

Алгебра Лекции

Дима Трушин
2024

Содержание

1	Бинарные операции	2
1.1	Определения	2
1.2	Свойства	3
1.2.1	Ассоциативность	3
1.2.2	Нейтральный элемент	4
1.2.3	Обратный элемент	4
1.2.4	Коммутативность	5
2	Группы	5
2.1	Определение	5
2.2	Мультипликативная и аддитивная нотации	6
2.3	Подгруппы	7
2.4	Циклические группы	7
2.5	Смежные классы	11
2.6	Теорема Лагранжа	12

1 Бинарные операции

В математике часто изучаются разные структуры. Обычно это множества снабженные дополнительной структурой. В алгебре обычно множества снабжаются разного рода операциями. Простейший тип операций – бинарные операции, то есть операции с двумя аргументами. Давайте обсудим какие бывают бинарные операции и после перейдем к определению самой простой алгебраической структуры – группы.

1.1 Определения

Определение 1. Пусть X – некоторое множество. Бинарная операция на X – это отображение $\circ: X \times X \rightarrow X$ по правилу $(x, y) \mapsto x \circ y$ для всех $x, y \in X$.

В этом случае \circ – это имя операции. Проще говоря, операция – это правило, которое съедает два элемента из X и выплевывает один новый элемент, называемый $x \circ y$, из того же множества X . Новый элемент $x \circ y$ обычно называется произведением элементов x и y .¹

Обратите внимание, что у бинарных операций есть функциональный стиль обозначения, когда имя операции пишется не между аргументами, а в виде имени функции перед аргументами. Давайте я повторю определение операции в функциональном стиле.

Определение 2. Пусть X – некоторое множество. Бинарная операция на X – это отображение $\mu: X \times X \rightarrow X$ по правилу $(x, y) \mapsto \mu(x, y)$ для всех $x, y \in X$.

Это не новое определение, это всего лишь переобозначение предыдущего. Я буду предпочитать операторное обозначение.

Примеры 3. Бинарные операции:

1. Сложение целых чисел. В операторной форме

$$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

В функциональной форме

$$\text{add}: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto \text{add}(m, n) = m + n$$

Так как мы привыкли к сложению в форме $m + n$, мы хотим, чтобы общее определение было похоже на привычную нам запись. С другой стороны, многие языки программирования допускают оба вида нотаций. Но по сути $\text{add}(m, n)$ и $m + n$ это одно и то же.

2. Умножение целых чисел. В операторной форме

$$\cdot: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

В функциональном стиле

$$\text{mult}: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto \text{mult}(m, n) = m \cdot n$$

3. Максимум целых чисел. В операторной форме

$$\vee: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m \vee n$$

В функциональной форме

$$\text{max}: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto \text{max}(m, n) = m \vee n$$

На всякий случай поясню, что $\text{max}(m, n) = m \vee n$, то лишь разные обозначения максимума.

¹Операция может быть какой угодно, например, на множестве целых чисел можно рассматривать сложение, взятие максимума, или что-либо другое, но с абстрактной точки зрения результат операции все равно называется произведением элементов. Не забывайте, что математика – это искусство обозначать одинаковые вещи по-разному и разные вещи одинаково.

4. Минимум целых чисел. В операторной форме

$$\wedge: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m \wedge n$$

В функциональной форме

$$\min: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto \min(m, n) = m \wedge n$$

Как и выше $\min(m, n) = m \wedge n$ это разные обозначения минимума.

5. Просто случайная дурацкая бинарная операция на целых числах

$$\phi: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m^2 - n^2$$

Давайте резюмируем, что бинарная операция на X – это любое отображение вида $f: X \times X \rightarrow X$. И вы вольны задать его как вам вздумается по любому правилу. Но разные операции будут иметь разные свойства, какие-то операции будут лучше, чем другие. Давайте теперь обсудим какие же есть свойства у операций.

1.2 Свойства

Можно рассматривать множество различных свойств операций. Я хочу обсудить лишь те, которые нам понадобятся в дальнейшем для определения группы.

1.2.1 Ассоциативность

Определение 4. Операция $\circ: X \times X \rightarrow X$ называется ассоциативной, если для любых элементов $x, y, z \in X$ выполнено $(x \circ y) \circ z = x \circ (y \circ z)$.

Если у вас есть бинарная операция \circ на множестве X , то вы можете посчитать произведение трех элементов x, y, z двумя разными способами:

- сначала посчитаем произведение $w = x \circ y$ и потом вычислим $w \circ z = (x \circ y) \circ z$.
- сначала посчитаем произведение $u = y \circ z$ и потом вычислим $x \circ u = x \circ (y \circ z)$.

Если операция взята произвольно, то может случиться, что эти два способа дают разные результаты для каких-то значений x, y и z . Ассоциативность означает, что не важен порядок, в котором вы вычисляете операции. Кроме того, если $(x \circ y) \circ z = x \circ (y \circ z)$ для всех $x, y, z \in X$, то на самом деле не имеет значения, как вы расставляете скобки в произвольных произведениях. Например, все следующие выражения равны $(x \circ y) \circ (z \circ w)$, $x \circ (y \circ (z \circ w))$ and $((x \circ y) \circ z) \circ w$, а значит мы можем убрать все скобки и просто записать $x \circ y \circ z \circ w$. Поэтому для ассоциативных операций обычно не используют скобки, так как они не существенны.

Примеры 5. Ниже примеры ассоциативных и не ассоциативных операций.

1. Целочисленное сложение ассоциативно.

$$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Если $m, n, k \in \mathbb{Z}$, то мы знаем, что $(m + n) + k = m + (n + k)$.

