

Capitolo 3

Richiami sui campi

3.1 Il campo dei quozienti di un dominio di integritá

Sia D un dominio d'integritá. La relazione \sim su $D \times D^*$ definita da

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

risulta d'equivalenza ed il relativo insieme quoziente si denota con $Q(D)$. La classe d'equivalenza $[(a, b)]$ di una coppia (a, b) , che si denota con

$$\frac{a}{b} \text{ o con } a/b,$$

si chiama *frazione di numeratore a e denominatore b* . Le seguenti proprietá sono di facile verifica:

- $\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a, b) \sim (c, d) \Leftrightarrow ad = bc$;
- $\frac{ac}{bc} = \frac{a}{b}$, per ogni elemento $c \in D^*$;
- $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$;
- $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Risultano, pertanto, ben definite in $Q(D)$ le seguenti operazioni di addizione e moltiplicazione:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

La struttura $(Q(D), +)$ é un gruppo abeliano additivo nel quale lo zero é dato dalla frazione $\frac{0}{d}$, con $d \in D^*$ e l'opposto di un elemento $\frac{a}{b}$ é $\frac{-a}{b}$. La moltiplicazione é associativa, commutativa, distributiva rispetto all'addizione ed eredita dalla moltiplicazione di D anche la validitá della

legge di annullamento del prodotto, cioè

$$\frac{a}{b} \frac{c}{d} = 0 \Leftrightarrow \frac{a}{b} = 0 \text{ o } \frac{c}{d} = 0.$$

Ne segue che $Q(D)^* = Q(D) \setminus \{0\}$ é stabile rispetto alla moltiplicazione. La struttura $(Q(D)^*, \cdot)$ é un gruppo abeliano moltiplicativo nel quale l'unitá é data dalla frazione $\frac{a}{a}$, con $a \in D \setminus \{0\}$, e l'inverso di un elemento non nullo $\frac{a}{b}$ é $\frac{b}{a}$. Resta pertanto provata la seguente proposizione.

PROPOSIZIONE 3.1.1. *La struttura $(Q(D), +, \cdot)$ é un campo.* \square

DEFINIZIONE 3.1.2. Il campo $(Q(D), +, \cdot)$ prende il nome di *campo dei quozienti* del dominio di integritá D e sará denotato semplicemente con $Q(D)$. \square

OSSERVAZIONE 3.1.3. Il campo $(Q(\mathbb{Z}), +, \cdot)$ dei quozienti di \mathbb{Z} é il campo Q dei razionali. \square

Fissato ora un elemento $b \in D^*$, definiamo l'applicazione

$$i : a \in D \rightarrow \frac{ab}{b} \in Q(D)$$

e osserviamo che essa non dipende dalla scelta di b in D^* perché é

$$\frac{ab}{b} = \frac{ac}{c},$$

per ogni $c \in D^*$. Inoltre, risultando

$$\begin{aligned} i(x+y) &= \frac{(x+y)b}{b} = \frac{xb+yb}{b} = \frac{xb}{b} + \frac{yb}{b} = i(x) + i(y); \\ i(xy) &= \frac{xyb}{b} = \frac{xyb}{b} \frac{b}{b} = \frac{xyb}{b^2} = \frac{xb}{b} \frac{yb}{b} = i(x)i(y), \end{aligned}$$

la funzione i é un omomorfismo con nucleo nullo

$$\text{Ker } i = \{a \in D : \frac{ab}{b} = 0\} = \{0\}.$$

Ne segue che i é un monomorfismo canonico, nel senso che é indipendente dalla scelta dell'elemento b in D^* , e quindi

$$D \sim i(D) = \left\{ \frac{ab}{b} : a \in D \right\} \subseteq Q(D).$$

Abbiamo cosí che $Q(D)$ contiene il sottoanello $i(D)$ canonicamente isomorfo ad D .

Nel seguito, con abuso di linguaggio e di notazione, identificheremo D e $i(D)$, cioè penseremo D come sottoanello di $Q(D)$, e scriveremo $a = i(a)$, per ogni $a \in D$. Con questa notazione, per ogni $\frac{x}{y} \in Q(D)^*$, abbiamo

$$\frac{x}{y} = \frac{xb}{b} \frac{b}{yb} = \frac{xb}{b} \left(\frac{yb}{b} \right)^{-1} = i(x)i(y)^{-1} = xy^{-1}$$

e così possiamo scrivere

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

ESEMPIO 3.1.4. L'anello $Z[x]$ dei polinomi a coefficienti interi é un dominio d'integritá e quindi possiamo considerare il suo campo dei quozienti

$$Q(Z[x]) = \left\{ \frac{f(x)}{g(x)} \quad : \quad f, g \in Z[x], g \neq 0 \right\}.$$

Gli elementi di $Q(Z[x])$ si chiamano *funzioni razionali* su Z . □

ESEMPIO 3.1.5. Se F é un campo, il campo dei quozienti di $F[x]$, l'anello dei polinomi a coefficienti in F , si denota con $F(x)$. Gli elementi di $F(x)$ si chiamano *funzioni razionali* su F . □

ESERCIZIO 3.1.6. Siano D_1, D_2 domini di integritá isomorfi e $f : D_1 \rightarrow D_2$ un isomorfismo. Provare che l'applicazione

$$\varphi : \frac{a}{b} \in Q(D_1) \rightarrow \frac{f(a)}{f(b)} \in Q(D_2)$$

é ben definita e risulta un isomorfismo fra $Q(D_1)$ e $Q(D_2)$. □

ESERCIZIO 3.1.7. Provare che il campo dei quozienti del dominio d'integritá $(2Z, +, \cdot)$ é isomorfo al campo razionale. □

OSSERVAZIONE 3.1.8. Due domini d'integritá non isomorfi possono avere campi dei quozienti isomorfi. Abbiamo, infatti, visto che $(Z, +, \cdot)$ e $(2Z, +, \cdot)$, che non sono isomorfi, hanno entrambi campo dei quozienti isomorfo al campo razionale. □

PROPOSIZIONE 3.1.9. Siano K un corpo e A un sottoanello commutativo di K . Allora A é un dominio di integritá e $Q(A)$ é isomorfo al sottocampo F di K definito da

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

In particolare, se A é un campo, abbiamo $F = A$, cioè ogni campo é isomorfo al proprio campo dei quozienti.

