

ЛЕКЦИЯ 14

Определение 1. Пусть G – непустое множество с одной бинарной операцией $(x, y) \mapsto x * y$. Тогда G называется *группой*, если выполнены следующие три аксиомы.

- для любых $x, y, z \in G$ выполнено $(x * y) * z = x * (y * z)$ (ассоциативность);
- существует $e \in G$ такой, что $\forall x \in G$ выполнено $e * x = x * e = x$. (нейтральный элемент);
- для каждого $g \in G$ существует $g^{-1} \in G$ такой, что $g * g^{-1} = g^{-1} * g = e$ (обратный элемент).

Если из контекста не понятно, какая операция имеется в виду, то используют обозначение $(G, *)$.

Определение 2. Группа G называется *абелевой* (коммутативной) группой, если

- для любых $x, y \in G$ выполнено $x * y = y * x$ (коммутативность).

Замечание 1. Если просто задано множество с одной бинарной операцией, то оно называется *группоидом*. Если данная операция ассоциативна (удовлетворяет только первой аксиоме), то данное множество называется *полугруппой*. Если же у полугруппы есть нейтральный элемент, то она называется *моноидом*.

Примеры групп.

- (1) Числовые группы (все они абелевы)
 - по сложению $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$.
 - по умножению $\mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}, \cdot)$, $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot)$, $(\{1, -1\}, \cdot)$.
- (2) векторы по сложению (все они абелевы) $(\mathbb{R}^n, +)$, $(\text{Mat}_{mn}(\mathbb{R}), +)$, $(\mathbb{Q}^n, +)$, $(\text{Mat}_{mn}(\mathbb{Q}), +)$, $(\mathbb{Z}^n, +)$, $(\text{Mat}_{mn}(\mathbb{Z}), +)$.
- (3) Группа вычетов (остатков) по модулю n : $(\mathbb{Z}_n, +)$. (Это абелева группа.)
- (4) Симметрические группы (S_n, \circ) . (при $n \geq 3$ не абелевы)
- (5) Невырожденные матрицы по умножению (при $n \geq 2$ не абелевы)

$$\text{GL}_n(\mathbb{R}) = (\{A \in \text{Mat}_{nn}(\mathbb{R}) \mid \det A \neq 0\}, \cdot),$$

$$\text{GL}_n(\mathbb{Q}) = (\{A \in \text{Mat}_{nn}(\mathbb{Q}) \mid \det A \neq 0\}, \cdot).$$

- (6) Группы преобразований (почти всегда не абелевы)
 - $(S(X), \circ)$ – группа биекций $X \rightarrow X$ для некоторого фиксированного множества X .
 - группа движений плоскости $(\text{Iso}(\mathbb{R}^2), \circ)$.

Множества с операциями, не являющиеся группами.

- $(\mathbb{N}, +)$ (нет нейтрального элемента, это полугруппа)
- $(\mathbb{N} \cup \{0\}, +)$ (не к любому элементу есть обратный, это моноид)
- (\mathbb{Z}, \cdot) (не к любому элементу есть обратный, это моноид)
- $(\text{Mat}_{nn}(\mathbb{R}), \cdot)$ (не к любому элементу есть обратный, это моноид)
- $(\mathbb{Z} \setminus \{3, -3\}, +)$ (не корректно определена операция, даже не группоид)
- $(\mathbb{Z}, *)$, где $x * y = x + 2y$ (операция не ассоциативна, это группоид, но не полугруппа)

Мультипликативная и аддитивная терминологии

Во многих примерах операция – это умножение. На самом деле это вопрос терминологии. Любую операцию в любой группе можно назвать умножением и писать $xy = x \cdot y$ вместо $x * y$. Нейтральный элемент группы будем также называть единицей группы (обозначается e). Такая терминология и обозначения называются мультипликативными.

В других примерах операция – это сложение. Однако обычно с операцией сложения получается абелева группа. Операцию в произвольной абелевой группе принято называть сложением. При этом нейтральный элемент называется нулем группы (обозначается 0), а обратный элемент к x – противоположным (обозначается $-x$). Такая терминология и обозначения называются аддитивными.

Заметим, что абелева группа является частным случаем произвольной группы. Поэтому к ней применимы обе терминологии. Это не должно вызывать путаницы, надо лишь научиться переводить выражения с одного языка на другой.

Простейшие следствия из аксиом

- Нейтральный элемент в группе единственный. Допустим противное: пусть e и e' – нейтральные элементы группы G . Тогда $e = ee' = e'$.
- Обратный элемент к данному элементу единственный. Допустим противное: пусть h и h' – обратные элементы к элементу g группы G . Тогда $h = h(gh') = (hg)h' = h'$.

