1 Teoria dei campi

1.1 Estensione di campi

Introduciamo ora un concetto fondamentale nella teoria algebrica dei numeri e nello studio delle radici polinomiali, che costituirà la base della teoria di Galois.

Definizione

Una coppia di campi $\mathbb{K}$ e $\mathbb{L}$ con $\mathbb{K} \subseteq \mathbb{L}$ si dice estensione di campi e si denota con $\mathbb{L}/\mathbb{K}$.

Resta inteso che $\mathbb{K}$ ha le stesse operazioni binarie di $\mathbb{L}$, cioè che $\mathbb{K}$ è un sottocampo di $\mathbb{L}$. Inoltre, in questo caso la notazione $\mathbb{L}/\mathbb{K}$ non ha nulla a che vedere con il quoziente di campi.

Esempio. Se consideriamo $\mathbb{R}$ e $\mathbb{C}$ con le usuali operazioni di somma e prodotto, $\mathbb{R}$ è un sottocampo di $\mathbb{C}$, dunque $\mathbb{C}/\mathbb{R}$ è un'estensione di campi. $\square$

Se $\mathbb{L}/\mathbb{K}$ è un'estensione di campi, sia $\cdot_{|_{\mathbb{K}\times\mathbb{L}}}$ la restrizione a $\mathbb{K}$ della prima componente del prodotto $\cdot : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ del campo $\mathbb{L}$. Considerando tale moltiplicazione per gli elementi di $\mathbb{K}$ e la usuale somma di $\mathbb{L}$, si ha che $(\mathbb{L}, +, \cdot)$ ha la struttura di uno spazio vettoriale su $\mathbb{K}$. Infatti, possiamo pensare gli elementi di $\mathbb{K}$ come scalari e quelli di $\mathbb{L}$ come vettori.

Definizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Definiamo grado dell'estensione $\mathbb{L}/\mathbb{K}$ la dimensione[1] $\dim_{\mathbb{K}}(\mathbb{L}) \in \mathbb{N} \cup \{\infty\}$ dello spazio vettoriale $\mathbb{L}$ sul campo $\mathbb{K}$, e si denota con $|\mathbb{L} : \mathbb{K}|$.

La scelta del termine "grado", che richiama il concetto di grado di un polinomio, sarà più chiara in seguito, quando approfondiremo i legami tra estensione di campi e polinomi.

Esempio. Se consideriamo $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con le usuali operazioni di somma e prodotto, si ha che $|\mathbb{C} : \mathbb{R}| = 2$ perché $\mathcal{B} = \{1, i\}$ è una base per $\mathbb{C}$, e $|\mathbb{R} : \mathbb{Q}| = \infty$ perché $\mathbb{R}$ non è numerabile, quindi non ammette una base finita su $\mathbb{Q}$, che invece è numerabile. $\square$

Definizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Un elemento $a \in \mathbb{L}$ si dice:
(i) algebrico su $\mathbb{K}$ se esiste un polinomio non nullo $f(x) \in \mathbb{K}[x]$ tale che $f(a) = 0$;
(ii) trascendente su $\mathbb{K}$ se non è algebrico.

Esempio. Se consideriamo $\mathbb{R}/\mathbb{Q}$, l'elemento $a = \sqrt{2}$ è algebrico perché $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ e $f(a) = 0$, mentre e e π sono entrambi elementi trascendenti.[2] $\square$

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$. Detta $\phi_a : \mathbb{K}[x] \to \mathbb{L}$ la valutazione in a, essendo ϕ_a un omomorfismo si ha che $\ker(\phi_a) \lhd \mathbb{K}[x]$. SISTEMARE TUTTO.

[1] Ricordiamo che la dimensione di uno spazio vettoriale è la cardinalità di una sua base, cioè un insieme di vettori linearmente indipendenti che generano tutto lo spazio.

[2] La dimostrazione è tutt'altro che elementare e prende il nome di *Teorema di Lindemann-Weierstrass*.

Definizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ un elemento algebrico su $\mathbb{K}$. Il generatore monico di $\ker(\phi_a)$ è detto polinomio minimo di a e si denota con $\min_{a,\mathbb{K}}(x) \in \mathbb{K}[x]$.

Proposizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ algebrico su $\mathbb{K}$. Sia $f(x) \in \mathbb{K}[x]$ tale che:
(i) $f(a) = 0$;
(ii) $f(x)$ è monico;
(iii) $f(x)$ è irrudicibile.
Allora, $f(x)$ è il polinomio minimo di a, cioè $f(x) = \min_{a,\mathbb{K}}(x)$.

Dimostrazione. Per (i) si ha che $f(x) \in \ker(\phi_a)$, dunque esiste un polinomio $q(x) \in \mathbb{K}[x]$ tale che $f(x) = q(x) \cdot \min_{a,\mathbb{K}}(x)$. Essendo $f(x)$ irriducibile per (iii), almeno uno fra $q(x)$ e $\min_{a,\mathbb{K}}(x)$ è invertibile; tuttavia, $\min_{a,\mathbb{K}}(x) \notin \mathbb{K}[x]^\times$ e quindi CONCLUDERE ■

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $S \subseteq \mathbb{L}$ un sottoinsieme.

Proposizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ algebrico su $\mathbb{K}$. Allora, $\mathbb{K}(a) = \mathbb{K}[a]$.

Dimostrazione. Sia $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{K}[x]$. Poiché $c_i \in \mathbb{K} \subseteq \mathbb{K}(a)$ e $a \in \mathbb{K}(a) \Rightarrow a^k \in \mathbb{K}(a)$ essendo $\mathbb{K}(a)$ chiuso rispetto al prodotto, $f(a) \in \mathbb{K}(a)$. Dunque, per l'arbitrarietà di $f(x)$ concludiamo che $\mathrm{Im}(\phi_a) = \mathbb{K}[a] \subseteq \mathbb{K}(a)$. FINIRE, ESERCIZIO PER CASA XD COME SEI SIMPATICO ■

Manca anche la lezione del 30/10/2019, al momento è solo cartacea, e contiene cose davvero molto importanti tipo la formula del grado.