2. Вычитание целых чисел не ассоциативно.

$$-: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Тогда равенство $(m - n) - k = m - (n - k)$ не выполняется для всех целых чисел. Действительно, если взять $m = n = 0$ и $k = 1$, то левая часть равенства будет -1 , а правая -1 . Так что, $(0 - 0) - 1 \neq 0 - (0 - 1)$.

1.2.2 Нейтральный элемент

Определение 6. Пусть $\circ: X \times X \rightarrow X$ – некоторая операция на X . Элемент $e \in X$ называется нейтральным если для каждого элемента $x \in X$ выполнены равенства $x \circ e = x$ и $e \circ x = x$.

По простому, нейтральный элемент $e \in X$ – это такой элемент, который ничего не меняет по умножению в смысле операции.

Примеры 7. Нейтральный элемент может существовать, а может и не существовать.

1. Целочисленное сложение имеет нейтральный элемент.

$$+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Ясно, что элемент $e = 0$ удовлетворяет всем требованиям на нейтральный элемент. Действительно, для всех $m \in \mathbb{Z}$ имеем $m + 0 = m$ и $0 + m = m$.

2. Целочисленное вычитание не имеет нейтрального элемента.

$$-: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Давайте покажем, что нет элемента $e \in \mathbb{Z}$ такого, что $e - m = m$ для всех $m \in \mathbb{Z}$. Действительно, если такой e существует, то $e = 2m$ для каждого $m \in \mathbb{Z}$. Но это не возможно, поскольку для $m = 0$, $e = 0$ а для $m = 1$, $e = 2$, противоречие. С другой стороны, отметим, что $m - 0 = m$ для всех $m \in \mathbb{Z}$. То есть 0 является нейтральным только с одной стороны для вычитания.

Последний пример показывает, что вообще говоря не достаточно проверять только одно из условий $x \circ e = x$ или $e \circ x = x$. Это очень частая ошибка. Постарайтесь не забыть оба условия.

Правильный вопрос, которым теперь надо задаться: а сколько нейтральных элементов может быть? Правильный ответ – не более одного. Давайте покажем это.

Утверждение 8. Пусть X – некоторое множество и $\circ: X \times X \rightarrow X$ – бинарная операция. Тогда существует не более одного нейтрального элемента.

Доказательство. Если нейтральных элементов нет, то и доказывать нечего. Пусть теперь e и e' – два произвольных нейтральных элемента. Мы должны показать, что они равны. Рассмотрим произведение $e \circ e'$. Так как e является нейтральным элементом, $e \circ x = x$ для любого $x \in X$. В частности при $x = e'$ мы получим, что $e \circ e' = e'$. С другой стороны, так как e' является нейтральным элементом, то $x \circ e' = x$ для любого $x \in X$. И значит в частности при $x = e$ имеем $e \circ e' = e$. То есть $e = e \circ e' = e'$. \square

1.2.3 Обратный элемент

Я хочу начать с замечания, что это свойство зависит от предыдущего. А именно, для того чтобы говорить об обратных элементах необходимо, чтобы для операции существовал нейтральный элемент. Если же нейтрального элемента нет, то нет и способа говорить об обратимых элементах.

Определение 9. Пусть $\circ: X \times X \rightarrow X$ – некоторая операция с нейтральным элементом $e \in X$. Элемент $y \in X$ называется обратным к элементу $x \in X$, если выполнено $x \circ y = e$ и $y \circ x = e$.

Я напомним, что нейтральный элемент единственный если существует. Потому элемент e корректно определен в равенствах выше.

Правильный вопрос, которым надо задаться: а сколько может быть обратных элементов для заданного элемента $x \in X$? Оказывается, что не больше одного, если операция ассоциативна.

Утверждение 10. Пусть $\circ: X \times X \rightarrow X$ – некоторая ассоциативная бинарная операция с нейтральным элементом $e \in X$. Тогда, для любого $x \in X$ существует не более одного обратного элемента.

Доказательство. Давайте зафиксируем элемент $x \in X$. Если для него нет обратного, то и доказывать нечего. Теперь предположим, что y_1 и y_2 – это два обратных элемента к x . Последнее означает, что выполнены равенства

$$\begin{cases} x \circ y_1 = e \\ y_1 \circ x = e \end{cases} \quad \text{и} \quad \begin{cases} x \circ y_2 = e \\ y_2 \circ x = e \end{cases}$$

Теперь рассмотрим произведение $y_1 \circ x \circ y_2$. Так как \circ ассоциативна, то расстановка скобок не имеет значения, то есть $(y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2)$. Если посчитать левую часть, то получим:

$$(y_1 \circ x) \circ y_2 = e \circ y_2 = y_2$$

А для правой части имеем:

$$y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$$

Значит $y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1$ и все доказано. \square

Так как в общем случае существует не более одного обратного для элемента x , то его принято обозначать через x^{-1} .

Примеры 11. 1. Предположим, что операция – сложение целых чисел.

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Нейтральный элемент у нас 0. Если $n \in \mathbb{Z}$, то обратный к нему будет $-n$. Действительно, $n + (-n) = 0$ и $(-n) + n = 0$. Значит любой элемент имеет обратный для этой операции.

2. Предположим, что операция – это умножение целых чисел

$$\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

Нейтральный элемент – 1. Если $n = 1$, то его обратный будет тоже 1. Если $n = -1$, то его обратный будет -1 . Если же $n \neq \pm 1$, то обратного не существует в \mathbb{Z} . Потому только два элемента обратимы для этой операции.

