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 $H = k\mathbb{Z}$. □

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 $|\langle g \rangle| = m$. $\square$

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 $g \in G$.*

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.

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. □

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