Лекция 6 | Тензорное произведение расширений и сепарабельные расширения.

Тензорное произв $V \otimes_{\mathbb{K}} W$ – вект. пр-в $/\mathbb{K}$.

было определение через унив. св-во:

$$\begin{tikzcd} V \times W \arrow[d] \arrow[dd, bend left] \arrow[dd, bend right] \\ V \otimes W \arrow[d, dashed, "\exists!"] \\ U \end{tikzcd}$$

удобнее пользоваться определением через разл. тензоры $V \otimes_{\mathbb{K}} W = \langle \text{"} v \otimes w \text{"} \mid \text{с условиями линейности} \rangle$.

Если V, W – алгебры $/\mathbb{K}$. (коммутативные).

тогда на $V \otimes_{\mathbb{K}} W$ имеется естеств. стр-ра (комм.) алгебры,

умножение покомпонентно:

$$(v \otimes w) \cdot (v' \otimes w') := (v v') \otimes (w \cdot w').$$

<u>Пример.</u> $\mathbb{K}[x_1, \dots x_n] \otimes_{\mathbb{K}} \mathbb{K}[y_1, \dots, y_m] = \mathbb{K}[x_1, \dots x_n, y_1, \dots, y_m]$.

Базисы – мономы.

$$\mathbb{K}[x_1, \dots x_n]/(f(x)) \otimes \mathbb{K}[y_1 \dots y_m]/(g(y)) = \mathbb{K}[x_1, \dots x_n, y_1 \dots y_m]/(f(x), g(y))$$

<u>Пример.</u> $\mathbb{E}/\mathbb{K}$, $\mathbb{F}/\mathbb{K}$ – поля $/\mathbb{K}$.

тогда $\mathbb{E} \otimes_{\mathbb{K}} \mathbb{F}$ – алгебра $/\mathbb{K}$.

$$\mathbb{E} \xrightarrow{e \mapsto e \otimes 1} \mathbb{E} \otimes_{\mathbb{K}} \mathbb{F} \xleftarrow{1 \otimes f \,\leftarrow\, f} \mathbb{F}$$

Если в $\mathbb{E} \otimes_{\mathbb{K}} \mathbb{F}$ выбрать максимальный идеал m,

то получим диаграмму полей.

$$\begin{tikzcd} & \mathbb{E} \arrow[dr] & \\ \mathbb{K} \arrow[ur] \arrow[dr] & & \mathbb{E} \otimes \mathbb{F}/m \\ & \mathbb{F} \arrow[ur] & \end{tikzcd}$$

$=: \mathbb{L}$ – поле содержащее $\mathbb{E}$ и $\mathbb{F}$, как подполя.

Замечание $\mathbb{E} \otimes_{\mathbb{k}} \left(\mathbb{k}[t] / (f(t)) \right) \cong \mathbb{E}[t] / (f(t))$

замена констант.

f - неприводимый в $\mathbb{k}$, , мн-н $f(t)$ мог стать приводимым в $\mathbb{E}$.

$\mathbb{k}[t]$ — полиномы с коэф в $\mathbb{k}$, $\mathbb{E} \otimes_{\mathbb{k}} \mathbb{k} = \mathbb{E}$

$\mathbb{E} \otimes_{\mathbb{k}} \mathbb{k}[t] = \mathbb{E}[t]$ — полиномы с коэф в $\mathbb{E}$.

Пример.
$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[t] / (t^2+1) \simeq \mathbb{C}[t] / (t^2+1) \overset{\text{КТО}}{\simeq} \mathbb{C}[t] / (t+i) \oplus \mathbb{C}[t] / (t-i) \simeq$$

$\mathbb{C} = \mathbb{R}[t] / (t^2+1)$ $\qquad t^2+1 = (t+i)\cdot(t-i)$

$$\simeq \mathbb{C} \oplus \mathbb{C}.$$

В качестве максимального идеала можно взять одно из слагаемых.