1.2.4 Коммутативность

Определение 12. Бинарная операция $\circ : X \times X \rightarrow X$ называется коммутативной если для любых $x, y \in X$ выполнено $x \circ y = y \circ x$.

То есть коммутативность означает, что нам не важен порядок операндов в операции.

Примеры 13. 1. Целочисленное сложение коммутативно.

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Действительно, для любых $m, n \in \mathbb{Z}$, мы имеем $m + n = n + m$.

2. Целочисленное вычитание не коммутативно.

$$- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Коммутативность означает равенство $m - n = n - m$ для всех целых m, n . Ясно, что это не выполнено уже в случае $m = 0$ и $n = 1$.

2 Группы

2.1 Определение

Теперь мы готовы к тому, чтобы дать определение одного из самых важных в алгебре объектов – группы. Прежде чем сделать это, я хочу пояснить, что мы встретим много абстрактных определений в будущем и все они будут сотканы по единому шаблону. Давайте я проясню этот шаблон в начале. В любом абстрактном определении есть две части. В первой части говорится какие данные нам даны. А во второй части говорится каким аксиомам эти данные должны удовлетворять.²

Определение 14. Определение группы

- **Данные:**

²Если проводить аналогию с программированием, то первая часть описывает интерфейс, а вторая часть – это контракт на интерфейс.

1. G – множество.
2. Операция $\circ: G \times G \rightarrow G$.

• **Аксиомы:**

1. Операция \circ ассоциативна.
2. Операция \circ обладает нейтральным элементом.
3. Каждый элемент $x \in G$ имеет обратный.

В этом случае мы будем говорить, что пара (G, \circ) является группой. Чтобы упростить обозначения, мы будем обычно говорить, что просто G является группой, подразумевая, что на G задана некоторая фиксированная операция. Если в дополнение к аксиомам выше выполнена следующая аксиома

4. Операция \circ коммутативна.

То группа G называется абелевой или просто коммутативной.

Если коротко, то группа – это множество с «хорошей» операцией. Здесь слово «хорошая» означает, что нам не важно как расставлять скобки, у нас есть нейтральный элемент и на любой элемент можно поделить. Если же в дополнение ко всему не важно в каком порядке стоят аргументы операции, то группа называется абелевой.

- Примеры 15.*
1. Целые числа по сложению $(\mathbb{Z}, +)$ образуют абелеву группу. Действительно, операция $+$ ассоциативна, нейтральный элемент – 0, для каждого числа n есть его обратный $-n$ и порядок аргументов в сложении не важен $n + m = m + n$. Мы обычно называем эту группу просто \mathbb{Z} подразумевая, что операция обязательно сложение.
 2. Целые числа по умножению (\mathbb{Z}, \cdot) группу не образуют. Мы знаем, что операция ассоциативна и есть нейтральный элемент 1. И мы уже проверяли, что только ± 1 являются обратимыми элементами.
 3. Не нулевые вещественные числа по умножению (\mathbb{R}^*, \cdot) образуют абелеву группу. Действительно, умножение ассоциативно. Нейтральным элементом будет 1, для всякого элемента x обратным будет $1/x$, и порядок аргументов в умножении не важен $xy = yx$.
 4. Пусть n – положительное целое, тогда множество $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ с операцией $a + b \pmod{n}$ является абелевой группой. Для простоты операция сложения по модулю n так же обозначается просто $+$.
 5. Пусть n – положительное целое. Положим $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid (m, n) = 1\}$ (множество всех чисел из \mathbb{Z}_n взаимно простых с n), а операцию зададим как $a \cdot b \pmod{n}$. В этом случае мы так же получим абелеву группу. Для простоты операция в \mathbb{Z}_n^* обозначается как операция умножения \cdot .

2.2 Мультипликативная и аддитивная нотации

В определении группы G мы обозначали операцию \circ . Если надо использовать произведение нескольких элементов, то нам приходится писать $x \circ y \circ z \circ w$. Это не очень удобно. Вместо этого есть два более привычных стиля. А именно, давайте будем обозначать операцию как умножение \cdot или как сложение $+$. Тогда получаются две разные нотации: мультипликативная и аддитивная.

	Мультипликативная	Аддитивная
Операция	$\cdot: G \times G \rightarrow G$	$+: G \times G \rightarrow G$
На элементах	$(x, y) \mapsto xy$	$(x, y) \mapsto x + y$
Нейтральный элемент	1	0
Обратный элемент	x^{-1}	$-x$
Степень элемента	$x^n = \underbrace{x \cdot \dots \cdot x}_n$	$nx = \underbrace{x + \dots + x}_n$

Обычно мультипликативная нотация используется в случае неабелевых групп или когда свойство коммутативности вообще говоря не известно. А аддитивная нотация зарезервирована сугубо для абелевых групп. Я буду в основном использовать мультипликативную нотацию.

Я подчеркну, что указанные нотации – это всего лишь два разных способа обозначать операцию \circ , а не какие-то новые специальные операции. То есть мы выбираем обозначение для \circ в виде \cdot или $+$ в зависимости от наших предпочтений. Не надо путать эти обозначения с операциями сложения и умножения целых чисел. В случае произвольной группы G путаницы быть не должно, потому что там нет никаких заранее заданных операций сложения и умножения. Однако, если мы работаем с целыми числами (вещественными, рациональными, комплексными и т.д.), то операции $+$ и \cdot обозначают обычные сложение и умножение.

2.3 Подгруппы

Определение 16. Пусть G – некоторая группа.³ Определим подгруппу H в группе G следующим образом.

