

КЛШ 2016

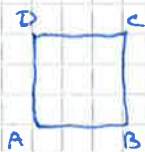
Группы и Симметрии

Лекция 1

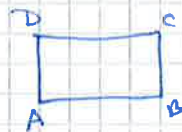
Группы преобразований

① Симметрии / Преобразования

Какая фигура "более симметрична?"



или



?

Перечислим симметрии: отображения плоскости сохраняющие фигуру

[квадрат: $I, R_{90}, R_{180}, R_{270}, S_x, S_y, S_{x+y}, S_{x-y}$
прямоугольник: I, R_{180}, S_x, S_y

Композиция отображений:

$$a) S_1 \circ S_2 (P) \equiv S_1(S_2(P))$$

Таблица умножения (для прямоугольника)

	I	R_{180}	S_x	S_y
I	I	R_{180}	S_x	S_y
R_{180}	R_{180}	I	S_y	S_x
S_x	S_x	S_y	I	R_{180}
S_y	S_y	S_x	R_{180}	I

[следует из верности]

Рассмотрим преобразования точки прямоугольника, который переносим в сетку.

Два важных свойства: множество таких преобразований

1) композиция двух преобразований — преобразование

2) Для каждого преобразования есть преобразование, которое ему обратное (тоже в этом множестве)

Определение Множество G преобразований множества A

$$g: A \rightarrow A \quad g \in G$$

называется группой (или преобразованием A), если оно обладает свойствами 1), 2)

Пример: Множество перемещений плоскости

Перемещения — отображения сохраняющие расстояния

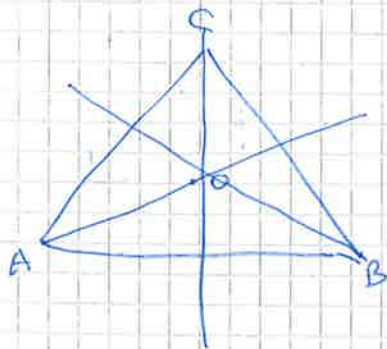
A — множество точек плоскости

G — перемещения (повороты, трансляции, отражения)

Разница между примерами? (нельзя для группы)

Коммутативность

Коммутативна ли композиция



$$S_{OA} \circ S_{OB} = R_0^{-120^\circ} \neq R_0^{120^\circ} = S_{OB} \circ S_{OA}$$

Ассоциативность

Доказать, что всегда $F_3 \circ (F_2 \circ F_1) = (F_3 \circ F_2) \circ F_1$

То есть $F_3(F_2(F_1(x))) = F_3(F_2(F_1(x)))$ ✓

Пример:

$$A = \{A, B, C, D\}$$

$$I, \quad Q: (ABCD) \rightarrow (CDAB)$$

$$L_1: (ABCD) \rightarrow (DCBA)$$

$$L_2: (ABCD) \rightarrow (BADC)$$

Таблица умножения?

Та же таблица что и для прямоугольника ✓

Первое законство с изоморфизмом групп

Группа перестановки (симметрическая группа)

X - конечное мн-во $X = \{1, 2, \dots, n\} = A$

S_n - группа перестановки элементов X

Обозначения: $s \in S_n \quad s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix}$

например $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$

Сколько элементов в S_n ? $|S_n| = n!$

Очевидно, что $\begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3, \dots, n \\ s(2) & s(1) & s(3) & \dots & s(n) \end{pmatrix}$ - перестановка элементов

Композиция перестановки:

$$f \circ g(x) = f(g(x))$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1, 2, 3 \\ 2, 1, 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2, 1, 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Обратная перестановка:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$S \quad S^{-1} \quad I \quad I$

Умножение $(s_1 s_2 \dots s_m) \equiv \begin{pmatrix} s_1 & s_2 & s_3 & \dots & s_m \\ s_2 & s_3 & s_4 & \dots & s_1 \end{pmatrix}$ — циклическая перестановка.

↑
краткая запись

$$(1, 2, 3) \in S_5$$

↑
краткая запись для

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

Упр. $(12) \circ (13) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$= (1, 3, 2)$

ч.т.д.

