

Алгебра. Экзамен

Бобень Вячеслав
[@darkkeks](#), [GitHub](#)

2020

“Какой-то ты слишком идеальный, редуцируем его!”.

— Bottom text

Содержание

1	Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Подгруппы. Описание всех подгрупп в группе $(\mathbb{Z}, +)$	3
2	Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы	5
3	Смежные классы. Индекс подгруппы. Теорема Лагранжа	6
4	Пять следствий из теоремы Лагранжа	7
5	Нормальные подгруппы и факторгруппы	8
6	Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства	9
7	Теорема о гомоморфизме для групп	10
8	Классификация циклических групп	11
9	Прямое произведение групп. Разложение конечной циклической группы. Теорема о строении конечных абелевых групп	12
10	Экспонента конечной абелевой группы и критерий цикличности	13
11	Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи Хеллмана обмена ключами. Криптосистема Эль-Гамала	14
12	Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем	15
13	Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец	16
14	Кольцо многочленов от одной переменной над полем: деление с остатком, наибольший общий делитель двух многочленов, теорема о его существовании и линейном выражении	17
15	Теорема о том, что кольцо многочленов от одной переменной над полем является кольцом главных идеалов	18
16	Неприводимые многочлены. Факториальность кольца многочленов от одной переменной над полем	19

17 Критерий того, что факторкольцо $\mathbb{K}[x]/(h)$ является полем. Базис и размерность факторкольца $\mathbb{K}[x]/(h)$ как векторного пространства над полем \mathbb{K}	20
18 Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов	21
19 Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов	22
20 Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций	23
21 S -многочлены. Критерий Бухбергера	24
22 Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал	25
23 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала	26
24 Теорема Гильберта о базисе идеала	27
25 Редуцируемость к нулю S -многочлена двух многочленов с взаимно простыми старшими членами	28
26 Характеристика поля. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений	29
27 Присоединение корня неприводимого многочлена. Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители	30
28 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства	31
29 Подполе в расширении полей, порождённое алгебраическим элементом	32
30 Порядок конечного поля. Автоморфизм Фробениуса	33
31 Теорема существования для конечных полей	34
32 Цикличность мультипликативной группы конечного поля и неприводимые многочлены над \mathbb{Z}_p	35

1 Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Подгруппы. Описание всех подгрупп в группе $(\mathbb{Z}, +)$

Определение 1. Множество с бинарной операцией — это множество M с заданным отображением

$$M \times M \rightarrow M, \quad (a, b) \mapsto a \circ b.$$

Множество с бинарной операцией обычно обозначают (M, \circ) .

Определение 2. Множество с бинарной операцией (M, \circ) называется *полугруппой*, если данная бинарная операция ассоциативна, то есть

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{для всех } a, b, c \in M.$$

Не все естественно возникающие операции ассоциативны. Например, если $M = \mathbb{N}$ и $a \circ b = a^b$, то

$$2^{(1^2)} = 2 \neq (2^1)^2 = 4.$$

Другой пример неассоциативной бинарной операции: $M = \mathbb{Z}$ и $a \circ b := a - b$.

Полугруппу обычно обозначают (S, \circ) .

Определение 3. Полугруппа (S, \circ) называется *моноидом*, если в ней есть *нейтральный элемент*, то есть такое элемент $e \in S$, что $e \circ a = a \circ e = a$ для любого $a \in S$.

Замечание. Если в полугруппе есть нейтральный элемент, то он один. В самом деле, $e_1 \circ e_2 = e_1 = e_2$.

Определение 4. Моноид (S, \circ) называется *группой*, если для каждого элемента $a \in S$ найдется *обратный элемент*, то есть такой $b \in S$, что $a \circ b = b \circ a = e$.

Обратный элемент обозначается a^{-1} .

Группу принято обозначать (G, \circ) или просто G , когда понятно, о какой операции идёт речь. Обычно символ \circ обозначения операции опускают и пишут просто ab .

