Алгебра
Лекции

Дима Трушин

2024

Содержание

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 $\circ\colon X \times X \to X$ 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 $\mu\colon X \times X \to X$ 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

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

   В функциональной форме

$$\mathrm{add}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{add}(m, n) = m + n$$

   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 $\mathrm{add}(m, n)$ и $m + n$ это одно и то же.

2. Умножение целых чисел. В операторной форме

$$\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

   В функциональном стиле

$$\mathrm{mult}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{mult}(m, n) = m \cdot n$$

3. Максимум целых чисел. В операторной форме

$$\vee\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \vee n$$

   В функциональной форме

$$\max\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \max(m, n) = m \vee n$$

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

[1] Операция 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

$$\wedge\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m\wedge n$$

В функциональной форме

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

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

5. Просто случайная дурацкая бинарная операция на целых числах

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

Давайте резюмируем, что бинарная операция на X – это любое отображение вида $f\colon X\times X\to X$. 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 $\circ\colon X\times X\to X$ 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 случится, 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.

$$+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m+n$$

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

2. Вычитание целых чисел не ассоциативно.

$$-\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m-n$$

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 равенство будет -1, а правая – 1. Так что, $(0-0)-1\neq 0-(0-1)$.

1.2.2 Нейтральный элемент

Определение 6. Пусть $\circ\colon X \times X \to X$ – 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.

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

   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.

$$-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

   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 $\circ\colon X \times X \to X$ – 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 $e = e \circ e' = e'$. □

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 $\circ\colon X \times X \to X$ – 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 напомню, 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 $\circ\colon X \times X \to X$ – 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 значение, 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. □

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.

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

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

$$\cdot \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

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 $\circ \colon X \times X \to X$ 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.

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

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

2. Целочисленное вычитание не коммутативно.

$$- \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

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:**

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

1. G – множество.
2. Операция $\circ\colon G \times G \to G$.

- **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 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 $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ 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	$\cdot\colon G \times G \to G$	$+\colon G \times G \to G$
На элементах	$(x, y) \mapsto xy$	$(x, y) \mapsto x + y$
Нейтральный элемент	1	0
Обратный элемент	x^{-1}	$-x$
Степень элемента	$x^n = \underbrace{x \cdot \ldots \cdot x}_{n}$	$nx = \underbrace{x + \ldots + x}_{n}$

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

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

$$(xy)z = xyz = xyy^{-1}x^{-1} = xx^{-1} = 1$$

[3] Строго 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

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

При подстановке $g_1 = \ldots = g_n = g$, 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

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

С другой стороны

$$(g^n)^{-1} = \left(\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-n}\right)^{-1} = \underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{-n}$$

где последнее равенство берется из предыдущего пунка утверждения.

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

$$(g^{-1})^n = \left(\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}\right) \quad \text{и} \quad g^{-n} = \left(\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}\right)$$

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

$$(g^{-1})^{-n} = \left(\underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{n}\right) \quad \text{и} \quad g^{-(-n)} = \left(\underbrace{g \cdot \ldots \cdot g}_{n}\right)$$

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. $n \geqslant 0$ and $m \geqslant 0$.
2. $n < 0$ and $m \geqslant 0$.
3. $n \geqslant 0$ and $m < 0$.
4. $n < 0$ and $m < 0$.

Пусть у нас первый случай:

$$g^n g^m = \underbrace{g \cdot \ldots \cdot g}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m} = \underbrace{g \cdot \ldots \cdot g}_{n+m} = g^{n+m}$$

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

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

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

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

Если $n < m$, имеем

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

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

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

Что и требовалось показать. □

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

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

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

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

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 $\operatorname{ord} g$.

Замечания

- Обратите внимание, что $g = 1$ тогда и только тогда, когда $\operatorname{ord} g = 1$.
- 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 $1, g, g^2, \ldots, g^{n-1}$ различны. Более того, степени повторяются по циклу, а именно в ряду*

$$\underbrace{\ldots, g^{-2}, g^{-1}}, \underbrace{1, g, g^2, \ldots, g^{n-1}}, \underbrace{g^n, g^{n+1}, \ldots, g^{2n-1}}, \underbrace{g^{2n}, \ldots}$$

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

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

При этом $n = \operatorname{ord} g$.

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 $1, g, \ldots, g^{n-1}$ 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 $1, g, \ldots, g^{n-1}$. Для этого поделим N с остатком на n, получим $N = qn + r$, где $0 \leqslant r < n$. Тогда

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

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

[4] Действительно, 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 $\operatorname{ord} g$ совпадает с количеством элементом 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 должно 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

$$mk = \underbrace{k + \ldots + k}_{m} \in H \;\text{ и }\; (-n)k = \underbrace{(-k) + \ldots + (-k)}_{n} \in H \;\text{ для любых }\; m, n \in \mathbb{N}$$

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 $0 \leqslant r < k$. 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. □

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 $k \mod n$, $k\mathbb{Z}_n$ 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 $0 \leqslant r < k$. 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 $k\mathbb{Z}_n$. □

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 $\sigma \in S_n \subseteq A_n$, множество σA_n состоит из всех нечетных перестановок. Потому, есть всего два левых смежных класса поA_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)⇔(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)⇔(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. □

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: $g_1H \cap g_2H = \varnothing$.*
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 $h^{-1}h' \in H$. □

Замечание 31. Обратим внимание, что $g_1H = g_2H$ тогда и только тогда, когда $g_1H \cap g_2H \neq \varnothing$. 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

$$\phi\colon H \to gH \quad x \mapsto gx$$

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

$$\psi\colon gH \to H \quad x \mapsto g^{-1}x$$

Поэтому ϕ и ψ являются взаимно обратными биекциями. □

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 дизъюнктным объединением своих смежных классов, то есть $G = g_1H \sqcup \ldots \sqcup g_kH$. С другой стороны, утверждение 32 говорит, что все смежные классы $g_1H, \ldots, g_kH$ имеют один и тот же размер $|H|$. Значит

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

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 $\mathrm{ord}(g)$ делит $|G|$. Действительно, $\mathrm{ord}(g) = |\langle g \rangle|$ 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 $|G| = \mathrm{ord}(g)k$. Значит,
$$g^{|G|} = g^{\mathrm{ord}(g)k} = \left(g^{\mathrm{ord}(g)}\right)^k = 1^k = 1$$
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.

