Лекция 1

ГРУППЫ

Определение. Группой G *называется непустое множество, в котором для любых двух элементов* $x, y \in G$ *определен элемент* $xy \in G$ *(произведение), причем:*

1) $(xy)z = x(yz) \quad \forall x, y, z \in G$;

2) $\exists 1 \in G \quad : \quad 1 \cdot x = x \cdot 1 = x \quad \forall x \in G$;

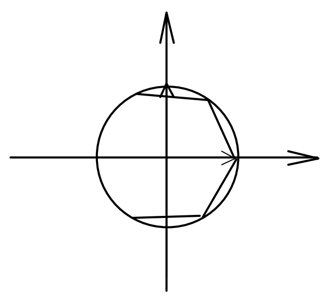
3) $\forall x \in G \quad \exists x^{-1} \in G \quad : \quad xx^{-1} = x^{-1}x = 1$.

Примеры групп:

1) $GL(n, C)$ - невырожденные матрицы размера $n \times n$ с комплексными коэффициентами – группа относительно операции умножения матриц;

2) $Z,+$ - целые числа – группа относительно операции сложения целых чисел;

3) Группа диэдра $D_n, \quad n \geq 3$:



Рассмотрим на плоскости ортонормированный базис, приведем окружность единичного радиуса с центром в начале координат. Впишем в нее правильный n-угольник, одна из вершин которого находится в конце вектора e_1. D_n - это все движения плоскости, переводящие этот n-угольник в себя.

Убедимся в том, что это множество будет группой относительно композиции движений:

1) композиция движений ассоциативна;

2) в качестве единичного элемента можно взять тождественное движение;

3) в качестве обратного элемента можно взять обратное движение.

Рассмотрим эту группу более подробно. При любом таком движении центр n-угольника остается на месте, следовательно, это ортогональное преобразование плоскости, т.е. либо поворот на некоторый угол, либо симметрия относительно некоторой прямой.

Т.к. при повороте вершина e_1 должна перейти в какую-то вершину, то поворот может быть только на угол $\frac{2\pi k}{n}$, где $0 \leq k < n$. Обозначим матицу поворота на угол $\frac{2\pi}{n}$ за $a = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \in D_n$. В качестве симметрии подходит, например, симметрия относительно оси x, матрица такого преобразования $b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in D_n$.

Теорема. *Группа* D_n *состоит из* $2n$ *элементов, а именно* $1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots ba^{n-1}$ *и* $a^n = (ba^k)^2 = 1 \quad \forall k = 0, 1, \ldots, n-1$.

Доказательство.

Как уже говорилось, поворот может быть только на угол $\frac{2\pi k}{n}$, где $0 \leq k < n$. Запишем матрицу такого поворота: $\begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}$, но ни что иное как a^k. Следовательно $1, a, a^2, \ldots, a^{n-1}$ - это все повороты, входящие в группу D_n.

Пусть теперь b_1 - это какая-нибудь симметрия из группы D_n. Тогда bb_1 тоже принадлежит этой группе, причем это ортогональная матрица и ее определитель равен $\det(bb_1) = \det b \cdot \det b_1 = (-1)\cdot(-1) = 1$. Следовательно, это поворот, т.е. $bb_1 = a^k \Rightarrow b^2 b_1 = ba^k$. Т.к. $b^2 = E$, то $b_1 = ba^k$, следовательно, все симметрии из D_n - это $b, ba, ba^2, \ldots, ba^{n-1}$.

Мы доказали, что группа D_n не содержит ничего кроме элементов $1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots ba^{n-1}$, докажем теперь, что все эти элементы различны. Все элементы a^i различны, т.к. это повороты на разные углы. Если $a^k = ba^s$, то $1 = \det a^k = \det ba^s = \det b \cdot \det a^s = -1$, что невозможно. Если $ba^k = ba^s$, то $a^k = b^2 a^k = b^2 a^s = s^s$, а мы уже доказали, что это невозможно.

И последнее утверждение теоремы. a^n - это поворот на угол $\frac{2\pi}{n} \cdot n = 2\pi$, т.е. тождественное движение. Т.к. $\det ba^k = -1$, то это симметрия относительно некоторой прямой, но симметрия в квадрате это всегда тождественное движение, следовательно, $(ba^k)^2 = 1$. ◊

Упражнение. *Доказать, что* $ba = a^{-1}b$.

4) приведем пример еще одной группы – группы кватернионов Q_8. Рассмотрим матрицы

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Упражнение. Доказать, что $I^2 = J^2 = K^2 = -E$, $IJ = K = -JI$, $JK = I = -KJ$, $KI = J = -IK$. Доказать, что матрицы $\pm E, \pm I, \pm J, \pm K$ образуют группу относительно операции умножения матриц.

Упражнение. Докажите, что в любой группе единичный элемент 1 определен однозначно и для любого элемента x обратный элемент x^{-1} также определен однозначно.

Определение. Порядком группы G *называется количество элементов в группе, обозначается* $|G|$.

Упражнение. Рассмотрим группу $GL(n, F_q)$ - невырожденные матрицы $n \times n$ над полем из q элементов. Доказать, что ее порядок равен $|GL(n, F_q)| = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1})$.

Определение. *Пусть* G *- группа. Непустое подмножество* H *в* G *называется* **подгруппой**, *если*
1) $g, h \in H \Rightarrow gh \in H \quad \forall g, h$;
2) $g \in H \Rightarrow g^{-1} \in H \quad \forall g$.

Замечание. Единичный элемент всегда принадлежит любой подгруппе. Т.к. H непустое, то там есть хотя бы один элемент a. По свойству 2) $a^{-1} \in H$, по свойству 1) $1 = aa^{-1} \in H$.

Упражнение. Докажите, что в любой группе пересечение любого числа подгрупп тоже будет подгруппой.

Примеры подгрупп:

1) Группа $GL(n, C)$. Ее подгруппы: $GL(n, R)$; $SL(n, R)$ - вещественные матрицы с определителем единица; $SL(n, C)$; $U(n, C)$ - унитарные матрицы; $SU(n, C)$ - унитарные матрицы с определителем единица; $O(n, R)$ - ортогональные матрицы; $SO(n, R)$; (D_n ; Q_8 - подгруппы в группе $GL(2, C)$);

2) S_n - группа подстановок. A_n (четные подстановки) – подгруппа. В частном случае, если $n=4$ множество $A_4 \supset V = \{1,(12)(34),(13)(24),(14)(23)\}$ также будет подгруппой;

3) C^* - группа ненулевых комплексных чисел относительно умножения. Ее подгруппы: $U = \{z \in C \quad : \quad |z| = 1\}$ - единичная окружность; $U_n = \{z \in C \quad : \quad z^n = 1\}$ - корни из единицы.

Определение. *Пусть* $a \in G$ *- элемент группы и* $n \in Z$ *- целое число, тогда* $a^n \overset{def}{=} \begin{cases} 1, & n = 0 \\ \underbrace{a \cdot \ldots \cdot a}_{n}, & n > 0 \\ \left(a^{|n|}\right)^{-1}, & n < 0 \end{cases}$.

Теорема. *Если* $n,m \in Z$*, то* $\left(a^n\right)^m = a^{nm}$ *и* $a^n a^m = a^{n+m}$.

Упражнение. Докажите теорему.

Определение. *Пусть* $a \in G$. **Порядком элемента** a *(обозначается* $o(a)$ *или* $|a|$*) называется наименьшее натуральное* n *такое, что* $a^n = 1$*. Если такого числа не существует, то элемент имеет бесконечный порядок.*

Упражнение. Найдите порядок элемента $\frac{3}{5} + i\frac{4}{5} \in C^*$.

Предложение. Пусть $|a| = n$. Для целого числа $m \in Z$ следующие условия эквивалентны:

1) $a^m = 1$;
2) $n \mid m$.

Доказательство.

$2) \Rightarrow 1)$. Пусть $m = n \cdot k$, $k \in Z$, тогда $a^m = a^{nk} = \left(a^n\right)^k = 1^k = 1$.

$1) \Rightarrow 2)$. Пусть $m = nq + r$, где $0 \le r < n$, тогда $a^r = a^{m-nq} = a^m \left(a^n\right)^{-q} = 1$. Следовательно $r = 0$, т.к. иначе имели бы $|a| = r < n$. Следовательно $n \mid m$. $\Diamond$.

ЦИКЛИЧЕСКИЕ ГРУППЫ

Определение. *Пусть* $a \in G$. **Циклической подгруппой** $\langle a \rangle$*, порожденной элементом* a*, называется множество* $\{a^k, \quad k \in Z\}$.

Это определение корректно, т.к. $a^n a^m = a^{n+m}$ - снова степень a, $\left(a^k\right)^{-1} = a^{-k}$ - снова степень a.

Определение. *Группа* G *-* **циклическая***, если* $\exists a \in G$ *такой, что* $G = \langle a \rangle$.

Примеры циклических групп:

1) $Z,+$, т.к. $Z = \langle 1 \rangle = \langle -1 \rangle$;
2) $U_n = \langle \varepsilon \rangle$, где $\varepsilon = \exp\left(\frac{2\pi i}{n}\right) = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Теорема. *Пусть* $G = \langle a \rangle$*, тогда* $|G| = |a|$.

Доказательство.

Допустим, что найдутся такие $s > m$, что $a^s = a^m$. Тогда $a^{s-m} = 1$ и $s - m > 0$. Следовательно, порядок элемента a конечен $|a| = n < \infty$. Пусть $M \in Z$ и $M = nq + r$, тогда $a^M = a^{nq+r} = a^r$. Следовательно, группа G состоит из элементов $\{1, a, a^2, \ldots, a^{n-1}\}$. Докажем, что они все различны. Пусть $0 \le r_1 < r_2 < n$ и $a^{r_1} = a^{r_2}$, тогда $a^{r_2 - r_1} = 1$ и $|a| = r_2 - r_1 < n$. Получили противоречие, следовательно $G = \{1, a, a^2, \ldots, a^{n-1}\}$, все элементы различны и всего из n штук, т.е. $|G| = |a| = n$.

Если же все степени a будут различны, то $|G| = |a| = \infty$. ◊

Теорема. *Любая подгруппа циклической группы сама является циклической.*
Доказательство.

Пусть $H \subset G = \langle a \rangle$. Тогда H состоит из каких-то степеней элемента a. Заметим, что если $a^k \in H$, то и $a^{-k} \in H$. Если $H = \{1\}$, то $H = \langle 1 \rangle$. Если же H содержит не только единичный элемент, то H содержит какой-то элемент a^k, где $k > 0$ (в силу нашего замечания выше). Пусть m - наименьшее натуральное число такое, что $b = a^m \in H$. Пусть $a^M \in H$ и $M = mq + r$, где $0 \le r < m$. Тогда $a^r = \underset{\in H}{a^M} \underset{\in H}{\left(a^m\right)^{-q}} \in H$. Если $r \ne 0$, то мы получаем противоречие с выбором числа m, следовательно, $r = 0$ и $a^M = \left(a^m\right)^k = b^k$. Следовательно $H = \langle b \rangle$. ◊

Следствие 1. Пусть $m_1, \ldots, m_k \in Z$ и $d = НОД(m_1, \ldots, m_k)$, тогда $\exists u_1, \ldots, u_k \in Z$ такие, что $d = u_1 m_1 + \ldots + u_k m_k$.

Следствие 2. Пусть $G = \langle a \rangle_n$ (порядка n) и H - подгруппа в G, тогда $H = \langle a^d \rangle$, причем $d \mid n$.
Доказательство.

По теореме $H = \langle a^k \rangle$. Пусть $d = НОД(n, k) = ku + nv$, тогда $a^d = \left(a^k\right)^u \left(a^n\right)^v = \left(a^k\right)^u \in H$. Следовательно $\langle a^d \rangle \subseteq H$. Докажем теперь включение в другую сторону. Пусть $\left(a^k\right)^s \in H$, но $k = dl$, следовательно $\left(a^k\right)^s = \left(a^{dl}\right)^s = \left(a^d\right)^{ls} \in \langle a^d \rangle$. Следовательно $H \subseteq \langle a^d \rangle$, т.е. $H = \langle a^d \rangle$, причем $d \mid n$. ◊

Упражнение. Докажите, что $\left|\langle a^d \rangle\right| = \dfrac{n}{d}$, где $n = \left|\langle a \rangle\right|$.

Лекция 2

СМЕЖНЫЕ КЛАССЫ

Определение. *Пусть у нас заданы группа G и подгруппа H, пусть также дан элемент $g \in G$.* **Левым смежным классом** *называется множество $gH = \{gh \mid h \in H\}$.* **Правым смежным классом** *называется множество $Hg = \{hg \mid h \in H\}$.*

Примеры:

1) Пусть $G = S_n$ и $H = S_{n-1}$ - группы подстановок. Доопределим подстановки из S_{n-1} следующим образом: n они переводят в n. Тогда получим, что S_{n-1} - это подгруппа S_n. Пусть $g = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}$. Левый смежный класс – это по определению множество $gS_{n-1} = \{g\sigma \mid \sigma \in S_{n-1}\}$. Т.к. $\forall \sigma$ имеем, что $\sigma(n) = n$, то $g\sigma(n) = i_n \quad \forall \sigma$. Верно и обратное, если $\tau(n) = i_n$, то $\tau \in gS_{n-1}$. Т.е. левый смежный класс gS_{n-1} - это множество подстановок, переводящих n в i_n.

2) Аналогично пусть $G = S_n$ и $H = S_{n-1}$ и $g = \begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix}$. Аналогичными рассуждениями можно получить, что $S_{n-1}g$ - это множество подстановок, переводящих i_n в n.

На этих примерах видно, что левый смежный класс не совпадает с правым, т.е. $gH \neq Hg$.

Предложение. $|H| = |gH|$.
Доказательство.
Пусть $|H| = n < \infty$, $H = \{h_1, \dots, h_n\}$, $h_i \neq h_j$ при $i \neq j$. $gH = \{gh_1, \dots, ghn\}$. Убедимся в том, что все элементы gh_i различны. Если $gh_i = gh_j$, то $g^{-1}gh_i = g^{-1}gh_j$, следовательно, $h_i = h_j$, следовательно $i = j$, следовательно $|gH| = |H|$.

Если $|H| = \infty$, то аналогичными рассуждениями получаем, что $|gH| = \infty$. ◊

Предложение. Если $y \in xH$, тогда $yH = xH$.
Доказательство.
Т.к. $y \in xH$, то $\exists h \in H : y = xh$. Тогда $\forall u \in H$ имеем, что $yu = x\underbrace{(hu)}_{\in H} \in xH$, следовательно, $yH \subseteq xH$. Обратно. Т.к. $x = yh^{-1}$, то $\forall u \in H$ имеем, что $xu = y\underbrace{(h^{-1}u)}_{\in H} \in yH$, следовательно $xH \subseteq yH$, т.е. $xH = yH$. ◊

Следствие. Любые два левых (правых) смежных класса либо совпадают, либо не пересекаются.

Теорема (Лагранж). *Пусть H - подгруппа конечной группы G, тогда $|G| = j|H|$, где j - число различных левых (правых) смежных классов G по H.*
Доказательство.
Пусть $g \in G$, тогда $g = g \cdot 1 \in gH$. Т.е. любой элемент группы G попадает в некоторый смежный класс, таким образом, вся группа G разбивается на j непересекающихся множеств, каждое из которых имеет $|H|$ элементов, следовательно $|G| = j|H|$. ◊

Упражнение. Докажите, что $xH = yH$ тогда и только тогда, когда $x^{-1}y \in H$.

Следствие 1. Порядок элемента делит порядок группы.
Доказательство.
Пусть $g \in G$, тогда $|g| = |\langle g \rangle|$. По теореме Лагранжа $|\langle g \rangle|$ делит порядок группы, следовательно и порядок элемента делит порядок группы. ◊

Следствие 2. Группа простого порядка циклическая.
Доказательство.
Пусть $|G| = p$ - простое число. Возьмем элемент $g \neq 1, g \in G$, тогда $|g| > 1$ и $|g|$ делит p. Следовательно $|g| = p$, следовательно $|\langle g \rangle| = p$ и $G = \langle g \rangle$. ◊

Теорема. *Пусть G - конечная подгруппа в C^*. Тогда G - циклическая.*
Доказательство.
Пусть $|G| = n$, если $z \in G$, то по следствию 1 $z^n = 1$, т.е. любой элемент из G является корнем n-й степени из 1. Следовательно $G \subseteq U_n = \left\langle \exp\left(\frac{2\pi i}{n}\right) \right\rangle$. U_n циклическая, а подгруппа циклической группы тоже циклическая. ◊

Упражнение. Докажите эту теорему для любого поля.

МОРФИЗМЫ

Определение. *Отображение* $f:G\to H$ *называется* **гомоморфизмом**, *если* $f(xy)=f(x)f(y)$. *Инъективный гомоморфизм называется* **мономорфизмом**. *Сюръективный гомоморфизм называется* **эпиморфизмом**. *Биективный гомоморфизм называется* **изоморфизмом**. *Изоморфизм группы на себя называется* **автоморфизмом**.

Примеры:

1) $G=GL(n,C)$, $H=C^*$. $f(A)=\det A$ - гомоморфизм.

2) $G=S_n$, $H=\{1;-1\}$. $f(A)=(-1)^\sigma$ - гоморфизм.

3) $Aff(n)$ - группу аффинных преобразования n-мерного пространства отобразим на $GL(n)$ - группу линейных преобразований n-мерного пространства. Будем ставить аффинному преобразованию в соответствие его дифференциал, т.е. $f(x)=Ax+B$ - аффинное преобразование перейдет в $D(f)=Ax$. Это будет гомоморфизмом.

4) Пусть есть группа G, возьмем элемент $g\in G$. Автоморфизм сопряжения с помощью элемента g: $f(x)=gxg^{-1}$. Этот автоморфизм нетривиален (не тождественный), если найдется x такой, что $gx\neq xg$.

Определение. *Группа называется* **абелевой** *(***коммутативной***), если* $\forall x,y \quad xy=yx$.

Предложение. Если $f:G\to H$ - гомоморфизм, то $f(1_G)=1_H$ и $f(x^{-1})=f(x)^{-1}$.

Здесь 1_G - единичный элемент группы G, 1_H - единичный элемент группы H. x^{-1} - обратный к x элемент группы G, $f(x)^{-1}$ - обратный к $f(x)$ элемент группы H.

Доказательство.

1) Т.к. $1_G\cdot 1_G=1_G$, то $f(1_G)f(1_G)=f(1_G)$. Имеем
$f(1_G)=f(1_G)^{-1}f(1_G)f(1_G)=f(1_G)^{-1}f(1_G)=1_H$.

2) $1_H=f(1_G)=f(xx^{-1})=f(x)f(x)^{-1}$, следовательно $f(x^{-1})=f(x)^{-1}$. ◊

Предложение. Гомоморфизм $f:G\to H$ является мономорфизмом тогда и только тогда, когда из $f(x)=1$ следует $x=1$, т.е. полный прообраз единицы равен единице.

Доказательство.

$\Rightarrow$ Если f мономорфизм и $f(x)=1$. Т.к. $f(1)=1$ и f инъективно, то $x=1$.

$\Leftarrow$ Пусть $f^{-1}(1)=1$ (полный прообраз) и $f(x)=f(y)$. Тогда
$f(x^{-1}y)=f(x)^{-1}f(y)=f(y)^{-1}f(y)=1$. По условию $x^{-1}y=1$, т.е. $x=y$. Следовательно f - инъективно, т.е. является мономорфизмом. ◊

Определение. *Пусть отображение* $f:G\to H$ *- гомоморфизм групп. Тогда* **ядром** *этого отображения называется множество* $\mathrm{Ker}\, f=f^{-1}(1)$, *т.е. полный прообраз единицы.*

По предыдущему предложению получаем, что f - мономорфизм тогда и только тогда, когда $\mathrm{Ker}\, f=\{1\}$.

Упражнение. Пусть $f:G\to H$ - гомоморфизм групп, доказать, что $\mathrm{Im}\, f$ является подгруппой в H.

Определение. *Подгруппа* N *в группе* G *называется* **нормальной** *(обозначается* $N\triangleleft G$*), если* $\forall x\in G \quad xNx^{-1}\subseteq N$, *т.е. если* $\forall x\in G \quad \forall y\in N \quad xyx^{-1}\in N$.

Предложение. Пусть N - подгруппа в G, тогда следующие утверждения эквивалентны:

1) $N \triangleleft G$;

2) $xNx^{-1} = N \quad \forall x \in G$;

3) каждый правый смежный класс совпадает с левым, т.е. $Nx = xN$.

Доказательство.

$2) \Rightarrow 1)$ Очевидно.

$1) \Rightarrow 3)$ Надо доказать, что $Nx = xN$, пусть $a \in N$, тогда $x^{-1}ax \in N$. Поэтому $ax = x(x^{-1}ax) \in xN$, следовательно $Nx \subseteq xN$. Обратно аналогично: $xa = (xax^{-1})x \in Nx$, следовательно $xN \subseteq Nx$ и $Nx = xN$.

$3) \Rightarrow 2)$ Мы имеем, что $Nx = xN$. Возьмем произвольный элемент $a \in N$, тогда $xa \in xN = Nx$, т.е. $\exists b \in N : xa = bx$, но тогда $xax^{-1} = b \in N$. Мы получили, что $xNx^{-1} \subseteq N$. Теперь покажем, что таким образом можно получить любой элемент из N, т.е. что $xNx^{-1} = N$. Если $b \in N$, то $bx \in Nx = xN$, следовательно $\exists a \in N : bx = ax$, но тогда $b = xax^{-1}$. Следовательно $xNx^{-1} = N$. ◊

Пример:

При помощи этого предложения можно доказать, что S_{n-1} не является нормальной подгруппой в S_n, т.к. ее левые и правые смежные классы не совпадают.

Теорема. *Пусть* $f : G \to H$ *- гомоморфизм, тогда* $\operatorname{Ker} f \triangleleft G$.

Доказательство.

Сначала докажем, что $\operatorname{Ker} f$ является подгруппой в G.

Если $x, y \in \operatorname{Ker} f$, то и $xy \in \operatorname{Ker} f$, т.к. $f(xy) = f(x)f(y) = 1 \cdot 1 = 1$.

Если $x \in \operatorname{Ker} f$, то и $x^{-1} \in \operatorname{Ker} f$, т.к. $f(x^{-1}) = f(x)^{-1} = 1^{-1} = 1$.

Теперь докажем нормальность этой подгруппы.

$\forall g \in G \quad \forall x \in \operatorname{Ker} f \quad f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(g)^{-1} = 1$, следовательно $gxg^{-1} \in \operatorname{Ker} f$ и $\operatorname{Ker} f \triangleleft G$. ◊

Примеры:

1) $f : GL(n, C) \to C^*$, $f(A) = \det A$. Тогда $\operatorname{Ker} f = SL(n, C) \triangleleft GL(n, C)$.

2) $f : S_n \to \{1; -1\}$, $f(\sigma) = \sigma^{-1}$. Тогда $\operatorname{Ker} f = A_n \triangleleft S_n$.

3) $f : (R, +) \to U = \{z \in C^* : |z| = 1\}$, $f(r) = \exp(2\pi i r)$. Тогда $\operatorname{Ker} f = Z \triangleleft R$.

Предложение. Если $f : G \to H$ - гомоморфизм и $x \in G$, тогда $f^{-1}(f(x)) = x \operatorname{Ker} f$.

Доказательство.