DIMOSTRAZIONE. L'applicazione

$$f : \frac{a}{b} \in Q(A) \rightarrow ab^{-1} \in K$$

é un monomorfismo. Allora $f(Q(A)) = F$ é un campo perché isomorfo a $Q(A)$. □

PROPOSIZIONE 3.1.10. Se D é un dominio di integritá, $Q(D)$ non contiene sottocampi propri contenenti D .

DIMOSTRAZIONE. Sia F un sottocampo di $Q(D)$ contenente D . Allora

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

□

PROPOSIZIONE 3.1.11. *Sia D un dominio di integritá. Sia F un campo contenente D come sottoanello e privo di sottocampi propri contenenti D . Allora F é isomorfo a $Q(D)$.*

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

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

COROLLARIO 3.1.12. *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 .*

3.2 Sottocampo fondamentale di un corpo

Sia A un anello.

DEFINIZIONE 3.2.1. Se non esiste alcun intero positivo n tale che $na = 0$, per ogni elemento a di A , si dice che A ha *caratteristica zero*. Nel caso contrario, il minimo intero positivo c per cui $ca = 0$, per ogni elemento a di A , prende il nome di *caratteristica di A* . \square

OSSERVAZIONE 3.2.2. L'anello nullo é l'unico anello di caratteristica 1. \square

ESERCIZIO 3.2.3. *Provare che:*

- *l'anello Z degli interi ha caratteristica zero;*
- *l'anello Z_m degli interi modulo m ha caratteristica m ;*
- *il campo razionale Q , il campo reale R ed il campo complesso C hanno caratteristica zero;*
- *l'anello $M_n(A)$ delle matrici quadrate d'ordine n su un anello A ha la stessa caratteristica di A ;*
- *l'anello $A[x]$ dei polinomi a coefficienti in un anello A ha la stessa caratteristica di A . \square*

Supponiamo ora che l'anello A sia unitario e non nullo. Denotati con u l'unitá di A e con 1 l'unitá di Z , l'applicazione

$$f : n \in Z \rightarrow nu \in A \tag{3.1}$$

é un morfismo di anelli unitari; infatti, per ogni $n, m \in Z$, si ha

$$1. f(n + m) = (n + m)u = nu + mu = f(n) + f(m),$$

$$2. f(nm) = (nm)u = n(mu) = (nu)(mu) = f(n)f(m),$$

3. $f(1) = 1u = u$.

DEFINIZIONE 3.2.4. L'immagine dell' omomorfismo (3.1),

$$\text{Im } f = \{nu : n \in Z\} \sim Z/\text{Ker } f, \quad (3.2)$$

che é un sottoanello di A , prende il nome di *sottoanello fondamentale* di A e si denota con $E(A)$. \square

TEOREMA 3.2.5. *Il sottoanello fondamentale $E(A)$ di un anello unitario e non nullo A é isomorfo a Z o a Z_c , secondo che A abbia caratteristica rispettivamente 0 o c .*

DIMOSTRAZIONE. Dalle (3.1) e (3.2) segue che $E(A) (\sim Z/\text{ker } f)$ é isomorfo ad un quoziente di Z e da ciò segue l'asserto. \square

PROPOSIZIONE 3.2.6. *Sia A un anello unitario integro di caratteristica $c \neq 0$. Allora c é un numero primo ed $E(A)$ é un campo finito d'ordine c .*

DIMOSTRAZIONE. Se $c \neq 0$ e A é integro, anche $E(A) \sim Z_c$ é integro. Ne segue che $E(A)$ é un campo d'ordine finito c e c é primo. \square

PROPOSIZIONE 3.2.7. *Sia A un dominio d'integritá unitario di caratteristica $p > 0$. Per ogni intero positivo n e per ogni $a, b \in A$, risulta*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}. \quad (3.3)$$

DIMOSTRAZIONE. Osserviamo che risulta

$$\begin{aligned} (a + b)^p &= \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} \\ &= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} \\ &= a^p + b^p + \sum_{i=1}^{p-1} p \frac{(p-1)(p-2)\cdots(p-i-1)}{i!} a^i b^{p-i}. \end{aligned}$$

Poiché

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i-1)}{i!}$$

é un intero e p é primo,

$$\frac{(p-1)(p-2)\cdots(p-i-1)}{i!}$$

deve essere a sua volta un intero, per ogni i tale che $1 \leq i \leq p-1$. Ne segue che per tali valori di i , il binomiale $\binom{p}{i}$ é un multiplo di p e quindi $\binom{p}{i} a^i b^{p-i} = 0$. Resta cosí provato che

$$(a + b)^p = a^p + b^p.$$

Ora, se nell'ultima uguaglianza eleviamo n volte ambo i membri alla potenza p -esima, otteniamo l'asserto. \square

DEFINIZIONE 3.2.8. Sia K un corpo. Allora il sottoanello fondamentale $E(K)$ é un dominio di integritá e la caratteristica c di K é zero o un numero primo. Inoltre il campo dei quozienti $Q(E(K))$ di $E(K)$ é isomorfo al sottocampo di K

$$\overline{E}(K) = \{ab^{-1} : a \in E(K), b \in E(K)^*\}.$$

Il sottocampo $\overline{E}(K)$ si chiama *sottocampo fondamentale* di K . □

PROPOSIZIONE 3.2.9. Sia K un corpo di caratteristica c . Allora si ha

- $c = 0 \Rightarrow \overline{E}(K) \sim Q$;
- $c \neq 0 \Rightarrow c$ é un primo e $\overline{E}(K) \sim Z_c$;
- $\overline{E}(K)$ é l' intersezione di tutti i sottocorpi di K .

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. □

3.3 Estensioni di campi

Siano F e K due campi.

DEFINIZIONE 3.3.1. Diciamo che F é un' *estensione* di K se K é un sottocampo di F . Per indicare che F é estensione di K si usa la notazione F/K .

