φ – самосопряженное. Оно наз. неотрицательным, если все собственные числа неотрицательны. Если все собственные числа строго положительные, то φ наз. положительным.

Теорема. Для любого неотрицательного самосопряженного преобразования существует корень квадратный, причем единственный.

$\forall$ φ неотр. $\exists$ единтсв. неотр. ψ / $\psi^2=\varphi$

Д-во: 1) $\exists$ $e_1,...,e_n$ - базис из собственных векторов. $\lambda_1,...,\lambda_n$ - собственные числа.

Пусть $\mu_j = \pm\sqrt{\lambda_j}$ (j=1,..,n).

Преобразование ψ определим следующим образом: $\psi e_j = \mu_j e_j$

$\psi^2 e_j = \psi(\psi e_j) = \psi(\mu_j e_j) = \mu_j^2 e_j = \lambda_j e_j$

2) λ_j - различные собственные числа

d_j - геометрическая кратность λ_j, n_j - алгебраическая кратность

Для унитарного преобразования, а значит и для самосопряженного $d_j = n_j$ и $\sum_{j=1}^{m} d_j = n$

$(\varphi-\lambda_j \varepsilon)x=0$ x – собственный вектор $x \in \mathrm{Ker}\varphi$

$\mathrm{Ker}(\varphi-\lambda_j \varepsilon)=W_j$ $V= W_1 \oplus ... \oplus W_m$ - прямая.

$x \in \mathrm{Ker}(\psi-\mu_j \varepsilon)$ (Для него $d'_j = n'_j$). А тогда $x \in \mathrm{Ker}(\varphi-\lambda_j \varepsilon)$

Имеем $n= n_1 + ... + n_m$, $n= n'_1 + ... + n'_m$ и $n'_j \le n_j$ (j=1,..,m). Отсюда $n'_j = n_j$

Т.о. корень единственный, т.к. ядра совпадают.

Теорема. Любое невырожденное преобразование φ можно представить единственным образом φ=ψχ, где ψ- положительное самосопряженное преобразование и χ – унитарное

Д-во: $\varphi^* = \chi^* \psi^*$

$\varphi\varphi^* = \psi\chi\chi^*\psi^* = \psi^2$

$(\varphi x, \varphi x) > 0$ $\forall x \neq 0$ φ – невырожденное.

Все собственные числа положительные, следовательно $\varphi\varphi^*$ - неотрицательное самосопряженное. Следовательно по предыдущей теореме можно извлечь корень из этого преобразования.

Легко проверить, что $\chi = \psi^{-1}\varphi$ – унитарное.

Единственность следует из единственности квадратного корня.

АБСТРАКТНАЯ АЛГЕБРА

О. Алгебраическая система (алгебра, абстрактная алгебра) – это множество M, на котором заданы бинарные операции (1),…,(s)

$\forall$ (i) $a \in M$ и $b \in M$ следует, что $a(i)b \in M$ $\Leftrightarrow$ {M, (1),…,(s)} – замкнутая

Пример

{N,+,-,*} – незамкнутая система

{Z,+,-,*} – замкнутая система

О. Подалгебра – это алгебра {M', (1),…,(s)}, где M' – подмножество M и {M', (1),…,(s)} – замкнута.

Заметим, что пересечение подалгебр есть подалгебра. (док-ся тривиально)

О. Гомоморфизм. Пусть даны две алгебры {M, (1),…,(s)} и {M', [1],…,[s]}.

Если существует отображение φ: M→M', сохраняющее операции, т.е. i=1,..,s $\varphi(a(i)b)=\varphi a[i]\varphi b$.

{φ(M), [1],…,[s]} – гомоморфный образ

Если φ – биекция, то гомоморфизм наз. изоморфизмом.

Лемма. Гомоморфный образ алгебры есть алгебра.

Д-во: Рассмотрим гомоморфный образ алгебры M. Докажем, что он замкнут относительно операций второй алгебры. $\forall a,b \in \varphi(M)$ $\exists a', b' \in M / \varphi(a')=a, \varphi(b')=b$ => $a[i]b=\varphi(a(i)\varphi(b))$ => $a[i]b \in \varphi(M)$, т.е. замкнуто.

Если число операций s=1, то алгебра наз. моноидом

О. Моноид наз. полугруппой, если операция ассоциативна, т.е. (ab)c=a(bc)

Теорема 1. (об обобщенной ассоциативности) (см. 1 семестр)

О. Полугруппа наз. коммутативной (**абелевой**), если ab=ba.

Пример не абелевой полугруппы - полугруппа матриц.

Теорема 2. (об обобщенной коммутативности) (см .1 семестр)

Рассмотрим два моноида (M, ○) и (M', □)

Теорема. Если первый – полугруппа, то гомоморфный образ (φM, □) есть полугруппа.

Д-во: a', b', c' $\in$ φM => $\exists$ a, b, c $\in$ M / φa=a', φb=b', φc=c'

a'□(b'□c')=(a'□b')□c'

a'□(b'□c')=φa□(φb□φc)=φa□φ(b○c)=φ(a○(b○c))=φ((a○b)○c)=φ(a○b)□φc=(φa□φb)□φc=(a'□b')□c'

О. e – левый нейтральный элемент, если ea=a $\forall$ a $\in$ M

e' – правый нейтральный элемент, если ae'=a $\forall$ a $\in$ M

Лемма 1. Если в полугруппе есть левый и правый нейтральный элементы, то они равны и единственные. Если она мультипликативная – то 1, если аддитивная – 0.

Д-во: e=ee'=e'

Если ab=e, то b наз. правый обратный (в аддитивной - противоположный). Аналогично – левый.

Лемма 2. Если в абелевой полугруппе существуют правый и левый обратный, то они совпадают и единственные.

Д-во: b=eb=(ca)b=c(ab)=ce=c

О. G –группа, если 1) оно содержит e, 2) для любого элемента существует обратный.

Лемма. $\left.\begin{matrix} ax=b \\ ya=b \end{matrix}\right\}$(3) в группе имеет единственное решение

!!! **В любой группе из ax=ax' следует, что x=x'**

Теорема. Если в непустой полугруппе уравнения (3) имеют решение, то она группа.

Д-во: a $\in$ M

Рассмотрим ax=a, для него x_a - решение. x_a=e' – это правая единица. Докажем, что bx_a=b

bx_a=(ya)x_a=y(ax_a)=ya=b

ya=a y_a=e – аналогично левая единица. Следовательно по лемме это просто единица.

Рассмотрим ax=e, ya=e => сущ. обратный. Т.о. это группа.

О. Полугруппа наз. полугруппой с сокращениями, если из ax=ax' следует, что x=x', а из ya=y'a => y=y'.

Лемма. Если G – конечная полугруппа с сокращением {|G|< ∞}, тогда она группа.

Д-во: G={ $g_1,...,g_n$ }

$g_iG = \{g_ig_1,...,g_ig_n\} \subseteq G$, т.к. замкнуто. Но все элементы различны (следует из определения), а всего их n штук, следовательно $g_iG = G$

Отсюда $\forall$ j $\exists$ k / $g_ig_k = g_j$ Т.о. каждое уравнение ax=b имеет решение. (a= g_i, b= g_k)

Для ya=b аналогично: $Gg_i = G$

Рассмотрим Ø≠H$\subseteq$G

Теорема. Непустое множество H в группе является подгруппой, если:

а) a $\in$ H и b $\in$ H => ab $\in$ H

и б) a $\in$ H => $a^{-1} \in$ H

в) a $\in$ H и b $\in$ H => $ab^{-1} \in$ H

г) |H|< ∞ + (a)

Д-во: ассоциативность в H следует из ассоциативности в G.

а) и б) H – непустое, следовательно, $\exists$ a $\in$ H => из пункта б) следует, что $\exists a^{-1} \in$ H => e $\in$ H. По опред. H – группа.

в) H - непустое => $\exists$ a $\in$ H => $aa^{-1} \in$ H, т.е. e $\in$ H

Если b $\in$ H, то b^{-1}=$eb^{-1} \in$ H. Следовательно H – группа (она замкнута!).

г) Следует из предыдущей теоремы, т.к. H – полугруппа с сокращениями. Любая группа – полугруппа с сокращениями.

Лемма. Пересечение подгрупп есть подгруппа. (д-во самостоятельно)

Рассмотрим два моноида {M, ○} и {N, □}

Пусть φ – гомоморфизм, φ:M→N, т.е. φa□φb=φ(a○b)

В таком случае полугруппа переходит в полугруппу, левый (правый) нейтральный элемент переходит в левый (правый) нейтральный элемент, левый (правый) обратный в левый (правый) обратный, группа перейдет в группу.

$e \in M$, т.е. $e \circ a = a \ \forall a \in M \Rightarrow \varphi e \square \varphi a = \varphi(e \circ a) = \varphi a \Rightarrow \varphi e$ – левый нейтральный в N

остальное доказывается аналогично

Легко доказывается, что гомоморфный образ группы – это группа.

Рассмотрим F_M - множество всех биекций (группа).

Теорема Кэли. Для любой группы G существует H - подгруппа F_G, что G изоморфна H.

Д-во:

$\varphi(g) \quad x \xrightarrow{\varphi} gx \quad \varphi(g)$ – биекция

$G \to G$

$\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) \qquad x \to g_1 g_2 x$

$g_1(g_2 x) = \varphi(g_1)(\varphi(g_2)x)$

g_1, g_2 - одинаковые биекции.

Если $|M|=n$, то $F_M \approx S_n$ - симметрическая группа подстановок n-ой степени.

Пусть дана группа G и подгруппа H. $a \in G$ и $a \in H$.

Построим минимальную подгруппу H, содержащую элемент a.