Пример.
$$\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}] \cong \mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[t] / (t^2-3) = \mathbb{Q}(\sqrt{2})[t] / (t^2-3) \simeq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

неприводим

$$\Rightarrow [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Как при помощи тензорного произведения расширений строить алгебраич. замыкание поля.

Конструкция Пусть $\mathbb{k}$ — поле, Ω — мн-во всех неприводимых $/\mathbb{k}$ мн-нов.

$\bigotimes_{\mathbb{k}, \alpha \in \Omega} \mathbb{k}_\alpha$, где $\mathbb{k}_\alpha := \mathbb{k}[x] / f_\alpha(x)$ $\quad f_\alpha$ — соотв. неприв. мн-н.

бесконечно. но приближается конечными тензорными произв-ями

бесконечное тензорное произведение — линейная оболочка разложимых тензоров вида $v_1 \otimes v_2 \otimes \ldots \otimes v_N \otimes 1 \otimes 1 \ldots$

S - конечное подмн-во Ω.

конечные

$$S \subset T \subset \Omega$$

$\mathbb{k}_S := \bigotimes_{\alpha \in S} \mathbb{k}_\alpha$ - корректно определено,

$$\left(\bigotimes_{\alpha \in S} \mathbb{k}_\alpha \right) \xrightarrow{\mathrm{Id} \otimes 1 \otimes \ldots \otimes 1} \left(\bigotimes_{\alpha \in T} \mathbb{k}_\alpha \right)$$

Про $\bigotimes_{\alpha \in \Omega} \mathbb{k}_\alpha$ следует думать, как про $\bigcup_{S \subset \Omega} \mathbb{k}_S$.

Пусть m — максимальный идеал в $\bigotimes_{\alpha\in\Omega} \mathbb{K}_\alpha = A = \bigcup_S K_S$

и $\mathbb{K}' := \bigotimes_{\alpha\in\Omega} \mathbb{K}_\alpha / m$ имеет корень для каждого неприв. $f_\alpha \in \Omega$.

т.к. $\mathbb{K}_\alpha \hookrightarrow \mathbb{K}'$.

Далее можно продолжить и построить цепочку алгебраических расширений:

$$\boxed{\underbrace{\mathbb{K} \subset \mathbb{K}'}_{\text{алгебр}} \underbrace{\subset \mathbb{K}''}_{\text{алгебр.}} \subset \dots}$$

Почему алгебраических, т.к. $\mathbb{K}_S / \mathbb{K}$ — конечное $\Rightarrow$ алгебраическое.

и композиция алгебраич. расширений — алгебраическое.

Пусть $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L} \ni \alpha$ — алгебр $/\mathbb{F}$ $\Rightarrow$ α — корень мн-на $f(x) \in \mathbb{F}[x]$.

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$.

$\Rightarrow$ α — корень мн-на $f(x) \in \mathbb{K}(a_0, a_1, \dots, a_n) =: \mathbb{E}$

(a_i — алгебр. $/\mathbb{K}$)

$\Rightarrow$ $\mathbb{E}/\mathbb{K}$ — конечное расширение.

$\Rightarrow$ $\mathbb{E}(\alpha)/\mathbb{K}$ — тоже конечное $\quad \mathbb{E}(\alpha) \supset \mathbb{E} \supset \mathbb{K}$

$\Rightarrow$ α — алгебраич. $/\mathbb{K}$.

Тогда $\bigcup_{i=0}^{\infty} \mathbb{K}^{(i)}$ — поле. алгебр $/\mathbb{K}$.

Поэтому все мн-ны из $\mathbb{K}$ будут разложимы в $\bigcup \mathbb{K}^{(i)}$

$\Rightarrow$ оно алгебр. замкнуто.

Определение из коммутативной алгебры. в честь Артина.

(Коммутативное) кольцо с единицей наз-ся $\boxed{\text{артиновым}}$, если оно является конечномерной алгеброй $/\mathbb{K}$.

