КМБО -17 3-й семестр

1. Арифметика.

Делитель числа, одно число делится на другое, одно число делит другое. Простое число. Любое натуральное число, > 1, можно разложить на простые множители, причем единственным образом, если не учитывать порядок множителей (это - основная теорема арифметики). НОД(a;b)=(a;b) и НОК(a;b). Если разложить a и b на простые множители, то поиск НОД и НОК элементарен. Задача: НОК(a;b)НОД(a;b)=ab (если они положительны). Взаимно простые числа. Задача. Если (a;b)=1 и $a|bc$, то $a|c$.

Деление с остатком: если a и b – целые ненулевые числа, то существует, и притом единственная, пара целых чисел (q,r) таких, что a=bq+r, причем $0 \leq r < |b|$.

Алгоритм Евклида нахождения наибольшего общего делителя двух целых чисел НОД(a,b)=(a,b)

Диофантовы уравнения - это когда нас интересуют только целые решения.

1) Линейные диофантовы уравнения $ax + by = c$, где коэффициенты – целые числа и ищутся целые решения.

Теорема. Если $d = (a, b)$, то существуют целые m и n такие, что $am + bn = d$ (это следует из алгоритма Евклида)

Пример. (187,55)=11; $187 = 3 \cdot 55 + 22$; $55 = 2 \cdot 22 + 11$; $22 = 2 \cdot 11$; $11 = 55 - 2 \cdot 22 = 55 - 2(187 - 3 \cdot 55) = 7 \cdot 55 + (-2) \cdot 187$

– уравнение $ax + by = c$ разрешимо в целых числах iff (a, b) делит c (то есть c делится на (a, b)).

Замечание. Если $(a, b) = d \neq 1$, есть смысл сразу поделить уравнение на d - ведь в этом случае c также делится на d. Поэтому будем считать, что $(a, b) = 1$.

Если $c = 0$, то есть у нас однородное уравнение $ax+by = 0$, то общее решение имеет вид $x = bt$; $y = -at$

Общее решение неоднородного уравнения может быть записано в виде $x = x_0+bt$; $y = y_0-at$, где $(x_0; y_0)$ – частное решение неоднородного уравнения. Иными словами, общее решение неоднородного уравнения есть сумма частного решения неоднородного уравнения и общего решения соответствующего однородного.

Аналогично можно решить диофантово уравнение с n неизвестными (сократив при необходимости, можем считать, что НОД коэффициентов при неизвестных равен 1). Скажем, если неизвестных 3, объединим два из них в скобку, вынеся НОД коэффициентов перед ними за скобку. Обозначив скобку новой буквой, получаем уравнение с 2 неизвестными.

Цепные дроби.

Получается из обычной дроби многократным выделением целой части. Оказывается, чтобы найти частное решение уравнения $ax + by = 1$, надо b/a записать в виде цепной дроби, отбросить последнюю получившуюся дробь $1/t$ м снова свернуть дробь в обычную u/v. Получаем частное решение $x = u$; $y = v$.

Возможен доклад на тему "Цепные дроби". Можно воспользоваться, например книгой Хинчина "Цепные дроби".

Сравнение по модулю.

$a \equiv b \pmod n$ (a сравнимо с b по модулю n), если их разность делится на n (иными словами, они дают одинаковые остатки при делении на n).

Теорема. Если $a \equiv b \pmod n$; $c \equiv d \pmod n$, то

$$a \pm c \equiv b \pm d;\ ac \equiv bd$$

(естественно, по тому же модулю).

Конечно, как следствие, сравнение по модулю можно возводить в натуральную степень, умножать на число, прибавлять число. А вот деление сравнения на сравнение или хотя бы деление на число, даже если обе части нацело делятся на него, может привести к ошибке. Например, 3 сравнимо с 9 по модулю 3, но поделив на 3, получаем 1 и 3, которые уже не сравнимы по модулю 3. Но: если $ac \equiv bc \pmod n$, причем $(c; n) = 1$, то $a \equiv b \pmod n$.

Эта теорема позволяет корректно определить операции в множестве $\mathbb{Z}_n$ остатков от деления на фиксированное натуральное число n.

Группа.

Группоид (есть бинарная операция); полугруппа (+ассоциативность); моноид (+ единичный элемент); группа (+ все элементы обратимы).

Конечная группа, бесконечная группа, порядок группы, порядок элемента. Подгруппы (тривиальные и нетривиальные), коммутативная (абелева) группа, циклическая группа конечного (бесконечного) порядка.

Примеры. $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; $(\mathbb{C}, +)$; $(\mathbb{Q} \setminus \{0\} = \mathbb{Q}^*, \cdot)$; $(\mathbb{R}^*, \cdot)$; $(\mathbb{C}^*, \cdot)$; $(\mathbb{R}^n, +)$; $\mathbb{R}^{m\times n}, +)$; $\mathrm{GL}(n, \mathbb{C}), \cdot)$; $(n\mathbb{Z}, +)$; $\mathbb{Z}_n, +)$; $(\mathbf{U} = \{z \in \mathbb{C} : \ |z| = 1\}, \cdot)$; $(\mathbf{C}_n = \{z \in \mathbb{C} : \ z^n = 1\}, \cdot)$.

Важный пример. $S(X)$ – все биективные преобразования множества X; операция – суперпозиция. Если X – конечное множество, можно считать, что оно состоит из первых n натурвальных чисел, тогда $S(X)$ называется множеством подстановок S_n.

