МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА. СЕМИНАРЫ. ЧАСТЬ 2

ТИМАШЕВ
ДМИТРИЙ АНДРЕЕВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТКУ МЕХАНИКО-МАТЕМАТИЧЕСКОГО ФАКУЛЬТЕТА МГУ
КОЩЕЕВУ АННУ ВИТАЛЬЕВНУ

Содержание

Лекция 1

Понятие группы

Определение 1.1. *Группа - это множество G с бинарной операцией $G \times G \to G$, $(x, y) \mapsto x \cdot y$, обычно называемой умножением, удовлетворяющей аксиомам:*
1. Ассоциативность:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in G$$

2. Нейтральный элемент:

$$\exists\, e \in G\, \forall x \in G: \quad e \cdot x = x \cdot e = x$$

3. Обратный элемент:

$$\forall\, x \in G \;\; \exists\, y \in G: \; x \cdot y = y \cdot x = e$$

Простейшие свойства.

1) Единственность нейтрального элемента.

   Пусть e, e' - оба нейтральны. Тогда с одной стороны $e \cdot e' = e$ по нейтральности e', а с другой стороны, $e \cdot e' = e'$ по нейтральности e. Получили, что $e = e'$.

2) Единственность обратного элемента.

   Пусть y, y' - оба обратные к x. Рассмотрим $y \cdot x \cdot y'$. С одной стороны, $(y \cdot x) \cdot y' = e \cdot y' = y'$, а с другой $y \cdot (x \cdot y') = y$. Получили, что $y = y'$.
   Поскольку обратный элемент единственный, можно ввести обозначение $y = x^{-1}$.

Упражнение 1.1. *Из второй и третьей аксиом следует, что нейтральный (обратный) элемент нейтрален (обратен) с обеих сторон.*
Теперь ослабим наши требования: пусть операция по-прежнему ассоциативна, но нейтральный (обратный) элемент нейтрален (обратен) только с одной стороны. Скажем, только $x \cdot e = x\ \forall x \in G$ и $\forall x \in G\ \exists y \in G: \; x \cdot y = e$.
Имеем множество G с ассоциативной бинарной операцией, правой едницей и правым обратным элементом. Показать, что в таком случае G - группа.

Определение 1.2. *Если к нашим трем аксиомам добавить*
4) Коммутативность:

$$x \cdot y = y \cdot x, \quad \forall x, y \in G,$$

то в классе всех групп получим некий подкласс - класс коммутативных (или абелевых) групп.

Нередко для абелевых групп используется не мультипликативная, а аддитивная терминология (операция в группе называется сложением).

Мультипликативная терминология	Аддитивная терминология (для абелевых групп)
умножение: $x \cdot y$	сложение: $x + y$
единица: e или 1	нуль: 0
Обратный элемент: x^{-1}	Противоположный элемент: $-x$
Степень: $g^n = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, \ n \in \mathbb{N}, \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{\lvert n \rvert}, \ n \in \mathbb{Z}_{<0}, \\ e, \ n = 0 \end{cases}$	Кратное: $n \cdot g, \ n \in \mathbb{Z}$

Определение 1.3. *Напоминание: кольцо - это множество с бинарными операциями сложения и умножения, которое является абелевой группой по сложению (аддитивная группа кольца) и удовлетворяет свойству дистрибутивности.*

Примеры групп

1) Пусть $(A, +, \cdot)$ - кольцо, тогда $(A, +)$ - *аддитивная группа кольца.*
   Например, в качестве A можно взять $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
   Заметим, что $(\mathbb{N}, +)$ не образует группу, т.к. в нем нет нейтрального элемента.

2) Пусть $(A, +, \cdot)$ - ассоциативное кольцо с единицей. Тогда можно рассмотреть *мультипликативную группу кольца* $A^\times = \{x \in A \mid \ \exists y \in A : \ xy = yx = e\}$ - множетсво обратимых элементов A (это группа относительно умножения).
   Например, $\mathbb{Z}^\times = \{1, -1\}$.
   Напомним, что поле - это коммутативное ассоциативное кольцо, в котором каждый ненулевой элемент имеет обратный. Тогда мультипликативная группа поля K есть $K \backslash \{0\}$.
   В качестве K можно взять $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

3) Линейная группа (V - векторное пространство над полем K).
   Полная линейная группа $GL(V)$ - множество всех невырожденных линейных операторов на $\mathcal{A} : \ V \to V$. Они образуют группу относительно операции умножения (композиции).
   Ее можно рассматривать и как мультипликативную группу кольца всех линейных операторов $End(V)$.

   В $GL(V)$ есть разные подгруппы.

   Специальная линейная группа $GL(V) \supset SL(V)$ - линейные операторы с определителем 1 (разумеется, в предположении, что V конечномерно).

Если V - евклидово пространство (т.е. на нем введено скалярное произведение), то можно рассмотреть группу, которая это скалярное произведение сохраняет. $O(V) = \{\mathcal{A} : \ V \to V \mid (\mathcal{A}x, \mathcal{A}y) = (x, y), \ \forall x, y \in \mathcal{A}\}$ - *группа ортогональных операторов.*

Если пересечь $SL(V)$ с $O(V)$, получим *специальную ортогональную группу* $SO(V)$.

4) В некотором базисе конечномерного векторного пространства всякий линейный оператор можно записать в матричном виде (это взаимно-однозначное соответствие). Значит, все линейные группы имеют матричные аналоги.

   $GL_n(K)$ - *группа всех невырожденных матриц* размера $n \times n$ над полем K. Это то же, что и мультипликативная группа кольца квадратных матриц $Mat_n(K)^\times$.

   $GL_n(K) \supset SL_n(K)$ - матрицы $n \times n$ с определителем 1.
   $GL_n(K) \supset O_n(K) = \{A \mid A \cdot A^T = E\}$ - ортогональные матрицы $n \times n$.
   $SO_n(K) = \{A \in O_n(K) \mid \det A = 1\}$.
   $B_n(K)$ - группа невырожденных верхнетреугольных матриц.
   $U_n(K)$ - группа унитреугольных матриц (невырожденных верхнереугольных с единцами на главной диагонали).
   $T_n(K)$ - группа невырожденных диагональных матриц.

5) Группы движений.
   $\mathbb{E}^n$ - евклидово аффинное пространство. Рассмотрим в нем геометрическую фигуру $F \subset \mathbb{E}^n$ (некое подмножество). Рассмотрим *группу движений* этой фигуры (т.е. группу движений всего пространства, которые оставляют фигуру F на месте) $Isom(F) = \{\varphi : \ \mathbb{E}^n \to \mathbb{E}^n, \ \varphi(F) = F\}$.
   Как известно, движения бывают собственные и несобственные (сохраняющие ориентацию и меняющие ее). Можно в группе $Isom(F)$ рассмотреть *подгруппу собственных движений* $Isom^+(F)$.

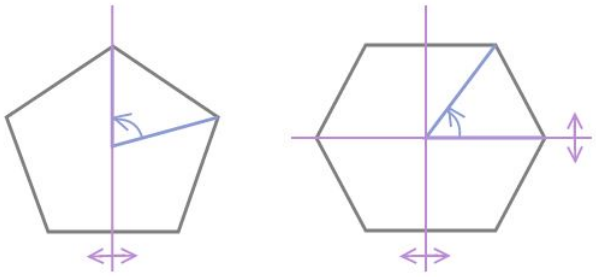
   Пример: группа Диэдра $D_n = Isom\Delta_n$ - группа движений плоскости, оставляющая на месте правильный n-угольник.
   Здесь принципиальное значение имеет четность количества вершин.

   Напоминание: какие бывают движения плоскости? Поворот, сдвиг, симметрия и скользящая симметрия.
   Какие из них могут сохранять правильный n-угольник?

   - Поворот относительно центра (на углы $\frac{2\pi}{n}$ и кратные, их n штук);
   - Симметрия относительно оси. В случае четного n ось может проходить через противоположные вершины или через середины противоположных

сторон, а в случае нечетного n - через вершину и середину противоположной стороны (в обоих случаях таких симметрий n штук).

Сдвиг и скользящая симметрия не сохраняют Δ_n, т.к. центр при таком движении должен переходить в центр. У сдвигов и скользящих симметрий нет неподвижных точек.



Итак, $D_n = \{$поворот на $\frac{2\pi k}{n},\ k = 0, \ldots, n-1, +n$ симметрий$\}$.
Замечание: $|D_n| = 2n$.

Подгруппа собственных движений состоит только из поворотов $R_n = Isom^+\Delta_n = \{$поворот на $\frac{2\pi k}{n},\ k = 0, \ldots, n-1\}$, $|Isom^+\Delta_n| = n$.

6) В предыдущих примерах были рассмотрены привычные множества с операцией умножения (= композиции). Теперь приведем пример произвольного множества с произвольным его преобразованием. Преобразование - взаимно-однозначное отображение на себя.

Группа преобразований множества X $S(X) = \{$взаимно-однозначные отображения $\varphi : X \to X\}$. Это группа относительно операции композиции.

Единица здесь - тождественное преобразование, а по взаимной однозначности у каждого преобразования есть обратное.

В частности, если X - конечное множество (а все конечные множества устроены, по существу, одинаково), можно считать $X = \{1, \ldots, n\}$. Тогда $S(X) = S_n$ - группа перестановок (симметрическая группа).
В S_n есть подгруппа A_n четных перестановок (знакопеременная группа).

Задание конечной группы таблицей умножения

Общий прием задания структуры группы на множестве.
Чтобы задать структуру группы, нужно задать операцию с некоторыми свойствами. Задать операцию - значит задать правило, по которому каждой паре элементов

группы сопоставляется результат этой операции. Правило может задаваться формулой, каким-то словесным описанием, но бывает и так, что нет ни формулы, ни описания, и нужно вручную прописать результат операции для каждой пары.

В случае конечных групп это можно сделать с помощью таблицы умножения. $G = \{g_1, \dots, g_n\}$ - конечное множество.

	g_1	$\dots$	g_i	$\dots$	g_n
g_1					
$\vdots$			$\vdots$		
g_j		$\dots$	$g_i g_j$		
$\vdots$					
g_n					

Некоторые свойства легко проверяются.

- Если g_i - нейтральный элемент, то i-тая строчка совпадает с верхней шапкой таблицы, а i-тый столбец совпадает с левой шапкой.
- Чтобы проверить, что у каждого элемента есть обратный, нужно у каждого элемента в строке найти ячейку нейтрального элемента ($g_i \cdot g_j = e$).
- В терминах таблицы коммутативность означает симметриность таблицы относительно диагонали.

Пример. Четверная группа Клейна $V_4 = \{e, a, b, c\}$.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Единица, коммутативность и существование обратного сразу видны из таблицы.

Чтобы показать ассоциативность, есть два способа:
1. перебрать все тройки руками (разумеется, все тройки перебирать не нужно, достаточно рассматривать только разные по типу, т.к. умножение устроено довольно симметричным образом);
2. найти другую группу, про которую мы точно знаем, что она является группой, в которой умножение будет устроено так же (простроить изоморфизм).

Изоморфизм

Чтобы построить некоторую общую теорию, важно понимать, какие группы устроены одинаково, а какие по-разному. Это позволяет переносить результаты, доказанные для одних групп, на другие.

Вообще говоря, это общая проблема любой математической теории - при наличии большого количества однотипных стурктур разбить эти стуктуры на классы эквивалентности в рамках данной теории. Решение всегда одно: нужно ввести понятие изоморфизма, тогда изоморфные структуры будем считать одинаковыми, а не изоморфные - разными.

Для разных типов математических структур изоморфизм определяется по-разному, но всегда довольно интуитивно. Если мы имеем дело со структурой на каком-то множестве, то изоморфизм - это взаимно-однозначное отображение одного множества на другое (аналогичное), которое уважает те структуры, которые на этих множествах заданы.

Определение 1.4. *Изомоорфизм групп - это взаимно-однозначное отображение* $\varphi:\ G \to H$, *для которого*

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y),\ \forall x, y \in G.$$

Обозначение: $\varphi:\ G \xrightarrow{\sim} H$.

Определение 1.5. *Группы изоморфны, если существует изоморфизм* $G \xrightarrow{\sim} H$ *(не обязательно единственный).*
Обозначение: $G \simeq H$.

Почему это понятие позволяет отождествлять разные группы в рамках теории групп?
Теория групп изучает групповые свойства, т.е. те свойства, которые могут быть выражены в терминах операций. Если между группами есть взаимно-однозначное соответствие, при котором операция в одной группе переходит в операцию в другой группе, то все свойства первой группы с помощью этого отображения переносятся и на вторую.

Пример 1.

Какие из следующих групп $(\mathbb{R}, +)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{R}^+, \cdot)$ изоморфны между собой?

- Чтобы показать, что две группы изоморфны, нужно предъявить какой-то изоморфизм.
- Чтобы показать, что они не изоморфны, нужно найти такое групповое свойство, которое в одной группе выполнено, а в другой нет.

1) $(\mathbb{R}, +) \simeq (\mathbb{R}^+, \cdot)$, $\varphi = \exp:\ x \mapsto e^x$.
   Взаимная однозначность есть, $\varphi^{-1}(y) = \ln y$.
   Согласованность операций: $\varphi(x_1 + x_1) = \exp(x_1 + x_2) = e^{x_1} \cdot e^{x_2} = \varphi(x_1) \cdot \varphi(x_2)$.

2) $(\mathbb{R},+),(\mathbb{R}^\times,\cdot)$ не изоморфны.
Рассмотрим уравнение
$$x+x=0 \qquad y\cdot y=1,$$
оно выражено только в терминах групповой операции.
В $(\mathbb{R},+)$ $\exists!$ решение $x=0$, а в $(\mathbb{R}^\times,\cdot)$ $\exists$ 2 решения $y=\pm 1$.
Если бы группы были изоморфны, уравнение имело бы в них одинаковое количество решений.

3) По транзитивности $(\mathbb{R}^\times,\cdot)$, $(\mathbb{R}^+,\cdot)$ не изоморфны.

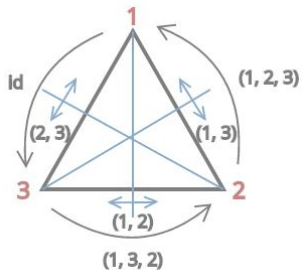
Упражнение 1.2. *Какие из следующих групп* $(\mathbb{Q},+)$, $(\mathbb{Q}^\times,\cdot),(\mathbb{Q}^+,\cdot)$ *изоморфны?*

Пример 2.

$(\mathbb{Z}_6,+)$ - группа вычетов по модулю 6, $|\mathbb{Z}_6|=6$;
S_3 - группа перестановок чисел $\{1,2,3\}$, напомним, что $|S_3|=3!=6$;
D_3 - группа движений правильного треугольника, $|D_3|=2\cdot 3=6$.
Какие из этих групп изоморфны?

Для конечных (да и вообще любых) групп необходимым условием изоморфности является совпадение мощностей (иначе не будет взаимной однозначности).

1) $S_3\simeq D_3$, т.к. всякое движение задает перестановку вершин треугольника.



Изоморфизм:
$$D_3\supset\varphi\mapsto\begin{pmatrix}1 & 2 & 3\\ \varphi(1) & \varphi(2) & \varphi(3)\end{pmatrix}\subset S_3$$
Это взаимно-однозначное отображение, потому что движение плоскости однозначно задается образами трех точек, не лежащих на одной прямой.
Кроме того, понятно, что композиции движений соответствует композиция перестановок.

2) $(\mathbb{Z}_6,+)$ - абелева (коммутативна), а S_3, D_3 - не абелевы. Например, при перемножении двух симметрий получаем поворот, направление которого зависит от порядка симметрий.
Значит, они не изоморфны.

Пример 3.

$(\mathbb{Z}_4, +)$ и V_4 - группа Клейна не изоморфны.

Определение 1.6. *Порядок элемента $g \in G$ - наименьшая натуральная степень, в которой этот элемент равен нейтральному. Если такой степени нет, то считаем порядок $o(g) = \infty$.*

В V_4 все элементы порядка 2 (кроме нейтрального). Это видно из таблицы умножения.
В $(\mathbb{Z}_4, +)$ только $\overline{2}$ имеет порядок 2 $(2 + 2 = 4 = 0)$.

Упражнение 1.3. *Изоморфны ли $GL_3(\mathbb{C})$ и $GL_2(\mathbb{C})$?*

Домашнее задание (задачник Кострикина, 3 издание): 55.25 п. а),б),г), 55.26 (без пункта про группу кватернионов), 56.9, 56.10, 56.11.

Лекция 2

Решение задачи 55.25

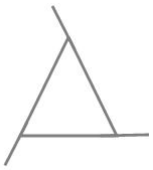
Задача. Привести примеры плоских геометрических фигур, группы движений которых изоморфны:
а) $\mathbb{Z}_2$; б) $\mathbb{Z}_3$; в) S_3; г) V_4.

Решение.

1) Пункт а). $F \subset \mathbb{E}^2$ - фигура на плоскости, $IsomF \simeq \mathbb{Z}_2$ - группа из двух элементов.
Следовательно, группа движений F тоже должна состоять из двух элементов. Тогда, например, F может быть равнобедренным треугольником (но не равносторонним, т.к. в таком случае сохраняющих движений будет больше).
Равнобедренный треугольник сохраняет тождественное движение (единичный элемент группы) и следующая осевая симметрия

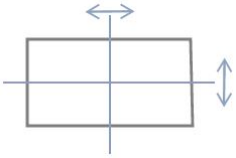
2) Пункт б). $F \subset \mathbb{E}^2$, $IsomF \simeq \mathbb{Z}_3$.
Например, это могут быть 3 отрезка на сторонах равностороннего треугольника, равные по длине половине стороны. Идея в том, чтобы из группы движений правильного треугольника убрать все симметрии и оставить только повороты.

Если мы хотим получить связную фигуру, то того же эффекта можно добиться наоборот за счет добавления чего-то к равностороннему треугольнику. Например,



3) Пункт в). $F \subset \mathbb{E}^2$, $IsomF \simeq S_3$.
На прошлом семинаре было показано, что $S_3 \simeq D_3$, а D_3 - это группа движений, сохраняющих равносторонний треугольник.

4) Пункт г). $F \subset \mathbb{E}^2$, $IsomF \simeq V_4$.
Это может быть прямоугольник (или ромб), который не является квадратом.



В группе движений прямоугольника две осевые симметрии и два поворота (на 0 и на π).
Это как раз группа Клейна: 3 неединичных элемента, квадрат каждого из которых равен единице (тождественному движению). Легко проверить, что произведение любых двух нединичных элементов дает третий.

Решение упражнения 1.3

Задача. Изоморфны ли $GL_3(\mathbb{C})$ и $GL_2(\mathbb{C})$?

Решение.

Попробуем найти некоторое групповое свойство, которое в одной группе выполнено, а в другой нет.
Посмотрим на элементы второго порядка $o(x) = 2$. Это матрица, квадрат которой равен единичной матрице. Сколько таких элементов в $GL_2(\mathbb{C})$ и $GL_3(\mathbb{C})$?

На матрицы удобно смотреть геометрически: они изображают линейные преобразования.

Из курса линейной алгебры: если A - линейный оператор, такой что $A^2 = E$, то в жордановой форме все его жордановы клетки имеют размер 1. Этот факт вытекает из решения такой задачи: как вычислить многочлен от жордановой клетки? В частности, жорданова клетка размера больше 1 при возведении в любую степень не может дать единичную матрицу.
Итак, жорданова нормальная форма у такого оператора диагональна. Кроме того, на диагонали должны стоять ± 1, т.к. при возведении в квадрат диагональные элементы будут возводиться в квадрат, а мы хотим в итоге получить единичную матрицу.

$$A^2 = E \;\Leftrightarrow\; J(A) = \begin{pmatrix} \pm 1 & & 0 \\ & \ddots & \\ 0 & & \pm 1 \end{pmatrix} \tag{2.1}$$

Соответствие взаимно-однозначное, потому что не важно, в каком базисе рассматривать линейный оператор: в исходном базисе или в жордановом.

Таким образом, мы охарактеризовали матрицы второго порядка в $GL_2(\mathbb{C})$ и $GL_3(\mathbb{C})$. Их бесконечно много, т.к. то, что матрица имеет такую жорданову нормальную форму, означает, что она путем замены базиса приводится к виду (2.1). Иначе говоря, матрицы A и $J(A)$ сопряжены.

$$A = CJ(A)C^{-1}, \tag{2.2}$$

где C - матрица перехода от исходного базиса к жорданову. C может быть любой невырожденной матрицей. Тогда матриц A - континуум.

Таким же образом можно вывести вид матриц порядка n: разница в том, что на диагонали будут стоять $\sqrt[n]{1}$, а дальше рассуждение такое же.

Элементов данного порядка в каждой из интересующих нас групп континуально много. Получается, по количеству элементов порядка n их не различить.

При этом, хотя элементов порядка 2 бесконечно много, матриц вида (2.1) конечное число (единичную мы исключаем, т.к. у нее порядок 1). В $GL_2(\mathbb{C})$ их 3, а в $GL_3(\mathbb{C})$ их 7.

Осталось сформулировать это свойство в групповых терминах.

Заметим, что жорданова нормальная форма определена однозначно с точностью до перестановки жордановых клеток. Соответственно, перестановками можно добиться

$$J(A) = \begin{pmatrix} \pm 1 & & 0 \\ & \ddots & \\ 0 & & \pm 1 \end{pmatrix} \to \begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{pmatrix} \tag{2.3}$$

Разные жордановы формы вида (2.3) уже не могут соответствовать одной и той же матрице. По теореме единственности жордановой формы данную матрицу второго порядка можно привести к единственной жордановой нормальной форме (ЖНФ) вида (2.3).

Таким образом, с точки зрения групп нужно смотреть не на сами элементы второго порядка, а на то, как они разбиваются на классы сопряженности в силу (2.2). Понятие сопряженности является групповым, т.к формулируется в терминах групповых операций: умножения и взятия обратного. Значит, разбиение на классы сопряженности при любом изоморфизме должно сохраняться.
В частности, классов сопряженности должно быть одинаковое количество.

В В $GL_2(\mathbb{C})$ два класса сопряженности элементов второго порядка, которые представлены ЖНФ вида

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

В В $GL_2(\mathbb{C})$ три класса сопряженности элементов второго порядка

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Наконец, мы можем сделать вывод, что $GL_3(\mathbb{C})$ и $GL_2(\mathbb{C})$ не изоморфны.

Отношение сопряженности элементов группы

Определение 2.7. *Элементы $x, y \in G$ сопряжены ($x \sim y$), если $\exists\, g \in G$ - сопрягающий элемент такой, что*

$$x = g \cdot y \cdot g^{-1}.$$

Свойство.

Сопряженность - это отношение эквивалентности (3 свойства: рефлексивность, симметричность, транзитивность).
$x \sim x$, $g := e$;
$x \sim y \;\Rightarrow\; x = gyg^{-1} \;\Rightarrow\; y = g^{-1}xg \;\Rightarrow\; y \sim x$;
$x \sim y,\ y \sim z \;\Rightarrow\; x = gyg^{-1}, y = hzh^{-1} \;\Rightarrow\; x = (gh)z(g^{-1}h^{-1}) = (gh)z(gh)^{-1} \;\Rightarrow\; x \sim z$.

Определение 2.8. *Классы сопряженности - классы эквивалентности по отношению сопряженности.*
Обозначение: класс эквивалентности, содержащий элемент x, $C(x) = C_G(x) = \{gxg^{-1} \mid g \in G\}$.

Определение 2.9. *$x \in G$ - центральный, если $C(x) = \{x\} \Leftrightarrow\; gxg^{-1} = x \forall g \in G \;\Leftrightarrow\; gx = xg$.*

Т.е. центральные элементы - это такие элементы, которые коммутируют со всеми элементами группы. В частности, в абелевой группе все элементы центральные. Единичный элемент всегда центральный.

Определение 2.10. *$Z(G) = \{x \in G \mid gx = xg\ \forall g \in G\}$ - центр группы G.*

Утверждение 2.1. *$Z(G)$ - подгруппа в G.*

Доказательство. Чтобы это проверить, нужно взять два центральных элемента и проверить, что их произведение - центральный элемент, а также что обратный к любому центральному - центральный.
Случай произведения простой, поэтому покажем только для обратного элемента.
Имеем: $x \in Z(G),\ gx = xg,\ \forall g$. Тогда

$$x^{-1}gxx^{-1} = x^{-1}xgx^{-1} \;\Leftrightarrow\; x^{-1}g = gx^{-1} \;\Rightarrow\; x^{-1} \in Z(G).$$

□

Свойство. Если $x \sim y$, то $o(x) = o(y)$.

Доказательство. $x = gyg^{-1}$
При воздведении в степень происходит следующее

$$x^n = \underbrace{(gyg^{-1})(gyg^{-1})\dots(gyg^{-1})}_{n} = gy^ng^{-1}.$$

Если $y^n = e$, то $x^n = geg^{-1} = gg^{-1} = e$.
Если $x^n = e$, то, т.к. $y^n = g^{-1}xg$, $y^n = g^{-1}g = e$. □

Отношение сопряженности в группе подстановок

$G = S_n$. Хотим понять, как выглядят подстановки σ', сопряженные с $\sigma \in S_n$ (имеющие вид $\pi\sigma\pi^{-1}$, $\pi \in S_n$).

Основная теорема о стурктуре подстановок: всякая подстановка является произведением нескольких независимых циклов.

$$\sigma = (i_1, \dots, i_l) \cdot (j_1, \dots, j_m) \cdot \dots \cdot (k_1, \dots, k_p) \tag{2.4}$$

Тогда

$$\pi\sigma\pi^{-1} = \underbrace{\pi(i_1, \dots, i_l)\pi^{-1}}\underbrace{\pi(j_1, \dots, j_m)\pi^{-1}}\dots\underbrace{\pi(k_1, \dots, k_p)\pi^{-1}} \tag{2.5}$$

а) $\sigma = (i_1, \dots, i_l)$ - циклическая. Определим вид $\pi\sigma\pi^{-1}$.

Циклическая подстановка на элементах цикла действует следующим образом

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \xrightarrow{\sigma} \dots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_{k+1} \xrightarrow{\sigma} \dots \xrightarrow{\sigma} i_l \xrightarrow{\sigma} i_1,$$

при этом любой элемент i, не вошедший в этот цикл под действием σ, остается на месте.

Когда мы применяем π^{-1} к какому-то номеру i, то получаем новый номер j, на который дальше действует σ. При этом важно, попадает ли j в орбиту цикла или является отдельно стоящим.

1) Если $j = i_k = \pi^{-1}(i)$, то $i = \pi(i_k)$. Проследим за судьбой i:

$$i = \pi(i_k) \xrightarrow{\pi^{-1}} i_k \xrightarrow{\sigma} i_{k+1} \xrightarrow{\pi} \pi(i_{k+1})$$

Итоговое преобразование осуществляет сдвиг $\pi(i_k) \xrightarrow{\pi^{-1}\sigma\pi} \pi(i_{k+1})$. Таким образом, если мы возьмем все номера $i_1, \dots, i_l$ из орбиты исходного цикла и применим к ним отображение π, то получим новый набор из l номеров, на котором наша сопряженная подстановка действует по циклу в том же порядке.

$$\pi(i_1) \xrightarrow{\pi\sigma\pi^{-1}} \pi(i_2) \xrightarrow{\pi\sigma\pi^{-1}} \dots \xrightarrow{\pi\sigma\pi^{-1}} \pi(i_l) \xrightarrow{\pi\sigma\pi^{-1}} \pi(i_1)$$

2) Если $j = \pi^{-1}(i)$ - неподвижный элемент, то

$$i \xrightarrow{\pi^{-1}} j \xrightarrow{\sigma} j \xrightarrow{\pi} i$$

В итоге, $\pi\sigma\pi^{-1} = (\pi(i_1), \ldots, \pi(i_l))$.
Вывод: мы в явном виде научились сопрягать циклические подстановки.

б) Если σ распалась в произведение (2.4), то сопряженная подстановка распадется в произведение циклов (2.5), а каждый из сопряженных легко написать явно

$$\pi\sigma\pi^{-1} = (\pi(i_1), \ldots, \pi(i_l)) \cdot (\pi(j_1), \ldots, \pi(j_m)) \cdot \ldots \cdot (\pi(k_1), \ldots, \pi(k_p)),$$

т.е. получилось снова произведение такого же количества циклов тех же длин. Кроме того, эти циклы независимы, т.к. π - взаимно-однозначное соответствие.

Кратко: Подстановка, сопряженная с данной подстановкой σ, имеет ту же цикловую стурктуру.

в) Верно ли обратное: сопряжены ли две подстановки одинаковой цикловой структуры?
Пусть

$$\sigma = (i_1, \ldots, i_l) \cdot (j_1, \ldots, j_m) \cdot \ldots \cdot (k_1, \ldots, k_p)$$
$$\sigma' = (i'_1, \ldots, i'_l) \cdot (j'_1, \ldots, j'_m) \cdot \ldots \cdot (k'_1, \ldots, k'_p)$$

Как устроена сопрягающая подстановка π?
На элементах циклов

$$i_1 \xrightarrow{\pi} i'_1$$
$$\ldots$$
$$k_p \xrightarrow{\pi} k'_p$$

На неподвижных под действием σ номерах $r_1, \ldots, r_q$

$$r_1 \xrightarrow{\pi} r'_1$$
$$\ldots \quad ,$$
$$r_q \xrightarrow{\pi} r'_q$$

где $r'_1, \ldots, r'_q$ - другие неподвижные элементы, т.к. у σ и σ' одинаковая цикловая структура.
Согласно предыдущим вычислениям, $\sigma' = \pi\sigma\pi^{-1}$.

При это сопрягаяющая подстановка π определена не однозначно хотя бы потому, что порядок неподвижных элементов при отображении определен не однозначно.

Доказано утверждение

Утверждение 2.2. *Классы сопряженности в S_n состоят из всех подстановок одинаковой цикловой структуры.*

Найдем центр $Z(S_n)$.

По определению, центральный элемент - это такой элемент, в классе сопряженности которого только он сам. Чтобы подстановка была центральной, нам нужно придумать такую цикловую структуру, чтобы ей удовлетворяля единственная подстановка.

Так, транспозиция может быть центральной подстановкой $\Leftrightarrow$ транспозиция существует только одна, т.е. при $n = 2$.
То же можно сказать и про любую другую цикловую структуру.
1. Если в разложении есть цикл длины больше 2, то можно в нем поменять местами первые два элемента, а все остальное не трогать. Тогда получим другую пожстановку той же структуры. Значит, при наличии цикла длины больше 2 подстановка не может быть центральной.
2. Пусть все циклы имеют длину 2. Перемешав элементы из двух разных транспозиций, получим другую подстанову с такой же структурой.
3. Пусть транспозиция всего одна, $n > 2$. Тогда можно поменять элемент из транпозиции с любым другим неподвижным элементом, и снова нарушается центральность.

Остался только случай, когда циклов нет вообще, т.е. подстановка тождественная. Доказали следующее утверждение

Утверждение 2.3.

$$Z(S_n) = \begin{cases} \{\mathrm{id}\}, & n > 2 \\ S_2, & n = 2 \end{cases}$$

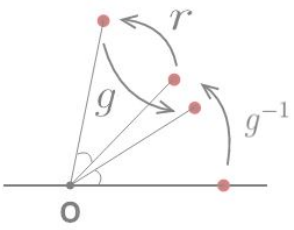
Отношение сопряженности в группе Диэдра

Напомним, что в группе D_n $2n$ элементов: n симметрий и n поворотов. Разберемся с сопряженностью в каждом из этих классов отдельно.

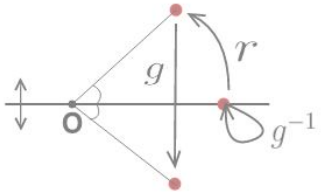
1. Пусть $r \in D_n$ - поворот. Как тогда выглядит $grg^{-1},\ g \in D_n$?

Легко различить поворот и симметрию: поворот сохраняет ориентацию, а симметрия меняет. g, g^{-1} одновременно лиюо сохраняют, либо меняют ориентацию, r ориентацию сохраняет. Следовательно, перемножив эти три преобразования, получим собственное движение.
Итак, grg^{-1} - тоже поворот.

Чтобы понять, что это за поворот, достаточно проследить за одной точкой.
а) Если g - поворот, то $grg^{-1} = r$.



б) Если g - симметрия, то $grg^{-1} = r^{-1}$ - поворот на противоположный угол.

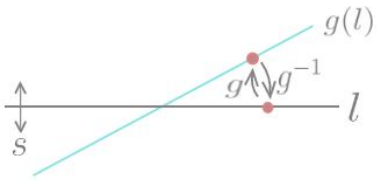


Таким образом, класс сопряженности поворота в D_n состоит из самого поворота и обратного к нему $C(r) = \{r, r^{-1}\}$. Если r - поворот на угол 0 или π, то $C(r) = \{r\}$.

2. Пусть $s \in D_n$ - симметрия.

gsg^{-1} - симметрия, т.к. если бы мы из симметрии получили поворот, то обратным сопряжением к этому повороту мы бы получили исходную симметрию. При этом из поворота с помощью сопряжения можно получить только поворот.
По-другому: каким бы мы ни выбрали g, в произведении gsg^{-1} ориентация поменяется нечетное число раз.

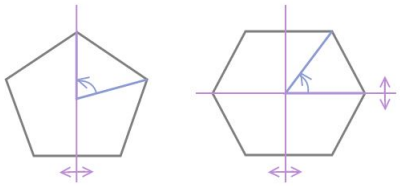
Пусть s - симметрия относительно оси l, $s = s_l$. С точки зрения преобразования s прямая l состоит из неподвижных точек. Соответственно, если мы хотим указать вид gsg^{-1}, то нужно указать ось этой симметрии.
Это будет прямая $g(l)$. В самом деле, проследим за движением точки прямой $g(l)$. Под лействием g^{-1} она попадает на прямую l, затем s оставляет ее на месте, а g переводит снова на прямую $g(l)$.



