1 Estensioni di Campi

Siano K, F campi. F si dice **estensione** di K se $F \supseteq K$.

Definizione 1.1.

Un elemento $\alpha \in F$ si dice **algebrico** su K se $\exists f(x) \in K[x] \setminus \{0\}$ tale che $f(\alpha) = 0$.
$\alpha \in F$ si dice **trascendente** su K se non è algebrico.

Esempio 1.2.

- $\sqrt{2}$ è algebrico su $\mathbb{Q}$ perché è radice di $x^2 - 2$.
- Si può dimostrare che π è trascendente su $\mathbb{Q}$.

Sia $F \supseteq K$ e sia $\alpha \in F$. Poniamo

$$K[\alpha] := \{f(\alpha) \mid f(x) \in K[x]\}.$$

Proposizione 1.3.

$\alpha \in F$ è trascendente su K se e solo se l'omomorfismo $\varphi_\alpha : K[x] \longrightarrow K[\alpha]$ definito da $\varphi(f(x)) = f(\alpha)$ è iniettivo.

Dimostrazione.

È banale verificare che φ_α è un omomorfismo di anelli. Ne segue che φ_α è iniettivo $\iff$ $\operatorname{Ker} \varphi_\alpha = \{f(x) \in K[x] \mid f(\alpha) = 0\} = \{0\}$ $\iff$ l'unico polinomio di $K[\alpha]$ che si annulla in α è quello identicamente nullo. ▲

Sia $\alpha \in F$ algebrico su K . Per la proposizione precedente
l'omomorfismo φ_α non è iniettivo, cioè

$$\operatorname{Ker} \varphi_\alpha = \{f(x) \in K[x] \mid f(\alpha) = 0\} \neq \{0\}$$

Sia $\mu_\alpha(x)$ un polinomio monico di grado minimo in $\operatorname{Ker} \varphi_\alpha$. Allora vale:

Proposizione 1.4.

1. $\mu_\alpha(x)$ è irriducibile in $K[x]$;
2. $\operatorname{Ker} \varphi_\alpha = (\mu_\alpha(x))$;
3. $\mu_\alpha(x)$ è l'unico polinomio monico irriducibile di $K[x]$ che si annulla in α .

Dimostrazione.

1. Sia $\mu_\alpha(x) = a(x)b(x)$ in $K[x]$. Valutando in α si ha: $0 = \mu_\alpha(\alpha) = a(\alpha)b(\alpha)$. Poiché tutti i termini dell'equazione precedente appartengono al campo F , per la legge d'annullamento del prodotto si ha $a(\alpha) = 0$ oppure $b(\alpha) = 0$.

   Poiché $\mu_\alpha(x)$ è di grado minimo tra i polinomi che si annullano in α si ha che $\deg a(x) = \deg \mu_\alpha(x)$ e quindi $b(x) \in K^*$ oppure $\deg b(x) = \deg \mu_\alpha(x)$ e quindi $a(x) \in K^*$, cioè $\mu_\alpha(x)$ è irriducibile.

2. Chiaramente $(\mu_\alpha(x)) = \mu_\alpha(x)K[x] \subset \operatorname{Ker} \varphi_\alpha$ perché tutti i multipli di $\mu_\alpha(x)$ si annullano in α .

   Viceversa, sia $p(x) \in \operatorname{Ker} \varphi_\alpha$ e sia $p(x) = \mu_\alpha(x)q(x) + r(x)$ con $r(x) = 0$ oppure $\deg r(x) < \deg \mu_\alpha(x)$. Valutando in α si ha $0 = p(\alpha) = q(\alpha)\mu_\alpha(\alpha) + r(\alpha) = r(\alpha)$. Per la minimalità del grado di $\mu_\alpha(x)$ necessariamente

   $r(x) = 0$, cioè $\mu_\alpha(x) \mid p(x)$, ovvero $p(x) \in (\mu_\alpha(x))$.

3. Ogni polinomio di $K[x]$ che si annulla in α appartiene a $(\mu_\alpha(x))$, cioè è multiplo di $\mu_\alpha(x)$, e nessun polinomio monico e irriducibile è un multiplo non banale di $\mu_\alpha(x)$.

▲

Definizione 1.5.

L'unico polinomio monico e irriducibile di $K[x]$ che si annulla in α si dice **polinomio minimo** di α su K .

Proposizione 1.6.

Sia $\alpha \in F$ algebrico su K e sia $\mu_\alpha(x)$ il suo polinomio minimo. Allora

$$K[\alpha] \cong K[x]/(\mu_\alpha(x)).$$

Dimostrazione.

Sia $\varphi_\alpha : K[x] \longrightarrow K[\alpha]$ l'omomorfismo di sostituzione. Poiché α è algebrico si ha che $\operatorname{Ker} \varphi_\alpha = (\mu_\alpha(x))$. È chiaro che φ_α è surgettivo, quindi dal I Teorema di omomorfismo si ha un isomomorfismo di gruppi. Si verifica facilmente che è anche un isomorfismo di anelli, cioè che $\varphi_\alpha(f(x)g(x)) = \varphi_\alpha(f(x))\varphi_\alpha(g(x))$. ▲

Corollario 1.7.