$y \in f^{-1}(f(x)) \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x^{-1}y) = 1 \Leftrightarrow x^{-1}y \in \operatorname{Ker} f \Leftrightarrow y \in x \operatorname{Ker} f$. ◊

Определение. *Пусть* $N \triangleleft G$, **фактор группа** G/N *- это множество смежных классов* G *по* N *с операцией* $(aN)(bN) = abN$.

Теорема. G/N *- группа.*

Доказательство.

Сначала докажем, что операция определена корректно. Пусть $aN = a'N$ и $bN = b'N$, покажем, что $abN = a'b'N$. Имеем $a' = an, \quad n \in N$ и $b' = bm, \quad m \in N$, тогда $a'b' = anbm = ab(b^{-1}nb)m = abkm$. Причем $k = b^{-1}nb \in N$, следовательно $a'b' \in abN \Rightarrow abN = a'b'N$.

Ассоциативность операции: $(aN \cdot bN) \cdot cN = abN \cdot cN = abcN = aN \cdot bcN = aN \cdot (bN \cdot cN)$.

Единичный элемент: $N = 1 \cdot N$.

Обратный элемент: $(aN)^{-1} = a^{-1}N$. ◊

Отображение $\pi : G \to G/N$, $\pi(x) = xN$ называется естественным эпиморфизмом.

Теорема. *Отображение* π *- эпиморфизм и* $\operatorname{Ker}\pi = N$.
Доказательство.
$\pi(xy) = xyN = (xN)(yN) = \pi(x)\pi(y)$, т.к. $xN = \pi(x)$, то у любого смежного класса есть прообраз, следовательно, это эпиморфизм. Т.к. $\forall x \in N \quad \pi(x) = xN = N = 1 \cdot N$, то $\operatorname{Ker}\pi = N$. ◊

Теорема (о гомоморфизме). *Пусть* $f : G \to H$ *- гомоморфизм групп, тогда* $\operatorname{Im} f \cong G/\operatorname{Ker} f$ *(изоморфно).*
Доказательство.
Построим изоморфизм $\operatorname{Im} f \cong G/\operatorname{Ker} f$: $\xi : \operatorname{Im} f \to G/\operatorname{Ker} f$, $\xi(f(x)) = x\operatorname{Ker} f$. Эта отображение определено корректно, т.к. $f(x) = f(y) \Leftrightarrow x\operatorname{Ker} f = y\operatorname{Ker} f$.
Докажем, что это гомоморфизм:
$\xi(f(x)f(y)) = \xi(f(xy)) = xy\operatorname{Ker} f = (x\operatorname{Ker} f)(y\operatorname{Ker} f) = \xi(f(x))\xi(f(y))$.
Докажем биективность, т.е. что это изоморфизм. Т.к. $f(x) = f(y) \Leftrightarrow x\operatorname{Ker} f = y\operatorname{Ker} f$, это отображение биективно. ◊

Пример:
Покажем, как при помощи этой теоремы доказать изоморфность $GL(n,C)/SL(n,C) \cong C^*$. Нам нужно задать гомоморфизм $f : GL(n,C) \to C^*$ такой, чтобы $\operatorname{Ker} f = SL(n,C)$. Например $f(A) = \det A$. Тогда по теореме о гомоморфизме будем иметь, что $GL(n,C)/SL(n,C) \cong C^*$.

Лекция 3

Теорема. *Циклическая группа порядка* n *изоморфна группе* Z/nZ.
Доказательство.
Пусть $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$. Зададим гомоморфизм $f : Z \to G$ следующим образом: $f(m) = a^m$. Это гомоморфизм, т.к. $f(m_1 + m_2) = a^{m_1+m_2} = a^{m_1}a^{m_2} = f(m_1)f(m_2)$. Тогда по теореме о гомоморфизме имеем $G \cong Z/nZ$. ◊

Упражнение. Бесконечная циклическая группа изоморфна группе Z.

Определение. *Пусть* G *- группа.* X *- произвольное множество.* G **действует на** X*, если есть отображение* $G \times X \to X$*, т.е. которое паре* (g,x) *ставит в соответствие некоторый элемент* $gx \in X$*. Причем* $1x = x$ *и* $g(hx) = (gh)x$.

Примеры:
1) $GL(n,C)$ действует на V - n-мерном комплексном пространстве, по следующему правилу: пусть e - базис, в нем вектор x имеет координаты $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, тогда $Ax = A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in V$.

2) Пусть H - подгруппа в G, тогда H действует на G по правилу $(h,g) \to hg$.

3) Пусть $G=S_n$ и $X=\{1,\dots,n\}$. Имеем естественное действие симметрической группы на множестве $\{1,\dots,n\}$.

4) Пусть $G=S_n$ и $X=k[T_1,\dots,T_n]$ - многочлены от n неизвестных. Действие определим по правилу $(\sigma, f(T_1,\dots,T_n))\to f(T_{\sigma(1)},\dots,T_{\sigma(n)})$.

5) G действует на $X=G$ сопряжением $(g,x)\to gxg^{-1}$. Т.к. $(1,x)\to 1x1^{-1}=x$ и $(gh,x)=ghx(gh)^{-1}=ghxh^{-1}g^{-1}=(g,(h,x))$, то это действительно будет действием.

Предложение. Пусть G действует на X и $g\in G$, тогда отображение $x\to gx$ является биекцией на множестве X.

Доказательство.

Для доказательства этого факта на достаточно указать обратное отображение. Им будет отображение $x\to g^{-1}x$. Оно действительно будет обратным, т.к. $x\to gx\to g^{-1}(gx)=(g^{-1}g)x=x$ и $x\to g^{-1}x\to g(g^{-1}x)=(gg^{-1})x=x$. Следовательно, это биекция. ◊

Определение. *Пусть* G *действует на* X *и* $x\in X$. **Орбита** x *- это множество* $\mathrm{Orb}_x=\{gx\mid g\in G\}$. **Стабилизатор** x *- это множество* $\mathrm{St}_x=\{g\in G\mid gx=x\}$.

Упражнение. Доказать, что St_x является подгруппой в G.

Определение. *Пусть* G*- группа* $x\in G$. **Централизатор** x *- это множество* $C(x)=\{g\in G\mid gx=xg\}$. **Класс сопряженных элементов, содержащий** x *- это множество* $K(x)=\{gxg^{-1}\mid g\in G\}$.

Примеры:

1) При действии $GL(n,C)$ на V - n-мерном пространстве будет всего две различные орбиты: все ненулевые векторы (орбита любого ненулевого вектора), ноль (орбита нуля).

2) При действии подгруппы H на группе G имеем $\mathrm{Orb}_x=Hx$ и $\mathrm{St}_x=\{1\}$.

3) При действии G на себе сопряжением имеем $\mathrm{Orb}_x=\{gxg^{-1}\mid g\in G\}=K(x)$, $\mathrm{St}_x=\{g\in G\mid gxg^{-1}=x\}=\{g\in G\mid gx=xg\}=C(x)$.

Предложение. Если орбиты пересекаются, то они совпадают.

Доказательство.

Пусть $z\in \mathrm{Orb}_x\cap \mathrm{Orb}_y \Rightarrow z=gx,\ g\in G$. $\forall h\in G$ имеем $hz=(hg)x\in \mathrm{Orb}_x$, следовательно $\mathrm{Orb}_z\subseteq \mathrm{Orb}_x$. $\forall u\in G$ имеем $ux=(ug^{-1})gx=(ug^{-1})z\in \mathrm{Orb}_z \Rightarrow \mathrm{Orb}_x\subseteq \mathrm{Orb}_z \Rightarrow \mathrm{Orb}_z=\mathrm{Orb}_x$. Аналогично имеем $\mathrm{Orb}_y=\mathrm{Orb}_z=\mathrm{Orb}_x$. ◊

Предложение. $|\mathrm{Orb}_x|=\dfrac{|G|}{|\mathrm{St}_x|}$.

Доказательство.

Допустим, что $gx=hx$, но тогда $(h^{-1}g)x=x\Leftrightarrow h^{-1}g\in \mathrm{St}_x\Leftrightarrow h\mathrm{St}_x=g\mathrm{St}_x$. Следовательно существует биекция между множеством орбит и множеством левых смежных классов G по St_x. Следовательно $|\mathrm{Orb}_x|$ - это число различных смежных классов, а по теореме Лагранжа это равно $\dfrac{|G|}{|\mathrm{St}_x|}$. ◊

Следствие. $|K(x)|=\dfrac{|G|}{|C(x)|}$.

Упражнение. Доказать, что если $N \lhd G$, то $\left| G/N \right| = \dfrac{|G|}{|N|}$.

Определение. *Пусть* G *действует на* X. *Элемент* $x \in X$ *называется* **неподвижным** *(***инвариантным***) относительно этого действия, если* $gx = x \quad \forall g \in G$*, т.е. если* $\mathrm{St}_x = G$.

Примеры:

1) При действии симметрической группы на многочлены неподвижными являются симметрические многочлены.

2) При действии G на себе сопряжением имеем, что элемент x неподвижен тогда и только тогда, когда $C(x) = G$. Множество всех неподвижных элементов группы называется **центром группы** G (обозначается $Z(G)$).

Упражнение. $Z(G)$ - нормальная абелевая подгруппа в G.

Теорема. *Пусть* k *-поле, тогда* $Z(GL(n,k)) = \{\lambda E \mid \lambda \in k^*\}$.

Доказательство.

Пусть $A \in Z(GL(n,k))$, если она неподвижна, то $E_{ij}A = AE_{ij} \quad \forall i,j$. Распишем это равенство:

$$E_{ij}A = \begin{array}{c} \\ i \\ \\ \\ \end{array}\begin{pmatrix} & 0 & \\ a_{j1} & \dots & a_{jn} \\ & 0 & \end{pmatrix} = \begin{array}{c} \\ i \\ \\ \\ \end{array}\begin{pmatrix} & a_{1i} & \\ 0 & \vdots & 0 \\ & a_{ni} & \end{pmatrix} = AE_{ij}.$$
$$\qquad\qquad j \qquad\qquad\qquad\qquad j$$

В левой матрице на месте (ij) стоит элемент a_{jj}, а в правой a_{ii}, следовательно $a_{jj} = a_{ii}$, а остальные элементы нули. Т.к. это верно для любых i,j, то матрица A диагональная и по диагонали стоят одинаковые числа, т.е. $A = \lambda E$. ◊

Упражнение. Найдите центры групп $SL(n,k)$ и $O(n,R)$.

Теорема. *При* $n \geq 3$ $Z(S_n) = \{1\}$.

Доказательство.

Возьмем $\sigma \in S_n \setminus \{1\}$ - любую не единичную подстановку. Разложим ее в произведение независимых циклов: $\sigma = (i_1 \dots i_k)(j_1 \dots j_m)\dots$

1) Пусть в этом разложении есть два цикла, т.е. $k, m \geq 2$. Возьмем подстановку $\pi = (i_1 j_1)$, тогда $\pi\sigma\pi^{-1} = (j_1 i_2 \dots i_k)(i_1 j_2 \dots j_m)\dots \Rightarrow \pi\sigma\pi^{-1} \neq \sigma$.

2) Пусть в этом разложении есть хотя бы один цикл длины 3, т.е. $\sigma = (i_1 \dots i_k)$, $k \geq 3$. Возьмем подстановку $\pi = (i_1 i_2)$, тогда $\pi\sigma\pi^{-1} = (i_2 i_1 i_3 \dots i_k) \neq \sigma$.

3) Пусть в этом разложении есть только один цикл длины 2, т.е. $\sigma = (i_1 i_2)$. Т.к. мы работаем в группе S_n при $n \geq 3$, то найдется $i_3 \notin \{i_1, i_2\}$. Возьмем подстановку $\pi = (i_1 i_3)$, тогда $\pi\sigma\pi^{-1} = (i_3 i_2) \neq \sigma$.

Оставшийся случай - ни одного цикла - это и будет единичная подстановка. Следовательно неподвижной может быть только единичная подстановка. ◊

Упражнение. Докажите, что $\pi(i_1 \dots i_k)\pi^{-1} = (\pi(i_1) \dots \pi(i_k)) \quad \forall \pi \in S_n$.

Теорема. Две подстановки из S_n сопряжены тогда и только тогда, когда они имеют одинаковое цикловое строение, т.е. наборы длин циклов у них одинаковые.

Доказательство.

$\Rightarrow$. Пусть $\sigma = (i_k \dots i_k)(j_1 \dots j_m)\dots$, тогда $\pi\sigma\pi^{-1} = [\pi(i_1 \dots i_k)\pi^{-1}][\pi(j_1 \dots j_m)\pi^{-1}]\dots = (\pi(i_1)\dots\pi(i_k))(\pi(j_1)\dots\pi(j_m))\dots$. Т.к. $i_* \neq j_{**}$, то и $\pi(i_*) \neq \pi(j_{**})$, следовательно, эти циклы независимые и мы получили такое же цикловое строение.

$\Leftarrow$. Покажем на примере, как по данным двум подстановкам σ и ρ найти подстановку π, такую что $\rho = \pi\sigma\pi^{-1}$. Пусть $\sigma = (12)(456) \in S_6$ и $\rho = (132)(45) \in S_6$, тогда $\pi\sigma\pi^{-1} = \pi(12)(456)\pi^{-1} = (\pi(1)\pi(2))(\pi(4)\pi(5)\pi(6)) = \rho = (45)(132)$, следовательно $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 3 & 2 \end{pmatrix}$. ◊

Определение. *Группа G называется p* **-группой***, если ее порядок является степенью простого числа p.*

Теорема. *Если G - p-группа, то $Z(G) \neq \{1\}$.*

Доказательство.

Разобьем G на классы сопряженных элементов (они не пересекаются) $G = K(x_1) \cup \dots \cup K(x_n)$. Одноэлементные классы состоят из одного центрального элемента. Если $K(x_i)$ - не одноэлементный класс, то $|K(x_i)| = \dfrac{|G|}{|C(x_i)|}$ - делится на p. Имеем, что $|G| = |Z(G)| + p \cdot N$, где $|Z(G)|$ отвечает всем одноэлементным классам, а $p \cdot N$ - не одноэлементным. Следовательно $|Z(G)| \vdots p$, следовательно $|Z(G)| > 1$. ◊

Следствие. Группа порядка p^2 (p просто) абелева.

Доказательство.

Если $|G| = p^2$, то по теореме $|Z(G)| = p$ или p^2.

1) Пусть $|Z(G)| = p$, тогда $\left|G/Z(G)\right| = \dfrac{|G|}{|Z(G)|} = \dfrac{p^2}{p} = p$. Следовательно $G/Z(G)$ циклическая, т.е. $G/Z(G) = \langle gZ(G) \rangle_p = \{Z(G), gZ(G), \dots, g^{p-1}Z(G)\}$. Пусть $a \in G$, тогда $a = g^i x, \quad x \in Z(G)$ и пусть $b \in G$, тогда $b = g^k y, \quad y \in Z(G)$, т.к. $G = Z(G) \cup gZ(G) \cup \dots \cup g^{p-1}Z(G)$. Имеем, что $ab = g^i x g^k y = g^i g^k xy = g^k g^i xy = g^k g^i yx = g^k y g^i x = ba$ (элементы x и y перестановочны с g и друг с другом, т.к. они центральные). Следовательно G - абелева и $Z(G) = G$, т.е. $|Z(G)| = |G| = p^2$, получили противоречие с тем, что $|Z(G)| = p$.

2) Если $|Z(G)| = p^2$, то $Z(G) = G$, следовательно, группа G абелева. ◊

Лекция 4

Теорема (1-ая теорема Силова). *Пусть G - группа порядка $p^n m$, где p - простое число, тогда в группе G существует подгруппа порядка p^n.*

Доказательство.

Доказательство проведем по индукции по порядку группы.

База индукции.

Если $|G| = p^n$ утверждение очевидно, в качестве подгруппы можно взять саму группу.

Индуктивный переход.

1) Пусть в группе G существует нецентральный элемент, т.е. $\exists x \in G \setminus Z(G)$. Пусть $K(x)$ - класс сопряженных элементов, содержащий x. Т.к. $x \notin Z(G)$, то $|K(x)| > 1$, кроме того $|K(x)| = \dfrac{|G|}{|C(x)|}$, где $C(x)$ - это централизатор элемента x. Мы знаем, что $C(x)$ всегда является подгруппой.

1а) Пусть $(p,|K(x)|)=1$, тогда $p^n \mid |C(x)|$ и $|C(x)|<|G|$. Тогда по предположению индукции (т.к. $|C(x)|=p^n k, \quad k<m$) в $C(x)$, а значит и в $|G|$, есть подгруппа порядка p^n.

1б) Пусть $(p,|K(x)|)\neq 1$, т.е. $p \mid |K(x)| \quad \forall x \in G \setminus Z(G)$. Разобьем группу G на непересекающиеся классы сопряженных элементов. $G=Z(G)\bigcup K(x_1)\bigcup\ldots\bigcup K(x_l)$, $|G|=|Z(G)|+|K(x_1)|+\ldots+|K(x_l)|$. Т.к. $p \mid |G|, \quad p \mid |K(x_i)| \quad \forall i$, то $p \mid |Z(G)|$.

Лемма. *Пусть H - конечная абелева группа и p - простое число, делящее $|H|$, тогда в H есть элемент порядка p.*

Доказательство.

Проведем индукция по порядку H.

База индукции: если $|H|=p$ утверждение очевидно.

Индуктивный переход.

1) Если порядок какого-нибудь элемента делится на p, то пусть $|b|=pq$, тогда $|b^q|=p$.

2) Пусть порядок любого элемента не делится на p. Возьмем произвольный (не единичный) элемент a. Рассмотрим $N=\langle a\rangle$, тогда $\left|H/N\right|=\dfrac{|H|}{|N|}=\dfrac{|H|}{|a|}$ - делится на p. По предположению индукции $\exists xN \in H/N$, т.ч. $|xN|=p$. Рассмотрим $\langle x\rangle$ в G. Пусть $\pi: H \to H/N$ - естественный гомоморфизм $\pi(x)=xN$, тогда $\pi(\langle x\rangle)=\langle xN\rangle$. По теореме о гомоморфизме $\langle xN\rangle \cong \langle x\rangle \big/ \operatorname{Ker}\pi\big|_{\langle x\rangle}$, тогда $p=|xN|=\dfrac{|\langle x\rangle|}{\left|\operatorname{Ker}\pi\big|_{\langle x\rangle}\right|}$. Т.е. p делит $|\langle x\rangle|$. Т.е. порядок x делится на p, что противоречит предположению пункта 2. Лемма доказана. $\Diamond$

Вернемся к доказательству теоремы. Мы имеем, что $p \mid |Z(G)|$, причем $Z(G)$ - абелева группа. По лемме в $Z(G)$ существует элемент a порядка p. Пусть $N=\langle a\rangle$, тогда $|N|=p$ и $N \lhd G$ (т.к. a - центральный элемент). Тогда $\left|G/N\right|=\dfrac{|G|}{|N|}=\dfrac{p^n m}{p}=p^{n-1}m<|G|$. По предположению индукции в G/N есть подгруппа H порядка p^{n-1}. Рассмотрим естественный гомоморфизм $\pi: G \to G/N$, рассмотрим полный прообраз подгруппы H: $U=\pi^{-1}(H)$, т.е. $\pi(U)=H$ и $\operatorname{Ker}\pi\big|_U=N$. По теореме о гомоморфизме $H \cong U/N$ и $|H|=\dfrac{|U|}{|N|} \Rightarrow |U|=|H||N|=p^{n-1}p=p^n$.

2) Если в G нет нецентральных элементов, то $G=Z(G)$, т.е. является абелевой группой. Рассуждая аналогично предыдущему пункту, применив лемму, получим утверждение теоремы. Теорема доказана. $\Diamond$.

Определение. *Пусть G - конечная группа и $|G|=p^n m$, где p - простое число и $(p,m)=1$. Тогда подгруппа в G порядка p^n называется* **силовской p-подгруппой**.

Теорема (2-ая теорема Силова). *Пусть G - конечная группа, p - простое число, делящее порядок группы. Тогда любая p-подгруппа (подгруппа порядка p^i) содержится в некоторой силовской, кроме того любые две силовские подгруппы сопряжены.*

Доказательство.

Пусть Γ - p-подгруппа в G, P - силовская p-подгруппа. Пусть $X=\{gP \mid g\in G\}$. Определим действие: Γ действует на X на правилу: если $u\in\Gamma$, то $u(gP)=ugP$. $|X|=\frac{|G|}{|P|}$ - не делится на p. Орбита $\mathrm{Orb}_{gP}=\{ugP \mid u\in\Gamma\}$. $|\mathrm{Orb}_{gP}|=\frac{|\Gamma|}{|\mathrm{St}_{gP}|}=p^{d(g)}$, где $d(g)$ - некая функция от g. Разобьем X на непересекающиеся орбиты действия Γ. Если все орбиты не одноэлементные, то $p \mid |X|$, что неверно. Следовательно, существует одноэлементная орбита, т.е. существует gP, такой что $\Gamma gP=gP$, что равносильно условию $g^{-1}\Gamma g\subseteq P\Leftrightarrow \Gamma\subseteq gPg^{-1}$, но $P'=gPg^{-1}$ - силовская подгруппа.

Если Γ - силовская, то $\Gamma=gPg^{-1}$, т.к. они имеют одинаковый порядок. Следовательно две силовские подгруппы сопряжены. ◊

Теорема (3-я теорема Силова). *Пусть N_p - число различных силовских p-подгрупп в G. Тогда N_p делит $|G|$ и $N_p\equiv 1 \bmod p$.*

Доказательство.

Пусть S - множество всех силовских p-подгрупп в G, тогда $|S|=N_p$. На S группа G действует сопряжением, т.е. если $p\in S$ и $g\in G$, то $g\cdot P=gPg^{-1}=\{gxg^{-1} \mid x\in P\}$. По 2-ой теореме Силова множество S является орбитой любой силовской p-подгруппы. Т.е. при таком действии существует всего одна орбита и $N_p=|S|=\frac{|G|}{\ldots}$, следовательно, $N_p \mid |G|$.

Пусть $S=\{P_0,P_1,\ldots,P_r\}$, рассмотрим действие P_0 в S сопряжением. S снова разбивается на орбиты, и порядок каждой из них делит $|P_0|$ и потому является степенью числа p. Но $\{P_0\}$ инвариантно относительно этого действия, т.е. $\{P_0\}$ - это одноэлементная орбита. Пусть есть еще какая-нибудь одноэлементная орбита, например, P_1, т.е. $xP_1x^{-1}=P_1 \quad \forall x\in P_0$. Пусть $H=P_0P_1=\{xy \mid x\in P_0 \quad y\in P_1\}$.

Лемма. *Множество H является подгруппой в G и $P_1 \lhd H$.*

Доказательство.

Пусть $x_1,x_2\in P_0$ и $y_1y_2\in P_1$. Тогда

$$(x_1y_1)(x_2y_2)=\underbrace{x_1x_2}_{\in P_0}\underbrace{\left(\overbrace{x_2^{-1}y_1x_2}^{\in P_1}\right)y_2}_{\in P_1}\in H \text{ и}$$

$(xy)^{-1}=y^{-1}x^{-1}=\underbrace{x^{-1}}_{\in P_0}\underbrace{\left(xyx^{-1}\right)}_{\in P_1}\in H$, т.е. H - действительно является подгруппой.