2.7 Гомоморфизмы и изоморфизмы

Существует много различных групп. Кроме того, мы с вами изучим методы по построению новых групп из уже имеющихся. В такой ситуации очень полезно иметь механизм для сравнения групп. Как понять, что мы построили уже знакомую нам группу? Чтобы ответить на этот вопрос, мы должны объяснить, что значит, что две группы одинаковые. То есть нам нужен способ сравнивать группы между собой. Тут на помощь нам приходят гомоморфизмы (способ сравнивать группы) и изоморфизмы (способ говорить, что две группы одинаковые). Давайте начнем с определений.

Определение 36. Пусть G и H – группы. Определим гомоморфизм $\varphi\colon G \to H$.

- **Данные** отображение $\varphi\colon G \to H$.
- **Аксиома** $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ для всех $g_1, g_2 \in G$.

В таком случае φ называется гомоморфизмом из G в H.

Замечание 37. Давайте я явно проговорю определение. Нам даны две группы $(G, \circ)$ и $(H, \cdot)$. Гомоморфизм $\varphi\colon G \to H$ – это отображение такое, что $\varphi(g_1 \circ g_2) = \varphi(g_1) \cdot \varphi(g_2)$. В левой части равенства мы берем элементы g_1 и g_2 из группы G и перемножаем их с помощью операции из G и потом отправляем результат в H. В правой части, мы сначала отправляем элементы g_1 и g_2 в группу H и только потом перемножаем образы с помощью операции из H.

Примеры 38. 1. Пусть $G = (\mathbb{Z}, +)$ и $H = (\mathbb{Z}_n, +)$, тогда отображение $\pi\colon \mathbb{Z} \to \mathbb{Z}_n$ по правилу $k \mapsto k \pmod n$ является гомоморфизмом.

2. Пусть $G = S_n$ – группа перестановок и $H = \mu_2 = \{\pm 1\}$ снабжено умножением. Тогда отображение $\operatorname{sgn}\colon S_n \to \mu_2$ сопоставляющее каждой перестановке ее знак (четные идут в 1, а нечетные в -1) является гомоморфизмом.

3. Пусть $G = (\mathrm{GL}_n(\mathbb{R}), \cdot)$ и $H = (\mathbb{R}^*, \cdot)$ – множество ненулевых вещественных чисел с операцией умножения. Тогда отображение $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ по правилу $A \mapsto \det(A)$ является гомоморфизмом.

4. Пусть $G = (\mathbb{R}, +)$ и $H = (\mathbb{R}^*, \cdot)$. Тогда отображение $\exp\colon \mathbb{R} \to \mathbb{R}^*$ по правилу $x \mapsto e^x$ является гомоморфизмом.

5. Пусть $G = (\mathbb{Z}, +)$, H – произвольная группа и $h \in H$ – произвольный элемент. Тогда отображение $\phi\colon \mathbb{Z} \to H$ по правилу $k \mapsto h^k$ является гомоморфизмом.

6. Пусть $G = (\mathbb{Z}_n, +)$, H – произвольная группа и $h \in H$ – произвольный элемент такой, что $h^n = 1$. Тогда отображение $\phi\colon \mathbb{Z}_n \to H$ по правилу $k \mapsto h^k$ является гомоморфизмом групп.

Давайте докажем некоторые свойства гомоморфизмов.

Утверждение 39. *Пусть $\varphi\colon G \to H$ – некоторый гомоморфизм групп. Тогда*

1. *$\varphi(1) = 1$, то есть нейтральный элемент G идет в нейтральный элемент H.*
2. *$\varphi(g^{-1}) = \varphi(g)^{-1}$ для любого $g \in G$.*

Доказательство. 1) Мы знаем, что $1 = 1 \cdot 1$. Давайте применим φ к этому равенству. Тогда мы получим

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \in H$$

Теперь умножим это равенство на $\varphi(1)^{-1}$, будет $1 = \varphi(1)$.

2) Пусть $g \in G$ – некоторый элемент. Тогда $gg^{-1} = 1$. Теперь применим φ к этому равенству и получим

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

Умножая полученное равенство слева на $\varphi(g)^{-1}$, мы получаем $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

Определение 40. Пусть G и H – группы. Определим изоморфизм $\varphi\colon G \to H$.

- **Данные** гомоморфизм $\varphi\colon G \to H$.
- **Аксиома** φ является биекцией.

В этом случае φ называется изоморфизмом между G и H. Если найдется изоморфизм между G и H, то группы G и H называются изоморфными.

Давайте я поясню немного определение. В начале давайте разберемся, что значит, что у нас есть биекция множеств $\varphi\colon X \to Y$. Предположим $X = \{1, 2, 3\}$, $Y = \{a, b, c\}$ и φ устроено так: $1 \mapsto a$, $2 \mapsto b$ и $3 \mapsto c$. Тогда можно думать про эту биекцию следующим образом. Множество X – это множество имен элементов, а множество Y – это множество других имен тех же самых элементов. Тогда на биекцию можно смотреть, как на процедуру переименования. То есть можно считать, что Y это то же самое множество элементов, что и X, только с другими названиями элементов.