Определение 5. Группа G называется *коммутативной* или *абелевой*, если групповая операция *коммутативна*, то есть $ab = ba$ для любых $a, b \in G$.

Если в случае произвольной группы G принято использовать мультипликативные обозначения для групповой операции — gh, e, g^{-1} , то в теории абелевых групп чаще используют аддитивные обозначения, то есть $a + b, 0, -a$.

Определение 6. *Порядок* группы G — это число элементов в G . Группа называется *конечной*, если её порядок конечен, и *бесконечной* иначе.

Порядок группы G обозначается $|G|$.

Приведем несколько серий примеров групп.

1. Числовые аддитивные группы:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +).$$

2. Числовые мультипликативные группы:

$$(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times), (\mathbb{C} \setminus \{0\}, \times), (\mathbb{Z}_p \setminus \{0\}, \times), p - \text{простое.}$$

3. Группы матриц:

$$\text{GL}_n(\mathbb{R}) = \{A \in \text{Mat}_{n \times n}(\mathbb{R}) \mid \det A \neq 0\};$$

$$\text{SL}_n(\mathbb{R}) = \{A \in \text{Mat}_{n \times n}(\mathbb{R}) \mid \det A = 1\}.$$

4. Группы перестановок:

симметрическая группа S_n — все перестановки длины n , $|S_n| = n!$;

знакопеременная группа A_n — чётные подстановки длины n , $|A_n| = \frac{n!}{2}$.

5. Группы преобразований: симметрия, движение.

Определение 7. Подмножество H группы G называется *подгруппой*, если выполнены следующие три условия:

1. $e \in H$;
2. $ab \in H$ для любых $a, b \in H$;
3. $a^{-1} \in H$ для любого $a \in H$.

В каждой группе G есть *несобственные* подгруппы $H = \{e\}$ и $H = G$. Все прочие подгруппы называются *собственными*. Например, чётные числа $2\mathbb{Z}$ образуют собственную подгруппу в $(\mathbb{Z}, +)$.

Предложение. Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторого целого неотрицательного k .

Доказательство. Очевидно, что все подмножества вида $k\mathbb{Z}$ являются подгруппами в \mathbb{Z} .

1. Пусть $H \subseteq \mathbb{Z}$ — подгруппа. Если $H = \{0\}$, то $H = 0\mathbb{Z}$.

Иначе положим $k = \min(H \cap \mathbb{N}) \neq 0$.

Тогда $k\mathbb{Z} \subseteq H$.

2. Покажем, что $k\mathbb{Z} = H$. Пусть $a \in H$. Поделим на k с остатком.

$a = qk + r$, где $q \in \mathbb{Z}$, $0 \leq r < k \implies r = a - qk \in H$.

В силу выбора k получаем $r = 0 \implies a = qk$. ■

2 Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы

Пусть G — группа, $g \in G$ и $n \in \mathbb{Z}$. Определим степень следующим образом:

$$g^n = \begin{cases} \underbrace{g \cdots g}_n, & n > 0, \\ e, & n = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_n, & n < 0. \end{cases}$$

Свойства:

1. $g^m \cdot g^n = g^{m+n}, \forall n, m \in \mathbb{Z}$;
2. $(g^k)^{-1} = g^{-k}, \forall k \in \mathbb{Z}$;
3. $(g^n)^m = g^{nm}, \forall n, m \in \mathbb{Z}$.

Определение 8. Пусть G — группа и $g \in G$. Циклической подгруппой, порожденной элементом g , называется подмножество $\{g^n \mid n \in \mathbb{Z}\}$ в G .

Циклическая подгруппа, порождённая элементом g , обозначается $\langle g \rangle$. Элемент g называется *порождающим* или *образующим* для подгруппы $\langle g \rangle$.

Например, подгруппа $2\mathbb{Z}$ в $(\mathbb{Z}, +)$ является циклической, и в качестве порождающего элемента в ней можно взять $g = 2$ или $g = -2$. Другими словами, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 9. Группа G называется *циклической*, если найдется такой элемент $g \in G$, что $G = \langle g \rangle$.

