Введение в теорию групп

Лекция 2

Теорема Лагранжа

Определение 1. Непустое подмножество H группы G называется *подгруппой*, если

$$\forall x, y \in H \; xy \in H \wedge x^{-1} \in H.$$

Задача 1. Для любой подгруппы $H \subset G : e \in H$.

Задача 2. Найдите все подгруппы группы целых чисел $(\mathbb{Z}, +)$.

Определение 2. Пусть H — подгруппа группы G, $g \in G$. Тогда *правым* (*левым*) *смежным классом элемента g по подгруппе H* называется множество

$$gH = \{gh \mid h \in H\} \quad (Hg = \{hg \mid h \in H\}).$$

Задача 3. Пусть G — группа, H — ее подгруппа, $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \emptyset$.

Задача 4 (теорема Лагранжа). Если G — конечная группа, H — ее подгруппа, то количество правых (левых) смежных классов G по H равно $G : H$ (это количество называется *индексом* подгруппы H в группе G).

Определение 3. *Порядком* элемента g группы G называется минимальное натуральное число $n > 0$ такое, что $g^n = e$. Если такого числа не существуют, то говорят, что порядок элемента g бесконечен.

Задача 5. В конечной группе порядок любого элемента делит порядок группы.

Задача 6 (малая теорема Ферма). Для любого простого числа p и любого натурального a, не делящегося на р, верно

$$a^{p-1} \equiv 1 \mod p.$$