Пусть $\forall m \in Z \ a^m \in H$. В H входят: $a^{-1}, a^0 = e, a, a^2, ..., a^m$

Если из $m \neq m'$ следует, что $a^m \neq a^{m'}$, то $\varphi m = a^m$ - изоморфизм. Мы получили подгруппу (она бесконечная). H – циклическая подгруппа бесконечного порядка.

Иначе если $m \neq m'$ и $a^m = a^{m'}$, то это гомоморфизм. Пусть $m > m'$ и $a^m = a^{m'}$, тогда $a^{m-m'} = e$

Обозначим $\min\{l \in N / a^l = e\} = n$.

Покажем, что порядок подгруппы H равен n, т.е $H = \{a, a^2, .., a^{n-1}\}$

Рассмотрим целое $m = qn + r$. $0 \le r \le n-1$. Имеем $a^m = (a^n)^q a^r = e^q a^r = a^r$

Покажем, что для любых $0 \le i < k \le n-1 \ a^i \neq a^k$. Пусть это не так, тогда $e = a^{k-i}$, причем $1 \le k-i \le n-1$. Т.о. n – не минимальное число, которое мы выбрали. Противоречие с построением.

Подгруппа H наз. циклической подгруппой элемента a.

О. Группа наз. циклической, если она совпадает с одной из своих циклических подгрупп.

Теорема. Пусть G –циклическая группа $G=(a)$. H – подгруппа G. Тогда выполняется следующее:

1. H – циклическая.
2. Если $|G| = \infty$, то $|H| = 1$ или ∞.
3. Если порядок $|a| = n$, то порядок H делитель n.

Д-во:

1. Существуют натуральные m, такие что $a^m \in H$. Среди всех этих степеней выберем минимальное. Обозначим его через d. Докажем, что $H = (a^d)$. Пусть a^m - произвольный элемент из H. Необходимо доказать, что m делится на d.

$m = qd + r \quad 0 \le r < d$

$a^m \in H$ и $a^d \in H \qquad a^m = (a^d)^q a^r \Rightarrow a^r \in H$. Следовательно d не минимально. Противоречие.

Отсюда r=0.

Следовательно, H – циклическая подгруппа.

2. Если бы H была конечная и отличалась от 1, значит она порождается элементом a^d. Но тогда найдутся такие $k \neq l$, что $a^{dk} = a^{dl}$, т.к. H – конечная. Но тогда G-конечная.

3. H – циклическая, следовательно, есть порождающий элемент, т.е. $H = (a^m)$

Докажем 2 леммы для нашей теоремы.

Лемма 1. НОД(m,n)=d $\Rightarrow \exists u, v \in Z$, что $d = um + vn$

Д-во: {Z,+}. Рассмотрим подгруппу H, порожденную m и n

$H = (m,n) = \{um + vn, \ u, v \in Z\}$ – подгруппа, т.е. циклическая $\Rightarrow H = (d)$

Лемма 2. Если НОД(m,n)=d, то $(a^m) = (a^d)$

Д-во: $m = m'd \Rightarrow a^m = (a^d)^{m'} \Rightarrow a^m \in (a^d)$

По Лемме 1 d=um+vn => $a^d = (a^m)^u (a^n)^v = (a^m)^u \quad (a^n)^v = e$, т.к. |a|=n => $a^d \in (a^m)$

Вернемся к теореме. Пусть d=НОД(m,n), тогда H=(a^d), но d есть делитель n.

Для нахождения НОД существует алгоритм Евклида (см. Курош).

a=qb+r $\quad 0 \le r < b$

НОД(a,b)=НОД(q,r)

$r_0 = q_1 r_1 + r_2$

$r_1 = q_2 r_2 + r_3$

$r_{i-1} = q_i r_i + r_{i+1}$

$r_{s-1} = q_s r_s \quad r_{s+1} = 0$

$$\begin{pmatrix} r_i \\ r_{i-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_i \end{pmatrix} \begin{pmatrix} r_{i+1} \\ r_i \end{pmatrix}$$

Оценка операций $s < \frac{\log_2 b}{2}$

Круговые многочлены.

Пусть данный ε^j (j-ый корень n-ой степени из 1). Можно ли из него построить все остальные корни. Необходимое и достаточное условие НОД(j,n)=1. Такие ε^j наз. первообразными корнями степени n из 1.

ε^j для какого-то n_j является первообразным. Как найти n_j.

НОД(j,n)= d_j $\quad$ n= n_j d_j => $\quad (e^j)^n = (e^{dj})^{nj} = 1$

j= d_j j'

Пусть НОД(j', n_j)=1 (сократили на НОД)

Корень ε^j является первообразным корнем степени n_j.

Рассмотрим $\Phi_n(x) = \prod_{j/НОД(j,n)=1} (x - \varepsilon^j)$ круговой многочлен, у которого корни - первообразные корни степени n

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

$$\prod_{j=0}^{n-1} (x - \varepsilon^j) = \prod_{d|n} \prod_{j/НОД(j,n/d)=1} (x - \varepsilon^j)$$

Факторизация

Пусть дана группа G и подгруппа H.

aH={ah, $h \in H$} – левый смежный класс группы G по подгруппе H.

Ha={ha, $h \in H$} – правый смежный класс группы G по подгруппе H

Введем отношение a~b, если они в одном смежном классе. a~b => $b \in aH$ => $\exists h \in H / b = ah$

1. a~a рефлексивность.
2. симметричность a~b => b~a

a~b => a=bh, т.е $bh^{-1} = a$ => $a \in bH$, т.к. $h^{-1} \in H$

3. транзитивность a~b, b~c => b~c

$c \in bH$ => $\exists h_1 \in H / c = bh_1$

$b \in aH$ => $\exists h_2 \in H / b = ah_2$ => $c = bh_1 = ah_2 h_1$ => c~a, т.к $h_2 h_1 \in H$

Разбиение на левые смежные классы.

G= $\bigcup_{G/H} aH$ - левое фактор-множество

В этой формуле скрыты 2 условия

1) $\forall g \in G$ существует $a \in G / g \in aH$
2) $a \neq b$ $a \in G/H$, $b \in G/H$ => $aH \neq bH$

Теорема 1. aH=bH $\Leftrightarrow$ $a^{-1} b \in H$ ($b^{-1} a \in H$)

Д-во: $a \in aH$, т.к. $ae=a$, $e \in H$

$a \in bH \Rightarrow \exists h \in H$, что $a=bh \Leftrightarrow h=b^{-1}a \in H$

Т.о. если $a \sim b$, то смежные классы совпадают.

Теорема 2. $Ha=Hb \Leftrightarrow ba^{-1} \in H$ $(ab^{-1} \in H)$

Аналогично.

Левые и правые разбиения могут быть разные (пример S_3)

О. Число элементов левого фактор-множества наз. левым индексом группы G по подгруппе H и обозначается $|G/H|$

Теорема Лагранжа. $|G|=|G/H||H|$

Д-во: Введем $\varphi_a h=ah \quad h \in H$ Прообраз – подгруппа, образ – левый смежный класс.

Заметим, что φ_a - биекция. Действительно, пусть $h \in H$, $h' \in H$, $h \neq h' \Rightarrow \varphi_a h'=ah' \neq ah=\varphi_a h$, иначе домножим на a^{-1}

Т.о. $|H|=|aH|$ при биекции, т.е. каждый класс состоит из стольких же элементов, что и H.

Всего классов $|G/H|$ и они все различные.

Следствие 1. Порядок подгруппы является делителем порядка группы.

Следствие 2. Левые и правые индексы равны.

О. Порядком элемента a наз. $|a|=|(a)|$

Следствие 3. Порядок элемента a является делителем порядка группы. ((a) – подгруппа G)

Следствие 4. Если n-простое и $|G|=n$, то G – циклическая группа. (из следствия 3)

Д-во: Если n=1, то G=(e). Пусть n>1 возьмем $a \neq e$. (a) подгруппа G, тогда $|a|$ делитель n, но n- простое $\Rightarrow |a|=1$ или $|a|=n$. В первом случае получаем, что a=e, чего быть не может. Следовательно $|a|=n$, т.е. группа совпдает с одной из своих циклических подгрупп, т.е. она циклическая.

О. Подгруппа H группы G наз. нормальным делителем (инвариантной подгруппой), если левые и правые разбиения на смежные классы совпадают.

$G=\bigcup_{G/H} aH \qquad G=\bigcup_{G/H} Ha$

$\forall a \in G \ \exists b \in G / aH=Hb \Leftrightarrow \forall a \in G / aH=Ha$

Теорема. H – нормальный делитель $G \Leftrightarrow \forall a \in G, \ \forall h \in H \quad a^{-1}ha \in H$ $(aha^{-1} \in H)$

Д-во: $\Rightarrow \forall a \in G, \ \forall h \in H \quad \exists h' \in H / ah=h'a \Rightarrow aha^{-1}=h' \in H$

$\Leftarrow aha^{-1}=h' \in H \Rightarrow ah=h'a \in Ha \Rightarrow aH \subseteq Ha$

Аналогично $Ha \subseteq aH$, т.к. $(aha^{-1})^{-1} \in H$

Рассмотрим G/H. И рассмотрим операцию $(aH)(bH)=abH$. Если H не нормальный делитель, то тут возникают проблемы. Если же H – нормальный делитель, то эта операция корректна.

Выберем в этих смежных классах по одному представителю.

$\exists h_1, h_2 / a'=ah_1, b'=bh_2 \quad a'b'=(ah_1)(bh_2)=a(h_1b)h_2=(ab)(h_3h_2)$, т.к. $\exists h_3 / h_1b=bh_3$

Три теоремы о связи гомоморфизма и нормального делителя.

Теорема 1. Рассмотрим отображение $\varphi a=aH \quad a \in G \quad aH \in G/H$

φ есть отображение G на G/H $\varphi: G \to G/H$

Теорема утверждает, что φ – гомоморфизм группы G на моноид, если H – нормальный делитель.

