Группы

Забродин Денис Александрович

7 сентября 2022 г.

Содержание

1 Группы **2**
1.1 Нейтральный элемент 2
1.2 Симметричный элемент 2
1.3 Группа 2
1.4 Порядок группы и элемента 4
1.5 Малая теорема Ферма 4

1 Группы

1.1 Нейтральный элемент

Пусть S - произвольное множество. Алгебраической операцией * на множестве S называется отображение *: $S * S \to S$

Элемент e ∈ S называется нейтральным элементом относительно операции *, если для каждого элемента a ∈ S верно

$$a * e = e * a = a$$

Утверждение 1. Нейтральный элемент (если он существует) единственен.

Доказательство проведем от обратного: пусть найдутся два нейтральных элемента e' ∈ S и e" ∈ S, e' ≠ e". Тогда

$$e' * e''$$

$$e' = e' * e'' = e''$$

1.2 Симметричный элемент

Для элемента a ∈ S элемент a ∈ S называется **симметричным**, если

$$a * a' = a' * a = e,$$

где e ∈ S - нейтральный элемент относительно операции *.

Утверждение 2. Симметричный элемент относительно ассоциативной операции (если он существует) единственен.

Доказательство проведем от обратного: пусть для некоторого элемента a ∈ S найдутся два симметричных элемента a' ∈ S и a" ∈ S, a' ≠ a". Тогда

$$a' * a * a''$$

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$$

1.3 Группа

Множество S с одной или несколькими введенными на нем операциями называется алгебраической структурой. Структура G = (S; *) (т. е. множество S с введенной на нем алгебраической операцией *) называется группой, если

1. операция * ассоциативна, т. е. для любых элементов a, b, c ∈ S верно

$$(a * b) * c = a * (b * c)$$

2. существует нейтральный элемент относительно операции *, т. е. найдется такой элемент e ∈ S, что для каждого элемента a ∈ S верно

$$a * e = e * a = a$$

3. для каждого элемента a ∈ S найдется симметричный к нему элемент a' ∈ S, т. е. такой что

$$a * a' = a' * a = e)$$

Если для группы G = (S; *) дополнительно выполнено, что операция * коммутативна, т. е. для любых элементов a, b ∈ S верно

$$a * b = b * a$$

то такая группа называется **коммутативной**, или **абелевой**.

Утверждение 3 (правило сокращения). Пусть G = (S; *) - группа. Тогда если для некоторых элементов a, b, c ∈ G верно

a * b = a * c (или b * a = c * a), то b = c

Доказательство. Пусть элемент a' ∈ G симметричен относительно операции * к элементу a ∈ G . Элемент a' ∈ G найдется, т. к. G – группа. Тогда

$$a * b = a * c$$

$$a' * a * b = a' * a * c$$

$$b = e * b = (a' * a) * b = (a' * a) * c = e * c = c$$

Утверждение 4. Таблица умножения конечной группы - это латинский квадрат. Напомню: латинский квадрат - это таблица чисел, в каждой строке и в каждом столбце которой записаны все элементы группы.

Доказательство. Обозначим элементы группы через $a_1, a_2, \ldots, a_n$. Какие элементы записаны в n-ом столбце? Те, что определяются умножением $a_n * a_1, a_n * a_2, a_n * a_3, \ldots, a_n * a_n$. Допустим, что два выражения из этого списка равны, то есть существуют два индекса j и k такие, что $a_n * a_i = a_n * a_k$. Так как a_n приводится в обеих частях выражения, по закону сокращения имеем $a_j = a_k$. Таким образом, в этом столбце нет двух одинаковых элементов! Но так как группа состоит из n элементов, а в столбце таблицы нужно записать n неповторяющихся элементов, то в этом столбце будут записаны все элементы группы

1.4 Порядок группы и элемента

Группа G = (S; *) называется **конечной**, если в множестве S конечное число элементов. Если группа G = (S; *) конечна, то число элементов в множестве S называется ее **порядком** и обозначается |G|

Пусть G = (S; *) - группа с нейтральным элементом e. Для элемента a ∈ G наименьшее натуральное число n (если оно существует), такое что

$$\underbrace{a * a * \ldots * a}_{n} = e$$

, называется его **порядком**
Вам может показаться, что это определение не имеет ничего общего с предыдущим, но это не так.