• **Данные:**

1. Подмножество $H \subseteq G$.

• **Аксиомы:**

1. Нейтральный элемент 1 группы G принадлежит H .
2. Если $x, y \in H$, то $xy \in H$.
3. Если $x \in H$, то $x^{-1} \in H$.

В этом случае, мы говорим, что H – подгруппа в группе G .

Стоит отметить, что если H – подгруппа в группе (G, \cdot) , то \cdot можно ограничить на H и получится операция на H . В этом случае (H, \cdot) удовлетворяет всем аксиомам группы. Таким образом подгруппа H сама является группой относительно той же самой операции (или точнее относительно ограничения операции), что была на группе G .

Примеры 17. Пусть $G = \mathbb{Z}$ по сложению.

1. Если $H \subseteq \mathbb{Z}$ – подмножество четных чисел $H = 2\mathbb{Z}$, то H является подгруппой.
2. Если $H \subseteq \mathbb{Z}$ – подмножество нечетных чисел $H = 1 + 2\mathbb{Z}$, то H не является подгруппой. В этом случае H не содержит нейтрального элемента 0 и не замкнуто относительно операции сложения.

2.4 Циклические группы

Пусть G – некоторая группа и $g \in G$ – ее элемент. Тогда мы можем определить целочисленные степени элемента g по следующим правилам.

Мультипликативная нотация	Аддитивная нотация
$g^n = \begin{cases} \underbrace{g \cdot \dots \cdot g}_n, & n > 0 \\ 1, & n = 0 \\ \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{-n}, & n < 0 \end{cases}$	$ng = \begin{cases} \underbrace{g + \dots + g}_n, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-g) + \dots + (-g)}_{-n}, & n < 0 \end{cases}$

Утверждение 18. Пусть G – некоторая группа. Тогда

1. Для любых $x, y \in G$ выполнено $(xy)^{-1} = y^{-1}x^{-1}$.
2. Для любого $g \in G$ верно $(g^{-1})^n = (g^n)^{-1} = g^{-n}$.
3. Для любого $g \in G$ и любых $n, m \in \mathbb{Z}$ верно $g^n g^m = g^{n+m}$.

Доказательство. 1) Нам надо показать, что $(xy)^{-1} = y^{-1}x^{-1}$. С психологической точки зрения удобно обозначить $y^{-1}x^{-1}$ через z . Если мы покажем, что $(xy)z = z(xy) = 1$, то это будет означать, что $z = (xy)^{-1}$ по определению. Теперь посчитаем

$$(xy)z = xy z = xy y^{-1} x^{-1} = x x^{-1} = 1$$

³Строго говоря (G, \cdot) , но я буду использовать более короткие обозначения.

Аналогично делается и второе равенство.

2) Сначала покажем первое равенство. Давайте применим предыдущее свойство несколько раз, получим

$$(g_1 \cdot \dots \cdot g_n)^{-1} = g_n^{-1} \cdot \dots \cdot g_1^{-1}, \text{ whenever } g_1, \dots, g_n \in G$$

При подстановке $g_1 = \dots = g_n = g$, получим нужное равенство для $n > 0$.

Если $n = 0$, то по определению $(g^{-1})^0 = 1$. С другой стороны, $(g^0)^{-1} = 1^{-1} = 1$ потому что обратный к 1 есть 1.

Если $n < 0$, то по определению

$$(g^{-1})^n = \underbrace{(g^{-1})^{-1} \cdot \dots \cdot (g^{-1})^{-1}}_{-n}$$

С другой стороны

$$(g^n)^{-1} = \underbrace{(g^{-1} \cdot \dots \cdot g^{-1})^{-1}}_{-n} = \underbrace{(g^{-1})^{-1} \cdot \dots \cdot (g^{-1})^{-1}}_{-n}$$

где последнее равенство берется из предыдущего пункта утверждения.

Теперь надо проверить второе равенство. В случае $n > 0$ имеем по определению

$$(g^{-1})^n = \underbrace{(g^{-1} \cdot \dots \cdot g^{-1})}_n \text{ и } g^{-n} = \underbrace{(g^{-1} \cdot \dots \cdot g^{-1})}_n$$

Значит левая часть равна правой. Если $n = 0$, то обе части равны 1. Теперь рассмотрим $n < 0$. Для удобства изменим степень с n на $-n$ и можно считать, что $n > 0$. Получаем

$$(g^{-1})^{-n} = \underbrace{((g^{-1})^{-1} \cdot \dots \cdot (g^{-1})^{-1})}_n \text{ и } g^{-(-n)} = \underbrace{(g \cdot \dots \cdot g)}_n$$

То есть теперь достаточно показать, что $(g^{-1})^{-1} = g$. А это делается по определению. Элемент g удовлетворяет равенствам $gg^{-1} = 1$ и $g^{-1}g = 1$, то есть g является обратным к g^{-1} , что и требовалось.

3) Мы должны рассмотреть следующие 4 случая:

1. $n \geq 0$ and $m \geq 0$.
2. $n < 0$ and $m \geq 0$.
3. $n \geq 0$ and $m < 0$.
4. $n < 0$ and $m < 0$.