- Если $xy = xz$, (или $yx = zx$), то $y = z$. Умножим обе части равенства на x^{-1} слева (справа).
- Если $gh = e$, то $g = h^{-1}$ и $h = g^{-1}$. Имеем $gh = e = gg^{-1}$, значит, $h = g^{-1}$. Второе аналогично.
- $(g^{-1})^{-1} = g$. В самом деле $gg^{-1} = e$, отсюда $(g^{-1})^{-1} = g$.
- Выполнена обобщенная ассоциативность. (Доказательство было ранее.)
- $(xy)^{-1} = y^{-1}x^{-1}$. Перемножим

$$xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e.$$

Определение 3. Пусть $g \in G$, $k \in \mathbb{Z}$. Определим

$$g^k = \begin{cases} gg \dots g & (k \text{ раз}), \text{ если } k > 0; \\ e, & \text{если } k = 0; \\ g^{-1}g^{-1} \dots g^{-1} & (-k \text{ раз}), \text{ если } k < 0. \end{cases}$$

Лемма 1. $g^a g^b = g^{a+b}$ и $(g^a)^b = g^{ab}$.

Упражнение 1. Докажите эту лемму.

Определение 4. Порядком элемента $g \in G$ называется минимальное натуральное k такое, что $g^k = e$. Если же такого числа k не существует, то говорят, что порядок равен ∞ . Обозначается порядок элемента g через $\text{ord}(g)$.

Упражнение 2. $\text{ord}(e) = 1$;

Порядок любого ненулевого числа в группе $(\mathbb{Z}, +)$ равен ∞ ;

Порядок -1 в группе $(\mathbb{Q} \setminus \{0\}, \cdot)$ равен 2.

Лемма 2. Порядок подстановки $\sigma \in S_n$ равен наименьшему общему кратному длин циклов в разложении σ в произведение независимых циклов.

Доказательство. Пусть разложение σ в произведение независимых циклов имеет вид $\sigma = \xi_1 \circ \dots \circ \xi_m$, где ξ_j – цикл длины l_j . Тогда, так как независимые циклы коммутируют выполнено

$$\sigma^k = \xi_1^k \circ \dots \circ \xi_m^k.$$

При этом подстановки ξ_1^k, \dots, ξ_m^k переставляют не пересекающиеся множества элементов. Из этого следует, что $\xi_1^k \circ \dots \circ \xi_m^k = \text{id}$ тогда и только тогда, когда для каждого j выполнено $\xi_j^k = \text{id}$. Но цикл в степени равен тождественной подстановке тогда и только тогда, когда данная степень делится на длину данного цикла. Получаем $\sigma^k = \text{id}$ тогда и только тогда, когда $l_j \mid k$ для всех j . Наименьшее такое k равно НОК(l_1, \dots, l_m). \square

Определение 5. Пусть G – группа с операцией $*$. Подмножество $H \subseteq G$ называется *подгруппой*, если H является группой относительно той же операции $*$.

Пример 1. Множество $(2\mathbb{Z}, +)$ четных целых чисел образует подгруппу в группе $(\mathbb{Z}, +)$.

Лемма 3. Любая подгруппа содержит нейтральный элемент группы.

Доказательство. Пусть H – подгруппа G и e – нейтральный элемент G . Тогда в H есть нейтральный элемент e' . Получаем $ee' = e' = e'e'$. Отсюда $e = e'$. \square

Лемма 4. Пусть H – подгруппа группы G . Рассмотрим $h \in H$ и пусть h^{-1} – обратный к h в G . Тогда $h^{-1} \in H$.

Доказательство. Так как H – группа, существует обратный элемент $h' \in H$. Тогда $hh' = hh^{-1} = e$. Отсюда $h' = h^{-1}$. \square

Теорема 1. Пусть H – подмножество группы G . Тогда H – подгруппа G тогда и только тогда, когда выполнены следующие условия:

- (1) $H \neq \emptyset$;
- (2) H замкнуто относительно операции, то есть если $h_1, h_2 \in H$, то $h_1 h_2 \in H$;
- (3) H замкнуто относительно взятия обратного, то есть если $h \in H$, то $h^{-1} \in H$.