Получили общее описание симметрии, сопряженной с данной симметрией.

$$gs_lg^{-1} = s_{g(l)}$$

На какие классы сопряженности распадается множество симметрий?
Напомним общий вид сей симметрии для нечетного и четного n.



1) n нечетно, тогда все оси устроены одинаково и любую ось можно перевести в другую с помощью поворота.
   Значит, все оси симметрии при нечетном n сопряжены.

2) n четно, тогда есть 2 типа осей симметрии: проходящие через вершины и через середины сторон.
   При помощи преобразования, которое сохраняет правильный многоугольник нельзя из оси одного типа получить ось другого типа. Действительно, при таком преобразовании вершины переходят в вершины, а середины сторон переходят в середины сторон.
   Оси одного типа можно переводить друг в друга с помощью поворота.

   Симметрии при четном n разбиваются на 2 класса сопряженности по $\frac{n}{2}$ элементов.

Найдем центр $Z(D_n)$.

Известно, как выглядят классы сопряженности в D_n. Из них нужно выбрать классы, состоящие из одного элемента.
Поворот на 0 (тождественное преобразование) всегда лежит в центре. При четном n там также содержится поворот на π.
Симметрия может быть центральной только если $n = 2$. (Если n нечетно, имеем класс сопряженности из $n > 1$ элементов, а если n четно, то 2 класса по $\frac{n}{2} \geq 1$ элементов.)

$$Z(D_n) = \begin{cases} \{e\}, & n = 2k+1 \\ \{e, r_\pi\}, & n = 2k,\ n > 2 \\ D_2 \simeq V_4, & n = 2 \end{cases}$$

Теорема Лагранжа и классификация конечных групп

Теорема 2.1. ***Лагранжа***
Пусть G - конечная группа, $G \supset H$ - подгруппа. Тогда $|H| \mid |G|$ (порядок группы делится на порядок подгруппы).

Следствие 2.1. *Пусть $|G| = n < \infty,\ g \in G$. Тогда $o(g) \mid n = |G|$. Отсюда $g^n = e$.*

Доказательство. $H := \langle g \rangle = \{g^k,\ k \in \mathbb{Z}\}$.
Если $o(g) = m$, то $\langle g \rangle = \{e,\ g,\ g^2,\ \ldots,\ g^{m-1}\} \simeq \mathbb{Z}_m$.

Если $o(g) = \infty$, то $\langle g \rangle \simeq \mathbb{Z}$.

$|H| = o(g)$, теперь можно применить теорему Лагранжа и получить утверждение следствия. $\square$

Классификация конечных групп

Утверждение 2.4. *Если $|G| = p$ - простое, то $G \simeq (\mathbb{Z}_p, +)$.*
Т.е. для простого порядка существует ровно одна группа данного порядка (с точностью до изоморфизма).

Доказательство. Возьмем любой элемент $e \neq g \in G$, тогда $1 < o(g) \mid |G| = p$. Отсюда $o(g) = p$ и $\langle g \rangle \subset G$, $\langle g \rangle = G$, т.к. их порядки совпадают.
Циклическая группа данного порядка только одна (с точностью до изоморфизма). $\square$

Пример. Пусть p составное, например, $p = 4$. Тогда мы знаем уже как минимум 2 группы порядка 4: $\mathbb{Z}_4$ и V_4, не изоморфные друг другу.

Упражнение 2.4. *Доказать, что любая группа порядка 4 изоморфна $\mathbb{Z}_4$ или V_4.*

Пример. Пусть $p = 6$, известные нам группы порядка 6: $D_3 \simeq S_3, \mathbb{Z}_6$.

Упражнение 2.5. *Доказать, что любая группа порядка 6 изоморфна $\mathbb{Z}_6$ или S_3.*

Домашнее задание из заданика: 56.7 б),в), 56.28, 57.30 б), 58.19 б), 58.22, 58.11 б),в).

Лекция 3

Решение задач 58.19 б), 57.30 б), 58.22

Задача 58.19 б) Найти центр группы A_n четных подстановок.

Решение. Мы знаем, как устроено отношение сопряженности в группе всех подстановок S_n. Т.е. умеем отвечать на следующий вопрос: если $\sigma, \sigma' \in S_n$, то существует ли $\pi \in S_n : \ \sigma' = \pi\sigma\pi^{-1}$?
Для этого необходимо и достаточно, чтобы подстановки σ и σ' имели одинаковую цикловую структуру. Более того, если две подстановки имеют одинаковую цикловую структуру, мы можем легко такую подстановку π построить.

В чем отличие, если мы рассматриваем сопряженность в группе четных подстановок?
Пусть $\sigma, \sigma' \in A_n$, тогда их цикловая струкутра уже не может быть любой. Четность подстановки по ее разложению на циклы легко определить: цикл четной длины - это нечетная подстановка, а цикл нечетной длины - четная. При произведении циклов четности перемножаются.

Сопрягающая подстановка π тоже должна быть четной.
Вообще говоря, если есть две подстановки одинаковой цикловой структуры, мы может подобрать подстановку из $\pi' \in S_n : \ \sigma' = \pi'\sigma(\pi')^{-1}$. Пусть π' оказалась нечетной. Предположим, существует еще одна четная подстановка π, которая сопрягает σ и σ': $\sigma' = \pi\sigma\pi^{-1}$.
Тогда выполнено

$$\sigma = \pi^{-1}\sigma'\pi = \pi^{-1}\pi'\sigma(\pi')^{-1} =: \psi\sigma\psi^{-1}.$$

При этом ψ будет нечетной как произведение четной и нечетной подстановок.

Вывод: Если одна четная подстановка переводится в другую с помощью сопряжения какой-то нечетной подстановкой, то для существования четной подстановки, выполняющей ту же работу, нужно, чтобы существовала нечетная подстановка ψ, оставляющая σ на месте.

Если для подстановки σ существует такая ψ, то любая подстановка σ', сопряженная с σ в группе S_n, сопряжена с σ и в группе A_n. *Класс сопряженности σ в S_n совпадает с классом сопряженности σ в A_n.*

Пусть такой подстановки не существует. Если мы будем сопрягать σ с помощью четных подстановок, то получим класс сопряженности σ в A_n. Если же будем сопрягать с помощью всех подстановок, то получим класс сопряженности σ в S_n. При этом $C_{A_n}(\sigma) \neq C_{S_n}(\sigma)$, иначе попадем в предыдущий случай. Класс сопряженности σ в группе S_n распадается на два

$$C_{S_n}(\sigma) = C_{A_n}(\sigma) \cup C_{A_n}(\sigma'),$$

где $\sigma' = \pi'\sigma(\pi')^{-1}$, π' - нечетная. σ' не сопряжена с σ в A_n, потому что иначе это первый случай.
С другой стороны, любая другая подстановка той же цикловой структуры либо получается из σ сопряжением с четной подстановкой и тогда она в $C_{A_n}(\sigma)$, либо она получается сопряжением с нечетной подстановкой и тогда она в $C_{A_n}(\sigma')$. Но всякую нечетную подстановку можно представить в виде произвдения π' на какую-то четную подстановку.

В S_2 есть 2 смежных класса, подгруппа A_n в S_n имеет индекс 2. Всякая нечетная подстановка получается из какой-то фиксированной нечетной подстановки путем умножения на всевозможные четные подстановки. Поэтому если мы будем сопрягать σс помощью нечетных подстановок, сначала можно ее сопрячь с помощью какой-то одной нечетной подстановки (π' фиксировано), а дальше сопрягать с помощью четных подстановок и получить все сопряженные с σ подстановки в S_n.

Критерий.

Для того, чтобы $C_{A_n}(\sigma)$ совпадал с $C_{S_n}(\sigma)$ необходимо и достаточно, чтобы существовала нечетная подстановка $\psi:\ \psi\sigma\psi^{-1} = \sigma$.
Иначе $C_{S_n}(\sigma) = C_{A_n}(\sigma) \cup C_{A_n}(\sigma')$, где $\sigma' = \pi'\sigma(\pi')^{-1}$, π' - нечетная.

Идею завершения решения приведем после следующей задачи.

Задача 57.30 б) Найти классы сопряженных элементов группы A_4.
Решение. В A_4 бывают следующие цикловые структуры:

$$\begin{gathered} e \\ (i\ j)(k\ l) \\ (i\ j\ k) \end{gathered}$$

Эти цикловые структуры задают классы сопряженности в группе S_4.
Теперь нужно понять, как каждый из этих классов распадается (если распадается) на классы сопряженности в группе A_4.

Критерий: существует ли сопрягающая подстановка $\psi \in S_n \backslash A_n:\ \psi\sigma\psi^{-1} = \sigma$?

1) $\sigma = e$, подходит любая $\psi \in S_n \backslash A_n$.
   Получаем 1 класс сопряженности.

2) $\sigma = (i\ j)(k\ l)$, например, $\psi = (i\ j)$.
   По правилу сопряжения при вычислении $\psi\sigma\psi^{-1}$ нужно в σ заменить каждвй элемент на его образ при подстановке ψ, получится

$$\psi\sigma\psi^{-1} = (j\ i)(k\ l) = (i\ j)(k\ l).$$

   Следовательно, класс сопряженности не распадается.

3) $\sigma = (i\ j\ k)$.
   Для того, чтобы тройной цикл перешел в себя, нужно, чтобы сопрягающая

подстановка тоже была тройным циклом, а четвертый элемент оставался на месте. При сопряжении мы просто на запись цикла действуем сопрягающим преобразованием. Четвертый элемент в эту запись не вошел, и не должен войти после преобразования.
ψ - это либо транспозиция двух номеров из i, j, k, либо тройной цикл на i, j, k.

Если ψ - транспозиция, то при сопряжении получим обратный цикл $(k\ j\ i)$.
Если ψ - тройной цикл, то это четная подстановка, а нас интересуют сопряжения с нечетными.

Таким образом, подстановки ψ из критерия не существует, и класс распадается на два.

Первый класс сопряженности.
Зафиксируем один тройной цикл (1 2 3) и рассмотрим его класс сопряженности в группе A_n. При сопряжении с некоторой подстановкой π получим $(\pi(i)\ \pi(j)\ \pi(k))$.
Значит, $C_{A_n}(1\ 2\ 3) = \{(\pi(i)\ \pi(j)\ \pi(k)),\ \pi \in A_4\}$.

Второй класс сопряженности.
Сначала сопрягаем с помощью какой-то нечетной подстановки, а потом к результату применяем всевозможные четные подстановки. Получим класс $C_{A_n}(2\ 1\ 3)$.

Заметим, что цикл (1 2 3) обратен циклу (2 1 3), откуда следует, что все циклы из первого класса сопряженности обратны соответствующим циклам из второго класса сопряженности. Т.е. класс сопряженности тройных циклов разбивается на два подкласса, которые взаимно обратны друг другу.

Задача 58.19 б) Найти центр A_n.
Идея.
Решается по той же схеме что и задача про центр группы S_n с учетом устройства классов сопряженности в A_n. Центр - это те элементы, которые сопряжены сами себе. Нужно определить, когда подстановка сопряжена только сама себе в A_n, в S_n ее класс сопряженности может состоять максимум из двух подстановок: она сама и некоторая σ', которая получается нечетным сопряжением.

Задача 58.22 Пусть G - множество верхних унитреугольных матриц порядка 3 с элементами поля $\mathbb{Z}_p$
1) Доказать, что G - некоммутативная группа порядка p^3 относительно умножения;
2) Найти центр группы G;
3) Найти все классы сопряженных элементов группы G.

Решение.

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c \in \mathbb{Z}_p \right\}$$

1) Нужно показать, что G - подгруппа группы матриц 3×3 над полем $\mathbb{Z}_p$. Т.е. нужно проверить замкнутость относительно операций.
$|G| = p^3$, потому что элементы этой группы зависят от трех параметров: a, b, c, и каждый и параметров пробегает p значений.

Чтобы понять, что умножение не коммутативно, перемножим две матрицы такого вида

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \in G \tag{3.1}$$

Если бы в правом верхнем углу произведения не было ac', то умножение было бы, очевидно, коммутативным. Если же мы переставим местами эти две матрицы, то ac' поменяется на $a'c$.

Группа также должна быть замкнута относительно операции взятия обратного элемента. Покажем, что это так. Подберем в (3.1) a', b', c' так, чтобы в правой части получилась единичная матрица.

$$\begin{cases} a + a' = 0 \\ c + c' = 0 \\ b + b' + ac' = 0 \end{cases} \Rightarrow \begin{cases} a' = -a \\ c' = -c \\ b' = ac - b \end{cases}$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in G$$

Таким образом, G - некоммутативная подгруппа в группе всех матриц порядка 3 над полем $\mathbb{Z}_p$.

2) Если мы найдем классы сопряженности, то легко напишем и центр - множество одноэлементных классов сопряженности. Поэтому решаем сразу и пункт 2), и пункт 3).
Запишем общий вид сопряженной матрицы

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & xy-z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & y+b+xc \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & xy-z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & a & b+xc-az \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \tag{3.2}$$

Получили, что сопряженная матрица от исходной отличается только в одном элементе на слагаемое $xc - az$. Меняя сопрягающую матрицу, мы можем получить любой элемент $\mathbb{Z}_p \ni g = b + xc - az$. Таким образом,

$$C\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix} = \left\{\begin{pmatrix}1 & a & *\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\right\},\ \ a \neq 0 \text{ или } c \neq 0.$$

Если $a = 0$ и $c = 0$, то

$$C\begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = \left\{\begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\right\}$$

$$Z(G) = \left\{\begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},\ b \in \mathbb{Z}_p\right\}$$

Классификация конечных групп. Группы порядка 4

Классификация групп порядка 4 (решение упражнения 2.4)

Покажем, что любая группа порядка 4 изоморфна $\mathbb{Z}_4$ или V_4.

Решение. Пусть $|G| = 4$. Заметим, что $\forall g \in G\ o(g) \mid |G| = 4$, т.е. $o(g) = 1, 2, 4$.

Случай 1. Пусть $\exists$ элемент g порядка 4. Тогда $G = \langle g\rangle_4$ (обозначение: $\langle g\rangle_4$ - циклическая группа порядка 4).
Все циклические группы данного порядка изоморфны, $G \simeq \mathbb{Z}_4$.

Случай 2. Пусть теперь $\forall g \in G\ g^2 = e$. Обозначим элементы группы

$$G = \{e, a, b, c\},\ a^2 = b^2 = c^2 = e.$$

Это часть тех соотношений, которые выполняются в группе Клейна. Проверяем остальные соотношения.
ab может быть равно любому из $\{e, a, b, c\}$.
$ab \neq e$, т.к. тогда b был бы обратен к a, но к a обратен a, потому что $a^2 = e$.
$ab \neq a$, т.к. $b \neq e$.
$ab \neq b$, т.к. $a \neq e$.
Получается, $ab = c$.

Аналогично, $ab = ba = c,\ ac = ca = b,\ bc = cb = a$.
Таким образом, $G \simeq V_4$.

Классификация конечных групп данного порядка

Выпишем, какие группы небольших порядков нам известны.

$\|G\|$	G
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ V_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ S_3 \simeq D_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ Q_8,\ D_4+$ еще 2 абелевы группы
9	$\mathbb{Z}_9$ + еще 1 абелева группа
10	$\mathbb{Z}_{10},\ D_5$

Все группы простого порядка единственны с точностью до изоморфизма.
По упражнению 2.4, есть только 2 группы порядка 4.
По упражнению 2.5, есть только 2 группы порядка 6.
Нам пока известны 3 группы порядка 8.
Покажем, что $\mathbb{Z}_8,\ Q_8,\ D_4$ не изоморфны.
Q_8 не изоморфна D_4, т.к. в Q_8 существует единственный элемент порядка 2 (а именно, -1), в D_4 5 элементов порядка 2 (4 симметрии и $r_p i$).
$\mathbb{Z}_8$ не изоморфна Q_8 и D_4, т.к. $\mathbb{Z}_8$ абелева, а Q_8 и D_4 - нет.

Нормальные подгруппы

Определение 3.11. *Подгруппа $H \subseteq G$ называется нормальной ($H \triangleleft G$), если выполнены эквивалентные условия:*
(1) $gH = Hg$, $\forall g \in G$,
(2) $gHg^{-1} = H$, $\forall g \in G$.

Условие (2) можно немного ослабить:
(3) $gHg^{-1} \subseteq H$, $\forall g \in G$ или, эквивалентно:
(4) $\forall g \in G,\ h \in H\ \ ghg^{-1} \in H$.

Другими словами, условие (3) означает, что при каждом сопряжении подгруппа H не выходит за свои пределы, а условие (4) означает, что подгруппа H является объединением некоторого количества целых классов сопряженности.

Почему (2) эквивалентно (3)? Очевидно, (2) $\Rightarrow$ (3). Покажем, что (3) $\Rightarrow$ (2).
Дано, что $\forall g \in G\ \ gHg^{-1} \subseteq H$. Домножим каждое из этих двух подмножеств на g^{-1} слева и на g справа, при это включение сохранится. Получим $H \subseteq g^{-1}Hg$, $\forall g \in G$.
Теперь можно вместо g взять g^{-1} и получить равенство.

Примеры нормальных подгрупп.

1) Пусть G - группа, тогда тривиальные подгруппы $\{e\}, G \triangleleft G$.

2) Пусть G - абелева группа. Тогда любая ее подгруппа нормальна, т.к. умножение коммутативно.

3) $Z(G) \triangleleft G$, т.к. если $H := Z(G)$, то по определению центра H коммутирует с любым элементом группы, а это уловие (1).

Решение задач на перечисление нормальных подгрупп

Задача 58.4 а) Найти все нормальные подгруппы, отличные от тривиальных, в группе S_3.

Решение. *Общий подход к решению* задач, где нужно перечислить все нормальные подгруппы, следующий: удобно пользоваться эквивалентным условием (4). Нормалная подгруппа всместе с каждым ее элементом содержит и все ему сопряженные, т.е. нормальная подгруппа получается объединением нескольких классов сопряженности.

Классы сопряженности в группе S_3 нам известны:

$$\{e\}$$
$$(i,\ j)$$
$$(i,\ j,\ k)$$

Теперь нужно понять, какие из них мы можем объединить, чтобы получить подгруппу.

Во-первых, обязательно нужно включить единичный элемент. Во-вторых, нужно проверить замкнутость полученного множества относительно умножения и взятия обратного.

С обратным элементом все просто: он имеет ту же цикловую структуру, а значит лежит в том же классе сопряженности.
Для проверки замкнутости умножения нужно производить некоторые вычисления, поэтому сначала попробуем определить группу по косвенным признакам.
Используем следующее соображение: порядок подгруппы должен делить порядок группы.

$$|S_3| = 6$$

Выпишем мощности классов сопряженности:

$$\{e\} \text{ - 1 элемент,}$$
$$(i,\ j) \text{ - 3 элемента,}$$
$$(i,\ j,\ k) \text{ - 2 элемента.}$$

Кандидаты на нормальную подгруппу:

$$H_1 = \{e\},\ \ \{e\} \cup (i,\ j,\ k),\ \ H_3 = \{e\} \cup (i,\ j),\ \ H_4 = \{e\} \cup (i,\ j) \cup (i,\ j,\ k)$$

H_1, $|H_1| = 1$, очевидно, нормальная подгруппа.
H_2, $|H_2| = 3$ - это в точности подгруппа A_3 четных подстановок, поэтому умножение не проверяем. $A_3 \lhd S_3$.
$H_3, |H_3| = 4$, 4 не делит 6, значит, это не подгруппа.
$H_4, |H_4| = 6$, $H_4 = S_3$ - тривиальная нормальная подгруппа.

Ответ: $A_3 \lhd S_3$

Заметим, что в ходе решения были перечислены не все подгруппы группы S_3. Можно составить подгруппу из единичного элемента и любой конкретной транспозиции. Транспозиция - это элемент порядка 2, он порождает подгруппу второго порядка. Таких подгрупп будет еще 3, но каждая из них не будет нормальной. Как легко понять, больше подгрупп не бывает.

Задача 58.4 в) Найти все нормальные подгруппы, отличные от тривиальных, в группе S_4.

Решение. Перечислим все классы сопряженности в S_4 и их мощности .

$$\begin{array}{ccc} \{e\} & - & 1 \text{ элемент} \\ (i,\ j) & - & 6 \text{ элементов} \\ (i,\ j)(k,\ r) & - & 3 \text{ элемента} \\ (i,\ j,\ k) & - & 8 \text{ элементов} \\ (i,\ k,\ r,\ p) & - & 6 \text{ элементов} \end{array}$$

- Транспозицию $(i,\ j)$ можно выбрать $C_4^2 = 6$ способами.
- В произведении двух независимых транспозиций первую из них можно выбрать 6 способами, при этом вторая определяется однозначно. При этом не важно, какую из транспозиций мы поставим первой, поэтому количество таких произведений уменьшается вдвое и равно 3.
- Чтобы перебрать все тройные циклы, нужно выбрать элемент, который в этот цикл не войдет (4 способа) и циклически переставить тройку элементов в цикле (2 способа).
- Циклов из 4 элементов осталось $|S_4| - 1 - 6 - 3 - 8 = 4! - 18 = 6$.

$$|S_4| = 24$$

Будем искать объединения классов сопряженности порядка, делящего 24.

1) $H_1 = \{e\}$, H_1 - тривиальная нормальная подгруппа.
2) $H_2 = \{e\} \cup (i,\ j)(k,\ r)$, $|H_2| = 4$
   Обратный к паре транспозиций - это пара транспозиций, т.к. транспозиция - это элемент второго порядка.

Проверим произведение: $(1,\ 2)(3,\ 4)\cdot(1,\ 3)(2,\ 4) = (1,\ 4)(2,\ 3)$, т.е. при перемножении двух пар транспозиций получаем третью оставшуюся.
Получили, что $H_2 \simeq V_4$.
Условно можно записать: $V_4 \lhd S_4$.

3) $H_3 = \{e\} \cup (i,\ j)(k,\ r) \cup (i,\ j,\ k)$, $|H_4| = 12$
$H_3 = A_4 \lhd S_4$.

4) $H_4 = \{e\} \cup (i,\ j) \cup (i,\ j)(k,\ r) \cup (i,\ j,\ k) \cup (i,\ k,\ r,\ p)$, $H_4 = S_4 \lhd S_4$

Ответ: V_4, A_4

Домашнее задание из задачника: 58.4 б), 58.3, 58.10, 58.11 а).

Лекция 4

Задача о нормальных подгруппах в A_4

Задача 58.4 б) Найти все нормальные подгруппы, отличные от тривиальных, в группе A_4.

Решение. Выпишем классы сопряженности в группе A_4 (их подробное описание можно найти в предыдущем семинаре). Начнем с цикловой структуры.

$$\{e\}$$
$$(i,\ j)(k,\ l)$$
$$(i,\ j,\ k)$$

Далее нужно понять, какие из этих классов распадаются на два в группе четных подстановок, а какие остаются единым классом сопряженности.
Критерий: Класс $C(\sigma)$ не распадается $\Leftrightarrow$ существует нечетная подстановка ψ, которая при сопряжении оставляет σ на месте.

Для $(i,\ j)(k,\ l)$ $\psi = (i,\ j)$, этот класс не распадается.
Если подстановка π при сопряжении оставляет цикл $(i,\ j,\ k)$ на месте, то π может быть id, $(i,\ j,\ k)$, $(i,\ j,\ k) \cdot (i,\ j,\ k)$ - все это четные подстановки.
Следовательно, класс $(i,\ j,\ k)$ распадается на 2.

Теперь определим мощности классов сопряженности. В $\{e\}$ 1 элемент, в $(i,\ j)(k,\ l)$ 3 элемента, а $(i,\ j,\ k)$ распадается на 2 класса по 4 элемента.

$|A_4| = \frac{4!}{2} = 12$, поэтому есть только 1 способ составить нетривиальную подгруппу из классов сопряженности.
$H_1 = \{e\}$, $H_3 = \{e\} \cup (i,\ j)(k,\ l) \cup (i,\ j,\ k)$.
$H_2 = \{e\} \cup (i,\ j)(k,\ l) \simeq V_4 \triangleleft A_4$.

Ответ: V_4.

Задача 58.10 Доказать, то группа A_5 является простой (в ней нет нетривиальных нормальных подгрупп).

Решается по тому же принципу: нужно выписать классы сопрженности и показать, что из них никак нельзя скомпоновать множество, порядок которого делит порядок группы.

Факторгруппы

Пусть G - группа, $K \triangleleft G$. Нормальность означает, что левые смежные классы по подгруппе совпадают с правыми смежными классами.
Можно рассмотреть множество смежных классов и ввести на этом множестве структуру группы - получим факторгруппу.

Определение 4.12. *Факторгруппа* $G/K = \{gK \mid g \in G\}$.
Операция: пусть $A = aK,\ B = bK$, *тогда*

$$A \cdot B = \{x \cdot y \mid x \in A,\ y \in B\}.$$

Проверим, что $A \cdot B$ тоже является смежным классом.
Перепишем операцию произведения по-другому: $A \cdot B = a \cdot K \cdot b \cdot K$. В нормальной подгруппе левые смежные классы совпадают с правыми смежными классами, и в середине произведения $a \cdot K \cdot b \cdot K$ находится правый смежный класс $K \cdot b$. Заменим его на $b \cdot K$, получим $a \cdot b \cdot K \cdot K = a \cdot b \cdot K$.

Проверка аксиом группы для $a \cdot b \cdot K$ вытекает из того, что эти аксиомы выполнены в самой группе G. По сути, операция на смежных классах определяется через операцию на самой группе G.

Отметим, что нейтральный элемент в G/K - это $e \cdot K = K$.
Существование обратного: $(g \cdot K)^{-1} = g^{-1}K$.

Одно из применений факторгрупп в том, что можно строить новые группы (подгруппы) с помощью уже известных нам (нормальных подгрупп).

Пример. $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Заметим, что в группе $\mathbb{Z}$ есть только подгруппы - множества целых чисел, кратных какому-то n ($n\mathbb{Z}$). Других подгрупп не бывает, т.к. подгруппы в циклической группе тоже циклические, а циклическая подгруппа - группа, порожденная каким-то одним элементом $\langle m \rangle = m\mathbb{Z}$.
Подгруппа $m\mathbb{Z}$ нормальна, т.к. $\mathbb{Z}$ абелева, а в абелевых группах все подгруппы нормальны.

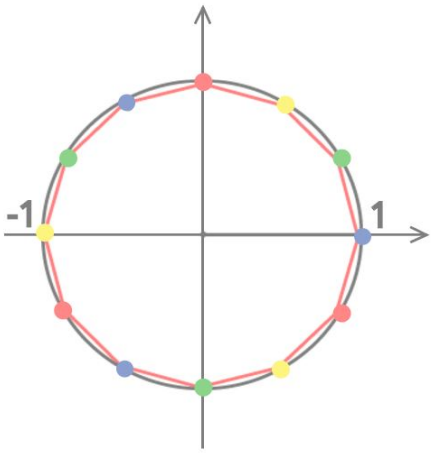
По определению вычетов получаем, что факторгруппа $\mathbb{Z}/m\mathbb{Z}$ является группой вычетов по модулю m.

Обозначение: $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$.
Это циклическая группа порядка n. Есть первообразный корень (на самом деле, их много): можно взять корень с самым маленьким аргументом $\frac{2\pi}{n}$, тогда его степени образуют множество всех корней из 1 степени n.
Таким образом, $\mathbb{U}_n \simeq \mathbb{Z}_n$.

Задача. Найти $\mathbb{U}_{12}/\mathbb{U}_3$.

Решение. Ясно, что любой корень 3 степени является корнем 12 степени, так что $\mathbb{U}_3$ - подгруппа $\mathbb{U}_{12}$. $\mathbb{U}_{12} \triangleright \mathbb{U}_3$, т.к. $\mathbb{U}_{12}$ абелева.

Отметим на комплексной плоскости все элементы $\mathbb{U}_{12}$ и выделим среди них (синим) элементы $\mathbb{U}_3$.



Теорема Лагранжа: количество смежных классов по подгруппе $H \subset G$ равно $\frac{|G|}{|H|}$.

Согласно этой теореме, $|\mathbb{U}_{12}/\mathbb{U}_3| = 4$. Изобразим эти смежные классы.

Один из них уже отмечен синим - это сама подгруппа $\mathbb{U}_3$ - единичный элемент факторгруппы.
Чтобы получить смежный класс, нужно взять какой-то элемент группы $\mathbb{U}_{12}$ и умножить его на все элементы из подгруппы.

Аргументы элементов $\mathbb{U}_3$: $\{0,\ \frac{2\pi}{3},\ \frac{4\pi}{3}\}$.

1) Возьмем элемент с аргументом $\frac{2\pi}{12}$ (отметим его зеленым). При перемножении с элементами $\mathbb{U}_3$ аргументы складываются. Получим класс с аргументами $\{\frac{\pi}{6},\ \frac{5\pi}{6},\ \frac{3\pi}{2}\}$.

2) Класс сопряженности элемента с аргументом $\frac{4\pi}{12}$ отметим желтым.

3) Класс сопряженности элемента с аргументом $\frac{6\pi}{12}$ отметим красным.

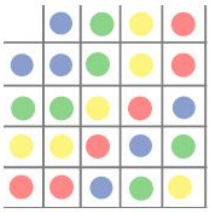
Наша факторгруппа имеет порядок 4, следовательно, она изоморфна либо V_4, либо $\mathbb{Z}_4$. Чтобы понять, какой именно группе она изоморфна, нужно описать операцию умножения.
Поскольку группа маленькая, удобно это сделать с помощью таблицы.

Как понять, что из себя представляет произведение двух смежных классов?
Нужно выбрать по подному представителю, перемножить их и посмотреть, в какой класс попдает произведение.

Первая строчка таблицы.
В синем классе удобно выбирать элемент с аргументом 0. Синий класс - это нейтральный элемент факторгруппы, поэтому при умножении любого класса на него получаем тот же класс.
Умножение коммутативно, следовательно, таблица симметрична относительно диагонали. Сразу записываем и первый столбец.

При умножении двух зеленых ($\frac{pi}{6} + \frac{5\pi}{6} = \pi$) попадаем в желтый.
При умножении двух желтых ($\frac{pi}{3} + \pi = \frac{4\pi}{3}$) попадаем в синий.
При умножении двух красных ($\frac{pi}{2} + \frac{7\pi}{6} = \frac{5\pi}{3}$) попадаем в желтый.

При умножении зеленого на желтый ($\frac{pi}{6} + \frac{\pi}{3} = \frac{\pi}{2}$) попадаем в красный.
При умножении зеленого на красный ($\frac{pi}{6} + \frac{\pi}{2} = \frac{2\pi}{3}$) попадаем в синий.
При умножении желтого на красный ($pi + \frac{\pi}{2} = \frac{3\pi}{2}$) попадаем в зеленый.



Получили таблицу умножения $\mathbb{Z}_4$.

Ответ: $\mathbb{U}_{12}/\mathbb{U}_3 \simeq \mathbb{Z}_4$.

В этом примере мы все посчитали вручную по определению. Ясно, что в общем случае вычисление факторгрупп таким образом - трудоемкая задача. Существует более универсальный метод вычисления факторгрупп, связанный с гомоморфизмами.

Гомоморфизм групп

Определение 4.13. *Гомоморфизм групп G, H - это отображение $\varphi : \ G \to H$ такое, что*

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y), \ \ \forall x, y \in G.$$

Заметим, что биективность здесь не требуется. Значит, отождетвлять группы с помощью гомоморфизма нельзя, но он сохраняет информацию о свойствах группы. Хотя часть информации может теряться при склеивании элементов, это может даже быть удобным, т.к. струкура группы может упроститься.

Образ гомоморфизма $\operatorname{Im}\varphi = \{h = \varphi(g) \mid g \in G\}$ - подгруппа в H.
Ядро гомоморфизма $\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e\}$ - нормальная подгруппа в G.

Утверждение 4.5. *Пусть $K \lhd G$, тогда K является ядром гомоморфизма $\pi : G \to G/K$.*

π называется *каноническим гомоморфизмом* (или канонической проекцией на факторгруппу).

$$\pi(g) = gK, \ \forall g \in G$$

По определению видно, что элементы $g : \pi(g) = e \in G/H$ лежат в K, т.к. $G/H \ni e = K$.

$$\operatorname{Ker}\pi = K$$

Теорема 4.2. ***(Основная теорема о гомоморфизмах)***
Пусть $\varphi : G \to H$ - гомоморфизм, тогда $\exists!$ изоморфизм $\overline{\varphi} : G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ такой, что

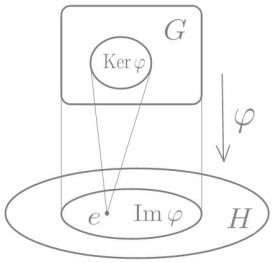
$$\varphi = \overline{\varphi} \circ \pi.$$

Другими словами, следующая диаграмма коммутативна.

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "\varphi"'] & G/\operatorname{Ker}\varphi \arrow[d, "\overline{\varphi}"] \\ H & \operatorname{Im}\varphi \arrow[l, phantom, "\supset"] \end{tikzcd}$$

Замечание. $\overline{\varphi}(g \operatorname{Ker}\varphi) = \varphi(g)$

Поясним смысл основной теоремы о гомоморфизмах на следующей картинке.



Посмотрим, как устроено отображение из группы G на подгруппу $\operatorname{Im}\varphi$. Это сюръекция по определению. Рассмотрим теперь прооообраз точки из $\operatorname{Im}\varphi$.
Если мы возьмем нейтральный элемент группы H, то прообразом будет $\operatorname{Ker}\varphi$.
Прооообразом любого другого элемента будет его смежный класс.