Пусть $z\in P_1$ и $xy\in H$, где $x\in P_0$ и $y\in P_1$, тогда

$(xy)z(xy)^{-1}=x\left(yzy^{-1}\right)x^{-1}\in P_1$, т.е. $P_1\lhd H$. Лемма доказана. ◊

Завершим доказательство теоремы. Рассмотрим эту подгруппу H. Тогда $\left|H/P_1\right|=\frac{|H|}{|P_1|}$, т.е. $|H|=\left|H/P_1\right||P_1|$. Пусть $\pi: H\to H/P_1$ - естественный гомоморфизм. Тогда $\pi(P_0)=\{xP_1 \mid x\in P_0\}$. Но если $h\in H$, то $h=xy$, где $x\in P_0$ и $y\in P_1$, тогда $hP_1=xyP_1=xP_1$, следовательно $\pi(P_o)=H/P_1$. В этом случае

$\left|H/P_1\right|$ делит $\left|P_0\right|$, т.е. $\left|H/P_1\right|$ - степень числа p. Следовательно $\left|H\right| = \left|H/P_1\right| \cdot \left|P_1\right|$ - степень числа p и $\left|H\right| \geq \left|P_1\right|$. Т.к. P_1 - силовская, что $\left|H\right| = \left|P_1\right|$. Но $P_1 \subseteq H \Rightarrow P_1 = H$. Аналогично получаем, что и $P_0 = H$. Но по предположению P_0 и P_1 различны, получили противоречие.

Итак в S только одна одноэлементная орбита (P_0), значит порядок любой другой орбиты делится на p, следовательно, $N_p = \left|S\right| = 1 + pd \equiv 1 \bmod p$. ◊

Приложения теорем Силова.

1) Возьмем группу $GL(n, F_p)$, найдем силовские p-подгруппы. мы знаем, что $\left|GL(n, F_p)\right| = (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1}) = (p^n - 1)p(p^{n-1} - 1)\ldots p^{n-1}(p-1) = p^{1+2+\ldots+n-1} \cdot \ldots$, т.е. $\left|GL(n, F_p)\right| = p^{\frac{n(n-1)}{2}} \cdot \ldots$ и силовская p-подгруппа имеет порядок $p^{\frac{n(n-1)}{2}}$. Одна из силовских подгрупп - это подгруппа $\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, остальные ей сопряжены, т.е. равны $A\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}A^{-1}$.

2) Рассмотрим группу S_3. $\left|S_3\right| = 6 = 2 \cdot 3$. Ее силовские 2-подгруппы (всего их 3): $\{1, (12)\}$, $\{1, (13)\}$, $\{1, (23)\}$. Ее силовская 3-родгруппа (она всего одна): $\{1, (123), (132)\}$.

3) Рассмотрим группу S_4. $\left|S_4\right| = 24 = 2^3 \cdot 3$. Силовских 2-подгрупп всего может быть либо 1, либо 3. Возьмем $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$. Рассмотрим подгруппы $V_4 \bigcup (12)V_4$, $V_4 \bigcup (13)V_4$, $V_4 \bigcup (23)V_4$, … Они все силовские и среди них есть различные, следовательно всего существует три силовские 2-подгруппы. Силовские 3-подгруппы (всего их 4): $\{1, (123), (132)\}$, $\{1, (124), (142)\}$, $\{1, (134), (143)\}$ и $\{1, (234), (243)\}$.

Упражнение. Докажите, что если q - наименьшее простое число, делящее $\left|G\right|$ и H - подгруппа индекса q (существует всего q различных смежных классов G по H), то $H \lhd G$.

Лекция 5

В качестве еще одного приложения теорем Силова, решим следующую задачу:

Теорема. Пусть $p < q$ - простые числа и p не делит $q - 1$. Тогда группа порядка pq является циклической.

Доказательство.

В нашей группе существуют силовская p-подгруппа порядка p и силовская q-подгруппа порядка q. Т.к. p и q - простые числа, то они циклические, пусть это подгруппы $\langle a\rangle_p$ и $\langle b\rangle_q$. Число N_q силовских q-подгрупп делит pq и $N_q \equiv 1 \bmod q$, следовательно N_q равно либо 1, либо p. Имеем, что $N_q = 1 + qk$, где $k \geq 0$, если $k > 0$, то $N_q > q > p$, следовательно $k = 0$ и $N_q = 1$, т.е. существует всего одно силовская q-подгруппа.

Если $x \in G$, то $x\langle b\rangle_q x^{-1}$ - снова силовская подгруппа, но она у нас единственна, следовательно $x\langle b\rangle_q x^{-1} = \langle b\rangle_q$, т.е. эта подгруппа нормальна. Пусть $aba^{-1} = b^t$, где $0 \leq t \leq q - 1$. Тогда:

$$a^2ba^{-2} = a(aba^{-1})a^{-1} = ab^t a^{-1} = b^{t^2}$$

$$\ldots$$

$$a^p ba^{-p} = b^{t^p} = b \Rightarrow b^{t^p - 1} = 1.$$

Следовательно, $q\,|\left(t^{p}-1\right)$. $t\in Z_q$ и в мультипликативной группе Z_q^* элемент t имеет порядок делящий p, т.к. $t^p=1$. Но $\left|Z_q^*\right|=q-1$. Если t имеет порядок p, то $p\,|\,q-1$, что неверно по условию, следовательно, $|t|=1$,т.е. $t=1$. Но тогда будем иметь, что $aba^{-1}=b\Leftrightarrow ab=ba$.

Покажем, что $|ab|=pq$. Пусть $(ab)^k=1\Leftrightarrow a^kb^k=1\Rightarrow a^{pk}b^{pk}=1\Rightarrow b^{pk}=1$, т.е. $q\,|\,pk$. Т.к. $(q,p)=1$, то $q\,|\,pk\Rightarrow q\,|\,k$. Аналогично получаем, что и $p\,|\,k$ и, опять используя $(q,p)=1$, получаем $pq\,|\,k$. Минимальное ненулевое такое k - это pq, следовательно $|ab|=pq$ и наша группа равна $\langle ab\rangle_{pq}$, т.е. является циклической. ◊

Следствие. Группа порядка 15 циклическая.

ПРОСТЫЕ ГРУППЫ

Определение. *Неабелевая группа называется простой, если в ней всего две нормальные подгруппы - единичная и сама группа.*

Приведем несколько примеров простых групп:

Теорема. *Группы A_n при $n\geq 5$ простые.*

(группа $A_3=\langle(123)\rangle_3$ абелева, следовательно не простая; группа A_4 содержит нормальную подгруппу V_4, следовательно не простая).

Доказательство.

Лемма 1. *Подгруппа A_n порождается тройными циклами.*

Доказательство.

Мы знаем, что каждая подстановка есть произведение циклов длины 2 (транспозиций). Т.к. подстановки в A_n четны, то они равны произведению четного числа транспозиций. Рассмотрим произведение двух транспозиций:

$(ij)(kl)=(ijk)(jkl)$, если i,j,k,l различны,

$(ij)(jk)=(ijk)$, если i,j,k различны,

$(ij)(ij)=1$.

Т.е. сгруппировав транспозиции по две, мы получим произведение циклов длины 3. ◊

Пусть в A_n существует нормальная подгруппа $N\triangleleft A_n$, причем $N\neq\{1\}$.

Лемма 2. *Если N содержит тройной цикл ($(ijk)\in N$), то $N=A_n$.*

Доказательство.

Возьмем произвольный тройной цикл (abc), возьмем $\sigma=\begin{pmatrix} i & j & k & u & v & \dots \\ a & b & c & u' & v' & \dots \end{pmatrix}$, такую что $(u',v')=(u,v)$ или $(u',v')=(u,v)$, далее все элементы переходят в себя. Одна из таких подстановок будет четной, выберем ее. Получим $\sigma(ijk)\sigma^{-1}=(abc)\in N$, т.к. $N\triangleleft A_n$. Следовательно подгруппе N принадлежат все тройные циклы, следовательно (по лемме 1), $N=A_n$. ◊

Лемма 3. *Если N содержит подстановку σ, у которой в разложении на независимые циклы встречается цикл длины ≥ 4, то $N=A_n$.*

Доказательство.

Пусть $\sigma=(ijkl\dots)\dots$, тогда $\tau=\underbrace{(ijk)\sigma(ijk)^{-1}}_{\in N}\underbrace{\sigma^{-1}}_{\in N}=(ijl)\in N$. Т.е. N содержит цикл длины 3, следовательно (по лемме 2), $N=A_n$. ◊

Лемма 4. *Если* N *содержит подстановку* σ, *у которой в разложении на независимые циклы содержится хотя бы два цикла длины 3, то* $N = A_n$.

Доказательство.

Пусть $\sigma = (ijk)(abc)\ldots$, тогда $\tau = \underbrace{(kab)\sigma(kab)^{-1}}_{\in N}\underbrace{\sigma^{-1}}_{\in N} = (ickab) \in N$. Т.е. N содержит цикл длины 5, следовательно (по лемме 3), $N = A_n$. ◊

Лемма 5. *Если* N *содержит подстановку* σ, *у которой в разложении на независимые циклы содержится один цикл длины 3 и циклы длины 2, то* $N = A_n$.

Доказательство.

Пусть $\sigma = (ijk)(ab)\ldots$, тогда $\sigma^2 = (ikj) \in N$, следовательно (по лемме 2), $N = A_n$. ◊

Лемма 6. *Если* N *содержит подстановку* σ, *у которой в разложении на независимые циклы содержатся только циклы длины 2, то* $N = A_n$.

Доказательство.

Если $\sigma = (ij)(ab)$, то, т.к. у нас не менее пяти символов, $\exists c \notin \{i, j, a, b\}$. Тогда $\tau = (ijc)\sigma(ijc)^{-1}\sigma^{-1} = (icj) \in N$, следовательно (по лемме 2), $N = A_n$.

Если $\sigma = (ij)(ab)(uv)(pq)\ldots$, то $(ja)(bu)\sigma(bu)(ja)\sigma^{-1} = (iub)(jav) \in N$, следовательно (по лемме 4), $N = A_n$.

Теперь, собственно, докажем теорему. Возьмем произвольную $\sigma \in N \setminus \{1\}$. Она удовлетворяет условию одной из наших лемм, следовательно $N = A_n$. Теорема доказана. ◊

Приведем еще один пример простой группы: группа $SO(3, R)$ - ортогональных симметричных матриц.

Определение. Коммутатором $[x, y]$ *элементов* x, y *из группы* G *называется элемент* $[x, y] = xyx^{-1}y^{-1}$.

Упражнение. $[x, y] = 1 \Leftrightarrow xy = yx$.

Предложение. В S_n имеем $[(ij),(jk)] = (ikj)$, если i, j, k различны.

Доказательство.

$(ij)(jk)(ij)^{-1}(jk)^{-1} = (ikj)$. ◊

Предложение. В группе $GL(n,k)$ имеем $[E + \alpha E_{ij}, E + \beta E_{jk}] = E + \alpha\beta E_{ik}$, если i, j, k различны.

Доказательство.

$$(E + \alpha E_{ij})(E + \beta E_{jk})(E - \alpha E_{ij})(E - \beta E_{jk}) = \left(E + \alpha E_{ij} + \beta E_{jk} + \alpha\beta \underbrace{E_{ij} E_{jk}}_{= E_{ik}} \right)(E - \alpha E_{ij} - \beta E_{jk} + \alpha\beta E_{ik}) =$$

$$= E + \alpha E_{ij} + \beta E_{jk} + \alpha\beta E_{ik} - \alpha E_{ij} - \beta E_{jk} - \alpha\beta E_{ik} + \alpha\beta E_{ik} = E + \alpha\beta E_{ik}$$

◊

Определение. Коммутант *группы -* G' *(или* $[G,G]$*) - это множество всех произведений коммутаторов.*

Предложение. $G' \triangleleft G$.

Доказательство.

Пусть $u = [x_1, y_1]\ldots[x_k, y_k]$ и $v = [t_1, z_1]\ldots[t_n, z_n]$, тогда $uv = [x_1, y_1]\ldots[x_k, y_k][t_1, z_1]\ldots[t_n, z_n] \in G'$. И, т.к. $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$, то $u^{-1} = [x_1, y_1]^{-1}\ldots[x_k, y_k]^{-1} = [y_k, x_k]\ldots[y_1, x_1] \in G'$. Следовательно G' - это подгруппа, докажем теперь ее нормальность.

Пусть $z \in G$, тогда $zuz^{-1} = z[x_1, y_1]z^{-1} \cdot z[x_2, y_2]z^{-1} \cdot \ldots \cdot z[x_k, y_k]z^{-1}$.
$z[x, y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = (zxz^{-1})(zyz^{-1})(zxz^{-1})^{-1}(zyz^{-1})^{-1} = [zxz^{-1}, zyz^{-1}]$ - снова коммутатор, следовательно zuz^{-1} равно произведению коммутаторов, т.е. $G' \lhd G$. ◊

Теорема.

1) $S_n' = A_n$ *при* $n \geq 3$ *и* $A_n' = A_n$ *при* $n \geq 5$.

2) $GL(n, k)' = SL(n, k) = SL(n, k)'$ *при* $n \geq 3$.

Доказательство.

1) $G = S_n$, $[x, y] = xyx^{-1}y^{-1}$ - четная подстановка, следовательно, $S_n' \subseteq A_n$. Более того мы доказали ранее, что $(ikj) = [(ij), (jk)]$ и что любая четная подстановка является произведением тройных циклов, т.е. произведением коммутаторов. Следовательно $S_n' = A_n$.

Имеем, что $A_n' \lhd A_n$, следовательно A_n' либо единичная, либо совпадает с A_n. Но A_n - это неабелевая группа, следовательно $A_n' \neq \{1\}$, следовательно $A_n' = A_n$.

2) $G = GL(n, k)$, $[A, B] = ABA^{-1}B^{-1}$ имеет определитель равный единице, следовательно $GL(n, k)' \subseteq SL(n, k)$. Более того мы знаем, что $H = \prod\limits_{i \neq j}(E + \alpha E_{ij}) = \prod\limits_{i \neq j}[E + E_{ik}, E + \alpha E_{kj}]$, если $H \in SL(n, k)$. Следовательно $GL(n, k)' = SL(n, k)$. Из этого же соображения получаем, что $SL(n, k)' = SL(n, k)$. ◊

Упражнение. Докажите, что $A_4' = V_4$.

Лекция 6

Предложение. Пусть $N \lhd G$, тогда следующие условия эквивалентны:

1) G/N - абелева;

2) $G' \subseteq N$.

Доказательство.

Напишем цепочку эквивалентных утверждений: G/N - абелева $\Leftrightarrow [xN, yN] = N \Leftrightarrow$
$\Leftrightarrow (xN)(yN)(x^{-1}N)(y^{-1}N) = N \Leftrightarrow xyx^{-1}y^{-1}N = N \Leftrightarrow [x, y]N = N \Leftrightarrow [x, y] \in N \Leftrightarrow G' \subseteq N$. ◊

РАЗРЕШИМЫЕ ГРУППЫ

Определение. *Пусть* G *- группа. Положим* $G^{(0)} = G, G^{(1)} = G', G^{(k+1)} = [G^{(k)}, G^{(k)}]$. *Группа* G *называется* **разрешимой***, если* $\exists k \geq 1 : G^{(k)} = 1$.

Примеры:

1) абелевые группы разрешимы, т.е. $G^{(1)} = G' = 1$.

2) $G = S_4, G' = A_4, (G')' = V_4, ((G')')' = 1$, т.к. $|V_4| = 4 = 2^2$, следовательно, V_4 - абелевая группа. Следовательно, $S_4^{(3)} = 1$ и S_4 разрешима.

3) При $n \geq 5$ мы знаем, что $S_n' = A_n = A_n'$. Следовательно, $S_n^{(k)} = A_n$ для любого $k \geq 1$, и группа S_n неразрешима.

Предложение. Пусть $f : G \to H$ - гомоморфизм групп. Тогда $f\left(G^{(k)}\right) \subseteq H^{(k)}$ и, если f - сюръективно, то $f\left(G^{(k)}\right) = H^{(k)}$.

Доказательство. (по индукции по k)

База индукции. $k = 0$, оба утверждения верны.

1) Пусть для $k-1$ утверждение верно, докажем его для k. $G^{(k)} = \left[G^{(k-1)}, G^{(k-1)}\right]$. Если $x \in G^{(k)}$, то $x = [x_1, y_1] \cdot \ldots \cdot [x_m, y_m]$, где $x_i, y_i \in G^{(k-1)}$, тогда $f(x) = [f(x_1), f(y_1)] \cdot \ldots \cdot [f(x_m), f(y_m)] \in H^{(k)}$, т.к. по предположению индукции $f(x_i), f(y_i) \in H^{(k-1)}$.

2) Аналогично, пусть для $k-1$ утверждение верно, докажем его для k. Нам надо доказать, что для любого элемента $h \in H^{(k)}$ найдется $x \in G^{(k)}$, такой что $h = f(x)$. Имеем, что $h = [h_1, g_1] \cdot \ldots \cdot [h_n, g_n]$, где $h_i, g_i \in H^{(k-1)}$, по предположению индукции $h_i = f(x_i), g_i = f(y_i)$, где $x_i, y_i \in G^{(k-1)}$. Но тогда $h = f\left(\underbrace{[x_1, y_1] \cdot \ldots \cdot [x_n, y_n]}_{\in G^{(k)}}\right)$, следовательно, $G^{(k)} = H^{(k)}$. ◊

Предложение. $G^{(k)} \lhd G \ \forall k$.

Доказательство. (по индукции по k)

База индукции. $k = 0$, утверждение верно.

Пусть утверждение верно для $k-1$, докажем его для k. Возьмем произвольный $x \in G^{(k)}$, тогда $x = [x_1, y_1] \cdot \ldots \cdot [x_m, y_m]$, где $x_i, y_i \in G^{(k-1)}$. Пусть $z \in G$, тогда $zxz^{-1} = \left[zx_1z^{-1}, zy_1z^{-1}\right] \cdot \ldots \cdot \left[zx_mz^{-1}, zy_mz^{-1}\right] \in G^{(k)}$, т.к. по предположению индукции $zx_iz^{-1}, zy_iz^{-1} \in G^{(k-1)}$. Следовательно, $G^{(k)} \lhd G$. ◊

Упражнение. Пусть H - подгруппа в G. Если G - разрешима, то H тоже разрешима.

Предложение. Если $N \lhd G$, то следующие два утверждения эквивалентны:

1) G разрешима;

2) N и G/N разрешимы.

Доказательство.

$1) \Rightarrow 2)$.

В силу предыдущего упражнения N будет разрешима. Рассмотрим естественный гомоморфизм $\pi : G \to G/N$, $\pi(g) = gN$. Этот гомоморфизм всегда сюръективен, следовательно $\forall k$ имеем, что $\pi\left(G^{(k)}\right) = \left(G/N\right)^{(k)}$. Т.к. G - разрешима, то $\exists M > 0$, такое что $G^{(M)} = 1$, следовательно $\left(G/N\right)^{(M)} = \pi\left(G^{(M)}\right) =$ $= \pi(1) = 1 \cdot N$, следовательно G/N разрешима.

$2) \Rightarrow 1)$.

Пусть $N^{(T)} = 1$ и $\left(G/N\right)^{(R)} = 1$. Тогда $\pi\left(G^{(R)}\right) = \left(G/N\right)^{(R)} = 1 \cdot N$, следовательно, $G^{(R)} \subseteq \operatorname{Ker}\pi = N$. Следовательно, $G^{(R+T)}\left(G^{(R)}\right)^{(T)} \subseteq N^{(T)} = 1$, т.е. G разрешима. ◊

Теорема. *Пусть G - группа. Следующие утверждения эквивалентны:*

1) G - разрешима;

2) существует ряд нормальных подгрупп $G = G_0 \supset G_1 \supset \ldots \supset G_k = 1$, $G_i \lhd G$, такой, что G_i/G_{i+1} - абелева.

Доказательство.

$1) \Rightarrow 2)$.

Положим $G_i = G^{(i)}$, тогда $G_i \lhd G$ и $G_i/G_{i+1} = G^{(i)}/\left[G^{(i)}, G^{(i)}\right]$ - абелева, т.к. фактор группа по коммутанту всегда абелева.

$2) \Rightarrow 1)$ (по индукции по k).

База индукции, $k=1$. Тогда $G_1=1$ и $G=G/1$ - абелева, следовательно, разрешима.

Пусть утверждение верно для $k-1$, докажем его для k. В группе G_1 есть ряд длины $k-1$, следовательно, по предположению индукции G_1 разрешима. Более того, $G_1 \triangleleft G$ и G/G_1 - абелева (разрешима), следовательно и G - разрешима. ◊

Теорема. *Конечная p-группа разрешима.*

Доказательство. (индукция по порядку группы).

База индукции, $|G|=p$, следовательно G - абелева и разрешима.

Пусть утверждение верно для $|G|=p^{m-1}$, докажем его для $|G|=p^m$. Рассмотрим центр $Z(G)$, мы знаем, что $Z(G)\triangleleft G$, $Z(G)$ - абелева (разрешима) и $Z(G)\neq 1$, т.е. $\left|G/Z(G)\right|<|G|\le p^{m-1}$ (разрешима по предположению индукции), следовательно и G разрешима. ◊

Рассмотрим множество $T(n,k)=\left\{\begin{pmatrix}\alpha_1 & & * \\ & \ddots & \\ 0 & & \alpha_n\end{pmatrix} \mid \alpha_i \neq 0\right\}$ - множество верхнетреугольных матриц размера $n\times n$ с ненулевыми числами поля k на диагонали. Рассмотрим еще множество $UT(n,k)=\left\{\begin{pmatrix}1 & & * \\ & \ddots & \\ 0 & & 1\end{pmatrix}\right\}$ - подмножество в $T(n,k)$ с единицами на диагонали.

Упражнение. Докажите, что $T(n,k)$ - группа по умножению матриц, а $UT(n,k)$ подгруппа в ней.

Предложение. $T(n,k)' \subseteq UT(n,k)$ и $UT(n,k)\triangleleft T(n,k)$.

Доказательство.

Рассмотрим отображение $\psi : T(n,k)\to\{(\beta_1,\ldots,\beta_n)\mid \beta_i\in k^*\}=G$, отображение в G - множество наборов из n ненулевых чисел поля k. Это отображение действует по правилу $\psi\begin{pmatrix}\alpha_1 & & * \\ & \ddots & \\ 0 & & \alpha_n\end{pmatrix}=(\alpha_1,\ldots,\alpha_n)$.

Введем операцию умножения в множестве G: $(\alpha_1,\ldots,\alpha_n)(\beta_1,\ldots,\beta_n)=(\alpha_1\beta_1,\ldots,\alpha_n\beta_n)$. Теперь G - это абелевая группа и ψ - гомоморфизм групп, причем $\operatorname{Ker}\psi=UT(n,k)$, следовательно $UT(n,k)\triangleleft T(n,k)$. Следовательно $\operatorname{Im}\psi$ - это абелевая группа, изоморфная $T(n,k)/UT(n,k)$, т.е. $T(n,k)/UT(n,k)$ - абелева. Рассмотрим естественный гомоморфизм $\pi : T(n,k)\to T(n,k)/UT(n,k)$, тогда $\pi\left(T(n,k)'\right)=\left(T(n,k)/UT(n,k)\right)'=1$. Следовательно, $T(n,k)'\subseteq \operatorname{Ker}\pi=UT(n,k)$. ◊

Теорема. *Группа $T(n,k)$ всегда разрешима.*

Доказательство.

Для доказательства теоремы, нам достаточно доказать разрешимость группы $UT(n,k)$ и воспользоваться предыдущим предложением. Докажем это по индукции по n.

База индукции, $n=1$. $UT(n,k)=\{(1)\}$ - разрешима.

