

ЛЕКЦИЯ 1

Определение 1. Пусть G – некоторое множество. n -арной операцией на множестве G называется отображение

$$G \times \dots \times G \rightarrow G$$

из n -ой декартовой степени множества G в множество G .

Рассмотрим бинарную операцию $*$ на множестве G :

$$G \times G \rightarrow G, \quad (g_1, g_2) \rightarrow g_1 * g_2.$$

Определение 2. Непустое множество G с фиксированной бинарной операцией $*$ называется *группоидом*.

Рассмотрим следующие условия (аксиомы) на операцию $*$.

A1. Ассоциативность. Для любых элементов $a, b, c \in G$ выполнено $(a * b) * c = a * (b * c)$.

A2. Существование нейтрального элемента. Существует такой элемент $e \in G$, что для любого $g \in G$ выполняется $eg = ge = g$.

A3. Существование обратного элемента. Для каждого элемента $g \in G$ существует элемент $g^{-1} \in G$ такой, что $g * g^{-1} = g^{-1} * g = e$.

A4. Коммутативность. Для любых элементов $a, b \in G$ выполнено $a * b = b * a$.

Накладывая на операцию $*$ различные множества условий, мы будем получать различные алгебраические структуры.

Определение 3. Если $*$ удовлетворяет условию A1, то G называется *полугруппой*.

Если $*$ удовлетворяет условиям A1 и A2, то G называется *моноидом*.

Если $*$ удовлетворяет условиям A1 и A2 и A3, то G называется *группой*.

Условие A4 добавляет к названию структуры слово абелев (или, что то же самое, коммутативный). Так условия A1 и A4 задают *абелеву (коммутативную) полугруппу*, условия A1, A2 и A4 задают *абелев (коммутативный) моноид*, условия A1, A2, A3 и A4 задают *абелеву (коммутативную) группу*.

Обозначение 1. Если не очевидно, какая операция на множестве G имеется в виду, то будем использовать обозначение $(G, *)$ для множества G с операцией $*$.

Упражнение 1. Рассмотрим аксиому, являющуюся "половиной" аксиомы A2.

A2': Существует такой элемент $e \in G$, что для любого $g \in G$ выполняется $eg = g$. Докажите, что если структура $(G, *)$ удовлетворяет условиям A1, A2' и A3, то G является группой.

Задача 1. Рассмотрим аксиому, являющуюся "половиной" аксиомы A3.

A3': Для каждого элемента $g \in G$ существует элемент $g^\vee \in G$ такой, что $g * g^\vee = e$.

Существует ли структура $(G, *)$, удовлетворяющая условиям A1, A2 и A3', но не являющаяся группой.

Рассмотрим некоторые элементарные следствия из аксиом.

Лемма 1. Простые следствия из аксиом.

1) (Обобщенная ассоциативность) Пусть $(G, *)$ – полугруппа. И пусть $g_1, \dots, g_k \in G$. Тогда как бы ни были расставлены скобки в выражении $g_1 * g_2 * \dots * g_k$ результат будет одинаковым.

- 2) В моноиде есть единственная единица.
 3) В группе для каждого элемента есть единственный обратный.
 4) Пусть $(G, *)$ – группа. Пусть $a, b \in G$. Тогда если $a * b = e$, то $b = a^{-1}$. Аналогично если $b * a = e$, то $b = a^{-1}$.
 5) Пусть $(G, *)$ – группа, $a, b \in G$. Тогда $(a * b)^{-1} = b^{-1} * a^{-1}$.
 6) Пусть $(G, *)$ – группа, $g \in G$. Тогда $(g^{-1})^{-1} = g$.

Доказательство. 1) Докажем это утверждение индукцией по k .

База индукции $k = 3$. В этом случае обобщенная ассоциативность совпадает с ассоциативностью, то есть с аксиомой A1.

Шаг индукции. Предположим, что для $k < n$ данное утверждение уже доказано. Докажем его для $k = n$. Среди всех расстановок скобок есть стандартная (при ней действия выполняются справа-налево):

$$(\dots (g_1 * g_2) * g_3) * \dots * g_{n-1}) * g_n = g.$$

Достаточно доказать, что результат, который получается при произвольной расстановке скобок, совпадает с g . Фиксируем некоторую расстановку скобок. Для этой расстановки скобок есть последнее действие, которое даст операцию от двух скобок. Длинной скобки назовем количество g_i , входящих в нее. Докажем, что результат совпадает с g индукцией по длине правой скобки (обозначим эту длину s).