Таким образом, нужно показать, что два элемента имеют один и тот же образ $\Leftrightarrow$ они отличаются на множитель из ядра.
$\varphi(g') = \varphi(g) \Leftrightarrow \varphi(a) = e \Leftrightarrow a \in K$, т.к.
$g^{-1}g' = a, \;\; g' = ga \Rightarrow \varphi(g') = \varphi(g)\varphi(a)$.

Применение основной теоремы о гомоморфизмах к вычислению факторгрупп

Пусть задана $K \triangleleft G$, хотим вычислить G/K.
Нужно придумать гомоморфизм в какую-то группу H $\varphi : G \to H$ такой, что

$K = \operatorname{Ker}\varphi$. Тогда $G/K \simeq \operatorname{Im}\varphi$.

Пример 1. $A_n \triangleleft S_n$, S_n/A_n–?

Решение. Реализуем подгруппу A_n как Ker(sgn). sgn является гомоморфизмом $\operatorname{sgn} : S_n \to \mathbb{R}^\times$.
Тогда $S_n/A_n \simeq \operatorname{Im}(\operatorname{sgn}) = \{\pm 1\}$ - группа второго порядка.

Пример 2. $SL_n(K) \triangleleft GL_n(K)$, K - поле, $GL_n(K)/SL_n(K)$–?

Решение. Не будем непосредственно проверять, что это нормальная подгруппа, а сразу перейдем к вычислениям.
$SL_n(K) = \operatorname{Ker}(\det)$. Отображение det - гомоморфизм $\det : GL_n(K) \to K^\times$.
$GL_n(K)/SL_n(K) \simeq Im(\det) = K^\times$.
Для любого $\lambda \in K^\times$ можно придумать матрицу $g \in G$, определитель которой равен λ. Например,

$$g = \begin{pmatrix} \lambda & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

Задача 58.31 б) Найти $\mathbb{C}^\times/\mathbb{R}^\times$.
Решение. Нужно придумать гомоморфизм φ такой, чтобы в единицу переходило $\mathbb{R}^\times$ и только оно.
$\varphi(z) = \frac{z^2}{|z|^2}$, $\varphi : \mathbb{C}^\times \to \mathbb{C}^\times$.
Это гомоморфизм, произведение переходит в произведение. Квадраты нужны, чтобы расширить ядро от $\mathbb{R}^+$ (в случае $\varphi = \frac{z}{|z|}$, тогда в 1 переходят только положительные числа) до $\mathbb{R}^\times$ (при $\varphi = \frac{z^2}{|z|^2}$, в 1 переходят все ненулевые вещественные числа).
$\operatorname{Ker}\varphi = \mathbb{R}^\times$, тогда $\mathbb{C}^\times/\mathbb{R}^\times \simeq \operatorname{Im}\varphi$.

$z = r(\cos\alpha + i\sin\alpha)$, $\varphi(z) = \cos(2\alpha) + i\sin(2\alpha)$, если мы будем брать любые r и любые α, то в образе получим единичную окружность $\mathbf{U}$.
Ответ: $\mathbf{U}$.

Автоморфизм группы

Определение 4.14. *Автоморфизм группы G - это изоморфизм $\varphi : G \xrightarrow{\sim} G$ на себя.*

Множество автоморфизмов $\operatorname{Aut}(G)$ - группа относительно операции композиции.

Группа автоморфизмов является важной характеристикой группы G (ее структурным свойством).
Например, если у двух групп неизоморфные группы автоморфизмов, то эти группы и сами не могут быть изоморфны.

Таким образом, $\mathrm{Aut}(G)$ - некий инвариант группы.

Пример. Вычислим группу автоморфизмов циклической группы.

Пусть сначала G - **конечная циклическая группа**. Тогда $G \simeq (\mathbb{Z}_m, +)$.
Пусть есть гомоморфизм $\varphi : \mathbb{Z}_m \to \mathbb{Z}_m$. Как он устроен?
Основное его свойство - сумма переходит в сумму.

Чтобы задать гомоморфизм из циклической группы в какую-то другую группу, нужно сказать, куда переходит порождающий элемент. Потому что тогда мы также определим, куда переходит его сумма с самим собой любое число раз.

В нашем случае порождающий элемент - это $\overline{1}$ по модулю m. Положим

$$\varphi(\overline{1}) = \overline{k}$$

Отсюда

$$\varphi(\overline{n}) = \varphi(\underbrace{\overline{1} + \ldots + \overline{1}}_{n}) = \underbrace{\varphi(\overline{1}) + \ldots + \varphi(\overline{1})}_{n} = \overline{k} \cdot \overline{n}$$

Таким образом, всякий эндоморфизм (гомоморфизм в себя) группы вычетов - это умножение на некоторый фиксированный вычет.
Всякий эндоморфизм задается некоторым вычетом $\varphi = \varphi_{\overline{k}}$.
Понятно, что и наоборот: умножение на любой вычет является эндоморфизмом.

Пусть есть 2 эндоморфизма $\varphi = \varphi_{\overline{k}}$, $\psi = \psi_{\overline{l}}$. Рассмотрим их композицию

$$\varphi \circ \psi = \varphi_{\overline{k} \cdot \overline{l}}$$

Вопрос: в каком случае эндоморфизм, задаваемый умножением на $\overline{k}$ будет автоморфизмом?
Т.е. когда $\varphi = \varphi_{\overline{k}}$ обратим?
Ответ: когда $\overline{k}$ обратим, т.е. найдется такое l, что $\overline{k} \cdot \overline{l} = \overline{1}$. Другими словами, $\overline{k} \in \mathbb{Z}_m^{\times} = \{\overline{k} \mid \text{НОД}(k, m) = 1\}$.

Получаем, что

$$\mathrm{Aut}(\mathbb{Z}_m, +) \simeq \mathbb{Z}_m^{\times}$$

Пусть теперь G - **бесконечная циклическая группа**, $G \simeq (\mathbb{Z}, +)$.

В случае конечной группы мы рассматривали кольцо вычетов и показывали, то каждый автоморфизм его аддитивной группы - это умножение на некоторый обратимый элемент кольца вычетов.

Теперь вместо кольца вычетов будет $\mathbb{Z}$ - оно тоже порождено как группа одним элеиентом (единицей).
Так что любой эндоморфизм - это умножение на какое-то фиксированное целое число. Композиции эндоморфизмов соответствует произведение целыъ чисел, а если

мы хотим, чтобы эндоморфизм был обратимым, то этот множитель должен быть обратимым в $\mathbb{Z}$.
Таким образом,

$$\mathrm{Aut}(\mathbb{Z}, +) \simeq \mathbb{Z}^{\times} = \{\pm 1\}$$

Как видно, автоморфизмов у группы целых чисел не много, а вот у группы вычетов автоморфизмов может быть довольно много. Их количество равно функуции Эйлера $\varphi(m)$ - количество натуральных чисел $< m$, взаимно простых с m.

Задача 57.39 б) Найти группу автоморфизмов группы $\mathbb{Z}_6$.

Решение. Общий ответ:

$$\mathrm{Aut}(\mathbb{Z}_6) \simeq \mathbb{Z}_6^{\times}$$

Теперь выпишем эти обратимые вычеты

$$\mathbb{Z}_6^{\times} = \{\overline{1}, \overline{5}\}$$

Это группа из двух элементов, значит, она изоморфна $\mathbb{Z}_2$.

Ответ: $\mathrm{Aut}(\mathbb{Z}_6) \simeq \mathbb{Z}_2$.

а) Найти группу автоморфизмов группы $\mathbb{Z}_5$.

Решение. Общий ответ:

$$\mathrm{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_5^{\times}$$

Выпишем эти обратимые вычеты

$$\mathbb{Z}_5^{\times} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

Получилась группа из 4 элементов. Значит, она может быть изоморфна $\mathbb{Z}_4$ или V_4.

Чтобы показать, что группа автоморфизмов изоморфна $\mathbb{Z}_4$, укажем ее порождающий элемент: $\mathbb{Z}_5^{\times} = \langle \overline{2} \rangle$.
Действительно,

$$\overline{2}^2 = \overline{4}$$
$$\overline{2}^3 = \overline{8} = \overline{3}$$
$$\overline{2}^4 = \overline{16} = \overline{1}$$

Ответ: $\mathrm{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_4$.

Автоморфизм произвольных групп

Есть класс автоморфизмов, которые заведомо существуют для любой группы.

Внутренние автоморфизмы. Произвольному элементу $g \in G$ можно сопоставить автоморфизм φ_g такой, что

$$\varphi_g(x) = g \cdot x \cdot g^{-1}.$$

Это автоморфизм: сопряжение к произведению - это произведение сопряженных сомножителей (проверялось на лекциях), обратный элемент: $(\varphi_g)^{-1} = \varphi_{g^{-1}}$.

Получаем отображение

$$\varphi : G \to \mathrm{Aut}(G),$$
$$\varphi : g \to \varphi_g.$$

Отображение φ - это гомоморфизм групп G и $\mathrm{Aut}(G)$.

Действительно, если мы сопрягаем с произведением двух элементов, это равносильно сопряжению сначала с одним, а потом с другим. А сопряжение с произведением двух элементов - это композиция композиция сопряжений с сомножителями. Т.е. при таком отображении произведение переходит в композицию сопрягающих сомножителей.

Как выглядит ядро этого отображения? В него войдут такие элементы $g \in G$, что всегда $\varphi_g(x) = x$. Это центральные элементы G.

$$\mathrm{Ker}\,\varphi = Z(G)$$

$$\mathrm{Im}\,\varphi =: \mathrm{Inn}(G),$$

$\mathrm{Inn}(G)$ - группа внутренних автоморфизмов, подгруппа в $\mathrm{Aut}(G)$. По основной теореме о гомоморфизмах

$$\mathrm{Inn}(G) \simeq G/Z(G)$$

Утверждение 4.6. $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$

Доказательство. Здесь удобно применить следующее эквивалентное определение нормальности: подгруппа нормальна, если вместе с каждым элементом она содержит все его сопряженные.
Проверим, что $\forall \varphi_g \in \mathrm{Inn}(G)$ и $\forall \psi \in \mathrm{Aut}(G)$ $\psi \cdot \varphi_g \cdot \psi^{-1} \in Inn(G)$.

$$(\psi \cdot \varphi_g \cdot \psi^{-1})(x) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)\psi(\psi^{-1}(x))\psi(g^{-1}) = \psi(g)x\psi(g)^{-1}$$

Получили сопряжение с $\psi(g)$.

$$\psi \cdot \varphi_g \cdot \psi^{-1} = \varphi_{\psi(g)}$$

□

Обозначение:

$$\mathrm{Aut}(G)/\,\mathrm{Inn}(G) =: \mathrm{Out}(G),$$

$\mathrm{Out}(G)$ - группа "внешних автоморфизмов" .
В определении стоят кавычки, потому что $\mathrm{Out}(G)$ состоит не из автоморфизмов, а

из смежных классов всех автоморфизмов по внутренним.

Например, у абелевой группы все автоморфизмы, кроме тождественного, являются внешними, потому что сопряжение в абелевой группе тривиально.

В неабелевой группе внутренние автоморфизмы существуют, а наличие внешних автоморфизмов требует исследования.

Домашнее задание: 58.31 а),д),е), 58.32 а),г),д), 57.39, 57.41, 57.42, 57.40, 58.42. Дополнительные задачи: 57.43, 57.44.

Лекция 5

Разбор домашних задач

Задача 58.42 Доказать, что группа всех автоморфизмов некоммутативной группы не может быть циклической.

Доказательство. На лекциях было доказано, что если G не коммутативна, то факторгруппа $G/Z(G)$ не может быть циклической. С другой стороны, $G/Z(G) \simeq \mathrm{Inn}(G)$, т.е. $\mathrm{Inn}(G)$ не циклическая.
$\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$, откуда $\mathrm{Aut}(G)$ не может быть циклической, т.к. любая подгруппа циклической группы тоже циклическая. □

Задача 57.40 Доказать, что:
а) $\mathrm{Aut}(S_3) \simeq S_3$, причем все автоморфизмы группы S_3 внутренние;
б) $\mathrm{Aut}(V_4) \simeq S_3$, причем внутренним для V_4 является лишь тождественный автоморфизм.

Доказательство. **а)** На самом деле, нужно доказать, что $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$. При этом известно, что $\mathrm{Inn}(S_3) \simeq S_3/Z(S_3)$.
Ранее было показано, что $Z(S_3) = \{e\}$, тогда $S_3/Z(S_3) \simeq S_3$ и все, что остается доказать - что все автоморфизмы внутренние.

Пусть есть автоморфизм $\varphi \in \mathrm{Aut}(S_3)$. Чтобы показать, что он внутренний, нужно подобрать подстановку $\pi \in S_3 : \ \varphi(\sigma) = \pi\sigma\pi^{-1}$.
Рассмотрим образ транспозиции. Транспозиция - это элемент порядка 2, и других элементов порядка 2 в группе S_3 нет. Образ элемента порядка 2 должен быть снова элементом порядка 2, т.е. транспозицией.

$$\varphi(i,\ j) = (i',\ j')$$

б) Группа V_4 абелева, а у абелевой группы внутренние автоморфизмы бывают только тождественные.

$$\mathrm{Inn}(V_4) = \{\mathrm{id}\}$$

Как устроена группа всех автоморфизмов?

$$\mathrm{Aut}(V_4) \simeq S_3$$

Действительно, в группе V_4 есть единичный элемент и 3 неединичных, следовательно, чтобы задать автоморфизм, нужно указать перестановку, перемешивающую неединичные элементы между собой. Единичный элемент при этом должен переходить в единичный.
Заметим, что перестановку можно взять какую угодно, потому что групповой закон в группе V_4 устроен так, что все правила умножения симметричны относительно перестановки букв. □

Далее рассмотрим еще одну важную конструкцию в теории групп, которая позволяет строить новые группы из уже имеющихся. Две такие конструкции уже были рассмотрены на предыдущих семинарах: это факторгруппа по нормальной подгруппе и группа автоморфизмов.

Внутреннее и внешнее прямое произведение групп

Для удобства мы будем говорить о случае двух сомножителей, хотя конструкцию можно по индукции обобщить и на несколько сомножителей.

Определение 5.15. *Внутреннее прямое произведение групп.*
Группа G является прямым произведением своих подгрупп A и B, обозн.: $G = A \times B$, если выполнено:

1) $A, B \triangleleft G$,
2) $A \cap B = \{e\}$,
3) $G = A \cdot B$ *(каждый элемент из G представляется в виде произведения элементов из A и B).*

Свойства:

1) $\forall a \in A,\ b \in B,\ ab = ba$.

Доказательство.
$$ab = ba \ \Leftrightarrow\ aba^{-1}b^{-1} = e$$
Выражение $[a, b] = aba^{-1}b^{-1}$ называется коммутатором элементов a и b. Основное свойство коммутатора как раз записано выше: коммутатор двух элементов равен единице тогда и только тогда, когда эти элементы коммутируют.

Заметим теперь, что в $[a, b]$ можно по-разному группировать множители:
1. В случае $[a, b] = a(ba^{-1}b^{-1})$ и первый, и второй множители лежат в A, потому что $A \triangleleft G$,
2. В случае $[a, b] = (aba^{-1})b^{-1}$ оба множителя лежат в B.

Таким образом, $[a, b] \in A \cap B$, но по условию $A \cap B = \{e\}$, откуда $aba^{-1}b^{-1} = e$. □

2) $\forall g \in G\ \exists!\ a \in A, b \in B : g = ab$.

Доказательство. Пусть $g = a \cdot b = a' \cdot b'$. Домножим это равенство на $(a')^{-1}$ слева и на $(b')^{-1}$ справа, получим
$$(a')^{-1}a \cdot b(b')^{-1} = (a')^{-1}a' \cdot b'(b')^{-1} \ \Leftrightarrow\ (a')^{-1}a \cdot b(b')^{-1} = e \ \Leftrightarrow\ (a')^{-1}a = b'b^{-1}.$$
Отсюда $(a')^{-1}a = b'b^{-1} \in A \cap B = \{e\}$.
$$(a')^{-1}a = e, b'b^{-1} = e \ \Rightarrow\ a' = a, b' = b$$
□

Таким образом, каждый элемент группы G задается парой элементов из групп A и B, и наоборот.

3) Пусть $g = ab, g' = a'b'$, тогда

$$gg' = aba'b' = aa'bb' = (aa')(bb').$$

Это показывает, что структура группы G полностью задается структурой подгрупп A и B

Эти наблюдения позволяют ввести следующую конструкцию.

Определение 5.16. *Внешнее прямое произведение групп.*
Группа G является прямым произведением групп A и B, обозн.: $G = A \times B$, если

$$G = \{(a, b) \mid a \in A, b \in B\}$$

с операцией

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b').$$

Понятно, что это определение подсказано свойством 3) внутреннего произведения.

Почему для этой операции выполнены аксиомы группы?
Ассоциативность: на каждой компоненте в паре происходит умножение внутри соответствующей группы, а в этих группах умножение по определению ассоциативно.
Нейтральный элемент: (e, e).
Обратный элемент: $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Таким образом, мы ввели групповую структуру на декартовом произведении, и она уже не зависит ни от какой большей группы, которая содержит A и B.

Утверждение 5.7. *Внутреннее и внешнее прямое произведение эквивалентны.*

Доказательство. ($\Rightarrow$) Каждое внутреннее прямое произведение изоморфно внешнему прямому произведению. Как раз это мы доказывали в свойствах внутреннего прямого произведения. Свойство 2) показывает взаимно-однозначное соответствие между элементами большой группы и парами элементов из ее подгрупп. Свойство 3) показывает согласованность умножения.

($\Leftarrow$) Внешнее прямое произведение можно рассматривать как внутреннее. А именно, пусть есть внешнее прямое произведение двух групп $A \times B$. Можно ли группу $A \times B$ разложить во внутреннее прямое произведение двух каких-то подгрупп?

Можно взять подгруппы $A \times e$ и $e \times B$, тогда

$$A \times B = (A \times e) \times (e \times B).$$

Эти две подгруппы пересекаются только по единичому элементу (e, e).
Они обе нормальны, поскольку и умножение, и сопряжение происходят покомпонентно. При этом, сопрягая по второй компоненте (в группе $A \times e$), мы ничего, кроме e, не получим. Наконец,

$$\forall (a, b) = (a, e) \cdot (e, b)$$

$\square$

По сути, внешнее и внутреннее прямое произведение - это два разных способа посмотреть на один и тот же объект - группу $G = A \times B$.

Применение этой конструкции состоит в следующем: если мы смогли разложить группу $G = A \times B$ в прямое произведение ее подгрупп, то изучение группа G полностью сводится к изучению групп A и B.

Замечание по терминологии: используем мультипликативную терминологию, но в группах, где операция называется сложением, терминология меняется на аддитивную. В таком случае говорят про прямую сумму $G = A \oplus B$.
Аддитивную терминологию применяем только если группа абелева. В этом случае условие нормальности подгрупп оказывается лишним, потому что выполняется автоматически.

Определение 5.17. *Тривиальные разложения.*
Любую группу G можно представить в виде $G = G \times \{e\}$.

Решение задач о возможности разложения группы в прямое произведение (сумму) подгрупп

Задача. Можно ли данную группу разложить нетривиальным способом в прямое произведение или прямую сумму?

Задача 1. $G = \mathbb{Z}$
Решение. Операция в группе - сложение, т.е. ищем разложение в прямую сумму $\mathbb{Z} = A \oplus B$.

Всякая подгруппа в циклической группе свляется циклической, т.е. если A, B - подгруппы, то они порождаются одним элементом, например, $A = k\mathbb{Z}, B = l\mathbb{Z}$. Тогда

$$A \cap B \ni k \cdot l \neq e.$$

Значит, $\mathbb{Z}$ в прямую сумму не разлагается.

Ответ: нет.

Задача 2. $G = \mathbb{Q}$

Решение. Ищем разложение в прямую сумму $\mathbb{Q} = A \oplus B$.
Попробуем, как и ранее, предъявить ненулевой элемент, лежащий в пересечении двух любых подгрупп. Предположим,

$$A \ni a = \frac{k}{l} \neq 0,\ B \ni b = \frac{m}{n} \neq 0,$$

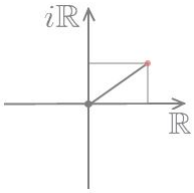
тогда $k \cdot m \in A \cap B$, т.к.

$$km = \underbrace{a + \ldots + a}_{lm} = \underbrace{b + \ldots + b}_{kn}.$$

Здесь необходимо уточнение: вообще говоря, числа k, l, m, n могут быть отрицательными, но тогда есть и обратные им положительные, поскольку $\mathbb{Q}$ - аддитивная группа.

Ответ: нет.

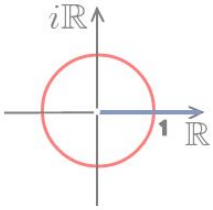
Задача 3. $G = \mathbb{C}$
Решение. Применим алгебраическую форму записи комплексоно числа. Геометрическая интерпретация наглядно демонстрирует выполнение всех аксиом прямого произведения.



Известно, что $\mathbb{R}, i\mathbb{R}$ - подгруппы, пересекаются они только по 0 и каждое комплексное число единственным образом представляется в виде суммы действительной и мнимой части.

Ответ: $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$

Задача 4. $G = \mathbb{C}^{\times}$
Решение. Пусть $A = \mathbf{U}$ - единичная окружность, $B = \mathbb{R}^{+}$ - луч.



Тогда $G = A \times B$.
Ясно, что A, B нормальны, пересекаются они по единичному элементу. Представление любого комплексного числа в виде произведения элементов этих двух подгрупп следует из тригонометрической формы записи комплексного числа

$$z = r(\cos\varphi + i\sin\varphi).$$

Ответ: $\mathbb{C}^\times = \mathbb{R}^+ \oplus \mathbf{U}$

Задача 5. $G = S_3$
Решение. Есть единственная нетривиальная нормальная подгруппа $A_3 \lhd S_3$. Для разложения в прямое произведение нужно как минимум 2 различных нетривиальных нормальных подгруппы.

Ответ: нет.

Задача 6. $G = \mathbb{Z}_m \simeq \mathbb{Z}_k \oplus \mathbb{Z}_l,\ m = k \cdot l$, НОД$(k, l) = 1$.

Доказательство. Есть 2 способа доказательства.
1. Можно работать с внутренней прямой суммой, т.е. искать в группе $\mathbb{Z}_m$ две подгруппы, которые изоморфны $\mathbb{Z}_k$ и $\mathbb{Z}_l$ и которые образуют прямую сумму.
2. Можно использовать внешнюю прямую сумму, т.е. рассметривать внешнюю прямую сумму $\mathbb{Z}_k$ и $\mathbb{Z}_l$ и доказывать, что эта прямая сумма изоморфна $\mathbb{Z}_m$.

Для наглядности докажем утверждение обоими способами.

1) Предъявим подгруппы $A, B \in \mathbb{Z}_m$ такие, что $A \simeq \mathbb{Z}_k$ и $B \simeq \mathbb{Z}_l$.

   Положим $A = \langle \bar{l} \rangle$ - циклическая группа, положденная вычетом $\bar{l}$ по модулю m.

$$A = \langle \bar{l} \rangle = \{\overline{0}, \bar{l}, \overline{2l}, \overline{3l}, \ldots\}$$
$$B = \langle \bar{k} \rangle = \{\overline{0}, \bar{k}, \overline{2k}, \overline{3k}, \ldots\}$$

   Заметим, что $A \simeq \mathbb{Z}_k, |A| = k$, т.к. вычет числа l по модулю m имеет порядок k (k раз его нужно сложить с самим собой, чтобы получить $\overline{0}$ по модулю m). Аналогично, $B \simeq \mathbb{Z}_l, |B| = l$.

   Проверим, что эти подгруппы в прямой сумме образуют группу $\mathbb{Z}_m$.

   - Эти подгруппы нормальны в силу коммутативности $\mathbb{Z}_m$.
   - $A \cap B = \{\overline{0}\}$, т.к. в A лежат вычеты чисел, кратных l, а в B лежат вычеты чисел, кратных k, при этом НОД$(k, l) = 1$.
   - Любой вычет из $\mathbb{Z}_m$ представляется в виде суммы вычетов из группы A и из группы B. Действительно, из условия НОД$(k, l) = 1$ мы уже знаем, что A и B образуют прямую сумму, вопрос только в ее размере. Также известно, что внутренняя прямая сумма изоморфна внешнеф прямой сумме, а

внешняя прямая сумма определяется как декартово произведение. Порядок такого произведения равен произведению порядков сомножителей, а это есть $k \cdot l = m = |\mathbb{Z}_m|$.

Заметим, можно было показать и прямо, что каждый вычет по модулю m является суммой вычета, кратного k, и вычета, кратного l. Это факт теории чисел, который следует из алгоритма Евклида. Действительно, НОД$(k, l) = 1 = p \cdot k + q \cdot l$.
$\overline{1} = \overline{p \cdot k} + \overline{q \cdot l}$, где первое слагаемое из A, а второе из B. А если вычет $\overline{1}$ можно представить таким образом, то и вычет любого числа тоже, потому что $\overline{1}$ порождает группу $\mathbb{Z}_m$.

Отсюда следует, что $\mathbb{Z}_m = A \oplus B$.

2) Надо доказать, что внешняя прямая сумма $\mathbb{Z}_k \oplus \mathbb{Z}_l$ изоморфна $\mathbb{Z}_m$. Т.е. нужно показать, что $\mathbb{Z}_k \oplus \mathbb{Z}_l$ - циклическая группа.
Группа будет иметь порядок m, т.к. порядок прямой суммы равен произведению порядков слагаемых.

Укажем порождающую пару:

$$\mathbb{Z}_k \oplus \mathbb{Z}_l = \langle (1 mod k, 1 mod l) \rangle$$

Чтобы доказать, что в группе порядка m некоторый элемент является порождающим, нужно показать, что порядок этого элемента равен m. Потому что тогда циклическая группа, и порожденная, имеет порядок m и совпадает со всей группой.
Найдем $o(\overline{1}, \overline{1})$. Если сложить элемент $(\overline{1}, \overline{1})$ с собой n раз, получим пару $n(\overline{1}, \overline{1}) = (\overline{n}, \overline{n})$. Далее, $(\overline{n}, \overline{n}) \Leftrightarrow n$ делится на k и n делится на l. Наименьшее такое n равно m, и это по определению есть порядок элемента.

$\square$

Пусть $m = p_1^{k_1} \dots p_s^{k_s}$ - разложение на простые (попарно различные) числа. Пользуясь задачей 6, получаем разложение группы $\mathbb{Z}_m$

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

Конечная группа, порядок которой равен степени простого числа, называется *примарной*.

Задача 6. $G = \mathbb{Z}_{p^k}$, p - простое число.
Решение. Покажем, что $\mathbb{Z}_{p^k}$ нельзя разложить в прямую сумму двух подгрупп $A \oplus B$.
Поскольку порядок прямой суммы есть произведение порядков слагаемых, порядки групп A и B должны быть степенями числа p. Пусть $A \simeq \mathbb{Z}_{p^r}$, $B \simeq \mathbb{Z}_{p^s}$.

Без ограничения общности, $r \geq s$. Пусть $(a, b) \in A \oplus B$, тогда $n(a, b) = (na, nb)$. Сколько раз достаточно сложить любую пару с собой, чтобы получить $(\overline{0}, \overline{0})$? Ответ - p^r раз.

При этом в группе $\mathbb{Z}_{p^k}$ существует элемент порядка $p^k > p^r$. Значит, при любых r, s группы $\mathbb{Z}_{p^k}$ и $\mathbb{Z}_{p^r} \oplus \mathbb{Z}_{p^s}$ не изоморфны.

Ответ: нельзя разложить.

Полупряморе произведение

Возьмем конструкцию внутреннего прямого произведения, условия 2) и 3) оставим без изменения, а условие 1) немного ослабим.

Определение 5.18. *Внутреннее полупрямое произведение групп.*
Группа G является полупрямым произведением своих подгрупп A и B, обозн.: $G = A \rtimes B$, если выполнено:

1) $A \triangleleft G, B \subset G$ *- просто подгруппа,*
2) $A \cap B = \{e\}$,
3) $G = A \cdot B$ *(каждый элемент из G представляется в виде произведения элементов из A и B).*

Проанализируем **свойства** по аналогии с внутренним произведением:

1) По-прежнему, каждый элемент из группы G единственным образом разлагается в произведение элементов из A и из B.

   Доказательство аналогично случаю внутреннего произведения. Мы пользовались тем, что пересечение групп A и B нулевое и только этим свойством.

2) A и B между собой не коммутируют.

   Ранее для доказательства этого свойства мы пользовались нормальностью подгрупп A и B, что в новой констуркции уже не выполнено.

3) Пусть $g = a \cdot b,\ g' = a' \cdot b'$, тогда

$$g \cdot g' = a \cdot b \cdot a' \cdot b' = a \cdot (b \cdot a' \cdot b^{-1}) \cdot b \cdot b'$$

   В силу того, что $A \triangleleft G$, множитель $a \cdot (b \cdot a' \cdot b^{-1}) = a \cdot \varphi_b(a')$ лежит в A. Множитель $b \cdot b'$ лежит в B.
   Значит, мы получили разложение произведения элементов из G в произведение элементов из A и B, но по новому правилу.

КАждому элементу b мы сопоставляем автоморфизм φ_b группы A. Получается отображение

$$\varphi : B \to \mathrm{Aut}(A), \quad b \mapsto \varphi_b : A \to A.$$

Ясно, что φ - гомоморфизм групп.
Этот гомоморфизм полностью задает операцию перемножения разложений. В отличие от прямого произведения, чтобы уметь умножать элементы из группы G, нужно не только уметь умножать элементы в A и B, но и знать гомоморфизм φ.

Определение 5.19. *Внешнее полупрямое произведение групп.*
Группа G является полупрямым произведением групп A и B с гомоморфизмом $\varphi : B \to \mathrm{Aut}(A)$, обозн.: $G = A \leftthreetimes B$, если

$$G = \{(a, b) \mid a \in A, b \in B\}$$

с операцией

$$(a, b) \cdot (a', b') = (a \cdot \varphi_b(a'), b \cdot b').$$

Гораздо больше групп можно разложить в полупрямое произведение, чем в прямое. Для упрощения структуры группы и сведения ее изучения к более маленьким группам такая конструкция тоже полезна.

Примеры. Можно ли разложить данную группу в полупрямое произведение?

1) S_n

Ранее было показано, что группу S_3 в прямое прозведение разложить нельзя. Покажем, что в полупрямое произведение группу S_n разложить можно.

В качестве нормальной подгруппы возьмем A_n. В качетве второй подгруппы возьмем группу, порожденную транспозицией $\langle(1, 2)\rangle_2$.

Действительно, пересечение групп A_n, $\langle(1, 2)\rangle_2$ единичное, потому что в группе, порожденной транспозицией, только единичный элемент является четным. Каждая подстановка π из S_n представляется в виде произведения подстановки из A_n и подстановки из $\langle(1, 2)\rangle_2$. Если π четная, то $\pi = \pi \cdot e$. Если π нечетная, то при умножении на транспозицию она становится четной, а если еще раз умножить на эту транспозицию, получится снова π.

Ответ: $S_n = A_n \leftthreetimes \langle(1, 2)\rangle_2$

2) D_n

В качестве нормальной подгруппы возьмем группу поворотов R_n, а в качестве дополнительной группы - группу, порожденную какой-нибудь одной симметрией $\langle s\rangle_2$.

Группа R_n нормальна, потому что при сопряжении поворот переходит либо в себя, либо в обратный поворот.
Ясно, что пересекаются эти подгруппы только по единице.
Каждый элемент из D_n представляется в виде произведения элементов из R_n и $\langle s\rangle_2$, т.к. если эти подгруппы пересекаются по единице, то они образуют полупрямое произведение и остается только проверить равенство мощностей. $2n = |D_n| = |R_n| \cdot |\langle s\rangle_2| = n \cdot 2$.

С другой стороны, $R_n \simeq \mathbb{Z}_n$ и $\langle s\rangle_2 \simeq \mathbb{Z}_2$, тогда D_n представима в виде внешнего полупрямого произведение $\mathbb{Z}_n \leftthreetimes \mathbb{Z}_2$.
Это полупрямое произведение задается гомоморфизмом $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^\times$.

Домашнее задание: определить, как устроен гомоморфизм φ.

Ответ: $D_n = R_n \leftthreetimes \langle s\rangle_2 \simeq \mathbb{Z}_n \leftthreetimes \mathbb{Z}_2$

Домашнее задание:

Упражнение 5.6. *В задаче 60.2 определить, какие группы можно разложить в полупрямое произведение.*

Задача. Разложить в полупрямое произведение группы 1) $GL_n(K)$, 2) группу невырожденных верхнетреугольных матриц порядка n.

Из задачника: 60.2 б),в),г), 60.7, 60.8, 60.5.

Лекция 6

Решение задачи 60.7

Задача 60.7 Доказать, что при $n \geq 3$ мультипликативная группа кольца вычетов $\mathbb{Z}_{2^n}^{\times}$ является произведением подгруппы $\{\pm 1\}$ и циклической группы порядка 2^{n-2}.

Решение. Какие вычеты обратимы по модулю 2^n? Это вычеты нечетных чисел (взаимно простых с модулем, по которому берутся вычеты). Отсюда $|\mathbb{Z}_{2^n}^{\times}| = 2^{n-1}$. Хотим показать, что

$$\mathbb{Z}_{2^n}^{\times} = \{\pm\overline{1}\} \times \langle\overline{3}\rangle_{2^{n-2}}.$$

$2^{n-1} = 2 \cdot 2^{n-2}$, т.е. нужно показать, что эти две подгруппы действительно образуют прямое произведение (2) и что эти группы именно такого порядка (1), тогда их прямое произведение автоматически исчерпает группу $\mathbb{Z}_{2^n}^{\times}$.

