НМУ Алгебра I
Константин Логинов

ЗаТеХано Потошином Георгием

2024

Глава 1

Векторные пространства

1.1 Жорданова нормальная форма

Матрица называется жордановым блоком, если она имеет вид

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

Болок размера $k \times k$ с λ на диагонали и с 1 над диагональю. В прошлый раз мы доказали, что для любого линейного эндоморфизма векторных конечномерных пространств над алгебраически замкнутым полем есть базис, в котором матрица имеет блочно диагональный вид, с жордановыми блоками.

Поле называется алгебраически замкнутым, если каждый многочлен над этим полем положительной степени имеет корень.

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & & 0 \\ & J_{k_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{k_n}(\lambda_n) \end{pmatrix}$$

Стоит отметить, что λ_i и k_i

Пример: Пусть полем будет $\mathbb{k} = \mathbb{R}$, а пространством $V = \mathbb{R}^2$. Заметим, что $x^2 + 1$ неприводим в этом поле. Тогда возьмём оператор поворота на 90 градусов.

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

Для неё нет жордановой нормальной формы над $\mathbb{R}$, так как у неё нет собственных значений. Если бы они были, то были бы корнем характеристического многочлена $\chi_A(t) = t^2 + 1$, а у него корней нет. Над $\mathbb{C}$, наш оператор приводим, так как $\pm\sqrt{-1}$ его собственные значения, а тогда

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

Заметим, что по жордановой нормальной форме легко вычислять инварианты, так как след – сумма диагональных элементов, $\mathrm{tr}(A) = \sum k_i\lambda_i$.

Замечание: базис, в котором оператор имеет жорданову нормальную форму, вообще говоря не единственен, например тривиальный оператор I.

Тем не менее кое-что определено канонически. Давайте означим за $n_{\lambda,k}$ – количество клеток вида $J_k(\lambda)$ в нашей матрице.

Утверждение:

$$\sum_{p=1}^{k} pn_{\lambda,p} + \sum_{p=k+1}^{\inf} kn_{\lambda,p} = \dim\mathrm{Ker}(A - \lambda\mathrm{Id})^k,\ \forall\lambda, k$$

Следовательно, $n_{\lambda,k}$ – инварианты A.

Для доказательства, давайте запишем матрицу в жордановой нормальной форме и посчитаем ядро $\dim\mathrm{Ker}(A - \mathrm{Id})^\lambda$. В таком виде нас будут интересовать только клетки, в которых стоит λ. Тогда можно предполагать, что оператор состоит только из клеток с λ. Если посмотреть на то, что происходит с клетками, то мы увидим

$$J_k(\lambda) - \lambda\mathrm{Id} = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

И если мы возведем в степень такие клетки, то равенство станет очевидным.

Замечание: Пусть $A \in \mathrm{End}(V)$. Заметим, что задать оператор A, равносильно заданию на V структуры $\mathbb{k}[t]$-модуля. Структура $\mathbb{k}[t]$-модуля это в точности $\mathbb{k}$-модуль с действием t. Зададим это действие следующим образом $t^l \cdot v = A^l(v)$, $v \in V$ и продолжим его по линейности. В обратную сторону, мы зададим оператор через действие t, то есть $A(v) = t \cdot v$. И это также эквивалентно заданию гомоморфизма (колец?) $\phi : \mathbb{k}[t] \to \mathrm{End}(V)$, где образ t будет оператором A. (Скорее всего это работает только в коммутативном случае, когда на $\mathrm{End}(V)$ Есть структура модуля и я бы брал гомоморфизмы модулей!).

Например если $A = J_k(\lambda)$, то $V \cong \mathbb{k}[t]/(t-\lambda)^k$. Давайте поймём почему этот изоморфизм имеет место. Нам нужно во первых убедится, что они изоморфны как $\mathbb{k}$-векторные пространства, а во вторых, что A действует в V также как t умножением в $\mathbb{k}[t]/(t-\lambda)^k$. Первое верно из наблюдения размерности, в обоих случаях она k. Для второго, нужно понять как $A-\lambda\mathrm{Id}$ действует на базисные вектора, а именно $e_1 \mapsto 0$ и $e_{i+1} \mapsto e_i$ для $1 \leq i \leq k$. Заметим, что $\{(t-\lambda)^i\}_{0\leq i\leq k}$ $\mathbb{k}$-базис фактор кольца, и в нём $t-\lambda$ умножением действует точно также на элементы кольца, а значит у нас есть изоморфизм $\mathbb{k}[t]$-модулей.

Следствие (из теоремы о существовании ЖНФ) Для $A \in \mathrm{End}(V)$, V – $\mathbb{k}[t]$-модуль. То $V \cong_{\mathbb{k}[t]} \bigoplus_{i=1}^{N} \mathbb{k}[t]/(t-\lambda_i)^{k_i}$, где действие A соответствует действию t, а сумма идёт по жордановым блокам. Это верно, так как матрица оператора блочно диагональная, а значит пространство раскладывается в прямую сумму подпространств, так, что на каждом подпространстве наш оператор действует как жорданов блок, а тогда применив предыдущий результат, мы получаем искомое. Такая формулировка теоремы о жордановой нормальной форме более правильная, так как она имеет обобщения, то есть на классификацию конечно порожденных модулей. В частности классификация конечных и конечно порожденных абелевых групп.