Примеры $\mathbb{F}/_{\mathbb{K}}$ конечное, $\mathbb{E} \otimes_{\mathbb{K}} \mathbb{F}$

Упр. Если $\dim_{\mathbb{K}} A < \infty$, то любая цепочка убывающих идеалов $A \supset I_0 \supset I_1 \supset I_2 \supset \dots$ стабилизируется: $\exists N$: $I_N = I_{N+1} = \dots$.

Опр. артинова алг-ра A — наз-ся полупростой, если в A нет нильпотентов.

(любое ~~представление~~ / модуль полупрост, т.е. является прямой суммой простых). $A \otimes M \to M$, $M = \oplus M_i$ ← простые

Теор. $\dim_{\mathbb{K}} A < \infty$ и A — полупроста $\Longleftrightarrow$ $A \simeq \bigoplus_{i=1}^{N} \mathbb{F}_i$, где $\mathbb{F}_i/\mathbb{K}$ — конечное расширение поля $\mathbb{K}$.

(Комментарий: максимальные идеалы в $\bigoplus_{i=1}^{N} \mathbb{F}_i$ = $\bigoplus_{j\neq i} \mathbb{F}_i$, соотв. простые — это $\mathbb{F}_i$)

любой A-мод $\simeq \bigoplus_{i\in S} \mathbb{F}_i^{n_i}$.

Д-во: ($\Leftarrow$) очевидно. Если $a = (a_1, \dots, a_N)$ — нильпотент $\Leftrightarrow$ $a^M = 0 = (a_1^M, \dots, a_N^M) \Rightarrow a_i^M = 0 \Rightarrow a_i = 0$.

($\Rightarrow$) (Идемпотент это эл-нт $e \in A$, т.ч. $e^2 = e$. $\Leftrightarrow$ $e\cdot(1-e) = 0$. тогда $eA \subset A$ и $A = eA \oplus (1-e)A$.)

Построим идемпотент, выберем минимальный идеал $I \subset A$. $I \neq 0$.

(если такого нет, то A — это поле, т.к. иначе $(z) = A$ $\forall z \in A$, $z \neq 0$ $\Rightarrow (z) \ni 1 \Rightarrow \exists w: zw = 1$.)

$\forall z \in I$, $z \neq 0$ имеем $(zI) \subseteq I \Rightarrow (zI) = I$

и эл-ты $\underbrace{1, z, z^2, z^3, \dots z^N}$ линейно зависимы т.к. $\dim_{\mathbb{K}} A < \infty$. как операторы в $\mathrm{End}(I)$.

$\Rightarrow$ $1 = a_1 z + a_2 z^2 + \dots + a_N z^N = f(z)$

Утв-ся, что $f(z)$ — идемпотент, проектирующий на I.

$f(z) \equiv 1 \mod I. \Rightarrow f(z)^2 = f(z).$

Имеем $A \simeq I \cdot f(z) \oplus (1-f(z)) A$

Далее индукция по $\dim A$.

<u>Лемма</u> Разложение в прямую сумму полей у полупростой артиновой алг-ры однозначно.

т.е. $A \simeq \mathbb{K}_1 \oplus \ldots \oplus \mathbb{K}_s \simeq \mathbb{F}_1 \oplus \ldots \oplus \mathbb{F}_t.$

<u>Д-во:</u>

$$\mathbb{K}_i = A \cap \mathbb{K}_i = \mathbb{F}_1 \cap \mathbb{K}_i \oplus \mathbb{F}_2 \cap \mathbb{K}_i \oplus \ldots \oplus \mathbb{F}_t \cap \mathbb{K}_i.$$

$\mathbb{F}_i \cap \mathbb{K}_j$ — это поле (без дел. нуля).

$$\Rightarrow \mathbb{F}_i \cap \mathbb{K}_j = \begin{cases} 0 \\ \mathbb{K}_i \end{cases} \qquad \square.$$

<u>Цель</u> 1) предъявить критерий, когда $A/_\mathbb{K}$ — полупроста,

2) выяснить, когда $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{E}$ — полупроста.