1) Ясно, что $\{\pm\overline{1}\}$ - группа порядка 2.

   Чтобы определить порядок циклической группы $\langle\overline{3}\rangle$, нужно посчитать порядок порождающего элемента $o(\overline{3})$. Порядок элемента $\overline{3}$ делит порядок группы $|\mathbb{Z}_{2^n}^{\times}| = 2^{n-1}$, откуда $o(\overline{3}) = 2^k$.
   Определим, для какого наименьшего k $\overline{3}^k = \overline{1}$. На языке целых чисел это означает

   $$3^{2^k} \equiv 1 \pmod{2}^n \Leftrightarrow 3^{2^k} - 1 \,\vdots\, 2^n.$$

   На какую степень двойки может делиться число $3^{2^k} - 1$? Разложим это число на множители

   $$3^{2^k} - 1 = (3^{2^{k-1}} + 1)(3^{2^{k-1}} - 1) = (3^{2^{k-1}} + 1)(3^{2^{k-2}} + 1)(3^{2^{k-2}} - 1) = \ldots =$$
   $$= (3^{2^{k-1}} + 1)(3^{2^{k-2}} + 1)\ldots(3^2 + 1)(3 + 1)(3 - 1).$$

   Выпишем, какую максимальную степень двойки можно вынести из каждого сомножителя. Для любого $l \in \mathbb{N}$ число $3^{2^l} + 1$ делится на 2, но не делится на 4. Действительно,

   $$3^{2^l} + 1 \equiv (-1)^{2^l} + 1 \pmod{4}, \;\; (-1)^{2^l} + 1 = 2, \; l > 0.$$

   Тогда

   $$\underbrace{(3^{2^{k-1}} + 1)}_{2^1}\underbrace{(3^{2^{k-2}} + 1)}_{2^1}\ldots\underbrace{(3^2 + 1)}_{2^1}\underbrace{(3 + 1)}_{2^2}\underbrace{(3 - 1)}_{2^1}.$$

   Всего в таком произведении $k + 1$ сомножителей, значит, максимальная степень двойки, на которую делится число $3^{2^k} - 1$ равна 2^{k+2}.

   Подберем такое наименьшее k, что $2^{k+2} \,\vdots\, 2^n$:

   $$k = n - 2 \Rightarrow o(\overline{3}) = 2^{n-2}.$$

2) Осталось проверить, что подгруппы $\{\pm\overline{1}\}$ и $\langle\overline{3}\rangle$ образуют прямое произведение.

- $\{\pm\overline{1}\}, \langle\overline{3}\rangle \triangleleft \mathbb{Z}_{2^n}^{\times}$, потому что группа $\mathbb{Z}_{2^n}^{\times}$ абелева.
- $\{\pm\overline{1}\} \cap \langle\overline{3}\rangle = \{\overline{1}\}$.
  Теоретически элемент $-\overline{1}$ мог бы оказаться в группе $\langle\overline{3}\rangle$, т.е.
  $$-\overline{1} = \overline{3}^N. \tag{6.1}$$
  $-\overline{1}$ - это элемент порядка 2, а в группе $\langle\overline{3}\rangle$ есть единственный элемент порядка 2 - это $\overline{3}^{2^{n-2}/2} = \overline{3}^{2^{n-3}}$. Отсюда $N = 2^{n-3}$.
  Перепишем равенство (6.1) в виде
  $$\overline{3}^{2^{n-3}} + 1 \,\vdots\, 2^n,\ n \geq 3. \tag{6.2}$$
  Если $n = 3$, то (6.2) примет вид $4 \,\vdots\, 8$, что не верно.
  Если $n > 3$, то $\overline{3}^{2^{n-3}} + 1$ делится на 2, но не делится на 4, при этом в правой части (6.2) стоит $2^n > 2^3$.

  Таким образом, $-\overline{1} \notin \langle\overline{3}\rangle$ и второе условие прямого произведения выполнено.
- То, что произведения элементов из $\{\pm\overline{1}\}$ и $\langle\overline{3}\rangle$ порождают всю группу $\mathbb{Z}_{2^n}^{\times}$ мы уже пояснили, когда установили совпадение мощностей.

Утверждение задачи доказано.

Разложение группы Диэдра в полупрямое произведение

На прошлом семинаре было показано, что

$$D_n = R_n \leftthreetimes \langle s\rangle_2,$$

где R_n - группа поворотов, а $\langle s\rangle_2$ - группа, порожденная какой-то симметрией. Как абстрактные группы, $R_n \simeq \mathbb{Z}_n$, $\langle s\rangle_2 \simeq \mathbb{Z}_2$, тогда

$$D_n = R_n \leftthreetimes \langle s\rangle_2 \simeq \mathbb{Z}_n \leftthreetimes_{\varphi} \mathbb{Z}_2.$$

Полупрямое произведение $\mathbb{Z}_n \leftthreetimes_{\varphi} \mathbb{Z}_2$ задается гомоморфизмом

$$\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^{\times}.$$

Покажем, как устроен гомоморфизм φ для $R_n \leftthreetimes \langle s\rangle_2$.
Если рассматривать $\mathbb{Z}_2$ как группу вычетов по модулю 2, то она содержит нейтральный элемент $\overline{0}$ и порождающий элемент $\overline{1}$.

$$\varphi_{\overline{0}} = \mathrm{id}\ (= \overline{1} \in \mathbb{Z}_n^{\times})$$

Как выглядит $\varphi_{\overline{0}}$? Абстрактное внешнее полупрямое произведение $\mathbb{Z}_n \leftthreetimes_\varphi \mathbb{Z}_2$ соответствует внутреннему полупрямому произведению $R_n \leftthreetimes \langle s\rangle_2$. Гомоморфизм φ соответствует гомоморфизму из $\langle s\rangle_2$ в группу $\mathrm{Aut}(R_n)$ такому, что

$$\varphi_s(r) = srs^{-1} = r^{-1},\ r \in R_n.$$

Переходя к абстрактному полупрямому произведению, используем аддитивную форму записи

$$\varphi_{\overline{1}}(\overline{k}) = -\overline{k},\ \ -\overline{k} \in \mathbb{Z}_n^\times.$$
$$\varphi_{\overline{1}} = -\overline{1} \in \mathbb{Z}_n^\times$$

Разложение обратимых матриц над полем K

Задача. Разложить группу $GL_n(K)$ в полупрямое произведение.

Решение. Покажем, что

$$GL_n(K) = SL_n(K) \leftthreetimes H,$$

где

$$H = \{\begin{pmatrix} \lambda & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},\ \lambda \in K^\times\}.$$

$SL_n(K) \ \triangleleft\ GL_n(K)$, т.к. это ядро гомоморфизма det. При этом H нормальной не будет.

Осталось проверить 2 свойства полупрямого произведения.

- $SL_n(K) \cap H = \{E\}$, потому что определитель матрицы $A \in H$ равен λ, и если $A \in SL_n(K)$, то $\lambda = 1$.
- Любую матрицу из $GL_n(K)$ можно представить в виде произведения матриц из $SL_n(K)$ и H.
  Пусть $A \in GL_n(K)$, покажем, что $A = BC,\ B \in SL_n(K), C \in H$. Можно взять

  $$C = \begin{pmatrix} \det A & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},$$

  тогда $\det B = 1$, т.к. $\det A = \det B \cdot \det C = \det B \cdot \det A$. Отсюда

  $$B = AC^{-1}.$$

  При умножении матрицы A справа на диагональную матрицу C^{-1} первый столбец матрицы A делится на $\det A$.

Конечнопорожденные абелевы группы. Свободные абелевы группы

Определение 6.20. *Группа G порождена некоторым множеством своих элементов*

$$G = \langle g_i \mid i \in I \rangle,$$

если $\forall\, g \in G\, \exists\, i_1, \ldots, i_N \in I,\ \exists\, \varepsilon_1, \ldots, \varepsilon_N \in \{\pm 1\}$ *такие, что*

$$g = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_N}^{\varepsilon_N}.$$

Определение 6.21. *Группа G является конечнопорожденной, если множество I конечно.*

Случай конечнопорожденных абелевых групп

Определение 6.22. *Абелева группа G порождена конечным набором своих элементов*

$$G = \langle g_1, \ldots, g_n \rangle,$$

если $\forall\, g \in G\, \exists\, k_1, \ldots, k_n \in \mathbb{Z}$ *такие, что*

$$g = g_1^{k_1} \ldots g_n^{k_n}.$$

В аддитивной записи этого определения элемент g представляется в виде линейной комбинации

$$g = k_1 g_1 + \ldots + k_n g_n.$$

Можно заметить сходство с линейной алгеброй. Как будет показано далее, некоторые факты из теории векторных пространств практически дословно переносятся в теорию конечнопорожденных абелевых групп.

Примеры.

1) $\mathbb{Z}_m$ $(m \in \mathbb{N} \cup \{\infty\})$

   Если $m = \infty$, условно считаем, что имеем дело с группой $\mathbb{Z}$.
   Это конечнопорожденная группа

$$\mathbb{Z}_m = \langle 1 \pmod m \rangle\ (= \langle 1 \rangle,\ m = \infty)$$

2) $(\mathbb{R}, +)$

   Любая конечнопорожденная абелева группа не более чем счетна, потому что каждый элемент группы задается набором целых чисел - коэффициентами линейной комбинации. Причем разным наборам целых чисел может соответствовать один и тот же элемент, т.е. элементов группы может оказаться меньше, чем таких наборов.
   Известно, что наборов целых чисел заданной длины счетное множество.

   $(\mathbb{R}, +)$ не конечно порождена, т.к. она несчетна.

3) $(\mathbb{Q}, +)$

От противного: пусть $(\mathbb{Q}, +)$ конечно порождена: $\mathbb{Q} = \langle g_1, \ldots, g_n \rangle$. Т.е. любое рациональное число представляется в виде линейной комбинации чисел $g_1, \ldots, g_n$.

Обозначим
$$g_1 = \frac{a_1}{b_1},\ g_2 = \frac{a_2}{b_2},\ \ldots,\ g_2 = \frac{a_2}{b_2}$$
$$\forall g \in G,\ \ g = k_1 \frac{a_1}{b_1} + \ldots + k_n \frac{a_n}{b_n} = \frac{N}{b_1 \ldots b_n} \tag{6.3}$$
Однако не любое рациональное число может быть представлено в таком виде, т.к. знаменатель $b_1 \ldots b_n$ содержит лишь конечное число простых сомножителей. Тогда дробь $\frac{1}{p}$, где p - простое, не входит в данный набор простых множителей, не представима в виде (6.3). Противоречие.

$(\mathbb{Q}, +)$ не конечнопорожденная.

4) $(\mathbb{Q}^\times, \cdot)$

Рассуждаем аналогично примеру 3). Если бы $(\mathbb{Q}^\times, \cdot)$ была конечно порождена, то
$$\forall g \in G,\ \ g = g_1^{k_1} \ldots g_n^{k_n} = \frac{a_1^{k_1}}{b_1^{k_1}} \ldots \frac{a_n^{k_n}}{b_n^{k_n}} = \frac{a}{b}$$
В числитель и знаменатель дроби $\frac{a}{b}$ входят только те множители, которые входили в числители и знаменатели дробей $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$. Таких простых множителей конечное число, а простых чисел бесконечно много.

$(\mathbb{Q}^\times, \cdot)$ не конечнопорожденная.

Определение 6.23. *Множество $\{g_1, \ldots, g_n\}$ является базисом абелевой группы G, если*

1) *G порождена этими элементами (любой $g \in G$ представляется в виде линейной комбинации $g_1, \ldots, g_n$);*

2) *система $\{g_1, \ldots, g_n\}$ линейно независима: никакая нетривиальная линейная комбинация этих элементов не равна нулю.*

Определение 6.24. *Абелева группа G называется свободной, если у нее существует базис.*

Примеры.

1) $\mathbb{Z}_m$ $(m \in \mathbb{N})$

Эта группа не свободна. Возьмем произвольное множество элементов $g_1, \ldots, g_n \in \mathbb{Z}_m$, тогда
$$mg_1 + \ldots + mg_n = 0 + \ldots + 0 = 0,$$
следовательно, условие линейной независимости нарушается.

2) $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n}$

Элементы этой группы представляют собой строки (или столбцы) целых чисел длины n с операцией покомпонентного сложения.
Группа $\mathbb{Z}^n$ свободна, т.к. можно предъявить стандартный базис - строки $e_1, \ldots, e_n$,

$$e_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0).$$

Линейная независимость этих строк, а также то, что с помощью их линейной комбинации можно получить любой элемент $\mathbb{Z}^n$, проверяется как в линейной алгебре.

Имеют место следующие факты:

- Во всех базисах свободной абелевой группы G одинаковое число элементов, которое называется *рангом* группы G.
  Обозначение: $n = \operatorname{rk} G$.

- Если G - свободная абелева группа ранга n, то $G \simeq \mathbb{Z}^n$.
  Построим этот изоморфизм. Пусть $g_1, \ldots, g_n$ - базис G, $e_1, \ldots, e_n$ - базис $\mathbb{Z}^{\ltimes}$, тогда

  $$g_i \leftrightarrow e_i.$$

  Далее изоморфизм можно продолжить по линейности:

  $$g = k_1 g_1 + \ldots + k_n g_n \leftrightarrow k_1 e_1 + \ldots + k_n e_n = (k_1, \ldots, k_n).$$

  Таким образом, свободная группа ранга n с точностью до изоморфизма одна.

Произвольные конечнопорожденные абелевы группы

Пусть $G = \langle g_1, \ldots, g_n \rangle$ - конечнопорожденная абелева группа. Рассмотрим свободную абелеву группу $F = \langle f_1, \ldots, f_n \rangle$ с базисом из того же числа элементов.

Построим соответствие между элементами групп F и G. А именно, гомоморфизм

$$\pi : F \to G,$$

$$f_i \mapsto g_i.$$

Соответствено, линеная комбинация переходит в линейную комбинацию с теми же коэффициентами.

Отождествим F с $\mathbb{Z}^n \simeq F$, получим

$$\pi : (k_1, \ldots, k_n) \mapsto k_1 g_1 + \ldots + k_n g_n.$$

π не изоморфизм, т.к. g разлагается в линейную комбинацию $g_1, \ldots, g_n$ не единственным образом, т.к. $\{g_1, \ldots, g_n\}$ - не базис.

$$H := \operatorname{Ker}\pi = \{(k_1, \ldots, k_n) \mid k_1 g_1 + \ldots + k_n g_n = 0\}$$

Если рассматривать H как подгруппу в $\mathbb{Z}^n$, то это будет группа линейных зависимостей между порождающими элементами группы G.

$$\operatorname{Im}\pi = G \simeq F/H$$

Подгруппа в свободной абелевой группе тоже свободна и, в частности, конечно порождена.
Таким образом, H конечно порождена, $H = \langle h_1, \ldots, h_m \rangle$,

$$h_j = k_{1j} f_1 + k_{2j} f_2 + \ldots + k_{nj} f_n.$$

Для каждого h_j получили столбец координат, составим из этих столбцов матрицу размера $n \times m$.

$$K = \begin{pmatrix} K_{11} & \ldots & K_{1j} & \ldots & K_{1m} \\ \vdots & & \vdots & & \vdots \\ K_{n1} & \ldots & K_{nj} & \ldots & K_{nm} \end{pmatrix}$$

Здесь по столбцам записаны координаты порождающих группы H в базисе группы F.

Любую целочисленную матрицу элементарными целочисленными преобразованиями строчек и столбцов можно привести к стандартному виду.
Целочисленные элеметарные преобразования строк:
1. прибавить к одной строке другую с целым коэффициентом;
2. переставить 2 строчки местами;
3. умножить строку на ± 1.

При элементарном целочисленном преобразовании строк матрицы K мы осуществляем замену базиса в группе F. Целочисленным элементарным преобразованиям столбцов соответствует замена системы порождающих группы H.

Поскольку все целочисленные элементарные преобразования обратимы, то существует и обратный переход от матрицы стандартного вида к матрице K. Таким образом, новый набор элементов тоже является системой порождающих, т.е. мы переходим от одной системы порождающих к другой.

Утверждение 6.8. *Любую целочисленную матрицу K целочисленными элементарными преобразованиями можно привести к виду*

$$K' = \begin{pmatrix} m_1 & & & & & 0 \\ & \ddots & & & & \\ & & m_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$$

Таким образом, мы перешли к новому базису $F = \langle f'_1, \ldots, f'_n \rangle$ и новой системе порождающих $H = \langle h'_1, \ldots, h'_m \rangle$.

$$h'_i = \begin{cases} m_i f'_i, & i \leq r \\ 0, & i > r \end{cases}$$

В новом базисе мы записали подгруппу H в стандартном виде: порождающие элементы H - это элементы, пропорциональные каким-то базисным элементам большой группы.

Для элемента $h \in F$

$$h = k_1 f'_1 + \ldots + k_n f'_n,$$

$$h \in H \;\Leftrightarrow\; \begin{cases} k_i = 0, & i > r \\ k_i \vdots m_i, & i \leq r \end{cases}$$

Определим теперь как выглядит смежный класс $g + H$ произвольного элемента $F \ni g = l_1 f'_1 + \ldots + l_n f'_n$ по подгруппе H.
При прибавлении к g элемента из H координаты l_i, $i > r$ не меняются, а при $i \leq r$ к l_i прибавляется любое число, кратное m_i. Таким образом при $i \leq r$, сама координата l_i меняется, но остается неизменным ее класс вычетов по модулю m_i.

Таким образом, было показано, что

Утверждение 6.9.

$$G = F/H \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z}^{n-r}$$

Любая конечнопорожденная абелева группа изоморфна прямой сумме некоторого количества конечных циклических групп и некоторого количества бесконечных циклических групп.

Алгоритм, описанный выше, позволяет явно найти это разложение, т.е. найти тип произвольной конечнопорожденной абелевой группы.

Решение задачи 60.52

Задача 60.52 б) F - свободная абелева группа ранга 3 с базисом f_1, f_2, f_3. H - подгруппа в F, $H = \langle h_1, h_2, h_3 \rangle$,

$$\begin{aligned} h_1 &= 4f_1 + 5f_2 + 3f_3, \\ h_2 &= 5f_1 + 6f_2 + 5f_3, \\ h_3 &= 8f_1 + 7f_2 + 9f_3. \end{aligned}$$

Требуется найти факторгруппу F/H в смысле утверждения 6.9.

Решение. Запишем матрицу координат h_1, h_2, h_3 в базисе f_1, f_2, f_3.

$$K = \begin{pmatrix} 4 & 5 & 8 \\ 5 & 6 & 7 \\ 3 & 5 & 9 \end{pmatrix} \overset{(1)}{\to} \begin{pmatrix} -1 & -1 & -2 \\ 5 & 6 & 7 \\ 3 & 5 & 9 \end{pmatrix} \overset{(2)}{\to} \begin{pmatrix} -1 & 0 & 0 \\ 5 & 1 & 12 \\ 3 & 2 & 12 \end{pmatrix} \overset{(3)}{\to}$$

$$\overset{(3)}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 12 \\ 0 & 2 & 12 \end{pmatrix} \overset{(4)}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 12 \\ 0 & 0 & -12 \end{pmatrix} \overset{(5)}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 12 \end{pmatrix} = K'$$

(1) - вычтем из первой строки вторую
(2) - вычтем из второго столбца первый, прибавим к третьему столбцу первый
(3) - прибавим первую строку ко второй и третьей с коэффициентами 5 и 3
(4) - из третьей строки вычтем вторую с коэффициентом 2
(5) - прибавим ко второй строке третью и умножим третью строку на -1

$\mathbb{Z}_1 = \{0\}$, поэтому $F/H = \{0\} \oplus \{0\} \oplus \mathbb{Z}_2 = \mathbb{Z}_2$.

Ответ: $F/H = \mathbb{Z}_2$

Домашнее задание.

Задача. Являются ли конечнопорожденными следующие группы:
1. $G = \{\frac{m}{n} \mid$ все простые множители n среди $p_1, \ldots, p_s -$ простые$\}$, операция - сложение;
2. $G = \{\frac{m}{n} \neq 0 \mid$ все простые множители m, n среди $p_1, \ldots, p_s -$ простые$\}$, операция - умножение.

Из задачника: 60.52 а), г), д).

Лекция 7

Решение задачи 60.48

Задача 60.48 Доказать, что конечнопорожденная подгруппа G мультипликативной группы комплексных чисел $\mathbb{C}^\times$ разлагается в прямое произведение свободной абелевой группы и конечной циклической.

Доказательство. $G = G_1 \times \ldots \times G_r \times G_{r+1} \times \ldots \times G_s$, где $G_1, \ldots, G_r$ - конечные циклические группы, а $G_{r+1}, \ldots, G_s$ - бесконечные циклические группы.
Обозначим

$$H := G_1 \times \ldots \times G_r, \quad F := G_{r+1} \times \ldots \times G_s$$

тогда $G = H \times F$ - прямое произведение двух подгрупп, одна из которых свободна (F), а вторая является конечной абелевой группой (H).

Остается доказать, что H - циклическая.
Пусть $|H| =: m$, тогда $\forall z \in H \ z^m = 1$. Отсюда $H \subseteq \mathbb{U}_m$ - группа корней степени m из 1. При этом $\mathbb{U}_m \simeq \mathbb{Z}_m$ - циклическая группа, а любая подгруппа циклической группы - циклическая. $\square$

Замечание. На самом деле, любая конечная подгруппа в мультипликативной группе поля комплексных чисел - это группа корней из 1 какой-то степени. Во вложении $H \subseteq \mathbb{U}_m$ должно стоять равенство, потому что m - это порядок группы H, а в группе корней степени m из 1 как раз m корней.

Решение задачи 60.52

Задача 60.52 A - свободная абелева группа с базисом x_1, x_2, x_3, B - ее подгруппа, порожденная y_1, y_2, y_3.

$$y_1 = 8x_1 + 4x_2 - 4x_3$$
$$y_2 = 3x_1 + 4x_2 + x_3$$
$$y_3 = 2x_1 - 4x_2 - 6x_3$$

Разложить в прямую сумму циклических групп факторгруппу A/B.
Кроме того, известно разложение элемента $x \in A$, $x = 5x_1 + 6x_2 + x_3$. В факторгруппе лежит смежный класс $x + B$ элемента x по подгруппе B. Найти порядок $o(x + B)$ как элемента факторгруппы.

Решение. Опишем алгоритм решения.

Составим матрицу, в столбцах которой будут координаты порождающих элементов подгруппы B в базисе группы A. Далее целочисленными элементарными преобразованиями приведем матрицу к диагональному виду, что будет означать переход к новому базису группы A.

$$\begin{pmatrix} 8 & 3 & 2 \\ 4 & 4 & -4 \\ -4 & 1 & -6 \end{pmatrix} \to \begin{pmatrix} m_1 & 0 & 0 \\ 0 & m_2 & 0 \\ 0 & 0 & m_3 \end{pmatrix}$$

Тогда

$$A/B \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \mathbb{Z}_{m_3}$$

Как теперь найти порядок смежного класса конкретного элемента?
Пусть смежный класс $x + B$ в факторгруппе A/B представлен вычетами

$$x + B = (\overline{k_1},\ \ \overline{k_2},\ \overline{k_3}).$$

Известно, как найти порядок элемента в прямой сумме (произведении). Вопрос в том, как найти тройку $(\overline{k_1},\ \ \overline{k_2},\ \overline{k_3})$.

В новом базисе элемент x можно записать как

$$x = k_1 x_1' + k_2 x_2' + k_3 x_3'.$$

Прибавляя к x элементы из подгруппы B, мы можем изменить координату k_i на число, кратное m_i. Таким образом, когда мы перейдем от элемента к его смежному классу, инвариантом смежного класса будет тройка вычетов $\overline{k_i}$ по модулю m_i.

Итак, задача состоит в том, чтобы найти координаты элемента x в новом базисе. Для этого к исходной матрице нужно приписать столбец координат элемента x и проследить за его преобразованиями.

Заметим, что над расширенной матрицей нельзя в полном объеме производить элементарные преобразования столбцов.
Столбец с координатами x нельзя прибавлять к предыдущим столбцам, т.к. тогда мы изменим подгруппу B. Первые 3 столбца к столбцу x прибавлять можно, т.к. в первых трех столбцах стоят элементы из подгруппы B, и мы попадаем в смежный класс $x + B$.

$$\left(\begin{array}{ccc|c} 8 & 3 & 2 & 5 \\ 4 & 4 & -4 & 6 \\ -4 & 1 & -6 & 1 \end{array}\right) \overset{(1)}{\to} \left(\begin{array}{ccc|c} 0 & 5 & -10 & 7 \\ 0 & 5 & -10 & 7 \\ -4 & 1 & -6 & 1 \end{array}\right) \overset{(2)}{\to} \left(\begin{array}{ccc|c} -4 & 1 & -6 & 1 \\ 0 & 5 & -10 & 7 \\ 0 & 0 & 0 & 0 \end{array}\right) \overset{(3)}{\to}$$

$$\overset{(3)}{\to} \left(\begin{array}{ccc|c} -4 & -4 & 4 & -6 \\ 0 & 5 & -10 & 7 \\ 0 & 0 & 0 & 0 \end{array}\right) \overset{(4)}{\to} \left(\begin{array}{ccc|c} -4 & 0 & 0 & 2 \\ 0 & 5 & -10 & 7 \\ 0 & 0 & 0 & 0 \end{array}\right) \overset{(4)}{\to} \left(\begin{array}{ccc|c} 4 & 0 & 0 & -2 \\ 0 & 5 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

(1) - прибавим ко второй строке третью, а к первой строке прибавим третью с коэффициентом 3
(2) - вычтем из первой строки вторую и поменяем местами первую и третью строки
(3) - вычтем из первой строки вторую
(4) - вычтем первый стоблец из второго и четвертого, прибавим первый столбец к третьему
(5) - прибавим второй столбец к третьему с коэффициентом 2 и вычтем второй столбец из четвертого, поменяем знак в первой строке

Разложение факторгруппы:

$$A/B \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}$$

При данном изоморфизме смежный класс $x+B$ соответствует следующему набору вычетов

$$x + B = (\overline{-2} \pmod 4,\ \overline{2} \pmod 5,\ 0)$$

$$o(x+B) = \text{НОК}(o(\overline{-2} \pmod 4),\ o(\overline{2} \pmod 5),\ o(0)) = \text{НОК}(2,\ 5,\ 1) = 10$$

Замечание. Если бы на месте числа 0 получилось число 1, то его порядок был бы равен ∞, как и порядок всего смежного класса.

Ответ: $A/B \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}$, $\ o(x+B) = 10$.

Решение задачи 60.51

Задача 60.51 A - свободная абелева группа с базисом $x_1, \ldots, x_n$. $A \supseteq B$ - подгруппа, порожденная n элементами $B = \langle y_1, \ldots, y_n \rangle$,

$$y_j = \sum_{i=1}^{n} k_{ij} x_i.$$

Другими словами, координаты y_j в базисе $x_1, \ldots, x_n$ записаны в j-том столбце матрицы

$$K = \begin{pmatrix} k_{11} & \ldots & k_{1n} \\ \vdots & & \vdots \\ k_{n1} & \ldots & k_{nn} \end{pmatrix}.$$

Доказать, что факторгруппа A/B конечна $\Leftrightarrow$ матрица K невырождена и $|A/B| = |\det K|$.

Доказательство. При вычислении A/B мы приводим матрицу K с помощью целочисленных элементарных преобразований к диагональному виду

$$K \longrightarrow K' = \begin{pmatrix} m_1 & & 0 \\ & \ddots & \\ 0 & & m_n \end{pmatrix}$$

Определитель при элементанрых преобразованиях может только поменять знак, т.к. целочисленное элементарное преобразование 1 типа не меняет определитель, а преобразования 2 и 3 типов меняют его знак. Можно сказать, что

$$\det K = \pm \det K' = \pm m_1 \cdot \ldots \cdot m_n.$$

С другой стороны, если мы привели матрицу K к виду K', то

$$A/B \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_n}, \tag{7.1}$$

где $\mathbb{Z}_0 = \mathbb{Z}$.

($\Rightarrow$) A/B конечна, следовательно, в разложении (7.1) нет бесконечных циклических слагаемых. Это значит, что на диагонали матрицы K' нет нулей, что в точности означает $\det K' = m_1 \dots m_n \neq 0$.

($\Leftarrow$) $|\mathbb{Z}_{m_i}| = m_i$, а порядок прямой суммы равен произведению порядков слагаемых

$$|A/B| = m_1 \dots m_n = |\det K|$$

$\square$

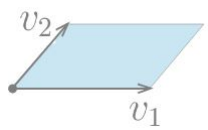
Вычисление объема целочисленного параллелепипеда

Рассмотрим линейно независимые векторы $v_1, \dots, v_n \in \mathbb{Z}^n \subset \mathbb{R}^n$ и n-мерный параллелепипед Π, натянутый на эти векторы с началом координат в нуле

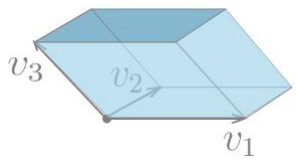
$$\Pi = \Pi(v_1, \dots, v_n) = \{v = t_1 v_1 + \dots + t_n v_n \mid 0 \leq t_1, \dots, t_n \leq 1\}.$$

- Если $n = 1$, то имеем единственный вектор v_1, и $\Pi(v_1)$ заполняет отрезок длины $|v_1|$ с началом координат в нуле.

- Если $n = 2$, то $\Pi(v_1, v_2)$ - параллелограмм.



- $n = 3$.



Обозачение: $\operatorname{vol}\Pi$ - объем Π.

Грань параллелепипеда задается выбором координат $1 \le i_1, \dots, i_k \le n$, которым придаются крайние значения и набором значений $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$, которые мы будем придавать этим координатам.

$$\Gamma = \Gamma_{i_1,\dots,i_k} = \{v \in \Pi \mid t_{i_1} = \varepsilon_1, t_{i_2} = \varepsilon_2, \dots, t_{i_k} = \varepsilon_k\}$$

Свободными остаются $n - k$ координат, соответственно, грань имеет размерность $\dim \Gamma = n - k$.
Например, в случае $n = 3$ выделенная грань задается следующим образом:

$$t_3 = 1, \quad \dim \Gamma = 2.$$

Формула для вычисления объема (задача - доказать ее)

$$\operatorname{vol}\Pi = \text{ число целых точек в } \Pi \text{ за вычетом граней, не содержащх } 0 \tag{7.2}$$

Так, например, чтобы посчитать площадь целочисленного параллелограмма ($n = 2$), нужно посчитать число целых точек параллелограмма, кроме точек, лежащих на сторонах, не содержащих v_1, v_2.

Чтобы доказать формулу (7.2), нужно использовать теорию конечнопорожденных абелевых групп и задачу 60.51.

Формулу (7.2) можно сделать симметричной. Суть в том, чтобы точки на разных гранях учитывать с разными весами. Задача - получить формулу (7.3) из (7.2).

$$\operatorname{vol}\Pi = \sum_{k=0}^{n} \frac{1}{2^k}(\text{ число целых точек внутри граней размерности } n-k) \tag{7.3}$$

Сам параллелепипед тоже является своей гранью размерности n, т.е. когда $k = 0$. Поскольку $k = 0$, точки внутри Π берем с весом 1. Число точек внутри граней размерности $n - 1$ считаем с коэффициентом $\frac{1}{2}$ и т.д.
Число вершин (нульмерных граней) равно 2^n, потому что нужно каждое из неравенств $0 \le t_1, \dots, t_n \le 1$ обратить в равенство. Их мы берем с весом $\frac{1}{2^n}$, т.е. все вершины дают вклад в сумму, равный 1.

Упражнение 7.7. *Из* (7.3) *для двумерного случая вывести формулу Пика для площади целочисленного многоугольника P на плоскости*

$$S(P) = (\textit{ число целых точек внутри } P) + \frac{1}{2}(\textit{ число целых точек на периметре } P) - 1.$$

Конечные абелевы группы

Пусть A - конечная абелева группа (по сложению).
Всякая конечная абелева группа тем более является конечнопорожденной. Значит,

к конечным абелевым группам можно применить общие результаты о конечнопорожденных абелевых группах.

Согласно общей теории,

$$A \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r},$$

причем в разложении могут присутствовать только конечные циклические группыю. В свою очередь каждую конечную циклическую группу можно разложить в прямую сумму примарных циклческих групп (групп, порядок которых равен степени простого числа).

$$A \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}},$$

$p_1, \ldots, p_s$ - простые числа (которые могут повторяться), $k_1, \ldots, k_s \in \mathbb{N}$.
Набор $(p_1^{k_1}, \ldots, p_s^{k_s})$ называется типом конечной абелевой группы A. Он определен однозначно.

Таким образом, можно все конечные абелевы группы классифицировать по их типам.

Отметим, что именно набор $(p_1^{k_1}, \ldots, p_s^{k_s})$ определен однозначно. Если разложить гурппу A в прямую сумму примарных циклических подгрупп

$$A = A_1 \oplus \ldots \oplus A_s, \quad A_i \simeq \mathbb{Z}_{p_i^{k_i}}$$

то таких разложений может быть много.

Пример. $A = V_4 = \{e, a, b, c\}$
Здесь временно прейдем в мультипликативную терминологию.

$$A = \langle a \rangle_2 \times \langle b \rangle_2$$

Корректность: $\langle a \rangle_2 = \{a, e\}, \langle b \rangle_2 = \{b, e\},\ c = a \cdot b.$

Другие разложения:

$$A = \langle a \rangle_2 \times \langle c \rangle_2$$

$$A = \langle b \rangle_2 \times \langle c \rangle_2$$

Имеем 3 разных изоморфных между собой разложения.

