Teorema Sia $f(x) \in \mathbb{K}[x]$, $\mathbb{K}$ campo. Sia $\deg f(x) = n \geq 1$. Allora $f(x)$ ha al più n radici in $\mathbb{K}$ (contate con molteplicità).

- λ radice $\Rightarrow$ $f(x) = (x-\lambda)\, q(x) + r(x)$, $\begin{cases} \deg r(x) = 0 \\ r(\lambda) = 0 \end{cases} \Rightarrow r(x) = 0 \Rightarrow$

$\Rightarrow f(x) = (x-\lambda)\, q(x)$.

...

- λ_n radice $\to f(x) = (x-\lambda)(x-\lambda_2) \cdots (x-\lambda_n)\, q_n(x)$

Poiché $\deg f(x) = n$, $\deg q_n(x) = \deg f(x) - \deg (x-\lambda) \cdots =$

$= 0 \Rightarrow q_n(x)$ è costante

In particolare, se $f(x)$ avesse un'altra radice avrei due fattorizzazioni per $f(x)$, impossibile poiché $\mathbb{K}[x]$ è un UFD in quanto euclideo.

$\boxtimes$

Teorema Sia $\mathbb{K}$ campo e G un sottogruppo moltiplicativo finito di $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$, con $|G| = n$. Allora G è ciclico.

$n = \sum_{d \mid n} \varphi(d)$. Definisco $\forall\, d \mid n$ il sottoinsieme di G:

$$X_d = \{ a \in G \mid o(a) = d \}$$

G è finito
$\Downarrow$
$o(a) < +\infty$
$\forall a \in G$

Vale $\sum_{d \mid n} |X_d| = n$. Se G non fosse ciclico, allora $|X_n| = 0$.

Poiché $\sum_{d \mid n} \varphi(d) = \sum_{d \mid n} |X_d|$ deve esistere un $d \mid \varphi(d) < |X_d|$.

In particolare $1 \leq \varphi(d) < |X_d|$. Sia $g \in X_d$, vale per definizione $o(g) = d$ e in particolare tutti gli elementi di (g) sono radici di $x^d - 1$. Notiamo che in (g) ci sono esattamente $\varphi(d)$ elementi di ordine d e quindi $|(g) \cap X_d| = \varphi(d)$. Poiché $|X_d| > \varphi(d)$, $\exists\, h \notin (g) \mid h \in X_d \wedge h$ radice di $x^d - 1$. Esisterebbero però più di d radici, assurdo $\lightning$.
Quindi G è ciclico.

$\boxtimes$

OSS. $\mathbb{Z}_p^*$ è quindi ciclico $\forall p$ primo, in quanto $\mathbb{Z}_p$ è un campo.

OSS. Siano $\mathbb{K}$ campo e $f(x)$ irriducibile $\in \mathbb{K}[x]$, allora $\mathbb{K}[x]/(f(x))$ è un campo che "contiene" $\mathbb{K}$ e in cui vi è una radice di $f(x)$. Infatti $f(x + (f(x))) = a_0 + a_1\bar{x} + \dots + a_n\bar{x}^n =$
$= \overline{f(x)} = \bar{0}$.

Def. Dato E campo e A suo sottoanello, si dice che A è un SOTTOCAMPO di E se $\forall a \in A$, $a \neq 0$, $a^{-1} \in A$.

Def. Dati due campi $K \subseteq L$, diremo che L è un'ESTENSIONE di $\mathbb{K}$.

Oss. L e' spazio vettoriale su K.

Def. Sia $K \subseteq L$ e prendo $a \in L$. Considero tutti i sottocampi di L che contengono K e a. La loro intersezione e' il sottocampo minimo che contiene K e a. Esso e' detto $K(a)$.

Dati $K \subseteq L$ e $\alpha \in L$, considero $\varphi_\alpha : K[x] \longrightarrow L$, $f(x) \longmapsto f(\alpha)$, che e' un omomorfismo, e $\ker \varphi$.

$\ker \varphi$
- $\{0\} \Rightarrow \alpha$ non e' mai radice, eccetto per $f(x) = 0$
- $\neq \{0\}$

Def. $\ker \varphi = \{0\}$, si dice che $\alpha \in L$ e' **TRASCENDENTE** su K.

es. π ed e sono trascendenti su $\mathbb{Q}$.

