

# Capitolo 8

## Polinomi

### 8.1 Divisibilità in un dominio di integrità unitario

Molti dei risultati riguardanti la divisibilità e la fattorizzazione di interi relativi e polinomi su un campo possono ottenersi, come vedremo nel seguito, anche nel contesto più generale dei domini di integrità unitari. Sia dunque  $D = (D, +, \cdot)$  un dominio di integrità unitario e ricordiamo che  $U(D)$  denota l'insieme degli elementi invertibili di  $D$ .

**DEFINIZIONE 8.1.1** Se  $a, b \in D$ , con  $b \neq 0$ , si dice che  $b$  divide  $a$  o che  $a$  è divisibile per  $b$ , in simboli  $b|a$ , se esiste un elemento  $c \in D$  tale che  $a = bc$ . In tale ipotesi si dice anche che  $b$  è un divisore di  $a$ , o che  $b$  è un fattore di  $a$ , ovvero che  $a$  è un multiplo di  $b$ .  $\diamond$

Le seguenti proprietà sono di facile verifica:

- $a|a, \quad 1|a, \quad a|0, \quad$  per ogni  $a \in D^*$ ;
- $a|b, \quad b|c \Rightarrow a|c$ ;
- $a \in U(D) \Leftrightarrow a|1$ ;
- $a \in U(D) \Rightarrow a|b, \quad$  per ogni  $b \in D$ ;
- $b|a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subseteq (b)$ .

**OSSERVAZIONE 8.1.2** Se  $D$  è un dominio di integrità unitario, allora  $(D^*, \cdot)$  risulta un semigrupp commutativo, regolare e unitario. Poiché la teoria della divisibilità riguarda essenzialmente la struttura moltiplicativa  $D^*$  di  $D$ , essa può svolgersi nell'ambito dei *semigrupp commutativi, regolari e unitari*.  $\diamond$

**DEFINIZIONE 8.1.3** Siano  $a, b \in D^*$ . Si dice che  $a$  è associato a  $b$ , in simboli  $a \sim b$ , se esiste un elemento invertibile  $u \in U(D)$  tale che  $a = bu$ .  $\diamond$

La relazione  $\sim$  risulta di equivalenza in  $D^*$  e si ha subito che

$$a \sim b \Leftrightarrow a|b \text{ e } b|a \Leftrightarrow a, b \text{ hanno gli stessi multipli e gli stessi divisori.}$$

**ESERCIZIO 8.1.4** Siano  $a, b$  elementi associati di  $D$ . Provare che  $a$  é invertibile se, e solo se,  $b$  é invertibile. Dedurre che, se  $a$  é invertibile, allora la classe degli elementi associati ad  $a$  é  $U(D)$ .

**ESERCIZIO 8.1.5** Siano  $a, b$  elementi di  $D$ . Allora risulta  $(a) = (b)$  se, e solo se,  $a$  e  $b$  sono associati.

**DEFINIZIONE 8.1.6** Sia  $a \in D^*$ . Un divisore  $b$  di  $a$  si dice *proprio* se  $a$  non divide  $b$ , cioè se  $a$  e  $b$  non sono associati. Nel caso contrario,  $b$  si dice divisore *improprio* di  $a$ .  $\diamond$

**ESERCIZIO 8.1.7** Siano  $a, b$  elementi di  $D$ . Allora  $b$  é un divisore proprio di  $a$  se, e solo se,  $(a) \subset (b) \subset D$ .

**OSSERVAZIONE 8.1.8** Ogni elemento  $a \in D^*$  ha come divisori i suoi associati e tutti gli elementi invertibili di  $D$ . Tali divisori di  $a$  si dicono *banali*.  $\diamond$

**DEFINIZIONE 8.1.9** Un elemento  $a \in D^*$  si dice *irriducibile* se non é invertibile e i suoi unici divisori sono quelli banali. Nel caso contrario  $a$  si dice *riducibile*.  $\diamond$

**DEFINIZIONE 8.1.10** Un elemento  $a \in D^*$  si dice *primo* se non é invertibile e se

$$a|bc \Rightarrow a|b \text{ o } a|c.$$

$\diamond$

**OSSERVAZIONE 8.1.11** Notiamo esplicitamente che le definizioni appena date sono formalmente uguali a quelle usate nel primo capitolo relativamente all'anello degli interi.  $\diamond$

**PROPOSIZIONE 8.1.12** Sia  $a \in D$  irriducibile. Se  $b, c \in D$  sono tali che  $a = bc$ , allora uno tra i fattori  $b$  e  $c$  é associato ad  $a$  e l'altro é invertibile.

**DIMOSTRAZIONE.** Se  $b, c$  fossero entrambi invertibili,  $a$  sarebbe invertibile e ciò non può essere. Se supponiamo  $b \notin U(D)$ , allora  $a$  e  $b$  sono associati e

$$a = bc, b = ah, \text{ con } h \in D^* \Rightarrow b = bch \Rightarrow 1 = ch \Rightarrow c \in U(D),$$

ció é l'asserto.  $\diamond$

**ESERCIZIO 8.1.13** Siano  $a, b, c$  elementi di  $D$  diversi da zero tali che  $a = bc$ . Provare che, se  $b$  é associato ad  $a$ , allora  $c$  é invertibile.

**PROPOSIZIONE 8.1.14** Se  $a \in D$  é irriducibile e  $b \in D$  é associato ad  $a$ , allora  $b$  é irriducibile.

**DIMOSTRAZIONE.** Basta osservare che  $a$  e  $b$  hanno gli stessi divisori.  $\diamond$

**PROPOSIZIONE 8.1.15** Se  $a \in D$  é primo, allora é irriducibile.

**DIMOSTRAZIONE.** Se  $a = bc$ , sappiamo che  $a|b$  o  $a|c$ . Se per esempio supponiamo che  $a|c$ , abbiamo che  $a$  e  $c$  sono associati ( $a = bc \Rightarrow c|a$ ) e risulta:

$$a|c \Rightarrow c = ad \Rightarrow a = bc = bad = abd \Rightarrow bd = 1 \Rightarrow b \in U(D) \Rightarrow b \text{ é invertibile.}$$

Così  $b$  e  $c$  sono divisori banali di  $a$  e l'asserto é provato.  $\diamond$

**OSSERVAZIONE 8.1.16** A differenza di quanto accade nell'anello degli interi, la proposizione precedente non é in generale invertibile. Esistono, infatti, domini di integrità contenenti elementi irriducibili che non sono primi, come mostra l'esempio che segue. Il teorema 8.1.18 fornisce invece una classe di domini, gli anelli principali, in cui ogni elemento irriducibile é anche primo.  $\diamond$

**ESEMPIO 8.1.17** Consideriamo l'estensione quadratica  $Z[\sqrt{-3}]$  di  $Z$  (cfr.par.7.3.2) cioè il dominio d'integrità

$$Z[\sqrt{-3}] = (\{a + b\sqrt{-3} : a, b \in Z\}, +, \cdot)$$

e ricordiamo che la funzione norma  $n$  (cfr.7.3.32) é definita da:

$$n(a + b\sqrt{-3}) = |a^2 - (-3)b^2| = a^2 + 3b^2.$$

L'elemento  $z = 1 + \sqrt{-3}$  é irriducibile in  $Z[\sqrt{-3}]$ . Infatti si ha

$$z = xy, \quad x, y \notin U(D) \Rightarrow n(xy) = n(x)n(y) = 4$$

e quindi  $n(x) = n(y) = 2$ ; ciò é assurdo perché non esistono due interi  $a, b$  tali che  $a^2 + 3b^2 = 2$ . Ne segue che, se  $z = xy$ , allora o  $x$  o  $y$  deve essere invertibile, cioè  $z$  é irriducibile.

