Лекции по высшей алгебре Н.А. Вавилова, второй семестр бакалавриата Чебышёва (набор 2015 года)

8 июля 2016 г.

Планы на семестр:

1. Вычислительная линейная алгебре (определители, собственные числа и вектора, канонические формы матриц, в т.ч. Жорданова форма) + кусок многочленов от n переменных в середине
2. Геометрия пространств со скалярными произведениями, квадратичные формы
3. Теория групп
4. Теория представлений

Оглавление

Глава 1

Вычислительная линейная алгебра

Опять план:

1. Элементарные преобразования
2. Определители
3. Маленький кусочек многочленов от нескольких переменных, в частности симметрических многочленов
4. Собственные числа
5. Канонические формы матриц

1.1 Элементарные преобразования

1.1.1 Элементарные трансвекции

Rem. Вспомним, что обычно мы работаем над ассоциативным кольцом с единицей R, пока не начинаем что-нибудь доказывать. $M(n,R)$ — матрица степени n над R; $GL(n,R) = M(n,R)* = \{x \in M(n,R) | \exists\ y \in M(n,R) : xy = e = yx\}$ — полная линейная группа степени n над R.

Def. $t_{ij}(\xi) = e + \xi e_{ij},\ 1 \leq i \neq j \leq n, \xi \in R$ — элементарная трансвеция, матрица вида

$$\begin{pmatrix} 1 & \dots & \dots & 0 \\ 0 & \ddots & \dots & 0 \\ \dots & \xi & \ddots & \dots \\ 0 & \dots & \dots & 1 \end{pmatrix}$$

— как единичная, только с приписанной буквой ξ на месте (i,j), которую можно рассматривать как отображение:

$$t_{ij}(\xi) : R \to M(n,R)$$

$$\xi \mapsto t_{ij}(\xi)$$

Lemma. *t_{ij} аддитивно:*

$$\forall\ \xi, \phi \in R\ t_{ij}(\xi + \phi) = t_{ij}(\xi) t_{ij}(\phi)$$

Corollary (1)**.** Заметив, что $t_{ij}(0) = e$, понимаем, что $t_{ij}^{-1}(\xi) = t_{ij}(\xi^{-1})$.

То есть отображение t_{ij} — гомоморфизм групп (из аддитивной R в мультипликативную $M(n, R)$, на самом деле даже в $GL(n, R)$).

Corollary (2)**.** $t_{ij}(\xi) \in GL(n, R)$

Note (На будущее)*.* $det(t_{ij}(\xi)) = 1$

Левая нижняя и правая верхняя унитреугольные матрицы — откуда названия? Унипотентный элемент — т.ч. $(x-e)^n = 0$. Потом узнаем, что матрица унитреугольная над коммутативным $R \Leftrightarrow$ все собственные числа равны 1.

Proof. 1. Напишем правую часть:

$$(e + \xi e_{ij})(e + \phi e_{ij}) = e + \xi e_{ij} e + e\phi e_{ij} + \xi e_{ij}\phi e_{ij} = e + (\xi + \phi)e_{ij} + \xi\phi(e_{ij})^2 =$$

$$= (i \neq j)e + (\xi + \phi)e_{ij},$$

а это в точности левая часть.

2. (Метод Лагранжа) НУО мы можем считать, что $i = 1, j = 2$, потому что нас действительно интересует поведение только двух столбцов и двух строк в матрице. То есть достаточно провести вычисление с матрицами 2×2.

$$\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \phi \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \xi + \phi \\ 0 & 1 \end{pmatrix}$$

□

Note. Аналогично, если в вычислениях участвует k индексов, достаточно проводить вычисления для матриц $k \times k$.

Rem. Коммутатор элементов группы x, y $[x, y] = xyx^{-1}y^{-1}$

Theorem 1.1.1 (Коммутационная формула Шевалле)**.**

$$\xi, \phi \in R, i \neq j, h \neq k;\ [t_{ij}(\xi) t_{hk}(\phi)] = \begin{cases} e, j \neq h, i \neq k \\ t_{ik}(\xi\phi), j = h, i \neq k \\ t_{hj}(-\phi\xi), j \neq h, i = k \end{cases}$$

Note. В оставшемся нерассмотренным случае никакого более короткого выражения для записи коммутатора нету.

Proof. 1.

$$(e+\xi e_{ij})(e+\phi e_{hk})(e-\xi e_{ij})(e-\phi e_{hk}) =$$

$$= (e+\xi e_{ij}+\phi e_{hk}+\xi\phi e_{ij}e_{hk})(e-\xi e_{ij}-\phi e_{hk}+\xi\phi e_{ij}e_{hk}) = e+\xi\phi e_{ij}e_{hk}-\phi\xi e_{hk}e_{ij}$$

Как это мы так взяли и сделали последний переход? А мы внимательно посмотрели на скобочки и подумали, сколько слагаемых получается с каким-нибудь e_{st} и в какой суммарной по (i,j) и (h,k) ешки. С нулевой степенью мы все написали, со степенью хотя бы три все обнуляется, потому что произведение обязательно превратится в 0, со степенью один все сократится, со степенью два все выписали.

Теперь посмотрим: $\xi\phi e_{ij}e_{hk} \neq 0$ $j=h, -\phi\xi e_{hk}e_{ij} \neq 0$ $i=k$, и оба условия одновременно не выполняются.

2. Достаточно рассматривать матрицы 4×4, но если нам нужна матрица 4×4, то там заведомо все обнуляется при перемножении, кроме главной диагонали, так что интересные случаи - только 3×3, но их немного.

□

Упражнение. Посмотреть на исключенный случай 2×2:

$$\begin{pmatrix}1 & \xi\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ \phi & 1\end{pmatrix}$$

и понять, что действительно ничего хорошего.

Def (Парочка важных подгрупп в GL)**.** $E(n,R) = \langle t_{ij}(\xi), 1\leq i\neq j\leq n, \xi\in R\rangle \subseteq GL(n,R)$ — элементарная группа степени n над кольцом R.

$SL(n,R) = \{g\in GL(n,R) | det(g)=1\}\subseteq GL(n,R)$, даже $\trianglelefteq GL(n,R)$ — специальная линейная группа.

Note (Спойлер). Теорема Суслина: R коммутативно, $n\geq 3 \Rightarrow E(n,R)\trianglelefteq GL(n,R)$.

А совсем скоро мы узнаем, что $E(n,K) = SL(n,K)$.

1.1.2 Элементарные псевдоотражения

Def. Как водится, R ассоциативное с 1. $1\leq i\leq n, \epsilon\in R^*; d_i(\epsilon) = e+(\epsilon-1)e_{ii} = diag(1,\dots,\epsilon,\dots,1)$ — псевдоотражение (diagonal dilation; называется так потому, что $\epsilon=-1$ — геометрическое отражение вектора).

Rem. $diag(\epsilon_1,\dots,\epsilon_n)^{-1} = diag(\epsilon_1^{-1},\dots,\epsilon_n^{-1}), \epsilon_i\in R^*$

Обычное умножение диагональных матриц совпадает с умножением по Адамару:

$$diag(\epsilon_1,\dots,\epsilon_n)diag(u_1,\dots,u_n) = diag(\epsilon_1u_1,\dots,\epsilon_nu_n)$$

Lemma.

$$d_i : R^*\to GL(n,R)$$
$$\epsilon\mapsto d_i(\epsilon)$$

— *гомеоморфизм, т.е.* $d_i(\xi)d_i(\eta) = d_i(\epsilon\eta)$

Lemma (2)**.**

$$[d_i(\epsilon), d_j(\eta)] = 1, i \neq j; = d_i([\epsilon, \eta]), i = j$$

Lemma (3)**.**

$$\epsilon \in R^*, \xi \in R; d_i(\epsilon) t_{jh}(\xi) d_i^{-1}(\epsilon) = \begin{cases} t_{jh}(\xi), i \neq j, h \\ t_{jh}(\epsilon\xi), i = j \\ t_{jh}(\xi\epsilon), i = h \end{cases}$$

Def. $1 \leq i \neq j \leq n, \epsilon \in R^*; d_{ij}(\epsilon) = d_i(\epsilon) d_j(\epsilon^{-1})$

Lemma (4)**.**

$$\xi, \phi \in R, 1 + \xi\phi \in R^*; t_{ij}(\xi) t_{ji}(\phi) d_j(1 + \phi\xi) = d_i(1 + \xi\phi) t_{ji}(\phi) t_{ij}(\xi)$$

Corollary. $1 + \phi\xi \in R^*$

Corollary (2, важное!)**.** $d_{ij}(\epsilon) \in E(n, R)$

Def (И еще одна группа)**.** $GE(n, R) = \langle t_{ij}(\xi), d_h(\epsilon), 1 \leq i \neq j \leq n, 1 \leq h \leq n, \epsilon \in R^*, \xi \in R \rangle$ и по Лемме 3 $E(n, R) \trianglelefteq GE(n, R) \leq GL(n, R)$

1.1.3 Матрицы перестановки

$$S_n \hookrightarrow GL(n, R) = Aut_R(n, R^n), R - \text{кольцо с } 1$$

$$\pi \mapsto (\pi) - \text{ матрица перестановки}$$

— гомоморфизм.

Слева переставляются $1, \ldots n$, справа матрица переставляет базисные вектора $\mathbb{R}^n$: $e_1, \ldots e_n$.

$$(\pi)_{ij} = \delta_{i,\pi(j)}$$

Упражнение. Как-нибудь понять, что это действительно гомоморфизм.

Note. Вообще мы еще не знаем, но очень скоро узнаем, что

$$S_n = \langle (i, j), 1 \leq i < j \leq n \rangle$$

— группа перестановок породлается всеми транспозициями, на самом деле хватает еще меньше:

$$\langle (1, 2), (2, 3), \ldots (n - 1, n) \rangle$$

И вот чтобы не проверять, что та штука —- гомоморфизм, можно задать образы транспозиций

Def.

$$(i,j)\mapsto w_{ij}=\begin{pmatrix}
1 & 0 & \dots & 0\\
0 & \ddots & \dots & 0\\
0 & \dots & 1 & \dots & 0\\
\dots & 0 & \dots & 1 & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & \ddots & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & 1 & \dots & 0 & \dots & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & \ddots & 0
\end{pmatrix}=e-e_{ii}-e_{jj}+e_{ij}+e_{ji}\in GE(n,R),$$

почему она там лежит (метод Лагранжа):

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}-1&0\\0&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

но если бы не было последней слева матрицы, которая меняет нам знак на правильный, то получилась бы тоже какая-то осмысленная матрица. Это дело называют signed permutation matrices = означенные матрицы перестановки. Эти матрицы занимаются перестановками означенного базиса (signed base): $\pm e_1,\cdots\pm e_n$, но это не совсем перестановки $2n$ элементов (в определенном смысле такая перестановки "уважает"знак).

$$(i,j)\mapsto \tilde{w_{ij}}=\begin{pmatrix}
1 & 0 & \dots & 0\\
0 & \ddots & \dots & 0\\
0 & \dots & 1 & \dots & 0\\
\dots & 0 & \dots & 1 & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & \ddots & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & -1 & \dots & 0 & \dots & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & 1 & \dots & 0\\
\dots & \ddots & 0
\end{pmatrix}=e-e_{ii}-e_{jj}+e_{ij}-e_{ji}\in E(n,R)$$

и *det* у них кстати $=1$, они просто произведение элементарных трансвекций.

Def. $N(n,R)$ — группа мономиальных матриц $\leq GL(n,R)$ таких, что в $\forall$ столбце/строке есть ! ненулевой элемент (они все автоматически обратимые).

1.1.4 Элементарные преобразования матриц

умножение на матрицу одного из трех типов

1. $t_{ij}(\xi), \xi \in R$
2. $d_i(\epsilon), \epsilon \in R^*$
3. w_{ij}

с какой-то стороны.

Note. $A \in M(m, n, R)$, ну и соответстующие элементарные преобразования из $M(*, R)$ разных размеров в зависимости от того, с какой стороны на них умножаем.

1.

$$t_{ij}(\xi)A = (e + \xi e_{ij})A = (e + \xi e_{ij}) \begin{pmatrix} a_{i1} & \dots & a_{in} \\ \vdots & \dots & \vdots \\ a_{j1} & \dots & a_{jn} \end{pmatrix} = \begin{pmatrix} a_{i1} + \xi a_{j1} & \dots & a_{in} + \xi a_{jn} \\ \vdots & \dots & \vdots \\ a_{j1} & \dots & a_{jn} \end{pmatrix}$$

$$At_{ij}(\xi) = \begin{pmatrix} a_{1i} & \dots & a_{1j} & \\ \vdots & \vdots & \vdots & \\ a_{mi} & & \dots & a_{mj} \end{pmatrix} (e + \xi e_{ij}) = \begin{pmatrix} a_{1i} & \dots & a_{1j} + a_{1i}\xi & \\ \vdots & \vdots & \vdots & \\ a_{mi} & \dots & a_{mj} + a_{mi}\xi & \end{pmatrix}$$

2.

$$d_i(\xi)A = (e + (\epsilon - 1)e_{ii})A = \begin{pmatrix} \dots & \dots & \dots \\ \epsilon a_{i1} & \dots & \epsilon a_{in} \\ \dots & \dots & \dots \end{pmatrix}$$

$$Ad_i(\epsilon) = \begin{pmatrix} \dots & a_{1i}\epsilon & \dots \\ \vdots & \vdots & \vdots \\ \dots & a_{mi}\epsilon & \dots \end{pmatrix}$$

3. Не то, чтобы мы не умели уже делать это преобразование, коли оно почти композиция трансвекций, но оно важное, так что пропишем его явно тоже:

$$w_{ij}A = (e - e_{ii} - e_{jj} + e_{ij} + e_{ji})A = (e - e_{ii} - e_{jj} + e_{ij} + e_{ji}) \begin{pmatrix} a_{i1} & \dots & a_{in} \\ \vdots & \dots & \vdots \\ a_{j1} & \dots & a_{jn} \end{pmatrix} = \begin{pmatrix} a_{j1} & \dots & a_{jn} \\ \vdots & \dots & \vdots \\ a_{i1} & \dots & a_{in} \end{pmatrix}$$

$$Aw_{ij} = \begin{pmatrix} a_{1i} & \dots & a_{1j} & \\ \vdots & \vdots & \vdots & \\ a_{mi} & & \dots & a_{mj} \end{pmatrix} w_{ij} = \begin{pmatrix} a_{1j} & \dots & a_{1i} & \\ \vdots & \vdots & \vdots & \\ a_{mj} & & \dots & a_{mi} \end{pmatrix}$$

1.1.5 Комбинаторная эквивалентность матриц

= приведеине матриц элементарными преобразованиями над строками (к определенному "каноническому"виду).

Note. Всем понятно, что в этом вопросе очень важно, над каким кольцом R у нас матрицы. Задача нормально решается только тогда, когда R — поле (ну или тело), и сейчас будет видно, почему.

Итак, мы считаем, что $R = K$ — поле, и $x \in M(m, n, K)$. Можно проследить за доказательством и понять, что в случае тела почти ничего не меняется.

Theorem 1.1.2.

$$\forall\ x \in M(m,n,K)\ \exists\ h \in GE(m,K):$$

$$hx = \left(\begin{array}{cccccccccccccc} 0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * \\ & & & & & & & \dots & & & & & & & \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & * & \dots & * \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ & & & & & & & \dots & & & & & & & \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

— "эшелонированный вид"(row echelon), единички называются ведущими элементами (pivot), все нулевые строки в конце.

Proof. Индукция по m. База: $m = 1 : (0, \dots), *, \dots), * \neq 0$, умножили строчку на обратный слева.

Переход: Несколько первых столбцов матрицы возможно нулевые. Находим первый ненулевой, переставляем строчку с ненулевым элементом наверх, умножаем на обратные к элементу, на это месте получилась единичка. Делаем под единичной нули в столбце, вычитая из строк домноженную на нужный коэффициент первую строку, и теперь к матрице x' справа снизу от единички применяем индукционное предположение. После этого над первым ведущим элементом x' тоже можем получить все нолики, повычитав строчку, домноженную на нужные коэффициенты, из тех, которые над ней.

$$x = \begin{pmatrix} 0 & \dots & 0 & * & \dots \\ \vdots & \vdots & \vdots & x' & \\ 0 & \dots & 0 & & \end{pmatrix}$$

□

Corollary (То утверждение, которое называют комбинаторной эквивалентностью)**.**

$$\forall\ x \in M(m,n,K)\ \exists\ h \in GE(m,K), w \in W_n (S_n \cong W_n : \pi \leftrightarrow (\pi) = w):$$

$$hxw = \left(\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & * & \dots & * \\ 0 & 1 & \dots & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & * & \dots & * \\ \hline 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \multicolumn{3}{c}{\dots\dots\dots} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right) \in GE(m,K) \setminus M(m,n,K)/W_n$$

— ступенчатые (трапециевидные матрицы).

Размер блока с единичками по диагонали называется рангом матрицы x, и для поля такое определение совпадает с остальными всевозможными определениями ранга. Матрицу из $*$ пока не контролируем, потому что класс преобразований, которые мы применяем справа, маловат.

1.1.6 Строгая эквивалентность матриц

$x \in M(m,n,K)$

Corollary (из того, что было уже понято в предыдущем разделе)**.**

$$\forall\ x \in M(m,n,K)\ \exists\ h \in GE(n,K)\ \exists\ g \in E(n,K):$$

$$hxg = \left(\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \multicolumn{3}{c}{\dots\dots\dots} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right)$$

— окаймляющая единичная матрица

То есть при элементарных преобразованиях есть три инварианта: $m, n, r = rank(x)$.

Морально это мы сейчас сказали, что линейные отображения из векторного пространства в векторное пространство конечных размерностей одинаковые $\Leftrightarrow$ размерности их образов одинаковые.

Theorem 1.1.3.

$$\forall\ x \in M(m,n,K)\ \exists\ h \in E(n,K)\ \exists\ g \in E(n,K):$$

$$hxg = \left(\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \multicolumn{3}{c}{\dots\dots\dots} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right) \quad \textit{или при}\ \ m = n\ \ = \begin{pmatrix} 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & \vdots & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & \epsilon \end{pmatrix}, \epsilon \in K^*$$

Def. Вот этот вот ϵ — определитель (det) матрицы x.

//если в квадратной матрице единички заканчиваются раньше, то есть на месте ϵ стоит 0, то $det = 0$; то же самое, когда матрица не квадратная.

Note. Почему такой ϵ в последней строке единственный (то есть почему новое представление единственное) сходу неясно. Над телом, кстати, это вообще неверно.

Proof. Пристально посмотрим на доказательство теоремы из предыдущего параграфа. Увидев в строке ведущий обратимый элемент с помощью трансвекций мы сможем сделать на его месте единицу, поменяв при этом какую-то другую строчку. Ничего не сможем сделать только если $rk = m$, то есть осталась последняя строчка, наверху уже все единички по диагонали, а у нас не единица:

$$\begin{pmatrix} 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & \vdots & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & \epsilon \end{pmatrix}$$

Иначе у нас ситуация

$$\left(\begin{array}{ccccc|c} 1 & \dots & \dots & 0 & 0 & \dots \\ \vdots & \ddots & \vdots & \vdots & 0 & \dots \\ 0 & \vdots & \ddots & 1 & 0 & \dots \\ 0 & \dots & \dots & 0 & \epsilon & \dots \end{array}\right) (n > m)$$

□

Note. Про единственность определителя все еще ничего не ясно, этим мы займемся, когда будем изучать теорию определителей.

Для тела единственность ϵ мы будем иметь в следующем смысле: ! в $T^*/[T^*, T^*] \cup \{0\}$

$M(n, T) \to T^*/[T^*, T^*] \cup \{0\}$ объединенная с нулем факторгруппа

$$x \mapsto det(x)$$

(результат Dieudonne)

Почему это так:

$$\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix} \begin{pmatrix} (\eta\epsilon)^{-1} & 0 \\ 0 & \eta\epsilon \end{pmatrix} \in E(2, R), \epsilon, \eta \in R^* = \begin{pmatrix} \epsilon\eta\epsilon^{-1}\eta^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

Ну и если хотим считать, что $det = 1$, то стоит отождествлять коммутатор с единицей, ну а над полем это получается автоматически.

1.2 Определитель

Краткий исторический экскурс в историю определителя, (не обязательно к прочтению).

Впервые понятие было введено в XVII веке одновременно Лейбницем и японским математиком, скорее всего, под влиянием одного и того же китайского труда.

Это первое определение звучало так:

$x \in M(n, R), R$ - коммутативное с единицей, S_n — симметрическая группа степени n. Матрице x сопоставляется элемент кольца $\mathbb{R}$ $det(x) = \sum\limits_{\pi \in S_n} sign(\pi) x_{1,pi(1)} \dots x_{n,\pi(n)}$.

Знак перестановки - это формально единственные нетривиальный гомоморфизм $S_n \to \{-1, +1\} (\pi \mapsto sign(\pi), sign(\pi\gamma) = sign(\pi) sign(\gamma))$. Все транспозиции, таким образом, переходят либо в 1, либо в -1 одновременно, а S_n порождена ими, так что ! нетривиальные гомоморфизм — это когда все транспозиции перешли в -1.

А если кольцо R некоммутативно, то можно рассматривать $\sum\limits_{\pi \in S_n} sign(\pi) x_{pi(1),1} \dots x_{\pi(n),n}$, которые называют row determinant, и это не то же самое, что column determinant: например, посмотрим на это матрицу:

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix}$$

А вообще понятно, что это плохой способ считать определитель, ведь там $n!$ слагаемых (и никто никогда так определитель не считает). Кроме того, непонятно, почему рассматривать такую странные штуку вообще интересно, почему менее интересно рассматривать перманент — аналогичную беззнаковую сумму ($per(x) = \sum\limits_{\pi \in S_n} x_{1,pi(1)} \dots x_{n,\pi(n)}$)?

Осталось сказать еще о двух значимых событиях в истории определителя: в начале XIX века Grassmann перешел от вычислительных упражнений с определителями к их геометрической интерпретации, а в конце XIX века Вейерштрасс придумал облегченную теорию определителей, чтобы учить студентов, и это ровно то, что будет сейчас рассказано.

1.2.1 Определитель по Вейерштрассу (Det)

Пусть $x = (x_{*1}, \dots x_{*n}) \in M(n, R), x_{*i} \in R^n, R$ — **коммутативное** кольцо с единицей.

Rem. Можно завести или рассматривать определитель по строкам, но мы докажем, что в случае коммутативного кольца это одно и то же: $Det(x) = Det(x^T)$. А еще потом докажем, что $det(x) = Det(X)$.

Def (Определитель по Вейерштрассу)**.**

$$Det : R^n \times \dots \times R^n \to R :$$

1. Det линеен по каждому аргументу = полилинеен
2. Det знакопеременен
3. Det нормирован: $Det(e_1, \dots e_n) = 1 = det(e)$

Расшифровка первых двух свойств:

1. = линейны все парциальные отображения (фиксируются все аргументы кроме одного и рассматривается это как функция)

   Def. $f : U_1 \times \dots \times U_n \to V$ — n-линейно, если

   $$\forall\ i \in \{1, \dots n\}\ \forall\ u_j \in U_j j \neq i\ \forall u_i', u_i'' \in U_i\ \forall\ \lambda \in R$$

   $f(u_1, \dots u_{i-1}, u_i' + u_i''\lambda, \dots u_n) = f(u_1, \dots u_{i-1}, u_i', \dots u_n) + f(u_1, \dots u_{i-1}, u_i'', \dots u_n)\lambda$

   — аддитивность + однородность степени 1.

2. $Det = 0$, когда два аргумента равны = антисимметричность.

   В этом месте важно отметить, что из знакопеременности следует кососимметричность (= что-то меняет знак при перестановке двух аргументов). Это легко проверяется, если расписать $f(\dots, u_i + u_j, \dots u_i + u_j, \dots)$. Но обратное неверно: из того, что $f(\dots u, \dots u, dots) = -f(\dots u, \dots u, \dots)$ не следует, что $f(\dots, u, \dots, u, \dots) = 0$ в поле характеристики 2. Вот, например, в определении определителя в Википедии ошибка.

Rem. Почему определитель $\exists, !$ нам не понятно.

Corollary (из определения)**.** Определитель хорошо меняется при элементарных преобразованиях над столбцами (про строки ничего пока сказать не можем):

1. $Det(xt_{ij}(\xi)) = Det(x)$
2. $Det(xd_i(\epsilon)) = Det(x)\epsilon$, верно и при $\epsilon \notin R^*$
3. $Det(xw_{ij}) = -Det(x)$

Corollary (2)**.** Если $x = (x_{*1}, \dots, x_{*n}), x_{*i} = \sum\limits_{j \neq i} x_{*j}\lambda_j \Rightarrow Det(x) = 0$

//в случае R не поля здесь написана не линейная зависимость

1.2.2 Определитель как альтернированная сумма (det)

Def. R — коммутативное с единицей,

$$x \in M(n,R), det(x) = \sum_{\pi \in S_n} sign(\pi) x_{1\pi(1)} \dots x_{n\pi(n)}$$

$$sign(\pi) = (-1)^{inv(\pi)}, inv(\pi) = |\{(ij) : i < j, \pi(i) > \pi(j)\}|$$

— знакопеременная формула для определителя.

Note (Про знаки перестановок и около). 1. Каждое слагаемое в сумме без знака - это расстановка n небьющих друг друга ладей на доске $n \times n$

2. Если R коммутативно, то $det(x) = \sum_{\pi \in S_n} x_{\pi^{-1}(1)1} \dots x_{\pi^{-1}(n)n}$, ведь $sign(\pi) = sign(\pi^{-1})$

3. $\sigma, \pi \in S_n, x_{\sigma(1)\pi(1)} \dots x_{\sigma(n)\pi(n)} = x_{1\pi\sigma^{-1}(1)} \dots x_{n\pi\sigma^{-1}(n)} = x_{\sigma\pi^{-1}(1)1} \dots x_{\sigma\pi^{-1}(n)n}$

   Общее правило знаков: произведение $x_{\sigma(1)\pi(1)} \dots x_{\sigma(n)\pi(n)}$ входит в det со знаком $sign(\pi\sigma^{-1}) = sign(\sigma)sign(\pi^{-1}) = sign(\pi)sign(\sigma)$

Rem (Про транспонирование). $T : M(m,n,R) \to M(n,m,R^{opp})$; R коммутативно $\Rightarrow R = R^{opp}$, т.е. у нас $M(n,R) \to M(n,R), x \mapsto x^T$, и операция обладает следующими свойствами: $(x+y)^T = x^T + y^T, (xy)^T = y^T x^T, e^T = e$

Теперь нам интересно, как связаны определители матрицы и ее транспонированной.

Theorem 1.2.1.

$$det(x) = det(x^T)$$

Proof. R коммутативно и $sign(\pi) = sign(\pi^{-1})$:

$$det(x^T) = \sum_{\pi \in S_n} sign(\pi)(x^T)_{1\pi(1)} \dots (x^T)_{n\pi(n)} = \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots x_{\pi(n)n} = (\text{по Note})\, det(x)$$

□

1.2.3 Цикленный тип и дискриминант

Def. Пусть $\pi \in S_n, i \in \{1, \dots n\}$; $\lessdot i, \pi(i), \dots, i$, ведь π обратима, так что по крайней мере $\pi^{n!} = id$.

$$\exists\, m : \{i, \pi(i), \dots \pi^{m-1}(i)\} - - - \text{все различны}, \pi^m(i) = i$$

Тогда это множество называется орбитой элемента i под действием перестановки π.

Lemma. *Скажем, что $i \sim j \Leftrightarrow$ орбита i = орбита j. Принадлежать одной орбите под действием π — отношение эквивалентности.*

Орбита i одноэлементна $\Leftrightarrow\ \pi(i) = i$. Такие элементы i называются неподвижными, а орбиты — тривиальными.

$$Fix(\pi) := \{i | 1 \leq i \leq n, \pi(i) = i\};\ Mob(\pi) := \{1, \dots n\} \setminus Fix(\pi)$$

Перестановка π действует на орбитах по циклу, циклы, отвечающие орбитам порядка 2 и больше — истинные циклы. Циклы, отвечающие разным орбитам, называются **независимыми**, и $\{1, \dots n\}$ = дизъюнктное объединение классов эквивалентности, т.е. независимых циклов.