(ij) Транспозиция $\begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & 3 & \dots & j & \dots & i & \dots & n \end{pmatrix}$

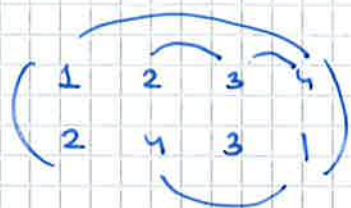
$(i, i+1)$ Транспозиция соседних

Любая перестановка может быть записана как композиция перестановки соседних (Докажите!)

3 нов перестановки $\text{sign}(s)$ $s \in S_n$

$\text{inv}(s)$ - число инверсий s

- число пар $i < j$ таких, что $s(i) > s(j)$



$$\text{inv}(s) = 4$$

$$\text{sign}(s) = (-1)^{\text{inv}(s)}$$

s - четная, если $\text{inv}(s)$ - чет
 $\text{sign}(s) = +1$

s - нечет, если $\text{inv}(s)$ - нечет
 $\text{sign}(s) = -1$

Утверждение:

Если s - композиция N транспозиций соседних,
то $\text{sign}(s) = (-1)^N$

Доказательство:

Умножив перестановку справа на транспозицию или
создаст новую инверсию, или убавит столько

$$\Rightarrow N = \text{inv}(s) \pmod{2} \Rightarrow (-1)^N = (-1)^{\text{inv}(s)} = \text{sign}(s)$$

Следствие $\text{sign}(s \circ t) = \text{sign}(s) \cdot \text{sign}(t)$

\Rightarrow Четные перестановки образуют группу A_n

так что $|A_n| = \frac{n!}{2}$ (для $n \geq 2$)

Эта группа называется знакопеременной группой

Лекция 2

Понятие абстрактной группы

Группы образованы $\xrightarrow{\text{ободз.}}$ абстрактных группы
композиция $\xrightarrow{\text{ободз.}}$ "произведение"
бинарная операция

Бинарная операция

G - множество

(a, b) - упорядоченная пара элементов $a \in G, b \in G$

Бинарная операция: отображение $(a, b) \rightarrow c$

Пишут $a * b = c$

сложение чисел, умножение чисел, композиция отображений
— примеры бинарных операций

Если $a * b = b * a$ (a, b коммутируют)

Если $a + b = b + a \quad \forall a, b$, то операция — коммутативна
(тогда часто пишут $a + b$)

Пример 1

Обычное сложение на множестве \mathbb{Z} всех целых чисел
[бинарная операция]

Пример 2

Умножение на \mathbb{Z} [бинарная операция]

Пример 3

Являются ли на множестве \mathbb{Z} бинарными операц.

а) деления

б) вычитания

Коммутативны ли эти операции?

Перемножить a, b, c не меняя порядк. $a \cdot b \cdot c$?

Если

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \text{ то}$$

тройка a, b, c — ассоцирующая

Если $= \forall a, b, c$, то операция $*$ — ассоциативная

Можно писать $a \cdot b \cdot c$ если $*$ — ассоциативна...

- Пример:
- a) композиция перемещений
 - b) сложение и умножение действ. чисел ?
 - c) деление и возведение в степень
($a \cdot n = a^n$)

Определение (абстрактной) группы

Множество G с бинарной операцией $*$ называется группой, если выполняются 3 аксиомы

I) \exists единственный элемент $e \in G$ такой, что
 $a * e = e * a = a$ для всех $a \in G$

II) Для каждого $a \in G$ существует единственный
 $a^{-1} \in G$ такой, что $a * a^{-1} = a^{-1} * a = e$

III) $*$ — ассоциативна : $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$

Если $*$ — коммутативна, то группа называется абелевой
или коммутативной

Пример: сложение целых чисел

$$G = \mathbb{Z} \quad * = + \quad e = 0 \quad "a^{-1}" = -a$$

это группа абелева

а) Группа изометрий отображ. фигуру F в себя
(группа симметрии фигуры F)

б) Аддитивная группа рациональных чисел
(действительных)

в) Мультипликативная группа положительных рациональных
(положительных действительных) чисел

