Конспект по теории групп

Коченюк Анатолий

27 февраля 2018 г.

Борис Лаевский – преподователь

0.1 Перестановка

конечное множество $N = \{1, 2, ..., n\}$

Определение 0.1. *Перестановкой будем называть биективную функцию $\alpha : N \to N$*

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

Определение 0.2. *Тождественной перстановкой будем обозначать перестановку, оставляющюю все элементы на своих местах*

Рассмотрим композицию двух перестановок

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

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

$$ab = a(b(X)) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Определение 0.3. S_n *— множество всех перестановок множества из n элементов*

множество перестановок — группа Если она обладает следущими свойствами:

1. $\forall a, b, c \in S_n \quad (ab)c = a(bc)$
2. $\forall a \in S_n \quad ea = ae = a$
3. $\forall a \in S_n \quad \exists a^{-1} \in S_n : aa^{-1} = a^{-1}a = e$

Определение 0.4.

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$$

Будем называть перстановку a k-циклом, если:

1. $a(i) = i + 1 \quad i = \overline{1, k}$

2. $a(k) = 1$

Пример:

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

$$a = (2, 3, 4, 1)$$

Определение 0.5. *Транспозиция — цикл длины 2*

Задача 0.1. *Сколко различных 57-циклов в S_{57}?*
Ответ : 56!
Решение (n) – количество

$$\begin{pmatrix} 1 & 2 & 3 & \dots & 56 & 57 \\ (56) & (55) & (54) & \dots & (1) & (1) \end{pmatrix}$$

Для первого нельзя поставить 1 $\Rightarrow$ осталось 56 Для второго нельзя поставить прошлый элемент и 2-ой

Задача 0.2. *Доказать, что любые два независимых цикла коммутируют (коммутативны относительно умножения)*

Доказательство. □

ДЗ:

- S_5 количество циклов и транспозиций
- При каких условиях произведение двух транспозиций является циклом

* При каких условиях произведение двух циклов является циклом

1. S_5

   Транспозиций – ((5), (4)) – 5*4/2 = 10

   3-циклов – $C_5^3 * 2 = 24$

   4-циклов – $C_5^4 * 3! = 5$

   5-циклов – $C_5^5 * 4! = 24$

   Всего – 10+24+5+4 ()

   65 – мало

2. a, b – транспозиции ab – цикл, если они зависимы, т.е. изменяют один и тот же элемент в множестве.

3. a, b – циклы ab – цикл, когда они зависимы —||—

$C_n^k = \dfrac{n!}{k!(n-k)!}$ количество выбрать из n элементов группы по k элементов, не обращая внимания на порядок

Теорема 0.1. *Любая перестановка представима в виде произведения (n-1) транспозиции*

Доказательство. д/з ☐

$S_1 \quad \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}$. (k, l) – беспорядок, если $i_k < i_l$ и $j_k > j_l$

Перестановка чётная, если в каноническом виде (числа сверху расположены по порядку) количесвто беспорядков чётное.

Также перестановка чётная, если в не каноническом виде сумма количеств беспорядков сверху и снизу чётное

Теорема 0.2. *Докажем эквивалентность этих определений*

Доказательство. .
Для доказательства введём ещё одно определение, которое эквивалентно и тому и другому.

перестановка b – чётная, если количество пар чисел (k, l) таких, что $(i_k > i_l)\&(j_k < j_l)$

1 и 3 эквивалентны:

применим 3 к каноническому виду. тогда мы получим, что считаем то же самое

2 и 3 эквивалентны:

фиксируем $k, l \in \mathbb{N}$ не умаляя общности, скажем, что $k < l$

1. $(i_k < i_l)\&(j_k > j_l)$ тогда эта пара даёт $+1$ к количеству беспорядков по 3-му определению. А по 2-му она не добавляет ни одной к верхней строчке и одну к нижней. Таким образом тоже $+1$

   Случай с обратными знаками аналогичен, просто беспорядок добавляется к верхней строчке, а не к нижней

2. $(i_k < i_l)\&(j_k < j_l)$аналогично

☐

- Доказать, что при умножении на транспозицию справа или слева чётность меняется

  Доказательство. $a = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & & a_i & & a_j & & a_n \end{pmatrix}$

  $t = (i, j)$

  $at = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & & a_j & & a_i & & a_n \end{pmatrix}$