База второй индукции $s = 1$. Наша расстановка скобок имеет вид $(\dots) * g_n$. По предположению первой индукции в левой скобке можно расставить скобки произвольным образом. В том числе стандартным образом. Но тогда в целом мы получим стандартную расстановку скобок. Значит, результат при нашей расстановке скобок совпадает с результатом при стандартной расстановке скобок.

Шаг второй индукции. Пусть при $s < t$ утверждение доказано ($t \geq 2$). Докажем при $s = t$. Последнее действие при нашей фиксированной расстановке скобок имеет вид $(a) * (b)$. Поскольку длина скобки (b) равна $t \geq 2$, то $b = (c) * (d)$. Тогда $(a) * (b) = (a) * ((c) * (d))$. Применяя аксиому A1, получаем

$$(a) * ((c) * (d)) = ((a) * (c)) * (d).$$

Но длина скобки (d) строго меньше, чем длина скобки $(b) = ((c) * (d))$. Значит, по предположению второй индукции результат получающийся при расстановке скобок $((a) * (c)) * (d)$ совпадает с g .

2) Предположим, что в моноиде $(G, *)$ есть две единицы: e и s . Рассмотрим $e * s$. Поскольку e – единица, получаем $e * s = s$. С другой стороны так как s – единица, то $e * s = e$. Таким образом, $e = s$.

3) Пусть $(G, *)$ – группа. Предположим, что $g \in G$ – элемент, у которого есть хотя бы два обратных: f и h . Тогда $f = f * (g * h) = (f * g) * h = h$.

4) Пусть $a * b = e$. Рассмотрим операцию элемента a^{-1} и левой части и приравняем к операции элемента a^{-1} и правой части. (Домножим на a^{-1} слева.) Получим $a^{-1} * a * b = a^{-1} * e$. То есть $b = a^{-1}$.

Если $b * a = e$, то аналогично домножая слева на a^{-1} , получаем $b = a^{-1}$.

5) Обозначим $b^{-1} * a^{-1} = c$. Рассмотрим $(a * b) * c = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$. Значит, $c = (a * b)^{-1}$.

6) $g^{-1} * g = e$, значит $g = (g^{-1})^{-1}$. □

Определение 4. Подмножество H группы $(G, *)$ называется *подгруппой*, если $(H, *)$ является группой.

Подмножество S группы $(G, *)$ называется *замкнутым относительно операции $*$* , если для любых $a, b \in S$ выполнено $a * b \in S$. Подмножество S группы $(G, *)$ называется *замкнутым относительно взятия обратного*, если для любого $s \in S$ элемент s^{-1} также принадлежит S .

Предложение 1. *Непустое подмножество H группы $(G, *)$ является подгруппой тогда и только тогда, когда оно замкнуто относительно операции и замкнуто относительно взятия обратного.*

Доказательство. Если $(H, *)$ – группа, то операция $*$ корректно определена на H . Значит, H замкнуто относительно операции $*$. Пусть e – нейтральный элемент группы G , а s – нейтральный элемент группы H . Получаем $s * s = s$. В группе G есть обратный к s элемент s^{-1} . Умножая на него слева предыдущее равенство, получаем $s = e$. То есть единицы у групп G и H совпадают. Для каждого $g \in H$ есть обратный элемент g^{-1} в группе G и есть обратный элемент обратный элемент $g^\vee$ в группе H . Тогда $g * g^{-1} = e = g * g^\vee$. Умножив слева на g^{-1} , получаем $g^{-1} = g^\vee$. Поскольку для группы $(H, *)$ выполнена аксиома А3, то H замкнуто относительно взятия обратного.

Пусть теперь подмножество H замкнуто относительно операции и взятия обратного. Так как H замкнуто относительно операции, $(H, *)$ – группоид. Поскольку ассоциативность выполнена в G , то она выполнена и в H . Подмножество не пусто. Возьмем элемент $h \in H$. Так как H замкнуто относительно взятия обратного, $h^{-1} \in H$. Пользуясь замкнутостью H относительно операции, получаем $h * h^{-1} = e \in H$. Таким образом, в H выполнена аксиома А2. Поскольку H замкнуто относительно взятия обратного, в H выполнена и аксиома А3. $\square$

Зачастую вместо слова "операция" используют слово "умножение". Суть от этого не меняется и имеется в виду некоторая операция в группе. При этом на письме так же как и в случае обычного умножения чисел знак умножения можно опускать. Нейтральный элемент группы в этом случае зачастую называют "единицей группы". Такие обозначения называются *мультипликативными*.

Если заранее известно, что группа абелева, то часто используют *аддитивные* обозначения. Операция называется сложением и обозначается знаком $+$ нейтральный элемент называется нулем, а обратный элемент называется "противоположным элементом".

