Corso:Algebra IV I1/Richiami sui campi/Ripasso di teoria dei campi

1 Estensioni di campi

Definizione 1.1

Sia M un campo, e K un sottoanello di M , che è a sua volta un campo. Diciamo che $M \supseteq K$ è un'*estensione di campi* (si scrive anche M/K). Il campo M può essere visto come spazio vettoriale su K . La dimensione di M come spazio vettoriale su K si dice *grado dell'estensione*, e si indica con $|M : K|$.

Teorema 1.1 (teorema della torre)

Supponiamo di avere K, L, M campi con $K \subseteq L \subseteq M$, allora $|M : K|$ è finito se e solo se sono finiti $|M : L|$ e $|L : K|$. In tal caso: $|M : K| = |M : L| * |L : K|$.

Dimostrazione

$1 \longrightarrow 2$: Supponiamo che $|M : K|$ sia finito, allora siccome $L \subseteq M$, anche $|L : K|$ è finito (infatti L e' un sottospazio di M). Sia inoltre $\{\gamma_1, \ldots, \gamma_t\}$ una base per M su K .

Allora ogni $\alpha \in M$ si può scrivere come

$$\sum_i k_i \gamma_i$$

per certi $k_i \in K \subseteq L$, quindi $\{\gamma_i\}_{i=1}^t$ è un insieme finito di generatori per M su L , e anche $|M : L|$ è finito.

$2 \longrightarrow 1$: Viceversa, siano $n = |M : L| < \infty$ e $m = |L : K| < \infty$, e siano $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_m\}$ basi rispettivamente di M su L e di L su K . **Affermo che $\mathcal{B} = \{\alpha_i \beta_j | i = 1, \ldots, n,\ j = 1 \ldots, m\}$ è una base per M su K** , infatti:

1. **$\mathcal{B}$ genera M** . Prendo $\alpha \in M$, allora siccome gli $\{\alpha_i\}_{i=1}^n$ sono una base per M su L posso scrivere
$$\alpha = \sum_i l_i \alpha_i$$
per certi $l_i \in L$. Inoltre i $\{\beta_i\}_{i=1}^m$ sono una base di L su K , quindi per $i = 1, \ldots, n$ posso scrivere
$$l_i = \sum_j k_{ij} \beta_j$$

e sostituendo nell'espressione di α :

$$\alpha = \sum_i \sum_j k_{ij}\beta_j\alpha_i,$$

cioè $\mathcal{B}$ genera M .

2. **Gli elementi di $\mathcal{B}$ sono linearmente indipendenti**, infatti supponiamo per assurdo che non lo siano, allora per certi $\bar{k}_{ij} \in K$ si ha

$$\sum_{i,j} \bar{k}_{ij}\alpha_i\beta_j = 0$$

$$\longrightarrow \sum_i (\sum_j \bar{k}_{ij}\beta_j)\alpha_i = 0$$

Posto $\bar{l}_i = \sum_j \bar{k}_{ij}\beta_j$ la condizione si riscrive come

$$\sum_i \bar{l}_i\alpha_i = 0$$

e siccome gli $\{\alpha_i\}_{i=1}^m$ sono una base per M su L , si deve avere $\bar{l}_i = 0,\ \forall i = 1, \ldots, n$, e considerando l'espressione degli $\bar{l}_i$, si ha

$$\sum_j \bar{k}_{ij}\beta_j = 0$$

Siccome i $\{\beta_i\}_{i=1}^m$ sono una base per L su K , l'unica possibilità per cui la condizione sia verificata è che $\bar{k}_{ij} = 0,\ \forall i, \forall j$, cioè segue l'indipendenza lineare degli elementi di $\mathcal{B}$.