Важный пример. **Движением** плоскости E^2 (рассматриваемой как множество точек) назовем любую функцию $f : E^2 \to E^2$ (отображение, преобразование), которая является биекцией и сохраняет расстояние между точками плоскости. Множество всех движений плоскости будем обозначать

$$\mathrm{Isom}\ E^2.$$

Очень часто бывает полезно выделить одну точку плоскости (начало отсчета) и рассматривать только движения плоскости, не сдвигающие эту точку. Поскольку все точки плоскости можно идентифицировать с векторами, идущими из начала отсчета в эти точки, мы получаем линейное пространство. Расстояние между началом отсчета и точкой равно длине соответствующего вектора. Поэтому мы получаем биекцию в линейном евклидовом пространстве, сохраняющую скалярное произведение: $(\mathcal{A}(x), \mathcal{A}(x)) = (x, x)$. Про линейность мы ничего не знаем, но оказывается, ее можно доказать:

$$(\mathcal{A}(x+y) - \mathcal{A}(x) - \mathcal{A}(y), \mathcal{A}(x+y) - \mathcal{A}(x) - \mathcal{A}(y)) = \ldots = \bar{0};$$

$$(\mathcal{A}(\lambda x) - \lambda\mathcal{A}(x), \mathcal{A}(\lambda x) - \lambda\mathcal{A}(x)) = \ldots = \bar{0}$$

Поэтому множество движений плоскости, не сдвигающих начало отсчета, совпадает с множеством ортогональных операторов на этой плоскости. Это множество будем обозначать как O_2.

Если на плоскости E^2 выделено некоторое множество X, в группе $\mathrm{Isom}\ E^2$ выделяется подгруппа движений

$$\mathrm{Sym}\ X = \{f \in \mathrm{Isom}\ E^2 : \ f(X) = X\};$$

которая называется группой симметрии фигуры X.

Если X – это правильный n-угольник, то его группа симметрии называется группой диэдра и обозначается D_n. На лекции выписать все элементы этой группы для случая треугольника. Там юудет три поворота и три отражения.

Вместо E^2 можно было бы рассмотреть E^3.

Еще одна важная группа, являющаяся подгруппой $\mathrm{Sym}\ X$ – это группа вращений $\mathrm{Rot}\ X$ (у Винберга она обозначается как $\mathrm{Sym}\ _+X$) (обычно при этом считается, что X – это правильный многогранник).

Например, если X – это треугольник Δ, то $\mathrm{Sym}\ \Delta$ на плоскости совпадает с $\mathrm{Rot}\ \Delta$ в пространстве; и то и то – группа диэдра D_3.

Докажем несколько простых утверждений относительно группы.

1. Единственность нейтрального элемента.
2. Единственность обратного элемента.
3. $(ab)^{-1} = b^{-1}a^{-1}$
4. Существование и единственность решения уравнения $ax = b$ $(xa = b)$
5. $(x^n)^{-1} = (x^{-1})^n$ (оба будут записываться как x^{-n}; $n \in \mathbb{N}$.
6. $x^n \cdot x^m = x^{n+m}$
7. $(x^n)^m = x^{nm}$
8. Таблица умножения конечной группы называется таблицей Кэли. В каждой строчке (и в каждом столбце) все элементы группы встречаются, причем ровно по одному разу.

Задача. Составить все возможные таблицы Кэли для групп 1-го, 2-го, 3-го, 4-го, 5-го, 6-го порядка.

Задача. Доказать, что если $|a| = n$, то все элементы $e;\ a;\ a^2;\ \ldots;\ a^{n-1}$ различны. Если же $|a| = \infty$, e и все целые степени a различны.

Утв. Единица подгруппы совпадает с единицей группы. Обратный в подгруппе совпадает с обратным в группе

Теорема. Критерий подгруппы. - непустое подмножество, замкнутое относительно умножения и взятия обратного.

Симметрическая группа (группа подстановок)

$X = \{1;\ 2;\ \ldots;\ n\}$; $S(X) = S_n$ – множество биективных функций. $|S_n| = n!$
Умножение подстановок. тождественная подстановка. Обратная подстановка. Циклическая подстановка = цикл. Независимые циклы.

Утверждение. Независимые циклы перестановочны.

Утверждение. Любую подстановку можно разбить в произведение независимых циклов, и при этом единственным образом.

Утв. Длина цикла α совпадает с порядком $|\alpha|$.

Цикленный тип подстановки - это набор длин независимых циклов, на которые он распадается. Будем записывать их в сторону убывания, в фигурных скобках.

Теорема. Порядок подстановки равен НОК чисел, образующих цикленный тип этой подстановки.

Цикл длины 2 называется **транспозицией**.

Говорят, что группа G порождена множеством K ее элементов, если каждый элемент G можно получить из элементов K и обратных к ним.

Теорема. Если $n \geq 2$, то S_n порождена транспозициями.

Доказательств существует много. Например, можно заметить, что цикл $(ijkl) = (ij)(jk)(kl) = (il)(ik)(ij)$. Или заметить, что если умножить транспозицию $(k_i k_j)$ на подстановку с k_l в нижней строчке, то k_i и k_j поменяются местами. Поэтому можно постепенно в нижней строчке сделать числа в порядке возрастания.

Инверсия в перестановке - это когда меньшее число стоит правее большего.

Четная подстановка – если сумма чисел инверсий в первой и второй строчке четная. Соответственно нечетная подстановка. Знак подстановки 1 у четной, минус 1 у нечетной. Можно это записать как $(-1)^{\text{сумма чисел инверсий в первой и второй строчках}}$

Теорема Знак произведения подстановок равен произведению знаков сомножителей.

Транспозиция нечетна (если между i и j k чисел, то инверсий 2k+1). Цикл длины k может быть разложен в произведение k-1 транспозиций, поэтому цикл четной длины является нечетной подстановкой и наоборот. Четная подстановка разбивается в произведение четного числа транспозиций, нечетная - нечетного числа.