Пусть утверждение верно для $n-1$, докажем его для n. Рассмотрим отображение $\phi : UT(n,k)\to UT(n-1,k)$, определенное по следующему правилу: пусть $x=\left(\begin{array}{ccc:c}1 & & * & * \\ & \ddots & & \vdots \\ 0 & & 1 & * \\ \hdashline 0 & \ldots & 0 & 1\end{array}\right)=\left(\begin{array}{c:c} & * \\ A & \vdots \\ & * \\ \hdashline 0 \ \ldots \ 0 & 1\end{array}\right)$, тогда $\phi(x)=A$. Если $x\in UT(n,k)$, то $\phi(x)=A\in UT(n-1,k)$.

Лемма. ϕ *- гомоморфизм групп.*

Доказательство.

$$\phi\left[\left(\begin{array}{c:c} A & a \\ \hdashline 0 & 1 \end{array}\right)\left(\begin{array}{c:c} B & b \\ \hdashline 0 & 1 \end{array}\right)\right] = \phi\left(\begin{array}{c:c} AB & c \\ \hdashline 0 & 1 \end{array}\right) = AB = \phi\left(\begin{array}{c:c} A & a \\ \hdashline 0 & 1 \end{array}\right)\phi\left(\begin{array}{c:c} B & b \\ \hdashline 0 & 1 \end{array}\right). \ \lozenge$$

Рассмотрим $\operatorname{Ker}\phi = \left\{\left(\begin{array}{c:c} E_{n-1} & * \\ \hdashline 0 & 1 \end{array}\right)\right\}$, т.к. $\left(\begin{array}{c:c} E_{n-1} & a \\ \hdashline 0 & 1 \end{array}\right)\left(\begin{array}{c:c} E_{n-1} & b \\ \hdashline 0 & 1 \end{array}\right) = \left(\begin{array}{c:c} E_{n-1} & a+b \\ \hdashline 0 & 1 \end{array}\right)$, то $\operatorname{Ker}\phi$ - абелева группа (разрешима). Кроме того $UT(n,k)/\operatorname{Ker}\phi \cong UT(n-1,k)$ - по предположению индукции разрешима. Следовательно $UT(n,k)$ разрешима и $T(n,k)$ разрешима. ◊

ПРЯМЫЕ ПРОИЗВЕДЕНИЯ ГРУПП

Определение. *Пусть G - группа и $G_1,\dots,G_n$ ее нормальные подгруппы. Тогда G является* **прямым** *(***внутренним***)* **произведением** *групп $G_1,\dots,G_n$, если каждый элемент группы G имеет и притом единственное представление $g = g_1\cdot\ldots\cdot g_n$, где $g_i \in G_i$. Обозначается $G = G_1\times\ldots\times G_n$ (если операция в группе - сложение, то обозначается $G = G_1\oplus\ldots\oplus G_n$ - прямая сумма).*

Упражнение. Докажите, что $|G| = |G_1|\cdot\ldots\cdot|G_n|$.

Предложение. Если $G = G_1\times\ldots\times G_n$ и $g_i \in G_i$, $g_j \in G_j$, $i \neq j$, то $g_i g_j = g_j g_i$.

Доказательство.

Рассмотрим коммутатор $g = [g_i, g_j] = \underbrace{g_i g_j g_i^{-1}}_{\in G_j} g_j^{-1} \in G_j$, аналогично $g \in G_i$. Следовательно, $g = 1\cdot\ldots\cdot 1\cdot \underset{i}{g}\cdot 1\cdot\ldots\cdot 1 = 1\cdot\ldots\cdot 1\cdot \underset{j}{g}\cdot 1\cdot\ldots\cdot 1$, в силу единственности разложения имеем, что $g = 1$, т.е. $g_i g_j = g_j g_i$.

◊

Следствие. Пусть $g = g_1\cdot\ldots\cdot g_n = G = G_1\times\ldots\times G_n$, $h = h_1\cdot\ldots\cdot h_n \in G$, тогда $gh = (g_1 h_1)\cdot\ldots\cdot(g_n h_n)$ и $g^{-1} = g_1^{-1}\cdot\ldots\cdot g_n^{-1}$.

Доказательство.

$gh = (g_1\ldots g_n)(h_1\ldots h_n) = g_1\ldots g_n h_1\ldots h_n = g_1 h_1 g_2\ldots g_n h_2\ldots h_n = \ldots = g_1 h_1\ldots g_n h_n$, здесь элемент h_i перестановочен с элементами g_j и h_j при $j \neq i$ по предложению.

Имеем $(g_1\ldots g_n)(g_1^{-1}\ldots g_n^{-1}) = (g_1^{-1}\ldots g_n^{-1})(g_1\ldots g_n) = 1 \Rightarrow g^{-1} = (g_1^{-1}\ldots g_n^{-1})$. ◊

Пример.

$C^* = U\times R^+$, где U - окружность единичного радиуса, R^+ - положительные вещественные числа. Т.е. любое число $z \in C^*$ представимо и притом однозначно в виде $z = e^{i\phi}|z|$.

Лекция 7

Теорема. *Группа $(Z,+)$ не представима в виде прямой суммы.*

Доказательство. (от противного)

Допустим, что $Z = A\oplus B$, где $A,B \neq \{0\}$, тогда $A\cap B = \{0\}$. Возьмем $n \in A$ и $m \in B$, $n,m > 0$. Рассмотрим элемент nm, он $nm = \underbrace{n+\ldots+n}_{m} \in A$ и $nm = \underbrace{m+\ldots m}_{n} \in B$. Получили, что $nm \in A\cap B$ и $nm \neq 0$ - противоречие с $A\cap B = \{0\}$. ◊

Теорема. *Пусть $G = G_1\times\ldots\times G_n$ и $g \in G$, $g = g_1\cdot\ldots\cdot g_n$, где $g_i \in G_i$. Тогда $|g| = \text{НОК}(|g_1|,\ldots,|g_n|)$.*

Доказательство.

Имеем $g^m = 1 \Leftrightarrow (g_1\cdot\ldots\cdot g_n)^m = 1 \Leftrightarrow g_1^m\cdot\ldots\cdot g_n^m = 1 \Leftrightarrow g_1^m = \ldots = g_n^m = 1$. Следовательно, $m \vdots |g_1|,\ldots,m \vdots |g_n|$, т.е. m - это общее кратное порядков элементов $g_1,\ldots,g_n$. Значит минимальное такое m - НОК порядков. ◊

Посмотрим, как раскладываются в прямые суммы конечные циклические группы (только что мы доказали, что бесконечные циклические группы не раскладывается, т.к. они изоморфны Z).

Теорема. *Если G - конечная группа и $G = G_1 \times \ldots \times G_n$, то следующие условия эквивалентны:*

1) G - циклическая;

2) $G_1, \ldots, G_n$ - циклические и их порядки $|G_1|, \ldots, |G_n|$ взаимно просты.

Доказательство.

$1) \Rightarrow 2)$. G_i - являются подгруппами в G, следовательно, они циклические. Возьмем произвольный $g = g_1 \cdot \ldots \cdot g_n$, $g \in G$, $g_i \in G_i$. Пусть порядки $|G_1|, \ldots, |G_n|$ не взаимно просты, тогда $M = \text{НОК}(|G_1|, \ldots, |G_n|) < |G_1| \cdot \ldots \cdot |G_n|$. Тогда $g^M = g_1^M \cdot \ldots \cdot g_n^M$, по следствию из теоремы Лагранжа $g_i^M = 1$, т.к. $M \,\vdots\, |G_i| \,\vdots\, g_i$. Следовательно, порядок каждого элемента $|g| \le M < |G_1| \cdot \ldots \cdot |G_n| = |G|$, т.е. группа G не циклическая. Получили противоречие с тем, что порядки $|G_1|, \ldots, |G_n|$ не взаимно просты.

$2) \Rightarrow 1)$. Имеем, что $G_i = \langle a_i \rangle_{n_i}$ и $(n_i, n_j) = 1$ при $i \ne j$. Возьмем элемент $a = a_1 \cdot \ldots \cdot a_n \in G$, тогда $|a| = \text{НОК}(|a_1|, \ldots, |a_n|) = \text{НОК}(n_1, \ldots, n_n) = n_1 \cdot \ldots \cdot n_n = |G|$, следовательно $G = \langle a \rangle$. ◊

Следствие 1. Пусть p - простое число. Циклическая группа порядка p^m не разложима.

Следствие 2. Если $G = \langle a \rangle_n$ и $n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$, тогда $G = \langle a_i \rangle_{p_1^{m_1}} \times \ldots \times \langle a_k \rangle_{p_k^{m_k}}$.

Доказательство.

Группа $\langle a_i \rangle_{p_1^{m_1}} \times \ldots \times \langle a_k \rangle_{p_k^{m_k}}$ состоит из элементов группы G и ее порядок равен порядок равен $|G|$. ◊

ВНЕШНЕЕ ПРОИЗВЕДЕНИЕ

Определение. *Пусть заданы группы $G_1, \ldots, G_n$. Пусть $G = G_1 \times \ldots \times G_n$, т.е. $G = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$ с операцией $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$. Множество G с этой операцией называется* **внешним произведением групп** $G_1, \ldots, G_n$.

Теорема. *G - группа.*

Доказательство.

Единичный элемент - $e = (1, \ldots, 1)$, обратный элемент $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$. ◊

Рассмотрим множества $\overline{G_i} = \{(1, \ldots, 1, \underset{i}{x}, 1, \ldots, 1) \mid x \in G_i\}$.

Упражнение. Докажите, что $\overline{G_i} \lhd G$, отображение $x \to (1, \ldots, 1, x, 1, \ldots, 1)$ задает изоморфизм G_i и $\overline{G_i}$ и $G = \overline{G_1} \times \ldots \times \overline{G_n}$ - прямое произведение. Таким образом прямые и внешние произведения можно отождествлять.

Теорема (факторизация по множителям). *Пусть $G = G_1 \times \ldots \times G_m$, $N_i \lhd G_i$ и пусть $N = N_1 \times \ldots \times N_m$, тогда $N \lhd G$ и $G/N \cong G_1/N_1 \times \ldots \times G_m/N_m$.*

Доказательство.

Рассмотрим отображение $\pi : G \to G_1/N_1 \times \ldots \times G_m/N_m$, если $g = g_1 \cdot \ldots \cdot g_m \in G$, то $\pi(g) = (g_1 N_1, \ldots, g_m N_m) \in G_1/N_1 \times \ldots \times G_m/N_m$. Пусть $h = h_1 \cdot \ldots \cdot h_m \in G$, тогда $gh = g_1 h_1 \cdot \ldots \cdot g_m h_m$ и $\pi(gh) = (g_1 h_1 N_1, \ldots, g_m h_m N_m) = ((g_1 N_1)(h_1 N_1), \ldots, (g_m N_m)(h_m N_m)) = \pi(g)\pi(h)$, следовательно π - это гомоморфизм, причем сюръективный, т.к. $(g_1 N_1, \ldots, g_m N_m) = \pi(g_1 \cdot \ldots \cdot g_m)$. Ядро этого гомоморфизма - это $\operatorname{Ker}\pi = \{g = g_1 \cdot \ldots \cdot g_m \mid (g_1 N_1, \ldots, g_m N_m) = (N_1, \ldots, N_m)\}$, т.е. $\forall i\ g_i N_i = N_i \Leftrightarrow g_i \in N_i$. Следовательно, $\operatorname{Ker}\pi = N$ и по теореме о гомоморфизме $G/N \cong G_1/N_1 \times \ldots \times G_m/N_m$. ◊

Упражнение. Докажите, что циклические группы порядка n изоморфны U_n, бесконечные циклические группы изоморфны $(Z, +)$, кроме того $Z/n \cong U_n$.

КОНЕЧНО-ПОРОЖДЕННЫЕ ГРУППЫ, СВОБОДНЫЕ ГРУППЫ

Определение. *Абелевая группа A называется* **конечно-порожденной**, *если $\exists m_1,\dots,m_n \in A$, такие что $\forall a \in A\ a = k_1 m_1 + \ldots + k_n m_m$, где $k_i \in Z$.*

Упражнение. Доказать, что $(Q,+)$ не конечно-порожденная.

Определение. *Абелевая группа A называется* **свободной**, *если в ней есть базис, т.е. такой набор элементов $e = (e_1,\dots,e_n)$, что $\forall a \in A\ \exists! k_i \in Z : a = k_1 e_1 + \ldots + k_n e_n$.*

Теорема. *Абелевая группа A свободна тогда и только тогда, когда $A \cong Z \oplus \ldots \oplus Z$.*

Доказательство.

$\Rightarrow$. Пусть $e = (e_1,\dots,e_n)$ - базис A, тогда если $a \in A$, то $a = k_1 e_1 + \ldots + k_n e_n$, $k_i \in Z$. Возьмем отображение $\psi : A \to Z \oplus \ldots \oplus Z$ по правилу $\psi(a) = (k_1,\dots,k_n)$. ψ - это изоморфизм, следовательно $A \cong Z \oplus \ldots \oplus Z$.

$\Leftarrow$. Пусть $A \cong \underbrace{Z \oplus \ldots \oplus Z}_{n}$. Предъявим базис в A: $e_1 = (1,0,\dots,0), e_2 = (0,1,0,\dots,0),\dots, e_n = (0,\dots,0,1)$, тогда $a = (k_1,\dots,k_n) = k_1 e_1 + \ldots + k_n e_n$. ◊

Определение. Ранг *свободной абелевой группы равен числу векторов в базисе.*

Теорема. *Ранг свободной абелевой группы определен однозначно.*

Доказательство.

Мы докажем эту теорему немного необычным, но красивым способом.

Пусть A имеем базис $e = (e_1,\dots,e_n)$, рассмотрим группу $Z/2 = \{0,1\}$. Пусть $f : A \to Z/2$ - гомоморфизм. Если $a = k_1 e_1 + \ldots + k_n e_n$, то $f(a) = k_1 f(e_1) + \ldots + k_n f(e_n)$. Таким образом f однозначно задается значениями на базисных элементах: $f(e_1),\dots,f(e_n)$. Следовательно всего различных гомоморфизмов будет $2^n = |\mathrm{Hom}(A, Z/2)|$. Пусть в A есть базис из m элементов, тогда $2^n = |\mathrm{Hom}(A, Z/2)| = 2^m \Leftrightarrow n = m$. ◊

Теорема. *Пусть A - свободная абелевая группа ранга n и B - подгруппа в A. Тогда B - свободная абелевая группа ранга $\le n$.*

Примечание. В подобной теореме о размерности линейных пространств из совпадения размерностей. следовало совпадение подгруппы с самой группой, однако здесь это не верно. Пример: группа Z и подгруппа $2Z$ имеют ранг 1.

Доказательство. (по индукции)

$n = 1$, имеем, что $A \cong Z$ и утверждение теоремы выполнены, т.к. любая бесконечная подгруппа Z является изоморфной Z, т.е. свободной абелевой ранга 1.

Пусть для $n-1$ теорема доказана. Докажем ее для n. Пусть $e = (e_1,\dots,e_n)$ - базис в A. Рассмотрим множество $H = \left\{ \sum_{i=1}^{n-1} k_i e_i \mid k_i \in Z \right\}$ - линейная оболочка первых $n-1$ базисных элементов (является свободной абелевой группой с базисом $(e_1,\dots,e_{n-1})$. Рассмотрим отображение $\pi : A \to Z$ такое, что если $a = k_1 e_1 + \ldots k_n e_n$, то $\pi(a) = k_n$. Тогда π - это эпиморфизм и $\mathrm{Ker}\,\pi = H$. $\pi(B)$ - это подгруппа в Z.

Если $\pi(B) = \{0\}$, то $B \subseteq H$ и (по предположению индукции) B - свободная абелевая группа ранга $\le n-1 \le n$.

Если $\pi(B) \ne \{0\}$, то $\pi(B) = dZ$. $B \bigcap H$ - свободная подгруппа в H с базисом $f_1,\dots,f_s$, $s \le n-1$ (по предположению индукции), следовательно $B \bigcap H$ - свободная подгруппа в B. $\exists$ элемент $f_{s+1} \in B$, такой что $\pi(f_{s+1}) = d$. Покажем, что $f_1,\dots,f_{s+1}$ - базис в B, $s+1 \le n$.

Пусть $b \in B$, тогда $\pi(b) = dt$, $t \in Z$, тогда $\pi(b - tf_{s+1}) = 0$, следовательно, $b - tf_{s+1} \in B \bigcap H$. Т.е. $b - tf_{s+1} = c_1 f_1 + \ldots + c_s f_s$ и $b = c_1 f_1 + \ldots + c_s f_s + tf_{s+1}$. Существование представления мы доказали, осталось доказать его единственность, для этого достаточно доказать, что из $\lambda_1 f_1 + \ldots + \lambda_{s+1} f_{s+1} = 0$ следует, что все $\lambda_i = 0$. Имеем $\pi(\lambda_1 f_1 + \ldots + \lambda_{s+1} f_{s+1}) = \lambda_{s+1} d = 0 \Rightarrow \lambda_{s+1} = 0$ и от нашего равенства остается $\lambda_1 f_1 + \ldots + \lambda_s f_s = 0$. Следовательно, т.к. $f_1,\dots,f_s$ - базис в $B \bigcap H$ и все остальные коэффициенты λ_i равны нулю. ◊

Лекция 8

ЭЛЕМЕНТАРНЫЕ ПРЕБРАЗОВАНИЯ СТРОК И СТОЛБЦОВ ЦЕЛОЧИСЛЕННЫХ МАТРИЦ

Теорема. *Любая целочисленная прямоугольная матрица элементарными преобразованиями строк и столбцов приводится к диагональному виду* $\begin{pmatrix} \alpha_1 & & 0 \\ & \alpha_2 & \\ 0 & & \ddots \end{pmatrix}$*, где* $\alpha_i \geq 0$.

Доказательство. (по индукции по числу строк)

База индукции $n = 1$. Матрица имеет вид $(a_1 \quad a_2 \quad \dots \quad a_n)$. Если она нулевая, то она уже имеет искомый вид. Если она не нулевая, то без ограничения общности можем считать, что a_1 - это наименьший по модулю ненулевой элемент (иначе переставим столбцы). Также мы можем считать, что $a_1 > 0$ (иначе умножим столбец на -1), таким же образом сделаем все элементы положительными. Пусть $a_2 = a_1 q + r$, где $0 \leq r < a_1$. Вычитая из второго столбца $a_1 q$, получим строку $(a_1 \quad r \quad a_3 \quad \dots)$. Если $r \neq 0$, то наименьший модуль ненулевого элемента уменьшился, проделывая эту операцию несколько раз, получим, что модуль больше не может уменьшаться, т.к. он больше нуля. Следовательно, $r = 0$, и мы получим строку $(a_1 \quad 0 \quad a_3 \quad \dots)$. Проделав это несколько раз, мы в итоге получим строку $(0 \quad \dots \quad 0 \quad d \quad 0 \quad \dots \quad 0)$, поменяв местами столбцы, получим $(d \quad 0 \quad \dots \quad 0)$ - диагональная матрица, причем $d \geq 0$.

Индуктивный переход. Пусть утверждение теоремы верно для $n-1$ строк, докажем его для n строк. Мы имеем матрицу $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ Обозначим через $\delta(A) = \min\{|a_{ij}|, a_{ij} \neq 0\}$. Предположим, что привели A к $A' = \begin{pmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{m1} & \dots & a'_{mn} \end{pmatrix}$ так, что дальше $\delta(A')$ не уменьшается. Переставив строчки и столбцы и, если надо, умножив на -1, получим, что это минимум достигается на элементе a'_{11}, причем $a'_{11} > 0$. Тогда мы получим, что $|a_{ij}| \geq a_{11}$, если $a_{ij} \neq 0$.

Лемма. *Все элементы первой строки* a'_{1i} *и первого столбца* a'_{i1} *делятся на* $a'_{11} = \delta(A')$.

Доказательство.

Возьмем произвольный элемент из первой строки a'_{1i}, получим, что $a'_{1i} = a'_{11} q + r$, где $0 \leq r < a'_{11}$. Если $r \neq 0$, то вычтя из i-го столбца первый, умноженный на q, получим на месте $1i$ число $0 < r < a'_{11}$, следовательно $\delta(A')$ уменьшилось, что невозможно. Значит $r = 0$ и все элементы первой строки делятся на a'_{11}. Аналогично доказываем и про первый столбец. ◊

Раз все элементы первой строки и первого столбца делятся на a_{11}, то вычитая первую строку (умноженную на нужный коэффициент) из остальных, и вычитая первый столбец (умноженный на нужный коэффициент) из остальных, получим матрицу $B = \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix}$, причем $b_{11} > 0$. Дальше, по предположению индукции, мы можем привести к диагональному виду матрицу $\begin{pmatrix} b_{22} & \dots & b_{2n} \\ \vdots & \ddots & \vdots \\ b_{m2} & \dots & b_{mn} \end{pmatrix}$, состоящую из $n-1$ строк. В итоге получим искомое разложение. ◊

Упражнение. Число $\delta(A')$ равно набольшему общему делителю всех элементов матрицы.

Пример:

Приведем к диагональному виду матрицу $\begin{pmatrix} 2 & 3 & 0 \\ -4 & 0 & 2 \\ 3 & 4 & -2 \end{pmatrix}$, имеем, что $\delta(A') =$ НОДу всех элементов $=1$.

Следовательно, 1 можно получить (например, умножив первый столбец на -1 и прибавив к нему второй): $\begin{pmatrix} 1 & 3 & 0 \\ 4 & 0 & 2 \\ 1 & 4 & -2 \end{pmatrix}$, ну а дальше будем действовать по алгоритму из доказательства теоремы:

$$\begin{pmatrix} 1 & 3 & 0 \\ 4 & 0 & 2 \\ 1 & 4 & -2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 4 & -12 & 2 \\ 1 & 1 & -2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -12 & 2 \\ 0 & 1 & -2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -12 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & -22 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 22 \end{pmatrix}.$$

Теорема. *Пусть A - свободная абелевая группа и B - ее подгруппа, тогда в A существует такой базис $f_1,\dots,f_n$, что существуют $d_1>0,\dots,d_k>0$, такие что $d_1f_1,\dots,d_kf_k$ - базис в B.*

Доказательство.

Пусть $e_1,\dots,e_n$ - базис в A. Пусть $g_1,\dots,g_k$ - базис в B, тогда

$$\begin{matrix} g_1 = e_1a_{11} + \dots + e_na_{n1} \\ \vdots \\ g_k = e_1a_{1k} + \dots + e_na_{nk} \end{matrix}$$

. Получим целочисленную матрицу $A = \begin{pmatrix} a_{11} & \dots & a_{ik} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nk} \end{pmatrix}$, приведем ее к диагональному виду $\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{pmatrix}$. При проведении элементарных преобразований, мы просто перешли к новому базису в A и в B, таким образом, мы нашли базис $f_1,\dots,f_n$ в A, такой что $d_1f_1,\dots,d_kf_k$ будет базисом в B. ◊

Вспомним определение конечно-порожденной абелевой группы и докажем

Теорема. *Пусть H - конечно-порожденная абелевая группа, тогда H является прямой суммой свободной абелевой группы и примарных циклических групп (циклических групп, порядок которых равен степени простого числа).*

Доказательство.

