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 $ng = 0$.

[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.