Группы. Некоторые свойства и примеры.

1. Какие группы нам уже встречались?

Соберём в одном разделе группы, попадавшиеся нам в предыдущих заданиях. Среди них были и конечные, и бесконечные. Число элементов конечной группы G называется её ***порядком***, порядок обозначается $|G|$, и мы его тоже будем указывать. Начнём с конечных групп.

Группа $\mathbb{Z}_n$ остатков по модулю n по сложению является важным примером абелевой группы. В частности, благодаря наличию $\mathbb{Z}_n$ можно утрверждать существование группы любого натурального порядка ($|\mathbb{Z}_n| = n$). Группа $(\mathbb{Z}_p)^*$ ненулевых остатков от деления на простое p по умножению имеет порядок $p-1$ И тоже абелева.

Напомним, почему $(\mathbb{Z}_p)^*$ группа. Ассоциативность очевидна, нейтральный элемент — единица, замкнутость ясна из того, что произведение чисел, не кратных p не может быть кратно p. Осталось показать наличие обратного. Для этого для любого остатка k рассмотрим $p-1$ ненулевых чисел: k, $2k$, $3k$, $\ldots(p-1)k$. Все они различны, ибо если $mk = nk$ $(m > n)$, то $(m-n)k$ кратно p, а так как $НОД\,(k\,;p) = 1$, то $(m-n)$ кратно p, но $0 < m-n < m < p$, так что это невозможно. Значит, среди указанных чисел есть все ненулевые остатки, в том числе и единица.

Группа всех перестановок из n элементов обозначается S_n и является (при $n > 2$) важнейшим примером неабелевой конечной группы. Чётные перестановки из $n > 2$ элементов составляют подгруппу в S_n. Эта подгруппа обозначается A_n. A_n также неабелева при $n > 4$. Про порядки можно сказать, что $|S_n| = n!$ и $|A_n| = \frac{n!}{2}$.

Группа самосовмещений правильного n-угольника обозначается D_n. Она неабелева при $n > 2$. $|D_n| = 2n$

Из бесконечных абелевых групп нам встречались $\mathbb{Z}$ (она же $n\mathbb{Z}$), $\mathbb{R}_+^*$, $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{Q}_+^*$, $\mathbb{Q}^*$, $\mathbb{Q}$, $\mathbb{C}^*$, $\mathbb{C}$. Примером бесконечной неабелевой группы служит группа M всех движений плоскости.

То, что $\mathbb{Z} = n\mathbb{Z}$, мы знаем. Есть ли среди названных групп ещё изоморфные? Какие заведомо неизоморфны? Во-первых, все группы из рациональных чисел счётны и заведомо неизоморфны остальным. Далее была задача о том, что в группе по умножению есть неединичный элемент, обратный себе (-1) а в остальных типах групп такого нет. Далее, в C^* есть элемент i, четвёртая степень которого равна 1, что показывает уникальность этой группы в списке. Для общего развития детей можно сказать им, что $\mathbb{R}_+^* = \mathbb{R}$, изоморфизм осуществляет экспонента/логарифм. Группа $\mathbb{Q}_+^*$ не изоморфна $\mathbb{Q}$: если бы это было так и числу 2 в $\mathbb{Q}_+^*$ соответствовало бы x в $\mathbb{Q}$, то числу $\frac{x}{2}$ в $\mathbb{Q}$, соответствовало бы такое y в $\mathbb{Q}_+^*$, что $y^2 = 2$. Но такого нет. А вот $\mathbb{C}$ и $\mathbb{R}$ изоморфны, но доказательство этого факто сложное.

2. Циклическая группа.

Структура группы $\mathbb{Z}_n$ (при $n > 1$) особенно проста. В ней содержится элемент 1, который можно "умножать" на себя несколько раз (помним, что "умножением" в $\mathbb{Z}_n$ служит *сложение* остатков!), причём при этом будут получены все элементы группы: $1*1 = 2$, $1*1*1 = 3$, $1*1*1*1 = 4$, и так далее. Каждый элемент такой группы есть ***степень*** одного конкретного элемента (который называется ***образующим элементом***), то есть группа состоит из образующего a и всех его степеней: a^2, a^3, $\ldots a^{n-1}$ и $a^n = e$. При этом структура группы задана: любое умножение осуществляется по правилу $a^i \cdot a^j = a^{i+j}$.

Можно доказать, что $(\mathbb{Z}_p)^* = \mathbb{Z}_{p-1}$, но это сложная теорема.

3. Порядок элемента.

Рассмотрим любой элемент $a \in G$ конечной группы. Будем выписывать его степени: a, a^2, a^3 и так далее. Рано или поздно впервые встретится степень, равная e: $a^k = e$. В самом деле, ввиду конечности группы наступит момент, когда $a^i = a^j$ при $i \geqslant j$, а тогда $a^{i-j} = e$. А раз существует показатель степени, при котором получается e, то и минимальный такой тоже существует. Минимальное k, при котором $a^k = e$, называется ***порядком*** элемента a в группе G.

Все степени любого элемента a, порядок которого k, образуют подгруппу в G. Эта подгруппа абелева (даже если G неабелева!), циклическая и изоморфна $\mathbb{Z}_k$. Она обозначается $\{a\}$ и называется ***порождённой*** элементом a.

4. Частный случай теоремы Лагранжа.

Рассмотрим элемент $a \in G$ порядка k. Выпишем порождённую им подгруппу $\{a\}$: a, a^2, a^3,..., $a^k = e$. Если этим списком G не исчерпывается, в G найдётся ещё один элемент b. Тогда выпишем такие элементы: ba, ba^2, a^3,..., $ba^k = b$. Все они различны и не совпадают ни с одним из первого списка, что несложно проверить. Если в G ещё остались элементы, например, c, выписываем такую серию: ca, ca^2, ca^3,..., $ca^k = c$. Это снова новые элементы группы. (В самом деле, если бы $ca^i = ba^j$, то $c = ba^{j+k-i}$, то есть c есть во второй серии, а это не так.) В конце концов, G исчерпается и окажется разбитой на серии, в каждой из которых по k элементов. Это означает, что ***порядок группы делится на порядок любого элемента этой группы***: $|G| \vdots |k|$.