Пусть $H = \langle h_1,\dots,h_n \rangle$, т.е. H порождена элементами $h_1,\dots,h_n$. F - свободная абелевая группа с базисом $e_1,\dots,e_n$. Построим гомоморфизм $\omega: F \to H$ по правилу $\omega(x_1e_1 + \dots x_ne_n) = x_1h_1 + \dots + x_nh_n \in H$. Очевидно, что отображение ω сюръективно. Его ядро $\operatorname{Ker}\omega$ является подгруппой в F. Пусть $f_1,\dots,f_n$ - базис в F, такой что $d_1f_1,\dots,d_kf_k$ - базис в $\operatorname{Ker}\omega$ (здесь $d_i>0$ и $k \le n$). В итоге имеем, что

$F = Zf_1 \oplus \dots \oplus Zf_n$

$\operatorname{Ker}\omega = Zd_1f_1 \oplus \dots \oplus Zd_nf_n$, здесь положим $d_i = 0$ при $i > k$.

$H \cong F/\operatorname{Ker}\omega \cong Zf_1/Zd_if_1 \oplus \dots \oplus Zf_n/Zd_nf_n$ (по теореме о факторизации слагаемых).

Рассмотрим отдельное слагаемое $Zf_i/Zd_if_i = \begin{cases} Z, & d_i = 0 \\ Z/d_i, & d_i \ne 0 \end{cases}$, следовательно

$$H \cong \underbrace{Z/d_1 \oplus \dots \oplus Z/d_k}_{\text{примарные циклические группы}} \oplus \underbrace{Z \oplus \dots \oplus Z}_{\text{свободная абелевая группа}}$$

. Вообще говоря группы Z/d_i могут быть и не примарными, но в этом случае они раскладывают дальше в прямую сумму примарных циклических групп. ◊

Следствие. Конечная абелевая группа является прямой суммой примарных циклических групп.

Доказательство.

Любая конечная абелевая группа является конечно-порожденной. И т.к. свободная абелевая группа счетная, то ее нет в разложении, предложенном в теореме. Следовательно, остаются только примарные циклические группы. ◊

Пример.

Возьмем группу G порядка $72 = 2^3 \cdot 3^2$, тогда возможны следующие варианты:

1) $G \cong Z/2 \oplus Z/2 \oplus Z/2 \oplus Z/3 \oplus Z/3$
2) $G \cong Z/4 \oplus Z/2 \oplus Z/3 \oplus Z/3$
3) $G \cong Z/8 \oplus Z/3 \oplus Z/3$
4) $G \cong Z/2 \oplus Z/2 \oplus Z/2 \oplus Z/9$
5) $G \cong Z/4 \oplus Z/2 \oplus Z/9$
6) $G \cong Z/8 \oplus Z/9$

Следовательно всего существует 6 не изоморфных абелевых групп порядка 72.

Определение. *Группа* G **не имеет кручения**, *если она не содержит неединичных элементов конечного порядка.*

Теорема. *Конечно-порожденная абелевая группа без кручения является свободной.*

Доказательство.

По предыдущей теореме имеем, что $H = F \oplus \underbrace{Z/d_1 \oplus \ldots \oplus Z/d_k}_{\text{элементы конечного порядка}}$, следовательно этих слагаемых нет и $H = F$ - свободная абелевая группа. ◊

ДИСКРЕТНЫЕ ПОДГРУППЫ В R^n

Определение. *Аддитивная подгруппа* A *в* R^n *называется* **дискретной**, *если существует окрестность нуля* $U(0)$, *такая что* $A \bigcap U(0) = \{0\}$, *т.е. в некоторой окрестности нуля нет ни одного элемента подгруппы* A *кроме нулевого.*

Теорема. *Дискретная подгруппа в* R^n *свободна.*

Доказательство.

Пусть $f_1, \ldots, f_k$ - максимальная независимая (над R) система векторов из A. Если $a \in A$, то $a = \lambda_1 f_1 + \ldots + \lambda_k f_k$, где $\lambda_k \in R$. Разложим λ на целые и дробные части: $a = \underbrace{[\lambda_1] f_1 + \ldots + [\lambda_k] f_k}_{\in A} + \alpha_1 f_1 + \ldots + \alpha_k f_k$, где $0 \le \alpha_i < 1$, следовательно, $\alpha_1 f_1 + \ldots + \alpha_k f_k \in A$. Рассмотрим множество $\Gamma = \{\xi_1 f_1 + \ldots + \xi_k f_k \mid 0 \le \xi_i \le 1\}$ - компакт.

Лемма. $A \bigcap \Gamma$ *- конечно.*

Доказательство.

Если $A \bigcap \Gamma$ бесконечно, то в $A \bigcap \Gamma$ существует сходящаяся последовательность $\Big\{\underset{\in A \bigcap \Gamma}{x_n}\Big\} \to x \in \Gamma$, следовательно x_n - последовательность Коши, т.е. $\forall \varepsilon > 0 \quad \exists N = N(\varepsilon) : \forall n_1, n_2 > N \quad \Big|\underbrace{x_{n_1} - x_{n_2}}_{\in A}\Big| < \varepsilon$. Следовательно в любой окрестности нуля $U(0)$ будут элементы из A, что противоречит дискретности A. Следовательно $A \bigcap \Gamma$ конечно. ◊

Таким образом, получили, что A - конечно-порожденная группа (порождается элементами $A \bigcap \Gamma$ и $f_1, \ldots, f_k$) и у нее нет элементов конечного порядка. Следовательно она свободна. ◊

Теорема. *Пусть* A *- дискретная подгруппа в* R^n *и* $e_1, \ldots, e_k$ *- базис в* A. *Тогда* $e_1, \ldots, e_k$ *- линейно независимы над* R.

Доказательство.

Пусть эти вектора линейно зависимы, т.е. без ограничения общности можем считать, что $e_1 = \lambda_2 e_2 + \ldots + \lambda_k e_k$, $\lambda_i \in R$. Рассмотрим множество $\Gamma = \left\{\sum_{i=1}^{k} \alpha_i e_i \mid 0 \le \alpha_i \le 1\right\}$, по лемме $A \bigcap \Gamma$ - конечно. Для любого целого $d \ge 1$ имеем, что $de_1 = d\lambda_2 e_2 + \ldots + d\lambda_k e_k = [d\lambda_2] e_2 + \ldots + [d\lambda_k] e_k + \underbrace{\beta_2 e_2 + \ldots + \beta_k e_k}_{\in A \bigcap \Gamma}$. Этих остатков, принадлежащих $A \bigcap \Gamma$, конечное число, следовательно $\exists m > d$, такое что $me_1 - de_1 = t_2 e_2 + \ldots + t_k e_k$, здесь $t_i \in Z$, следовательно $(\underbrace{m - d}_{\ne 0}) e_1 = t_2 e_2 + \ldots + t_k e_k$. Следовательно $e_1, \ldots, e_k$ линейно зависимы над Z, что невозможно. ◊

Лекция 9

КРИСТАЛЛО-ГРАФИЧЕСКИЕ ГРУППЫ (ПРИЛОЖЕНИЕ ТЕОРИИ ГРУПП)

Пусть нам задано евклидово пространство E размерности n. Пусть нам также задана метрика $\|x-y\| = \sqrt{(x-y, x-y)}$, где (a,b) - скалярное произведение векторов a и b. Движение пространства E - это биективное преобразование Φ пространства E , сохраняющее расстояние между векторами, т.е. $\|\Phi(x)-\Phi(y)\| = \|x-y\| \quad \forall x, y$.

Упражнение. Будет ли произвольное преобразование, сохраняющее длины, биекцией?

Теорема. *Пусть* Φ *- движение, тогда* $\Phi(x) = \phi(x) + b$*, где* $\phi(x)$ *- ортогональное преобразование* E *и* $b \in E$ *- некоторый вектор. Также верно и обратное утверждение.*

Доказательство этой теоремы было в курсе Линейной Алгебры. ◊

Рассмотрим множество $Iso(E)$ - все движения пространства E.

Теорема. $Iso(E)$ *- группа относительно операции композиции преобразований.*

Доказательство.

Пусть $\Phi(x) = \phi(x) + b$ и $\Psi(x) = \psi(x) + d$, тогда $\Psi(\Phi(x)) = \Psi(\phi(x)+b) = \psi(\phi(x)+b) + d = \psi\phi(x) + \psi(b) + d$ - снова движение.

Единичное преобразование - это тождественное преобразование.

Обратное преобразование - это $\Phi^{-1}(x) = \phi^{-1}(x) - \phi^{-1}(b)$. ◊

Рассмотрим множество $N = \{\Phi(x) = x + b\}$ - множество всех сдвигов. Из формулы последней теоремы видно, что N - это подгруппа в $Iso(E)$. Рассмотрим также множество $O(E)$ - множество всех ортогональных преобразований E , это множество также будет подгруппой в $Iso(E)$.

По первой теореме произвольное преобразование имеет вид $\Phi(x) = \phi(x) + b$. В этой записи вектор b определен однозначно, т.к. $b = \Phi(0)$. Следовательно и ортогональное преобразование $\phi(x) = \Phi(x) - b$ определено однозначно. Это преобразование ϕ называется **дифференциалом** преобразования Φ и обозначается $\phi = D_\Phi$.

Из формулы второй теоремы имеем, что $D_{\Psi\Phi} = D_\Psi \cdot D_\Phi$, т.е. дифференциал обладает свойством мультипликативности.

Теорема. *Сопоставление движению* Φ *его дифференциала* D_Φ *является эпиморфизмом* $Iso(E) \to O(E)$*, причем ядро этого эпиморфизма равно* N.

Доказательство.

То, что это гомоморфизм групп следует из свойства мультипликативности дифференциала. Если $\phi \in O(E)$, то $\phi = D_{\phi(x)}$, следовательно этот гомоморфизм сюръективен (т.е. это эпиморфизм). Ядро - это все движения, дифференциал которых равен тождественному преобразованию, т.е. все движения вида $\Phi(x) = x + b$, т.е. множество сдвигов N. ◊

Следствие. $N \lhd Iso(E)$ и $Iso(E)/N \cong O(E)$.

Предложение. $N \cong (E,+)$.

Доказательство.

Пусть $\Phi(x) = x + b$ - сдвиг на вектор b , сопоставим такому преобразованию этот вектор b. Тогда, если $\Psi(x) = x + c$ - сдвиг на вектор c, $\Psi\Phi(x) = x + b + c$ - сдвиг на вектор $b + c$. Это сопоставление преобразованию вектора является биективным, следовательно $N \cong (E,+)$. ◊

Определение. *Подгруппа* G *в* $Iso(E)$ *называется* **кристалло-графической***, если*

1) $G \cap N$ *- дискретная подгруппа группы* E *ранга* n,

2) $G/G \cap N = \Delta$ *- конечная группа.*

Опишем все кристалло-графические группы в двумерном случае.

Предложение. Если $(x+a)\in G\bigcap N$ и $\phi(x)\in\Delta$, то $(x+\phi(a))\in G\bigcap N$.

Доказательство.

Пусть $\Psi\in G$, $\Psi(x)=x+a$ - сдвиг на a, и $\Phi\in G$, $\Phi(x)=\phi(x)+b$ - преобразование с дифференциалом $\phi(x)$. Тогда $\Phi\Psi\Phi^{-1}(x)=\Phi\Psi(\phi^{-1}(x)-\phi^{-1}(b))=\Phi(\phi^{-1}(x)-\phi^{-1}(b)+a)=x-b+\phi(a)+b=x+\phi(a)$, следовательно $(x+\phi(a))\in G\bigcap N$ (т.к. N - нормальна). ◊

Пусть $f_1,\dots,f_n$ - базис в $G\bigcap N$ (это также будет базис во всем линейном пространстве E). В группе G лежат все целочисленные комбинации этих векторов, т.е. целочисленная решетка, порожденная этими векторами. Предыдущим упражнением мы доказали, что группа Δ переводит эту решетку в себя. Матрица любого оператора $\phi\in\Delta$ целочисленная в базисе $f_1,\dots,f_n$, т.е. $\operatorname{tr}\phi$ - это целое число.

Группа $G\bigcap N$ называется **пространственной** группой.

Группа Δ называется **точечной** группой.

Теорема. *Пусть* $n=2$ *и* $\Delta\subseteq SO(E)$ *- группа ортогональных операторов с определителем* 1 *(т.е.* Δ *содержит только собственные преобразования). Тогда* Δ *- циклическая группа порядка* $1,2,3,4,6$.

Доказательство.

Пусть e_1,e_2 - ортогональный базис пространства E и $\phi\in\Delta$, тогда его матрица имеет вид $A_\phi=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}$. Кроме того, ее след $\operatorname{tr}A_\phi=2\cos\alpha$ - целое число. Следовательно $\cos\alpha=0,\pm\frac{1}{2},\pm1$, т.е. $\alpha=0,\pm\frac{\pi}{3},\pm\frac{2\pi}{3},\pi$. Укажем все возможные варианты группы Δ в зависимости о того, какие повороты в ней лежат:

повороты, лежащие в группе	элементы группы	порядок
0	E	1
$0,\pi$	$E,-E$	2
$0,\pm\frac{2\pi}{3}$	$E,\begin{pmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{pmatrix},\begin{pmatrix}\cos\left(-\frac{2\pi}{3}\right) & -\sin\left(-\frac{2\pi}{3}\right)\\ \sin\left(-\frac{2\pi}{3}\right) & \cos\left(-\frac{2\pi}{3}\right)\end{pmatrix}$	3
$0,\pm\frac{\pi}{2},\pi$	$E,\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},-E$	4
$0,\pm\frac{\pi}{3},\pm\frac{2\pi}{3},\pi$	$E,\begin{pmatrix}\cos\frac{\pi}{3} & -\sin\frac{\pi}{3}\\ \sin\frac{\pi}{3} & \cos\frac{\pi}{3}\end{pmatrix},\begin{pmatrix}\cos\left(-\frac{\pi}{3}\right) & -\sin\left(-\frac{\pi}{3}\right)\\ \sin\left(-\frac{\pi}{3}\right) & \cos\left(-\frac{\pi}{3}\right)\end{pmatrix},\begin{pmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{pmatrix},$ $\begin{pmatrix}\cos\left(-\frac{2\pi}{3}\right) & -\sin\left(-\frac{2\pi}{3}\right)\\ \sin\left(-\frac{2\pi}{3}\right) & \cos\left(-\frac{2\pi}{3}\right)\end{pmatrix},-E$	6

В этой таблице не все матрицы целочисленные, однако существуют такие базисы (для каждого случая он свой), что в них эти матрицы будут целочисленными. Например, в базисе e_1,e_2, где вектор e_2 повернут относительно e_1 на угол $\frac{2\pi}{3}$ матрица поворота на угол $\frac{2\pi}{3}$ будет иметь вид $\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$ (тогда все матрицы в случае группы порядка 3), а если e_2 повернут относительно e_1 на угол $\frac{\pi}{3}$, то матрица поворота на угол $\frac{\pi}{3}$ имеет вид $\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$ (тогда все матрицы в случае группы порядка 6 будут целочисленные). ◊

Теорема. *Пусть* $n=2$ *и* $\Delta\not\subseteq SO(E)$*, т.е. в* Δ *есть несобственное преобразование (преобразование с определителем* -1*), тогда* Δ *- одна из следующих групп:*

1) V_4,

2) D_3, D_4, D_6,

3) циклическая группа порядка 2.

Доказательство.

Пусть $b \in \Delta$ и $b \notin SO(E)$. Если $c \in \Delta$ и $c \notin SO(E)$, тогда $bc \in SO(E)$. b - это отражение относительно некоторой оси, следовательно матрица b в некотором базисе имеет вид $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, но в любом базисе имеем $b^2 = c^2 = E$.

Имеем, что $\Delta \bigcap SO(E) = \langle a \rangle_k$, где $k = 1,2,3,4,6$. $\langle a \rangle_k$ - подгруппа индекса 2 в Δ, следовательно $\langle a \rangle_k \triangleleft \Delta$ и $\Delta = \langle a \rangle_k \bigcup b\langle a \rangle_k$. Т.к. ba - это снова симметрия относительно некоторой оси, то $(ba)^2 = 1$ и $baba = 1 \Rightarrow bab = a^{-1} \Rightarrow bab^{-1} = a^{-1}$, т.к. $b^{-1} = b$. Следовательно группа Δ - это группа диэдра.

В случае $k = 2$ эта группа превращается в группу V_4.

В случае $k = 1$ это циклическая группа порядка 2. ◊

Покажем теперь, как можно получить все эти варианты групп Δ (пусть f_1, f_2 - базис):

1) если f_1, f_2 не перпендикулярны и имеют разные длины, то $\Delta = \langle a \rangle_2$, где a - центральная симметрия;

2) если f_1, f_2 перпендикулярны и имеют разные длины, то $\Delta = V_4 = D_2$;

3) если f_1, f_2 перпендикулярны и имеют одинаковые длины, то $\Delta = D_4$;

4) если f_1, f_2 не перпендикулярны, имеют равные длины и не образуют правильный треугольник, то $\Delta = V_4 = D_2$;

5) если f_1, f_2 образуют правильные треугольник, то $\Delta = D_6$.

6) также допустимы подгруппы этих групп, таким образом, получаются все указанные нами группы.

Двумерный случай разобран полностью. Есть также теорема, утверждающая, что порядок конечной подгруппы в группе ортогональных матриц ограничен для каждого n числом $L(n)$ (в случае $n = 2$ имеем $L(2) = 12$), т.е. таких групп Δ конечное число для любого n.

Приведем описание (без доказательства) трехмерного случая:

Пусть Δ - конечная подгруппа в $SO(3, R)$, тогда Δ - это:

1) циклическая группа порядка $1,2,3,4,6$;

2) V_4;

3) D_3, D_4, D_6;

4) A_4;

5) S_4;

6) A_5.

Лекция 10

ПРЕДСТАВЛЕНИЯ ГРУПП

Пусть нам задано поле k и линейное пространство V над этим полем. Пусть $GL(V)$ - все обратимые линейные операторы, тогда $GL(V)$ - группа относительно операции умножения операторов. Пусть G - произвольная группа, тогда **представление** G в V - это гомоморфизм $G \to GL(V)$.

Если $g \in G$ и $x \in V$, то $gx = \phi(g)x$. По свойству гомоморфизма имеем $(gh)x = g(hx)$ и $1 \cdot x = x$. таким образом, мы получили действие G на V как на множестве.

Примеры:

1) Рассмотрим группу S_4 - группу симметрий тетраэдра - тем самым у нас есть гомоморфизм $S_4 \to O(3, R) \subset GL(3, R)$. Т.е. имеем представление группы S_4. Это пример трехмерного представления группы S_4.

2) Рассмотрим куб и группу вращений (относительно некоторой оси), переводящих его в себя. Возьмем диагонали куба (всего из 4). Каждое вращение переставляет диагонали, т.е. является подстановкой из S_4. Надо доказать, что любая подстановка из S_4 реализуется, оставим это в качестве упражнения. Еще надо доказать однозначность, т.е. если диагонали остались на месте (т.е. перестановка единична) , то и все вершины остались

на месте (т.е. преобразование единственно), это тоже оставим в качестве упражнения. Таким образом, мы получили еще одно представление группы S_4. Это пример еще одного трехмерного представления.

3) Мы знаем что $S_3 \cong D_3$, при изоморфизме $(123) \to a$ - поворот на угол $\frac{2\pi}{3}$ и $(12) \to b$ - симметрия относительно оси Ox. Получаем представление группы S_3 в виде группы симметрий правильного треугольника (это представление двумерно).

4) Вернемся к группе S_4, построим двумерное представление этой группы. Рассмотрим многочлены:

$f_1 = x_1x_2 + x_3x_4$

$f_2 = x_1x_3 + x_2x_4$

$f_3 = x_1x_4 + x_2x_3$

Если $\sigma \in S_4$, то $\sigma(f_k)$ - перестановка переменных в соответствии с подстановкой σ. Но как бы мы не переставляли переменные, мы опять получим один из этих многочленов. Т.е. перестановка $\sigma \in S_4$ как-то переставит наши три многочлена. Мы получили гомоморфизм $S_4 \to S_3$ (причем его ядро - это V_4), также есть гомоморфизм $S_3 \to D_3$. Из композиция - это гомоморфизм $S_4 \to D_3$ - двумерное представление группы S_4.

5) Рассмотрим группу S_n, укажем бесконечномерное представление этой группы. Возьмем кольцо многочленов $V = k[x_1, \dots, x_n]$. Тогда гомоморфизм по правилу $(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ будет преставлением (бесконечномерным) группы S_n.

6) Рассмотрим группу $GL(n,k)$ и кольцо многочленов $V = k[x_1, \dots, x_n]$. Пусть $A = (a_{ij}) \in GL(n,k)$, тогда гомоморфизм по правилу $(Af)(x_1, \dots, x_n) = f\left(\sum_{i=1}^{n} a_{1i}x_i, \dots, \sum_{i=1}^{n} a_{ni}x_i\right)$ будет представлением группы $GL(n,k)$.

Пусть $\psi : G \to GL(V)$ и $\phi : G \to GL(W)$. Представления ψ и ϕ называются **эквивалентными**, если существует такое биективное линейное отображение $\omega : V \to W$, что $\forall g \in G$ и $\forall x \in V$ имеем $\omega[\psi(g)x] = \phi(g)[\omega(x)]$.

На языке матриц (в случае $V = W$) это означает следующее:

Пусть e - базис в V, A_g - матрица $\psi(g)$ в базисе e, B_g - матрица $\phi(g)$ в базисе e, C - матрица ω в базисе e. Тогда условие эквивалентности представлений перепишется в виде: $\forall g \quad CA_g = B_gC$, т.е. $A_g = C^{-1}B_gC$. Т.е. B_g и A_g - это матрицы одного и того же оператора в базисах e и Ce. Отсюда, в частности, вытекает, что $\operatorname{tr} A_g = \operatorname{tr} B_g$.

Рассмотрим снова группу S_3 и два ее двумерных представления:

ψ : $(12) \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $(123) \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ и ϕ: $(12) \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $(123) \to \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.

Упражнение. Если $\operatorname{char} k \neq 3$ (характеристика поля), то эти представления эквивалентны. А если $\operatorname{char} k = 3$, то не эквивалентны.

В дальнейшем будем считать, что поле k - это поле вещественных или комплексных чисел.

Теорема. *Любое конечномерное вещественное (комплексное) представление конечной группы G эквивалентно ортогональному (унитарному).*

Доказательство.

Возьмем произвольный базис $e_1, \dots, e_n$ и зададим скалярное произведение: если $x = x_1e_1 + \dots + x_ne_n$ и $y = y_1e_1 + \dots + y_ne_n$, то $(x,y) = x_1\overline{y_1} + \dots + x_n\overline{y_n}$. Введем еще одно скалярное произведение $\langle x,y \rangle = \frac{1}{|G|}\sum_{g \in G}(gx, gy)$.

Докажем, что это действительно скалярное произведение: $\langle y,x \rangle = \frac{1}{|G|}\sum_{g \in G}(gy, gx) = \frac{1}{|G|}\sum_{g \in G}\overline{(gx, gy)} = \overline{\langle x,y \rangle}$. Если $\langle x,x \rangle = 0 = \frac{1}{|G|}\sum_{g \in G}(gx, gx)$, то $(gx, gx) = 0 \quad \forall g$, следовательно $gx = 0 \quad \forall g \Rightarrow x = 0$. Т.е. это действительно будет скалярным произведением.

Пусть $h \in G$, тогда $\langle hx, hy \rangle = \frac{1}{|G|}\sum_{g\in G}(ghx, ghy) \overset{Gh=G}{=} \frac{1}{|G|}\sum_{u\in G}(ux, uy) = \langle x, y \rangle$. Следовательно любой оператор сохраняет скалярное произведение и является ортогональным (унитарным). ◊

Следствие. Если подпространство U инвариантно относительно всех операторов $\phi(g)$, где $g \in G$, то $V = U \oplus W$, где подпространство W также инвариантно относительно всех операторов $\phi(g)$.