Носитель цикла — элементы, на которые действует данный цикл.

Из этого рассуждения вытекает следующее очень важное соображение:

Statement. *Два независимых цикла коммутируют.*

Это нам очевидно, ведь они при действии затрагивают разные элементы, а значит все равно, в каком порядке их применять.

Corollary. Любая перестановка — произведение независимых циклов.

Ex.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 1 & 5 & 3 & 6 & 9 & 8 & 2 \end{pmatrix} = (1453) \circ (2879) \circ (6)$$

— это каноническое разложение, и строится оно так: пока у нас не закончились цифры в верхнем ряду, мы берем наименьшую из оставшихся, смотрим, куда она переходит, и помечаем эту вершину в верхнем ряду, и так идем по циклу, пока не пришли туда, откуда начинали цикл: $1 \to 4 \to 5 \to 3 \to 3$, следующей берем 2 и тд.

2-циклы называются транспозициями.

Выпишем длины получившихся в каноническом разложении по убыванию длины: $(4, 4, 1)$. Эта последовательность называется цикленным типом перестановки:

$$n_1 \geq n_2 \cdots \geq n_t, (n_1, \dots n_t), \sum n_i = n$$

Def. Величина $derc(\pi) = n - t$ называется декрементом перестановки π.

Theorem 1.2.2. *Две перестановки в S_n сопряжены ($\pi \sim \sigma \in S_n\ \Leftrightarrow\ \exists\ \rho \in S_n :\ \sigma = \rho\pi\rho^{-1}$) $\Leftrightarrow$ они имеют одиноковый цикленный тип.*

Proof. $\Rightarrow$ Пусть $(i_1, \dots i_m)$ — независимый цикл π, тогда $(\rho(i_1), \dots \rho(i_m))$ — независимый цикл для σ:

$$\sigma(\rho(i_1), \dots \rho(i_m)) = \rho\pi(i_1, \dots i_m) = (\rho(i_2), \dots \rho(i_m), \rho(i_1))$$

$\Leftarrow$

$$\pi = (i_1, \dots i_{n_1}) \circ (h_1, \dots h_{n_2}) \circ \cdots \circ (l_1, \dots l_{n_t})$$
$$\sigma = (j_1, \dots j_{n_1}) \circ (k_1, \dots k_{n_2}) \circ \cdots \circ (m_1, \dots l_{m_t})$$

$$\rho = \begin{pmatrix} i_1 & \dots & i_{n_1} & h_1 & \dots & h_{n_2} & \dots \\ j_1 & \dots & j_{n_1} & k_1 & \dots & k_{n_2} & \dots \end{pmatrix}$$

— предъявим полную запись перестановки (там в верхней строке циферки не в правильном порядке стоят, но нам все равно, ведь каждая там есть и ровно один раз, ведь мы удачно решили, что будет записывать и циклы длины один, и у нас $\sum n_i = n$).

Ну осталось только пристально посмотреть и осознать, что это то, что надо. □

Ex (Про циклические типы)**.** Количество циклических типов в S_k — это ровно количество способов разложить k на сумму натуральных слагаемых без учета из порядка. Ну и еще это можно нарисовать в виде диаграмм Юнга, если очень хочется.

$$S_2 : 2 = 2 = 1 + 1 : (12), (1)(2)$$

$$S_3 : 3 = 3 = 2 + 1 = 1 + 1 + 1 : (123), (12)(3), (1)(2)(3)$$

$$S_4 : 4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1 :$$

$$(1234), (123)(4), (12)(34), (12)(3)(4), (1)(2)(3)(4)$$

В качестве веселого упражнения можно выписать цикленные типы у S_5 и S_6.

Theorem 1.2.3.

$$sign(\pi) = (-1)^{decr(\pi)}$$

Proof. Знак, как мы это себе представляем, — это четность количества инверсий в перестановке, или четность количества транспозиций, с помощью которых второй ряд полной записи приводится к первому (четность этого одинаковая, вообще это надо доказывать, но мы справимся). Так вот, умножение на любую транспозицию меняет *decr* на единицу. Действительно, если мы применяем транспозицию внутри цикла, то они разбивает цикл на два, а если снаружи, то она объединяет два цикла. А $decr(t_{ij})$ нечетный. □

Note. Сложнее сказать, что *decr* = *минимальному* количеству транспозиций, необходимому для выражения π в качестве их композиции.

Statement (Как определить знак перестановки по каноническому разложению)**.** *Циклы нечетной длины четны, и π нечетна $\Leftrightarrow$ в ней четное количество циклов четной длины.*

Def.

$$A_n = \{\pi \in S_n | sign(\pi) = 1\}$$

— знакопеременная (alternating) группа.

И, кстати,

$$S_n = A_n \sqcup A_n(ij) \; i \neq j$$

1.2.4 Существование Det

Theorem 1.2.4. *$det(x) \in Det(x)$: определитель как альтернирующая сумма — это определитель по Вейерштрассу.*

Proof. Ну проверим три свойства:

1. Полилинейность. Пусть $x_{*i} = y + z, y, z \in R^n$ — столбцы.

$$det(x) = \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots x_{\pi(i)i} \dots x_{\pi(n)n} =$$

$$= \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots y_{\pi(i)} + z_{\pi(i)} \dots x_{\pi(n)n} =$$

$$= \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots y_{\pi(i)} \dots x_{\pi(n)n} + \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots z_{\pi(i)} \dots x_{\pi(n)n} =$$

$$= det(\dots y \dots) + det(\dots z \dots)$$

   Ну и если около одного из столбцов скаляр приписать, то конечно его можно вынести.

2. Знакопеременность. $x_{*i} = x_{*j}$

$$det(x) = \sum_{\pi \in S_n} sign(\pi) x_{\pi(1)1} \dots x_{\pi(i)i} \dots x_{pi(j)j} \dots x_{\pi(n)n} =$$

$$= \sum_{\pi \in A_n} (x_{\pi(1)1} \dots x_{\pi(i)i} \dots x_{pi(j)j} \dots x_{\pi(n)n} - x_{\pi(1)1} \dots x_{\pi(j)j} \dots x_{pi(i)i} \dots x_{\pi(n)n}),$$

   и поскольку все такие скобки обращаются в 0, то и их сумма обращается в 0.

3. $det(e) = 1$ — очевидно.

□

Lemma. *det верхней треугольной матрицы равен произведению диагональных элементов.*

Proof. Принцип Дирихле (ну сколькими способами мы там сможем расставить n небьющих друг друга ладей? ну только одним) □

1.2.5 Единственность определителя (det = Det)

Theorem 1.2.5. *Отображение $(x_1, \dots x_n) \mapsto det(x_1, \dots x_n)$ — единственное отображение $R^n \times \dots \times R^n$ (n раз) $\to R$, удовлетворяющее свойствам определителя Вейерштрасса Det.*

Proof. Пусть $e_1, \dots e_2$ — стандартный базис в R^n.

$$Det(x_1, \dots x_n) = Det(e_1x_{11} + \dots + e_nx_{n1}, \dots, e_1x_{1n} + \dots + e_nx_{nn}) =$$

$$= \sum_{(i_1,\dots i_n), 1 \le i_j \le n} Det(e_{i_1}, \dots e_{i_n})x_{i1} \dots x_{in} = (\text{знакопеременность})$$

$$\sum_{\text{по перестановкам}} Det(e_{i_1}, \dots e_{i_n})x_{i1} \dots x_{in} = (\text{кососимметричность})$$

$$\sum_{\pi \in S_n} sign(\pi) Det(e_1, \dots e_n)x_{1\pi(1)} \dots x_{n\pi(n)},$$

а $Det(e_i) = 1$ по третьему свойству. □

1.2.6 Блочные матрицы

Пусть $x \in M(m, n, R)$; $m = m_1 + \dots + m_s, \mu = (m_1, \dots m_s)$ — разбиение (неупорядоченное разбиение, которое для краткости будем называть просто разбиением) $m, m_i \in \mathbb{N}; n = n_1, \dots n_t, \nu = (n_1, \dots n_t)$ — разбиение n. Тогда из нашей старой матрицы сделаем новую матрицу: разобьем ее на строки высотой m_i и столбцы, шириной n_j. Строки и столбцы разобьют всю матрицу на блоки: X^{hk} — блок матрицы в пересечении hй строки и kго столбца.

Наша новая матрица

$$\tilde{x} = \begin{pmatrix} x^{11} & \dots & \dots \\ \dots & \ddots & \dots \\ \dots & \dots & x^{st} \end{pmatrix}$$

— размера $s \times t$, вместо элементов — блоки: $\tilde{x}^{hk} \in M(m_h, n_k, R)$. Будем обозначать это как $\tilde{x} \in M(\mu, \nu, R)$ (хотя разумеется матрица теперь вовсе не над тем кольцом, которое тут в скобках написано).

Над такими матрицами можно работать почти как обычно, в терминах блоков, а не элементов, если размерности согласованы.

Сложение: $x, y \in M(\mu, \nu, R)$; $(x + y)^{hk} = x^{hk} + y^{hk}$, если x, y разбиты на ряды и столбцы одинаково.

Умножение: $x \in M(\lambda, \mu, R); y \in M(\mu, \nu, R)$;
$\lambda = (l_1, \dots l_r), \sum l_i = l$
$\mu = (m_1, \dots m_s), \sum m_i = m$
$\nu = (n_1, \dots n_t), \sum n_i = n$
$xy \in M(\lambda, \nu, R); (xy)^{hk} (1 \le h \le r, 1 \le k \le t) = x^{h1}y^{1k} + \dots + x^{hs}y^{sk}$

Note. x^{ij}, y^{hk} сами матрицы и умножение элементов теперь некоммутативно!

Как мы уже наблюдали в курсе лекций по алгоритмам, самые эффективные алгоритмы над матрицами — это алгоритмы над блочными матрицами. Значит самые идеологически правильные формулы — это некоммутативные формулы.

Theorem 1.2.6.

$$M(mn, R) \equiv M(m, M(n, R))$$

— в общем, только что проверили это.

Заметим, что кроме всего прочего, нам никто не запрещает проводить элементарные преобразования над блочными матрицами, лишь бы размеры строк и столбцов, над которыми они проводятся, были бы согласованы.

1.2.7 Определитель блочно-треугольной матрицы

R — коммутативное с 1

Theorem 1.2.7. $X \in M(m, R), Y \in M(n, R)$

$$det \begin{pmatrix} X & * \\ 0 & Y \end{pmatrix} = det(X)det(Y)$$

//ну и понятно какое общее утверждение можно сформулировать и доказать по индукции

Proof. 1. Принцип Дирихле + вложение $S_m \times S_n \hookrightarrow S_{m+n}, sign(\sigma, \pi) = sign(\sigma)sign(\pi)$, $(\sigma, \pi) \in S_m \times S_n$ — посмотрим, откуда в большой сумме в определении определителя могут взяться ненулевые слагаемые.

2. Доказательство Кронекера

   //сейчас будет изложена очень идейная штука, полезная очень много где

   Любую конечную полиномиальную формулу для коммутативных колец достаточно проверить только для полей.

   Почему это так:

   (a) Т.к. в нашей формуле конечное число буковок, ее достаточно проверить для нетеровых колец: породим ими алгебру над $\mathbb{Z}$

   (b) То, что достаточно проверять для нетеровых колец, достаточно проверять для колец многочленов: скажем, что буковки — независимые переменные. $\mathbb{Z}$ — область целостности, значит и $\mathbb{Z}[x_{ij}, y_{nk}]$ — область целостности.

   (c) Любая область целостности вкладывается в поле.

   Итак, путь $R = K$ — поле.

(a) Пусть $y = e$;

$$det \begin{pmatrix} x & * \\ 0 & e \end{pmatrix} = det(x)$$

— потому что посмотрим на $det \begin{pmatrix} x & * \\ 0 & e \end{pmatrix}$ как на функцию от x: она полилинейная, знакопеременная и нормированная, а значит ровно она определитель.

(b) $det \begin{pmatrix} x & * \\ 0 & y \end{pmatrix} = 0$, если $\begin{bmatrix} det(x) = 0 \\ det(y) = 0 \end{bmatrix}$. Потому что последнее равносильно линейной зависимости столбцов x или строк y, а значит и у новой матрицы столбцы или строки линейно зависимы.

(c) Пусть $det(x) \neq 0$; обозначим $d(y) = det \begin{pmatrix} x & * \\ 0 & y \end{pmatrix} \frac{1}{det(x)}$ (мы же можем, у нас же поле). Это опять полилинейная кососимметрическая нормированная функция от столбцов y, значит это определитель.

□

1.2.8 Мультипликативность определителя

R — комм с 1

Theorem 1.2.8. $x, y \in M(n, R)$

$$det(xy) = det(x)det(y)$$

Proof. Вычисление $\begin{pmatrix} x & 0 \\ -e & y \end{pmatrix}$ двумя способами.

1.

$$det \begin{pmatrix} x & 0 \\ -e & y \end{pmatrix} = det(x)det(y)$$

2. Проведем элементарные преобразования над блочными матрицами:

$$\begin{pmatrix} x & 0 \\ -e & y \end{pmatrix} \begin{pmatrix} e & y \\ 0 & e \end{pmatrix} = \begin{pmatrix} x & xy \\ -e & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -e \\ e & 0 \end{pmatrix} \begin{pmatrix} x & xy \\ -e & 0 \end{pmatrix} = \begin{pmatrix} e & 0 \\ x & xy \end{pmatrix}$$

По дороге определитель матрицы не поменялся: первый шаг — элементарная трансвекция, второй — композиция трех элементарных преобразований (уже выясняли это когда-то).

$$\begin{pmatrix} e & 0 \\ x & xy \end{pmatrix} = det(xy)$$

□

Corollary.

$$det(q^{-1}) = det(g)^{-1}$$

Corollary (2)**.** Очень полезный факт:
$x \in M(n,R) lg \in GL(n,R)$

$$det(gxg^{-1}) = det(g)det(x)det(g^{-1}) = det(x)$$

Note (Зачем вообще определитель нужен). Определитель - гомоморфизм из матриц во что-то коммутативное. Иногда это удобно.

Rem. Потому поймем, что каждой матрице сопоставляется набор собственных чисел, определитель матрицы равен их произведению и не зависит от сопряженности (сопряжение не меняет определитель).

Rem. Вообще для определителя придумали кучу формул, но на языке, которым мы владеем сейчас, это слишком сложно доказывается, и неясно, откуда что берется. Так что нам расскажут про это потом.

Вот, например, один из таких фактов — это теорема Бине-Коши: $x \in M(m,n,R); y \in M(n,m,R); det(xy) = 0, m > n$, иначе получается нетривиальная формула с минорами.

1.2.9 Миноры и алгебраические дополнения

$x \in M(m,n,R), R$ комм. с 1

Def. $1 \le r \le min(m,n)$
$1 \le i_1, \dots i_r \le m;\ I = \{i_1, \dots i_r\}\ i_1 < \dots < i_r$
$1 \le j_1, \dots j_r \le n;\ J = \{j_1, \dots j_n\}\ j_1 < \dots < j_r$

$$M_J^I(x) = M_{j_1,\dots j_r}^{i_1,\dots i_r} = det((x_{ij}), i \in I, j \in J)$$

— минор x, стоящий на пересечении строк с номерами из I и столбцов из J.

Def. $m = n, |I| = |J| = r$

$$\overline{M}_J^I(x) = \overline{M}_{j_1,\dots j_r}^{i_1,\dots i_r}(x) = det((x_{ij}), i \notin I, j \notin J) = M_{\underline{n}\setminus J}^{\underline{m}\setminus I}(x) = M_{\bar{J}}^{\bar{I}}(x)$$

— дополнительный минор

Def.

$$A_J^I(x) = (-1)^{\sum i_k + \sum j_k} \overline{M}_J^I(x)$$

— алгебраическое дополнение к минору $M_J^I(x)$

Особенно популярный вариант алгебраических дополнений — это

$$A_j^i(x) = A_{ij}(x)$$

— алгебраическое дополнение к элементу x_{ij}

1.2.10 Разложение определителя по строке

$x \in M(n, R), R$ комм с 1

$fix 1 \le i \le n$ (строку)

Theorem 1.2.9.

$$det(x) = x_{i1}A_{ij}(x) + \cdots + x_{nj}A_{nj}(x),$$

правая часть называется разложением определителя по iй строке.

Аналогично, если fix $1 \le j \le n$ (столбец)

$$det(x) = x_{1j}A_{ij}(x) + \cdots + x_{nj}A_{nj}(x)$$

Proof. Разложить iю строку $det(x)$ в сумму n штук строк (в кажой по одному ненулевому элементу, а остальные нули):

$$x_{i*} = x_{i1}f_1 + \cdots + x_{in}f_n, f_1 = (1, 0, \dots 0); \dots f_n = (0, \dots 0, 1)$$

$$det(x) = det \begin{pmatrix} \dots & \dots & \dots & \dots \\ x_{i1} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \end{pmatrix} + \cdots + det \begin{pmatrix} \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & x_{in} \\ \dots & \dots & \dots & \dots \end{pmatrix},$$

ну и понятно, что $det \begin{pmatrix} \dots & \dots & \dots \\ \dots & x_{ij} & \dots \\ \dots & \dots & \dots \end{pmatrix}$ — ровно $A_{ij}(x)$: сдвинем в левый верхний угол x_{ij}: сменим знак $i - 1 + j - 1$ раз, потому что столько произошло смен местами строк и столбцов соответственно. □

Note. Эту формулу еще называют определением определителя по Лапласу (индуктивное определение).

Corollary.

$$i \ne j \Rightarrow x_{i1}A_{j1}(x) + \cdots + x_{in}A_{jn}(x) = 0,$$

аналогично по столбцам. Потому что представим себе соответствующую такому определителю матрицу: у нее строки линейно зависимы, ну значит эта сумма — ноль.

$$\begin{pmatrix} \dots & \dots & \dots \\ x_{i1} & \dots & x_{in} \\ \dots & \dots & \dots \\ x_{i1} & \dots & x_{in} \\ \dots & \dots & \dots \end{pmatrix}$$

//следующая теорема — еще один пример того, какие страшные формулы для определителя бывают, которые мы еще не умеем доказывать

Theorem 1.2.10 (*Лапласа)**.**

$$det(x) = \sum_{|J|=m} M_J^I(x)A_J^I(x), I = \{i_1, \dots i_m\} \subseteq \{1, \dots n\}$$

Ну может быть даже и понятно, что через это можно продраться по индукции, но видно, что технически очень сложно на языке, который есть. В третьем семестре мы сможем доказать это быстро, просто и естественно.

1.2.11 Теорема Краммера

$x \in M(n, R)$

Def. Присоединенная к x матрица (adjugate, или adjoint matrix; говорят, второе название слегка устарело и его теперь стараются не использовать в связи с появлением нового объекта, ассоциирующегося с этим прилагательным)

$$adj(x) = (A_{ji}(x), 1 \leq i, j \leq n)$$

— состоит из алгебраических дополнений к элементам, стоящим на местах (i, j).

Note. Замети, что в предыдущем параграфе фактически было доказано следующее:

$$adj(x)x = det(x)e = xadj(x)$$

Theorem 1.2.11.

$$adj(xy) = adj(y)adj(x)$$

Proof. Почему это так, после недлительной медитации становится понятно. □

Theorem 1.2.12 (Краммера)**.**

$$x \in M(n, R) \in GL(n, R) = M*(n, R) \Leftrightarrow det(x) \in R^*$$

и тогда

$$x^{-1} = \frac{1}{det(x)} adj(x)$$

Proof. $\Rightarrow$ $x \in GL(n, R) \Rightarrow det(x)^{-1} = det(x^{-1})$, т.е. определитель действительно $\in R^*$
$\Leftrightarrow$ по предыдущей Note понятно □

Corollary. Пусть дана система линейных уравнений $Ax = y$. Система имеет единственное решение над K $\Leftrightarrow A$ обратима и тогда $x = A^{-1}y$

Note. Обратная матрица никогда вот так, как мы тут описали, не ищется, хотя полезно знать, что такая явная формула есть. Как она ищется быстро на самом деле, мы обсуждали на практике: мы элементарными преобразованиями над строчками и столбцами приводим матрицу к стандартному виду (см. комбинаторная эквивалентность); если матрица привелась к единичной, то она обратима. Понимаем, что фактически A — произведение транспозиций и перестановок строк и столбцов, и обратную матрицу к этому произведению мы умеем искать.

Осталось лишь заметить, что над произвольным коммутативным кольцом проделать это нам в общем случае не удастся.

1.2.12 Чем полезны определители

Утверждается, что на самом деле область применения этой конструкции не слишком разнообразна: полезно уметь описывать и считать лишь определители нескольких классов.

1. Альтернант

   $f_1, \dots f_n$ — функции от одной переменной, $x_1, \dots x_n$ — аргументы

   $$det \begin{pmatrix} f_1(x_1) & \dots & f_1(x_n) \\ \vdots & \vdots & \vdots \\ f_n(x_1) & \dots & f_n(x_n) \end{pmatrix}$$

   — такой определитель и называется альтернантом.

   Если f от двух arg, $x_1, \dots x_n; y_1, \dots y_n$ — наборы аргументов, то

   $$det \begin{pmatrix} f(x_1, y_1) & \dots & f(x_1, y_n) \\ \vdots & \vdots & \vdots \\ f(x_n, y_1) & \dots & f(x_n, y_n) \end{pmatrix}$$

   называется двойным альтернантом.

2. (Ex к 1)

   Определитель Вандермонда:

   $$det \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \vdots & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i)$$

   Определитель Коши:

   $$det \begin{pmatrix} \frac{1}{x_1+y_1} & \dots & \frac{1}{x_1+y_n} \\ \vdots & \vdots & \vdots \\ \frac{1}{x_n+y_1} & \dots & \frac{1}{x_n+y_n} \end{pmatrix}$$

3. Циркулянт:

   $$det \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_n & x_1 & \dots & x_{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ x_2 & x_3 & \dots & x_1 \end{pmatrix}$$

Rem. Вообще, если хочется посмотреть, зачем людям в реальной жизни нужны определители, были посоветованы статьи Краттенхалера (Krattenthaler). Это такой современный дяденька, который занимается физикой и комбинаторикой, и у него есть любопытные статьи о современных методах вычисления определителей.

1.3 Канонические формы линейного оператора

Вступление: рассказ о том, какие задачи мы решать умеем, а какие нет.

Дело происходит над полем K.

1. $\phi : U \to V$; если мы меняем базис в U и V, то матрица линейного отображения x домножается слева и справа на обратимую: $x' = h^{-1}xg$. Утверждается, что классифицировать матрицы соответствующие линейным отображениям можно, это называется каноническая форма линейного отображения, и ответ дается, что называется, в форме дискретных инвариантов.

2. $\phi : V \to V$; теперь у нас оператор и мы считаем, что если мы меняем базис, то меняем его как бы одновременно в двух копиях пространства, матрица оператора меняется как $g^{-1}xg$. Ответ на задачу классификации дается в форме инвариантов, причем уже не обязательно дискретных. Была фактически решена в XIX веке Фробениусом, впрочем, ответ люди понимали и в $XVIII$ веке и активно этим пользовались.

3. Задача о паре линейных отображений (задача Кронекера-Вейрештрасса)

$$\phi, \psi : U \to V$$

$$(x, y) \mapsto (h^{-1}xg, h^{-1}yg)$$

Классификация, как и в случае 1, дается в форме дискретных инвариантов; плюс, задача не сильно сложнее, чем 1.

В это месте стоит заметить, что задачи, которые мы умеет решать про отображения и операторы, кончились. Задачи $1 - 3$ называют "ручными" , дальше пошли "дикие" задачи:

4. Т.н. задача о паре матриц

$$\phi, \psi : V \to V$$

$$(x, y) \mapsto (g^{-1}xg, g^{-1}yg)$$

Невзможно описать инварианты.

Плюс, Теорема Гельфанда-Пономарева гласит, что если бы нам удалось классифицировать пары линейных операторов, то мы смогли бы классифицировать любые mки операторов. То есть, фактически, могли бы классифицировать конечнопорожденные алгебры.

5. Над $\mathbb{Z}/p^2\mathbb{Z}$ нельзя решить задачу 2.

А вот над $\mathbb{Z}$ можно, и это называется нормальная форма Смита (кстати начали этим на практике заниматься).

1.3.1 Инвариантные подпространства

K, V — в.п. над $K, dimV = n < \infty$

$\phi : V \to V \in End_k(V)$ — эндоморфизм = линейный оператор на V

$v_1, \dots v_n$ — базис. $\phi \mapsto [\phi]_v = x$ — матрица линейного оператора в базисе v

Def. $U \subseteq V$ — инвариантное подпространство ϕ, если $\phi(U) \subseteq U \Leftrightarrow \forall u \in U \phi(u) \in U$

Чем замечательно инвариантное подпространство? ϕ можно разложить на два отображения: на отображение $\phi|_U$, и на отображение $\phi|_{V/U}$.

Ex. 1. $0, V \subseteq V$

2. $\frac{d}{dx} : K[x] \to K[x]$ (определить можно, хотя и бесконечная размерность, ну а можно ограничить степень)

   $K[x]_{\leq n}$ (подпространство многочленов степени не выше n) — инвариантно.

3. У любого элементарного преобразования есть инвариантно подпространство: $t_{ij}(\xi) \sim$ инвариантная гиперплоскость, она же линейная оболочка.

Def. $U \subseteq V$ инвариантное подпространство ϕ.

$u_1, \dots u_m$ — базис ϕ, $u_{m+1}, \dots u_n$ — относительный базис V над U = согласованный с U базис V.

Theorem 1.3.1. *В базисе V, согласованном с инвариантным подпространством U оператора ϕ матрица ϕ имеет вид*

$$[\phi]_U = \left(\begin{array}{c|c} [\phi|_U]_U & * \\ \hline 0 & [\phi_{V/U}]_{u+U} \end{array} \right),$$

причем сказать, что будет на месте $*$, действительно сложно (этим занимается гомологическая алгебра)

Proof.

$$\begin{array}{ccc} \phi & \longrightarrow & \phi|_U \in End(U) \\ & \searrow & \\ & & \phi_{V/U} \in End(V/U) \end{array}$$

$\phi_{V/U} = (v + U), \phi(U) \subseteq U \Rightarrow \phi_{V/U}(v + U) = \phi(v) + U$, т.е. такое определение корректно и определяет оператор на факторпространстве.

Докажем теперь, что левый верхний и правый нижний блоки имеют именно такой вид, как написано:

1. $\phi(u_j)(1 \leq j \leq m) \in U = \langle u_1, \dots u_m \rangle ; \phi(u_j) = \sum\limits_{i=1}^{m} u_i \lambda_{ij}$, то есть в первых m столбцах в строчках дальше m стоят нули.

2. $\phi(u_j)(m < j \leq n) = \sum_{i=1}^{m} u_i \lambda_{ij} + u_{m+1}\lambda m + 1j + \cdots + u_n \lambda_{nj}$

   $V/U = \langle u_{m+1} + U, \ldots u_n + U \rangle$, ну значит ровно какие надо коэффициенты там и стоят.

□

Note. Вообще у нас остались две проблемы:

1. Верхний правый угол
2. А что если мы не смогли найти инвариантного подпространства? Обещается, что в K^{alg} оно обязательно есть (это задача 13 листка Eigenvalue).

   Попробуем для начала решить проблему 1. Неплохо бы, чтобы там были нули, но в общем случае неверно, что у U есть инвариантное прямое дополнение $U \oplus W = V$:

Ex. $U = \langle e_1 \rangle$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : K^2 \to K^2$

Theorem 1.3.2. *Пусть $V = U \oplus W$, где U, W инвариантны. Тогда в объединенном базисе U и W матрица ϕ имеет вид*

$$[\phi]_U = \left(\begin{array}{c|c} [\phi|_U]_U & 0 \\ \hline 0 & [\phi_{V/U}]_{u+U} \end{array} \right),$$

Note. Сведение к наиболее хорошему виду — это собственные числа и вектора.

