Теория групп

Антон Айзенберг

Введение в теорию групп.

В математике есть такие понятия, без знания которых трудно описывать те или иные явления. Рассмотрим такой пример: числа, или, скажем, множества. Сами по себе эти понятия чересчур общие и трудно сформулировать их конкретные приложения (сам вопрос "зачем нужны числа?" кажется довольно идиотским), однако без них математики не могли бы между собой общаться и передавать друг другу те или иные мысли. Таким образом, числа и множества являются скорее важным словом в словаре математика, нежели самостоятельным объектом для изучения.

В школе изучение таких основополагающих понятий ограничивается числами, функциями и (изредка) множествами. Приходя в университет, специализирующийся на математике, бывший школьник понимает, что математика чрезвычайно богата структурами, без знания которых невозможно математическое общение. Одной из таких структур как раз и посвящен этот курс.

Группа. В самом примитивном понимании, группа — это термин для описания множества симметрий некоторого объекта. В таком виде группы возникают в химии и лежат в основе многих фундаментальных физических теорий. Кроме того, абстрактное определение группы приводит к множеству приложений как в теоретической, так и в прикладной математике. Цель курса — показать, как принципиально новое для школьников абстрактное понятие может применяться к задачам из на первый взгляд разных областей.

Ввиду своей абстрактности курс не рекомендуется никому, кроме особо заинтересованных и имеющих некоторый математический background. Для записи на курс требуется знать в минимальном объеме теорию множеств, теорию чисел, комбинаторику и комплексные числа и сдать экзамен Множества. Отношения. Знание простейших геометрических преобразований приветствуется. Полезно знать, что такое граф.

Реквизит: правильные многогранники, призмы. FIT (пять тетраэдров в додекаэдре)

1 день

Первый день посвящен преимущественно разбору примеров.

Движение пространства = преобразование, сохраняющее расстояния.

Задача 1.1. Какими бывают движения плоскости?

Понятие ориентации. Преобразования, сохраняющие и меняющие ориентацию.(?продумать)

Задача 1.2.* Движения пространства, сохраняющие ориентацию и имеющие неподвижную точку, = повороты вокруг оси.

Симметрия фигуры = преобразование пространства, переводящее фигуру в себя.

Задача 1.3. Найти количество симметрий правильного n-угольника.

Задача 1.4. Найти количество симметрий тетраэдра. Куба. Октаэдра. *Додекаэдра. Окружности. Призмы. Антипризмы. Цилиндра. Еще примеры (из химии?, буквы).

Задача 1.5. Найти композицию двух заданных движений куба a и b. Описать $a \circ b$ и $b \circ a$.

Задача 1.6. Найти количество "симметрий" n-элементного множества. Тут нужно понять, что симметрией логично назвать любую перестановку элементов множества.

Группа — это множество G, на котором задана операция умножения (или композиции) $G \times G \to G$, $(g, h) \mapsto g \cdot h$, удовлетворяющая свойствам:

(1) Ассоциативность $\forall g, h, k \in G$: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$;

(2) Существование единицы $\exists e \in G \forall g \in G : e \cdot g = g \cdot e = g$;

(3) Существование обратного элемента $\forall g \in G \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$.

Тут нужно надолго остановиться и пояснить каждое слово в абстрактном определении, чтобы в дальнейшем не осталось непонятных мест.

Порядок группы = ее мощность.

Задача 1.7. Доказать, что множество движений пространства, сохраняющих заданную фигуру, с операцией композиции движений является группой. Каков смысл единицы и обратного элемента?

Замечание: в группе не обязана выполняться коммутативность: $a \cdot b$ может не совпадать с $b \cdot a$, как показывает пример с движениями.

Задача 1.8. Еще примеры. Являются ли группами следующие множества с операциями: $(\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{R}[x], +), (\mathbb{R}[x], \cdot)$, $(C(x), \cdot)$, $(C(x) \setminus 0, \cdot)$, $(2^M, \cap)$, $(2^M, \cup)$, $(2^M, \Delta)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(S^1, \cdot)$, еще MORE! (здесь 2^M — множество всех подмножеств множества M, Δ — операция симметрической разности, S^1 — комплексные числа с длиной 1).

2 день

Этот день посвящен перестановкам.