Oss. $K[x] / \underbrace{\ker \varphi}_{(0)} \cong \underbrace{\mathrm{Imm}\, \varphi}_{K[\alpha]} \Longrightarrow K[x] \cong K[x]/(0) \cong K[\alpha]$

Sia $\ker \varphi \neq (0)$, poiché $\ker \varphi$ e' un ideale di $K[x]$ e $K[x]$ e' euclideo, allora $\ker \varphi$ e' un PID, ossia monogenerato. Allora $\ker \varphi =$
$= (g(x))$ per un qualche $g(x) \in K[x]$.

Def. Si dice che $g(x)$ e' un **POLINOMIO MINIMO** di α, ossia generatore di $\operatorname{Ker} \varphi$. In generale si indica con il polinomio minimo l'unico polinomio minimo monico.

OSS. Tale polinomio minimo e' irriducibile in $K[x]$. Se non lo fosse, avrebbe un fattore valutato nullo in α, e non sarebbe quindi minimo.

OSS. $\underbrace{K[x]/(g(x))}_{\text{campo}} \cong \underbrace{K[\alpha]}_{\text{campo}}$.

$\Longrightarrow$

Poiché $\underbrace{K[a] \subseteq K(a)}_{k_0 + k_1 a + \dots \in K(a)}$ e $\underbrace{K(a) \subseteq K[a]}_{\text{per proprietà di } K(a)}$, allora $K(a) = K[a]$.

OSS. $\mathbb{K}[\lambda_1] \cong \mathbb{K}[\lambda_2] \cong \dots \quad \forall \lambda_i$ radice di $g(x)$

Def. Se $\operatorname{Ker} \varphi \neq (0)$, si dice che α e' **ALGEBRICO** su K.

Teorema dati $K \subseteq L$ campi. Sia $f(x)$ irriducibile in $K[x]$ che ha due radici distinte α, β in L. Allora esiste un isomorfismo $\varphi: K[\alpha] \to K[\beta]$, ossia $K[\alpha] \cong K[\beta]$.

OSS $F \subset K$, $\alpha \in K$, allora $F(\alpha)$ spazio vettoriale su F.

$\dim F(\alpha) = +\infty$ se $1, \alpha, \alpha^2, \dots$ sono tutti lin. ind. su F.
Altrimenti esistono $f_0, f_1, \dots, f_n \in F \mid f_0 + f_1 \alpha + \dots + f_n \alpha^n = 0$ con almeno un $f_i \neq 0$. WLOG $f_n \neq 0$, $n \geq 1$. Allora $g(x) := f_0 + f_1 x + \dots + f_n x^n$ è t.c. $g(\alpha) = 0 \Rightarrow$ α è algebrico su F. Viceversa, nel caso infinito, α è trascendente.

$\varphi_\alpha : F[x] \longrightarrow K$, $f(x) \longmapsto f(\alpha)$

Se α è algebrico, $\exists\, g(x) \in F[x] \mid \varphi_\alpha(g(x)) = 0 \Rightarrow$
$\Rightarrow g(x) \in \operatorname{Ker} \varphi_\alpha \Rightarrow \operatorname{Ker} \varphi_\alpha \neq \{0\} \Rightarrow \exists\, p(x) \neq 0 \mid \operatorname{Ker} \varphi_\alpha =$
$= (p(x))$.

$\underbrace{F[x]/(p(x))}_{\substack{\text{campo} \\ \text{perché } p(x) \text{ è} \\ \text{irriducibile}}} \cong \operatorname{Im} \varphi_\alpha$. Quindi $\operatorname{Im} \varphi_\alpha$ è un sottocampo di K.
In particolare $\operatorname{Im} \varphi_\alpha \cong F[\alpha] \subset F(\alpha)$. Tuttavia $F(\alpha) \subset F[\alpha]$, quindi $F[\alpha] = F(\alpha)$.

In particolare $\overbrace{F[x]/(p(x))}^{\cong F(\alpha)}$ è uno spazio di dimensione $\deg p(x) + 1$.
Quindi $\dim K(\alpha) < +\infty$.

Quindi F, K campi, $F \subset K$, $\alpha \in K$, α e' algebrico $\iff$

$\iff$ dim $F(\alpha) < +\infty$.

Def. F, K campi, $F \subset K$, $[K : F] := \dim_F K$.

Proposizione F, K, L campi, $F \subset K \subset L$. Supponiamo $[L:K] = m \in \mathbb{N}$,

$[K:F] = n \in \mathbb{N}$, allora $[L:F] = mn$.

