно переформулировать для аддитивных групп, если рассматривать кратные некоторого элемента a, полагая

$$0 \cdot a = 0.$$

Пр.2.

(4) $G_4 = \mathbb{Z} = \langle 1 \rangle$ – аддитивная бесконечная цикличес-кая группа.

(5) $G_5 = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} = \langle \bar{1} \rangle$ – аддитивная циклическая группа порядка n.

Т.1. Пусть G – группа, $g \in G \backslash \{1\}$ и $|g| = n$, $n \in \mathbb{N}$.

Тогда имеют место следующие утверждения:

(1) $g^m = 1 \Leftrightarrow m \vdots n$,

(2) $g^k = g^l \Leftrightarrow k \equiv l (mod\ n)$.

Сл.1. Если $|g| = n$, то $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ и

$$|\langle g \rangle| = |g| = n.$$

Т.2. Если $|g| = n$, то для любого $k \in \mathbb{N}$:

$$\left|g^k\right| = \frac{n}{(n,k)}.$$

Сл.2. Элемент g^k можно взять в качестве порождающего элемента конечной циклической группы $\langle g \rangle$ порядка $n \Leftrightarrow$ когда $(n, k) = 1$.

§4. Отображения. Инъективные и сюръективные отображения. Изоморфизм групп.

О.1. Пусть A и B – некоторые множества. Отображением множества A в множество B называют всякое правило φ, по которому каждому элементу множества A сопоставляют единственный элемент множества B. Обозначается: $\varphi: A \to B$.

Если элементу $a \in A$ сопоставлен $b \in B$, то b называют образом элемента a, а $a -$ прообразом элемента b при отображении φ и обозначают $\varphi(a) = b$.

Множество $\varphi(A) = \{\varphi(a) | a \in A\}$ будем называть образом множества A во множестве B.

О.2. Отображение φ: $A \to B$ называется:

1) сюръективным (или отображением на множество B), если каждый элемент из B является образом хотя бы одного элемента из A, т.е. $\forall b \in B \ \ \exists a \in A$: $\varphi(a) = b$ или $\varphi(A) = B$.

2) инъективным (инъекцией), если образы различных элементов множества A будут различными элементами множества B, т. е. если $a_1 \neq a_2$, то $\varphi(a_1) \neq \varphi(a_2)$, где $a_1, a_2 \in A$ и $\varphi(a_1), \varphi(a_2) \in B$.

3) биективным (биекцией или взаимно однозначным соответствием), если оно сюръективно и инъективно.

О.3. Пусть заданы две группы $(G_1,\circ)$ и $(G_2,*)$. Группы G_1 и G_2 будем называть *изоморфными* и записывать $G_1 \cong G_2$, если существует биективное отображение φ: $G_1 \to G_2$, называемое *изоморфизмом*, для которого сохраняется операция, т. е.

$$\varphi(a \circ b) = \varphi(a) * \varphi(b), \forall a, b \in G_1.$$

Пр.1. Доказать, что мультипликативная группа

$$G_1 = \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix} \middle| \, k \in \mathbb{Z} \right\}$$

изоморфна аддитивной группе $G_2 = 2\mathbb{Z}$.

Т.1. Всякая бесконечная циклическая группа изоморфна аддитивной группе $\mathbb{Z}$. Всякая конечная циклическая группа порядка n изоморфна аддитивной группе $\mathbb{Z}_n$.

Пр.2. Показать, что мультипликативная циклическая группа $G_1 = \{-1, 1, i, -i\} = \langle i \rangle$ изоморфна аддитивной циклической группе $G_2 = \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Установим отображение φ по следующему правилу:

$$\varphi(1) = \varphi(i^0) = \overline{0},$$

$$\varphi(i) = \varphi(i^1) = \overline{1},$$

$$\varphi(-1) = \varphi(i^2) = \overline{2},$$

$$\varphi(-i) = \varphi(i^3) = \overline{3}.$$

§5. Подгруппы циклических групп.

Т.1. Всякая подгруппа циклической группы является циклической группой. В циклической группе порядка n порядок любой ее подгруппы делит число n, и, наоборот, для любого делителя d числа n существует единственная циклическая подгруппа порядка d.

§6. Задание конечной группы таблицей Кэли. Теорема Кэли.

О.1. Пусть $G = \{1 = g_1, g_2, \dots, g_n\}$ – конечная группа порядка n. Составим таблицу вида:

$\cdot$	$1 = g_1$	g_2	$\dots$	g_n
$1 = g_1$	1	g_2	$\dots$	g_n
g_2	g_2	$g_2 g_2$	$\dots$	$g_2 g_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_n	g_n	$g_n g_2$	$\dots$	$g_n g_n$

Таблица такого вида называется *таблицей Кэли*.

