Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 1

Полугруппы и группы: основные определения и примеры. Группы подстановок и группы матриц. Подгруппы. Порядок элемента и циклические подгруппы. Смежные классы и индекс подгруппы. Теорема Лагранжа и её следствия.

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 $(M, \circ)$.

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

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

Не все естественно возникающие операции ассоциативны. Например, если $M = \mathbb{N}$ и $a \circ b := a^b$, то

$$2^{(1^2)} = 2 \neq (2^1)^2 = 4.$$

Другой пример неассоциативной бинарной операции: $M = \mathbb{Z}$ и $a \circ b := a - b$ (проверьте!).

Полугруппу обычно обозначают $(S, \circ)$.

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 $a \in S$.

Во Франции полугруппа $(\mathbb{N}, +)$ является моноидом, а в России нет.

Замечание 1. Если в полугруппе есть нейтральный элемент, то он один. В самом деле, $e_1 \circ e_2 = e_1 = e_2$.

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

Упражнение 1. Докажите, что если обратный элемент существует, то он один.

Обратный элемент обозначается a^{-1}. Группу принято обозначать $(G, \circ)$ или просто G, когда понятно, о какой операции идёт речь. Обычно символ $\circ$ для обозначения операции опускают и пишут просто ab.

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

Если в случае произвольной группы G принято использовать мультипликативные обозначения для групповой операции — gh, e, g^{-1}, то в теории абелевых групп чаще используют аддитивные обозначения, т. е. $a + b$, 0, $-a$.

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

Порядок группы G обозначается $|G|$.

Приведём несколько серий примеров групп.

1) Числовые аддитивные группы: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_n, +)$.

2) Числовые мультипликативные группы: $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$, $(\mathbb{Z}_p \setminus \{\overline{0}\}, \times)$, p — простое.

3) Группы матриц: $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}$; $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) = 1\}$.

4) Группы подстановок: симметрическая группа S_n — все подстановки длины n, $|S_n| = n!$;

знакопеременная группа A_n — чётные подстановки длины n, $|A_n| = n!/2$.

Упражнение 2. Докажите, что группа S_n коммутативна $\Leftrightarrow n \leqslant 2$, а A_n коммутативна $\Leftrightarrow n \leqslant 3$.

Определение 7. Подмножество H группы G называется *подгруппой*, если H непусто и $ab^{-1} \in H$ для любых $a, b \in H$.

Упражнение 3. Проверьте, что H является подгруппой тогда и только тогда, когда выполнены следующие три условия: (1) $ab \in H$ для любых $a, b \in H$; (2) $e \in H$; (3) $a^{-1} \in H$ для любого $a \in H$.

В каждой группе G есть *несобственные* подгруппы $H = \{e\}$ и $H = G$. Все прочие подгруппы называются *собственными*. Например, чётные числа $2\mathbb{Z}$ образуют собственную подгруппу в $(\mathbb{Z}, +)$.

Предложение 1. *Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторого целого неотрицательного k.*

Доказательство. Пусть H — подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, положим $k = 0$. Иначе пусть k — наименьшее натуральное число, лежащее в H (почему такое есть?). 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 $H = k\mathbb{Z}$. □

Определение 8. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порождённой элементом g, называется подмножество $\{g^n \mid n \in \mathbb{Z}\}$ в G.

Циклическая подгруппа, порождённая элементом g, обозначается $\langle g \rangle$. Элемент g называется *порождающим* или *образующим* для подгруппы $\langle g \rangle$. Например, подгруппа $2\mathbb{Z}$ в $(\mathbb{Z}, +)$ является циклической, и в качестве порождающего элемента в ней можно взять $g = 2$ или $g = -2$. Другими словами, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 9. 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 $\mathrm{ord}(g)$. Заметим, что $\mathrm{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

Следующее предложение объясняет, почему для порядка группы и порядка элемента используется одно и то же слово.

Предложение 2. *Пусть G — группа и $g \in G$. Тогда* $\mathrm{ord}(g) = |\langle g \rangle|$.

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

Определение 10. Группа G называется *циклической*, если найдётся такой элемент $g \in G$, что $G = \langle g \rangle$.

Ясно, что любая циклическая группа коммутативна и не более чем счётна. Примерами циклических групп являются группы $(\mathbb{Z}, +)$ и $(\mathbb{Z}_n, +)$, $n \geq 1$.

Перейдем ещё к одному сюжету, связанному с парой группа–подгруппа.

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

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

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

Доказательство. Предположим, что $g_1H \cap g_2H \neq \varnothing$, 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 $gH = \{gh; h \in H\}$, 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 $|gH| = |H|$. □

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 $[G : H]$.

Теорема Лагранжа. Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

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

Доказательство. Каждый элемент группы G лежит в (своём) левом смежном классе по подгруппе H, разные смежные классы не пересекаются (лемма 1) и каждый из них содержит по $|H|$ элементов (лемма 2). □

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

Следствие 2. *Пусть G — конечная группа и $g \in G$. Тогда $\mathrm{ord}(g)$ делит $|G|$.*

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

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

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

Следствие 4 (Малая теорема Ферма)**.** *Пусть $\overline{a}$ — ненулевой вычет по простому модулю p. Тогда*

$$\overline{a}^{p-1} = \overline{1}.$$

Доказательство. Вытекает из следствия 3, применённого к группе $(\mathbb{Z}_p \setminus \{\overline{0}\}, \times)$. □

Следствие 5. *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 $G = \langle g \rangle$. □

Наряду с левым смежным классом можно определить *правый смежный класс* элемента g группы G по подгруппе H:

$$Hg = \{hg \mid h \in H\}.$$

Повторяя доказательство теоремы Лагранжа для правых смежных классов, мы получим, что для конечной группы G число правых смежных классов по подгруппе H равно числу левых смежных классов и равно $|G|/|H|$. В то же время равенство $gH = Hg$ выполнено не всегда. Разумеется, оно выполнено, если группа G абелева. Подгруппы H (неабелевых) групп G, для которых $gH = Hg$ выполнено для любого $g \in G$, будут изучаться в следующей лекции.

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 4, § 1,3,5)
[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 4, § 1-2)
[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 1, § 2)
[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 13, § 54-56)