Лекция №6

1.6 Классы вычетов и теорема Лагранжа

1.6.1 Свойства классов вычетов

Определение 1. *Пусть G – группа, H – подмножество в G. Для $\forall a \in G$ обозначим $aH = \{ah | h \in H\}$ (аналогично, $Ha = \{ha | h \in H\}$) и $aHa^{-1} = \{aha^{-1} | h \in H\}$). Если H – подгруппа в G, то множество aH называется левым классом вычетов, Ha – правым классом вычетов, а элемент a называется представителем класса. За $|aH|$, $|Ha|$ будем обозначать число элементов в aH, Ha соответственно.*

Лемма 1. *Пусть H – подгруппа в группе G, $a, b \in G$. Тогда*

1. $a \in aH$;
2. $aH = H \Leftrightarrow a \in H$;
3. $aH = bH \Leftrightarrow a \in bH (b \in aH)$;
4. $aH = bH$ или $aH \cap bH = \varnothing$;
5. $aH = bH \Leftrightarrow a^{-1}b \in H$;
6. $|aH| = |bH|$;
7. $aH = Ha \Leftrightarrow H = aHa^{-1}$;
8. aH – подгруппа в $G \Leftrightarrow a \in H$.

1.6.2 Теорема Лагранжа и следствия

Теорема 1 (Лагранжа)**.** *Если G – конечная группа, H – подгруппа G, тогда $|H|$ делит $|G|$. Кроме того, число различных левых (правых) классов вычетов по подгруппе H в G равно $\frac{|G|}{|H|}$.*

Определение 2. *Число различных левых классов вычетов по подгруппе H в группе G называется индексом подгруппы H в G. Обозначается $|G : H|$ или $(G : H)$.*

Следствие 1. *Если G – конечная группа, H – подгруппа в G, то $(G : H) = \frac{|G|}{|H|}$.*

Следствие 2. *В конечной группе порядок каждого элемента группы делит порядок самой группы.*

Следствие 3. *Группа простого порядка – циклическая.*

Следствие 4. *Пусть G – конечная группа, $a \in G$. Тогда $a^{|H|} = e$.*

Следствие 5 (Малая теорема Ферма)**.** *Для произвольных целого a и простого p справедливо $a^p \equiv 1 (mod\ p)$.*

1.6.3 Приложение классов вычетов к группам перестановок

Определение 3. *Пусть G – группа перестановок множества S. Для $\forall i \in S$ положим*

$$stab_G(i) = \{\varphi \in G | \varphi(i) = i\}.$$

Данное множество называется стабилизатором элемента i в G.

Определение 4. *Пусть G – группа перестановок множества S. Для $\forall s \in S$ положим*

$$orb_G(s) = \{\varphi(s) | \varphi \in G\}.$$

Данное множество называется орбитой элемента s относительно G.

Теорема 2. *Пусть G – конечная группа перестановок множества S. Тогда для произвольного $i \in S$ имеет место:*

$$|G| = |orb_G(i)| \cdot |stab_G(i)|.$$