Теорема. Если $\alpha \in S_n$ имеет цикленный тип $\{k_1, k_2, \ldots, k_m; k_1 + k_2 + \ldots + k_m = n$, то $\operatorname{sgn} \alpha = (-1)^{n-m}$.
Доказательство. $\operatorname{sgn} \alpha = (-1)^{k_1-1} \cdot \ldots \cdot (-1)^{k_m-1} = (-1)^{k_1+\ldots+k_m-m} = (-1)^{n-m}$

Теорема Множество четных подстановок образует подгруппу A_n (знакопеременная группа).

Теорема. $|A_n| = \frac{n!}{2}$
(умножая четную подстановку на фиксированную транспозицию, получаем нечетную подстановку, причем разные четные переходят в разные нечетные. Поэтому четных подстановок не больше, чем нечетных. Точно так же нечетную можно превратить в четную.

Свойства порядка элемента

Лемма 1. $|g| = n$ и $g^k = e \Rightarrow n|k$
Доказательство. $k = nq + r$; $0 \le r < n$; $g^k = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = e^q g^r = g^r = e \Rightarrow r = 0$

Лемма 2. $|g| = n$; $g^k = g^m \Rightarrow k \equiv m(\mod n)$
Д-во. $g^{k-m} = e \Rightarrow n|(k-m)$

Следствие. $|g| = n \Rightarrow g^0 = e;\ g;\ g^2;\ g^{n-1}$ все различны.

Следствие. $|g| = \infty \Rightarrow$ все целые степени g различны.

Л.3. Если все натуральные степени g различны, g имеет бесконечный порядок.
Л. 3'. Если существуют целые $k \neq m$ такие, что $g^k = g^m$, то g имеет конечный порядок.

Л.4. $|g| = n \Rightarrow |g^k| = \frac{n}{(n,k)}$.
Д-во. Пусть $n = d \cdot n_1$; $k = d \cdot k_1$; $(n_1, k_1) = 1 \Rightarrow \frac{n}{(n,k)} = n_1$.
1) $(g^k)^{n_1} = g^{kn_1} = g^{dk_1n_1} = g^{nk_1} = (g^n)^{k_1} = e^{k_1} = e$.
2) Пусть $(g^k)^m = e;\ g^{km} = e \Rightarrow$ по лемме 1 $n|km;\ dn_1|dk_1m;\ n_1|k_1m$. Но $(n_1; k_1) = 1 \Rightarrow n_1|m$.

Циклические группы

Циклическая группа конечного порядка n: $G =< g >= \{e;\ g;\ g^2\ \ldots;\ g^{n-1}\}$.
Циклическая группа бесконечного порядка: $G =< g >= \{\ldots;\ g^{-2};\ g^{-1};\ e;\ g;\ g^2;\ \ldots\}$.

Примеры: $(\mathbb{Z}; +) =< 1 >=< -1 >$; $(\mathbb{Z}_n; +) =< 1 >$; $\mathbf{C}_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi ki/n}\} =< e^{2\pi i/n} >$.

Теорема 1. Любая подгруппа циклической группы циклична.

Д-во. Оно простое, но требует аккуратности.Пусть $G =< g >$. Если подгруппа H состоит из одного элемента (e), ничего доказывать не надо. В противном случае в H найдется неединичный элемент. При необходимости переходя к обратному элементу, можно считать, что этот элемент является натуральной степенью g. Пусть m – минимальное натуральное число такое, что $g^m \in H$. Докажем, что $H =< g^m >$. Пусть $g^k \in H$; можно считать, что k – натуральное число. Разделим k на m с остатком и докажем, что остаток равен 0: $k = mq + r$; $0 \le r < m$; $r = k - mq$; $g^r \in H$; $g^r = g^{k-mq} = g^k g^{-mq} \in H \Rightarrow r = 0$.

Теорема 2. Пусть G – циклическая группа, $|G| = n < \infty$; $H < G \Rightarrow |H| \mid |G|$.
Д-во. $|G| = n$; $G =< g >_n$; $H < G \Rightarrow H =< g^m >$. Но $|H| = |g^m| = \frac{n}{(n,m)} \Rightarrow |H| \mid |G|$.

Теорема 3. Для любого делителя k порядка n циклической группы конечного порядка существует и притом единственная подгруппа порядка k.

Д-во. Пусть k делитель n; $n = km \Rightarrow |g^m| = \frac{n}{(n,m)} = \frac{n}{m} = k$; $| < g^m > | = k$.

Таким образом, $G = \{e;\ g;\ g^2;\ \ldots;\ g^m;\ g^{m+1};\ \ldots;\ g^{n-1}\}$; $H = \{e;\ g^m;\ g^{2m};\ \ldots;\ g^{(k-1)m}\}$.

Понятно, что если другая подгруппа ($\Rightarrow$ циклическая)порождена элементом g^l, где l – минимальное натуральное число с этим условием, то если $l \neq m$, то g^{kl} или не дотянет до e, если $l < m$, или перескочит через него.

Теорема 4. Пусть $G =< g >_n$. Тогда $G =< g^m > \Leftrightarrow (n, m) = 1$.

Д-во сразу следует из нашей любимой формулы $|g^m| = \frac{n}{(n,m)}$

Примеры. $\mathbb{Z}_{12}$; выписать все подгруппы.

Для следующего утверждения нам потребуется определение изоморфизма групп. ...

Теорема 5. Любая бесконечная циклическая группа изоморфна $(\mathbb{Z}; +)$. Любая циклическая группа порядка n изоморфна $(\mathbb{Z}_n; +)$.

Отображение факторизации

Говорят, что на множестве X задано отношение T, если задано множество $T \subset X \times X$. Можно сказать, что само множество T является отношением на множестве X. Если точка $(x; y) \in T$, будем писать xTy и говорить, что эти элементы находятся в отношении T.

Примеры.

Отношение называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно. В случае отношения эквивалентности вместо xTy принято писать $x \sim_T y$ или просто $x \sim y$.

Разбор отношений, удовлетворяющих части этих условий или всем условиям.

