Содержание

1. Введение в теорию групп **2**
1.1 Преобразования 2
1.2 Группы. Определение, примеры, базовые конструкции. 3
1.3 Порождение, циклические группы, порядок элемента 4
1.4 Гомоморфизм, изоморфизм 5
1.5 Действие группы на множестве 5
1.6 Дальнейший план того, что я не написал еще 6

1. Введение в теорию групп

Общая конва такова: следуем [Б01], добавляя нужные конкретно нам примеры. Делаем мощный упор в действие

1.1 Преобразования

Определение 1. Пусть M — некоторое множество элементов произвольной природы. Если каждой упорядоченной паре элементов из M поставлен в соответствие определённый элемент также из M, то говорят, что на M задана бинарная операция (обозначим её за $\circ$).

Говоря чуть более взрослым языком, бинарная операция — это отображение

$$\circ\colon M \times M \to M, \quad (m, m) \mapsto m \circ m \in M.$$

Пример 1. Для начала, всякие скучные числовые примеры.

Причём же тут преобразования? Оказывается, бинарные операции — удобный способ записывать, что происходит, когда мы проделываем последовательно много различных преобразований. Рассмотрим сначала некоторые примеры.

Пример 2. Повороты равностороннего треугольника, переводящие его в себя, *переставляют* вершины. Композиция преобразований — бинарная операция. Какие у неё свойства? Выпишем *таблицу умножения* (см. [Б01, пример 1]).

А еще есть симметрии, их тоже можно композицировать (и композицировать с поворотами).

Коллеги, сюда напишите Ваш любимый пример про строки и любимый пример про графы (по штуке, соовтественно).

Теперь давайте подумаем, какие свойства естественно было бы требовать от преобразований.

- Если мы говорим о преобразованиях одного типа, то естественно требовать, чтобы когда мы проделывали несколько одно за другим, получалось преобразование того же типа (как композиция поворотов — поворот).
- Во всех примерах мы видели, что есть *тождественное* преобразование (которое просто не делает ничего).
- Кроме того, композиция преобразований естественным образом *ассоциативна.* То есть, для любых преобразований f, g, h мы имеем $f \circ (g \circ h) = (f \circ g) \circ h = f \circ g \circ h$.
- В примерах мы также видели, что для каждого преобразования g существует преобразование h, которое после применения g возвращает ситуацию в исходный вид.

Теперь попробуем сделать наши примеры немного более строгими.

Определение 2. Напоминиание про функции, инъекции, сюръекции, биекции.

Приведём какой-нибудь не слишком скучный пример.

Пример 3. Пусть отображение φ ставит в соответствие каждому городу мира первую букву из его названия на русском языке (например, φ(Санкт-Петербург) = С). Будет ли φ отображением всех городов мира **на** весь русский алфавит?

Нет, не будет (так как едва ли есть город, начинающийся на ъ, например). Будет ли это отображение инъективным? Очевидно, что тоже нет.

Пока что мы понимали слово *преобразование* наивно, дадим теперь строгое математическое определение.

Определение 3. Произвольное взаимно однозначное отображение множества M на себя, $g\colon M \to M$, мы будем для краткости называть *преобразованием* множества M.

Пример 4. Если множество M конечное, то можно писать табличку и будет перестановка (слово перестановка тут еще не говорим), но тем не менее.

Определение 4. Так как преобразование — это взаимно однозначное отображение, то для каждого преобразования g существует обратное преобразование g^{-1}, которое определяется следующим образом: если $g(A) = B$, то $g^{-1}(B) = A$.

Пример 5. Выписать обратное преобразование для какой-нибудь композиции поворота и симметрии.

Если у нас есть некоторое фиксированное множество M и все его преобразования, то мы можем определить их произведение (композицию):

$$(g_1 g_2)(A) = g_1(g_2(A)),$$

то есть сначала делаем g_2, а потом g_1.

Определение 5. Пусть некоторое множество преобразований G таково, что

1. если преобразования g_1 и g_2 содержатся в G, то и их произведение $g_3 = g_1 g_2$ содержится в G;
2. если преобразование g содержится в G, то и обратное ему преобразование g^{-1} содержится в G.

Тогда такое множество преобразований G мы будем называть *группой преобразований.*

1.2 Группы. Определение, примеры, базовые конструкции.

И вот мы наконец плавно подошли к одному из главных определений в нашем курсе.

Определение 6. Множество G с заданной на нём бинарной операцией $\circ$ (мы часто будем называть её умножением) называется *группой*, если

1. $(a \circ b) \circ c = a \circ (b \circ c) = a \circ b \circ c$.
2. Существует *нейтральный* элемент $e \in G$, то есть такой элемент, что $e \circ g = g \circ e = g$ для всех элементов $g \in G$.
3. У всех элементов $g \in G$ есть обратный элемент g^{-1}, то есть такой, что $g \circ g^{-1} = g^{-1} \circ g = e$.

Замечание. Заметим, что любая группа преобразований является группой. Группы бывают разные, но в дальнейшем, группы преобразований будут основным примером групп для нас.