Св-во 1. Два элемента группы перестановочны $\Leftrightarrow$ соответствующие им элементы в таблице Кэли совпадают.

Св-во 2. Группа абелева $\Leftrightarrow$ ее таблица Кэли симметрична относительно главной диагонали.

Св-во 3. Все элементы, стоящие в некоторой строке (столбце) таблицы Кэли различны между собой.

Пр.1. Составить таблицу Кэли для $G = \{-1, 1, i, -i\}$.

Т.1 (Кэли). Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Пр.2. Пусть $G = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ – аддитивная группа и

$$H = \left\{e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\} \leq S_3.$$

Установим отображение $\varphi: \mathbb{Z}_3 \longrightarrow H$ по правилу:

$$\varphi(0) = e, \varphi(1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \varphi(2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Покажем, что $G \cong H$.

§7. Смежные классы. Теорема Лагранжа.

О.1. Пусть G – группа, $H \leq G$ и $g \in G$. Множество

$$gH = \{gh | h \in H\}$$

называется *левым смежным классом* группы G по подгруппе H с представителем g.

Т.1. Любые два левых смежных класса группы G по подгруппе H либо не пересекаются, либо совпадают между собой.

Т.2. Любой смежный класс группы G по подгруппе H имеет ту же мощность, что и подгруппа H.

О.2. Пусть G – группа, $H \leq G$ и $g \in G$. Множество

$$Hg = \{hg | h \in H\}$$

называется *правым смежным классом* группы G по подгруппе H с представителем g.

Очевидно, что для правых классов также будут справедливы теоремы 1 и 2.

О.3. Пусть G – группа и $H \leq G$. Так как $H -$ группа, то $1 \in H$ и левый смежный класс gH (правый смежный класс Hg) будет содержать элемент $g \cdot 1 = g \in gH$ ($1 \cdot g = g \in Hg$). Элемент $g \in gH$ ($g \in Hg$) называется представителем смежного класса.

Если взять в качестве представителя единичный элемент группы G, то $1 \cdot H = \{1 \cdot h | h \in H\} = H$ и $H \cdot 1 = H$. Значит, подгруппу H можно рассматривать в качестве смежного класса.

Если группа имеет конечное число смежных классов, то это количество будет одинаковым для правых и левых смежных классов.

О.4. Конечное число смежных классов (левых или правых) группы G по подгруппе H называют индексом подгруппы H в группе G и обозначают $|G:H|$.

Пр.1. Найти разложение группы

$$S_3 = \{e, \pi_1, {\pi_1}^2, \pi_2, \pi_3, \pi_4\}, \text{ где}$$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, {\pi_1}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

на смежные классы по подгруппе $H_1 = \{e, \pi_1, {\pi_1}^2\}$.

Разложение на смежные классы группы G по подгруппе H будем записывать в виде:

$$G = H \dot{\cup} g_2 H \dot{\cup} \ldots \dot{\cup} g_k H, \text{ считаем } g_1 = 1.$$

3.1. Для аддитивных групп левый (правый) смежный класс будет иметь вид $g + H$ $(H + g)$, а разложение аддитивной группы G на смежные классы по подгруппе H можно записать в виде:

$$G = H \dot{\cup} (g_2 + H) \dot{\cup} \ldots \dot{\cup} (g_k + H), \text{ считаем } g_1 = 0.$$

Пр.2. Найти разложение аддитивной группы $\mathbb{Z}$ на смежные классы по подгруппе $3\mathbb{Z}$.

Т.3 (Лагранжа). Если G – конечная группа и $H \leq G$, то

$$|G| = |H| \cdot |G:H|.$$

Сл.1. Порядок любой подгруппы H конечной группы G делит порядок группы.

Сл.2. Порядок любого элемента конечной группы делит порядок группы.

Сл.3. Всякая конечная группа простого порядка является циклической.

§8. Нормальные подгруппы. Фактор-группа.

О.1. Пусть G – группа и $H \leq G$. Подгруппа H называется *нормальной* или *инвариантной подгруппой* группы G, если

$$g^{-1}Hg = \{g^{-1}hg | h \in H\} = H, \forall g \in G.$$

Обозначается: $H \lhd G$.

Т.1. Пусть G – группа и $H \leq G$. $H \lhd G \Leftrightarrow gH = Hg, \forall g \in G$.