Пусть у нас первый случай:

$$g^n g^m = \underbrace{g \cdot \dots \cdot g}_n \cdot \underbrace{g \cdot \dots \cdot g}_m = \underbrace{g \cdot \dots \cdot g}_{n+m} = g^{n+m}$$

Для удобства рассмотрим $g^{-n} g^m$ где $n > 0$ and $m \geq 0$ во втором случае. Тогда

$$g^{-n} g^m = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_n \cdot \underbrace{g \cdot \dots \cdot g}_m$$

Мы сокращаем множители в середине выражения. Если $n > m$, получим

$$\underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{n-m} = g^{-n+m}$$

Если $n < m$, имеем

$$\underbrace{g \cdot \dots \cdot g}_{m-n} = g^{m-n}$$

Если $n = m$ получается $1 = g^{m-n}$.

Третий случай по сути является вторым с переставленными множителями. Значит остается разобрать четвертый случай. Опять же для удобства будем считать, что нам даны g^{-n} и g^{-m} , где $n > 0$ и $m > 0$. Тогда

$$g^{-n} g^{-m} = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_n \cdot \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_m = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{n+m} = g^{-n-m}$$

Что и требовалось показать. □

Определение 19. Пусть G – группа и $g \in G$ – некоторый элемент. Тогда обозначим множество всех целых степеней g следующим образом

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} = \{g^k \mid k \in \mathbb{Z}\}$$

Данное подмножество удовлетворяет определению подгруппы в группе G .⁴ Эта группа называется циклической подгруппой порожденной g . Элемент g называется порождающим подгруппы $\langle g \rangle$.

В аддитивной нотации циклическая подгруппа имеет вид

$$\langle g \rangle = \{\dots, -2g, -g, 0, g, 2g, \dots\} = \{kg \mid k \in \mathbb{Z}\}$$

По построению $\langle g \rangle$ – это самая маленькая подгруппа в G содержащая элемент g .

Определение 20. Пусть G – некоторая группа. Если найдется элемент $g \in G$ такой, что $\langle g \rangle = G$, то группа G называется циклической.

Примеры 21. 1. Группа $(\mathbb{Z}, +)$ является циклической. Ее образующие 1 и -1 .

2. Группа $(\mathbb{Z}_n, +)$ является циклической.

3. Группа перестановок на n элементах S_n не является циклической при $n > 2$.

4. Группа $(\mathbb{R}, +)$ не является циклической.

Определение 22. Пусть G – некоторая группа и $g \in G$ – ее элемент. Порядок элемента g – это минимальное положительное целое число такое, что $g^n = 1$ и ∞ если такого числа нет. Порядок g обозначается $\text{ord } g$.

Замечания

- Обратите внимание, что $g = 1$ тогда и только тогда, когда $\text{ord } g = 1$.
- Если мы используем аддитивную нотацию, то есть будем обозначать операцию через $+$, то порядок $g \in G$ – это такое минимальное положительное целое n , что $ng = 0$.

Утверждение 23. Пусть G – некоторая группа и $g \in G$ ее элемент. Тогда есть два возможных случая

1. Все элементы g^n и g^m различны при различных $n, m \in \mathbb{Z}$.
2. Существует положительное целое n такое, что степени $1, g, g^2, \dots, g^{n-1}$ различны. Более того, степени повторяются по циклу, а именно в ряду

$$\underbrace{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots, g^{n-1}}_{\text{элементы } g^{kn}, g^{1+kn}, \dots, g^{n-1+kn} \text{ совпадают с элементами } 1, g, \dots, g^{n-1} \text{ для любого } k \in \mathbb{Z}. \text{ В частности, в этом случае}}$$

элементы $g^{kn}, g^{1+kn}, \dots, g^{n-1+kn}$ совпадают с элементами $1, g, \dots, g^{n-1}$ для любого $k \in \mathbb{Z}$. В частности, в этом случае

$$\langle g \rangle = \{1, g, \dots, g^{n-1}\}$$

При этом $n = \text{ord } g$.

Доказательство. Если $g^n \neq g^m$ для всех различных $m, n \in \mathbb{Z}$, то доказывать нечего, у нас первый случай.

Давайте предположим, что для каких-то $m \neq n \in \mathbb{Z}$ у нас выполнено равенство $g^n = g^m$. Можно считать, что $n > m$. Тогда умножим обе части равенства на g^{-m} и по правилам перемножения степеней получим $g^{n-m} = 1$. Значит для некоторого $n > 0$ имеем $g^n = 1$.

Рассмотрим минимальное положительное n такое, что $g^n = 1$. Я утверждаю, что все степени $1, g, \dots, g^{n-1}$ различны. Действительно, если $g^k = g^s$ для некоторых $k, s \in [0, n-1]$ и $k > s$, тогда $g^{k-s} = 1$. А это значит, что $k-s$ не ноль и строго меньше, чем n . Последнее противоречит выбору n .

Теперь проверим, что любая степень g^N совпадает со степенью из списка $1, g, \dots, g^{n-1}$. Для этого поделим N с остатком на n , получим $N = qn + r$, где $0 \leq r < n$. Тогда

$$g^N = g^{qn+r} = (g^n)^q g^r = g^r$$

Осталось лишь заметить, что выбранное нами n по определению является $\text{ord } g$. □

⁴Действительно, нейтральный элемент содержится в ней. Это множество замкнуто по умножению в силу свойства (3) предыдущего утверждения и в силу свойства (2) предыдущего утверждения с каждым элементом лежит его обратный.

Замечания

- Отметим, что n может быть равным 1 в случае, когда g совпадает с нейтральным элементом.
- Из предыдущего утверждения следует, что $\text{ord } g$ совпадает с количеством элементов в подгруппе $\langle g \rangle$.

Теперь я хочу описать все подгруппы в группе целых чисел по сложению.