Se F é un' estensione di K ed a un elemento di F , denotiamo con $K[a]$ e $K(a)$ rispettivamente il sottoanello ed il sottocampo di F generati da $K \cup \{a\}$. □

PROPOSIZIONE 3.3.2. Sia F un' estensione di K . Per ogni elemento $a \in F$, risulta

$$K[a] = \{f(a) : f \in K[x]\}. \tag{3.4}$$

Ne segue che $K(a)$ é il campo dei quozienti di $K[a]$, cioè

$$K(a) = \{f(a)g(a)^{-1} : f, g \in K[x], g(a) \neq 0\}. \tag{3.5}$$

DIMOSTRAZIONE. Ogni sottoanello di F contenente K ed a contiene tutte le potenze a^n , $n \geq 0$, e quindi tutti gli elementi del tipo

$$b_0 + b_1a + b_2a^2 + \dots + b_na^n$$

al variare di n in N_o e degli a_j in K . Tali elementi formano un sottoanello di F contenente K ed a e abbiamo cosí la (3.4). La (3.5) segue dal corollario 3.1.12. □

Nel seguito F denoterá sempre un' estensione di K e a un elemento di F .

DEFINIZIONE 3.3.3. Il sottocampo $K(a)$ di F , generato da $K \cup \{a\}$, é un' estensione di K che si chiama *estensione semplice* di K mediante a . \square

OSSERVAZIONE 3.3.4. L'estensione $K(a)$ di K é il minimo (rispetto all' inclusione) sottocampo di F contenente K e l'elemento a . Naturalmente $K(a)$ contiene $K[a]$. \square

ESERCIZIO 3.3.5. *Provare che $K[a] = K$ se, e soltanto se, $a \in K$.* \square

Ricordiamo che vale il seguente teorema.

PROPOSIZIONE 3.3.6. *L'anello $K[x]$ dei polinomi a coefficienti in un campo K é principale e, quindi, ogni suo ideale é generato da un unico elemento. Inoltre, i generatori di un ideale J di $K[x]$ sono tutti e soli i polinomi di grado minimo contenuti in J ¹. Infine, un ideale J é massimale se, e solo se, un suo generatore (e quindi tutti) é un polinomio irriducibile.* \square

DEFINIZIONE 3.3.7. Detto a un elemento di F , possiamo considerare l' ideale $I_a = I_a(K)$ di $K[x]$ definito da

$$I_a := \{f \in K[x] : f(a) = 0\}.$$

Se $I(a) \neq (0)$, cioè se esiste un polinomio non nullo a coefficienti in K avente a come radice, l' elemento a si dice *algebrico su K* ; nel caso contrario si dice *trascendente su K* . Nell' ipotesi che a sia algebrico su K , il polinomio minimo $p(x)$ dell' ideale I_a si chiama anche *polinomio minimo* di a su K ; in altre parole $p(x)$ é l'unico polinomio monico tra tutti i polinomi in $K[x]$ di grado minimo che si annullano su a . \square

PROPOSIZIONE 3.3.8. *Sia $a \in F$ un elemento algebrico su K . Allora il polinomio minimo $p(x)$ di a su K é irriducibile e, di conseguenza, I_a é un ideale massimale di $K[x]$.*

DIMOSTRAZIONE. Nelle nostre ipotesi, se poniamo $p = fg$, con $f, g \in K[x]$, abbiamo $p(a) = f(a)g(a) = 0$ e quindi deve essere $f(a) = 0$ oppure $g(a) = 0$. Nel primo caso, avendosi $\deg(f) \leq \deg(p)$ ed essendo p di grado minimo tra i polinomi di $K[x]$ che si annullano su a , risulta $\deg(f) = \deg(p)$ e quindi g é una costante. Nel secondo caso si ragiona allo stesso modo e si ottiene cosí l' asserto. \square

ESEMPIO 3.3.9. Riportiamo alcuni esempi di numeri reali trascendenti² sul campo razionale.

$$\bullet \quad 0,1010010000001 \underbrace{0\dots 0}_4 1 \underbrace{0\dots 0}_5 1 \underbrace{0\dots 0}_6 \dots = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

Questo é storicamente il primo esempio di numero trascendente; la sua trascendenza fu provata da *J.Liouville* nel 1844.

- e = base dei logaritmi naturali.

¹Tra i polinomi che generano J ve ne é uno solo monico: il *polinomio minimo* di J .

²La distinzione fra numeri algebrici e trascendenti su Q fu fatta esplicitamente per la prima volta nel 1744 da *L.Euler* e solo dopo un secolo fu trovato il primo esempio di numero trascendente.

La trascendenza di questo numero fu provata da *C.Hermite* nel 1873.

- π = rapporto fra la misura di una circonferenza e quella di un suo diametro.

La trascendenza di questo numero fu provata da *C.Lindemann* nel 1882.

- Se a, b sono algebrici, $a \neq 0, 1$ e b è irrazionale, allora a^b è trascendente. Per esempio, $2^{\sqrt{2}}$ è trascendente. \square

ESERCIZIO 3.3.10. Sia $a \in F$ un elemento algebrico su K . Provare che ogni elemento di K è algebrico su K e che l'elemento a appartiene a K se, e solo se, il polinomio minimo di a su K è $(x - a)$. \square

ESERCIZIO 3.3.11. Siano a, b due numeri reali tali che $a + b$ e ab sono razionali (per esempio $3 + \sqrt{2}$ e $3 - \sqrt{2}$). Provare che a e b sono algebrici sul campo razionale. \square

PROPOSIZIONE 3.3.12. Siano F/K un'estensione ed a un elemento di F . Provare che l'applicazione

$$\varphi_a : f(x) \in K[x] \rightarrow f(a) \in K[a] \quad (3.6)$$

è un epimorfismo di anelli. Dedurne che:

- l'ideale $\text{Ker}\varphi_a = I_a$ e

$$K[x]/I_a \sim K[a]; \quad (3.7)$$

- a è trascendente su $K \Leftrightarrow K[x] \sim K[a] \Leftrightarrow K(x) = Q(K[x]) \sim K(a)$;

- se a è algebrico su K , detto $p(x)$ il polinomio minimo di I_a , risulta

$$I_a = (p) \quad \text{e} \quad K[a] \sim K[x]/(p). \quad (3.8)$$

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. \square

ESERCIZIO 3.3.13. Sia $p(x) \in K[x]$ un polinomio monico, irriducibile e tale che $p(a) = 0$, con a elemento di un'estensione di K . Provare che $p(x)$ è il polinomio minimo di a su K . \square

PROPOSIZIONE 3.3.14. L'elemento a è algebrico su K se, e solo se, risulta

$$K[a] = K(a).$$

DIMOSTRAZIONE. Sia a algebrico su K e sia $p(x)$ il polinomio minimo di a su K . Poiché $p(x)$ è irriducibile su K , l'ideale I_a è massimale in $K[x]$ e quindi $K[x]/I_a$ è un campo. Allora $K[a]$, essendo isomorfo a $K[x]/I_a$, è un campo contenuto in $K(a)$ e quindi risulta $K[a] = K(a)$.