Теперь пусть у нас задан изоморфизм групп $\varphi\colon G \to H$. Такой гомоморфизм как минимум биекция, а значит мы можем считать, что подлежание множества G и H на самом деле одинаковые. Кроме того, условие $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ означает, что при нашем отождествлении G и H операция на G превращается в операцию на H. То есть мы можем думать, что H – это то же самое множество, что и G с той же самой операцией, что на G. Или другими словами, мы считаем, что группа H – это та же самая группа, что и G, но только с другим множеством имен и другим обозначением операции. Однако, по существу это одна и та же группа. Как следствие, изоморфные группы имеют одинаковые свойства.

Примеры 41. 1. Пусть $G = (\mathbb{Z}_n, +)$ и $H = \mu_n \subseteq \mathbb{C}$ – множество комплексных корней из единицы степени n с операцией умножения. Давайте фиксируем примитивный корень $\xi \in \mu_n$. Тогда отображение $\mathbb{Z}_n \to \mu_n$ по правилу $k \mapsto \xi^k$ является изоморфизмом.

2. Пусть $G = (\mathbb{Z}, +)$ и
$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$$
с операцией умножения. Тогда отображение $\varphi\colon \mathbb{Z} \to H$ по правилу $k \mapsto \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ является изоморфизмом.

3. Пусть $G = (\mathbb{C}, +)$ и $H = (\mathbb{R}^2, +)$. Тогда отображение $\varphi\colon \mathbb{C} \to \mathbb{R}^2$ по правилу $z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$ является изоморфизмом.

4. Пусть $G = (\mathbb{C}^*, \cdot)$ и
$$H = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \text{ такие что } a^2 + b^2 \neq 0 \right\}$$
с операцией умножения. Тогда отображение $\varphi\colon \mathbb{C}^* \to H$ по правилу $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ является изоморфизмом.

5. Claim 23 говорит, что циклическая группа $G = \langle g \rangle$ изоморфна $\mathbb{Z}$ или $\mathbb{Z}_n$ в зависимости от порядка образующего. Если $\operatorname{ord} g = \infty$, тогда $G \simeq \mathbb{Z}$. Если $\operatorname{ord} g = n$, тогда $G \simeq \mathbb{Z}_n$.

С каждым гомоморфизмом мы можем ассоциировать специальные подгруппы: ядро и образ.

Определение 42. Пусть $\varphi\colon G \to H$ – некоторый гомоморфизм групп. Тогда

1. ядро φ – это $\ker \varphi = \{g \in G \mid \varphi(g) = 1\} \subseteq G$.

2. образφ – это $\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\} = \varphi(G) \subseteq H$.

Стоит отметить, что ядро является подмножеством в G, а образ – в H.

Утверждение 43. *Пусть $\varphi\colon G \to H$ – гомоморфизм групп. Тогда*

1. *$\operatorname{Im} \varphi \subseteq H$ является подгруппой.*

2. *$\ker \varphi \subseteq G$ является нормальной подгруппой.*

3. *Отображение φ сюръективно тогда и только тогда, когда $\operatorname{Im} \varphi = H$.*

4. *Отображение φ инъективно тогда и только тогда, когда $\ker \varphi = \{1\}$.*

Доказательство. 1) Давайте проверим, что все свойства подгруппы выполняются. Во-первых, $1 = \varphi(1) \in \operatorname{Im} \varphi$, значит нейтральный элемент лежит в образе. Во-вторых, $\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) \in \operatorname{Im} \varphi$, то есть образ замкнут относительно операции. В-третьих, $\varphi(g)^{-1} = \varphi(g^{-1}) \in \operatorname{Im} \varphi$, то есть с каждым элементом образ содержит его обратный.

2) В начале проверим, что ядро – подгруппа. Во-первых, $\varphi(1) = 1$, значит $1 \in \ker \varphi$ по определению. Во-вторых, если $x, y \in \ker \varphi$, тогда $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1$, то есть $xy \in \ker \varphi$. В-третьих, если $x \in \ker \varphi$, то $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$. Значит $x^{-1} \in \ker \varphi$. Мы только что проверили, что $\ker \varphi$ является подгруппой. Теперь надо показать, что $g \ker \varphi = \ker \varphi g$ для всех $g \in G$. По утверждению 29, достаточно проверить, что $g \ker \varphi g^{-1} \subseteq \ker \varphi$ для каждого $g \in G$. То есть мы должны показать, что $\varphi(g \ker \varphi g^{-1}) = 1$ для каждого $g \in G$. Действительно, пусть $h \in \ker \varphi$, тогда
$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g) \cdot 1 \cdot \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

3) Это условие тривиально по определению.

4) Предположим, что φ инъективно и $x \in \ker \varphi$. Это значит, что $\varphi(x) = 1$. С другой стороны, мы всегда имеем $\varphi(1) = 1$. Значит, x и 1 идут в один и тот же элемент 1. По инъективности получаем $x = 1$.

Теперь предположим, что $\ker \varphi = \{1\}$. Рассмотрим два элемента $x, y \in G$ таких, что $\varphi(x) = \varphi(y)$. Умножим это равенство на $\varphi(x)^{-1}$ и получим
$$1 = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1})$$
Значит $yx^{-1} \in \ker \varphi = \{1\}$. Поэтому $yx^{-1} = 1$. Тогда $y = x$, что завершает доказательство. □

2.8 Произведение групп

Вообще говоря нам не очень хочется каждый раз строить группы с нуля. Хочется иметь механизм по построению новых групп из уже заданных. Существует много подобных процедур в алгебре. Мы собираемся изучить одну из таких.

Определение 44. Пусть G и H – некоторые группы. Определим новую группу $G \times H$ следующим образом

1. Как множество это декартово произведение подлежащих множеств групп G и H: $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$.
2. Операция
$$\cdot\colon (G \times H) \times (G \times H) \to G \times H$$
задана по правилу
$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2), \quad g_1, g_2, \in G,\ h_1, h_2 \in H$$

Группа $G \times H$ называется произведением групп G и H.

