Разложение группы по подгруппе

Пусть G – группа, H – её подгруппа. Определим отношение λ правилом

$$x\ \lambda\ y, \text{ если } x^{-1}y \in H.$$

Отношение λ рефлексивно, симметрично и транзитивно, поскольку H – подгруппа.

Следовательно, отношение λ определяет разбиение группы G.

Пусть M – некоторое подмножество группы G, $a \in G$, не обязательно принадлежащий M. Обозначим через aM множество $\{am \mid m \in M\}$. Тогда условие $x^{-1}y \in H$ равносильно $y \in xH$. Это означает, что каждый класс эквивалентности отношения λ совпадает с множеством xH для некоторого элемента x из этого класса.

?	Верно ли, что в качестве x можно брать любой элемент из этого класса?

Пусть e – нейтральный элемент группы G. Тогда класс eH совпадает с H, т.е. сама подгруппа H является одним из классов разбиения.

Выберем из каждого класса (кроме H) по элементу: a_1, a_2, … . Тогда

$$G = H \cup a_1H \cup a_2H \cup \ldots .$$

Такое представление группы называется её ***левым разложением по подгруппе***.

?	Каким будет левое разложение группы G, если $H = \{e\}$? А если $H = G$?

Естественно рассмотреть отношение ρ, которое определяется равенством

$$x\ \rho\ y, \text{ если } yx^{-1} \in H.$$

Отношение ρ тоже является отношением эквивалентности. Каждый класс разбиения для этого отношения представлен множеством Hx. Соответствующее представление группы как объединения классов этого разбиения называется ***правым разложением по подгруппе***.

Если группа коммутативна, то очевидно, что левое разложение группы по подгруппе совпадает с правым.

!	Пусть $G = S_3$, $H = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}; \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\right\}$. Постройте левое и правое разложения группы G по подгруппе H и убедитесь, что они различны.

Посмотрев на построенные вами разложения, вы можете увидеть, что во всех классах – и правых, и левых – одно и то же число элементов. Да и классов в каждом разложении тоже одинаковое количество. Это не случайное совпадение.

Теорема. Любые два класса разложения группы по подгруппе равномощны. Множество левых классов разложения равномощно множеству правых классов.

Доказательство. Покажем, что любой левый класс равномощен подгруппе H. Определим отображение f: $H \to xH$ правилом $f(h) = xh$. Всюду определённость, однозначность и сюръективность функции f очевидна. Если вдруг $f(h) = xh_1$, из $xh = xh_1$ следует, что $h = h_1$, т.е. отображение f инъективно. Аналогично любой правый класс равномощен подгруппе H, а значит, и все классы между собой равномощны.

Теперь определим отображение f множества левых классов разложения в множество правых правилом $f(xH) = Hx^{-1}$. Для этого отображения всюду определённость и сюръективность очевидны.

Докажем однозначность отображения f. Допустим, что $f(xH) = f(yH)$, т.е. $Hx^{-1} = Hy^{-1}$. Это означает, что $x^{-1} \rho y^{-1}$, т.е. $y^{-1}(x^{-1})^{-1} \in H$. Но $y^{-1}(x^{-1})^{-1} = y^{-1}x$, так что $y \lambda x$, поэтому $yH = xH$.

Докажем инъективность отображения f. Пусть совпали прообразы разных классов Hx^{-1} и Hy^{-1}, т.е. $xH = yH$. Тогда $x \lambda y$, т.е. $x^{-1}y \in H$. Но $x^{-1}y = x^{-1}(y^{-1})^{-1}$, так что $y^{-1} \rho x^{-1}$. Следовательно, $Hy^{-1} = Hx^{-1}$.

Если группа G конечна, то количество элементов в группе называется ***порядком группы***. Обозначение $| G |$ или $o(G)$. Количество классов в разложении группы по подгруппе (ввиду теоремы неважно в левом или правом) называется ***индексом подгруппы в группе***. Индекс подгруппы H в группе G обозначают $|G : H|$.

Из теоремы с очевидностью вытекает

Следствие 1 (теорема Лагранжа). Порядок конечной группы равен произведению порядка подгруппы на её индекс.

Формулой это записывается так: $| G | = | H | \, |G : H|$.

Следствие 2. Группа простого порядка циклическая.

Доказательство. Пусть a – элемент группы простого порядка, отличный от нейтрального. Тогда подгруппа $< a >$ должна совпасть со всей группой, иначе её порядок больше 1 и при этом делит порядок группы, который есть простое число – противоречие.