Se $K[a] = K(a)$, allora $K[x]/I_a$ è un campo. Ne segue che I_a è un ideale massimale, quindi non nullo, in $K[x]$. Esistono dunque polinomi non nulli in $K[x]$ che si annullano su a e così a è algebrico su K . \square

PROPOSIZIONE 3.3.15. *Se l'elemento a è algebrico su K ed n è il grado del suo polinomio minimo $p(x)$ su K , allora ogni elemento $b \in K(a)$ si scrive in modo unico nella forma*

$$b = b_0 + b_1a + b_2a^2 + \cdots + b_{n-1}a^{n-1}, \quad (3.9)$$

con $b_j \in K$; risulta cioè

$$K(a) = \{f(a) : f \in K[x], \deg(f) < n\}. \quad (3.10)$$

DIMOSTRAZIONE. Se $b \in K(a)$, in forza della proposizione precedente, abbiamo $b = f(a)$, con $f \in K[x]$. Se $q(x), r(x)$ sono quoziente e resto di $f(x)$ per $p(x)$, abbiamo

$$b = f(a) = p(a)q(a) + r(a) = r(a)$$

e, essendo $r(x)$ nullo o di grado minore di $p(x)$, si ha subito la (3.9). Ora, se supponiamo

$$b = c_0 + c_1a + c_2a^2 + \cdots + c_{n-1}a^{n-1},$$

risulta

$$0 = (b_0 - c_0) + (b_1 - c_1)a + (b_2 - c_2)a^2 + \cdots + (b_{n-1} - c_{n-1})a^{n-1},$$

da cui, essendo n il grado del polinomio minimo di a su K , ricaviamo

$$b_0 = c_0, b_1 = c_1, \dots, b_{n-1} = c_{n-1},$$

come volevamo dimostrare. □

ESERCIZIO 3.3.16. *Sia $K[x]$ l'anello dei polinomi su un campo K nell'indeterminata x . Provare che il campo $Q(K[x])$ delle funzioni razionali su K è un'estensione di K , che x è un elemento trascendente su K e che $K(x) = Q(K[x])$. Inoltre, usando la (3.7), provare che un'estensione semplice $K(a)$ è isomorfa a $Q(K[x])$ se, e solo se, a è trascendente su K . Dedurre che estensioni semplici mediante elementi trascendenti di uno stesso campo sono tra loro isomorfe. □*

DEFINIZIONE 3.3.17. La nozione di estensione semplice di un campo K si generalizza nel seguente modo. Siano a_1, a_2, \dots, a_n elementi di F , ove F è un'estensione di K . Il sottocampo di F generato da $K \cup \{a_1, a_2, \dots, a_n\}$ è un'estensione di K che si chiama *estensione di K mediante gli elementi a_1, a_2, \dots, a_n* e si denota con $K(a_1, a_2, \dots, a_n)$. □

OSSERVAZIONE 3.3.18. Siano F/K un'estensione e a_1, a_2, \dots, a_n elementi di F . Il campo

$$K(a_1, a_2, \dots, a_n)$$

è il minimo (rispetto all'inclusione) sottocampo di F contenente K e gli elementi a_1, a_2, \dots, a_n . Il campo $K(a_1, a_2, \dots, a_n)$ contiene il sottoanello di F generato da $K \cup \{a_1, a_2, \dots, a_n\}$, che denotiamo con $K[a_1, a_2, \dots, a_n]$, ed è isomorfo al campo dei quozienti $Q(K[a_1, a_2, \dots, a_n])$ di tale anello. □

ESERCIZIO 3.3.19. *Provare che, per ogni $a_1, a_2, \dots, a_n \in F$, risulta*

$$K[a_1, a_2, \dots, a_n] = \{f(a_1, a_2, \dots, a_n) : f \in K[x_1, x_2, \dots, x_n]\}.$$

Ne segue che

$$K(a_1, a_2, \dots, a_n) = \{f(a_1, a_2, \dots, a_n)g(a_1, a_2, \dots, a_n)^{-1} : f, g \in K[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0\}.$$

Provare inoltre che

$$(K(a_1, a_2, \dots, a_{n-1}))(a_n) = K(a_1, a_2, \dots, a_n).$$

□

Sia F/K una estensione. Allora F può essere considerato come spazio vettoriale su K e, in questo contesto, parleremo di insiemi di elementi di F indipendenti su K , di basi di F su K , ecc. .

DEFINIZIONE 3.3.20. La dimensione di F su K prende il nome di *grado* di F su K e si denota con $(F : K)$. □

OSSERVAZIONE 3.3.21. E' chiaro che risulta $(F : K) = 1$ se, e solo se, $F = K$. □

ESEMPIO 3.3.22. L'insieme $\{1, i\}$ é una base di C su R e quindi risulta $(C : R) = 2$. □

ESEMPIO 3.3.23. Siano a un elemento algebrico su un campo K ed n il grado del polinomio minimo di a su K . La prop. 3.3.15 assicura che $(K(a) : K) = n$. □

PROPOSIZIONE 3.3.24. *Siano F e K due campi finiti e supponiamo F estensione di K di grado n . Allora, se K ha ordine q , il campo F ha ordine q^n .*

