Семинар №2 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Подгруппы

Определение 1 (Подгруппа)
H называется подгруппой группы $G = \langle M, * \rangle$, если $H = \langle M', * \rangle$ — это группа и $M' \subset M$. Это обозначается $H < G$.

Замечание 1
Несложно убедиться, что для того, чтобы H была подгруппой G необходимо и достаточно выполнение трёх условий (помимо $H \subseteq G$):

1. $e \in H$
2. $\forall a, b \in H \quad a \cdot b \in H$
3. $\forall x \in H \quad x^{-1} \in H$

В учебнике, например, именно они даны как определение подгруппы.

Пример 1
В группе целых чисел по сложению, числа кратные m образуют подгруппу.

Теорема 1 (Критерий подгруппы)

$$H < G \quad \Leftrightarrow \quad \forall a, b : a, b \in H \quad a \cdot b^{-1} \in H$$

Доказательство $\Rightarrow$. В эту сторону все достаточно очевидно. Если $H < G$, то

$$\forall a, b \in H \quad b^{-1} \in H \text{ (3 акс.)} \Rightarrow ab^{-1} \in H \text{(замкнутость)}$$

$\Leftarrow$. Пусть $\forall a, b \in H \; ab^{-1} \in H$. Тогда

1. Если H непусто, то $\exists x \in H$. Пусть $a = b = x$, тогда
$$ab^{-1} = xx^{-1} = e \in H$$
2. Пусть $a = e$, тогда
$$\forall b \in H \; eb^{-1} = b^{-1} \in H$$
3. Возьмем произвольные $x, y \in H$. Из п.2 $y^{-1} \in H$. Пусть $a = x, b = y^{-1}$, тогда
$$\forall x, y \in H \; ab^{-1} = x(y^{-1})^{-1} = xy \in H$$

Лемма 1 (Пересечение подгрупп)
Пересечение подгрупп является подгруппой.

Доказательство Пусть $H_1, H_2 < G$. Пусть $a, b \in H_1 \cap H_2$. То есть $a, b \in H_1$; $a, b \in H_2$, откуда $ab^{-1} \in H_1$; $ab^{-1} \in H_2$.
Значит, $ab^{-1} \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 < G$, ч.т.д.

Определение 2 (Смежные классы)
Пусть $H < G$, а x — это элемент G.
Левым смежным классом с представителем x называется

$$xH = \{y \mid y = xh, h \in H\}$$

Правым смежным классом с представителем x называется

$$Hx = \{y \mid y = hx, h \in H\}$$

Замечание 2
Мы используем общую нотацию перемножения множеств:

$$AB = \{ab \mid a \in A, b \in B\}$$

Исходя из этого определения, ясно что

$$A = B \iff XA = XB$$

В частности, это верно для одноэлементных множеств (мы опускаем скобки, записывая $\{x\}A$ как xA).

Стоит обратить внимание, что существует понятие левых и правых смежных классов. В общем случае группы некомутативны, и левый и правый смежные классы с одним и тем же представителем могут различаться. В связи с этим, выделяют подгруппы, где этого не происходит.

Определение 3 (Нормальная подгруппа)
Подгруппа $H < G$ называется *нормальной* подгруппой группы G, если

$$\forall x \in G \quad xH = Hx$$

Замечание 3
Очевидно, что в коммутативной группе все подгруппы являются нормальными.

Замечание 4
Стоит обратить внимание, что, говоря о совпадении классов, мы говорим о равенстве множеств. *Из того, что при любом x выполняется $xH = Hx$ не следует, что для всех $h \in H$ выполняется $xh = hx$. Поэтому нормальные подгруппы бывают не только у абелевых групп.*

Теорема 2 (Теорема о смежных классах)
Левые (правые) смежные классы по одной подгруппе либо совпадают, либо не пересекаются.

