

ЛЕКЦИЯ 1

Определение 1. Пусть G – некоторое множество. *бинарной операцией* на множестве G называется отображение

$$G \times G \rightarrow G$$

из 2-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 $*$.

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 ·	сложение +
нейтральный элемент e	единица e	ноль 0
обратный элемент g^{-1}	обратный элемент g^{-1}	противоположный элемент $-g$

Предложение 1. (Простые следствия из аксиом.)

Пусть $(G, *)$ – группа.

- 1) (*Обобщенная ассоциативность*) 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 G есть единственная единица.
- 3) В G для каждого элемента есть единственный обратный.
- 4) 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 $g \in G$. Тогда $(g^{-1})^{-1} = g$.
- 6) Пусть $a, b \in G$. Тогда $(a * b)^{-1} = b^{-1} * a^{-1}$.

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 слева-направо):

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

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 дает операцию от двух скобок. Длиной скобки назовем количество g_i , входящих в нее. Обозначим длину правой скобки через s .

Случай 1 $s = 1$. Наша расстановка скобок имеет вид $(\dots) * g_n$. По предположению 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.

Случай 2 $s \geq 2$. Последнее действие при нашей фиксированной расстановке скобок имеет вид $(a) * (b)$. Длина скобки b меньше n . По предположению индукции можно считать, что в скобке b расстановка скобок стандартная. Таким образом, стандартная расстановка скобок в скобке b дает $b = d * g_n$. То есть $g = a * (d * g_n) = (a * d) * g_n$. По случаю 1 мы получаем, что в g можно расставить скобки стандартным образом.

2) Предположим, что в $(G, *)$ 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) 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 $g = (g^{-1})^{-1}$. \square

Определение 4. Порядок группы G – это количество элементов в этой группе. (То есть мощность множества G .) Порядок группы G обозначается $|G|$.

Определение 5. 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 .

Лемма 1. Пусть H – подмножество группы $(G, *)$. Тогда H является подгруппой в G тогда и только тогда, когда выполнены следующие три условия

- 1) H не пусто;
- 2) H оно замкнуто относительно операции;
- 3) H замкнуто относительно взятия обратного.

Доказательство. Если $(H, *)$ – группа, то операция $*$ корректно определена на H . Значит, H замкнуто относительно операции $*$. Так как по определению группы в ней есть нейтральный элемент, она является непустым множеством. 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 непустое 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

Примеры групп.

- 1) Числовые аддитивные (то есть по сложению) 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) 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.

3) 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 .

4) Группы перестановок. 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 2. Пусть есть четыре множества: X, Y, Z и W . И пусть фиксированы отображения между этими множествами $\varphi: X \rightarrow Y, \psi: Y \rightarrow Z$ и $\zeta: Z \rightarrow W$. 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 $X = Y = Z = W = \{1, 2, \dots, n\}$ получаем ассоциативность S_n . Порядок группы S_n равен $n!$. При $n \geq 3$ группа S_n не коммутативна.

5) Матричные группы. Пусть \mathbb{K} – поле, например, \mathbb{Q}, \mathbb{R} или \mathbb{C} .

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 в $GL(\mathbb{K})$ замкнуто относительно умножения и взятия обратного. Следовательно, это подгруппа.

в) $O_n(\mathbb{K})$ – множество ортогональных матриц $n \times n$ с элементами из \mathbb{K} . Это подмножество в $GL(\mathbb{K})$ замкнуто относительно умножения и взятия обратного. Следовательно, это подгруппа.

Эти группы конечны тогда и только тогда, когда поле \mathbb{K} конечно. Они не коммутативны при $n \geq 2$.

6) Группы преобразований.

а) (Обобщение примера 4) 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 2.

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

- Группа обратимых линейных преобразований V .
- Группа ортогональных линейных преобразований V .
- 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.

в) Группа симметрий фигуры (то есть движений, сохраняющих фигуру).

Упражнение 1. Докажите, что движения, сохраняющие данную фигуру, образуют подгруппу в группе всех движений.