1.3.2 Собственные числа и вектора (eigenvalues & eigenvectors)

//собственные вектора – ровно базисы одномерных инвариантных подпростанств
$\phi : V \to V$ — в.п. над K с базисом $e_1, \ldots e_n (V = K^n)$

Def. $\lambda \in K$ — собственное число оператора ϕ, если $\exists\ v \in V \neq 0 : \phi(v) = v\lambda$, а все вектора, для которых выполняется такое соотношение (существует такая константа, что $\ldots$) — собственные вектора.

//нулевой вектор — собственный вектор любого собственного числа; будем так считать, чтобы спокойно говорить про подпространства собственных векторов.

Note. Различают левые собственные числа и правые собственные числа, но для коммутативных колец это одно и то же:
$x \in M(n, R)$ левый модуль, $u \in R^n; M(n, K) \times K^n \to K^n : x, u \mapsto xu$

$$xu = u\lambda$$

— собственный столбец и правое собственное число.

${}^nK \times M(n,K)$ правый модуль $\to {}^nK : v, x \to vx$

$$vx = \lambda v$$

— собственная строка и левое собственное число.

Def. $\phi : V \to V, V$ — в.п. над $K; \lambda \in K$ — сингулярное собственное число оператора ϕ, если $\phi - \lambda id_V$ необратимый оператор.

Ex (Про собственные числа разных операторов)**.** 1.

$$\begin{pmatrix} 0 & \dots & \dots & \dots & 1 \\ 1 & 0 & \dots & \dots & 0 \\ 1 & \dots & \dots & \dots & 0 \\ 0 & \ddots & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \epsilon \\ \vdots \\ \epsilon^n \end{pmatrix}$$

//кстати это фробениусова клетка для $x^{n-1} - 1$

2. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, собственные числа ± 1

3. Оператор дифференцирования $\frac{d}{dt} : K[t] \to K[t], char(K) = 0$. У него все собственные числа 0 (как и у любого нильпонентного оператора, впрочем)

4. $t\frac{d}{dt} : K[t] \to K[t]$ (хорош тем, что степень сохраняет). В стандартном базисе $K[t]$ $1, t, t^2, \dots$ его матрица выглядит так:

$$\begin{pmatrix} 0 & \dots & \dots & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 2 & \dots \\ 0 & \dots & 0 & \ddots \end{pmatrix}$$

И собственные числа — все натуральные.

1.3.3 Диагонализуемые операторы

ϕ, V, K как обычно

Lemma. *Следующие условия эквивалентны:*

1. *ϕ диагонализуем над K (существует базис, в котором $[\phi]_v$ диагональна)*

2. *в V существует базис из собственных векторов оператора*

Proof. Пусть $v_1, \dots v_n$ — базис, в котором $[\phi]_v$ диагональна, значит он состоит ровно из собственных векторов:

$$\phi(v_i) = \lambda_i v_i = v_i \lambda_i$$

//вообще пользуемся во втором равенстве коммутативностью

Обратно действительно понятно, что матрица в базисе из собственных чисел будет выглядеть именно так, как сказано. □

Диагональный вид хороший и простой, и мы были бы очень рады всегда приводить оператор к таком виду. Но не всегда можно. Когда можно?

Theorem 1.3.3. *Пусть $dimV = n$; если у оператора $\phi : V \to V$ существует n попарно различных собственных чисел $\lambda_i \in K \Rightarrow \phi$ диагонализуем.*

Proof. Пусть v_i — собственные ненулевые вектора собственных чисел λ_i соответственно. Докажем тогда, что они линейно независимы (а значит, раз их n, то они образуют базис, и по предыдущей лемме оператор в базисе из них имеет желаемый вид).

Пусть они линейно зависимы, посмотрим на их самую короткую нетривиальную линейную зависимость:

$$v_1\alpha_1 + \dots + v_m\lambda_m = 0$$

($m \geq 2 : v_1\alpha_1 = 0$) вряд ли верно, НУО это первые m векторов.

Построим тогда более короткую линейную комбинацию:

$$\phi(v_1\alpha_1 + \dots + v_m\lambda_m) = v_1\lambda_1\alpha_1 + \dots + v_m\lambda_m\alpha_m = \phi(0) = 0$$

Домножим изначальную л.к. на λ_m и посмотрим на разность этого и образ изначальной:

$$v_1\alpha_1(\lambda_1 - \lambda_m) + \dots + v_{m-1}\alpha_{m-1}(\lambda_{m-1} - \lambda_m) = 0$$

— это нетривиальная л.к., ведь все собственные числа разные, равная нулю ?!? □

Note. С диагональным представлением у нас возникнут проблемы, например, когда $\lambda_i \notin K; \in K^{alg}$

Def. Оператор ϕ называется полупростым, если диагонализуем над K^{alg}.

Ex.

$$\begin{pmatrix} 0 & \dots & \dots & \dots & 1 \\ 1 & 0 & \dots & \dots & 0 \\ 1 & \dots & \dots & \dots & 0 \\ 0 & \ddots & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & \dots & \dots & \dots \\ 0 & \epsilon & 0 & \dots & \dots \\ 0 & 0 & \epsilon^2 & 0 & \dots \\ 0 & \dots & \dots & \ddots & \dots \\ 0 & \dots & \dots & \dots & \epsilon^{n-1} \end{pmatrix}, \epsilon^n = 1$$

//говорят, что матрица перехода здесь — ровно матрица дискретного преобразования Фурье

1.3.4 Характеристический многочлен оператора

$\phi, V(=K^n), K, e_1, \dots e_n$ — базис

$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ в этом базисе, $\phi(v) = v\lambda$.

$$\phi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1\lambda \\ \vdots \\ x_n\lambda \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix} = \lambda id_V \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\Leftrightarrow (\phi - \lambda id_V) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0,$$

т.е. мы могли определить собственный вектор как элемент ядра такого оператора.

Def. Собственное подпространство, отвечающе собственному числу $\lambda \in K$ — это $Ker(\phi - \lambda id_V)$

$v \in V$ — собственный вектор, отвечающий собств. числу λ — это такой вектор, что $(\phi - \lambda id_V)(v) = 0$

λ — собственное число ϕ, если $Ker(\phi - \lambda id_V) \neq 0$.

Рассуждение, которое позволяет понять, как все-таки искать эти собственные числа:

Пусть A — матрица оператора в базисе $e_1, \dots e_n$. $Ker(\phi - \lambda id_V) \neq 0 \Leftrightarrow \phi - \lambda id_V$ не обратим $\Leftrightarrow A - \lambda E \notin GL(n, K) \Leftrightarrow$ (по теореме Краммера) $det(A - \lambda E) = 0$.

Посмотрим на тот нулевой определитель как на многочлен от λ:

Def. $A \in M(n, R)$ (коммутативное с единицей); $\chi_A(t) = det(A - tE) \in R[t]$ — характеристический многочлен матрицы A. $deg(\chi_A(t)) = n; a - te \in M(n, R[t])$.

Характеристическим многочленом оператора называют такую штуку в каком-то $=$ в любом базисе, потому что при замене базиса этот определитель не меняется:

$$a \mapsto g^{-1}(a - te)g = g^{-1}ag - te; det(g^{-1}(a - te)g) = det(a - te) = det(g^{-1}ag - te)$$

Theorem 1.3.4. *Если $R = K$, то $\forall$ линейного оператора ϕ (его матрицы) понятия собственного числа 1, 2, 3 совпадают:*

1. *левые*
2. *правые*
3. *сингулярные*

Rem. Над телом все бывает гораздо сложнее, например, у многочлена бывает больше корней, чем у него степень.

Corollary. Т.к. многочлен степени n над полем имеет не более n корней, то у любого линейного оператора в линейном пространстве размерности n не более n собственных чисел.

1.3.5 Алгебраическая и геометрическая кратность собственных чисел

ϕ, K, V

Def. Геометрическая кратность собственного числа λ оператора ϕ — это размерность его собственного подпространства ($dimKer(\phi - \lambda id_v) = dimv_\lambda$).

Алгебраическая кратность собственного числа λ — его кратность как корня $\chi_p hi$.

Lemma. *Геометрическая кратность собственного числа не превосходит алгебраическую.*

Proof. Пусть $dim(v_\lambda) = l; v_1, \dots v_l$ — собственные вектора λ = базис собственного подпространства, а $v_{l+1}, \dots v_l$ — дополнение до базиса V. Заметим, что v_λ — инвариантное подпространство относительно нашего оператора, а значит матрица оператора в предъявленном базисе выглядит как

$$\left(\begin{array}{ccc|c} \lambda & \dots & 0 & \dots \\ 0 & \ddots & 0 & * \\ 0 & \dots & \lambda & \dots \\ \hline 0 & \dots & 0 & \dots \\ 0 & \ddots & 0 & * \\ 0 & \dots & 0 & \dots \end{array}\right)$$

То есть видно, что кратность λ в $\chi_\phi \geq l$. □

Note. Геометрическая кратность бывает меньше алгебраической, ведь мы знаем о существовании корневых векторов и вот этого вот всего.

Ex.

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & \dots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & \dots & \ddots & 1 \\ \dots & \dots & \dots & \lambda \end{pmatrix}$$

— жорданова клетка порядка n собственного числа λ. Алгебраическая кратность λ тут — n, геометрическая — 1 (кстати может принимать любое значение $1 - n$).

Note. Какие вообще проблемы бывают с тем, чтобы диагонализовать оператор?

1. Корни характеристического многочлена не в K, а в K^{alg} (но это можно считать, что не проблема)

2. Геометрическая кратность < алгебраической (собственных векторов не хватает для того, чтобы базис из них составить) — с этой проблемой научимся бороться только благодаря конечной размерности.

Ex (Иллюстрирующий предыдущее замечание)**.** $V = \langle \dots e_{-2}, e_{-1}, e_0, e_1, \dots \rangle, \phi(e_i) = e_{i+1}$ — у такого линейного оператора нет инвариантных подпространств, поэтому там сложно что-то сказать о хорошем виде оператора (такими штуками занимается спектральная теория операторов).

Ex (d' Alambert & Euler & Bernoulli)**.** Первый и самый важный пример, показывающий, что такое корневые вектора:

Посмотрим на оператор $\frac{d}{dt}$ на $Exp\circ_{\mathbb{R}}$ — конечные линейные комбинации стандартных экспонентциальных мономов вида $t^m e^{\lambda t}, m \in \mathbb{N}_0, \lambda \in \mathbb{R}$ — кольцо экспонентциальных мономов.

$$\frac{d}{dt}f = \frac{d}{dt}(a_1 t^{m_1} e^{\lambda_1 t} + \dots + a_s t^{m_s} e^{\lambda_s t}) = a_1 m_1 t^{m_1} e^{\lambda_1 t} + a_1 \lambda_1 t^{m_1} e^{\lambda_1 t} + \dots$$

— $at^m e^{\lambda t}$ — не собственные вектор, но очень похож; такие векторы называются корневыми:

$$(\frac{d}{dt} - \lambda)(t^m e^{\lambda t}) = m t^{m-1} e^{\lambda t}$$

$$(\frac{d}{dt} - \lambda)^k (t^m e^{\lambda t}) = \frac{m!}{k!} t^{m-1} e^{\lambda t}$$

$$(\frac{d}{dt} - \lambda)^{m+1} (t^m e^{\lambda t}) = 0$$

$t^m e^{\lambda t}$ — корневой вектор оператора $\frac{d}{dt}$ высоты $m+1$

1.3.6 Корневые векторы

ϕ, V, K

Def. $Ker(\phi - \lambda id_V)^m$ — пространство корневых векторов высоты lem

$$V(\lambda) = \cup_{m \le n} Ker(\phi - \lambda id_V)^m; dim V = n < \infty$$

— корневое подпространство, отвечающее собственному числу λ; его элементы называются корневыми векторами.

Цепочка $0 \subseteq Ker(\phi - \lambda id_V) \subseteq Ker(\phi - \lambda id_V)^2 \subseteq \dots$ стабилизируется, так что $V(\lambda) = Ker(\phi - \lambda id_V)^n$

Высостой корневого вектора называется наименьшее $m : Ker(\phi - \lambda id_V)^m v = 0$

$//m = 0$ — подходит только $v = 0; m = 1$ — собственные векторы

1.3.7 Многочлены от оператора

1. $K[t], A$ — K-алгебра с единицей, $c \in A$

   $f \in K[t] = a_n t^n + \cdots + a_1 t + a_0$; умеем подставлять туда c :

   $$ev_c : K[t] \to A$$

   $$f \mapsto f(c)$$

   — гомоморфизм эвалюации в c.

   Можнем в качестве A взять операторы или матрицы:

   (a) $x \in M(n, K)$

   $$ev_x : K[t] \to M(n, K)$$

   $$f \mapsto f(x) = a_n x^n + \cdots + a_1 x + a_0 e$$

   $f, g \in K[t]$ **коммутируют, а раз** ev_x **— гомоморфизм, то** $fg(x) = gf(x)$

   (b) $\phi \in End(V); f(\phi) = a_n \phi^n + \cdots + a_1 \phi + a_0 id_V$

2. **Def.** Матричный многочлен — это $M(n, K)[t]$.

   Немедленно заметим, что эти ребята не коммутируют, и это сразу показывает, что многочлен от матрицы и матричный многочлен — это не одно и то же.

   Theorem 1.3.5.

   $$M(n, K)[t] = M(n, K[t])$$

   Proof. Ну просто посмотреть и понять, что это так: $a^m, \ldots a^0 \in M(n, K)$

   $a^m t^m + \cdots + a^0; (a^m t^m + \cdots + a^0)_{ij} = a^m_{ij} t^m + \cdots + a^0_{ij}$ □

3. Что происходит с матрицей многочлена от оператора при подстановке в многочлен?

   Statement. *x — матрица $\phi \in End(V)$ в базисе $e_1, \ldots e_n$ $\Rightarrow$ матрица $f(\phi)$ в том же базисе выглядит как $f(x)$*

   Proof. $\phi \mapsto x$ — гомоморфизм. □

4. Что происходит с собственными числами?

   Theorem 1.3.6. *Пусть $v \in V \phi(v) = \lambda v, \lambda \in K, f \in K[t] \Rightarrow v$ — собственный вектор $f(\phi)$, отвечающий собственному числу $f(\lambda)$*

   Proof. Это вытекает из

Lemma. *$v \in V$ — общий собственный вектор операторов $\phi, \psi \in End(V)$, соотв с.ч. $\lambda, \mu; \alpha \in K$. Тогда*

(a) v — собств. вектор $\phi + \psi$, отв. с.ч. $\lambda + \mu$

(b) v — собств. вектор $\phi \circ \psi$, отв. с.ч. $\lambda\mu$

(c) v — собств. вектор $\alpha\phi$, отв. с.ч. $\lambda\alpha$

Это все легко проверить, посмотрим на первое, например: $(\phi+\psi)(v) = \lambda v + \mu v = (\lambda + \mu)v$ □

1.3.8 Теорема Кэли-Гамильтона (Cayley - Hamilton): алгебраическое и геометрическое доказательства

Rem. $dimM(n,k) \leq n^2$, т.е. полиномом степени n^2 любая матрица из указанного кольца точно обнуляется. Но мы хотели бы иметь более точную оценку сверху.

Theorem 1.3.7 (Теорема Кэли-Гамильтона)**.**

$$\chi_x(x) = 0, x \in M(n, R)$$

Note. Теорема не была доказана людьми, в честь которых названа. Гамильтон и Кэли рассмотрели случаи $n = 2$ и 3 соответственно:

$n = 2$

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; x^2 - tx(x)x + det(x)e = 0 : \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

— ну просто убедиться, что правда.

Кстати, у этого выражения есть глубинный смысл, связанный с комплексными числами: здесь написано, что любое комплексное число является корнем квадратного уравнения с вещественными коэффициентами (ну вот если вспомнить про конструкцию Кэли комплексных чисел).

$n = 3$

$$x^3 - tx(x)x + *x - det(x)e = 0,$$

где $*$ — сумма главных миноров порядка 2 (повычеркивали столбцы и строки диагональных элементов).

1. Доказательство Фробениуса. По теореме Лапласа (так называется утверждение о том, что $adj(x)x = det(x)e = xadj(x)$)

$$adj(x - te)(x - te) = det(x - te)e = (x - te)adj(x - te)$$

Подставим в это тождество $t = x$ и получим, что $x - xe = 0 \Rightarrow \chi_x(x) = 0$ □

Note (О правде и обмане). Доказательство выше выглядит как какая-то темная магия, и с первого взгляда не скажешь, что операции, проведенные выше, законны.

Раз они законны, то почему бы не делать так:

$$\chi_x(x) = det(x - xe) = det(0) = 0$$

Вроде похожее рассуждение, но гораздо короче.

Фишка в том, что второе рассуждение конечно проводить нельзя, а вот первое можно, и почему так, как раз и обсуждалось в предыдущем параграфе. Ведь во втором рассуждении равенство рассматривается с точки зрения матричных многчленов, а туда нельзя просто так взять и подставить матрицу.

2. Геометрическое доказательство. Для начала необходимо понять, что доказательство утверждения можно проводить **над полем**, ведь мы хотим опять проверить какую-то полиномиальную формулу. А еще заметим, что можно доказывать над K^{alg}: матрица от этого не поменяется, зато появятся все корни у характеристического многочлена: $K^{alg} \Leftrightarrow \ \forall\ \phi \in End(V)$ имеет собственный вектор.

Дальше ведем индукцию по размерности пространства; база очевидна (одномерное подпространство), переход:

$\phi \in End(V), dimV = n, v$ — собств. вектор $\phi \ \Rightarrow \ \exists\ \lambda \in K^{alg} : \phi(v) = \lambda v, v = \langle v, v_1, \dots v_{n-1}\rangle$ — базис $V, U = \langle v_1, \dots v_{n-1}\rangle \ \Rightarrow V = vk \oplus U$, и в этом базисе матрица оператора выглядит так:

$$\begin{pmatrix} \lambda & * \\ 0 & y \end{pmatrix}, [\phi_v]|_U = y; V/vk \cong U$$

$\Rightarrow \chi_x(x) = (\lambda - t)\chi_y(t)$, причем второй сомножитель равен 0 по и.п. (тут кстати написан определитель ступенчатой матрицы).

$$\Rightarrow \ \chi_y(x) = \begin{pmatrix} \lambda & * & \dots & * \\ 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \Rightarrow Im(\chi_y(x)) \subseteq vk,$$

а векторы отсюда обнуляются $\lambda - t$. □

3. Пояснения к доказательству Фробениуса. R — коммутативное кольцо.

Здесь будет написана сейчас комбинация доказательства теоремы из стандартных учебников и пояснения к доказательству Фробениуса, причем от первого рассуждение будет отличаться тем, что будет понятным.

$$adj(x - te)(x - te) = det(x - te)e = (x - te)adj(x - te) \in M(n, K[t])$$

Распишем $adj(x - te)$ по степеням t:

$$b_{n-1}t^{n-1} + \dots + b_0, b_i \in M(n, R)$$

$$\chi_x(y) = (b_{n-1}y^{n-1} + \cdots + b_0)(x - y), y \in M(n, R)$$

— вообще непонятно, когда можно в правую часть подставлять какой-то объект? Ну только когда он коммутирует с коэффициентами b_i и коэффициенты коммутируют между собой.

Мы знаем один случай, когда так бывает. Когда b_i — многочлены от x. То есть если мы докажем это утверждение, все сразу станет ясно.

Lemma. *b_{n-i} — многочлен степени $i-1$ от x*

Proof. Сравнение коэффициентов при степенях t в $adj(x-te)(x-te) = chi_x(x)e$ начиная со старшего:

$$\chi_x(x) = (-1)t^n + c_{n-1}t^{n-1} + \cdots + c_1t + c_0$$

b_{n-1} — $deg 0$

$b_{n-2} = xb_{n-1} - c_{n-1}$, и далее пишем рекуррентную формулу и получаем. □

После этого мы имеем право подставить x в равенство

$$\chi_x(y) = (b_{n-1}y^{n-1} + \cdots + b_0)(x - y), y \in M(n, R)$$

и получить справа 0. □

Corollary. $dimM(n, K) = n^2; x \in M(n, K), e, x, \ldots x^{n^2}$ линейно зависимы, т.е. $\forall\, x\ \exists\, p \in K[t] : deg(p) \leq n^2, p(x) = 0$.

Def. Такой p — аннулирующий многочлен матрицы x.

Только что доказанная теорема говорит нам, что степень минимального такого многочлена не превосходит n.

Rem. Конечно многочлены от x образуют в $M(n, K)$ нечно замкнутое и коммутативное, как мы знаем, и вполне естественно, что размерность этой штуки гораздо меньше, чем размерность всего пространства.

Corollary (2)**.** $det(x) \neq 0 \ \Rightarrow x^{-1}$ — многочлен от $x \in K[x]$ (это совсем понятно, если написать теорему Кэли-Гамильтона, а вот если определитель необратим, это интереснее)

Упражнение. R называется почти коммутативным (module finite), если R конечно порождено как модуль над коммутативным кольцом. Доказать, что над таким кольцом обратная матрица — тоже многочен от x.

1.3.9 Минимальный многочлен оператора

//summary: $K[t]$ — PID (так что то же самое с произвольным коммутативным кольцом уже не работает)

$\phi \in End(V), V$ — в.п. над $K, v \in V$.

Def. $f \in K[t]$ — аннулирующий многочлен вектора v относительно ϕ, если $f(\phi)v = 0$

Аннулятором вектора называется множество

$$Ann(v, \phi) = \{f \in K[t] | f(\phi)v = 0\}$$

Lemma.

$$Ann(v, \phi) \trianglelefteq K[t]$$

Proof. Ровно это обсуждалось в параграфе 7: $+, \circ$ и домножение на скаляр не выводят из множества (последнее говорит нам, что это не только идеал кольца, но и идеал алгебры). □

Corollary. у $Ann(v, \phi)$ если пораждающий элемент, и он называется

Def. μ_v — минимальный аннулирующий многочлен (ровно пораждающий элемент аннулятора)

Понятно, что определение, в котором говорится про минимальную степень — это ровно то же самое определение в силу свойств $K[t]$.

Def. $Ann_\phi = \cap_{v \in V} Ann(v, \phi) \trianglelefteq K[t]$ (пересечение идеалов — идеал) — аннулятор оператора.

Многочлен, пораждающий аннулятор оператора — аннулирующий многочлен оператора (μ_ϕ).

Corollary. Теорема Гамильтона-Кэли утверждает, что $deg \mu_\phi \leq n$.

1.3.10 Ядро операторного многочлена

//summary: $K[t] = PID \Rightarrow$ взаимная простотам там $\equiv$ комаксимальность

$\phi :\in End(V), V$ — в.п. над K, $f \in K[t]; Ker(f(\phi)) \subseteq V$

Lemma. $\forall f, g \in K[t]$ $Ker(f(\phi))$ — *инвариантное подпространство оператора* $g(\phi)$

Proof. Как мы знаем, операторы $f(\phi)$ и $g(\phi)$ коммутируют. Хотим сказать, что $\forall\, v \in Ker(f(\phi))g(\phi)v \in Ker(f(\phi))$:

$$f(\phi)g(\phi)v = g(\phi)f(\phi)v = g(\phi)0 = 0$$

□

Theorem 1.3.8. $f \in K[t], f = gh, (g, h) = 1, \phi \in End(\phi)$

$$\Rightarrow \;\; Ker(f(\phi)) = Ker(g(\phi) \oplus Ker(h(\phi)))$$

Proof. $(g,h) = 1 + K[t] = PID \Rightarrow \ \exists\, p,q : \ gp + qh = 1$

1.

   Lemma. $g|f \Rightarrow \ Ker(g(\phi)) \subseteq Ker(f(\phi))$

   Так что в равенстве, которое мы доказываем, правая часть содержится в левой.

2. Сумма прямая: пусть $v \in Ker(g(\phi)) \cap Ker(h(\phi))$, тогда

$$g(\phi(v)) = h(\phi(v)) = 0$$

$$p(\phi)g(\phi) + g(\phi)h(\phi) = id_v,$$

   то есть если это применить к v, слева получится 0, справа v, т.е. единственный вектор в пересечении — это 0, что и хотелось.

3. Левая часть содержится в правой: $v \in Ker(f(\phi))$

$$v = p(\phi)g(\phi)(v) + g(\phi)h(\phi)(v)$$

   Одно слагаемое в правой части содержится в $Ker(g(\phi))$, другое в $Ker(h(\phi))$, так что правая часть содержится в прямой сумме, что и надо было.

□

1.3.11 Примарное разложение

корневое разложение — частный случай для K^{alg}

$\phi \in End(V), \chi_\phi = (-1)^n p_1^{m_1} \dots p_s^{m_s}, p_i \in K[t]$ — неприводимые нормированные многочлены над K, попарно взаимно простые.

Def. $V(p_i) = Ker(p_i^{m_i}(\phi))$ — примарное подпространство оператора ϕ, отвечающее неприводимому множителю.

Theorem 1.3.9.

$$V = V(p_1) \oplus \dots \oplus V(p_s),$$

такое разложение пространства в прямую сумму называется примарным.

Rem. Морально это ровно КТО: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_s^{m_s}\mathbb{Z}$

Proof. Уже выяснили все, что нам надо. $Ker(\chi_\phi) = V$, мы начинаем по теореме в предыдущем параграфе потихоньку раскладывать пространство в прямую сумму, пока взаимно простые множители не закончатся (индукция по количеству простых множителей в разложении характеристического многочлена). □

Самый хороший и понятно устроенный случай разложения — это конечно когда все неприводимые множители χ_ϕ линейны. Характеристический многочлен произвольного оператора над V так раскладывается, когда поле алгебраически замкнуто (но мы пока так считать не будем и посмотрим просто на какой-то хороший оператор).

$$\chi_\phi(t) = (\lambda_1 - t)^{m_1} \dots (\lambda_s - t)^{m_s}, \lambda_i \in K, \lambda_i \neq \lambda_j$$

$\Rightarrow \lambda_i$ — попарно различные (сингулярные, но у нас это то же самое, что любое другое значение этого слова) собственные числа алгебраичесских кратностей m_i.

Corollary.

$$V = V(\lambda_1) \oplus \dots \oplus V(\lambda_s),$$

$V(\lambda_i)$ — коренвые подпространства, все вместе — корневое разложение.

Corollary (Равенство алгебраических и геометрических кратностей)**.** $dim(V(\lambda_i)) \leq m_i$, но $\sum\limits_{m_i} = n \Rightarrow m_i = dim(V(\lambda_i))\ \forall i$

Corollary. Высота любого вектора из $V(\lambda_i) \leq m_i$.

1.3.12 Формулировка и план доказательства теоремы о Жордановой форме (классический вариант)

$\phi \in End(V), dimV = n$

Пусть для конкретного оператора ϕ $\chi_\phi = \prod (\lambda_i - t)^{m_i}$, ну или работаем над K^{alg} (все собственные числа — элементы поля).

Def.

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & \dots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & \dots & \ddots & 1 \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

— жорданова клетка

Def. Прямая сумма матриц x, y — это

$$x \oplus y = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

Theorem 1.3.10 (Фробениуса о жордановой форме)**.** *Если χ_ϕ полностью раскладывается на линейные множители, то в пространстве V существует базис, называемый жордановым, в котором $[\phi]_v$ является жордановой матрицей, то есть прямой суммой жордановых клеток*

$$J_{l_1}(\mu_1) \oplus \dots \oplus J_{l_t}(\mu_t),$$

μ_i — собственные числа ϕ (среди которых могут быть и одинаковые), и $\sum_i l_i = n$

Представление в виде такой матрицы единственно с точностью до перестановки блоков.

Rem. Откуда там блоки с одинаковыми собственными числами.

Вот была у нас задача про A^3, где A — жорданова клетка с нулевыми собственными числами.

