Лекция 4 | Расширение полей / колец.

Поле $\mathbb{K} \subset \mathbb{F}$ называется расширением,
обозначение $\mathbb{F}/\mathbb{K}$ (Фактор-полей не бывает).

Если $A \subset B$ — расширение колец, то B - наз-ся алгеброй над A.
(Сегодня будем работать с полями, так как это проще).

Замечание $\mathbb{L} \supset \mathbb{F} \supset \mathbb{K} \Rightarrow$
$[\mathbb{L}:\mathbb{K}] = [\mathbb{L}:\mathbb{F}]\cdot[\mathbb{F}:\mathbb{K}]$.

$\mathbb{F}$ - вект. пр-во над $\mathbb{K}$.
Введём обозначение $[\mathbb{F}:\mathbb{K}] := \dim_{\mathbb{K}} \mathbb{F}$.
Если $[\mathbb{F}:\mathbb{K}] < \infty$, то расширение наз-ся конечным.

Пример 1 Конечное поле из q - эл-ов $\mathbb{F}_q$ имеет $\operatorname{char} \mathbb{F}_q = p$.

$\Rightarrow [\mathbb{F}_q : \mathbb{F}_p] = n \Rightarrow q = p^n$.

$\mathbb{F}_q / \mathbb{F}_2 \Leftrightarrow q = 2^m$, т.е. $\mathbb{F}_{p^n} \supset \mathbb{F}_{p^m} \Leftrightarrow n \vdots m$.

($\Leftarrow$) Вложение $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ следует из явной конструкции

поле $\mathbb{F}_{q^n} := \left\{ \begin{matrix} \text{Мн-во корней} \\ \text{мн-на } x^{q^n} - x \end{matrix} \right\}$.

Пример 2 $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{C}:\mathbb{Q}] = \infty$

$[\mathbb{K}(t):\mathbb{K}]$; $\mathbb{K}(t_1, \dots, t_n)$ — поле рац. функций от n - переменных

$\uparrow$ поле рациональных ф-ий,

$\|$

Поле частных кольца $\mathbb{K}[t_1, \dots, t_n]$.

Пример 3 $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ - базис $1, \sqrt{3}$, т.к. элементы вида $a + b\sqrt{3}$ - замкнуты относительно всех операций в поле.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ - базис $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, но д-ть это напрямую требует некоторых усилий.
и мы не будем это делать явно.

Можно показать, что $(a + b\sqrt{2})^2 \neq 3 \Leftarrow a^2 + 2b^2 + 2ab\sqrt{2} = 3 \Rightarrow 2ab = 0 \Rightarrow \left[\begin{matrix} a = 0 \\ b = 0 \end{matrix}\right.$

Пример 4 $\mathbb{K}[t]/(f(t))$, если $f(x)$ – неприводимый многочлен.

Это один из очень обычных, но центральных примеров.

Опр. – Элемент $a \in \mathbb{F}/\mathbb{K}$ называется алгебраическим над $\mathbb{K}$, если $\exists$ мн-н $f(x) \in \mathbb{K}[x]$, т.ч. $f(a)=0$, т.е. a – корень мн-на с коэф из $\mathbb{K}$.

– Расширение $\mathbb{F}/\mathbb{K}$ наз-ся алгебраическим, если любой его эл-нт алгебраичен над $\mathbb{K}$.

– Ненулевой мн-н минимальной степени, со старшим коэф. 1, аннулирующий алгебраич. эл-нт $a \in \mathbb{F}/\mathbb{K}$ называется минимальным.

Лемма $\mu_a(x)$ – неприводим, $\mathbb{K}[a] = \mathbb{K}(a)$.

Д-во $\mathbb{K}[x] \xrightarrow{\varphi} \mathbb{K}[a]$ – минимальное подкольцо, содержащее a.

$\ker\varphi = (\mu_a(x))$, Тогда $\mathbb{K}[x]/(\mu_a(x)) \simeq \mathbb{K}[a] \subset \mathbb{F}$.

Если $\mu_a(x)$ – приводим, то в образе есть делители нуля, чего не может быть.

$\Rightarrow \mathbb{K}[x]/(\mu_a(x))$ – это поле. с базисом $1, x, x^2, \dots, x^{d-1}$.