2 Estensioni semplici

Sia $E \supseteq F$ un'estensione di campi, e sia S un sottoinsieme di E . Allora indichiamo con $F[S]$ il minimo sottoanello di E contenente S e F ,

cioè $F[S] := \bigcap R$ al variare di R sottoanello di E tale che $F, S \subset R$ ovvero

$$F[S] := \bigcap_{R\ sottoanello\ di\ E\ con\ F,S\subseteq R} R.$$

Indichiamo invece con $F(S)$ il minimo sottocampo di E contenente S, F , cioè $F(S) := \bigcap K$, al variare di K sottocampo di E tale che $F, S \subset K$,

ovvero

$$F(S) := \bigcap_{K\ sottocampo\ di\ E,\ con\ F,S\subseteq K} K.$$

In particolare, quando $S = \{\alpha\}$, il minimo sottoanello e sottocampo si indicano rispettivamente con $F[\alpha], F(\alpha)$.

Più in generale, dato $S = \{\alpha_1, \ldots, \alpha_n\}$, $\alpha_i \in E$, posso scrivere $F[\alpha_1, \ldots, \alpha_n]$ per indicare $F[S]$ e $F(\alpha_1, \ldots, \alpha_n)$ per indicare $F(S)$, eliminando le parentesi graffe che racchiudono il contenuto degli insiemi.

3 Elementi algebrici e trascendenti

Sia $\alpha \in E$, e' facile convincersi che

$$F[\alpha] = \{f(\alpha) : f(x) \in F[x]\}$$
$$F(\alpha) = \{f(\alpha)g(\alpha)^{-1} : f(x), g(x) \in F[x],\ g(\alpha) \neq 0\}$$

Per caratterizzare ulteriormente l'anello $F[\alpha]$ e il campo $F(\alpha)$ devo distinguere due casi:

Definizione 1.2

1. α si dice *algebrico* su F se esiste un polinomio non nullo in $F[x]$ che ammette α come radice.
2. α si dice *trascendente* su F altrimenti, ovvero se l'unico polinomio di $F[x]$ che si annulla in α è il polinomio nullo.

Definizione 1.3

Indico con ϕ_α l'*omomorfismo di valutazione* : $F[x] \to E$ tale che $g(x) \mapsto g(\alpha)$, così l'immagine di ϕ_α è $F[\alpha]$ (x una indeterminata su F).

CASO 1: se α è trascendente su F , $\ker \phi_\alpha = \{0\}$, allora l'omomorfismo di valutazione è iniettivo e $F[\alpha] \cong F[x]$. Inoltre ϕ_α si solleva (in modo unico) a un omomorfismo iniettivo, $\bar{\phi}_\alpha : F(x) \to E$, tale che $\frac{f(x)}{g(x)} \mapsto f(\alpha)g(\alpha)^{-1}$, la cui immagine coincide con $F(\alpha)$. Abbiamo quindi $F(\alpha) \cong F(x)$ dove $F(x)$ è il campo delle funzioni razionali su F .

CASO 2: se α è algebrico su F , esiste in $F[x]$ un polinomio monico, di grado minimo tra i polinomi non nulli in $F[x]$ che ammettono α come radice. Dalla definizione segue subito che è unico e irriducibile in $F[x]$, e viene chiamato il *polinomio minimo di* α e indicato con $m(x)$. Osservo che $\ker \phi_\alpha$ coincide con l'ideale generato da $m(x)$, e quindi $F[\alpha] \cong \frac{F[x]}{(m(x))}$. Il polinomio $m(x)$ è irriducibile e quindi $(m(x))$ è massimale in $F[x]$, allora $\frac{F[x]}{(m(x))}$ è un campo, e quindi deduco che $F[\alpha] = F(\alpha)$.

4 Fonti per testo e immagini; autori; licenze

4.1 Testo

- **Corso:Algebra IV I1/Richiami sui campi/Ripasso di teoria dei campi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Richiami_sui_campi/Ripasso_di_teoria_dei_campi?oldid=48355 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

4.2 Immagini

4.3 Licenza dell'opera