# Элементы общей алгебры

продолжение...

# Подгруппы

**Подмножество $H$ группы $G$, которое само является группой относительно операции $\otimes$ группы $G$, называется *подгруппой* $H$ группы $G$. Подмножество $H \subset G$ является подгруппой в том и только в том случае, если нейтральный элемент $e$ группы $G$ входит в $H$, т.е. $e \in H$, и $H$ замкнуто относительно умножения и взятия обратного.**

Например, множество четных чисел с операцией сложения образует подгруппу аддитивной группы множества целых чисел с операцией сложения.

**Один из путей построения подгруппы $H$ конечной группы $G$ состоит в выборе произвольного элемента $h$ группы $G$, называемого *образующей* группы, и формировании $H$ как множества элементов, образованным последовательным многократным умножением $h$ на себя. Таким образом, строим последовательность элементов**

$$h, \quad h \otimes h, \quad h \otimes h \otimes h, \quad h \otimes h \otimes h \otimes h, \ldots$$

# Группы, подгруппы…

обозначая их для простоты через $h, h^2, h^3, \ldots$ .Так как $G$ конечна, то только конечное число элементов различно, так что с некоторого элемента последовательность начнет повторяться. Первым повторяющимся элементом должен быть сам элемент $h$. В свою очередь, если $h^m = h$, то $h^{m-1} = e$. Множество $H$ называется подгруппой, *порожденной* элементом $h$. Число $k$ элементов $H$ называется *порядком* элемента $h$. Множество элементов $h, h^2, h^3, \ldots, h^k = e$ называется *циклом*. Цикл является подгруппой, так как произведение двух элементов такого вида снова является элементом этого вида, и элемент, обратный элементу $h^m$, равен $h^{k-m}$ и, следовательно, является одним из элементов цикла. Группа, состоящая из всех степеней одного из ее элементов, называется *циклической группой*.

# Группы, подгруппы…

Для заданной конечной группы $G$ и ее подгруппы $H$ существует важная операция, которая устанавливает некоторые взаимосвязи между $G$ и $H$ и называется *разложением группы $G$ на смежные классы по $H$*. Опишем ее.

Обозначим через $h_1, h_2, h_3, \ldots, h_n$ элементы из $H$, причем через $h_1$ обозначим единичный элемент: $h_1 = e$. Элементы группы $G$, не входящие в $H$, обозначим $g_2, g_3, \ldots, g_m$. Построим таблицу следующим образом.

Первая строка таблицы состоит из элементов подгруппы $H$, причем *первым слева* записывается *единичный* элемент $h_1 = e$ и каждый элемент из $H$ записывается в строке один и только один раз.

Выберем *произвольный* элемент группы $G$, *не содержащийся* в первой строке. Назовем его $g_2$ и используем в качестве *первого* элемента *второй* строки. Остальные элементы второй строки получаются умножением *слева* элементов подгруппы $H$, стоящих в первой строке, на этот первый элемент и записываются под ним.

# Группы, подгруппы…

Аналогично строим третью, четвертую и т.д. строки: каждый раз в качестве элемента первого столбца выбираем не использованный на предыдущих шагах элемент $g_3, g_4, \dots, g_m$ группы $G$. Построение заканчивается тогда, когда после некоторого шага оказывается, что *каждый* элемент группы записан в некотором месте таблицы. Процесс обрывается в силу того, что группа $G$ конечна. В результате получается следующая таблица:

$$\begin{array}{ccccc}
h_1 = e & h_2 & h_3 & \dots & h_n \\
g_2 \otimes h_1 = g_2 & g_2 \otimes h_2 & g_2 \otimes h_3 & \dots & g_2 \otimes h_n \\
g_3 \otimes h_1 = g_3 & g_3 \otimes h_2 & g_3 \otimes h_3 & \dots & g_3 \otimes h_n \\
. & . & . & . & . \\
. & . & . & . & . \\
g_m \otimes h_1 = g_m & g_m \otimes h_2 & g_m \otimes h_3 & \dots & g_m \otimes h_n
\end{array} \tag{7.14}$$

Первый элемент $g_i$ слева в каждой строке называется *лидером* (или *образующим элементом*) *смежного класса*. Каждая *строка* таблицы (включая верхнюю) называется *левым смежным классом*, а в случае абелевой группы – просто *смежным классом*.