Пример 6. Вновь глупые числовые примеры ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}$). Пояснение примеров из прошлого параграфа.

Замечание. Вот в этом месте я бы хотел сделать такой **разгон** про то, зачем это всё на самом деле (зачем переходить от изучения *конкретных преобразований* к изучению *групп, как обще алгебраических структур.* Хороший пример такого разгона в первых пяти минутах этой лекции, гляньте пж. Мне кажется, что это **очень важно** при изложении групп детям.

После того, как мы вдоволь насладились примерами, можно начать изучать наши объекты с общей точки зрения.

Наблюдение 1. Нейтральный элемент группы единственен. Обратный элемент к элементу группы $g \in G$ единственен.

Замечание. Какими аксиомами группы мы пользовались для доказательства?

Определение 7. Два элемента группы $a, b \in G$ называются *коммутирующими* (или, перестановочными), если $ab = ba$. Если все элементы группы G коммутируют между собой, G называется *Абелевой* или *коммутативной.*

Замечание. Заметим, что **не абелевы** группы бывают. Например, рассмотренная нами ранее группа симметрий треугольника $S_3 \cong D_3$.

Пример 7. Заметим, что $(ab)^1 = b^{-1}a^{-1}$ (*Сначала мы надеваем носок, а потом ботинок. С другой стороны, сначала мы снимаем ботинок, а потом носок*).

В качестве проверки понимания можно задать слушателям такой вопрос: (*очень уж много носков*) Пусть $a_1, a_2, \ldots, a_n$ — элементы некоторой группы A. Какой элемент будет обратным к $a_1a_2\ldots a_n$?

Наблюдение 2. В группе можно сокращать равенство справа и слева.

Пример 8.

Определение 8. Пусть X — множество. Множество взаимно однозначных отображений $X \to X$ образует группу (отностельно композиции), её мы будем называть *симметрической группой* на множестве X и обозначать S_X.

Замечание. Если множество X конечно и в нём n элементов, то мы можем думать про него, как про множество $\{1, 2, \ldots, n\}$. Тогда перестановки можно записывать в виде табличек вида

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Симметрическу группу множества $\{1, 2, \ldots, n\}$ мы будем обозначать, как S_n.

Теперь рассмотрим еще одну важную конструкцию.

Определение 9. Пусть $(G_1, \circ), (G_2, *)$ — группы. Тогда их *прямое произведение* — это группа, как множество совпадающая с $G_1 \times G_2$, опреации на котором вводятся покомпонентно.

Пример 9. $\mathbb{Z} \times \mathbb{Z}$, например.

1.3 Порождение, циклические группы, порядок элемента

Определение 10. Пусть S — подмножество группы G. Подгруппой, порожденной множеством S, называется наименьшая подгруппа в G, содержащая S. Её мы будем обозначать, как $\langle S \rangle$.

Определение 11. Пусть G — группа, S — подмножество. Подгруппа, порожденная S — это наименьшая подгруппа в G. Мы будем обозначать её, как $\langle S \rangle$.

Предложение 1. *$\langle S \rangle$ состоит из всех элементов $s_1s_2\ldots s_k$, где $k \in \mathbb{N}$, а $s_i \in S \cup S^{-1}$.*

Замечание. Переписать это в абелеву нотацию.

Определение 12. Порядком элемента g группы G называют наименьшее натуральное n, для которого $g^n = e$. Если такого n не существует, то говорят, что g имеет бесконечный порядок.

Порядок элемента g мы будем обозначать, как $\operatorname{ord} g$.

Пример 10. Например, порядок элемнта 2 в группе $\mathbb{Z}/10$ равен 5. А вот в группе $\mathbb{Z}$ любой ненулевой элемент имеет бесконечный порядок.

Пример 11. Рассмотрим правильный n-угольник и все повороты плоскости, переводящие его в себя. Заметим, что если мы возьмём поворот $R = R_{\frac{2\pi}{n}}$, то

$$R^n = R_{2\pi} = e, R^{n+1} = R, \; R^{n+2} = R^2$$

и так мы получим в точности все повороты, оставляющие n-угольник на месте.

Определение 13. Группу G, состоящую из элементов $e, a^1, \ldots, a^{n-1}$ (где элемент a имеет порядок n) называют *циклической группой порядка n, порожденной элементом a* (а обозначать её мы будем, как C_n). Элемент a называется *образующей* этой группы.

Как видно из примера выше, повороты правильного n-угольника образуют циклическую группу порядка n.

Замечание. А еще бывает *бесконечная циклическая группа*, это $\mathbb{Z}$ (а образующая у неё 1). Про неё логично думать именно так, так как любой её элемент можно представить в виде $n \cdot 1$, где n — целое число.

Чуть позже иы увидим, что подгруппа порожденная одним элементом g — это в точности циклическая группа порядка $\operatorname{ord} g$.

1.4 Гомоморфизм, изоморфизм

Мы уже видели, что между многими группами можно построить теоретико-множественную биекцию, но ведь это не говорит нам, что эти группы одинаковые.