Ora osserviamo che é

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2 \cdot 2$$

e quindi  $z|2 \cdot 2$ . Ora, se  $z$  fosse primo dovrebbe dividere 2 e si avrebbe

$$\begin{aligned} z|2 &\Rightarrow \text{esistono due interi } a, b \text{ tali che } 2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (a + b)\sqrt{-3} \\ &\Rightarrow a - 3b = 2 \text{ e } a + b = 0 \Rightarrow a, b \notin Z \end{aligned}$$

e ciò é assurdo. Abbiamo così che  $z$  non é primo in  $Z[\sqrt{-3}]$ .  $\diamond$

**PROPOSIZIONE 8.1.18** Un elemento  $a$  di un anello principale  $D$  é irriducibile se, e soltanto se, é primo.

**DIMOSTRAZIONE.** Dobbiamo soltanto provare che, se  $a$  é irriducibile, allora é anche primo. Supponiamo, dunque,  $a$  irriducibile e  $a|bc$ . Consideriamo l'ideale

$$I = (a, b) = \{ax + by \quad : \quad x, y \in D\}$$

e osserviamo che, essendo  $D$  principale, possiamo porre  $I = (d)$ , con  $d$  opportuno elemento di  $I$ .

Poiché  $a \in I$ , abbiamo  $a = dr$  e, essendo  $a$  irriducibile, uno tra gli elementi  $d$  e  $r$  deve essere invertibile. Allora:

•  $d \in U(D) \Rightarrow I = D \Rightarrow$  esistono  $x, y \in D$  tali che  $1 = ax + by \Rightarrow c = acx + bcy$  ( $a|bc$ )  $\Rightarrow a|c$ .

•  $r \in U(D) \Rightarrow (a) = (d) = I$  (e sappiamo che  $b \in I$ )  $\Rightarrow b = at \Rightarrow a|b$ .

L'asserto é così provato.  $\diamond$

**ESERCIZIO 8.1.19** *Un elemento  $a \in D$  é primo se, e soltanto se, l'ideale principale  $(a)$  é un ideale primo.*

**DEFINIZIONE 8.1.20** Siano  $a, b$  due elementi di un dominio di integritá unitario  $D$ . Un elemento  $d \in D$  si dice *massimo comune divisore* di  $a$  e  $b$  se  $d$  divide  $a$  e  $b$  e se ogni divisore di  $a$  e  $b$  é anche un divisore di  $d$ .  $\diamond$

Osserviamo che due elementi di  $D$  risultano entrambi massimo comune divisore di  $a$  e  $b$  se, e soltanto se, sono associati. Se  $1$  é un massimo comune divisore di  $a$  e  $b$ , allora  $a$  e  $b$  si dicono *coprime*.

**ESERCIZIO 8.1.21** *Provare che, se un massimo comune divisore di due elementi  $a, b$  di  $D$  é invertibile, allora  $a$  e  $b$  sono coprime.*

**TEOREMA 8.1.22** *Siano  $D$  un anello principale e  $a, b$  due suoi elementi non nulli. Allora esiste in  $D$  un massimo comune divisore  $d$  di  $a$  e  $b$ . Inoltre, esistono  $x, y \in D$  tali che*

$$d = xa + yb \quad (\text{identitá di Bezout}).$$

**DIMOSTRAZIONE.** Consideriamo l'ideale generato da  $a$  e  $b$

$$I = (a, b) = \{ua + vb : u, v \in D\}.$$

Essendo  $D$  principale, esiste  $d \in D$  tale che  $I = (d) = \{td : t \in D\}$  ed é  $d = xa + yb$ , con  $x, y$  opportuni elementi di  $D$ . Abbiamo allora che  $d$  é un divisore comune di  $a$  e  $b$  in quanto  $a$  e  $b$ , appartenendo a  $(d)$ , sono multipli di  $d$ . D'altra parte, se  $c$  é un divisore comune di  $a$  e  $b$ , allora  $c$  divide  $xa + yb = d$  e l'asserto é completamente provato.  $\diamond$

Il corollario seguente discende direttamente dalla dimostrazione del teorema 8.1.22.

**COROLLARIO 8.1.23** *Siano  $D$  un anello principale e  $a, b$  due suoi elementi non nulli. Allora un elemento  $d \in D$  é un massimo comune divisore di  $a$  e  $b$  se, e solo se,  $d$  é un generatore dell'ideale  $(a, b)$ .*

**ESERCIZIO 8.1.24** *Dare la definizione di minimo comune multiplo e provare che in un anello principale i minimi comuni multipli di due elementi non nulli  $a, b$  sono tutti e soli i generatori dell'ideale  $(a) \cap (b)$ .*

## 8.2 Divisibilitá in anelli di polinomi

La teoria della divisibilitá fin qui svolta puó applicarsi all'anello dei polinomi a coefficienti in un dominio di integritá unitario che, come sappiamo, é a sua volta un dominio di integritá unitario.

**ESERCIZIO 8.2.1** *Sia  $D$  un dominio di integritá unitario,  $c \in D$  una costante non nulla e  $f \in D[x]$  un polinomio che divide  $c$ . Allora  $f$  é costante.*

**PROPOSIZIONE 8.2.2** *Sia  $D$  un dominio di integritá unitario. Allora l'insieme degli elementi invertibili di  $D[x]$  coincide con l'insieme  $U(D)$  degli elementi invertibili di  $D$ .*

**DIMOSTRAZIONE.** Poich   $D$  e  $D[x]$  hanno la stessa unit , abbiamo  $U(D) \subseteq U(D[x])$ . D'altra parte abbiamo:

$$f \in U(D[x]) \Rightarrow \text{esiste } g \in D[x] \text{ tale che } fg = 1 \Rightarrow f|1 \text{ e } g|1.$$

Ne segue che  $f, g$  sono costanti non nulle e, quindi, elementi invertibili in  $D$ .  $\diamond$

**OSSERVAZIONE 8.2.3** Le due precedenti propriet  non sono in generale vere se  $D$  non   un dominio di integrit . Per esempio, in  $Z_4[x]$  abbiamo

$$(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1 \Rightarrow (2x + 1)^{-1} = 2x + 1,$$

cio   $2x + 1$ , che non   una costante, divide la costante 1 ed   invertibile.  $\diamond$

**PROPOSIZIONE 8.2.4** *Siano  $f, g$  due polinomi non nulli associati a coefficienti in un dominio di integrit  unitario  $D$ . Allora  $f$  e  $g$  hanno lo stesso grado.*

**DIMOSTRAZIONE.** Abbiamo:

$$g = fh \text{ e } f = gh' \Rightarrow f = fh'h' \Rightarrow hh' = 1$$

$$\Rightarrow h \text{   una costante non nulla } \Rightarrow \deg(f) = \deg(g).$$

$\diamond$

**OSSERVAZIONE 8.2.5** Anche la precedente proposizione non   in generale invertibile, nel senso che polinomi dello stesso grado possono non essere associati. Per esempio in  $Z[x]$  i polinomi  $x^2$  e  $5x^2$  non sono associati. Osserviamo che, nel caso  $D$  sia un campo, abbiamo:

$$f, g \neq 0, f \sim g \Leftrightarrow f = ag, a \in U(D) = D^*,$$

cos  , per esempio,  $x^2$  e  $5x^2$  sono associati in  $Q[x]$ .  $\diamond$

**ESERCIZIO 8.2.6** *Sia  $K$  un campo. Generalizzare al caso dei polinomi su  $K$  l'algoritmo di Euclide delle divisioni successive per il calcolo di un massimo comune divisore.*