Ну и вообще все зависит от того, какая жорданова башня получатся будет, а она (башня, т.е. пока что семейство жордановых клеток для одного собственного числа) с ростом кратности корня бывает все разнообразнее и разнообразнее:

$n = 3$

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

На первый взгляд может показаться, что это все можно различать с помощью $rk(x - \lambda e)$: у этих трех матриц он соответственно $2, 1$ и 0. Но уже для следующего размера видно, что это не так:

$n = 4$

$$\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Тут эти ранги соответсвенно $3, 2, 2, 1, 0$; различить можно по $rk(x - \lambda e)^2$, потом по $rk(x - \lambda e)^3$ и тд.

Proof. **План доказательства:**

1. Корневое разложение сводит общий случай к случаю единственного собственного числа λ (если $(f, g) = 1$, то $Ker f(\phi)$ инвариантно относительно g).

2. $\lambda \to 0$: найти жорданов базис ϕ — равно найти жорданов базис для $\phi - \lambda_i id_V$ ($\lambda_i id_V$ со всем комутирует).

   Теорема Гамильтона-Кэли утверждает, что ϕ нильпотентный $\Leftrightarrow$ все собственные числа ϕ равны нулю. $\phi^m = 0 \ \Rightarrow \ \phi^n = 0$, где $dim V = n$.

3. Доказательство $\exists$ жордановой формы сведено к доказательству существования жордановой формы у нильпотентного оператора.

   ? $g \in GL(nK) : g^{-1} x g = J, x^{\cdots} = 0$, а потом надо будет доказать единственность: выразить размеры жордановых клеток через $rk(x - \lambda e)^m$ (а эти уж величины зависят только от начальной матрицы x).

□

1.3.13 Разложение Жордана-Шевале

//современный взгляд на жорданову форму и что на самом деле там утверждается

Нам, в общем, понятно, что самые замечательные и правильные утверждения не должны зависеть от того, работаем мы в алгебраически замкнутом поле или нет. Диагонализуемым операторам над K соответствуют полупростые операторы (диагонализуемые над K^{alg}). Заметим про жорданову клетку такую замечательную вещь:

$$\begin{pmatrix} \lambda & 1 & \dots & 0 \\ 0 & \ddots & \ddots & 0 \\ \dots & 0 & \ddots & 1 \\ \dots & 0 & \dots & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \ddots & \dots & 0 \\ \dots & 0 & \ddots & 0 \\ \dots & 0 & \dots & \lambda \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ \dots & 0 & \ddots & 1 \\ \dots & 0 & \dots & 0 \end{pmatrix},$$

причем первое слагаемое, как видно, полупростое, а второе — нильпотентное.

Note. 1. x — полупростая/нильпотентная, $g \in Gl(n, K) \Rightarrow g^{-1}xg$ — соответственное тоже.

2. x, y — полупростые/нильпотентные, $\Rightarrow x \oplus y$ — тоже.

Значит после приведения к жордановой форме вся матрица разбилась на сумму простая + нильпотентная, причем, так как при элементарных преобразованиях ничего не изменилось, то изначальная матрица тоже имела такое представление!

Def. Поле называется совершенным, если $charK = 0$ или $charK = p$ и $K^p = K$.

Theorem 1.3.11 (Аддитивное разложение Жордана - Шевале)**.** *K — произвольное совершенное поле, $x \in M(n, K)$; тогда $\exists\ x_s, x_n \in M(n, K)$:*

//s for semi-simple, n for nilpotent

1. *x_s полупроста, x_n нильпонентна*
2. *$x = x_s + x_n$*
3. *x_s, x_n коммутируют, и при этом предположении x_s и x_n единственны*
4. *(следствие из 1-3) x_s, x_n — многочлены от x*

Rem. Аналогичную теорему, называемую мультипликативным разложением Жордана - Шевале, формулируют так же, только $1, 2$ заменяют на x_u — унипотентна, $x = x_s x_u$.

1.3.14 Жорданов базис нильпотентного оператора

$\phi \in End(V)$ над $K, n = dim(V), \phi^n = 0$

Напомним, доказательство существования жордановой формы было сведено к доказательству существования оной у нильпотентного оператора, этим сейчас и займемся.

Пусть $mmin : \phi^m = 0$ (наибольшая высота корневых векторов оператора). Посмотрим на ядра последовательных степеней оператора:

$$0 = Ker(\phi^0 = id) \lneqq Ker(\phi) \lneqq Ker(\phi^2) \lneqq \cdots \lneqq Ker(\phi^m) = V$$

Пусть $u_1, \dots u_{nm}$ — относительный базис V над $Ker(\phi^{m-1})$.

Lemma. *Пусть $u_1, \dots u_r \in Ker(\phi^l)$ и линейно независимы по отношению к $Ker(\phi^{l-1}) \Rightarrow \phi(u_i) \in Ker(\phi^{l-1})$ и линейно нещависимы по отношению к $Ker(\phi^{l-2})$*

//каждая следующая разность размерностей в цепочке строго меньше предыдущей

Proof. Пусть $\phi(u_1)\lambda_1 + \cdots + \phi(u_r)\lambda_r \in Ker(\phi^{l-2})$; слева написано $\phi(\sum u_i\lambda_i)$

Значит $\sum u_i\lambda_i \in Ker(\phi^{l-1}) \Rightarrow \lambda_i = 0$ по условию линейной независимости по отношению к ядру. □

Итак, мы взяли относительный базис $u_1, \dots u_{nm}$ V над $Ker(\phi^{m-1})$; лемма фактически утверждает, что $\phi(u_1), \dots \phi(u_{nm})$ можно дополнить до относительного базиса $Ker(\phi^{m-1})$ над $Ker(\phi^{m-2}) : v_1, \dots v_{n(m-1)}$. Дополним образы получившийся набора до относительного базиса $Ker(\phi^{m-2})$ над $Ker(\phi^{m-3}) : \phi^2(u_1), \dots \phi^2(u_{nm}), \phi(v_1), \dots \phi(v_{n(m-1)})$, $w_1, \dots w_{n(m-2)}$, продолжим процесс, пока нам не придется дополнять образы очередного набора до относительного базиса $Ker(\phi^2)$ до $Ker(\phi) : \phi^{m-1}(u_1), \dots \phi^{m-1}(u_{nm}), \dots$ $\phi(x_1), \dots \phi(x_{n2}), y_1, \dots y_{n1}$.

Этот процесс можно представлять себе в виде соответствующей картинки:

$$m \; u_1 \dots u_{nm}$$

$$m-1 \; \phi(u_1), \dots \phi(u_{nm}), v_1, \dots v_{n(m-1)}$$

$$m-2 \; \phi^2(u_1), \dots \phi^2(u_{nm}), \phi(v_1), \dots \phi(v_{n(m-1)}), w_1, \dots w_{n(m-2)}$$

$$\vdots$$

$$2 \; \phi^{m-2}(u_1), \dots \phi^{m-2}(u_{nm}), \phi^{m-3}(v_1), \dots \phi^{m-3}(v_{n(m-1)}), \dots x_1, \phi^{m-4}(w_1), \dots \phi^{m-4}(w_{n(m-2)}), \dots$$

$$\dots, x_1, \dots x_{n2}$$

$$1 \; \phi^{m-1}(u_1), \dots \phi^{m-1}(u_{nm}), \phi^{m-2}(v_1), \dots \phi^{m-2}(v_{n(m-1)}), \phi^{m-3}(w_1), \dots \phi^{m-3}(w_{n(m-2)}), \dots$$

$$\dots, \phi(x_1), \dots \phi(x_{n2}), y_1, \dots y_{n1}$$

Theorem 1.3.12. *У нильпотентного оператора существует жорданов базис, в котором его матрица равна*

$$\underbrace{J_m(0) \oplus \cdots \oplus J_m(0)}_{nm} \oplus \underbrace{J_{m-1}(0) \oplus \cdots \oplus J_{m-1}(0)}_{n(m-1)} \oplus \cdots \oplus \underbrace{J_1(0) \oplus \cdots \oplus J_1(0)}_{n1}$$

и ni определены однозначно.

Proof. Надо доказать, что получившийся на последнем шаге набор векторов является базисом. В нем очевидно матрица оператора имеет нужный вид. Для того, чтобы понять, что наш набор — это система пораждающих, надо читать табличку снизу вверх, что линейно независимы — сверху вниз.

Почему ni определены однозначно:

По построению

$$dimKer(\phi) = \sum_{i=1}^{m} ni$$

$$dimKer(\phi^2) - dimKer(\phi) = \sum_{i=2}^{m} ni$$

$$\vdots$$

$$dimKer(\phi^m) - imKer(\phi^{m-1}) = nm$$

Это линейная система уравнений, и чтобы понять, что у нее есть единственное решение, надо вспомнить, что $dimKer(\phi^m) = dimV = n$. □

Мы построили базис не с тем определением жордановой клетки, которое было, а с единичками под диагональю:

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & \lambda \end{pmatrix}$$

Rem. Как нам известно с пар практики, есть два элементарных метода строить жорданов базис: "снизу вверх"и "сверху вниз". То, что было сейчас изложено — так называемый "сверху вниз". Этот способ любят в Америке, в России традиционно считают иначе. Это обусловлено тем, что тут как-то понятно, с чего начинать, и для счета "руками"это быстрее. Компьютеру же это быстрее сделать именно "сверху вниз потому что иначе надо искать характеристический многочлен, найти собственные вектора, это долго. А этим способом нужно найти относительный базис, и утверждается, чтоб этих векторов так много, что можно взять хоть вектора стандартного базиса и они с высокой вероятностью подойдут.

1.3.15 Теорема Жордана-Шевале для алгебраически замкнутого поля, мультипликативное разложение Жордана-Шевале

Во-первых заметим, если мы еще этого не сделали, что для того, чтобы выполнялся п.4 теоремы об аддитивном разложении, нам надо потребовать, чтобы $charK = 0$.

Proof. У нас есть матрица x, и если поле алгебраически замкнуто, то мы умеем приводить ее к жордановой форме: $y = g^{-1}xg$. Как выглядит жорданова клетка? ну это $J_m(\lambda) = \lambda e + J_m(0)$, причем первая матрица полупроста, а вторая нильпотентна. То есть можем сказать, что $y = y_s + y_n$. Хочется сказать тогда, что $x_s = gy_sg^{-1}; x_n = gy_ng^{-1}$, значит было бы верно $1, 2$ и x_s, x_n очевидно коммутировали бы. Но неясно, почему, если поле у нас не алгебраически замкнуто, мы попадем обратно в K.

Скажем, что x_s и x_n — это многочлены с коэффициентами из K от x. Хотим решить задачу ? $\exists\ f : f(J)n(\lambda)) = e$. Это ровно интерполяционная задача с кратным узлом, потому что для $f \in K[t]$

$$f(J_n(\lambda)) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \dots & \frac{f^{(n-1)(\lambda)}}{(n-1)!} \\ 0 & \ddots & \ddots & \frac{f^{(n-2)(\lambda)}}{(n-2)!} \\ 0 & \dots & f(\lambda) & f'(\lambda) \\ 0 & \dots & 0 & f(\lambda) \end{pmatrix}$$

Чтобы это понять, надо научиться возводить в степень жорданову клетку, и у нас была такая задача в листке Eigenvalue.

Итого мы поняли, что в равенстве $J_n(\lambda) = \lambda e + J_n(0)$ слева стоит многочлен от Жордановой клетки, справа λe — тоже многочлен от жордановой клетки, а то, что осталось, автоматически многочлен как разность двух многочленов. Ну значит и x_s, x_n — многочлены от x, потому что применим к получившемуся равенству g справа, g^{-1} слева и получим.

Единственность:

Lemma. *Сумма двух коммутирующих нильпотентных матриц нильпотентна*

Proof. Бином Ньютона (степень, которую нужно написать — это как минимум сумма степеней, в которых матрицы в первый раз дают 0). □

Lemma (2)**.** *Сумма двух коммутирующих полупростых матриц полупроста.*

Ну значит если $x = x_s + x_n = x'_s + x'_n \Rightarrow x_s - x'_s = x'_n - x_n$, слева полупростая, справа — нильпотентная, ну значит и там, и там написан 0. □

Note. Хочется еще раз подчеркнуть, что мы смогли что-то тут доказать только для случая алгебраически замкнутого поля, хотя верно это для произвольного совершенного.

Def. Элемент u называется унипонетнтым, если $u - e$ — нильпотентный, т.е. $u = e + y, y^m = 0$.

Lemma. *Унипотентная матрица обратима*

Proof.

$$(e + y)(e - y + y^2 - \dots) = e$$

□

Theorem 1.3.13. *K — произвольное совершенное поле, $x \in GL(n,K)$; $\exists\ x_s, x_u \in GL(n,K)$:*

1. *$x = x_s x_u$*
2. *x_s — полупростая*
3. *x_u — унипотентная*
4. *$x_s x_u = x_u x_s$*
5. *Такие x_s, x_u единственны и они являются многочленами от x.*

Proof.

$$x = x_s + x_n = x_s(e + x_s^{-1} x_n),$$

и вторую скобку как раз можем объявить нужной унипотентной матрицей.

Все, что нужно, доказали в предыдущей теореме. □

1.3.16 Вещественная жорданова форма

Мы хотим вложить $M(n,\mathbb{R})$ в $M(n,\mathbb{C})$.

Комплексное пространство — это вещественное пространство вдвое большей размерности $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C} = V \oplus iV$

$\phi : V \to V$ — в.п. над $\mathbb{R}$; такому оператору сопоставляется т.н. комплексификация:

$$\phi_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$$

$e_1, \dots e_n$ — базис V над $\mathbb{R}$

$e_1, \dots e_n$ — базис $V_{\mathbb{C}}$ над $\mathbb{C}$

$dim_{\mathbb{C}}(V_{\mathbb{C}}) = dim_{\mathbb{R}}(V); dim_{\mathbb{R}}(V_{\mathbb{C}}) = 2dim_{\mathbb{R}}(V)$, и $e_1, \dots e_n$ в $V_{\mathbb{C}}$ — это $e_1, ie_1, \dots e_n, ie_n$ (тут e_i — это базис V).

$\phi_{\mathbb{C}}$ приводится над $\mathbb{C}$ к Жордановой форме; как выглядят клетки?

Ну они бывают двух видов. Бывают клетки чисто вещественных собственных чисел, а остальные клетки бьются на пары: если есть $J_m(\lambda), \lambda = \alpha + i\beta, \beta \neq 0 \Rightarrow$ есть клетка для $\bar{\lambda}$, и она такого же размера. Это потому что $\chi_\phi \in \mathbb{R}[t]$ и $(x - \lambda e)^m u = 0 \Leftrightarrow (x - \bar{\lambda} e)^m \bar{u} = 0$, то есть корневому векторы высоты k в одном примарном подпространстве оператора соответствует сопряженный покомпонентно вектор такой же высоты в другом примарном подпространстве.

То есть в примарном разложении пространства $V_{\mathbb{C}}$ есть слагаемые $J_m(\alpha + i\beta) \oplus J_m(\alpha - i\beta)$, и суммарно в этих примарных подпространствах $2m$ векторов:

$$u, (x - \lambda e)u, (x - \lambda e)^2 u, \dots, (x - \lambda e)^{m-1} u$$

$$\bar{u}, (x - \bar{\lambda} e)\bar{u}, (x - \bar{\lambda} e)^2 \bar{u}, \dots, (x - \bar{\lambda} e)^{m-1} \bar{u}$$

$$J_m(\alpha+i\beta)\oplus J_m(\alpha-i\beta)\sim(\mathbb{C})\begin{pmatrix}\alpha & \beta & 1 & 0 & \dots & 0\\ -\beta & \alpha & 0 & 1 & \dots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots\\ \vdots & \vdots & \ddots & \ddots & 1 & 0\\ \vdots & \vdots & \ddots & \ddots & 0 & 1\\ \vdots & \vdots & \vdots & \vdots & \alpha & \beta\\ \dots & \dots & \dots & \dots & -\beta & \alpha\end{pmatrix}=J_m(\alpha,\beta)$$

— вещественная жорданова клетка.

И матрица над $\mathbb{R}$ выглядит как сумма таких клеток и еще нескольких с чисто вещественными собственными числами.

Rem. Примерно с этого места и дальше речь пойдет о том и о сем, но в том числе будет вестись подготовка к классификации конечнопорожденных модулей над PID

1.3.17 Циклические пространства

$K, V, \phi \in End(V), dimV < \infty$

Def. Наименьшее ϕ-инвариантное подпространство $U \subseteq V$, содержащее $v \in V$, называется циклическим продпространством, порожденным v:

$$U = \langle v, \phi(v), \dots, \phi^{m-1}(v)\rangle$$

— применяем ϕ, до какого-то места то, что получается, будет линейно независимым, потом л.к. предыдущих: $\phi^{m-1}(v) \in U$, и $v, \phi(v), \dots \phi^{m-1}(v)$ — базис циклического подпространства. Как выглядит $[\phi|_U]$? Пусть $\phi^m(v) = \sum\limits_{i=0}^{m-1} \alpha_i\phi^i(v)$, тогда

$$[\phi|_U] = \begin{pmatrix}0 & \dots & \dots & \alpha_0\\ 1 & \ddots & \dots & \alpha_1\\ 0 & \ddots & \ddots & \vdots\\ 0 & \dots & 1 & \alpha_{m-1}\end{pmatrix}$$

Заметим, что если f — минимальный аннулирующий многочлен, тогда

$$f = t^m - \alpha_{m-1}t^{m-1} - \dots - \alpha_1 t - \alpha_0,$$

потому что $f(\phi)(v)$ как раз $= 0$.

Матрица, написанная выше, называется фробениусовой клеткой; по отношению к f называется сопровождающей матрицей многочлена $B(f)(= M_f$, обозначение с практики).

Если бы матрица была разбита на такие блоки, нам бы тоже наверное понравилось, и оказывается, что матрица приводится к такой форме.

Теорема о фробениусовой нормальной форме, неформально, утверждает, что

$\forall\ \phi \in End(V), dimV < \infty\ \forall K$ допускает разложение в прямую сумму каких-то циклических подпространств и в соответственном согласованном с разложением базисе базис $[\phi]$ имеет вид

$$B(f_1) \oplus B(f_2) \oplus \cdots \oplus B(f_s), f_i \in K[t]$$

— фробениусова форма.

Такое разложение совсем не единственно, что бы нам предположить про f_i, чтобы стало ! с точностью до чего-нибудь понятного?

Заметим, что $\chi_{B(t)} = (-1)^m f$.

А еще что с помощью такой формы просто сводить операции с многочленами к операциям над матрицами (а это более правильные операции, ибо все некоммутативно, значит степень свободы меньше, значит понятнее, что делать).

Если f_i не неприводим, то подпространство можно разложить еще в прямую сумму, так что если хотим единственности, то f_i заведомо должны быть степенями неприводимых многочленов.

Итого, варианты решения проблемы:

1. Сделать f_i примарными
2. (инвариантные делители) считать, что $f_1|f_2|f_3\ldots$, и ровно это называется нормальной формой Смита.

1.3.18 Нормальная форма Смита

//существование разложения над $\mathbb{Z}$ доказано Смитом, над произвольным PID — Фробениусом

Над полем K любую матрицу можем привести к диагональному виду, причем по диагонали стоят единички. Над кольцом очевидно провернуть то же самое не получится: мы в итерациях метода Гаусса очень любим зарабатывать единичку, а тут делить не умеем.

Но оказывается не все так плохо: класс колец, где любая матрица диагонализуема — почти PID (для сносного вида кажется хватает свойств колец Безу, но там получается не столь же простая форма).

Theorem 1.3.14 (Нормальная форма Смита)**.** *Пусть R — PID, $a \in M(m,n,R) \Rightarrow \exists\, h \in GL(m,R), g \in GL(n,R)$:*

$$hag = \begin{pmatrix} f_1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \ldots & f_r & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}, f_i \in R^\bullet = R \setminus \{0\}, f_1|f_2\ldots|f_r$$

и вид единственный с точностью до сопряженности f_i

Rem. Класс дедекиндовых колец тоже неплох (любой идеал порождается двумя главными): там можно приводить матрицу почти к верхнетреугольному виду, только под главной диагональю тоже может что-то стоять.

Аудиторию заинтересовал следующий вопрос:

нётеровы кольца	ненётеровы кольца
PID	кольца Безу
дедекиндовы	прюферовы

Вроде понятно, что будет во всех случаях, кроме прюферовых колец: там идеал может быть порожден любым количеством главных. Вопрос о канонической форме матрицы в этих кольцах исследован плохо.

Для Евклидовых колец доказательство теоремы о нормальной форме Смита проще, хоть оно и неконструктивное; кроме того, утверждение, которое фактически доказывается, сильнее. Так что разберемся сначала со случаем Евклидовых колец.

Theorem 1.3.15. $a \in M(m,n,R), R$ *Евклидово* $\Rightarrow \exists\ h \in GE(m,R), g \in GE(n,R)$:

$$hag = \begin{pmatrix} f_1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & f_r & \vdots & \vdots \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix}, f_i \neq 0, f_1 | \dots | f_r$$

на самом деле матрицы h, g *даже из* $E(n,R)$.

Proof. Напомним, что $GE(n,R) = E(n,R) * D(n,R), E(n,R) = \langle t_{ij} \rangle, D(n,R) = \langle diag \rangle$.

Индукция по m, n; можем вычеркнуть нулевые строки и столбцы. $a \neq 0 \Rightarrow \lessdot X = \{hag = |h \in E(n,R), g \in E(n,R)\}$; пусть $l = \min_{b \in X, 1 \leq i \leq m, 1 \leq j \leq n : b_{ij} \neq 0} \delta(b_{ij}), \delta : R \to \mathbb{N}_0 \cup \{-\infty\}$. Минимум есть, потому что у a есть ненулевой элемент. Пусть $b \in X : \delta(b_{ij}) = l$ для какой-то пары (i,j). НУО считаем теперь, что $a = b$ и этот элемент — a_{11}. Тогда $a_1 1 | a_{1j}\ \forall 2 \leq j \leq n, a_1 1 | a_{i1}\ \forall 2 \leq i \leq m$, иначе бы элементарным преобразованием получили бы $b' \in X$ с элементом меньшей нормы: деление с остатком. Значит мы умеем приводить матрицу к виду

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

В блоке снизу справа умеем применять индукционное предположение; теперь прибавим вторую строку к первой и поймем, что $a_{11} = f_1 | f_2$, значит и все остальные (то же рассуждение, что и выше, про деление с остатком) $\square$

Corollary. Если R — евклидово, то $E(n,R) = SL(n,R); GE(n,R) = GL(n,R)$

Задача: это так и для коммутативных (полу)локальных колец.

Кольцо локальное, если там существует единственный максимальный идеал, полулокальное — если там конечное число максимальных идеалов.

Для PID это неправда: $SL(2,R) \neq E(2,R)$

Вернемся к случаю R — **PID**.

Lemma. *Хотим привести* $(x,y) \to (gcd(x,y),0)$

Proof. Пусть $d = gcd(x,y) \Rightarrow \exists\, u,v \in R : d = xu + yv$ и $(u,v) = 1 \Rightarrow (PID) \exists\, w,z \in R : 1 = uw + vz$. $det \begin{pmatrix} u & v \\ -z & w \end{pmatrix} = 1$, значит она обратимая, значит

$$\begin{pmatrix} u & v \\ -z & w \end{pmatrix}^{-1} = \begin{pmatrix} w & -v \\ z & u \end{pmatrix}$$

Ну на самом деле можем взять $w = \frac{x}{d}, z = \frac{y}{d}$.

То есть

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} u & -\frac{y}{d} \\ v & \frac{x}{d} \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}$$

, причем матрица, на которую мы домножаем, не обязательно обязана быть произведением элементарных преобразований, это и есть ключевое отличие от случая Евклидова кольца. Знаем только, что она обратимая.

Итак, из пары элементов обратимой матрицей умеем делать $(gcd, 0)$. □

Доказательство основной теоремы параграфа.

$$\begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} \in M(m,n,R)$$

Умножая на обратимые матрицы 2×2 в разных позициях (то есть это большие матрицы, которые на самом деле маленькие, разбавленные нулями и единицами в нужных местах), ну или переставляем столбцы и строки, домножаем на

$$\begin{pmatrix} * & * & 0 & \dots \\ * & * & 0 & \vdots \\ 0 & \dots & 1 & \vdots \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix},$$

потом переставляем обратно, получим $a_{11} = gcd(a_1 1, \dots a_{1n}, a_{21}, \dots a_{m1})$, приводим начальную матрицу к виду

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & * & \dots & * \end{pmatrix},$$

применяем и.п., получили диагональный вид.

Чтобы $f_1|\dots|f_r$, нужно еще чуть-чуть повозиться с диагональю:

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \sim \begin{pmatrix} gcd & 0 \\ 0 & lcm \end{pmatrix} :$$

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \sim (d = a_1u + a_2v) \begin{pmatrix} a_1 & 0 \\ d & a_2 \end{pmatrix} \sim \begin{pmatrix} 0 & \frac{-a_1a_2}{d} \\ d & 0 \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & \frac{a_1a_2}{d} \end{pmatrix}$$

И отсюда же следует единственность с точностью до ассоциированности:

$$f_1 = gcd(a_{ij})$$

$$f_2 = \frac{gcd(a_{ij}a_{hk} - a_{ik}a_{hj})}{f_1}$$

$$\vdots$$

$$f_i = \frac{gcd(\text{миноров порядка i})}{f_{i-1}\dots f_1}$$

□

Rem. Доказывать, что получится хороший диагональный вид, можно было и по-другому: когда мы сделали нулевыми первый столбец и строку кроме верхнего левого элемента, можем прибавить в первой строке вторую, заменить a_{11} снова на gcd, первый столбец тоже испортился, так что придется поправлять и его, и тд, процесс по нетеровости загнется. Но это как-то очень долго и муторно, привести просто к диагональному виду сначала приятнее.

1.3.19 Конечно порожденные модули над PID

R в ближайших нескольких параграфах — коммутативное, нётерово, область целостности, и все это очень важно.

Note. Утверждается, что сейчас переосмыслим теорему о жордановой форме, в случае $R = \mathbb{Z}$ — теорему о нормальной форме Смита, $R = K[t]$ — о фробениусовой форме.

Факт о конечнопорожденности модуля $M = \langle x_1, \dots x_n \rangle$ будет использоваться так: любое конечное количество элементов можно привести к общему знаменателю.

Def (Подмодуль кручения (для области целостности))**.** $x \in M$ — периодический (или элемент кручения), если $\exists\ \lambda \in R \neq 0 : \lambda x = 0$

Rem. Если $\lambda, \mu \in R$, оба $\neq 0$, но $\lambda\mu = 0\ \Rightarrow\ \forall\ x \in M \lambda(\mu x) = 0$.

Значит если хотим дать аналогичное определение для колец с делителями нуля, то правильно будет говорить $\lambda\ \in R_{reg}$(не делители нуля).

Def. $T(M) = \{x \in M | \ \exists\ \lambda \in R_{reg} : \lambda x = 0\}$ — подмодуль кручения (корректность проверяется ниже)

$//\lambda \in R \setminus \{0\} = R^\bullet$ для областей целостности

M — модуль без кручения, если $T(M) = 0$ (torsion-free).

Lemma. *R — коммутативная область целостности*

1. *$T(M) \leq M$ — подмодуль кручения*
2. *$M/T(M)$ — подмодуль без кручения*

Proof. 1. (a) $x, y \in T(M) \Rightarrow\ \exists\ \lambda, \mu \in R^\bullet : \lambda x = \mu y = 0$, тогда $\lambda\mu(x - y) = 0$ и $\lambda\mu \neq 0$ (ровно здесь ломается доказательство не для области целостности).

(b) $\lambda x = 0, \lambda \neq 0 \Rightarrow\ \lambda(\mu x) = \mu(\lambda x) = 0$ (коммутативность)

2. хотим доказать, что $T(M/T(M)) = 0$

Пусть $\lambda(x + T(M)) = 0\ \Rightarrow\ \lambda x \in T(M) \Rightarrow\ \exists\ \mu \neq 0 : (\mu\lambda)x = \mu(\lambda x) = 0$ и $\lambda\mu \neq 0$. □

Ex. $R/\lambda R$ — модуль кручения.