Определение. *Пусть* $V = U \oplus W$ *и* $\phi : G \to GL(U)$, $\psi : G \to GL(W)$, *тогда представление* $\Phi : G \to GL(V)$, *такое что* $\Phi(g)(u + w) = \phi(g)u + \psi(g)w$, *называется* **прямой суммой** *представлений* ϕ *и* ψ. *А представления* ϕ *и* ψ *называются* **подпредставлениями** *в* Φ.

Из курса линейной алгебры мы знаем, что если U - инвариантное подпространство V, то матрица любого оператора имеет вид $A = \left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right)$. А если $V = U \oplus W$, то $A = \left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$.ъ

Определение. *Представление* $\phi : G \to GL(V)$ **неприводимо**, *если в* V *нет нетривиальных (отличных от нуля и самого пространства) инвариантных подпространств. Представление* **вполне приводимо**, *если оно является прямой суммой неприводимых.*

Теорема Машке. *Любое конечномерное вещественное (комплексное) представление конечной группы вполне приводимо.*

Доказательство.

Пусть $\phi : G \to GL(V)$, U - инвариантное подпространство минимальной ненулевой размерности, тогда $V = U \oplus U^{\perp}$, $U^{\perp}$ тоже инвариантно относительно $\phi(g)$ $\forall g$, тогда наше представление разложится в прямую сумму неприводимого (U) и подпредставления меньшей размерности. Далее можно применить индукцию по размерности представления. ◊

Пример неприводимого представления:

$S_3 \cong D_3$. Докажем, что это представление неприводимо, как вещественное. Допустим, что оно приводится, т.е. существует инвариантное подпространство, т.е. по теореме Машке оно является прямой суммой одномерных представлений, т.е. существует базис, в котором матрицы записывается в диагональном виде $\psi(\sigma) = \begin{pmatrix} \lambda_\sigma & 0 \\ 0 & \lambda'_\sigma \end{pmatrix}$, т.к. любые такие матрицы коммутируют, то $\psi[(12)(123)] = \psi(12)\psi(123) = \psi(123)\psi(12) = \psi[(123)(12)]$, но это не верно. Получили противоречие с предположением о существовании инвариантного подпространства, следовательно оного не существует и представление неприводимо.

Упражнение. Докажите, что рассмотренные нами в начале лекции два трехмерных представления группы S_4 не эквивалентны и оба неприводимы.

Теорема. *Любое неприводимое конечномерное комплексное представление абелевой группы одномерно.*

Доказательство.

Пусть задано представление $\phi : G \to GL(V)$. Пусть $g \in G$, тогда $\phi(g)$ имеет собственное значение λ_g и собственный вектор $x \neq 0$. Тогда подпространство собственных векторов $U = \{y \in V \mid \phi(g)y = \lambda_g y\}$ ненулевое. Более того, докажем, что оно инвариантно относительно всех операторов $\phi(h)$:

Возьмем $h \in G$ и $y \in U$, пусть $z = \phi(h)y$, тогда $\phi(g)z = \phi(g)\phi(h)y \overset{gh=hg}{=} \phi(h)\phi(g)y = \phi(h)\lambda_g y = \lambda_g z$, следовательно z - снова собственный вектор и подпространство инвариантно.

Т.е. $U = V$, т.к. представление неприводимо и U отлично от нуля. Т.е. $\forall g \in G \quad \exists \lambda_g \in C \ : \ \forall x \quad \phi(g)x = \lambda_g x$. Возьмем произвольный $x \neq 0$ и $W = \langle x \rangle$ - это инвариантное подпространство, следовательно $V = \langle x \rangle$ - одномерно. ◊

Теорема. *Число неэквивалентным неприводимых комплексных представлений конечной абелевой группы* G *равно ее порядку.*

Доказательство.

Возьмем произвольную абелевую группу G, тогда $G = \langle a_1 \rangle_{p_1^{n_1}} \times \ldots \times \langle a_k \rangle_{p_k^{n_k}}$. Если a_j переходит в λ_j, то $1 = a_j^{p_j^{n_j}}$ переходит в $\lambda_j^{p_j^{n_j}} = 1$, т.е. a_j должен переходит в корень $p_j^{n_j}$ степени из единицы. Для каждого a_i существует столько вариантов, какой его порядок, комбинируя из все, получим что всего существует столько вариантов, каков порядок группы. ◊

Примеры:

1) $G = \langle a \rangle_4$, всего существует 4 неприводимых комплексных представления, напишем их в табличке:

	1	a	a^2	a^3
ψ_1	1	1	1	1
ψ_2	1	-1	1	-1
ψ_3	1	i	-1	$-i$
ψ_4	1	$-i$	-1	i

(здесь в таблице стоит то, во что переходит элемент из столбца при представлении из строки).

2) $G = \langle a \rangle_2 \times \langle b \rangle_2$ - опять будет 4 представления:

	1	a	b	ab
ψ_1	1	1	1	1
ψ_2	1	-1	1	-1
ψ_3	1	1	-1	-1
ψ_4	1	-1	-1	1

3) $G = \langle a \rangle_2$, всего будет 2 представления:

	1	a
ψ_1	1	1
ψ_2	1	-1

Лекция 11

Одномерное представление - это гомоморфизм $\phi : G \to k^*$. Опишем все такие гомоморфизмы. Т.к. $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi \subseteq k^*$, то $G/\operatorname{Ker}\phi$ - абелевая группа. Следовательно, ядро этого гомоморфизма должно содержать коммутант группы, т.е. $\operatorname{Ker}\phi \supseteq G'$. По заданному гомоморфизму ϕ, мы можем рассмотреть гомоморфизм $\overline{\phi} : G/G' \to k^*$, действующий по правилу: $\overline{\phi}(xG') = \phi(x)$. И обратно, если задан гомоморфизм $\psi : G/G' \to k^*$, мы можем рассмотреть гомоморфизм $\phi : G \to k^*$, являющийся композицией естественного гомоморфизма $\pi : G \to G/G'$ и гомоморфизма ψ. Таким образом, мы можем отождествить гомоморфизмы $G \to k^*$ и гомоморфизмы $G/G' \to k^*$.

Примеры:

1) $G = S_n$, $G' = A_n$, $G/G' = S_n/A_n$ - группа порядка 2, $S_n/A_n = \{A_n, S_n \setminus A_n\}$. У нее существует всего два представления: $A_n \to 1,\ \ S_n \setminus A_n \to 1$ и $A_n \to 1,\ \ S_n \setminus A_n \to -1$. Т.е. у группы S_n существует всего два одномерных представления: $\sigma \to 1$ и $\sigma \to (-1)^\sigma$.

2) $G = D_n = \{1, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1} \mid a^n = b^2 = (ba)^2 = 1\}$, $G' = \langle a \rangle$, если n - нечетно и $G' = \langle a^2 \rangle$, если n - четно.

Если n - нечетно. Имеем $D_n/D_n{}' = \{\langle a \rangle_n, b\langle a \rangle_n\}$, существует два представления: $x \to 1$ и $x \to \det x$ ($a \to 1$, $b \to -1$).

Если n - четно. Имеем $D_n/D_n{}' = \{\langle a^2 \rangle, a\langle a^2 \rangle, b\langle a^2 \rangle, ab\langle a^2 \rangle\}$, существуют четыре представления ($a \to \pm 1$ и $b \to \pm 1$).

Теорема. *Любое неприводимое комплексное представление группы D_n имеет размерность ≤ 2.*

Доказательство.

Пусть V - пространство представлений. Пусть $x \in V$, рассмотрим $U = \langle gx \mid g \in D_n \rangle$ - конечномерно. Если $h \in D_n$, то $h(gx) = (hg)x \in U$. Следовательно, U - инвариантное подпространство, т.е. в силу неприводимости представления $U = V$, следовательно, V конечномерно.

Оператор a имеет собственные вектор $y \neq 0$, такой что $ay = \lambda y$. Обозначим $W = \langle y, by \rangle$, покажем, что W - инвариантно. Имеем, $a(\alpha y + \beta by) = \alpha(ay) + \beta(aby) = \alpha\lambda y + \beta(ba^{-1}y) = \alpha\lambda y + \beta b\lambda^{-1}y = \alpha\lambda y + \beta\lambda^{-1}by \in W$ и $b(\alpha y + \beta by) = \alpha by + \beta b^2 y = \alpha by + \beta y \in W$. Следовательно, W - инвариантно и в силу неприводимости представления $W = V$, следовательно, $\dim V = \dim W \leq 2$. ◊

Если $e_1 = y$, $e_2 = by$, то матрица представления группы D_n имеет вид $a \to \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $b \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Т.к. $a^n = 1$, то $\lambda^n = 1$, т.е. λ - это корень степени n из 1.

Вернемся к представлениям группы S_n. Пусть $(\operatorname{char} k, n) = 1$, т.е. n и характеристика поля взаимнопросты. Рассмотрим пространство V с базисом $(e_1, \ldots, e_n)$, тогда $\sigma(e_i) = e_{\sigma(i)}$ - это представление. Выделим два подпространства: $U = \langle e_1 + \ldots + e_n \rangle$ и $W = \langle x_1e_1 + \ldots + x_ne_n \mid x_1 + \ldots + x_n = 0 \rangle$. Они инвариантны.

Упражнение. Докажите, что $V = U \oplus W$ (здесь важно, что $(\operatorname{char} k, n) = 1$).

Теорема. *Если $(\operatorname{char} k, n) = 1$, то W - неприводимо.*

Доказательство.

Пусть $h = h_1e_1 + \ldots + h_ne_n \in W \setminus \{0\}$. $h_1 + \ldots + h_n = 0$, причем существует $h_i \neq 0$ (без ограничения общности будем считать, что $h_1 \neq 0$). Если $h_1 = \ldots = h_n$, то $nh_1 = 0 \Rightarrow h_1 = 0$ (т.к. $n \wr \operatorname{char} k$). Следовательно, не все h_i равны между собой (без ограничения общности будем считать, что $h_1 \neq h_2$).

Имеем $h = h_1e_1 + h_2e_2 + h_3e_3 + \ldots + h_ne_n$, $(12)h = h_1e_2 + h_2e_1 + h_3e_3 + \ldots + h_ne_n$. Тогда $h - (12)h = (h_1 - h_2)(e_1 - e_2)$ и $(e_1 - e_2) = \frac{1}{h_1 - h_2}(h - (12)h)$. Т.е. мы можем получить вектор $(e_1 - e_2)$. Аналогичным образом (подставляя вместо e_2 любой вектор e_i) получим все вектора $e_1 - e_3, \ldots, e_1 - e_n$ (если $h_1 = h_k$, то $h_2 \neq h_k$, получим вектор $e_2 - e_k$, прибавим к нему $e_1 - e_2$, получим $e_1 - e_k$). Эти $n-1$ вектор образуют базис в W, следовательно в W нет инвариантного подпространства (т.к. из одного вектора h мы можем получить все вектора W), следовательно W неприводимо. ◊

При $n = 3$ только что полученное нами представление эквивалентно группе диэдра D_3 (двумерное представление).

При $n = 4$ это представление эквивалентно группе симметрий тетраэдра (трехмерное представление).

При $n = 5$ существует одномерное и $n-1$ мерное представления.

АЛГЕБРЫ И ПОЛЯ

Кольцом называется абелевая группа по сложению с операцией умножения xy, для которой выполнены следующие свойства: $(x + y)z = xz + yz$ и $x(y + z) = xy + xz$.

Кольцо называется **коммутативным**, если $xy = yx$.

Кольцо называется **ассоциативным**, если $(xy)z = x(yz)$.

Кольцо называется **антикоммутативным**, если $x^2 = 0$.

Кольцо называется кольцом **Ли**, если $x^2 = (xy)z + (yz)x + (zx)y = 0$.

В любом кольце $0 \cdot x = x \cdot 0 = 0$. Действительно $0x = (0 + 0)x = 0x + 0x$ и $0 = -0x + 0x = -0x + 0x + 0x = 0x$.

Элемент 1 в кольце называется **единицей**, если $\forall x \quad 1 \cdot x = x \cdot 1 = x$.

Определение. Полем *называется коммутативное, ассоциативное кольцо с единицей, в котором у каждого ненулевого элемента есть обратный.*

Определение. Телом *называется ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.*

Примеры:

$Q, Z_p, Q(\sqrt{p}) = \{a + b\sqrt{p} \mid a, b \in Q\}, C, k(x)$

$H = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in C \right\}$ - поле кватернионов. Это действительно будет полем, т.к. $\begin{vmatrix} a & b \\ -\overline{b} & \overline{a} \end{vmatrix} = a\overline{a} + b\overline{b} = |a|^2 + |b|^2 > 0$, если матрица ненулевая, следовательно у нее существует обратная: $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix}$.

Определение. *Пусть k - поле. Кольцо A, являющееся векторным пространством над k, называется* k **- алгеброй***, если* $\alpha(xy) = (\alpha x)y = x(\alpha y) \quad \forall \alpha \in k \quad \forall x, y \in A$.

Упражнение. В антикоммутативной алгебре (кольце) выполнено тождество $xy = -yx$.

Упражнение. Пусть A - ассоциативная алгебра, положим $[x, y] = xy - yx$. Докажите, что A относительно нового умножения $[x, y]$ является алгеброй Ли.

Определение. *Элемент x алгебры A с единицей называется* **обратимым***, если* $\exists x^{-1} : xx^{-1} = x^{-1}x = 1$.

Определение. *Элемент $x \in A \setminus \{0\}$ называется* **левым** *(***правым***)* **делителем нуля***, если* $\exists y : xy = 0$ *(* $yx = 0$ *).*

Предложение. Все обратимые элементы ассоциативной алгебры с единицей образуют группу по умножению. Обратимый элемент не может быть делителем нуля.

Доказательство.

Если x, y - обратимы, тогда xy - обратим, $(xy)^{-1} = y^{-1}x^{-1}$.

Если x - обратим, то и x^{-1} - обратим, $(x^{-1})^{-1} = x$.

Следовательно это действительно группа по умножению.

Пусть x обратим и $xy = 0$, тогда $y = x^{-1}xy = x^{-1}0 = 0$, что противоречит определению делителя нуля. ◊

Определение. *Алгебра называется* **областью***, если в ней нет делителей нуля.*

Определение. Подалгеброй *B в алгебре A называется подпространство, являющееся кольцом, для которого выполнены свойства:*

1) $x, y \in B \Rightarrow \alpha x + \beta y \in B, xy \in B \quad \forall \alpha, \beta \in k$,

2) B не пусто.

Пусть A - ассоциативная k-алгебра с единицей, и пусть $z \in A$. Рассмотрим множество $k[z] = \left\{ \sum_{i \geq 0} \alpha_1 z^i \mid \alpha_i \in k \right\}$ - все такие <u>конечные</u> суммы.

Упражнение. $k[z]$ является наименьшей подалгеброй с единицей в A, содержащей элемент z.

Определение. Идеалом *I кольца (алгебры) называется подгруппа аддитивной группы (подпространство), такая что если $x \in I$, $y \in A$, то $xy \in I$ и $yx \in I$. Т.е. идеал выдерживает умножение слева и справа на все элементы кольца (алгебры).*

Определение. *Кольцо (алгебра) называется* **простым***, если в нем всего два идеала: 0 и оно само.*

Предложение. Пусть в ассоциативной алгебре с единицей идеал содержит обратимый элемент, тогда идеал совпадает со всей алгеброй.

Доказательство.

Пусть x - обратимый и $x \in I$. Если $a \in A$, то $a = (ax^{-1})x \in I$, следовательно $I = A$. ◊

Следствие. Любое тело, любое поле всегда просты.

Пусть A - ассоциативная коммутативная алгебра с 1 и $z_1, \ldots, z_n \in A$. Рассмотрим множество $(z_1, \ldots, z_n) = \left\{ \sum_{i=1}^{n} a_i z_i \mid a_i \in A \right\}$.

Упражнение. $(z_1, \ldots, z_n)$ - идеал в A, содержащий $z_1, \ldots, z_n$.

(z) называется **главным идеалом**, порожденным элементом $z \in A$.

Лекция 12

Определение. *Коммутативная ассоциативная область (без делителей нуля) с единицей называется кольцом (алгеброй)* **главных идеалов***, если в нем любой идеал главный.*

Например в кольце целых чисел Z любой идеал всегда подгруппа, т.е. $I = nZ$, т.е. любой идеал главный и это кольцо главных идеалов.

Теорема. *Пусть k - поле. Тогда $k[x]$ - кольцо главных идеалов.*

Доказательство.

Пусть $I \lhd k[x]$ и $I \neq 0$. Пусть $f \in I \setminus \{0\}$ - многочлен наименьшей степени. Пусть $g \in I \setminus \{0\}$, тогда мы можем поделить g на f с остатком: $g = qf + r$, где либо $r = 0$, либо $\deg r < \deg f$. Но $r = g - qg$, следовательно, $r \in I$. Т.к. у f была наименьшая степень, то $r = 0$, т.е. $g \vdots f \quad \forall g$. Следовательно I - главный идеал, порожденный многочленом f и $k[x]$ - кольцо главных идеалов. ◊

Упражнение. Доказать, что кольцо $k[x, y]$ не является кольцом главных идеалов. Указание: рассмотреть идеал I - все многочлены с нулевым свободных членов и доказать, что он не является главным.

Рассмотрим кольцо $Z[i] = \{a + bi \mid a, b \in Z\}$.

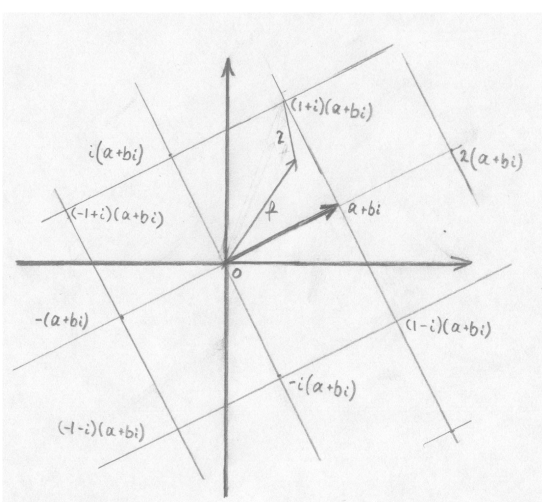
Теорема. $Z[i]$ *- кольцо главных идеалов.*

Доказательство.

Выведем на этом множестве аналог алгоритма Евклида (деление с остатком). Введем норму $\|a + bi\| = a^2 + b^2$, тогда $\|(a + bi)(c + di)\| = \|a + bi\| \cdot \|c + di\|$.

Лемма. *Пусть $z = a + bi \neq 0$, тогда $\forall f \in Z[i]$ существуют такие $q, r \in Z[i]$, что $f = q(a + bi) + r$, причем $\|r\| < \|a + bi\|$.*

Доказательство.



Рассмотрим все числа вида $(a + bi)(c + di) = c(a + bi) + di(a + bi)$. Получим что-то типа решетки, сторона квадрата - это $|a + bi|$. Возьмем произвольное число $f \in Z[i]$. Оно попадет в один из таких квадратов, тогда расстояние от не до какой-то вершины квадрата будет не больше $\frac{|a + bi|}{\sqrt{2}}$.

В качестве числа q возьмем такое число, чтобы $q(a + bi)$ была эта вершина. r - вектор от этой вершины до f. Тогда $\|r\| \le \frac{|a + bi|}{\sqrt{2}} \le \frac{\|a + bi\|}{\sqrt{2}} < \|a + bi\|$. ◊

Пусть теперь $I \triangleleft Z[i]$, $I \neq 0$. Выберем $a+bi \in I \setminus \{0\}$ такое, что его норма минимальна. Далее рассуждая также как и в прошлой теореме с многочленами (применяя описанное выше деление с остатком), получаем, что все остальные числа делятся на него, т.е. I - главный идеал и $Z[i]$ - кольцо главных идеалов. $\lozenge$

Теперь мы перейдем к рассмотрению некоммутативных колец. Пусть R - ассоциативное кольцо с единицей, $I \triangleleft R$. Пусть $K = Mat_n(R)$ - квадратные матрицы с коэффициентами из кольца R.

Упражнение. $Mat_n(I) \triangleleft Mat_n(R)$.

Теорема. *Пусть* $J \triangleleft Mat_n(R)$. *Тогда* $\exists I \triangleleft R$, *такой что* $J = Mat_n(I)$.

Доказательство.

Пусть $I = \{a \in R \mid aE_{11} \in J\}$. Докажем, что $I \triangleleft R$. Пусть $a \in I$ и $b \in R$, тогда $(bE)\underbrace{aE_{11}}_{\in J} = baE_{11} \in J$, следовательно, $ba \in I$. Аналогично $ab \in I$, следовательно, $I \triangleleft R$.

Пусть $A = \begin{pmatrix} a_{11} & \dots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in J$, тогда $E_{ij}AE_{ji} = a_{ij}E_{11} \in J$. Следовательно, $a_{ij} \in I$, т.е. все коэффициенты матриц из J содержатся в идеале I. Следовательно $J \subseteq Mat_n(I)$. Пусть $X = (x_{ij})$, $x_{ij} \in I$ - произвольная матрица из $Mat_n(I)$. Тогда $X = \sum x_{ij}E_{ij} = \sum x_{ij}E_{i1}E_{11}E_{1j} = \sum E_{i1}\left(\underbrace{x_{ij}E_{11}}_{\in J}\right)E_{1j} \in J$. Следовательно $Mat_n(I) \subseteq J$, т.е. $Mat_n(I) = J$. $\lozenge$

Напомним, что **к**ольцо (алгебра) R называется **простым**, если в нем только два идеала: ноль и оно само.

Следствие. Если R - тело, то $Mat_n(R)$ - простое кольцо.

Определение. *Отображение* $f : A \to B$ *называется* **гомоморфизмом** *алгебр, если*

1) $f(a+b) = f(a) + f(b)$,

2) $f(ab) = f(a)f(b)$,

3) $f(\alpha a) = \alpha f(a)$.

Изоморфизмом *называется биективный гомоморфизм.*

Автоморфизмом *называется изоморфизм алгебры на себя.*

Мономорфизмом *называется инъективный гомоморфизм.*

Эпиморфизмом *называется сюръективный гомоморфизм.*

Ядром *гомоморфизма называется полный прообраз нуля* $\mathrm{Ker}\, f = f^{-1}(0)$.

Предложение. $\mathrm{Ker}\, f \triangleleft A$.

Доказательство.

Пусть $a, b \in \mathrm{Ker}\, f$, тогда $f(\alpha a + \beta b) = \alpha f(a) + \beta f(b) = \alpha \cdot 0 + \beta \cdot 0 = 0 \Rightarrow \alpha a + \beta b \in \mathrm{Ker}\, f$.

Пусть $a \in \mathrm{Ker}\, f$, $c \in A$, тогда $f(ac) = f(a)f(c) = 0 \cdot f(c) = 0 \Rightarrow ac \in \mathrm{Ker}\, f$. $\lozenge$

Упражнение. $\mathrm{Ker}\, f = 0$ тогда и только тогда, когда f - мономорфизм.

Пусть $f : D \to B$, где D - тело. Тогда $\mathrm{Ker}\, f \triangleleft D$, но в D всего для идеала: ноль и оно само. Следовательно, либо f - нулевой, либо мономорфизм.