<u>Ответ:</u> ($\mathbb{F}/_\mathbb{K}$ $\mathbb{E}/_\mathbb{K}$ — сепарабельные расширение).

<u>Опр.</u> Симметричная билинейная форма $g(\cdot,\cdot)$ на A наз-се инвариантной, если

$$g(ab, c) = g(a, bc) \qquad \forall a,b,c \in A.$$

<u>Замечание</u> $g(a,b) = g(ab, 1) =: \varepsilon(ab).$

Поэтому инвариантная форма определяется линейным функционалом

$$\varepsilon: A \to \mathbb{K}.$$

<u>Опр.</u> Пара (A, g) - артинова алгебра, невырожд. сим. инвар. форма наз-се фробениусовой алгеброй.

<u>Замеч.</u> Если $\mathbb{F}/_\mathbb{K}$ — расширение полей, $\varepsilon: \mathbb{F} \to \mathbb{K}$ ненулевой ф-ал, то $g(a,b) := \varepsilon(ab)$ — явл. невырожд. симм. формой.

т.к. $\varepsilon(a) \neq 0$ то $g(x, x^{-1}a) = \varepsilon(a) \neq 0 \Rightarrow g$ — невырожд.

С каждой артиновой алгеброй $A/_{\mathbb{K}}$ связана форма следа.

$a \in A \rightsquigarrow L_a : A \to A$, $x \to ax$, $\varepsilon(a) := tr(L_a)$.

$g(x,y) := tr(L_{xy})$.

Теорема $A/_{\mathbb{K}}$ - арт. алг. $\dim_{\mathbb{K}} A < \infty$

и форма следа $g(x,y) := tr(L_{xy})$ - невырождена,

$\Rightarrow$ то A - полупростая. (то есть $A \simeq \bigoplus_{i=1}^{n} \mathbb{F}_i$ - полей) (в A нет нильпотентов)

Д-во в след. раз.

Лекция 7

Д-во:

Если A - не полупроста, то $\exists x \in A$ - нильпотент.

Тогда L_x - нильп. оператор. $\Rightarrow tr(L_x) = 0$.

$\forall y \in A$ xy - нильп. $\Rightarrow tr\, L_{xy} = 0$ $\forall y \in A$. $\Rightarrow$ форма вырождена.

Пример. Пусть $A = \mathbb{F}_p(\sqrt[p]{t}) = \mathbb{F}_p(t)[x]/(x^p - t)$, т.е. $x = \sqrt[p]{t}$.

$\mathbb{K} = \mathbb{F}_p(t)$.

неприводим. мн-н по крит. Эйзенштейна.

Базис $A/_{\mathbb{K}}$ — $1, x, x^2, \ldots x^s, \ldots x^{p-1}$

Опер. умн. на L_{x^s} : $x^a \to \begin{cases} x^{a+s}, & a+s < p \\ t x^{a+s-p}, & a+s \geq p. \end{cases}$ - переставляет базисные вектора.

$tr(L_{x^s}) = \begin{cases} 0, & s \neq 0 \\ tr(Id) = \dim A/_{\mathbb{K}} = p = 0. \end{cases}$

Опр. Алгебраический эл-т $\alpha \in F/_{\mathbb{K}}$ наз-ся <u>сепарабельным</u>, если его минимальный мн-н $\mu_\alpha(x) \in \mathbb{K}[x]$ <u>не имеет кратных</u> корней.

неприводимый мн-н.

Замечание Неприводимый мн-н $f(x) \in \mathbb{K}[x]$ – несепарабельный (т.е. имеет кратные корни в своем поле разложения) если и только если $f'(x) \equiv 0$.

Пример. $\frac{\partial}{\partial x}(x^p - t) = p x^{p-1} = 0$.