Основной результат темы:

Theorem 1.3.16. *R — PID*

1. *Любой подмодуль $M \leq R^n$ сам является свободным модулем ранга $m \leq n$*
2. *Любой конечно порожденный модуль без кручения свободен*
3. *Любой конечно порожденный модуль M представляется в виде $M = T(M) \oplus R^k$*

Данная теорема сводит изучение подмодулей к изучению подмодулей кручения.

Theorem 1.3.17. *R — PID, $M \leq R^n$; тогда $\exists$ базис $e_1, \dots e_m$ в R^n т.ч. $M = \langle \lambda_1 e_1, \dots, \lambda_m e_m \rangle$ (т.е. $\cong R^m$) где $\lambda_1 | \dots | \lambda_m, \lambda_m \neq 0$ — в точности нормальная форма Смита.*

Theorem 1.3.18 (Следствие из предыдущей)**.** *Любой конечно порожденный периодический модуль M над $R = PID$ — это $\oplus$ циклических:*

$$M = R/\lambda_1 R \oplus \dots \oplus R/\lambda_m R, \lambda_1 | \dots | \lambda_m \neq 0$$

и такое представление единственно с точностью до изоморфизма.

Def. $R/\lambda R$ — циклический модуль

$R/p^l R, p$ неприводимый — примарный циклической модуль

Theorem 1.3.19 (Следствие предыдущей + КТО)**.** *Любой конечно порожденный модуль кручения над PID R является прямой суммой примарных циклических:*

$$M = R/p_1^{m_1}R \oplus \cdots \oplus R/p_s^{m_s}R,$$

p_i неприводимы и такое разложение единственно с точностью до изоморфизма.

Proof. 1.3.16

Theorem 1.3.20. *Пусть R — область целостности, M — конечно порожденный модуль без кручения над $R \Rightarrow$ M вкладывается в конечно порожденный свободный модуль R^m над R + можно вложить так, чтобы имел ненулевые пересечения со всеми "координатными осями".*

Proof. Пусть $M = \langle x_1, \dots x_n \rangle ; y_1, \dots y_m$ линейно независимы в M с максимальным m (максимальный по включению набор найдется, т.к. работаем с областью целостности). $\exists$ линейное $\phi : R^n \to M$ $e_i \mapsto x_i$; пусть $v_1, \dots v_m$ — прообразы $y_1, \dots y_m$ относительно $\phi \Rightarrow v_i$ линейно независимы над $R \Rightarrow v_1, \dots v_m \in K^n$ и над K тоже линейно независимы ($R^n \leq K^n$, то есть понятно какое поле мы рассматриваем, и если линейно зависимы над K, значит домножим на знаменатели и получим линейную зависимость над R). Тогда по теореме Штейница $m \leq n$.

$\Lsh N = \langle y_1, \dots y_m \rangle \cong R^m \Rightarrow M$ вкладывается в N:

$y_1, \dots y_m$ — максимальная линейно независимая система $\Rightarrow \forall\, i\ x_i, y_1, \dots y_m$ линейно зависимая система, т.е. $\exists\ \lambda_i \in R :\ \lambda_i x_i \in N, \lambda_i \neq 0$. Возьмем $\lambda = \lambda_1 \dots \lambda_n \neq 0; \lambda x_i \in N\ \forall i \in \{1, \dots n\}$ (коммутативность, которую забываем, но которая все время есть).

Посмотрим на $\psi : M \to N; v \mapsto \lambda v$; это инъекция (ведь модуль без кручения), N — свободный модуль ранга m, значит M вложился в N и со всеми координатными осями M пересекается.

$//+$ доказали, что вкладывается в свободный модуль ранга $m \leq n$. □

Theorem 1.3.21 (Характеризация модулей без кручения)**.** *R — PID $\Leftrightarrow$ $\forall$ подмодуль конечно порожденного свободного модуля R^n сам является свободным модулем ранга $\leq n$.*

Proof. Индукция по n.

База $n = 1$ — в точности определение PID.

Для R^n доказали;

$$\Lsh \pi : R^{n+1} \to R^n$$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{n+1} \end{pmatrix} \mapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} : R^{n+1} = R^n \oplus R$$

$M \leq R^{n+1}; \Lsh \pi(M) \leq R^n; \pi(M) \cong M/Ker(\pi|_M)$, а $Ker(\pi|_M) = M \cap R$ — свободный модуль ранга не больше 1 по базе индукции. $\pi(M)$ — свободный модуль ранга $\leq n$ по и.п.

$$M/Ker(\pi|_M) \cong R^m, m \leq n$$

$Ker(\pi|_M) = 0$ — доказали все, $\neq 0 \Rightarrow \cong R \Rightarrow\ M \cong Ker(\pi|_M) \oplus R^m$:

Lemma. *Пусть R — коммутативное кольцо; $N \leq M : M/N \cong R^m \Rightarrow\ M \cong N \oplus R^m$*

А еще мы поняли, что ранг $M \leq n + 1$. □

Итого, нам осталось доказать пункт 3 теоремы:

Пусть M — конечно порожденный модуль и $T(M) \leq M \Rightarrow M/T(M)$ — конечно порожденный модуль без кручения, значит по уже доказанному он свободен, т.е. $M/T(M) \cong R^m$, по лемме имеем утверждение 3. □

Осталось понять, как устроены конечно порожденные периодические модули над PID.

Proof. 1.3.17 Знаем, что $M \cong R^m$ для $m \leq n$; пусть $x_1, \dots x_n$ — какой-то базис $R^n, y_1, \dots, y_m$ — базис M, тогда $\exists\ a \in M(n, m, R) : (x_1, \dots x_n)a = (y_1, \dots y_m)$. Теперь просто надо заменить подходящим образом:

$$(x_1, \dots x_n)ha = (y_1, \dots y_m)g; h \in GL(n, R), g \in GL(m, R)$$

Умеем приводить a к hag^{-1}, значит умеем и приводить к нормальной форме Смита. □

Note. Все, что сказано, применимо к $R = \mathbb{Z}$, а это ровно классификация конечнопорожденных абелевых групп: теорема 1 говорит, что если A — конечнопорожденная абелева группа, то $A \cong B \oplus \mathbb{Z}^n, |B| < \infty$, а теорема 2 как раз классифицирует эти самые конечные B — $B \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_s^{m_s}\mathbb{Z}, p_i \in \mathbb{P}$.

Rem. Аналогичную классификацию можно провернуть для дедекиндовых колец, это теорема Штейница-Капланского, там вместо свободных модулей фигурируют проективные.

Сейчас мы покажем, что из этого всего вытекает теорема о фробениусовой форме. $K, V, dim(V) = n < \infty, \phi \in End_K(V)$

1. (V, ϕ) — это $K[t]$ модуль, на котором t действует посредством ϕ, т.е. $\forall\ v \in V\ tv = \phi(v)\ \Rightarrow\ \forall f \in K[t] f \cdot v = f(\phi)(v)$

   Пространство вместе с оператором — это то же самое, что кольцо многочленов: V_ϕ — $K[t]$-модуль.

2. $\phi, \psi \in End(V); \phi \sim \psi$ (сопряжены, то есть есть замена базиса, в которой матрица ϕ выглядит так же, как матрица ψ) $\Leftrightarrow V_\phi \cong V_\psi$ как $K[t]$-модули.

   Выобр базиса в V устанавливает изоморфизм $V \cong K^n; End(V) \cong M(n, K)$

   $\phi \mapsto a, \psi \mapsto b\ \exists\ g \in GL(n, K) : b = g^{-1}ag\ \Leftrightarrow V_a \cong V_b$

   $V_a \cong V_b$ как $K[t]$ модули равносильно тому, что $\forall v \ni K^n a(gv) = g(bv) \Leftrightarrow ag = gb\ \Leftrightarrow g^{-1}ag = b$.

Значит задача классификация оператора — это то же самое, что задача классификации $K[t]$-модулей.

Но мы только что решили эту задачу: как выглядит любой конечно порожденный модуль над$K[t]$?

$$V_\phi \cong K[t]/f_1K[t] \oplus \cdots \oplus K[t]/f_sK[t] \oplus K[t]^m, f_1|\dots|f_s \neq 0$$

$dimV_\phi$ над K меньше бесконечности, так что последнего слагаемого нет. $dim_K(K[t]/fK[t]) = deg(f)$(поэтому скажем, что $degf_i \geq 1$). В качестве базиса $K[t]/fK[t]$ можно взять $1, \dots t^{deg(f)-1}$, НУО f нормирован $= t^{deg(f)-1} + \cdots + a_1t + a_0$, значит уножение на t в этом базисе действует так:

$$B(f) = \begin{pmatrix} 0 & \dots & \dots & -\alpha_0 \\ 1 & \ddots & \dots & -\alpha_1 \\ 0 & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & -\alpha_{deg(f)-2} \end{pmatrix}$$

— ровно сопровождающая матрица многочлена f (companion matrix).

Значит матрица оператора в базисе выглядит как прямая сумма фробениусовых клеток. Плюс, такое представление в виде прямой суммы модулей единственно, так что матрицу можно записать в таком виде единственным образом.

Theorem 1.3.22 (Rational canonical form = фробениусова форма)**.** *Для любого оператора ϕ на конечномерном пространстве над полем существует базис, в котором его матрица имеет вид*

$$B(f_1) \oplus \cdots \oplus B(f_s), f_1|\dots|f_s \neq 0,$$

$f_i \in K[t]$ *нормированы,* $\sum\limits_{i=1}^{s} deg(f_i) = dim(V)$ *и такие f_i единственны.*

Мы еще знаем, что каждое слагаемое раскладывается в сумму примарных.

Theorem 1.3.23. *В тех же обозначениях существует базис, в котором матрица оператора ϕ имеет вид*

$$B(p_1^{m_1}) \oplus \cdots \oplus B(p_l^{m_l}),$$

p_i — неприводимые нормированные многочлены (! не обязательно попарно различные), $\sum deg(p_i)m_i$ равна размерности пространства, и при этом набор $(p_1^{m_1}, \dots p_l^{m_l})$ единственный с точностью до порядка.

Если $p = t-\lambda$, то у нас жорданова клетка. $B(p_i^{m_i})$ — циклические подпространства; сменим там базис по аналогии с построением жордановой башни — будем смотреть на степень многочлена, которая фактически обнуляет данный вектор, и блок $B(p^m)$ тогда будет выглядеть так:

$$\left(\begin{array}{c|c|c} B(p) & 1 & \dots \\ \hline \vdots & \ddots & 1 \\ \hline \dots & \dots & B(p) \end{array}\right)$$

Там, где стоят единички, единички стоят только в нижнем левом углу, остальное — нули.

? это называется форма Ковалевского, или не это, а какой-то другой канонический вид, в общем любопытно выяснить, какой.

Глава 2

Геометрия пространств со скалярным произведением

Определить какие-то понятия сможем и над произвольным коммутативным кольцом, но доказывать все равно все будем над полем характеристики не 2.

$V = K^n; B : V \times V \to K$ — билинейная форма, если

1. $B(u_1 + u_2, v) = B(u_1, v) + B(u_2, v)$
2. $B(u, v_1 + v_2) = B(u, v_1) + B(u, v_2)$
3. $B(u\alpha, v) = B(u, v)\alpha$
4. $B(u, v\beta) = B(u, v)\beta$

$\alpha, \beta \in R, u_i, v_i \in V$

Rem. Над некоммутатичным кольцом это все бессмысленно, потому что попробуем вынести скаляры в разном порядке из $B(u\alpha, v\beta)$.

Мораль в том, что над некоммутативным кольцом над рассматривать полуторалинейные формы, откуда скаляры из аргументов выносятся в разные стороны: $B(u\alpha, v\beta) = \bar{\alpha}B(u, v)\beta$; и надо завести функцию сопряжения со свойствами

1. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$
2. $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$
3. $\overline{1} = 1$
4. $\overline{\overline{\alpha}} = \alpha$

(инволюция).

2.1 Билинейные скалярные произведения

K — поле, V — конечномерное в.п. над ним

Def. Билинейная форма $B : V \times V \to K$ на V называется билинейным скалярным произведением, если B рефлексивна:

$$\forall\ u, v \in V\ B(u, v) = 0 \Rightarrow\ B(v, u) = 0$$

Два вектора ортогональны $u \perp v \Leftrightarrow\ B(u, v) = 0$; вектор изотропный, если $u \perp u \Leftrightarrow\ B(u, u) = 0$.

//минимальное свойство, позволяющее строить элементарную геометрию

Ex (Свойства симметрии). 1. Если B — симметричная билинейная форма, т.е. $\forall\ u, v \in V\ B(u, v) = B(v, u)$ (ровно то, что называлось скалярным произведением у нас в геометрии).

В частности, т.н. евклидово скалярное произведение: $K^n \times K^n \to K$

$$\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right) \mapsto x_1 y_1 + \cdots + x_n y_n = x^T y$$

2. B — симплектическая (антисимметричная; symplectic), если $\forall\ u \in V\ B(u, u) = 0$ — все векторы изотропны; симплектические пространства.

   Пример симплектического скалярного произведения $K^2 \times K^2 \to K$

$$\left(\begin{pmatrix} x_1 \\ x_{-1} \end{pmatrix}, \begin{pmatrix} y_1 \\ y_{-1} \end{pmatrix} \right) \mapsto x_1 y_{-1} - x_{-1} y_1$$

   Хочется это перепутать с

3. B — кососимметрическая (skew - symmetric), если $\forall\ u, v \in V\ B(u, v) = -B(v, u)$

   Из предыдущего пункта следует этот, а обратно не следует в случае харатеристики поля 2 (была аналогичная выкладка).

2.2 Каждое билинейное скалярное произведение симметрическое или симплектическое

//если хочется почитать что-то о рассказанном здесь, то книжка Артина "Геометрическая алгебра" хорошо для этого подходит

Theorem 2.2.1. *Каждое билинейное скалярное произведение $B : V \times V \to K$ симметрическое или симплектическое*

Proof. $u, v, w \in V$

$$B(u, vB(u,w) - wB(u,v)) = 0 \Rightarrow B(vB(u,w) - wB(u,v), u) = 0$$

$$B(v,u)B(u,w) = B(w,u)B(u,v)$$

Подставим в это равенство $u = v$:

$$B(u,u)(B(u,w) - B(w,u)) = 0$$

ну то есть если $B(u,u) \neq 0 \Rightarrow B(u,w) = B(w,u)\ \forall\ w \in V$.

Осталось понять, почему не может быть кусками одно, а кусками другое (то есть не может быть так, что часть векторов изотропна, а у оставшейся симметрическое скалярное произведение).

Пусть $\exists\ u, v \in V : B(u,v) \neq B(v,u) \Rightarrow B(u,u) = B(v,v) = 0$

$$B(v,u)B(u,w) = B(w,u)B(u,v)$$

Для любого вектора $w \in V$ либо $B(u,w) \neq B(w,u)$, либо $B(w,u) = B(u,w) = 0$. Аналоично можно считать, что $B(w,v) = B(v,w) = 0$.

Если первое, то $B(w,w) = 0$.

Если второе, то $B(u, v+w) = B(u,v) + B(u,w) \neq B(v,u) + B(w,u) = B(v+w,u)$, значит $B(v+w, v+w) = 0$. А это $B(v,v) + B(v,w) + B(w,v) + B(w,w)$, первые три равны нулю, значит $B(w,w) = 0$, и это для всех векторов из V. □

2.3 Матрица Грама

V — в.п. над K с базисом $e_1, \dots e_n; B : V \times V \to K (B \in L(V, V; K)$ — пространство билинейных форм на V).

$u, v \in V; u = \sum\limits_{i=1}^{n} e_i u_i; v = \sum\limits_{i=1}^{n} e_i v_i$

$$B(u,v) = \sum_{i,j=1}^{n} B(e_i, e_j) u_i v_j = \sum_{i,j=1}^{n} u_i B(e_i, e_j) v_j$$

Def. $G = (B(e_i, e_j))_{1 \leq i,j \leq n}$ — матрица Грама билинейной формы B в базисе e_i

Выбор базиса устанавливает изоморфизм $V \cong K^n : v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$

Statement.

$$B(u,v) = u^T G v$$

То есть билинейная форма задается матрицей Грама; какая матрица может задавать билинейную форму? Ну мы знаем, что скалярное произведение бывает либо симметрическое, либо симплектическое.

B — симметрическое $\Leftrightarrow\ B(v,u) = v^T G u = (v^T G u)^T = u^T G^T v \Leftrightarrow\ G = G^T$ //если на куче векторов значения Av и Bv равны, то и матрицы равны.

B — симплектическое $\Leftrightarrow$ G — антисимметричная $\Leftrightarrow G^T = -G$ и $G_{ii} = 0$ (последнее не следует из первого, если характеристика 2).

Def. $Rad(V) = \{v \in V |\ \forall u \in V\ B(u,v) = 0\} = V^{\perp}$ — радикал.

B — невырожденная $\Leftrightarrow\ Rad(V) = 0\ \Leftrightarrow\ \ \forall v \neq 0 \in V\ \exists\ u \in V\ B(u,v) \neq 0.$

Statement. *B невырожденная $\Leftrightarrow$ G невырожденная $\Leftrightarrow$ (поле) $det(G) \neq 0$.*

//Теперь посмотрим, как преобразуется матрица Грама при замене базиса.

//сейчас будет видно, что она преобразуется не так, как матрица; это потому что оно морально не матрица, а тензор.

$e_1, \dots e_n; e'_1, \dots e'_n$ — первый и второй базисы

$$(e_1, \dots, e_n) = (e'_1, \dots e'_n)h; h \in GL(n, K)$$

$$B(u,v) = u^T G v, u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$$h^{-1}u = \begin{pmatrix} u'_1 \\ \vdots \\ u'_n \end{pmatrix}, h^{-1}v = \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix}$$

Хотим

$$B(u,v) = u^T G v = (h^{-1}u)^T (?)(h^{-1}v) \Rightarrow ? = G' = h^T G h$$

Theorem 2.3.1.

$$G' = h^T G h$$

//видно, что это что-то странное, обычно матрица так не преобразуется; сжульничали, когда в сумме в самой первой выкладке компоненты векторов разбрасывали туда-сюда: там на самом деле должны быть тензорные операции

Rem. Классифицировать квадратичные формы $\Leftrightarrow$ классифицировать матрицы Грама с точностью до ровно таких преобразований.

Кстати, классификация квадратичных форм над произвольным полем — открытый вопрос (над алгебраически замкнутым — норм, расскажут про классификацию над рациональными числами с трудом в 4 семестре).

2.4 Скалярные произведения и двойственное пространство

V — в. п. над K с базисом $e_1, \dots e_n$

$\nu \in V^* = Hom(V, K)$ — двойственное пространство ($\nu : V \to K$).

Двойственный базис $e_1^*, \dots e_n^* : e_i^*(e_j) = \delta_{ij}$

Можно задать изоморфизм $V^* \cong V : e_i^* \mapsto e_i$.

Но если поменяем базис, то поменяем и изоморфизм. А что на самом деле значит зафиксировать изоморфизм?

$B : V \times V \to K; u \in V; B(u, \_) : V \to K : v \mapsto B(u, v)$

$B(u, \_) \in V^*$ — линейность по второму аргументу.

$\tilde{B} : V \to V^* : u \mapsto B(u, \_)$ — это отображение линейно: линейность формы по первому аргументу

$\chi : L(V, V; K) \to Hom(V, V^*) : B \mapsto \tilde{B}$ — тоже линейно. Оно инъективно. Размерность у пространств $n^2 \Rightarrow$ построенное отображение — изоморфизм.

При этом это каноническое сопоставление, ни от чего не зависит.

Theorem 2.4.1.

$$L(V, V; K) = Hom(V, V^*)$$

Если посмотрим справа на $ISO(V, V^*)$, то поймем, что изоморфизмы — в точности невырожденные билинейные формы.

Rem. При задании неканонического изоморфизма V, V^* вводится сильнейшая дополнительная структура, и не стоит ей пользоваться: стоит различить строки и столбцы.

2.5 Изометрии и классификация пространств со скалярным произведением

$(U, B_U); (V, B_V)$ — в.п. со скалярными произведениями над полем K.

Def. $\phi : U \to V$ — изометрия, если это изоморфизм векторных пространств и $\forall\, u, v \in U\ B_V(\phi(u), \phi(v)) = B_U(u, v)$.

Композиция изометрий — изометрия; id_V — изометрия, ϕ^{-1} — изометрия, так что $Isom(V, B)$ — группа (если $U = V$).

1. Если B_V — симметрическое, то V — квадратичное пространство.

$B : V \times V \to K; Q_B : V \to K : v \mapsto B(v, v); Q_B$ — квадратичная форма, $B(v, v)$ — скалярный квадрат.

$Isom(V, B_V) = O(V, B_V)$ — ортогональная группа

2. B — симплектическое, V — симплектическое пространство, $Isom(V, B_V) = S_p(V, B)$ — симплектическая группа (Абель, Якоби, Риман ...)

3. B — эрмитова/антиэрмитова: $B(u, v) = \overline{B(v, u)}/B(u, v) = -\overline{B(v, u)}$ (заменой $B \mapsto iB$ можно получить одно из другого). V — эрмитово/унитарное, а группа изометрий называется $U(V, B_V)$ — унитарная группа.

Хотим классифицировать пространства со скалярным произведением.

Очевидные инварианты пространств со скалярным произведением с точностью до изометрии:

1. $dim(V)$
2. ранг матрицы Грама: $rk(V, B) = rk(G)$

Есть еще третий, но уже эти два позволяют классифицировать что надо в двух важнейших случаях.

Сейчас будут анонсы результатов, которые собираемся доказать до конца этой главы.

Theorem 2.5.1. *Два симплектических пространства над произвольным полем изометричны ($dimV = n, rk(V) = 2l$)$\Leftrightarrow$ у них одинаковые размерности и ранги.*

Пространство невырождено $\Leftrightarrow$ $dim(V) = rk(V)$. То есть невырожденные симплектические пространства над полем $\exists$ только в четных размерностях и ровно одно.

Theorem 2.5.2. *Два квадратичных пространства над квадратично замкнутым полем характеристики не два (иначе диагонализовать плохо) изометричны $\Leftrightarrow$ у них одинаковые размерности и ранги.*

Theorem 2.5.3. *Над $\mathbb{R}$ у квадратичного пространство появляется третий инвариант — сигнатура (n, q, p).*

Теорема инерции Сильвестра — о том, что больше инвариантов нет.

Точно так же классифицируются эрмитовы пространства над $\mathbb{C}$.

Третий инвариант в общем случае — $disc(V) = det(G)(K^*)^2 \in K^*/(K^*)^2$.

Вот $\mathbb{R}^*/(\mathbb{R}^*)^2 \cong \{\pm 1\}; \mathbb{F}_q^*/(\mathbb{F}_q^*)^2 \cong \{\pm 1\}$ при $q \neq 2^m$

Theorem 2.5.4. *Над $\mathbb{F}_q$ при нечетных q инварианты квадратичного пространства с точность до изометрии — это размерность, ранг и если $n = r$ — дискриминант.*

2.6 Ортогональное дополнение к подпространству

V — в.п. над $K, B : V \times V \to K, U \leq V$

Def. $U^\perp = \{v \in V | \ \forall\ u \in U\ B(u, v) = 0\}$ — подпространство, ортогональное к U.

Сразу возникает парочка вопросов:

1. ${}^\perp U = U^\perp$ — потому что B — скалярное произведение
2. $U^\perp \leq V$ — потому что B линейна по второму аргументу.

Получили соответствие $U \mapsto U^\perp$; обладает следующими свойствами:

1. $0^\perp = V$
2. $V^\perp = Rad(V) = \{v \in V : \ \forall\ u \in V B(v,u) = 0\}$

   Если V невырожденная, то радикал ноль, ну и из любой формы можем изготовить невырожденную, профакторизовав по радикалу: $V \mapsto V/Rad(V)$; такая факторизация сводит все вопросы к случаю невырожденного пространства.
3. $\forall\ U \leq V\ U \cap U^\perp = Rad(U)$

   Еще конечно U — тоже пространство со скалярным произведением, если рассмотреть $B|_{U\times U}$
4. $(U^\perp)^\perp \geq U$
5. $U \leq W \Rightarrow\ U^\perp \geq W^\perp$

   Если вспомнить теорему о размерности суммы и пересечения, то хочется думать, что выполняются аналоги формулы Де Моргана
6. $(U+W)^\perp = U^\perp \cap W^\perp$
7. $(U \cap W)^\perp \geq U^\perp + W^\perp$
8. Если наше пространство со скалярным произведением невырождено, то $(U \cap W)^\perp = U^\perp + W^\perp$

Proof. упражнения □

Def. $U \perp W \ \Leftrightarrow\ \forall\ u \in U, w \in W\ B(u,w) = 0$

2.7 Ортогональная прямая сумма

$(U, B_U); (V, B_V)$

Def. $(U, B_U) \boxplus (V, B_V) = (U \oplus V, B_{U\oplus V})$ — внешняя ортогональная прямая сумма U и V,

$$B_{U\oplus V}((u,v),(u_2,v_2)) = B_U(u,u_2) + B_V(v,v_2)$$

упражнение: это действительно скалярное произведение

Пусть теперь $U, W \leq V, U \leq W^\perp \Leftrightarrow W \leq U^\perp$; если еще $U \cap W = 0 \Rightarrow\ U+W$, на которой в качестве скалярного произведения задано сужение обычного на сумму, изоморфно $U \boxplus W$

$$(U+W, B_{U+W}) \cong U \boxplus W$$

Ex. $Rad(V) \leq V, U$ — любое дополнение к радикалу ($\Leftrightarrow\ U \cap Rad = 0; U + Rad(V) = V$); ортогональным дополнением к радикалу является все пространство, значит первое условие в пред. рассуждении выполнено, так что U невырождено и $U \boxplus Rad(V) = V$

Дефект V — размерность радикала.

Так что для классификации надо указывать дефект и класс эквивалентности невырожденного подпространства U

$U \boxplus W$ невырождено $\Leftrightarrow U, W$ невырождены. То есть классифицировать стоит что-то невырожденное, что так не раскладывается.

2.8 Теорема об ортогональном разложении

(V, B) — пространство со скалярным произведением над $K; U \leq V$

Theorem 2.8.1. *Если U невырождено (B_U), то $V = U \boxplus U^\perp$*

Proof. // рассуждение ниже проходит только для конечномерных пространств, можно для бесконечномерных, но совсем по-другому

1. $U \cap U^\perp = 0$, ведь $Rad(U) = 0$ и $U \perp U^\perp$
2. раз $U \boxplus U^\perp \leq V$, для доказательства равенства достаточно доказать, что $dim(V) = dim(U) + dim(U^\perp)$. А это ровно теорема о размерности ядра и образа:

   Есть вложение U в V, соответствующее $p : V^* \to U^*$; плюс, $B : V \times V \to K$ соответствует $\tilde{B} : V \to V^*$

   Посмотрим на линейное отображение $V \xrightarrow{\tilde{B}} V^* \xrightarrow{p} U^*$. Ограничение этого дела на U — это $\tilde{B_U}$. Это ограничение сюръективно, по условию это изоморфизм.
3. Значит $Im(p \circ \tilde{B}) = U^*, dimU^* = dimU$. А $Ker(p \circ \tilde{B}) = \{v \in V | B(v, u) = 0\ \forall\ u \in U\} = U^\perp$.

   Ну а теперь надо сказать про теорему о размерности ядра и образа.

□

Rem. Невырожденности V не достаточно: из нее вытекает, что $dimV = dimU + dimU^\perp$, но сумма не обязательно прямая: если ограничение на U вырождено, например

Def. $U \leq V$ называется вполне изотропным, если $U \leq U^\perp$.

U называется максимальным вполне изотропным, если $U = U^\perp$.

Theorem 2.8.2. *Если U, V невырождены, то $V = U \boxplus U^\perp = U^\perp \boxplus (U^\perp)^\perp$; в частности, $(U^\perp)^\perp = U$*

Proof. По предыдущей теореме $V = U \boxplus U^\perp$, значит $U^\perp$ невырождено, значит $V = U^\perp \boxplus (U^\perp)^\perp, U \leq (U^\perp)^\perp, dim(U) = dim((U^\perp)^\perp) \Rightarrow\ U = (U^\perp)^\perp$. □

2.9 Теорема Лагранжа

V — в.п. с симметрическим скалярным произведением над полем (квадратичное пространство).