Понятие изоморфизма

Определение


Гомоморфизм если
преобр. не взаимнооднозначное

Группы G и H называются изоморфными, если
существует взаимнооднозначное отображение $\varphi: G \rightarrow H$,
сохраняющее произведение, т.е.

$$\varphi(a) \varphi(b) = \varphi(a \cdot b)$$

Это отображение называется изоморфизмом $G \cong H$

"абстрактно равные группы"

 группа симметрии
правильного
треугольника



Группа S_3
перестановок

То же абстрактная группа

Важная задача теории групп — классификация групп
с точностью до изоморфизма

Подгруппа

Подмножество $H \subset G$ группы G называется подгруппой G если

- 1) $e \in H$
- 2) для любого $a \in H$ чл. $a^{-1} \in H$
- 3) $\forall a, b \in H \quad a * b \in H$

Опр: Порядок элемента $a \in G$ - наименьшее положительное целое число n такое, что $a^n = e$
(если n не существует, то порядок a бесконечный)

Пример: Порядок перестановки $s \in S_n$ - $\text{НОК}(n_1, n_2, \dots, n_k)$,
где n_1, \dots, n_k - порядки циклов в разложении s

Теорема Лагранжа

Порядок любой подгруппы (число элементов),
также как порядок любого элемента группы,
является делителем порядка группы

Лекция 3

Различные Группы

Теорема Кэли: Любая конечная группа (G, \circ) изоморфна некоторой подгруппе группы перестановок.

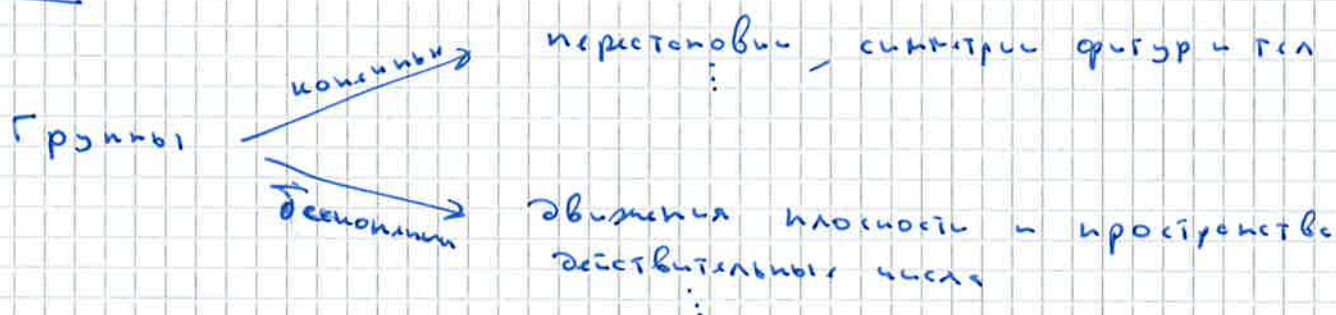
Доказ. $a \in G \rightarrow \pi_a : \pi_a(g) = a \circ g \quad \forall g \in G$

$$\pi_a : G \rightarrow G$$

$$ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y$$

\Rightarrow различные элементы G переводятся в различ.

$\Rightarrow \pi_a$ - перестановка элементов G
 $\forall a \in G$



Классификация конечных групп

[с точностью до изоморфизма]

не решенная задача

Упростили: классификация простых конечных групп

простые группы - элементарные кирпичики из которых можно составить все остальные группы

Похоже на разложение чисел на простые множители, но нет теории об однозначности, т.е. из данного набора простых групп ^{в од. сл.} можно составить различные, неэквивалентные группы

Что такое простая группа?