Определение: $A \in \mathrm{End}(V)$ называется полупростым, если существует базис, в котором матрица A диагональна. A называется нильпотентом, если $A^m = 0$ для $m > 1$.

Следствие (из ЖНФ): $A \in \mathrm{End}(V)$, то $A = A_{ss} + A_n$, где A_{ss} – полупрост, а A_n – нильпотент. И эти два оператора коммутируют.

$$J_k(\lambda) = \lambda\mathrm{Id} + \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

Теорема (Гамильтона-Кэли): $A \in \mathrm{End}(V) \Rightarrow \chi_A(A) = 0$. Поле не обязательно алгебраически замкнуто. $\chi_{J_k(\lambda)}(t)|_{t=a} = (t-\lambda)^k|_{t=A} = (A-\lambda)^k = 0$. А значит в каждом блоке будет 0, теорему доказали, но жульничество в том, что нам необходима алгебраическая замкнутость поля, но жульничество можно обойти, показав, что каждое поле вложено в алгебраически замкнутое.

Доказательство:
$(tE-A)(\widehat{tE-A}) = (\widehat{tE-A})(tE-A) = \chi_A(t)\mathrm{Id}$ в кольце $\mathcal{M}at_{n\times n}(\mathbb{k}[t]) = (\mathcal{M}at_{n\times n}(\mathbb{k}))[t]$. Определим отображение

$$\phi : R \to \mathcal{M}at_{n\times n}(\mathbb{k}),$$

где $R = Z_A(\mathcal{M}at_{n\times n}(K)[t])$, а устроено оно вычислением в A, то есть $\phi(\sum B_i t^i) = \sum B_i A^i$, где $B_i \in \mathcal{M}at_{n\times n}(\mathbb{k})$. Заметим, что ϕ является гомоморфизмом.

$\chi_A(A) = \phi(\chi_A(t)E) = \phi((\widehat{tE - A})(tE - A)) = \phi(\widehat{tE - A}\phi(tE - A) = \phi(\widehat{tE - A})(A - A) = 0$.

Замечание: $A \in \mathrm{End}(V)$ задание эндоморфизма эквивалентно заданию гомоморфизма $\phi : \mathbb{k}[t] \to \mathrm{End}(V)$. По теореме Гамильтона-Кэли мы знаем, что $\chi_A(t) \in \mathrm{Ker}(\phi)$. С другой стороны $\mathrm{Ker}(\phi) = (m_A(t))$, тогда можно определить m_A минимальный многочлен оператора A, минимальный многочлен оператора A, он определен однозначно, если старший коэффициент брать за 1. Заметим, что минимальны многочлен делит характеристический.

Упражнение: Существует N, что $\chi_a(t) \mid m_a(t)^N$.

Пример:

- $m_A(t) = t - \lambda$, для $A = \lambda E$. Тогда $\chi_A(t) = (t - \lambda)^k$.
- $m_A(t) = t^k$, тогда $A -$ и $\chi_A(t) = t^n$. Можно взять нулевой жорданов блок и нулевую матрицу и соединить их в блочно диагональной манере.
- Если $m_A(t) = (t - 1)^k$, то A называется унипотентом.
- Если $m_A(t) = t(t - 1)$, то A – проектор, идемпотентен

Глава 2

Поля и их расширения

Пусть $\Bbbk$ – поле. Тогда можно рассмотреть гомоморфизм $\varkappa : \mathbb{Z} \to \Bbbk, 1 \mapsto 1$, у него есть ядро $\mathrm{Ker}(\varkappa) \subseteq \mathbb{Z}$, это идеал в $\mathbb{Z}$, он главный, так как идеал кольца главных идеалов, пусть он равен (d).

Утверждение: d – простое число или 0.

Доказательство: Ядро – прообраз простого идеала, а значит ядро просто.

Определение: d – характеристика $\Bbbk$, её мы обозначаем $\mathrm{char}(\Bbbk) = d$, то есть простое число или 0, которое однозначно определяется по полю.

- $\mathrm{char}(\mathbb{Q}) = 0$
- $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$

Напоминание: Если $f : \mathbb{K} \to \mathbb{L}$ гомоморфизм полей, то он инъективен. Так как несобственный идеал только 0.

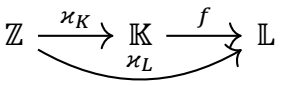
$A = \mathrm{Im}(\varkappa)$ – область целостности. Тогда можно рассмотреть поле частных $\mathrm{Frac}(A) \leq \Bbbk$, подполе в $\Bbbk$, оно называется простым подполем.

$$\mathrm{Frac}(A) \cong \begin{cases} \mathbb{Q} & \mathrm{char}(\Bbbk) = 0 \\ \mathbb{Z}/p\mathbb{Z} & \mathrm{char}(\Bbbk) = p \end{cases}$$

Простое подполе определено однозначно, так как гомоморфизм $\varkappa$ определен однозначно, канонически. Оно называется простым, так как в нём нет собственных подполей.

Утверждение: Пусть $f : \mathbb{K} \to \mathbb{L}$ – гомоморфизм полей. Тогда $\mathrm{char}(\mathbb{K}) = \mathrm{char}(\mathbb{L})$ и f индуцирует изоморфизм простых подполей в $\mathbb{K}$ и $\mathbb{L}$.