Сл.1. Любая подгруппа абелевой группы является нормальной.

3.1. Если группа G неабелева, то смежные классы gH и Hg могут быть не равны. Например, $G = S_3$ и $\pi_1 H_2 \neq H_2 \pi_1$.

Сл.2. Если $H \leq G$ и $|G:H| = 2$, то $H \lhd G$.

З.2. В любой группе G нормальными являются подгруппы E и G.

О.3. Неединичная группа G, нормальными подгруппами которой являются лишь E и G, называется *простой группой*.

В частности, циклические группы простых порядков являются простыми группами. Абелевы группы, которые не являются циклическими, обязательно имеют собственные подгруппы, которые будут нормальными, поэтому они не могут быть простыми. Т. о. все простые нециклические группы являются неабелевыми группами. Наименьший порядок у конечной неабелевой простой группы равен 60.

О.3. Пусть G – группа и $H \lhd G$. Рассмотрим множество

$$\bar{G} = \{gH | g \in G\}$$

всех смежных классов группы G по подгруппе H и введем на этих классах операцию умножения по следующему правилу:

$$(g_1H)(g_2H) = (g_1g_2)H, \ \forall g_1, g_2 \in G. \quad (1)$$

Несложно убедиться, что умножение смежных классов, заданное таким образом, является корректным, т. е. не зависит от выбора представителей смежных классов.

Т.2. Если $H \lhd G$, то множество $\bar{G} = \{gH | g \in G\}$ образует группу относительно операции умножения смежных классов. Эту группу будем обозначать G/H и называть фактор-группой группы G по подгруппе H.

Сл.3. Пусть G – конечная группа и $H \lhd G$. Тогда

$$|G/H| = |G:H|.$$

Пр.1. Найти фактор-группу группы

$$S_3 = \{e, \pi_1, {\pi_1}^2, \pi_2, \pi_3, \pi_4\}, \text{ где}$$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, {\pi_1}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

по подгруппе $H_1 = \{e, \pi_1, {\pi_1}^2\}$.

3.2. Мы определили операцию на смежных классах для мультипликативной группы. Однако, ее можно было определить и для аддитивных групп.

Пусть G – аддитивная группа и $H \lhd G$, т. е. $g + H = H + g$ для всех $g \in G$. Тогда множество

$$G/H = \bar{G} = \{g + H | g \in G\}$$

с операцией $(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H$ образует группу с нулевым элементом $0 + H = H$ и противоположным элементом $-(g + H) = -g + H$.

Пр.2. Найти фактор-группу аддитивной группы $\mathbb{Z}$ по подгруппе $3\mathbb{Z}$.

Т.3. Всякая фактор-группа абелевой группы является абелевой. Всякая фактор-группа циклической группы является циклической.

§9. Гомоморфизмы групп.

О.1. Пусть заданы две группы $(G_1,\circ)$ и $(G_2,*)$. Отображение $\varphi\colon G_1 \to G_2$ будем называть *гомоморфизмом*, если оно сохраняет операцию, т. е.

$$\varphi(a \circ b) = \varphi(a) * \varphi(b),\ \forall a, b \in G_1.$$

Если гомоморфизм φ является биекцией, то φ будет изоморфизмом групп G_1 и G_2.

Св-во 1. Пусть $\varphi: G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2. Тогда $\varphi(1_{G_1}) = 1_{G_2}$, т. е. образом единичного элемента группы G_1 является единичный элемент группы G_2.

Св-во 2. Пусть $\varphi: G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2. Тогда $\forall a \in G_1$: $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

О.2. Множество $Ker\varphi = \{a \in G_1 | \varphi(a) = 1_{G_2}\}$ элементов группы G_1, которые при отображении $\varphi: G_1 \to G_2$ перейдут в единичный элемент группы G_2, называется *ядром гомоморфизма* φ.

Св-во 3. Пусть $\varphi: G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2. Тогда $Ker\varphi \lhd G$.

О.3. Пусть $\varphi: G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2. Множество $\varphi(G_1) = Im\varphi = \{\varphi(a) | a \in G_1\}$ образов всех элементов группы G_1 при гомоморфизме φ будем называть *образом гомоморфизма* φ.

Св-во 4. Пусть $\varphi: G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2. Тогда $Im\varphi \leq G_2$.

О.4. Пусть φ: $G_1 \to G_2$ – гомоморфизм группы G_1 в группу G_2.

Если $Ker\varphi = \{1_{G_1}\}$, то гомоморфизм φ называют *мономорфизмом*.

