Лекция 7. Группы. Подгруппы. Смежные классы. Разложение группы по подгруппе. Нормальные подгруппы. Фактор-группы.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте https://mk.cs.msu.ru

Нейтральный элемент

Пусть S — произвольное множество.

Алгебраической операцией $*$ на множестве S называется отображение $* : S \times S \to S$.

Элемент $e \in S$ называется **нейтральным элементом** относительно операции $*$, если для каждого элемента $a \in S$ верно

$$a * e = e * a = a.$$

Нейтральный элемент

Предложение 1. *Нейтральный элемент (если он существует) единственен.*

Доказательство. Пусть $e' \in S$ и $e'' \in S$ — нейтральные элементы. Тогда

$$\begin{array}{ccccc} & & e' * e'' & & \\ e' & = & e' * e'' & = & e'' \end{array}$$

□

Симметричный элемент

Для элемента $a \in S$ элемент $a' \in S$ называется **симметричным**, если

$$a * a' = a' * a = e,$$

где $e \in S$ — нейтральный элемент относительно операции $*$.

Симметричный элемент

Предложение 2. *Симметричный элемент относительно ассоциативной операции (если он существует) единственен.*

Доказательство. Пусть для некоторого элемента $a \in S$ элементы $a' \in S$ и $a'' \in S$, $a' \neq a''$ — симметричные. Тогда

$$\begin{array}{rcl} & & a' * a * a'' \\ a' = & a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' & = a'' \end{array}$$

□

Алгебраическая структура

Множество S с одной или несколькими введенными на нем операциями называется *алгебраической структурой*.

Группа

Структура $G = (S; *)$ (т. е. множество S с введенной на нем алгебраической операцией $*$) называется **группой**, если

1) операция $*$ ассоциативна, т. е. для любых элементов $a, b, c \in S$ верно

$$(a * b) * c = a * (b * c);$$

2) существует нейтральный элемент относительно операции $*$, т. е. найдется такой элемент $e \in S$, что для каждого элемента $a \in S$ верно

$$a * e = e * a = a;$$

3) для каждого элемента $a \in S$ найдется симметричный к нему элемент $a' \in S$, т. е. такой что

$$a * a' = a' * a = e.$$

Группа

Если для группы $G = (S; *)$ дополнительно выполнено, что
4) операция $*$ коммутативна, т. е. для любых элементов $a, b \in S$ верно

$$a * b = b * a,$$

то такая группа называется **коммутативной**, или **абелевой**.

Правило сокращения

Предложение 3 (правило сокращения). *Пусть* $G = (S; *)$ — *группа. Тогда если для некоторых элементов* $a, b, c \in G$ *верно*

$$a * b = a * c \ (\text{или } b * a = c * a),$$

то $b = c$.

Правило сокращения

Доказательство. Пусть элемент $a' \in G$ симметричен относительно операции $*$ к элементу $a \in G$. Элемент $a' \in G$ найдется, т. к. G – группа. Тогда

$$a * b = a * c$$
$$a' * a * b = a' * a * c$$
$$b = e * b = (a' * a) * b = (a' * a) * c = e * c = c$$

□

Терминология

Общая	Аддитивная	Мультипликативная
$*$ операция	$+$ сложение	$\cdot$ умножение
e нейтральный	0 ноль	1 единица
a' симметричный	$-a$ противоположный	a^{-1} обратный
$\underbrace{a * a * \ldots * a}_{n}$	na	a^n степень

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

2. $S = \{e, a\}$; $x * e = e * x = x$, где $x = e, a$;
Чему равно $a * a =$?
Если $a * a = a$, то $a * a = a * e$ и $a = e$ — противоречие.
Значит, $a * a = e$.

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

2. $S = \{e, a\}$; $x * e = e * x = x$, где $x = e, a$;
Чему равно $a * a =$?
Если $a * a = a$, то $a * a = a * e$ и $a = e$ — противоречие.
Значит, $a * a = e$.

3. $S = \{e, a, b\}$;

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Перечисленные группы коммутативны.