Доказательство:



Давайте тогда заметим, что композиция является гомоморфизмом $\varkappa$ для $\mathbb{L}$, так как композиция переводит единицу в единицу. Отсюда следует, что ядро $\varkappa_L$ равно ядру $\varkappa_K$, так как f вложение. Более того $\mathrm{Im}(\varkappa_K) \cong_f \mathrm{Im}(\varkappa_L)$, а значит простые подполя изоморфны, а характеристики равны.

Определение: $K \leq L$ называется расширением полей, если $K \hookrightarrow L$, то есть следующий набор данных, поле K, поле L и вложение. Иногда это обозначается (L/K) и черта читается как "над".

Если $K \leq L$, то L является векторным пространством над K. Тогда можно говорить о размерности L над K и если $\dim_K L \leq \infty$, то расширение мы называем конечным, а размерность мы будем писать чуть иначе $\dim_K L = [L : K]$.

$K_1 \leq K_2 \leq ... \leq K_s$ мы называем башней полей, а расширение $K_i \leq K_{i+1}$ – этаж этой башни.

Пример: $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ в этой башне только второй этаж конечен.

Утверждение: Если $F \leq K \leq L$, то $[L : F] = [L : K][K : L]$

Доказательство: Пусть $K = \langle x_i \rangle_F$, $x_i \in K$, где $\{x_i\}$ базис K над L и пусть $L = \langle y_j \rangle_K$, $y_j \in L$, где $\{y_j\}$ базис L над F. Тогда мы можем построить базис L над F, а именно $L = \langle x_i y_j \rangle_F$ поверим это. Пусть $a \in L$, тогда его можно разложить над $\{y_j\}$, то есть $a = \sum a_j y_j$, $a_j \in K$. Но тогда a_j можно разложить над $\{x_i\}$, то есть $a_j = \sum a_{i,j} x_i$, $a_{i,j} \in F$, а тогда $a = \sum a_{i,j} x_i y_j$, что означает $\{x_i y_j\}$ порождает L над F.

Пусть теперь $\sum a_{i,j} x_i y_j = 0$, пойдя в обратную сторону и положив $a_j = \sum a_{i,j} x_i \in K$, мы получи $\sum a_j y_j = 0$, а тогда по свойству базиса $\{y_j\}$ получим $a_j = 0$, но тогда и $\sum a_{i,j} x_i = 0$, и по свойству базиса $\{x_i\}$ получим $a_{i,j} = 0$, что означает линейную независимость $\{x_i y_j\}$, тогда это и вправду базис и его кардинал равен произведению кардиналов базисов $\{x_i\}$ и $\{y_j\}$.

Следствие: Для конечной башни полей $K_1 \leq K_2 \leq ... \leq K_s$ расширение $K_1 \leq K_s$ конечно, ттогда $K_i \leq K_{i+1}$ конечны $\forall i$.

Определение: Пусть $K \leq L$ расширение полей, элемент $0 \neq \alpha \in L$ называется алгебраичным, что $f(\alpha) = 0$ для некоторого $0 \neq f(x) \in K[x]$. Расширение $K \leq L$ называется алгебраичным, если $\forall \alpha \in L$ оно либо нуль либо алгебраично.

Утверждение: Для любого конечного расширения $K \leq L$ известно, что оно алгебраично.

Доказательство: Для ненулевого $\alpha \in L$ элементы $1, \alpha, \alpha^2, ..., \alpha^n$, где $n = [L : K]$, линейно зависимы, а значит найдутся коэффициенты $a_i \in L$, что $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$, а тогда можно положить $f(x) = a_0 + a_1 x + ... + a_n x^n \in K[x]$ и расширение алгебраично.

Обратное не верно, так как бывают бесконечные алгебраические расширения.

Пусть $K \leq L$ – расширение полей, тогда для любого $\alpha \in L$ можно устроить гомоморфизм колец

$$\phi_\alpha : K[x] \longrightarrow L$$
$$g(x) \mapsto g(\alpha)$$

Тогда обозначим целостное кольцо $K[\alpha] = \operatorname{Im}\phi_\alpha \leq L$, а его поле частных мы обозначим за $K(\alpha) = \operatorname{Frac} K[\alpha]$.

Заметим, что если α алгебраичен, то ϕ_α не вложение. Действительно, ядро не будет тривиальным по определению алгебраичного элемента. Тогда $\operatorname{Ker}\phi_\alpha \leq K[x]$ является нетривиальным идеалом, но как мы уже обсуждали многочлены над полем образуют кольцо главных идеалов, а значит $\operatorname{Ker}\phi_\alpha = (p(x))$ и $p(x) \neq 0$ и можем считать, что старший коэффициент единица. Будем называть $p(x)$ минимальным многочленом α или неприводимый, то есть $\operatorname{Irr}_\alpha^K(x)$.

Утверждение: Если $\alpha \in L$ алгебраичен над K, то $K(\alpha) = K[\alpha]$, а также степень расширения полей равна $[K(\alpha) : K] = \deg \operatorname{Irr}_\alpha^K(x)$.