Если $Im\varphi = G_2$, то гомоморфизм φ называют *эпиморфизмом*.

Гомоморфизм φ, который одновременно является моно- и эпиморфизмом, называется *изоморфизмом*, а группы G и H – изоморфными, и пишут $G_1 \cong G_2$.

Пр.1. Пусть даны две группы: $G_1 = S_3$ и $G_2 = \{-1,1\}$.

Определим отображение $\varphi: G_1 \to G_2$ следующим образом:

$$\varphi(\pi) = \begin{cases} -1, \text{если } \pi - \text{нечетная подстановка}, \\ 1, \text{если } \pi - \text{четная подстановка}, \end{cases} \quad \forall \pi \in S_3.$$

Показать, что отображение φ является эпиморфизмом.

О.5. Гомоморфизм группы в себя будем называть *эндоморфизмом* этой группы, а изоморфизм группы на себя – *автоморфизмом* группы.

Обозначим через $EndG$ и $AutG$ соответственно множество всех эндоморфизмов и автоморфизмов группы G.

Пр.2. Рассмотрим группы $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ и $\mathbb{R}^+ = \{x \in \mathbb{R} | x > 0\}$.

Зададим отображение $\varphi: \mathbb{C}^* \to \mathbb{R}^+$ по правилу:

$$\varphi(z) = |z|, \forall z \in \mathbb{C}^*.$$

Показать, что φ – эндоморфизм группы $\mathbb{C}^*$, найти его ядро и образ.

Пр.3. Рассмотрим группу $\mathbb{Z}$. Зададим отображение $\varphi: \mathbb{Z} \to \mathbb{Z}$ по правилу: $\varphi(z) = -z, \forall z \in \mathbb{Z}$.

Показать, что φ – автоморфизм группы $\mathbb{Z}$, найти его ядро и образ.

§10. Теорема о гомоморфизме.

В §9 мы доказали, что если $\varphi -$ гомоморфизм группы G, то $Ker\varphi \lhd G$.

Пусть $H -$ произвольная нормальная подгруппа группы G. Тогда каждому элементу $g \in G$ можно поставить в соответствие смежный класс gH. Множество смежных классов будет образовывать группу по операции из G, т.о.

$\varphi: G \to G/H -$ гомоморфизм группы G в группу G/H с ядром

$$Ker\varphi = \{g \in G | \varphi(g) = H\} = \{g \in G | gH = 1H\} =$$

$$\{g \in G | g \in H\} = H.$$

Этот гомоморфизм называют естественных гомоморфизмом группы G на ее фактор-группу G/H. Отсюда, в частности, вытекает, что все нормальные подгруппы группы и только они будут служить ядрами всевозможных гомоморфизмов этой группы.

Пусть $G -$ группа. Можно ли описать образы группы G при различных гомоморфизмах?

Т.1 (основная о гомоморфизме). Пусть $\varphi: G \to Im\varphi$ – гомоморфизм группы G на $Im\varphi$. Тогда

$$G/Ker\varphi \cong Im\varphi,$$

т. е. все образы группы G при различных гомоморфизмах исчерпываются с точностью до изоморфизма фактор-группами самой группы.

МОДУЛЬ-2

ЭЛЕМЕНТЫ ТЕОРИИ КОЛЕЦ

§11. Кольцо. Подкольцо. Примеры и простейшие свойства элементов. Характеристика кольца и кольца характеристики ноль.

О.1. Непустое множество K с заданными на нем бинарными операциями $+$ и $\cdot$ называется *кольцом*, если выполнены следующие условия (аксиомы кольца):

(1) K – аддитивная абелева группа (аддитивная группа кольца K);

(2) операция $\cdot$ дистрибутивна на K относительно $+$, т. е.

$\forall a, b, c \in K\colon\ a(b + c) = ab + ac$ и $(a + b)c = ac + bc$.

Следствия из аксиом кольца:

Сл.1. $a0 = 0a = 0,\ \forall a \in K.$

Сл.2. $a(-b) = (-a)b = -ab, \forall a, b \in K.$

Сл.3. $a(b - c) = ab - ac$ и $(a - b)c = ac - bc, \forall a, b, c \in K.$

О.2. Кольцо K называется *коммутативным*, если операция $\cdot$ коммутативна на K, т. е. $ab = ba, \forall a, b \in K$.

О.3. Кольцо K называется *ассоциативным*, если операция $\cdot$ ассоциативна на K, т. е. $(ab)c = a(bc), \forall a, b, c \in K$.