Доказательство Зафиксируем какую-то $H < G$. По сути, утверждение теоремы таково: если $xH \cap yH \neq \varnothing$, то $xH = yH$.
Пусть $xH \cap yH \ni z$. Тогда $z = xh_1 = yh_2$. Отсюда $x = yh_2h_1^{-1} \in yH$; $y = xh_1h_2^{-1} \in xH$.
Итак, $x \in yH$, то есть $\exists h_x : \ x = yh_x$. Возьмем произвольный $t \in xH$.
$t = xh_t = yh_xh_t \in yH$. Значит, $xH \subseteq yH$.
Аналогично, $yH \subseteq xH$. Значит, $xH = yH$.

$e \in H$, поэтому $\forall g \in G \ g \in gH$, то есть всякий элемент группы лежит в каком-то классе.
Тогда теорема о смежных классах по сути говорит нам, что при фиксированной подгруппе H вся группа разивается на так называемые *классы смежности* по данной подгруппе. Рассмотрим какой-то класс xH. Возьмем $h_1, h_2 \in H, h_1 \neq h_2$. Мы знаем, что $xh_1 \neq xh_2$ (мы говорили об этом на прошлом семинаре, в учебнике это называется свойством *сократимости*, которое есть у всех групп). Тогда $|xH| = |H|$.
Таким образом, вся группа разбивается на объединение смежных классов одинаковой мощности, равной мощности H.

Определение 4 (Индекс подгруппы)
Индексом подгруппы $H < G$ называется число смежных классов по данной подгруппе.
Обозначение: $(G : H)$.

Таким образом, мы доказали важную теорему.

Теорема 3 (Теорема Лагранжа)
Пусть $H < G$. Тогда

$$|G| = (G : H) \cdot |H|$$

В частности, порядок H делит порядок группы.

Из этих же рассуждений ясно, что число левых и правых смежных классов по подгруппе совпадает (но не факт, что совпадают сами классы!). Таким образом, понятие индекса подгруппы корректно.

Сформулируем утверждение о принадлежности элементов одному классу смежности.

Лемма 2
Два элемента группы g_1 и g_2 принадлежат одному классу смежности по подгруппе H тогда и только тогда, когда $g_1^{-1} g_2 \in H$.

Доказательство Это ясно из того, что $g_1 H = g_2 H \iff H = g_1^{-1} g_2 H$ (мы домножили обе части уравнения на g^{-1}).

Циклические группы

Определение 5 (Циклическая группа)
Группа называется циклической, если выполнено следующее

$$\exists a : a \in M \quad \forall b : b \in M \quad \exists k : k \in \mathbb{Z} \quad b = a^k$$

Элемент a называют *порождающим* элементом.

Пример 2
Группа корней из единицы, о которой мы говорили ранее, является циклической группой. В ней порождающим элементом является $\exp \frac{2\pi i}{n}$.

Теорема 4 (Коммутативность циклических групп)
Циклические группы коммутативны.

Доказательство Пусть a — это порождающий элемент.

$$\forall\ b, c :\ \ b * c = a^k * a^t = a^{k+t} = a^{t+k} = a^t * a^k = c * b$$

Пример 3
Порождающий элемент может быть не единственным. Например, рассмотрим группу остатков от деления на 4. *В ней, очевидно,* 1 *является порождающим элементом, но можно так же заметить, что им является и* 3.

$$3 = 3;\ 3 + 3 = 2;\ 3 + 3 + 3 = 1;\ 3 + 3 + 3 + 3 = 0$$

Рассмотрим устройство циклических групп.

1. Все степени порождающего элемента различны. Тогда это бесконечная группа, по существу совпадающая (т.е. *изоморфная* — об этом позже) с группой $\langle \mathbb{Z}, + \rangle$.