Отношение эквивалентности позволяет по каждому элементу множества X строить множество $T(x) = \{y \in X : \; x \sim y$ – класс эквивалентности отношения T (класс эквивалентных элементов). Ясно, что $x \in T(x)$, поэтому классы эквивалентности покрывают все множество X, а также что если два таких класса пересекаются, то они совпадают. Итак, X оказывается разбито на непересекающиеся подмножества, причем два элемента принадлежат одному подмножеству тогда и только тогда, когда они эквивалентны.

Множество классов эквивалентных элементов называется фактормножеством множества X по отношению эквивалентности T и обозначается X/T. Переход от множества X к фактормножеству X/R называется отображением факторизации.

Примеры.

Для нас интересным является случай, когда на множестве X задана операция (например, когда X является группой) с тем, чтобы попытаться с помощью этой операции задать операцию на фактормножестве (чтобы получить факторгруппу). Это возможно в случае, когда отношение эквивалентности *согласовано* с операцией, то есть если в одном классе эквивалентных элементов взять два элемента x_1 и y_1, и в другом классе взять два элемента x_2 и y_2, то класс эквивалентных элементов, построенный для элемента x_1x_2, должен совпадать с классом, построенным для элемента y_1y_2:

$$x_1 \sim y_1; \; x_2 \sim y_2 \Rightarrow x_1x_2 \sim y_1y_2.$$

Если это так, то в X/T можно ввести операцию по формуле

$$T(x_1)T(x_2) = T(x_1x_2)$$

Если X является группой, и отношение эквивалентности согласовано с операцией, то фактормножество становится группой. Операцию мы уже определили, ассоцомтивность очевидно наследуется, класс элементов, эквивалентных e, будет играть роль единицы в факторгруппе, класс элементов, эквивалентных x^{-1}, будет играть роль элемента, обратного классу элементов, эквивалентных элементу x.

Пример, который рассматривают всегда первым, это группа $(\mathbb{Z}; +)$, в которой эквивалентность задается с помощью сравнения по модулю некоторого натурального числа n:

$$a \sim b \Leftrightarrow a \equiv b \pmod n$$

Если в $\mathbb{Z}$ рассмотреть подгруппу $n\mathbb{Z}$ чисел, делящихся на n, то выписанное условие эквивалентности можно переписать как $a \sim b \Leftrightarrow a - b$ делится на $n \Leftrightarrow b = a + nk \Leftrightarrow b - a \in n\mathbb{Z}$. Ясно, что это отношение эквивалентности согласовано с операцией сложения, поэтому в фактормножестве операция сложения, индуцированная сложением в $\mathbb{Z}$, определена корректно. Получающаяся группа обозначается как $\mathbb{Z}_n$. Кстати, отношение эквивалентности согласовано не только со сложением, но и с умножением, так что в $\mathbb{Z}_n$ определено и умножение. Тем самым, $\mathbb{Z}_n$ является кольцом, а в случае, когда $n = p$ – простое число – даже полем. В последнем случае все ненулевые элементы обратимы; они образуют так называемую мультипликативную группу $\mathbb{Z}_p^*$, в которой $p - 1$ элемент.

Проведем аналогичное рассуждение для произвольной группы и ее подгруппы. К фактормножеству в этом случае мы по любому научимся переходить, а вот к факторгруппе - только если подгруппа так называемая нормальная (в коммутативном случае никаких проблем не будет).

Итак, пусть $H < G$; будем говорить, что $g_1 \equiv g_2 \pmod H$ (элементы сравнимы по модулю подгруппы), если $g_2 = g_1 h$, где $h \in H$; иными словами, если

$$g_1^{-1} g_2 \in H$$

Теорема. Сравнение по модулю подгруппы H задает отношение эквивалентности на группе G.

Классы эквивалентных элементов называются левыми смежными классами; они имеют вид gH. Множество этих классов обозначается G/H. Можно было бы рассмотреть другое отношение эквивалентности – с помощью равенства $g_2 = hg_1$, то есть $g_2 g_1^{-1} \in H$. В этом случае мы получили бы правые смежные классы, имеющие вид Hg. Множество таких классов можно было бы обозначить $H \setminus G$.

Теорема Лагранжа. В случае конечной группы порядок группы равен произведению порядка подгруппы на количество левых смежных классов (оно же количество правых смежных классов; назовем это количество индексом подгруппы).

Следствие. Порядок подгруппы делит порядок группы.
Следствие. Порядок элемента делит порядок группы.
Следствие. Конечная группа простого порядка циклична.
Следствие. Если $|G| = n$, то $g^n = e$ для любого элемента группы.

Следствие (малая теорема Ферма). Если p – простое число, и a не делится на p, то

$$a^{p-1} \equiv 1 \pmod p$$

В самом деле, $\mathbb{Z}_p^*$ является группой по умножению, ее порядок равен $p-1$, поэтому по предыдущему следствию для любого элемента этой группы $g^{p-1} = 1$.

Теорема Эйлера. Если a взаимно просто с n, то

$$a^{\varphi(n)} \equiv 1 \pmod n,$$

где $\varphi(n)$ – функция Эйлера, равная количеству чисел, меньших n и взаимно простых с n (эта функция задает число элементов в группе $\mathbb{Z}_n^*$ обратимых элементов кольца $\mathbb{Z}_n$).

Переходим к самому важному – в каком случае факторизация по подгруппе, то есть переход (для определенности) к левым смежным классам приводит к фактормножеству, на котором групповая операция на всей группе задает структуру группы, то есть когда выбор того или иного элемента в смежном классе не влияет на конечный результат.