DIMOSTRAZIONE. Il campo F , come spazio vettoriale su K , ha dimensione n e, quindi, é isomorfo allo spazio vettoriale numerico K^n . Abbiamo cosí

$$|F| = |K^n| = |K|^n = q^n,$$

cioé l'asserto. □

TEOREMA 3.3.25. (teorema della moltiplicazione dei gradi) *Siano F/L e L/K estensioni di grado finito. Allora F/K é una estensione di grado finito e risulta*

$$(F : K) = (F : L)(L : K).$$

DIMOSTRAZIONE. Siano

$$X = \{x_1, \dots, x_n\}$$

una K -base di L ,

$$Y = \{y_1, \dots, y_m\}$$

una L -base di F e poniamo

$$B = \{x_i y_j : i = 1, \dots, n, j = 1, \dots, m\}.$$

Ora osserviamo che $B \subseteq F$ é indipendente su K perché

$$\begin{aligned} \sum b_{ij}x_iy_j = 0, b_{ij} \in K &\Rightarrow \\ \sum b_{ij}x_iy_j = \sum_j \left(\sum_i b_{ij}x_i \right) y_j = 0, \sum_i b_{ij}x_i \in L &\Rightarrow \\ \sum_i b_{ij}x_i = 0, \forall j &\Rightarrow b_{ij} = 0, \forall i, j. \end{aligned}$$

D'altra parte abbiamo

$$\begin{aligned} a \in F &\Rightarrow a = c_1y_1 + c_2y_2 + \dots + c_my_m, c_j \in L \Rightarrow \\ c_j &= b_{1j}x_1 + b_{2j}x_2 + \dots + b_{nj}x_n, b_{ij} \in K \Rightarrow \\ a &= \left(\sum b_{i1}x_i \right) y_1 + \left(\sum b_{i2}x_i \right) y_2 + \dots + \left(\sum b_{im}x_i \right) y_m = \sum b_{ij}x_iy_j, \end{aligned}$$

e quindi B é un generatore di F su K . Ne segue l'asserto. \square

Il teorema precedente ammette la seguente generalizzazione, la cui dimostrazione é lasciata come esercizio al Lettore.

PROPOSIZIONE 3.3.26. *Siano F/L e L/K estensioni. Siano, inoltre, X una base di L su K e Y una base di F su L . Provare che*

$$B = \{xy : x \in X, y \in Y\}$$

é una base di F su K .

DEFINIZIONE 3.3.27. Si dice che F é un'estensione algebrica di K , o che F é algebrico su K , se ogni elemento di F é algebrico su K . Nel caso contrario, cioè se F contiene almeno un elemento trascendente su K , si dice che F é un'estensione trascendente di K , o che F é trascendente su K . \square

PROPOSIZIONE 3.3.28. *Sia F/K un'estensione di grado finito n . Allora F é algebrico su K e ogni elemento di F é radice di un polinomio su K di grado non superiore ad n .*

DIMOSTRAZIONE. Sia a un elemento di F^* . Se esistono $i, j \in \{0, 1, \dots, n\}$ tali che $a^i = a^j$, allora a é radice del polinomio $(x^i - x^j) \in K[x]$. Nel caso contrario, $a^0 = 1, a^1 = a, a^2, \dots, a^n$ sono $n + 1$ elementi a due a due distinti di F e quindi linearmente dipendenti su K . Ne segue che esistono degli elementi $b_j \in K$ non tutti nulli tali che

$$b_0 + b_1a + b_2a^2 + \dots + b_na^n = 0.$$

L'elemento a é dunque radice del polinomio non nullo

$$f(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n \in K[x]$$

ció l'asserto. \square

COROLLARIO 3.3.29. *Siano F/K un' estensione e a un elemento di F algebrico su K . Allora $K(a)$ é algebrico su K .*

DIMOSTRAZIONE. L'asserto segue dall' essere $(K(a) : K)$ uguale al grado del polinomio minimo di a su K . \square

PROPOSIZIONE 3.3.30. *Sia F/K un' estensione. Allora F ha grado finito su K se, e soltanto se, esistono degli elementi a_1, a_2, \dots, a_n in F algebrici su K e tali che $F = K(a_1, a_2, \dots, a_n)$.*

DIMOSTRAZIONE. Sia $(F : K) = n$ e sia $\{a_1, \dots, a_n\}$ una K -base di F . Allora $K(a_1, \dots, a_n) \subseteq F$ e, per ogni $b \in F$, abbiamo

$$b = b_1 a_1 + \dots + b_n a_n, \quad b_i \in K \Rightarrow b \in K(a_1, \dots, a_n).$$

Ne segue che $F = K(a_1, \dots, a_n)$ e ogni a_i é algebrico su K perché F , avendo grado finito su K , é algebrico su K .

Sia ora $F = K(a_1, \dots, a_n)$, con tutti gli a_i algebrici su K . Poiché per $n = 1$, $K(a_1)$ ha grado finito su K , possiamo ragionare per induzione su $n > 1$. In queste ipotesi, $L = K(a_1, \dots, a_{n-1})$ ha grado finito su K e a_n , essendo algebrico su K , é algebrico su L . Ne segue che

$$K(a_1, \dots, a_{n-1})(a_n) = K(a_1, \dots, a_n)$$

ha grado finito su K , per il teorema della moltiplicazione dei gradi. \square

PROPOSIZIONE 3.3.31. *Siano F/L e L/K estensioni algebriche. Allora F/K é un' estensione algebrica.*

DIMOSTRAZIONE. Un elemento a di F , essendo algebrico su L , verifica una relazione del tipo

$$b_0 + b_1 a + b_2 a^2 + \dots + b_n a^n = 0,$$

con b_0, b_1, \dots, b_n elementi di L non tutti nulli. Poiché ogni b_j é algebrico su K , il campo $K(b_0, b_1, \dots, b_n)$ ha grado finito su K (cfr. prop. 3.3.30) e, essendo a algebrico su $K(b_0, b_1, \dots, b_n)$, il campo $K(b_0, \dots, b_n, a)$ ha grado finito su K e quindi é algebrico su K (cfr. prop. 3.3.28). Ne segue che a é algebrico su K , cioè l'asserto. \square

OSSERVAZIONE 3.3.32. Assegnata l' estensione F/K , denotiamo con \overline{K} l'insieme degli elementi di F algebrici su K . Ovviamente \overline{K} contiene K . Se a, b sono elementi di \overline{K} , allora $K(a, b)$ é contenuto in \overline{K} ; quindi $a - b$ e, se $b \neq 0$, ab^{-1} appartengono a \overline{K} . Ne segue che \overline{K} é un sottocampo di F . \square

DEFINIZIONE 3.3.33. Sia F/K un' estensione. Il sottocampo \overline{K} di F degli elementi di F algebrici su K si chiama *chiusura algebrica di K in F* . \square

PROPOSIZIONE 3.3.34. *La chiusura algebrica \overline{Q} di Q in R ha grado infinito su Q .*

DIMOSTRAZIONE. Osserviamo che, in forza del teorema di Eisenstein, $x^m - 2$ é un polinomio irriducibile su $Q[x]$; inoltre esso é il polinomio minimo su Q di $\sqrt[m]{2}$, che quindi é un elemento algebrico su Q .