Соберем эти обозначения в таблице.

общие обозначения	мультипликативные обозначения	аддитивные обозначения
произвольная группа	произвольная группа	абелева группа
операция $*$	умножение $\cdot$	сложение $+$
нейтральный элемент e	единица e	ноль 0
обратный элемент g^{-1}	обратный элемент g^{-1}	противоположный элемент $-g$

Определение 5. Порядок группы G – это количество элементов в этой группе. (То есть мощность множества G .) Порядок группы G обозначается $|G|$.

Определение 6. Пусть g – элемент группы G , а n – целое число. Определим n -ю степень элемента g следующим образом. Если n положительное, то $g^n =$

$g \cdot \dots \cdot g$ – произведение n элементов g . Если n отрицательное, то $g^n = (g^{-1})^n$. Нулевая степень любого элемента равна нейтральному элементу e .

Упражнение 2. Выполнены следующие свойства степеней элемента группы:

- 1) $g^m g^n = g^{m+n}$,
- 2) $(g^m)^n = g^{mn}$

Указание. Рассмотреть все случаи знаков m и n .

Определение 7. Пусть g – элемент группы G . Порядок g – это минимальное натуральное число n такое, что $g^n = e$. Если такого числа не существует, то порядок элемента g равен бесконечности. Порядок элемента g обозначается $\text{ord}g$.

Лемма 2. Пусть g – элемент группы G такой, что $\text{ord}g = n$, а m – целое число. Тогда

$$\text{ord}g^m = \frac{n}{\text{НОД}(m, n)}.$$

Доказательство. По свойству степеней $(g^m)^k = g^{mk}$. Следовательно порядок g^m – это минимальное натуральное k такое, что mk делится на n .

Рассмотрим разложения на простые множители чисел n и m . Можем считать, что простые множители входящие в m и n одинаковы, но при этом степени вхождения могут быть равны нулю.

$$n = p_1^{\alpha_1} \dots p_l^{\alpha_l}, \quad m = p_1^{\beta_1} \dots p_l^{\beta_l}.$$

Имеем: $\text{НОД}(m, n) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_l^{\min\{\alpha_l, \beta_l\}}$.

Отсюда

$$\begin{aligned} \frac{n}{\text{НОД}(m, n)} &= p_1^{\alpha_1 - \min\{\alpha_1, \beta_1\}} \dots p_l^{\alpha_l - \min\{\alpha_l, \beta_l\}} = \\ &= p_1^{\max\{\alpha_1 - \beta_1, 0\}} \dots p_l^{\max\{\alpha_l - \beta_l, 0\}} \end{aligned}$$

Легко видеть, что это минимальное число k такое, что km делится на $p_i^{\alpha_i}$ для каждого i . $\square$

Конечную группу можно задавать с помощью таблицы умножения. Таблица умножения – это квадратная таблица, строки и столбцы которой соответствуют элементам группы. А на пересечении строки и столбца стоит произведение элемента, соответствующее строки и элемента, соответствующего столбцу.

Пример 1. Построим таблицу сложения для группы $(\mathbb{Z}_2, +) = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

Примеры групп.

1) Числовые аддитивные группы:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +).$$

Нейтральный элемент 0, обратный к элементу x – это $-x$. Выполнение аксиом следуют из свойств сложения чисел. Все данные группы бесконечны и коммутативны.

2) Группа вычетов (остатков) по модулю n : $(\mathbb{Z}_n, +)$. Сложение происходит по модулю n . Нейтральный элемент 0 , обратный к элементу x – это $n - x$. Выполнение аксиом следуют из свойств остатков. Данная группа коммутативна и имеет порядок n .

3) Числовые мультипликативные группы:

$$\mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}, \cdot), \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot), \mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot).$$

Нейтральный элемент 1 , обратный к элементу x – это $\frac{1}{x}$. Выполнение аксиом следуют из свойств умножения чисел. Данные группы бесконечны и коммутативны.

4) (Обобщение примера 3) Пусть R – кольцо с единицей. Обозначим множество обратимых элементов через $R^\times$. Рассмотрим группу обратимых элементов $(R^\times, \cdot)$. Нейтральный элемент – единица кольца. Обратные элементы существуют так как $R^\times$ состоит из обратимых элементов. Если R – коммутативное кольцо, то $R^\times$ – коммутативная группа.

Задача 2. Приведите пример некоммутативного кольца R такого, что $R^\times$ – коммутативная группа порядка больше 1.