$[\mathbb{K}(a) : \mathbb{K}] = \deg \mu_a(x)$

Сл-ие Если $\mathbb{F}/\mathbb{K}$ – алгебраическое $\Rightarrow \forall a_1, \dots, a_n \in \mathbb{F}$ минимальное подполе $\mathbb{K}(a_1, \dots, a_n)$, содержащее $a_1, \dots, a_n$ совпадает с минимальным подкольцом $\mathbb{K}[a_1, \dots, a_n]$, содержащим $a_1, \dots, a_n$.

Сл-ие. Расширение $\mathbb{F}/\mathbb{K}$ является конечным, если и только если оно конечно-порождено и алгебраично.

Сл-ие $a \in \mathbb{F}/\mathbb{K}$ алгебраичен над $\mathbb{K}$ $\Leftrightarrow$ Подрасширение $\mathbb{K}(a)/\mathbb{K}$ – конечное.

Предложение 1) Сумма и разность алгебраических эл-ов алгебраичны.

2) Подмн-во алгебраических элементов в поле образуют подполе.

Опр. $\overline{\mathbb{Q}} \subset \mathbb{C}$ – алгебраич. замыкание ~~поля~~ $\mathbb{Q}$ в $\mathbb{C}$.

($\dim_{\mathbb{Q}} \overline{\mathbb{Q}}$ – счётно!).

Однако, как все знают бывают и не только алгебр. числа.
они наз-ся трансцендентными.

Опр. набор эл-ов $a_1, \ldots, a_n \in \mathbb{F}/\mathbb{K}$ наз-ся алгебраич. зависимыми над $\mathbb{K}$,
если $\exists f \in \mathbb{K}[x_1, \ldots, x_n]$ т.ч. $f(a_1, \ldots, a_n) = 0$

Теор. Если $a_1, \ldots, a_n$ – алгебр. независимы, то
$$\begin{array}{ccc} \mathbb{K}[a_1, \ldots, a_n] & \xleftarrow{\sim} & \mathbb{K}[x_1, \ldots, x_n] \\ \cap & & \cap \\ \mathbb{K}(a_1, \ldots, a_n) & \xleftarrow{\sim} & \mathbb{K}(x_1, \ldots, x_n). \end{array}$$

Опр. Базис трансцендентности $\mathbb{F}/\mathbb{K}$ = максимальное количество алгебр. нз элементов.
Мощность базиса трансц. ~~обозначается~~ $\mathrm{tr.deg}_{\mathbb{K}} \mathbb{F}$.

Теор. $\mathrm{tr.deg}_{\mathbb{K}} \mathbb{F}$ – корректно определена.

Д-во (Упражнение, сложное, но понятное).

Замеч. $|\mathrm{tr.deg}_{\mathbb{Q}} \mathbb{C}|$ – континуум.

$\boxed{\text{Ещё одно д-во Т. Г. о нулях:}}$

Пусть $I = (f_1, \ldots, f_m) \subset \mathbb{C}[x_1, \ldots, x_n]$, хотим найти общий корень.
Рассмотрим $\mathbb{K} \supset \mathbb{Q}$ – порождённое коэф. f_i.
$I_0 \subset J_0 \subset \mathbb{K}[x_1, \ldots, x_n]$ – максимальный идеал, содержащий $f_1, \ldots, f_m$.

Тогда $\mathbb{F} := \mathbb{K}[x_1, \ldots, x_n]/J_0$ – поле и $f_1, \ldots, f_m$ имеют совместный корень в $\mathbb{F}^n$.

Построим г-зм поля $\mathbb{F} \xrightarrow{\varphi} \mathbb{C}$, постоянный на $\mathbb{K}$.

$$\begin{tikzcd} \mathbb{F} \arrow[rr, "\varphi"] & & \mathbb{C} \\ & \mathbb{K} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Можно считать, что $x_1,\dots,x_k$ - алгебраически независимы, а x_i - алгебраичны над $\mathbb{K}[x_1,\dots,x_{i-1}]$ для $i > k$.

Тогда строим φ следующим образом:

$\varphi(x_1),\dots,\varphi(x_k)$ - произвольный набор алгебраич. независимых эл-ов в $\mathbb{C}/\mathbb{K}$, такие найдутся, т.к. $\mathbb{C}/\mathbb{Q}$, а значит и $\mathbb{C}/\mathbb{K}$ имеют несчётную степень трансцендентности.

x_i для $i > k$ можно переводить в корни минимальных мн-нов.

Тем самым имея вложение $\mathbb{F} \overset{\varphi}{\hookrightarrow} \mathbb{C}$ мы находим общий корень мн-нов $f_1,\dots,f_m$ $(\varphi(x_1),\dots,\varphi(x_n))$.