Утверждение 24. *Всякая подгруппа H группы \mathbb{Z} , точнее $(\mathbb{Z}, +)$, имеет вид $k\mathbb{Z}$ для некоторого неотрицательного целого k .*

Доказательство. В начале давайте проверим, что $k\mathbb{Z}$ действительно является подгруппой для любого k . Мы должны проверить три свойства подгруппы. Во-первых, $k\mathbb{Z}$ должно быть замкнуто по сложению. Но это ясно из определения. Во-вторых, нейтральный элемент, то есть ноль, должен быть в $k\mathbb{Z}$. Это так же ясно, так как $0 = k \cdot 0$. В-третьих, для любого $m = kh \in k\mathbb{Z}$, его обратный $-m = k(-h)$ так же в \mathbb{Z} , и мы проверили все три свойства.

Теперь покажем, что всякая подгруппа H имеет вид $k\mathbb{Z}$ с неотрицательным k . Если H содержит только нейтральный элемент 0, то $H = 0\mathbb{Z}$ и все доказано. Предположим H содержит ненулевой элемент. Возьмем произвольное ненулевое $n \in H$. Если $n < 0$, то $-n$ должно быть в H по определению подгруппы. А значит, мы можем считать, что H содержит некоторое положительное число. Пусть k – наименьшее положительное число в H . Давайте покажем, что $H = k\mathbb{Z}$.

В начале покажем, $H \supseteq k\mathbb{Z}$. Действительно, если $k \in H$, то по определению и вся подгруппа степеней k лежит в H . В аддитивной записи это значит, что

$$mk = \underbrace{k + \dots + k}_m \in H \text{ и } (-n)k = \underbrace{(-k) + \dots + (-k)}_n \in H \text{ для любых } m, n \in \mathbb{N}$$

Значит, $k\mathbb{Z} \subseteq H$.

Теперь покажем, что $H \subseteq k\mathbb{Z}$. Если $n \in H$ – произвольный элемент, давайте разделим его на k с остатком: $n = qk + r$, где $q \in \mathbb{Z}$ и $0 \leq r < k$. Мы уже знаем, что $qk \in k\mathbb{Z} \subseteq H$. Значит, $r = n - qk \in H$. Но r является неотрицательным целым числом из H меньшим k . Так как k является минимальным положительным целым в H , то остается только случай $r = 0$. А значит, $n = qk \in k\mathbb{Z}$ и все доказано. \square

Утверждение 25. *Всякая подгруппа H группы \mathbb{Z}_n , точнее $(\mathbb{Z}_n, +)$, имеет вид $k\mathbb{Z}_n = \{kh \in \mathbb{Z}_n \mid h \in \mathbb{Z}_n\}$ для некоторого положительного целого $k \mid n$.*

Доказательство. В начале проверим, что все числа кратные k для $k \mid n$ образуют подгруппу в \mathbb{Z}_n . Во-первых, покажем, что $k\mathbb{Z}_n$ замкнуто относительно сложения по модулю n . Допустим $m_1 = kh_1$ и $m_2 = kh_2$ – элементы $k\mathbb{Z}_n$. Тогда их сумма по модулю n – это остаток r такой, что $m_1 + m_2 = r \pmod{n}$. В этом случае

$$r = m_1 + m_2 + qn = kh_1 + kh_2 + qn$$

Так как k делит n все выражение целиком делится на k . Значит и r делится на k . Последнее означает, что $k\mathbb{Z}_n$ замкнуто относительно сложения по модулю n . Во-вторых, надо проверить, что нейтральный элемент содержится в $k\mathbb{Z}_n$. Это ясно из равенства $0 = k \cdot 0 \in k\mathbb{Z}_n$. В-третьих, если $m \in k\mathbb{Z}_n$ – не нулевой элемент, то его обратный имеет вид $n - m$. А так как n делится на k , то и $n - m$ делится на k , а значит лежит в $k\mathbb{Z}_n$. В случае $m = 0$ его обратный есть 0, а он лежит в $k\mathbb{Z}_n$. Потому для любого $k \mid n$, $k\mathbb{Z}_n$ является подгруппой в \mathbb{Z}_n .

Теперь давайте покажем, что любая подгруппа H в \mathbb{Z}_n совпадает с подгруппой вида $k\mathbb{Z}_n$ где $k \mid n$. Подгруппа H должна содержать нейтральный элемент 0. Если больше нет других элементов в H , то $H = \{0\} = n\mathbb{Z}_n$ и все доказано. Значит, мы можем предположить, что в H есть ненулевые элементы. Пусть k – наименьший положительный элемент в H . По определению циклическая подгруппа $k\mathbb{Z}_n$ лежит в H . Потому нам надо показать только обратное включение $H \subseteq k\mathbb{Z}_n$ и показать, что k делит n .

В начале покажем, что k делит n . Давайте разделим n с остатком на k , мы получим $n = qk + r$, где $0 \leq r < k$. Теперь, $r = n - qk$, а значит $r = -qk \pmod{n}$. Так как $k \in H$, последнее означает, что r тоже в H . Но это противоречит выбору k , оно было наименьшим положительным целым в H . Значит, r должен быть нулем, а это и означает, что k делит n . Теперь, давайте покажем, что каждый элемент H лежит в $k\mathbb{Z}_n$. Возьмем произвольный элемент $h \in H$. Разделим его на k с остатком и получим $h = qk + r$. Значит, $r = h - qk$. Так как $h \in H$ и $k \in H$, все выражение $h - qk$ лежит в H , то есть $r \in H$. Так как k был наименьшим положительным целым в H , получается, что $r = 0$. Последнее означает, что h делится на k , то есть лежит в $k\mathbb{Z}_n$. \square

2.5 Смежные классы

Алгебра тяготеет к тому, чтобы изучать группы с помощью подгрупп, а не только элементов. Важным инструментом в таком подходе являются смежные классы.

