Ответы на вопросы 36-38

Александр Старовойтов <Telegram>

5 января 2022 г.

1. Вопрос 36

Дать определение группы подстановок. Сформулировать и доказать теорему о разложении подстановки в произведение независимых циклов и произведение транспозиций.

Определение 1 (Группа подстановок (или группа перестановок))**.** Это множество всех биекций n-элементного множества на себя с операцией композиции биекций. Множество всех перестановок множества $\{1, 2, \dots n\}$ обозначается S_n.

Элемент этой группы называется подстановкой:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

$\pi(1) = i_1, \pi(2) = i_2 \dots$

Операцию композиции будем называть произведением $(\pi \circ \rho)(x) = \rho(\pi(x))$.

Через $\begin{pmatrix} i_1 & i_2 & \dots & i_n \end{pmatrix}$ обозначается цикл длины n, который переводит $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, ..., $i_n \mapsto i_1$. Циклы являются независимыми, если они представляют непересекающиеся множества элементов.

Транспозицией называется цикл длины 2.

Теорема 1 (О разложении подстановки в произведение независимых циклов и произведение транспозиций)**.** *а) Любая перестановка разбивается в произведение непересекающихся циклов. б) Любая перестановка может быть представлена в виде произведения транспозиций.*

Доказательство. а) Пусть $\pi \in S_n$. Если $\forall$i π(i)=i, то π = e.

Пусть $\exists i : \pi(i) \neq i$ и i_1 — первый такой элемент, что $\pi(i_1) \neq i_1 \Rightarrow \pi(i_1) > i_1$

Тогда пусть $\pi(i_1) = i_2$; Ясно, что $\pi(i_2) \neq i_2$ (иначе перестановка не взаимооднозначна) $\Rightarrow \pi(i_2) = i_3$

$|M| < \infty \Rightarrow \exists k \in \mathbb{N} : i_k \neq i_1, i_{k+1} = \pi(i_k) = i_1$

$\pi_1 = \begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$

Рассмотрим $\pi' = \pi\pi_1^{-1}$

В π' элементы $1, 2, \dots i_1$ остаются на месте. Также остаются на месте элементы $i_2, \dots, i_k$. Повторим рассуждение для π'. Получим цикл π_2, не пересекающийся с π_1; $\pi'' = \pi\pi_1^{-1}\pi_2^{-1}$, в π'' неподвижных элементов стало больше и т.д.

После конечного числа шагов получим

$$\pi\pi_1^{-1}\pi_2^{-1}\dots\pi_s^{-1} = e$$

$\pi = \pi_s\pi_{s-1}\dots\pi_1$ — требуемое разложение

Единственность: пусть $\pi = \pi_1\pi_2\dots\pi_s = \tau_1\tau_2\dots\tau_r$ — два таких разложения. i_1 — первый элемент, который не остается на месте: $\pi(i_1) \neq i_1$. Можно считать, что i_1 входит в π_1 и τ_1. Далее легко видеть, что $\pi_1 = \tau_1 \Rightarrow \pi_2 = \tau_2, \dots, \pi_s = \tau_r$

б) Ввиду а) достаточно разложить на транспозиции любой цикл.

$$\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix} = \begin{pmatrix} i_1 & i_2 \end{pmatrix}\begin{pmatrix} i_1 & i_3 \end{pmatrix}\dots\begin{pmatrix} i_1 & i_k \end{pmatrix}$$

□

2. Вопрос 37

Дать определение чётной и нечётной подстановки. Объяснить и обосновать, как чётность подстановки определяется по её разложению в произведение транспозиций. Дать определение знакопеременной группы.

Определение 2 (Четная и нечетная подстановка)**.** Подстановка $\pi \in S_n$ четная, если количество инверсий в π четное, и нечетная в противном случае.
$\pi \in S_n$, $1 \leq i < j \leq n$. Пара (i, j) — инверсия, если $\pi(i) > \pi(j)$.

