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-Гамаля 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

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

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:
   $(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times), (\mathbb{C} \setminus \{0\}, \times), (\mathbb{Z}_p \setminus \{\overline{0}\}, \times)$, p — простое.
3. Группы матриц:
   $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid \det A \neq 0\}$ — полная линейная группа;
   $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid \det A = 1\}$ — специальная линейная группа.
4. Группы перестановок (с операцией композиции):
   симметрическая группа S_n — все перестановки длины n, $|S_n| = n!$;
   знакопеременная группа A_n — чётные подстановки длины n, $|A_n| = \dfrac{n!}{2}$.
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 $\mathbb{Z}$.

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

Иначе положим $k = \min(H \cap \mathbb{N}) \neq 0$. (это множество непусто, так как $\forall x \implies -x \in H$)

Тогда $k\mathbb{Z} \subseteq H$.

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

$a = qk + r$, где $q \in H$, $0 \leqslant r \leqslant k \implies r = a - qk \in H$.

В силу выбора k получаем $r = 0 \implies a = qk \in k\mathbb{Z}$. ■

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. $\left(g^k\right)^{-1} = g^{-k}$, $\forall k \in \mathbb{Z}$;
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 $\operatorname{ord}(g)$. Заметим, что $\operatorname{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

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

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 $e = g^0, g = g^1, g^2, \ldots, g^{m-1}$ попарно различны. Далее, для всякого $n \in \mathbb{Z}$ мы имеем $n = mq + r$, где $0 \leqslant r \leqslant m - 1$, и

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

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

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

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа

Пусть G — группа, $H \subseteq G$ — подгруппа. Определим отношение L_H следующим образом: $(a,b) \in L_H \iff a^{-1}b \in H$.

Предложение. L_H — отношение эквивалентности.

Доказательство.
1. $a^{-1}a = e \in H$;
2. $a^{-1}b \in H \implies b^{-1}a = (a^{-1}b)^{-1} \in H$;
3. $a^{-1}b \in H, b^{-1}c \in H \implies a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

∎

Заметим, что $a^{-1}b \in H \iff b \in aH$, поэтому класс эквивалентности элемента $a \in G$ совпадает с множеством aH.

Определение 11. *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 смежный классов формулируются и доказываются аналогично.

Лемма 3.1. 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 3.2 (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 $\operatorname{ord}(g)$ делит $|G|$.

Доказательство. Вытекает из следствия 1 и факта, что $\operatorname{ord}(g) = |\langle g \rangle|$. ∎

Следствие. Пусть G — конечная группа и $g \in G$. Тогда $g^{|G|} = e$.

Доказательство. Согласно следствию 2, мы имеем $|G| = \operatorname{ord}(g) \cdot s$, откуда $g^{|G|} = \left(g^{\operatorname{ord}(g)}\right)^s = e^s = e$. ∎

Следствие (малая теорема Ферма)**.** Пусть $\overline{a}$ — ненулевой вычет по простому модулю p. Тогда $\overline{a}^{p-1} = 1$.

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 нееединичным элементов.

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. $G = S_3, G = \{\mathrm{Id}, (12)\}$. 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) $gH = Hg \implies gHg^{-1} = H$.

(2) $\implies$ (3) Очев.

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

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 $g_1'H = g_1H$ и $g_2'H = g_2H$. Тогда $g_1' = g_1h_1$, $g_2' = g_2h_2$, где $h_1, h_2 \in H$.

$$(g_1'H)(g_2'H) = (g_1'g_2')H = (g_1h_1g_2h_2)H = (g_1g_2\underbrace{g_2^{-1}h_1g_2}_{\in H})h_2H \subseteq (g_1g_2)H \implies (g_1'g_2')H = (g_1g_2)H.$$

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 $\varphi\colon G \to F$ 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 $\varphi\colon G \to F$ — 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 $\varphi\colon G \to F$ называется *изоморфизмом*, если отображение φ биективно.

Определение 17. Группы G и F называет *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 $\varphi\colon G \to F$ 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 $\varphi\colon G \to F$ 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 $\varphi\colon G \to F$ является изоморфизмом тогда и только тогда, когда $\ker \varphi = \{e_G\}$ и $\operatorname{Im} \varphi = F$.