Определение 10. Пусть G — группа и $g \in G$. *Порядком* элемента g называется такое наименьшее натуральное число m , что $g^m = e$. Если такого натурального числа m не существует, говорят, что порядок элемента g равен бесконечности.

Порядок элемента обозначается $\text{ord}(g)$. Заметим, что $\text{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

Следующее предложение объясняет, почему для порядка группа и порядка элемента используется одно и то же слово.

Предложение. Пусть G — группа и $g \in G$. Тогда $\text{ord}(g) = |\langle g \rangle|$.

Доказательство. Заметим, что если $g^k = g^s$, то $g^{k-s} = e$. Поэтому если элемент g имеет бесконечный порядок, то все элементы $g^n, n \in \mathbb{Z}$, попарно различны, и подгруппа $\langle g \rangle$ содержит бесконечно много элементов. Если же порядок элемента g равен m , то из минимальности числа m следует, что элементы $e = g^0, g = g^1, g^2, \dots, g^{m-1}$ попарно различны. Далее, для всякого $n \in \mathbb{Z}$ мы имеем $n = mq + r$, где $0 \leq r \leq m-1$, и

$$g^n = g^{mq+r} = (g^m)^q g^r = e^q g^r = g^r.$$

Следовательно, $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$ и $|\langle g \rangle| = m$. ■

Ясно, что всякая циклическая группа коммутативна и не более чем счётна. Примерами циклических групп являются группы $(\mathbb{Z}, +)$ и $(\mathbb{Z}_n, +), n \geq 1$.

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа

Определение 11. Пусть G — группа, $H \subseteq G$ — подгруппа и $g \in G$. *Левым смежным классом* элемента g группы G по подгруппе H называется подмножество

$$gH = \{gh \mid h \in H\}.$$

Наряду с левым смежным классом можно определить *правый смежный класс* элемента g :

$$Hg = \{hg \mid h \in H\}.$$

Все дальнейшие доказательства для правых смежных классов формулируются и доказываются аналогично.

Лемма 3.1. Пусть G — группа, $H \subseteq G$ — её подгруппа и $g_1, g_2 \in G$.

Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \emptyset$.

Доказательство. Предположим, что $g_1H \cap g_2H \neq \emptyset$, то есть $g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$. Нужно доказать, что $g_1H = g_2H$. Заметим, что $g_1H = g_2h_2h_1^{-1}H \subseteq g_2H$. Обратное включение доказывается аналогично. ■

Лемма 3.2. Пусть G — конечная группа и $H \subseteq G$ — конечная подгруппа.

Тогда $|gH| = |H|$ для любого $g \in G$.

Доказательство. Поскольку $gH = \{gh \mid h \in H\}$, в gH элементов не больше, чем в H . Если $gh_1 = gh_2$, то домножаем слева на g^{-1} и получаем $h_1 = h_2$. Значит, все элементы вида gh , где $h \in H$, попарно различны, откуда $|gH| = |H|$. ■

Определение 12. Пусть G — группа и $H \subseteq G$ — подгруппа. *Индексом* подгруппы H в группе G называется число левых смежных классов G по H .

Индекс группы G по подгруппе H обозначается $[G : H]$.

Теорема 3.3 (Теорема Лагранжа). Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

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

Доказательство. Каждый элемент группы G лежит в (своём) левом смежном классе по подгруппе H , разные смежные классы не пересекаются (лемма 1) и каждый из них содержит по $|H|$ элементов (лемма 2). ■

4 Пять следствий из теоремы Лагранжа

Теорема 4.1 (Теорема Лагранжа). Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

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

Рассмотрим некоторые следствия из теоремы Лагранжа.

Следствие. Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда $|H|$ делит $|G|$.

Следствие. Пусть G — конечная группа и $g \in G$. Тогда $\text{ord}(g)$ делит $|G|$.