Sia $\alpha \in F$ algebrico su K . Allora $K[\alpha]$ è un campo.

Dimostrazione.

Il polinomio $\mu_\alpha(x)$ è irriducibile, quindi per il Corollario **??** $K[x]/(\mu_\alpha(x))$ è un campo. Per la proposizione precedente $K[x]/(\mu_\alpha(x)) \cong K[\alpha]$ come anello e quindi $K[\alpha]$ è un campo. ▲

Osservazione 1.8.

Sia $\alpha \in F$, poniamo

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[x] \; g(\alpha) \neq 0 \right\}$$

Il corollario precedente dice che se α è algebrico allora $K[\alpha] = K(\alpha)$.

Se F è un'estensione di campi, in particolare F è un $K-$ spazio vettoriale.

Definizione 1.9.

Si dice **grado** dell'estensione F/K la dimensione di F come $K-$ spazio vettoriale, in simboli

$$[F : K] := \dim_K F.$$

Un'estensione F/K si dice **finita** se $[F : K] < +\infty$.

Teorema 1.10.

F/K estensione e sia $\alpha \in F$, allora

$$[K[\alpha] : K] = \begin{cases} +\infty & \text{se } \alpha \text{ è trascendente} \\ \deg \mu_\alpha & \text{se } \alpha \text{ è alg. su } K \text{ e} \\ & \mu_\alpha \text{ è il suo pol. minimo} \end{cases}$$

Dimostrazione.

Se α è trascendente, dalla Proposizione 1.3 si ha che $K[\alpha] \cong K[x]$ e quindi ha dimensione $+\infty$ su K .

Viceversa se α è algebrico allora $K[\alpha] \cong K[x]/(\mu_\alpha(x))$.

Il Teorema **??** assicura che $\dim_K K[x]/(\mu_\alpha(x)) = \deg \mu_\alpha(x) = n$ e che $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ è una $K-$ base.

Da questo segue che $\dim_K K[\alpha] = n$ e che $1, \alpha, \ldots, \alpha^{n-1}$ è una $K-$ base di $K[\alpha]$. ▲

Teorema 1.11.

Se F/K è un'estensione finita, allora ogni $\alpha \in F$ è algebrico su K .

Dimostrazione.

Sia $[F : K] = n$, allora $\{1, \alpha, \ldots, \alpha^n\}$ sono linearmente dipendenti su K perché si tratta di $n + 1$ elementi in uno spazio vettoriale di dimensione n . Quindi $\exists\ a_0, \ldots, a_n \in K$ non tutti nulli tali che $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Allora

$$f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$$

è un polinomio che si annulla in $\alpha \Rightarrow \alpha$ è algebrico su K . ▲

Teorema 1.12.

Siano $K \subset F \subset L$ campi, e siano $n = [L : F]$ e $m = [F : K]$. Allora $[L : K] = nm$.

Dimostrazione.

Sia $\{w_i\}_{i=1,\ldots,n}$ una $F-$ base di L e sia $\{v_j\}_{j=1,\ldots,m}$ una $K-$ base di F . Mostriamo che

$$\{w_i v_j\}_{i=1,\ldots,n, j=1,\ldots,m}$$

è una $K-$ base di L .

Per prima cosa vediamo che generano L su K : infatti, $\forall \alpha \in L$ si ha $\alpha = \sum_{i=1}^{n} \lambda_i w_i$ con $\lambda_i \in F$; d'altra parte $\forall i, \quad \lambda_i = \sum_{j=1}^{m} a_{ij} v_j$, con $a_{ij} \in K$, quindi sostituendo

$$\alpha = \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} v_j) w_i = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} v_j w_i.$$

Mostriamo ora che sono linearmente indipendenti: infatti, sia

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} v_j w_i = 0$$

con $a_{ij} \in K$. Allora $\sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} v_j) w_i = 0$, e essendo i w_i linearmente indipendenti su F si ottiene $\sum_{j=1}^{m} a_{ij} v_j = 0 \; \forall i$. Usando ora l'indipendenza dei v_j su K si ottiene $a_{ij} = 0 \quad \forall i \, \forall j$. ▲

Definizione 1.13.

Sia L/K un'estensione di campi e siano $\alpha_1, \dots \alpha_r \in L$ algebrici su K . Poniamo

$$K[\alpha_1, \dots \alpha_r] := \{p(\alpha_1, \dots \alpha_r) \,|\, p(x_1, \dots, x_r) \in K[x_1, \dots, x_r]\}.$$

Teorema 1.14.

Con la notazione sopra introdotta si ha che $K[\alpha_1, \dots \alpha_r]$ è un campo ed è l'intersezione dei sottocampi di L che contengono sia K che $\alpha_1, \dots, \alpha_r$.

Dimostrazione.