Иными словами, должно выполняться следующее: пусть $g_2 = g_1 h_1$; $g_4 = g_3 h_2$; тогда должен существовать h_3 такой, что $g_2 g_4 = g_1 g_3 h_3$. То есть $g_1 h_1 g_3 h_2 = g_1 g_3 h_3$; $h_1 g_3 h_2 = g_3 h_3$; $h_1 g_3 = g_3 h_3 h_2^{-1}$; то есть $h_1 g_3 = g_3 h_4$. Здесь g_3 – произвольный элемент группы G, будем писать поэтому просто g. Здесь h_1 – произвольный элемент подгруппы H, будем писать поэтому просто h. Теперь полученное равенство можно проинтерпретировать так: для любых $g \in G$; $h \in H$ существует такой $\tilde{h} \in H$, что $hg = g\tilde{h}$. А можно, домножив слева на g^{-1}, записать так: $g^{-1} h g = \tilde{h}$. Считая g фиксированным элементом группы и заставляя h пробегать всю подгруппу H, получаем, что

$$g^{-1} H g \subseteq H$$

(причем это выполнено для каждого элемента группы). Легко показать, что на самом деле знак включения можно заменить на знак равенства. Домножая обе части слева на g, а справа на g^{-1}, получаем $H \subseteq gHg^{-1} = (g^{-1})^{-1} H g^{-1} \subseteq H$. Итак, получили равносильное условие

$$g^{-1} H g = H,$$

которое можно переписать в виде

$$Hg = gH$$

(здесь записано условие совпадения левых и правых смежных классов) Подгруппа, удовлетворяющая этим равносильным условиям, называется *нормальной*. В этом случае будем писать $H \lhd G$.

Теорема. Если $H \lhd G$, то операция на множестве G/H левых (= правых) смежных классов, индуцированная операцией на G, задает на G/H группу (она называется факторгруппой группы G по нормальной подгруппе H).

Вдогонку приведем еще одно следствие теоремы Лагранжа (точнее, следствие из теоремы Ферма).

Теорема Вильсона. Если p – простое число, то $(p-1)! \equiv -1(\mod p)$

В самом деле, по теореме Ферма $1;\ 2;\ \ldots;\ p-1$ являются корнями многочлена $x^{p-1}-1$ в поле $\mathbb{Z}_p$, откуда следует, что $x^{p-1}-1 = (x-1)(x-2)\ldots(x-(p-1))$. Далее можно или воспользова ться теоремой Виета, или подставить $x = 0$. В любом случае получится равенство $-1 = (-1)^{p-1}(p-1)!$. Остается разобрать два случая. Если $p > 2$, то p является нечетным числом, поэтому $(p-1)! = -1$. Если $p = 2$, то $-1 = 1$, и снова теорема Вильсона верна.

Морфизмы

Отображение $f : G_1 \to G_2$, где G_1 и G_2 – группы, называется гомоморфизмом, или короче морфизмом, если $f(ab) = f(a)f(b)$ для любых $a,\ b \in G_1$.

Мономорфизм, эпиморфизм, изоморфизм (он у нас уже был), эндоморфизм, автоморфизм. Кстати, endo на латыни означает внутри, что объясняет название. Ядро $\operatorname{Ker} f$ гомоморфизма, образ $\operatorname{Im} f$ гомоморфизма.

Свойства гомоморфизма.

1. $f(e_1) = e_2$

2. $f(a^{-1}) = (f(a))^{-1}$

3. $\operatorname{Ker} f < G_1$

4. $\operatorname{Im} f < G_2$

5. f – мономорфизм $\Leftrightarrow \operatorname{Ker} f = \{e_1\}$

6. $\operatorname{Ker} f \lhd G_1$

7. Множество Aut G всех автоморфизмов группы G является группой относительно суперпозиции.

8. При каждом фиксированном $a \in G$ отображение $i_a : G \to G$; $i_a(b) = aba^{-1}$ является автоморфизмом (он называется внутренним автоморфизмом).

9. Множество Int G всех внутренних автоморфизмов является группой. Тем самым Int $G <$ Aut G.

10. Int $G \lhd$ Aut G.

11. Теорема о гомоморфизме. Пусть $f : G_1 \to G_2$ – гомоморфизм групп. Тогда

$$G_1/\operatorname{Ker} f \simeq \operatorname{Im} f$$

Этот изоморфизм задается формулой

$$\varphi(a\operatorname{Ker} f) = f(a)$$

12. Следствие из теоремы о гомоморфизме. Если $f : G_1 \to G_2$ – мономорфизм, то $G_1 \simeq \operatorname{Im} f$.

13. Каждая нормальная подгруппа является ядром некоторого гомоморфизма.Иными словами: группа нормальна тогда и только тогда, когда она является ядром некоторого гомоморфизма.

14. Если G – конечная группа, то $|G| = |\mathrm{Ker}\, f| \cdot |\mathrm{Im}\, f|$.

Пример 1. $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12};\ f(a) = 15a$ – гомоморфизм групп по сложению (на самом деле, гомоморфизм колец). $\mathrm{Ker}\, f =< 4 >_3$; $\mathrm{Im}\, f =< 3 >_4$.

Пример 2. $f : S_n \to C_2 < \mathbb{C}$; $f(\sigma) = \mathrm{sgn}\ \sigma$; $\mathrm{Ker}\, f = A_n$; $\mathrm{Im}\, f = C_2 = \{\pm 1\}$.

Пример 3. $f : \mathbb{C} \to \mathbb{C}$; $f(z) = z^n$

Пример 4. $S_4/V_4 \simeq S_3$. Красивое доказательство из Винберга. $f : S_4 \to S_3$; каждая подстановка из S_4 задает перестановку индексов многочленов $P_1 = x_1x_2 + x_3x_4$; $P_2 = x_1x_3 + x_2x_4$; $P_3 = x_1x_4 + x_2x_3$ и тем самым переставляет их местами. Но перестановка трех элементов (обычно это числа 1, 2, 3, у нас это многочлены, занумерованные числами 1, 2, 3) задается подстановкой из S_3. То, что это гомоморфизм, почти очевидно. Винберг доказывает, что образ совпадает с S_3, но это делать необязательно. Достаточно найти ядро (Винберг ищет и его), доказать, что в нем 4 элемента, а тогда порядок образа находится из 14-го свойства, он равен 6, и поэтому образ совпадает с S_3. Ядро оказывается четверной группой Клейна

$$V_4 = \{e;\ (12)(34);\ (13)(24);\ (14)(23)\}.$$

Это, кстати, автоматически доказывает, что V_4 является нормальной подгруппой.