Доказательство. Пусть $k = \text{ord}(g)$. Тогда из следствия 2: $|G| = k \cdot s \implies g^{|G|} = g^{ks} = (g^k)^s = e^s = e$. ■

Следствие (малая теорема Ферма). p — простое число, $\text{НОД}(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Применим следствие 3 к группе $(\mathbb{Z}_p \setminus \{0\}, \times)$. ■

Следствие. Пусть G — группа. Предположим, что $|G|$ — простое число. Тогда G — циклическая группа, порождаемая любым своим неединичным элементом.

Доказательство. Пусть $g \in G$ — произвольный неединичный элемент. Тогда циклическая подгруппа $\langle g \rangle$ содержит более одного элемента и $|\langle g \rangle|$ делит $|G|$ по следствию 1. Значит, $|\langle g \rangle| = |G|$, откуда $G = \langle g \rangle$. ■

5 Нормальные подгруппы и факторгруппы

Определение 13. Подгруппа H группы G называется *нормальной*, если $gH = Hg$ для любого $g \in G$.

Пример.

1. G — абелева. Тогда любая подгруппа H нормальная.
2. $G = S_3, H = \{\text{Id}, (12)\}$. Тогда H не является нормальной.
3. Несобственные подгруппы $H = G$ и $H = \{0\}$ нормальны.

Предложение. Для подгруппы $H \subseteq G$ следующие условия эквивалентны:

1. H нормальна;
2. $gHg^{-1} = H$ для любого $g \in G$;
3. $gHg^{-1} \subseteq H$ для любого $g \in G$.

Доказательство.

$$(1) \implies (2) \quad gH = Hg \implies gHg^{-1} = H.$$

$$(2) \implies (3) \quad \text{Очев.}$$

$$(3) \implies (1) \quad gHg^{-1} \subseteq H \implies gH \subseteq Hg. \text{ Теперь возьмем } g = g^{-1}. \text{ Тогда } g^{-1}Hg \subseteq H \implies Hg \subseteq gH \implies gh = Hg. \quad \blacksquare$$

Рассмотрим множество смежных классов по нормальной подгруппе G/H .

Определим на G/H бинарную операцию, полагая $(g_1H)(g_2H) = (g_1g_2)H$.

Корректность Пусть $g'_1H = g_1H$ и $g'_2H = g_2H$. Тогда $g'_1 = g_1h_1, g'_2 = g_2h_2$, где $h_1, h_2 \in H$.

$$(g'_1H)(g'_2H) = (g'_1g'_2)H = (g_1h_1g_2h_2)H = (g_1g_2(\underbrace{h_1g_2h_2}_{\in H}))H \subseteq (g_1g_2)H \implies (g'_1g'_2)H = (g_1g_2)H.$$

Структура группы G/H .

1. Ассоциативность очевидна.
2. Нейтральный элемент — eH .
3. Обратный к gH — $g^{-1}H$.

Определение 14. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H .

Пример. Если $G = (\mathbb{Z}, +)$ и $H = n\mathbb{Z}$, то G/H — это в точности группа вычетов $(\mathbb{Z}_n, +)$.

6 Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства

Определение 15. Пусть (G, \circ) и (F, \cdot) — две группы.

Отображение $\varphi: G \rightarrow F$ называется *гомоморфизмом*, если

$$\varphi(g_1 \circ g_2) = \varphi(g_1) \cdot \varphi(g_2), \quad \forall g_1, g_2 \in G.$$

Замечание. Пусть $\varphi: G \rightarrow F$ — гомоморфизм групп, и пусть e_G и e_F — нейтральные элементы группы G и F соответственно. Тогда:

1. $\varphi(e_G) = e_F$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ для любого $a \in G$.

Доказательство.

1. Имеем $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) \varphi(e_G)$.

Теперь умножая крайние части этого равенства на $\varphi(e_G)^{-1}$, получим $e_F = \varphi(e_G)$.

