

campo dei quozienti di un dominio d'integritá

PROPOSIZIONE 1 *Se D é un dominio d'integritá, $Q(D)$ non contiene sottocampi propri contenenti D .*

DIM. Sia K un sottocampo di $Q(D)$ contenente D . Allora

$$K \supseteq D \Rightarrow ab^{-1} \in K, \forall a, b \in D, b \neq 0 \Rightarrow K \supseteq Q(D).$$

PROPOSIZIONE 2 *Sia D un dominio d'integritá. Sia K un campo contenente D come sottoanello e privo di sottocampi propri contenenti D . Allora K é isomorfo a $Q(D)$.*

DIM. La prop.?? assicura che $F = \{ab^{-1} : a, b \in D, b \neq 0\}$ é un sottocampo di K contenente D e isomorfo a $Q(D)$. Ne segue che $K = F \sim Q(D)$.

Le ultime due proposizioni hanno il seguente corollario di immediata dimostrazione.

COROLLARIO 3 *Siano K un campo ed A un sottoanello di K . Allora il sottocampo di K generato da A é isomorfo al campo dei quozienti di A .*

Avvertiamo il Lettore che nel seguito, se K é un campo e A un suo sottoanello, con abuso di notazione, identificheremo spesso $Q(A)$ col sottocampo di K generato da A ; porremo cioè

$$Q(A) = \{ab^{-1} : a, b \in A, b \neq 0\}. \quad (1)$$

estensioni quadratiche

Sia A un sottoanello unitario del campo C dei numeri complessi e osserviamo che A é un dominio di integritá. Sia inoltre u un elemento non quadrato di A , cioè un elemento per cui non esiste alcun $x \in A$ tale che $x^2 = u$.

DEFINIZIONE 4 Sia \sqrt{u} un numero complesso il cui quadrato sia u . Si chiama *estensione quadratica di A ottenuta aggiungendo una radice quadrata \sqrt{u} di u* , e si denota con $A[\sqrt{u}]$, il sottoanello di C generato da $A \cup \{\sqrt{u}\}$, cioè

$$A[\sqrt{u}] = \{a + b\sqrt{u} \quad : \quad a, b \in A\}.$$

DEFINIZIONE 5 Se $z = a + b\sqrt{u}$ é un elemento di $A[\sqrt{u}]$, l'elemento $\bar{z} = a - b\sqrt{u}$ si chiama *coniugato* di z . Il prodotto $n(z) = z\bar{z}$ si chiama *norma* di z .

Poiché risulta

$$n(a + b\sqrt{u}) = (a + b\sqrt{u})(a - b\sqrt{u}) = a^2 - ub^2,$$

la norma di un elemento di $A[\sqrt{u}]$ é un elemento di A . Inoltre si ha:

- $\bar{\bar{a}} = a \Leftrightarrow a \in A$;
- $n(a) = a^2 \Leftrightarrow a \in A$;
- $n(0) = 0$ e $n(1) = 1$;
- $n(z_1 z_2) = n(z_1) n(z_2)$;
- $n(z^{-1}) = n(z)^{-1}$.

estensioni quadratiche

PROPOSIZIONE 6 Un elemento $z \in A[\sqrt{u}]$ é invertibile in $A[\sqrt{u}]$ se, e solo se, la norma $n(z)$ é invertibile di A . Inoltre, se A é un campo, allora $A[\sqrt{u}]$ é un campo.

DIM. Se z é invertibile in $A[\sqrt{u}]$, risulta

$$1 = n(1) = n(zz^{-1}) = n(z)n(z)^{-1},$$

ció $n(z)$ é invertibile in A . Se $n(z)$ é invertibile in A , risulta

$$1 = n(z)n(z)^{-1} = z\bar{z}n(z)^{-1} = z(\bar{z}n(z)^{-1}),$$

ció z é invertibile in $A[\sqrt{u}]$.

Per la seconda parte, basta osservare che, se A é un campo, la norma di un suo elemento $\neq 0$ non é nulla, altrimenti u sarebbe un quadrato in A .

OSSERVAZIONE 7 Il campo dei numeri complessi é l'estensione quadratica del campo reale ottenuta aggiungendo una radice quadrata di -1 .

