Определение 1. Группой $(G, \cdot)$ называется множество G с заданной на нем бинарной операцией $\cdot$, то есть отображением $G \times G \to G$, значение которого на элементах a и b из G обозначается $a \cdot b$ или ab, со следующими свойствами

$$a(bc) = (ab)c \ \ \forall a, b, c \in G \tag{1}$$

$$\exists\, e \in G: \ \forall a \in G \ ea = ae = a \tag{2}$$

$$\forall a \in G \ \exists\, a^{-1} \in G: \ aa^{-1} = a^{-1}a = e \tag{3}$$

Иными словами, существует нейтральный элемент (иногда он называется просто единицей группы и обозначается цифрой 1), и для каждого элемента существует обратный к нему. Свойство (1) называют ассоциативностью.

Замечание 1. Когда операция в группе $(G, \cdot)$ оговорена заранее, то такую группу обозначают просто G.

Задача 1. Проверить, являются ли группами следующие множества с указанными операциями: **а)** $(\mathbb{Z}, +)$; **б)** $(\mathbb{Z}\backslash\{0\}, \cdot)$; **в)** $(\mathbb{R}, \cdot)$; **г)** $(\mathbb{R}\backslash\{0\}, \cdot)$; **д)** $(\mathbb{Z}_m, +)$; **е)** $(\mathbb{Z}_m\backslash\{0\}, \cdot)$; **ж)** S_n с операцией композиции;

з)* Множество $\{a, b, c, d\}$ с операцией $\times$ и таблицей умножения

×	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Задача 2. **а)** Докажите, что в уравнениях в группе можно сокращать, то есть если $ac = bc$ или $ca = cb$, то $a = b$.

Задача 3°. **а)** Докажите, что нейтральный элемент в группе единственный. **б)** Докажите, что для каждого элемента группы обратный элемент единственный. **в)** Докажите, что в группе уравнения $ax = b$ и $xa = b$ имеют единственные решения и найдите их. **г)** Найдите обратный к элементу ab.

Задача 4*. Докажите, что если в определении группы заменить свойства (2) и (3), на «существует элемент e такой, что для любого $a \in G$ $ae = a$ (правая единица) и для любого элемента a существует такой элемент a^{-1}, что $aa^{-1} = e$ (правый обратный)», то определенный объект останется группой.

Группы преобразований

Определение 2. Группой преобразований множества M называется любой непустой набор G биекций этого множества на себя со следующими условиями:

$$g, h \in G \Longrightarrow g \circ h \in G$$

$$g \in G \Longrightarrow g^{-1} \in G$$

То есть множество биекций G замкнуто относительно композиции и взятия обратного отображения.

Задача 5. Покажите, что группа преобразований G произвольного множества M является группой (относительно какой операции?), укажите в явном виде единицу этой группы.

Определение 3. Группой диэдра D_n называется совокупность преобразований правильного n-угольника, являющихся движениями (движение сохраняет расстояние между точками).

Определение 4. Группа G называется абелевой или коммутативной, если $\forall\, a, b \in G$ $ab = ba$.

Задача 6. Покажите, что группа диэдра действительно является группой.

Задача 7. Какие из групп задачи 1 абелевы? Верно ли, что группа диэдра абелева?

Задача 8. **а)** Перечислите все элементы группы D_3 **б)** Перечислите все элементы группы D_4 **в)** Перечислите все элементы группы D_n

1 а	1 б	1 в	1 г	1 д	1 е	1 ж	1 з	2 а	3 а	3 б	3 в	3 г	4	5	6	7	8 а	8 б	8 в

Подгруппы, обыкновенные

Определение 5. Подгруппой H группы G называется такое непустое подмножество элементов группы G, что оно само является группой относительно операции в группе G.

Задача 9. Опишите все подгруппы группы D_3

Задача 10. Рассмотрим элемент g группы G и множество всех его степеней – $\{\dots g^{-2}, g^{-1}, g^0 = e, g, \dots\}$. Докажите, что это множество является подгруппой в G.

Определение 6. Циклической группой называется такая группа G, что существует элемент g такой, что любой элемент группы G является некоторой степенью элемента g. Обозначение $G = \langle g \rangle$

Задача 11. Какие из этих групп являются циклическими? **а)** $(\mathbb{Z}, +)$; **б)** D_4; **в)** $(\mathbb{Q}\backslash\{0\}, \cdot)$; **г)** $(\mathbb{Z}_m, +)$; **д)*** $(\mathbb{Z}_p\backslash\{0\}, \cdot)$, где p – простое число.

Смежные классы по подгруппе

Определение 7. Пусть задана группа G и ее подгруппа H, $g \in G$. Тогда назовем левым смежным классом элемента g по подгруппе H множество элементов вида gh, где $h \in H$. Обозначение gH. Аналогично определяем правый смежный класс элемента g (Hg).

Задача 12. Рассмотрим группу S_3 и ее подгруппу $\{(1,2), id\}$. Выпишите все левые и правые смежные классы по этой подгруппе и покажите, что левые и правые смежные классы совпадают не у всех элементов.

Задача 13. Пусть есть два левых смежных класса gH и g_1H. Докажите, что тогда они либо не пересекаются, либо совпадают.

Задача 14. Сопоставим элементам gh_1, $gh_2 \dots$ смежного класса gH элементы g_1h_1, $g_1h_2 \dots$ смежного класса g_1H, не пересекающегося с gH. Докажите, что это отображение смежных классов как множеств биективно.

Определение 8. Порядком конечной группы G называется число ее элементов. Обозначение $\operatorname{ord} G$ или $|G|$.

Определение 9. Порядком элемента g конечной группы G называется $\min\{k \in \mathbb{N} : g^k = e\}$. Обозначение $\operatorname{ord} g$.

Задача 15. Докажите, что $g^k = e \Longleftrightarrow \operatorname{ord} g | k$.

Задача 16. **а)** Докажите, что множество элементов группы G есть дизъюнктное объединение различных левых смежных классов по данной подгруппе H. **б)** (*Теорема Лагранжа*) Пусть группа G конечна. Докажите, что порядок группы G делится на порядок любой ее подгруппы H. **в)** В условиях предыдущего пункта докажите, что порядок G делится на порядок любого своего элемента.

Задача 17. Докажите, что конечная группа является циклической тогда и только тогда, когда существует элемент, порядок которого совпадает с порядком группы.

Задача 18. Пусть циклическая группа $\langle g \rangle$ имеет порядок k. Рассмотрим циклическую подгруппу этой группы, порожденную m-й степенью g, то есть $\langle g^m \rangle$. В каких случаях эта подгруппа будет совпадать со всей группой?

Задача 19. Докажите, что любая группа порядка p, где p – простое число, циклическая.

Задача 20. Объясните решение задачи 13[32] на языке теории групп.

Задача 21. Докажите теорему Эйлера: $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ – количество чисел, не превосходящих m и взаимнопростых с m с помощью теории групп.

9	10	11 а	11 б	11 в	11 г	11 д	12	13	14	15	16 а	16 б	16 в	17	18	19	20	21