(Производная в кольце мн-нов корректно определена над произвольным полем, кольцом). $\frac{\partial}{\partial x} x^n = n x^{n-1}$.

Если есть кратные корни, $R(f, f') \neq 0$, $\deg \text{Нод}(f, f') > 0$ $\in \mathbb{F}[x]$.

однако из алг-ма Евклида следует, что $\text{Нод}(f, f') \in \mathbb{K}[x]$.

неприводим.

$\Rightarrow \text{Нод}(f, f') \vdots f \Rightarrow f' \equiv 0$.

$\text{Нод}(f, f') = f$.

Теорема Следующие усл-ия на конечное расширение $\mathbb{F}/\mathbb{K}$ эквивалентны и наз-ся сепарабельным расширением:

(1) Все эл-ты $\alpha \in \mathbb{F}$ сепарабельны $/\mathbb{K}$.

$\Uparrow$

(2) алг-ра $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{F}$ – полупроста.

$\Uparrow$

(3) ф-ма следа $\operatorname{tr} \mathbb{F}/\mathbb{K}$ – невырождена.

Сл-ие Если α - сепарабельный $\mathbb{K}(\alpha)/\mathbb{K}$ – сепарабельное расш.

Д-во $(3) \Rightarrow (2)$ Если $\operatorname{tr} \mathbb{F}/\mathbb{K}$ – невырожд.

то форма следа $\operatorname{tr}\left(\mathbb{F} \otimes_{\mathbb{K}} \mathbb{F} / \mathbb{K}\right)$ – тоже невырр. $= \operatorname{tr} \mathbb{F}/\mathbb{K} \cdot \operatorname{tr} \mathbb{F}/\mathbb{K}$.

т.к. $\operatorname{tr}(L_{a \otimes b} : A \otimes B \to A \otimes B) = \operatorname{tr}(L_a) \cdot \operatorname{tr}(L_b)$

$\mathbb{F} \otimes_{\mathbb{K}} \mathbb{F}$ – полупроста.

$(2) \Rightarrow (1)$ Пусть $\alpha \in \mathbb{F}/\mathbb{K}$ несепарабельный, тогда $\mu_\alpha(x) = (x-\alpha)^k \cdot g(x)$ в поле разложения.

$\mathbb{K}(\alpha) \simeq \mathbb{K}[x]/\mu_\alpha(x) \simeq \mathbb{K}(\beta)$ β – другой корень $\mu_\alpha(x)$.

$g(x)$, $(x-\alpha)^k$ – взаимно просты в $\mathbb{F}$ $k > 1$.

Тогда $\mathbb{K}(\alpha)\underset{\mathbb{K}}{\otimes}\mathbb{K}(\alpha) \overset{\smile}{\simeq} \mathbb{K}(\alpha)\underset{\mathbb{K}}{\otimes}\mathbb{K}[x]/\mu_\alpha(x) \simeq \mathbb{K}(\alpha)[x]/\mu_\alpha(x) \simeq$

$\simeq \mathbb{K}(\alpha)[x]/(x-\alpha)^k g(x) \overset{\text{КТО}}{\simeq} \mathbb{K}(\alpha)[x]/(x-\alpha)^k \oplus \mathbb{K}(\alpha)[x]/g(x)$

есть нильпотент. $(x-\alpha)$, т.к. $k>1$

$\mathbb{K}(\alpha)\underset{\mathbb{K}}{\otimes}\mathbb{K}(\alpha) \subset \mathbb{F}\underset{\mathbb{K}}{\otimes}\mathbb{F}$

есть нильпотент. $\Longrightarrow$ не полупроста.