Доказательство корректности умножения см. выше.

G/H – гомоморфный образ группы G => G/H – группа, а именно факторгруппа.

Теорема 2. Если φ гомоморфизм группы G в группу $\overline{G}$, то $H=Ker\varphi=\{x \in G / \varphi x=\overline{e}\}$ – нормальный делитель группы G.

Д-во: Ясно, что H – подгруппа G $\varphi e=\overline{e} \quad \varphi(xy)=\varphi x \varphi y=\overline{e} \quad \varphi(x^{-1})=(\varphi x)^{-1}=\overline{e}$

$\forall a \in G, \ \forall h \in H \quad \varphi(a^{-1}ha)=(\varphi a)^{-1}(\varphi h)(\varphi a)=\overline{e}$, т.к. $\varphi h=\overline{e}$

$\varphi(a^{-1}b)=(\varphi a)^{-1}(\varphi b)=(\varphi a)^{-1}(\varphi a)=\overline{e} \qquad \varphi a=\varphi b \Leftrightarrow aH=bH \Leftrightarrow a^{-1}b \in H$

Теорема 3. Если $\varphi G=\overline{G}$, т.е. φ – гомоморфизм группы G на группу $\overline{G}$, то $\overline{G} \sim G/H$, где $H=Ker\varphi$

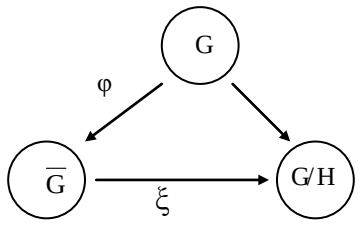
Д-во: Пусть x' – произвольный элемент группы $\overline{G}$, а x такое элемент группы G, что $\varphi x=x'$. Так как для любого элемента a из $H=Ker\varphi \ \varphi a=\overline{e}$. То $\varphi(ax)=\varphi a \varphi x=\overline{e}x'=x'$

Т.о. все элементы смежного класса xH отображаются при φ в элемент x'

С другой стороны, если z- любой такой элемент группы G, что $\varphi z=x'$, то $\varphi(x^{-1}z)=\varphi(x^{-1})\varphi z=(\varphi x)^{-1}\varphi z=x'^{-1}x'=\overline{e}$, т.е $x^{-1}z$ содержится в H.

Т.о. собирая все те элементы группы G, которые при гомоморфизме φ отображаются в фиксированный элемент x' группы $\overline{G}$, мы получим точно смежный класс xH.

Соответствие ξ, относящее каждому элементу x' из $\overline{G}$ тот смежный класс группы по нормальному делителю H, который состоит из всех элементов G, имеющих x' своим образом при φ, будет биекцией. Ξ – изоморфизм, т. к. если ξx'=xH, ξy'=yH, т.е. φx=x', φy=y', то φ(xy)=φxφy=x'y', а поэтому ξ(x'y')=xyH=xHyH= =ξx'ξy'



КОЛЬЦА, ПОЛЯ

О. Множество наз. кольцом, если в нем определены две операции - сложение и умножение, обе коммутативные и ассоциативные, а также связанные законом дистрибутивности.

Лемма. Непустое множество в кольце является подкольцом, если оно замкнуто относительно операции – и +.

О. Тело, если каждый элемент, отличный от единицы, имеет обратный. А коммутативное тело наз. полем.

Кольцо вычетов.

Рассмотрим {Z,+}. Дано натуральное n.

Сделаем отображение φm=res $_n$ ь

φ(m+l)=φm ⊕ φl ⊕ - сложение по mod n

Z/n={i+(n), i=0,..,n-1} – смежные классы.

φ(ml)=φm○φl 0 – умножение по mod n

(i+an)(j+bn)=ij+(…)n

Т.о. мы построили гомоморфный образ, который будет кольцом – кольцом вычетов по mod n.

Тело кватернионов.

Кватернион – четырехмерное пространство.

Комментарий автора:

Кватернион представляет собой упорядоченную четверку действительных чисел s, a, b, c, которые связаны с четырьмя базисными элементами 1, i, j, k, обладающими следующими свойствами:

$i^2=j^2=k^2=-1$, $ij=k, jk=i, ki=j$, $ji=-k, kj=-i, ik=-j$

Возьмем кватернионы α= $a_1 + a_2 i + a_3 j + a_4 k$, β= $b_1 + b_2 i + b_3 j + b_4 k$

Рассмотрим R^{4x4}. Возьмем вектора E, I= $\left(\begin{array}{cc|cc} & 1 & & \\ -1 & & & \\ \hline & & & -1 \\ & & 1 & \end{array}\right)$, J= $\left(\begin{array}{cc|cc} & & & 1 \\ & & 1 & \\ \hline -1 & & & \\ & -1 & & \end{array}\right)$, K= $\left(\begin{array}{cc|cc} & & & 1 \\ & & -1 & \\ \hline & 1 & & \\ -1 & & & \end{array}\right)$

L(E,I,J,K) – 4-хмерное линейное пространство, т.к. матрицы линейно независимы.

Но это множество также подкольцо.

	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	K	$-E$	I
K	K	$-J$	I	$-E$

Все это легко проверяется

Теперь рассмотрим вектора A= $a_1E + a_2I + a_3J + a_4K$, $\overline{A} = a_1E - a_2I + a_3J + a_4K$

αβ= $a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 + (a_1b_2 + a_2b_1 + a_3b_4 + a_4b_3)i + (a_1b_3 + a_3b_1 - a_2b_4 - a_4b_2)j + (a_1b_4 + a_4b_1 + a_2b_3 + a_3b_2)k$

A= $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & -a_4 & a_3 \\ -a_3 & a_4 & a_1 & -a_2 \\ -a_4 & a_3 & a_2 & a_1 \end{pmatrix}$ $\overline{A} = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & -a_3 & -a_2 & a_1 \end{pmatrix}$

$A\overline{A}=(a_1^2+a_2^2+a_3^2+a_4^2)E$

Матрица $A\overline{A}=0 \Leftrightarrow A=0$

Значит для любой матрицы $A\neq 0$ в нашем кольце матриц есть обратная, а находится она так:

$r=\sqrt{a_1^2+a_2^2+a_3^2+a_4^2}$

$A^{-1}=\frac{1}{r^2}\overline{A}$

Это тело кватернионов.

В кватернионах часто выделяют скалярную и векторную часть.

$\alpha=a_1+u$ $\beta=b_1+v$

$u=a_2i+a_3j+a_4k$, $v=b_2i+b_3j+b_4k$

$\alpha\beta=a_1b_1-(u,v)+a_1v+b_1u+[u,v]$

ПРИЛОЖЕНИЯ КВАТЕРНИОНОВ

Наиболее естественным способом, позволяющим описывать повороты в трехмерном пространстве, является использование операторов преобразования и соответствующих им матриц. Однако использование кватернионов позволяет дать более простую форму этого поворота. Представление трехмерных вращений при помощи кватернионов удобно тем, что кватернион определяет непосредственно его геометрические характеристики: ось вращения и угол поворота. При обычном описании вращения при помощи матриц для определения оси вращения и угла поворота необходимо проделать некоторые вычисления, а при использовании кватернионов он находится естественным образом.

Кольцо формальных степенных рядов и многочленов.

Рассмотрим кольцо K. Обозначим через K_∞ множество из элементов a, где $a=(a_0,a_1,...)$ $a_i\in K$

$b=(b_0,b_1,...)$

$a+b=(a_0+b_0,a_1+b_1,...)$ Относительно такого покомпонентного сложения это множество будет абелевой группой.

Умножение определим следующим образом:

$c=ab=(c_0,c_1,...)$, где $c_k=\sum_{i+j=k}a_ib_j=\sum_{i=0}^{k}a_ib_{k-i}$

Необходимо доказать ассоциативность и две дистрибутивности.

a(b+b')=ab+ab' ?

$c'=ab'=(c'_0,c'_1,...)$ $c'_k=\sum_{i=0}^{k}a_ib'_{k-i}$

$c+c'=(c_0+c'_0,c_1+c'_1,...)$ $(c+c')_k=\sum_{i=0}^{k}a_ib_{k-i}+\sum_{i=0}^{k}a_ib'_{k-i}=\sum_{i=0}^{k}a_i(b_{k-i}+b'_{k-i})=(a(b+b'))_k$

(ab)d=a(bd) ab=c bd=g cd=f ag=h

$f_m=\sum_{k+j=m}c_kd_j=\sum_{k+j=m}(\sum_{i=0}^{k}a_ib_{k-i})d_j=\sum_{i+j+l=m}a_ib_jd_l$

Легко доказывается, что $f_m=h_m$

Т.о. $\{K_\infty,+,*\}$ – кольцо.

$e^{(i)}=(0,..,0,1,0,..,0)$ - 1 на i-ом месте.

$e^{(i)}$ - единица в кольце K_∞.

$e^{(1)}e^{(i)}=e^{(i+1)}$ По индукции доказывается, что $e^{(i)}e^{(j)}=e^{(i+j)}$

Получили степенной ряд.

$a(x)=a_0+a_1x+...$

$K_\infty[x]\sim K_\infty$ - кольцо формальных степенных рядов от x.

$K[x]=\{a(x)\in K_\infty[x] / \exists n / a_{n+1}=..=0\}$ –кольцо многочленов

n – степень a(x).