Определение 26. Пусть G – некоторая группа, $H \subseteq G$ – ее подгруппа и $g \in G$ – произвольный элемент. Тогда множество

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

называется левым смежным классом элемента g по подгруппе H . Аналогично определяются правые смежные классы. Множество

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

называется правым смежным классом элемента g по подгруппе H .

Замечания

1. Стоит заметить, что если G коммутативна, то нет разницы между левыми и правыми смежными классами для любой подгруппы $H \subseteq G$.
2. Сама подгруппа H является левым и правым смежным классом. Действительно, $H = 1 \cdot H = H \cdot 1$.
3. В произвольной группе, вообще говоря левый смежный класс gH не обязан равняться правому смежному классу Hg как показывает пример ниже.

Примеры 27. Некоторые примеры смежных классов.

1. Пусть $G = (\mathbb{Z}, +)$ и $H = 2\mathbb{Z}$ – подгруппа четных целых чисел. Тогда $2\mathbb{Z}$ и $1 + 2\mathbb{Z}$ – все возможные смежные классы H .
2. Пусть $G = S_3$ – группа перестановок на трех элементах и $H = \langle (1, 2) \rangle$ – циклическая подгруппа порожденная элементом $(1, 2)$. Мы можем перечислить все элементы G и H

$$G = \{1, (1, 2), (1, 3), (2, 3), (1, 2, 3), (3, 2, 1)\}, H = \{1, (1, 2)\}$$

Теперь мы видим, что есть три разных левых смежных класса H

$$H = \{1, (1, 2)\}, (1, 3)H = \{(1, 3), (1, 2, 3)\}, (2, 3)H = \{(2, 3), (3, 2, 1)\}$$

А так же, три разных правых смежных класса H

$$H = \{1, (1, 2)\}, H(1, 3) = \{(1, 3), (3, 2, 1)\}, H(2, 3) = \{(2, 3), (1, 2, 3)\}$$

Этот пример показывает, что $(1, 3)H \neq H(1, 3)$. Так же этот пример показывает, что

$$(1, 2)H = H, (1, 3)H = (1, 2, 3)H, (2, 3)H = (3, 2, 1)H$$

То есть одинаковые смежные классы могут порождаться разными элементами.

3. Пусть $G = S_n$ – группа перестановок на n элементах и $H = A_n$ – подгруппа четных перестановок. Тогда для всякой четной перестановки $\sigma \in A_n$, множество σA_n состоит из всех четных перестановок. Аналогично, для всякой нечетной перестановки $\sigma \in S_n \setminus A_n$, множество σA_n состоит из всех нечетных перестановок. Потому, есть всего два левых смежных класса по A_n , это

$$A_n \text{ и } (1, 2)A_n$$

Аналогично мы можем заметить, что есть всего два правых смежных класса по A_n , это

$$A_n \text{ и } A_n(1, 2)$$

Более того, мы видим, что $\sigma A_n = A_n \sigma$ для всех $\sigma \in S_n$.

Определение 28. Пусть G группа и H ее подгруппа. Подгруппа H называется нормальной если $gH = Hg$ для любого элемента $g \in G$.

Утверждение 29. Пусть G – некоторая группа и H – ее подгруппа. Следующие условия эквивалентны:

1. $gH = Hg$ для любого $g \in G$.
2. $gHg^{-1} = H$ для любого $g \in G$.
3. $gHg^{-1} \subseteq H$ для любого $g \in G$.

Доказательство. (1) \Leftrightarrow (2). Предположим $gH = Hg$. Умножая это равенство справа на g^{-1} , мы получаем $gHg^{-1} = H$. А если нам задано равенство $gHg^{-1} = H$, умножая его справа на g , мы получим $gH = Hg$.

(2) \Leftrightarrow (3). Надо проверить, что если выполнено $gHg^{-1} \subseteq H$ для любого $g \in G$, то и $gHg^{-1} = H$ выполнено для любого $g \in G$. Если $gHg^{-1} \subseteq H$ для любого $g \in G$, то оно выполнено и для g^{-1} вместо g . Значит, $g^{-1}Hg \subseteq H$ для любого $g \in G$. Умножим это равенство слева на g , получим $Hg \subseteq gH$. Теперь умножим это равенство справа на g^{-1} и получим $H \subseteq gHg^{-1}$. А это завершает доказательство. \square

2.6 Теорема Лагранжа

Свойства смежных классов Прежде всего я хочу доказать некоторые свойства смежных классов. Так окажется, что левые смежные классы образуют разбиение группы G на не пересекающиеся множества одного размера. Аналогичное верно и для правых смежных классов. Подобное утверждение позволяет применить к изучению группы комбинаторные соображения.

Утверждение 30. Пусть G – некоторая группа, $H \subseteq G$ – ее подгруппа и $g_1, g_2 \in G$ – произвольные элементы. Тогда возможны только два случая:

1. Смежные классы не пересекаются: $g_1H \cap g_2H = \emptyset$.
2. Смежные классы совпадают: $g_1H = g_2H$.

Последнее означает, что каждый элемент группы G лежит в единственном смежном классе.

Доказательство. Если g_1H не пересекает g_2H , то доказывать нечего.