По-хорошему нам надо бы показать, что $G \times H$ действительно является группой. Мы только что определили все необходимые данные для группы, но осталось проверить аксиомы. Давайте я напомню их

- Операция ассоциативна
$$(g_1, h_1)\Big((g_2, h_2)(g_3, h_3)\Big) = \Big((g_1, h_1)(g_2, h_2)\Big)(g_3, h_3)$$
- Существует нейтральный элемент, $1 = (1, 1)$.
- У каждого элемента есть обратный, $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Все свойства проверяются прямым вычислением. Если у нас есть несколько групп $G_1, \ldots, G_k$, мы можем определить произведение $G_1 \times \ldots \times G_k$ аналогично тому, как мы определили произведение двух групп.

2.9 Конечные абелевы группы

Теперь я хочу сосредоточиться на очень важном классе групп, класс конечных абелевых групп.

Определение 45. Конечная абелева группа – это коммутативная (абелева) группа G с конечным числом элементов.

Само по себе определение – не большой сюрприз, название говорит само за себя. Однако обратите внимание на следующий результат.

Утверждение 46. *Пусть G – конечная абелева группа, тогда G изоморфна группе вида $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.*

Я не буду доказывать этот результат. Доказательство не сложно, но требует некоторой технической работы, на которую у нас нет времени. Кроме того, само доказательство не проливает свет на какие-либо свойства конечных абелевых групп и потому не так интересно. На мой взгляд куда важнее научиться понимать как использовать этот результат. Давайте начнем с некоторых примеров.

Примеры 47. 1. Пусть $G = \mathbb{Z}_8^*$ с операцией умножения. Очевидно, что это конечная абелева группа, а значит она должна представляться в виде произведения циклических групп. Действительно, давайте проверим, что
$$\mathbb{Z}_8^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$
Отображение задающее биекцию и уважающее операции можно задать так:
$$1 \leftrightarrow (0, 0),\ 3 \leftrightarrow (1, 0),\ 5 \leftrightarrow (0, 1),\ 7 \leftrightarrow (1, 1)$$
Это не единственный способ отождествить эти две группы. Например, вот другой изоморфизм:
$$1 \leftrightarrow (0, 0),\ 3 \leftrightarrow (1, 0),\ 7 \leftrightarrow (0, 1),\ 5 \leftrightarrow (1, 1)$$
Я не собираюсь описывать все изоморфизмы, самое главное, что мы видим, что таких изоморфизмов много. Так же обратите внимание, что группа не является циклической, так как в ней нет элемента порядка 4.

2. Пусть $G = \mathbb{Z}_9^*$ с операцией умножения. Это так же конечная абелева группа. В этом случае мы имеем:

$$\mathbb{Z}_9^* \simeq \mathbb{Z}_6$$

вот пример двух разных изоморфизомв

$$\begin{array}{ccc} \mathbb{Z}_6 \to \mathbb{Z}_9^* & & \mathbb{Z}_6 \to \mathbb{Z}_9^* \\ k \mapsto 2^k & \text{и} & k \mapsto 5^k \end{array}$$

Так же заметим, что в этом случае группа является циклической. Элементы 2 и 5 являются различными образующими группы. Изоморфизмы выше соответствуют одному из выбору образующего.

Утверждение 48 (Китайская теорема об остатках)**.** *Пусть $m, n \in \mathbb{N}$ – два взаимно простых натуральных числа, то есть $(m, n) = 1$. Тогда отображение*

$$\Phi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad k \mapsto (k \mod m,\ k \mod n)$$

является изоморфизмом групп.

Доказательство. В начале мы должны показать, что отображение является гомоморфизмом. Надо показать, что $\Phi(k+d) = \Phi(k) + \Phi(d)$, то есть

$$\Phi(k+d) = ((k+d) \mod m,\ (k+d) \mod n) = ((k \mod m) + (d \mod m),\ (k \mod n) + (d \mod n)) =$$
$$= (k \mod m,\ k \mod n) + (d \mod m,\ d \mod n) = \Phi(k) + \Phi(d)$$

Теперь я утверждаю, что гомоморфизм инъективен. Утверждение 43 пункт (4) гласит, что достаточно проверить, что ядро гомоморфизма содержит только нейтральный элемент. По определению, имеем

$$\ker \Phi = \{k \in \mathbb{Z}_{mn} \mid k = 0 \pmod m,\ k = 0 \mod n\}$$

Значит $k \in \ker \Phi$ тогда и только тогда, когда m делит k и n делит k. Так как m и n взаимно просты, последнее означает, что mn делит k. А значит, $k = 0$ в $\mathbb{Z}_{mn}$.

Чтобы показать, что Φ является изоморфизмом, нам надо показать сюръективность. Давайте посчитаем количество элементов в обеих группах. По определению $|\mathbb{Z}_{mn}| = mn$. С другой стороны, $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$. Значит Φ – это инъективное отображение между множествами одинакового размера. А отсюда получаем, что оно обязательно сюръективно. □

В предыдущем утверждении явно сказано, как отображать элементы из $\mathbb{Z}_{mn}$ в элементы из $\mathbb{Z}_m \times \mathbb{Z}_n$. Однако, стоит сказать, как строится обратное отображение. Так как m и n взаимно просты, мы имеем $1 = um + vn$ для некоторых $u, v \in \mathbb{Z}$ по расширенному алгоритмы Евклида. Теперь рассмотрим элемент $a_1 = um = 1 - vn$. Ясно, что $a_1 \mapsto (0, 1)$ под действием отображения Φ. Аналогично, элемент $a_2 = vn = 1 - um$ идет в $(1, 0)$. Значит, элемент (a, b) соответствует элементу $aa_1 + ba_2 \pmod{mn}$ в группе $\mathbb{Z}_{mn}$.