Пусть $I \triangleleft R$, тогда I - подгруппа в R (по сложению), причем нормальная, следовательно R/I - факторгруппа (по сложению), т.е. $R/I = \{x + I \mid x \in R\}$. Тогда

$$(x+I) + (y+I) = (x+y) + I$$
$$(x+I)(y+I) = xy + I \quad (*)$$
$$\alpha(x+I) = \alpha x + I \quad (**)$$

Предложение. Умножение $(*)$ и умножение на скаляры $(**)$ определены корректно.

Доказательство.

$x' \in x + I$, $y' \in y + I \overset{?}{\Rightarrow} x'y' + I = xy + I$.

$x' = x + i$, $y' = y + j$, $i, j \in I$.

$x'y' = (x+i)(y+i) = xy + \underbrace{(iy + xj + ij)}_{\in I} \in xy + I$.

Следовательно умножение $(*)$ определено корректно.

$\alpha x' = \alpha(x+i) = \alpha x + \underbrace{\alpha i}_{\in I} \in \alpha x + I$.

Следовательно умножение на скаляры $(**)$ определено корректно. ◊

Идеалы и факторгруппы строятся в любом кольце (не только в ассоциативном или коммутативном). R/I - фактоалгебра (факторкольцо).

Рассмотрим гомоморфизм $\pi : R \to R/I$, т.ч. $\pi(x) = x + I$ (естественный гомоморфизм).

Упражнение. π является эпиморфизмом и $\operatorname{Ker}\pi = I$.

Теорема (о гомоморфизме). *Пусть $f : A \to B$, тогда $\operatorname{Im} f$ - подалгебра, изоморфная $A/\operatorname{Ker} f$.*

Доказательство.

Определим изоморфизм $\xi : \operatorname{Im} f \to A/\operatorname{Ker} f$ следующим образом: $\xi(f(x)) = f^{-1}(f(x)) = x + \operatorname{Ker} f$ (см. теорему о гомоморфизме в теории групп). Проверим некоторые свойства изоморфизма (остальные проверены в теории групп):

$\xi(f(x) \cdot f(y)) = \xi(f(xy)) = xy + \operatorname{Ker} f = (x + \operatorname{Ker} f)(y + \operatorname{Ker} f) = \xi(f(x)) \cdot \xi(f(y))$

$\xi(\alpha f(x)) = \xi(f(\alpha x)) = \alpha x + \operatorname{Ker} f = \alpha(x + \operatorname{Ker} f) = \alpha \xi(f(x))$, следовательно это изоморфизм. ◊

Примеры:

1) $Z_n \cong Z/nZ$. Гомоморфизм $f : Z \to Z_n$, где $f(k)$ - остаток от деления k на n, тогда $\operatorname{Ker} f = nZ$.

2) $C[x,y]/(y) \cong C[x]$. Гомоморфизм $f : C[x,y] \to C[x]$, где $f(g(x,y)) = g(x,0) \in C[x]$, тогда $\operatorname{Ker} f = (y)$.

3) $R[x]/(x^2+5) \cong C$. Гомоморфизм $f : R[x] \to C$, где $f(g(x)) = g(i\sqrt{5}) \in C$, тогда $\operatorname{Ker} f = (x^2+5)$.

Если k - подполе в K, тогда K является алгеброй над k. Все автоморфизмы K как алгебры над k образуют группу Галуа $Gal(K/k)$.

АЛГЕБРА ВЕЙЛЯ

Рассмотрим $V = C[x_1, \dots, x_n]$ и рассмотрим операторы $p_i(f) = \dfrac{\partial f}{\partial x_i}$ и $q_i(f) = x_i f$.

Предложение. $p_i p_j = p_j p_i$, $q_i q_j = q_j q_i$, $p_i q_j - q_j p_i = \delta_{ij}$.

Доказательство.

Первые два соотношения очевидны, докажем третье:

$$(p_i q_j - q_j p_i) f = (p_i q_j) f - (q_j p_i) f = \frac{\partial}{\partial x_i}(x_j f) - x_j\left(\frac{\partial f}{\partial x_i}\right) = \frac{\partial x_j}{\partial x_i} f + \frac{\partial f}{\partial x_i} x_j - \frac{\partial f}{\partial x_i} x_j = \frac{\partial x_j}{\partial x_i} f = \delta_{ij} f.$$ ◊

Определение. Алгеброй Вейля $A_n(C)$ *называется подалгебра с единицей в алгебре всех линейных операторов на V, порожденная операторами $p_1, \dots, p_n, q_1, \dots, q_n$.*

Каждый элемент F из $A_n(C)$ можно представить в как $F = \sum \lambda_* q_1^{m_1} \cdot \ldots \cdot q_n^{m_n} p_1^{s_1} \cdot \ldots \cdot p_n^{s_n}$ или как $F = \sum F_i(q_1, \dots, q_n) \overline{F_i}(p_1, \dots, p_n)$ $(*)$.

Предложение. Пусть F представлено в виде $(*)$, тогда

1) $q_i F - F q_i = \sum_i F_i(q_1,\ldots,q_n)\dfrac{\partial \overline{F_i}(p_1,\ldots,p_n)}{\partial p_i}$

2) $p_i F - F p_i = \sum_i \dfrac{\partial F_i(q_1,\ldots,q_n)}{\partial q_i}\overline{F_i}(p_1,\ldots,p_n)$

Доказательство.

В любой алгебре A положим $[x,y] = xy - yx$, тогда $[x,yz] = [x,y]z + y[x,z]$, т.е. эта операция имеет такие же свойства как и дифференцирование, будем этим пользоваться. Посчитаем $[p_i,F]$ - дифференцирование многочлена F по переменной p_i:

$$[p_i,F] = \frac{\partial F}{\partial p_i} = \frac{\partial}{\partial p_i}\sum_i F_i(q_1,\ldots,q_n)\overline{F_i}(p_1,\ldots,p_n) = \sum_i \frac{\partial}{\partial p_i}\left[F_i(q_1,\ldots,q_n)\overline{F_i}(p_1,\ldots,p_n)\right] =$$

$$= \sum_i F_i(q_1,\ldots,q_n)\frac{\partial}{\partial p_i}\overline{F_i}(p_1,\ldots,p_n).$$

Аналогично доказывает и второй пункт. ◊

Лекция 13

Вернемся к рассмотрению алгебры Вейля. Напомним, что мы рассматривали пространство $V = C[x_1,\ldots,x_n]$ и линейные операторы $p_i(f) = \dfrac{\partial}{\partial x_i} f$, $q_i(f) = x_i f$, которые обладали свойством $[p_i,q_j] = \delta_{ij}$ и $[p_i,p_j] = [q_i,q_j] = 0$, где $[a,b] = ab - ba$. Алгебра Вейля – это $A_n(C)$, если $F \in A_n(C)$, то $F = \sum f_i(q_1,\ldots,q_n) g_i(p_1,\ldots,p_n)$, то $[p_j,F] = \sum \dfrac{\partial f_i}{\partial q_j} g_i$ и $[q_j,F] = \sum f_i \dfrac{\partial g_i}{\partial p_j}$.

Теорема. $A_n(C)$ *проста.*

Доказательство.

Пусть $I \lhd A_n(C)$, $I \neq 0$. Пусть $F \in I$, $F \neq 0$, тогда $[q_n,F] \in I$.

Если $F = \sum_{i\ge 0} u_i(q_1,\ldots,q_n,p_1,\ldots,p_{n-1})p_n^i$, то $[q_n,F] = \sum_{i\ge 0} u_i(q_1,\ldots,p_{n-1}) i p_n^{i-1}$, т.е. степень p_n уменьшилась. Продолжая эту операцию и дальше, мы вообще избавимся от p_n. Далее таким же образом мы можем избавиться от всех p_i, и, рассматривая $[p_i,F]$, мы можем избавиться от всех q_i. В итоге получим, что некая константа (не нулевая) принадлежит нашему идеалу. Следовательно, т.к. константа обратима, наш идеал совпадает со всей алгеброй. Т.е. алгебра проста. ◊

Предложение. Многочлены $q_1^{m_1}\cdot\ldots\cdot q_n^{m_n}\cdot p_1^{l_1}\cdot\ldots\cdot p_n^{l_n}$ линейно независимы в $A_n(C)$ при разных m_i, l_i.

Доказательство.

Действительно, если $F = \sum u_i(q_1,\ldots,q_n,p_1,\ldots,p_{n-1})p_n^i = 0$, то будем действовать аналогично доказательству предыдущей теоремы, т.е. $0 = [q_n,F] = \sum u_i(q_1,\ldots,p_{n-1}) i p_n^{i-1}$ и т.д. В итоге мы получим, что ненулевая константа должна равняться нулю, что невозможно. ◊

Следствие. Алгебра Вейля бесконечномерна.

Рассмотрим поле R. Над R мы знаем следующие тела:

1) R над R;
2) C над R;
3) H над R - поле кватернионов.

Сейчас мы докажем, что других тел нет (т.е. все тела изоморфны какому-то из этих).

Лемма. *Центр* H *равен* $R\cdot E$, *т.е. все матрицы с одинаковыми вещественными числами по диагонали.*

Доказательство.

Пусть $z=\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ - элемент центра. Тогда $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix}=\begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ для любых x и y. Т.е. получаем систему $\begin{cases} ax-b\overline{y}=ax-\overline{b}y \\ ay+b\overline{x}=bx+\overline{a}y \\ -\overline{b}x-\overline{a}\overline{y}=-a\overline{y}-\overline{b}\overline{x} \\ -\overline{b}y+\overline{a}\overline{x}=-b\overline{y}+\overline{a}\overline{x} \end{cases}$ на элементы a,b. Решая ее, получаем утверждение леммы. ◊

Определение. *Пусть* A *- ассоциативная алгебра с единицей над полем* k. *Элемент* $a\in A$ *называется* **алгебраическим**, *если существует многочлен* $f(T)\in k[T]$ *такой, что* $f(a)=0$. **Минимальным многочленом** *алгебраического элемента* a *называется многочлен наименьшей степени со страшим коэффициентом* 1 *такой, что* $f(a)=0$.

Упражнение. Пусть a - алгебраический элемент из A и I - все такие $g\in k[T]$, что $g(a)=0$. Докажите, что $I\lhd k[T]$ и $I=(f)$, где f - минимальный многочлен элемента a.

Теорема. *Пусть* $f\in k[T]$, *тогда* $\dim k[T]/(f)=\deg f$.

Доказательство.

Возьмем $h\in k[T]$, $h=fq+r$, где $\deg r<\deg f$, следовательно, $h+(f)=(fq+r)+(f)=r+(f)$. Следовательно, $k[T]/(f)=\langle 1+(f),T+(f),\ldots,T^{n-1}+(f)\rangle$, где $n=\deg f$. Если $\alpha_0(1+(f))+\ldots+\alpha_{n-1}(T^{n-1}+(f))=0+(f)$, то $\Bigl(\underbrace{\alpha_0+\alpha_1T+\ldots+\alpha_{n-1}T^{n-1}}_{u(T)}\Bigr)+(f)=0+(f)$. Следовательно, $u(T)\in(f)$, т.е. $u(T)=f\cdot v(T)$. Если $u(T)\neq 0$, то $n-1\geq\deg u=\deg f+\deg v=n+\deg v$, что невозможно. Следовательно $u(T)=0$, следовательно, все $\alpha_i=0$ и элементы $1+(f),\ldots,T^{n-1}+(f)$ независимы. ◊

Теорема. $k[T]/(f)$ *является полем тогда и только тогда, когда многочлен* f *неприводим.*

Доказательство.

$\Rightarrow$. Пусть f приводим, т.е. $f=uv$, где $\deg u,\deg v<\deg f$. Тогда $u+(f),v+(f)\neq 0$, и $[u+(f)][v+(f)]=uv+(f)=f+(f)=0+(f)$, т.е. есть делители нуля. Следовательно $k[T]/(f)$ не поле.

$\Leftarrow$. Пусть f неприводим и $g+(f)$ - ненулевой элемент. Тогда f не делит g, т.е. $(f,g)=1$. Следовательно $1=fh+gw$. Тогда $[w+(f)][g+(f)]=1+(f)$, т.е. каждый ненулевой элемент обратим. Следовательно $k[T]/(f)$ поле. ◊

Определение. *Пусть* A *- алгебра и* $a\in A$. *Множество* $k[a]=\{\lambda_0+\lambda_1a+\ldots+\lambda_na^n \mid \lambda_i\in k\}$ *называется* **подалгеброй, порожденной элементом** a.

Предложение. Пусть A - область (ассоциативная алгебра с единицей и без делителей нуля) и $a\in A$. Тогда минимальный многочлен f для a неприводим и $k[a]\cong k[T]/(f)$. В частности $k[a]$ является полем.

Доказательство.

Пусть $f = uv$, где $\deg u, \deg v < \deg f$. Тогда $0 = f(a) = u(a)v(a)$ при $u(a), v(a) \neq 0$, но в A нет делителей нуля. Получили противоречие, следовательно, f неприводим.

Рассмотрим $\Phi : k[T] \to A$, такой что $\Phi(h) = h(a)$. Тогда $\operatorname{Im}\Phi = k[a]$ и $\operatorname{Ker}\Phi = (f)$. По теореме о гомоморфизме получаем, что $k[a] \cong k[T]/(f)$ - поле. ◊

Предложение. Пусть A - конечномерное тело над R и $a \in A \setminus R$. Тогда $R[a] \cong C$.

Доказательство.

Пусть f - минимальный многочлен из $R[T]$ для a. Если $f = T - \lambda$, $\lambda \in R$, то $0 = f(a) = a - \lambda$, следовательно $a = \lambda \in R$, противоречие. Следовательно $f = T^2 + pT + q$ - неприводимый над R. Тогда $R[a] \cong R[T]/(f) \cong C$. (пусть c - комплексный корень f Тогда зададим $\Psi : R[T] \to C$, т.ч. $\Psi(h) = h(c)$ и воспользуемся т. о гомоморфизме). ◊

Теорема. *Пусть A - поле, являющееся конечномерной алгеброй над R. Тогда $A = R$ или $A = C$.*

Доказательство.

Пусть $A \neq R$, тогда (по предыдущему предложению) $A \supseteq C \supset R$. Пусть $z \in A$ и $f(T)$ - минимальный многочлен для z над C, тогда f неприводим. Следовательно $f = T - \mu$, где $\mu \in C$ и $0 = f(z) = z - \mu$, т.е. $z = \mu \in C$. Следовательно $A = C$. ◊

Теорема (Фробениуса). *Пусть A - конечномерное некоммутативное тело над R, тогда $A \cong H$.*

Доказательство.

Т.к. A некоммутативно, то $A \neq R$. Пусть $a \in A \setminus R$. Тогда $R[a] = C$, следовательно $A \supseteq C \supset R$. A является левым векторным пространством над C. Рассмотрим оператор $R_i(x) = xi$, это линейный оператор, т.к. $R_i((a+bi)x) = ((a+bi)x)i = (a+bi)(xi) = (a+bi)R_i(x)$ и $R_i^4(x) = id$. Т.е. нам задано комплексное представление группы $G = \langle a \rangle_4$, $a(x) = xi$. Рассмотрим множества:

$$\begin{aligned} A_1 &= \{x \mid R_i(x) = x\} \\ A_i &= \{x \mid R_i(x) = ix\} \\ A_{-1} &= \{x \mid R_i(x) = -x\} \\ A_{-i} &= \{x \mid R_i(x) = -ix\} \end{aligned}, \text{ тогда } A = A_1 \oplus A_i \oplus A_{-1} \oplus A_{-i}.$$

Если $x \in A_1$, то $xi = x$, т.е. $x(i-1) = 0$ Т.к. в A нет делителей нуля, то $x = 0$, т.е. $A_1 = \{0\}$. Аналогично $A_{-1} = \{0\}$. Следовательно $A = A_i \oplus A_{-i}$.

Лемма 1. $A_i = C$.

Доказательство.

Пусть $a \in A_i$, тогда $ai = ia$, следовательно $A_i \supseteq C$. Но A_i - подалгебра A, являющееся конечномерным расширением C. А мы уже знаем, что в этом случае $A_i = C$. ◊

Лемма 2. *Пусть $y \in A_{\varepsilon i}$, $z \in A_{\tau i}$, где $\varepsilon, \tau = \pm 1$. Тогда $yz \in A_{\varepsilon\tau i}$.*

Доказательство.

$(yz)i = y(zi) = y((\tau i)z) = \tau(yi)z = \tau\varepsilon iyz \Rightarrow yz \in A_{\tau\varepsilon i}$. ◊

Лемма 3. *Пусть $y \in A_{\varepsilon i}$, тогда $yA_{ei} = A_i$ и $yA_{-\varepsilon i} = A_{-i}$.*

Доказательство.

По предыдущей лемме $yA_{\varepsilon i} \subseteq A_{\varepsilon i}A_{\varepsilon i} \subseteq A_i$. Следовательно $\dim_R yA_{\varepsilon i} \leq \dim_R A_i \leq \dim_R yA_i \leq \dim_R A_{\varepsilon i}$. Но с другой стороны $\dim_R yA_{\varepsilon i} \geq \dim_R A_{\varepsilon i}$ (т.к. в A

нет делителей нуля). Следовательно все эти неравенства обращаются в равенства и $yA_{\varepsilon i} = A_i$. Аналогично доказываем, что $yA_{-\varepsilon i} = A_{-i}$. ◊

По лемме 1 имеем $A_i = C$ и $\dim_C A_i = 1$. Возьмем $j \in A_{-i}$, тогда $j^2 \in A_i = C$. Минимальный многочлен для j над R имеет степень 2. Следовательно $j^2 = a + bj$, где $a, b \in R$. Более того: $ij^2 = j^2 i$ (т.к. $j^2 \in A_i$) и $ij = -ji$ (т.к. $j \in A_{-i}$). Следовательно, $b = 0$. Т.е. получаем, что $j^2 = a \in R$, причем $a \neq 0$.

Если $a = d^2 > 0$, то $j^2 - d^2 = (j-d)(j+d) = 0$, т.е. $j \in R$, что невозможно.

Следовательно, $j^2 = -d^2$, где $d \in R$. Следовательно $\left(\frac{j}{d}\right)^2 = -1$. Пусть $J = \frac{j}{d}$, тогда $iJ = -Ji$ и $J^2 = -1$. Пусть $K = iJ$, тогда $K^2 = -1$, $Ki = -iK$ и $KJ - = JK$.

В итоге мы получили, что $A = A_i \oplus A_{-i} = C \oplus C_j = R \oplus R_i \oplus R_J \oplus R_K$. Т.е. мы получили группу кватернионов $A = H$ (правила умножения совпадают). ◊

Лекция 14

Определение. *Пусть A - область над полем* k *и $a \in A$. Элемент a называется* **алгебраическим**, *если $\exists f(t) \in \mathrm{k}[t]$, такой что $f(a) = 0$. Многочлен f, наименьшей степени со старшим коэффициентом 1, такой что $f(a) = 0$, называется* **минимальным аннулирующим** *многочленом для a.*

Если f - минимальный многочлен для a, то $k[a] \cong k[T]/(f)$.

Предложение. Если p ненулевой над k, тогда $\mathrm{k}[T]/(p)$ - поле. Элемент $a = T + (p)$ является корнем $p = p(T)$ в поле $\mathrm{k}[T]/(p)$.

Доказательство.

Пусть $p(T) = \alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n$, $\alpha_i \in \mathrm{k}$. Тогда

$$p(a) = \alpha_0 + \alpha_1 (T + (p)) + \ldots + \alpha_n (T + (p))^n = \alpha_0 + \alpha_1 T + \ldots + \alpha_n T^n + (p) = p + (p) = 0 + (p).\ ◊$$

Следствие. Пусть $f \in \mathrm{k}[T]$ - произвольный. Тогда существует поле $\mathrm{K} \supseteq \mathrm{k}$, в котором многочлен f имеем корень.

Здесь K называется **расширением** поля k, записывается это как K/k.

Определение. *Пусть $f \in \mathrm{k}[T]$ и $\deg f \geq 1$. Поле K/k называется* **полем разложения** *для f, если:*

1) над K многочлен f разлагается на линейные множители;

2) никакое промежуточное поле K' ($\mathrm{K} \supset \mathrm{K}' \supseteq \mathrm{k}$) этим свойством не обладает.

Теорема. *Пусть $f \in \mathrm{k}[T]$ и $\deg f \geq 1$. Тогда:*

1) поле разложения K/k существует;

2) если K_1 и K_2 - поле разложения для f, то K_1 и K_2 изоморфны как k-алгебры.

Доказательство.

1) Существование (доказательство по индукции).

Если $\deg f = 1$, то $\mathrm{K} = \mathrm{k}$.

Пусть теперь $\deg f = n \geq 2$ и для всех меньших степеней существование поля разложения уже доказано. Разложим f на неприводимые многочлены $f = p_1 \cdot \ldots \cdot p_m$, p_i - неприводим. $F = {k[T]}/{(p_1)}$ снова поле, и в нем многочлен p_1 имеет корень α. Тогда в этом поле $f = (T-\alpha) f_1$, где $\alpha \in F$, $f_1 \in F[T]$ и $\deg f_1 = n-1 < n$. По предположению индукции, существует K/F - поле разложения для f_1. Следовательно K/F будет полем разложения для f.

2) Единственность (тоже по индукции).

Если $\deg f = 1$, то поле разложения единственно и равно k.

Если $\deg f = n$. Пусть $f = p_1 \cdot \ldots \cdot p_m$. Пусть α_1 и α_2 - корни p_1 в полях K_1 и K_2 соответственно. Тогда $k[\alpha_1] \cong {k[T]}/{(p_1)} \cong k[\alpha_2]$. Без ограничения общности можно считать, что $k[\alpha_1] = k[\alpha_2]$ и $\alpha_1 = \alpha_2$. Тогда K_1 и K_2 - поля разложения многочлена $\dfrac{f}{(T-\alpha_1)}$ над $k[\alpha_1]$. По предположению индукции поля K_1 и K_2 совпадают. ◊

Вспомним из первого семестра, что, если F - поле, то $\operatorname{char} F$ либо 0, либо простое число. Если характеристика равно нулю, то поле содержит в себе поле рациональных чисел. Если характеристика равна p, то поле содержит в себе поле вычетов по модулю p.

Теорема. *Пусть* F *- конченое поле и* $\operatorname{char} F = p$*, тогда* $|F| = p^n$.

Доказательство.

Т.к. $F \supseteq \mathbf{Z}_p$, то F является векторным пространством над $\mathbf{Z}$ размерности n. Пусть $e_1, \ldots, e_n$ - базис в F над $\mathbf{Z}_p$. Следовательно, $x \in F \Leftrightarrow x = x_1 e_1 + \ldots + x_n e_n$, где $x_i \in \mathbf{Z}_p$. Следовательно $|F| = p^n$. ◊

Предложение. Пусть F - поле характеристики p. Тогда $\forall x, y \in F$, $\forall m \geq 1$ $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.

Доказательство.

Докажем сначала для степени p. По биному Ньютона

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \ldots + \binom{p}{t} x^{p-t} y^t + \ldots + y^p.$$

Биноминальный коэффициент $\binom{p}{t}$ равен $\dfrac{p!}{t!(p-t)!} \in \mathbf{Z}$. Причем $p! \vdots p$, а $t!(p-t)! \not\vdots\, p$, следовательно, $\binom{p}{t} \vdots\, p$. Т.е. в поле $\mathbf{Z}_p$ этот коэффициент равен нулю. Следовательно $(x+y)^p = x^p + y^p$.

