Def.

Un campo è un anello $(K, +, \cdot)$ commutativo con unità tale che ogni elemento $x \in K \setminus \{0\}$ è invertibile

Esempi: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

$\mathbb{F}_p = \mathbb{Z}/_p$ p primo

Campi di funzioni razionali $K(x)$ K campo

Se K campo, un sottocampo di K è un sottoanello di K che è a sua volta un campo.

Un omomorfismo di campi è una funzione $f: K \to L$ morfismo di anelli con unità. $f(1)=1$

Oss.

Un morfismo di campi è sempre iniettivo. (Un campo non ha ideali propri).

Caratteristica di un campo: è il minimo $n > 0$ t.c. $n \cdot 1 = 0$ se esiste;

è 0 altrimenti.

Es: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ hanno caratteristica 0

$\mathbb{F}_p$ ha caratteristica p

$car(K(x)) = car(K)$.

<u>Fatto</u>: se K campo, $car(K)$ è 0 o è un numero primo.

<u>Def.</u> se E, F sono campi e $F \subseteq E$ si dice che E è estensione di F : E/F

<u>Def.</u> Sia E/F un'estensione; e $\alpha \in E$

1) si dice che α è algebrico su F se esiste un polinomio non costante $f(x) \in F[x]$ tale che $f(\alpha) = 0$.

2) se α non è algebrico su F, α si dice trascendente su F.

3) Se ogni $\alpha \in E$ è algebrico su F, diciamo che E/F è un'estensione algebrica; ~~al.~~ Altrimenti diciamo che E/F è una estensione trascendente.

Algebrico, trascendente ~~su~~ si intende su <u>$\mathbb{Q}$</u>

<u>Esempi</u>: • $\alpha \in K$ è algebrico su K.

- X è trascendente su K
- se $\alpha \in E$ e $\alpha^n = \beta \in F$, allora α è algebrico su F.
- $\mathbb{C}/\mathbb{R}$ è algebrica: se $\alpha = a + bi \in \mathbb{C}$, α è radice del polinomio

$$X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X].$$

- $\alpha = \sqrt{2} + \sqrt[3]{5}$ è algebrico su $\mathbb{Q}$

$$\alpha - \sqrt{2} = \sqrt[3]{5}$$

$$(\alpha - \sqrt{2})^3 = 5$$

$$\alpha^3 - 3\sqrt{2}\,\alpha^2 + 6\alpha - 2\sqrt{2} = 5$$

$$\alpha^3 + 6\alpha - 5 = \sqrt{2}\,(3\alpha^2 + 2)$$

$$(\alpha^3 + 6\alpha - 5)^2 = 2\,(3\alpha^2 + 2)^2$$

$$\rightsquigarrow \alpha^6 - 6\alpha^4 - 10\alpha^3 + 12\alpha^2 - 60\alpha + 17 = 0.$$

<u>Oss.</u> l'esempio precedente mostra un caso in cui una somma di numeri algebrici (su $\mathbb{Q}$) è algebrico (su $\mathbb{Q}$).
Vedremo che questo avviene sempre.

GENERATORI DI UN'ESTENSIONE

Sia E/F un'estensione di campi e

$S \subseteq E$ un sottoinsieme.

Diciamo che S è un insieme di generatori di E su F se ogni elemento α di E si scrive come

$$\alpha = \frac{f(s_1, \dots s_m)}{g(t_1, \dots t_n)} \quad \text{con } f, g \in F$$

$f \in F[X_1, \dots, X_m]$, $g \in F[X_1, \dots, X_n]$, $s_1 - s_m, t_1, \dots, t_n \in S$

In altre parole: il più piccolo sottocampo di E contenente F e S è E stesso.

Se $S = \{s_1, \dots, s_n\}$ è finito, scriviamo

$E = F(s_1, \dots, s_n)$.

Se $S = \{s\}$, cioè $E = F(s)$, diremo che E/F è un'estensione semplice:

$$F(s) = \left\{ \frac{f(s)}{g(s)} \;\middle|\; f, g \in F[x] \text{ e } g(s) \neq 0 \right\}$$

Oss.

Difficile provare che α è trascendente su F.

1) esistono numeri trascendenti (argomento di cardinalità)

2) e è trascendente (Liouville 1873)

3) Lindemann $\rightsquigarrow$ π trascendente
(impossibile quadrare il cerchio)

Sia E/F un'estensione e sia $\alpha \in E$
Consideriamo

$$\theta : F[x] \longrightarrow E$$
$$f(x) \longrightarrow f(\alpha)$$

si vede facilmente che θ omom. di anelli
e $\ker\theta = \{ f(x) \in \mid f(\alpha) = 0 \}$
Quindi
1) Se α è trascendente $\Rightarrow \ker\theta = \{0\}$
$\Rightarrow$ θ iniettivo
$\Rightarrow$ E contiene un sottoanello isomorfo
a $F(x)$ $\qquad F[x] \simeq F[\alpha]$
$\Rightarrow F(x) \simeq F(\alpha)$.
2) Se α è algebrico $\Rightarrow \ker\theta \neq \{0\}$
$\ker\theta$ ideale non nullo in $F[x]$ PID
$\Rightarrow \ker\theta = (f(x))$
Possiamo prendere $f(x)$ = polinomio <u>monico</u>
<u>di grado minimo</u> t.c. $f(\alpha) = 0$.

$f(x)$ si dice polinomio minimo di α su F.
Il grado di $f(x)$ si dice grado di α su F.

<u>Proposizione</u>
Se $\alpha \in E$ è algebrico su F, allora il suo polinomio minimo è irriducibile.
Viceversa, ogni polinomio monico irriducibile $f(x) \in F[x]$ è polinomio minimo di qualche elem. α algebrico su F.

<u>Dim.</u>
θ induce omomorfismo $\frac{K[x]}{\ker\theta} \hookrightarrow E$

l'immagine è un dominio $\Rightarrow \ker\theta$ è primo
$\Rightarrow \ker\theta = 0$ oppure θ è irriducibile

<u>Viceversa</u>
Se $f(x) \in K[x]$ è irrid. $\Rightarrow E = \frac{K[x]}{(f(x))}$ è un campo e $\alpha = \bar{x}$ è radice di f
$\Rightarrow f$ è polinomio minimo di α. ■

Proposizione

1) α algebrico su $K \iff K(\alpha) = K[\alpha]$

2) Se α algebrico di grado n su F, ogni elemento di $K(\alpha)$ si scrive in modo unico come polinomio in α di grado $\leq n-1$

$$K(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in K\}.$$

Dim. Sia $f(x) \in K[x]$ pol. min. di α su K

1) Se $\theta : K[x] \to E$

α alg. $\iff \ker\theta \neq (0) \iff K[\alpha] = \frac{K[x]}{(f)}$ è un campo

$\iff K[\alpha] = K(\alpha)$

2) Sia $\beta \in K[\alpha]$, $\beta = g(\alpha)$ $\quad g(x) \in K[x]$

$g(x) = f(x)q(x) + r(x)$

$g(\alpha) = r(\alpha) \qquad \deg r \leq n-1$

Unicità $\quad r(\alpha) = s(\alpha) \Rightarrow (r-s)(\alpha) = 0$

con $\deg(r-s) < \deg f \Rightarrow r(\alpha) = s(\alpha)$. ■