Примеры 49.

1. В случае $m = 3$ и $n = 2$, мы имеем $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$. Здесь элемент 1 идет в $(1, 1)$. Значит $(1, 1)$ является образующим циклической группы $\mathbb{Z}_3 \times \mathbb{Z}_2$. Так как $1 = 3 - 2$, мы видим, что 3 идет в $(0, 1)$ и -2 идет в $(1, 0)$ (обратим внимание, что $-2 = 4$ в $\mathbb{Z}_6$). Потому, обратное отображение задано по правилу $(a, b) \mapsto -2a + 3b = 4a + 3b \pmod 6$.

2. Группа $\mathbb{Z}_2 \times \mathbb{Z}_2$ не является циклической. Значит, не существует изоморфизма между ней и группой $\mathbb{Z}_4$.

3. Еще один пример различного представления абелевой группы в виде произведения циклических

$$\mathbb{Z}_{30} \simeq \mathbb{Z}_6 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Так что, все пять конструкций дают одну и ту же циклическую группу.

4. В общем случае, если $m = p_1^{k_1} \dots p_r^{k_r}$, где p_i – простые, имеем

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$$

Как мы видели выше, одна и та же абелева группа может быть записана совершенно разными способами. Как же быстро понять, что два представления задают одну и ту же группу? Ответ содержится в следующем утверждении.

Утверждение 50. *Пусть G – конечная абелева группа. Тогда*

1. *G единственным образом представляется в следующем виде*

$$G = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}, \quad \text{где } 1 < d_1 | d_2 | \ldots | d_k \text{ натуральные}$$

2. *С точностью до перестановки множителей G единственным образом представляется в следующем виде*

$$G = \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}, \quad \text{где } p_i \text{ – не обязательно различные простые числа, } k_i \text{ – натуральные}$$

Важно упомянуть, что простые p_i могут повторяться во втором представлении, например $\mathbb{Z}_2 \times \mathbb{Z}_4$ – один из возможных случаев.

Примеры 51. 1. Пусть $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ и $H = \mathbb{Z}_{12}$. Обе эти группы представлены в первой форме. Так как такое представление единственно, то G и H не изоморфны.

2. Пусть $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ и $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Мы видим, что G представлено в первой форме, а H представлено во второй. Давайте пересчитаем G во второй форме, используя Китайскую теорему об остатках:

$$G = \mathbb{Z}_2 \times \mathbb{Z}_6 = \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) = H$$

Значит группы изоморфны.

Теперь я хочу сформулировать вторую версию китайской теоремы об остатках.

Утверждение 52. *Пусть $m, n \in \mathbb{N}$ – два взаимно простых целых числа, то есть $(m, n) = 1$. Тогда отображение*

$$\Phi \colon \mathbb{Z}^*_{mn} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n, \quad k \mapsto (k \mod m, k \mod n)$$

является корректно определенным изоморфизмом групп.

Доказательство. Так как m и n взаимно простые, мы уже знаем, что отображение $\Phi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ является биекцией, по утверждению 48. Ясно, что число k взаимно просто с mn тогда и только тогда, когда оно взаимно просто с m и взаимно просто с n одновременно. Последнее означает, что Φ индуцирует биекцию $\Phi \colon \mathbb{Z}^*_{mn} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n$.

Теперь надо показать, что Φ уважает умножение. С одной стороны имеем

$$\Phi(k_1 k_2) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$

С другой стороны

$$\Phi(k_1)\Phi(k_2) = (k_1 \mod m, k_1 \mod n)(k_2 \mod m, k_2 \mod n) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$

А это доказывает, что $\Phi(k_1 k_2) = \Phi(k_1)\Phi(k_2)$, что и требовалось. □

Последний результат означает, что вычисление группы $\mathbb{Z}^*_n$ можно свести к вычислению групп $\mathbb{Z}^*_{p^k}$ где p простое. Действительно, если $n = p_1^{k_1} \ldots p_r^{k_r}$, то

$$\mathbb{Z}^*_n \simeq \mathbb{Z}^*_{p_1^{k_1}} \times \ldots \times \mathbb{Z}^*_{p_r^{k_r}}$$

Чтобы закончить вычисление, нам надо знать ответ для степеней простых. Давайте сформулируем необходимые результаты без доказательства.

Утверждение 53. *Если p – нечетное простое и n – произвольное положительное целое, тогда*

$$\mathbb{Z}^*_{p^n} \simeq \mathbb{Z}_{p^{n-1}(p-1)}$$

является циклической группой. Кроме того, целое $a \in \mathbb{Z}_{p^n}$ является образующим $\mathbb{Z}^*_{p^n}$ тогда и только тогда, когда a является образующим в $\mathbb{Z}^*_p$ и $a^{p-1} \neq 1 \pmod{p^2}$. Значит, любой элемент $\mathbb{Z}^*_{p^n}$ однозначно представляется в виде a^k, где $0 \leqslant k < p^{n-1}(p-1)$.

В случае степени 2 ответ будет следующим

$$\mathbb{Z}_{2^n}^* \simeq \begin{cases} 0, & n \leqslant 1 \\ \mathbb{Z}_2, & n = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}, & n \geqslant 3 \end{cases}$$

В случае $n = 2$ группа порождена элементом $3 = -1$. В случае $n \geqslant 3$, первый множитель $\mathbb{Z}_2$ порожден элементом $2^n - 1 = -1$, а второй множитель $\mathbb{Z}_{2^{n-2}}$ порожден элементом 5. Таким образом, любой элемент $\mathbb{Z}_{2^n}^*$ однозначно представляется в виде $\pm 5^k$, где $0 \leqslant k < 2^{n-2}$.