Прямое произведение групп

Сначала – **внешнее** прямое произведение n групп. На декартовом произведении $G = G_1 \times G_2 \times \ldots \times G_n$ этих групп задаем покоординатное умножение. Наличие ассоциативности, единицы и обратного к каждому элементу очевидны.

Свойства внешнего прямого произведения

1. $|G| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$.

2. $|(g_1, g_2, \ldots, g_n)| = \text{НОК}(|g_1|, |g_2|, \ldots, |g_n|)$.

3. Если все группы цикличны и конечного порядка, причем эти порядки попарно взаимно просты, то их прямое произведениециклично, и его порядок равен произведению порядков сомножителей. Если же среди их порядков есть не взаимно простыми, то произведение не будет цикличным, что можно усмотреть их второго свойства, поскольку в произведении не будет элемента нужного порядка. Также будут проблемы с цикличностью, если среди групп есть циклічные группы бесконечного порядка. Ну а из нециклчных получить циклическую - это вообще за гранью разумного.

4. В G есть подгруппы, изоморфные сомножителям; будем их обозначать $\tilde{G}_i$; иногда волну будем "забывать".

5. Эти подгруппы пересекаются только по единичному элементу.

6. Элементы этих подгрупп коммутируют друг с другом.

7. Каждый элемент прямого произведения распадается, причем единственным образом, в произведение элементов, взятых по одному из каждой группы.

8. Эти подгруппы нормальны.

9. Прямое произведение коммутативно $\Leftrightarrow$ все сомножители коммутативны.

Пример. $C_5 =< a > \times C_7 =< b > \simeq C_{35} =< (a, b) >$.

Пример: $C_6 =< a > \times C_{10} =< b > \not\simeq C_{60}$, так как $|(a, b)| = \text{НОК}(|a|, |b|) = 30$; в прямом произведении нет элемента порядка 60.

10. Обобщение свойства 5. $\forall i\ G_i \cap G_1 \times \ldots \times \{e_i\} \times \ldots G_n = \{e\}$.

Внутреннее прямое произведение подгрупп

Нужно выделить какие-то свойства подгрупп G_i группы G, чтобы эти свойства гарантировали, что их внешнее прямое произведение изоморфно G. Естественно выбирать эти свойства из доказанных свойств внешнего прямого произведения. Хорошая тема для доклада – перепробовать все возможные минимальные комбинации свойств, гарантирующих требуемый изоморфизм. Мы же пойдем по самому простому пути – предъявим одну из возможных минимальных комбинаций свойств. Назовем эту ситуацию внутренним прямым произведением и докажем, что внутреннее прямое произведение изоморфно внешнему. Выбираем 6-е и 7-е свойства. Итак,

Определение. Говорим, что группа G является внутренним прямым произведением своих подгрупп $G_1,\ G_2,\ \ldots, G_n$, если
(i) $g_i g_j = g_j g_i$;
(ii) $\forall g \in G\ \exists\ !\ g_i \in G_i :\ g = g_1 g_2 \ldots g_n$

Теорема. Внутреннее прямое произведение подгрупп изоморфно внешнему прямому произведению.

Надо построить гомоморфизм $f\ :\ G_1 \times \ldots \times G_n\ \to\ G$. Более или менее очевидно, что он должен задаваться формулой

$$f((g_1, \ldots, g_n)) = g_1 \ldots g_n$$

1) f – гомоморфизм – благодаря перестановочности элементов этих подгрупп.
2)f – мономорфизм. Пусть $(g_1, \ldots, g_n) \in \operatorname{Ker} f$, то есть $g_1 \ldots g_n = e$. Но по второму свойству внутреннего прямого произведения e может быть представлен в виде произведения единственным способом, то есть $e \ldots e$
3) f – эпиморфизм. Это также следует из второго свойства.

Приведем некоторые эквивалентные определения внутреннего прямого произведения.

Сначала – **лемма**. Если 2 нормальные подгруппы пересекаются только по 1, то элементы этих подгрупп перестановочны.

2-е определение Скажем, (i) заменяем на нормальность, а (ii) оставляем.

Если выполнено первое определение, то подгруппы нормальны.
Если выполнено второе определение, то подгруппы пересекаются по 1 - иначе не было бы единственности разложения, а тогда по лемме имеем перестановочность.

3-е определение – для конечной группы. (i) оставляем, проверяем $|G| = |G_1| \ldots |G_n|$ и разложение любого элемента. Единственность разложения не требуем - она следует автоматически.

Проще рассуждать, когда у нас две подгруппы.

Лемма Если $H \cap K = \{e\}$ и $G = HK \Rightarrow$ каждый элемент раскладывается единственным образом.

4-е определение для случая 2-х групп. Пересечение состоит из 1 и существует разложение всех элементов, а также перестановочность.

5-е определение для 2-х подгрупп Заменяем перестановочность на нормальность

6-е определение для n подгрупп:
нормальность подгрупп,
G порождается этими подгруппами,
каждая подгруппа пересекается только по 1 с подгруппой, порожденной остальными подгруппами.

Теорема $(G_1 \times G_2)/G_1 \simeq G_2$

Рассмотрим функцию $f : G_1 \times G_2 \to G_2$; $f((g_1, g_2)) = g_2$; докажем, что она является гомоморфизмом, эпиморфизмом, докажем, что $\operatorname{Ker} f = \bar{G}_1$.