(1) $\Rightarrow$ (3)

Если $\mathbb{L} \supset \mathbb{F} \supset \mathbb{K}$ (α, β)

$\text{tr}\, L_\alpha \in \text{End}_{\mathbb{K}}\mathbb{L}$
$\in \text{End}_{\mathbb{F}}\mathbb{L}$

" $\boxed{\text{tr}_{\mathbb{L}/\mathbb{K}} \overset{\neq 0}{} \Leftarrow \text{tr}_{\mathbb{F}/\mathbb{K}} \overset{\neq 0}{} \circ \text{tr}_{\mathbb{L}/\mathbb{F}} \overset{\neq 0}{}}$ "

Поэтому достаточно показать невырожденность формы следа для примитивного расширения $\mathbb{K}(\alpha)/\mathbb{K}$, если α — сепарабельный.

Т.к. $\mu_\alpha(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_s)$ все α_i — различные.

Тогда $\left(\ln(\mu_\alpha(x))\right)' = \frac{\mu_\alpha'(x)}{\mu_\alpha(x)} = \frac{1}{(x-\alpha_1)} + \frac{1}{(x-\alpha_2)} + \ldots + \frac{1}{(x-\alpha_s)} = \frac{x^{-1}}{1-x^{-1}\alpha_1} + \ldots + \frac{x^{-1}}{1-x^{-1}\alpha_s} =$

$\boxed{\mathbb{K}(x)}$ $= \sum_{n=0}^{\infty} x^{-n-1}\cdot\underbrace{(\alpha_1^n+\alpha_2^n+\ldots+\alpha_s^n)} = \sum_{n=0}^{\infty} x^{-n-1}\,\underline{\text{tr}(L_{\alpha^n})} =$

Т.к. $\mathbb{K}(\alpha) = \mathbb{K}[x]/\mu_\alpha(x)$, х-й мн для α — $\mu_\alpha(x)$. - имеет разл. корни.

$\Rightarrow$ х-й мн-н для α^n - имеет корни $\alpha_1^n,\ldots,\alpha_s^n$.

Т.к. $\mu_\alpha' \neq 0$ то $\frac{\mu_\alpha'(x)}{\mu_\alpha(x)} \neq 0 \Rightarrow \exists N: \text{tr}\, L_{\alpha^N} \neq 0 \Rightarrow$ ф-ма следа невырождена.

Пример 1 Квадратичное расширение в поле char $\neq 2$.

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ - $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$

$\mu_\alpha(x) = (x-\alpha)(x-\beta)$.
Gal : $\alpha \leftrightarrow \beta$ $= \mathbb{Z}/2\mathbb{Z}$

Пр-р 2 $\mathbb{F}_{p^n}/\mathbb{F}_p$. - поле разложения мн-на $x^{p^n}-x$. Gal : $(F: a \to a^p)$ $\simeq \mathbb{Z}/n\mathbb{Z}$

Пр-р. $\mathbb{Q}(\zeta)/\mathbb{Q}$ $\zeta - \sqrt[n]{1}$ - поле разлож мн-на x^n-1. $\simeq (\mathbb{Z}/n\mathbb{Z})^*$.

$\Phi_n(x) = \prod_{\zeta\text{-примит.}}(x-\zeta)$

Главное Определение (Теорема)

Конечное Расширение $\mathbb{F}/\mathbb{K}$ наз-ся расширением Галуа, если выполнено одно из следующих эквив. усл-ий

(а) $\mathbb{F}$ — поле разложения сепарабельного мн-на.

(б) $\mathbb{K} = \mathbb{F}^{Gal(\mathbb{F}/\mathbb{K})}$, где $Gal(\mathbb{F}/\mathbb{K}) := Aut_{\mathbb{K}}(\mathbb{F})$ — $\mathbb{K}$-линейные автоморфизмы $\mathbb{F}$.

(в) $\exists$ конечная группа $G \subset Aut(\mathbb{F})$, т.ч. $\mathbb{K} = \mathbb{F}^G = \{\alpha \in \mathbb{F} \mid g(\alpha) = \alpha \ \forall g \in G\}$.

(г) $\mathbb{F}/\mathbb{K}$ — нормальное сепарабельное расширение.