2. $\varphi(g \cdot g^{-1}) = e_F = \varphi(g) \varphi(g^{-1})$. Умножив обе части на $\varphi(g)^{-1}$ получаем необходимое. ■

Определение 16. Гомоморфизм групп $\varphi: G \rightarrow F$ называется *изоморфизмом*, если отображение φ биективно.

Определение 17. Группы G и F называют *изоморфными*, если между ними существует изоморфизм.

Обозначение: $G \simeq F$.

В алгебре рассматривают с точностью до изоморфизма: изоморфные группы считаются «одинаковыми».

Определение 18. С каждым гомоморфизмом групп $\varphi: G \rightarrow F$ связаны его *ядро*

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_F\},$$

и *образ*

$$\operatorname{Im} \varphi = \varphi(G) = \{a \in F \mid \exists g \in G : \varphi(g) = a\}.$$

Ясно, что $\ker \varphi \subseteq G$ и $\operatorname{Im} \varphi \subseteq F$ — подгруппы.

Лемма 6.1. Гомоморфизм групп $\varphi: G \rightarrow F$ инъективен тогда и только тогда, когда $\ker \varphi = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен то $\ker \varphi = \{e_G\}$.

Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \ker \varphi$, поскольку $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_F$. Отсюда $g_1^{-1}g_2 = e_G$ и $g_1 = g_2$. ■

Следствие. Гомоморфизм групп $\varphi: G \rightarrow F$ является изоморфизмом тогда и только тогда, когда $\ker \varphi = \{e_G\}$ и $\operatorname{Im} \varphi = F$.

Предложение. Пусть $\varphi: G \rightarrow F$ — гомоморфизм групп. Тогда подгруппа $\ker \varphi$ нормальна в G .

Доказательство. Достаточно проверить, что $g^{-1}hg \in \ker \varphi$ для любых $g \in G$ и $h \in \ker \varphi$. Это следует из цепочки равенств

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e_F\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_F. \quad \blacksquare$$

7 Теорема о гомоморфизме для групп

Теорема 7.1 (Теорема о гомоморфизме). Пусть $\varphi: G \rightarrow F$ — гомоморфизм групп. Тогда группа $\text{Im } \varphi$ изоморфна факторгруппе $G/\ker \varphi$.

Доказательство. Рассмотрим отображение $\psi: G/\ker \varphi \rightarrow \text{Im } \varphi$, заданное формулой $\psi(g \ker \varphi) = \varphi(g)$.

1. Корректность.

$$g_1 \ker \varphi = g_2 \ker \varphi \implies g_1 h_1 = g_2 h_2 \text{ для некоторых } h_1, h_2 \in \ker \varphi.$$

$$\psi(g_1 \ker \varphi) = \varphi(g_1) = \varphi(g_1 h_1) = \varphi(g_2 h_2) = \varphi(g_2) = \psi(g_2 \ker \varphi).$$

2. ψ — гомоморфизм.

$$\psi((g_1 \ker \varphi)(g_2 \ker \varphi)) = \psi((g_1 g_2) \ker \varphi) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = \psi(g_1 \ker \varphi) \psi(g_2 \ker \varphi).$$

3. Сюръективность из построения.

4. Инъективность.

$$\psi(g_1 \ker \varphi) = \psi(g_2 \ker \varphi) \implies \varphi(g_1) = \varphi(g_2) \implies \varphi(g_1) \varphi(g_2)^{-1} = e_F \implies \varphi(g_1 g_2^{-1}) = e_F \implies g_1 g_2^{-1} \in \ker \varphi \implies g_1 \ker \varphi = g_2 \ker \varphi. \quad \blacksquare$$

Тем самым, чтобы удобно реализовать факторгруппу G/H , можно найти такой гомоморфизм $\varphi: G \rightarrow F$ в некоторую группу F , что $H = \ker \varphi$, и тогда $G/H \simeq \text{Im } \varphi$.