Пример 12. Ну, например есть группа $\mathbb{Z}/6$ и группа S_3. Так как обе группы имеют порядок 6, между ними легко построить теоретико-множественную биекцию, но видно, что группы на самом деле существенно разные (можно привести какой-то пример, где элементы разного порядка, или что-то в таком духе).

Определение 14. Отображение f между группами $(G, \circ)$ и $(H, *)$ называется *гомоморфизмом*, если

$$\forall a, b \in G \quad f(a \circ b) = f(a) * f(b).$$

Условие в определении гомоморфизм говорит о *сохранении стркутуры.*

Определение 15. Пусть $\varphi \colon G \to H$ — гомоморфизм групп. Его *ядром* называют $\varphi^{-1}(e_H) \subset G$. Иными словами,

$$\operatorname{Ker} \varphi \overset{\text{def}}{=} \{g \in G \mid \varphi(g) = e_H\} = \varphi^{-1}(e_H).$$

Образом φ называют его образ, как функции, то есть

$$\mathrm{Im}\varphi = \{\varphi(g) \mid g \in G\} \subset G$$

1.5 Действие группы на множестве

Определение 16. Пусть G — группа, а X — множество. Будем говорить, что G действует на X и писать $G \curvearrowright X$, если задана операция $G \times X \to X$ (образ пары (g, x)обозначается обычно просто gx), обладающая для любого $x \in X$ и $g, h \in G$ следующими свойствами:

1. $g(hx) = (gh)x$ (внешняя ассоциативность);

2. $1 \cdot x = x$ (унитальность).

Пример 13. Рассмотрим много примеров действий, чтобы понять, что же всё-таки происходит.

1. Группа S_n естественно действует на $\{1, \ldots, n\}$.
2. Гомоморфизм $\theta\colon G \to S_X$ задаёт действие по правилу

$$gx = \theta(g)(x).$$

3. $\mathrm{GL}_n(V) \curvearrowright V$.
4. Пусть $G = (\mathbb{R}^2, +)$. Зафиксируем векотр v и рассмотрим действие $G \curvearrowright \mathbb{R}^2$, заданное по правилу $x \mapsto x + v$.

Теперь заметим, что действие само по себе естественным образом задаёт гомоморфизм $G \to S_X$, как $\theta(g)(x) = gx$ (тут нужны формальные проверки). Так мы получаем равносильное определение действия группы на множестве.

Определение 17. Орбитой элемента $x \in X$ под действием G называется множество $\mathrm{Orb}(x) = \{gx \mid g \in G\}$. Количество элементов в данной орбите называется *длиной орбиты* (в разных орбитах может быть разное количество элементов).

Лемма 1. Любые две орбиты либо не пересекаются, либо совпадают. Таким образом, множество Xразбивается в дизъюнктное объединение орбит.

Определение 18. Неподвижными точками элемента $g \in G$ называются те $x \in X$, для которых $gx = x$. Множество неподвижных точек элемента g мы будем обозначать через $\mathrm{Fix}(g)$.

Определение 19. Множество элементов группы G, оставляющих на месте данный элемент $x \in X$ называется стабилизатором элемента x и обозначается через $\mathrm{Stab}(x)$. Другими словами, $\mathrm{Stab}(x) = \{g \in G \mid gx = x\}$. Очевидно, что стабилизатор является подгруппой в G.

1.6 Дальнейший план того, что я не написал еще

1. Группы перестановок, группы движений, аффинные преобразования, строковые примеры.
2. Циклические группы, остатки, порядок группы.
3. Гомоморфизмы и изоморфизмы, как сохранение структуры (и как разный способ записывать одни и те же преобразования) .
4. Подгруппы.
5. Действие группы на множестве, сопряжения, нормальные подгруппы.
6. (?) классы смежности, индекс, теорема Лагранжа.
7. (?) нормальные подгруппы и фактор.
8. (?) Теорема о гомоморфизме.
9. (?) Образующие и соотношения.

Лекции:

1. Введение самая база преобразования $\Rightarrow$ группы моноиды
2. Примеры 1
3. Примеры 2 (где-то среди них разговор как задать группу и разговор про циклические группы)
4. Примеры 3 + симметрические группы
5. Гомоморфизмы + подгруппы

6. Действие группы на множестве. Примеры. Орбиты, стабилизаторы, фиксаторы. Действие, как гомоморфизм в группу перестановок.
7. Всё еще действия. Больше примеров и какие-то содержательные факты про орбиты/стабилизаторы.
8. Свободная группа $\leftrightarrow$ языки, регулярные корневые деревья, самоподобие.
9. Автоматы (как преобразование языка или как модель машины с кончной памятью). Побольше примеров.
10. Рост,

Листики:

1. Банальщина про биекции и группы и моноиды (такая-то операция дает что).
2. Задачки про группы и перестановки.
3. Пропаганда гомоморфизмов (всякие свойства и какие-то примеры).
4.

Идеи для листочков (это артему добавить) действие группы на автомате дает симметрии языка + язык григорчука

Список литературы

[Б01] Алексеев В. Б. *Теорема Абеля в задачах и решениях.* 1-е изд. М.: МЦНМО, 2001. URL: https://old.mccme.ru/free-books/pdf/alekseev.pdf.