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 правильный треугольник ABC (с внутренностью, точки A, B, C идут по часовой стрелке). Обозначим через s_a, s_b и s_c симметрии относительно прямых, содержащих соответствующие высоты треугольника. Далее, обозначим через r_0, r_1 и r_2 повороты вокруг центра треугольника на 0°, 120° и 240° против часовой стрелки соответственно.
а) Докажите, что $G = \{s_a, s_b, s_c, r_0, r_1, r_2\}$ образует группу преобразований треугольника;
б) Выпишите таблицу умножения в этой группе (например, $s_b \circ s_a = r_1$);
в) Придумайте группу преобразований треугольника, состоящую из трёх 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. Если множество X конечно, то группа $S(X)$ называется *симметрической группой* и обозначается S_n.

Задача 4. Пусть множество X является подмножеством прямой, плоскости или пространства. Рассмотрим множество преобразований $\mathrm{Isom}(X) = \{\varphi \in S(X) \mid \varphi \text{ сохраняет расстояния}\}$. Докажите, что вне зависимости от X множество преобразований $\mathrm{Isom}(X)$ является группой. Эта группа называется *группой движений* X.

Задача 5. Докажите, что группа движений треугольника совпадает с группой, описанной в задаче 2.

Задача 6. **а)** Опишите группу движений квадрата (то есть найдите и опишите все её элементы).
б) Придумайте две различных группы преобразований квадрата, состоящих из четырёх преобразований.

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

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

Задача 7. Найдите порядок каждого элемента групп из задач 6 и 2.

Задача 8. Докажите, что в конечной группе каждый элемент имеет конечный порядок.

Задача 9. 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 9б) называется *группой диэдра* и обозначается D_m.

Циклические подгруппы и смежные классы

Задача 10. Рассмотрим множество X остатков по модулю n. Пусть преобразование g — домножение на остаток g (то есть $g(0) = 0$, $g(1) = g$, $g(2) = (2g \mod n)$ и и т. д.).
а) Для $n = 7$ для каждого g расположите остатки X по кругу и нарисуйте стрелочками, куда переходит каждый элемент X при действии g.
б) Нарисуйте аналогичные картинки для остатков по модулю 6.
в) Для каких g и $x \in X$ цепочка стрелочек, начинающаяся с x, заканчивается в 0?
г) Для каких g и $x \in X$ цепочка стрелочек идёт по кругу, проходя через все ненулевые остатки?
д) Для каких g и $x \in X$ цепочка стрелочек никогда не приводит в 0?

Определение 5. Любое подмножество H группы G, являющееся группой преобразований, называется подгруппой. Обозначение: $H \subset G$.

Задача 11. Пусть G — группа преобразований некоторого множества X и g — некоторый её элемент.
а) Докажете, что множество преобразований $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} = \{e, g, g^{-1}, g \circ g, g^{-1} \circ g^{-1}, ...\}$ является подгруппой в G.
б) Пусть порядок элемента g равен k. Тогда в подгруппе $\langle g \rangle$ в точности k элементов.

Определение 6. Если для некоторого элемента g группы $G = \langle g \rangle$, то группа G называется *циклической,* а про элемент g говорят, что он *порождает* группу G.

Задача 12. Пусть $G = \langle g \rangle$ — конечная циклическая группа из n элементов.
а) Найдите порядок элемента g^k;
б) Докажите, что элемент g^k порождает G тогда и только тогда, когда $(n, k) = 1$;
в) Докажите, что подгруппа циклической группы — циклическая.

Определение 7. Пусть G — группа преобразований, а H — её подгруппа. Будем говорить, что элементы $g_1, g_2 \in G$ *сравнимы по модулю* H, и писать $g_1 \equiv g_2 \pmod H$, если найдётся элемент $h \in H$ такой, что $g_2 = g_1 \circ h$. Это определение обобщает определение сравнимости чисел по модулю n.

Задача 13. Докажите, что **а)** если $g_1 \equiv g_2 \pmod H$, то $g_2 \equiv g_1 \pmod H$; **б)** если $g_1 \equiv g_2 \pmod H$ и $g_2 \equiv g_3 \pmod H$, то $g_1 \equiv g_3 \pmod H$;

Определение 8. Таким образом все элементы группы G разбиваются на классы, в которых каждые два элемента сравнимы по модулю H. Эти классы называются *левыми смежными классами* группы G по подгруппе H. Класс элемента g обозначается через gH. Множество всех смежных классов группы G по подгруппе H обозначается через G/H.

Задача 14. (*Теорема Лагранжа*) Докажите, что если G — конечная группа, и H — любая её подгруппа, то $|G| = |H| \cdot |G/H|$.

Задача 15. Докажите, что порядок любого элемента группы делит порядок группы.

Задача 16. Докажите, что всякая конечная группа простого порядка является циклической.

Определение 9. Функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним, называется *функцией Эйлера* и обозначается через $\varphi(n)$.

Задача 17. 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) (*теорема Эйлера*) Докажите, что если числа a и n взаимно просты, то $a^{\varphi(n)} \equiv 1 \pmod n$.

Орбиты и стабилизаторы

Определение 10. *Орбитой* элемента $x \in X$ при действии группы преобразований G называется множество $\{g(x) \mid g \in G\} \subset X$. **Обозначение** Gx.

Задача 18. Найдите орбиту каждой точки при действии группы движений
а) квадрата; **б)** куба; **в)** правильного m-угольника.