Опр

$\alpha: G \rightarrow H$ упрощающий гомоморфизм если

$\alpha(G) \subset H$ состоит более или из одного элемента,
но не из, или $\in G$

Опр

Конечная группа G — простая, если у неё
нет упрощающих гомоморфизмов

Пример: Z_p — простая если и только если p — простое.

$$Z_p = \{z, z^2, \dots, z^p = e\} \quad z = \begin{pmatrix} 1 & 2 & 3 & \dots & (p-1) & p \\ 2 & 3 & 4 & \dots & p & 1 \end{pmatrix} \in S_p$$

Доп: \forall если $\alpha(z^k) = z^l$ если

$$\text{то } \alpha(z^{k-e}) = e$$

$$\Rightarrow \alpha(z^{2k-1}) = \alpha(z^{3k-1}) = \dots = e$$

$$\Rightarrow \alpha(z^k) = e \quad \forall k$$

Если p — не простое, то Z_p — не простая

Контрпример $Z_4 \rightarrow Z_2$

$$\{0, 1, 2, 3\} \rightarrow \{0, 1\} \quad \begin{array}{l} 0, 2 \rightarrow 0 \\ 1, 3 \rightarrow 1 \end{array}$$

упрощ. гомоморфизм

$Z_n \rightarrow Z_m$ n — делитель m в общем случае.

2 Алгебраические серии

$$Z_p$$

p -простая — бесконечная серия простых групп

Ещё одна серия

$$A_n$$

пр- $n > 4$ — простая

↙ n переменных группа $|A_n| = \frac{n!}{2}$

Полная классификация?

[Считается известной и доказанной в серии работ около 100 авторов 1955-2004, около 15000 журнальных страниц.]

16 - геометрических серий [подгруппы групп Ли]

Теорема: Любая конечная группа - это либо одна из 26 sporadic groups, либо принадлежит одному из следующих трёх семейств:

- 1) циклические группы Z_p , простого порядка p) алгебр
- 2) знакопеременные группы A_n , для $n \geq 4$
- 3) простые группы типа Ли) геометрических

Пример из 2) $SL_2(F_p) / (\pm 1)$ $p \geq 5$ ($PSL(n, F_q)$)

26 sporadic groups

- наибольшая M_{24} , 18612 $2^4 \cdot 3^2 \cdot 5 \cdot 7 = 7920$ элем

наибольшая F_1 (или M)
осн. и повороты 6 пр-ва изометрии 196883

Число элементов 808 017 424 794 512 875 886 455 304

961 710 737 005 754 368 $\cdot 10^5$

"big monster" $\approx 10^{54}$

Еще раз о теореме Лагранжа

Теорема: Порядок k любого элемента ^{конечной} группы G делит порядок группы $|G|$

Группа ортогональных:

а) в конечной группе порядка $|G|$ для любого $g \in G$ справедливо $g^{|G|} = e$

б) Порядок любой конечной группы делится на произведение простых порядков с элементами

Пример 1

Группа симметрии додекаэдра

120°

порядок

3

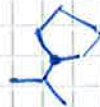
72°

5

180°

2

$$3 \cdot 5 \cdot 2 = 30$$



12

$\Rightarrow |D|$ делится на 30

[решение 60]

Пример 2

или докажем, что

$$7^8 - 1, 11^8 - 1, 13^8 - 1, 17^8 - 1, 19^8 - 1, 23^8 - 1, 29^8 - 1 \text{ делится на } 30?$$

Пусть $\Phi(m)$ — количество натуральных чисел $< m$ и взаимно простых с m

на $\Phi(m)$ * — умножение по модулю m

$$m = 30: \quad 7 \cdot 17 = 119 = 3 \cdot 30 + 29 \\ 7 * 17 = 29 \pmod{30}$$

$\Phi(m)$ образует абелеву группу

а) $a * b = b * a \in \Phi(m)$

б) $1 \in \Phi(m) \quad a * 1 = 1 * a = a$

в) $\exists a^{-1}: a * a^{-1} = 1 \pmod{m}$

$\varphi(m)$ - порядок группы $\phi(m)$

$$\Rightarrow a^{\varphi(m)} = 1 \Rightarrow a^{\varphi(m)-1} - \text{делится на } m$$

$$m=30 \quad \phi(m) = \{1, 7, 11, 13, 17, 19, 23, 29\} \Rightarrow \varphi(m) = 8$$

$$\Rightarrow 7^8 - 1 : 30 \text{ кт. 2.}$$

Возможные проекты на В И П

(выставка итоговых
проектов)

- 1) Расираси правильных многоугольников
и малая теорема Ферма
- 2) Расираси многогранников и теорема Полюса
о перенесении
- 3) Игра в "15".
- 4) Группы симметрий игры Судоку