В частности группа $\mathbb{Z}_p^*$ циклическая порядка $p-1$ для любого простого числа p. Мы позже докажем более общий результат используя абстрактный алгебраический аппарат.

Утверждение 54. *Элемент $m \in \mathbb{Z}_n$ является образующим тогда и только тогда, когда m и n взаимно просты.*

Доказательство. ($\Rightarrow$). Предположим, что $(m, n) = d > 1$. Тогда все элементы $\langle m \rangle$ делятся на d. В частности, мы никогда не получим 1. Значит m – не образующий, противоречие. То есть m и n обязаны быть взаимно простыми.

($\Leftarrow$). Мы хотим показать, что $\langle m \rangle = \mathbb{Z}_n$. Так как 1 – образующий $\mathbb{Z}_n$, достаточно показать, что $1 \in \langle m \rangle$. В силу взаимной простоты m и n существуют элементы $a, b \in \mathbb{Z}$ такие, что $1 = am + bn$. Значит $1 = am \pmod{n}$. Последнее означает, что 1 является a-ой степенью m, а значит, $1 \in \langle m \rangle$. □

3 Криптография

3.1 Общие слова

Давайте предположим, что у вас есть жена и любовница[5] и вы очень хотите послать сообщение любовнице. Однако, вы опасаетесь это делать в открытую, так как кто-то в вашей семье недавно купил дробовик и вы точно уверены, что это не вы. В такой неловкой ситуации приходится прибегать к помощи криптографии.

Основная идея стоящая за криптографическими методами состоит в следующем. Оказывается, что есть процедуры, которые в одну сторону вычисляются быстро, а в обратную очень медленно, то есть посчитать прямое отображение легко, а обратное сложно. На основе таких отображений можно строить более хитрые процедуры. Например, процедуры, которые легко выполняются, когда вы знаете некоторую дополнительную секретную информацию и сложно, если вы такой информацией не владеете.

Прежде чем переходить к деталям, давайте я дам пример самых популярных процедур, которые в одну сторону считаются легко, а в другую сложно.

- Очень легко считать произведение целых чисел, даже очень больших.[6] Однако, процедура разложения целого числа на множители очень сложная, в том смысле, что принципиально лучше чем прямой перебор множителей, мы ничего не знаем.
- Предположим, нам задана некоторая абелева группа G и ее элемент $g \in G$. Тогда очень легко считается g^n для любого n. А именно у нас есть алгоритм быстрого возведения в степень, который работает приблизительно за $O(\log n)$ операций. С другой стороны, если группа G подобрана правильно, то обратная операция будет медленной. То есть для $h \in \langle g \rangle$ найти такое $n \in \mathbb{Z}$, что $h = g^n$ будет сложной операцией.

Первая процедура активно используется в алгоритме шифрования RSA, а вторая в процедуре шифрования Диффи-Хеллмана.

3.2 Быстрое возведение в степень

В начале я хочу напомнить алгоритм быстрого возведения в степень. Пусть G – группа и $g \in G$ – некоторый элемент и $n \in \mathbb{N}$. Тогда в мультипликативной и аддитивной нотации имеем

$$g^n = \begin{cases} g(g^2)^k, & n = 2k+1 \\ (g^2)^k, & n = 2k \end{cases} \quad \text{or} \quad ng = \begin{cases} g + k(2g), & n = 2k+1 \\ k(2g), & n = 2k \end{cases}$$

[5] Или муж и любовник, если угодно.

[6] На сегодняшний день существует множество хитрых алгоритмов для перемножения очень больших чисел.

Обратите внимание, что левая часть от правой отличается лишь нотацией, то есть в обоих случаях мы умеем лишь применять операцию в группе к двум элементам, а надо быстро найти n кратное применение операции к одному элементу. Давайте для определенности сосредоточимся на мультипликативной нотации.

Дано: $g \in G$, $n \in \mathbb{N}$.

Вывод: $g^n \in G$.

Мы используем три временные переменные $r, d \in G$ и $k \in \mathbb{N}$. Будем поддерживать инвариант $rd^k = g^n$. Алгоритм останавливается, когда $k = 0$, при этом результат будет записан в r.

Алгоритм:

1. Инициализация $r = 1 \in G$, $d = g \in G$, $k = n \in \mathbb{N}$.
2. В цикле проверяем является ли k четным или нечетным. Останавливаем цикл, если $k = 0$.
   (a) Если k четное, то делаем присваивания $r = r$, $d = d^2$, $k = k/2$.
   (b) Если k нечетно, то делаем присваивания $r = r \cdot d$, $d = d^2$, $k = (k-1)/2$.

Замечания Давайте разберемся, как работает алгоритм. В процессе вычисления, мы имеем $rd^k = g^n$. В самом начале $r = 1$, $d = g$, $k = n$. Теперь посмотрим, что происходит на каждом шаге в обоих случаях:

- $k = 2m$. Тогда, $rd^{2m} = r(d^2)^m$. И мы обновляем данные $r = r$, $d = d^2$, и $k = m = k/2$.
- $k = 2m + 1$. Тогда, $rd^{2m+1} = (rd)(d^2)^m$. И мы обновляем данные $r = rd$, $d = d^2$, и $k = m = (k-1)/2$.

Таким образом наш инвариант поддерживается на протяжении всего алгоритма и при $k = 0$ в r будет содержаться ответ.

Я хочу обратить внимание на еще одну похожую процедуру. Пусть для определенности $n = 11$. Тогда в двоичной записи $11 = 1 + 2 + 2^3 = 1 + 2(1 + 2(0 + 2))$. Теперь можно вот как расписать возведение в степень

$$g^{11} = g^{1+2(1+2(0+2))} = g(g^{1+2(0+2)})^2 = g(g(g^{0+2})^2)^2 = g(g(g^2)^2)^2$$

Если $n = 2^k$, то вам потребуется в точности k операций. Например, если $n = 8 = 2^3$, то $g^8 = ((g^2)^2)^2$. Таким образом у нас $\log_2 n$ операций. В общем случае количество операций будет пропорционально $\log_2 n$. Но я не хочу считать его аккуратно.