Степень нулевого многочлена –1 или $-\infty$

Степень a(x)+b(x) не превосходит степени a(x),b(x)

$a(x)b(x)=(a_0+\ldots+a_nx^n)(b_0+\ldots+b_mx^m)=(a_0b_0+\ldots+a_nb_mx^{n+m})$

$a_n b_m$ не обязательно не равно 0, если $a_n \neq 0,\ b_m \neq 0$

Если кольцо имеет делители 0, то степень a(x)b(x) не превосходит степениа(x)+степенib(x)

$a(x) \in K_\infty[x]$ $\quad a(x)=\sum_{j=0}^{\infty} a_j x^j$ $\quad a'(x)=\sum_{j=0}^{\infty} j a_j x^{j-1}$

Неверно, что степень производной от многочлена меньше степени многочлена на 1. Контрпример – многочлен в система вычетов по mod n

$a(x)= a_0 + a_1 x + ... + a_n x^n$

$a(\alpha)=\sum_{j=0}^{n} a_j \alpha^j$ - правое значение многочлена

$a(\alpha)=\sum_{j=0}^{n} \alpha^j a_j$ - левое значение многочлена

В общем случае кольцо не коммутативное.

$b(x)= b_0 + b_1 x + ... + b_m x^m$ $\quad b(\alpha)= \sum_{k=0}^{m} b_k \alpha^k$

$a(\alpha) \pm b(\alpha)=(a \pm b)(\alpha)$

(*) $\quad a(\alpha)b(\alpha)=(ab)(\alpha)$

Вообще говоря это неверно.

Лемма. Если α перестановочный с коэффициентами b(x) , т.е. $\alpha b_k = b_k \alpha$ k=0,…,m, то равенство (*) верно.

Д-во: Индукцией по i доказывается, что $\alpha^i b_k = b_k \alpha^i$ для любого $i \in N$

$\alpha^{i+1} b_k = \alpha^i \alpha b_k == \alpha^i b_k \alpha = b_k \alpha^i \alpha = b_k \alpha^{i+1}$

$a(\alpha)b(\alpha)= \sum_{j=0}^{n} a_j \alpha^j \sum_{k=0}^{m} b_k \alpha^k = \sum_{k=0}^{m}\sum_{j=0}^{n} a_j \alpha^j b_k \alpha^k = \sum_{s=0}^{m+n}(\sum_{j+k=s} a_j b_k)\alpha^s$

О. α – правый корень многочлена a(x), если a(α)=0.

Теорема. Даны многочлены $a(x)= a_0 + a_1 x + ... + a_n x^n$ и $b(x)= b_0 + b_1 x + ... + b_m x^m$.Если для коэффициента b_m в кольце K существует такой элемент c, что c – обратный элемент к b_m, то существует единственные многочлены q(x) и r(x), причем degr(x)<degb(x) или r(x)=0, что a(x)=q(x)b(x)+r(x). r(x) – правый остаток при делении. Если r(x)=0, то говорят, что a(x) делится справа на b(x).

Д-во: *единственность* Пусть существует $q_1(x) \neq q(x)$, что $a(x)=q_1(x)b(x)+r_1(x)$

$(q(x)-q_1(x))b(x)=r_1(x)-r(x)$

$q(x)-q_1(x) \neq 0 \Rightarrow \deg(q(x)-q_1(x))=v$

Тогда степень произведения не меньше m. Действительно, если $h_v \neq 0$ - старший коэффициент $q(x)-q_1(x)$, то коэффициент при x^{m+v} равен $h_v b_m$. Допустим $h_v b_m=0$, умножим справа на c, тогда, т.к. $b_m c=1$, $h_v=0$. Противоречие.

Но $\deg(r_1(x)-r(x))<m$. Снова противоречие.

существование Пусть m>n b(x) тождественно не 0, тогда r(x)=a(x) q(x)≡0

Пусть n≥m. Проведем индукцию по n

$\bar{a}(x)=a(x)- a_n b(x) c\, x^{n-m}$

Степень $\deg \bar{a}(x)<\deg a(x)=n$, следовательно $\bar{a}(x)= \bar{q}(x)b(x)+ \bar{r}(x)$

$q(x)= \bar{q}(x)+ a_n c\, x^{n-m}$

$r(x)= \bar{r}(x)$

Следствие 1. Если K – тело, то можно делить на любой ненулевой многочлен

Следствие 2. Если $K=F^{nxn}$, то необходимое условие $\det b_m \neq 0$

Следствие 3. Если b(x)=x-α, то $r(x)=r_0 \in K$ и $r_0=a(\alpha)$

$a(\alpha)=q(\alpha)(\alpha-\alpha)+r_0$ $\quad q(\alpha)(\alpha-\alpha)=0$ по лемме

Обобщенная теорема Безу

α –правый корень многочлена a(x) ⇔ a(x) делится на (x-α) справа

Схема Горнера

a(x)= $a_0x^n + a_1x^{n-1} + ... + a_n = (b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-1})(x-\alpha) + b_n$

$a_0 = b_0$ $\quad$ $\underline{b_0 = a_0}$

$a_1 = b_1 - b_0\alpha$ $\quad$ $\underline{b_j = a_j + b_{j-1}\alpha}$

…

$a_j = b_j - b_{j-1}\alpha$

…

$a_n = b_n - b_{n-1}\alpha$

Идеалы

$I \subseteq K$ – левый идеал K если

1. {I,+} – подгруппа {K,+}
2. $KI \subseteq I$

Правый, если $IK \subseteq I$

Если идеал правый и левый, то он двухсторонний

Пусть K – кольцо, I – идеал.

{K/I, $\oplus$ } – факторгруппа по сложению. Класс имеет вид a+I

$(a+I) \oplus (b+I) = a+b+I$

$(a+I)^\circ(b+I) = ab+I$ – операция корректна, если I – двухсторонний.

$a' \in a+I$ $\quad$ $b' \in b+I$ $\quad$ $a'b' \in ab+I$

$\exists i_1 \in I / a' = a+i_1$

$\exists i_2 \in I / b' = b+i_2$

$a'b' = (a+i_1)(b+i_2) = ab+ai_2 + i_1(b+i_2) = ab+i$ $\quad$ $i \in I$

Т.о. операция корректна

Естественный гомоморфизм $\varphi a = a+I$ $\quad$ $a \in K$

φ –гомоморфизм кольца K на множество {K/I, $\oplus$,°}

Т.о. {K/I, $\oplus$,°} – факторкольцо кольца K по идеалу I

Задан гомоморфизм φ: K→K'

$Ker\varphi = \{x \in K / \varphi x = 0\}$

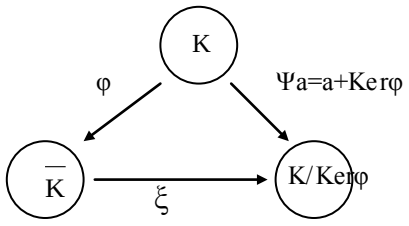
Теорема 1. $Ker\varphi$ – идеал в K

Теорема 2. $\varphi a = \varphi b \Leftrightarrow a-b \in K$

Д-во: из определения гомоморфизма и ядра.

Теорема 3. Если φ – гомоморфизм K на $\overline{K}$ => $K/Ker\varphi \underline{\sim} \overline{K}$

Д-во:



$\xi(a+Ker\varphi) = \varphi a$

$\xi(b+Ker\varphi) = \varphi b$

Это отображение является биекций и не зависит от представителей.

$\xi((a+Ker\varphi)\circ(b+Ker\varphi)) = \xi(ab+Ker\varphi) = \varphi(ab) = \varphi a\varphi b = \xi(a+Ker\varphi)\xi(b+Ker\varphi)$

Напомним, что P – поле, если $0 \neq e \in P$

Рассмотрим отображение $Z \xrightarrow{\varphi} P$ $\quad$ φ – отображение Z в P

$\varphi n = ne = \sum_{i=1}^{n} e_i$ $\quad$ $e_i = e$

Заметим, что φ – гомоморфизм.

$Ker\varphi = \begin{cases} \{0\} \\ (p) \quad p - число \end{cases}$

Характеристикой поля является 0 если $Ker\varphi = \{0\}$ или p, если $Ker\varphi = (\varphi)$

$\chi(P)=0$ $\chi(P)=p$
Докажем, что p – простое
Пусть это не так, т.е. p=kl
Тогда (ke)(le)=kle=pe=0
Так как в поле не может быть делителей 0, то либо ke=0, либо le=0, следовательно, p – не минимально.
Если характеристика поля равна p,то для любого элемента a из этого поля имеет место равенство pa=(pe)a=oa=0
Теорема. 1. Если $\chi(P)=0$, то $\varphi(Z)\underset{\sim}{}Z$
2. P содержит минимальное подполе $F\underset{\sim}{}Q$
3. Если $\chi(P)=p$, то $\varphi(Z)\underset{\sim}{}Z/p$, $\varphi(Z)$ – минимальное подполе в поле P
Д-во: 1. $\varphi n=ne$. Это отображение φ устанавливает однозначное соответствие между Z и $\varphi(Z)$, т.к. $Ker\varphi=\{0\}$
Т.о. $Z\underset{\sim}{}\varphi(Z)$
2. Для любого элемента существует обратный
$\varphi(Z)=\{ne,\ n\in Z\}$
$F=\{ne/me,\ n\in Z,\ m\in N\}$
$\varphi(Z)$ – коммутативно, т.к. $Z\underset{\sim}{}\varphi(Z)$ => F – коммутативно
Докажем, что если $\frac{m}{n}=\frac{mq}{nq}$, то $\frac{me}{ne}=\frac{mqe}{nqe}$. Если бы это было не так, то не выполнялось бы menqe=nemqe.
Имеем биективное отображение между F и Q. Докажем, что это изоморфизм.
Пользуясь предыдущим свойством легко доказывается, что сложение будет таким же как и в поле рациональных чисел.
3. $Ker\varphi=(p)$
По теореме 3 о гомоморфизмах $\varphi(Z)\underset{\sim}{}Z/p$, т.к. $Ker\varphi=(p)$
Докажем, что $\varphi(Z)$ – поле
je, $1\le j\le p-1$
Док-ть, что существует обратный.
j, p – взаимно просты (p – простое!) => $\exists u,v$ / uj+vp=1 (по Лемме 1)
$uj\equiv 1(p)$ => (je)(ue)=e => существует обратный $\forall$ je
Т.о. $\varphi(Z)$ – поле.

