Алгебра

Авдеев Р. С.

Содержание

1 Лекция №1

Лекция 07.04.20

1.1 Бинарные операции

Пусть M – некоторое множество

Определение.

Бинарная операция на множестве M – это отображение $\circ : M \times M \mapsto M$. Пара $(M, \circ)$ называется множеством с бинарной операцией

1.2 Полугруппы, моноиды, группы, коммутативные (абелевы) группы

Определение.

1. $(M, \circ)$ называется группой, если выполнены следующие условия:
   (a) $(a \circ b) \circ c = a \circ (b \circ c)$ – ассоциативность
   (b) $\exists$ нейтральный элемент, то есть такой $e \in M$, что $\forall a \in M : e \circ a = a \circ e = a$
   (c) $\forall a \in M \ \exists$ обратный элемент (a^{-1}), то есть такой b, что $a \circ b = b \circ a = e$
2. $(M, \circ)$ называется полугруппой, если требуется только условие (a)
3. $(M, \circ)$ называется моноидом, если требуются только (a) и (b)

1.2.1 Примеры

$(\mathbb{N}, +)$ – полугруппа, но не моноид
$(\mathbb{N} \cup \{0\}, +)$ – моноид

Замечание.

1. Примеры неассоциативных операций: $(\mathbb{Z}, -)$, $(\mathbb{N}, a \circ b = a^b)$
2. Нейтральный элемент единственен (если существует)

   Если e_1, e_2 – два нейтральных, то $e_1 = e_1 \circ e_2 = e_2$
3. Обратный элемент единственен (если существует)

   b_1, b_2 – два обратных к $a \Rightarrow b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$
4. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ a^{-1} = e$$

Определение.

Группа G называется коммутативной (абелевой), если $\forall a, b \in G : ab = ba$

Абстрактные группы: мультипликативная запись: ab, e, a^{-1}
Абелевы группы: аддитивная запись: $a + b, 0, -a$

1.3 Порядок группы

Определение.

Порядок группы G – это число элементов в ней. Обозначается $|G|$.
G называется конечной, если $|G| < \infty$, бесконечной, если $|G| = \infty$

1.4 Примеры групп

1. Числовые аддитивные группы:
   $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +)$
2. Числовые мультипликативные группы:
   $(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times), (\mathbb{C} \setminus \{0\}, \times), (\mathbb{Z}_n \setminus \{\bar{0}\}, \times)$
3. Группы матриц (операция $\times$):
   $GL_n(\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) \mid \det A \neq 0\}$ – полная линейная группа
   $SL_n(\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) \mid \det A = 1\}$ – специальная линейная группа
4. Группы перестановок (операция $\times$):
   симметрическая группа S_n – все перестановки длины n, $|S_n| = n!$
   знакопеременная группа A_n – все чётные перестановки длины n, $|A_n| = n!/2$

1.5 Подгруппы

Определение.

Подмножество H группы G называется подгруппой, если

1. $e \in H$
2. $a, b \in H \Rightarrow ab \in H$
3. $a \in H \Rightarrow a^{-1} \in H$

Несобственные подгруппы: $\{e\} \subseteq G$, $G \subseteq G$.
Остальные подгруппы называются собственными

Пример.

$2\mathbb{Z}$ (все целые числа кратные 2) – подгруппа в $(\mathbb{Z}, +)$

1.6 Описание всех подгрупп в группе целых чисел по сложению

Предложение.

Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторого $k \geqslant 0$

Доказательство.

Пусть $H \in \mathbb{Z}$ – подгруппа.
Если $H = \{0\}$, то $H = 0\mathbb{Z}$
Пусть теперь $H \neq \{0\}$. Тогда $x \in H \Leftrightarrow -x \in H$
Положим $k = \min\limits_{\neq \varnothing}(H \cap \mathbb{N})$

Тогда $k\mathbb{Z} \subseteq H$(если мы k сложим с собой много раз, то результат тоже будет лежать в подгруппе)
Пусть $a \in H \Rightarrow$ разделим a на k с остатком: $a = q \cdot k + r$, $0 \leqslant r < k$
Тогда $r = \underset{\in H}{a} - q \cdot \underset{\in H}{k} \in H$
Так как k – минимальна $\Rightarrow r = 0 \Rightarrow a = q \cdot k \Rightarrow a \in k\mathbb{Z} \Rightarrow k\mathbb{Z} = H \quad \boxdot$

1.7 Циклические подгруппы

Пусть G – группа, $g \in G$, $n \in \mathbb{Z}$

$$g^n = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, \ n > 0 \\ e, \ n = 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|}, \ n < 0 \end{cases}$$

Определение.

Пусть $g \in G$. $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ называется циклической подгруппой, порождаемой элементом g

g – образующий или порождающий элемент

Пример.

$2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$

1.8 Порядок элемента группы

Пусть G – группа, $g \in G$
$M(g) = \{n \mid g^n = e\}$

Определение.

Порядок элемента g – это

$$\operatorname{ord}(g) := \begin{cases} \min M(g), \text{ если } M(g) \neq \varnothing \\ \infty, \text{ если } M(g) = \varnothing \end{cases}$$

Замечание.

$\operatorname{ord}(g) = 1 \Leftrightarrow g = e$

1.9 Связь между порядком элемента и порядком порождаемой им циклической подгруппы

Предложение.

$\operatorname{ord}(g) = |\langle g \rangle|$

Доказательство.

Имеем $g^k = g^s \Rightarrow g^{k-s} = e$ $(\star)$

1. $\operatorname{ord}(g) = \infty \underset{(\star)}{\Rightarrow} \forall k > s : g^k \neq g^s \Rightarrow |\langle g \rangle| = \infty$
2. $\operatorname{ord}(g) = m < \infty \Rightarrow$ элементы $g^0 = e, g^1 = g, g^2, \ldots, g^{m-1}$ попарно различны (если $\exists\, k, s : g^k = g^s \Rightarrow g^{k-s} = e$, но $\operatorname{ord}(g) = m$)

   $n \in \mathbb{Z} \Rightarrow n = q \cdot m + r,\ 0 \leqslant r < m$

   $\Rightarrow g^n = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = g^r$

   $\Rightarrow \langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\} \Rightarrow |\langle g \rangle| = m = \operatorname{ord}(g)$ $\quad \boxdot$

1.10 Циклические группы

Определение.

Группа G называется циклической, если $G = \langle g \rangle$ для некоторого $g \in G$

Пример.

$(\mathbb{Z}, +) = \langle 1 \rangle$

Замечание.

G циклична $\Leftrightarrow$ G – коммутативна и $\leqslant$ счётна

1.11 Левые смежные классы группы по подгруппе, разбиение группы на левые смежные классы

Пусть G – группа, $H \subseteq G$ – подгруппа

Отношение L_H на G:

$(a, b) \in L_H \Leftrightarrow a^{-1}b \in H$

Предложение.

L_H – отношение эквивалентности

Доказательство.

1. Рефлексивность: $a^{-1}a = e \in H$
2. Симметричность: $a^{-1}b \in H \Rightarrow b^{-1}a = (ab^{-1})^{-1} \in H$
3. Транзитивность: $a^{-1}b \in H,\ b^{-1}c \in H \Rightarrow a^{-1}c = \underset{\in H}{a^{-1}b} \cdot \underset{\in H}{b^{-1}c} \in H$ $\quad \boxdot$

$a^{-1}b \in H \Leftrightarrow b \in aH \Rightarrow$ класс элемента a это в точности множество aH.

Определение.

Множество $aH := \{ah \mid h \in H\}$ называется левым смежным классом элемента a по подгруппе H