Доказательство: Обозначим $f(x) = \operatorname{Irr}_\alpha^K(x)$. Пусть есть некий ненулевой элемент $\beta \in K[\alpha]$, тогда мы найдем $g(x) \in K[x]$, что $\beta = g(\alpha)$. Заметим, что $f(x)$ неприводим, так как прост. Тогда $(f(x), g(x)) = 1$, так как $f(x)$ не может делить $g(x)$, в противном случае мы бы имели $\beta = g(\alpha) = kf(\alpha) = 0$. Тогда мы можем найти соотношение Безу $f(x)h(x) + g(x)s(x) = 1$, подставим в него α, тогда останется $g(\alpha)s(\alpha) = 0$, а значит $\beta s(\alpha) = 1$ обратим, из этого заключаем, что $K[\alpha]$ - поле и совпадает со своим полем частных $K(\alpha)$.

Заметим, что в $K(\alpha) = K[\alpha] = \langle 1, \alpha, ..., \alpha^{n-1}\rangle_K$ есть базис. Он порождает, так как старшие степени α могут быть вычислены из тех, что мы выписали по минимальному многочлену и он линейно независим, так как иначе мы бы нашли меньший многочлен, зануляющий α, а у нас уже наименьший.

С расширениями полей такая история, что начав изучать, невозможно остановиться

Следствие: Пусть $K \leq L, \alpha_i \in L$ – алгебраичны над K и $L = K(\alpha_1, \dots, \alpha_n)$, тогда степень расширения $[L : K] < \infty$. Под $K(\alpha_1, \dots, \alpha_n)$ можно понимать как минимальное поле, содержащее все элементы в скобках, так и значения рациональных дробей многих переменных, выичсленных в тех же элементах, без обращения знаменателя в ноль.

Доказательство: Рассмотрим башню

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \dots \leq K(\alpha_1, \dots, \alpha_n)$$

Заметим, что α_{i+1} алгебраичен над $K(\alpha_1, \dots, \alpha_i)$, а значит каждый этаж башни конечен, а тогда и L/K конечно.

Утверждение: Пусть $F \leq K \leq L$ – башня полей, тогда L/F алгебраично равносильно тому, что K/F и L/K алгебраичны.

Доказательство Если L/F алгебраично, то для любого $\alpha \in K$, по включению $\alpha \in L$, а значит α – корень некого многочлена $f(x) \in F[x]$ и K/F алгебраично. Точно также так как для любого $\alpha \in L$, есть его зануляющий многочлен $f(x) \in F[x]$, то так как $F[x] \subseteq K[x]$, он же является многочленом над K, а заначит L/K алгебраично. Покажем теперь импликацию в обратную сторону. Пусть K/F и L/K алгебраичны, тогда для $\alpha \in L$ мы найдем зануляющий многочлен $f(x) = x^n + a_n x^{n-1} + ... + a_1$ с коэффициентами в K. Тогда построим башню $F \leq F(a_n, ..., a_1) \leq F(a_n, ..., a_1)(\alpha)$, здесь каждый этаж башни конечен, тогда конечна и вся башня, а тогда $F(a_n, ..., a_1)(\alpha)/F$ конечно, а значит алгебраично, а тогда a алгебраично над F, а тогда и расширение L/F алгебраично.

Определение: Поле L алгебраически замкнуто, если для любого $f(x) \in L[x]$ есть корень.

Пример: $\mathbb{C}$

Утверждение: Любое поле можно вложить в алгебраически замкнутое.

План: Пусть удалось построить башню полей

$$K \leq K_1 \leq K_2 \leq K_2 \leq ...$$

с условием, что любой многочлен $f(x) \in K_i[x]$ имеет корень в K_{i+1}. Тогда можно взять объединение $L = \bigcup_{i=1}^{\infty} K_i$. Это поле, так как если $\alpha, \beta \in L$, то мы найдем $\alpha \in K_i$ и $\beta \in K_j$, то можно выбрать номер побольше, что $\alpha, \beta \in K_{\max(i,j)}$ и там их уже можно сложить, умножить, поделить, взять обратные, и так далее. Это поле будет алгебраически замкнутым, так как если $f(x) = x^n + b_1 x^{n-1} + ... + b_n \in L[x]$, то найдутся индексы, что $b_j \in K_{i_j}$, тогда обозначим за $K_l = K_{\max_j(i_j)}$ и $f(x) \in K_l[x]$, а значит имеет корень в K_{l+1}.

Теперь давайте явно построим такую башню. Для этого опишем как по полю F построить поле $\widetilde{F}$, что для любого многочлена над F, $f(x) \in F[x]$ найдется корень в $\widetilde{F}$, тогда применяя бесконечное число раз эту конструкцию можно построить эту башню. Рассмотрим $\Lambda = F[\{t_f\}_{f \in F[x]}]$ кольцо многочленов от бесконечного числа переменных, заиндексированных многочленами от x над F.

Давайте построим идеал $I = (f(t_f))_{f \in F[x] \setminus F}$. Покажем, что он собственный, то есть что $\Lambda \neq I$. Если бы $I = \Lambda$, то $1 \in I$, и $g_1 f_1(t_{f_1}) + g_2 f_2(t_{f_2}) + ... + g_n f_n(t_{f_n}) = 1$

Лемма: Если K поле и $f(x) \in K[x] \setminus K$, то всегда есть расширение L, что $f(\alpha) = 0$, $\alpha \in L$ многочлен в нем имеет корень.

Можно профакторизовать по неприводимому множителю.