Рассмотрим поле характеристики p.

$$(a\pm b)^p=\sum_{j=0}^{p}\binom{p}{j}a^j(\pm b)^{p-j}=a^p\pm b^p$$

В силу коммутативности мы пользовались тем, что $a^kb^l=b^la^k$.

$1\le j\le p-1$ $\binom{p}{j}=p\frac{(p-1)...(p-j+1)}{j!}\equiv 0(p)$, т.к. коэффициент целый, а p не делится на j!, значит все остальное делится на него, т.е. коэффициент делится на p.

$(a\pm b)^{p^k}=a^{p^k}\pm b^{p^k}$ k – натуральное.
Док-во индукцией по k (уже взрослые!)

Далее $(\sum_{j=1}^{t}a_j)^{p^k}=\sum_{j=1}^{t}a_j{}^{p^k}$. Аналогично индукцией по k. (не смотрите на меня так)

Рассмотрим частный случай k=1, a_j=a. Получаем по предыдущему $(ta)^p=ta^p$

Отсюда вытекает Малая теорема Ферма. $t^p\equiv t(p)$ => $t^{p-1}\equiv 1(p)$

НОД многочленов - НОД(f, g)
Если f=0,g=0, то НОД(f, g)=0
Если хотя бы один $f\neq 0, g\neq 0$, то это общий делитель наибольшей степени.

Можем считать, что если $d\neq 0$, то его старший коэффициент равен 1.
Многочлены взаимно просты, если НОД(f, g)=1
Лемма 1. НОД(f, φ)=НОД(f, ψ)=1 => НОД(f, $\varphi\psi$)=1
Лемма 2. fg делится на φ и НОД(f, φ)=1 => g делится на φ
Лемма 3. φ, ψ – делители f и НОД(φ, ψ)=1 => $\varphi\psi$ делит f
О. $0\neq f(x)$ наз. приводимым над F, если существует q(x), s(x), оба степени меньшей, чем f, такие, что f(x)=q(x)s(x). В противном случае он неприводим.

Лемма. Если fg делится на неприводимый многочлен p, то хотя бы одиниз этих множителей делится на p(x)
Д-во: Если f(x) не делится на p(x), то НОД(f, p)=1, но тогда по Лемме 2 g(x) делится на p(x)

Теорема. Для любого $0 \neq f(x) \in F[x]$ существуют такие неприводимые над F многочлены $p_i(x)$ со старшими коэффициентами равными 1, что $f(x)=c\prod_{i=1}^{n} p_i^{ki}(x)$, причем такое представление единственное с точностью до перестановки сомножителей.

Д-во: существование. Если многочлен сам неприводим, то указанное произведение состоит всего из одного множителя. Если же он приводим, то может быть разложен в произведение множителей меньшей степени. Если среди этих множителей снова имеются приводимые, то производим дальнейшее разложение на множители и т.д. Этот процесс должен остановиться после конечного числа шагов, т.к. при любом разложении f(x) на множители сумма степеней множителей должна равняться n и поэтому число множителей, зависящих от x, не может превосходить n.

единственность. Доказательство индукцией по степени многочлена. Пусть есть еще одно представление $f(x)=c\prod_{i=1}^{m} q_i^{li}(x)$.

$q_1(x)$ - делитель f(x) => по Лемме $q_1(x)$ будет делителем хотя одного из многочленов $p_i(x)$, т.е. $p_i(x)=q_1(x)$

Сократим на эти множители. Получим многочлен меньшей степени, для которого по предположению индукции представление единственное. Противоречие.

Если F=C, то $p_i(x)$ – многочлены первой степени

Если F=R, то $p_i(x)$ – многочлены либо1-ой, либо 2-ой степени

Следствие 1. Над любым F количество неприводимых многочленов бесконечно.

Д-во: Если поле бесконечное, то неприводимыми очевидно являются $x-\alpha$. Для конечного поля см. Следствие 2.

Следствие 2. Если поле конечно, то для любого n существует неприводимый p(x), что degp(x)≥n

Д-во: Допустим, что $p_1,\ldots,p_s$ - все неприводимые многочлены.

Рассмотрим $f(x)=\prod_{i=1}^{s} p_i(x)+1$. Он раскладывается в произведение $p_1,\ldots,p_s$, но он взаимно прост с каждым p_i. Противоречие.

Если $k_i>1$, то $p_i(x)$ – кратный множитель, а k_i - кратность.

Лемма 1. Если p(x) – к-кратный неприводимый множитель f(x), то p(x) – s-кратный неприводимый множитель f ’(x), где s≥k-1

Д-во:

$f(x)=p^k(x)q(x)$

$f'(x)=kp^{k-1}(x)q(x)p'(x)+p^k(x)q'(x)=p^{k-1}(x)(kq(x)p'(x)+p(x)q'(x))$

Если характеристика поля равна 0, то s=k-1, т.к. p’(x) не делится на p(x) и q(x) не делится на p(x)

Выделение кратных множителей. (см. Курош)

Лемма 2. $a(x)=\sum_{i=0}^{m} a_i x^i \in F[x]$, $\chi(F)=p$. Тогда $a'(x)=0 \Leftrightarrow ia_i \equiv 0\ (p) \Leftrightarrow \exists b(x) / a(x)=b^p(x)$

Д-во:

$=> a'(x)=\sum_{i=1}^{m} ia_i x^{i-1}$ $\qquad a'(x)=0 => ia_i \equiv 0\ (p)$

(i,p)=1 => $a_i=0$ все промежуточные коэффициенты при степенях, не кратных p, равны 0.

$a(x)=\sum_{\nu=0}^{[m/p]} a_{p\nu} x^{p\nu}$

$b(x)=\sum_{\nu=0}^{[m/p]} a_{p\nu} x^{\nu}$

Равенство в условии теоремы выполняется, т.к. верна формула бинома Ньютона на полем характеристики p.

<= Дифференцируем.

Теорема. f(x) не имеет кратных множителей ⇔ (f,f’)=1

Д-во: Для χ(F)=0 тривиально

<= Пусть f(x) имеет кратные множители => он содержит $p^k(x)$ ($k\geq 2$)
Но тогда f'(x) содержит его в степени не меньше (1), тогда НОД не 1.
=> Пусть d(x)=НОД(f,f') f(x) не имеет кратных множителей. Докажем, что d(x)=1. Пусть не так.
Если d(x)=0, то ясно, что кратных множителей бесконечно много.
Пусть $d(x)\neq 0 \Rightarrow \exists p$, d' $d(x)=p^s(x)d'(x)$ $s\geq 1$, причем p – неприводим.
s=1, иначе есть p(x)=НОД(f,f')<d(x)
$f(x)=p(x)f_1(x)$ $f_1(x)$ не делится на p(x)
$f'(x)=p'(x)f_1(x)+p(x)f_1'(x)$
f'(x) делится на p(x) => $p'(x)f_1(x)$ делится на p(x) => p'(x) делится на p(x) $\Leftrightarrow$ p'(x)=0 => по Лемме 2 получаем, что p(x) – приводим. Противоречие.
Следовательно d(x)=1

Теорема. Пусть дан ненулевой идеал $I \supseteq F[x]$. Тогда
1. $\exists f(x) / I=(f(x))$
2. $F[x]/(f(x))=\overline{F} \supseteq F' \tilde{} F$, т.е. факторкольцо содержит подполе F', изоморфное полю F, и $\overline{F}$ - линейное пространство над F' и $\dim \overline{F} = \deg f(x)$
3. $\overline{F}$ - поле $\Leftrightarrow$ f(x) неприводим над F

Д-во:
1.
2. Формируем гомоморфизм φ
$g(x) \in F[x]$ $\varphi(g(x))= res_{f(x)} g(x) = r_o + r_1 x + ... r_{n-1}x^{n-1}=r(x)$ $n=\deg f(x)$
φ(r(x))=r(x)
остаток - r'(x)≠r(x) –остаток => r(x)=φ(r(x))≠φ(r'(x))=r'(x)
$\overline{F} \supseteq F'$. Классы соответствующие r_0 будем считать элементами F'.

Обозначим через $\bar{1}$ - все многочлены, при делении на f(x) дающие на 1. И т.д. получаем систему $1, \bar{x}, .., \bar{x}^{n-1}$
$\bar{r}(x)=\{r(x)+f(x)q(x)\}$
$\bar{x}=\{x+f(x)q(x)\}$
$\bar{r}(x)= \overline{r_0}\bar{1}+...+\overline{r_{n-1}}\bar{x}^{n-1}$

О. Матричный многочлен – это многочлен над кольцом матриц, т.е. его коэффициенты – матрицы.
Если матрицы невырожденные, то можно делить многочлены с остатком.
$A[\lambda]= A_0 + A_1\lambda + ... + A_n\lambda^n$
$B[\lambda]= B_0 + B_1\lambda + ... + B_m\lambda^m$

Теорема Гамильтона-Кэли. Всякая матрица является корнем своего характеристического многочлена.
Д-во:
Пусть дана матрица A.
Ее характеристический многочлен $|\lambda E-A|= \lambda^n + S_1\lambda^{n-1} + ... + S_n$
Рассмотрим матрицу λE-A и B(λ) – присоединенную к ней.
(λE-A)B(λ)=B(λ)(λE-A)=|λE-A|E
Т.о. образом матричный многочлен |λE-A|E делится на многочлен (λE-A). А тогда A является корнем |λE-A|
Т. Гамильтона-Кэли является следствием обобщенной теоремы Безу.