**OSSERVAZIONE 8.2.7** Chiudiamo questo paragrafo facendo notare che l'anello dei polinomi su un anello principale pu  non essere principale. Un esempio a proposito   dato dall'anello  $Z$  degli interi. Consideriamo infatti in  $Z[x]$  l'ideale

$$I = \{2b + xa(x) \quad : \quad a(x) \in Z[x], b \in Z\}$$

e supponiamo  $I = (h(x))$ . In queste ipotesi abbiamo

$$2 = h(x)f(x) \quad \text{e} \quad x = h(x)g(x);$$

$$0 = \deg(2) = \deg(h) + \deg(f) \Rightarrow \deg(h) = \deg(f) = 0 \Rightarrow h, f \in Z.$$

D'altra parte

$$2 = hf \Rightarrow h = \pm 1 \quad \text{oppure} \quad h = \pm 2$$

e, poich   $1 \notin I$ , deve essere  $h = \pm 2$ . Le ultime uguaglianze implicano che  $x = \pm 2g(x)$ , che   un assurdo; cos   $I$  non pu  essere principale.  $\diamond$

### 8.3 Radici di un polinomio

Sia  $A$  un anello commutativo unitario e

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

un polinomio di grado  $n$  a coefficienti in  $A$ .

**DEFINIZIONE 8.3.1** Un'equazione del tipo  $f(x) = 0$  si chiama *equazione algebrica di grado  $n$*  e un elemento  $c \in A$  si dice *radice* o *zero* di  $f$  se risulta  $f(c) = 0$ .  $\diamond$

**PROPOSIZIONE 8.3.2 (teorema del resto)** *Siano  $f$  un polinomio a coefficienti in un anello commutativo unitario  $A$  e  $c$  un elemento di  $A$ . Allora esiste un unico polinomio  $q \in A[x]$  tale che  $f = (x - c)q + f(c)$ .*

**DIMOSTRAZIONE.** Poiché  $(x - c)$  ha coefficiente direttore 1, che é invertibile in  $A$ , possiamo dividere  $f$  per  $(x - c)$  (cfr.7.3.9) e da ciò segue facilmente l'asserto.  $\diamond$

Il teorema del resto ha i seguenti due corollari di dimostrazione immediata.

**COROLLARIO 8.3.3 (teorema di Ruffini)** *Sia  $f$  un polinomio a coefficienti in anello commutativo unitario  $A$ . Allora  $c$  é una radice di  $f$  se, e solo se,  $(x - c)$  divide  $f$ .*

**COROLLARIO 8.3.4** *Siano*

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

*un polinomio di grado positivo  $n$  a coefficienti in un anello commutativo unitario  $A$ , e*

$$q(x) = q_0 + q_1x + q_2x^2 + \dots + q_{n-1}x^{n-1}$$

*il quoziente della divisione di  $f$  per  $(x - c)$ ,  $c \in A$ . Allora risulta:*

$$q_{n-1} = a_n, q_{n-2} = a_{n-1} + cq_{n-1}, \dots, q_1 = a_2 + cq_2, q_0 = a_1 + cq_1, a_0 + cq_0 = f(c).$$

**OSSERVAZIONE 8.3.5** Il corollario 8.3.4 permette di semplificare l'algoritmo della divisione di  $f$  per  $(x - c)$ . Si può infatti eseguire sinteticamente questa divisione usando lo schema seguente

	$a_n$	$a_{n-1}$	$\dots$	$a_1$	$a_0$
$c$		$cq_{n-1}$	$\dots$	$cq_1$	$cq_0$
	$a_n = q_{n-1}$	$a_{n-1} + cq_{n-1} = q_{n-2}$	$\dots$	$a_1 + cq_1 = q_0$	$a_0 + cq_0 = f(c)$

Per esempio, lo schema da usare per trovare il quoziente  $q(x)$  e il resto  $r(x)$  della divisione fra  $x^3 - 3x^2 + 7x - 10$  e  $x - 4$  é

	1	-3	7	-10
4		4	4	44
	1	1	11	34

da cui si ricava  $q(x) = x^2 + x + 11$  e  $r(x) = 34$ .  $\diamond$

**PROPOSIZIONE 8.3.6** *Siano  $D$  un dominio di integritá unitario,  $f \in D[x]$  e  $c_1, c_2, \dots, c_n$  radici a due a due distinte di  $f$ . Allora*

$$(x - c_1)(x - c_2) \cdots (x - c_n) \text{ divide } f.$$

**DIMOSTRAZIONE.** Per  $n = 1$  l'asserto é vero, riducendosi al teorema di Ruffini. Se supponiamo  $n > 1$  e procediamo per induzione su  $n$ , abbiamo:

$$\begin{aligned} f &= (x - c_1)q \text{ e, per ogni } i > 1, f(c_i) = (c_i - c_1)q(c_i) = 0 \\ \Rightarrow q(c_i) &= 0 \Rightarrow q = (x - c_2)(x - c_3) \cdots (x - c_n)h, h \in D[x] \\ &\Rightarrow f = (x - c_1)(x - c_2) \cdots (x - c_n)h. \end{aligned}$$

L'asserto é cosí completamente provato.  $\diamond$

**COROLLARIO 8.3.7** *Siano  $D$  un dominio di integritá unitario,  $f \in D[x]$  e  $\deg(f) = n > 0$ . Allora  $f$  possiede al piú  $n$  radici in  $D$ .*

**DIMOSTRAZIONE.** Se  $c_1, c_2, \dots, c_m$  sono radici distinte di  $f$  abbiamo

$$(x - c_1)(x - c_2) \cdots (x - c_m) \mid f \Rightarrow m \leq \deg(f),$$

cioé l'asserto.  $\diamond$

**OSSERVAZIONE 8.3.8** Nelle due proposizioni precedenti, l'ipotesi che  $D$  sia dominio di integritá é essenziale. Per esempio, se consideriamo il polinomio

$$f(x) = x^2 + x \in \mathbb{Z}_6[x],$$

abbiamo:

- $f(0) = f(3) = 0$  e  $f$  non é del tipo  $f(x) = x(x - 3)g(x)$ ;
- oltre alle radici 0 e 3,  $f$  ha anche le radici 2 e 5.  $\diamond$

**ESERCIZIO 8.3.9** *Trovare in  $\mathbb{Z}_6$  tutte le radici del polinomio  $x^2 + 2x + 4$ .*

**ESERCIZIO 8.3.10** *Provare che nel campo  $\mathbb{Z}_p$ ,  $p$  primo, 1 e  $p - 1$  sono gli unici elementi che coincidono col proprio inverso.*

**TEOREMA 8.3.11 (principio di identitá dei polinomi)** *Se  $D$  é un dominio di integritá unitario infinito, allora in  $D[x]$  vale il principio di identitá dei polinomi; cioé, se  $f, g \in D[x]$ , allora  $f = g$  se, e solo se, la funzione polinomiale di  $f$  é uguale a quella di  $g$ .*

**DIMOSTRAZIONE.** La prima implicazione é ovvia. Per la seconda, se supponiamo  $f \neq g$ , abbiamo:

$$\begin{aligned} \bar{f} = \bar{g} &\Rightarrow f(a) = g(a) \text{ per ogni } a \in D \\ \Rightarrow (f - g)(a) &= f(a) - g(a) = 0 \text{ per ogni } a \in D \\ \Rightarrow \text{possiamo trovare in } D &\text{ un numero di radici di } f - g \text{ maggiore di } \deg(f - g) \\ \Rightarrow f - g = 0 &\Rightarrow f = g \Rightarrow \text{assurdo.} \end{aligned}$$

$\diamond$

## 8.4 Polinomi irriducibili e primi

Sia  $D$  un dominio di integritá unitario.