Доказательство. Необходимость первых двух условий очевидна. Необходимость третьего условия следует из предыдущей леммы. Докажем достаточность. Пусть условия выполнены. Тогда из условий 1 и 2 H – непустое множество с бинарной операцией (той же, что и в G , а значит, ассоциативной). По условию 1 найдется $h \in H$. По условию 3, $h^{-1} \in H$. По условию 2, $hh^{-1} = e \in H$, то есть в H есть нейтральный элемент. По условию 3 каждый элемент имеет обратный. \square

Пример 2. *С помощью данной теоремы можно доказать, что следующие подмножества являются подгруппами.*

- $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$;
- $A_n \subset S_n$, где A_n – множество четных подстановок длины n ;
- $B_n \subset \text{GL}_n$, где B_n – множество невырожденных верхнетреугольных матриц;
- $D_n \subset \text{GL}_n$, где D_n – множество невырожденных диагональных матриц;
- $\text{SL}_n \subset \text{GL}_n$, где SL_n – множество матриц $n \times n$ с определителем 1;
- пересечение любого количества подгрупп является подгруппой.

Докажем, например, что A_n – подгруппа в S_n . Используя теорему надо проверить свойства непустоты, замкнутости относительно композиции и замкнутости относительно взятия обратного. Непустота следует из того, что тождественная подстановка является четной, а значит, лежит в A_n . Произведение четных подстановок является четной и обратная к четной подстановке является четной.

Упражнение 3. Докажите остальные пункты.

Определение 6. Пусть H – подгруппа группы G . Левый смежный класс элемента $g \in G$ по подгруппе H – это подмножество

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

Лемма 5. *Левые смежные классы gH и $g'H$ либо не пересекаются, либо совпадают.*

Доказательство. Пусть два смежных класса gH и $g'H$ пересекаются. Докажем, что они совпадают. Пусть f – общий элемент этих смежных классов, то есть $f = gh = g'h'$ для некоторых $h, h' \in H$. Тогда $g' = ghh'^{-1}$. Получаем

$$g'H = \{g'\hat{h} \mid \hat{h} \in H\} = \{ghh'^{-1}\hat{h} \mid \hat{h} \in H\}.$$

\square

При этом когда \hat{h} пробегает всю группу H , элемент $hh'^{-1}\hat{h}$ также пробегает всю группу H . Это следует из того, что отображение $H \rightarrow H$, $\hat{h} \mapsto hh'^{-1}\hat{h}$ является биекцией (проверьте это!). Следовательно, $g'H = gH$.

Пример 3. *Рассмотрим подгруппу $H = (3\mathbb{Z}, +)$ в группе $G = (\mathbb{Z}, +)$. Левые смежные классы имеют вид $m + 3\mathbb{Z}$. Смежные классы $0 + 3\mathbb{Z}$ и $3 + 3\mathbb{Z}$ совпадают (они состоят из чисел, делящихся на 3). Аналогично, смежные классы $1 + 3\mathbb{Z}$ и $7 + 3\mathbb{Z}$ совпадают. При этом смежные классы $0 + 3\mathbb{Z}$ и $1 + 3\mathbb{Z}$ не пересекаются.*

Определение 7. *Индексом подгруппы H в группе G называется мощность множества (различных) левых смежных классов. Обозначается индекс через $[G : H]$.*

Определение 8. *Порядком группы G называется мощность множества ее элементов $|G|$. Если количество элементов в группе G конечно, то группа называется *конечной*, а иначе – *бесконечной*.*

Лемма 6. *Пусть H – конечная подгруппа группы G . Тогда $|gH| = |H|$ для любого $g \in G$.*

Доказательство. Установим биекцию $\varphi: H \rightarrow gH$, $\varphi(h) = gh$. Докажем, что φ – биекция. В самом деле, если $gh_1 = gh_2$, то $h_1 = h_2$ (нужно домножить на g^{-1} слева). Это доказывает инъективность φ . Сюръективность φ следует из определения: любой элемент gH имеет вид gh и потому лежит в образе φ . \square

Замечание 2. Вообще говоря, утверждение данной леммы верно (с тем же доказательством) и для бесконечной подгруппы H .

Теорема 2 (Теорема Лагранжа). *Пусть G – конечная группа. Тогда $|G| = |H| \cdot [G : H]$.*

Доказательство. Так как любой элемент g группы G лежит в своем левом смежном классе gH (это следует из того, что $e \in H$) и различные левые смежные классы не пересекаются, левые смежные классы образуют разбиение G на непересекающиеся подмножества. При этом в каждом подмножестве $|H|$ элементов. Количество этих подмножеств равно $[G : H]$. Значит, общее количество элементов в G равно произведению количества подмножеств на мощность каждого подмножества. \square