Sia $W = \{\underline{w_1}, \dots, \underline{w_n}\}$ una base di K su F. Sia $V = \{\underline{v_1}, \dots, \underline{v_m}\}$ una base di L su K. Si consideri $VW = \{\underline{v_i}\,\underline{w_j} \mid 1 \leq i \leq m \;\; 1 \leq j \leq n\}$.

$\forall\, \underline{a} \in L_K$, $\underline{a} = \alpha_1 \underline{v_1} + \dots + \alpha_m \underline{v_m}$, con $\alpha_i \in K_F \Rightarrow \alpha_i = \beta_1 \underline{w_1} + \dots + \beta_m \underline{w_n}$.

Quindi $\underline{a} = \gamma_1 \underline{v_1}\,\underline{w_1} + \dots + \gamma_{mn} \underline{v_m}\,\underline{w_n}$, $\gamma_i \in F$. Allora VW genera.

Si consideri $\gamma_1 \underline{v_1}\,\underline{w_1} + \dots + \gamma_{mn} \underline{v_m}\,\underline{w_n} = \underline{0}$. $\overbrace{\gamma_i}^{\in F} \overbrace{\underline{w_j}}^{\in K_F} \in K_F \Rightarrow$

$\Rightarrow \alpha_j = \gamma_i \underline{w_j} \in K$. $\alpha_1 \underline{v_1} + \dots + \alpha_m \underline{v_m} = \underline{0} \Rightarrow \alpha_1 = \dots = \alpha_m = 0$.

$\gamma_i \underline{w_j} = \underline{0} \Rightarrow \gamma_i = 0$. Quindi VW e' lin. ind.

Pertanto VW è base $\Rightarrow [L:F] = mn$.

$\square$

Prop. F, K campi, $F \subset K$. $\alpha, \beta \in K$ algebrici su F. Allora $\alpha \pm \beta$, $\alpha\beta$ e α/β (i.e. $\alpha\beta^{-1}$, $\beta \neq 0$) sono algebrici su F.

$[F(\alpha) : F] = m \in \mathbb{N}$ $\quad$ $[F(\beta) : F] = k \in \mathbb{N}$

$[F(\alpha)(\beta) : F(\alpha)] \leq k \}$ poiché $\deg \underbrace{p(x)}_{\text{pol. min.}} \leq n$

$$[F(\alpha)(\beta) : F] = [F(\alpha)(\beta) : F(\alpha)]\,[F(\alpha) : F] \leq km < +\infty.$$

Poiché $F(\alpha \pm \beta)$, $F(\alpha\beta)$, $F(\alpha\beta^{-1}) \subset F(\alpha)(\beta)$ sono spazi vettoriali e sottospazi di $F(\alpha)(\beta)$, hanno dimensione finita su F.

Quindi $\alpha \pm \beta$, $\alpha\beta$ e $\alpha\beta^{-1}$ sono algebrici su F. $\boxtimes$

Corollario F, K campi, $F \subset K$. Allora gli elementi algebrici di K su F formano un sottocampo di K che contiene F.

es. $\mathbb{Q} \subseteq \mathbb{C}$ $\quad$ Sia $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \text{ algebrici su } \mathbb{Q}\}$

$\mathbb{Q} \subsetneq \overline{\mathbb{Q}} \subsetneq \mathbb{C}$

Def. Siano F, K campi, $F \subset K$. L'estensione $F \subseteq K$ è **ALGEBRICA** se ogni elemento $\alpha \in K$ è algebrico su F.

Prop. Siano $F \subseteq K \subseteq L$ campi, se L è est. alg. per K e K lo è per F, L lo è per F.

Sia $\alpha \in L$, allora $\exists\ p(x) \in K[x] \mid p(\alpha) = 0$. Sia $p(x) = a_0 + a_1 x + \dots + a_n x^n$. Sicuramente $[F(a_0) : F] < \infty$, perché K è algebrico su F. Allora anche $[F(a_0, a_1) : F] < \infty$, $\dots$, $[F(a_0, \dots, a_n) : F] < \infty$.

Inoltre $[F(\alpha, a_0, \dots, a_n) : F(a_0, \dots, a_n)] < \infty$ perché α è radice di $p(x)$. Allora $[F(\alpha, \dots, a_n) : F] =$
$= [F(\alpha, \dots, a_n) : F(a_1, \dots, a_n)]\,[F(a_1, \dots, a_n) : F(a_1, \dots, a_{n-1})] \cdot \dots \cdot [F(a_1) : F] < \infty$.

Poiché $F(\alpha) \subset F(\alpha, \dots, a_n)$, si ha che $[F(\alpha) : F] < \infty$. $\square$