Группы и подгруппы.

Напомним, что если в группе G с операцией умножения $\circ$ есть подмножество H, являющееся группой относительно операции $\circ$, то говорят, что H — ***подгруппа*** группы G и пишут $H \leqslant G$.

1) Докажите, что если G конечна, то любое подмножество H, замкнутое относительно групповой операции (то есть, такое, что произведение любых двух элементов из H снова принадлежит H), является подгруппой в G.

2) Приведите пример, показывающий, что для бесконечной группы G утверждение задачи 1, вообще говоря, неверно.

3) Докажите, что каждая подгруппа циклической группы циклическая.

4) а) Докажите, что если $H_1 \leqslant G$ и $H_2 \leqslant G$, то $H_1 \cap H_2 \leqslant G$.
б) Докажите, что пересечение любого набора подгрупп некоторой группы снова является её подгруппой.

5) Докажите, что а) $\mathbb{Z}_4 \leqslant \mathbb{Z}_{12}$, б) $\mathbb{Z}_n \leqslant D_n$, в) $\mathbb{Z}_4 \leqslant \mathbb{C}^*$, г) $D_n \leqslant S_n$, д) $\mathbb{Z}_4 \leqslant S_4$.

6) Докажите ***теорему Лагранжа***: Порядок конечной группы делится на порядок любой её подгруппы. Для этого, если $H \neq G$, найдите элемент $g \in G$, не лежащий в H, и умножьте его на все элементы группы H: gh_1, gh_2, gh_3, gh_4 ... Если и на этом G не исчерпалась, выберите ...

7) Выведите из теоремы Лагранжа, что порядок конечной группы делится на порядок любого элемента.

* * *

8) Рассмотрим для натурального $n > 1$ множество $\mathbb{Z}_n^*$ натуральных чисел, меньших n и взаимно простых с n. На этом множестве рассмотрим операцию умножения по модулю n. Докажите, что $\mathbb{Z}_n^*$ группа и найдите её порядок.

9) Используя предыдущие задачи, докажите теорему Ферма-Эйлера: если a и n $(n > 1)$ взаимно просты, то $a^{\varphi(n)} = 1 (\bmod n)$.

10) Докажите теорему Вильсона: если p — простое, то $(p-1)! = -1 (\bmod p)$.

* * *

11) Рассмотрим *алфавит* (множество букв) $A = a_1, a_2, \ldots a_n$ и *«антиалфавит»* $\bar{A} = \bar{a}_1, \bar{a}_2, \ldots \bar{a}_n$. Назовём *словом* конечную (возможно, пустую) последовательность букв, в которой рядом не стоят буква и соответствующая ей антибуква. Произведением слов α и β будем считать слово, получающееся, если после слова α приписать слово β, а затем последовательно убрать все пары соседей «буква-антибуква». Докажите, что множество слов с такой операцией является группой. Эта группа называется ***свободной группой***, порождённой алфавитом A.

Группы и подгруппы.

Напомним, что если в группе G с операцией умножения $\circ$ есть подмножество H, являющееся группой относительно операции $\circ$, то говорят, что H — ***подгруппа*** группы G и пишут $H \leqslant G$.

1) Докажите, что если G конечна, то любое подмножество H, замкнутое относительно групповой операции (то есть, такое, что произведение любых двух элементов из H снова принадлежит H), является подгруппой в G.

2) Приведите пример, показывающий, что для бесконечной группы G утверждение задачи 1, вообще говоря, неверно.

3) Докажите, что каждая подгруппа циклической группы циклическая.

4) а) Докажите, что если $H_1 \leqslant G$ и $H_2 \leqslant G$, то $H_1 \cap H_2 \leqslant G$.
б) Докажите, что пересечение любого набора подгрупп некоторой группы снова является её подгруппой.

5) Докажите, что а) $\mathbb{Z}_4 \leqslant \mathbb{Z}_{12}$, б) $\mathbb{Z}_n \leqslant D_n$, в) $\mathbb{Z}_4 \leqslant \mathbb{C}^*$, г) $D_n \leqslant S_n$, д) $\mathbb{Z}_4 \leqslant S_4$.

6) Докажите ***теорему Лагранжа***: Порядок конечной группы делится на порядок любой её подгруппы. Для этого, если $H \neq G$, найдите элемент $g \in G$, не лежащий в H, и умножьте его на все элементы группы H: gh_1, gh_2, gh_3, gh_4 … Если и на этом G не исчерпалась, выберите …

7) Выведите из теоремы Лагранжа, что порядок конечной группы делится на порядок любого элемента.

* * *

8) Рассмотрим для натурального $n > 1$ множество $\mathbb{Z}_n^*$ натуральных чисел, меньших n и взаимно простых с n. На этом множестве рассмотрим операцию умножения по модулю n. Докажите, что $\mathbb{Z}_n^*$ группа и найдите её порядок.

9) Используя предыдущие задачи, докажите теорему Ферма-Эйлера: если a и n ($n > 1$) взаимно просты, то $a^{\varphi(n)} = 1 (\operatorname{mod} n)$.

10) Докажите теорему Вильсона: если p — простое, то $(p-1)! = -1 (\operatorname{mod} p)$.

* * *

11) Рассмотрим *алфавит* (множество букв) $A = a_1, a_2, \dots a_n$ и *«антиалфавит»* $\bar{A} = \bar{a}_1, \bar{a}_2, \dots \bar{a}_n$. Назовём *словом* конечную (возможно, пустую) последовательность букв, в которой рядом не стоят буква и соответствующая ей антибуква. Произведением слов α и β будем считать слово, получающееся, если после слова α приписать слово β, а затем последовательно убрать все пары соседей «буква-антибуква». Докажите, что множество слов с такой операцией является группой. Эта группа называется ***свободной группой***, порождённой алфавитом A.