**DEFINIZIONE 8.4.1** Sia  $f$  un polinomio non nullo a coefficienti in  $D$ . Si dice che  $f$  é *irriducibile* su  $D$  se  $f$  é un elemento irriducibile di  $D[x]$ , cioè se non é invertibile in  $D[x]$  e

$$f = gh \text{ con } g, h \in D[x] \Rightarrow g \text{ o } h \text{ e' invertibile in } D[x].$$

Se  $f$  non é irriducibile, si dice *riducibile*.

Analogamente, si dice che  $f$  é *primo* su  $D$  se  $f$  é un elemento primo di  $D[x]$ , cioè se non é invertibile in  $D[x]$  e

$$f | gh \text{ con } g, h \in D[x] \Rightarrow f | g \text{ o } f | h.$$

◇

**PROPOSIZIONE 8.4.2** Sia  $K$  un campo. Allora un polinomio  $f \in K[x]$  é irriducibile su  $K$  se, e solo se, é un elemento primo dell'anello  $K[x]$ .

**DIMOSTRAZIONE.** L'anello  $K[x]$  é principale, cosí l'asserto segue dalla prop.8.1.18. ◇

**TEOREMA 8.4.3** Siano  $K$  un campo e  $f \in K[x]$ . Allora  $(f)$  é un ideale massimale in  $K[x]$  se, e soltanto se,  $f$  é irriducibile su  $K$ .

**DIMOSTRAZIONE.** Supponiamo  $(f)$  massimale in  $K[x]$  e  $f = gh$  con  $g, h \in K[x]$ . In queste ipotesi abbiamo  $(f) \subseteq (g)$  e quindi

$$(f) = (g) \text{ oppure } (g) = K[x].$$

Nel primo caso abbiamo  $\deg(f) = \deg(g)$  e  $h$  é una costante. Nel secondo caso  $g$  é una costante e  $\deg(f) = \deg(h)$ . Ne segue che  $f$  é irriducibile.

Supponiamo ora  $f$  irriducibile e sia  $I = (g)$  un ideale di  $K[x]$  che contiene  $(f)$ . Allora esiste  $h \in K[x]$  tale che  $f = gh$  e, essendo  $f$  irriducibile abbiamo

$$g = \text{costante} \text{ oppure } h = \text{costante}.$$

Nel primo caso risulta  $I = K[x]$ , nel secondo  $(f) = (g)$ . Ne segue che  $I$  é massimale. ◇

**ESERCIZIO 8.4.4** Sia  $K$  un campo. Provare che ogni polinomio di grado positivo a coefficienti in  $K$  é prodotto di polinomi irriducibili su  $K$ .

**PROPOSIZIONE 8.4.5** Sia  $D$  un dominio di integritá unitario. Allora  $x$  é un elemento primo in  $D[x]$ .

**DIMOSTRAZIONE.** Supponiamo  $x | fg$ , con  $f, g \in D[x]$  e

$$f(x) = a_0 + a_1x + \dots, \quad g(x) = b_0 + b_1 + \dots.$$

Allora, deve essere  $a_0b_0 = 0$  e essendo  $D$  un dominio di integritá, abbiamo  $a_0 = 0$  o  $b_0 = 0$ . Nel primo caso  $x | f$ , nel secondo  $x | g$  e resta cosí provato che  $x$  é primo. ◇

**PROPOSIZIONE 8.4.6** *Sia  $D$  un dominio di integritá unitario tale che  $(x)$  sia un ideale massimale di  $D[x]$ . Allora  $D$  é un campo.*

**DIMOSTRAZIONE.** Sia  $a \in D^*$  e osserviamo che

$$a \notin (x) = \{xf(x) : f \in D[x]\}$$

e quindi  $(x)$  é propriamente contenuto nell'ideale  $(a, x)$ , pertanto deve essere  $(a, x) = A[x]$ . Allora devono esistere due polinomi

$$h(x) = h_0 + h_1x + \dots \quad e \quad k(x) = k_0 + k_1x + \dots$$

tali che  $1 = ah(x) + xk(x)$ , da cui segue che  $ah_0 = 1$ , cioè  $a$  é invertibile.  $\diamond$

**PROPOSIZIONE 8.4.7** *Sia  $A$  un anello commutativo unitario tale che  $A[x]$  sia principale. Allora  $A$  é un campo.*

**DIMOSTRAZIONE.**  $A$  é sottoanello di  $A[x]$  e quindi é un dominio di integritá. Allora l'ideale principale  $(x)$ , essendo  $x$  primo e  $A[x]$  principale, risulta massimale in  $A[x]$ . Ne segue che  $A$  é un campo.  $\diamond$

**ESERCIZIO 8.4.8** *Provare che un polinomio di primo grado a coefficienti in un campo  $K$  ha una radice in  $K$  ed é ivi irriducibile.*

**PROPOSIZIONE 8.4.9** *Siano  $K$  un campo ed  $f \in K[x]$  un polinomio irriducibile di grado maggiore di 1. Allora  $K$  non contiene radici di  $f$ .*

**DIMOSTRAZIONE.** Supponiamo per assurdo che  $K$  contenga una radice  $c$  di  $f$ . Allora avremo:

$$f = (x - c)q \Rightarrow \deg(f) = 1 + \deg(q) > 1 \Rightarrow \deg(q) > 0 \Rightarrow f \text{ riducibile,}$$

un assurdo.  $\diamond$

**ESERCIZIO 8.4.10** *Provare che:*

- il polinomio  $x^2 - 2$  é irriducibile su  $\mathbb{Q}$  e riducibile su  $\mathbb{R}$ ;
- il polinomio  $x^2 + 4$  é irriducibile su  $\mathbb{R}$  e su  $\mathbb{Q}$ .

**OSSERVAZIONE 8.4.11** In generale, la proposizione 8.4.9 non si puó invertire; per esempio il polinomio  $(x^2 - 2)(x^2 - 3)$ , pur essendo riducibile sul campo  $\mathbb{Q}$  dei razionali, non ha radici razionali. Essa puó invece invertirsi nel caso dei gradi 2 e 3.  $\diamond$

**PROPOSIZIONE 8.4.12** *Siano  $K$  un campo,  $f \in K[x]$  di grado 2 o 3 e si supponga che  $f$  non abbia radici in  $K$ . Allora  $f$  é irriducibile su  $K$ .*

**DIMOSTRAZIONE.** Supponiamo per assurdo che  $f$  sia riducibile. Allora

$$f = gh \text{ con } \deg(g) > 0 \text{ e } \deg(h) > 0 \Rightarrow \deg(f) = \deg(g) + \deg(h) \in \{2, 3\}$$

$$\Rightarrow g \text{ o } h \text{ ha grado uguale ad 1, per esempio } g$$

$$\Rightarrow \text{esiste } c \in K \text{ tale che } g(c) = 0 \Rightarrow f(c) = 0,$$

un assurdo.  $\diamond$

Figura 8.1: L.Euler (1707-1783)

**ESERCIZIO 8.4.13** Sia  $K$  un campo. Provare che un polinomio  $f \in K[x]$  di grado 2 o 3 è riducibile su  $K$  se, e solo se,  $f$  ha una radice in  $K$ .