2. Какие-то две степени совпадают, т.е. $a^{n+m} = a^n,\ m \neq 0$.
   В этом случае $a^{n+m} = a^n a^m = a^n \Rightarrow a^m = e$.
   Так как $a^m = e \Leftrightarrow a^{-m} = e$, то для определенности будем считать $m > 0$. Тогда получается, что для хотя бы одного натурального числа m выполняется $a^m = e$.
   Возьмём наименьшее такое число q.

Определение 6 (Порядок элемента)
Порядком элемента a называется наименьшее натуральное число q такое, что $a^q = e$.
Если такого числа нет, то элемент имеет *бесконечный порядок*.

Рассмотрим два числа $t, l:\quad 1 \leqslant l < t \leqslant q - 1$. Пусть $a^t = a^l$.
Тогда $a^{t-l} = e$, но $t - l < q$, значит q не будет наименьшим. Значит, все a^k, где $0 \leqslant k < q$, различны.
Рассмотрим произвольный a^n. Разделим с остатком: $n = sq + m,\ 0 \leqslant m < q$.
Тогда $a^n = (a^q)^s \cdot a^m = e \cdot a^m = a^m$.
Значит, вся группа выглядит как $G = \left\{a^n \mid 0 \leqslant n < q,\ n \in \mathbb{N}\right\}$

Циклические подгруппы

Рассмотрим произвольную группу. Возьмём некоторый элемент a и его всевозможные целые степени.

Определение 7 (Группа, порожденная элементом)
Подгруппа, *порожденная элементом* a группы G:

$$\langle a \rangle = \left\{a^n \mid n \in \mathbb{Z}\right\}$$

Из предыдущих рассуждений ясно, что это будет циклическая группа с порождающим элементом a. В частности, это подтверждает, что это действительно подгруппа группы G.

Подчеркнём, что **любой** элемент группы будет порождать циклическую подгруппу, причем порядок этой группы совпадает с порядком элемента (отсюда и одно и то же название). Вспомнив теорему Лагранжа, получаем два важных утверждения.

Теорема 5 (О порядках элементов)
Порядок любого элемента делит порядок группы.

Лемма 3 (О группах простого порядка)
Группа простого порядка не имеет *нетривиальных* (т.е. отличных от всей группы и $\{e\}$) подгрупп. Помимо этого, она является циклической.

Также без доказательства (оно есть в учебнике) приведем утверждение о подгруппах циклических групп:

Теорема 6 (О подгруппах циклических групп)
Подгруппы циклических групп также циклические.

Задача 1 (Группы многогранников)
Рассмотрим группы правильных многогранников, то есть группы вращений, переводящих многогранники сами в себя (как ГМТ).
Найдём порядки таких групп.

Решение Из геометрических соображений ясно, что вращение должно быть поворотом вокруг оси, проходящей через центр многогранника. При этом вершины переходят в вершины, а соседние (то есть соединенные ребром) вершины переходят также в соседние.

Рассмотрим некоторую вершину A. Пусть вращение оставляет её на месте, тогда ось вращения проходит через центр многогранника O и вершину A. Множество соседних с A вершин должно переходить в себя.
Множество таких вращений — это группа H_A поворотов вокруг оси OA на углы $\frac{2\pi m}{k}$, где k — число соседних с A вершин. Это циклическая группа порядка $|H_A| = k$.

Рассмотрим смежные классы по H_A. Согласно Лемме 2, два элемента g_1 и g_2 лежат в одном классе смежности $\Leftrightarrow g_1^{-1}g_2 \in H_A$.
Последнее условие равносильно $(g_1^{-1}g_2)(A) = A \iff g_1(A) = g_2(A)$. Таким образом, один смежный клас по H_A образуют вращения, переводящие вершину A в определенную вершину B.

Любая вершина многогранника некоторым вращением совмещается с любой другой, поэтому число смежных классов по H_A равно числу вершин многогранника n: $(G : H_A) = n$.
По теореме Лагранжа порядок группы: $|G| = (G : H_A) \cdot |H_A| = nk$.