Летний экзамен по алгебре

hse-ami-open-exams

Содержание

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

1.1 Бинарные операции.

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 $(M, \circ)$.

1.2 Полугруппы, моноиды и группы.

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

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

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

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

1.3 Коммутативные группы.

Определение 5. *Группа $(G, \circ)$ называется* ***коммутативной*** *или* ***абелевой****, если групповая операция коммутативна, т.е. $a \circ b = b \circ a$ для любых $a, b \in G$.*

1.4 Примеры 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 – простое.
3. Группы матриц: $GL_n(\mathbb{R}) = \{A \in Mat(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}; SL_n(\mathbb{R}) = \{A \in Mat(n \times n, \mathbb{R}) \mid \det(A) = 1\}$.
4. Группы подстановок: симметрическая группа S_n – все подстановки длины n, $|S_n| = n!$; знакопеременная группа A_n – четные подстановки длины n, $|A_n| = n!/2$.

1.5 Порядок группы.

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

1.6 Описание всех подгрупп в группе $(\mathbb{Z}, +)$

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

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

Утверждение 1. *Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$ для некоторого целого неотрицательного k.*

Доказательство. Пусть H – подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, положим $k = 0$. Иначе пусть $k = \min(H \cap \mathbb{N})$ – наименьшее натуральное число, лежащее в H. Тогда $k\mathbb{Z} \subseteq H$. С другой стороны, если $a \in H$ и $a = qk + r$ – результат деления a на k с остатком, то $0 \leqslant r \leqslant k - 1$ и $r = a - qk \in H$. Отсюда $r = 0$ и $H = k\mathbb{Z}$. $\square$

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

2.1 Циклические подгруппы.

Определение 8. *Пусть G – группа и $g \in G$.* ***Циклической подгруппой****, порожденной элементом g, называется подмножество $\{g^n \mid n \in \mathbb{Z}\}$. Циклическая подгруппа, порожденная элементом g, обозначается $\langle g \rangle$. Элемент g называется* ***порождающим*** *или* ***образующим*** *для подгруппы $\langle g \rangle$.*

2.2 Циклические группы.

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

2.3 Порядок элемента.

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 $ord(g)$.*

2.4 Связь между порядком элемента и порядком порождаемой им циклической подгруппы.

Утверждение 2. *Пусть G – группа и $g \in G$. Тогда $ord(g) = |\langle g \rangle|$.*

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 элеметы $e = g^0, g = g^1, g^2, ..., g^{m-1}$ 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, $\langle g \rangle = \{e, g, ..., g^{m-1}\}$ и $|\langle g \rangle| = m$. □

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа.

3.1 Смежные классы.

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*

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

3.2 Индекс подгруппы.

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 $[G : H]$.*

3.3 Теорема Лагранжа.

Лемма 1. *Пусть G – группа, $H \subseteq G$ – ее подгруппа и $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$.*

Доказательство. Предположим, что $g_1G \cap g_2H \neq \varnothing$, т.е. $g_1h_1 = g_2h_2$ 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 2. *Пусть G – 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 $|gH| = |H|$. □

Теорема 1. *Пусть G – конечная группа и $H \subseteq G$ – подгруппа. Тогда*

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

Доказательство. Каждый элемент группы G лежит в (своем) 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.

4.1 Следствие 1.

Следствие 1. *Пусть G – конечная группа и $H \subseteq G$ – подгруппа. Тогда $|H|$ делит $|G|$.*

4.2 Следствие 2.

Следствие 2. *Пусть G – конечная группа и $g \in G$. Тогда $ord(g)$ делит $|G|$.*

Доказательство. Это вытекает из следствия 1 и утверждения 2. □

4.3 Следствие 3.

Следствие 3. *Пусть G – конечная группа и $g \in G$. Тогда $g^{|G|} = e$.*

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

4.4 Следствие 4.

Следствие 4. *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 $G = \langle g \rangle$. □

4.5 Следствие 5.

Следствие 5 (малая теорема Ферма)**.** *Пусть p – простое число и НОД$(a, p) = 1$. Тогда $a^{p-1} \equiv 1 \mod p$.*

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

5 Нормальные подгруппы и факторгруппы.

5.1 Нормальные подгруппы.

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

5.1.1 Эквивалентность условий нормальности группы.