Тогда по лемме есть поле L в котором найдутся $\alpha_1, \dots, \alpha_n \in L$, что $f_i(\alpha_i) = 0$, тогда подставив $t_{f_i} = \alpha_i$ мы слева получим 0, а справа 1. Значит I собственный, а значит он вложен в некий максимальный идеал $\mathfrak{m}$. Тогда можно положить $\widetilde{F} = F[t_f]/\mathfrak{m}$. В этом поле любой многочлен $f(x)$ имеет корень $[t_f]$. Поэтому у любого поля есть алгебраически замкнутое надполе.

Определение: $K \leq \overline{K}$ называется алгебраическим замыканием, если $\overline{K}$ алгебраически замкнуто и любой $\alpha \in \overline{K}$ алгебраичен ($K \leq \overline{K}$ алгебраическое расширение).

Утверждение: $\overline{K}$ существует (но и единственно)

Доказательство: $K \leq L$, где L - алгебраически замкнуто, тогда положим $\overline{K} = \{$Все элементы $\alpha \in L$, что α алгебраичен над $K\}$. Проверим, что $\overline{K}$ – поле. Пусть $\alpha, \beta \in \overline{K}$. Можно посмотреть на расширение $K \leq K(\alpha, \beta)$ оно конечно, а значит алгебраично, это значит, что $\alpha + \beta$, $\alpha\beta$, α/β алгебраичны над K, а значит лежат в $\overline{K}$. Теперь давайте увидим, что $\overline{K}$ замкнуто, тогда пусть $f(x) \in \overline{K}[x]$ и мы хотим найти у него корень в $\overline{K}$, но на него можно посмотреть как на многочлен над L и в L у него есть корень α, но $f = x^k + a_1 x^{n-1} + \dots + a_n$ и в нём a_i алгебраичны над K. Тогда можно посмотреть на следующую башню

$$K \leq K(a_1, \dots, a_n) \leq K(a_1, \dots, a_n)[\alpha]$$

В этой башне первый этаж конечен, второй тоже, так как α зануляет $f(x)$, а значит вся башня тоже конечна, а тогда $K(a_1, \dots, a_n)[\alpha]/K$ конечно, а значит алгебраично, а тогда алгебраичен и α, то есть $\alpha \in \overline{K}$ и $\overline{K}$ алгебраически замкнуто.

Примеры: $\mathbb{C} = \overline{\mathbb{R}}$, $\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a$ алгебраичен над $\mathbb{Q}\}$, а что можно сказать о $\overline{\mathbb{F}_p}$?

2.1 Поле разложения многочлена

Определение: L называется полем разложения многочлена $f(x) \in K[x]$, если $K \leq L$, $f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_i \in L$ и $K(\alpha_1, \dots, \alpha_n) = L$.

Поле L строится по полю K и $f(x) \in K[x]$.

Поле L существует, так как мы можем например найти все корни в $\overline{K}$, выпишем эти корни $\alpha_i \in \overline{K}$. Тогда $L = K(\alpha_1, \dots, \alpha_n)$. Проверим однозначность конструкции, пусть $L' = K(\alpha_1', \dots, \alpha_n')$ где $\alpha_i' \in L'$ лежат в каком-то другом поле. Тогда можно устроить морфизм $\sigma : L' \mapsto \overline{K}$, $\sigma(\alpha_i') = \alpha_i$. Проверим, что это корректно [..?].

Пусть $\mathbb{F}_q$ – конечное поле с q элементами, его характеристика может быть равна только простому числу p, а тогда мы имеем вложение $\mathbb{F}_p \hookrightarrow$

$\mathbb{F}_q$ и $\mathbb{F}_q$ будет векторным пространством над $\mathbb{F}_p$, а тогда $q = p^n$ может равняться только степени p. Пусть теперь есть поле $\mathbb{F}_q$ и посмотрим на многочлен $p(x) = x^q - x \in \mathbb{F}_p[x]$. Пусть $\mathbb{F}_q^\times$ – мультипликативная группа, её порядок $|\mathbb{F}_q^\times| = q-1$, а это означает, что для любого $\alpha \in \mathbb{F}_q^\times$, $\alpha^{q-1}-1 = 0$. А тогда нетрудно видеть, что любой $\alpha \in \mathbb{F}$ является корнем $p(x)$. Тогда по теореме Безу $p(x)$ раскладывается на множители степени 1 над $\mathbb{F}_q$

$$x^q - x = \prod_{\alpha_i \in \mathbb{F}_q} (x - \alpha_i),.$$

Тогда можно посмотреть на вложение $\mathbb{F}_p(\alpha_1, \dots, \alpha_q) \leq \mathbb{F}_q$ и оно тривиально является равенством, а тогда $\mathbb{F}_q$ – поле разложения многочлена $x^q - x$.

Чем конечные поля замечательны, в теории полей, если есть расширение $K \leq L$, основной объект, который обычно изучают, это $\mathrm{Aut}_K(L)$ автоморфизмы L над K, те изоморфизмы поля L, что они сохраняют поле K. в конечном случае автоморфимы легко посчитать $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{p^n}) = \mathbb{Z}/n\mathbb{Z}$ циклическая группа, с образующей $\phi : \mathbb{F}_q \to \mathbb{F}_q = x \mapsto x^p$.