Перестановка на множестве M — это биекция M в себя. Запись перестановки в виде $\left(\begin{smallmatrix} 1 & 2 & \dots & m \\ i_1 & i_2 & \cdots & i_m \end{smallmatrix}\right)$

Группа перестановок S_n. Перемножение перестановок справа налево — таково будет соглашение. Пояснение: перестановки — это частный случай отображения. Заметим, что композиция отображений (или композиция функций) читается справа налево. Запись $\cos x^2$ означает, что мы вначале возводим x в квадрат, а затем берем косинус, то есть читаем справа налево. Применение перестановки к элементу множества.

Задача 2.1. Перемножить $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right)$.

Задача 2.2. Обратить $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{smallmatrix}\right)$.

Другие похожие примеры.

Граф перестановки σ. Вершины — элементы множества $[n]$, от вершины i ведем стрелку (ор. ребро) к вершине $\sigma(i)$.

Задача 2.3. В полученном орграфе в каждую вершину входит и выходит ровно одно ребро. Следствие: граф представляет из себя набор несвязных ориентированных циклов.

Цикл в перестановке. Запись перестановки в виде произведения независимых циклов.

Задача 2.4. Записать в виде произведения независимых циклов перестановку $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{smallmatrix}\right)$. Другие примеры.

Задача 2.5. Сколько бывает циклов длины n в S_n?

Транспозиция — цикл длины 2. Наглядный смысл.

Задача 2.6. Доказать, что цикл можно представить в виде произведения транспозиций (с указанием).

Задача 2.7. Доказать, что любую перестановку можно записать в виде произведения транспозиций.

Задача 2.8. Представить в виде произведения транспозиций перестановку $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 1 & 3 \end{smallmatrix}\right)$.

Задача 2.9. Верно ли что представление в виде произведения транспозиций единственно? !Придумать нетривиальный пример

Замечание. Оказывается, что четность числа транспозиций в произвольном таком представлении является инвариантом. Доказательство этого факта — цель нашей последующей деятельности.

Числом беспорядков для перестановки $\sigma \in S_n$ называется количество таких пар $i < j$, $i, j \in [n]$, для которых $\sigma(i) > \sigma(j)$. *Замечание: не зависит от порядка на множестве $[n]$.

Четностью перестановки σ называется четность числа беспорядков σ.

Задача 2.10. Доказать, что транспозиция — нечетна.

Задача 2.11.* Доказать, что домножение перестановки слева (или справа) на транспозицию меняет четность. !Продумать оптимальное доказательство. Видимо, самое простое — через обобщенную запись перестановки. !Подумать над альтернативными и более понятными определениями четности.

Таким образом, четность перестановки совпадает с четностью числа транспозиций в любом разложении перестановки в произведение транспозиций.

Задача 2.12. Четная перестановка $\times$ четная $=$ четная, четная $\times$ нечетная $=$ нечетная, нечетная $\times$ нечетная $=$ четная.

Четные перестановки сами по себе образуют группу, лежащую внутри другой группы.

Определение. Подгруппа $H \subseteq G$.

Четные перестановки образуют подгруппу $A_n \subset S_n$.

Задача 2.13. Найти порядок группы A_n. Указание: при $n > 1$ построить биекцию между четными и нечетными перестановками с помощью домножения на транспозицию $(1, 2)$. Т.о. ответ $\frac{n!}{2}$.

Замечание: идею этого доказательства надо запомнить. Она еще пригодится.

Задача 2.14. Игра “в пятнадцать”. В собранном состоянии пятнашек поменяли местами фишки с номерами 14 и 15. Доказать, что переставляя фишки по правилам игры нельзя получить требуемую в игре комбинацию.

Задача 2.15.* (Доп.) Доказать, что любая четная перестановка представляется в виде произведения циклов длины 3.

Задача 2.16.* (Доп.) Доказать, что любая перестановка представляется в виде произведения транспозиций, переставляющих соседние элементы.

3 день

Этот день посвящен геометрии и гомоморфизмам.

Группа $\mathbb{Z}_n$ остатков mod n по сложению. Группа X_n комплексных корней степени n из 1 с операцией комплексного умножения.

Задача 3.1. Осознать, что X_n “это то же самое”, что и $\mathbb{Z}_n$.