Supponiamo ora, per assurdo, $(\overline{Q} : Q) = n \in N$ e sia m un intero maggiore di n . Allora $\sqrt[m]{2} \in \overline{Q}$ sarebbe radice di un polinomio su Q di grado non superiore ad n e ciò é assurdo. \square

Del teorema che segue omettiamo la dimostrazione.

TEOREMA 3.3.35. (teorema di Cantor) *Sia F/K una estensione e si supponga K numerabile. Allora la chiusura algebrica di K in F é numerabile.*

COROLLARIO 3.3.36. *La chiusura algebrica di Q in R é numerabile; di conseguenza l'insieme $R \setminus \overline{Q}$ dei numeri reali trascendenti su Q ha la potenza del continuo.*

PROPOSIZIONE 3.3.37. *Siano K un campo ed $f \in K[x]$ un polinomio di grado positivo n . Allora esiste un'estensione F di K contenente un elemento a tale che $f(a) = 0$ e $F = K(a)$.*

DIMOSTRAZIONE. Supponiamo per il momento che il polinomio

$$f(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

sia irriducibile in $K[x]$. In queste ipotesi, l'ideale $I = (f)$ é massimale in $K[x]$ e quindi $K[x]/I = F$ é un campo. Inoltre, si ha:

- L'applicazione

$$i : u \in K \rightarrow u + I \in F = K[x]/I$$

é un monomorfismo e quindi K é isomorfo a $i(K)$. Questo significa che F contiene il sottocampo $i(K)$ isomorfo a K e quindi può ritenersi una estensione di K .

Nel seguito identificheremo K e $i(K)$, ponendo $u = i(u)$, per ogni ogni elemento $u \in K$.

- Il monomorfismo $i : K \rightarrow F$ può estendersi ad un monomorfismo fra $K[x]$ e $F[x]$ ponendo

$$i(c_0 + c_1x + \cdots + c_mx^m) = i(c_0) + i(c_1)x + \cdots + i(c_m)x^m.$$

- Essendo $K \sim i(K)$, abbiamo $K[x] \sim i(K)[x]$ e possiamo identificare ogni polinomio $g \in K[x]$ col polinomio $i(g) \in i(K)[x]$. Mediante tale identificazione abbiamo

$$f = i(f) = (b_0 + I) + (b_1 + I)x + (b_2 + I)x^2 + \cdots + (b_n + I)x^n$$

e, posto $a = x + I$, risulta

$$\begin{aligned} i(f)(a) &= (b_0 + I) + (b_1 + I)(x + I) + \cdots + (b_n + I)(x + I)^n \\ &= (b_0 + I) + (b_1x + I) + \cdots + (b_nx^n + I) \\ &= (b_0 + b_1x + \cdots + b_nx^n) + I = f + I = I, \end{aligned}$$

cioé $f(a) = 0$. Abbiamo cosí che f ha uno zero in F .

Ora proviamo che $i(K)(a) = F$, tenendo presente che $i(K)(a) \subseteq F$. Abbiamo:

$$\begin{aligned} g + I \in F \text{ con } g = c_0 + c_1x + \cdots + c_mx^m \in K[x] &\Rightarrow \\ g + I = (c_0 + I) + (c_1 + I)(x + I) + \cdots + (c_m + I)(x + I)^m = \\ (c_0 + I) + (c_1 + I)a + \cdots + (c_m + I)a^m \text{ con } c_j + I \in i(K) &\Rightarrow \\ g + I \in i(K)(a) &\Rightarrow F \subseteq i(K)(a). \end{aligned}$$

L'asserto é dunque provato nel caso che f sia irriducibile.

Nell'ipotesi che f non é irriducibile, esiste un polinomio irriducibile $p \in K[x]$ che divide f . Per tale polinomio esistono F ed $a \in F$ tali che $p(a) = 0$ e $F = K(a)$. Ne segue che $f(a) = 0$ e l'asserto é completamente provato. \square

DEFINIZIONE 3.3.38. Il campo $F = K(a)$ di cui al precedente teorema si chiama *estensione di K mediante l'aggiunta di una radice di f* . \square

ESEMPIO 3.3.39. Siano $K = R$, $f(x) = x^2 + 1$ e $I = (f)$ l'ideale di $R[x]$ generato da f . In $F = R[x]/I$, posto $i = x + I$, abbiamo

$$f(i) = i^2 + 1 = (x^2 + I) + (1 + I) = (x^2 + 1) + I = I = 0.$$

Ne segue che $F = R(i) = \{a + ib : a, b \in R\} = C$. \square

ESEMPIO 3.3.40. In $Z_3[x]$ consideriamo il polinomio

$$f(x) = x^5 + 2x^2 + 2x + 2 = (x^2 + 1)(x^3 + 2x + 2)$$

e l'ideale $I = (x^2 + 1)$. Nel campo $F = Z_3[x]/I$, posto $i = x + I$, abbiamo $i^2 + 1 = 0$ e quindi $f(i) = 0$. Ne segue che

$$F = Z_3(i) = \{a + ib : a, b \in Z_3\} \text{ e } |F| = 9.$$

Se invece consideriamo in $Z_3[x]$ l'ideale $J = (x^3 + 2x + 2)$, possiamo costruire il campo $F' = Z_3[x]/J$ e, posto $j = x + J$, abbiamo $j^3 + 2j + 2 = 0$ e quindi $f(j) = 0$. Ne segue che

$$F' = Z_3(j) = \{a + bj + cj^2 : a, b, c \in Z_3\} \text{ e } |F'| = 27.$$

\square

OSSERVAZIONE 3.3.41. L'ultimo teorema non vale su anelli commutativi arbitrari. Per esempio, $2x + 1 \in Z_4[x]$ non ha radici in nessuna estensione di $Z_4[x]$ perché

$$2j + 1 = 0 \Rightarrow 0 = 2(2j + 1) = 4j + 2 = 2,$$

il che é assurdo. \square

DEFINIZIONE 3.3.42. Sia $f \in K[x]$ un polinomio di grado $n > 0$. Un'estensione F di K si chiama *campo di spezzamento di f su K* se esistono in F elementi a_1, a_2, \dots, a_n e $b \in K$ per cui risulta

$$f(x) = b(x - a_1)(x - a_2) \cdots (x - a_n)$$

e $F = K(a_1, a_2, \dots, a_n)$. □

OSSERVAZIONE 3.3.43. Notiamo esplicitamente che un campo di spezzamento di un polinomio f su un campo K ha grado finito su K e quindi è algebrico su K . □