Подстановка $\pi \in S_n$ является четной $\Leftrightarrow$ количество транспозиций в ее разложении на транспозиции четно.

Доказательство. Достаточно доказать, что если τ — транспозиция, то подстановки π и $\tau\pi$ имеют разную четность.

Если $\tau = (i\ j) = (i\ i+1)(i+1\ i+2)\dots(j-1\ j)(j-2\ j-1)\dots(i\ i+1)$. В этом разложении $j-i+j-i-1 = 2(j-i)-1$ — нечетное число транспозиций. $\Rightarrow$ можно считать, что τ переставляет соседние элементы.

Пусть $\tau = (k\ k+1)$
$\tau' = \tau\pi$

$$\pi = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ i_1 & \dots & i_k & i_{k+1} & \dots & i_n \end{pmatrix}$$

$$\pi' = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ i_1 & \dots & i_{k+1} & i_k & \dots & i_n \end{pmatrix}$$

$\forall (l, m)$ — инверсия в π
$l \neq k, k+1, m \neq k, k+1 \Rightarrow (l, m)$ — инверсия и в π'
$l = k, m > k+1 \Rightarrow$ пара $(k+1, m)$ — инверсия в π'
$l = k+1 \Rightarrow (k, m)$ — инверсия в π'
$l \neq k, k+1, m = k$ или $k+1$ — аналогично

Пара $(k, k+1)$ правильная для $\pi \Leftrightarrow$ она инверсия для $\pi' \Rightarrow i(\pi') = i(\pi)+1$ т.е. четность разная.
Аналогично, если $(k, k+1)$ - инверсия для π, то она правильная для π' $\Rightarrow i(\pi') = i(\pi) - 1$ т.е. четность разная. □

Определение 3 (Знакопеременная группа)**.** Множество всех четных подстановок в группе S_n образует подгруппу и называется знакопеременной группой на n элементах. Обозначается A_n.

3. Вопрос 38

Дать определение кольца. Какое кольцо называется ассоциативным, коммутативным, кольцом с единицей? Сформулировать и обосновать основные положения теории делимости в кольце целых чисел: бесконечность множества простых чисел, деление с остатком, наибольший общий делитель и алгоритм Евклида, основная теорема арифметики.

Определение 4 (Кольцо)**.** Кольцо — алгебраическая структура $(R, +, \cdot)$ с двумя бинарными операциями, удовлетворяющими аксиомам кольца:
1. $(R, +)$ — абелева группа;
2. Дистрибутивность: $\forall a, b, c \;\; a(b + c) = ab + ac$ и $(a + b)c = ac + bc$

Если операция умножения ассоциативна, то R называют *ассоциативным кольцом*; коммутативна — *коммутативным кольцом.* Если существует нейтральный элемент по умножению, его обозначают 1, а кольцо называют *кольцом с единицей.*

Теорема 2 (О бесконечности множества простых чисел)**.** *Множество простых чисел бесконечно.*

Доказательство. Пусть $p_1, \ldots, p_k$ — все простые числа. Рассмотрим число $p = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. p не делится ни на одно из $p_1, \ldots, p_k$. Оно либо само простое, либо делится на простое $\neq p_1, \ldots, p_k$. Противоречие. □

Теорема 3 (О делении с остатком)**.** *Пусть $a, b \in \mathbb{Z}, b \neq 0$. Тогда $\exists! q, r \in \mathbb{Z}, 0 \leq r < |b| : a = qb + r$, где q — (неполное) частное, а r — остаток.*

Доказательство. Рассмотрим множество $M = \{a - k \cdot b \mid k \in \mathbb{Z}\}$. r — минимальное неотрицательное число множества M.