Def. Базис $e_1, \dots e_n$ называется ортогональным, если $B(e_i, e_j) = 0 \ \forall \ i \neq j$.

Theorem 2.9.1. *Если характеристика поля не два, то в любом квадратичном пространстве над K существует ортогональный базис (морально это значит, что любую квадратичную форму можно привести к диагональному виду = сумме квадратов).*

Proof. Индукция по размерности пространства. Хотим выделять одномерные пространства.

Lemma. *Если $B \neq 0 \Rightarrow$ в пространстве над полем характеристики не два существует неизотропный = анизотропный вектор.*

Proof. Есть два вектора такие, что $B(u, v) \neq 0$; пусть оба изотропны, тогда $B(u + v, u + v) = 2B(u, v) \neq 0$, то есть $u + v$ анизотропный. □

Пусть e_1 анизотропный, значит порожденное им пространство невырожденное, значит $V = \langle e_1 \rangle \boxplus \langle e_1 \rangle^\perp$, причем $dim \langle e_1 \rangle^\perp = dim V - 1$, дальше индукция. □

Доказали, что

$$V = e_1 K \boxplus e_2 K \boxplus \dots \boxplus e_n K = (B(e_i, e_i) = a_i; e_i K = \langle a_i \rangle) \ \langle a_i \rangle \boxplus \dots \boxplus \langle a_n \rangle$$

Rem. Если нормировать вектора и переставлять, класс изометрии не изменится, но этот вид не является классификацией.

2.10 Гиперболические плоскости

Def. $H = \langle e_1, e_2 \rangle$ — гиперболическая плоскость, если e_1, e_2 изотропны и $B(e_1, e_2) = +1$.

То есть матрица Грама в симметрическом случае $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, в симплектическом — $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Lemma. *Пусть V — невырожденное пространство с симметрическим/симплектическим скалярным произведением над полем характеристики не два, и $\neq 0$ — изотропный, тогда он вкладывается в гиперболическую плоскость.*

То есть существует $v \in V : B(v, v) = 0, B(u, v) = 1$

Proof. Поскольку пространство невырожденное и вектор ненулевой, то есть $w \in V$: $B(u,w) \neq 0$; НУО можем считать, что $B(u,w) = 1$. Для симплектической формы мы уже все нашли, и даже не использовали условие про характеристику. Попробуем поискать v в виде $v = w + \lambda u$;

$$B(v,v) = B(w+\lambda u, w+\lambda u) = B(w,w) + 2\lambda B(u,w) \Rightarrow \lambda = -\frac{B(w,w)}{2B(u,w)}$$

□

Lemma (2)**.** *Гиперболическая плоскость невырожденная, так что она всегда выделяется прямым слагаемым:* $V = H \boxplus H^{\perp}$

Corollary. Пусть $v \in V, \notin Rad(V)$ — в квадратическом или симплектическом пространстве. Если вектор анизотропен, то вкладывается в одномерное невырожденное подпространство (свою линейную оболочку), если изотропен, то вкладывается в двумерную гиперболическую плоскость.

То есть все у нас разложится в сумму одно и двумерных подпространств, ну в характеристике два с симметрической формой ну не повезло, понадобится больше видов плоскостей.

2.11 Классификация симплектических пространств

K — произвольное поле, (V,B) симплектическое пространство.

Theorem 2.11.1. *У симплектических пространств над произвольным полем ровно два инварианта с точностью до изометрии:*

1. $dimV$
2. $rk(V) = rk(B)$,

то есть

$$V = H \boxplus \cdots \boxplus H \boxplus Rad(V),$$

гиперболических плоскостей l *штук,* $2l = r$.

Corollary. В каждой четной размерности существует единственное невырожденное симплектическое пространство с точностью до изометрии $V = H \boxplus \cdots \boxplus H$ — l гиперболических гиперплоскостей, $n = r = 2l$

Proof. Индукция по n.

Во-первых, $V = U \boxplus Rad(V), U$ невырожденное. Во-вторых, любой ненулевой изотропный вектор в невырожденном пространстве вкладывается в гиперболическую плоскость, значит по теореме о разложении $V = H \boxplus H^{\perp}, dimH^{\perp} = dim(V) - 2$, применили индукционное предположение. □

$V = H \boxplus \cdots \boxplus H$ — l штук, выберем там базис $e_1, e_{-1}, \dots e_l, e_{-l}$; тогда $B(e_{\pm i}, e_{\pm j}) = 0, B(e_i, e_i) = 0, B(e_i, e_{-i}) = sign(i)$.

Возможные нумерации базисов:

1. $e_1, \dots e_l, e_{-1}, \dots e_{-l}$
2. $e_1, e_{-1}, \dots e_l, e_{-l}$
3. $e_1, \dots e_l, e_{-l}, \dots e_{-1}$

В этих базисах матрица Грамма выглядят так:

1.
$$\left(\begin{array}{ccc|ccc} \dots & \dots & \dots & 1 & \dots & 0 \\ \dots & 0 & \dots & \vdots & \ddots & \vdots \\ \dots & \dots & \dots & 0 & \dots & 1 \\ \hline -1 & \dots & 0 & \dots & \dots & \dots \\ \vdots & \ddots & \vdots & \dots & 0 & \dots \\ 0 & \dots & -1 & \dots & \dots & \dots \end{array}\right)$$

2.
$$\begin{pmatrix} 0 & 1 & \dots & \dots & \dots & \dots \\ -1 & 0 & \dots & \dots & \dots & \dots \\ \vdots & \vdots & \ddots & \dots & \dots & \dots \\ \vdots & \vdots & \ddots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & 0 & 1 \\ \dots & \dots & \dots & \dots & -1 & 0 \end{pmatrix}$$

3.
$$\left(\begin{array}{ccc|ccc} \dots & \dots & \dots & 0 & \dots & 1 \\ \dots & 0 & \dots & \vdots & \ddots & \vdots \\ \dots & \dots & \dots & 1 & \dots & 0 \\ \hline 0 & \dots & -1 & \dots & \dots & \dots \\ \vdots & \ddots & \vdots & \dots & 0 & \dots \\ -1 & \dots & 0 & \dots & \dots & \dots \end{array}\right)$$

$$B\left(\begin{pmatrix} x_1 \\ \vdots \\ x_l \\ x_{-l} \\ \vdots \\ x_{-1} \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_l \\ y_{-l} \\ \vdots \\ y_{-1} \end{pmatrix}\right) = (x_1 y_{-1} - x_{-1} y_1) + \dots + (x_l y_{-l} - x_{-l} y_l)$$

И это единственная невырожденная симплектическая форма, и она ровно одна для каждой четной размерности.

Def. $S_p(2l, K) = \{g \in GL(2l, K) | g^T J g = J\}$ — симплектическая группа = группа изометрий $H \boxplus \cdots \boxplus H, l$ раз. Алгебраисты называют это ($\boxplus$ гиперболических плоскостей) гиперболическим пространством. Что обычно подразумевают под этим, будет сказано в районе параграфа 13.

Rem. Мы полностью изучили симплектические пространства.

2.12 Квадратичные формы

Переходим к изучению ортогональных пространств, и вынуждены считать, что $charK \neq 2$

(V, B) — ортогональное пространство с симметрическим скалярным произведением.

Def. $Q : V \to K$ называется квадратичной формой, если

1. Q однородно степени два, то есть $\forall\ v \in V\ \forall\ \lambda \in K\ Q(v\lambda) = Q(v)\lambda^2$
2. Существует симметрическое скалярное произведение (билинейная форма) $B : V \times V \to K$ такая, что $Q(v) = B(v, v)$

Statement. *Тогда такая симметрическая билинейная форма автоматически единственна и выражается через квадратичную форму так:*

$$B(u, v) = \frac{1}{2}(Q(u + v) - Q(u) - Q(v))$$

Пусть $dimV = n, G = (g_{ij})$ — матрица Грамма, то есть

$$B\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right) = \sum_{i,j} x_i g_{ij} y_j$$

а $Q(v) = B(v, v)$,

$$Q\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \sum x_i g_{ij} x_j,$$

то есть $Q(x_1, \ldots x_n) = \sum g_{ij} x_i x_j \in K[x_1, \ldots x_n]_2$, то есть квадратичная форма, с другой стороны, однородный многочлен степени два (другой взгляд на вещи, но обычно геометрически мыслить проще).

То есть для задания формы достаточно задать скалярные квадраты всех векторов, в отличие от симплектической формы, где скалярные квадраты были равны нулю и не несли никакой информации.

Теорема Лагранжа говорит нам, что любая квадратичная форма над полем характеристики не два приводится к сумме квадратов: $Q \sim a_1 x_1^2 + \ldots a_n x_n^2$.

То есть все будем формулировать одновременно для симметических билинейных скалярных произведений и квадратичных форм.

2.13 Классификация квадратичных пространств над $\mathbb{C}$ и над $\mathbb{R}$

Над $\mathbb{C}$ — это квадратично замкнутое поле характеристики не два, так что

Theorem 2.13.1. *Любое квадратичное пространство над $\mathbb{C}$ с точностью до изометрии определяется двумя инвариантами: размерностью и рангом.*

То есть $Q(x_1, \dots x_n) = x_1^2 + \dots x_r^2$, эквивалентно, матрица Грама имеет вид окаймленной единичной (до какого-то места, а именно до r, единички по диагонали).

Proof. Теорема Лагранжа позволяет построить ортогональный базис, а еще можем извлекать квадратные корни и нормировать. □

Над $\mathbb{R}$: $\mathbb{R}^*/(\mathbb{R}^*)^2 = \{\pm 1\}; e_1, \dots e_n$ — ортогональный базис. $B(e_i, e_i) \neq 0$, не можем заменить e_i на $\frac{e_i}{\sqrt{B(e_i,e_i)}}$, потому что может быть отрицательное, но можем поделить на корень из модуля: $e_i \mapsto \frac{e_i}{\sqrt{|B(e_i,e_i)|}}$.

Def. Ортонормированный базис — ортогональный базис $e_1, \dots e_n$ такой, что $B(e_i, e_i) = 1, -1$ или 0.

Theorem 2.13.2. *В каждом квадратичном пространстве над R существует ортонормированный базис, и матрица Грама выглядит так:*

Иными словами, каждая квадратичная форма над $\mathbb{R}$ выглядит так:

$$Q(x_1, \dots, x_n) = x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_{p+q}^2,$$

и количество положительных квадратов, количество отрицательных квадратов — инварианты самой формы (закон инерции Сильвестра, доказательство см. в конспекте по геометрии).

Def. $(n, p, q); (n, r = p + q, s = p - q)$ — сигнатура квадратичной формы.

Ex.

1. V невырожденное $\Leftrightarrow p + q = n, V = \mathbb{R}^{p,q}$ — псевдоевклидово пространство
2. $p = n = r, q = 0, V = \mathbb{R}^n$ — евклидово, ровно означает, что B положительно определена, матрица Грама единичная
3. $p = q$ или $q{+}1$ расщепляемое (невырожденное) пространство $\mathbb{R}^{p,p}$ или $\mathbb{R}^{p,p-1}$, матрица Грама перединичная (единички на другой диагонали, потому что $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ можем превратить в $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : e_1, e_2 \mapsto \frac{e_1+e_2}{\sqrt{2}}, \frac{e_1-e_2}{\sqrt{2}}$)

4. $\mathbb{R}^{p,1}$ — гиперболическое пространство (не в алгебре); часто встречаются в физике, вот $\mathbb{R}^{3,1}$ — пространство Минковского.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \dots & \dots \\ \vdots & \vdots & 1 & 0 \\ \dots & \dots & \dots & -1 \end{pmatrix}$$

5. $q = 0, V$ — полуевклирово скалярное произведение — положительно полуопределенное: $Q(v) \geq 0$.

$$\begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots \\ \vdots & \ddots & \dots & \dots & \dots & \dots \\ \vdots & \vdots & 1 & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & 0 & \vdots & 0 \end{pmatrix}$$

2.14 Теория Витта

Мораль: обычно стремимся выбирать ортогональный базис и приводить матрицу Грама к диагональному виду, где по диагонали плюс-минус единички. Но, оказывается, это не всегда лучший вариант, в других базисах бывает структура виднее.

Основа теории — теорема о продолжнеии изометрии, которая гласит, что у невырожденных пространств со скалярным произведением большая группа изометрий.

Theorem 2.14.1 (Witt extension Theorem)**.** *(V, B) — невырожденное пространство, $U, W \leq V, \psi : U \to W$ — изометрия (относительно подпространств не предполагается, что они невырожденные). Тогда $\exists\ \phi : V \to V$ — изометрия такая, что $\phi|_U = \psi$.*

Ex. 1. $u, v \in V : B(u, u) = B(v, v) \Rightarrow\ \exists$ изометрия $\phi : V \to V : \phi(u) = v$.

   (a) $B(u, u) = B(v, v) \neq 0$

   (b) $B(u, u) = B(v, v) = 0$ — это база, и доказательство для этих двух случаев разное.

   Контрпример (о нужности условия про невырожденность пространства): V — вырождено, u, v — два вектора, один из радикала, а другой нет, и никакими силами не перевести один в другой.

   О том, почему мы изучаем именно квадратичные формы:

Theorem 2.14.2. *Если F — невырожденная форма степени 3 или выше над полем характеристики ноль, то ее группа изометрий конечна.*

То есть там не может быть никакой теории, аналогичной той, что изучаем про квадратичный формы (к вопросу о том, почему изучаются скалярные произведения не от трех аргументов: нет никакой нетривиальной геометрии для таких форм).

Theorem 2.14.3 (Теорема Витта о сокращении (Witt cancellation Theorem))**.** *U_1, V_1 и U_2, V_2 невырожденные пространства, $U_1 \cong U_2, U_1 \boxplus V_1 \cong U_2 \boxplus V_2 \Rightarrow V_1 \cong V_2$*

Из теоремы о скоращении вытекает теорема о продолжении в случае, когда U, W невырожденные, потому что $U \cong W, V = U \boxplus U^\perp = W \boxplus W^\perp \Rightarrow U^\perp = W^\perp$; зададим на ортогональных дополнениях ту изометрию, которая получается. Но мы пока не доказали ни одну из теорем.

Что мы пока знаем? Когда $U = W$ невырожденные: $\phi = \psi \boxplus id_{U^\perp}, V = U \boxplus U^\perp$. Из этого мы выведем, что нам нужно.

2.15 Отражение относительно неизотропного вектора

$v \in V$ над $K, char(K) \neq 2$, B — симметрическое скалярное произведение.

Def. $v \in V, B(v,v) \neq 0$ — анизотропный вектор. Отражением w_v относительно анизотропного вектора называется линейное преобразование $V \to V$:

1. $w_v(v) = -v$
2. $\forall\ u \in \langle v \rangle^\perp\ \ w_v(u) = u$

Statement (А точнее это первый пункт задачи 12 из листка 6)**.** *Это изометрия и*

$$w_v(x) = x - 2\frac{B(x,v)}{B(v,v)}v$$

Lemma (ключевой случай доказательства теоремы Витта о продолжении изоморфизма)**.** *$v, u \in V, B(u,u) = B(v,v) \neq 0 \Rightarrow\ \exists$ изометрия V переводящая u в v*

Proof. Один из векторов $u+v, u-v$ анизотропен.

1. $u - v$ анизотропен, тогда можно отразить относительно него и получить сразу что нужно: $w_{v-u}(v) = u$
2. если разность изотропна, тогда $v+u$ анизотропен, тогда $w_{v+u}(v) = -u, w_u(-u) = u$

□

2.16 Доказательство теоремы Витта о продолжении изометрии для невырожденного случая

Иногда в курсах линейной алгебры проводят болеее общее и сложное рассуждение, но мы уже сказали, что случай симплектических пространств нам не интересен, а в случае ортогональных мы можем пользоваться диагонализацией.

Итак, доказываем: V над K $char \neq 2; U, W \leq V, \psi : U \to W \Rightarrow \ \exists\ \phi : V \to V$: продолжает ψ.

Proof. Доказательство для случая, когда U, W невырожденные. Индукция по размерности U. Случай, когда $dim(U) = dim(W) = 1$, то есть база, описан в предыдущем параграфе.

$\lessdot v \in U : B(v, v) \neq 0 \Rightarrow \ U = vK \boxplus (vK)^{\perp}_{U}$. Посмотрим на изометрию в W; раз изометрия, что $B(\psi(v), \psi(v)) = B(v, v) \neq 0 \Rightarrow \ W = \psi(v)K \boxplus (\psi(v)K)^{\perp}_{W}$. При этом $\psi((vK)^{\perp}_{U}) = (\psi(v)K)^{\perp}_{W}$, потому что пара ортогональных векторов переходит в пару ортогональных и размерности совпадают.

По лемме из предыдущего параграфа есть изометрия $\theta : V \to V : \theta(v) = \psi(v); \theta^{-1}\psi(v) = v$, и эта штука постоянна на всех векторах, ортогональных $v, \psi(v)$. Заменим $W \mapsto \theta^{-1}(W), \psi \mapsto \theta^{-1}\psi$; теперь у нас гарантировано появился вектор $v \in U \cap \theta^{-1}(W), \theta^{-1}\psi(vK)^{\perp}_{U} \cong (vK)^{\perp}_{\theta^{-1}(W)}$, а тут размерности меньше и применим индукционное предположени: $\exists\ \nu\ (vK)^{\perp}_{V} \to (vK)^{\perp}_{V}$, продолжающая $\theta^{-1}\psi \Rightarrow \theta^{-1}\psi = 1_{vK} \boxplus \nu \Rightarrow \psi = \theta(1_{vK} \boxplus \nu) \in Isom(V, B)$. □

2.17 Доказательство теоремы Витта для вырожденного случая

$U \leq V, V$ невырождено, U вырождено. Тогда построим подпространство $U \leq \overline{U} \leq V$ невырожденное такое, что любая изоматрия U в невырожденное пространство продолжается на $\overline{U}$.

Идейно это вложение изотропного вектора в гиперболическую плоскость, но не абы какую, а подходящую.

Пусть $U = U_0 \boxplus Rad(U), U_0$ — невырожденное; пусть $e_1, \dots e_r$ — базис радикала; сейчас построим $e_{-1}, \dots e_{-r}$ так, что все вместе порождает гиперболическое пространство. Индукция по r. Возьмем пересечение ортогональных дополнений к $e_1, \dots e_{r-1}$ и U_0 тоже: $(U_0 + e_1K + \dots + e_{r-1}K)^{\perp}_{V}$; там найдется $e_{-r} : B(e_r, e_{-r}) = 1$ и изотропный, потому что придуманное подпространство содержит $U^{\perp}$ (и не равно ему): там есть вектор v такой, что $B(e_r, v) \neq 0$, тогда можем отнормировать его: $v \mapsto \frac{v}{B(e_r, v)}$, а потом $v \mapsto \ v - \lambda e_r$, чтобы был изотропным. Теперь и.п.

Theorem 2.17.1 (что доказали)**.** *Если V невырожденное квадратичное пространство над K $char \neq 2$, тогда для любого подпространства $U \leq V\ \exists$ невырожденное*

подпространство $\overline{U} \geq U$:

$$\overline{U} = U_0 \boxplus \cdots \boxplus H \leq V, H \text{ек } d \text{ штук},$$

где $U = U_0 \boxplus Rad(U), d = dim(Rad(U)), \overline{U}$ *невырожденное.*

Ну значит закончим доказательство теоремы Витта о продолжении изоморфизма для вырожденного случая, сказав, что уже умеем продолжать изоморфизм с $\overline{U}$:

$U, W \leq V$ вырожденные, $\psi : U \to W, U \leq \overline{U}, W \leq \overline{W}$; $\exists\ \overline{\psi} : \overline{U} \to \overline{W}$: $W_0 = \psi(U_0), e_1, \dots e_r$ — базис $Rad(U) \mapsto\ \psi(e_1), \dots \psi(e_r)$ — базис $Rad(W)$, теперь дополним оба до $e_{-1}, \dots e_{-r}; f_{-1}, \dots f_{-r}$ и достроим до $\overline{\psi}$, переведя их друг в друга.

2.18 Теорема Витта о разложении

Сейчас узнаем, что такое разложение Витта, базис Витта и индекс Витта.

Def. $U \leq V$ — вполне изотропно, если $U \leq U^{\perp} \Leftrightarrow\ \forall\ u, v \in U\ B(u, v) = 0$.

Если B симметрическое, а характеристика поля не два, это ровно значит, что любой вектор подпространства изотропен.

Def. $U \leq V$ изотропное, если в нем есть ненулевой изотропный вектор.

Corollary (из теоремы о продолжении)**.** Если $U, W \leq V$ — два вполне изотропных подпространства одинаковой размерности в невырожденном пространстве над полем характеристики не два, то $\exists\ \psi \in Isom(V, B) : \psi(U) = W$. То есть у таких подпространств единственный инвариант — размерность.

Corollary (2)**.** В частности, все максимальные вполне изотропные подпространства имеют одинаковую размерность.

Proof. Пусть U, W — максимальны, пусть $dimU \leq dimW\ \Rightarrow\ \exists\ \phi : \phi(U) \leq W \Rightarrow U \leq \phi^{-1}(W)$, но оно максимально, так что они равны. □

Def. Индекс Витта $V = ind(V)$ — размерность максимального вполне изотропного подпространства.

Согласно теореме из предыдущего вопроса для любого максимального вполне изотропного подпространства $U \leq V\ \exists$ дополнительное максимальное вполне изотропное подпространство $\overline{U} = \left\langle e_{-1}, \dots e_{-ind(V)} \right\rangle : U \oplus \overline{U} = H \boxplus \cdots \boxplus$.

Def. V анизотропно, если $\forall\ v \in V B(v, v) = 0 \Rightarrow\ v = 0$.

А там любое подпространство выделяется прямым слагаемым, потому что сужение формы на него невырождено.

Theorem 2.18.1 (Следствие из рассуждения = Теорема Витта о разложении)**.** *Любое квадатичное пространство V над K характеристики не два представляется в виде*

$$V_0 \boxplus H \boxplus \cdots \boxplus H \boxplus Rad(V), Hек\ ind(V)\ штук,$$

где V_0 анизотропно, при этом по теореме Витта о сокращении V_0 определено однозначно с точностью до изометрии.

Гораздо полезнее выбирать базис, согласованный с этим разложением, ведь группа изометрий у выделенных в ортогональную прямую сумму подпространств понятно устроена (кроме анизотропных, у которых она увы сложно устроена).

Def. Базис Витта:

1. $e_1, e_{-1}, \ldots e_r, e_{-r}$
2. базис анизотропной части
3. базис радикала

2.19 Эрмитовы формы и полуторалинейные скалярные произведения

Def. $\phi : R \to R$ — инволюция, $a \mapsto \bar{a} = \phi(a)$, если это антиавтоморфизм порядка два:

1. $\overline{a+b} = \bar{a} + \bar{b}$
2. $\overline{ab} = \bar{b}\bar{a}$ (анти)
3. $\bar{1} = 1$
4. $\bar{\bar{a}} = a$

//вот транспонирование матриц — инволюция над коммутативным кольцом
//над коммутативными кольцами оно тоже есть, просто выглядит как автоморфизм; вот хорошо видно, что над комплексными числами превращается в автоморфизм, а в кватернионах $a + bi + cj + dk \mapsto a - bi - cj - dk$ таки антиавтоморфизм.

K — поле с инволюцией $\lambda \mapsto \bar{\lambda}$

Def. $\phi : U \to V$ называется полулинейным, если

1. $\phi(u+v) = \phi(u) + \phi(v)$
2. $\phi(u\lambda) = \bar{\lambda}\phi(u)$

Def. $B : V \times V \to K$ называется полулинейной формой, если B линейно по второму аргументу и полулинейно по первому.

1. $B()$

2.

3. $B(u\lambda, v\mu) = \bar{\lambda} B(u,v)\mu$

B называется скалярным произведением, когда отношение ортогональности симметрично.

Но чаще рассматривают полулинейные формы с дополнительным условием симметрии:

B называется эрмитовым, если $B(u,v) = \overline{B(v,u)}$, антиэрмитовым — если $B(u,v) = -\overline{B(v,u)}$

Как уже говорилось, с полулинейными формами это все равно, в основном люди работают с эрмитовыми, но профессионалы в области — с антиэрмитовыми.

Сейчас все будет то же самое, только где-то черточки появятся.

Пусть $e_1, \dots e_n$ — базис V, $G = (B(e_i, e_j)), u, v \in V = K^n$

$$B(u,v) = \bar{u}^T G v$$

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \bar{u} = \begin{pmatrix} \bar{u_1} \\ \vdots \\ \bar{u_n} \end{pmatrix}$$

и все свойства — невырожденность, симметричность, эрмитовость — выражаются в терминах матрицы Грама.

B эрмитова $\Leftrightarrow$ G эрмитова, т.е. $G = \bar{G}^T$

h — матрица замены базиса, тогда матрица Грама в новом базисе — это $\bar{h}^T G h$.

Теперь поинтересуемся, как связано B с двойственным пространством.

$$\tilde{B} : V \to V^* : u \mapsto B(u, -)$$

— теперь не линейное, а полулинейное

Сопряженное пространство $V \mapsto \overline{V}$ — там скаляр выносится с сопряжением.

$$\tilde{B} V \to \overline{V^*} : u \mapsto B(-, u)$$

— линейное.

И поэтому первое тоже задание линейного отображения $V \to \overline{V^*}$.

И видно, что во всех формулках и теоремах надо просто придумать, где написать черту.

2.20 Классификация эрмитовых пространств над $\mathbb{C}$

V — в.п. над $\mathbb{C}, B : V \times V \to \mathbb{C}$ — эрмитово скалярное произведение.

$$Q(x_1, \dots x_n) = \sum_{i,j} a_{ij} \bar{x_i} x_j$$

$$B(v\lambda, v\lambda) = \bar{\lambda} B(v, v)\lambda$$

То есть выносится квадрат нормы комплексного числа, то есть вещественное неотрицательное число.

И $B(v, v) = \overline{B(v, v)} \in \mathbb{R}$, то есть получим все то же самое, что для вещественных скалырных произведений.

Def. Базис e_i пространства ортогональный, если $B(e_i, e_j) i \neq j$, и ортонормированным, если при этом $B(e_i, e_i) = \pm 1$ или 0.

В кажестве упражнения читалетю оставляется доказать аналоги теоремы о разложении и теоремы Лагранжа.

Theorem 2.20.1. *В любом эрмитовом пространстве над $\mathbb{C}$ существует ортонормированный базис, причем количество векторов со скалярным квадратом $+1$ во всех таких базисах одинаково.*

Def. V невырожденное, тогда такое пространство обозначается $\mathbb{C}^{p,q} (p + q = n)$.

В случае с положительно определенным скалярным произведением — $\mathbb{C}^n \Leftrightarrow$ матрица Грама единична. Обычно такое пространство называют унитарным пространством, ну или, если хочется уточнить, классически унитарным. В ФАНе это называют конечномерным гильбертовым пространством.

В координатах скалярное произведение задается так:

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, B(u, v) = \bar{u_1} v_1 = \dots \bar{u_p} v_p - \bar{u_{p+1}} v_{p+1} - \dots - \bar{u_{p+q}} v_{p+q}$$

и других не бывает с точностью до замены базиса.

2.21 Вещественная и мнимая части эрмитова скалярного произведения

$B : V \times V \to \mathbb{C}, B(u, v) = \overline{B(v, u)}$

Это комплексное число, и конечно имеет вещественную и минмую части.