5) Группа комплексных корней из единицы n -ой степени. Пусть $\mathcal{C}_n$ – множество всех комплексных корней степени n из 1. Тогда $(\mathcal{C}_n, \cdot)$ – абелева группа порядка n . Докажем это. Для того, чтобы доказать, что $\mathcal{C}_n$ – группа мы воспользуемся, тем, что это подмножество в известной нам группе $\mathbb{C}^\times$. Нам надо лишь проверить, что $\mathcal{C}_n$ замкнуто относительно умножения и взятия обратного. Пусть $a, b \in \mathcal{C}_n$, то есть $a^n = b^n = 1$. Тогда $(ab)^n = a^n b^n = 1$, значит, $ab \in \mathcal{C}_n$. Мы доказали, что $\mathcal{C}_n$ замкнуто относительно умножения. С другой стороны $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, следовательно, $\mathcal{C}_n$ замкнуто относительно взятия обратного. То, что группа $\mathcal{C}_n$ абелева следует из того, что она является подгруппой в абелевой группе $\mathbb{C}^\times$.

Единица этой группы – это 1, обратный к элементу x – это $\frac{1}{x}$.

6) Группы перестановок.

а) Множество S_n всех перестановок n элементов с операцией композиции $\circ$ является группой. Докажем это. Нейтральный элемент этой группы – это тождественная перестановка, обратный элемент – обратная перестановка. Ассоциативность следует из следующей важной леммы.

Лемма 3. Пусть есть четыре множества: X, Y, Z и T . И пусть фиксированы отображения между этими множествами $\varphi: X \rightarrow Y, \psi: Y \rightarrow Z$ и $\zeta: Z \rightarrow T$. Тогда $(\zeta \circ \psi) \circ \varphi = \zeta \circ (\psi \circ \varphi)$.

Доказательство. Возьмем элемент $x \in X$. Тогда

$$(\zeta \circ \psi) \circ \varphi(x) = (\zeta \circ \psi)(\varphi(x)) = (\zeta(\psi(\varphi(x)))).$$

С другой стороны

$$\zeta \circ (\psi \circ \varphi)(x) = \zeta(\psi \circ \varphi(x)) = (\zeta(\psi(\varphi(x)))).$$

□

Применяя данную лемму к случаю $X = Y = Z = T = \{1, 2, \dots, n\}$ получаем ассоциативность S_n . Порядок группы S_n равен $n!$. При $n > 3$ группа S_n не коммутативна.

б) Множество A_n четных перестановок из S_n с операцией композиции образует *группу четных перестановок*. Докажем, что A_n – подгруппа S_n . Это следует из того, что произведение четных перестановок – четная перестановка и обратная к четной перестановке четная. Группа A_n не коммутативна при $n \geq 4$.

в) Группа Клейна. Рассмотрим множество перестановок (в виде произведения независимых циклов) $\{\text{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Несложно проверить, что это множество замкнуто относительно композиции и что каждая перестановка из этого множества обратна самой себе. Получаем, что данные перестановки образуют подгруппу в S_4 , которая обозначается V_4 . Эта группа коммутативна.

б') (Обобщение примера ба) Пусть X – некоторое множество (возможно бесконечное). Рассмотрим множество $S(X)$ биекций $X \rightarrow X$ с операцией композиции. Если $|X| < \infty$, то получаем группу перестановок. В общем случае получаем *группу симметрий множества X* . Нейтральный элемент – тождественное преобразование. Обратный – обратное преобразование. Ассоциативность следует из леммы 3.

7) Матричные группы. Пусть $\mathbb{K}$ – поле.

а) $GL_n(\mathbb{K})$ – множество невырожденных матриц $n \times n$ с элементами из $\mathbb{K}$. Легко видеть, что это множество замкнуто относительно умножения матриц. Умножение матриц ассоциативно, единичная матрица – нейтральный элемент и все невырожденные матрицы обратимы (обратная также невырождена). Следовательно, $(GL(\mathbb{K}), \cdot)$ – группа.

б) $SL_n(\mathbb{K})$ – множество $n \times n$ матриц с определителем 1 с элементами из $\mathbb{K}$. Это подмножество замкнуто относительно умножения и взятия обратного.

Эти группы конечны тогда и только тогда, когда поле $\mathbb{K}$ конечно.

8) Группы преобразований векторного пространства. (Подгруппы в группе $S(V)$, где V – векторное пространство.)

а) Группа обратимых линейных преобразований V .

б) Группа ортогональных линейных преобразований V .

в) Группа обратимых аффинных преобразований V .

г) Группа движений V .

Во всех этих группах нейтральный элемент – тождественное преобразование, а обратный элемент – обратное преобразование. Эти группы конечны тогда и только тогда, когда поле, над которым V – векторное пространство конечно и размерность V конечна.