**DEFINIZIONE 8.4.14** Siano  $F$  e  $K$  due campi con  $K$  sottocampo di  $F$ . Detto  $a$  un elemento di  $F$ , possiamo considerare l'ideale  $I_a = I_a(K)$  di  $K[x]$  definito da

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

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  $I_a$  (cfr.7.3.15) si chiama anche *polinomio minimo* di  $a$  su  $K$ ; in altre parole  $p(x)$  è l'unico polinomio monico tra tutti i polinomi in  $K[x]$  di grado minimo che si annullano su  $a$ .

Figura 8.2: C.Hermite (1822-1901)

**PROPOSIZIONE 8.4.15** Siano  $K$  un sottocampo del campo  $F$  e  $a \in F$  un elemento algebrico su  $K$ . Allora il polinomio minimo  $p(x)$  di  $a$  su  $K$  è irriducibile e, di conseguenza,  $I_a$  è 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.  $\diamond$

Figura 8.3: C.L.F.von Lindemann (1852-1939)

**ESEMPI 8.4.16** Riportiamo alcuni esempi di numeri reali trascendenti<sup>1</sup> sul campo razionale.

$$\bullet \quad 0, 1010010000001 \underbrace{0\dots 0}_4 1 \underbrace{0\dots 0}_5 1 \underbrace{0\dots 0}_6 \dots$$

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

- $e$  = base dei logaritmi naturali.

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

- $\pi$  = 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 e  $b$  é irrazionale, allora  $a^b$  é trascendente. Per esempio,  $2^{\sqrt{2}}$  é trascendente.  $\diamond$

**ESERCIZIO 8.4.17** Siano  $K$  un sottocampo del campo  $F$  e  $a \in F$  un elemento algebrico su  $K$ . Provare che ogni elemento di  $K$  é algebrico su  $K$  e che l'elemento  $a$  appartiene a  $K$  se, e solo se, il polinomio minimo di  $a$  su  $K$  é  $(x - a)$ .

**ESERCIZIO 8.4.18** 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.

<sup>1</sup>La 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.

Figura 8.4: J.Liouville (1809-1882)

## 8.5 Polinomi irriducibili su $Q$ e $Z$

**DEFINIZIONE 8.5.1** Un polinomio  $f \in Z[x]$  si dice *primitivo* se il massimo comune divisore dei suoi coefficienti non nulli é 1.  $\diamond$

**PROPOSIZIONE 8.5.2 (lemma di Gauss)** *Il prodotto di due polinomi primitivi é un polinomio primitivo.*

**DIMOSTRAZIONE.** Siano  $f, g \in Z[x]$  primitivi e supponiamo per assurdo che  $fg$  non lo sia. Esiste allora un primo  $p$  che divide il massimo comune divisore dei coefficienti non nulli di  $fg$  e possiamo considerare i polinomi  $\bar{f}, \bar{g}, \bar{f}\bar{g} \in Z_p[x]$  riducendo modulo  $p$  i coefficienti di  $f, g, fg$ .

Dall'essere  $Z_p[x]$  un dominio di integritá, avendosi  $\bar{f}\bar{g} = \overline{fg} = 0$ , ricaviamo che o  $\bar{f} = 0$  oppure  $\bar{g} = 0$ . Ne segue che  $p$  divide tutti i coefficienti di  $f$  oppure tutti i coefficienti di  $g$  e ció é assurdo.  $\diamond$

**TEOREMA 8.5.3** *Sia  $f \in Z[x]$ . Se  $f$  é riducibile su  $Q$ , allora é riducibile anche su  $Z$ .*

**DIMOSTRAZIONE.** Supponiamo  $f = gh$  con  $g, h \in Q[x]$  e osserviamo che non é restrittivo supporre che  $f$  sia primitivo<sup>2</sup>.

- Denotiamo con  $a$  un minimo comune multiplo dei denominatori dei coefficienti di  $g$  e con  $b$  quello dei denominatori dei coefficienti di  $h$ . Allora,  $abf = (ag)(bh)$ , e  $ag, bh \in Z[x]$ .

- Denotiamo con  $c_1$  il *MCD* dei coefficienti di  $ag$  e con  $c_2$  quello dei coefficienti di  $bh$ . Allora,  $ag = c_1g_1$  e  $bh = c_2h_1$ , ove  $g_1, h_1 \in Z[x]$ , sono polinomi primitivi, e abbiamo

$$abf = c_1c_2g_1h_1.$$

- Poiché  $f$  é primitivo, il massimo comune divisore dei coefficienti di  $abf$  é  $ab$ . Analogamente, poiché  $g_1h_1$  é primitivo (per il lemma di Gauss), il massimo comune divisore dei coefficienti di  $c_1c_2g_1h_1$  é  $c_1c_2$ . Ne segue che

$$ab = c_1c_2.$$

---

<sup>2</sup>In caso contrario basta dividere i membri dell'uguaglianza  $f = gh$  per un massimo comune divisore dei coefficienti di  $f$ .

- Possiamo ora concludere che é

$$f = g_1 h_1 \quad \text{con} \quad g_1 h_1 \in Z[x]$$

e l'asserto é dimostrato.  $\diamond$

**OSSERVAZIONE 8.5.4** Notiamo che la proposizione precedente non può invertirsi. Per esempio, il polinomio  $5(x^2 + 1)$  é riducibile su  $Z$ , perché  $5$  e  $x^2 + 1$  sono elementi irriducibili di  $Z[x]$ , ma é irriducibile su  $Q$ .  $\diamond$

**ESERCIZIO 8.5.5** Sia  $f(x) \in Z[x]$  un polinomio primitivo. Provare che  $f(x)$  é irriducibile su  $Z$  se, e solo se, é irriducibile su  $Q$ .

Figura 8.5: F.Gauss (1777-1855)

**TEOREMA 8.5.6 (criterio di Eisenstein)** Sia

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n$$

un polinomio a coefficienti interi ed esista un primo  $p$  tale che

$$p|a_0, p|a_1, \dots, p|a_{n-1}; \quad p \nmid a_n; \quad p^2 \nmid a_0.$$

Allora  $f$  é irriducibile su  $Q$ .

**DIMOSTRAZIONE.** Supponiamo per assurdo  $f$  riducibile su  $Q$  e quindi su  $Z$ , per cui abbiamo

$$f = gh \quad \text{con} \quad g, h \in Z[x], \quad 1 \leq \deg(g), \deg(h) < n.$$

Poniamo

$$g(x) = b_0 + \cdots + b_r x^r \quad \text{e} \quad h(x) = c_0 + \cdots + c_s x^s.$$

- $p$  divide uno soltanto degli interi  $b_0, c_0$  perché  $p|a_0 = b_0 c_0$  e  $p^2 \nmid a_0$ . Supponiamo

$$p|b_0 \quad \text{e} \quad p \nmid c_0.$$

Inoltre

$$p \nmid b_r$$

perché  $p \nmid a_n = b_r c_s$ .