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

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

$$\varphi(g^{-1} h g) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1}) e_F \varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_F.$$ ■

7 Теорема о гомоморфизме для групп

Теорема 7.1 (Теорема о гомоморфизме)**.** *Пусть* $\varphi\colon G \to F$ *— гомоморфизм групп. Тогда группа* $\operatorname{Im}\varphi$ *изоморфна факторгруппе* $G/\ker\varphi$*.*

Доказательство. Рассмотрим отображение $\psi\colon G/\ker\varphi \to \operatorname{Im}\varphi$, заданное формулой $\psi(g\ker\varphi) = \varphi(g)$.

1. Корректность.

   $g_1\ker\varphi = g_2\ker\varphi \implies g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in \ker\varphi$.

   $\psi(g_1\ker\varphi) = \varphi(g_1) = \varphi(g_1h_1) = \varphi(g_2h_2) = \varphi(g_2) = \psi(g_2\ker\varphi)$.

2. ψ — гомоморфизм.

   $\psi\left((g_1\ker\varphi)(g_2\ker\varphi)\right) = \psi((g_1g_2)\ker\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1\ker\varphi)\psi(g_2\ker\varphi)$.

3. Сюръектинвость из построения.

4. Инъективность.

   $\psi(g_1\ker\varphi) = \psi(g_2\ker\varphi) \implies \varphi(g_1) = \varphi(g_2) \implies \varphi(g_1)\varphi(g_2)^{-1} = e_F \implies \varphi(g_1g_2^{-1}) = e_F \implies g_1g_2^{-1} \in \ker\varphi \implies g_1\ker\varphi = g_2\ker\varphi$. ∎

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

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

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

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. Пусть $G = \langle g \rangle$. Рассмотрим отображение $\varphi\colon \mathbb{Z} \to G$, $k \mapsto g^k$.

Тогда $\varphi(k+l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l)$, поэтому φ — гомоморфизм. Из определения циклической группы следует, что φ сюръективет, то есть $\operatorname{Im}\varphi = G$. Тогда по теореме о гомоморфизме мы получаем $G \simeq \mathbb{Z}/\ker\varphi$. Так как $\ker\varphi$ — подгруппа в $\mathbb{Z}$, то получаем $\ker\varphi = m\mathbb{Z}$ для некоторого $m \geqslant 0$. (так как любая подгруппа $\mathbb{Z}$ имеет вид $k\mathbb{Z}$) Если $m = 0$, то $\ker\varphi = \{0\}$, откуда $G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$. Если $m > 0$, то $G \simeq \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. ■

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 операцией $(g_1, \dots, g_m)(g'_1, \dots, g'_m) = (g_1 g'_1, \dots, g_m g'_m)$.

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 $|G_1 \times \dots \times G_m| = |G_1| \cdots |G_m|$.

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

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

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

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

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 $n \geqslant 2$ — натуральное число и $n = p_1^{k_1} \cdots p_s^{k_s}$ — 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 $ma = 0 \iff m \vdots \operatorname{ord}(a) \ \forall a \in A$ и $m \in \mathbb{Z}$, то определение экспоненты можно переписать ещё в виде $\exp A = \text{НОД}\{\operatorname{ord}(a) \mid a \in A\}$.

2. Так как $|A| \vdots \operatorname{ord}(a) \ \forall a \in A$, то $|A|$ — общее кратное множества $\{\operatorname{ord}(a) \mid a \in A\}$, а значит, $|A| \vdots \exp A$.

   В частности, $\exp A \leqslant |A|$.

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

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

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

$\Longrightarrow$ Если $\exp A = n$, то для $i = 1, \ldots, s$ существует элемент $c_i \in A$, такой что $\operatorname{ord} c_i = p_i^{k_i} m_i$, где $m_i \in \mathbb{N}$. Для каждого $i = 1, \ldots, s$ положим $a_i = m_i c_i$, тогда $\operatorname{ord}(a_i) = p_i^{k_i}$. Теперь рассмотрим элемент $a = a_1 + \cdots + a_s$ и покажем, что $\operatorname{ord}(a) = n$. Пусть $ma = 0$ для некоторого $m \in \mathbb{N}$, то есть $ma_1 + \cdots + ma_s = 0$. При фиксированном $i \in \{1, \ldots, s\}$ 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, $mn_i \vdots p_i^{k_i}$, а так как n_i не делится на p_i, то $m \vdots p_i^{k_i}$. В силу произвольности выбора i отсюда вытекает, что $m \vdots n$. Так как $na = 0$, то мы окончательно получаем $\operatorname{ord}(a) = n$. Значит, $A = \langle a \rangle$ — циклическая группа. ■

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

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

Определение 23. *Кольцо* — это множество R, на котором заданы две бинарные операции «+» (сложение) и «·» (умножение), удовлетворяющее следующим условиям:

1. $(R, +)$ — абелева группа;
2. $\forall a, b, c, \in R \quad a(b + c) = ab + ac$ и $(a + b)c = ac + bc$;
3. $\forall a, b, c, \in R \quad (ab)c = a(bc)$.
4. $\exists 1 \in R$, такой что $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.

