Гомоморфизмы групп

Гомоморфизм алебраических структур – это отображение, перестановочное с операциями на этих структурах. То есть если мы сначала применяем операцию, а потом к ее результату применяем отображение, результат получается такой же, как если бы мы сначала выполнили отображение, а потом к полученным образам применили бы операцию (уже в другой структуре).

Например, линейное отображение – это гомоморфизм линейных пространств.

Для групп это, в частности, означает, что если в группе G определена операция $*$, а в группе H – операция $\odot$, и f – гомоморфное отображение из G в H, то для любых элементов u и v группы G верно равенство $f(u * v) = f(u) \odot f(v)$.

Если гомоморфизм является помимо прочего еще и биекцией, он называется *изоморфизмом*, а структуры, между которыми существует изоморфизм, называются *изоморфными*. Фактически эти структуры отличаются только обозначениями элементов, все алгебраические свойства этих структур полностью одинаковы. Например, изоморфны любые пространства заданной размерности над одним и тем же полем (если зафиксировать в этих пространствах базисы, в качестве изоморфизма можно выбрать отображение, которое сопоставляет каждому вектору одного пространства вектор другого пространства с теми же координатами).

Ядром гомоморфизма называют множество элементов группы G, образ которых равен нейтральному элементу группы H (вспомните ядро линейного отображения). Легко проверить, что и ядро, и образ группы являются группами (подгруппами, соответственно G и H). При этом ядро обязательно является нормальной подгруппой, а образ может быть нормальной подгруппой, а может и не быть.

Справедлива следующая теорема (ее часто называют *первой теоремой о гомоморфизме*).

<u>Теорема.</u> Гомоморфный образ группы изоморфен факторгруппе отображаемой группы по ядру гомоморфизма: $f(G) \cong G \,/\, Kerf$.

В качестве примера рассмотрим гомоморфизмы циклических групп. Пусть G – это группа порядка n с образующей a и операцией $*$, а H – группа порядка m с образующей b и операцией $\odot$.

Для начала заметим, что образ гомоморфизма – это подгуппа группы G, следовательно, порядок образа должен делить порядок группы G. В то же время, образ изоморфен факторгруппе группы G, следовательно, его порядок должен делить и порядок группы G.

Теперь вспомним, что всякая подруппа циклической группы сама является циклической. Отсюда следует, что образующая группы G должна под действием гомоморфизма переходить в элемент группы H, порядок которого делит порядок этой группы. В итоге мы видим, что порядок образа гомоморфизма должен быть общим делителем порядков G и H, пусть это будет число d. В группе H есть только одна подгруппа порядка d: это подгруппа U, состоящая из степеней элемента $c = b^{\frac{m}{d}}$. Этот элемент (или какой-нибудь другой образующий элемент подруппы U) и должен быть образом образующего элемента группы G, то есть все возможные гомоморфизмы выбранных групп устроены так: $f(a) = c^k$, где k – произвольное целое число, взаимно простое с (то есть любая образующая группы U), для всех остальных элементов группы G образ определяется по правилу : $f(a^t) = c^{tk}$. Заметим, что если e и e_1 – нейтральные элементы групп G и H соответственно, то верно равенство $f(a^n) = f(e) = c^{nk} = b^{\frac{mnk}{d}} = e_1$, то есть при построенном нами гомоморфизме, как и положено, нейтральный элемент перешел в нейтральный.

Ядро у всех этих гомоморфизмов одно и то же – это множество элементов вида a^{dt}, они, очевидно, образуют подгруппу порядка $\frac{n}{d}$.

В завершение заметим, что любой гомоморфизм из группы G в группу H однозначно определяется выбором элемента $b^{\frac{mk}{d}}$, и это определение будет корректно тогда и только тогда, когда число d является общим делителем порядков групп G и H. Обратите внимание: число k при этом может быть любым, но если оно взаимно просто с d, то мы получим гомоморфизм с образом порядка d, а если k и d имеют обшие делители, то порядок образа будет делителем числа d.

Итак, количество разных гомоморфизмов циклических групп G и H, образ которых состоит из d элементов (где d – общий делитель порядков групп G и H), равно количеству натуральных чисел, меньших d и взаимно простых с ним (напомним, что это число называется функцией Эйлера от d).

Мультипликативная группа кольца вычетов

Напомним, что мультипликативной группой поля или коммутативного кольца с единицей называется множество всех его элементов, обратимых по умножению. Для начала заметим, что это множество обязательно является группой (проверьте это самостоятельно).

Очевидно, что в поле это просто множество всех его элементов, отличных от 0. В произвольном кольце это не так, например, в кольце целых чисел обратимых элементов всего два (1 и –1), а в кольце многочленов над полем обратимыми являются все ненулевые константы. Довольно часто группу обратимых элементов кольца называют *группой единиц*.

Основная теорема о мультипликативной группе конечного поля гласит, что эта группа обязательно является циклической.

Рассмотрим в качестве примера поле классов вычетов по модулю 13. Мультипликативная группа этого поля состоит из 12 элементов: $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}$. Образующим элементов в этой группе является например, , $\overline{2}$. Ниже приведен список последовательных степеней этого элемента: $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^4 = \overline{3}$, $\overline{2}^5 = \overline{6}$, $\overline{2}^6 = \overline{12}$, $\overline{2}^7 = \overline{11}$, $\overline{2}^8 = \overline{9}$, $\overline{2}^9 = \overline{5}$, $\overline{2}^{10} = \overline{10}$, $\overline{2}^{11} = \overline{7}$, $\overline{2}^{12} = \overline{1}$. Из этого списка, в частности, видно, что образующими в этой группе также являются элементы $\overline{2}^5 = \overline{6}$, $\overline{2}^7 = \overline{11}$ и $\overline{2}^{11} = \overline{7}$. Все остальные элементы имеют порядок строго меньше, чем 12.

Рассмотрим теперь кольцо вычетов по модулю 12. В этом кольце 12 элементов: $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{0}$, причем обратимыми из них являются только 4: $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. Действительно, если класс $\overline{a}$ обратим по модулю 12, это значит, что найдется класс $\overline{b}$, такой, что разность $ab - 1$ делится на 12, но если число a имеет нетривиальный общий делитель с 12, эта разность при любом b будет взаимно проста с 12. Поэтому обратимыми элементами кольца являются только те классы, представители которых взаимно просты с модулем, то есть те, которые мы перечислили.

Теперь легко проверить, что что эта группа не является циклической: $\overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$. Заметим, что это самая маленькая нециклическая группа, она носит название *четверная группа Клейна* (в память о немецком математике Феликсе Клейне, который первым ее описал). Эта группа является прямым произведением двух циклических подгрупп (например, $\{\overline{1}, \overline{5}\}$ и $\{\overline{1}, \overline{7}\}$). Также она изоморфна группе самосовмещений ромба (тождественное преобразование, поворот на 180 градусов и два поворота вокруг диагоналей). Каждое из этих самосовмещений, кроме тождественного, имеет порядок 2, и произведение любых двух из них равно третьему.