$\Delta_k(\lambda,A)$ – наибольший общий делитель миноров k-ого порядка в матрице λE-A
Присоединенная матрица B(λ) состоит из миноров n-1 порядка матрицы λE-A => все элементы делятся на $\Delta_{n-1}(\lambda,A)$. Тогда $B(\lambda)= \Delta_{n-1}(\lambda,A)C(\lambda)$, причем НОД миноров матрицы C(λ) равен 1.
$|\lambda E-A|= \Delta_n(\lambda,A)$
Δ_n делится на Δ_{n-1}, т.к. Δ_n можно разложить в сумму n миноров n-1 порядка
Т.о. $\Delta_n(\lambda,A)=\Delta_{n-1}(\lambda,A)d_n(\lambda)$
Имеем $\Delta_{n-1}(\lambda,A)(\lambda E-A)C(\lambda)=\Delta_{n-1}(\lambda,A)C(\lambda)(\lambda E-A)=d_n(\lambda)\Delta_{n-1}(\lambda,A)E$

$(\lambda E-A)C(\lambda)= C(\lambda)(\lambda E-A)=d_n(\lambda)E$

По обобщенной теореме Безу, т.к. $d_n(\lambda)E$ делится на $(\lambda E-A)$, A является корнем $d_n(\lambda)$.

О. $f(\lambda) \in F[\lambda]$ аннулирует A, если $f(A)=0$

Характеристический многочлен аннулирует матрицу A.

I_a - множество аннулириующих многочленов A – идеал в кольце $F[\lambda]$

$I_A=(d_A)$ Пусть у d_A старший коэффициент равен 1

Существует единственный минимальный d_A. Действительно если и есть разные минимальные, то одинаковой степени (иначе кто-то меньше), но тогда вычтем один из другого и получим аннулирующий многочлен меньшей степени.

О. $d_A(\lambda)$ – минимальный многочлен для матрицы A.

Любой минимальный многочлен делитель характеристического многочлена. Его степень не превосходит n.

Теорема. $d_n = \dfrac{\Delta_n(\lambda, A)}{\Delta_{n-1}(\lambda, A)}$ - минимальный многочлен для матрицы A.

Д-во: Пусть $\delta(\lambda)$ – минимальный для A

Тогда $d_n(\lambda)=\delta(\lambda)q(\lambda)$

Т.к. $\delta(A)=0$, то $\delta(\lambda)E$ делится без остатка на $\lambda E-A$, т.е. $\delta(\lambda)E = (\lambda E-A)Q(\lambda)$, следовательно

$(\lambda E-A)C(\lambda)=q(\lambda)(\lambda E-A)Q(\lambda)$

$C(\lambda)=q(\lambda)Q(\lambda)$

Однако, НОД элементов $C(\lambda)$ равен 1. Поэтому многочлен $q(\lambda)$ имеет нулевую степень, а его страший коэффициент равен 1 => $q(\lambda)=1$

λ-матрицы

$(F[\lambda])^{mxn}$ – кольцо матриц с элементами из многочленов – λ-матрицы.

О. $A(\lambda) \sim B(\lambda)$, если $B(\lambda)$ можно получить из $A(\lambda)$ серией элементарных преобразований следующих видов

$(i)'=C(i)$ $C \in F\setminus\{0\}$

$(i,k)=i+k$

$(i)'=(i)+\varphi(\lambda)(k)$ $\varphi(\lambda) \in F[\lambda]$

Каждое из этих преобразований эквивалентно домножению слева на матрицу (см. 1 семестр), которая называется элементарной.

О. $D(\lambda)$ – диагональную матрицу назовем нормально-диагональной (форма Смита), если

$D(\lambda)=diag(d_1(\lambda),\ldots,d_r(\lambda),0,\ldots,0)$. Причем $d_i(\lambda) \vdots d_{i-1}(\lambda)$, а старшие коэффициенты у них равны 1.

Теорема. $\forall A(\lambda) \in (F[\lambda])^{mxn}$ существует единственная нормально-диагональная матрица $D(\lambda)$ такая, что $D(\lambda) \sim A(\lambda)$.

Лемма. $a_{11}(\lambda) \neq 0$ и $\exists$ i, j / $a_{ij}(\lambda)$ не делится на $a_{11}(\lambda)$, тогда $\exists A'(\lambda) \sim A(\lambda) / a'_{11}(\lambda) \neq 0$ и $dega'_{11}(\lambda) < dega_{11}(\lambda)$

Д-во: Допустим, что i=1

$a_{1j}(\lambda)=q(\lambda)a_{11}(\lambda)+r(\lambda)$

$[j]'=[j]-q(\lambda)[1]$ (действия со столбцами)

Затем поменяем местами [1,j]

Если j=1, то доказательство аналогично

Пусть теперь $i \neq 1$, $j \neq 1$. Т.е. $a_{i1}(\lambda)=q_i(\lambda)a_{11}(\lambda)$ i=2,..,m

Тогда для каждой строчки $(i)'=(i)-q_i(\lambda)(1)$

$(1)'=(1)+(i)$

$a'_{11}=a_{11}$

$a'_{ij}(\lambda)=a_{ij}(\lambda)-q_i(\lambda)a_{1j}(\lambda)$

$a'_{1j}(\lambda)=a_{1j}+a'_{ij}=(1-q_i(\lambda))a_{1j}(\lambda)+a_{ij}(\lambda)$ не делится на a'_{11}

Возвращаемся к первому случаю.

Бесконечное число раз лемму не применим, т.к. степень конечная.

Т.о. получится матрица, в которой все элементы делятся на a_{11}.

По индукции. Допустим для матриц (m-1)x(n-1) теорема верна. Докажем для A.

Сделаем преобразование строк.

$(i)'=(i)-q_i(1)$ i=2,..,m $a'_{i1}=0$

При этом делимость на a_{11} сохраняется. Такое же преобразование сделаем со столбцами

Получим матрицу:

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

Для A’ справедливо предположение индукции. Получаем матрицу

$$\left(\begin{array}{c|ccc|cc} a_{11} & 0 & & & 0 & \\ \hline & d_1 & & & & \\ 0 & & \ddots & & 0 & \\ & & & d_r & & \\ \hline & & & & 0 & \\ 0 & 0 & & & \ddots & \\ & & & & & 0 \end{array}\right)$$

Все элементы A’ делятся на a_{11}. Нормализуем a_{11}, сделав старший коэффициент 1. Теорема доказана.

$\Delta_k(A(\lambda))$ – НОД миноров k порядка в матрице A.

Лемма. Если $B(\lambda)\sim A(\lambda) \Rightarrow \Delta_k(A(\lambda))=\Delta_k(B(\lambda))$

Д-во: Из определения получаем, что $B(\lambda)=P(\lambda)A(\lambda)Q(\lambda)$, где $P(\lambda)$, $Q(\lambda)$ – невырожденные матрицы, причем $|P(\lambda)|=const\neq 0$, $|Q(\lambda)|=const\neq 0$

Из формулы Бине-Коши получаем, что любой минор k порядка в матрице B делится $\Delta_k(A(\lambda))$

Рассмотрим нормально-диагональную матрицу D

$\Delta_k(D(\lambda))$ k=1,..,r остальные равны 0

$\Delta_1(D(\lambda))=d_1$

$\Delta_k(D(\lambda))=d_1 \dots d_k$

$d_k(\lambda)=\frac{\Delta_k(D(\lambda))}{\Delta_{k-1}(D(\lambda))}=\frac{\Delta_k(A(\lambda))}{\Delta_{k-1}(A(\lambda))}$ (по Лемме 2) $k\geq 1$ $\Delta_0(D(\lambda))=1$

О. Матрица $P(\lambda)$ наз унимодулярной над $F[\lambda]$, если $\det(P(\lambda)) \in F\setminus\{0\}$, т.е. не зависит он λ

$P^{-1}(\lambda)$ имеет элементы из $F[\lambda]$. Вообще говоря, обратная не обязательно состоит из многочленов.

Только унимодулярная обладает таким свойством.

Следствие. $A(\lambda)\sim B(\lambda) \Leftrightarrow$ существуют унимодулярные $P(\lambda)$, $Q(\lambda)$ / $B(\lambda)=P(\lambda)A(\lambda)Q(\lambda)$

Док-во: => по определению, т.к. элементарные матрицы – унимодулярные. А $B(\lambda)$ получается из $A(\lambda)$ серией элементарных преобразований.

<= Из теоремы следует, что для унимодулярных матриц нормально-диагональная форма это E. Тогда можем свести $P(\lambda)$ к E, т.е. $P(\lambda)=P_s \dots P_1 E Q_1 \dots Q_t = P_s \dots P_1 Q_1 \dots Q_t$ => можем элементарными преобразованиями свести $B(\lambda)$ к $A(\lambda)$.

Ax=b над кольцом Z

Обычно мы решаем методом Гаусса, но в кольце делить нельзя.

Сделаем замену x=Qy. Если Q – унимодулярная, то Q^{-1} - целочисленная, $y=Q^{-1}x$ => если x – целое, то y – целое

Автоморфизм – сложение + умножение на элементы Z

Автоморфизм целочисленное решетки происходит при помощи матрицы Q

Имеем Aqy=b

Существует такая матрица P, что PAQ=D нормально-диагональная (в качестве Q возьмем вторую матрицу)

PAQy=Pb

Dy=Pb=b’

Чтобы решение существовало надо, чтобы b'_i делилось на d_i

Если надо решать систему линейных уравнение над $F[\lambda]$, то это все тоже выполняется ($P(\lambda)$, $Q(\lambda)$ - унимодулярные)

Если даны квадратные матрицы над полем F. Как определить подобны они или нет? Ведь они не всегда могут быть диагонализируемы.