Решение задач 60.39 д),г), 60.40 б)

Задача 60.39 г) Перечислить с точностью до изоморфизма все конечные абелевы группы порядка 12.

Решение. $|A| = 12$. Разложим 12 на простые множители

$$12 = 2^2 \cdot 3.$$

$$A_1 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3$$
$$A_2 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Тип определен однозначно, эти 2 разложения не изоморфны друг другу. Убедимся в этом напрямую.

Элементы порядка 2 в группе A_1:

$$(\overline{2}, \overline{0})$$

Элементы порядка 2 в группе A_2:

$$(\overline{1}, \overline{1}, \overline{0}), \quad (\overline{0}, \overline{1}, \overline{0}), \quad (\overline{1}, \overline{0}, \overline{0})$$

Как видно, количества эелементов порядка 2 в группах A_1 и A_2 не совпадают.

Задача 60.39 д) Перечислить с точностью до изоморфизма все конечные абелевы группы порядка 16.

Решение. $|A| = 12$. Разложим 12 на простые множители

$$16 = 2^4.$$

$$A_1 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$A_2 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_8$$
$$A_3 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$$
$$A_4 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
$$A_5 \simeq \mathbb{Z}_{16}$$

Покажем, что среди этих групп нет двух изоморфных друг другу. Выпишем, какие бывают порядки у элементов этих групп. Возможные порядки вычисляются как НОК порядков элементов в группах из прямой суммы.

A_1	1, 2, 4
A_2	1, 2, 4, 8
A_3	1, 2
A_4	1, 2, 4
A_5	1, 2, 4, 8, 16

По этой таблице можно различить все группы, кроме A_1 и A_4.
Рассмотрим решения уравнения

$$2 \cdot x = 0. \tag{7.4}$$

Это будут элементы 2 порядка и нулевой элемент (порядка 1).

- Решения в группе A_1, $x = (x_1, x_2)$, $x_1, x_2 \in \mathbb{Z}_4$.

$$2(x_1, x_2) = (\overline{0}, \overline{0}) \Leftrightarrow \left[\begin{array}{l} 2x_1 = \overline{0} \\ 2x_2 = \overline{0} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x_1 = \overline{2}, \overline{0} \\ x_2 = \overline{2}, \overline{0} \end{array}\right.$$

  Таким образом, есть 4 решения уравнения (7.4).

- Решения в группе A_4, $x = (x_1, x_2, x_3)$, $x_1, x_3 \in \mathbb{Z}_2$, $x_2 \in \mathbb{Z}_4$.

$$2(x_1, x_2, x_3) = (\overline{0}, \overline{0}, \overline{0}) \Leftrightarrow \left[\begin{array}{l} 2x_1 = \overline{0} \\ 2x_2 = \overline{0} \\ 2x_3 = \overline{0} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x_1 = \overline{0}, \overline{1} \\ x_1 = \overline{0}, \overline{2} \\ x_2 = \overline{0}, \overline{1} \end{array}\right.$$

  В этой группе есть 8 решений уравнения (7.4).

Задача 60.40 б) Существует ли в абелевой группе A типа $(2, 16)$ подгруппа B типа $(4, 4)$?

Решение.

$$A \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{16}$$
$$B \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$$

Найдем количество решений уравнения $2x = 0$ в этих разложениях.

- В группе B, $x = (x_1, x_2)$, $x_1, x_2 \in \mathbb{Z}_4$.

$$2(x_1, x_2) = (\overline{0}, \overline{0}) \Leftrightarrow \left[\begin{array}{l} 2x_1 = \overline{0} \\ 2x_2 = \overline{0} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x_1 = \overline{2}, \overline{0} \\ x_2 = \overline{2}, \overline{0} \end{array}\right.$$

  Есть 4 решения.

- В группе A, $x = (x_1, x_2)$, $x_1 \in \mathbb{Z}_2$, $x_2 \in \mathbb{Z}_{16}$.

$$2(x_1, x_2) = (\overline{0}, \overline{0}) \Leftrightarrow \left[\begin{array}{l} 2x_1 = \overline{0} \\ 2x_2 = \overline{0} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x_1 = \overline{0}, \overline{1} \\ x_2 = \overline{0}, \overline{1} \end{array}\right.$$

  Снова 4 решения.

С помощью уравнения (7.4) группы A и B различить нельзя.

Посмотрим на количество решений уравнения $4x = 0$.

- В группе B, $x = (x_1, x_2)$, $x_1, x_2 \in \mathbb{Z}_4$.

$$4(x_1, x_2) = (\overline{0}, \overline{0}) \Leftrightarrow \left[\begin{array}{l} 4x_1 = \overline{0} \\ 4x_2 = \overline{0} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x_1 = \overline{0}, \overline{1}, \overline{2}, \overline{3} \\ x_2 = \overline{0}, \overline{1}, \overline{2}, \overline{3} \end{array}\right.$$

  Есть 16 решений.

- В группе A, $x = (x_1, x_2)$, $x_1 \in \mathbb{Z}_2$, $x_2 \in \mathbb{Z}_{16}$.

$$4(x_1, x_2) = (\overline{0}, \overline{0}) \;\Leftrightarrow\; \left[\begin{array}{l} 4x_1 = \overline{0} \\ 4x_2 = \overline{0} \end{array}\right. \;\Leftrightarrow\; \left[\begin{array}{c} x_1 = \overline{0}, \overline{1} \\ x_2 = \overline{0}, \overline{4}, \overline{8}, \overline{12} \end{array}\right.$$

  Получили 8 решений.

Ответ: нет.

Домашнее задание: 60.54, 60.39 е),ж),д), 60.40 а),б),в).

Лекция 8

Задача об объеме целочисленного параллелепипеда

Задача. $v_1, \ldots, v_n \in \mathbb{Z}^n$ - линейно независимые векторы,

$$\Pi = \Pi(v_1, \ldots, v_n) = \{v = t_1 v_1 + \ldots + t_n v_n \mid 0 \leq t_1, \ldots, t_n \leq 1\}.$$

Покажем, что

1. $\operatorname{vol}\Pi =$ число целых точек в $\Pi \backslash \{$ грани, не содержащие начало координат $\}$

и что

2. $\operatorname{vol}\Pi = \sum\limits_{k=0}^{n} \frac{1}{2^k}($ число целых точек внутри граней размерности $n-k)$.

Доказательство. **Пункт 1.**
Из линейной алгебры известно, что

$$\operatorname{vol}\Pi = |\det(v_1, \ldots, v_n)|.$$

С точки зрения конечнопорожденных абелевых групп

$$|\det(v_1, \ldots, v_n)| = |\mathbb{Z}^n / \langle v_1, \ldots, v_n \rangle|.$$

Факторгруппа - это множество смежных классов. Как устроен смежный класс в нашем случае?
Пусть $w \in \mathbb{Z}^n$, тогда его смежный класс - это множество всевозможных сдвигов вектора w на целочисленные линейные комбинации векторов $v_1, \ldots, v_n$.

Определим количество этих смежных классов.

Формально покажем, что с помощью сдвигов на целочисленные линейные комбинации $v_1, \ldots, v_n$ произвольный вектор w может попасть в множество
$\Pi \backslash \{$грани, не содержащие начало координат$\}$.

Векторы $v_1, \ldots, v_n$ образуют базис n-мерного пространства, тогда

$$w = t_1 v_1 + \ldots + t_n v_n.$$

Здесь $t_1, \ldots, t_n$ не обязательно лежат в $[0, 1]$ и они не обязательно целые.
Вычитая или прбавляя к w целочисленную линейную комбинацию $v_1, \ldots, v_n$, коэффициент t_i можно изменить на некоторое целое число. Тогда путем прибавления/вычитания целого числа t_i можно привести в диапазон $[0, 1)$.
Таким образом, можно каждое число t_i заменить на его дробную часть.

То, что $t_i \in [0, 1)$, как раз и означает, что конец вектора w не лежит на грани, не содержащей начало координат. Грани, не содержащие 0, задаются условием $t_j = 1$.

Получается, что в смежном классе любого $w \in \mathbb{Z}^n$ есть вектор, лежащий в $\Pi \backslash \{$грани, не содержащие начало координат$\}$. Сколько представителей в этом множестве имеет данный смежный класс?
Если есть 2 линейных комбинации $v_1, \ldots, v_n$ с коэффициентами $t_i \in [0, 1)$, то разность двух таких векторов не может иметь целые координаты, поэтому у каждого смежного класса представитель один.

Итак,

$$|\mathbb{Z}^n / \langle v_1, \ldots, v_n \rangle| = \text{ число целых точек в } \Pi \backslash \{ \text{ грани, не содержащие начало координат } \}.$$

Пункт 2.
Как устроены грани размерности $n-k$? Грань задается выбором $1 \leq i_1, \ldots, i_k \leq n$ и $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$

$$\Gamma_{i_1,\ldots,i_k}^{\varepsilon_1,\ldots,\varepsilon_k} = \{v \in \Pi \mid t_{i_1} = \varepsilon_1, \ldots, t_{i_k} = \varepsilon_k\}$$

Зафиксируем набор $i_1, \ldots, i_k$, тогда граней $\Gamma_{i_1,\ldots,i_k}^{\varepsilon_1,\ldots,\varepsilon_k}$ 2^k штук. Из этих граней только одна содержит начало координат - это $\Gamma_{i_1,\ldots,i_k}^{0,\ldots,0}$.

Грани с фиксированным набором $i_1, \ldots, i_k$ отличаются друг от друга целочисленными сдвигами. Количество целых точек во всех таких параллельных друг другу гранях одинаково.

Воспользуемся формулой из пункта 1, в которой из всех параллельных друг другу 2^k граней нужно учеть только одну - $\Gamma_{i_1,\ldots,i_k}^{0,\ldots,0}$. Если теперь мы будем считать число целых точек внутри всех граней размерности $n-k$, то получим число больше нужного в 2^k раз. Отсюда получаем коэффициент в формуле из пенкта 2.

Итак,

$$\operatorname{vol} \Pi = \sum_{k=0}^{n} \frac{1}{2^k} (\text{ число целых точек внутри граней размерности } n-k).$$

□

Решение задачи 60.41

Задача 60.41 $A = \langle a \rangle_9 \oplus \langle b \rangle_{27} \simeq \mathbb{Z}_9 \oplus \mathbb{Z}_{27}$ - конечная абелева группа типа (9, 27). $A \supset B = \langle 3a + 9b \rangle_3 \simeq \mathbb{Z}_3$ - подгруппа типа (3).

Найти факторгруппу A/B (т.е. ее разложение).

Решение. Общий подход к решению задач такого типа.
Известен алгоритм нахождения факторгруппы для факторгруппы свободной абелевой группы по какой-то ее подгруппе. Теперь нужно свести задачу нахождения

факторгруппы конечной абелевой группы по своей подгруппе к уже известному алгоритму.

Обозначим $C := A/B$.

Напомним алгоритм описания структуры конечнопорожденной абелевой группы A.
Строим сюръективный гомоморфизм из свободной абелевой группы с базисом, равным по модулю числу порождающих группы A. Линейная комбинация элементов базиса свободной группы переходит в линейную комбинацию порождающих элементов A с теми же коэффициентами.
Релизуем эту схему в нашем случае.

Существует канонический гомоморфизм $\pi : A \to C$, группа A порождена элементами a и b. Тогда группа C порождена смежными классами элементов a и b, т.к. при гомоморфизме линейная комбинация a и b переходит в линейную комбинацию образов a и b. Поскольку π сюръективен, такие линейные комбинации покроют всю группу C.

$$C = \langle \pi(a), \pi(b) \rangle$$

Пусть F - свободная абелева группа с базисом $\{x, y\}$. Построим гомоморфизм

$$\varphi : F \to A,$$

$$\varphi(x) = a, \quad \varphi(y) = b.$$

Тогда

$$\psi = \pi \circ \varphi : F \to C,$$

$$\psi(x) = \pi(a), \quad \psi(y) = \pi(b),$$

будет гомоморфизмом из свободной группы в группу C.

Обозначим $\operatorname{Ker} \psi =: K$. Тогда

$$C \simeq F/K.$$

Алгроитм поиска факторгруппы свободной абелевой группы по подгруппе известен, а значит осталось понять, как устроено ядро K.

$$K = \operatorname{Ker} \psi = \varphi^{-1}(\operatorname{Ker} \pi) = \varphi^{-1}(B) \ni 3x + 9y$$

Кроме того, $\varphi^{-1}(B) \supseteq \varphi^{-1}(0) = \operatorname{Ker} \varphi = \langle 9x, 27y \rangle$.

Заметим, что $\varphi^{-1}(B) = \langle 3x + 9y,\ 9x,\ 27y \rangle$.

Действительно, предположим, что $z \in F :\ \varphi(z) \in B$. Другими словами, $\varphi(z) = k \cdot (3a + 9b)$.
С другой стороны, существует элемент $k \cdot (3x + 9y) = z' \in F$ с таким же образом.

Пусть $w = z' - z$, тогда $\varphi(w) = \varphi(z') - \varphi(z) = 0$.

Значит, $w \in \operatorname{Ker}\varphi$ и $w = l \cdot 9x + m \cdot 27y$.
$z = z' - w$, тем самым z' выражается через $3x + 9y$, а w выражается через $9x$, $27y$, откуда любой элемент из $\varphi^{-1}(B)$ выражается через $3x + 9y$, $9x$, $27y$.

Итак, чтобы найти порождающие элементы $\operatorname{Ker}\psi$, нужно взять порождающие элементы подгруппы B, взять какие-то их прообразы и добавить к ним порождающие элементы $\operatorname{Ker}\varphi$.

Теперь, зная $F = \langle x, y\rangle$ и $K = \langle 3x + 9y,\ 9x,\ 27y\rangle$, можем найти F/K.
Записываем по столбцам координаты порождающих элеентов K в базисе F.

$$\begin{pmatrix} 9 & 0 & 3 \\ 0 & 27 & 9 \end{pmatrix} \overset{(1)}{\to} \begin{pmatrix} 9 & -9 & 3 \\ 0 & 0 & 9 \end{pmatrix} \overset{(2)}{\to} \begin{pmatrix} 0 & -9 & 3 \\ 0 & 0 & 9 \end{pmatrix} \overset{(3)}{\to}$$

$$\overset{(3)}{\to} \begin{pmatrix} 0 & 0 & 3 \\ 0 & 27 & 9 \end{pmatrix} \overset{(4)}{\to} \begin{pmatrix} 0 & 0 & 3 \\ 0 & 27 & 0 \end{pmatrix} \overset{(5)}{\to} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 27 & 0 \end{pmatrix}$$

(1) - прибавим ко второму столбцу третий с коэффициентом -3
(2) - прибавим второй столбец к первому
(3) - прибавим ко второму столбцу третий с коэффициентом 3
(4) - прибавим ко второй строке первую с коэффициентом -3
(5) - поменяем первый столбец с третим

$$C \simeq F/K \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_{27}$$

Ответ: $\mathbb{Z}_3 \oplus \mathbb{Z}_{27}$

Решение задачи 60.43 а)

Задача 60.43 а) A - нециклическая абелева группа порядка 12. Сколько в A подгрупп
1. порядка 2;
2. порядка 6?

Решение. Любая конечная абелева группа разлагается в прямую сумму примарных циклических групп. Для произвольной абелевой группы порядка 12 есть 2 варианта разложения

$$A \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \qquad A \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$$

Циклическая группа должна содержать порождающий элемент порядка 12. В группе $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ пара $(\overline{1},\ \overline{1})$ является таким элементом, значит, $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$ - циклическая.

Таким образом, подходит единственное разложение

$$A \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

1) Найдем все подгруппы $B \subset A$ порядка 2.

Любая группа порядка 2 циклическая $B = \langle b \rangle_2 = \{0, b\}$. Чтобы перечислить все подгруппы порядка 2 необходимо и достаточно перечислить все элементы группы $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ порядка 2.

$b = (b_1,\ b_2,\ b_3),\ \ b_1, b_2 \in \mathbb{Z}_2,\ b_3 \in \mathbb{Z}_3.$
Порядок b равен НОК порядков $b_1,\ b_2,\ b_3$, соответственно, порядки этих элементов должны быть равны 1 или 2.

$$b_1, b_2 = \left[\begin{array}{l} \overline{0} \\ \overline{1} \end{array}\right.$$

В группе $\mathbb{Z}_3$ нет элементов порядка 2 (2 не делит 3), поэтому

$$b_3 = \overline{0}.$$

Всего есть 3 подходящих варианта и 3 подгруппы порядка 2, порожденные элементами

$$(b_1,\ b_2,\ b_3) = \left[\begin{array}{l} (\overline{0},\ \overline{1},\ \overline{0}) \\ (\overline{1},\ \overline{0},\ \overline{0}) \\ (\overline{1},\ \overline{1},\ \overline{0}) \end{array}\right.$$

2) Найдем все подгруппы $C \subset A$ порядка 6.

Разложение на примарные циклические группы для C единственно

$$C \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_6.$$

$$C = \langle c \rangle_6 = \{0,\ c,\ 2c,\ 3c,\ 4c,\ 5c\} = \langle 5c \rangle_6$$

Количество подгрупп порядка 6 равно половине количества элементов порядка 6 в группе A, т.к. у каждой такой подгруппы есть 2 разных порождающих.

Напоминание: если элемент c порождает циклическую группу C, то $k \cdot c$ порождает $C \Leftrightarrow\ (k, |C|) = 1$.

$c = (c_1,\ c_2,\ c_3),\ \ c_1, c_2 \in \mathbb{Z}_2,\ c_3 \in \mathbb{Z}_3.$

$$c_1, c_2 = \left[\begin{array}{l} \overline{0} \\ \overline{1} \end{array}\right.$$

$$c_3 = \left[\begin{array}{l} \overline{1} \\ \overline{2} \end{array}\right.$$

Всего есть 6 элементов порядка 6

$$(b_1,\ b_2,\ b_3) = \left[\begin{array}{l}(\overline{0},\ \overline{1},\ \overline{1})\\(\overline{0},\ \overline{1},\ \overline{2})\\(\overline{1},\ \overline{0},\ \overline{1})\\(\overline{1},\ \overline{0},\ \overline{2})\\(\overline{1},\ \overline{1},\ \overline{1})\\(\overline{1},\ \overline{1},\ \overline{2})\end{array}\right.$$

и $6/2$ порожденных ими подгрупп.

Ответ: 1) 3, 2) 3.

Действия группы на множестве

Определение 8.25. *Действие группы G на множестве X - это отображение*

$$G \times X \to X,$$
$$(g,\ x) \mapsto g \cdot c,$$

которое паре элементов (g, x) сопоставляет результат действия элемента $g \in G$ на элемент $x \in X$ со свойствами:

1) $e \cdot x = x,\ \ \forall x \in X;$

2) $g \cdot (h \cdot x) = (g \cdot h) \cdot x,\ \ \forall g, h \in G,\ x \in X.$

Альтернативное определение.

Определение 8.26. *Действие группы G на множестве X - это гомоморфизм*

$$\varphi : G \to S(X),$$
$$g \mapsto \varphi_g,$$

где $S(X)$ - группа, состоящая из биекций множества X на себя, с операцией композиции.

Какая свзяь между этими определениями?

По отображению действия из первого определения построим гомоморфизм из второго определения.

$$\varphi_g : X \to X,$$
$$\varphi_g(x) = g \cdot x.$$

То, что такое отображения являетмя биекцией и гомоморфизмом выводится из аксиом первого определения.

Обратно: если задан гомоморфизм φ в группу биекций, то по правилу $\varphi_g(x) = g \cdot x$ можно определить отображение действия из первого определения и проверить его аксиомы.

Обозначение действия G на X: $G \curvearrowright X$.

Орбиты действия

Определение 8.27. *Орбита $G \cdot x = \{y = g \cdot x \mid g \in G\}$ - это все возможные элементы, которые получаются из данного элемента x действием всевозможных элементов группы G.*

Свойство: Всевозможные орбиты образуют разбиение множества X на попарно не пересекающиеся подмножества.

Пример. $GL_n(K) \curvearrowright K^n$ - действие группы невырожденых матриц на пространстве векторов-столбцов.
Зададим отображение действия

$$(A, x) \mapsto A \cdot x.$$

Действие = произведение матрицы на столбец. Легко видеть, что аксиомы из первого определения выполнены по свойствам умножения матриц.

Сколько орбит у такого действия? Умножением на подходящую матрицу любой столбец, кроме нулевого, можно перевести в любой другой столбец (кроме нулевого).

Покажем, как можно получить любой ненулевой столбец из некоторого ненулевого.

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \neq 0$$

Приведем матрицу A такую, что $Ae_1 = a$. В первом ее столбце должен стоять вектор a, т.к. первый столбец в матрице - это образ первого базисного вектора под действием линейного оператора, задаваемого этой матрицей. В остальных столбцах могут стоять произвольные числа такие, чтобы система всех столбцов была линейно независима. Подобрать такие числа всегда можно, потому что любой ненулевой вектор можно дополнить до базиса.

$$A = \left(\begin{array}{c|c} a_1 & \\ a_2 & \\ \vdots & \\ a_n & \end{array}\right)$$

Таким образом, есть 2 орбиты :

$$\{0\}, \quad K^n \backslash \{0\}$$

Решение задачи 57.1 а)

Задача 57.1 а) G - группа верхнетреугольных невырожденных матриц над полем K.

Найти орбиты действия $G(K) \curvearrowright K^n$.

Решение. Наивный подход к решению задач на разбиение множества на орбиты под действием некторой группы.
Возьмем какую-то точку из множества X и посмотрим на ее орбиту (т.е. подействуем на эту точку всеми элементами группы). Если полученная орбита заполнила множество X, на этом процесс останавливается, иначе берем точку не принадлежающуу этой орбите, и вычисляем ее орбиту и т.д.
Может оказаться, что такой процесс бесконечен, т.к. орбит бесконечное число, тогда нужно угадывать некоторые семейства орбит, зависящие от параметра.

В любом случае сначала нужно определить, как действует произвольный элемент группы G на произвольный элемент множества X.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & \dots & \dots & a_{1n} \\ & a_{22} & \dots & \dots & \dots & a_{2n} \\ & & \ddots & & & \vdots \\ & & & a_{ii} & \dots & a_{in} \\ & 0 & & & \ddots & \vdots \\ & & & & & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix} = y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_i \\ \vdots \\ y_n \end{pmatrix}$$

$$\begin{gathered} y_1 = a_{11}x_1 + \ldots + a_{1n}x_n \\ y_2 = a_{22}x_2 + \ldots + a_{nn}x_n \\ \vdots \\ y_i = a_{ii}x_i + \ldots + a_{nn}x_n \\ \vdots \\ y_n = a_{nn}x_n \end{gathered}$$

Видно, что на i-тую координату образа элемента x под действием элемента группы $A \in G$ влияют только координаты $\geq i$.

Орбиты базисных векторов $G \cdot e_j$ - это столбцы вида

$$\begin{pmatrix} * \\ \vdots \\ * \\ * \neq 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{8.1}$$

где на первых $j-1$ местах стоят произвольные числа, на j-том месте ненулевое число, а дальше - нули.

Всего орбит такого типа n штук. Они покрывают ножество X, кроме случая действия на нулевой столбец.

Ответ: $(8.1) + \{0\}$ - полное описание орбит действия $G(K) \curvearrowright K^n$.

Домашнее задание: 60.42, 60.43 б),в), 57.1 б),в), 57.2, 57.3.

Лекция 9

Решение задач 57.1 б), 57.9 а). Свойства стабилизаторов

Задача 57.1 б) Найти все орбиты группы G ортогональных линейных операторов, действующих на n-мерном пространстве V.

Решение. Эта задача вытекает из 57.1 г), где G - группа операторов, матрицы которых в базисе $e_1, \ldots, e_n$ верхнетреугольные, и нужно найти стабилизатор вектора $a = e_1 + \ldots + e_n$.

Пусть $G \curvearrowright X$ и $x \in X$. Стабилизатор точки $G_x = \{g \in G \mid g \cdot x = x\}$ - это подгруппа в G. Синоним: G_x - стационарная подгруппа точки x.

Чтобы найти стабилизатор G_a в нашей задаче, нужно подействовать на a произвольным элементом $g \in G$ и записать условие $g \cdot a = a$. $a = e_1 + \ldots + e_n$ - столбец из единиц.

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & \ldots & \ldots & a_{1n} \\ & a_{22} & \ldots & \ldots & \ldots & a_{2n} \\ & & \ddots & & & \vdots \\ & & & a_{ii} & \ldots & a_{in} \\ & 0 & & & \ddots & \vdots \\ & & & & & a_{nn} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} + \ldots + a_{1n} \\ a_{22} + \ldots + a_{nn} \\ \vdots \\ a_{ii} + \ldots + a_{nn} \\ \vdots \\ a_{nn} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

Это и есть описание стабилизатора a, т.к. по виду матрицы можно понять, принадлежит ли она G_a.

Задача 59.9 а) $X = \{1, \ldots, 10\}$, $\sigma \in S_{10}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix}.$$

$G = \langle \sigma \rangle \subset S_{10}$, $G \curvearrowright X$. Описать все орбиты и все стабилизаторы этого действия.

Решение. Чтобы описать орбиты, разложим σ в произведение независимых циклов.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix} = (1,\ 5,\ 4,\ 9)(2,\ 8)(6,\ 10,\ 7)$$

Посмотрим на орбиты конкретных точек, например,

$$G \cdot 1 = \{1,\ 4,\ 5,\ 9\} = G \cdot 4 = G \cdot 5 = G \cdot 9.$$

При действии степенью подстановки σ каждый элемент внутри независимого цикла сдвигается на несколько позиций внутри этого цикла.

$$G \cdot 2 = G \cdot 8 = \{2,\ 8\}$$

$$G \cdot 6 = G \cdot 10 = G \cdot 7 = \{6,\ 7,\ 10\}$$
$$G \cdot 3 = \{3\}$$

Получилось 4 орбиты действия с элементами из независимых циклов.

Теперь найдем стабилизаторы элементов.
Сначала перечислим все элементы группы G. Ее мощность равна порядку σ, который равен НОК порядков независимых циклов. А именно, $|G = 12|$.

$$G = \{\mathrm{id},\ \sigma,\ \sigma^2,\ \ldots,\ \sigma^{11}\}$$

$$G_1 = \{\mathrm{id},\ \sigma^4,\ \sigma^8\} = G_4 = G_5 = G_9$$
$$G_2 = G_8 = \{\mathrm{id},\ \sigma^2,\ \sigma^4,\ \sigma^6,\ \sigma^8,\ \sigma^{10}\}$$
$$G_6 = G_{10} = G_7 = \{\mathrm{id},\ \sigma^3,\ \sigma^6,\ \sigma^9\}$$
$$G_3 = G$$

Заметим, что стабилизаторы точек из одной орбиты оказались одинаковыми.

Сравним количество элементов в стабилизаторе и орбите элемента.

Орбита		Стабилизатор	
$G \cdot 1$	4	G_1	3
$G \cdot 2$	2	G_2	6
$G \cdot 6$	3	G_6	4
$G \cdot 3$	1	G_3	12

Видно, что произведение количества чисел в орбите и в стабилизаторе дает порядок группы.

Свойства стабилизаторов

1) Пусть $G_x = H,\ y = g \cdot x$, тогда $G_y = gHg^{-1}$.

2) Взаимно-однозначное соответствие между точками орбиты $G \cdot x$ и левыми смежными классами по стабилизатору

$$G \cdot x \ \leftrightarrow\ G/G_x,$$

$$y = g \cdot x \ \leftrightarrow\ g \cdot H.$$

Заметим, что элемент g определен неоднозначно, т.к. его можно домножить справа на любой элемент из стабилизатора.

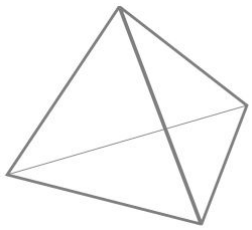
3) Следствие из свойства 2). $|G| < \infty \ \Rightarrow\ |G \cdot x| = \frac{|G|}{|G_x|}$.

Правильные многогранники. Их двойственность

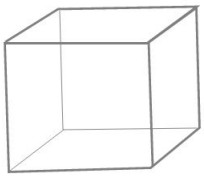
Определение 9.28. *Правильный многогранник - это выпуклый многогранник, грани которого являются одинаковыми правильными многоугольниками.*

Всего таких правильных многоугольников 5.

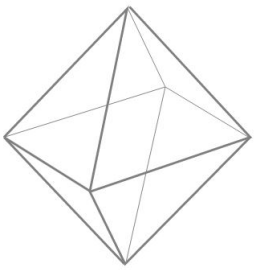
1. Тетраэдр **T**. Имеет 4 грани, которые являются правильными треугольниками.



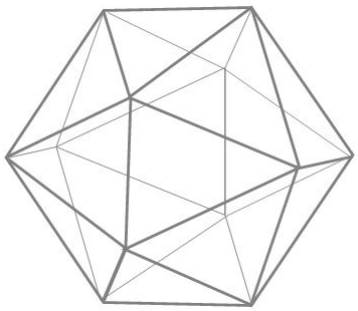
2. Куб **C**.



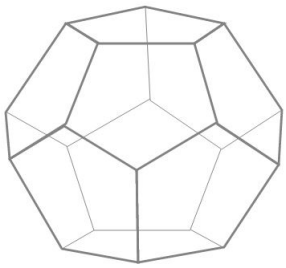
3. Октаэдр **O**. Имеет 8 граней - правильных треугольников. Две правильных четырехгранных пирамиды соединяются друг с другом основаниями.



4. Икосаэдр **I**. Имеет 20 граней - правильных треугольников. Две правильные пятигранные пирамиды повернуты относительно друг друга и их основания соединены правильными треугольниками.



5. Додекаэдр $\mathbf{D}$. 12 граней - правильных пятиугольников. В каждой вершине смыкаются 3 правильных пятиугольника.



Двойственность

Если $\mathbf{P}$ - правильный многогранник, то ему соответствует двойственный многогранник $\mathbf{P}^*$.
Вершины $\mathbf{P}^*$ - это центры граней исходного многогранника $\mathbf{P}$. Две вершины $\mathbf{P}^*$ соединяются ребром в том случае, когда соответствующие грани $\mathbf{P}$ соседние.

- Двойственный многогранник к тетраэдру - это подобный ему тетраэдр. Поэтому, если понимать совпадение многогранников с точностью до подобия, $\mathbf{T} \sim \mathbf{T}^*$.
- Двойственный многогранник к кубу $\mathbf{C}$ - октаэдр $\mathbf{O}$.
- Двойственный многогранник к икосаэдру $\mathbf{I}$ - додекаэдр $\mathbf{D}$.

Применяя операцию двойственности 2 раза, получим

$$\mathbf{P}^{**} \sim \mathbf{P}.$$

Группы, связанные с правильными многогранниками

Группа движений правильного многогранника $\operatorname{Isom}\mathbf{P}$ - множество движений трехмерного пространства, которые оставляют $\mathbf{P}$ на месте.

Подгруппа $\operatorname{Isom}^+\mathbf{P} \subset \operatorname{Isom}\mathbf{P}$ - группа собственных движений.
Если какое-то движение сохраняет правильный многогранник, то оно сохраняет и его центр. Как устроены собственные движения трехмерного пространства с неподвижной точкой? Это могут быть только повороты.
Таким образом, $\operatorname{Isom}^+\mathbf{P}$ - группа вращений правильного многогранника.

В группе $\operatorname{Isom}\mathbf{P}$ $\operatorname{Isom}^+\mathbf{P}$ является подгруппой индекса 2.
В с.д., движение с неподвижной точкой можно считать линейным преобразованием, тогда у собственного движения определитель равен 1, а у несобственного -1. Определитель является гомоморфизмом из группы $\operatorname{Isom}\mathbf{P}$ в группу $\{\pm 1\}$. Ядро этого гомоморфизма $\operatorname{Isom}^+\mathbf{P}$ будет подгруппой индекса 2.

Замечание 9.1. *У двойственных друг другу многогранников группы движений одинаковы.*
Действительно, если движение сохраняет многогранник $\mathbf{P}$*, то оно как-то переставляет его вершины, ребра и грани, а следовательно переставляет центры граней - вершины двойственного многогранника.*

В силу двойственности, чтобы описать группы движений правильного многогранника, достаточно рассмотреть 3 случая (вместо 5).

Группа движений куба. Подгруппа собственных движений куба.

$\operatorname{Isom}^+\mathbf{C}$.
Сначала определим порядок этой группы. Рассмотрим действие группы $\operatorname{Isom}^+\mathbf{C}$ на множестве, где сможем посчитать порядок орбиты и порядок стабилизатора, тогда найдем и порядок всей группы.

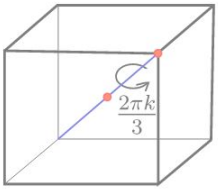
$$G = \operatorname{Isom}^+\mathbf{C} \curvearrowright \{\text{вершины } \mathbf{C}\}$$

У этого действия одна орбита (содержащая 8 элементов), т.к. любую вершину можно перевести в любую другую подходящим вращением куба.

Рассмотрим теперь стабилизатор некоторой вершины x.

Точка x и центр куба при собственном движении должны остаться на месте, значит, ось вращения - диагональ куба, проходящая через x и центр. Подходят повороты на углы $\frac{2\pi k}{3}$, $k = 0, 1, 2$.

$$G_x = \{\mathrm{id},\ r_{\frac{2\pi}{3}},\ r_{\frac{4\pi}{3}}\}$$



$$|G| = |G \cdot x| \cdot |G_x| = 8 \cdot 3 = 24 (= |S_4|)$$

Гипотеза: $\mathrm{Isom}^+ \mathbf{C} \simeq S_4$. Чтобы это показать, нужно придумать действие группы $\mathrm{Isom}^+ \mathbf{C}$ на множестве из 4 элементов.