Как **следствие** – если факторгруппа по подгруппе G_1 не изоморфна другой подгруппе G_2, то группа не есть прямое произведение этих подгрупп.

Несколько простых утверждений.

Лемма 1. Если $N_1 \lhd G_1;\ N_2 \lhd G_2$, то $N_1 \times N_2 \lhd G_1 \times G_2$.

Замечание. Если нам заданы гомоморфизмы $f_1 : G_1 \to G_3$ и $f_2 : G_2 \to G_4$, то можно построить гомоморфизм, который можно обозначить как $f_1 \times f_2$ или (f_1, f_2) из $G_1 \times G_2$ в $G_3 \times G_4$;

$$(f_1, f_2)((g_1, g_2)) = (f_1(g_1), f_2(g_2).$$

Лемма 2. $\operatorname{Ker}(f_1, f_2) = (\operatorname{Ker} f_1) \times (\operatorname{Ker} f_2)$

Лемма 3. $\operatorname{Im}(f_1, f_2) = (\operatorname{Im} f_1) \times (\operatorname{Im} f_2)$

Теорема. Если $N_1 \lhd G_1;\ N_2 \lhd G_2$, то

$$(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$$

Строим $f : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2),\ f((g_1, g_2)) = (g_1N_1, g_2N_2)$. Доказываем, что это гомоморфизм, ищем его ядро

Теорема Кэли
Любая конечная группа, состоящая из n элементов, изоморфна некоторой подгруппе группы S_n.

Занумеруем элементы группы в произвольном порядке. Рассмотрим функцию, сопоставляющую каждому элементу группы подстановку, задаваемую умножением всех элементов группы на этот элемент (так называемый левый сдвиг):

$$l : G \to S(G) = S_n;\ (l(g))(x) = gx$$

Нужно доказать, что $l(g)$ является биекцией. Отдельно доказываем сюръекцию и инъекцию

Далее нужно доказать, что l – гомоморфизм, более того, мономорфизм. А тогда или просто сказать, что теорема доказана, или сослаться на теорему о гомоморфизме.

Автоморфизмы
Автоморфизм – это изоморфизм на себя.

Примеры 1. Левый сдвиг не является автоморфизмом, если $g \neq e$

2. В множестве невырожденных матриц транспонирование и переход к обратной матрице не являются гомоморфизмами, но если применить и то, и то, то получаем автоморфизм

Теорема Множество всех автоморфизмов является группой $\operatorname{Aut} G$.

Эта теорема уже была раньше.

Теорема. Aut $(\mathbb{Z}_n,+) \simeq (\mathbb{Z}_n^*,\cdot)$

Доказательство. $\mathbb{Z}_n =< 1 >_n$; надо знать, куда переходит 1. Пусть $f_k : \mathbb{Z}_n \to \mathbb{Z}_n$– гомоморфизм, $f_k(1) = k \Rightarrow f_k(m) = f(1+1+\ldots+1) = f(1)+f(1)+\ldots+f(1) = k+k+\ldots+k = mk$. Это мы нашли все гомоморфизмы.Когда такой гомоморфизм является изоморфизмом? То есть когда есть обратный гоморфизм f_t?

$f_k \cdot f_t = f_{kt} = id$, то есть $f_{kt}(x) = ktx = x$ для всех $x \in \mathbb{Z}_n$. Взяв x взаимно простой с n, можем поделить на него, откуда $kt \equiv 1 \pmod n$, то есть k обратим в $\mathbb{Z}_n$. Итак, f_k – автоморфизм тогда и только тогда, когда kобратим в $\mathbb{Z}_n$ (то есть когда k взаимно просто с n).

Внутренние автоморфизмы – уже были. В частности (10-е свойство гомоморфизмов)существует гомоморфизм $\Phi : G \to \text{Aut } G$; $\Phi(a) = i_a$; $i_a(x) = axa^{-1}$. Его образ – подгруппа Int G группы G; найдем его ядро.

$\operatorname{Ker}\Phi = \{a \in G : \ \Phi(a) = id\} = \{a : axa^{-1} = x \ \forall x\} = \{a : \ ax = xa \ \forall x\}$.

Этот факт оправдывает введение еще одного понятия.

Центр $Z(G)$ группы G – это множество всех элементов группы, коммутирующих со всеми элементами группы. Поскольку ядро гомоморфизма является группой, причем нормальной, центр группы является подгруппой группы G, причем нормальной. Это можно считать теоремой.

Таким образом, по теореме о гомоморфизме

$$G/\mathbb{Z}(G) \simeq \text{Int } G$$

Теорема. При гомоморфизме $|f(x)|$ делит $|x|$. При мономорфизме (в частности при изоморфизме) порядок элемента остается прежним.

Доказательство. Возьмем ограничение f на $< x >$, причем для простоты будем обозначать его той же буквой. Образ f также является циклической группой, $\operatorname{Im} f =< f(x) >$. Теорема о гомоморфизме дает $< x > /\operatorname{Ker} f \simeq< f(x) >$, откуда $| < x > | = |x| = |\operatorname{Ker} f| \cdot | < f(x) > | = |\operatorname{Ker} f| \cdot |f(x)|$, то есть порядок $f(x)$ делит порядок x.

Эта теорема сразу позволяет доказать, что множество $Hom(\mathbb{Z}_n; \mathbb{Z}_m)$ всех гомоморфизмов сводится к тривиальному гомоморфизму, если $(n; m) = 1$.

Примеры. 1. G – коммутативна $\Leftrightarrow Z(G) = G$; Int $G = \{id\}$

2. Если $n \geq 3$, то $Z(S_n) = \{id\}$; Int $S_n \simeq S_n$.