# Пример…

Пусть $G = \langle Z+;+\rangle$ – аддитивная группа неотрицательных целых чисел, $H = \langle \{5*x, x \in Z+,\}\rangle$ – аддитивная подгруппа неотрицательных целых чисел, кратных *5*. Найти разложение группы *G* на смежные классы по подгруппе *H*.

Элементы подгруппы *H*: $h_1 = e = 0$, $h_2 = 5$, $h_3 = 10$, $h_4 = 15, \ldots$

Группы G и H являются коммутативными в силу коммутативности операции сложения, поэтому левые и правые смежные классы совпадают.

В соответствии с правилами, строим таблицу смежных классов:

| $h_1 = e = 0$ | $h_2 = 5$ | $h_3 = 10$ | $h_4 = 15$ | $h_5 = 20$ | … |
|---|---|---|---|---|---|
| $g_2 = 1$ | $g_2 + h_2 = 6$ | *11* | *16* | *21* | |
| *2* | *7* | *12* | *17* | *22* | |
| *3* | *8* | *13* | *18* | *23* | |
| *4* | *9* | *14* | *19* | *24* | |

Получили 5 смежных классов. В один смежный класс попадают числа, которые при делении на *5* дают одинаковые остатки. Хотя группы *G* и *H* бесконечны, смежных классов получилось конечное число.

# Группы, кольца, поля…

Рассмотрим две группы, имеющих в информатике большое теоретическое и практическое значение.

Предварительно введем некоторые понятия.

Пусть числа $z, k, m$ и $r$ являются целыми числами, т.е. $z, k, m, r \in \mathbb{Z}$, причем $m > 0$. Любое целое число $z$ может быть представлено в виде

$$z = km + r, \qquad (0 \le r < m).$$

Если число $m$ фиксировано, то оно называется *модулем*, число $k$ носит название *частного*, а $r$ - *остатка*. Остаток называется также *вычетом по модулю* $m$, или просто вычетом.

## Операции, отношения, алгебраические системы и алгебры

Целые числа $a$ и $b$ ***сравнимы по*** $\mathrm{mod}\, m$: $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow a - b = mq$, где $m$ – целое, $m > 1$ (если остатки от деления этих чисел на $m$ равны). Иными словами $a$ содержится в арифметической прогрессии: *{..., -3m+b, -2m+b, -m+b, b, m+b, 2m+b, 3m+b, ...}*. Символ $\equiv$ читается как «равно по модулю или сравнимо по модулю». Сравнения по $\mathrm{mod}\, m$ обладают следующими свойствами:

1) если $a \equiv b(\mathrm{mod}\, m)$ и $d \mid m$ ($d$ делится без остатка на $m$), то $a \equiv b(\mathrm{mod}\, d)$;

2) если $a \equiv b(\mathrm{mod}\, m)$ и $a \equiv b(\mathrm{mod}\, n)$, то $a \equiv b(\mathrm{mod}[m,n])$, где $[m,n]$ – наименьшее общее кратное чисел $m,n$;

3) если $a \equiv b(\mathrm{mod}\, m)$ и $c \equiv d(\mathrm{mod}\, m)$, то $a + c \equiv (b + d)(\mathrm{mod}\, m)$ и $a - c \equiv (b - d)(\mathrm{mod}\, m)$;

4) если $a \equiv b(\mathrm{mod}\, m)$ и $k$ – произвольное целое число, то $ka \equiv kb(\mathrm{mod}\, m)$;

5) если $a \equiv b(\mathrm{mod}\, m)$, то при любом целом $n > 0$ $a^n \equiv b^n(\mathrm{mod}\, m)$

6) в сравнении можно отбрасывать или добавлять слагаемые, делящиеся на модуль.

***Классом по данному модулю m*** называется множество всех целых чисел, сравнимых с некоторым данным целым числом *a*. Число классов по *mod m* конечно и равно *m*

Даны 3 числа: 78, 210 и 346. Сравнимы ли они с 27 по *mod 11*?
В соответствии с определением операции сравнения по модулю, вычтем из этих чисел 27:

78 – 27 = 51;

210 – 27 = 183;

346 – 27 = 319.

Из этих чисел только 319 делится на 11, значит, только 346 сравнимо с 27 по *mod 11* (при делении на 11 и 346 и 27 дают в остатке 5).