О.4. Говорят, что кольцо K *имеет делители нуля*, если

$$\exists a \neq 0, b \neq 0 \in K : ab = 0.$$

Если таких элементов нет, то говорят, что K – кольцо без делителей нуля.

О.5. Кольцо K называется *кольцом с единицей*, если

$$\exists 1 \in K : a1 = 1a = a, \ \forall a \in K.$$

О.6. Пусть K – кольцо и $\emptyset \neq K_1 \subseteq K$. Если K_1 является кольцом относительно тех же операций, которые заданы на K, то его называют *подкольцом* кольца K.

Т.1 (критерий подкольца). Пусть K – кольцо и $\emptyset \neq K_1 \subseteq K$. Тогда K_1 является подкольцом в $K \Leftrightarrow$ когда выполнены следующие условия:

(1) $\forall a, b \in K_1 : a + (-b) \in K_1$;

(2) $\forall a, b \in K_1 : ab \in K_1$.

О.7. Пусть K – ассоциативно-коммутативное кольцо с единицей. Если $\exists n \in \mathbb{N}: \underbrace{1+1+\cdots+1}_{n \text{ раз}} = 1 \cdot n = 0$, причем n – наименьшее с таким свойством, то n называют *характеристикой* кольца K. Обозначается: $n = charK$.

Если такого числа n не существует, то говорят, что данное кольцо имеет характеристику 0.

Пр.1. Рассмотрим некоторые примеры колец.

(1) Числовые множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – коммутативные и ассоциативные кольца с единицей относительно обычных операций $+$ и $\cdot$ без делителей нуля.

Так как $\underbrace{1+1+\cdots+1}_{n \text{ раз}} = 1 \cdot n = n \in \mathbb{N} \Rightarrow n \neq 0$, то все числовые кольца имеют характеристику 0.

(2) Множество $2\mathbb{Z}$ – коммутативное и ассоциативное кольцо без единицы и без делителей нуля, $char 2\mathbb{Z} = 0$.

(3) Множество $\mathbb{Z}_n$ всех классов вычетов по модулю n – коммутативное и ассоциативное кольцо с единицей, $char\mathbb{Z}_n = n$.

Если n – простое число, то $\mathbb{Z}_n$ не имеет делителей нуля; если n – составное число, то $\mathbb{Z}_n$ имеет делителей нуля.

(4) Множество $M_n(P)$ квадратных матриц над полем P – некоммутативное ассоциативное кольцо с единицей.

§12. Отношение делимости в ассоциативно-коммутативных кольцах с единицей.

Пусть K – ассоциативно-коммутативное кольцо с единицей.

О.1. Будем говорить, что элемент $a \in K$ *делится* на $b \in K$, если $\exists q \in K\colon\ a = bq$. Обозначается: $a \vdots b$. Элемент b называется *делителем* элемента a.

З.1. В числовых кольцах понятие делимости обычно совпадает с обычной делимостью.

Пр.1. Рассмотрим делимость в нечисловых кольцах.

(1) Пусть $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$. Найти элементы кольца, которые делятся на $\bar{2}$.

(2) Пусть $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} -$ кольцо целых гауссовых чисел. Показать, что $(23 + 2i) : (2 + 3i)$, но $(23 + 2i)$ не делится на $(1 - i)$.

Свойства отношения делимости

Св-во 1. Отношение делимости рефлексивно, т. е.

$$\forall a \in K\colon\ a \vdots a.$$

Св-во 2. Отношение делимости транзитивно, т. е.

если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.

Св-во 3. Если $a \vdots c$, то $ab \vdots c$, $\forall b \in K$.

Св-во 4. Если $a \vdots c$ и $b \vdots c$, то $a \pm b \vdots c$.

Св-во 5. Если $a \vdots c$, а b не делится на c, то $a \pm b$ не делится на c.

Св-во 6. $0 \vdots a$, $\forall a \in K$.

Св-во 7. $a \vdots 1$, $\forall a \in K$.

§13. Обратимые элементы кольца. Группа обратимых элементов кольца.

О.1. Пусть K – ассоциативно-коммутативное кольцо с единицей. Элемент $a \in K$ называется *обратимым*, если $\exists a^{-1} \in K: aa^{-1} = a^{-1}a = 1$. Элемент $a^{-1} \in K$ называется обратным к элементу a.

Пр.1. Найдите обратимые элементы в кольце:

(1) $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;

(2) $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$;

(3) $\mathbb{Z}[i] = \{a + bi | ab \in \mathbb{Z}\}$ целых гауссовых чисел.