($\forall \alpha \in \mathbb{F}$ $\mu_\alpha(x)$ — раскладывается на линейные мн-лы в $\mathbb{F}$).

(д) $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{F} \simeq \underbrace{\mathbb{F} \oplus \ldots \oplus \mathbb{F}}_{[\mathbb{F}:\mathbb{K}]}$, как $\mathbb{K}$-алгебра.

(е) $\# Aut_{\mathbb{K}}(\mathbb{F}) = [\mathbb{F}:\mathbb{K}]$.

Д-во: (а) $\Rightarrow$ (б). Пусть $\mathbb{K}' := \mathbb{F}^{Aut(\mathbb{F}/\mathbb{K})} \supset \mathbb{K}$.

Если $f(x) \in \mathbb{K}[x] \subset \mathbb{K}'[x]$ и $\mathbb{F}/\mathbb{K}$ — поле разложения $f(x)$.

Тогда $\boxed{\# Aut_{\mathbb{K}'} \mathbb{F}/\mathbb{K}' = [\mathbb{F}:\mathbb{K}']}$ также $\mathbb{F}/\mathbb{K}'$ — поле разложения. (Теор. о подъёме 2-зма).

(было $\leq$), но если корни различные (т.к. сепарабельно) то достигается р-во.

$$\# Aut_{\mathbb{K}} \mathbb{F}/\mathbb{K} = [\mathbb{F}:\mathbb{K}] \Rightarrow \mathbb{K} = \mathbb{K}'.$$

$$\geq \qquad \leq$$

$$Aut_{\mathbb{K}'} \mathbb{F}/\mathbb{K}' = \# Aut_{\mathbb{K}} \mathbb{F}/\mathbb{K}' = [\mathbb{F}:\mathbb{K}'] \qquad \square.$$

т.к. $\mathbb{K}'$ — неподв отн. $\mathbb{K}$-лин. авт.

(в) $\Rightarrow$ (г) $\mathbb{K} = \mathbb{F}^G$, тогда $\forall \alpha \in \mathbb{F}$ р-ть орбиту действие G на $\mathbb{F}$.

$\alpha = \alpha_1, \ldots, \alpha_s$. $\prod_{i=1}^{s}(x - \alpha_i) \in \mathbb{F}[x]$

но $g\left(\prod_{i=1}^{s}(x-\alpha_i)\right) = \prod_{i=1}^{s}(x-\alpha_i) \in \mathbb{F}^G[x] = \mathbb{K}[x]$.

сепарабельный мн-н и $\mu_\alpha(x)$ его делит.

$(2) \Rightarrow (a)$. $\mathbb{F}/_{\mathbb{K}}$ – конечное $\Rightarrow \mathbb{F} = \mathbb{K}[\alpha_1, \ldots, \alpha_k]$. выпишем минимальные ми-мы $\mu_{\alpha_1}, \ldots, \mu_{\alpha_k}$.

Возьмём $f(x) = \prod\limits_{i\text{-различные}} \mu_{\alpha_i}(x)$. неприв. $\Rightarrow$ или взаимно просты или совпадают.

Все μ_{α_i} – сепарабельные.

$\Rightarrow f(x)$ – сепарабельный

и $\mathbb{F}$ – поле разложения $f(x)$..

т.к. $\mathbb{F} \supset \mathbb{K}(\alpha_1, \ldots \alpha_k)$ из нормальности.

$(2) \Rightarrow (g)$ $\mathbb{F}/_{\mathbb{K}}$ - сепарабельно $\Rightarrow \forall$ промежуточного р-ия $\mathbb{F} \supset \mathbb{L} \supset \mathbb{K}$

$\mathbb{L}/_{\mathbb{K}}$ – тоже сепарабельно

Упр. $\Rightarrow \mathbb{F} \otimes_{\mathbb{K}} \mathbb{L}$ – полупростая

$\Rightarrow \mathbb{F} \otimes_{\mathbb{K}} \mathbb{L} \simeq \bigoplus\limits_{i=1}^{s} \mathbb{F}_i$ и

$$\begin{tikzcd} & \mathbb{F} \arrow[dr] & \\ \mathbb{K} \arrow[ur] \arrow[dr] & & \mathbb{F}_i \\ & \mathbb{L} \arrow[ur] & \end{tikzcd}$$

Тогда возьмём цепочку примитивных расширений.