Предположим, что пересечение смежных классов $g_1H \cap g_2H$ не пусто. Мы должны доказать, что $g_1H = g_2H$. Предположим, что $g \in g_1H \cap g_2H$. Тогда $g \in g_1H$, $g = g_1h_1$ для некоторого $h_1 \in H$. Аналогично, $g \in g_2H$ влечет $g = g_2h_2$ для некоторого $h_2 \in H$. Значит $g_1h_1 = g_2h_2$. Разделив на h_1 справа, мы получим $g_1 = g_2h_2h_1^{-1}$. Так как H является подгруппой, то $h = h_2h_1^{-1} \in H$. То есть $g_1 = g_2h$ для некоторого $h \in H$.

Давайте покажем, что $g_1H \subseteq g_2H$. Предположим, что произвольный элемент $g \in g_1H$ имеет вид $g = g_1h'$, где $h' \in H$. Тогда $g = g_2hh'$ $\in g_2H$ потому что $hh' \in H$. Аналогично показывается обратное вложение $g_2H \subseteq g_1H$. А именно, возьмем $g \in g_2H$ в виде $g = g_2h'$ где $h' \in H$. Значит, $g = g_1h^{-1}h' \in g_1H$ потому что $h^{-1}h' \in H$. \square

Замечание 31. Обратим внимание, что $g_1H = g_2H$ тогда и только тогда, когда $g_1H \cap g_2H \neq \emptyset$. Более того, это происходит тогда и только тогда, когда найдется элемент $h \in H$ такой, что $g_1 = g_2h$. Последнее эквивалентно условию $g_2^{-1}g_1 \in H$. Это дает нам удобный способ проверять являются ли смежные классы одинаковыми.

Утверждение 32. Пусть G – некоторая группа, $H \subseteq G$ – конечная подгруппа и $g \in G$ – некоторый элемент. Тогда $|gH| = |H| = |Hg|$.

Доказательство. Я докажу утверждение для левых смежных классов. Для правых делается аналогично. Рассмотрим отображение

$$\phi: H \rightarrow gH \quad x \mapsto gx$$

Оно переводит элементы H в элементы gH . С другой стороны, существует обратное отображение

$$\psi: gH \rightarrow H \quad x \mapsto g^{-1}x$$

Поэтому ϕ и ψ являются взаимно обратными биекциями. \square

Утверждение 33. Пусть G – конечная группа и $H \subseteq G$ – ее подгруппа. Тогда

1. Количество левых смежных классов группы H равно $|G|/|H|$.
2. Количество правых смежных классов группы H равно $|G|/|H|$.

В частности, количество левых и правых смежных классов одно и то же.

Доказательство. Я докажу первое равенство для левых смежных классов. Утверждение 30 показывает, что G является дизъюнктивным объединением своих смежных классов, то есть $G = g_1H \sqcup \dots \sqcup g_kH$. С другой стороны, утверждение 32 говорит, что все смежные классы g_1H, \dots, g_kH имеют один и тот же размер $|H|$. Значит

$$|G| = |g_1H| + \dots + |g_kH| = |H| + \dots + |H| = k|H|$$

Здесь k – это число различных левых смежных классов. □

Определение 34. Пусть G – конечная группа и $H \subseteq G$ – некоторая ее подгруппа. Тогда количество левых смежных классов H называется индексом H и обозначается $(G : H)$. Это число так же совпадает с количеством правых смежных классов.

Используя это определение, мы можем переписать утверждение 33 следующим образом.

Утверждение 35 (Теорема Лагранжа). Пусть G – конечная группа и $H \subseteq G$ – некоторая ее подгруппа. Тогда, $|G| = (G : H)|H|$

Следствия теоремы Лагранжа

1. Пусть G – конечная группа и $H \subseteq G$ – ее некоторая подгруппа. Тогда $|H|$ делит $|G|$.
2. Пусть G – конечная группа и $g \in G$ – произвольный элемент. Тогда $\text{ord}(g)$ делит $|G|$. Действительно, $\text{ord}(g) = |\langle g \rangle|$ по утверждению 23. Но $|\langle g \rangle|$ делит $|G|$ по предыдущему пункту.
3. Пусть G – конечная группа и $g \in G$ – некоторый элемент. Тогда $g^{|G|} = 1$. Действительно, мы уже знаем, что $|G| = \text{ord}(g)k$. Значит,

$$g^{|G|} = g^{\text{ord}(g)k} = \left(g^{\text{ord}(g)}\right)^k = 1^k = 1$$

4. Пусть G – группа простого порядка. Тогда G циклическая. Действительно, так как порядок G прост, то он больше 1. Значит, существует элемент $g \in G$ такой, что $g \neq 1$. Тогда подгруппа $\langle g \rangle$ имеет порядок больше 1. Но $|\langle g \rangle|$ делит $|G| = p$. Так как p простое, единственно возможный случай – это $|\langle g \rangle| = p = |G|$. Последнее означает, что $\langle g \rangle = G$ и все доказано.
5. Малая теорема Ферма. Пусть $p \in \mathbb{Z}$ – простое число и $a \in \mathbb{Z}$. Если p не делит a , то p делит $a^{p-1} - 1$. Действительно, давайте рассмотрим группу (\mathbb{Z}_p^*, \cdot) . Для любого элемента $b \in \mathbb{Z}_p^*$, имеем $b^{|\mathbb{Z}_p^*|} = 1 \pmod{p}$ по пункту (3). Но \mathbb{Z}_p^* состоит из $p - 1$ элемента. Теперь возьмем произвольное $a \in \mathbb{Z}$ взаимно простое с p . Пусть b – остаток от деления a на p . Тогда $a^{p-1} = b^{p-1} = 1 \pmod{p}$ и все доказано.