Т.1. Множество K^* обратимых элементов кольца K образует мультипликативную абелеву группу.

Пр.2. Группы обратимых элементов:

(1) $\mathbb{Z}^* = \{-1,1\} =< -1 >$.

(2) $\mathbb{Z}^*{}_n = \{\bar{a} | (a,n) = 1\}.$;

(3) $\mathbb{Z}^*[i] = \{1, -1, i, -i\}$.

Т.2. Если $a \vdots b$ и $\varepsilon \in K^*$, то $a \vdots b\varepsilon$.

3.1. Напомним, что ассоциативно-коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется полем.

§14. Область целостности. Отношение делимости в области целостности. Ассоциированные элементы кольца. Простые и составные элементы кольца.

О.1. Пусть $K -$ ассоциативно-коммутативное кольцо с единицей. Если K не имеет делителей нуля, то его называют областью целостности.

Все числовые кольца являются областями целостности. Нечисловое кольцо $\mathbb{Z}_n, n -$ составное число, имеет делители нуля. Значит не является областью целостности.

Свойства делимости в области целостности

Св-во 1. Если $a \in K\backslash\{0\}$, то из равенства $ab = ac$ следует $b = c$, т. е. возможно сокращение равенства на ненулевой элемент.

Сл.1. Если $a : b$ и $b \neq 0$, то результат такого деления в области целостности определен однозначно.

О.2. Элементы a и b из области целостности K будем называть *ассоциированными*, если $\exists \varepsilon \in K^*: \ a = b\varepsilon$.

Пр. 1.

(1) 5 и -5 ассоциированы в кольце $\mathbb{Z}$.

(2) $5 + 2i$ и $-2 + 5i$ ассоциированы в кольце $\mathbb{Z}[i]$.

Св-во 2. Ассоциированность элементов в области целостности является отношением эквивалентности.

Отношение ассоциированности будет обозначать $\sim$.

Св-во 3. Пусть $a, b \in K\backslash\{0\}$, $K -$ область целостности. Тогда $a \vdots b$ и $b \vdots a \Leftrightarrow a \sim b$.

О.3. Элемент $a \in K -$ область целостности называется *простым*, если:

(1) $a \notin K^*$, т.е. a не обратим в K.

(2) если $a \vdots b$, то либо $b \in K^*$, либо $b \sim a$.

Элементы, которые не являются простыми, называются составными.

Пр.2. 5 – простой элемент кольца $\mathbb{Z}$, но

5 – составной элемент в кольце $\mathbb{Z}[i]$:

$$5 = \underbrace{(1+2i)}_{\notin \mathbb{Z}[i]^*}\underbrace{(1-2i)}_{\notin \mathbb{Z}[i]^*}.$$

§15. Идеалы кольца. Идеал, порожденный множеством элементов кольца.

О.1. Непустое подмножество элементов I кольца K называется *идеалом* этого кольца, если:

(1) $\forall a, b \in I\colon\ a - b \in I$;

(2) $\forall a \in I$ и $k \in K\colon\ ak \in I$.

Множества $\{0\}$ и K являются идеалами кольца K. Эти идеалы называют тривиальными.

Из О.1. вытекает, что любой идеал кольца K является подкольцом в K (в этом несложно убедиться, используя критерий подкольца). Обратное утверждение неверно.

Т.1. Пусть $K-$ ассоциативно-коммутативное кольцо с единицей, $a_1, a_2, \dots, a_n \in K$. Тогда множество

$$I = \{k_1 a_1 + k_2 a_2 + \cdots + k_n a_n | k_i \in K, i = 1, 2, .., n\}$$

является идеалом кольца K.

О.2. Идеал

$$I = \{k_1 a_1 + k_2 a_2 + \cdots + k_n a_n | k_i \in K, i = 1, 2, .., n\}$$

называется *идеалом, порожденным элементами* $a_1, a_2, \dots, a_n$ и обозначается $I = (a_1, a_2, \dots, a_n)$.

Т.2. Если I_1 и I_2 – идеалы в K, то $I_1 \cap I_2$ – идеал в K.

Сл.1. Пересечение любого множества идеалов кольца K является идеалом этого кольца.

Т.3. Пусть $K -$ кольцо, $I -$ его идеал. Если $1 \in I$, то $K = I$.

Т.4. Пусть $K -$ кольцо, $I -$ его идеал и $\varepsilon \in K^*$. Если $\varepsilon \in I$, то $K = I$.