Утверждение 3. *Для подгруппы $H \subseteq G$ следующие условия эквивалентны:*

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

Доказательство. (1) $\Rightarrow$ (2) Пусть $h \in H$ и $g \in G$. Поскольку $gH = Hg$, имеем $gh = h'g$ для некоторого $h' \in H$. Тогда $ghg^{-1} = h'gg^{-1} = h' \in H$.
(2) $\Rightarrow$ (3) Так как $gHg^{-1} \in H$, остается проверить обратное включение. Для $h \in H$ имеем $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, поскольку $g^{-1}hg \in H$ в силу пункта (2), где вместо g взято g^{-1}.
(3) $\Rightarrow$ (1) Для произвольного $g \in G$ в силу (3) имеем $gH = gHg^{-1}g \subseteq Hg$, так что $gH \subseteq Hg$. Аналогично проверяется обратное включение.

□

5.2 Факторгруппы.

5.2.1 Корректность.

Обозначим через G/H множество смежных классов группы G по нормальной подгруппе H. На G/H можно определить бинарную операцию следующим образом:

$$(g_1H)(g_2H) := g_1g_2H.$$

Утверждение 4. *Указанная выше операция корректна.*

Доказательство. Заменим g_1 и g_2 другими представителями g_1h_1 и g_2h_2 тех же смежных классов. Нужно проверить, что $g_1g_2H = g_1h_1g_2h_2H$. Это следует из того, что $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$ и $g_2^{-1}h_1g_2$ лежит в H. Ясно, что указанная операция на множестве G/H ассоциативна, обладает нейтральным элементом eH и для каждого элемента gH есть обратный элемент $g^{-1}H$. □

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

5.2.2 Примеры факторгрупп.

1. 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.

6.1 Гомоморфизмы групп.

Определение 15. *Пусть G и F – группы. Отображение $\varphi : G \to F$ называется **гомоморфизмом**, если $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in G$.*

6.2 Простейшие свойства гомоморфизмов.

Лемма 3. *Пусть $\varphi : G \to F$ – гомоморфизм групп и пусть e_G и e_F – нейтральные элементы групп G и F соответственно. Тогда*

(а) $\varphi(e_G) = e_F$

(б) $\varphi(a^{-1}) = \varphi(a)^{-1}$ *для любого* $a \in G$.

Доказательство. (а) Имеем $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Теперь умножая крайние части этого равенства на $\varphi(e_G)^{-1}$ (например, слева) получим $e_F = \varphi(e_G)$.
(б) Имеем $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_F$, откуда $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

6.3 Изоморфизмы групп.

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

6.4 Ядро и образ гомоморфизма групп, их свойства.

Определение 17. *С каждым гомоморфизмом групп $\varphi : G \to F$ связаны его ядро*

$$\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e_F\}$$

и образ

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

Ясно, что $\mathrm{Ker}(\varphi) \subseteq G$ *и* $\mathrm{Im}(\varphi) \subseteq F$ *– подгруппы.*

Лемма 4. *Гомоморфизм групп $\varphi : G \to F$ инъективен тогда и только тогда, когда* $\mathrm{Ker}(\varphi) = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен, то $\mathrm{Ker}(\varphi) = \{e_G\}$. Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \mathrm{Ker}(\varphi)$, 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 6. *Гомоморфизм групп $\varphi : G \to F$ является изоморфизмом тогда и только тогда, когда* $\mathrm{Ker}(\varphi) = \{e_G\}$ *и* $\mathrm{Im}(\varphi) = F$.

Утверждение 5. *Пусть $\varphi : G \to F$ – гомоморфизм групп. Тогда подгруппа* $\mathrm{Ker}(\varphi)$ *нормальна в G.*

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

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

□

7 Теорема о гомоморфизме для групп.

Теорема 2. *Пусть* $\varphi : G \to F$ *– гомоморфизм групп. Тогда группа* $\mathrm{Im}(\varphi)$ *изоморфна факторгруппе* $G/\operatorname{Ker}(\varphi)$.

Доказательство. Рассмотрим отображение $\psi : G/\operatorname{Ker}(\varphi) \to F$, заданное формулой $\psi(g\operatorname{Ker}(\varphi)) = \varphi(g)$. Проверка корректности: равенство $\varphi(gh_1) = \varphi(gh_2)$ для любых $h_1, h_2 \in \operatorname{Ker}(\varphi)$ следует из цепочки равенств

$$\varphi(gh_1) = \varphi(g)\varphi(h_1) = \varphi(g) = \varphi(g)\varphi(h_2) = \varphi(gh_2).$$

Отображение ψ сюръективно по построению и инъективно в силу того, что $\varphi(g) = e_F$ тогда и только тогда, когда $g \in \operatorname{Ker}(\varphi)$ (т.е. $g\operatorname{Ker}(\varphi) = \operatorname{Ker}(\varphi)$). Остается проверить, что ψ – гомоморфизм:

$$\psi((g\operatorname{Ker}(\varphi))(g'\operatorname{Ker}(\varphi))) = \psi(gg'\operatorname{Ker}(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(g\operatorname{Ker}(\varphi))\psi(g'\operatorname{Ker}(\varphi)).$$

□

8 Классификация циклических групп.

