Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 05-05-2020

Testi di riferimento

Per la parte di teoria dei campi potranno essere utili in particolare i seguenti testi.

- D.J.H. Garling, *A Course in Galois Theory*
  Soprattutto i capitoli 4 e 7-12.
- J.S. Milne, *Fields and Galois Theory*, disponibile all'indirizzo
  `http://www.jmilne.org/math/CourseNotes/ft.html`
  Soprattutto i capitoli 1-3.
- I.N. Herstein, *Algebra*
  Capitolo 5.
- Dispense di R. Schoof e B. van Geemen, disponibili all'indirizzo
  `http://www-dimat.unipv.it/canonaco/notealgebra.pdf`
  Capitolo 14.

Caratteristica di un anello

Definizione

La caratteristica di un anello A è $\mathrm{char}(A) \in \mathbb{N}$ tale che, se $f : \mathbb{Z} \to A$ indica l'unico omomorfismo di anelli, $\mathrm{char}(A)\mathbb{Z} = \ker(f)$.

Esempio

$\mathrm{char}(\mathbb{Z}) = 0$ e $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n \ \forall\, n > 0$.
$\mathrm{char}(A) = \mathrm{char}(B)$ se $\exists\, A \to B$ omomorfismo iniettivo di anelli.

Osservazione

$\mathrm{im}(f) \cong \mathbb{Z}/\mathrm{char}(A)\mathbb{Z}$ per il primo teorema di isomorfismo.

- Poiché $\mathrm{im}(f) = \{n_A \,:\, n \in \mathbb{Z}\} = \langle 1_A \rangle$,

$$\mathrm{char}(A) = \begin{cases} \mathrm{ord}(1_A) & \text{se } \mathrm{ord}(1_A) < \infty \\ 0 & \text{se } \mathrm{ord}(1_A) = \infty. \end{cases}$$

- A dominio (in particolare campo) $\implies$ $\mathrm{im}(f)$ dominio $\implies$ $\mathrm{char}(A)\mathbb{Z}$ ideale primo $\implies$ $\mathrm{char}(A)$ è 0 o un numero primo.

Campo dei quozienti di un dominio

Indichiamo con $Q(A)$ il campo dei quozienti (o delle frazioni) di un dominio A. Vediamo A come sottoanello di $Q(A)$ identificando $a \in A$ con $a/1 \in Q(A)$.

Lemma

$f : A \to K$ omomorfismo iniettivo di anelli con A dominio e K campo $\implies \exists!\, \tilde{f} : Q(A) \to K$ omomorfismo di anelli tale che $\tilde{f}|_A = f$; inoltre $\tilde{f}$ è iniettivo.

Corollario

K campo tale che $\mathrm{char}(K) = 0 \implies \exists!\, \mathbb{Q} \to K$ omomorfismo (iniettivo) di anelli.

Dimostrazione.

$\exists!\, f : \mathbb{Z} \to K$ omomorfismo di anelli, e f è iniettivo perché $\mathrm{char}(K) = 0$. Per il Lemma $\exists!\, \tilde{f} : Q(\mathbb{Z}) = \mathbb{Q} \to K$ omomorfismo (iniettivo) di anelli (tale che $\tilde{f}|_{\mathbb{Z}} = f$). □

Dimostrazione del Lemma

- unicità: $\tilde{f}(a/b) = \tilde{f}(ab^{-1}) = \tilde{f}(a)\tilde{f}(b)^{-1} = f(a)f(b)^{-1}$ $\forall\, a \in A, \forall\, b \in A \setminus \{0\}$.
- $\tilde{f}(a/b) := f(a)f(b)^{-1}$ $\forall\, a \in A, \forall\, b \in A \setminus \{0\}$ è ben definito: $f(b) \in K \setminus \{0\} = K^*$ perché f iniettivo; $a/b = a'/b'$ (con $a', b' \in A$ e $b' \neq 0$) $\implies$ $ab' = a'b$ $\implies$ $f(ab') = f(a'b)$ $\implies$ $f(a)f(b') = f(a')f(b)$ $\implies$ $f(a)f(b)^{-1} = f(a')f(b')^{-1}$.
- $\tilde{f}$ è un omomorfismo di anelli: $\forall\, a, c \in A$ e $\forall\, b, d \in A \setminus \{0\}$ $\tilde{f}((a/b)+(c/d)) = \tilde{f}((ad+bc)/(bd)) = f(ad+bc)f(bd)^{-1} = f(a)f(b)^{-1} + f(c)f(d)^{-1} = \tilde{f}(a/b) + \tilde{f}(c/d)$; $\tilde{f}((a/b)(c/d)) = \tilde{f}((ac)/(bd)) = f(ac)f(bd)^{-1} = f(a)f(b)^{-1}f(c)f(d)^{-1} = \tilde{f}(a/b)\tilde{f}(c/d)$; $\tilde{f}(1_{Q(A)}) = f(1_A) = 1_K$.
- $\tilde{f}|_A = f$ perché $\tilde{f}(a) = \tilde{f}(a/1) = f(a)f(1)^{-1} = f(a)$ $\forall\, a \in A$.
- $\tilde{f}$ iniettivo perché $Q(A)$ è un campo e $K \neq \{0\}$.

