ОВАиТК-1

Ум сугубо математический будет правильно работать, только если ему заранее известны все определения и начала, в противном случае он сбивается с толку и становится невыносимым

Блез Паскаль

Рефлексируем над семинаром

Определение 1. *Пара $G = (X, \cdot)$ из множества X и "правила умножения" на нем, т.е. отображения $\cdot : X \times X \to X$ называется группой, если выполнены три аксиомы:*

1. *Операция умножения ассоциативна: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ для любых x, y, z из X*
2. $\exists! e \in X : \ \forall x \in X \ ex = xe = x$
3. $\forall x \in X \ \exists! y : \ xy = yx = e$

Если это не приводит к путанице, множество X (*носитель* группы) будем обозначать той же буквой, что и группу, а также пропускать знак умножения при записи формул. Обратный к x элемент из третьей аксиомы также принято записывать x^{-1}.

Определение 2. *Группа G называется коммутативной, или абелевой, если $\forall x, y \in G \ xy = yx$*

Существует негласное соглашение обозначать операцию в абелевой группе с помощью знака $+$, а нейтральный и обратный элементы — как 0 и $-x$ соответственно.

На семинаре мы познакомились с некоторыми примерами групп. Вот их список:

1. "Числовые" группы по сложению.

   Сюда относятся множества рациональных, вещественных и комплексных чисел с операцией сложения. Далее будем обозначать их как $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ соответственно.

2. "Числовые" группы по умножению.

   Множества из предыдущего пункта не образуют группы по умножению, однако если выбрать среди них все обратимые элементы (все числа, кроме нуля), то все аксиомы группы будут выполнены. Будем их обозначать так: $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

3. Все линейные пространства над $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ с операцией сложения. Аксиомы линейного пространства можно найти на википедии или в любом учебнике по линейной алгебре. Сюда же можно отнести и $Mat(n, F)$ — множество всех квадратных матриц $n \times n$ с операцией сложения над F. Здесь и далее под F подразумевается любое из множеств $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$, а словосочетание "матрица над F" означает, что элементами матрицы являются элементы из F.

4. Матричные группы по умножению. Так же, как и "числовые" группы, множество всех матриц не образует группу из-за необратимых элементов. Поэтому самая большая по включению группа матриц по умножению — $GL(n, F)$ (general linear) которая состоит из всех обратимых матриц ($\det A \neq 0$) рамера $n \times n$ над F.

   Другие известные группы:

(a) $SL(n, F)$ (special linear) — группа матриц с детеминантом 1. Напомню, что $\det(AB) = \det A \cdot \det B$, из-за чего произведение двух матриц из $SL(n, F)$ лежит в $SL(n, F)$.

(b) $O(n, F)$ — ортогональные матрицы. Задаются условием $AA^T = A^T A = E$ и являются матрицами перехода между ортонормированными базисами.

5. Группа перестановок S_n множества $\{1, \ldots, n\}$ (она же группа биекций на себя, она же группа автоморфизмов).
6. Диэдральная группа D_n — группа поворотов и отражений правильного n-угольника.
7. Группа вычетов по сложению $\mathbb{Z}_n$ — остатки от деления на n с операцией сложения по модулю n.
8. Группа вычетов по умножению $\mathbb{Z}_n^*$ — остатки от деления на n, взаимо простые с n, с операцией умножения по модулю n.

Домашнее задание

1. Аксиоматика группы

Докажите, что следующая система аксиом эквивалентна Определению 1:

1. Операция умножения ассоциативна: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ для любых x, y, z из X
2. $\exists e_l \in X : \ \forall x \in X \ e_l x = x$
3. $\exists e_r \in X : \ \forall x \in X \ x e_r = x$
4. $\forall x \in X \ \exists y_l : \ y_l x = e$
5. $\forall x \in X \ \exists y_r : \ x y_r = e$

2. Ортогональные матрицы

Покажите, что ортогональные матрицы являются группой.

3. Абелева группа

Для любого элемента x некоторой группы G выполнено $x^2 = e$. Докажите, что G — абелева.

4. Таблица умножения

Для группы G из n элементов можно записать таблицу умножения $n \times n$. Докажите, что она является разновидностью "магического квадрата": в каждом столбце и строке такой таблицы каждый элемент встречается ровно один раз.

5. Изоморфизм

В теории групп очень важное место занимает понятие "изоморфизм" — такая биекция между группами, сохраняющая операцию. Более формально, это такое биективное отображение ϕ из носителя группы G в носитель группы H, что $\forall a, b \in G : \ \phi(xy) = \phi(x)\phi(y)$. Группы, между которыми есть изоморфизм, называются *изоморфными*.

Можно сказать так: две группы изоморфны, если в них одинаковой число элементов, и их таблицы умножения получаются друг из друга переобозначением элементов.

Докажите, что группа вычетов по сложению $\mathbb{Z}_n$ изоморфна группе поворотов плоскости на углы, кратные $\dfrac{2\pi}{n}$

6*. Изоморфизм-2

Покажите, что $\mathbb{Z}_5^*$ не изоморфно $\mathbb{Z}_{12}^*$, хотя они содержат одинаковое число элементов.