Пример. Пусть $G = (\mathbb{R}, +)$ и $H = (\mathbb{Z}, +)$. Рассмотрим группу $F = (\mathbb{C} \setminus \{0\}, \times)$ и гомоморфизм

$$\varphi: G \rightarrow F, \quad a \mapsto e^{2\pi i a} = \cos(2\pi a) + i \sin(2\pi a).$$

Тогда $\ker \varphi = H$ и факторгруппа G/H изоморфна окружности S^1 , рассматриваемой как подгруппа в F , состоящая из комплексных чисел с модулем 1.

8 Классификация циклических групп

Пусть G — циклическая группа. Тогда

1. Если $|G| = \infty$, то $G \simeq (\mathbb{Z}, +)$,
2. Если $|G| = n < \infty$, то $G \simeq (\mathbb{Z}_n, +)$.

Доказательство. По определению, если G — циклическая, то $G = \langle g \rangle$ для некоторого $g \in G$.

1. $\varphi: \mathbb{Z} \rightarrow G, k \mapsto g^k$

Это гомоморфизм и биекция \implies изоморфизм.

2. $\varphi: \mathbb{Z}_n \rightarrow G, k \mapsto g^k$.

Рассмотрим, куда переходит $k + ns$, где $0 \leq k \leq n - 1$.

$$k + ns \mapsto g^{k+ns} = g^k g^{ns} = g^k (g^n)^s = g^k.$$

■

9 Прямое произведение групп. Разложение конечной циклической группы. Теорема о строении конечных абелевых групп

Определение 19. *Прямым произведением* групп G_1, \dots, G_m называется множество

$$G_1 \times \dots \times G_m = \{(g_1, \dots, g_m) \mid g_1 \in G_1, \dots, g_m \in G_m\}$$

с операциями $(g_1, \dots, g_m)(g'_1, \dots, g'_m) = (g_1g'_1, \dots, g_mg'_m)$.

Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, \dots, e_{G_m})$ и для каждого элемента (g_1, \dots, g_m) есть обратный элемент $(g_1^{-1}, \dots, g_m^{-1})$.

Замечание. Группа $G_1 \times \dots \times G_m$ коммутативна в точности тогда, когда коммутативна каждая из групп G_1, \dots, G_m .

Замечание. Если все группы G_1, \dots, G_m конечны, то $|G_1 \times \dots \times G_m| = |G_1| \dots |G_m|$.

Определение 20. Группа G *раскладывается в прямое произведение* своих подгрупп H_1, \dots, H_m если отображение $H_1 \times \dots \times H_m \rightarrow G$, $(h_1, \dots, h_m) \mapsto h_1 \dots h_m$, является изоморфизмом.

Теорема 9.1. Пусть $n = ml$ — разложение натурального числа n на два взаимно простых сомножителя. Тогда имеет место изоморфизм групп

$$\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l.$$

Доказательство. Рассмотрим отображение

$$\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}_m \times \mathbb{Z}_l, \quad (k \bmod n) \mapsto (k \bmod m, k \bmod l).$$

Поскольку m и l делят n , отображение φ определено корректно. Ясно, что φ — гомоморфизм. Далее, $a \bmod n \in \ker \varphi \implies a \bmod m = 0, a \bmod l = 0 \implies a : m, a : l$.

Так как $\text{НОД}(m, l) = 1$, то $a : n \implies a \bmod n = 0 \implies \ker \varphi = \{0\}$.

Отсюда следует, что гомоморфизм φ инъективен. Поскольку множества \mathbb{Z}_n и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. ■

Следствие. Пусть $n \geq 2$ — натуральное число и $n = p_1^{k_1} \dots p_s^{k_s}$ — его разложение в произведение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}.$$

Определение 21. Конечная абелева группа A называется *примарной*, если $|A| = p^k$, где p — простое и $k \in \mathbb{N}$.

Теорема 9.2. Пусть A — конечная абелева группа. Тогда $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_t^{k_t}}$, где p_1, \dots, p_t — простые числа (не обязательно различные!) и $k_1, \dots, k_t \in \mathbb{N}$. Более того, набор примарных циклических множителей $\mathbb{Z}_{p_1^{k_1}}, \dots, \mathbb{Z}_{p_t^{k_t}}$ определен однозначно с точностью до перестановки (в частности, число этих множителей определено однозначно).