Теорема 2. Матрица A и B подобны над полем F тогда и только тогда, когда их характеристические матрицы эквивалентны над кольцом F[λ].

Д-во:

$\Rightarrow A \approx B \Rightarrow \exists S \ (\det S \neq 0) / B = S^{-1} AS$

S – унимодулярная матрица в кольце F[λ] (все степени λ равны 0)

$B = S^{-1} AS$

$\lambda E - B = P(\lambda)(\lambda E - A)Q(\lambda)$ $P(\lambda) = S^{-1}$ $Q(\lambda) = S$

Легко проверяется что верно (перемножить)

$\Leftarrow \lambda E - B = P(\lambda)(\lambda E - A)Q(\lambda) = \ldots$ (1)

$P(\lambda) = (\lambda E - B)P_1(\lambda) + P_0$ (2) P_0, Q_0 от λ не зависят

$Q(\lambda) = (\lambda E - B)Q_1(\lambda) + Q_0$ (3)

$\ldots = ((\lambda E - B)P_1(\lambda) + P_0)(\lambda E - A)Q(\lambda) = P_0(\lambda E - A)Q(\lambda) + (\lambda E - B)P_1(\lambda)(\lambda E - A)Q(\lambda) =$

$= P_0(\lambda E - A)Q(\lambda) + (\lambda E - B)P_1(\lambda)P^{-1}(\lambda)(\lambda E - B)$, т.к.

Из (1) следует, что $(\lambda E - A)Q(\lambda) = P^{-1}(\lambda)(\lambda E - B)$ (4)

Аналогично $P(\lambda)(\lambda E - A) = (\lambda E - B)Q^{-1}(\lambda)$ (5)

$P_0(\lambda E - A)Q(\lambda) = P_0(\lambda E - A)Q_0 + P_0(\lambda E - A)Q_1(\lambda)(\lambda E - B) =$

$= P_0(\lambda E - A)Q_0 + P(\lambda)(\lambda E - A)Q_1(\lambda)(\lambda E - B) - (\lambda E - B)P_1(\lambda)(\lambda E - A)Q_1(\lambda)(\lambda E - B) =$

$P_0(\lambda E - A)Q_0 + (\lambda E - B)Q^{-1}(\lambda)Q_1(\lambda)(\lambda E - B) - (\lambda E - B)P_1(\lambda)(\lambda E - A)Q_1(\lambda)(\lambda E - B)$

Т.о. $\lambda E - B = P_0(\lambda E - A)Q_0 + (\lambda E - B)(Q^{-1}(\lambda)Q_1(\lambda) - P_1(\lambda)(\lambda E - A)Q_1(\lambda) + P_1(\lambda)P^{-1}(\lambda))(\lambda E - B)$

$\lambda E - B - P_0(\lambda E - A)Q_0 = (\lambda E - B)[\ldots](\lambda E - B)$

Слева многочлен первой степени от λ. Справа,е сли выражение в квадратных скобках не равно 0, то это все справа это многочлен 2 степени от λ. Значит […]=0.

Следовательно, $\lambda E - B = P_0(\lambda E - A)Q_0$

Все коэффициенты равны, т.к. многочлены равны, следовательно

$P_0 Q_0 = E$, $B = P_0 A Q_0$

Т.е. A и B подобны.

Заодно мы получили алгоритм

Следствие 1. $S = Q_0 = Q(B) = (P(B))^{-1}$

Д-во: Подставим в (3) B вместо λ.

Следствие 2. $A \approx B \Leftrightarrow \Delta_k(\lambda, A) = \Delta_k(\lambda, B)$ $k = 1, .., n \Leftrightarrow d_k(\lambda, A) = d_k(\lambda, B) = \dfrac{\Delta_k(\lambda, B)}{\Delta_{k-1}(\lambda, B)}$

$d_k(\lambda, A)$ – инвариатный множитель матрицы A.

!!!! Т.о. у подобных матриц одинаковые минимальные многочлены. Следовательно для преобразования φ в различных базисах один и тот же минимальный многочлен, т.к. матрицы φ для разных базисов подобны.

Фробениус. Как написать по многочлену матрицу, чтобы ее характеристический многочлен совпадал с этим.

$\lambda^n + a_1\lambda^{n-1} + \ldots + a_n = |\lambda E - A|$

$$A = \begin{pmatrix} -a_1 & \cdots & -a_{n-1} & -a_n \\ 1 & & 0 & 0 \\ & \ddots & & \\ 0 & & 1 & 0 \end{pmatrix} \qquad \lambda E - A = \begin{pmatrix} \lambda + a_1 & \cdots & a_{n-1} & a_n \\ 1 & & 0 & 0 \\ & \ddots & & \\ 0 & & 1 & \lambda \end{pmatrix}$$

Нормальная форма Фробениуса – матрица состоит из блоков $A_1, .., A_s$

$$\begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_s \end{pmatrix}$$

$A_1, .., A_s$ - матрицы Фробениуса

И характеристический многочлен A_i должен быть делителем характеристического многочлена A_{i+1}

Теорема. Для любой матрицы существует единственная нормальная форма Фробениуса, подобная этой матрице A.

Теорема 3. Пусть $f(\lambda)$ – минимальный для φ. $f(\lambda)=f_1(\lambda)\dots f_s(\lambda)$, где сомножители попарно взаимно просты, т.е. $НОД(f_i,f_k)=1 \ \forall i\neq k$.Тогда $V=V_1\oplus\dots\oplus V_s$, где $V_i=Kerf_i(\varphi)$, V_i - инвариантно относительно φ

Д-во: Рассмотрим в начале произвольные многочлены $g(\lambda)$, $h(\lambda)$

Ясно, что $g(\varphi)h(\varphi)=gh(\varphi)$

$\varphi f_i(\varphi)=f_i(\varphi)\varphi$

Пусть $x\in V_i$, т.е. $f_i(\varphi)x=0$, но V_i - инвариантно относительно φ, тогда $0=\varphi 0=\varphi f_i(\varphi)x=f_i(\varphi)\varphi x=0$

Индукция по s.

$s=2 \quad f(\lambda)=g(\lambda)h(\lambda) \quad НОД(f,g)=1$

$\exists u,v \,/\, u(\lambda)g(\lambda)+v(\lambda)h(\lambda)=1$ подставим φ

$u(\varphi)g(\varphi)x+v(\varphi)h(\varphi)x=x$

$x_1=u(\varphi)g(\varphi)x \qquad x_2=v(\varphi)h(\varphi)x$

$x=x_1+x_2$

$h(\varphi)x_1=0 \Rightarrow x_1\in Ker(h(\varphi))$

$g(\varphi)x_2=0 \Rightarrow x_2\in Ker(g(\varphi))$

Пространство разложилось в сумму. Сумма прямая, т.к.

О. $f(\lambda)$ аннулирует линейное преобразование φ на W, если $\forall x\in W \ f(\varphi)x=0$

Среди всех многочленов, аннулирующих φ, выберем минимальной степени. Это минимальный многочлен подпространства.

Утверждения.

1) Минимальный многочлен существует и единственный $\forall\varphi$ и $\forall W$
2) Если $W_1\subseteq W_2$, то $f_1(\lambda)$ делитель $f_2(\lambda)$
3) $НОК(f_1(\lambda),f_2(\lambda))$ –минимальный многочлен W_1+W_2
4) Минимальный многочлен $W_1\cap W_2$ делитель $НОД(f_1(\lambda),f_2(\lambda))$

Пусть есть линейное пространство V над полем Ф и есть линейное преобразование φ.

$e_1,\dots,e_n$ - базис

$$[\varphi]_e=\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

Тогда V раскладывается в прямую сумму $V=V_1\oplus V_2$

V_1, V_2 - инвариантны относительно φ

$|[\varphi]-\lambda E|=f_1f_2=|A-\lambda E||B-\lambda E|$

Минимальный для φ $НОК(f_1,f_2)$

Для любой матрицы A существует единственная фробениусовая матрица F: $F\sim A$

$F=diag(F_1,\dots,F_t)$ (по теореме)

F_i - клетка Фробениуса, она имеет вид $F_i=\begin{pmatrix} -a_1 & & -a_{n_i-1} & -a_{n_i} \\ 1 & & 0 & 0 \\ & \ddots & & \\ 0 & & 1 & 0 \end{pmatrix}$

$n=n_1+\dots+n_t$

$\lambda E-A\sim diag(1,..,1,d_{n-t+1}(\lambda),..,d_n(\lambda))$

$|\lambda E-F_i|=d_{n-i+1}(\lambda)$

В базисе $e_1,\dots,e_n$ $[\varphi]_e=A$, а в другом $[\varphi]=F$

Т.о. если мы будем рассматривать нормальную форму Фробениуса для φ, то получим, что $V=V_1\oplus\dots\oplus V_t$

О. p_j^{kij} элементарный делитель, если степень отлична от 0.

Минимальный многочлен на подпространство V_i есть $|\lambda E-F_i|$. Это следует из след. леммы.

Лемма. У матрицы Фробениуса характеристический и минимальный многочлен одинаковы.

Д-во:

Для F_i $M_{ni}=d_{n-i+1}(\lambda)$

M_{ni-1}=1. т.к. есть минор этого порядка, соответствующий E (см. под главной диагональю)

Если f(λ) – минимальный многочлен V

$f(\lambda)=f_1(\lambda)\dots f_s(\lambda)$, то по теореме 3 имеем разложение $V=W_1\oplus\dots\oplus W_s$, где $W_i=Kerf_i(\varphi)$

$f_i(\lambda)$ – минимальный многочлен на W_i

$A\sim(A_1,\dots,A_s)$

A_i - матрица сужения преобразования φ на W_i

Имеем второе разложение (через Фробениуса).