Утверждение 6. *Пусть G – циклическая группа. Тогда:*

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

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

1. $\varphi : \mathbb{Z} \to G, \varphi : k \mapsto g^k$
   Это гомоморфизм и биекция $\Rightarrow$ изоморфизм.
2. $\varphi : \mathbb{Z} \to G, \varphi : k \mapsto g^k$
   Рассмотрим, куда переходит $k + ns$, где $0 \leqslant k \leqslant n - 1$
   $k + ns \mapsto g^{k+ns} = g^k g^{ns} = g^k (g^n)^s = g^k$.

□

9 Прямое произведение групп. Разложение конечной циклической группы.

9.1 Прямое произведение групп.

Определение 18. ***Прямым произведением*** *групп $G_1, ..., G_m$ называется множество*

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

с операцией $(g_1, ..., g_m)(g'_1, ..., g'_m) = (g_1 g'_1, ..., g_m g'_m)$. Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, ..., e_{G_m})$ и для каждого элемента $(g_1, ..., g_m)$ есть обратный элемент $(g_1^{-1}, ..., g_m^{-1})$.

`https://youtu.be/1oceAPu3b8o`

9.2 Разложение конечной циклической группы.

Определение 19. *Группа G раскладывается в прямое произведение своих подгрупп $H_1, ..., H_m$, если отображение $H_1 \times ... \times H_m \to G, (h_1, ..., h_m) \mapsto h_1 \cdot ... \cdot h_m$ является изоморфизмом.*

`https://youtu.be/1oceAPu3b8o?t=293`

Теорема 3. *Пусть $n = ml$ – разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

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

Доказательство. Рассмотрим отображение

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

Поскольку m и l делят n, отображение φ определено корректно. Ясно, что φ – гомоморфизм.
Далее, $a \mod n \in \mathrm{Ker}(\varphi) \Rightarrow a \mod m = 0, a \mod l = 0 \Rightarrow a$ делится на m, a делится на k. Так как НОД$(m,l) = 1$, то a делится на $n = ml \Rightarrow a \mod n = 0 \Rightarrow \mathrm{Ker}(\varphi) = \{0\}$. Следовательно, гомоморфизм φ инъективен. Поскольку множества $\mathbb{Z}_n$ и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. □

`https://youtu.be/1oceAPu3b8o?t=585`

Следствие 7. *Пусть $n \geqslant 2$ – натуральное число и $n = p_1^{k_1} ... p_s^{k_s}$ – его разложение в произвежение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп*

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

`https://youtu.be/1oceAPu3b8o?t=1061`

10 Подгруппы p-кручения в абелевых группах. Разложение конечной абелевой группы в прямое произведение подгрупп p-кручения.

10.1 Подгруппы p-кручения в абелевых группах.

Определение 20. *Пусть $(A, +)$ – абелева группа, p – простое число. Положим*

$$T_p(A) := \{a \in A \mid \exists k \geqslant 0 : p^k \cdot a = 0\} = \{a \in A \mid \exists m \geqslant 0 : \operatorname{ord}(a) = p^m\}$$

– подгруппа в A. Тогда $T_p(A)$ называется ***подгруппой p-кручения****.*

https://youtu.be/1oceAPu3b8o?t=1260

10.2 Разложение конечной абелевой группы в прямое произведение подгрупп p-кручения.

Утверждение 7 (без доказательства)**.** *Пусть $|A| < \infty$ и $T_p(A) = A$ для некоторого простого p. Тогда $A \simeq \mathbb{Z}_{p^{k_1}} \times ... \times \mathbb{Z}_{p^{k_s}}, k_i \geqslant 1$, причем число множителей и их порядки определены однозначно (с точностью до перестановки).*

https://youtu.be/1oceAPu3b8o?t=1474

Утверждение 8. *Пусть $|A| < \infty, |A| = p_1^{k_1} \times ... \times p_s^{k_s}$ – разложение на простые множители. Тогда $A = T_{p_1}(A) \times ... \times T_{p_s}(A)$.*