Задача 19. **а)** Опишите группу движений единичного круга; **б)** Найдите орбиту каждой точки при действии этой группы; **в)** Найдите преобразование, не имеющее конечного порядка.

Задача 20. Докажите, что любые две орбиты либо совпадают, либо не пересекаются. Следует ли отсюда, что всё множество X есть объединение непересекающихся орбит?

Задача 21. Докажите, что для любых двух элементов одной орбиты $a, b \in Gx$ найдётся элемент $g \in G$, такой что $g(a) = b$.

Определение 11. *Стабилизатором* элемента $x \in X$ при действии группы преобразований G называется множество $\{g \mid g(x) = x\} \subset G$. **Обозначение:** G_x.

Задача 22. Найдите стабилизаторы каждой из точек следующих множеств при действии их групп движений: **а)** квадрата; **б)** куба; **в)** правильного m-угольника.

Задача 23. 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 24. Пусть задана группа преобразований G множества X. Докажите, что стабилизатор любого элемента $x \in X$ также является группой преобразований множества X.

Задача 25. Пусть группа G конечна. Докажите, что для любых двух элементов одной орбиты $a, b \in Gx$ выполнено $|G_a| = |G_b|$.

Задача 26. Пусть группа G конечна. Докажите, что для любого $x \in X$ верно $|G| = |Gx| \cdot |G_x|$.

Задача 27. 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 $a^{p-1} \equiv 1 \pmod{p}$.

Задача 28. Образует ли группу множество преобразований плоскости, переводящих прямые в прямые? Что это за преобразования?

Изоморфизмы групп

Определение 12. Пусть G — группа преобразований множества X, а H — группа преобразований множества Y. Группы G и H называются *изоморфными,* если найдётся биекция $\varphi\colon G \to H$, при которой тождественное преобразование переходит в тождественное, обратное — в обратное, а композиция преобразований — в композицию преобразований, то есть:
(i) $\varphi(\mathrm{id}_X) = \mathrm{id}_Y$;
(ii) для каждого $g \in G$ верно: $\varphi(g^{-1}) = (\varphi(g))^{-1}$;
(iii) для любых $g_1, g_2 \in G$ верно: $\varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2)$.
Отображение φ в этом случае называется *изоморфизмом.* **Обозначение:** $G \simeq H$, $G \overset{\varphi}{\simeq} H$.

Задача 29. Правда ли, что если $G \simeq H$, то **а)** $\#G = \#H$; **б)** $\#X = \#Y$?

Задача 30. Пусть $\varphi\colon G \to H$ — биекция, такая что выполнено условие (iii) определения 12. Докажите, что φ является изоморфизмом.

Задача 31. Докажите, что следующие группы изоморфны:
а) группа вращений правильной 4-угольной призмы (не являющейся кубом) и группа движений квадрата;
б) группа движений куба и группа движений октаэдра;
в) группа вращений правильного n-угольника и группа вычетов по модулю n (см. задачу 35в). Эта группа обозначается $\mathbb{Z}_n$ или $\mathbb{Z}/n\mathbb{Z}$;
г)* группа движений тетраэдра и группа вращений куба.

Задача 32. Пусть $\varphi\colon G \to H$ — изоморфизм. Докажите, что для любого элемента $g \in G$ верно: $\mathrm{ord}(g) = \mathrm{ord}(\varphi(g))$;

Задача 33. Какие из следующих групп изоморфны:
1) группа вращений правильного 24-угольника;
2) группа движений правильного 12-угольника;
3) группа движений правильной 6-угольной призмы;
4) группа движений правильного тетраэдра;
5) группа S_4?

Абстрактные группы

Определение 13. *Абстрактной группой* (или просто *группой*) называется множество G с операцией умножения, обладающей следующими свойствами:
(i) $(ab)c = a(bc)$ для любых $a, b, c \in G$ (*ассоциативность*);
(ii) существует такое элемент $e \in G$ (*единица*), что $ae = ea = a$ для любого $a \in G$;
(iii) для всякого элемента $a \in G$ существует такой элемент $a^{-1} \in G$ (*обратный элемент*), что $aa^{-1} = a^{-1}a = e$.

Задача 34. Докажите, что всякая группа преобразований с операцией композиции является абстрактной группой.

Задача 35. Являются ли следующие множества с указанными операциями группами:
а) $(\mathbb{Z}, +)$; **б)** $(\mathbb{R} \setminus \{0\}, \cdot)$; **в)** (остатки по модулю $5, +$); **г)** (остатки по модулю $5, \cdot$);
д) (ненулевые остатки по модулю $5, \cdot$); **е)** то же самое по модулю 10.

Задача 36. **а)** Пусть G — группа преобразований множества X, и $h \in G$. Докажите, что отображение $L_h\colon G \to G$, $g \overset{L_h}{\longmapsto} h \circ g$ является преобразованием G (такое преобразование называется *левым сдвигом);*
б) Реализуйте произвольную абстрактную группу как группу преобразования некоторого множества.

Задача 37. Докажите, что в группе может быть только одна единица, только один обратный элемент.

Задача 38. Докажите, что группы 1) вращений окружности; 2) комплексных чисел, по модулю равных 1 с операцией умножения; и 3) группа матриц вида $\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ с операцией умножения $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{smallmatrix}\right)$ изоморфны.