Естественное такое множество - 4 диагонали куба. Каждое вращение куба их каким-то образом переставляет.

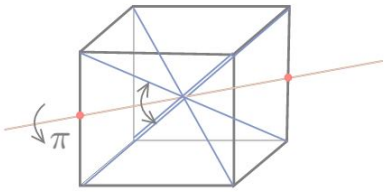
$$G = \mathrm{Isom}^+ \mathbf{C} \curvearrowright Y = \{\text{диагонали } \mathbf{C}\}$$

Согласно второму определению действия, если G действует на множестве Y, то возникает гомоморфизм из G в группу перестановок элементов Y.

$$\varphi : G \to S(Y) = S_4$$

Итак, $|G| = 24 = |S_4|$ и задан гомоморфизм φ. Чтобы показать, что φ - изоморфизм, достаточно проверить либо что φ - инъекция, либо что φ - сюръекция. Покажем сюръективность: всякая перестановка диагоналей куба реализуется с помощью вращения.

Достаточно реализовать транспозицию, т.к. любая другая перестановка - это произведение транспозиций.
Ясно, что все диагонали равноправны и достаточно научиться представлять перестановку одной пары диагоналей с помощью вращения. Ось вращения соединяет середины противоположных граней, угол поворота π.



Две диагонали, которые мы хотим поменять местами, перейдут одна в другую. Две другие диагонали перпендикулярны оси вращения, и при повороте на π они переворачиваются, т.е. их концы (и все точки симметричные относительно центра) меняются местами.

Таким образом, φ сюръективен, а значит он инъективен, поскольку множества имеют одинаковую мощность.

$$\operatorname{Isom}^+ \mathbf{C} \simeq S_4$$

Группа $\operatorname{Isom} \mathbf{C}$ в 2 раза больше группы $\operatorname{Isom}^+ \mathbf{C}$, т.е. чтобы найти группу $\operatorname{Isom} \mathbf{C}$, нужно за счет чего-то расширить $\operatorname{Isom}^+ \mathbf{C}$.

Центральная симметрия относительно центра куба не является собственным движением. Если считать это движение линейным преобразованием, то оно равно $-E$. Такая центральная симметрия коммутирует со всеми остальными преобразованиями, в частности, с любым вращением.

В группе $\operatorname{Isom} \mathbf{C}$ есть подгруппа $\operatorname{Isom}^+ \mathbf{C}$ и подгруппа второго порядка $\{\pm E\}$. Эти подгруппы коммутируют друг с другом, пересекаются по E, следовательно, образуют прямое произведение. Заметим, что $\operatorname{Isom}^+ \mathbf{C}$ нормальна как ядро гомоморфизма, а $\{\pm E\}$ коммутирует со всеми элементами группы и тоже нормальна.

$$|\operatorname{Isom}^+ \mathbf{C}| \cdot |\{\pm E\}| = \frac{|G|}{2} \cdot 2 = |G| = |\operatorname{Isom} \mathbf{C}|,$$

откуда

$$\operatorname{Isom} \mathbf{C} = \operatorname{Isom}^+ \mathbf{C} \times \{\pm E\} \simeq S_4 \times \mathbb{Z}_2.$$

Домашнее задание. Показать, что

1)
$$\operatorname{Isom} \mathbf{T} \simeq S_4 \qquad \operatorname{Isom}^+ \mathbf{T} \simeq A_4$$

2)
$$\operatorname{Isom} \mathbf{T} \simeq S_4 \qquad \operatorname{Isom}^+ \mathbf{T} \simeq A_4$$

Подготовительные задачи к п.2) 57.9 б),в), 57.14 б), 57.12 в).

Действие произвольной группы G на себе

Как можно определить $G \curvearrowright G$?

- Умножениями слева:
$$g \circ x = g \cdot x, \quad g, x \in G.$$
У этого действия 1 орбита, т.к. любой элемент группы G можно перевести в любой другой, умножив его слева на подходящий элемент из G.
Стабилизатор каждой точки состоит только из единичного элемента.

- Умножениями справа:
$$g \circ x = x \cdot g^{-1}, \quad g, x \in G.$$

Умножать нужно на g^{-1}, т.к. действие должно удовлетворять свойству ассоциативности

$$\underbrace{g_1 \circ (\underbrace{g_2 \circ x}_{xg_2^{-1}})}_{xg_2^{-1}g_1^{-1}} = g_1 g_2 \circ x = x(g_1 g_2)^{-1}$$

У этого действия также 1 орбита. Стабилизатор любого элемента тривиален.

- Действие сопряжениями:

$$g \circ x = g \cdot x \cdot g^{-1}, \quad x, g \in G.$$

Орбиты - это классы сопряженности $C(x) = C_G(x) = \{gxg^{-1} \mid g \in G\}$.
Стабилизатор элемента x - это его централизатор $Z(x) = Z_G(x) = \{g \in G \mid gxg^{-1} = x \Leftrightarrow gx = xg\}$. Другими словами, централизатор элемента x состоит из элементов группы G, которые с x коммутируют. Можно сказать, что центр группы - это пересечение всех централизаторов ее элементов.

Утверждение 9.10. *Пусть* $|G| < \infty$, *тогда*

$$|C(x)| = \frac{|G|}{|Z(x)|}, \quad \forall x \in G.$$

Отсюда следует, что порядок любого класса сопряженности делит порядок группы.

Решение задачи 57.23 а)

Задача 57.23 а) $G = S_4, \ \ \sigma = (1,\ 2)(3,\ 4)$. Найти $Z(\sigma)$.

Решение. $Z(\sigma)$ состоит из подстановок π, которые коммутируют с σ.
Известен общий вид сопряженной подстановки

$$\pi\sigma\pi^{-1} = (\pi(1),\ \pi(2))(\pi(3),\ \pi(4)).$$

Перечислим все такие π, что

$$(\pi(1),\ \pi(2))(\pi(3),\ \pi(4)) = \sigma = (1,\ 2)(3,\ 4).$$

$\pi(1)$	$\pi(2)$	$\pi(3)$	$\pi(4)$	π
1	2	3	4	id
2	1	3	4	$(1,\ 2)$
1	2	4	3	$(3,\ 4)$
2	1	4	3	$(1,\ 2)(3,\ 4)$
3	4	1	2	$(1,\ 3)(2,\ 4)$
3	4	2	1	$(1,\ 3,\ 2,\ 4)$
4	3	1	2	$(1,\ 4,\ 2,\ 3)$
4	3	2	1	$(1,\ 4)(2,\ 3)$

Этот результат можно было получить и другим способом.

$$C(\sigma) = \{(i,\ j)(k,\ l)\} = \{(1,\ 2)(3,\ 4), (1,\ 3)(2,\ 4), (1,\ 4)(2,\ 3)\}$$

$$|Z(\sigma)| = \frac{|S_4|}{|C(\sigma)|} = \frac{24}{3} = 8$$

Теперь определим, какие именно подстановки входят в $Z(\sigma)$.
Сразу можно сказать, что с σ коммутируют id, степени σ, транспозиции $(1,\ 2),\ (3,\ 4)$.
Кроме того, реализация абелевой группы V_4 как подгруппы S_4 есть

$$V_4 = \{\mathrm{id}, (i,\ j)(k,\ l)\} \ni \sigma.$$

Отсюда $Z(\sigma) \ni V_4$. $|Z(\sigma) = 8|,\ |V_4| = 4$, значит, нужно расширить группу V_4 в 2 раза.
Это можно сделать с помощью полупрямого произведения V_4 и подгруппы $\langle(1,\ 2)\rangle_2$.

$$Z(\sigma) \simeq V_4 \leftthreetimes \langle(1,\ 2)\rangle_2$$

Подгруппа V_4 нормальна, $V_4 \cap \langle(1,\ 2)\rangle_2 = \mathrm{id}$, произведение их порядков дает порядок группы, следовательно, такое представление корректно.

Ответ: $Z(\sigma) \simeq V_4 \leftthreetimes \langle(1,\ 2)\rangle_2 =$ все подстановки π из таблицы.

Формула классов для конечной группы

Пусть G - конечная группа, рассмотрим действие $G \curvearrowright G$ сопряжениями. Тогда вся группа G разбивается на попарно непересекающиеся классы сопряженности.
Тогда чтобы посчитать $|G|$, нужно просуммировать порядки классов сопряженности.

Классы сопряженности элементов из центра G содержат только 1 элемент. Количество таких элеентов равно сумме порядков их классов сопряженности и равно $|Z(G)|$.

Остается просуммировать порядки классов сопряженности элементов, не лежащих в центре. Можно в каждом из этих классов выбрать одного представителя x_i, тогда в классе сопряженности x_i содержится $\frac{|G|}{|Z(x_i)|}|$ элементов.

В итоге получаем **формулу классов**

$$|G| = |Z(G)| + \sum_{x_i} \frac{|G|}{|Z(x_i)|}. \tag{9.1}$$

Следствие 1. Пусть $|G| = p^k$, p - простое. Тогда $Z(G) \neq \{e\}$.

Доказательство. Обратимся к формуле классов (9.1).

В сумме $\sum\limits_{x_i} \frac{|G|}{|Z(x_i)|}$ каждое слагаемое имеет порядок $\frac{p^k}{p^l} = p^{k-l}$. Поскольку в этой сумме только порядки нецентральных классов сопряженности, $k - l > 0$.
Значит, каждое слагаемое делится на p и вся сумма делится на p.

Т.к. $|G|$ тоже делится на p, $|Z(G)|$ делится на p. В $|Z(G)|$ есть хотя бы один элемент (e), значит, $Z(G) \neq \{e\}$. $\square$

Классификация p-групп.

1) $|G| = p$, тогда G циклическа порядка p.

2) $|G| = p^2$
   $|Z(G)| = 1,\ p,\ p^2$. По Следствию 1, $|Z(G)| \neq 1$.

$$|G/Z(G)| = p, 1$$

   Факторгруппа некоммутативной группы по центру не может быть циклической, откуда $|G/Z(G)| \neq p$.

   Остается один вариант $|Z(G)| = p^2,\ |G/Z(G)| = 1$.

$$G = Z(G),$$

   другими словами, G абелева. Всякая абелева группа является суммой примарных циклческих групп, в нашем случае

$$G \simeq \mathbb{Z}_{p^2} \ \ or \ \ G \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

Домашнее задание.

Задача. Классификация групп порядка p^3.

Из задачника: 58.43

Лекция 10

Решение задачи классификации групп порядка p^3

Задача. Пусть $|G| = p^3$, G не коммутативна. Найти $|Z(G)|$, количество классов сопряженности и количество элементов в каждом классе сопряженности.

Решение. Порядок центра G может принимать значения $1, p, p^2, p^3$.

Группа G не абелева, следовательно, $|Z| \neq p^3$. Центр p-группы нетривиален, поэтому $|Z| \neq 1$.
Рассмотрим порядок факторгруппы. Он может принимать 2 возможных значения (т.к. 2 значения порядка $Z(g)$ мы уже исключили).

$$|G/Z| = p^2, \ \ p$$

Если $|G/Z| = p$, то G/Z циклическая. Факторгруппа некоммутативной группы по ее центру не может быть циклической, значит, $|G/Z| \neq p$.

Остается единственная возможность $|Z| = p$, $|G/Z| = p^2$.

Таким образом, в группе G есть p одноэлементных классов сопряженности (классы сопряженности элементов из центра). Оставшиеся классы сопряженности не являются центральными.

Пусть $x \notin Z(G)$, тогда $|C(x)| = \frac{|G|}{|Z(x)|}$. Найдем $|Z(x)|$.

$|C(x)| = \frac{|G|}{|Z(x)|}$ может принимать значения $1, p, p^2, p^3$.
Поскольку $x \notin Z(G)$, $|C(x)| > 1$. Тогда $|Z(x)|$ может принимать значения $p^2, p, 1$.
$Z(x) \supset Z(G)$, т.к. элементы $Z(G)$ коммутируют со всеми элементами группы, а элементы $Z(x)$ только с элементом x. Отсюда $|Z(x)| \geq p$. Кроме того, $Z(x) \ni x$, и $x \notin Z(G)$ по предположению. Значит, $|Z(x)| > p \ \Rightarrow \ |Z(x)| = p^2$ и $|C(x)| = p$.

В каждом нецентральном классе сопряженности p элементов. Чтобы понять, сколько всего таких классов, нужно все нецентральные элементы разбить на группы по p элементов. Получим

$$\frac{p^3 - p}{p} = p^2 - 1.$$

Ответ: G состоит из p одноэлементных классов сопряженности и $p^2 - 1$ нецентралных классов сопряженности по p элементов в каждом.

Решение задачи 57.31

Задача 57.31 Найти все конечные группы G, в которых:
а) 1 класс сопряженности;
б) 2 класса сопряженности;

в) 3 класса сопряженности;

Решение.

а) Единичный элемент группы образует класс сопряженности из одного элемента - он сопряжен сам себе. Если в группе нет других классов сопряженности, значит, $G = \{e\}$.

Ответ: $G = \{e\}$

б) Единичный элемент всегда образует класс сопряженности, значит, все остальные элементы входят в другой класс сопряженности C_2.
Пусть $|G| = n$, тогда $n = 1 + a$, где $a = |C_2|$. Количество элементов в классе сопряженности делит порядок группы, поэтому $a = n - 1 \mid n$. Это возможно только если $n = 2$.

Ответ: $G \simeq \mathbb{Z}_2$

в)
$$G = \{e\} \cup C_2 \cup C_3,$$
где C_2, C_3 - два класса сопряженности. Тогда $|G| = n = 1 + a + b$, где $a = |C_2|, b = |C_3|$. При этом $a \mid n,\ b \mid n$.
Выпишем все возможности для чисел n, a, b. Без ограничения общности, $a \leq b$.

n	a	b	G
3	1	1	$G \simeq \mathbb{Z}_3$
4	1	2	не реализуется
6	2	3	$G \simeq S_3$

a, b - делители n, следовательно, $a \leq \frac{n}{2},\ b \leq \frac{n}{2}$. Они не могут быть одновременно равны $\frac{n}{2}$, значит, один из них строго меньше $\frac{n}{2}$. Если делитель меньше $\frac{n}{2}$, то он не превосходит $\frac{n}{3}$.
Можно считать, что $a \leq \frac{n}{3},\ b \leq \frac{n}{2}$. Тогда $n = a + b + 1 \leq 1 + \frac{n}{3} + \frac{n}{2} = 1 + \frac{5}{6}n$. Значит, в таблице перечислены все наборы чисел.

Если $|G| = 3$, то $G \simeq \mathbb{Z}_3$. Группа порядка 3 абелева, в ней каждый класс сопряженности состоит из 1 элемента. Эта возможность реализуется.

Если $|G| = 4$, то $G \simeq \mathbb{Z}_4$ - абелева. В ней нет классов сопряженности из двух элементов, эта возможность не реализуется.

Если $|G| = 6$, то $G \simeq S_3$. Класс сопряженности подстановки определяется цикловой структурой: id, $(i,\ j)$, $(i,\ j,\ k)$. Тождественная подстановка одна,

транспозиций 3, тройных цикла 2.

Показать, что такая группа порядка 6 - единственная можно двумя способами.

1. Воспользуемся следующим фактом: существует 2 группы порядка 6 с точностью до изоморфизма - это S_3 и $\mathbb{Z}_6$. $\mathbb{Z}_6$ абелева, поэтому не подходит. Значит, есть только одна группа порядка 6 с тремя классами сопряженности.

2. Покажем, что G со структурой $G = \{e\} \cup C_2 \cup C_3$ изоморфна S_3. Для этого придумаем действие группы G на множестве из трех элементов, которое задает гомоморфизм из G в S_3 и показать, что это изоморфизм.
Рассмотрим действие $G \curvearrowright C_3$ сопряжениями.

$$g : x \mapsto gxg^{-1}$$

$$\varphi : G \to S(C_3) \simeq S_3$$

$K = \operatorname{Ker}\varphi \triangleleft G$. $|K|$ - делитель $|G|$, т.е. может принимать значения 1, 2, 3, 6. Тогда соответствующее количество элементов в $\operatorname{Im}\varphi$ может быть равно 6, 3, 2, 1, что соответствует группам S_3, A_3, $\langle(1,\ j)\rangle$, $\{\mathrm{id}\}$.
Упражнение: покажите, что $|K| \neq 2$, $|\operatorname{Im}\varphi| \neq 2$, $|\operatorname{Im}\varphi| \neq 1$.
Останется единственный вариант $|K| = 1$, $\operatorname{Im}\varphi = S_3$.

Ответ: $G \simeq \mathbb{Z}_3$ и $G \simeq S_3$

Коммутатор и коммутант

Определение 10.29. *Пусть G - группа. Коммутатором элементов $a, b \in G$ называется произведение*

$$[a, b] = aba^{-1}b^{-1}.$$

Основное свойство коммутатора:

$$ab = [a, b] \cdot ba$$

$$ab = ba \ \Leftrightarrow\ [a, b] = e$$

Чем больше в группе неединичных коммутаторов, тем более она некоммутативна. Совокупность всех коммутаторов - это мера некоммутативности.

Определение 10.30. *Пусть G - группа. Коммутатором группы G (производной группой) называется подгруппа в группе G, порожденная всеми коммутантами*

$$[G, G] = G' = \langle [a, b] \mid a, b \in G\rangle.$$

Обратный элемент к коммутатору:

$$[a,b]^{-1} = [b,a]$$

Можно сказать, что $[G,G]$ как множество состоит из всевозможных произведений конечного количества коммутаторов элементов группы G (не добавляя, что тудп должны входить обратные коммутаторы, т.к. обратный к коммутатору - тоже коммутатор).

$$G' = \{[a_1,b_1]\cdot[a_2,b_2]\cdot\ldots\cdot[a_n,b_n] \mid a_i,b_i \in G\}$$

Отметим, что коммутант $\neq$ множество всех коммутаторов.

Домашнее задание.
Задача. Известно, что $SL_2'(\mathbb{R}) = SL_2(\mathbb{R})$. Доказать, что матрица $-E \in SL_2(\mathbb{R})$ не является коммутатором двух элементов из $SL_2(\mathbb{R})$.

Свойства коммутанта как подгруппы

1) $G' \triangleleft G$

2) G/G' абелева

3) Пусть $G \triangleright K$, G/K абелева. Тогда $K \supseteq G'$.
Другими словами, коммутант группы G - это наименьшая нормальная подгруппа, фактор по которой абелев.

Метод вычисления коммутанта
1. Вычислим достаточно много коммутаторов в группе G

$$[a_i,b_i],\ i \in I$$

и породим этими коммутаторами подгруппу

$$H = \langle [a_i,b_i] \mid i \in I\rangle \subseteq G'.$$

Получили оценку коммутатора снизу.
2. Ищем $K \triangleleft G$ такую, что G/K абелева. Например, строим гомоморфизм в абелеву группу A $\varphi : G \to A$. Тогда

$$K = \operatorname{Ker}\varphi \Rightarrow G/K \simeq \operatorname{Im}\varphi,$$

$\operatorname{Im}\varphi = A$, откуда G/K абелева. По свойству 3) коммутанта $K \supseteq G'$.
Получили оценку коммутанта сверху.
3. Если $H = K$, то $H = K = G'$. Иначе нужно увеличить число порождающих H или построить другой гомоморфизм φ с меньшим ядром.

Известные коммутанты

1) $S'_n = A_n$
Покажем это с помощью метода, описанного выше.
1. Вычислим $[(i,\ j)(k,\ l)]$:
1. Если транпозиции независимы, то $[(i,\ j)(k,\ l)] = 1$;
2. Пусть транспозиции зависимы

$$[(i,\ j)(j,\ k)] = (i,\ j)(j,\ k)(i,\ j)^{-1}(j,\ k)^{-1} = (i,\ j)(j,\ k)(i,\ j)(j,\ k) = (i,\ j,\ k)^2 = (i,\ k,\ j)$$

В силу произвольности i, j, k можем получить любой тройной цикл. Тройные циклы порождают группу A_n.
Оценка снизу: $S'_n \supset A_n = H$.
2. Возьмем гомоморфизм $\varphi = \operatorname{sgn} : S_n \to \{\pm 1\}$.

$$K = \operatorname{Ker} \operatorname{sgn} = A_n \supseteq S'_n$$

3. $H = K = A_n = S'_n$.

2) $A'_n = A_n,\ n \geq 5$
$A'_4 = V_4$
$A'_n = \{\mathrm{id}\},\ n \leq 3$

3) $GL'_n(K) = SL_n(K)$, кроме случая $n = 2, |K| = 2$;
$SL'_n(K) = SL_n(K)$, кроме случая $n = 2,\ |K| = 2$ или 3.

Решение задач на вычисление коммутантов групп

Задача. Вычислить коммутант группы

$$G = \{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix},\ a, b, c \in \mathbb{R}, c \neq 0 \}$$

Решение. Сначала определим, как в группе G устроено умножение.

$$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix} \begin{pmatrix} 1 & a' & 0 \\ 0 & 1 & 0 \\ 0 & b' & c' \end{pmatrix} = \begin{pmatrix} 1 & a + a' & 0 \\ 0 & 1 & 0 \\ 0 & b + cb' & cc' \end{pmatrix} \tag{10.1}$$

Получили матрицу такого же вида. Следовательно, множество таких матриц замкнуто относительно умножения. Проверим замкнутость относительно взятия обратного элемента.

$$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & 0 \\ 0 & -\frac{b}{c} & \frac{1}{c} \end{pmatrix}$$

Найдем оценку коммутанта сверху. Нужно придумать гомоморфизм из группы G в некоторую абелеву группу. Коммутативность умножения нарушается в элементе $b + cb'$ матрицы (10.1). В таком случае φ можно задать следующим образом

$$\varphi \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix} = c$$

Тогда $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$. Заметим, что $\varphi(x) = \det x$. $\operatorname{Ker}\varphi$ - матрицы с $c = 1$. Из этого гомоморфизма можно сделать новый с меньшим ядром

$$\varphi \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & b & c \end{pmatrix} = (c, a)$$

$$\varphi : G \to \mathbb{R}^{\times} \times \mathbb{R}$$

Группа $\mathbb{R}^{\times} \times \mathbb{R}$ абелева.

$$K = \operatorname{Ker}\varphi = \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & b & 1 \end{pmatrix}, \quad b \in \mathbb{R}\} \tag{10.2}$$

Получим теперь оценку снизу. Запишем коммутатор двух матриц и подберем параметры так, чтобы полученный коммутатор порождал группу, равную K.

$$[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & z \end{pmatrix}] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & z \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{z} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & z \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -x & \frac{1}{z} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x - zx & 1 \end{pmatrix}$$

$x - zx = (1 - z)x$, задача - подобрать x и z так, чтобы $(1 - z)x = b$. Пусть, например, $z = 2$ (или любое другое ненулевое число), тогда $x = \frac{b}{1-z} = -b$ находится однозначно.

Получили, что любой элемент K является коммутатором двух матриц из G. Отсюда $G' \supseteq K$.

Итак, $G' = K$.

Ответ: группа (10.2)

Домашнее задание.

Задача. Найти коммутант группы

$$G = \{A = \begin{pmatrix} 1 & 0 & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix}, \quad \det A \neq 0\}$$

Кратные коммутанты. Разрешимые группы

Кратные коммутанты:

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$$

$$G^{(0)} = G$$

Производный ряд: $G \triangleright G' \triangleright G'' \triangleright \ldots \triangleright G^{(k-1)} \triangleright G^{(k)} \triangleright \ldots$

Эта цепочка может закончиться на некотором элементе (например, $GL'_n(K) = SL_n(K)$, $SL'_n(K) = SL_n(K)$) или дойти до коммутатора $\{e\}$.

Определение 10.31. *Группа G разрешима, если $\exists n: \ G^{(n)} = \{e\}$. Наименьшее такое n называется ступенью разрешимости.*

Пример. Разрешимые группы ступени 1 - это абелевы группы.

Произвольные разрешимые группы - это в некотором смысле следующий по сложности класс после абелевых групп.
Закон умножения в разрешимой группе можно исследовать по этажам: сначала исследуем умножение в группе G по модулю первого коммутанта (группа G/G' коммутативна), т.е. с точностью до поправок из первого коммутанта умножение в G коммутативно. Далее можно рассматривать умножение в самом коммутанте и факторгруппу G'/G'' и т.д.
Если мы в итоге дойдем до $G^{(k)} = \{e\}$, то получится, что группа G составлена из коммутативных этажей $G^{(i)}/G^{(i+1)}$.

Свойства разрешимых групп

1) Пусть G разрешима, $G \supseteq H$ - подгруппа. Тогда H тоже разрешима.

   Доказательство. Действительно, по индукции можно показать, что $H^{(k)} \supseteq G^{(k)}$. Тогда если $G^{(k)} = \{e\}$, то и $H^{(k)} = \{e\}$. □

2) Пусть G разрешима, $G \triangleright H$. Тогда G/H тоже разрешима.

   Доказательство. Существует канонический гомоморфизм $\pi : G \to G/H$. При гомоморфизме коммутант отображается на коммутант образа, потому что коммутаторы отображаются в коммутаторы образов.
   Если теперь применить π к G' и взять коммутант G'', то G'' отображается на второй коммутант факторгруппы и т.д.

   Образом при канонической проекции k-того коммутанта группы G является k-тый коммутант факторгруппы.

   Таким образом, если ряд коммутантов группы G дойдет до $\{e\}$, то и ряд их образов тоже. □

3) Критерий разрешимости.
   Пусть $G \triangleright H$, причем H и G/H разрешимы. Тогда G разрешима.

Доказательство. Идея. Возьмем кратные коммутанты группы G и рассмотрим их образы при канонической проекции π. Это будут кратные коммутанты факторгруппы.
Поскольку дано, что факторгруппа разрешима, то на каком-то шаге образ кратного коммутанта при π будет тривиален. Тогда этот кратный коммутант содержится в ядре π, т.е. в подгруппе H.

Как только k-тый кратный коммутант попал в подгруппу H, можно воспользоваться разрешимостью подгруппы H. □

Примеры разрешимых групп

1) S_n и A_n разрешимы при $n \leq 4$ и неразрешима при $n > 4$.

Доказательство.

$$S_n' = A_n \quad \forall n\mathbb{N}$$

$$A_n' = \begin{cases} A_n, & n \geq 5 \\ A_4' = V_4 - \text{абелева} \\ A_n' = \{e\}, & n \leq 3 \end{cases}$$

□

2) D_n разрешима.

Доказательство. Воспользуемся критерием разрешимости.
Группа поворотов $R_n \lhd D_n$ - циклическая группа, порожденная элементом $\langle r_{\frac{2\pi}{n}} \rangle_n$.

$$R_n \simeq \mathbb{Z}_{\ltimes}$$

$\mathbb{Z}_{\ltimes}$ абелева, следовательно, разрешима.

$|D_n/R_n| = 2 \;\Rightarrow\; D_n/R_n \simeq \mathbb{Z}_{\not\ltimes}$, т.к. группа порядка 2 единственна с точностью до изоморфизма. $\mathbb{Z}_{\not\ltimes}$ разрешима, поскольку абелева, значит, все условия критерия разрешимости выполнены и D_n разрешима. □

Это простейший пример некоммутативной разрешимой группы, ступень разрешимости D_n равна 2.

Действительно, R_n - нормальная подгруппа, фактор по которой абелев. Значит, $D_n' \subseteq R_n$, откуда ступень разрешимости $D_n \leq 2$. При этом D_n не коммутативна, поэтому ступень разрешимости > 1.

3) $GL_n(K)$ и $SL_n(K)$ неразрешимы, кроме случаев $n = 2,\ |K| \leq 3$.

Доказательство. $GL_n'(K) = SL_n(K)$, кроме случая $n = 2, |K| = 2$;
$SL_n'(K) = SL_n(K)$, кроме случая $n = 2,\ |K| = 2$ или 3. □

Домашнее задание.

Задача. Доказать, что $GL_2(\mathbb{Z}_2) \simeq S_3$ (а группа S_3 разрешима).

Из задачника: 62.20, 62.19, 62.7 г), 62.8 б), 58.37 (из нее следует, что $GL_2(\mathbb{Z}_3)$ разрешима).

Лекция 11

Силовские подгруппы

Определение 11.32. *Пусть $|G| = n$ и p - простое число такое, что $n = p^k \cdot m$, p не делит m.*
Тогда силовская p-подгруппа группы G - это подгруппа порядка p^k.

Теоремы Силова

1. $\forall p$ - простого существует силовская p-подгруппа P в группе G.

2. Все силовские p-подгруппы сопряжены при данном p в данной группе G.

3. Любая p-подгруппа $H \subseteq G$ содержится в некоторой силовской p-подгруппе P.

4. Количество силовских p-подгрупп $N_p(G) \equiv 1 \pmod p$.

5. $N_p(G) = \frac{|G|}{|N_G(P)|}$, где P - какая-то силовская p-подгруппа, $N_G(P)$ - ее нормализатор. $N_p(G)$ делит m.

6. $P \lhd G \;\Leftrightarrow\; N_p(G) = 1$.

Определение 11.33. *Пусть $H \subseteq G$ - подгруппа, тогда $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ - ее нормализатор. Это подгруппа в G, как и любой стабилизатор.*

Равенство $gHg^{-1} = H$ заведомо выполнено для $g \in H$, поэтому $N_G(H) \supseteq H$.
$N_G(H) = G \;\Leftrightarrow\; H \lhd G$.

Формула 5. вытекает из того, что все силовские p-подгруппы сопряжены, т.е. они образуют одну орбиту при действии на множестве подгрупп сопряжениями. Тогда количество элементов в орбите можно посчитать как порядок группы, деленный на порядок стабилизатора.

Отсюда вытекает, что $N_G(H)$ делит m, потому что в знаменателе формулы 5. стоит порядок нормализатора, а нормализатор содержит подгруппу P. Т.е. в знаменателе будет присутствовать множитель p^k.

Свойство 6. сразу следует из 5., т.к. нормальность подгруппы означает, что ее нормализатор совпадает со всей группй и имеет порядок n.

Решение задач на нахождение силовских подгрупп

Задача 69.3 б) + 59.4 б) Найти все силовские подгруппы в группе $G = A_4$. Найти все сопрягающие элементы, с помощью которых можно одну силовскую подгруппу перевести в другую.

Решение.

$$|A_4| = 12 = 2^2 \cdot 3$$

1. $p = 2$. Любая силовская 2-подгруппа имеет порядок $|P| = 4$.

Кроме того, по теореме Силова 4. $N_2 \equiv 1 \pmod 2$ - нечетное число. По теореме Силова 5. N_2 делит число $m = 3$. Следовательно, N_2 может быть либо 1, либо 3.

Исходя из общих рассуждений, однозначно установить количество силовских 2-подгрупп нельзя, найдем эти подгруппы явно .

$$A_4 \ni (i,\ j,\ k),\ \mathrm{id},\ (i,\ j)(k,\ l)$$

Какие из этих подстановок могут входить в группу порядка 4? У тройного цикла порядок 3, поэтому он не может входить в группу порядка 4. У произведения независимых транспозиций и тождественной подстановки порядки равны, соответственно, 2 и 1, они могут входить в P.

Всего есть 3 пары независимых транспозиций: $(1,\ 2)(3,\ 4), (1,\ 3)(2,\ 4), (1,\ 4)(2,\ 3)$. Значит, P содержит все эти произведения транспозиций и $\{\mathrm{id}\}$.

Итак, существует единственная силовская 2-подгруппа

$$P = \{\mathrm{id}, (1,\ 2)(3,\ 4), (1,\ 3)(2,\ 4), (1,\ 4)(2,\ 3)\} \simeq V_4.$$

Заметим, что подгруппа $P \simeq V_4$ нормальна и единственно, что подтверждает теорему Силова 6.

2. $p = 3$. Любая силовская 3-подгруппа имеет порядок $|P| = 3$.

По теореме Силова 4., $N_3 \equiv 1 \pmod 3$. По теореме Силова 5. N_3 делит $m = 4$. Итак, есть следующие варианты: $1, 4$.

Определим, как могут быть устроены силовские 3-подгруппы. Сразу можно выписать следующую группу порядка 3:

$$P_1 = \{\mathrm{id}, (1,\ 2,\ 3), (1,\ 2,\ 3)^{-1} = (3,\ 2,\ 1)\} = \langle (1,\ 2,\ 3)\rangle_3$$

Такие же группы можно породить и другими циклами.

$$P_2 = \{\mathrm{id}, (1,\ 2,\ 4), (1,\ 2,\ 4)^{-1} = (4,\ 2,\ 1)\} = \langle (1,\ 2,\ 4)\rangle_3$$

$$P_3 = \{\mathrm{id}, (1,\ 3,\ 4), (1,\ 3,\ 4)^{-1} = (4,\ 3,\ 1)\} = \langle (1,\ 3,\ 4)\rangle_3$$

$$P_4 = \{\mathrm{id}, (2,\ 3,\ 4), (2,\ 3,\ 4)^{-1} = (4,\ 3,\ 2)\} = \langle (2,\ 3,\ 4)\rangle_3$$

Укажем сопрягяющие подстановки. Отметим, что эти подстановки должны быть четными.

$$P_1 \to P_2 \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$P_2 \to P_3 \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$P_3 \to P_4 \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$P_4 \to P_1 \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

Задача 59.13 $G = SL_2(\mathbb{Z}_p)$, ясно, что эта группа конечна.

$$G \supset P = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \ \ a \in \mathbb{Z}_p\}$$

а) Доказать, чтоP - силовская p-подгруппа группы G;
б) Найти нормализатор $N_G(P)$;
в) Найти количество всех силовских p-подгрупп в G.