10 Экспонента конечной абелевой группы и критерий цикличности

Определение 22. Экспонентой конечной абелевой группы A называется число

$$\exp A := \min\{m \in \mathbb{N} \mid ma = 0 \ \forall a \in A\}.$$

Замечание.

1. Так как $ma = 0 \iff m : \text{ord}(a) \ \forall a \in A$ и $m \in \mathbb{Z}$, то определение экспоненты можно переписать ещё в виде $\exp A = \text{НОД}\{\text{ord}(a) \mid a \in A\}$.
2. Так как $|A| : \text{ord}(a) \ \forall a \in A$, то $|A|$ — общее кратное множества $\{\text{ord}(a) \mid a \in A\}$, а значит, $|A| : \exp A$.
В частности, $\exp A \leq |A|$.

Предложение. $\exp A = |A| \iff A$ — циклическая группа.

Доказательство. Пусть $|A| = n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ — разложение на простые множители, где p_i — простое и $k_s \in \mathbb{N}$. ($p_i \neq p_j$ при $i \neq j$)

\Leftarrow Если $A = \langle a \rangle$, то $\text{ord } a = n$, откуда сразу получаем $\exp A = n$.

\Rightarrow Если $\exp A = n$, то для $i = 1, \dots, s$ существует элемент $c_i \in A$, такой что $\text{ord } c_i = p_i^{k_i} m_i$, где $m_i \in \mathbb{N}$. Для каждого $i = 1, \dots, s$ положим $a_i = m_i c_i$, тогда $\text{ord}(a_i) = p_i^{k_i}$. Теперь рассмотрим элемент $a = a_1 + \dots + a_s$ и покажем, что $\text{ord}(a) = n$. Пусть $ma = 0$ для некоторого $m \in \mathbb{N}$, то есть $ma_1 + \dots + ma_s = 0$. При фиксированном $i \in \{1, \dots, s\}$ умножим обе части последнего равенства на $n_i := n/p_i^{k_i}$. Легко видеть, что $mn_i a_j = 0$ при всех $i \neq j$, поэтому в левой части выживет только слагаемое $mn_i a_i$, откуда получаем $mn_i a_i = 0$. Следовательно, $mn_i : p_i^{k_i}$, а так как n_i не делится на p_i , то $m : p_i^{k_i}$. В силу произвольности выбора i отсюда вытекает, что $m : n$. Так как $na = 0$, то мы окончательно получаем $\text{ord}(a) = n$. Значит, $A = \langle a \rangle$ — циклическая группа. ■

- 11 Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи Хеллмана обмена ключами. Криптосистема Эль-Гамала

12 Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем

- 13 Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец

- 14 Кольцо многочленов от одной переменной над полем: деление с остатком, наибольший общий делитель двух многочленов, теорема о его существовании и линейном выражении

- 15 Теорема о том, что кольцо многочленов от одной переменной над полем является кольцом главных идеалов

16 **Неприводимые многочлены. Факториальность кольца многочленов от одной переменной над полем**

- 17 Критерий того, что факторкольцо $\mathbb{K}[x]/(h)$ является полем. Базис и размерность факторкольца $\mathbb{K}[x]/(h)$ как векторного пространства над полем \mathbb{K}

18 Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов

- 19 Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов

20 Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций

22 Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал

- 23 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала

25 Редуцируемость к нулю S -многочлена двух многочленов с взаимно простыми старшими членами

26 Характеристика поля. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений

- 27 Присоединение корня неприводимого многочлена. Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители

28 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства

29 Подполе в расширении полей, порождённое алгебраическим элементом

31 Теорема существования для конечных полей

32 Цикличность мультипликативной группы конечного поля и неприводимые многочлены над \mathbb{Z}_p