Т.5. Если ассоциативно-коммутативное кольцо с единицей содержит только тривиальные идеалы, то оно является полем.

§16. Главные идеалы кольца.

Пусть $K-$ ассоциативно-коммутативное кольцо с единицей.

О.1. Идеал кольца K, порожденный одним элементом a этого кольца, будем называть главным идеалом и обозначать

$$(a) = \{ka | k \in K\}.$$

Рассмотрим основные свойства главных идеалов кольца.

Св-во 1. Главный идеал, порожденный нулевым элементом, содержит только нулевой элемент. Главный идеал, порожденный единицей кольца, совпадает со всем кольцом.

Св-во 2. Главный идеал, порожденный обратимым элементом, совпадает со всем кольцом.

Св-во 3. Если $b \in (a)$ и $c \in (a)$, то $b - c \in (a)$ и $kb \in (a)$.

Св-во 4. $a \vdots b \Leftrightarrow (a) \subseteq (b)$.

Св-во 5. Если $a \sim b$, то $(a) = (b)$.

Св-во 6. Если K −область целостности и $(a) = (b)$, то $a \sim b$.

§17. Операции над идеалами.

Пусть $K-$ ассоциативно-коммутативное кольцо с единицей.

О.1. Пусть I_1 и I_2- идеалы кольца K. Суммой этих идеалов будем называть множество вида

$$I_1 + I_2 = \{a_1 + a_2 | a_1 \in I_1, a_2 \in I_2\}.$$

Т.1. $I_1 + I_2 -$ идеал кольца K.

З.1. Используя метод математической индукции, несложно доказать, что сумма любого конечного числа идеалов кольца также будет идеалом этого кольца.

О.2. Пусть I_1 и I_2 – идеалы кольца K. Произведением этих идеалов будем называть множество вида

$$I_1 I_2 = \{a_1 a_2 | a_1 \in I_1, a_2 \in I_2\}.$$

Т.2. Объединение возрастающей цепочки идеалов

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

в ассоциативно-коммутативном кольце K является идеалом этого кольца.

З.2. На самом деле, условие ассоциативности в Т.2 можно было бы отбросить.

§18. НОД и НОК идеалов.

В св-ве 4 §16 мы показали, что делимость элементов кольца равносильна вложимости идеалов, т.е.

$$a \vdots b \Leftrightarrow (a) \subseteq (b).$$

Обобщим понятие делимости на идеалы.

О.1. Пусть I_1 и I_2 – идеалы кольца K. Будем говорить, что

$$I_1 \vdots I_2 \Leftrightarrow I_1 \subseteq I_2.$$

Рассмотрим свойства делимости для идеалов.

Св-во 1. Делимость идеалов рефлексивна, т.е.

$$I \vdots I, \forall I - \text{идеал в } K.$$

Св-во 2. Делимость идеалов транзитивна, т.е.

$$\text{если } I_1 \vdots I_2 \text{ и } I_2 \vdots I_3, \text{ то } I_1 \vdots I_3.$$

О.2. Будем говорить, что идеал I является НОДом идеалов I_1 и I_2, если выполняются следующие условия:

1) $I -$ общий делитель I_1 и I_2, т.е. $I_1 \vdots I$ и $I_2 \vdots I$.

2) I делится на любой другой общий делитель I_1 и I_2.

Обозначается: $I = \text{НОД}(I_1, I_2)$.

Т.1. Любые два идеала ассоциативно-коммутативного кольца K с единицей имеют НОД и

$$\text{НОД}(I_1, I_2) = I_1 + I_2.$$

О.3. НОКом идеалов I_1 и I_2 кольца K будем называть идеал I^* кольца K, который удовлетворяет условиям:

1) $I^* -$ общее кратное I_1 и I_2, т.е. $I^* \vdots I_1$ и $I^* \vdots I_2$.

2) если любой другой идеал $D^* \vdots I_1$ и $D^* \vdots I_2$, то $D^* \vdots I^*$.

Обозначается: $I^* = \text{НОК}(I_1, I_2)$.

Т.2. Любые два идеала ассоциативно-коммутативного кольца K с единицей имеют НОК и

$$\text{НОК}(I_1, I_2) = I_1 \cap I_2.$$

Пр.1. Найти НОД и НОК главных идеалов в кольце $\mathbb{Z}$:

(24) и (40).

3.1. НОД и НОК главных идеалов кольца $\mathbb{Z}$ являются главными идеалами в этом кольце. Однако, НОД и НОК не обязаны быть главными идеалами во всех кольцах.