Утверждение: ϕ - гомоморфизм (Фробениуса).

Пусть есть алгебраическое замыкание $\mathbb{F}_p \leq \overline{\mathbb{F}_p}$. Возьмём многочлен $x^{p^n} - x$, у него есть $\alpha_i \in \overline{\mathbb{F}_p}$ все корни, тогда мы возьмём $\mathbb{F}_p(\alpha_1, \dots, \alpha_{p^n})$. Осталось проверить, что в $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \dots, \alpha_p^n)$ q элементов, для этого перепишем многочлен через фробениуса $\phi(x) = x^p$, а тогда $\phi^n(x) = x^{p^n}$. Тогда видно, что если α, β корни $x^q - x$, то $\alpha + \beta$, $\alpha\beta$ и α/β корни, так как оперции пропускаются через гомоморфизм Фробениуса. Единственная проблема, что в $\overline{\mathbb{F}_p}$ может быть кратные корни, но кратность корня эквивалентна тому, что это корень производнойб. но $(x^(p^n) - x)' = -1$ корней нет, а значит всего p^n различных корней.

Можно пойти по иному пути и факторизовать многочлены, но как бы мы не старались, поле всегда будет полем разложения полинома $x^q - x$.

Давайте теперь убедимся, что автоморфизмы $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ порождены автоморфизмом Фробениуса. То есть группа Галуа очень просто устроена. Про $\mathbb{F}_q^\times$ известно, что она циклическая. Пусть $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ автоморфизм поля, тогда он в частности является автоморфизмом циклической мультипликативной группы, а они устроены как возведение в некую степень, но и ноль в некоторой степени тоже ноль. Тогда $f(x) = x^k$. В частности это верно для $f(x+1) = (x+1)^k = x^k + 1$, а это означает, что каждый x должен быть корнем $\sum_{i=1}^{k-1} C_k^i x^i$. Тогда если...

Если $\sigma : K \to L$ – гомоморфизм полей, то для $a \in K$ будем обозначать $a^\sigma = \sigma(a)$. И если $f(x) = \sum a_i x^i \in K[x]$, то введем обозначение $f^\sigma(x) = \sum a_i^\sigma x^i$.

Определение: Пусть $\sigma : K \to L$ гомоморфизм полей и пусть K'/K, L'/L – расширения полей. Тогда мы будем говорить, что $\tau : K' \to L'$ – гомоморфизм полей продолжающий σ, если $\tau|_K = \sigma$.

Утверждение Пусть $\sigma : K \to L$ – гомоморфизм полей, K'/K и L'/L – расширения полей и $K' = K(\alpha)$ и α алгебраичен над K и пусть $p(x) = \mathrm{Irr}_\alpha^K(x)$ – минимальный многочлен α, тогда множество гомоморфизмов $\tau : K' \to L'$ находится в биекции с множеством корней $p^\sigma(x)$ в L'.

Доказательство: Пусть $\tau : K' \to L'$ такой, что $\tau|K = \sigma$. Давайте тогда вычислим $p^\sigma(\alpha^\tau) = p^\tau(\alpha^\tau) = (p(\alpha))^\tau = 0$, таким образом мы получили, что α^τ – это корень $p^\sigma(x)$.

Обратно, пусть $\beta \in L'$ такой, что $p^\sigma(\beta) = 0$. Тогда у нас есть $K' = K(\alpha) = K[\alpha]$, так как α алгебраичен. Тогда мы знаем, что всякий элемент из K' представляется в виде $f(\alpha)$, где $f(x) \in K[x]$. Тогда будем отправлять $\tau : f(\alpha) \mapsto f^\sigma(\beta)$. Проверим корректность, $K' = K(\alpha) = K[\alpha] = K[x]/(p(x))$, а α зануляет этот идеал. Более точно, если $f(\alpha) = g(\alpha)$ для некоторых $f, g \in K[x]$, то $(f-g)(\alpha) = 0$, а значит $f(x) - g(x) = p(x)h(x)$, но тогда $f^\sigma(\beta) - g^\sigma(\beta) = h^\sigma(\beta)p^\sigma(\beta) = 0$, а это означает, что образ при таком задании не зависит от многочлена.

Тогда есть биекция, так как по гомоморфиму мы построили корень, образ α, и по корню мы построили гомоморфизм, который отправляет α в корень, такое если есть, то он единственный, потому как по предположению $K(\alpha)$ представляется как полиномы от α.

Следствие: количество продолжений $\sigma : K \to L$ на $K' = K(\alpha)$, где α алгебраический, не превосходит $[K' : K] = \deg \mathrm{Irr}_\alpha^K(x)$.

Пример: Если $\mathbb{F}_p \leq \mathbb{F}_q, q = p^n$, есть гомоморфизм $\mathrm{Fr} : \mathbb{F}_q \to \mathbb{F}_q : a \to a^n$ и $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{F}_q)$. Про этот автоморфизм известно, что $\mathrm{ord}(\mathrm{Fr}) = n$, $\mathrm{Aut}(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. Это мы покажем чуть позже.

Определение: Пусть K'/K и K''/K – расширения полей, тогда если $\sigma : K' \to K''$ продолжает $\mathrm{Id}_K : K \to K$. То тогда σ называют гомоморфизмом над K.

Утверждение: Если L/K – алгебраическое расширение и $\sigma : L \to L$ – гомоморфизм над K, то σ – автоморфизм.