OSSERVAZIONE 8 L'applicazione

$$c : z \in A[\sqrt{u}] \rightarrow \bar{z} \in A[\sqrt{u}]$$

é un automorfismo di $A[\sqrt{u}]$, che si chiama *coniugio*. E' immediato verificare che c^2 é l'identità e che c fissa tutti gli elementi di A .

estensioni quadratiche

PROPOSIZIONE 9 *Gli unici automorfismi di $A[\sqrt{u}]$ che fissano ogni elemento di A sono il coniugio e l'automorfismo identico.*

DIM. Se f é un automorfismo del tipo richiesto e poniamo $v = \sqrt{u}$, abbiamo $u = v^2 = f(v^2) = f(v)^2$ e quindi

$$0 = v^2 - f(v)^2 = (v - f(v))(v + f(v)).$$

Ne segue che $v - f(v) = 0$ oppure $v + f(v) = 0$. Nel primo caso si ha subito che f é l'identitá. Nel secondo caso abbiamo $f(v) = -v$ e quindi, per ogni $z = a + bv \in A[\sqrt{u}]$,

$$f(z) = f(a + bv) = f(a) + f(b)f(v) = a - bv = \bar{z};$$

ne segue che f é il coniugio.

COROLLARIO 10 *Gli unici automorfismi del campo complesso che fissano ogni elemento del campo reale sono il coniugio e l'automorfismo identico.*

DEFINIZIONE 11 Denotata con $i = \sqrt{-1}$ l'unitá immaginaria di C , la estensione quadrati-ca

$$\mathbb{Z}[i] = \{a + bi \quad : \quad a, b \in \mathbb{Z}\}$$

si chiama *anello degli interi di Gauss*.

polinomi simmetrici

DEFINIZIONE 12 Siano K un campo e $f(x_1, x_2, \dots, x_n)$ un polinomio in n indeterminate a coefficienti in K . Possiamo allora considerare l'insieme

$$G_f = \{\sigma \in S_n : f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})\},$$

che, come subito si prova, risulta un gruppo di permutazioni su N_n . Tale gruppo si chiama *gruppo delle simmetrie* di f ; si dice inoltre che f é *simmetrico*, o *invariante*, rispetto ad un gruppo di permutazioni G su N_n se risulta $G \leq G_f$. Quando accade che $G_f = S_n$, il polinomio f si dice *simmetrico*.

ESEMPIO 13 Il polinomio $x_1^2 + x_1x_2 + x_2^2$ é simmetrico. Il polinomio

$$f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$$

non é simmetrico e il suo gruppo delle simmetrie é

$$G_f = \{1, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}.$$

ESEMPIO 14 I seguenti polinomi in n indeterminate a coefficienti in un campo K sono simmetrici:

$$\sigma_1 = x_1 + x_2 + \dots + x_n = \sum_{i=1}^n x_i,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n = \sum_{1 \leq i < j \leq n} x_i x_j,$$

$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k,$$

.....

$$\sigma_n = x_1x_2 \dots x_n;$$

essi prendono il nome di *polinomi simmetrici elementari*.

polinomi simmetrici

Riportiamo la proprietà fondamentale dei polinomi simmetrici elementari che, tra l'altro, giustifica anche l'aggettivo *elementare* usato per questi polinomi.

TEOREMA 15 *Siano K un campo e $f(x_1, x_2, \dots, x_n)$ un polinomio simmetrico a coefficienti in K . Allora esiste un unico polinomio*

$$f_s(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$$

tale che

$$f(x_1, x_2, \dots, x_n) = f_s(\sigma_1, \sigma_2, \dots, \sigma_n).$$

ESEMPIO 16 *Assegnato il polinomio simmetrico $f(x) = x_1^2 + x_1x_2 + x_2^2$, risulta*

$$f_s(x_1, x_2) = x_1^2 - x_2;$$

infatti si ha:

$$\begin{aligned} f_s(\sigma_1, \sigma_2) &= f_s(x_1 + x_2, x_1x_2) = \\ (x_1 + x_2)^2 - x_1x_2 &= x_1^2 + x_1x_2 + x_2^2 = f(x_1, x_2). \end{aligned}$$

ESERCIZIO 17 *Siano K un campo e $K_s[x_1, x_2, \dots, x_n]$ l'insieme dei polinomi simmetrici a coefficienti in K nelle indeterminate x_1, x_2, \dots, x_n . Provare che $K_s[x_1, x_2, \dots, x_n]$ è un sottoanello di $K[x_1, x_2, \dots, x_n]$ e che risulta*

$$K_s[x_1, x_2, \dots, x_n] = K[\sigma_1, \sigma_2, \dots, \sigma_n].$$

Provare, inoltre, che $K_s[x_1, x_2, \dots, x_n]$ non è un ideale di

$$K[x_1, x_2, \dots, x_n].$$