# *НМУ Алгебра I*
# *Константин Логинов*

Потошин Георгий

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 $\lambda$ 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 болочно 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 $\lambda_i$ и $k_i$

**Пример:** Пусть полем будет $\Bbbk = \mathbb{R}$, а пространством $V = \mathbb{R}^2$. Зметим, 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 бозначим за $n_{\lambda,k}$ – количество клеток вида $J_k(\lambda)$ в нашей матрице.

**Утверждение:**

$$\sum_{p=1}^{k} p n_{\lambda,p} + \sum_{p=k+1}^{\mathrm{inf}} k n_{\lambda,p} = \mathrm{dimKer}(A - \lambda \mathrm{Id})^k, \ \forall \lambda, k$$

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

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

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

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 $\Bbbk[t]$-модуля. Структура $\Bbbk[t]$-модуля это в точности $\Bbbk$-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?) $\phi : \Bbbk[t] \to \mathrm{End}(V)$, 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 $V \cong \Bbbk[t]/(t-\lambda)^k$. Давайте поймём почему этот изоморфизм имеет место. Нам нужно вопервых убедится, что они изоморфны как $\Bbbk$-векторные пространства, а во вторых, что $A$ действует в $V$ также как $t$ умножением в $\Bbbk[t]/(t-\lambda)^k$. Первое верно из наблюдения размерности, в обоих случаях она $k$. Для второго, нужно понять как $A - \lambda\mathrm{Id}$ дей ствует на базисные вектора, а именно $e_1 \mapsto 0$ и $e_{i+1} \mapsto e_i$ для $1 \le i \le k$. Заметим, что $\{(t-\lambda)^i\}_{0\le i\le k}$ $\Bbbk$-базис фактор кольца, и в нём $t - \lambda$ умножением действует точно также на элементы кольца, а значит у нас есть изоморфизм $\Bbbk[t]$-модулей.

**Следситвие (из теоремы о существовании ЖНФ)** Для $A \in \mathrm{End}(V)$, V – $\Bbbk[t]$-модуль. То $V \cong_{\Bbbk[t]} \bigoplus_{i=1}^N \Bbbk[t]/(t-\lambda_i)^{k_i}$, 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 деуствует 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 $\mathcal{M}at_{n\times n}(\Bbbk[t]) = (\mathcal{M}at_{n\times n}(\Bbbk))[t]$. Определим отображение

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

где $R = Z_A(\mathcal{Mat}_{n\times n}(K)[t])$, а устроено оно вычислением в $A$, то есть $\phi(\sum B_i t^i) = \sum B_i A^i$, где $B_i \in \mathcal{Mat}_{n\times n}(\mathbb{k})$. Заметим, что $\phi$ 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 страший коэффициент брать за 1. Заметим, что минимальны многочлен делит характеристичесий.

**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 жордановый блок и нулевуюматрицу и соединить их в блочно диагональной маньере.
- 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:** $d$ – характериситка $\Bbbk$, 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 $f : \mathbb{K} \to \mathbb{L}$ гомоморфиз 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 назаватеся 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:**

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\varkappa_K"] \arrow[rr, bend right, "\varkappa_L"'] & \mathbb{K} \arrow[r, "f"] & \mathbb{L} \end{tikzcd}$$

Давайте тогда заметим, что композиция является гомоморфизмом $\varkappa$ для $\mathbb{L}$, так как композиция перводит 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 $\dim_K L = [L : K]$.

$K_1 \leq K_2 \leq \ldots \leq K_s$ 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 кординал равен произведению кординалов базисов $\{x_i\}$ и $\{y_j\}$.

**Следствие:** Для конечной башни полей $K_1 \leq K_2 \leq \ldots \leq K_s$ 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 $1, \alpha, \alpha^2, \ldots, \alpha^n$, где $n = [L : K]$, линейно зависимы, а значит найдутся коэффициенты $a_i \in L$, что $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, а тогда можно положить $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ 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

$$\begin{aligned} \phi_\alpha : K[x] &\longrightarrow L \\ g(x) &\mapsto g(\alpha) \end{aligned}$$

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 $\alpha$ алгебраичен, то $\phi_\alpha$ 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 $\alpha$ или ниприводимый, 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 протвном 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 $\alpha$, 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 $\alpha$ могут быть вычислены из тех, что мы выписали по минимальному многочлену и он линейно независим, так как иначе мы бы нашли меньший многочлен, зануляющий $\alpha$, 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 $\alpha_{i+1}$ 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 $\alpha$ – 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 стороную. Пусть $K/F$ и $L/K$ алгебраичны, тогда для $\alpha \in L$ мы найдем зануляющий многочлен $f(x) = x^n + a_n x^{n-1} + \ldots + a_1$ с коэффициентами в $K$. Тогда построим башню $F \leq F(a_n, \ldots, a_1) \leq F(a_n, \ldots, a_1)(\alpha)$, здесь каждый этаж башни конечен, тогда конечна и вся башня, а тогда $F(a_n, \ldots, a_1)(\alpha)/F$ конечно, а значит алгебраично, а тогда $\alpha$ 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

$$K \leq K_1 \leq K_2 \leq K_2 \leq \ldots$$

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 $f(x) = x^n + b_1 x^{n-1} + \ldots + b_n \in L[x]$, 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 $g_1 f_1(t_{f_1}) + g_2 f_2(t_{f_2}) + \ldots + g_n f_n(t_{f_n}) = 1$

**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 наудутся $\alpha_1, \dots, \alpha_n \in L$, 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 либой $\alpha \in \overline{K}$ 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 $\alpha$ 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 $\alpha + \beta$, $\alpha\beta$, $\alpha/\beta$ 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 $\alpha$, 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 $\alpha$ 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 $\alpha$, 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 равнятся 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:** $\phi$ - 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 $\alpha, \beta$ корни $x^q - x$, то $\alpha + \beta$, $\alpha\beta$ и $\alpha/\beta$ 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 $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ пораждены автоморфизмом Фробениуса.