TEOREMA 3.3.44. Sia $f \in K[x]$ di grado $n > 0$. Allora esiste un campo di spezzamento F di f su K e risulta $(F : K) \leq n!$.

DIMOSTRAZIONE. Osserviamo che, se $n = 1$, il campo cercato è K stesso. Possiamo dunque fare induzione su $n > 1$. In questa ipotesi esiste $L = K(a_1)$ con $f(a_1) = 0$ e risulta

$$n \geq (L : K) = \text{grado del polinomio minimo di } a_1 \text{ su } K,$$

$$f = (x - a_1)g, \quad g \in L[x] \text{ e } \deg(g) = n - 1.$$

Per induzione, esiste un campo di spezzamento F di g su L tale che $(F : L) \leq (n - 1)!$ e $g(x) = b(x - a_2) \cdots (x - a_n)$, con $b \in L$ e $F = L(a_2, \dots, a_n)$. Ne segue che

$$F = K(a_1)(a_2, \dots, a_n) = K(a_1, a_2, \dots, a_n),$$

$$f(x) = (x - a_1)g = b(x - a_1)(x - a_2) \cdots (x - a_n) \text{ e } b \in K.$$

Allora F è campo di spezzamento di $f(x)$ su K e

$$(F : K) = (F : L)(L : K) \leq (n - 1)!n = n!$$

□

DEFINIZIONE 3.3.45. Siano F_1/K_1 e F_2/K_2 due estensioni e σ un isomorfismo di K_1 in K_2 . Un isomorfismo $\bar{\sigma}$ di F_1 in F_2 si chiama *prolungamento di σ a F_1 e F_2* se la restrizione di $\bar{\sigma}$ a K_1 coincide con σ . □

TEOREMA 3.3.46. Siano K_1, K_2 due campi, σ un isomorfismo di K_1 in K_2 e si consideri l'applicazione $\bar{\sigma}$ di $K_1[x]$ in $K_2[x]$ definita da

$$\bar{\sigma}(a_0 + a_1x + \cdots + a_nx^n) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n.$$

Allora $\bar{\sigma}$ è l'unico prolungamento di σ a $K_1[x]$ e $K_2[x]$ tale che $\bar{\sigma}(x) = x$.

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. □

TEOREMA 3.3.47. Siano K_1, K_2 due campi, σ un isomorfismo di K_1 in K_2 , $p_1 \in K_1[x]$ e $p_2 \in K_2[x]$ polinomi irriducibili di grado n tali che $p_2 = \bar{\sigma}(p_1)$. Siano

$$K_1(a_1) = \{b_0 + b_1a_1 + \cdots + b_{n-1}a_1^{n-1} \quad : \quad b_i \in K_1\},$$

$$K_2(a_2) = \{c_0 + c_1a_2 + \cdots + c_{n-1}a_2^{n-1} \quad : \quad c_i \in K_2\}$$

estensioni semplici di K_1 e K_2 ottenute aggiungendo una radice di p_1 a K_1 e una di p_2 a K_2 e si consideri l'applicazione τ di $K_1(a_1)$ in $K_2(a_2)$ definita da

$$\tau(b_0 + b_1a_1 + \cdots + b_{n-1}a_1^{n-1}) = \sigma(b_0) + \sigma(b_1)a_2 + \cdots + \sigma(b_{n-1})a_2^{n-1}.$$

Allora τ é l'unico prolungamento di σ a $K_1(a_1)$ e $K_2(a_2)$ tale che $\tau(a_1) = a_2$.

DIMOSTRAZIONE. Osservato che il polinomio $p_2 = \bar{\sigma}(p_1)$ é irriducibile su K_2 , si procede con i seguenti passi.

- Consideriamo l'applicazione

$$\gamma : f + (p_1) \in K_1/(p_1) \rightarrow \bar{\sigma}(f) + (p_2) \in K_2/(p_2)$$

e notiamo che essa é un isomorfismo di campi.

- Per $j = 1, 2$, sappiamo che esiste un isomorfismo

$$\alpha_j : K_j(a_j) \rightarrow K_j[x]/(p_j)$$

la cui restrizione a K_j é l'identitá su K_j e

$$\alpha_j(a_j) = x + (p_j).$$

- Allora τ é un prolungamento fra $K_1(a_1)$ e $K_2(a_2)$ perché $\tau = \alpha_1\gamma\alpha_2^{-1}$

$$\begin{array}{ccccc} K_1(a_1) & \xrightarrow{\alpha_1} & K_1[x]/(p_1) & \xrightarrow{\gamma} & K_2[x]/(p_2) & \xrightarrow{\alpha_2^{-1}} & K_2(a_2) \\ & & \uparrow & & \uparrow & & \\ & & K_1 & \xrightarrow{\sigma} & K_2 & & \end{array}$$

- Se β é un prolungamento di σ a $K_1(a_1)$ e $K_2(a_2)$ tale che

$$\beta(a_1) = a_2 \quad e \quad b_0 + b_1a_1 + \cdots + b_{n-1}a_1^{n-1} \in K_1(a_1),$$

abbiamo

$$\begin{aligned} & \beta(b_0 + b_1a_1 + \cdots + b_{n-1}a_1^{n-1}) = \\ & \beta(b_0) + \beta(b_1)\beta(a_1) + \cdots + \beta(b_{n-1})\beta(a_1^{n-1}) = \\ & \sigma(b_0) + \sigma(b_1)a_1 + \cdots + \sigma(b_{n-1})a_1^{n-1} = \\ & \tau(b_0 + b_1a_1 + \cdots + b_{n-1}a_1^{n-1}) \end{aligned}$$

e quindi $\beta = \tau$. □

PROPOSIZIONE 3.3.48. (teorema di prolungamento) *Siano assegnati:*

- due campi K_1, K_2 e un isomorfismo σ di K_1 su K_2 .
- un polinomio $f_1 \in K_1[x]$ e sia $f_2 = \bar{\sigma}(f_1) \in K_2[x]$.
- un campo di spezzamento F_1 di f_1 su K_1 e un campo di spezzamento F_2 di f_2 su K_2 .