Замечание.

1. $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$;
2. Если $|R| > 1$, то $1 \neq 0$.

Доказательство.

1. $a0 = a(0 + 0) = a0 + a0$, откуда $0 = a0$.
2. Следует из условий выше.

■

Пример.

1. числовые кольца $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
2. кольцо $\mathbb{Z}_n$ вычетов по модулю n;
3. кольцо матриц $\mathrm{Mat}_{n\times n}(\mathbb{R})$;
4. $\mathbb{R}[x]$ — кольцо многочленов от переменной x с коэффициентами из $\mathbb{R}$;
5. $\mathbb{R}[x_1, \ldots, x_n]$ — кольцо многочленов от нескольких переменных $x_1, \ldots, x_n$ с коэффициентами из $\mathbb{R}$;
6. $F(M, \mathbb{R})$ — кольцо функций из множества M в $\mathbb{R}$ (с поточечными операциями сложения и умножения):
   $(f_1 + f_2)(m) := f_1(m) + f_2(m), \quad (f_1 \cdot f_2)(m) := f_1(m) \cdot f_2(m)$.

Определение 24. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a, b \in RR$.

Определение 25. Элемент $a \in R$ называется *обратимым*, если найдется такой $b \in R$, что $ab = ba = 1$.

Замечание. Все обратимые элементы кольца R образуют группу по умножению.

Определение 26. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и $\exists b \in R$, $b \neq 0$, такой что $ab = 0$ (соответственно $ba = 0$).

Замечание. Если R коммутативно, то множества левых и правых делителей нуля совпадают. Тогда левые и правые делители нуля называются просто «делителями нуля».

Замечание. Все делители нуля в R необратимы. Если $ab = 0$, $a \neq 0$, $b \neq 0$ и существует a^{-1}, то получаем $a^{-1}ab = a^{-1}0$, откуда $b = 0$ — противоречние.

Определение 27. Элемент $a \in R$ называется *нильпотентным* (*нильпотентом*), если $a \neq 0$ и найдется такое $n \in \mathbb{N}$, что $a^n = 0$.

Замечание. Всякий нильпотент является делителем нуля: если $a \neq 0$ и n минимально, то $a = a^{n-1} = 0$.

Определение 28. Кольцо R называется *полем*, если оно коммутативно (ассоциативно с 1), $0 \neq 1$ и любой ненулевой элемент обратим.

Пример. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$.

Предложение. Кольцо вычетов $\mathbb{Z}_n$ является полем $\iff$ n — простое число.

Доказательство. Соглашение: $a \in \mathbb{Z} \rightsquigarrow \overline{a} \in \mathbb{Z}_n$ — вычет $a \bmod n$.

$\Longrightarrow$ Если $n = 1$, то $\mathbb{Z}_n = \{0\}$ — не поле.
Если $n > 1$ и $n = m \cdot k$, где $1 < m, k < n$, то $\overline{m} \cdot \overline{k} = \overline{0} \implies$ в $\mathbb{Z}_n$ есть делитель нуля $\implies \mathbb{Z}_n$ — не поле.

$\Longleftarrow$ $n = p$ — простое. Пусть $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$.
Тогда НОД$(a, p) = 1 \implies \exists k, l \in \mathbb{Z}$, такие что $ak + pl = 1$.
Значит, $\overline{a} \cdot \overline{k} + \overline{p} \cdot \overline{l} = \overline{1} \implies \overline{a} \cdot \overline{k} = \overline{1} \implies \overline{a}$ обратим. ■

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

21 S-многочлены. Критерий Бухбергера

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

24 Теорема Гильберта о базисе 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

30 Порядок конечного поля. Автоморфизм Фробениуса

31 Теорема существования для конечных полей

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