Существование: Покажем, что $r < |b|$:
Пусть $r \geq |b|$: $r = a - kb$
при $a \geq 0 : r' = a - (k + 1)b$
при $a < 0 : r' = a + (k - 1)b$
$r' \in M, r' \geq 0, r' < r$ — противоречие $\Rightarrow$ существование q и r

Единственность: Пусть $a = q_1 b + r_1 = q_2 b + r_2$; $0 \leq r_1 < |b|$, $0 \leq r_2 < |b|$
Пусть $r_2 \geq r_1$: $\underbrace{(q_1 - q_2)b}_{\geq |b|} = \underbrace{r_2 - r_1}_{< |b|} \Rightarrow$ противоречие, если $q_1 \neq q_2, r_1 \neq r_2$ □

Определение 5 (НОД)**.** Число $d \in \mathbb{N}$ называют *наибольшим общим делителем* чисел $a, b \in \mathbb{Z}$, если $d|a$, $d|b$, и d — наибольшее число с таким свойством ($a \neq 0$ или $b \neq 0$). Обозначается $d = \text{НОД}(a, b) = gcd(a, b) = (a, b)$.

Определение 6 (Алгоритм Евклида)**.**

$$\begin{aligned} a, b \in \mathbb{Z}, b \neq 0 \\ a = q_1 b + r_1, 0 \leq r_1 < |b| \\ b = q_2 r_1 + r_2, 0 \leq r_2 < r_1 \\ \dots \\ r_{k-2} = q_k r_{k-1} + r_k, 0 \leq r_n < r_{k-1} \\ r_{k-1} = q_{k+1} r_k \end{aligned}$$

r_k — последний ненулевой остаток.

Теорема 4 (НОД и алгоритм Евклида)**.**

$$d = (a, b) = r_k$$

Доказательство. Пойдем по алгоритму (сверху вниз) $d|a, d|b \Rightarrow d|r_1 \Rightarrow d|r_2 \Rightarrow \dots \Rightarrow d|r_k$
(снизу вверх) $r_k|r_{k-1} \Rightarrow r_k|r_{k-2} \Rightarrow \dots \Rightarrow r_k|b, r_k|a \Rightarrow r_k = d$ □

Лемма 1 (Следствие алгоритма Евклида)**.** *Пусть* $d = (a, b)$*. Тогда* $\exists u, v \in \mathbb{Z}, d = ua + vb$*.*

Доказательство. $d = r_k = r_{k-2} - q_k \cdot r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) = \dots = k_1 a + k_2 b$ — выражение через a и b □

Лемма 2. *Если* $a, b \in \mathbb{Z}, p$ *— простое и* $p|ab$*, то* $p|a$ *или* $p|b$

Доказательство. Пусть $p \nmid a$ и $p \nmid b \Rightarrow (p, a) = 1$ и $(p, b) = 1$
По Лемме 1 $\exists u_1, u_2, v_1, v_2 \in \mathbb{Z}$
$u_1 p + v_1 a = 1$
$u_2 p + v_2 b = 1$
перемножим: $u_1 u_2 p^2 + u_1 v_2 pb + u_2 v_1 pa + v_1 v_2 ab = 1 \Rightarrow p|1$ – противоречие □

Теорема 5 (Основная теорема арифметики)**.** *Любое целое число* $a \in \mathbb{Z}$ *можно представить в виде* $a = \pm p_1 p_2 \dots p_k$*, где* $p_1, \dots, p_k$ *— простые числа. Такое представление единственно с точностью до порядка множителей.*

Доказательство. Существование: $a \in \mathbb{Z}$. Если $a = \pm p$, p — простое, то $a = \pm p$ — требуемое разложение. Если a — составное, то $a = bc$, где $|b|, |c| < |a|$. Далее применяем те же рассуждения к b и c.

Единственность: $a = \pm p_1 \dots p_k = \pm q_1 \dots q_l$
$p_1|q_1 \dots q_l \Rightarrow$ (по Лемме 2) $\exists i p_i|q_i, p_i, q_i$ — простые $\Rightarrow p_i = q_i$. Можно считать, что $i = 1, \Rightarrow p_2 \dots p_k = q_2 \dots q_l$, и т.д. □