Для этого нужно доказать, что для каждой нетождественной подстановки найдется подстановка, которая с ней не коммутирует. Здесь нам поможет наша любимая формула

$$\beta(i_1 i_2 \ldots i_k)\beta^{-1} = (\beta(i_1)\beta(i_2)\ldots b(i_k))$$

3. Aut $S_3 \simeq S_3$

Идея доказательства состоит в том,что в Aut S_3 не меньше элементов, чем в Int $S_3 = S_3$, то есть не меньше, чем 6. Но там не может быть больше, чем 6 элементов, так как группа S_3 порождается своими тремя транспозициями, значит, любой автоморфизм задается своим действием на них, причем транспозицию он переводит в транспозицию.

Задача. Доказать, что:

Aut $(V_4) \simeq S_3$;

Aut $(\mathbb{Z}) \simeq \mathbb{Z}_2$;

Aut $(D_4) \simeq D_4$;

Aut $Q_8 \simeq S_4$ Продумать!

Еще одно определение нормальной подгруппы – она инвариантна под действием всех внутренних автоморфизмов.

Внутреннее полупрямое произведение

Если одна подгруппа нормальна, а вторая нет, шансы получить из них прямое произведение отсутствуют. Но некоторое подобие получить можно. У нас уже была задача, показывающая, что в этом случае NH является подгруппой:

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 \in NH;$$

$$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH.$$

Определение. $G = N \rtimes H$ – полупрямое произведение, если:

$N \lhd G$; $H < G$;

$N \cap H = \{e\}$;

$NH = G$

Второе условие требуется для того, чтобы была единственность представления каждого элемента в виде произведения.

Примеры: $S_n = A_n \rtimes <(12)>$; $S_4 = V_4 \rtimes S_3$

Внешнее полупрямое произведение.

Пусть нам даны две группы и гомоморфизм φ из второй из них в группу автоморфизмов первой. Зададим операцию на декартовом произведении этих групп по формуле, подсказанной внутренним прямым произведением:

$$(n_1; h_1)(n_2; h_2) = (n_1\varphi(h_1)(n_2); h_1h_2)$$

Аксиомы группы надо проверять. Например, надо понять, что будет обратным элементом. Подсказка - как строится обратный во внутреннем полупрямом произведении.

$$(n; h)^{-1} = (\varphi(h^{-1})(n^{-1}); h^{-1})$$

Проверка: $(n; h)(\varphi(h^{-1}(n^{-1}); h^{-1}) = (n\varphi(h)(\varphi(h^{-1})(n^{-1}); hh^{-1}) = (e; e)$

Надо проверить, что если, как и в случае внешнего прямого произведения, считать, что N и H являются подгруппами G, то G окажется внутренним полупрямым произведением этих подгрупп.

Надо проверить, что N нормальна в G – прямая выкладка.

Надо проверить, что N и H пересекаются по единичному элементу = это очевидно.

Надо проверить, что $G = NH$ – но это очевидно.

Важный пример. $C_3 \leftthreetimes C_4$

Aut $(C_3; \cdot) =$ Aut $(\mathbb{Z}_3; +) = (\mathbb{Z}_3^*; \cdot) = \{1;\ 2\} = C_2$

На языке $\mathbb{Z}_3$ единица – это тождественный автоморфизм id; $id(k) = k$ (умножение на 1; впрочем, на языке C_3 – это тоже тождественный автоморфизм $id(k) = k^1$. Тройка на языке $\mathbb{Z}_3$ – это автоморфизм умножения на 2; $\psi(k) = 2k$; на языке C_3 – это автоморфизм возведения во вторую степень; $\psi(k) = k^2$.

Может быть стоит хотя бы частично выписать таблицу Кэли этой группы.

Глупый пример. $C_4 \leftthreetimes C_3$

Aut $(C_4; \cdot) =$ Aut $(\mathbb{Z}_4; +) = (\mathbb{Z}_4^*; \cdot) = \{1;\ 3\} = C_2$

Этот пример оказался бессмысленным, так как единственный гомоморфизм из $\mathbb{Z}_3$ в Z_2 – тождественный, поскольку 2 и 3 взаимно просты (мы доказывали это недавно).

Приведем еще несколько примеров внутреннего полупрямого произведения.

Это, например, разложение D_n в произведение подгруппы вращений (поскольку ее индекс равен двум, она автоматически нормальна) и подгруппы, порожденной каким-нибудь отражением.

Рассмотрим и такой пример. Группа невырожденных матриц, то есть общая линейная группа, распадается в полупрямое произведение нормальной подгруппы матриц с определителем 1 (то есть специальной линейной группы) и группы диагональных матриц, у которых на диагонали стоят числа $(\lambda \neq 0;\ 1;\ \ldots;\ 1)$. Это подгруппы пересекаются только по единичной матрице, и каждый элемент из объемлющей группы распадается в произведение матриц из этих подгрупп. Для доказательства этого выпишем явное разложение. Матрица из специальной линейной группы получается из исходной матрицы делением всех элементов первого столбца на определитель D матрицы, а матрица из второй группы имеет диагональ $(D;\ 1;\ \ldots;\ 1)$

Кстати, можно упомянуть еще такое утверждение.

Теорема. Фактор полупрямого произведения по первому, то есть нормальному, множителю, изоморфен второму множителю.

Доказательство. $G = N \leftthreetimes H$; строим гомоморфизм $f : G \to H$; $f(n, h) = h$

Докажем, что это гомоморфизм. $f(g_1 g_2) = f(n_1 h_1 n_2 h_2) = f(n_1(h_1 n_2 h_1^{-1}) h_1 h_2) = h_1 h_2 = f(g_1) f(g_2)$.

Найдем ядро. $f(g) = f(nh) = h = e \Leftrightarrow g = n$, то есть $\operatorname{Ker} f = N$.

Найдем образ. Впрочем, чего его искать, ясно, что образ совпадает с H.

А тогда по теореме о гомоморфизме $G/N \simeq H$

Кстати, можно было провести доказательство на языке внешнего полупрямого произведения.