Решение.

а) $|P| = p$, т.к. это число различных значений a. Чтобы показать, что это силовская p-подгруппа, найдем $|G|$.

Сначала найдем $|GL_2(\mathbb{Z}_p)|$.
Невырожденная матрица 2×2 состоит из линейно независимых строк. Первой может стоять любая ненулевая строка, таких строк $p^2 - 1$. Вторая строка должна быть не пропорциональна первой строке, таких возможностей $p^2 - p$, потому что коэффициентов пропорциональности p штук.

$$|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$$

Теперь найдем $|SL_2(\mathbb{Z}_p)|$.
Существует гомоморфизм $\det : GL_2(\mathbb{Z}_p) \to \mathbb{Z}_p^\times$, $\mathrm{Im}(\det) = \mathbb{Z}_p^\times$, $\ker\det = SL_2(\mathbb{Z}_p)$. Тогда $SL_2(\mathbb{Z}_p) \triangleleft GL_2(\mathbb{Z}_p)$ как ядро гомоморфизма.

$$GL_2(\mathbb{Z}_p)/SL_2(\mathbb{Z}_p) \simeq \mathbb{Z}_p^\times$$

$$|SL_2(\mathbb{Z}_p)| = \frac{|GL_2(\mathbb{Z}_p)|}{|\mathbb{Z}_p^\times|} = \frac{(p^2-1)(p^2-p)}{p-1} = (p^2-1)p$$

Множитель $p^2 - 1$ не делится на p, поэтому p входит в разложение группы в максимальной степени 1. Значит, P - силовская подгруппа.

б) Пусть $N_G(P) \supseteq H$. Тогда количество силовских p-подгрупп $N_p(G) \leq \frac{|G|}{|H|}$, поскольку

$$N_p(G) = \frac{|G|}{|N_G(P)|}.$$

Т.е. оценка для нормализатора снизу дает оценку для количества силовских подгрупп сверху и наоборот.

$N_G(P) \supseteq P$, кроме того, диагональные матрицы тоже сохраняют матрицы вида P

$$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} = \begin{pmatrix} 1 & t_1 a t_2^{-1} \\ 0 & 1 \end{pmatrix}.$$

В $N_G(P)$ лежат унитреугольные и диагональные матрицы, значит, лежат и их произведения.

$$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t_1 & t_1 a \\ 0 & t_2 \end{pmatrix} \quad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} = \begin{pmatrix} t_1 & t_2 a \\ 0 & t_2 \end{pmatrix}$$

Эти произведения - верхнетреугольные матрицы с определителем 1.

$$N_G(P) \supseteq H = \{\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}, \ \ x \in \mathbb{Z}_p^\times, \ y \in \mathbb{Z}_p\}$$

Тогда получим следующую оценку

$$N_p(G) \leq \frac{(p^2-1)p}{(p-1)p} = p+1.$$

$N_p(G) \equiv 1 \pmod p$, тогда $N_p(G) = 1$ или $N_p(G) = p+1$.

Если есть еще хотя бы одна силовская p-подгруппа, кроме P, то $N_p(G) = p+1$. Это может быть, например, подгруппа нижнетреугольных матриц

$$Q = \{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \ \ a \in \mathbb{Z}_p\}.$$

Итак, $N_p(G) = p+1$, тогда

$$N_p(G) = \frac{(p^2-1)p}{(p-1)p} = p+1.$$

и $|N_G(P)| = (p-1)p$. Отсюда $N_G(P) = H$.

в) Из п. б) следует $N_p(G) = p+1$.

Домашнее задание: 59.13 г),д),е).

Силовские подгруппы прямого произведения групп

Пусть $G = A \times B$ и известно, как устроены силовские подгруппы в группах A и B.
Вопрос: как описать силовские подгруппы в группе G?

$$|G| = n = k \cdot l, \ \ k = |A|, \ l = |B|.$$

Пусть $k = p^i \cdot r, \;\; l = p^j \cdot s, \;\; r, s$ не делят p, тогда

$$n = p^{i+j} rs.$$

Если $P \subset G$ - силовская, то $|P| = p^{i+j}$.
Теперь найдем общий вид таких силовских p-подгрупп. Пусть $P = P_1 \times P_2$, где P_1 - силовская p-подгруппа в A, P_2 - силовская p-подгруппа в B.

$$|P_1| = p^i, \;\; |P_2| = p^j \;\Rightarrow\; |P| = p^{i+j}$$

Все ли силовские подгруппы в G устроены как прямые произведения силовских подгрупп в A и B?
Любая другая силовская p-подгруппа сопряжена подгруппе $P = P_1 \times P_2$, т.е. имеет вид

$$gPg^{-1} = abP_1 \times P_2 b^{-1} a^{-1} = \underbrace{aP_1a^{-1}}_{\text{силовская в } A} \times \underbrace{bP_2b^{-1}}_{\text{силовская в } B}$$

Тем самым, любая силовская p-подгруппа в G является произведением силовской p-подгруппы в A и силовской p-подгруппы в B.

Домашнее задание: найти все силовские подгруппы в $G = D_3 \times A_4$.

Арифметика конечных групп

Попробуем описать свойства конечной группы, если известен только ее порядок.

Напоминание:

- Если $|G| = p$, то G циклическая порядка p.
- Если $|G| = p^2$, то G абелева.
- Если $|G| = p^n$, то G разрешима.

Задача 59.22 б) $|G| = 80$. Доказать, что G не является простой, т.е. G не имеет нормальных подгрупп, кроме $\{e\}, G$.

Доказательство. Чтобы доказать, что G не проста, нужно предъявить нетривиальную нормальную подгруппу.

Поскольку известен только порядок группы, то можно утверждать только существование силовских p-подгрупп. Силовская p-подгруппа нормальна $\Leftrightarrow$ она единственна.

$$|G| = 80 = 2^4 \cdot 5$$

1. $p = 2,\ |P| = 16$. Согласно теоремам Силова,

$$N_2 \mid 5 \ \Rightarrow\ N_2 = 1,\ 5,$$

$$N_2 \equiv 1 \pmod 2 \ \Rightarrow\ N_2 \text{ нечетно.}$$

2. $p = 5,\ |P| = 5$. Согласно теоремам Силова,

$$N_5 \mid 16 \ \Rightarrow\ N_5 = 1,\ 2,\ 4,\ 8,\ 16,$$

$$N_5 \equiv 1 \pmod 5 \ \Rightarrow\ N_5 = 1,\ 16.$$

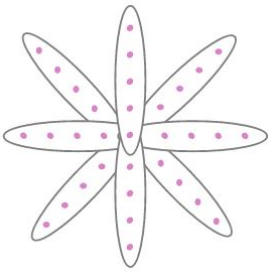
Нужно показать, что хотя бы в одном случае $N_p = 1$, т.е. исключить случай $N_5 = 16, N_2 = 5$.

1) Пусть $N_5 = 16$ и $P_1, \ldots, P_{16}$ - все силовские 5-подгруппы в G.

$$|P_i| = 5 \ \Rightarrow\ |P_1 \cup P_2 \cup \ldots \cup P_{16}| = 16 \cdot 4 + 1 = 65,$$

В с.д., $P_i \cap P_j = \{e\}$ в силу того, что пересечение двух подгрупп тоже является подгруппой в G, а также в P_i и в P_j. Порядок подгруппы делит порядок группы, поэтому $|P_i \cap P_j| = 1, 5$. Если $|P_i \cap P_j| = 5$, то $P_i = P_j$, поэтому $P_i \cap P_j = \{e\},\ i \neq j$.

Итак, пересечение 5-подгрупп выглядит следующим образом



Остюда следует, что

$$|P_1 \cup P_2 \cup \ldots \cup P_{16}| = 16 \cdot 4 + 1 = 65$$

Пусть теперь Q - силовская 2-подгруппа, P_i - силовская 5-подгруппа. Тогда $Q \cap P_i = \{e\}$.
Поскольку

$$|P_1 \cup P_2 \cup \ldots \cup P_{16} \cup Q| = 16 \cdot 4 + 1 \cdot 15 + 1 = 80,$$

силовская 2-подгруппа может быть только одна.

Значит, $N_2 = 1$ и существует нормальная силовская 2-подгруппа.

2) Если $N_5 \neq 16$, то $N_5 = 1$, и тогда существует нормальная силовская 5-подгруппа.

$\square$

Задача 62.18 б) $|G| = 12$. Доказать, что G разрешима.

Доказательство. Используем критерий разрешимости: Пусть $G \triangleright H$, причем H и G/H разрешимы. Тогда G разрешима.

Хотим найти разрешимую нормальную подгруппу, фактор по которой разрешим.

$$|G| = 12 = 2^2 \cdot 3$$

1) $p = 2,\ |P| = 4.$

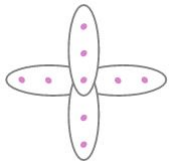
$$N_2 \mid m = 3 \ \Rightarrow\ N_2 = 1,\ 3,$$
$$N_2 \equiv 1 \pmod 2 \ \Rightarrow\ N_2 = 1,\ 3.$$

2) $p = 3,\ |Q| = 3.$

$$N_3 \mid m = 4 \ \Rightarrow\ N_3 = 1,\ 2,\ 4,$$
$$N_3 \equiv 1 \pmod 3 \ \Rightarrow\ N_3 = 1,\ 4.$$

Нужно показать, что существует единственная силовская 2-подгруппа или 3-подгруппа, она будет нормальной. Покажем, что вариант $N_2 = 3,\ N_3 = 4$ невозможен.

1) Пусть $N_3 = 4$ и $Q_1,\ Q_2,\ Q_3,\ Q_4$ - все силовские 3-подгруппы. Из представления их пересечения



следует, что

$$|Q_1 \cup Q_2 \cup Q_3 \cup Q_4| = 2 \cdot 4 + 1 = 9.$$

Остается 3 элемента, силовская 2-подгруппа имеет порядок 4 и тоже содержит $\{e\}$. Если P - силовская 2-подгруппа, то $P \cap Q_i = \{e\}$ и силовская 2-подгруппа может быть только одна.

Итак, $N_2 = 1$, существует нормальная силовская 2-подгруппа $P \triangleleft G$.

$$P \simeq \mathbb{Z}_4 - \text{ абелева, разрешима}$$

$$|G/Q| = \frac{|G|}{|Q|} = \frac{12}{4} = 3 \ \Rightarrow \ |G/Q| \simeq \mathbb{Z}_3 - \text{ абелева, разрешима}$$

Все условия критерия разрешимоти выполнены.

2) Если $N_3 \neq 4$, то $N_3 = 1$, существует нормальная силовская 3-подгруппа $Q \triangleleft G$.

$$Q \simeq \mathbb{Z}_3 - \text{ абелева, разрешима}$$

$$|G/Q| = \frac{|G|}{|Q|} = \frac{12}{3} = 4 \ \Rightarrow \ |G/Q| \simeq \mathbb{Z}_4 - \text{ абелева, разрешима}$$

Все условия критерия разрешимоти выполнены.

□

Домашнее задание: 59.22 а),в), 62.18 в),г),д),е)*.

Лекция 12

Разбор домашнего задания

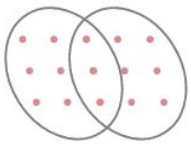
Задача 59.22 а) Доказать, что не существует простых групп порядка 36. (Группа проста, если в ней нет нетривиальных нормальных подгрупп.)

Доказательство. О группе G известен только ее порядок, поэтому нормальную подгруппу будем искать среди силовских подгрупп.

$$|G| = 36 = 2^2 \cdot 3^2$$

- $p = 2,\ |P| = 4.$
$$N_2 \mid m = 9 \ \Rightarrow\ N_2 = 1,\ 3,\ 9,$$
$$N_2 \equiv 1 \pmod 2 \ \Rightarrow\ N_2 = 1,\ 3,\ 9.$$
- $p = 3,\ |P| = 9.$
$$N_2 \mid m = 4 \ \Rightarrow\ N_2 = 1,\ 2,\ 4,$$
$$N_2 \equiv 1 \pmod 3 \ \Rightarrow\ N_2 = 1,\ 4.$$

Здесь метод решения подобных задач с прошлого семинара не работат, потому что 2 подгруппы порядка 9 могут пересекаться не только по единице. Например,



Все силовские подгруппы данного порядка сопряжены друг другу, т.е. $G \curvearrowright \{P_1,\ P_2,\ P_3,\ P_4\}$ сопряжениями, где $P_1,\ P_2,\ P_3,\ P_4$ - все силовские 3-подгруппы. Тогда существует гомоморфизм

$$\varphi : G \to S(P_1,\ P_2,\ P_3,\ P_4) = S_4.$$

Если бы φ был тривиальным, т.е. отображал все элементы G в e, это бы означало, что при всех сопряжениях каждая из групп $P_1,\ P_2,\ P_3,\ P_4$ остается на месте. Т.е. каждая из них была бы нормальной и, следовательно, единственной. Однако для любых P_i, P_j существует сопряжение, которое P_i переводит в P_j, откуда φ не может быть тривиальным.

$$\operatorname{Im}\varphi \neq \{\mathrm{id}\}$$

Кроме того, $\operatorname{Ker}\varphi \triangleleft G$. $\operatorname{Ker}\varphi \neq G$, т.к. $\operatorname{Im}\varphi \neq \{\mathrm{id}\}$. Если $\operatorname{Ker}\varphi = \{e\}$, то φ - инъекция, чего быть не может, т.к. $36 = |G| > |S_4| = 24$, значит, $\operatorname{Ker}\varphi \neq \{e\}$.

Итак, $\operatorname{Ker}\varphi$ - нетривиальная нормальная подгруппа в G. $\square$

Задача 59.24 Найти число элементов порядка 7 в простой группе G порядка 168.

Решение. Каждый элемент порядка 7 образует циклическую подгруппу порядка 7, которая является силовской.

$$168 = 7 \cdot 2^3 \cdot 3$$

$$P = \langle g \rangle_7 = \{e, \underbrace{g,\ g^2,\ g^3,\ g^4,\ g^5,\ g^6}_{\text{имеют порядок 7}}\},\ \ o(g) = 7.$$

На прошлом семинаре было показано, что две группы простого порядка могут либо совпадать, либо пересекаться по единице. Значит, если P_1, P_2 - две подгруппы порядк 7, то $P_1 \cap P_2 = \{e\}$.
Т.е. во всех подгруппах порядка 7 все элементы, кроме единичного, разные.

Таким образом, чтобы посчитать количество элементов порядка 7, нужно найти количество силовских 7-подгрупп и умножить на 6.

$$N_7 \mid m = 24 \ \Rightarrow\ N_7 = 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24,$$
$$N_7 \equiv 1 \pmod 7 \ \Rightarrow\ N_7 = 1,\ 8.$$

Если $N_7 = 1$, то единственная силовская 7-подгруппа будет нормальна в G, но по условию G проста, откуда $N_7 \neq 1$.
Остается вариант $N_7 = 8$, тогда число элементов порядка 7 равно $6 \cdot 8 = 48$.

Ответ: 48

Решение задач на арифметику конечных групп

Задача. $|G| = 455$, показать, что G коммутативна.

Доказательство. Найдем силовские подгруппы в G.

$$|G| = 5 \cdot 7 \cdot 13$$

- $p = 5,\ |P_5| = 5.$

$$N_5 \mid m = 7 \cdot 13 \ \Rightarrow\ N_5 = 1,\ 7,\ 13,\ 91,$$
$$N_5 \equiv 1 \pmod 5 \ \Rightarrow\ N_5 = 1,\ 91.$$

  Как группы простого порядка,

$$P_5 \simeq \mathbb{Z}_5$$

- $p = 7,\ |P_7| = 7.$

$$N_7 \mid m = 5 \cdot 13 \ \Rightarrow\ N_7 = 1,\ 5,\ 13,\ 65,$$
$$N_7 \equiv 1 \pmod 7 \ \Rightarrow\ N_7 = 1.$$

  Существует единственная силовская 7-подгруппа $P_7 \lhd G$.

$$P_7 \simeq \mathbb{Z}_7$$

- $p = 13,\ |P_{13}| = 13.$

$$N_{13} \mid m = 5 \cdot 7 \ \Rightarrow\ N_{13} = 1,\ 5,\ 7,\ 35,$$

$$N_{13} \equiv 1 \pmod{13} \ \Rightarrow\ N_{13} = 1.$$

Существует единственная силовская 13-подгруппа $P_{13} \lhd G$.

$$P_{13} \simeq \mathbb{Z}_{13}$$

$P_7 \cap P_{13} = \{e\}$, т.к. $P_7 \cap P_{13}$ - подгруппа в P_7 и в P_{13}, а значит $|P_7 \cap P_{13}|$ делит $|P_7|$ и $|P_{13}|$.
Тогда можно рассматривать прямое произведение

$$H = P_7 \times P_{13} \lhd G.$$

Подгруппа H нормальна в G, т.к. при сопряжении любым элементом из G группы P_7 и P_{13} остаются на месте, а значит и произведения их элементов не меняются.

$$|H| = 91$$

$|G| = 5|H|$. Проверим, что H и P_5 образуют полупрямое произведение:
$|H \cap P_5|$ делит $|H| = 91$ и $|P_5| = 5$. Отсюда $|H \cap P_5| = 1,\ \ H \cap P_5 = \{e\}$,
$H \lhd G$.

$$H \leftthreetimes P_5 \subseteq G$$

$$455 = 91 \cdot 5 = |H \leftthreetimes P_5| = |G| = 455 \ \Rightarrow\ G = H \leftthreetimes P_5$$

Если бы полупрямое произведение $H \leftthreetimes P_5$ было прямым, то мы получили бы разложение группы G в произведение циклических подгрупп - ответ на вопрос задачи. Чтобы доказать, что $H \leftthreetimes P_5 = H \times P_5$, нужно показать, что H и P_5 коммутируют.

Поскольку H является прямым произведением групп $P_7 \times P_{13}$, достаточно показать, что все элементы из P_7 и все элементы из P_{13} коммутируют с элементами из P_5.

1) $P_5 \cap P_7 = \{e\},\ \ P_7 \lhd G$, следовательно, они образуют полупрямое произведение

$$P_7 \leftthreetimes P_5 = S.$$

$$|S| = 35 = 5 \cdot 7$$

В S есть силовские 5-подгруппы и силовские 7-подгруппы, причем $P_7 \lhd S$ единственна.

$$N_5 \mid m = 7 \ \Rightarrow\ N_5 = 1,\ 7$$

$$N_5 \equiv 1 \pmod{5} \ \Rightarrow\ N_5 = 1.$$

Силовская 5-подгруппа единственна, следовательно, нормальна в S. Тогда

$$P_7 \leftthreetimes P_5 = P_7 \times P_5 \simeq \mathbb{Z}_5 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{35}.$$

$S \simeq \mathbb{Z}_{35}$ абелева.
P_5 и P_7 лежат внутри абелевой группы S, следовательно, коммутируют между собой.

2) Аналогично показывается, что P_5 и P_{13} коммутируют.

$$P_{13} \leftthreetimes P_5 = S.$$

$$|S| = 91 = 13 \cdot 7$$

В S есть силовские 5-подгруппы и силовские 13-подгруппы, причем $P_{13} \triangleleft S$ единственна.

$$N_5 \mid m = 13 \;\Rightarrow\; N_5 = 1,\ 13$$

$$N_5 \equiv 1 \pmod 5 \;\Rightarrow\; N_5 = 1.$$

Силовская 5-подгруппа нормальна в S. Тогда

$$P_{13} \leftthreetimes P_5 = P_{13} \times P_5 \simeq \mathbb{Z}_5 \times \mathbb{Z}_{13} \simeq \mathbb{Z}_{65}.$$

$S \simeq \mathbb{Z}_{65}$ абелева.
P_5 и P_{13} лежат внутри абелевой группы S.

Отсюда

$$G = H \times P_5 = P_7 \times P_{13} \times P_5 \simeq \mathbb{Z}_7 \times \mathbb{Z}_{13} \times \mathbb{Z}_5.$$

Группа G является прямым произведением абелевых групп, поэтому G коммутативна.
Более того, существует только одна группа порядка 455 с точностью до изоморфизма, т.к. цикловая структура определена однозначно.

$$G \simeq \mathbb{Z}_{455}$$

□

Домашнее задание: 59.20 в), г).

Теория представлений групп

Определение 12.34. *Линейное представление группы G в векторном пространстве V над полем K - это гомоморфизм*

$$\mathcal{R} : G \to GL(V),$$

где $GL(V)$ - полная линейная группа, группа всех невырожденных линейных операторов на V.

Будем рассматривать, в основном, конечномерные линейные представления, т.е. такие, что V конечномерно. Если V конечномерно, то в нем можно выбрать базис, что позволяет задать каждый линейный оператор своей матрицей. Тогда группу невырожденных линейных операторов можно отождествить с группой невырожденных матриц.

$$GL(V) \simeq GL_n(K)$$

Определение 12.35. *Матричное представление - гомоморфизм*

$$\mathrm{R} : G \to GL_n(K).$$

Переход от линейного представления к матричному и наоборот задается выбором базиса в векторном пространстве V.

Примеры.

1. $G = S_n, \;\; V = K^n$.

$$\mathcal{R} : S_n \to GL(K^n)$$

Чтобы задать линейный оператор в конечномерном векторном пространстве, нужно задать образы базисных векторов.

$$\mathcal{R}(\sigma)e_i = e_{\sigma(i)}$$

Линейные операторы, соответствующие перестановкам, переставляют базисные векторы. Ясно, что композиция перестановок соотвествует произведению линейных оперторов, так что $\mathcal{R}$ - гомоморфизм.

$$\mathcal{R}(\sigma)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$$

Действительно,

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1e_1 + x_2e_2 + \ldots + x_ne_n \mapsto x_1e_{\sigma(1)} + x_2e_{\sigma(2)} + \ldots + x_ne_{\sigma(n)} = \sum_{j=1}^{n} x_{\sigma^{-1}(j)}e_j$$

Такое представление $\mathcal{R}$ называется мономиальным.

2. $G \curvearrowright X, \quad V = \mathcal{F}(X, K)$ - пространство всех функций на множестве X со значениями в поле K.

$$\mathcal{R} : G \to GL(V)$$

Т.е. каждому элементы группы $g \in G$ сопоставим линейный оператор $\mathcal{R}(g)$, который действует в пространстве функций $\mathcal{R}(g)f, \;\; f \in \mathcal{F}$. Пусть

$$\big[\mathcal{R}(g)f\big](x) = f(g \cdot x), \;\; \forall f \in \mathcal{F}$$

Рассмотрим

$$\mathcal{R}(g')\big(\underbrace{\mathcal{R}(g)f}_{h}\big)(x) = h(g' \cdot x) = \big[\mathcal{R}(g)f\big](g' \cdot x) = f(gg' \cdot x)$$

при этом

$$\big[\mathcal{R}(g \cdot g')f\big](x) = f(g'g \cdot x),$$

т.е. нарушается правило гомоморфизма.
Корректно введенное представление будет таким

$$\big[\mathcal{R}(g)f\big](x) = f(g^{-1} \cdot x).$$

Решение задач на представления групп

Задача 69.8 $G = (\mathbb{R}, +), \quad V = \mathcal{F}(\mathbb{R}, \mathbb{R})$

$$G = (\mathbb{R}, +) \curvearrowright X = \mathbb{R} : t \cdot x = x + t$$

Это действие сдвигами. Оно задает линейное представление G в пространстве функций $\mathcal{F}$, которое действует на аргумент, сдвигая его в обратном направлении.

Рассмотрим подпространство $V \supset U = \langle \sin, \cos \rangle$.

Доказать, что U является инвариантным подпространством и задать $\mathcal{R}|_U$ матрицами в каком-либо базисе U.

Определение 12.36. *Подпространство $U \subset V$ называется инвариантным относительно представления $\mathcal{R}$, если*

$$\forall g \in G \;\; \mathcal{R}(g)U \subseteq U.$$

Тогда определено ограничение представления $\mathcal{R}$ на подпространство U - это гомоморфизм

$$\mathcal{R}|_U : G \to GL(U).$$

Каждый оператор $\mathcal{R}(g)$ на всем пространстве V при ограничении индуцирует оператор на U, поскольку он сохраняет U. Индуцированный оператор тоже обратим, т.к. у оператора $\mathcal{R}(g)$ есть обратный оператор $\mathcal{R}(g^{-1})$ в пространстве V, и обратный оператор тоже сохраняет U.
Отсюда следует, что $\mathcal{R}(g)U = U$.

Решение. Выпишем сначала, как действует группа действительных чисел в пространстве функций на действительной прямой.

$$\big[\mathcal{R}(t)f\big] = f(x - t)$$

Чтобы показать, что подпространство U инвариантно относительно представления $\mathcal{R}$, нужно проверить условие инвариантности для базисных векторов.

$$\big[\mathcal{R}(t)\sin\big](x) = \sin(x - t) = \sin x \cos t - \sin t \cos x$$
$$\mathcal{R}(t)\sin = \cos t \sin - \sin t \cos$$

$$\big[\mathcal{R}(t)\cos\big](x) = \cos(x - t) = \cos x \cos t + \sin x \sin t$$
$$\mathcal{R}(t)\cos = \sin t \sin + \cos t \cos$$

Применяя $\mathcal{R}(t)$ к каждому из базисных векторов U, снова попадаем в U. Т.о., U инвариантно.

Теперь ограничим $\mathcal{R}$ на U, т.е. рассмотрим действие $\mathcal{R}$ только на $\sin, \cos$ и их линейных комбинациях, и запишем матрицы этих операторов в базисе

$$\sin, \quad \cos.$$

По столбцам матрицы записаны образы sin и cos при $\mathcal{R}(t)$.

$$\mathcal{R}\mid_U = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$$

Группа действительных чисел действует на себе сдвигами, а в пространстве линейных комбинаций sin и cos возникает представление, матрицы которого - матрицы поворотов на угол t.

Ответ: матрицы поворотов на угол t

Домашнее задание: 69.7, 69.9.

Приводимые представления

Тривиальные инвариантные подпространства $\{0\}$ и V есть относительно любого линейного представления. Если к тому же есть некоторые нетривиальные инваринатные подпространства, это позволяет упростить вид матрицы линейного представления в подходящем базисе.

Определение 12.37. *Представление $\mathcal{R}$ называется приводимым, если существует нетривиальное инвариантное подпространство.*
Представление $\mathcal{R}$ называется неприводимым, если нетривиальных инвариантных подпространств не существует.

- В согласованном базисе подпространства (т.е. $\underbrace{e_1, \ \ldots, \ e_m}_{\text{базис } U}, e_{m+1}, \ \ldots, \ e_n$ - базис V)

$$\mathrm{R}(g) = \left(\begin{array}{c|c} \mathcal{R}(g)\mid_U & * \\ \hline 0 & * \end{array}\right)$$

- Если существует дополнительное инвариантное подпространство $W \subset V$ такое, что $V = U \oplus W$, то в согласованном с обоими подпространствами базисе ($\underbrace{e_1, \ \ldots, \ e_m}_{\text{базис } U}, \underbrace{e_{m+1}, \ \ldots, \ e_n}_{\text{базис } W}$ - базис V)

$$\mathrm{R}(g) = \left(\begin{array}{c|c} \mathcal{R}(g)\mid_U & 0 \\ \hline 0 & \mathcal{R}(g)\mid_W \end{array}\right)$$

Определение 12.38. *Представление $\mathcal{R}$ называется вполне приводимым, если для любого инвариантного пространства $U \subseteq V$ существует дополнительное инвариантное подпространство $W \subseteq V$ такое, что*

$$V = U \oplus W.$$

Свойство вполне приводимости наследуется при переходе к подпространствам.

Если $\mathcal{R}$ вполне приводимо и конечномерно, то последовательным разложением V на инвариантное подпространство и дополнительное инвариантное подпространство получим

$$V = U_1 \oplus \ldots \oplus U_s,$$

где в U_i нет инвариантных относительно $\mathcal{R}\mid_{U_i}$.
$\mathcal{R}\mid_{U_i} = \mathcal{R}_i$ неприводимы.

$$\mathcal{R}(g) = \begin{pmatrix} \mathcal{R}_1(g) & \ldots & \ldots & 0 \\ \vdots & \mathcal{R}_2(g) & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & \ldots & \mathcal{R}_s \end{pmatrix}$$

Решение задач на поиск инвариантных подпространств

Как искать инвариантные подпространства или доказывать неприводимость?

Пусть в пространстве V есть инвариантное подпространство U. Для $v \in U$

$$\mathcal{R}(g)v \in, \ \ \forall g \in G,$$

$$\sum_i \lambda_i \mathcal{R}(g_i)v \in U, \ \ \forall g_i \in G.$$

Получаем, что $U \subset U(v) = \{\sum\limits_i \lambda_i \mathcal{R}(g_i)v \mid \lambda_i \in K, \ g_i \in G\}$ - наименьшее инвариантное подпространство, содержащее вектор v.

Если $\forall v \in V, \ v \neq 0$ выполнено $U(v) = V$, то в V нет нетривиальных инвариантных подпространств и представление неприводимо.

Задача. Мономиальное представление группы $G = S_n$ в пространстве $V = K^n$, $\operatorname{char} K \neq 0$. Разложить его в прямую сумму неприводимых представлений.

Решение. Начнем с поиска какого-то инвариантного подпространства.

$$U = \{x \mid x_1 = \ldots = x_n\} = \langle e_1 + e_2 + \ldots + e_n \rangle$$

$\dim U = 1$ Дополнительное инвариантное подпространство должно быть $n+1$-мерно. Такая гиперплоскость в K^n задается одним уравнением.

$$W = \{x \mid x_1 + \ldots + x_n = 0\}$$

Покажем, что $U \cap W = \{0\}$. Если $x \in V \cap W$, то $x_1 = \ldots = x_n = 0$.

В U больше нет нетривиальных инвариантных подпространств относительно $\mathcal{R}\mid_U$, т.к. U одномерно. $\mathcal{R}\mid_U$ неприводимо.

Рассмотрим $\mathcal{R}\mid_W$ и поищем инвариантные подспространства в W. Возьмем вектор $(x_1, \ldots, x_n) = x \in W,\ x \neq 0$ и применим к нему линейные комбинации $\sum\limits_i \lambda_i \mathcal{R}(g_i)$.

$$x_1 + \ldots + x_n = 0 \ \Rightarrow\ \exists x_i \neq x_j$$

Подействуем на x перестановкой $\sigma = (i,\ j)$, получим вектор

$$(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) \ \to\ (x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = y = \mathcal{R}(i,\ j)x$$

$$x - y = (0, \ldots, 0, \underbrace{x_i - x_j}_{i}, 0, \ldots, 0, \underbrace{x_j - x_i}_{j}, 0, \ldots, 0)$$

Сократим на число $x_i - x_j$, получим вектор

$$0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0, \underbrace{-1}_{j}, 0, \ldots, 0) = e_i - e_j$$

Действуя разными перестановками σ, можем получить

$$\mathcal{R}(\sigma)(e_i - e_j) = e_k - e_l \ \ \forall k \neq l$$

Такие векторы порождают все W.
Тем самым, стартовав с любого ненулевого вектора и применяя подстановки и линейные комбинации, можем получить все пространство W, следовательно, $\mathcal{R}\mid_W$ неприводимо.

Ответ: $V = U \oplus W$, где $U = \{x \mid x_1 = \ldots = x_n\},\ W = \{x \mid x_1 + \ldots + x_n = 0\}$.

Лекция 13

Теорема Машке. Контрпримеры

На прошлом семинаре было показано, что описание вполне приводимых представлений сводится к описанию неприводимых представлений. Вопрос: когда все линейные представления группы вполне приводимы?

Теорема 13.3. ***(Теорема Машке)***
Любое линейное представление конечной группы G над полем K характеристики 0 вполне приводимо.

Заметим, что условие конечности группы и условие $\operatorname{char} K = 0$ существенны.

Контрпример для $|G| = \infty$. Задача 69.1 $G = \mathbb{Z}$, $K = \mathbb{C}$. Представление задано матрицами

$$\mathrm{R} : \mathbb{Z} \to GL_2(\mathbb{C}),$$
$$\mathrm{R}(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Доказать, что R приводимо, но не вполне приводимо.

Доказательство. Сначала убедимся, что R - действительно представление.
Проверим, что R - гомоморфизм. Должно быть выполнено равенство

$$\mathrm{R}(n) \cdot \mathrm{R}(m) = \mathrm{R}(n+m)$$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + n \cdot 0 & 1 \cdot m + n \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 & 0 \cdot m + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix}$$

Покажем теперь, что R - приводимое представление. $V = \mathbb{C}^2$, в нем нужно указать инвариантное подпространство.
Напоминание: В согласованном базисе подпространства (т.е. $\underbrace{e_1, \ \ldots, \ e_m}_{\text{базис } U}, e_{m+1}, \ \ldots, \ e_n$ - базис V)

$$\mathrm{R}(g) = \left(\begin{array}{c|c} \mathcal{R}(g)\mid_U & * \\ \hline 0 & * \end{array}\right)$$

В столбцах матрицы линейного оператора стоят образы базисных векторов. Отсюда следует, что

$$U = \langle e_1 \rangle - \text{ инвариантное подпространство.}$$

Теперь покажем, что R не является вполне приводимым, т.е. что не у каждого инвариантного подпространства есть инвариантное дополнение.
Предположим, что у U существует дополнительное инвариантное подпространство W

$$V = U \oplus W$$

Тогда $\dim W = \dim V - \dim U = 2 - 1 = 1$, значит, W порождается некоторым вектором $W = \langle e_2' \rangle$. Матрица оператора в согласованном с U и W базисе должна иметь диагональный вид. Это выполнено в базисе e_1, e_2'. В новом базисе

$$\mathrm{R}'(n) = \begin{pmatrix} 1 & 0 \\ 0 & \lambda(n) \end{pmatrix}$$

$\mathrm{R}(n)$ и $\mathrm{R}'(n)$ - матрицы одного линейного оператора в разных базисах. $\det \mathrm{R}'(n) = \lambda(n) = \det \mathrm{R}(n) = 1$, т.к. определитель не зависит от базиса.

$$\mathrm{R}'(n) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Матрицы всех операторов представления R не могут в некотором базисе стать единичными, т.к. единичная матрица - это матрица единичного оператора. Тогда матрица этого оператора в любом базисе должна быть единичной. Противоречие, R не вполне приводимо. □

Домашнее задание: Контрпример для $|G| < \infty$. Задача 69.2 Доказать, что отображение

$$\rho : \langle a \rangle_p \to GL_2(\mathbb{F}_p),$$

где p - простое,

$$\rho(a^k) = \begin{pmatrix} 1 & k \cdot 1 \\ 0 & 1 \end{pmatrix}$$

является приводимым двумерным представлением циклической группы $\langle a \rangle_p$ и не эквивалентно прямой сумме двух одномерных представлений.