$V \cong \mathbb{C}^n, e_1, \dots e_n$ — базис. Когда обсуждали комплексификацию, уже заметили, что $\mathbb{C}^n \cong \mathbb{R}^{2n}$ и естественный базис над $\mathbb{R}$ у этой штуки $e_1, ie_1, \dots e_n, ie_n$ — любое пространство над комплексными числами четномерно как пространство над вещественными.

$$B(u,v) = A(u,v) + iC(u,v), A(u,v), C(u,v) \in \mathbb{R}$$

— два линейных отображения $V \times V \to \mathbb{R}$

Theorem 2.21.1. *Пусть B — эрмитово скалярное произведение на V, A — его вещественная часть, а C — мнимая. Тогда*

1. *A, C — билинейные скалярные произведения на $V_{\mathbb{R}}$, причем первое — симметрическое, второе — симплектическое*
2. *$A(iu, iv) = A(u,v), C(iu, iv) = C(u,v)$*
3. *$A(iu, v) = C(u,v), C(iu, v) = -A(u,v) = -A(v,u)$*

Обратно, если A, C удовлетворяют этим условиям, то $B = A + iC$ является эрмитовым скалярным произведением.

Proof. $\Rightarrow$

A, C билинейны, потому что вещественные числа нормально выносятся, а сопоставление вещественной и мниной части линейно.

$$B(u,v) = \overline{B(v,u)}$$
$$A(u,v) + iC(u,v) = A(v,u) - iC(v,u)$$

и так как характеристика поля не два, это ровно 1.

$B(iu, iv) = B(u,v)$ очевидно, так что 2.

$-iB(u,v) = B(iu,v) = \overline{B(v,iu)}$, и все получается.

$\Leftrightarrow$ Ну надо просто написать и проверить. □

Морально, на пространстве задано одновременно и симплектическое скалярное произведение, и симметрическое, и поэтому на таком пространстве геометрия гораздо богаче (в смысле, это совсем не то же самое, что евклидово пространство).

Глава 3

Теория групп

Что мы знаем: что такое группа, подгруппа, нормальная подгруппа, произведение подмножеств группы по минковскому, что G/H — это множество смежных классов, и когда подгруппа нормальная, там есть структура фактор-группы. Порядок группы, индекс $|G : H|$. Знаем, что такое гомоморфизм, изоморфизм, ядро и образ, центр группы, коммутатор ($[h, g] = hgh^{-1}g^{-1}$), циклическая подгруппа, чем-нибудь порожденная, коммутант $[G, G]$ (подгруппа, порожденная всеми коммутаторами). Класс сопряженных элементов $x^G = \{y \in G | \ \exists\ g \in G : y = g^{-1}xg\}$, еще есть сопряженные с другой стороны ${}^Gx$. Прямое произведение групп.

Rem. Группа G называется совершенной, если $G = [G, G]$.

Кстати не видно прерятствий к их классификации, но это задача, которую пока не решили (сейчас она в таком состоянии как классификация конечных простых групп сто лет назад).

Что узнаем: действия групп на множестве, G-множества, конечные группы, в т.ч. теоремы Силова, полупрямые произведения и какие-то еще обобщения произведений, свободные группы и задания групп образующими соотношениями.

3.1 Действия групп на множествах

Def. G — группа, X — множество, и у нас задано $\alpha : G \times X \to X : \ g, x \mapsto gx$.

Такое отображение называется левым действием группы на множество (X является левым G-множеством: $G \curvearrowright X$), если

1. $\forall\ h, g \in G\ \forall\ x \in X\ (hg)x = h(gx)$
2. $1 \cdot x = x$

Отсюда сразу же вытекает, что $(x \mapsto gx)$ — биекция множества на себя (у каждого элемента группы есть обратный).

Правыми действием группы на множество называется отображение $X \times G \to X : \ x, g \mapsto xg$, если

1. $x(hg) = (xh)g$
2. $x \cdot 1 = x$

Это одно из мест, где моноид и группа принципиально отличаются: в моноиде правые и левые могут быть никак не связаны, а на группах у нас есть операция, которая позволяет превратить одно в другое: $(hg)^{-1} = g^{-1}h^{-1}$. Итак, любое правое G-множество превращается в левое G-множество: $g \circ x = xg^{-1}$.

То есть для групп это одно и то же и можем изучать только левые множества.

Def. X, Y — два левых G-множества. Тогда $\phi : X \to Y$ называется G-морфизмом (морфизмом G-множеств), если оно G-эквивариантно:

$$\phi(gx) = g\phi(x)$$

Этому определению соответствует такая коммутативная диаграмма:

$$\begin{array}{ccc} G \times X & \xrightarrow{\alpha_X} & X \\ \downarrow{\scriptstyle (id_G, \phi)} & & \downarrow{\scriptstyle \phi} \\ G \times Y & \xrightarrow{\alpha_Y} & Y \end{array}$$

то есть $\phi \circ \alpha_X = \alpha_Y \circ (id_G, \phi)$.

Rem. Вообще, если мы вдруг еще этого не заметили, коммутативные диаграмы очень полезные. Например, они помогают лучше разобраться в том, что происходит в более сложных случаях.

Например, есть у нас $H \curvearrowright X; G \curvearrowright Y$, хотим что-то такое же.

$$\begin{array}{ccc} H \times X & \xrightarrow{\alpha_X} & X \\ \downarrow{\scriptstyle (\psi, \phi)} & & \downarrow{\scriptstyle \phi} \\ G \times Y & \xrightarrow{\alpha_Y} & Y \end{array}$$
$$\psi : H \to G; \phi : X \to Y$$

ϕ называется ψ-эквивариантным, если

$$\phi(gx) = \psi(g)\phi(x)$$

3.2 Естественные действия

1. Естественное действие S_n

   Def. $S_n \curvearrowright \underline{n} = \{1, \ldots, n\}$

   $\pi \in S_n : \underline{n} \to \underline{n}$

   То, что это действие группы на множество — это ровно

(a) $\pi\sigma(i) = \pi(\sigma(i))$

(b) $id(i) = i$

и это называется естетсвенным действием группы на множество.

Пусть $G \curvearrowright X : G \times X \to X$; рассмотрим соответсвующие парциальные отображения $g \in G \mapsto \ \theta_g : X \to X(x \mapsto gx)$ — левая трансляция (left translation by g).

Это биекция и $\theta_g \in S_X$:

$$\theta_{g^{-1}}\theta_g = id_X$$

$$\theta_{hg} = \theta_h\theta_g$$

То есть $\theta : G \to S_x : g \mapsto \theta_g$ — гомоморфизм. Обратно, задав гомоморфизм $\theta : G \to S_x$, мы задаем на X структуру G-множества: $gx = \theta_g(x)$.

И это первый и самый важный пример действия группы на множестве.

То есть структура левого G-множества на X — ровно гомоморфизм $\theta : G \to S_x$. Структура правого множества — антигомоморфизм, и это еще одна причина, по которой мы изучаем левые множества (чтобы не говорить слово анти).

Def. Гомоморфизм $\theta : G \to S_x$ называется представлением группы G. То есть представление — это $\phi : G \to$ куда-то, где мы умеем считать.

Если $Ker(\phi) = 1$, то такое представление называется точным (faithful).

2. Естественное (векторное) действие (представление) $GL(n, R), R$ комм. с единицей. $GL(n, R) \curvearrowright R^n$:

$$GL(n, R) \times R^n \to R^n$$

$$u \mapsto gu$$

$$h, g \in GL(n, R)\ (hg)u = h(gu); eu = u$$

Это левое действие, естественное на столбцах.

Есть столь же естественное правое действие, на строчках, называется ковекторным представлением:

$$^nR \times GL(n, R) \to {}^nR : v, g \mapsto vg$$

И из одного можно сделать другое:

$$GL(n, R) \times R^n \to R^n : g, u \mapsto g^{-T}u$$

(контраградиентная матрица)

Заметим, что наше действие является еще и линейным, то есть все теты — автоморфизмы R^n на себя.

$$g(u+v) = gu + gv$$

$$g \in GL(n,R), u, v \in R^n, \lambda \in R$$

$$g(u\lambda) = (gu)\lambda$$

То есть линейные действия $G \curvearrowright R^n$ соответсвтуют линейным представлениям $G : \theta : G \to GL(n,R)$.

3. $GL(2,\mathbb{C}) \curvearrowright \overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ (одноточечная компактификация).

$$GL(2,\mathbb{C}) \times \overline{\mathbb{C}} \to \overline{\mathbb{C}}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \mapsto \frac{az+b}{cz+d}$$

Это корректно определенное отображение (дробно-линейное преобразование, дробно-линейное действие); упражнение: это действие.

Самая известная модель плоскости Лобачевского:

$$SL(2,\mathbb{R}) \curvearrowright H = \{z \in \mathbb{C} | Im(z) > 0\}$$

Очень часто в теории чисел рассматривается $SL(2,\mathbb{Z})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} C(GL(2,\mathbb{C})) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL(2,\mathbb{C})(projective)$$

$PSL(2,\mathbb{C}) = SL(2,\mathbb{C})/$центр

3.3 Действия, определяемые в терминах структуры группы

G — группа

1.

$$G \curvearrowright G : G \times G \to G(g, x \mapsto gx)$$

С этим мы связываем гомоморфизм $G \to S_G : g \mapsto (x \mapsto gx)$ (в скобочках — отображение L_g $G \to G : g \mapsto L_g$). Это действие группы на себе левыми трансляциями (левое регулярное представление группы G)

Теорема Кэли утверждает, что $L : G \to S_G$ — вложение. Мы уже знаем, что это гомоморфизм, а то, что это вложение, следует из того, что ядро тривиальное (единица).

Corollary. Каждая группа порядка n вкладывается в S_n.

2. Действие группы на себе правыми трансляциями (тоже левое действие группы на себе, правое регулярное представление).

$$G \curvearrowright G : G \times G \to G : g, x \mapsto xg^{-1}$$

Любая левая и правая трансляции коммутируют: $(hx)g^{-1} = h(xg^{-1})$. Здесь ровно написано, что $\forall\ h, g\ G\ L_h R_{g^{-1}} = R_{g^{-1}} L_h$.

3. Еще можно заметить, что $G \times G \curvearrowright G$:

$$(G \times G) \times G \to G$$

$$(h, g), x \mapsto hxg^{-1}$$

4. Действие на себе левыми сопряжениями

$$\Delta : G \to G \times G (g \mapsto (g, g))$$

$$G \times G \to G : g, x \mapsto {}^g x = gxg^{-1}$$

$I_g : G \to G\ (inner) : x \mapsto {}^g x$ — внутренний автоморфизм

$I : G \to S_G\ (g \mapsto I_g)$ — гомоморфизм, $I_{hg} = I_h I_g, I_1 = id, I_{g^{-1}} = (I_g)^{-1}$ — биекция, и $I_g(xy) = I_g(x)I_g(y) \Leftrightarrow\ {}^g(xy) = {}^g x \cdot {}^g y$. $I : G \to Aut(G) : g \mapsto I_g$ — представление автоморфизмами.

$Ker(I) = \{g \in G |\ \forall\ x \in G : {}^g x = x\} = C(G)$. Будет точным тогда и только тогда, когда G — группа без центра (то есть он тривиален). $Inner(G) = Im(I) = \{I_g | g \in G\} \leq Aut(G)$ — нормальная погруппа (группа внутренних автоморфизмов), т.е. $\forall\ \phi \in Aut(G)\ \phi I_g \phi^{-1} = I_{\phi(g)}$.

$Inn(G) = G/C(G); Aut(G)/Inn(G) = Out(G)$ — внешние автоморфизмы G.

3.4 Однородные пространства группы

G — группа, $H \leq G$; $G/H = \{gH | g \in G\}$ — множество правых смежных классов G по H.

$$G \curvearrowright G/H\ G \times G/H \to G/H$$

$$g, xH \mapsto\ gxH$$

— действительно левое действие. С такой структурой G/H — левое однородное G-множество (пространство).

Таким образом, сопоставление $g \mapsto (xH \mapsto gxH)$ задает гомоморфизм $G \mapsto S_{G/H}$ — здорово, потому что размер второго множества маленький; но прежде чем порадоваться, нам конечно хочется узнать, а какое ядро у этой штуки.

H нормальная $\Leftrightarrow$ $H^g \leq H \ \forall \ g \in G$ (множество сопряженных). С подгруппой можно связать еще две: $H^G = \langle H^g, g \in G \rangle$ — минимальная нормальная подгруппа, содержащая H, $H_G = \cap_{g \in G} H^g$ — сердцевина H, максимальная нормальная подгруппа, содержащаяся в H.

Theorem 3.4.1 (Обобщенная теорема Кэли)**.** *$H \leq G$. Ядро перестановочного представления $G \to S_{G/H}$ равно H_G.*

Proof. g лежит в ядре $\Leftrightarrow \ \forall \ x \in G \ gxH = xH$, т.е. $x^{-1}gx \in H \Leftrightarrow \ \forall \ x \in G \ g \in H^{x^{-1}}$; эквивалентно, $g \in H_G$ $(x := g)$. □

Corollary (1)**.** $H \leq G, [G : H] = n \Rightarrow \ |G : H| \mid n!$

Corollary (2)**.** Теорема Пуанкаре: если $H \leq G$ и $|G : H| < \infty \ \Rightarrow \ |G : H_G| < \infty$.

Corollary (3)**.** Если p — наименьший простой делитель $|G|, H \leq G, |G : H| = p \Rightarrow H$ — нормальная подгруппа.

//и можно вывести много следствий такого рода с нетривиальными оценками

Proof. $|G : H_G| \mid gcd(|G|, p!) = p$ □

3.5 Орбиты и стабилизаторы

$G \curvearrowright X, x \in X$

Def. $Gx = \{gx | g \in G\} \subseteq X$ — орбита элемента

$G_x = \{g \in G | gx = x\} \leq G$ — стабилизатор элемента (точки; он же нормализатор, централизатор, подгруппа изотропии).

Theorem 3.5.1.

$$Gx \cong G/G_x$$

//изоморфны как G множества

Corollary.

$$|Gx| = |G : G_x|$$

Proof. $gx \in Gx \mapsto \ gG_x$

Это отобаржение корректно ($hx = gx \Leftrightarrow \ g^{-1}hx = x \Leftrightarrow \ g^{-1}h \in G_x \Leftrightarrow \ hG_x = gG_x$), это биекция, это мы тоже только что доказали в выкладке. □

Statement. *Скажем, что два элемента Gмножества эквивалентны, если пересечение их орбит непусто. Это действительно отношение эквивалентности и $Gx \cap Gy \neq \emptyset \Leftrightarrow \ Gx = Gy$. Иными словами, либо орбиты двух точек не пересекаются, либо совпадают.*

Proof. Если $Gx \cap Gy \neq \emptyset \Leftrightarrow \exists\, h, g \in G : hx = gy$

$\Rightarrow\ y = g^{-1}hx \Leftrightarrow Gy \leq Gx$, и по тем же соображениям верно обратное включение: $x = h^{-1}gy \Leftrightarrow Gx \leq Gy$ □

Theorem 3.5.2 (Что мы только что поняли)**.** *X = дизъюнктное объединение различных орбит; $x_1, \dots x_n$ — представители различных орбит*

$$X = Gx_1 \sqcup \dots \sqcup Gx_n$$

Corollary. То есть например если у нас есть два непересевающихся множества, где задано действие одной и той же группы, то задано и действие этой группы на объединении (копроизведение G-множеств). Обратно, действие группы на множество сводится к действиям на его орбитах.

Def. Говорят, что X — однородное G-множество (или что действие G на X транзитивно), если $\forall\, x, y \in X\ \exists\, g \in G : y = gx$.

То есть теорема сводит изучение действий группы на множестве к изучению действий на однородных множествах.

Rem. То, что отличает теорию динамических систем от этого: при действии моноидов на множестве орбиты называются траекториями и могут пересекаться и не совпадать. Это потому что есть необратимые преобразования, и там все намного сложнее.

Зададимся вопросом, а как связаны стабилизаторы двух элементов x, y с одинаковыми орбитами?

$y = gx; hy = y \Rightarrow\ hgx = hy = y = gx \Rightarrow\ (g^{-1}hg)x = x$, то есть $g^{-1}G_y g \leq G_x$. По симметрии, $g^{-1}G_y g = G_x$

3.6 Классификация G-множеств

1. Поняли, что любое G-множество — дизъюнктное объединение орбит
2. Значит надо классифицировать G-множества, на которых G действует транзитивно.

   Знаем, что так ведет себя на G/H (да уже и на себе тоже). Оказывается, что больше ничего нету, и больше никаких изоморфизмов между стабилизаторами, кроме тех, что выше написали, нету.

   Theorem 3.6.1. *(a) Любое однородное G-множество изоморфно множеству вида G/H для некоторой подгруппы $H \leq G$*

   (b) Два множества G/F и G/H изоморфны если и только если $F \sim_G H$

   Proof. X — однородное, $x \in X$. Знаем, что $X = G_x \cong G/G_x$. А еще знаем, что если $F, H \leq G, F \sim_G H \Rightarrow\ G/F \cong G/H$. Построим изоморфизм явно; хотим $g^{-1}Fg = H \Leftrightarrow Fg = gH$. $xF \mapsto xgH$, это гомоморфизм и биекция.

   Обратно, пусть $G/F \cong G/H; F \mapsto gH \Rightarrow\ \forall\, x \in G\ xF \mapsto xgH \Rightarrow$ (??) $g^{-1}Fg = H$ (упражнение пока). □

3.7 Центр p-группы

Цель: доказательства центральных арифметических результатов про строения конечных групп в зависимости от разложения их порядка на простые множители (теоремы Силова).

Def. Группа G конечного порядка называется p-группой, если $|G| = p^m$.

$p^m = |G|_p$ — p-часть порядка $|G|$, если $p^m|||G|$.
То есть группа — это p-группа, если и только если $|G| = |G|_p$

Ex (Обриты и стабилизаторы, дейсвтия группы на себе сопряжениями). 1. $G \curvearrowright G$: $g, x \mapsto {}^g x$. Орбиты этого действия — классы сопряженных элементов группы; такой класс обозначается $x^G : \{gxg^{-1} | g \in G\}$. Стабилизатор обозначается $C_G(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$ — централизатор элемента.

Теорема из предыдущего параграфа утверждает, что каждый класс сопряженных элементов $x^G \cong G/C_G(x) \Rightarrow |x^G| = |G : C_G(x)|$. $|x^G| = 1 \Leftrightarrow x^g = \{x\} \Leftrightarrow x \in C(G)$ (элемент централен) $\Leftrightarrow$ централизатор $C_G(x) = G$. Это кстати ровно то, чем будет пользоваться для доказательства первой теоремы Силова.

2. $G \curvearrowright X$, с этим связано еще много действий группы: действия на подмножествах: $g \in G, Y \subseteq X$, тогда $gY = \{gy | y \in Y\}$.

   То есть группа действует сопряжениями на своих подмножествах.

   Когда орбита x относительно сопряжения одноэлементна? $\forall\, g \in G\ gg^{-1} \subseteq \Leftrightarrow X$ — объединение классов сопряженных элементов $\Leftrightarrow (x \in X \Rightarrow X^G \subseteq X)$

   Def. $N_G(X) = \{g \in G | gXg^{-1} = X\}$ — нормализатор X в G

$$\{gXg^{-1} | g \in G\} \cong G/N_G(X)$$

   В частности, количество сопряженных с X элементов $= |G : N_G(X)|$. Но как что себя там внутри ведет непонятно.

   Def. Централизатор $C_G(X) = \{g \in G |\ \forall\ x \in X\ gxg^{-1} = x\} = \cap C_G(x)$ — поточечный стабилизатор X. $C_G(X) \trianglelefteq N_G(X)$

Theorem 3.7.1 (Силов). *G — конечная p-группа* $\Rightarrow C(G) \neq 1$

Proof. $p \in \P; G \neq \{1\} \curvearrowright; X^G = \{x \in G |\ \forall\ g \in G\ gx = x\}$

Lemma. *Если индекс $\forall$ собственной подгруппы $H < (\neq) G$ делится на p, то $|X^G| = |X|(p)$*

Proof. $X = \sqcup$ различных обрит; ну они бывают из одного элемента изи из много: $X = X^G \sqcup Gx_1 \sqcup \cdots \sqcup Gx_s; |Gx_i| \geq 2 \Rightarrow\ Gx_i$ — собственные подгруппы в G. $|Gx_i| = |G : G_{x_i}| \Rightarrow |X| = |x^G| + \sum\limits_{i=1}^{s} |G : G_{x_i}|$, и вся эта сумма делится на p, ну вот и получили. $\square$

Применим лемму к случаю, когда $|G| = p^m$ и действует на себе сопряжением. Тогда инвариантные элементы — в точности элементы центра, а значит $|G| = |C(G)|(p)$, так что он не единичный. $\square$

Corollary. Любая группа порядка p — абелева :)

Задача: конечная p-группа удовлетворяет нормализаторному условию ($H <\neq G \Rightarrow\ N_G(H) >\neq H$)

3.8 Теорема Коши

Если $p||G| \ \Rightarrow\ \exists\, x \neq 1 \in G : x^p = 1$ (есть элемент такого порядка).

Theorem 3.8.1. *Если* $p||G| \Rightarrow\ p||\{x \in G | x^p = 1\}|$.

//и раз одно такое решение заведомо существует, то существует и нетривиальное.

McKay. //мораль — построение действия группы, которой нет в условии теоремы, на множестве, которого тоже нет в условии теоремы

$X := \{(g_1, \ldots g_p) \in G^p | g_1 \ldots g_p = 1\} \subseteq G^p$. На это множество подействуем циклическими перестановками $C_p = \langle RotateRight \rangle \curvearrowright X(RotateRight(g_1, \ldots g_p) = (g_p, g_1, \ldots g_{p-1}))$

$X^{C_p} \leftrightarrow \{x \in G | x^p = 1\}; |\{x \in G | x^p = 1\}| = |X|(p), |X| = |G|^{p-1}; p||G|$, так что получили что надо. $\square$

Rem. Такой же результат верен и для произвольного натурального числа, это теорема Фробениуса, это пока сложновато.

3.9 Теоремы Силова: формулировка

G конечная, $p \in \P$; если G абелева, то теорема о примарном разложении утверждает, что $\exists\, H \leq G : |H| = |G|_p$ (стуктурная теорема для конечных абелевых групп).

Буквально ничего подобного вроде примарного разложения не выполняется в неабелевом случае, но удивительным образом указанный выше результат сохраняется. Это и называется первой теоремой Силова.

Ex. $\mathbb{F}_q, q = p^m; SL(2, \mathbb{F}_q)$

Посмотрим на порядки

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Они равны p, а порядок произведения в случае $q = 2$, например, равен тройке.

Theorem 3.9.1 (Теоремы Силова)**.** $G, |G| < \infty, p \in \mathbb{P}$

E_p *, первая теорема Силова.* $\exists\ P \leq G, |P| = |G_p|$*:*

(a) P *— p-подгруппа*

(b) $|G : P| \perp$

— P *— силовская p-подгруппа.*

C_p *, вторая теорема Силова. Все силовские p-подгруппы в* G *сопряжены:* $P, Q \leq G, |P| = |Q| = |G_p|\ \exists\ g \in G : Q = gPg^{-1}$

D_p *, третья. Если* $H \leq G, |H| = p^h$*, то есть силовская p-подгруппа, такая, что* H *— ее подгруппа*

F_p *, четвертая, которую доказал Фробениус. Количество силовских p-подгрупп в* G *сравнимо с единицей по модулю p.*

Statement (Anzahlsatz Фробениуса)**.** *То, как формулировал и что доказывал Фробениус вместо четвертой теоремы Силова.*

$p^h||G|$*, тогда количество подгрупп* $H \leq G, |H| = p^h = 1(p)$*.*

Когда $p^h|||G|$*, это ровно четвертая теорема Силова, когда* $h = 1$ *— теорема Коши.*

Еще есть теорема Фробениуса, которая гласит, что $\forall\ n \in N|\{x^n = 1|x \in G\}|$

Доказывать последнее не будем.

Доказательство теорем Силова будет устаревшим, но с точки зрения лектора наиболее простым для начинающих. Будет опираться на то, как выглядят силовские p-подгруппы в парочке конкретных случаев: $GL(n, q) = GL(n, \mathbb{F}_q), q = p^m; S_n$.

3.10 Силовские p-подгруппы $GL(n, q)$

$\mathbb{F}_q$ — конечное поле, $q = p^m$

Theorem 3.10.1.

$$|GL(n, q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = q^{1+2+\dots+(n-1)}(q^n - 1)(q^{n-1} - 1) \dots (q - 1)$$

Proof. Ну что такое обратимый линейный оператор? Это такой, который базис в базис переводит. Так что порядок группы — это количество способов выбрать базис в $(\mathbb{F}_q)^n$.

Выбираем сначала любой ненулевой, он порождает прямую, нам подходит любой вектор не с этой прямой, новые два порождают плоскость, годится любой не с нее, а на ней q^2 элементов, ну и тд. □

Corollary.

$$|GL(n, q)|_p = p^{\frac{mn(n-1)}{2}}$$

Мы хотим построить подгруппу такого порядка. Ну так мы ее уже видели: это унитреугольные матрицы $U = U(n,q)$(unitriangular, она же максимальная унипотентная).

$$U(n,q) = \begin{pmatrix} 1 & \dots & * \\ 0 & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

Там звездочки все можно выбрать независимо какими угодно, выбрать каждую $p^m = q$ вариантов. **То есть $U(n,q)$ — силовская p-подгруппа в $GL(n,q)$.**

Corollary (2)**.** $SL(n,q)$ — с определителем единица

$$|SL(n,q)| = q^{\frac{n(n-1)}{2}}(q^n-1)\dots(q^2-1)$$

Упражнение: $|PGL(n,q)|, |PSL(n,q)|$

3.11 Первое доказательство Фробениуса теорем Силова

Rem. Формула индекса Фробениуса. $F, G \le G;\ \exists\ x_1, \dots x_s$:

$$G = Fx_1H \sqcup \dots \sqcup Fx_sH$$

Indestorwel:

$$|G:H| = |F : F \cap x_1Hx_1^{-1}| + \dots + |F : F \cap x_sHx_s^{-1}|$$
$$|G:F| = |H : H \cap x_1^{-1}Fx_1| + \dots + |H : H \cap x_s^{-1}Fx_s|$$

первой теоремы Силова. $G \hookrightarrow S_n \hookrightarrow GL(n,q), q = p^m$ — первое вложение — это теорема Кэли, второе — матрицы перестановки.

В $GL(n,q)$ если силовская p-подгруппа $U(n,q)$; разложим $GL(n,q)$ по двойному модулю $(G, U(n,q))$. $|GL(n,q) : U(n,q)|$ взаимно прост с p, пусть $x_1, \dots x_s$ — представители двойных смежных классов.

$$|GL(n,q) : U(n,q)| = |G : G \cap x_1U(n,q)x_1^{-1}| + \dots + |G : G \cap x_sU(n,q)x_s^{-1}|$$

все справа не может делиться на p, значит есть индекс такой, что $|G : G \cap x_jU(n,q)x_j^{-1}| \perp p$, то есть $G \cap x_1U(n,q)x_1^{-1}$ — силовская p-подгруппа в G. □

второй и третьей. $G, |G| < \infty, P$ — силовская p-подгруппа, H — какая-то p-подгруппа ($|H| = p^h$),

$$G = Hx_1P \sqcup \dots \sqcup Hx_sP$$

$|G:P| \perp p$,

$$|G:P| = |H : H \cap x_1Px_1^{-1}| + \dots + |H : H \cap x_sPx_s^{-1}|$$

$\Rightarrow\ \exists\ j : H \cap x_jPx_j^{-1} = H \Leftrightarrow\ H \le x_jPx_j^{-1}$

В качестве H можно взять другую силовскую p-подгруппу, и понимаем, что они сопряжены. □

3.12 Второе доказательство Фробениуса

$|G| < \infty, p||G| \Rightarrow \ \exists\ x \neq 1 \in G : x^p = 1$

Либо $x \in C(G)$, то есть порождает подгруппу подярка p, по которой можно профакторизовать, раз она нормальная: $|G/\langle x\rangle| <\neq |G|$. Индукция, база которой — абелевы группы. Считаем, что по индукции силовская p-подгруппа в $G/\langle x\rangle$ уже есть $= Q$, в качестве силовской p-подгруппы в нашей группе возьмем $p = \pi^{-1}(Q), \pi : G \to G/\langle x\rangle$.