Определение. Гомоморфизм групп. Гомоморфизмом из группы $(G, \times)$ в группу $(H, \cdot)$ называется такое отображение множеств $f\colon G \to H$, что

(1) $\forall g_1, g_2 \in G : f(g_1 \times g_2) = f(g_1) \cdot f(g_2)$;

(2) $f(e_G) = e_H$;

(3) $\forall g \in G : f(g^{-1}) = f(g)^{-1}$.

Пояснение. Изоморфизмом называется гомоморфизм, являющийся биекцией. Пояснение: изоморфные группы, значит одинаковые. Далее будет много примеров.

Задача 3.2. Доказать, что группы $(\mathbb{Z}_2, +), S_2, (\{\text{чет}, \text{нечет}\}, +), (\pm 1, \times)$ изоморфны.

Таблица умножения в группе.

Задача 3.3. Доказать, что все группы порядка 2 изоморфны $\mathbb{Z}_2$.

Задача 3.4. Рассмотрим отображение из S_n в $(\{\text{чет}, \text{нечет}\}, +)$, которое четной перестановке ставит в соответствие элемент “чет”, а нечетной — элемент “нечет”. Доказать, что такое отображение является гомоморфизмом из группы S_n в группу $\mathbb{Z}_2$.

Задача 3.5. (Доп.) Пусть задана некоторая фигура Φ в пространстве (на плоскости) и G_Φ — группа всех ее симметрий. Доказать, что отображение, сопоставляющее 0 движениям, сохраняющим ориентацию и 1 движениям, меняющим ориентацию, является гомоморфизмом из группы G_Φ в группу $\mathbb{Z}_2$.

Задача 3.6. Отображение, сопоставляющее “чет” четным числам и “нечет” нечетным числам является гомоморфизмом $(\mathbb{Z}, +) \to \mathbb{Z}_2$.

Задача 3.7. (Доп.) Гомоморфизм $\mathbb{Z} \to \mathbb{Z}_n$, сопоставляющий числу его остаток.

В последующих задачах надо предъявить явный гомоморфизм, являющийся биекцией. Потребуется лемма-задача.

Задача 3.8. Отображение двух равномощных конечных множеств является сюръекцией в том и только том случае когда это инъекция (и наоборот). Поэтому для биективности достаточно равенства мощностей и только инъективности (либо только сюръективности).

Задача 3.9. Доказать, что группа всех движений тетраэдра изоморфна группе перестановок четырех элементов. Подгруппа движений тетраэдра, сохраняющих ориентацию изоморфна подгруппе четных перестановок. Указание: каждое движение тетраэдра задает перестановку вершин. Это и есть требуемый гомоморфизм.

Задача 3.10. Группа движений куба, сохраняющих ориентацию, изоморфна группе S_4. Указание: перестановки главных диагоналей и совпадение порядков рассматриваемых групп. Любая транспозиция диагоналей реализуема поворотом.

Задача 3.11. Группа движений додекаэдра, сохраняющих ориентацию, изоморфна группе A_5. Указание: FIT (пять пересекающихся тетраэдров в додекаэдре). Проверяем, что любой поворот задает четную перестановку на множестве тетраэдров. Проверяем, что любой 3-цикл тетраэдров задается некоторым поворотом. Пользуемся задачей 2.15.

Задача 3.12. Задача, от которой всех дико прет. Доказать, что группы $(\mathbb{R}_{>0}, \cdot)$ и $(\mathbb{R}, +)$ изоморфны.

Задача 3.13. (Доп.) Доказать, что отображение $x \mapsto e^{2\pi i x}$ задает гомоморфизм $\mathbb{R} \to S^1$

4 день

Этот день посвящен немного теории чисел и крайне важной теореме Лагранжа.

Теорема Лагранжа. Если $H \subseteq G$ — подгруппа, и $|G| < \infty$, то $|G|$ делится на $|H|$ (порядок подгруппы делит порядок группы).

Мы будем плавно эту теорему доказывать.

Отношения. Отношения эквивалентности. Предполагается, что к этому моменту все сдали соответствующий экзамен. Если нет, то проводится краткий ликбез, после которого экзамен сдается без проблем.

Отношение на множестве X — произвольное подмножество $O \subseteq X \times X$. Если $(a, b) \in O$, то пишут $a|b$.