$\mathbb{F} = \mathbb{L}_0 \supset \mathbb{L}_1 \supset \ldots \supset \mathbb{L}_s = \mathbb{K}$, т.ч. $\mathbb{L}_i = \mathbb{L}_{i+1}(\alpha_i) \cong \mathbb{L}_{i+1}[x]/_{\mu_{\alpha_{i}}(x)}$

все $\mu_{\alpha_i}(x)$ – сепарабельные ми-ны, расклад. на лин. ми-ны в $\mathbb{F}$. (нормальность).

$$\mathbb{F} \otimes_{\mathbb{L}} \mathbb{L}(\beta) \simeq \mathbb{F} \otimes_{\mathbb{L}} \mathbb{L}[x]/_{\mu_\beta(x)} \cong \mathbb{F}[x]/_{(x-\beta_1)\ldots(x-\beta_k)} \overset{\text{КТО}}{\simeq} \mathbb{F}[x]/_{(x-\beta_1)} \oplus \ldots \oplus \mathbb{F}[x]/_{(x-\beta_k)}$$

$$\simeq \mathbb{F} \oplus \ldots \oplus \mathbb{F}.$$

Далее по индукции: Если $\mathbb{F} \otimes_{\mathbb{L}_{i+1}} \mathbb{L}_i \simeq \mathbb{F} \oplus \ldots \oplus \mathbb{F}$.

Знаю, что $\mathbb{F} \otimes_{\mathbb{L}} \mathbb{F} \simeq \underbrace{\mathbb{F} \oplus \ldots \oplus \mathbb{F}}_{m}$

и $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{L} \simeq \underbrace{\mathbb{F} \oplus \ldots \oplus \mathbb{F}}_{n}$

$$\Rightarrow \mathbb{F} \otimes_{\mathbb{K}} \mathbb{F} \simeq \mathbb{F} \otimes_{\mathbb{L}} (\mathbb{F} \otimes_{\mathbb{K}} \mathbb{L}) = \mathbb{F} \otimes_{\mathbb{L}} (\mathbb{F} \oplus \ldots \oplus \mathbb{F}) \simeq \oplus \mathbb{F}^{mn}.$$

$(g) \Rightarrow (2)$ сепарабельность из пол-пр-ты.

Если $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{F} = \mathbb{F} \oplus \ldots \oplus \mathbb{F}$

$$\begin{tikzcd} & \mathbb{K} \arrow[dl] \arrow[dr] & \\ \mathbb{F} \arrow[dr, "\subseteq"'] & & \mathbb{K}(\alpha) \arrow[dl] \\ & \mathbb{F}_i & \end{tikzcd}$$

тогда $\mathbb{F} \otimes_{\mathbb{K}} \mathbb{K}(\alpha) = \mathbb{F}_1 \oplus \ldots \oplus \mathbb{F}_s$ $\quad \mathbb{F}_i \subset \mathbb{F} \Rightarrow \mathbb{F}_i \simeq \mathbb{F}\ \forall i$

$\|$

$\mathbb{F}[x]/_{\mu_\alpha(x)} \overset{\text{КТО}}{=} \bigoplus \mathbb{F}[x]/_{g_i(x)}$ $\quad g_i$ – неир. сомн. $\mu_\alpha(x)$ в $\mathbb{F}$.

$\Rightarrow \mathbb{F}[x]/g_i(x) = \mathbb{F} \Rightarrow \deg g_i(x) = 1 \Rightarrow \mu_\alpha$ – разкл. на лин. мн-ли,

$\square$