Группы. Теория

Группой $(G, \circ)$ называется множество G с заданной на нём бинарной операцией $\circ$, удовлетворяющей следующим свойствам:

1. (замкнутость) Для любых элементов $a, b \in G$ верно, что $a \circ b \in G$;
2. (ассоциативность) Для любых элементов $a, b, c \in G$ выполняется равенство $a \circ (b \circ c) = (a \circ b) \circ c$;
3. (нейтральный элемент) Существует элемент $e \in G$ такой, что $a \circ e = e \circ a = a$ для любого $a \in G$. Этот элемент e называется нейтральным;
4. (обратный элемент) Для каждого элемента $a \in G$ найдётся элемент $b \in G$ такой, что $a \circ b = b \circ a = e$. Элемент b называется обратным для a и обозначается a^{-1}.

Если дополнительно для любых $a, b \in G$ выполняется свойство $ab = ba$, то группа называется **коммутативной** или **абелевой**.

Если не возникает путаницы, то группу обозначают также как и множество, на котором она задана. То есть вместо «группа $(G, \circ)$» говорят и пишут «группа G».

Порядком конечной группы G называется число её элементов. Обозначение: $|G|$.

Порядком элемента группы называется наименьшая натуральная степень, при возведении в которую элемент становится нейтральным: $g^m = g \circ \dots \circ g = e$. Если такой степени не существует, то говорят, что элемент имеет бесконечный порядок.

Примеры:

1. Числовые группы по сложению: $(\mathbb{Z}_n, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$.
2. Числовые группы по умножению: $(\mathbb{Z}_p \setminus \{0\}, *)$, $(\mathbb{Q} \setminus \{0\}, *)$, $(\mathbb{R} \setminus \{0\}, *)$, $(\mathbb{C} \setminus \{0\}, *)$.
3. Множество перестановок S_n и множество чётных перестановок A_n с операцией композиции.
4. Множества движений плоскости и пространства с операцией композиции.
5. Множество движений плоскости, переводящих правильный n-угольник в себя, с операцией композиции. Обозначение: D_n. Группа D_n состоит из n поворотов и n осевых симметрий.

Группы $(G, *)$ и $(H, \cdot)$ называются **изоморфными**, если существует взаимно однозначное соответствие $f : G \to H$, сохраняющее групповые операции: $\forall u, v \in G$ верно $f(u*v) = f(u) \cdot f(v)$. Отображение f называется **изоморфизмом** данных групп.

Левым смежным классом элемента $a \in G$ по подгруппе H называется множество $aH = \{ah \mid h \in H\}$. Аналогично определяется **правый смежный класс** $Ha = \{ha \mid h \in H\}$. Подгруппа H группы G называется **нормальной**, если $gH = Hg$ для всех $g \in G$.

Элементы g и h называются **сопряженными** в группе G, если найдётся элемент $f \in G$ такой, что $fg = hf$ (или $g = f^{-1}hf$). Обозначение: $g \sim h$.

Легко проверить, что $\sim$ является отношением эквивалентности. Соответствующие классы эквивалентности называются **классами сопряжённости**.

Группы. Задачи

Entry level:

1. Пусть $|G| = 2n$. Докажите, что найдётся элемент $g \in G$ порядка 2.

2. Докажите, что группа, в которой все неединичные элементы имеют порядок 2, абелева.

3. В группе есть три элемента порядка 4. Докажите, что найдется и четвертый элемент этого порядка.

4. *(Теорема Лагранжа.)* Если группа G конечна, а H — её произвольная подгруппа, то $|H|$ делит $|G|$.

Intermediate level:

5. Пусть подгруппа H имеет всего 2 левых смежных класса в G. Докажите, что H — нормальная подгруппа.

6. Опишите группу самосовмещений куба.

7. *(Теорема Кэли.)* Докажите, что любая конечная группа изоморфна какой-то подгруппе S_n для достаточно большого n.

Advanced level:

8. Докажите, что мощность класса сопряжённости элемента конечной группы $g \in G$ равна количеству левых смежных классов подгруппы $Z_g = \{z \in G \mid z^{-1}gz = g\}$ в G.

9. Покажите, что число неизоморфных конечных групп, содержащих менее миллиона классов сопряжённости, конечно.

10. Назовём элемент конечной группы угрюмым, если он не коммутирует ни с кем, кроме самого себя и единицы. Покажите, что в неединичной группе угрюмых элементов либо ровно половина, либо вовсе нет.