Sottocampi

Definizione

Se K è un campo, $F \subseteq K$ è un sottocampo di K se F è un sottoanello di K e come anello è un campo.

Chiaramente $F \subseteq K$ è un sottocampo di $K \iff$

- $1 \in F$;
- $a, b \in F \implies a - b, ab \in F$;
- $a \in F \setminus \{0\} \implies a^{-1} \in F$.

Esempio

Le seguenti inclusioni sono sottocampi:

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$;
- $K \subset K(X) := Q(K[X])$ $\forall\, K$ campo.

Osservazione

K campo, $F_\lambda \subseteq K$ sottocampi (con $\lambda \in \Lambda$) $\implies \bigcap_{\lambda \in \Lambda} F_\lambda \subseteq K$ sottocampo (esercizio).

Sottocampo primo di un campo

Definizione

Il sottocampo primo di un campo K è il più piccolo sottocampo di K, cioè l'intersezione di tutti i sottocampi di K.

Proposizione

K campo, $F \subseteq K$ sottocampo primo di K $\implies$

$$F \cong \begin{cases} \mathbb{Q} & \text{se } \operatorname{char}(K) = 0 \\ \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} & \text{se } \operatorname{char}(K) = p \text{ primo.} \end{cases}$$

Dimostrazione.

$f : \mathbb{Z} \to F$ unico omomorfismo di anelli, $c := \operatorname{char}(K) = \operatorname{char}(F)$.

- $c = p \implies$ per il primo teorema di isomorfismo per anelli $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker(f) \cong \operatorname{im}(f) \subseteq F$ sottocampo $\implies \operatorname{im}(f) = F$.
- $c = 0 \implies$ per il Corollario $\exists\ \tilde{f} : \mathbb{Q} \to F$ omomorfismo iniettivo $\implies \mathbb{Q} \cong \operatorname{im}(\tilde{f}) \subseteq F$ sottocampo $\implies \operatorname{im}(\tilde{f}) = F$.

Estensioni di campi

Definizione

Un'estensione di campi è un omomorfismo (necessariamente iniettivo) di anelli $K \to L$ con K e L campi.

Esempio

L campo, $K \subseteq L$ sottocampo $\implies$ l'omomorfismo di inclusione $K \to L$ è un'estensione di campi.

Osservazione

Sia $i\colon K \to L$ è un'estensione di campi.

- L è una K-algebra, e in particolare un K-spazio vettoriale.
- $K' := \mathrm{im}(i) \subseteq L$ sottocampo tale che $K \cong K'$.

Per abuso di notazione, spesso un'estensione di campi $i\colon K \to L$ viene indicata semplicemente con $K \subseteq L$, anche quando i non è un'inclusione. Tale abuso verrà evitato quando i sarà rilevante.

Grado di un'estensione di campi

Definizione

Il grado di un'estensione di campi $K \subseteq L$ è

$$[L : K] := \dim_K(L).$$

L'estensione si dice finita se $[L : K] < \infty$.

Se $K \subseteq L$ non è finita, scriveremo semplicemente $[L : K] = \infty$.

Osservazione

- $[L : K]$ non va confuso con l'indice di $K < L$.
- $[L : K] > 0$ e $[L : K] = 1 \iff K = L$.

Esempio

- $[\mathbb{C} : \mathbb{R}] = 2$ perché $\{1, i\}$ è una $\mathbb{R}$-base di $\mathbb{C}$.
- $[K(X) : K] = \infty$ perché $\{X^n : n \in \mathbb{N}\} \subset K[X] \subset K(X)$ è K-linearmente indipendente.