В общем случае ($m > 1$) имеем:

$$(x+y)^{p^m} = \left[(x+y)^p\right]^{p^{m-1}} = \left(x^p + y^p\right)^{p^{m-1}} = \left[\left(x^p + y^p\right)^p\right]^{p^{m-2}} = \left(x^{p^2} + y^{p^2}\right)^{p^{m-2}} = \ldots = x^{p^m} + y^{p^m}. \ ◊$$

Теорема. *Если* F *- поле из* q *элементов и* $x \in F$*, то* $x^q = x$.

Доказательство.

Пусть $x \neq 0$. Тогда $x \in F^* = F \setminus \{0\}$. Но F^* - группа по умножению порядка $q-1$, следовательно, $x^{q-1} = 1$, следовательно, $x^q = x$.

Если $x = 0$, то утверждение очевидно. ◊

Теорема. *Пусть* $q = p^n$*, где* p *- просто, тогда существует (и оно единственно) поле* F_q *и* q *элементов.*

Доказательство.

Рассмотрим поле $\mathbf{Z}_p$ и многочлен $f = x^q - x \in \mathbf{Z}_p[x]$. Пусть F_q - поле разложения для f. Пусть α и β - корни f, тогда $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, т.е. $\alpha\beta$ - тоже корень f. По доказанному выше предложению $(\alpha+\beta)^q = \alpha^q + \beta^q$, т.е. $\alpha+\beta$ - тоже корень f. Аналогично проверяем, что α^{-1} и $(-\alpha)$ тоже будут корнями f.

Если $z \in \mathbf{Z}_p$, то $z^p = z$, следовательно, и $z^q = z$. Все корни f образуют подполе. Следовательно F_q совпадает с множеством всех корней многочлена f. У многочлена f нет кратных корней, т.к. $f' = -1$ и $(f, f') = 1$ - взаимопросты. Следовательно $|\mathrm{F}_q| = q$. Единственность поля следует из единственности поля разложения для многочлена. ◊.

Теорема. *Пусть* F *- поле и* G *- конечная подгруппа в* F^*. *Тогда* G *- циклическая.*

Доказательство.

$G = S_1 \times \ldots \times S_m$, где S_i - силовская p_i - подгруппа. Нам достаточно доказать, что каждая S_i циклическая. $|S_k| = p^d$, где p - простое число. Пусть элемент $x \in S_k$ имеет максимальный порядок (p^M). Тогда $x^{p^M} = 1$ или $x^{p^M} - 1 = 0$. Рассмотрим многочлен $T^{p^M} - 1 \in \mathrm{F}[T]$. Любой элемент $y \in S_k$ имеет порядок p^N, где $N \le M$. Следовательно, $y^{p^N} - 1 = 0$ и $y^{p^M} - 1 = 0$. Т.е. все элементы S_k являются корнями многочлена $T^{p^M} - 1 = 0$. Но и всего p^M, следовательно, $M = d$ и порядок элемента x совпадает с порядком всей группы. Следовательно, группа S_k циклическая, порожденная элементом x. Следовательно и вся группа G циклическая. ◊

Следствие. $(\mathrm{F}_q)^*$ - циклическая группа.

Следствие. Пусть F_q - поле и $q = p^n$. Тогда существует многочлен $\tilde{p} \in \mathbf{Z}_p[T]$ степени n такой, что $F_q \cong Z_p[T]/(\tilde{p})$.

Доказательство.

$(F_q)^* = \langle a \rangle \Rightarrow Z_p[a] \cong Z_p[T]/(\tilde{p})$, где $\tilde{p}$ - минимальный аннулирующий многочлен. ◊

Теорема. *Группа автоморфизмов* F_q*, где* $q = p^n$ *является циклической группой порядка* n.

Доказательство.

Пусть ϕ - автоморфизм F_q, тогда $\phi(0) = 0$, $\phi(1) = 1$, $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 2$, т.е. $\phi(m) = m$, если $m \in \mathbf{Z}_p$. Тогда $F_q = Z_p[a] \cong Z_p[T]/(f)$, где f - минимальный аннулирующий многочлен для a, $\deg f = n$. Пусть $f(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_{n-1}a^{n-1} + a^n = 0$, тогда $f(\phi(a)) = \alpha_0 + \alpha_1\phi(a) + \ldots + \alpha_{n-1}\phi(a)^{n-1} + \phi(a)^n = 0$. Для $\phi(a)$ имеется не более n значений. Следовательно, существует не более n автоморфизмов F_q.

Укажем автоморфизм порядка n. $\xi(x) = x^p$, тогда $\xi(x+y) = \xi(x) + \xi(y)$ и $\xi(xy) = \xi(x)\xi(y)$. Тогда $\xi^n(x) = x^{p^n} = x$, т.е. ξ^n - тождественный автоморфизм. Если порядок ξ равен

$m < n$, то $x^{p^m} = x \;\; \forall x \in \mathrm{F}_q$ и тогда в поле F_q будет всего $p^m < p^n = q$ элементов. Следовательно, порядок ξ равен n и $Gal_{\mathbf{Z}_p}\left(\mathrm{F}_q\right) = \langle \xi \rangle_n$. ◊

АЛГЕБРЫ ЛИ

Определение. *Алгебра с умножением* $[x, y]$ *называется* **алгеброй Ли***, если это умножение не ассоциативно, антикоммутативно и выполняется тождество* $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$.

Примеры:

1) Пусть A - ассоциативная алгебра с умножением xy, тогда введем умножение $[x, y] = xy - yx$. Относительно этого нового умножения наша алгебра будет алгеброй Ли.

2) $sl(n, \mathrm{k})$ - множество матриц размера $n \times n$ над полем k со следом ноль. Операция умножения $[x, y] = xy - yx$, где xy - обычное матричное умножение.

3) $o(n, \mathrm{k})$ - множество кососимметричных матриц. Умножение $[x, y] = xy - yx$.

4) R^3, операция умножения - векторное произведение $x \times y$.

Определение. *Пусть* A *- алгебра.* **Дифференцированием** *на* A *называется линейный оператор* ∂, *такой что* $\partial(ab) = \partial(a)b + a\partial(b)$.

Упражнение. Если ∂_1 и ∂_2 - дифференцирования в алгебре A, то их коммутатор $[\partial_1, \partial_2] = \partial_1\partial_2 - \partial_2\partial_1$ - снова дифференцирование. И все дифференцирования образуют алгебру Ли.

Рассмотрим алгебру Ли $sl(2, C) = \left\{ \begin{pmatrix} x & z \\ y & -x \end{pmatrix} \mid x, y, z \in C \right\}$, построим в ней базис: $H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ и $Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Упражнение. Докажите, что $[X, Y] = H$, $[H, X] = 2X$, $[H, Y] = -2Y$.

Теорема. *Алгебра Ли* $sl(2, C)$ *проста.*

Доказательство.

Пусть $I \lhd sl(2, C)$ - ненулевой идеал, и пусть $u = \alpha X + \beta Y + \gamma H \in I \setminus \{0\}$ - ненулевой элемент.

1) Если $\alpha \neq 0$, тогда $[X, [X, u]] = -2\alpha X$. Следовательно, $X \in I \Rightarrow H \in I \Rightarrow Y \in I$ и $I = sl(2, C)$.

2) Если $\beta \neq 0$, то $[Y, [Y, u]] = 2\beta Y$, далее аналогично получаем, что $I = sl(2, C)$.

3) Если $\gamma \neq 0$ и $\alpha = \beta = 0$, то $H \in I$, а, следовательно, и $X, Y \in I$. И опять $I = sl(2, C)$. ◊

Упражнение. $(R^3, \times)$ - простая алгебра Ли.

Лекция 15.
Кольцо многочленов

Пусть K - коммутативное кольцо с единицей 1, A - некоторое его подкольцо, содержащее 1. Если $t \in K$, то наименьшее подкольцо в K, содержащее A и t, будут состоять из элементов вида

$$a(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n, \qquad (*)$$

где $a_s \in A$, $n \in Z$, $n \geq 0$. Мы обозначим его $A[t]$ и назовем кольцом, полученным из A присоединением элемента t, а выражение **(*)** - многочленом от t с коэффициентами в A. Что понимать под суммой и произведением многочленов, видно из простейших примеров (скажем, при $n=2$):

$$a(t)+b(t)=(a_0+a_1t+a_2t^2)+(b_0+b_1t+b_2t^2)=(a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2,$$

$$a(t)\cdot b(t)=a_0b_0+(a_0b_1+a_1b_0)t+(a_0b_2+a_1b_1+a_2b_0)t^2+(a_1b_2+a_2b_1)t^3+a_2b_2t^4.$$

Очевидно, что приведение подобных членов основано на попарной перестановочности всех элементов a_i, b_j, t^k.

Вспомним, что t - наугад взятый элемент кольца K, и поэтому внешне различные выражения **(*)** могут на самом деле совпадать. Если, скажем, $A=Q$, $t=\sqrt{2}$, то $t^2=2$ и $t^3=2t$ - соотношения, которые никоим образом не вытекают из формальных правил.

Многочлены от одной переменной. Пусть A - произвольное коммутативное кольцо с единицей. Построим новое кольцо B, элементами которого являются бесконечные упорядоченные последовательности

$$f=(f_0, f_1, f_2, \dots), \qquad f_i \in A, \tag{1}$$

такие, что все f_i, кроме конечного их числа, равны нулю. Определим на множестве B операции сложения и умножения, полагая

$$f+g=(f_0, f_1, f_2, \dots)+(g_0, g_1, g_2, \dots)=(f_0+g_0, f_1+g_1, f_2+g_2, \dots),$$

$$f\cdot g=h=(h_1, h_2, h_3 \dots),$$

где

$$h_k=\sum_{i+j=k} f_i g_j, \qquad k=0,1,2,\dots$$

Ясно, что в результате сложения и умножения получаются снова последовательности вида (1) с конечным числом отличных от нуля членов, т.е. элементы из B. Проверка всех аксиом кольца, кроме, разве, аксиомы ассоциативности, очевидна. В самом деле, поскольку сложение двух элементов из B сводится к сложению конечного числа элементов из кольца A, $(B,+)$ является коммутативной группой с нулевым элементом $(0,0,0,\dots)$ и элементом $-f=(-f_0,-f_1,-f_2,\dots)$, обратным к произвольному $f=(f_0,f_1,f_2,\dots)$.

Определение. Введённое выше кольцо B обозначается через $A[X]$ и называется кольцом многочленов над A от одной переменной X, а его элементы- многочленами.

Элементы f_i (и a_i) называются коэффициентами многочлена f. Многочлен f нулевой, когда все его коэффициенты равны нулю. Коэффициент f_0 при X в нулевой степени называется ещё постоянным членом. Если $f_n \neq 0$, то f_n называют старшим коэффициентом, а n - степенью многочлена и пишут $n=\deg f$. Нулевому многочлену приписывается степень $-\infty$. Многочлены степени $1,2,3,\dots$ называются соответственно линейными, квадратичными, кубичными и т.д.

Теорема 1. Если A - целостное кольцо, то и кольцо $A[X]$ является целостным.

Место кольца многочленов среди коммутативных колец отчасти поясняет следующая

Теорема 2. Пусть коммутативное кольцо K содержит A в качестве подкольца. Для каждого элемента $t \in K$ существует единственный гомоморфизм колец $\Pi_t : A[X] \to K$ такой, что

$$\forall a \in A \qquad \Pi_t(a)=a, \qquad \Pi_t(X)=t. \tag{2}$$

Доказательство. Предположим сначала, что такой гомоморфизм Π_t существует. Так как $\Pi_t(f_i)=f_i$ для каждого коэффициента многочлена f и $\Pi_t(X^k)=(\Pi_t(X))^k=t^k$, то

$$\Pi_t(f)=\Pi_t(f_0+f_1X+\dots+f_nX_n)=f_0+f_1X+\dots+f_nt^n, \tag{3}$$

т.е. $\Pi_t(f)$ определён однозначно и выражается формулой (3). Обратно: задав отображения Π_t формулой (3), мы удовлетворим условию (2) и получим гомоморфизм колец. Это ясно для отображения аддитивных групп колец, а что касается умножения, то применение Π_t к произведению

$$fg = f_0 g_0 + (f_0 g_1 + f_1 g_0)X + \ldots + (f_n g_m)X^{n+m}, \qquad (4)$$

а затем использование закона дистрибутивности даёт

$$\Pi_t(fg) = f_0 g_0 + (f_0 g_1 + f_1 g_0)X + \ldots + (f_n g_m)X^{n+m} =$$

$$= \left(\sum_{i=0}^{n} f_i t^i\right)\left(\sum_{j=0}^{m} g_j t^j\right) = \Pi_t(f)\cdot\Pi_t(g).$$

Результат применения отображения Π_t определённого формулой (3), к многочлену $f = f(X)$ называется подстановкой t и f вместо X или просто значением f при $X = t$, так что $\Pi_t(f) = f(t)$. Значить $\Pi_t(f)$ - значит уметь вычислить значение f при $X = t$.

Элемент $t \in K$ называется алгебраическим над A, если $\Pi_t(f) = 0$ для некоторого $f \in A[X]$. Если же $\Pi_t : A[X] \to K$ - изоморфное вложение, то t - трансцендентный над A элемент.

Теорема 3. Пусть A и K - произвольное коммутативные кольца, t - элемент из K и $A \to K$ - гомоморфизм.

Тогда существует, и притом единственное, продолжение φ до гомоморфизма $\varphi_t : A[X] \to K$ кольца многочленов $A[X]$ в K, переводящего переменную X в t.

Доказательство является незначительным видоизменением доказательства теоремы 2 и оставляется читателю в качестве упражнения.

Многочлены от многих переменных. Конструкция кольца $B = A[X]$ включала произвольное коммутативное кольцо A с единицей. Мы можем теперь заменить в нашей конструкции кольцо A на B и построить кольцо $C = B[Y]$, где Y - новая независимая переменная, играющая по отношению к B ту же роль, что и X по отношению к A. Элементы из C однозначно записываются в виде $\sum b_j Y^j, b_j \in B$, причём B отождествляется с подкольцом в C, а именно с множеством элементов $bY^0 = b\cdot 1$. Так как в свою очередь $b_j = \sum a_{ij} X^i$ - однозначная запись элементов $b_j \in B$, то любой элемент из C имеет вид

$$\sum_{i=0}^{k}\sum_{j=0}^{l} a_{ij} X^i Y^j, \qquad a_{ij} \in A,$$

причём подразумевается, что a_{ij} перестановочны с X и Y, а переменная X перестановочна с Y. Кольцо C называется кольцом многочленов над A от двух независимых переменных X и Y.

Повторив достаточное число раз эту конструкцию, мы получим кольцо $A[X_1,\ldots,X_n]$ многочленов над A от n независимых переменных $X_1,\ldots,X_n$.

Многочлен f равен нулю тогда и только тогда, когда равны нулю все его коэффициенты $a_{i_1\ldots i_n}$. При $n = 1$ это уже отмечалось в ходе построения кольца $A[X]$, а при $n > 1$ проще всего использовать индукцию по n.

Под степенью многочлена f относительно X_k понимается наибольшее целое число, обозначаемое $\mathbf{deg}_k f$, которое встречается в качестве показателя при X_k в $a_{(i)}X^{(i)}$ с $a_{(i)} \neq 0$.

Целое число $i_1 + \ldots + i_n$ называется (полной) степенью одночлена $X_1^{i_1}\ldots X_n^{i_n}$.

На кольцо $A[X_1,\ldots,X_n]$ переносятся многие результаты, полученные нами в п. 1 для $A[X]$. Например, опираясь на теорему 1 и используя индукцию по n, мы сразу же убеждаемся а том, что справедлива

Теорема $\mathbf{1}'$. Если A - целостное кольцо, то и кольцо $A[X_1,\dots,X_n]$ является целостным. В частности, кольцо многочленов от n переменных над любым полем P целостно.

Полезным уточнением теоремы $\mathbf{1}'$ служит

Теорема 4. Пусть f и g - произвольные многочлены от n переменных над целостным кольцом A. Тогда

$$\mathbf{deg}(fg) = \mathbf{deg}\, f + \mathbf{deg}\, g.$$

Алгоритм деления с остатком.

Теорема 5. Пусть A - целостное кольцо и g - многочлен в $A[X]$ со старшим коэффициентом, обратимым в A. Тогда каждому многочлену $f \in A[X]$ сопоставляется одна и только одна пара многочленов $q, r \in A[X]$, для которых

$$f = qg + r, \qquad \mathbf{deg}\, r < \mathbf{deg}\, g. \qquad (5)$$

Доказательство. Пусть

$$f = a_0 X^n + a_1 X^{n-1} + \dots + a_n,$$
$$g = b_0 X^m + b_1 X^{m-1} + \dots + b_m,$$

где $a_0 b_0 \neq 0$ и $b_0 \mid 1$. Применим индукцию по n. Если $n = 0$ и $m = \mathbf{deg}\, g > \mathbf{deg} f = 0$, то положим $q = 0, r = f$, а если $n = m = 0$, то $r = 0$ и $q = a_0 b_0^{-1}$. Допустим, что теорема доказана для всех многочленов степени $< n$ $(n > 0)$. Без ограничения общности считаем $m \le n$, поскольку в противном случае возьмём $q = 0, r = f$. Раз это так, то

$$f = a_0 b_0^{-1} X^{n-m} \cdot g + \bar{f},$$

где $\mathbf{deg}\bar{f} < n$.

Обращаясь к свойству единственности частного q и остатка r, предположим, что

$$qg + r = f = q'g + r'.$$

Тогда $(q' - q)g = r - r'$. По теореме 1 имеем $\mathbf{deg}(r - r') = \mathbf{deg}(q' - q) + \mathbf{deg}\, g$, что в наших условиях возможно только при $r' = r$ и $q' = q$.

Наконец, приведённые рассуждения показывают, что коэффициенты частного q и остатка r принадлежит тому же целостному кольцу A, т.е. $f, g \in A[X] \Rightarrow q, r \in A[X]$.

Замечание. Многочлены со старшим коэффициентом 1 часто называют нормализованными. Указанный выше процесс деления многочлена f на g, называемый евклидовым, несколько упрощается, если g - нормализованный многочлен. Говорят, что f делится на g, если остаток r равен нулю: $f = qg$.

Разложение в кольце многочленов. Обратимые элементы в K были названы нами делителями единицы. Часто их именуют ещё регулярными элементами. Совершенно очевидно, что многочлен $f \in A[X]$ обратим в точности тогда, когда $\mathbf{deg} f = 0$ и $f = f_0$ - обратимый элемент кольца A, поскольку $f\,g = 1 \Rightarrow \mathbf{deg} f + \mathbf{deg}\, g = \mathbf{deg}\, 1 = 0$.

Говорят, что элемент $b \in K$ делится на $a \in K$, если существует такой элемент $c \in K$, что $b = ac$. Если $a \mid b$ и $b \mid a$, то a и b называются ассоциированными элементами.

Элемент $p \in K$ называется простым, если p необратим и его нельзя представить в виде $p = ab$, где a, b - необратимые элементы. В поле P каждый ненулевой элемент обратим и в чаще неприводимым многочленом.

Отметим следующие основные свойства отношения делимости в целостном кольце K.

1) Если $a \mid b$, $b \mid a$, то $a \mid c$. Мы имеем $b = ab', c = bc'$, где $b', c' \in K$. Поэтому $c = (ab')c' = a(b'c')$.

2) Если $c \mid a$ и $c \mid b$, то $c \mid (a \pm b)$. В самом деле, по условию $a = ca', b = cb'$ для некоторых $a', b' \in K$, и ввиду дистрибутивности $a \pm b = c(a' \pm b')$.

3) Если $a \mid b$, то $a \mid bc$. Ясно, что $b = ab' \Rightarrow bc = (ab')c = a(b'c)$.

Комбинируя 2) и 3), получаем

4)Если каждый из элементов $b_1, b_2, \ldots, b_m \in K$ делится на $a \in K$, то на a будет делиться также элемент $b_1c_1 + b_2c_2 + \ldots + b_mc_m$, где $c_1, c_2, \ldots, c_m$ - произвольные элементы.

Теорема 6. Пусть K - произвольное целостное кольцо с разложением на простые множители. Однозначность разложения в K имеем место тогда и только тогда, когда любой простой элемент $p \in K$, делящий произведение $ab \in K$, делит по крайней мере один из множителей a и b.

НОД и НОК в кольцах. Пусть K -целостное кольцо. Под наибольшим общим делителем двух элементов $a, b \in K$ мы будем понимать элемент $d \in K$, обозначаемый НОД(a,b) и обладающий двумя свойствами:

$i)$ $d \mid a$, $d \mid b$;

$ii)$ $c \mid a$, $c \mid b \Rightarrow c \mid d$.

$iii)$ НО $iv)$ Д$(a,b) = a \Leftrightarrow a \mid b$;

$iv)$ НОД$(a, 0) = a$;

$v)$ НОД$(ta, tb) = t$ НОД(a,b);

$vi)$ НОД (НОД(a,b),c) = НОД (a,НОД(b,c)).

Теорема 7. Пусть для элементов a, b целостного кольца K существуют НОД(a,b) и НОК(a,b).

Тогда:

а) НОК$(a,b) = 0 \Leftrightarrow a = 0$ или $b = 0$.

б) $a, b \neq 0, m =$ НОК(a,b), $ab = dm \Rightarrow d =$ НОД(a,b).

Признак делимости. Пусть a, b - элементы факториального кольца K, записанные в виде

$$a = up_1^{k_1} \ldots p_r^{k_r}, \qquad b = vp_1^{l_1} \ldots p_r^{l_r},$$
$$u \mid 1, \quad v \mid 1; \quad k_i \geq 0, \quad l_i \geq 0; \quad p_i \in P; \qquad 1 \leq i \leq r. \tag{6}$$

Справедливы утверждения:

1) $a \mid b$ тогда и только тогда, когда $k_i \leq l_i$, $i = 1, 2, \ldots, r$;

2) НОД$(a,b) = p_1^{s_1} \ldots p_r^{s_r}$, где $s_i = \min\{k_i, l_i\}$, $i = 1, 2, \ldots, r$;

3) НОК$(a,b) = p_1^{t_1} \ldots p_r^{t_r}$, где $t_i = \max\{k_i, l_i\}$, $i = 1, 2, \ldots, r$;

Таким образом, в качестве s_i нужно брать наименьший из двух показателей k_i, l_i, а в качестве t_i -наибольший. В частности, элементы $a, b \in K$ взаимно просты в точности тогда, когда простые множители, входящие в разложение одного элемента, не входят в разложение другого.

Факториальность евклидовых колец. Алгоритм деления с остатком в Z и $P[X]$ делает естественным рассмотрение целостного кольца K, в котором каждому элементу $a \neq 0$ поставлено в соответствие неотрицательное целое число $\delta(a)$, т.е. определено отображение

$$\delta : K \setminus \{0\} = K^* \to N \cup \{0\}$$

так, что при этом выполняются условия:

$E1)$ $\delta(ab) \geq \delta(a)$ для всех $a, b \neq 0$ из K.

$E1)$ каковы бы ни были $a, b \in K$, $b \neq 0$, найдутся $q, r \in K$, для которых

$$a = qb + r; \qquad \delta(r) < \delta(b) \qquad \text{или} \qquad r = 0 \tag{7}$$

Целостное кольцо K с этими свойствами называется евклидовым кольцом. Полагая $\delta(a) = |a|$ для $a \in Z$ и $\delta(a) = \deg a$ для $a = a(X) \in P[X]$, мы приходим к выводу, что Z и $P[X]$ - евклидовы кольца.