Изоморфизм групп

Две группы $G_1 = (S_1; *)$ и $G_2 = (S_2; \circ)$ называются **изоморфными**, если найдется взаимно однозначное отображение

$$\varphi : S_1 \to S_2,$$

сохраняющее операцию, т. е. для любых элементов $a, b \in S_1$ верно

$$\varphi(a * b) = \varphi(a) \circ \varphi(b).$$

При этом взаимно однозначное отображение φ называется **изоморфизмом** групп G_1 и G_2.

Отметим, что перечисленные в п.п. 1–3 группы единственные с точностью до изоморфизма группы соответственно из одного, двух и трех элементов.

Свойства изоморфизма групп

Пусть $\varphi : S_1 \to S_2$ — изоморфизм групп $G_1 = (S_1; *)$ и $G_2 = (S_2; \circ)$. Тогда

1) $\varphi(e_1) = e_2$, где e_1, e_2 — соответственно нейтральные элементы групп G_1, G_2. В самом деле, если $a \in S_1$, то

$$\varphi(a) = \varphi(a * e_1) = \varphi(a) \circ \varphi(e_1),$$

откуда $\varphi(e_1) = e_2$.

2) $\varphi(a') = \varphi(a)'$, где $a' \in S_1, \varphi(a)' \in S_2$ — соответственно симметричные элементы к элементам $a \in S_1, \varphi(a) \in S_2$ групп G_1, G_2. В самом деле,

$$e_2 = \varphi(e_1) = \varphi(a * a') = \varphi(a) \circ \varphi(a'),$$

откуда $\varphi(a') = \varphi(a)'$.

Порядок группы

Группа $G = (S; *)$ называется **конечной**, если в множестве S конечное число элементов.

Если группа $G = (S; *)$ конечна, то число элементов в множестве S называется ее **порядком** и обозначается $|G|$.

Порядок элемента группы

Пусть $G = (S; *)$ — группа с нейтральным элементом e.

Для элемента $a \in G$ наименьшее натуральное число n (если оно существует), такое что

$$\underbrace{a * a * \ldots * a}_{n} = e,$$

называется его **порядком**.

Конечные коммутативные группы

Предложение 4. *Пусть* $G = (S; *)$ *— конечная коммутативная группа и* $e \in S$ *— ее нейтральный элемент. Тогда для любого элемента* $a \in S$ *верно* $\underbrace{a * \ldots * a}_{|G|} = a^{|G|} = e$.

Конечные коммутативные группы

Доказательство. Пусть $S = \{a_1, \ldots, a_n\}$, и $a \in S$. Рассмотрим элементы группы

$$a * a_1, \ a * a_2, \ \ldots, \ a * a_n.$$

Все эти элементы различны (почему?). И их ровно n. Значит, здесь перечислены все элементы группы.
Поэтому, с учетом коммутативности и ассоциативности операции $*$, получаем:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} (a * a_i) = a^{|G|} \prod_{i=1}^{n} a_i.$$

По правилу сокращения находим $a^{|G|} = e$.

□

Малая теорема Ферма

Следствие 4.1 (малая теорема Ферма). *Если p — простое число, то для каждого натурального числа a, $1 \leqslant a \leqslant p-1$, верно $a^{p-1} = 1 (\mathrm{mod}\ p)$.*

Доказательство. Пусть $S = \{1, 2, \ldots, p-1\}$ и $\cdot (\mathrm{mod}\ p)$ — операция умножения по модулю p чисел из S.

Несложно проверить, что $G = (S, \cdot (\mathrm{mod}\ p))$ — коммутативная группа порядка $(p-1)$ с нейтральным элементом $e = 1$.

Поэтому получаем, что $a^{p-1} = 1 (\mathrm{mod}\ p)$ для каждого $a \in S$.

□

Подгруппы

Пусть $G = (S; *)$ — группа, и $T \subseteq S$.

Если $H = (T; *)$ является группой, то она называется **подгруппой** группы $G = (S; *)$.

Если при этом $T \neq \{e\}$ и $T \neq S$, то подгруппа называется **собственной**.