- Sia  $t$  il piú piccolo intero tale che  $p \nmid b_t$  e osserviamo che  $t > 0$ . Il coefficiente

$$a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_1 c_{t-1} + b_0 c_t$$

non é divisibile per  $p$  perché  $b_t c_0$  non é divisibile per  $p$ , mentre tutti gli altri addendi lo sono. Allora deve essere  $t = n$ . Questo significa che  $g$  ha grado  $n$  e ciò é assurdo.  $\diamond$

Figura 8.6: F.G.M.Eisenstein (1823-1852)

**ESERCIZIO 8.5.7** *Sia  $n$  un intero positivo. Provare che il polinomio  $x^n - 2$  é irriducibile sul campo razionale e riducibile su quello reale.*

**ESERCIZIO 8.5.8** *Siano  $n$  un intero maggiore di 1 e  $a_n$  un numero reale radice  $n$ -esima di 2, cioè  $(a_n)^n = 2$ . Provare che  $a_n$  é un elemento algebrico sul campo razionale e che  $x^n - 2$  é il suo polinomio minimo su  $Q$ .*

**TEOREMA 8.5.9** *Siano  $p$  un primo e  $f \in Z[x]$  con  $\deg(f) > 0$ . Sia  $\bar{f} \in Z_p[x]$  il polinomio ottenuto da  $f$  riducendo i suoi coefficienti modulo  $p$ . Allora, se  $\bar{f}$  é irriducibile su  $Z_p$  e  $\deg(\bar{f}) = \deg(f)$ , il polinomio  $f$  é irriducibile su  $Q$ .*

**DIMOSTRAZIONE.** Supponiamo per assurdo  $f$  riducibile su  $Q$  e quindi su  $Z$ , per cui abbiamo

$$f = gh \quad \text{con} \quad g, h \in Z[x], \quad 1 \leq \deg(g), \deg(h) < \deg(f).$$

Riducendo modulo  $p$  i coefficienti di  $f, g, h$ , in  $Z_p[x]$  otteniamo

$$\bar{f} = \bar{g}\bar{h}$$

e, essendo  $\deg(f) = \deg(\bar{f})$ , deve essere

$$\deg(\bar{g}) = \deg(g) < \deg(\bar{f}), \quad \deg(\bar{h}) = \deg(h) < \deg(\bar{f}).$$

Quanto provato é assurdo perché  $\bar{f}$  é irriducibile su  $Z_p$ .  $\diamond$

**OSSERVAZIONE 8.5.10** Se  $\bar{f}$  é riducibile su  $Z_p$ , per qualche primo  $p$ , non é detto che  $f$  sia riducibile su  $Q$ . Per esempio, prendiamo

$$f(x) = 21x^3 - 3x^2 + 2x + 8 \in Z[x].$$

Se riduciamo  $f$  modulo 2 otteniamo il polinomio

$$\bar{f}(x) = x^3 + x^2 = x^2(x + 1)$$

riducibile su  $Z_2$ . Se riduciamo  $f$  modulo 5 otteniamo il polinomio

$$\bar{f}(x) = x^3 + 2x^2 + 2x + 3$$

il quale, essendo di terzo grado e non avendo radici in  $Z_5$ , é irriducibile su  $Z_5$ . Da ciò segue che  $f$  é irriducibile su  $Q$ .  $\diamond$

### 8.5.1 Irriducibilità di polinomi ciclotomici

Se  $p$  é un primo positivo, il polinomio

$$\xi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

si chiama  $p$ -esimo polinomio ciclotomico.

**TEOREMA 8.5.11** Per ogni primo  $p$ , il  $p$ -esimo polinomio ciclotomico é irriducibile su  $Q$ .

**DIMOSTRAZIONE.** Il polinomio

$$\begin{aligned} f(x) = \xi_p(x + 1) &= \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{(x + 1)^p - 1}{x} \\ &= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + p \end{aligned}$$

é irriducibile su  $Q$  per il criterio di Eisenstein. Supponiamo che esista una fattorizzazione non banale

$$\xi_p(x) = g(x)h(x)$$

di  $\xi_p(x)$  su  $Q$ . Allora

$$f(x) = \xi_p(x + 1) = g(x + 1)h(x + 1)$$

é una fattorizzazione non banale su  $Q$  di  $f$  e ciò é assurdo. Ne segue che il polinomio  $\xi_p(x)$  é irriducibile su  $Q$ .  $\diamond$

**ESERCIZIO 8.5.12** Sia  $p$  un intero primo positivo. Tenendo presente che

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$$

provare che non esiste alcun numero reale algebrico su  $Q$  e avente come polinomio minimo il polinomio ciclotomico  $\xi_p(x)$ .

## 8.6 Fattorizzazione unica in $Z[x]$

**TEOREMA 8.6.1** Sia  $f(x) \in Z[x]$  un polinomio non nullo diverso da  $-1$  e da  $1$ . Allora  $f(x)$  può essere scritto nella forma

$$f(x) = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x), \quad (8.1)$$

ove i  $b_i$  sono numeri primi e i  $p_i(x)$  sono polinomi irriducibili in  $Z[x]$ .

**DIMOSTRAZIONE.** Osserviamo che, se  $\deg(f) = 0$ , allora  $f$  é costante e il teorema segue dal teorema fondamentale dell'aritmetica. Possiamo quindi supporre  $\deg(f) > 0$ .

Osserviamo ora che se  $b$  é il massimo comune divisore dei coefficienti di  $f(x)$  e se  $b_1 b_2 \cdots b_s$  é la fattorizzazione in primi di  $b$ , possiamo scrivere  $f(x) = b_1 b_2 \cdots b_s f_1(x)$ , dove  $f_1 \in Z[x]$  é primitivo e ha grado positivo. Ne segue che, per provare il teorema, possiamo supporre che  $f(x)$  sia primitivo.

In queste ipotesi, se  $\deg(f) = 1$ ,  $f(x)$  é irriducibile e il teorema é vero; possiamo quindi procedere per induzione sul grado  $n$  di  $f(x)$ .

Se  $n > 1$  e  $f(x)$  é irriducibile non abbiamo nulla da provare; supponiamo dunque che  $f(x)$  sia riducibile, cioè  $f(x) = g(x)h(x)$ , ove  $g(x), h(x)$  sono primitivi e di grado minore di quello di  $f(x)$ . Allora, per induzione,  $g(x)$  e  $h(x)$  possono scriversi ciascuno come prodotto di polinomi irriducibili di grado positivo e l'asserto é provato.  $\diamond$

**DEFINIZIONE 8.6.2** Una decomposizione di  $f$  del tipo (8.1) si chiama *fattorizzazione di  $f$  in polinomi irriducibili*.

**TEOREMA 8.6.3** Siano

$$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$$

e

$$c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x)$$

due fattorizzazioni di  $f(x) \in Z[x]$  in polinomi irriducibili. Allora risulta  $s = t$ ,  $m = n$  ed esistono una permutazione  $\sigma \in S_s$  e una  $\tau \in S_m$  tali che

$$b_1 = \pm c_{\sigma(1)}, \dots, b_s = \pm c_{\sigma(s)}, \quad p_1(x) = \pm q_{\tau(1)}(x), \dots, p_m(x) = \pm q_{\tau(m)}(x).$$

**DIMOSTRAZIONE.** Poniamo  $b = b_1 \cdots b_s$ ,  $c = c_1 \cdots c_t$ . Poiché i  $p_j(x)$  e  $q_j(x)$  sono primitivi, per il lemma di Gauss, anche  $p_1(x)p_2(x) \cdots p_m(x)$  e  $q_1(x)q_2(x) \cdots q_n(x)$  sono primitivi. Ne segue che  $b$  e  $c$  sono uguali ad un massimo comune divisore dei coefficienti di  $f(x)$  e di conseguenza hanno lo stesso valore assoluto. Allora il teorema fondamentale dell'aritmetica assicura l'esistenza della permutazione  $\sigma$  con la proprietà desiderata.