Доказательство. Нужно доказать, что отображение $\varphi : T_{p_1}(A) \times ... \times T_{p_s}(A) \to A, (a_1, ..., a_s) \mapsto a_1 + ... + a_s$ является изоморфизмом. Ясно, что φ – гомоморфизм. Докажем инъективность. Пусть $(a_1, ..., a_s) \in T_{p_1}(A) \times ... \times T_{p_s}(A)$, такое что $a_1 + ... + a_s = 0$. Для любого $i, 1 \leqslant i \leqslant s \operatorname{ord}(a_i) = p_i^{m_i}, m_i \geqslant 0$. При фиксированном i умножим $a_1 + ... + a_s = 0$ на $n_i = p_1^{m_1} \cdot ... \cdot p_{i-1}^{m_{i-1}} \cdot p_{i+1}^{m_{i+1}} \cdot ... \cdot p_s^{m_s}$ и получим $n_i \cdot a_i = 0$. Следовательно, n_i делится на $p_i^{m_i} \Rightarrow m_i = 0 \Rightarrow \operatorname{ord}(a_i) = 1 \Rightarrow a_i = 0 \Rightarrow \operatorname{Ker}(\varphi) = 0$. Докажем сюръективность. $a \in A \Rightarrow \operatorname{ord}(a) = p_1^{m_1} \cdot ... \cdot p_s^{m_s}$ по следствию 7 о разложении конечной циклической группы. $\langle a \rangle = \langle b_1 \rangle \times ... \times \langle b_s \rangle$, где $b_i \in \langle a \rangle$ и $\operatorname{ord}(b_i) = p_i^{m_i}$ $\Rightarrow a = a_1 + ... + a_s$, где $a_i \in \langle b_i \rangle \subseteq T_{p_i}(A)$. $\square$

https://youtu.be/1oceAPu3b8o?t=1635

11 Примарные абелевы группы. Теорема о строении конечных абелевых групп, доказательство единственности.

11.1 Примарные абелевы группы.

Определение 21. *Конечная абелева группа A называется* ***примарной****, если $|A| = p^k$ для некоторого простого p.*

https://youtu.be/1oceAPu3b8o?t=2379

11.2 Теорема о строении конечных абелевых групп, доказательство единственности.

Теорема 4. *Пусть $|A| < \infty$ – конечная абелева группа. Тогда $A \simeq \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_s^{k_s}}$, где p_i – (не обязательно различные) простые числа ($k_i \geqslant 1$), причем в этом разложении число примарных циклических множителей и их порядки (с точностью до перестановки) определены однозначно.*

Доказательство. Существование следует из утверждений 7 и 8. Докажем единственность. Зафиксируем простое p. Тогда в разложении $A \simeq \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_s^{k_s}}$

$$\prod_{p_i=p} \mathbb{Z}_{p_i^{k_i}} \subseteq T_p(A).$$

Пусть $a \in A$. Тогда $a = (n_1, ..., n_s), n_i \in \mathbb{Z}_{p_i^{k_i}}$. Если $p^k \cdot a = 0$ для некоторого k, то для любого i $p^k \cdot n_i$ делится на $p_i^{k_i}$. Если $p \neq p_i$, то n_i делится на $p_i^{k_i} \Rightarrow n_i \equiv 0 \mod p_i^{k_i} \Rightarrow a \in T_p(A) \Leftrightarrow$ для любого i с условием $p \neq p_i$ $n_i = 0$ в $\mathbb{Z}_{p_i^{k_i}} \Rightarrow T_p(A) \subseteq \prod_{p_i=p} \mathbb{Z}_{p_i^{k_i}}$. Итог: достаточно доказать единственность каждого $T_p(A)$. Теперь пусть $B = T_p(A) \simeq \mathbb{Z}_{p^{m_1}} \times ... \times \mathbb{Z}_{p^{m_r}}$. Индукция по $|B|$. База: $|B| = p \Rightarrow$ по следствию 4 из теоремы Лагранжа $B \simeq \mathbb{Z}_p$. Теперь пусть $|B| > p, |B| = p^m$, где $m = m_1 + ... + m_r$. Рассмотрим подгруппу $pB \subseteq B$, где $pB = \{pb \mid b \in B\}$ $\Rightarrow pB \simeq \mathbb{Z}_{p^{m_1-1}} \times ... \times \mathbb{Z}_{p^{m_r-1}}$, в частности $|pB| < |B|$. Если $m_i = 1$, то соответствующий множитель исчезает. По предположению индукции набор ненулевых чисел среди $m_1 - 1, ..., m_r - 1$ определен однозначно с точностью до перестановки. Следовательно, однозначно восстанавливаются все m_i с условием $m_i > 1$ Число $m_i = 1$ однозначно восстанавливается из условия $m_1 + ... + m_r = m$. □

https://youtu.be/1oceAPu3b8o?t=2507

12 Экспонента конечной абелевы группы и критерий цикличности.