3.3 Сложность проблемы дискретного логарифмирования

Пусть G – группа, $g \in G$ и $h \in \langle g \rangle$. Напомню, что поиск такого $n \in \mathbb{N}$, что $g^n = h$ называется проблемой дискретного логарифмирования. Важно понимать, что эта процедура может выполняться как быстро, так и медленно. Давайте приведем соответствующие примеры.

Примеры 55.
1. Пусть $G = \mathbb{Z}$ со сложением, $g = 1$ и $h = k$. Тогда ясно, что требуемое n равно k. Действительно, $ng = h$. В этом случае проблема дискретного логарифмирования тривиальна и не требует никаких вычислений.[7]
2. Пусть $G = \mathbb{Z}_m$ со сложением, $g = a \in \mathbb{Z}_m$, и $h = b \in \mathbb{Z}_n$. Тогда нам надо найти такое $n \in \mathbb{N}$, что $na = b \pmod m$. Эта проблема эффективно решается с помощью расширенного алгоритма Евклида.
3. Пусть p – простое число, $G = \mathbb{Z}_p^*$ с умножением и $g = a \in \mathbb{Z}_p^*$ – некоторый порождающий группы и $h = b \in \mathbb{Z}_p^*$. Тогда проблема заключается в поиске $n \in \mathbb{N}$ такого, что $a^n = b \pmod p$. Весь опыт человечества подсказывает нам, что эта проблема по видимому действительно сложная и быстро не решается.

[7] Даже изменение g на другой элемент группы, не делает проблему сложнее.

3.4 Диффи-Хеллман

В начале нам надо фиксировать некоторую группу G, ее элемент $g \in G$ и посчитать его порядок $n = \operatorname{ord} g$. Возможный выбор группы будет такой: $G = \mathbb{Z}_p^*$, где p простое, а g – произвольный образующий. Порядок в этом случае будет равен $p-1$. Поиск образующего – неприятная задача, но ее достаточно проделать единожды.

Давайте я напомню контекст У нас есть три участника: вы, жена и любовница. Процесс обмены сообщениями состоит из следующих общих шагов.

1. Перевести текстовое сообщение (или его часть) в элемент группы $t \in G$.
2. Зашифровать элемент t и получить зашифрованный элемент $t' \in G$.
3. Элемент t' передается по сети и становится известен всем.
4. Расшифровать элемент t' и получить исходное сообщение в виде элемента t.
5. Перевести элемент t обратно в текстовое сообщение (или его часть).

Шаги (1) и (5) обычно делаются с помощью некой обще известной таблицы, которая известна всем участникам. То есть нет никакого секрета в том, как именно вы преобразуете сообщения из текста в элементы группы и обратно. Не волнуйтесь, ваша жена с этим справится. Все шифрование ведется только на уровне элементов групп.

Обмен ключами Прежде чем передавать зашифрованные сообщения, вы с любовницей должны подготовить специальный приватный ключ, с помощью которого и будет вестись шифровка и расшифровка. До создания такого ключа, коммуникация не возможна.

Давайте изобразим весь процесс на следующей диаграмме. Она показывает, что кому известно.

Участники	Вы	Жена	Любовница
Знания	G, g, n	G, g, n	G, g, n

Вы генерируете случайное число $a \in \mathbb{Z}_n^*$ и считаете открытый ключ $r = g^a \in G$. Ваша любовница генерирует случайное число $b \in \mathbb{Z}_n^*$ и считает свой открытый ключ $s = g^b \in G$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$	G, g, n	G, g, n $s{=}g^b$

Вы и любовница передаете всем свои открытые ключи r и s. Поэтому эти элементы становятся известны всем в том числе и жене. Но никто не знает элементов a и b, так как для их поиска надо решить задачу дискретного логарифмирования в группе G, а мы выбрали ее и элемент $g \in G$ так, чтобы эта проблема была сложной.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s	G, g, n r, s	G, g, n $s{=}g^b$, r

Теперь можно построить приватный ключ. Делается это так. Вы возводите элемент s в степень a и получаете $s^a = (g^b)^a = g^{ab}$. Любовница возводит элемент r в степень b и получает $r^b = (g^a)^b = g^{ab}$. Теперь у вас у обоих есть секретный ключ $k = g^{ab}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$	G, g, n r, s	G, g, n $s{=}g^b$, r $k{=}r^b$

В результате описанной выше процедуры у вас и любовницы есть общий приватный ключ $k \in G$ и никто, даже ваша жена, не способны его найти. Однако, чтобы эта процедура была надежная, надо аккуратно выбирать группу G и элемент $g \in G$.

Передача сообщений Теперь самое время слать сладкие сообщения друг другу. Как я уже описал, мы должны перевести текстовые сообщения в элементы группы G. Предположим, что мы используем русский алфавит с 33 буквами. Еще можно использовать точку, запятую, восклицательный знак и знак пробела. Итого в общей сложности 37 символов. Всего существует 37^m текстовых строк длины m. Если $37^m \leqslant n$, мы можем отобразить все такие последовательности в элементы группы G инъективно.

Таким образом у нас есть механизм перевода сообщения в элементы группы G.

