Группы преобразований

Напоминание. Отображение $\varphi\colon X \to Y$ из множества X в множество Y называется *взаимно однозначным* (или *биекцией*), если для каждого элемента $y \in Y$ существует ровно один элемент x такой, что $\varphi(x) = y$.

Преобразование ψ называется *тождественным*, если для каждого $x \in X$ выполнено равенство $\psi(x) = x$. Обозначение: $\psi = \mathrm{id}_X$.

Отображение $\varphi\colon X \to Y$ называется *обратным* для отображения $\psi\colon Y \to X$, если справедливы равенства $\varphi \circ \psi = \mathrm{id}_Y$ и $\psi \circ \varphi = \mathrm{id}_X$. Обозначение: $\varphi = \psi^{-1}$

Количество элементов во множестве X обозначается через $|X|$ или $\#X$.

Определение 1. *Преобразованием* множества X называется любая биекция $\varphi\colon X \to X$. Для множества всех преобразований X зарезервировано обозначение $S(X)$.

Определение 2. *Группой преобразований* множества X называется всякая непустая совокупность его преобразований G, удовлетворяющая следующим свойствам:

(i) G замкнута относительно композиции, то есть для всех $g, h \in G$ верно: $g \circ h \in G$;

(ii) G замкнута относительно взятия обратного преобразования, то есть для всех $g \in G$ преобразование g^{-1} лежит в G.

Задача 1. Докажите, что группа преобразований любого множества содержит тождественное преобразование.

Задача 2. Пусть множество X — это квадрат $ABCD$. Обозначим через s_{ac}, s_{bd}, s_H и s_V симметрии относительно диагонали AC, диагонали BD, горизонтали и вертикали квадрата соответственно. Далее, обозначим через r_0, r_1, r_2 и r_3 повороты вокруг центра квадрата на $0°$, $90°$, $180°$ и $270°$ соответственно.

а) Докажите, что $G = \{s_{ac}, s_{bd}, s_H, s_V, r_0, r_1, r_2, r_3\}$ образует группу преобразований квадрата.

б) Выпишите таблицу умножения в этой группе.

в) Придумайте группу преобразований квадрата, состоящую из четырёх преобразований.

Задача 3.

а) Докажите, что для любого множества X множество $S(X)$ является группой;

б) Пусть X — конечно, причём $|X| = n$. Найдите $|S(X)|$.

Замечание 1. В условиях задачи 3б) группа $S(X)$ называется *симметрической группой* и обозначается S_n.

Задача 4. **а)** Опишите все преобразования правильного треугольника, сохраняющие расстояния между любыми двумя его точками.

б) Докажите, что эти преобразования образуют группу.

Определение 3. *Порядком элемента* g группы преобразований G называется наименьшее натуральное k такое, что $g^k = \underbrace{g \circ \dots \circ g}_{k} = \mathrm{id}$. Обозначение: $\mathrm{ord}(g)$.

Определение 4. *Порядком группы* G называется количество элементов в G. Обозначение: $|G|$ или $\#G$.

Задача 5. Найдите порядок каждого элемента групп из задач 2 и 4.

Задача 6. Пусть множество X является подмножеством прямой, плоскости или пространства. Рассмотрим множество $\mathrm{Isom}(X) = \{\varphi \in S(X) \mid \varphi \text{ сохраняет расстояния}\}$. Докажите, что вне зависимости от X множество преобразований $\mathrm{Isom}(X)$ является группой. Эта группа называется *группой движений* X.

Задача 7. Перечислите все элементы и их порядки в группах движений следующих множеств:
а) прямоугольник; **б)** правильный m-угольник; **в)** правильный тетраэдр; **г)** куб; **д)*** октаэдр; **е)*** икосаэдр; **ж)*** додекаэдр.

(Подсказка: Как связаны между собой куб и октаэдр? Тот же вопрос для икосаэдра и додекаэдра.)

Замечание 2. Группа из задачи 7б) называется *группой диэдра* и обозначается D_m.

1	2 а	2 б	2 в	3 а	3 б	4 а	4 б	5	6	7 а	7 б	7 в	7 г	7 д	7 е	7 ж

Определение 5. *Орбитой* элемента $x \in X$ при действии группы преобразований G называется множество $\{g(x) \mid g \in G\} \subset X$. **Обозначение** Gx.

Задача 8. Найдите орбиту каждой точки при действии группы движений
а) квадрата; **б)** куба; **в)** правильного m-угольника.

Задача 9. **а)** Опишите группу движений единичного круга; **б)** Найдите орбиту каждой точки при действии этой группы; **в)** Найдите преобразование, не имеющее конечного порядка.

Задача 10. Докажите, что любые две орбиты либо совпадают, либо не пересекаются. Следует ли отсюда, что всё множество X есть объединение непересекающихся орбит?

Задача 11. Докажите, что для любых двух элементов одной орбиты $a, b \in Gx$ найдётся элемент $g \in G$, такой что $g(a) = b$.

Определение 6. *Стабилизатором* элемента $x \in X$ при действии группы преобразований G называется множество $\{g \mid g(x) = x\} \subset G$. **Обозначение:** G_x.

Задача 12. Найдите стабилизаторы каждой из точек следующих множеств при действии их групп движений: **а)** квадрата; **б)** куба; **в)** правильного m-угольника.

Задача 13. Рассмотрим группу движений куба G. Эта группа также является группой преобразований следующих множеств: **а)** множества вершин куба; **б)** множества диагоналей куба; **в)** множества граней куба; **г)*** множества пар вершин куба. Опишите орбиты и стабилизаторы во всех случаях.

Задача 14. Пусть задана группа преобразований G множества X. Докажите, что стабилизатор любого элемента $x \in X$ также является группой преобразований множества X.

Задача 15. Пусть группа G конечна. Докажите, что для любых двух элементов одной орбиты $a, b \in Gx$ выполнено $|G_a| = |G_b|$.

Задача 16. Пусть группа G конечна. Докажите, что для любого $x \in X$ верно $|G| = |Gx| \cdot |G_x|$.

Задача 17. Пусть p — простое число. Рассмотрим множество $\mathbb{Z}_p$ остатков по модулю p и группу G, состоящую из ненулевых остатков, действующих на $\mathbb{Z}_p$ домножениями (т.е. $G = \{1, 2, \ldots, p-1\}$ и $g(x) = x \cdot g$).
а) Найдите орбиты действия этой группы;
б) (*малая теорема Ферма*) Докажите, что $a^{p-1} \equiv 1 \pmod{p}$.

Определение 7. Функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним, называется *функцией Эйлера* и обозначается через $\varphi(n)$.

Задача 18. Пусть n — произвольное число. Рассмотрим множество $\mathbb{Z}_n$ остатков по модулю n, и группу G, состоящую из остатков, взаимно простых с n, действующих на $\mathbb{Z}_n$ домножениями.
а) Докажите, что такое множество преобразований образует группу;
б) Найдите орбиты действия этой группы;
в) (*теорема Эйлера*) Докажите, что если числа a и n взаимно просты, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Задача 19. Образует ли группу множество преобразований плоскости, переводящих прямые в прямые? Что это за преобразования?

8 а	8 б	8 в	9 а	9 б	9 в	10	11	12 а	12 б	12 в	13 а	13 б	13 в	13 г	14	15	16	17 а	17 б	18 а	18 б	18 в	19