Подгруппы

Предложение 5 (критерий подгруппы). *Пусть $G = (S; *)$ — группа и $T \subseteq S$. Тогда $H = (T; *)$ является группой в том и только в том случае, когда для любых элементов $a, b \in T$ верно $a * b' \in T$.*

Подгруппы

Доказательство. $\Leftarrow$. Проверим свойства группы.

1) ассоциативность операции $*$: т. к. G — группа;

2) существование нейтрального элемента e: если $a \in T$, то $a * a' = e \in T$;

3) для каждого элемента существование симметричного элемента: если $a \in T$, то $e * a' = a' \in T$;

4) алгебраичность операции $*$ для множества T: если $a, b \in T$, то по п. 3) $b' \in T$, и $a * (b')' = a * b \in T$.

$\square$

Подгруппы

Если $G = (S, \cdot)$ — мультипликативная группа и $a \in G$ — элемент порядка n в ней, то множество

$$T = \{a, a^2, \ldots, a^{n-1}, a^n = 1\}$$

с операцией $\cdot$ образует мультипликативную подгруппу $H = (T; \cdot)$ порядка n группы $G = (S; \cdot)$.

Циклическая группа

Мультипликативная группа называется **циклической**, если каждый из ее элементов является некоторой степенью выделенного элемента группы, который называется **образующим** элементом группы.

Группа с образующим элементом a обозначается как $\langle a \rangle$.

Если $G = (S; \cdot)$ — группа и $a \in S$, то подгруппа $H = \langle a \rangle$ — циклическая.

Смежные классы

Пусть $G = (S; *)$ — группа, а $H = (T; *)$, $T \subseteq S$, — ее подгруппа.

Определим на множестве S отношение R_H: если $a, b \in S$, то

$$R_H(a, b) \Leftrightarrow \exists h \in H : a * h = b.$$

Заметим, что отношение R_H можно задавать так: если $a, b \in S$, то

$$R_H(a, b) \Leftrightarrow a' * b \in H,$$

где элемент a' симметричен элементу a в группе G.

Отношение эквивалентности по подгруппе

Предложение 6. *Отношение R_H является отношением эквивалентности на множестве S.*

Отношение эквивалентности по подгруппе

Доказательство. Свойства отношения эквивалентности.

1) Рефлексивность. Для каждого $a \in S$ выберем $e \in H$ — нейтральный элемент. Тогда $a * e = a$, поэтому $R_H(a, a)$.

2) Симметричность. Пусть для элементов $a, b \in S$ верно $R_H(a, b)$, т. е. найдется такой элемент $h \in H$, что $a * h = b$. Тогда

$$a * h = b,\ \ a * h * h' = b * h', a = b * h'.$$

Т. к. H — группа, $h' \in H$. Поэтому $R_H(b, a)$.

Отношение эквивалентности по подгруппе

3) Транзитивность. Пусть для элементов $a, b, c \in S$ верно $R_H(a, b)$ и $R_H(b, c)$, т. е. найдутся такие элементы $h_1 \in H$ и $h_2 \in H$, что $a * h_1 = b$ и $b * h_2 = c$. Тогда

$$a * (h_1 * h_2) = (a * h_1) * h_2 = b * h_2 = c.$$

Т. к. H — группа, $h_1 * h_2 = h \in H$. Поэтому $R_H(a, c)$.

□

Смежные классы

Класс эквивалентности множества S по отношению эквивалентности R_H называется **левым смежным классом** группы G по подгруппе H.

Обозначение: левый смежный класс, порожденный элементом $a \in S$:

$$aH = \{b \in S \mid \exists h \in H : a * h = b\}.$$

В аддитивной символике обозначение:

$$a + H = \{b \in S \mid \exists h \in H : a + h = b\}.$$

Смежные классы

Напомним, что классы эквивалентности или не пересекаются, или совпадают. Поэтому отношение R_H **разбивает** множество S на левые смежные классы. Такое разбиение называется **левосторонним разложением группы** G **по подгруппе** H.

Аналогично вводится **правостороннее разложение группы** G **по подгруппе** H.