A questo punto possiamo scrivere in  $Z[x]$

$$p_1(x)p_2(x) \cdots p_m(x) = \pm q_1(x)q_2(x) \cdots q_n(x) \quad (8.2)$$

e considerare la (8.2) come un'uguaglianza fra polinomi in  $Q[x]$ . Allora, poiché i  $p_j$  e  $q_j$  sono irriducibili su  $Q$  e  $Q$  é un campo, essi sono anche primi su  $Q$ . Ne segue che esiste un indice  $\tau(1) \in \{1, 2, \dots, n\}$  tale che  $p_1(x)$  divide  $q_{\tau(1)}(x)$ , ed essendo  $p_1(x)$  e  $q_{\tau(1)}(x)$  primi e primitivi

(cfr.8.5.5), deve essere  $p_1(x) = \pm q_{\tau(1)}(x)$ . Allora eliminando questi due polinomi dalla (8.2), e supponendo per semplicità  $\tau(1) = 1$ , abbiamo

$$p_2(x)p_3(x) \cdots p_m(x) = \pm q_2(x)q_3(x) \cdots q_n(x)$$

e possiamo applicare lo stesso procedimento all'uguaglianza ottenuta.

Se fosse  $m < n$ , dopo  $m$  passi avremmo un'uguaglianza con 1 a primo membro e un polinomio non costante a secondo membro; un assurdo.

Se fosse  $m > n$ , dopo  $n$  passi avremmo un'uguaglianza con  $\pm 1$  a secondo membro e un polinomio non costante a primo membro; un assurdo. Ne segue che  $m = n$  e l'asserto é così completamente provato.  $\diamond$

## 8.7 Radici multiple di un polinomio

Sia  $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$  un polinomio a coefficienti in un anello commutativo unitario. Il polinomio

$$a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

si chiama *polinomio derivato* di  $f$  e si denota con  $Df$ .

**ESERCIZIO 8.7.1** *Provare che l'applicazione  $f \rightarrow Df$  é un endomorfismo del gruppo additivo di  $A[x]$ . Provare inoltre che*

$$D(fg) = fDg + gDf,$$

per ogni  $f, g \in A[x]$ .

**DEFINIZIONE 8.7.2** Siano  $A$  un dominio di integrità unitario e  $f \in A[x]$ . Una radice  $c$  di  $f$  si dice di *molteplicità*  $k$ , se

$$(x - c)^k | f \quad \text{e} \quad (x - c)^{k+1} \nmid f.$$

Se é  $k = 1$ , la radice  $c$  si dice *semplice*. Quando é  $k > 1$ , la radice  $c$  si dice *multipla*.  $\diamond$

**TEOREMA 8.7.3** *Siano  $A$  un dominio di integrità unitario,  $f \in A[x]$ , e  $f(c) = 0$ . Allora  $c$  é radice multipla di  $f$  se, e soltanto se,  $c$  é radice del polinomio  $Df$  derivato di  $f$ .*

**DIMOSTRAZIONE.** Se  $c$  é radice multipla di  $f$ , abbiamo:

$$\begin{aligned} f &= (x - c)^k g, \quad k > 1 \Rightarrow Df = k(x - c)^{k-1}g + (x - c)^k Dg \\ &= (x - c) [k(x - c)^{k-2}g + (x - c)^{k-1}Dg] \Rightarrow (x - c) | Df \Rightarrow c \text{ é radice di } Df. \end{aligned}$$

Se  $c$  é radice di  $f$  e  $Df$ , abbiamo:

$$\begin{aligned} f(c) = Df(c) = 0 &\Rightarrow f = (x - c)g, \quad Df = g + (x - c)Dg \\ \Rightarrow 0 = Df(c) = g(c) + (c - c)Dg(c) = g(c) &\Rightarrow g = (x - c)g_1 \\ \Rightarrow f = (x - c)g = (x - c)^2 g_1 &\Rightarrow c \text{ é radice multipla di } f. \end{aligned}$$

$\diamond$

**PROPOSIZIONE 8.7.4** *Siano  $K$  un campo,  $f \in K[x]$  e  $\deg(f) = n > 0$ . Allora la somma delle molteplicit  delle radici di  $f$  in  $K$  non supera  $n$ .*

**DIMOSTRAZIONE.** Siano  $c_1, c_2, \dots, c_m$  le radici (distinte) di  $f$  in  $K$  e  $k_1, k_2, \dots, k_m$  le loro rispettive molteplicit . Allora abbiamo

$$f = (x - c_1)^{k_1} (x - c_2)^{k_2} \dots (x - c_m)^{k_m} g,$$

ove  $g$    un polinomio non nullo a coefficienti in  $K$  e privo di radici in  $K$ . Ne segue che

$$n = \deg(f) = k_1 + k_2 + \dots + k_m + \deg(g) \geq k_1 + k_2 + \dots + k_m$$

e l'asserto   provato.  

**TEOREMA 8.7.5** *Sia  $K$  un campo e*

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + x^n$$

*un polinomio monico di grado positivo  $n$  a coefficienti in  $K$ . Se  $f$  ha  $n$  radici  $c_1, c_2, \dots, c_n$  in  $K$  e se  $\sigma_i(x_1, x_2, \dots, x_n)$  denota l' $i$ -esimo polinomio simmetrico elementare in  $n$  indeterminate, allora risulta*

$$a_j = (-1)^{n-j} \sigma_{n-j}(c_1, c_2, \dots, c_n),$$

per ogni  $j = 1, 2, \dots, n - 1$ .

**DIMOSTRAZIONE.** Nelle nostre ipotesi risulta

$$a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + x^n = (x - c_1)(x - c_2) \dots (x - c_n),$$

cos  l'asserto segue uguagliando i coefficienti del polinomio a primo membro con quelli omologhi del polinomio a secondo membro.  

**ESERCIZIO 8.7.6** *Siano  $f(x) = ax^2 + bx + c$  un polinomio di secondo grado a coefficienti complessi e  $c_1, c_2$  le sue radici. Verificare che risulta*

$$\frac{b}{a} = -(c_1 + c_2), \quad \frac{c}{a} = c_1c_2.$$

**ESERCIZIO 8.7.7** *Siano  $f(x) = ax^3 + bx^2 + cx + d$  un polinomio di terzo grado a coefficienti complessi e  $c_1, c_2, c_3$  le sue radici. Verificare che risulta*

$$\frac{b}{a} = -(c_1 + c_2 + c_3), \quad \frac{c}{a} = c_1c_2 + c_1c_3 + c_2c_3, \quad \frac{d}{a} = -c_1c_2c_3.$$

## 8.8 Fattorizzazione di polinomi su $C$ ed $R$

Riportiamo senza dimostrazione il seguente teorema.

**TEOREMA 8.8.1 (teorema fondamentale dell'algebra)** *Ogni polinomio di grado positivo sul campo complesso  $C$  ha almeno una radice in  $C$ . Ne segue che ogni polinomio su  $C$  di grado positivo può fattorizzarsi nel prodotto di polinomi di primo grado.*

Ricordiamo che, se  $z = a + ib$  è un numero complesso, il numero  $\bar{z} = z - ib$  si chiama *coniugato* di  $z$  e risulta  $\bar{\bar{z}} = z$  se, e solo se,  $z \in R$ . In modo analogo, se

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

è un polinomio a coefficienti complessi, si chiama *coniugato di  $f$*  il polinomio

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \cdots + \bar{a}_nx^n$$

e risulta  $\bar{\bar{f}} = f$  se, e solo se, tutti i coefficienti di  $f$  sono reali.