§19. Кольца главных идеалов (КГИ).

О.1. Область целостности будем называть КГИ, если любой идеал этого кольца является главным.

Т.1. Кольцо $\mathbb{Z}$ является КГИ.

Рассмотрим несколько важных свойств КГИ.

Св-во 1. В КГИ любые два ненулевых элемента обязательно имеют НОД. Кроме того, все НОД этих элементов будут ассоциированы между собой.

Св-во 2. Пусть K – КГИ, $a, b \in K$. Если $d = \text{НОД}(a, b)$, то $\exists r, s \in K\colon\ d = a \cdot r + b \cdot s$.

3.1. В утверждении свойства 1 мы предполагали, что НОД рассматривается для двух ненулевых элементов. Однако, это понятие можно обобщить на случай, когда только один элемент ненулевой. Так как $0 \vdots a, \forall a \in K \backslash \{0\}$, то $\text{НОД}(a, 0) = a$.

§20. Разложение элементов на простые множители в КГИ. Факториальные кольца.

О.1. Элемент области целостности будем называть простым, если он не имеет обратного элемента и делится либо только на 1, либо на обратимый элемент этого кольца.

Элемент c области целостности будем называть составным, если он допускает разложение на множители, т.е. $c = ab$, причем a и b не являются обратимыми элементами.

3.1. Простота одного и того же элемента зависит от того, в каком кольце он рассматривается. Например,

в кольце $\mathbb{Z}$ элемент 13 – простой,

в кольце $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$ элемент 13 – составной.

О.2. Два элемента области целостности будем называть взаимно простыми, если НОД этих двух элементов существует и является обратимым элементом этого кольца.

Далее будем рассматривать КГИ, в которых НОД обязательно существует.

Рассмотрим основные свойства взаимно простых элементов в КГИ.

Св-во 1. Если $ab \vdots c$, причем a и c взаимно просты, то $b \vdots c$.

Св-во 2. Если $ab \vdots p$, где $p -$ простой элемент, то либо $a \vdots p$, либо $b \vdots p$.

3.1. Св-во 2 с помощью метода мат. индукции можно перенести на любое конечное число сомножителей, т.е. если $a_1 a_2 \dots a_n \vdots p$, $p -$ простой элемент, то $\exists i \in \{1,2, \dots, n\}$: $a_i \vdots p$.

Св-во 3 (об обрыве строго возрастающей цепочки идеалов). В КГИ любая строго возрастающая цепочка идеалов

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$$

не может быть бесконечной, т. е. она всегда обрывается на конечном номере.

О.3. Область целостности будем называть *факториальным кольцом*, если любой ненулевой элемент этого кольца обладает однозначным разложением на простые множители с точностью до порядка записи этих множителей и ассоциированности.

Т.1. Любое КГИ является факториальным кольцом.

З.1. Из т.1. вытекает, что однозначность разложения на простые множители является отличительным признаком КГИ. Т.е. если в кольце присутствует неоднозначное разложение на множители, то оно не может быть КГИ.

§21. Евклидовы кольца.

О.1. Пусть K – область целостности, которая не является полем. Будем называть эту область целостности евклидовым кольцом, если существует такая функция α, действующая на ненулевых элементах этого кольца, которая ставит каждому такому элементу в соответствие неотрицательное число (его называют нормой), причем эта функция удовлетворяет следующим условиям:

(1) $\alpha(ab) \geq \alpha(a)$, причем $\alpha(ab) = \alpha(a) \Leftrightarrow b \in K^*$.

(2) $\forall a, b \in K, b \neq 0, \exists q, r \in K\colon\ a = bq + r$ и либо $r = 0$, либо $\alpha(r) < \alpha(b)$.

Пр.1. Кольцо $\mathbb{Z}$ является евклидовым.

Пр.2. Кольцо целых гауссовых чисел $\mathbb{Z}[i]$ является евклидовым.

Т.1. Любое евклидово кольцо является КГИ.

Сл.1. В евклидовом кольце для любых элементов a и b, из которых по крайней мере один является ненулевым, существует НОД.

З.1. В евклидовом кольце будет также выполняться процесс нахождения НОД с помощью алгоритма Евклида.

3.2. Имеют место строгие включения:

$$\{\text{евклидовы кольца}\} \subset \{\text{КГИ}\} \subset \{\text{факториальные кольца}\}.$$

Строгие включения означают, что существуют примеры КГИ, которые не являются евклидовыми кольцами, а также примеры факториальных колец, которые не будут КГИ.