Теперь можем считать, что $\forall$ p-элемент нецентрален, значит $|C(G)| \perp p$. Klassengleichung (class equation): $x_1, \dots x_s$ — представители нецентральных классов сопряженных элементов, тогда

$$|G| = |C(G)| + \sum_{i=1}^{s} G : C_G(x_i)$$

штука слева делится на p, $|C(G)|$ взаимно просто с ним, значит $\exists\ j : |G : C_G(x_j)| \perp p$. $C_G(x_j) <\neq G, |C_G(x_j)|_p = |G|_p$, индукция.

3.13 Силовские p-подгруппы в симметрической группе

$|S_n| = n!; p \leq n$. На какую степень p делится порядок S_n?

Statement (Формула Лежандра)**.**

$$V_p(n!) = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + \dots$$

$|S_p|_p = p = |C_p|$, и большой цикл (RotateRight) порождает силовскую p-подгруппу в S_p. Хотим в $|S_{p^2}|_p = p^{p+1}$. Можем завести циклы на каждом p-блоке и еще можем переставлять блоки местами — это называется $C_p \wr C_p$.

Какие вообще конструкции бывают над группами перестановок?

$H \curvearrowright X; G \curvearrowright Y$

Из этого можно сделать новую конструкцию $(H, X) \sqcup (G, Y) = (H \times G, X \sqcup Y)$:

$$(h, g)(x) = \begin{cases} hz, z \in X \\ gz, z \in Y \end{cases}$$

Еще одну: $(H, X) \times (G, Y) = (H \times G, X \times Y)$

$$(h, g)(x, y) = (hx, gy)$$

Еще есть сплетение групп (wreath product):

$$(H, X) \wr (G, Y) = (H \wr G, X \times Y)$$

— то что первое там написано, можно сейчас не объяснять, поймем, как это действует. У нас есть Y слоев X, и в каждом слое действует свой элемент группы H, зависящий от слоя, в котором мы находимся $(\underbrace{H \times H \times \cdots \times H}_{(Y)} \leftthreetimes G)$

$$|H \wr G| = |H|^{|Y|}|G|$$

$C_p = \langle RotareRight \rangle \leq S_p$ — силовская подгруппа; длинный цикл действует на p-элементном множестве. $|C_p \wr C_p| = p^{p+1}; |S_{p^2}|_p = p^{p+1}$. Указанное сплетение действует на множестве из p^2 элементов, то есть разбивает его на p частей и на каждой независимо действует степенью цикла. Значит $C_p \wr C_p \leq S_{p^2}$ — силовская p-подгруппа.

Ну сплетем еще разок. $|C_p \wr C_p \wr C_p| = p^{p^2+p+1}$. $|S_{p^3}|_p = p^{p^2+p+1}$, индукция

Corollary. $S = \underbrace{C_p \wr \cdots \wr C_p}_{m\text{раз}}$ — силовская p-подгруппа S_{p^m}.

Что в S_n? Представим n в p-ичной системе счисления: $n = a_m p^m + a_{m-1}p^{m-1} + \cdots + a_1 p + a_0, a_i < p$.

Там очевидно содержится так называемая подгруппа Юнга:

$$H = \underbrace{S_{p^m} \times \cdots \times S_{p^m}}_{a_m} \times \underbrace{S_{p^{m-1}} \times \cdots \times S_{p^{m-1}}}_{a_{m-1}} \times \cdots \times \underbrace{S_{p^1} \times \cdots \times S_{p^1}}_{a_1} \times \underbrace{S_{p^0} \times \cdots \times S_{p^0}}_{a_0}$$

Несложно заметить, что $|H|_p = |S_n|_p$.

Theorem 3.13.1. *Силовская p-подгруппа в S_n сопряжена с*

$$\underbrace{C_p^{\wr m} \times \cdots \times C_p^{\wr m}}_{a_m} \times \underbrace{{}_p^{\wr m-1} \times \cdots \times C_p^{\wr m-1}}_{a_{m-1}} \times \cdots \times \underbrace{C_p \times \cdots \times C_p}_{a_1}$$

Proof. По теореме Кэли G вкладывается в $S_{|G|}$ + □

Corollary. Первая теоремы Силова.

Куда можно обобщать теоремы Силова?

Вот мы знаем теорему Лагранжа: $H \leq G \Rightarrow \ |H| \mid |G|$; обратно (если какое-то число делит порядок группы, то если подгруппа такого порядка) неверно. Но если число простое, теорема Силова утверждает что-то про существование. А если брать произведение двух простых или что-нибудь еще?

Def. Подгруппа $H \leq G$ называется холловской, если $|H| \perp |G : H|$.

Вот любая силовская подгруппа является холловской.

Что такое морально такая подгруппа?

Пусть π — какое-то подмножество простых делителей порядка нашей группы. Можем определить pi-часть аналогично p-части: $|G|_\pi = \prod_{p \in \pi} |G|_p$; $|G|_{\pi'} = \prod_{p \notin \pi} |G|_p; |G| = |G|_\pi |G|_{\pi'}$.

Холловская π-подгруппа $H \leq G, |H| = |G|_\pi$

Def. $D_0(G) = G; D_1(G) = [G,G]; D_2(G) = [[G,G],[G,G]]; \dots D_n(G) = [D_{n-1}(G), D_{n-1}(G)]$
G — разрешима, если $\exists\ n : D_n(G) = 1$.

Theorem 3.13.2 (Томпсон-Файт)**.** *Если порядок группы не делится на два, тогда G разрешима.*

Theorem 3.13.3 (Теоремы Холла)**.** *$E_\pi, C_\pi, D_\pi \dots$, если G разрешима.*
Обратно, если $\forall\ p,q \in \mathbb{P} \mid |G|\ \exists$ холловская $\{p,q\}$ подгруппа, то G разрешима.

3.14 Произведения групп

Мы уже видели внешнее прямое произведение: $F, H \mapsto\ F \times H = \{(f,h) | f \in F, h \in H\}$ и умножение пар ввели покомпонентно.

Установили соотвествие с конструкцией $F, H \leq G$: внутреннее прямое произведение.

Когда $G \cong F \times H$? Тогда и только тогда, когда

1. $F \cap H = \{1\}$ (хотим биекцию $h \leftrightarrow (f,h)$)
2. $\langle F, H\rangle = G$
3. $F, H \trianglelefteq G$

Первые два понятно откуда взялись.

Rem.

$$[F,H] = \langle [f,h] \rangle\,, [f,h] = fhf^{-1}h^{-1}$$

— взаимный коммутант F, H.

$(fhf^{-1})h^{-1} = f(hf^{-1}h^{-1})$

то, что слева, лежит в H, если она нормальна, аналогично, то, что справа, в F. Так что три условия влекут $[F,H] = 1 \Leftrightarrow\ \forall\ f \in F, h \in H\ fh = hf$.

То есть в одну сторону мы доказали, в другую утверждается, что очевидно:

Они нормальны, потому что поэлементно коммутируют: $(f,h) = (f,1)(1,h)(F \hookrightarrow F \times H : f \mapsto (f,1); H \hookrightarrow F \times H : h \mapsto (1,h))$.

//в это месте мы доказали соответствующую теорему.//

Еще можно завести себе $H_1, \dots H_m \mapsto H_1 \times \dots H_m = \{(h_1, \dots h_m | h_i \in H_i)\}$ с опять покомпонентным умножением.

Theorem 3.14.1. $H_1, \dots H_m \leq G$, $G \cong H_1 \times \dots \times H_m \Leftrightarrow$

1. $\langle H_1, \dots H_m\rangle = G$
2. *H_i пересекается по единице с подгруппой, порожденной всеми отстальными H-ками*
3. $H_i \trianglelefteq G$

Для абелевых групп вместо прямого произведения пишут значок прямой суммы для конечного числа слагаемых.

Прямое произведение бесконечного числа $G_i, i \in I$ $\prod_{i\in I} G_i = \{(h_i)_{i\in I} | h_i \in G_i \ \forall \ i \in I\}$

$$(h_i)_{i\in I}(g_i)_{i\in I} = (h_i g_i)_{i\in I}$$

Ограниченное прямое произведение: $H_i \leq G_i; \prod_{i\in I\ H_i} G_i = \{(g_i)_{i\in I} | g_i \in G_i$и для почти всех$i \in I, g_i \in I\}$

$\prod_{i\in I\ 1} G_i = \{(g_i)_{i\in I} | g_i \in G_i$и для почти всех$i \in I, g_i = 1\}$

Если все G_i абелевы, то это обозначается $\oplus_{i\in I} G_i$ — бесконечная прямая сумма.

$F, H \leq G$

1. $F \cap H = \{1\}$
2. $\langle F, H\rangle = G$
3. $F, H \trianglelefteq G$

Хотим что-нибудь из этого ослабить, получить обобщение прямого произведения. Вот первое условие самое сильное как-то интуитивно, из него вытекает, что элементы подгрупп коммутируют.

Def. $G = F \circ H$ — центральное произведение, если

1. $[F, H] = 1 \Rightarrow F \cap H \leq C(G)$
2. $\langle F, H\rangle = G$
3. $F, H \trianglelefteq G$

Def (Обобщение, шикоро использующееся в топологии и геометрии)**.** $F, H \leq G$; почти прямое произведение, если

1. $|F \cap H| < \infty$
2. $\langle F, H\rangle = G$
3. $F, H \trianglelefteq G$

Если наши группы абелевы, то прямым проиведением мы не получим неабелевых групп, даже абелевых групп с элементами большего порядка: $\mathbb{Z}/10\mathbb{Z}$, перемножив с собой, не получим $\mathbb{Z}/100\mathbb{Z}$. Сейчас поговорим об этом.

3.15 Полупрямые произведения

Def. $F, H \leq G$; G является их полупрямым произведением, если

1. $F \cap H = \{1\}$
2. $\langle F, H \rangle = G$
3. $H \trianglelefteq G$, а $F \leq G$

F называется в этом случае дополнительной подгруппой.
$G = F \leftthreetimes H = H \rtimes F$ (хвостик в сторону нормальной подгруппы).

Rem. H перестановочна с любой подгруппой.

Тогда из последних двух условий будет следовать, что $\langle F, H \rangle = FH = HF$

Утверждается, что G однозначно задается (в отличае от прямого произведения, которое только первыми двумя) $F, H, F \curvearrowright H$.

Ex. 1. $S_n = A_n \rtimes C_2 = \langle (1,2) \rangle$

Мы уже можем строить неабелевы группы из абелевых: $S_3 = C_3 \rtimes C_2$

2. $GL(n, K) = SL(n, K) \rtimes K^* = \begin{pmatrix} 1 & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & \epsilon \end{pmatrix}, \epsilon \in K^*$

3. $B(n, K)$ — группа обратимых верхнетреугольных матриц (по диагонали обратимые элементы), $D(n, K) = diag, U(n, K)$ — верхнетреугольная с единичками по диагонали.

   $B(n, K) = D(n, K) \leftthreetimes U(n, K)$

4. $S_n \hookrightarrow GL(n, K)$ — преобразования-перестановки. $N(n, K)$ — группа мономиальных матриц (в каждой строке/столбце ровно один ненулевой элемент, и он обратим).

   $N(n, K) = D(n, K) \rtimes S_n$

5. $Aff(n, R)$ — аффинная группа степени n над R (отличается от векторного группой движений: у векторного — $GL(n, R)$, а у аффинного есть еще трансляции, они же переносы на вектор) $= GL(n, R) \leftthreetimes R^n$ $(g, u), g \in GL(n, R), u \in R^n$ То есть можно об этом думать как о множестве

$$\left\{ \begin{pmatrix} g & v \\ 0 & 1 \end{pmatrix} | g \in GL(n, R), v \in R^n \right\}$$

$$(h, u)(g, v) = (hg, hv + u)$$
$$\begin{pmatrix} h & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} hg & hv + u \\ 0 & 1 \end{pmatrix}$$

6. (Голоморф групп)

   G — произвольная группа, $Aut(G) \curvearrowright G$; могли бы определить $Aut(G) \leftthreetimes G$, если бы умели определять полупрямое произведение групп, одна из которых действует на другую. Истолкуем это как внутреннее произведение. $G \hookrightarrow S_{|G|}, Aut(G) \hookrightarrow S_{|G|}$

   $$G \trianglelefteq Hol(G)(\text{голоморф}) = \langle G, Aut(G)\rangle \leq S_{|G|}$$

   $G \cap Aut(G) = 1 \Rightarrow \ Hol(G) = Aut(G) \leftthreetimes G$

   //в $Hol(G)$ все автоморфизмы группы G становятся внутренними.

7. Но вообще тут зачем-то завели дополнительную конструкцию, а вообще определить нужно полупрямое произведение несложно:

   F, H — группы, $\phi : F \curvearrowright H$ — действие автоморфизмами $= \phi : F \to Aut(H) \leq S_H$

   $$F \leftthreetimes H = (\text{как множество})F \times H = \{(f, h)\}$$

   Туда вкладываются и F, и H $(f \mapsto (f, 1))$.

   $$(f_1, h_1)(f_2, h_2) = (f_1, f_2, \phi(f_2^{-1}(h_1)h_2)) = (\phi(f^{-1})(h) = h^f)\ (f_1 f_2, h_1^{f_2} h_2)$$

   потому что $(f_1, h_1)(f_2, h_2) = f_1 f_2 (f_2^{-1} h_1, f_2) h_2$

   Если бы поменяли множетели местами, то $(h_1, f_1)(h_2, f_2) = h_1 (f_1 h_2 f_1^{-1}) f_1 f_2$

   $$H \rightthreetimes F = H \times F = (h, f)$$
   $$(h_1, f_1)(h_2, f_2) = (h_1^{f_1} h_2)(f_1 f_2)$$

   То есть в конструкцию полупрямого произведения реально входят $F, H, \phi : F \to Aut(H) : F \leftthreetimes_\phi H$ — расщепляющееся расширение.

Rem (Экскурс в общую картину). Прямое произведение ослабили до полупрямого, дальше можем перестать требовать что-то еще, получим

1. расширения (Schreier, 1926); отказ от того, что F — подгруппа

   $1 \to H \to G \to F \to 1$ (стрелочки — гомоморфизмы); это ровно означает, что $H \trianglelefteq G, G/H \cong F$.

   G называется расширением F при помощи H.

   A_5 — знакопеременная группа, $|A_5| = 60$, наименьшая простая неабелева группа

   (a) $A_5 \trianglelefteq S_5; 1 \to A_5 \to S_5 \to \{\pm 1\} \to 1$
   S_5 — расширение C_2 при помощи A_5.

(b) $G = SL(2,5), |SL(2,5)| = 120; \{\pm e\} = Cent(SL(2,5))$

$$PSL(2,5) = SL(2,5)/\{\pm e\}; |PSL(2,5)| = 60$$

И это изоморфно A_5; $1 \to \{\pm e\} \to SL(2,5) \to A_5 \to 1$, то есть $SL(2,5)$ — расширение A_5 при помощи C_2.

Нормальный делитель называется ядром расширения, и с следующем семестре поймем, как устроены все расширения, если ядро абелево.

Полупрямое произведение, что логично, это ровно расширения, для которых фактор G/H тоже является подгруппой.

Школьное сложение до ста — это расширение $0 \to C_{10} \to C_{100} \to C_{10} \to 0$

2. факторизации (скрюченные произведения)

3.16 Группы порядка pq

$p < q \in \mathbb{P}$

Для равных

Theorem 3.16.1 (Нетто)**.** $|G| = p^2 \Rightarrow\ G \cong C_{p^2}$ *или* $C_p \times C_p$.

//доказательство сводится к тому, что фактор по центру не может быть циклическим

Theorem 3.16.2.

$$G; |G| = pq \Rightarrow\ G \cong C_p \leftthreetimes C_q$$

Ex (Еще один случай полупрямого произведения, он же случай $p = 2$)**.** D_n — диэральная группа, $D_n = 2n$; состоит из вращений и отражений правильного nугольника. Вращения $C_n; C_n \trianglelefteq D_n, |D_n : C_n| = 2; D_n = C_n \leftthreetimes$.

Proof. Теоремы Силова утверждают, что есть $P \leq G$ порядка p и $Q \leq G$ порядка q. Количество силовских p-подгрупп в $G = 1(p)$, а с другой стороны это $|G : N_G(P)|||G|$ по теорема Лагранжа. То есть получили два ограничения вместе. $|G| = pq$ делится на $1, p, q, pq$. Количество силовских q-подгрупп $= 1(q) \Rightarrow$ оно равно $1, 1+q, 1+2q \ldots$. Значит оно равно единице. Значит нормализатор силовской q-подгруппы равен G, то есть $Q \trianglelefteq G$. $P \cap Q = 1$ (посмотрим на порядок элемента в пересечении). И то, что $\langle P, Q\rangle = G$ тоже очевидно, ведь $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq$. То есть G — это полупрямое произведение наших подгрупп.

Зададимся еще вопросом о том, как такая штука устроена. Если $P \trianglelefteq G$, то $G = C_p \times C_q = C_{pq}$. А когда есть неабелевы группы порядка pq? (циклическая-то есть в любом порядке)

Задача: Доказать, что $|G| = 15 \Rightarrow\ G \cong C_{15}$

$m = 1(p)$ — количество силовских p-подгрупп. $m = 1 + ph|q \Rightarrow p|q-1$ — иначе $m = 1$, необходимое условие существования.

Это и достаточно условие. Автоморфизмов у циклической группы столько же, сколько у нее образующих: $Aut(C_q) = C_{q-1}$.

$|G| = pq; G = \langle X, Y | x^p = 1, y^q = 1, xyx^{-1} = y^r \rangle$ + условие $y = x^p y x^{-p} = y^{r^p} \Rightarrow\ r^p = 1(q) (x^2 y x^{-2} = y^{r^2}, x^3 y x^{-3} = y^{r^3}, \dots)$ □

3.17 Простота $A_n, n \geq 5$

Theorem 3.17.1 (Галуа). *A_n проста при $n \geq 5$.*

И ровно по этой же причине уравнения степени 5 и выше неразрешимы в радикалах (Теорема Руффини-Абеля).

Theorem 3.17.2 (Жордана - Диксона). *Группы $PSL(n, q)$ просты при $n \geq 2, q = p^m$ кроме групп $PSL(2, 2), PSL(2, 3)$ (и даже не совершенны).*

Theorem 3.17.3 (Классификация конечных простых групп, 2003). //

0 C_p

1 $A_n, n \geq 5$

2 *Группа типа Ли*

3 *одна из 26 спорадических групп*

//доказательство в 15 тысяч страниц

Rem. $A_5, |A_5| = 60$ — наименьшая неабелева простая группа;
//этот факт обсуждался на практике
$|G| < 60\ \Rightarrow\ G$ разрешима.

Proof. Пусть $\pi \in H \trianglelefteq A_n\ \Rightarrow\ \forall\ \sigma \in A_n\ [\pi, \sigma] = \pi\sigma\pi^{-1}\sigma^{-1} \in H$. В то же время, если мы возьмем сигму, не слишком отличающуюся от единичной перестановки ("маленькую сигму то есть сигму с маленьким численным инвариантом; возьмем в качестве него $|mov(\sigma)|$, то есть количество элементов, которые фактически сигма двигает), то получим и "маленькую"перестановку в H.

Lemma. *$A_n, n \geq 3$, порождается тремя циклами: $A_n = \langle (ijk), i \neq j \neq k \rangle$*

Lemma. *$A_n, n \geq 5$ порождается произведениями двух независимых транспозиций: $A_n = \langle (ij)(hk), i \neq j \neq h \neq k \rangle$*

//для A_4 последнее неверно: $V = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4$
И все трициклы тут не сопряжены (разбиваются на два класса сопряженности): $|g^G| = |G : C_G(g)|$, а порядок централизатора делит порядок группы.

Def. $G \hookrightarrow X; G$ называется дважды транзитивной, если любую пару $(x_1, x_2) : x_1 \neq x_2$ можно перевести в любую пару $(y_1, y_2), y_1 \neq y_2$, то есть $\exists\, g \in G : gx_1 = y_1; gx_2 = y_2$.

Аналогично можно определить m-транзитивность.

Ex. S_n — n-транзитивно на $\{1, \dots n\}$.

A_n — $n-2$-транзитивно (одна транспозиция портит не более двух элементов)

Итого, все трициклы образуют в $A_n, n \geq 5$ один класс сопряженности, значит, если в какой-то нормальной подгруппе есть один трицикл, то в ней есть все трициклы, то есть это вся группа (в A_4 это тоже правда, но не из этих соображений, а еще там нет подгруппы, точно содержащей трицикл, вот пример привели).

$C(A_4) = 1$, значит любая перестановка не коммутирует со всеми элементами. И значит она не коммутирует со всеми трициклами, ведь они все порождают. Т.е. $\exists\, (ijk) : \pi(ijk)\pi^{-1}(ihj) = [\pi, (ijh)] \neq 1 \in H$. Этот элемент перемещает не более шести элементов, поэтому все вычисления можно проводить в A_6. Какие классы сопряженности там есть? $(ijh), (ij)(hk), (ijhkl), (ijh)(klm)$, и тип $(ijkl)(hm)$ не встечается, потому что это на самом деле $3-3$.

1. случаи $(ijh), (ij)(hk)$ охватываются леммами
2. $(ijhkl)$

   $$[(ijhkl), (ijh)] = (ijhkl)(ijh)(ijh)(lkhji)(hji) = (ikj)$$

   (из соображений четности)

   То есть если есть 5-цикл, то есть и трицикл, то есть победили уже A_5
3. оставшийся

   $$[(ijh)(klm), (ijk)] = (ijh)(klm)(ijk)(mlk)(hji)(kji) = (ikhlj)$$

   а что происходит, если есть 5-цикл, мы уже видели.

□

Rem. Смотреть на "маленькие"элементы — стандартная техника для доказательства простоты чего-то.

Theorem 3.17.4 (Теорема Классификации (классификация конечных простых групп))**.** *Если G — конечная простая группа, то есть она не единичная и у нее ровно два нормальных делителя, то $G =$*

1. $C_p, p \in \mathbb{P}$
2. $A_5, n \geq 5$
3. *конечные группы типа Ли*

4. 26 *спорадических групп*

Простые группы типа Ли делятся на классические ($PSL(n,q), PSP(2l,q)$) и исключительные.

Спорадические группы. Первые пять — группы Матье: $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$. M_{12}, M_{24} — единственные известные пять транзитивные группы. Гипотеза Жордана гласит, что шесть транзитивных групп нет кроме A_n, S_n; M_{12}, M_{24} были придуманы в размышлениях об этой гипотезе.

Big Monster — тоже спорадическая группа! (FG — friendly giant с тех пор, как ее построили руками (потому что в ней 10^54 элементов, и добить таблицу умножения на компе так и не удалось)).

Глава 4

Образующие и соотношения (комбинаторная и геометрическая теория групп)

4.1 Свободные группы

X — произвольное множество

Def. Группа $F_X = (F(X))$ — свободная группа, свободно порожденная X, если $\forall\ G\ \forall\ \phi : x_i \in X \mapsto\ g\ \exists\ !$ гомоморфизм $\psi : F_X \to G$, ограничение которого на X совпадает с ϕ. То есть существует единственный гомоморфизм, делающий следующий треугольник коммутативным:

Def. Свободный моноид, свободно порожденный X — это моноид $W(X)$: существует единственный гомоморфизм моноидов, делающий соответствующий треугольник коммутативным:

Corollary. Из определения свободных моноида и группы следует, что если такие штуки существуют (а этого разумеется нам никто не гарантировал), то они единственны с точностью до изоморфизма.

Посмотрим, что представляет из себя свободный моноид. Пусть $X = \{x_1, \dots x_n\}$, или даже для наглядности $X = \{x, y\}$ (алфавит). Тогда моноид, куда вкладываются x, y, содержит $\wedge, x, y, xx, xy, yx, yy, \dots$ — "слова", операция — конкатенация строк (приписывание второй к первой).

Но в свободном моноиде плохо с обратимыми элементами (в представленной конструкции вот длины слов складываются). Так что если мы хотим сделать из этого свободную группу, то надо добавить формальные обратные к образующим и научиться сокращать то, что естественно было бы сократить.

$X = \{x_1, \dots x_n\}, X^{-1} = \{x_1^{-1}, \dots, x_n^{-1}\}.W(X \sqcup X^{-1})$ — тоже пока просто приписывание слов. Скажем, что $xx^{-1}, x^{-1}x = e$, а еще научимся вписывать такие штуки в слово: $uv \sim uxx^{-1}v \sim ux^{-1}xv \ \forall \ u, v \in W(X \sqcup X^{-1}) \ \forall \ x \in X$. Два слова назовем элементарно эквивалентными, если они получаются друг из друга вписыванием или вычеркиванием xx^{-1} или $x^{-1}x$. Устроим транзитивное замыкание этому отношению, итоговое назовем нужным $\sim$. Отфакторизуем $W(X \sqcup X^{-1})$ по нему.

Theorem 4.1.1. *Построенная конструкция $W(X \sqcup X^{-1})/\sim$ удовлетворяет универсальному свойству свободной группы.*

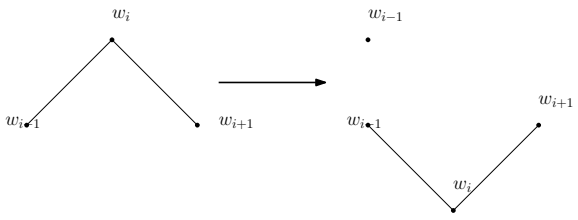
Proof. □

4.2 Свободная группа как группа редуцированных (приведенных) слов

Теперь считаем, что $F_X = W(X \sqcup X^{-1})/\sim, X$ — множество свободных образующих.

Theorem 4.2.1. *В каждом классе эквивалентности $W(X \sqcup X^{-1})$ по $\sim$ (описано в предыдущем параграфе) $\exists$! редуцированное слово (то есть такое, что в нем нет фрагментов вида xx^{-1} и $x^{-1}x$)*

Proof. Считаем, что существование нам очевидно, докажем единственность. Пусть w_0 и w_n — приведенные слова из одного класса; значит они связаны цепочкой элементарных эквивалентностей: $w_0, w_1, \dots, w_n$ (удобно наглядно представлять это в виде ломаной, где вершинки — это слова, а ребро соответствует изменению длины слова на 2). Докажем утверждение индукцией по n и по $l(w_0) + \dots + l(w_n)$ (сумма длин слов). "Убираем пики". Пусть $\exists \ w_i : 1 \le i \le n-1 : l(w_i) > l(w_{i-1}), l(w_{i+1})$; тогда эти звенья в цепочке эквивалентностей можно заменить либо на w_{i-1} (три на одно), либо на что-то, где длина w_i меньше длин соседей:



Это осуществляется вписыванием xx^{-1} или $x^{-1}x$ и вычеркиванием yy^{-1} или $y^{-1}y$. Если фрагменты, подвергшиеся действию этих операций, пересекаются, то $w_{i+1} = w_{i-1}$ (верхняя ситуация на рисунке, уменьшаем количество шагов в цепочке), если не пересекаются, то никто не мешает нам сначала вычеркнуть, а потом вписать (нижняя ситуация на рисунке, уменьшаем длину цепочки).

Таким образом, цепочка сократится до $w_0 = w_n$. □

Пусть F_X — множество редуцированных слов в $W(X \sqcup W^{-1})$, $\rho : W(X \sqcup X^{-1}) \to F_X : w \mapsto u, w \sim u, u \in F_X$. Скажем, что произведение слов $u, v \in F_X$ $uv = \rho(u + v) \in F_X$ — в точности умножение классов редуцированных слов.

Rem. $\rho(u * v) = \rho(\rho(u) * \rho(v))$

4.3 Задание групп образующими соотношениями

Нам понятно, что такое $G = \langle g_1, \dots g_n \rangle$. Будем понимать, что такое $G = \langle x_1, \dots x_n | w_1, \dots w_m \rangle$ — группа, заданная образующими x_i и определяющими соотношениями w_i.

//если $n < \infty$, то группа называется конечно порожденной, если $m < \infty$, то конечно представимой (пока считаем, что работаем с конечно представимыми группами, ? важно ли это считать).