Задача описания всех неприводимых представлений абелевой группы

Далее будем рассматривать представления произвольной конечной группы G над полем $\mathbb{C}$ ($\operatorname{char} \mathbb{C} = 0$).

Задача: описать все неприводимые представления G над $\mathbb{C}$.

I. G абелева.

Теорема 13.4. *Неприводимые представления абелевых групп над $\mathbb{C}$ всегда одномерны.*

Одномерное представление - это гомоморфизм

$$\mathrm{R} : G \to GL_1(\mathbb{C}) = \mathbb{C}^\times.$$

Всякая конечная абелева группа раскладывается в прямое произведение примарных циклических подгрупп

$$G = \langle g_1 \rangle_{m_1} \times \ldots \times \langle g_s \rangle_{m_s}.$$

Определим, куда при гомоморфизме R отображаются порождающие элементы этих циклических подгрупп $g_1, \ldots, g_s$.

$$\mathrm{R}(g_i) = \varepsilon_i, \quad \varepsilon_i^{m_i} = 1.$$

$g_1, \ldots, g_s$ переходят в комплексные корни соответствующих степеней из 1. $\forall g \in G$ представляется единственным образом в виде

$$g = g_1^{k_1} \cdot \ldots \cdot g_s^{k_s}.$$

$$\mathrm{R}(g) = \varepsilon_1^{k_1} \cdot \ldots \cdot \varepsilon_s^{k_s}$$

Представление R полностью определяется набором $\varepsilon_i : \mathrm{R} = \mathrm{R}_{\varepsilon_1, \ldots, \varepsilon_s}, \quad \varepsilon_i \in \mathbb{U}_{m_i}$. Наоборот: для каждого набора $\varepsilon_1, \ldots, \varepsilon_s$ формула

$$\mathrm{R}(g) = \varepsilon_1^{k_1} \cdot \ldots \cdot \varepsilon_s^{k_s}$$

задает представление R. От выбора показателей k_i по модулю m_i представление не зависит. Хотя разложение элемента $g = g_1^{k_1} \cdot \ldots \cdot g_s^{k_s}$ определено не однозначно, показатели k_i определены с точностью до прибавления кратных m_i, т.к. $\varepsilon_i^{m_i} = 1$.

Количество неприводимых представлений группы G над $\mathbb{C}$ равно

$$m_1 \cdot \ldots \cdot m_s = |G|.$$

Итак, количество неприводимых комплексных представлений конечной абелевой группы равно порядку этой группы.

Пример $G = V_4 = \{e, a, b, c\}$. Опишем все ее неприводимые представления над $\mathbb{C}$.

Разложим G в прямое произведение циклических групп

$$V_4 \supset \langle a \rangle_2, \ \langle b \rangle_2, \ \langle c \rangle_2$$

$\langle a \rangle_2 \cap \langle b \rangle_2 = \{e\}$, т.к. $\langle a \rangle_2 = \{e, a\}, \ \langle b \rangle_2 = \{e, b\}$. При этом $a \cdot b = c$, откуда $\langle a \rangle_2, \ \langle b \rangle_2$ образуют прямое произведение.

$$V_4 = \langle a \rangle_2 \times \langle b \rangle_2$$

Теперь опишем неприводимые представления G. Всего таких представлений $|G| = 4$.

e всегда переходит в 1, т.к. отображение - гомоморфизм. Элементы a и b порядка 2 могут переходить только в элементы порядка 2 в $\mathbb{C}$, т.е. в ± 1. Элемент c отображается в произведение образов a и b.

	e	a	b	c
R_1	1	1	1	1
R_2	1	1	-1	-1
R_3	1	-1	1	-1
R_4	1	-1	-1	1

Эта таблица полностью описывает все неприводимые (они же одномерные) представления группы V_4. Так можно описывать одномерные представления любой конечной абелевой группы. Если группа большая, достаточно указать, куда переходят ее порождающие элементы.

Домашнее задание: 70.2 ж),з), 70.10.

Задача описания всех одномерных представлений произвольной группы

II. G произвольна, опишем ее одномерные представления.

Одномерное представление - это гомоморфизм

$$\mathrm{R} : G \to \mathbb{C}^{\times}.$$

$\mathbb{C}^{\times}$ абелева, значит, $\operatorname{Im}\mathrm{R}$ абелев. При этом образ - это факторгруппа по ядру, Следовательно, ядро содержит коммутант

$$\operatorname{Ker}\mathrm{R} \supset G'.$$

Существует каноническая проекция $\pi : G \to G/G'$, а поскольку $\operatorname{Ker}\mathrm{R} \supset G'$ существует гомоморфизм

$$\overline{\mathrm{R}} : G/G' \to \mathbb{C}$$

такой, что

$$\mathrm{R} = \overline{\mathrm{R}} \circ \pi,$$

$$\overline{\mathrm{R}}(gG') = \mathrm{R}(g).$$

Определение $\overline{\mathrm{R}}$ корректно, т.к. от представителя смежного класса g не зависит образ $\mathrm{R}(g)$. Если умножить g на элемент из G', то образ g умножится на образ элемента из G', а $\operatorname{Ker}\mathrm{R} \supset G'$.

Возникает взаимно-однозначное соответствие между одномерными представлениями самой группы G и одномерными представлениями G/G'.

$$\mathrm{R} \leftrightarrow \overline{\mathrm{R}}$$

G/G' абелева, описание ее одномерных представлений известно.
Как следствие, количество одномерных представлений произвольной конечной группы G над $\mathbb{C}$ равно $|G/G'|$.

Пример. Описать все одномерные представления группы $G = S_3 \times D_5$.

Сначала найдем коммутант, а затем G/G'.

$$G' = (S_3 \times D_5)' = S_3' \times D_5' = A_3 \times R_5.$$

$$G/G' = S_3/A_3 \times G_5\ R_5$$

$|S_3/A_3| = 2$, эта факторгруппа состоит из двух смежных классов: четных подстановок и нечетных подстановок. Единичный элемент в ней A_3. Класс нечетных подстановок - порождающий элемент порядка 2.
$|D_5/R_5| = 2$, эта факторгруппа состоит из двух смежных классов: поворотов и симметрий. Единичный элемент в ней R_5. Симметрии - порождающий элемент порядка 2.

Таким образом, G/G' - это произведение двух циклических групп порядка 2, $|G/G'| = 4$. Тогда есть 4 одномерных представдения G/G' над $\mathbb{C}$.

Сначала опишем $\overline{\mathrm{R}}$, а потом согласно описанию $\mathrm{R} = \overline{\mathrm{R}} \circ \pi$, выпишем, куда отображается любой элемент группы G.

	четные подстановки	нечетные подстановки	повороты	симметрии
R_1	1	1	1	1
R_2	1	1	1	-1
R_3	1	-1	1	1
R_4	1	-1	1	-1

Классы четных подстановок и поворотов переходят в 1, т.к. являются нейтральными элементами. Классы нечетных подстановок и симметрий - это порождающие элементы порядка 2, значит, переходить они могут только в элементы порядка 2. т.е. ± 1.

Заметим, что

$$G/G' \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq V_4.$$

Определим теперь, куда отображается элемент $g \in G$. Заметим, что $g = (\sigma,\ d) = (\sigma,\ e) \cdot (e,\ d)$. Значит, нужно определить. куда отображаются пары $(\sigma,\ e), (e,\ d)$ и перемножить результаты.

	$g = (\sigma,\ e) \cdot (e,\ d)$
R_1	$1 \cdot 1 = 1$
R_2	$1 \cdot \det d = \det d$
R_3	$\operatorname{sgn} \sigma \cdot 1 = \operatorname{sgn} \sigma$
R_4	$\operatorname{sgn} \sigma \cdot \det d$

R_1 определен однозначно.
R_2 : σ отображается в 1, а d отображается в 1, если d поворот (собственное движение) и в -1, если d симметрия (несобственное движение). Под такое описание подходит инвариант $\det g$.
R_3 : d отображается в 1, а σ отображается в 1, если σ четна и в -1, если σ нечетна. Под такое описание подходит $\operatorname{sgn}\sigma$.
R_4 следует из R_2 и R_3.

Домашнее задание: Описать все комплексные одномерные представления группы $A_4 \times D_4$.

Задача описания всех представлений произвольной группы

III. Общий случай.

Факты из лекций:
1. Количество неприводимых представлений конечной группы G с точностью до изоморфизма равно количеству классов сопряженности в G.
Пусть $\mathcal{R}_i : G \to GL(V_i), \quad i = 1, \ldots, s.$ - все неприводимые представления. Обозначим $n_i = \dim V_i$.
2. $n_1 + \ldots + n_s = |G|$.
3. Количество $n_i = 1$ равно $|G/G'|$.

Часто этих трех ограничений бывает достаточно, чтобы найти $n_1, \ldots, n_s$.

Описание неприводимых комплексных представлений группы D_n

1) Сначала найдем количество s неприводимых представлений. Для этого нужно понять, как устроены классы сопряженности в D_n. Рассмотрим 2 случая.

1. $n = 2m + 1$. Всего $s = m + 2$ классов сопряженности.

классы сопряженности	их количество
все симметрии	1
$\{r,\ r^{-1}\},\ r \neq \mathrm{id}$	m
$\{\mathrm{id}\}$	1

2. $n = 2m$. Всего $s = m + 3$ классов сопряженности.

классы сопряженности	их количество
симметрии относительно диагоналей	1
симметрии от-но осей, соедин-х середины противоп. сторон	1
$\{r,\ r^{-1}\},\ r \neq \mathrm{id}, r_\pi$	m-1
$\{\mathrm{id}\}$	1
$\{r_\pi\}$	1

2) Найдем коммутант.

$$D'_n = \begin{cases} R_n, & n = 2m+1, \quad |D_n/D'_n| = 2 \\ R_{\frac{n}{2}}, & n = 2m, \quad |D_n/D'_n| = 4 \end{cases}$$

Т.о. если n нечетно, есть 2 одномерных представления, а если n четно, то 4.

3) Найдем остальные размерности. Без ограничения общности, $n_1 \leq \ldots \leq n_s$.

1. $n = 2m+1$. $n_1 = n_2 = 1 \leq n_3 \leq n_4 \leq \ldots \leq n_{m+2}$.

$$n_1^2 + n_2^2 + \ldots + n_{m+2}^2 = |D_n| = 2n = 4m+2$$

$$n_3^2 + \ldots + n_{m+2}^2 = 4m$$

В последней сумме m слагаемых, каждое из которых является квадратом целого числа > 1. Отсюда

$$n_3 = n_4 = \ldots = n_{m+2} = 2.$$

2. $n = 2m$. $n_1 = n_2 = n_3 = n_4 = 1 \leq n_5 \leq n_6 \leq \ldots \leq n_{m+3}$.

$$n_1^2 + n_2^2 + \ldots + n_{m+3}^2 = |D_n| = 2n = 4m$$

$$n_5^2 + \ldots + n_{m+2}^2 = 4m-4$$

В последней сумме $m-1$ слагаемое, каждое из которых является квадратом целого числа > 1. Отсюда

$$n_5 = n_6 = \ldots = n_{m+3} = 2.$$

4) Домашнее задание: описать одномерные представления D_n.
Опишем двумерные неприводимые комплексные представления D_n. Ранее было показано, что

$$D_n = R_n \leftthreetimes \langle s \rangle_2 = \langle r_{\frac{2\pi}{n}} \rangle_n \leftthreetimes \langle s \rangle_2,$$

где R_n - группа поворотов, а s - некоторая симметрия.

Чтобы задать представление $\mathcal{R} : D_n \to GL(V),\ \ \dim V = 2$ на любом элементе D_n, достаточно его задать на $r = r_{\frac{2\pi}{n}}$ и на s.

Обозначим $\mathcal{R}(r) = \mathcal{A}$, $\mathcal{R}(s) = \mathcal{B}$. Поскольку $o(r) = n$, $\mathcal{A}^n = \mathcal{E}$, аналогично $\mathcal{B}^2 = \mathcal{E}$.

Более того, между $\mathcal{A}$ и $\mathcal{B}$ существует соотношение.

$$srs^{-1} = r^{-1} \quad sr = r^{-1}s \quad rs = sr^{-1}$$

$$\mathcal{AB} = \mathcal{BA}^{-1}$$

Ограничим представление $\mathcal{R}$ на подгруппу поворотов $\mathcal{R}\mid_{R_n}$. R_n - циклическая группа, следовательно, она абелева. Все неприводимые представления абелевых групп одномерны. Представление $\mathcal{R}\mid_{R_n}$ двумерно, т.е. приводимо. Оно разлагается в прямую сумму неприводимых одномерных.

$V = V_1 \oplus V_2 = \langle e_1 \rangle \oplus \langle e_2 \rangle$, e_1, e_2 - базис V, оператор $\mathcal{A}$ в этом базисе диагонален.

$$\mathrm{A} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad \lambda^n = \mu^n = 1.$$

Возьмем первый базисный вектор e_1 (он является для оператора $\mathcal{A}$ собственным вектором с собственным значением λ) и подействуем на него оператором $\mathcal{B}$.

a) $\mathcal{B} \sim e_1$, но тогда e_1 является собственным вектором и для оператора $\mathcal{A}$, и для оператора $\mathcal{B}$. Значит, он порождает инвариантное одномерное подпространство $\langle e_1 \rangle = U \subset V$ для $\mathcal{R}$. Но это не так (представление неприводимо), противоречие.

b) $\mathcal{B} \nsim e_1$.

$$\mathcal{AB}e_1 = \mathcal{BA}^{-1}e_1 = \lambda^{-1}\mathcal{B}e_1 \;\Rightarrow\; \mu = \lambda^{-1}$$

Другими словами,

$$\mathrm{A} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad \lambda = \varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}. \tag{13.1}$$

Положим $e_2 = \mathcal{B}e_1$, тогда в базисе e_1, e_2 матрица A имеет вид (13.1), а матрица B есть матрица перестановки базисных векторов

$$\mathrm{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Таким образом, мы описали матрицы операторов $\mathcal{A}$ и $\mathcal{B}$.

В (13.1) $k = 1, \ldots, n$, а двумерных неприводимых представлений должно быть либо m, либо $m - 1$. Среди получившихся n представлений есть одинаковые. Например, если мы с помощью $\mathcal{B}$ переставим базисные векторы, то числа λ, λ^{-1} в матрице A заменятся на обратные. Таким образом, из всех корней $\lambda = \varepsilon_k$ нужно брать только половину.

Также λ не может принимать значения 1 и -1, т.к. оператор $\mathcal{A}$ является скалярным, и любой собственный вектор оператора $\mathcal{B}$ дает инвариантное подпространство, которого быть не должно.

Итак, качестве λ нужно брать только ε_k из верхней полуплоскости. Легко понять, что их количество равно m, если $n = 2m + 1$ и $m - 1$, если $n = 2m$.

Домашнее задание: описать неприводимые комплексные представления групп A_4 и Q_8.

Лекция 14

Кольца, алгебры, поля

Определение 14.39. *Кольцо $(A, +, \cdot)$ - это множество A с двумя бинарными операциями (сложения и умножения) такое, что*
1. $(A, +)$ - абелева группа;
2. Выполнено свойство дистрибутивности

$$\begin{array}{l}(x+y)\cdot z = x\cdot z + y\cdot z\\ z\cdot(x+y) = z\cdot x + z\cdot y\end{array} \quad \forall x, y, z \in A.$$

Если операция усмножения обладает дополнительными сойствами, то получим, соответственно, коммутативное кольцо, ассоциативное кольцо, кольцо с единицей и т.д.

Определение 14.40. *Алгебра $(A, +, \cdot, \times K)$ над полем K - это множество с операциями сложения, умножения и умножения на элементы поля такое, что*
1. $(A, +, \times K)$ - векторное поле;
2. Умножение $A \times A \to A$ линейно по каждому аргументу.

Примеры.

Кольца

1) Любое поле.

2) $\mathbb{Z}$ ассоциативное коммутативное кольцо с 1.

3) $\mathbb{Z}_m$ ассоциативное коммутативное кольцо с 1. Если m простое, то это поле (нет делителей нуля), а если m составное, то делители нуля есть.

Алгебры

1) $Mat_n(K)$ - ассоциативная некоммутативная алгебра с 1.

2) $K[x_1, \ldots, x_n]$ - коммутативная ассоциативная алгебра с 1.

3) $\mathbb{R}^3$ с операцией векторного умножения - неассоциативная алгебра. Вместо ассоциативности выполнено тождество Якоби. Кроме того, векторное умножение антикоммутативно: если поменять местами два множителя, то векторное произведение поменяет знак. Это пример алгебры Ли (с антикоммутативным умножением и тождеством Якоби).

4) Алгебра кватернионов $\mathbb{H}$ - ассоциативная некоммутативная с 1 алгебра с делением (у каждого ненулевого есть обратный).

Преимущество алгебр перед кольцами состоит в том, что в изучении алгебр можно использовать теорию векторных пространств.

Пусть A - конечномерная алгебра над полем K. В ней можно выбрать базис $e_1, \ldots, e_n$ (базис A как векторного пространства). Поскольку A алгебра, базисные векторы можно перемножать

$$e_i \cdot e_j = c_{ij}^1 e_1 + c_{ij}^2 e_2 + \ldots + c_{ij}^n e_n = \sum_{k=1}^{n} c_{ij}^k e_k,$$

$c_{ij}^k \in K$ - структурные константы алгебры A. Они полностью определяют структуру умножения в A.

$$\forall x, y \in A: \ x = x_1 e_1 + \ldots + x_n e_n, \ \ y = y_1 e_1 + \ldots + y_n e_n,$$

$$x \cdot y = \sum_{i,j=1}^{n} x_i y_j e_i e_j = \sum_{i,j,k=1}^{n} c_{ij}^k x_i y_j e_k,$$

поскольку умножение линейно по каждому аргументу.

Чтобы задать структуру конечномерной алгебры на векторном пространстве A, достаточно задать конечный набор (n^3) скаляров $c_{ij}^k \in K$. Более того, структурные константы определяют не только операцию умножения, но и все свойства алгебры.

Так, например, коммутативность умножения означает симметрию c_{ij}^k по двум нижним индексам: $c_{ij}^k = c_{ji}^k \ \forall i, j, k$. Достаточно проверять коммутативность только для базисных векторов.

Упражнение. Сформулировать свойство ассоциативности на языке структурных констант.

Замечание 14.2. *Набор структурных констант для данной алгебры определен неоднозначно: он зависит от выбора базиса.*

В частности, с помощью структурных констант можно определить изоморфность двух алгебр.

Утверждение 14.11. $A \simeq A' \ \Leftrightarrow$ *в некоторых базисах* $e_1, \ldots, e_n$ *для* A *и* $e'_1, \ldots, e'_n$ *для* A' *структурные константы* A *и* A' *одинаковы.*

Доказательство. Вытекает из определения изоморфизма. Если 2 алгебры изоморфны, то можно установить взаимно-однозначное соответствие, которое согласовано со всеми операциями: сложением, умножением и умножением на скаляр. В частности, согласованность с умножением на скаляр означает изоморфность векторных пространств.
При этом изоморфизме базис пространства A переходит в базис пространства A'. Поскольку изоморфизм согласован еще и с умножением, то не имеет значения, в каком порядке действовать: сначала перемножить 2 вектора базиса в A, а потом перейти в A' или сначала заменит e_i на e'_i, а потом перемножить их в алгебре A'.

Это и означает, что структурные константы A в базисе $e_1, \ldots, e_n$ и структурные константы A' в базисе $e'_1, \ldots, e'_n$ одинаковы.

И наоборот: если структурные константы A и A' одинаковы, то алгебры изоморфны, т.к. их можно отождествить друг с другом, сопоставив базисы. □

Описание алгебр с помощью структурных констант

Задача 63.21 а) Перечислить с точностью до изоморфизма все двумерные алгебры с единицей над $\mathbb{C}$.

Решение. Пусть A - двумерная алгебра с единицей над $\mathbb{C}$. Она определяется набором своих структурных констант в некотором базисе. Выберем базис в A: $(1, e)$ - он состоит из единицы и произвольного элемента.

Выпишем структурные константы, т.е. закон перемножения базисных векторов. Перемножение с единицей оставляет элемент на месте, т.е. $1 \cdot 1 = 1,\ 1 \cdot e = e,\ e \cdot 1 = e$. По-разному может быть устроено умножение e на себя, получится какой-то элемент алгебры A, который можно разложить по базису.

$$e^2 = \alpha \cdot 1 + \beta \cdot e, \quad \alpha, \beta \in \mathbb{C} \tag{14.1}$$

Это равенство можно назвать структурным уравнением для алгебры A. Оно полностью задает операцию умножения.

Тем самым, все двумерные алгебры над $\mathbb{C}$ с единицей определяются двумя комплексными параметрами.

Изоморфизм алгебр задается заменой базиса: если можно поменять базис A так, что структурное уравнение изменится и превратится в структурное уравнение другой алгебры с другими константами α и β, то A будет изоморфна полученной алгебре.

Упростим структурное уравнение с помощью замены базиса. Выделим в (14.1) полный квадрат.

$$e^2 - \beta \cdot e - \alpha \cdot 1 = 0$$

Можно считать, что $\mathbb{C} \subset A$, если представить это поле как $\mathbb{C} \cdot 1$. Алгебра с единицей содержит поле в качестве подалгебры, поэтому множитель 1 далее не пишем.

$$\left(e - \frac{\beta}{2}\right)^2 - \frac{\beta^2}{4} - \alpha = 0$$

$$\left(e - \frac{\beta}{2}\right)^2 = \alpha + \frac{\beta^2}{4} \tag{14.2}$$

Замена базиса:

$$(1,\ e)\ \to\ (1, e') = \left(1, e - \frac{\beta}{2}\right)$$

Обозначим правую часть (14.2) через γ, тогда структурное уравнение в новом базисе примет вид

$$(e')^2 = \gamma.$$

Получили структурное уравнение, зависящее от одного параметра. Любая из алгебр нашего класса изоморфна одной из алгебр, задаваемых параметром γ.

Сделаем еще одну замену базиса, чтобы окончательно избавиться от параметра.

1) $\gamma \neq 0$

$$(1,\ e')\ \to\ (1,\ e'') = (1,\ \frac{e'}{\sqrt{\gamma}})$$

Структурное уравнение примет вид

$$(e'')^2 = 1$$

Обозначим алгебру с таким уравнением A''.

2) $\gamma = 0$, параметр уже отсутствует. Структурное уравнение имеет вид

$$(e')^2 = 0$$

Обозначим алгебру с таким уравнением A'.

Таким образом, любая двумерная алгебра с единицей над полем $\mathbb{C}$ изоморфна либо A', либо A''.

Осталось показать, что A' и A'' не изоморфны друг другу.
Действительно, в алгебре A' есть элемент $a \neq 0$ такой, что $a^2 = 0$. В качестве примера можно взять $a = e'$.
Пусть теперь $a \in A''$, тогда

$$a = \lambda \cdot 1 + \mu \cdot e''.$$

$$a^2 = \lambda^2 + 2\lambda\mu e'' + \mu^2(e'')^2 = (\lambda^2 + \mu^2) \cdot 1 + 2\lambda\mu e'' = 0 \Leftrightarrow \begin{cases} \lambda^2 + \mu^2 = 0 \\ 2\lambda\mu = 0 \end{cases} \Leftrightarrow \begin{cases} \lambda = 0 \\ \mu = 0 \end{cases}$$

Единственный элемент в A'' со свойством $a^2 = 0$ - нулевой, а в алгебре A' существует ненулевой элемент с таким свойством.

Ответ: A', A''

Домашнее задание: 63.21 б), 63.22 а).

Замечание. Чтобы показать, что две алгебры изоморфны, нужно просто построить изоморфизм: заменить базис и получить такие же структурные константы. Чтобы показать, что две алгебры не изоморфны, нужно найти различающее свойство, сформулированное в терминах операций алгебры.

Идеалы

Определение 14.41. *Идеал в кольце/алгебре - это подгруппа по сложению $I \subset A$ для кольца или подпространство $I \subset A$ для алгебры со свойством*
$A \cdot I \subset I$ *(левый идеал)*
$I \cdot A \subset I$ *(правый идеал)*
$A \cdot I \subset I$ *и* $I \cdot A \subset I$ *(двусторонний идеал)*

Если умножение коммутативно, то нет разницы между левыми и правыми идеалами.

Задача 64.8 а) A - двумерная алгебра над $\mathbb{R}$ с базисом $(1,\ e)$, $e^2 = 0$. Найти все идеалы в A.

Решение. Алгебра коммутативна, т.к. базисные векторы коммутируют. I - подпространство в A, в A бывают нульмерные, одномерные и двумерные подпространства.

$$I_1 = A$$

$$I_2 = \{0\}$$

$$I = \langle a \rangle, \quad a \neq 0$$

$I_1,\ I_2$ - тривиальные идеалы. Они есть в любой алгебре.

Нужно определить, какие одномерные подпространства являются идеалами. Нужно проверить, что при умножении элемента I на любой элемент из A получается элемент из I. Достаточно провести проверку для базисных элементов: из A возьмем 1 и e, а из I - порождающий элемент a.

$1 \cdot a \in I$, т.к. $1 \cdot a = a \in I$.

$e \cdot a \in I$ - для каких a это выполнено?

$$a = \alpha \cdot 1 + \beta \cdot e$$

$$e \cdot a = \alpha e + \beta e^2 = \alpha e = \lambda \cdot a = \lambda \cdot \alpha + \lambda \cdot \beta e$$

При каких α, β существует такое λ? Сравним коэффициенты при 1 и e.

$$\begin{cases} \alpha = \lambda\beta \\ \lambda \cdot \alpha = 0 \end{cases} \quad \Rightarrow \ \alpha = 0, \quad \beta - \text{произвольно.}$$

Итак, $I = \langle a \rangle$ - идеал $\Leftrightarrow a \sim \beta$.

$$I = \langle \beta \cdot e \rangle = \langle e \rangle$$

Ответ: единственный нетривиальный идеал $I = \langle e \rangle$

Домашнее задание: 68.8 б).

Факторкольца и факторалгебры

Двусторонние идеалы в кольцах и группах выполняют ту же роль что и нормальные подгруппы в группах.

Определение 14.42. *Факторкольцо/факторалгебра A/I, где I - двусторонний идеал, определяется как факторгруппа по сложению.*
Умножение смежных классов:

$$(x+I)\cdot(y+I)=xy+I.$$

Здесь существенно, что идеал I двусторонний.

Примеры.

1) $A=\mathbb{Z}$
Любой идеал в $\mathbb{Z}$ является, в частности, подгруппой по сложению, а любая подгруппа циклической группы циклическая.
$I=m\cdot\mathbb{Z}=(m)$ - главные идеалы (идеалы, порожденные одним элементом).
Из определения вычетов следует, что факторкольца имеют вид

$$\mathbb{Z}/m\mathbb{Z}=\mathbb{Z}_m.$$

Терминологию вычетов используют и для произвольного факторкольца. Обозначения для смежных классов по идеалу:
$a+I=a \pmod I$ - класс вычетов элемента a по модулю идеала I.
Если идеал I фиксирован, то для краткости обозначим $a+I=a \pmod I=\overline{a}$.

2) Алгебра многочленов от одной переменной $A=K[x]$ (K- поле).
Как и в предыдущем примере, любой идеал в A порождается одним многочленом $I=(p)=\{f=p\cdot g \mid g\in K[x]\}$.
Опишем $F=K[x]/(p)$, где $p(x)=x^n+c_1x^{n-1}+\ldots+c_n$.
Свойства F:

1. Все элементы F можно записать в каноническом виде: $\forall\overline{f}\in F\ \exists!\ r\in K[x],\ \deg r<n:\ \overline{r}=\overline{f}$. Другими словами, можно смежные классы (элементы F) взаимно-однозначно пронумеровать многочленами степени $<n$.

   Для многочлена f произвольной степени $f=p\cdot q+r,\ \ f-r\,\vdots\,p\ \Rightarrow\ f-r\in I\ \Rightarrow\ \overline{f}=\overline{r}$.
   Таким образом,

   $$F\simeq\{f\in K[x]\mid \deg f<n=\deg p\}.$$

   При этом операции над многочленами f нужно выполнять в соответствии с операциями в F, т.е. сложение многочленов f и умножение их на константы не меняется, но если при перемножении двух многочленов степени $<n$ получится многочлен степени $>n$, то нужно его поделить с остатком на p.

2. Из свойства 1 следует, что факторалгебру можно отождествить с пространством многочленов степени $< n$, тогда базисом факторалгебры будет
$$\overline{1},\ \overline{x},\ \overline{x}^2,\ \ldots,\ \overline{x}^{n-1}.$$
$$\dim F = n = \deg p$$

3. Ясно, что алгебра F коммутативна, ассоциативна и содержит единицу. F является алгеброй с делением, т.е. полем $\Leftrightarrow$ p неприводим.

   Пусть $\overline{f} \in F$, $\overline{f} \neq \overline{0}$ и p неприводим, найдем $\overline{f}^{-1}$.
   $\overline{f} \neq \overline{0} \ \Leftrightarrow\ f \notin I \ \Rightarrow\ f$ не делится на p. Поскольку f неприводим, это означает, что f взаимно прост с p. С другой стороны,
$$1 = (f, p) = u \cdot f + v \cdot p.$$
   Тогда
$$\overline{f}^{-1} = \overline{u}.$$
   Это практический алгоритм нахождения обратного элемента в F, если F является полем.

4. Пусть p неприводим. Тогда в исходном поле K у многочлена p нет корней, за исключением случая $\deg p = 1$. В поле F у p есть корень - это $\overline{x}$.
$$p(\overline{x}) = \overline{x}^n + c_1\overline{x}^{n-1} + \ldots + c_n$$
   Операции над смежными классами определяются как операции над их представителями, а затем нужно взять смежный класс. Поэтому от $\overline{x}$ можно перейти к самому x, а потом взять смежный класс.
$$p(\overline{x}) = \overline{x^n + c_1x^{n-1} + \ldots + c_n} = \overline{p} = \overline{0}$$
   $K \subset F$ - расширение поля K, в котором p имеет корень.

Решение задач на присоединение корня

Задача. $\mathbb{Q}[x] \ni p(x) = x^3 - 3x + 1$, $\mathbb{Q} \subset F$ - расширение, полученное присоединением корня α многочлена p. Вычислить $\frac{\alpha}{\alpha+1}$.

Решение. Поле F изоморфно факторалгебре $\mathbb{Q}[x]/(p)$, элементы F единственным образом представляются в виде многочленов от α степени не выше 2. Представим искомую дробь в виде такого многочлена.

Деление = умножение на обратный элемент $\Rightarrow$ нужно найти $(\alpha + 1)^{-1}$. Нужно представить НОД$(\alpha + 1, p)$ в виде линейной комбинации этих двух многочленов.
$$(x + 1, x^3 - 3x + 1) = 1 = (ax^2 + bx + c)(x + 1) + d(x^3 - 3x + 1)$$

$$\begin{cases} x^3: \ a+d=0 \\ x^2: \ b+a=0 \\ x: \ b+c-3d=0 \\ 1: \ c+d=1 \end{cases} \Leftrightarrow \begin{cases} d=-a \\ b+a=0 \\ b+c+3a=0 \\ c-a=1 \end{cases} \Leftrightarrow \begin{cases} b=-a \\ c+2a=0 \\ c-a=1 \end{cases} \Leftrightarrow \begin{cases} b=\frac{1}{3} \\ c=\frac{2}{3} \\ a=-\frac{1}{3} \end{cases}$$

Согласно свойству 3,

$$(\alpha+1)^{-1} = -\frac{1}{3}\alpha^2 + \frac{1}{3}\alpha + \frac{2}{3}.$$

$$\alpha(\alpha+1)^{-1} = \alpha\left(-\frac{1}{3}\alpha^2 + \frac{1}{3}\alpha + \frac{2}{3}\right) = -\frac{1}{3}\alpha^3 + \frac{1}{3}\alpha^2 + \frac{2}{3}\alpha$$

Получили многочлен 3 степени, а нужен не выше степени 2.
$p(\overline{x}) = 0 \ \Rightarrow \ \alpha$ - корень многочлена $x^3 - 3x + 1$, $\alpha^3 = 3\alpha - 1$. Тогда

$$-\frac{1}{3}(3\alpha-1) + \frac{1}{3}\alpha^2 + \frac{2}{3}\alpha = -\alpha + \frac{1}{3} + \frac{1}{3}\alpha^2 + \frac{2}{3}\alpha = \frac{\alpha^2-\alpha+1}{3}.$$

Ответ: $\dfrac{\alpha^2-\alpha+1}{3}$

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