Доказательство: Достаточно проверить, что σ – сюрьективен. Пусть $\alpha \in L$, попробуем найти его прообраз. Так как расширение алгебраическое, то α удолетворяет некому полиномиальному уравнению, давайте обозначим $p(x) = \mathrm{Irr}_\alpha^K(x)$ – минимальный многочлен. Посмотрим на $\{\alpha_1, \dots, \alpha_m\}$ – множество корней $p(x)$ в L. Можно считать, что $\alpha_1 = \alpha$. Тогда рассмотрим $L' = K(\alpha_1, \dots, \alpha_m) \leq L$ подполе, порожденное всеми корнями $p(x)$. Заметим, что L'/K – конечно порождено и алгебраично над K. Тогда $\dim_K^{L'} < \infty$. Мы знаем, что $\sigma(\alpha_i) = \alpha_j$, а тогда $\sigma(L') \leq Li$, так как σ просто перестав-

ляет корни. Но $\sigma|_{L'}$ инъективен, так как гомоморфизм полей над K и K-линеен, а значит по конечномерности $\sigma|L'$ сюръективен, а тогда найдётся β, что $\sigma(\beta) = \alpha$. Отсюда и следует сюръективность, а значит σ автоморфизм.

Теорема: Если K'/K – алгебраическое расширение полей и $\sigma : K \to L$, где L – алгебраически замкнут, то существует $\sigma' : K' \mapsto L$, продолжающий σ.

Доказательство: Пусть $K'' \leq K'$ – максимальное подполе в K', на которое можно продолжить σ. Чуть позже мы покажем, что оно существует. Если $K'' = K'$, то победа, иначе, $\alpha \in K' \setminus K''$. Тогда $K'' \leq K''(\alpha)$ – алгебраическое расширение, так как α зануляется многочленом над K. Тогда мы можем продолжить σ на $\sigma'' : K'' \to L$ по предположению о K'', но тогда существует продолжение на $K''(\alpha)$, так как α алгебраичен над K'', а значит $(\mathrm{Irr}_\alpha^K)^\sigma(x)$ имеет корень в алгебраически замкнутом поле L. Противоречие, а значит $K'' = K'$. Осталось пояснить почему максимальный элемент существует. Пусть есть башня $K = K_0 \leq K_1 \leq K_2 \leq \ldots$ и есть $\sigma_i : K_i \to L$ т.ч. σ_i продолжает σ_j при $j < i$. Тогда положим $\widetilde{K} = \bigcup_i K_i$ – поле и расширение K_i. Осталось построить гомоморфизм $\tilde{\sigma} : \widetilde{K} \to L$, каждый элемент лежит в каком-то K_i, а значит продолжение говорит нам куда и что оправлять, а тогда это определено и по той же причине является гомоморфизмом. По лемме Цорна существует K''.

Следствие: Любые два алгебраических замыкание поля K изоморфны.

Доказательство Пусть $\overline{K}'/K$ и $\overline{K}''/K$ - алгебраические замыкания. Тогда по теореме существуют гомоморфизмы $\sigma : \overline{K}' \to \overline{K}''$ и $\tau : \overline{K}'' \to \overline{K}'$ такие, что это гомоморфизмы над K. Тогда посмотрим на 2 композиции $\tau \circ \sigma : \overline{K}' \to \overline{K}''$ и $\sigma \circ \tau : \overline{K}'' \to \overline{K}''$ они будут автоморфизмами, так как расширения алгебраические. Следовательно σ и τ изоморфизмы. Значит мы доказали единственность алгебраического замыкания.

Поле разложения

Пусть K-поле и $f(x) \in K[x]$ **Определение** L/K – поле разложения f, если F раскладывается на линейные множители, то есть $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ и $c \in K, \alpha_i \in L$ и $L = K(\alpha_1, \ldots, \alpha_n)$.

Утверждение: Пусть $K \leq \overline{K}$ – алгебраическое замыкание. Тогда для каждого многочлена $f(x) \in K[x]$ существует единственное подполе $L \subseteq \overline{K}$, что L – поле разложения f. И если есть $\sigma : L \mapsto \overline{K}$ над K является изоморфимом на свой образ. Следовательно поле разложения f является единственным с точностью до изоморфизма.

Доказательство: Пусть $K \leq \overline{K}$, тогда $f(x) = c(x-\alpha_1) \ldots (x-\alpha_i)$, где $c \in K$ и $\alpha_i \in \overline{K}$, тогда рассмотрим $L = \overline{K}(\alpha_1, \ldots, \alpha_i)$, заметим, что это поле разложения f. С другой стороны, если $L' \leq \overline{K}$ тоже поле разложения, то L' тоже

должен содержать все корни, а значит $L' = L$. Пусть $\sigma : L \to \overline{K}$ гомоморфизм, пусть по прежнему $\alpha_1, \dots, \alpha_n$ – корни $f(x)$ в $\overline{K}$. Тогда $f^\sigma(x) = f(x)$, так как гомоморфизм над K. Вычислим $f(\alpha_i^\sigma) = f^\sigma(\alpha_i^\sigma) = (f(\alpha_i))^\sigma = 0$, а значит корни f в L отправляются в корни $L' \leq \overline{K}$ в поле разложении в K, а тогда σ индуцирует гомоморфизм $L \to L'$, он инъективен, и так как является мономорфизмом конечномерного пространства, то изоморфизм. Теперь осталось доказать, что поле разложения единственно с точностью до изоморфизма. Пусть $L \leq \overline{K}$ и L' – поля разложения f. Тогда $\mathrm{id} : K \to \overline{K}$ можно продолжить на алгебраическое расширение L'/K, а тогда у нас будет продолжение $L' \to \overline{K}$ и по предыдущему утверждению это будет изоморфизм на $L \leq \overline{K}$.