Смежные классы

Пусть $H = \{h_1 = e, h_2, \ldots, h_m\}$ — конечная подгруппа группы $G = (S; *)$.

Тогда для каждого элемента $a \in S$ левый смежный класс

$$aH = \{a * h_1, a * h_2, \ldots, a * h_m\}$$

также содержит конечное число элементов.

Смежные классы

Предложение 7. *В каждом левом (правом) смежном классе группы по конечной подгруппе число элементов совпадает с порядком этой подгруппы.*

Смежные классы

Доказательство. Пусть $H = \{h_1 = e, h_2, \ldots, h_m\}$ — конечная подгруппа группы $G = (S; *)$.

Тогда для элемента $a \in S$ левый смежный класс aH состоит из элементов вида

$$a * h_1, a * h_2, \ldots, a * h_m.$$

Поэтому $|aH| \leqslant |H|$.

Предположим, что $|aH| < |H|$. т. е. найдутся такие элементы $h_i, h_j \in H$, $h_i \neq h_j$, что

$$a * h_i = a * h_j.$$

Тогда по правилу сокращения $h_i = h_j$ — противоречие. Следовательно, $|aH| = |H|$.

□

Теорема Лагранжа

Следствие 7.1 (теорема Лагранжа). *Порядок каждой подгруппы конечной группы делит порядок группы.*

Доказательство. Пусть $G = (S; *)$ — конечная группа, а H — ее подгруппа. Рассмотрим левостороннее разложение группы G по подгруппе H. Тогда все левые смежные классы равномощны, и их мощность равна порядку подгруппы H. Каждый элемент множества S лежит ровно в одном левом смежном классе, поэтому

$$|G| = |H| \cdot \{\text{число левых смежных классов}\}.$$

Поэтому $|H| \mid |G|$.

□

Порядок элемента конечной группы

Следствие 7.2. *Порядок каждого элемента конечной группы делит порядок группы.*

Доказательство. Пусть $G = (S; *)$ — конечная группа, и $a \in S$ — какой-то ее элемент. Достаточно рассмотреть циклическую ее подгруппу $H = \langle a \rangle$ с образующим элементом $a \in S$. Тогда порядок элемента a равен порядку группы H, а значит, делит порядок группы G.

□

Индекс подгруппы в группе

Число смежных классов конечной группы G по подгруппе называется **индексом подгруппы H в группе G** и обозначается как $(G : H)$.

Следствие 7.3. *Порядок конечной группы равен произведению порядка какой-то ее подгруппы на индекс этой подгруппы в группе, т. е.*

$$|G| = |H| \cdot (G : H),$$

где G — конечная группа, а H — ее подгруппа.

Пример: все неизоморфные группы из 5 элементов

Пример. Найдем все возможные группы из 5 элементов (с точностью до изоморфизма).

Решение. Пусть $|S| = 5$, и $G = (S; *)$ — группа.

Если $a \in S$, то порядок элемента a делит порядок группы, т. е. делит 5.
Т. е. каждый элемент этой группы имеет порядок или 1, или 5.
Но порядок 1 может иметь только нейтральный элемент e.
Значит, все другие элементы имеют порядок 5. Т. е. эта группа циклическая, и

$$S = \{a,\ a^2,\ a^3,\ a^4,\ a^5 = e\}.$$

Следовательно, с точностью до изоморфизма существует только одна группа из 5 элементов, и она является циклической.

Нормальные подгруппы

Пусть $G = (S; *)$ — группа, а $H = (T; *)$, $T \subseteq S$, — ее подгруппа.

Подгруппа H называется **нормальной подгруппой** (или **нормальным делителем**) группы G, если для каждого элемента $a \in S$ его левые и правые смежные классы совпадают, т. е. если

$$\forall a \in S \ aH = Ha.$$

Заметим, что каждая подгруппа коммутативной группы нормальна.

Если подгруппа H нормальна в группе G, то левостороннее и правостороннее разложения группы G по подгруппе H совпадают.