Рассмотрим $W_i\cap V_1$. Оно инвариантно относительно φ, как персечение инвариантных подпространств.

$f(\lambda)=d_n(\lambda)$

$d_n(\lambda)=f_1(\lambda)\dots f_s(\lambda)$

$d_n(\lambda)=p_1^{k11}(\lambda)\dots p_s^{k1s}$

У F_1 диагональный множитель $d_n(\lambda)=p_1^{k11}(\lambda)\dots p_s^{k1s}$

У F_2 диагональный множитель $d_{n-1}(\lambda)=p_1^{k21}(\lambda)\dots p_s^{k2s}$

У F_t диагональный множитель $d_{n-t+1}(\lambda)=p_1^{kt1}(\lambda)\dots p_s^{kts}$

дальше идут единицы.

Минимальный многочлен на W_1 - p_1^{k11}

$W_i=Kerf_i(\varphi)\Leftrightarrow f_i(A)x=0$

Применим теорему 3 к F_1. Тогда V_1 можно разложить в прямую сумму.

$F_1\sim diag(F_{11},..,F_{1s})$ F_{1l} - матрица Фробениуса для p_l^{k1l}

$|\lambda E-F_{1j}|=p_j^{k1j}$ F_{1j} - сопровождающая для p_j^{k1j}

Эти клетки находятся единственным образом. Для каждого элементарного делителя есть единственная соответствующая ему матрица Фробениуса.

Аналогичный результат получаем для $F_2,..,F_t$

$F_i\sim daig(F_{i1},\dots,F_{is})$

$|\lambda E-F_{ij}|=p_j^{kij}$

Т.о. мы доказали следующую теорему.

Теоерема 4. Любая матрица A подобна единственной с точностью до перестановки клеток блочно-диагональной матрице $diag(F_{ij})$ i=1,..,t j=1,..,s, где $|\lambda E-F_{ij}|=p_j^{kij}$, F_{ij} - клетка Фробениуса, соответствующая элементарному делителю $p_j^{kij}(\lambda)$ ($k_{ij}>0$)

Клетку Фробениуса можно заменить жордановой клеткой.

$p_j^k=(\lambda-\alpha_j)^k$

$$\begin{pmatrix}\alpha_j & & 0\\ 1 & \ddots & \\ & \ddots & \ddots \\ 0 & & 1 & \alpha_j\end{pmatrix}\sim\begin{pmatrix}\dots & & \\ 1 & & 0\\ & \ddots & & 0\\ 0 & & 1\end{pmatrix}$$ вверху коэффициенты бинома

т.к. система инвариантых множителей одинаковы.

Теорема Жордана. Над полем комплексных числе любая матрица A подобна единственной с точностью до перестановок жордановой матрице.

О. f(λ) – минимальный многочлен для вектора e

$f(\varphi)e=0$ f(λ) аннулирует φ на вектор e

минимальный это минимальный степени аннулирующий.

Рассмотрим такую систему $e,\varphi e,..,\varphi^{m-1}e,\varphi^m e$, что первые m векторов образуют линейную независимую систему. А система m+1 векторов уже линейно зависима.

$e\neq0$, тогда такое m существует.

Тогда существуют коэффициенты, что $\alpha_0 e + \varphi e + ... + \alpha_{m-1}\varphi^{m-1}e = \varphi^m e$

f(λ)=λ $\lambda^m - \alpha_{m-1}\lambda^{m-1} - ... - \alpha_1\lambda - \alpha_0$. Этот многочлен аннулирует φ на e и минимальный.

Теперь пусть для пространства V есть базис $e_1,..,e_n$. Для каждого вектора из базиса построим его минимальный многочлен. Получим систему $f_1(\lambda),..,f_n(\lambda)$. Тогда минимальный многочлен для V будет НОК($f_1(\lambda),..,f_n(\lambda)$)

Конечные поля

Лемма. Если a,b∈G, ab=ba, |a|=k, |b|=l, НОД(k,l)=1, то |ab|=kl

Д-во:

|a|=k => a^k=e и ∀ t<k $a^t \neq e$

Аналогично для b^l

ab=ba => легко по индукции доказывается, что $a^i b^j = b^j a^i$. Поэтому

$(ab)^{kl} = (a^k)^l (b^l)^k$=e

Докажем, что kl – min

$(ab)^m$=e. Докажем, что m делится на kl

e=$(ab)^{ml} = a^{ml}(b^l)^m = a^{ml}$ => a^{ml}=e => ml делится на k. А т.к. НОД(k,l)=1, то m делится на k.

Аналогично m делится на l.

Теорема. Если F – поле и G – конечная подгруппа мультипликативной группы из этого поля, т.е. |G|<∞ и G – подгруппа {F\{0},*}, тогда G- циклическая.

Д-во:

G={$g_1,\dots g_s$} Пусть $m_1,\dots m_s$ - порядки элементов g_i $(g_i)^{mi}$

m= $\max_i\{m_i\}$=m_k

m_i - делитель s (следствие 4 из теоремы Лагранжа) => $m_i \leq s$

Докажем, что m=s, т.е g_k будет порождающим элементом

Докажем, что m_i делитель m.

Пусть существует i, что m не делится на m_i, тогда существует простое p, что m_i=pl и $m_i \equiv 0(p)$, а $m \not\equiv 0(p)$

Тогда $|g_i^l|$=p , т.к. $(g_i^l)^p$=e $g_i^l \in G$

$g_k g_i^l \in G$

НОД(p,m)=1 => по лемме $|g_k g_i^l|$=pm≥m. Противоречие.

Пусть |F|=q

О. Элемент a наз. первообразным элементом поля F, если его порядок равен q-1 |a|=q-1

Следствие.

1) ∀ a∈F\{0} |a| - делитель (q-1)

2) Для любого d – делителя q-1 существует элемент a из поля F, что |a|=d

3) 0≠a∈F, 0≠b∈F и |a|=|b| => (a)=(b)

4) ∀ a∈F является корнем многочлена x^q=x. Этот многочлен не имеет кратных корней. (все корни различные)

|F|=q χ(F)=p – простое.

Z/p≅F_0={e,2e,…,(p-1)e,0} отождествляем с {1,2,…,p-1,0}

F_0 - минимальное подполе F

Рассмотрим кольцо многочленов F_0[x]

Лемма. ∀ a∈F ∃ f(x)∈F_0[x] / f(a)=0

Д-во: фиксируем a

Множество всех многочленов с этим свойством – идеал. Он имеет порождающий d(x)

d(x) – минимальный многочлен элемента a над полем F_0 вычетов

Теорема 2. |F|=q χ(F)=p – простое

1) ∃ n / q=p^n

2) Если F' – подполе F => $|F'|=p^m$, где m делитель n
3) F" – подполе F и $|F'|=|F"|$ => F'=F"
4) $\forall$ d – делителя n $\exists$ F' / $|F'|=p^d$

Д-во: Пусть $a \in F_0$

Через F_a обозначим минимальное подполе F, которое содержит этот элемент a.

Если a=0, то $F_a=F_o$

Пусть $a\neq 0$, но $a \in F_0$ => $F_a=F_0$

Рассмотрим $a \notin F_0$

$\{\alpha_0+\alpha_1 a\}$ $\alpha_i \in F_0$

Все $\alpha_0+\alpha_1 a$ различные. Действительно, пусть $\exists \beta_0,\beta_1 \in F_0$, что $\beta_0+\beta_1 a=\alpha_0+\alpha_1 a$

$\alpha_1=\beta_1$ => $\alpha_0=\beta_0$

$a_1\neq\beta_1$ => $(\beta_1-\alpha_1)a=\alpha_0-\beta_0$ $0\neq\beta_1-\alpha_1 \in F_0$ => существует обратный => $a \in F_0$ Противоречие.

Т.о. имеем p^2 различных элементов поля.

Любо эти p^2 исчерпывают все поле F => $p^2=q$

Либо нет.

Тогда рассмотрим $M_s=\{\alpha+\alpha_1 a+...+\alpha_{s-1}a^{s-1}\}$

$M_0=F_0$

Докажем, что $|M_s|=p^s$ (индукцией по s)

Пусть $a^s \notin M_s$, тогда сделаем множество M_{s+1}

Предположим, что $|M_{s-1}|=p^{s-1}$. Докажем, что $|M_s|=p^s$

$$\sum_{i=0}^{s}\alpha_i a^i \neq \sum_{i=0}^{d}\beta_i a^i \Rightarrow \alpha_s\neq\beta_s$$

$$(\beta_s-\alpha_s)a^s=\sum_{i=1}^{s-1}\gamma_i a^i$$ => как и раньше $a^s \in M_s$ Противоречие.

Теорема 3. $\forall$ p – простое, $\forall$ n – натуральное $\exists$ F / $|F|=p^n$

Д-во: $F_0=Z/p$

Рассмотрим над этим полем многочлен $f(x)=x^{p^n}-x$

Ф – поле, которое содержит все корни f(x). Действительно

$\{0,1,\alpha_2,\ldots,\alpha_{p^n-1}\}$ – все корни

Кратных корней нет, т.к. f'(x)=-1 (по лемме)

Ф – расширение F_0

Докажем, что это множество замкнуто относительно *

$\alpha,\beta \in \Phi$

$\alpha^{p^n}=\alpha$ $(\alpha\beta)^{p^n}=\alpha\beta$ $\forall \alpha,\beta\neq 0$

$\beta^{p^n}=\beta$

Докажем, что это множество поле.

$\alpha^{p^n-1}=1$

$(\alpha\beta)^{p^n}=\alpha\beta$ => $\alpha\beta((\alpha\beta)^{p^n-1}-1)=0$. Т.к. делителей 0 нет, то $(\alpha\beta)^{p^n-1}=1$