Теперь я собираюсь игнорировать стадию перевода. Наша цель – послать элемент группы G. Предположим, у нас есть элемент $h \in G$, который является сообщением, которое нужно послать любовнице.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h	G, g, n r, s	G, g, n $s{=}g^b$, r $k{=}r^b$

В начале надо зашифровать сообщение h. Зашифровка представляет из себя умножение h на приватный ключ k. Полученное сообщение $m = hk$ мы пересылаем любовнице.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h, $m = hk$	G, g, n r, s m	G, g, n $s{=}g^b$, r $k{=}r^b$ m

Любовнице, чтобы раскодировать сообщение надо поделить его на секретный ключ, то есть вычислить $h = mk^{-1}$. Если в группе операция взятия обратного отдельно не известна, то по следствию 3 из теоремы Лагранжа это выражение можно посчитать так: $h = mk^{-1} = mk^{n-1}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h, $m = hk$	G, g, n r, s m	G, g, n $s{=}g^b$, r $k{=}r^b$ m, $h = mk^{n-1}$

И вуаля, никто не пострадал, сообщение благополучно доставлено.

Модификация передачи В описанной выше схеме передачи информации приватный ключ остается одним и тем же на протяжение всего сеанса связи. Это делает систему более уязвимой. Существует следующая модификация с односторонней передачей информации. Глобально она устроена так: вы создаете и публикуете свой открытый ключ. Этот этап рассматривается как приглашение передавать вам информацию. Далее любовница начинает транслировать вам сообщение с переменным ключом. Давайте опишем этот процесс более аккуратно.

Для приглашения транслировать вам сообщения, вы должны придумать секретное $a \in \mathbb{Z}_n^*$ и передать всем открытый ключ $r = g^a$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$	G, g, n r	G, g, n r

Теперь предположим, что у любовницы есть последовательность сообщений $h_1, \ldots, h_k$. Тогда она выбирает для каждого сообщения h_i свое секретное $b_i \in \mathbb{Z}_n^*$. После создает открытый и приватный ключи по правилу $s_i = g^{b_i}$ и $k_i = r^{b_i}$. Каждое сообщение кодируется своим приватным ключом $m_i = h_i k_i$. После этого любовница транслирует в сеть пары $(m_1, s_1), \ldots, (m_k, s_k)$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$ (m_i, s_i)	G, g, n r (m_i, s_i)	G, g, n r $h_1, \ldots, h_k \in G$ $b_1, \ldots, b_k \in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

Чтобы расшифровать сообщение надо построить приватный ключ $k_i = s_i^a$. Это можете сделать только вы, так как только вы знаете a. Далее надо найти $h_i = m_i k_i^{-1}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$ (m_i, s_i) $k_i = {s_i}^a$, $h_i = m_i {k_i}^{-1}$	G, g, n r (m_i, s_i)	G, g, n r $h_1, \ldots, h_k \in G$ $b_1, \ldots, b_k \in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

Если мы хотим передавать сообщения в обратную сторону, то надо повторить всю схему с начала но симметрично. То есть любовница публикует свой открытый ключ, а вы уже генерируете серию зашифрованных сообщений.

3.5 RSA

Давайте я кратко расскажу, как работает схема шифрования RSA. Это схема односторонней передачи. Давайте я опишу ее по шагам.

Установка связи Если вы хотите, чтобы любовница передала вам сообщение вы должны проделать подготовительную работу. В начале вы придумываете два простых числа p и q и вычисляете $n = pq$. Число n публикуется для всех. И в качестве сообщений рассматриваются элементы $\mathbb{Z}_n^*$.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$	n, $\mathbb{Z}_n^*$	n, $\mathbb{Z}_n^*$

Теперь мы хотим построить открытый ключ, который позволит слать нам сообщения. Делается это так. В начале вычисляем $\varphi(n) = (p-1)(q-1)$.[8] Теперь мы берем произвольное число $e \in \mathbb{Z}_{\varphi(n)}^*$. Открытым ключом считается пара (e, n).

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

Теперь мы должны построить приватный ключ, для расшифровки сообщений. Для этого мы находим число $d \in \mathbb{Z}_{\varphi(n)}^*$ такое, что $de = 1$ в $\mathbb{Z}_{\varphi(n)}^*$. Это делается по расширенному алгоритму Евклида применяя его для поиска наибольшего общего делителя e и $\varphi(n)$. Приватным ключом считается пара (d, n). Обратите внимание, что никто не может получить d, так как для его вычисления надо знать $\varphi(n)$. А для ее вычисления надо знать разложение n на множители, что сложно.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

Передача сообщения Теперь предположим у любовницы есть для вас сообщение $h \in \mathbb{Z}_n^*$. Она должна вычислить зашифрованное сообщение по правилу $m = h^e \pmod{n}$. И сообщение m рассылается всем.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$ m	n, $\mathbb{Z}_n^*$ (e, n) m	$\mathbb{Z}_n^*$ (e, n) $h \in \mathbb{Z}_n^*$ $m = h^e \pmod{n}$

[8] Здесь $\varphi(n)$ – функция Эйлера, по определению $\varphi(n) = |\mathbb{Z}_n^*|$. С помощью результатов про структуру $\mathbb{Z}_n^*$ мы можем ее явно вычислить.

Чтобы расшифровать сообщение вы используете следующую функцию $h = m^d \pmod{n}$. Этот метод действительно работает, вот почему. Мы знаем, что $de = 1 \pmod{\varphi(n)}$. Это значит, что $de = 1 + \varphi(n)k = 1 + |\mathbb{Z}_n^*|k$. Теперь

$$m^d = h^{ed} = h^{1+|\mathbb{Z}_n^*|k} = h\left(h^{|\mathbb{Z}_n^*|}\right)^k = h \text{ в группе } \mathbb{Z}_n^*$$

Последнее равенство выполнено по следствию 3 из теоремы Лагранжа.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$ m $h = m^d \pmod{n}$	n, $\mathbb{Z}_n^*$ (e, n) m	$\mathbb{Z}_n^*$ (e, n) $h \in \mathbb{Z}_n^*$ $m = h^e \pmod{n}$