Это мы рассуждали про поле разложение одного многочлена, но конечно же можно совершенно аналогично говорить про поле разложения семейства многочленов. Если у нас есть $\{f_i\}_{i \in I}$, где i пробегает I и каждый $f_i \in K[x]$, то мы можем определить поле разложения L/K для этого семейства, если для любого i многочлен f_i раскладывается на линейные множители в L, и L порождено корнями f_i. Совершенно аналогичное определение.

Утверждение: Пусть $K \leq \overline{K}$ – алгебраическое замыкание и $\{f_i\}_{i \in I}$, где $f_i(x) \in K[x]$. Тогда существует единственно подполе $L \leq \overline{K}$, такое, что L – поле разложения для $\{f_i\}$. Для любого поля разложения L любой гомоморфизм $\sigma : L \to \overline{K}$ над K является изоморфизмом на единственное подполе разложения семейства в $\overline{K}$. И как следствие поле разложения семейства $\{f_i\}$ единственно с точностью до изоморфизма над K. Доказательсво, аналогично, в моменте с сюрьективность нужно будет провернуть трюк с конечным подрасширением. Последняя часть той же диаграммой и доказывается.

2.2 Нормальные расширения

Определение: Пусть L/K – алгебраическое расширение полей, тогда будем говорить L/K – нормально, если любой гомоморфизм $\sigma : L \to \overline{K}$ является автоморфизмом поля L.

Утверждение: Нормальность алгебраического расширения L/K эквивалентна тому, что для любого многочлена $f(x) \in K[x]$ если он имеет корень в L, то раскладывается на линейные множители.

Доказательство: $\underline{\Leftarrow:}$ Пусть $\sigma : L \to K$ гомоморфизм над K. Пусть $\alpha \in L$, тогда положим $p(x) = \mathrm{Irr}_\alpha^K(x)$. Тогда как мы уже сегодня обсуждали α^σ – тоже корень $p(x)$. Отсюда следует, что $\mathrm{Im}\,\sigma \leq L$, но тогда σ является автоморфизмом, так как L алгебраичен над K.

$\underline{\Rightarrow:}$ Пусть расширение L/K нормально. Пусть $f(x) \in K[x]$ и $\alpha \in L$ его корень в расширении и $\beta \in \overline{K}$ его корень в алгебраическом замыкании. Тогда как мы видели ранее существует гомоморфизм $\sigma : L \to \overline{K}$ такой, что $\alpha^\sigma = \beta$, а значит $\beta \in L$. А тогда любой корень $f(x)$ содержится в L.

Утверждение: Нормальность L/K эквивалентна тому, что L – поле разложения некоторого семейства $\{f_i\}_{i\in I}$ полиномов.

Доказательство: $\underline{\Rightarrow:}$ Пусть $\{\alpha_j\}_{j\in J}$ – порождающее множество L над K. Возьмём семейство многочленов $\{\mathrm{Irr}^K_{\alpha_j}(x)\}_{j\in J}$, тогда заметим, что L – поле разложения для этого семейства, так как любой полином из семейства имеет корень, и так как расширение нормально, то они раскладываются на линейные множители, а с другой стороны эти корни по конструкции порождают L.

$\underline{\Leftarrow:}$ Пусть L – поле разложения $\{f_i\}_{i\in I}$, тогда любой его гомоморфизм над K в алгебраическое расширение имеет одинаковый образ, а тогда оно нормально.

2.3 Конечные поля

Пусть $\mathbb{F} \leq \mathbb{F}_{\mathbb{q}}$, где $q = p^n$. Тогда у нас есть $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{F}_q)$. Мы знаем, что $\mathbb{F}_q$ – поле разложения $x^q - x$, так как он раскладывается на разные линейные множители в $\mathbb{F}_q$ и их ровно q штук. Заметим, что порядок $\mathrm{Ord}(\mathrm{Fr}) \leq n$, так как $\mathrm{Fr}^n = \mathrm{Id}$, что следует из факта, что любой элемент поля удовлетворяет $x^q - x = 0$. С другой стороны, если бы порядок был бы $k = \mathrm{Ord}(\mathrm{Fr}) < n$, то все корни бы удовлетворяли уравнению $x^{q'} - x = 0$, где $q' = p^k$, чего не может быть, так как корней было бы больше, чем степень многочлена, а значит $\mathrm{Ord}(\mathrm{Fr}) = n$. Теперь докажем, что $\mathrm{Aut}(\mathbb{F}_q \cong \mathbb{Z}/n\mathbb{Z}$. По утверждению, которое мы видели раньше, количество стрелок $\mathbb{F}_1 \to \overline{\mathbb{F}_p}$ не больше степени расширения, то есть n, но Fr порождает как раз n стрелок, а тогда это все стрелки.