Рассмотрим произвольный элемент группы, например a. Мы можем составить группу степеней a, то есть <a> = $a, a^2, a^3 \ldots$. Допустим, что a имеет порядок n в соответствии со вторым определением, то есть a^n - нейтральный элемент. Тогда перечень степеней остановиться на a^n = e и затем начнется сначала. Множество будет содержать всего n элементов. И это непростое множество: <a>, в свою очередь, является группой: оно содержит нейтральный элемент, результат операции над двумя степенями a всегда равен степени a, и элемент a^{n-i} является обратным для a^i. Следовательно, порядок элемента - это порядок множества, состоящего из его степеней

1.5 Малая теорема Ферма

$$\forall \text{ простого p; } \forall \text{ a} \in \mathbb{Z}$$

$$a^p - a \mid p$$

или

$$\forall \text{ просто p; } \forall \text{ a} \nmid \text{p}$$

$$a^{p-1} - 1 \mid p$$

Лемма: Для любого простого числа p и целого числа k, не кратного p, произведения k и чисел 1, 2, 3, . . . , p-1 при делении на p в остатке дают те же самые числа 1, 2, 3, . . . , p-1, возможно, записанные в некотором другом порядке.

Доказательство леммы: Произведение k и любого из чисел 1, 2, 3, . . . , p-1 не кратно, следовательно, в остатке не может получиться 0. Все остатки разные. Докажем последнее утверждение от противного. Пусть при $a, b \in 1, 2, 3, \ldots, p-1$ и $a \neq b$ два произведения ak и bk дают при делении

на p одинаковые остатки, тогда разность $ak - bk = (a - b)k$ кратна p, что невозможно, поскольку a - b не кратно p. Всего существует p - 1 различных ненулевых остатков от деления на p.

Доказательство: Пусть {1, 2, ..., p-1} - ненулевые остатки от деления на p, тогда согласно вышеприведённой лемме остатки от деления чисел $a, 2a, 3a, \ldots, (p-1)a$ - это с точностью до перестановки числа {1, 2, ..., p-1}, то $a * 2a * 3a, \ldots, (p-1) * a \equiv 1 * 2 * 3 * \ldots * (p-1)(mod\ p)$. Отсюда $a^{p-1}(p-1)! \equiv (p-1)!(mod\ p)$. Последнее соотношение можно сократить на (p-1)!, поскольку все сомножители являются числами, взаимно простыми с основанием p, в результате получаем требуемое утверждение
$a^{p-1} \equiv 1(mod\ p)$

Доказательство 2: $(a+b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b + \ldots + C_p^{p-1} + b^p$

$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p(p-1)!}{k!(p-k)!}$, тк $C_p^k \in \mathbb{Z}$, то и $\frac{p(p-1)!}{k!(p-k)!} \in \mathbb{Z}$

k $\in \{1, 2, 3, \ldots, p\text{-}1\} \Rightarrow p \nmid k!(p-k)! \Rightarrow (p-1)! \mid k!(p-k)!$

$\frac{(p-1)!}{k!(p-k)!} = l \in \mathbb{Z} \Rightarrow C_p^k = pl \Rightarrow C_p^k \mid p$

$(a+b)^p \equiv a^p + b^p \pmod{p}$

Дальнейшие вычисления происходят по модулю p

$(1+1)^p \equiv 1^p + 1^p \equiv 2 \equiv 2^p$

$(2+1)^p \equiv 2^p + 1^p \equiv 2 + 1 \equiv 3 \equiv 3^p$

$k \in \mathbb{N}$ **База:** Пусть верно, что $(k+1)^p \equiv k^p + 1^p \equiv k + 1$

Переход: Докажем для k + 1

$((k+1)+1)^p \equiv (k+1)^p + 1^p$, тк $(k+1)^p \equiv k + 1$, то
$(k+1)^p + 1^p \equiv k + 1 + 1 \equiv k + 2 \equiv (k+2)^p$ чтд

Для k < 0 доказывается аналогично $\Rightarrow$ k $\in \mathbb{Z} \Rightarrow$ Выражение $a^n \equiv a$ верно для a $\in \mathbb{Z}$

Замечание: Для k = 0 можно проверить руками
Для p = 2 и k < 0:
$(-k+1)^2 \equiv (-k)^2 - 2k + 1^p \equiv (-k)^2 + 1^p$