**ESEMPIO 8.8.2** Se  $f(x) = ax^2 + bx + c$  è un polinomio di secondo grado a coefficienti complessi, un numero complesso  $z$  è radice di  $f$  se, e solo se, risulta

$$z^2 + \frac{b}{a}z + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a};$$

cioè

$$\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Ne segue che  $f(x)$  ha due radici  $z_1, z_2$  date dalla nota formula

$$z_1, z_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Se  $f(x)$  ha tutti i coefficienti reali, le due radici  $z_1, z_2$  sono reali se, e solo se,  $b^2 - 4ac$  (il *discriminante* di  $f$ ) è non negativo.  $\diamond$

**ESERCIZIO 8.8.3** *Siano  $f(x) \in C$  e  $c$  una radice di  $f(x)$ . Provare che  $\bar{c}$  è radice del polinomio coniugato  $\bar{f}(x)$ . Se ne deduca che, se tutti i coefficienti di  $f(x)$  sono reali, allora  $\bar{c}$  è una radice di  $f(x)$ .*

**TEOREMA 8.8.4** *Un polinomio  $f \in R[x]$  è irriducibile se, e soltanto se, ha grado 1 oppure ha grado 2 e discriminante negativo.*

**DIMOSTRAZIONE.** Se poniamo  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ , abbiamo:

$$f \text{ irriducibile e } n > 1 \Rightarrow$$

$$f \text{ ha una radice } z = a + ib \in C \setminus R \Rightarrow f(\bar{z}) = 0$$

$\Rightarrow (x - z)(x - \bar{z})|f$  in  $C[x]$  e abbiamo

$$(x - z)(x - \bar{z}) = x^2 - 2ax + a^2 + b^2 = g \in R[x], \deg(g) = 2$$

$$\Rightarrow f = gh \text{ con } h \in R^* \Rightarrow \deg(f) = 2 \text{ e } f(x) = h(a^2 + b^2) - 2ahx + hx^2$$

$$\Rightarrow a_1^2 - 4a_0a_2 = 4a^2h^2 - 4h^2(a^2 + b^2) = -4h^2b^2 < 0.$$

Inoltre,

$$a_0 + a_1x + a_2x^2 = (b_0 + b_1x)(c_0 + c_1x) \text{ con } b_1, c_1 \neq 0$$

$$\Rightarrow a_0 + a_1x + a_2x^2 = b_0c_0 + (b_0c_1 + b_1c_0)x + b_1c_1x^2$$

$$\Rightarrow a_1^2 - 4a_0a_2 = (b_0c_1 + b_1c_0)^2 - 4b_0c_0b_1c_1 = (b_0c_1 - b_1c_0)^2 \geq 0.$$

◇

Dal teorema precedente e dall'esercizio 8.4.4 si ha subito il seguente corollario.

**COROLLARIO 8.8.5** *Ogni polinomio  $f \in R[x]$  di grado maggiore di 2 può decomporre nel prodotto di polinomi a coefficienti reali di primo e secondo grado irriducibili su  $R$ .*

**ESERCIZIO 8.8.6** *Provare che il polinomio  $x^4 + 1$  è riducibile su  $R$  e si decompone nel prodotto di due fattori irriducibili di secondo grado. Provare inoltre che tale polinomio è irriducibile su  $Q$ .*

## 8.9 Esercizi

**8.9.1** Sia  $D$  un dominio d'integrità non nullo nel quale due elementi qualsiasi sono associati. Provare che  $D$  è un campo.

**8.9.2** Spiegare perché la teoria della divisibilità in un dominio di integrità unitario  $D$  è priva di interesse, è cioè banale, nel caso in cui  $D$  sia un campo.

**8.9.3** Sia  $D$  un dominio d'integrità unitario. Provare che  $D$  è un campo se, e solo se, vale una delle seguenti condizioni:

- (a) due qualsiasi elementi non nulli di  $D$  sono associati;
- (b) la relazione di divisibilità è di equivalenza in  $D^*$ .

**8.9.4** Nell'anello  $Q[[x]]$  delle serie formali a coefficienti razionali calcolare gli elementi inversi dei polinomi  $1 + x$ ,  $1 - x^2$  e  $1 + x^2$ .

**8.9.5** Trovare i polinomi associati ad  $f(x) = x^3 - x^2 + x - 1 \in A[x]$ , nei casi  $A = Z, Z_3, Z_5$ . Trovare tre polinomi associati ad  $f(x)$  nel caso  $A = Q$ .

**8.9.6** Usando l'algoritmo di Euclide delle divisioni successive, trovare un massimo comune divisore dei polinomi  $f(x)$  e  $g(x)$ ,  $f, g \in R[x]$ , nei seguenti casi:

$$\begin{aligned} f(x) &= x^2 - 5x + 5, & g(x) &= x^2 - 4; \\ f(x) &= x^3 - 3x^2 + 3x - 1, & g(x) &= x^2 - 2x + 1; \\ f(x) &= x^2 + 2x + 20, & g(x) &= 3x^2 + 2; \\ f(x) &= x^4 - 6x^3 + 7x^2 + 6x - 2, & g(x) &= 2x^3 - 9x^2 + 7x + 3. \end{aligned}$$

**8.9.7** Calcolare in modo sintetico il quoziente e il resto della divisione di  $f(x)$  per  $(x - c)$  nei seguenti casi:

$$\begin{aligned} f(x) &= x^2 - 5x + 6, & c &= 4; \\ f(x) &= x^3 - 3x^2 + 6x - 5, & c &= 3; \\ f(x) &= x^4 - 3x^2 - 2x - 4, & c &= -3. \end{aligned}$$

**8.9.8** Verificare se in  $Q[x]$  il polinomio  $f(x)$  é divisibile per  $(x - c)$  nei seguenti casi:

$$\begin{aligned} f(x) &= 13x^{10} + 14x^5 + 1, & c &= -1; \\ f(x) &= 2x^4 - x^3 - 6x^2 + 4x - 8, & c &= \pm 2; \\ f(x) &= x^4 - 3x^3 + 3x^2 - 3x + 2, & c &= 1, c = 2. \end{aligned}$$

**8.9.9** Sia  $f \in K[x]$  un polinomio riducibile sul campo  $K$  di grado  $n > 0$ . Provare che  $f$  ha almeno un divisore irriducibile, monico e di grado non superiore a  $\frac{n}{2}$ .

**8.9.10** Sia  $K$  un campo. Provare che due polinomi non nulli a coefficienti in  $K$  sono associati se, e solo se, differiscono per una costante moltiplicativa non nulla.

**8.9.11** Provare che i seguenti numeri reali sono algebrici sul campo razionale e calcolare il corrispondente polinomio minimo:

$$5 + \sqrt{2}, \quad \sqrt{11 - 2\sqrt{5}}.$$

**8.9.12** Siano  $c_1, c_2, \dots, c_n$  numeri complessi tali che  $\sigma_i(c_1, c_2, \dots, c_n)$  sia un numero razionale, per ogni  $i = 1, 2, \dots, n$ . Provare che  $c_1, c_2, \dots, c_n$  sono algebrici su  $Q$ .

**8.9.13** Sia  $f(x)$  un polinomio a coefficienti complessi di grado positivo  $n$  e siano  $a_1, a_2, \dots, a_m$  le sue radici complesse distinte. Denotata con  $\nu_j$  la molteplicitá di  $a_j$ , per ogni  $j = 1, 2, \dots, m$ , provare che risulta

$$\nu_1 a_1 + \nu_2 a_2 + \dots + \nu_m a_m = n.$$