Отношение называется отношением эквивалентности, если выполнены следующие свойства:

1) $\forall a \in X : a|a$ (рефлексивность).

2) Если $a|b$, то $b|a$ (симметричность).

3) Если $a|b$ и $b|c$, то $a|c$ (транзитивность).

Отношение эквивалентности задает разбиение множества X на подмножества, т.н. классы эквивалентности. Все элементы одного класса эквивалентности эквивалентны друг другу. Элементы из разных классов не эквивалентны. Задать разбиение множества X на подмножества — это то же самое, что задать отношение эквивалентности. Для отношения эквивалентности вместо значка $|$ используется $\sim$.

Пусть G — группа, а $H \subseteq G$ подгруппа. Зададим на множестве G отношение: $g_1|g_2$, если $g_1 \cdot g_2^{-1} \in H$.

Задача 4.1. Доказать, что это отношение является отношением эквивалентности. Будем обозначать его $\sim_H$.

!Четче продумать структуру доказательства.

Задача 4.2. Доказать, что одним из классов эквивалентности построенного отношения эквивалентности является сама подгруппа H.

Задача 4.3.* Доказать, что между классом эквивалентности H и любым другим классом эквивалентности можно установить биекцию. Указание: вспомнить доказательство задачи 2.13 и понять как эти задачи связаны между собой.

Таким образом вся группа G распадается на классы эквивалентности, каждый из которых содержит $|H|$ элементов. Отсюда следует теорема Лагранжа.

Задача 4.4. Рассмотрим элемент $a \in G$, $a \neq e$ и образуем последовательность $e, a, a^2, a^3, \ldots$. Возможны две альтернативы: 1) в последовательности нет повторений 2) есть повторения. Доказать, что: 1) В первом случае множество $\{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$

является подгруппой, изоморфной $\mathbb{Z}$. 2) Во втором случае: существует такое наименьшее $n > 1$, что $a^n = e$. Множество $\{e, a, a^2, \ldots, a^{n-1}\}$ является подгруппой, изоморфной $\mathbb{Z}_n$.

Вывод. Все возможные степени элемента $a \in G$ образуют подгруппу, изоморфную либо $\mathbb{Z}$, либо $\mathbb{Z}_n$. Говорят, что элемент a порождает подгруппу. В первом случае говорят, что a имеет бесконечный порядок. Во втором случае говорят, что a имеет порядок n. Порядок — это наименьшее натуральное число n, такое что $a^n = e$. Примеры элементов конечного порядка — вращения в кубе, тетраэдре, октаэдре, порядки элементов в группе S_n. Разбор всех этих примеров.

Задача 4.5. Если группа G конечная, то порядок любого элемента делит порядок группы. Это прямое следствие теоремы Лагранжа (любой элемент конечной группы порождает подгруппу, порядок которой равен по определению порядку элемента).

Задача 4.6. Пример. Порядок группы додекаэдра 60. Поэтому там не может быть элементов порядка 7, скажем. И действительно, среди вращений додекаэдра есть вращения на $\frac{2\pi}{2}, \frac{2\pi}{3}, \frac{2\pi}{5}$, то есть элементы порядков $2, 3, 5$ соответственно. Числа $2, 3, 5$ — делители числа 60.

?Упоминание о теореме Силова?

Задача 4.7. Еще одно простое следствие. Если a — элемент конечной группы G, то $a^{|G|} = e$.

Теперь один чрезвычайно важный пример из теории чисел.

Задача 4.8. Являются ли остатки $\mod n$ группой относительно умножения?

Нет. Умножение задано, единица имеется, но нет обратных элементов.

Задача 4.9. Рассмотрим остатки $\mod 6$. Заведомо нет обратных элементов у остатков $0, 2, 3, 4$, то есть у всех тех остатков, которые имеют общий делитель с 6. Осознать общую ситуацию.

Задача 4.10.* Пусть n — число и $0 < k < n$ причем $(k, n) = 1$. Доказать, что существует такое число $0 < l < n$, что $kl = 1 \mod n$. Тут надо вспомнить теорию чисел, а именно следующий факт: если $d = (k, n)$, то существуют такие $x, y \in \mathbb{Z}$, что $kx + ny = d$ (это следствие из алгоритма Евклида).