  Если между i и j k перестановок, то количество беспорядков, возникающих при переставлении a_i и $a_j = 2k$-1. это число нечётное $\Rightarrow$ чётность количесва беспорядков меняется. ☐

- имеется 2 перестановки a, b. как определяется чётность через чётность a и чётность b

  Доказательство. $a = k$ транспозиций

  $b = l$ транспозиций

  $ab = k + l$ транспозиций □

в S_n равное количество чётных и нечётных ДЗ:

Теорема 0.3. $(ab)^{-1} = b^{-1}a^{-1}, \ a, b \in S_n$

Определение 0.6 (возведение перстановок в степень)**.** $a \in S_n$

1. $a^0 = e = id$
2. $a^{k+1} = a^k a$

Доказать, что $a^{-k} = (a^{-1})^k \quad \equiv a^{-k}$ *– обратное к* a^k

Доказательство. a^{-k} – обратное к k. Нужно доказать, что $a^{-k} = (a^{-1})^k$
$a^k \cdot (a^{-1})^k = e$?

$$a^k \cdot (a^{-1})^k = a \cdot \ldots \cdot a \cdot a \cdot a^{-1} \cdot a^{-1} \cdot \ldots \cdot a = a^k \cdot (a^{-1})^k =$$

$$= a \cdot \ldots \cdot a \cdot e \cdot a^{-1} \cdot \ldots \cdot a^{-1} = \ldots a \cdot a \cdot a^{-1}a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$

□

Найти все $a \in S_n$, что $\forall b \in S_n$

1. $ba = b$

   $b^{-1}ba = b^{-1}b$

   $a = e = id$
2. $ba = ab$
3. $ba = ab^{-1}$

Свойства стееней:

1. $a^{k+l} = a^k * a^l$
2. $a^{kl} = (a^k)^l$
3. Если $ab = ba$, то $ab^k = a^k b^k$ очевидно

$\forall(k,m)\&\forall a \quad a(k,m)=(k,m)a \Rightarrow a=e$

Мы знаем, что любая перстановка представима в виде произведения конечного числа циклов. И, возведя каждый из них в степень равную их длинне получим $id=e$. Мы можем возвести всю перстановку в степень равную НОК длин её составляющих, таким образом каждый цикл станет равен $id=e$, а их произведение будет тоже $id=e$

наименьшее такое k будем называть порядком перстановки

Теорема 0.4. $S_n \quad a \in S_n \quad a=c_1\dots c_i$

Тогда порядок аравен НОК$|c_1|\dots|c_n|$*, где* $|c|$*– порядок* c

Доказательство. $k=\text{НОК}(|c_1|\dots|c_i|)$

$k \vdots |c_j| \quad \forall j=\overline{1,i}$

$c_j^k=e$

$a=c_1\dots c_i$

$a^k=(c_1\dots c_i)^k=c_1^k\dots c_i^k=e\dots e=e$

Попробуем взять $l<k$такое, что $l \not\vdots |c_j| \quad c_j^l \neq e \quad a^e \neq e$ □

Пусть k – порядок a, тогда $a^n=e \Longleftrightarrow n \vdots k$

0.2 Группы

$\cdot : MxM \to M$ – бинарная операция

$(G,\cdot)$ – группа если:

1. $a(bc)=(ab)c$
2. $\exists c \in G : \forall a \in G \quad ac=ca=a$
3. $\forall a \in G \quad \exists a^{-1} \in G : aa^{-1}=a^{-1}a=e$

$(S_n,\cdot)$ – группа

Количество элементов в $G=|G|=$ порядок G

1. $(\mathbb{Z},+)$ да
2. $(\mathbb{Z},-)$ нет
3. $(\mathbb{N},*)$ нет
4. Множество чётных чисел относительно сложения
5. Множество нечётных чисел относительно сложения
6. $(f : X \to X,\cdot)$
7. $(B(A),\cup)$

8. $(B(A), \cap)$
9. $(B(A), \setminus)$
10. $(B(A), \triangle)$

$f : G \to H$ – изоморфизм, если :

1. f – биекция
2. $\forall x, y \in G \quad f(x \cdot y) = f(x) \cdot g(x)$

и трёх ээлементов Дз попарные неизоморфные группы из одного и двух элементов (3 и 4-х тоже)