Allora esiste un prolungamento di σ a F_1 e F_2 , cioè un isomorfismo $\tau : F_1 \rightarrow F_2$ tale che $\tau(b) = \sigma(b)$ per ogni $b \in K_1$.

DIMOSTRAZIONE. L'asserto é vero se $\deg(f_1) = 1$ e quindi possiamo fare induzione su $n = \deg(f_1) > 1$.

- Siano $p_1(x)$ un fattore irriducibile di f_1 su K_1 , a_1 uno zero di $p_1(x)$ in F_1 e a_2 uno zero di $p_2 = \bar{\sigma}(p_1)$ in F_2 .
- Esiste un prolungamento α di σ a $K_1(a_1)$ e $K_2(a_2)$ tale che $\alpha(a_1) = a_2$.
- Se scriviamo $f_1(x) = (x - a_1)g_1(x)$, con $g_1 \in K_1(a_1)[x]$, abbiamo che F_1 é campo di spezzamento di g_1 su $K_1(a_1)$ e F_2 é campo di spezzamento di $g_2 = \bar{\sigma}(g_1)$ su $K_2(a_2)$.
- Essendo $\deg(g_1) = n - 1$, per induzione esiste un prolungamento τ di α a F_1 e F_2 . Per costruzione, τ é anche un prolungamento di σ a F_1 e F_2 . \square

Se nell'enunciato del teorema precedente si pone $K = K_1 = K_2$ e $f = p_1 = p_2$, si ottiene il risultato seguente.

PROPOSIZIONE 3.3.49. (unicità del campo di spezzamento) *Siano K un campo e $f \in K[x]$, con $\deg(f) > 0$. Allora due campi di spezzamento F_1, F_2 di f su K sono isomorfi.*

ESEMPIO 3.3.50. Troviamo il campo di spezzamento su Q del polinomio

$$f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1).$$

- $Q(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in Q\}$ contiene due radici di $f(x) : \sqrt{2}, -\sqrt{2}$.

- In $Q(\sqrt{2})[x]$ abbiamo:

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1).$$

Osserviamo che gli elementi di $Q(\sqrt{2})$ sono numeri reali e quindi $x^2 + 1$ é irriducibile su $Q(\sqrt{2})$.

- Per ottenere il campo di spezzamento di $f(x)$ su Q dobbiamo ampliare $Q(\sqrt{2})$ con una radice di $x^2 + 1$.

- In conclusione il campo di spezzamento cercato é:

$$Q(\sqrt{2})(i) = \{\alpha + i\beta : \alpha, \beta \in Q(\sqrt{2})\} =$$

$$\{(a + b\sqrt{2}) + (c + d\sqrt{2})i : a, b, c, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}, i).$$

□

ESEMPIO 3.3.51. Troviamo il campo di spezzamento su \mathbb{Q} del polinomio

$$f(x) = x^n - a \quad \text{con } a \in \mathbb{Q}^+, a > 1, n > 2.$$

- Siano

$$b = \sqrt[n]{a} \in \mathbb{R}$$

e

$$\omega = \text{radice } n\text{-esima primitiva di } 1 \text{ su } \mathbb{C}.$$

Allora

$$b, b\omega, b\omega^2, \dots, b\omega^{n-1}$$

sono le n radici (a due a due distinte) di $f(x)$.

- L'estensione $\mathbb{Q}(b)$, essendo un sottocampo di \mathbb{R} non contiene ω .
- Il campo di spezzamento cercato é

$$\begin{aligned} \mathbb{Q}(b)(\omega) &= \{\alpha + \beta\omega : \alpha, \beta \in \mathbb{Q}(b)\} = \\ &= \{(x + yb) + (z + tb)\omega : x, y, z, t \in \mathbb{Q}\} = \mathbb{Q}(b, \omega). \end{aligned}$$

□

3.4 Campi algebricamente chiusi

Sia F un campo.

DEFINIZIONE 3.4.1. Si dice che F é un campo *algebricamente chiuso* se ogni polinomio $f(x) \in F[x]$ di grado positivo ha almeno una radice in F . □

ESEMPIO 3.4.2. É noto al Lettore che il campo complesso é algebricamente chiuso (*teorema fondamentale dell'algebra*). □

TEOREMA 3.4.3. Per un campo F sono equivalenti le seguenti proprietà:

- (a) F é algebricamente chiuso.
- (b) Ogni polinomio non costante a coefficienti in F si decompone su $F[x]$ nel prodotto di polinomi di primo grado.
- (c) Gli elementi irriducibili di $F[x]$ sono tutti e soli i polinomi di primo grado.

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. \square

TEOREMA 3.4.4. *Ogni campo K ammette un'estensione F algebricamente chiusa.*

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. \square

DEFINIZIONE 3.4.5. Sia F/K un'estensione. Si dice che F é *chiusura algebrica di K* se é F é un campo algebricamente chiuso e algebrico su K . \square

TEOREMA 3.4.6. *Sia F/K una estensione e si supponga F algebricamente chiuso. Allora la chiusura algebrica \overline{K} di K in F é un campo algebricamente chiuso. Ne segue che ogni campo ha una chiusura algebrica.*

DIMOSTRAZIONE. La prima parte segue da $\overline{\overline{K}} = \overline{K}$. Per la seconda parte, si consideri un'estensione F di K algebricamente chiusa; allora \overline{K} é una chiusura algebrica di K . \square

TEOREMA 3.4.7. *Due chiusure algebriche di K sono isomorfe.*