Задача 4.11. Множество всех остатков $\mod n$, взаимно простых с n, обозначим $\mathbb{Z}_n^*$. Таким образом, $\mathbb{Z}_6^* = \{1, 5\}$. Доказать, что $\mathbb{Z}_n^*$ является группой относительно умножения $\mod n$.

Задача 4.12.* Чему равен порядок группы $\mathbb{Z}_n^*$?

Эта задача сложна для тех, кто с этим раньше не сталкивался, поэтому далее приводится краткое содержание соответствующей теории. Эти задачи можно давать в качестве ДЗ.

Пусть $n \in \mathbb{N}$. Количество натуральных чисел меньших n и взаимно простых с n обозначается символом $\phi(n)$ и называется функцией Эйлера числа n.

Задача 4.13. Это даже не задача, а замечание. Порядок группы $\mathbb{Z}_n^*$ это и есть число $\phi(n)$.

Задача 4.14. Пусть p — простое число. Доказать, что $\phi(p) = p - 1$.

Задача 4.15. Пусть p — простое число. Доказать, что $\phi(p^k) = p^{k-1}(p - 1)$.

Задача 4.16. Пусть $(l, m) = 1$. Тогда $\phi(lm) = \phi(l)\phi(m)$ (так называемое мультипликативное свойство функции Эйлера).

Задача 4.17. Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ — представление числа в виде произведения простых множителей. Тогда

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_s - 1).$$

Таким образом, функция Эйлера вычисляется по явной формуле, если знать разложение числа на простые множители. Впрочем, явный вид этой формулы будет нам не очень важен.

Задача 4.18. Теорема Эйлера. Пусть $n \in \mathbb{N}$ и $a \in \mathbb{N}$ и $(a, n) = 1$. Тогда $a^{\phi(n)} = 1 \mod n$.

Эта задача следует напрямую из задач 4.7, 4.11, 4.13.

Задача 4.19. Малая теорема Ферма. Если p — простое число и a не делится на p, то $a^{p-1} = 1 \mod p$.

Эта теорема — частный случай теоремы Эйлера, поскольку $\phi(p) = p-1$ для простого числа p.

Замечание. Стоит сказать, что эти теоремы не обязательно доказывать с помощью групп. Имеются и теоретико-числовые доказательства.

5 день

Посвящен действию группы на множестве и лемме Бернсайда.

Задача 5.1. На краю тарелочки нарисованы 5 кружков. Каждый кружок может быть одного из трех цветов. Сколько существует различных тарелочек?

Замечание: если тарелочку повернуть на $\frac{2\pi}{5}$, то это будет та же тарелочка, поэтому ответ 3^5 — неверный. Мы не различаем тарелочки отличающиеся друг от друга поворотом.

Конкретно эта задача решается нехитрым, но аккуратным перебором. Ответ: 51.

Общие слова. Лемма Бернсайда позволяет решать эту и подобные задачи бездумным ремесленным способом. Вначале мы изучим способ и научимся его применять, а затем, если останется время, сформулируем, а то и докажем лемму Бернсайда, лежащую в основе этого способа.

Итак, тарелка. Казалось бы, раз мы не различаем тарелку и повернутую тарелку, то можно было бы посчитать количество “жестких” тарелок (т.е. тех, которые нельзя вращать, их 3^5), а затем поделить на число возможных поворотов, т.е. на 5. Но вот незадача: 3^5 нацело на 5 не делится, значит где-то в рассуждении ошибка. Ошибка в том, что некоторые раскраски жестких тарелок при повороте переходят сами в себя, поэтому их при делении на 5 не надо учитывать. Переходят в себя только одноцветные раскраски, которых всего 3. Поэтому итоговый ответ в этой задаче можно получить таким образом $(3^5 - 3)/5 + 3 = 51$.

Кстати, внимательный слушатель может в этом рассуждении усмотреть скрытое (комбинаторное) доказательство малой теоремы Ферма ($3^5 - 3$ делится на 5 нацело).

В некотором смысле алгоритм Бернсайда нужен, чтобы решать более сложные задачи тем же методом.

