

ОВАиТК-3

Рефлексируем над семинаром

На семинаре мы разобрали некоторые свойства гомоморфизма $\phi : G \rightarrow H$:

1. $\phi(e_G) = e_H$
2. $\phi(g)^{-1} = \phi(g^{-1})$
3. $\phi(g^n) = \phi(g)^n$
4. $\text{ord } \phi(g) \mid \text{ord } g$
5. $\ker \phi = \phi^{-1}(e) < G$

Скоро мы узнаем, какие подгруппы могут быть *ядром* гомоморфизма, а какие — нет.

Также мы разобрались с такой конструкцией, как декартово произведение групп $G \times H$. Носителем такой группы является декартово произведение $G \times H$ как декартово произведение множеств, а операций — поэлементное умножение: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$

Домашнее задание

1. Про абелевы группы

Докажите, что отображения $g \mapsto g^{-1}$ и $g \mapsto g^2$ являются гомоморфизмами тогда и только тогда, когда группа абелева

2. Разложение группы рациональных чисел

Существуют ли такие нетривиальные группы G и H , что $\mathbb{Q} \cong G \times H$?

3. Немного о числе решений уравнения $x^n = e$

Покажите, что если в некоторой *конечной* группе $\forall n$ уравнение $x^n = e$ имеет не более n корней, то эта группа — циклическая.

Note: Заметим, что обратное утверждение тривиально: если $G \cong C_n$, то уравнение $x^n = e$ имеет либо 0, либо n решений в зависимости от того, является n делителем порядка группы или нет.

4. Немного о числе решений уравнения $x^n = e$

Покажите, что в общем случае число решений $x^n = e$ в группе может быть сколь угодно велико.

Разбор домашнего задания №1

1. Аксиоматика группы

Левая единица равна правой:

$e_l \cdot e_r = e_l$ по определению правой единицы

$e_l \cdot e_r = e_r$ по определению левой единицы

Отсюда $e_l = e_r = e$, и e обладает свойствами единицы.

Для доказательства единственности единицы можно действовать от противного, предположить, что единицы две (e_1 и e_2) и рассмотреть произведение $e_1 e_2$. А можно просто заметить, что мы уже доказали, что *любая* левая единица и *любая* правая единица равны между собой, из чего автоматически следует единственность.

С обратным все то же самое, только надо рассматривать произведение $y_l x y_r$.

2. Аксиоматика группы

Можно было действовать по следующему плану:

- Доказать замкнутость операции: $(AB)^T = B^T A^T AB = B^T B = E$
- Сказать, что произведение ассоциативно, поскольку матрицы суть отображения, а их произведение суть композиция отображений (ассоциативность отображений мы разобрали на семинаре). Также можно было проверить это явно.
- Заметить, что E — ортогональная, а значит в $O(n, \mathbb{R})$ есть единица.
- Заметить, что обратная к ортогональной матрице ортогональна: $A^T (A^T)^T = A^T A = E$

Замечу, что доказывать единственность единицы и обратного элемента не нужно, поскольку мы ее уже доказали в общем случае в задаче №1.

3. Абелева группа

$$\forall x, y : xy = xy \cdot xx = xy \cdot xyx = (xy)^2 yx = yx$$

4. Таблица умножения

Предположим, что в некоторой строке есть два одинаковых значения. Пусть это строка с элементом a и столбцы b и c . Тогда $ab = ac$. Домножив это равенство на a^{-1} слева, получим $b = c$. Противоречие.

Аналогичное рассуждение со столбцами.

5. Изоморфизм

Искомая биекция ϕ сопоставляет остаток k углу $\frac{2\pi k}{n}$. Нетрудно видеть, что это действительно взаимно-однозначное соответствие между множествами.

Проверим, что операция сохраняется. Например, можно записать явное выражение для суммы. Сумма в \mathbb{Z}_n :

$$k_1 + k_2 = \begin{cases} k_1 + k_2, & k_1 + k_2 < n \\ k_1 + k_2 - n, & k_1 + k_2 \geq n \end{cases}$$

Сумма в группе поворотов (под $t(\alpha)$ будем понимать поворот на угол α):

$$t\left(\frac{2\pi k_1}{n}\right) + t\left(\frac{2\pi k_2}{n}\right) = \begin{cases} t\left(\frac{2\pi(k_1 + k_2)}{n}\right), & k_1 + k_2 < n \\ t\left(\frac{2\pi(k_1 + k_2)}{n} - 2\pi\right), & k_1 + k_2 \geq n \end{cases}$$

Отсюда следует равенство $\phi(k_1 + k_2) = \phi(k_1)\phi(k_2)$

6. Изоморфизм-2

Посмотрим на эту задачу с высоты новых знаний: можно заметить, что $\mathbb{Z}_5^* \cong C_4$ и $\mathbb{Z}_{12}^* \cong C_2 \times C_2$.

В первом случае порождающим элементом является, например, остаток 2:

$$2^1 = 2 \pmod{5}$$

$$2^2 = 4 \pmod{5}$$

$$2^3 = 3 \pmod{5}$$

$$2^4 = 1 \pmod{5}$$

Во втором случае отображение, устанавливающее изоморфизм, такое:

$$1 \mapsto (e, e)$$

$$5 \mapsto (a, e)$$

$$7 \mapsto (e, b)$$

$$11 \mapsto (a, b)$$

(проверьте корректность)

Чтобы показать, что C_4 и $C_2 \times C_2$ не изоморфны, достаточно рассмотреть порядки их элементов: в C_4 есть элемент порядка 4, а в $C_2 \times C_2$ — нет. В последней группе порядки всех элементов, кроме нейтрального, равны 2.

Самым простым способом решить эту задачу было заметить, что в \mathbb{Z}_{12}^* каждый элемент в квадрате дает себя, а в \mathbb{Z}_5^* — нет.