Mostriamo per induzione su r che $K[\alpha_1, \dots \alpha_r]$ è un campo. Il caso $r = 1$ è gia noto. Supponiamo allora di sapere che $F := K[\alpha_1, \dots \alpha_{r-1}]$ è un campo. Ne segue che $K[\alpha_1, \dots \alpha_r] = F[\alpha_r]$ è a sua volta un campo perchè estensione algebrica semplice (cioè generata da un solo elemento) del campo F .

Vediamo ora che $K[\alpha_1, \dots \alpha_r]$ coincide con è l'intersezione M dei sottocampi di L che contengono sia K che $\alpha_1, \dots, \alpha_r$. Per prima cosa il campo $K[\alpha_1, \dots \alpha_r]$ fa parte dei campi che interseco quindi $M \subseteq K[\alpha_1, \dots \alpha_r]$, inoltre M è un campo e contenendo $K, \alpha_1, \dots \alpha_r$ nesessariamente deve contenere $K[\alpha_1, \dots \alpha_r]$, quindi si ha l'uguaglianza.

Chiusura algebrica e campo di spezzamento

Definizione 1.15.

Un campo L si dice **algebricamente chiuso** se ogni polinomio non costante di $L[x]$ ha almeno una radice in L .

Osservazione 1.16.

L è algebricamente chiuso se e solo se gli unici polinomi irriducibili di $L[x]$ sono quelli di grado 1 .

Definizione 1.17.

Sia $\overline{K}/K$ un'estensione di campi. $\overline{K}$ è una **chiusura algebrica** di K se

- $\overline{K}$ è algebricamente chiuso.
- $\forall \alpha \in \overline{K}, \quad \alpha$ è algebrico su K .

Esempio 1.18.

- $\mathbb{C}$ è algebricamente chiuso ma non è algebrico su $\mathbb{Q}$, quindi non ne è la chiusura algebrica.
- $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$.

Teorema 1.19. (Esistenza e unicità della chiusura algebrica)

Sia K un campo. Esiste una chiusura algebrica di K . Inoltre due qualsiasi chiusure algebriche di K sono isomorfe (come anelli).

Definizione 1.20.

Sia K un campo e sia $\overline{K}$ una sua chiusura algebrica. Sia $f(x) \in K[x]$ e siano $\{\alpha_1, \dots, \alpha_n\}$ le radici di $f(x)$ in $\overline{K}[x]$. Si dice **campo di spezzamento** di $f(x)$ su K il campo $K[\alpha_1, \dots, \alpha_n]$.

Esempio 1.21.

- Sia $f(x) = (x^2 - 2)(x^2 - 3)$. Il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
- Il campo di spezzamento di $x^3 - 2$ su $\mathbb{Q}$ è $\mathbb{Q}[\sqrt[3]{2}, \xi_3]$.
  Infatti $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\xi_3)(x - \sqrt[3]{2}\xi_3^2)$, dove $\xi_3 \neq 1$ e $\xi_3^3 = 1$.
  Il suo campo di spezzamento è quindi $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2]$ ed è immediato verificare che coincide con $\mathbb{Q}[\sqrt[3]{2}, \xi_3]$.

Caratteristica di un campo

Sia F un campo e sia $\varphi_F : \mathbb{Z} \longrightarrow F$ l'omomorfismo (di anelli) definito da

$$\varphi_F(n) = \overbrace{1_F + \cdots + 1_F}^{n volte} .$$

Dal I Teorema di omomorfismo si ha che esiste un omomorfismo iniettivo

$$\tilde{\varphi_F} : \mathbb{Z}/\operatorname{Ker}\varphi_F \longrightarrow F$$

ed è banale verificare che è un omomorfismo di anelli.

Poiché $\operatorname{Ker}\varphi_F$ è un sottogruppo di $\mathbb{Z}$, si ha che $\operatorname{Ker}\varphi_F = n\mathbb{Z}$ con $n \in \mathbb{N}$.

Osserviamo che non può essere $n = 1$ in quanto in F si ha $1_F \neq 0_F$, e che n non può essere un numero composto, perché se fosse $n = ab$ con $a, b < n$ avremmo che $\overline{a}\overline{b} = \overline{0}$ con $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, da cui $\widetilde{\varphi_F}(\overline{a})\widetilde{\varphi_F}(\overline{b}) = 0$ e questo è assurdo poiché F è un campo.

Ne segue che

$$\operatorname{Ker} \varphi_F = \begin{array}{l} \nearrow 0 \\ \searrow p\mathbb{Z} \text{con } p \text{ primo} \end{array}$$

Se $\operatorname{Ker} \varphi_F = 0 \Rightarrow \mathbb{Z} \subset F$ e poiché F è un campo $\mathbb{Q} \subset F$, in particolare il campo contiene infiniti elementi.

Se $\operatorname{Ker} \varphi_F = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \subset F$.

Definizione 1.22.

Si dice che il campo F ha **caratteristica** 0 (in simboli $\operatorname{char} F = 0$) se $\operatorname{Ker} \varphi_F = 0$. Si dice che la **caratteristica** di F è un **primo** p se $\operatorname{Ker} \varphi_F = p\mathbb{Z}$.