Выпишем все возможные повороты, то есть углы $0, \frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}$. Для каждого поворота выпишем все возможные жесткие раскраски, которые при данном повороте переходят в себя. При повороте на 0 — все раскраски инвариантны, их 3^5. Для остальных поворотов инвариантных раскрасок будет всего 3 (это только одноцветные раскраски). Складываем все полученные числа и делим на число поворотов — это и будет ответ. В нашем случае получаем $\dfrac{3^5 + 3 + 3 + 3 + 3}{5} = 51$.

Остальные задачи решаются по тому же алгоритму.

Задача 5.2. Найти число тарелочек с 6 кружками, каждый из которых раскрашен в один из трех цветов.

Задача 5.3. Вершины тетраэдра покрашены в 4 цвета. Сколько таких тетраэдров существует с точностью до вращений?

Задача 5.4. Вершины (грани) куба покрашены в 3 цвета. Сколько способов это сделать (куб можно вращать, но не отражать).

Еще задачи MORE!!!

Теперь теория в кратком изложении. Действие группы G на множестве X. Пример: множество жестких раскрасок объекта и действие группы симметрий объекта. Отношение эквивалентности на X, порожденное действием. Классы эквивалентности — орбиты действия. Пример: действие S^1 на $\mathbb{C}$. Орбиты — окружности и ноль. Множество орбит обозначается X/G. Для каждого $g \in G$ определим подмножество неподвижных элементов $X_g \subseteq X$. Примеры: как все это соотносится с раскрасками.

Задача 5.5.** Лемма Бернсайда.

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X_g|.$$

Для доказательства потребуется определение стабилизатора $G_x \subseteq G$ точки $x \in X$.

Задача 5.6.* Пусть $O_x \subseteq X$ — орбита точки x, а $G_x \subseteq G$ — ее стабилизатор. Тогда $|O_x| \cdot |G_x| = |G|$.

Идея доказательства леммы Бернсайда: рассматриваем множество $\{(g, x) \in G \times X \mid g \cdot x = x\}$ и по разному считаем его мощность — послойно вдоль X или послойно вдоль G. Применяем предыдущую задачу.

Замечание. Доказательство леммы Бернсайда я так и не успел рассказать. Слушатели грозились вытащить из меня это доказательство ночью на последнем костре, но, похоже, им было не до того.

6 День

Этот день зачетный, поэтому особо желающие могли повышать свои балы дорешивая задачи из прошлых дней и досдавая экзамены. А нежелающие могли слушать дальше. Программа последнего дня была вольной. Возможные темы для лекции.

Прямое произведение групп. Пример: $\mathbb{Z}_2 \times \mathbb{Z}_3$ изоморфна $\mathbb{Z}_6$. Китайская теорема об остатках и ее формулировка на групповом языке. Геометрический смысл $\mathbb{Z} \times \mathbb{Z}$.

Задача 6.1. Группа $(2^{[m]}, \Delta)$ (см. первый день) изоморфна группе $\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$.

Образующие группы. Примеры: транспозиции для группы S_n, циклы длины 3 для A_n.

Задача 6.2.* Доказать, что группу S_n можно породить всего двумя образующими.

Задача 6.3. Доказать, что у группы $(\mathbb{Q}, +)$ не существует конечной системы образующих (чистая т.ч.).

Задача 6.4. Доказать, что у группы $(\mathbb{R}, +)$ не существует конечной системы образующих (соображения мощности).

Коммутативная группа, примеры.

Теорема (б.д.): Любая конечнопорожденная коммутативная группа изоморфна $\mathbb{Z}^k \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$.

Задача 6.5.* На этот раз теорема с доказательством. Теорема Кэли. Любая конечная подгруппа изоморфна некоторой подгруппе группы S_n. С указанием.

Еще дополнительные топики:

1) Группы Ли. Группы геометрических преобразований, набор модулей или сколько параметров, группа Клейна, окружность, группа $SO(3, \mathbb{R})$, группа единичных кватернионов $S^3 \cong SU(2)$. Физические теории и симметрии. Тор как группа. Эллиптическая кривая.

2) Разбор других примеров конечнопорожденных групп. Группа диэдра. Группа кос. Свободная группа. Задание группы при помощи образующих и соотношений (копредставление). Граф Кэли копредставления. Соотношения в известных группах.

3) Нормальные подгруппы. Фактор-группы. Примеры. Индекс подгруппы. Подгруппа индекса 2 является нормальной. Ядро гомоморфизма — нормальная подгруппа.