Определение 22. *Пусть A – конечная абелева группа.* ***Экспонента*** *группы A – это число*

$$\exp(A) = НОК\{\operatorname{ord}(a) \mid a \in A\} = min\{n \in \mathbb{N} \mid na = 0 \, \forall \, a \in A\}$$

https://youtu.be/1oceAPu3b8o?t=3792

Утверждение 9. *Пусть A – конечная абелева группа. Тогда* $\exp(A) = |A| \Leftrightarrow A$ *– циклическая группа.*

Доказательство. $\Leftarrow$ A – циклическая $\Rightarrow A \simeq \mathbb{Z}_n \Rightarrow \operatorname{ord}(a) = n = |A| \Rightarrow \exp(A) = |A|$

$\Rightarrow$ $\exp(A) = |A|$ Знаем, что $A \simeq T_{p_1}(A) \times ... \times T_{p_s}(A)$, где $|A| = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$. Пусть $b_i \in T_{p_i}(A)$ – элемент наибольшего порядка $\Rightarrow \operatorname{ord}(b_i) = p_i^{m_i}$. Тогда для любого $a_i \in T_{p_i}(A), ..., a_s \in T_{p_s}(A)$ получаем $\operatorname{ord}(a_i) = p_i^{l_i}$, где $l_i \leqslant m_i$. $\operatorname{ord}(a_1 + ... + a_s) = \operatorname{ord}(a_1) \cdot ... \cdot \operatorname{ord}(a_s)$ делит $\operatorname{ord}(b_1) \cdot ... \cdot \operatorname{ord}(b_s) = \operatorname{ord}(b_1 + ... + b_s)$. Следовательно, $\exp(A) = \operatorname{ord}(b_1 + ... + b_s) \Rightarrow |A| = \exp(A) = |\langle b_1 + ... + b_s \rangle| \Rightarrow \langle b_1 + ... + b_s \rangle = A \Rightarrow A$ – циклическая группа. $\square$

https://youtu.be/1oceAPu3b8o?t=4028

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

Пусть у нас есть G – конечная абелева группа. И также есть элемент $g \in G$, для которого $ord(g)$ будет достаточно большим значением.

13.1 Задача дискретного логарифмирования.

Дано: $h \in \langle g \rangle$. Найти такое α, что $g^\alpha = h$. Возведение в степень – задача более простая с технической стороны реализации. Существует алгоритм бинарного возведения в степень: $g^{16} = ((((g)^2)^2)^2)^2$. Задача нахождения степени решается только перебором или близким к перебору способом.

`https://youtu.be/1oceAPu3b8o?t=4480`

13.2 Система Диффи-Хеллмана обмена ключами.

Группа G и некоторый ее элемент g известны всем, причем g имеет достаточно большой порядок. Пусть есть два пользователя системы – A и B. A фиксирует свое секретное $\alpha \in \mathbb{N}$ и сообщает всем пользователям g^α. B совершает аналогичные действия: фиксирует $\beta \in \mathbb{N}$ и сообщает всем пользователям g^β. Теперь A и B опять совершают аналогичные действия – каждый из них возводит элемент другого в свою секретную степень, они оба получают элемент $g^{\alpha\beta}$, который известен только им двоим. Теперь по этому ключу можно устроить шифрованный канал связи, к которому никто не имеет доступа. В силу сложности задачи дискретного логарифмирования по g^α и g^β нельзя быстро получить $g^{\alpha\beta}$.

`https://youtu.be/mNd30oeCugc?t=78`

13.3 Криптосистема Эль-Гамаля.

Группа G и некоторый ее элемент g известны всем, причем g имеет достаточно большой порядок. Пусть есть два пользователя системы – A и B. A фиксирует свое секретное $\alpha \in \mathbb{N}$ и сообщает всем пользователям g^α. B хочет передать для A элемент $h \in G$. Для этого B фиксирует какое-то $k \in \mathbb{N}$ и объявляет пару $\{g^k, h \cdot (g^\alpha)^k\}$.

`https://youtu.be/mNd30oeCugc?t=360`