Критерий нормальности подгруппы

Предложение 8 (критерий нормальности подгруппы). *Подгруппа $H = (T; *)$ является нормальной подгруппой группы $G = (S, *)$ тогда и только тогда, когда для каждого элемента $a \in S$ для любого элемента $h \in H$ верно*

$$a' * h * a \in H,$$

где элемент a' симметричен к элементу a в группе G.

Критерий нормальности подгруппы

Доказательство.
$\Rightarrow$. Если для каждого элемента $a \in S$ верно $aH = Ha$, то для любого элемента $h \in H$ найдется такой элемент $h_1 \in H$, что

$$a * h_1 = h * a.$$

Получаем:

$$a' * (a * h_1) = a' * (h * a),\ h_1 = a' * h * a.$$

Т. е. $a' * h * a \in H$.

Критерий нормальности подгруппы

Доказательство.
$\Leftarrow$. Если для каждого элемента $a \in S$ для любого элемента $h \in H$ верно $a' * h * a \in H$, то

$$a' * h * a = h_1 \in H.$$

Получаем:

$$a * (a' * h * a) = a * h_1, \ \ h * a = a * h_1.$$

т. е. $Ha \subseteq aH$.
Включение $aH \subseteq Ha$ доказывается аналогично, рассматривая произведение $(a')' * h * a'$, $a' \in S$.
Поэтому $aH = Ha$.

$\square$

Фактор-группа

Пусть $G = (S; *)$ — группа и $N = (T; *)$ — ее **нормальная** подгруппа.

Рассмотрим разложение группы G по нормальной подгруппе N.

Введем операцию умножения смежных классов: если элементы $a, b \in S$, то

$$(aN)(bN) = (ab)N.$$

Фактор-группа

Предложение 9. *Если N — нормальная подгруппа группы $G = (S; *)$, то ввведенная выше операция умножения смежных классов корректна*.

Доказательство. Пусть $a, b \in S$ и $a_1 \in aN$ и $b_1 \in bN$. Докажем, что

$$(a_1N)(b_1N) = (aN)(bN) = (ab)N,$$

т. е. что результат операции не зависит от выбора элементов, по которым строятся смежные классы.

Фактор-группа

Доказательство. Пусть $h \in N$. Покажем, что найдется элемент $x \in N$, являющийся решением уравнения

$$a * b * h = a_1 * b_1 * x.$$

Т. к. $a_1 \in aN$, $b_1 \in bN$, найдутся такие элементы $h_1, h_2 \in N$, что $a_1 = a * h_1$, $b_1 = b * h_2$. Тогда

$$a * b * h = a_1 * b_1 * x = a * h_1 * b * h_2 * x, \;\; b * h = h_1 * b * h_2 * x.$$

Т. к. N — нормальная подгруппа, найдется такой элемент $h_3 \in N$, что $h_1 * b = b * h_3$. Поэтому

$$b * h = h_1 * b * h_2 * x = b * h_3 * h_2 * x, \;\; h = h_3 * h_2 * x.$$

Значит, $x = h_2' * h_3' * h \in N$, где элементы $h_2', h_3' \in N$ симметричны соответственно к элементам $h_2, h_3 \in N$.

Фактор-группа

Предложение 10. *Если N — нормальная подгруппа группы $G = (S; *)$, то множество смежных классов группы G по подгруппе N с операцией их умножения образует группу.*

Фактор-группа

Доказательство. Свойства группы.

1) Ассоциативность операции умножения: следует из ассоциативности операции $*$ в группе G.

2) Существование нейтрального элемента: $eN = N$, где $e \in S$ — нейтральный элемент группы G.

3) Для каждого элемента aN, где $a \in S$, существование симметричного элемента: $a'N$, где элемент $a' \in S$ симметричен к элементу a в группе G.

$\square$

Фактор-группа

Группа смежных классов группы G по ее нормальной подгруппе N с операцией их умножения называется **фактор-группой** группы G по подгруппе N и обозначается G/N.

Фактор-группа

Следствие 10.1. *Порядок фактор-группы G/N конечной группы G по ее нормальной подгруппе N равен индексу подгруппы N в группе G, т. е.*

$$|G/N| = (G : N) = \frac{|G|}{|N|}.$$

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Т. 1. С. 12–23.