

## divisibilità in un dominio di integrità unitario

Sia  $D = (D, +, \cdot)$  un dominio di integrità unitario.

**DEFINIZIONE 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  $b$ .

### ALCUNE PROPRIETÀ

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

**OSSERVAZIONE 2** Se  $D$  è un dominio di integrità unitario, allora  $(D^*, \cdot)$  risulta un semigruppato commutativo, regolare e unitario. Poiché la teoria della divisibilità riguarda essenzialmente la struttura moltiplicativa  $D^*$  di  $D$ , essa può svolgersi nell'ambito dei *semigruppato commutativi, regolari e unitari*.

**DEFINIZIONE 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  $a = bu$ .

**OSSERVAZIONE 4** La relazione  $\sim$  risulta di equivalenza in  $D^*$  e si ha subito che

$$a \sim b \quad \Leftrightarrow \quad a|b \quad \text{e} \quad b|a$$

$\Leftrightarrow \quad a, b$  hanno gli stessi multipli e gli stessi divisori.

## primi ed irriducibili

**ESERCIZIO 5** 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 6** Siano  $a, b$  elementi di  $D$ . Allora risulta  $(a) = (b)$  se, e solo se,  $a$  e  $b$  sono associati.

**DEFINIZIONE 7** 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  $a$ .

**ESERCIZIO 8** Siano  $a, b$  elementi di  $D$ . Allora  $b$  é un divisore proprio di  $a$  se, e solo se,  $(a) \subset (b)$ .

**OSSERVAZIONE 9** 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*.

**DEFINIZIONE 10** 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*.

**DEFINIZIONE 11** Un elemento  $a \in D^*$  si dice *primo* se non é invertibile e se

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

**OSSERVAZIONE 12** Notiamo esplicitamente che le definizioni appena date sono formalmente uguali a quelle analoghe relative all'anello degli interi.

## divisibilità in un dominio di integrità unitario

**PROPOSIZIONE 13** Sia  $a \in D$  irriducibile. Se  $b, c \in D$  sono tali che  $a = bc$ , allora uno tra i fattori  $b$  e  $c$  è associato ad  $a$  e l'altro è invertibile.

**DIM.** 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, perché  $a$  ha solo divisori banali, e

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

**ESERCIZIO 14** Siano  $a, b, c$  elementi di  $D$  diversi da zero tali che  $a = bc$ . Provare che, se  $b$  è associato ad  $a$ , allora  $c$  è invertibile.

**PROPOSIZIONE 15** Se  $a \in D$  è irriducibile e  $b \in D$  è associato ad  $a$ , allora  $b$  è irriducibile.

**PROPOSIZIONE 16** Se  $a \in D$  è primo, allora è irriducibile.

**DIM.** 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:

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

Così  $b$  e  $c$  sono divisori banali di  $a$  e l'asserto è provato.

**OSSERVAZIONE 17** A differenza di quanto accade nell'anello degli interi, la proposizione precedente non è in generale invertibile.

## un elemento irriducibile e non primo

**ESEMPIO 18** Consideriamo l'estensione quadratica  $Z[\sqrt{-3}]$  di  $Z$  cioè il dominio d'integritá

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

e ricordiamo che la funzione norma  $n$  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

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

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

$$z|2 \Rightarrow \text{esistono due interi } a, b \text{ tali che } 2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (a + b)\sqrt{-3}$$

$$\Rightarrow a - 3b = 2 \text{ e } a + b = 0 \Rightarrow a, b \notin Z$$

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

## divisibilità in un dominio di integrità unitario

**PROPOSIZIONE 19** *Un elemento  $a$  di un anello principale  $D$  è irriducibile se, e soltanto se, è primo.*

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

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

ove  $d$  è un generatore 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  $b \in I$ )  $\Rightarrow b = at \Rightarrow a|b$ .

**ESERCIZIO 20** *Un elemento  $a \in D$  è primo se, e soltanto se, l'ideale principale  $(a)$  è un ideale primo.*

**DEFINIZIONE 21** Siano  $a, b$  due elementi di un dominio di integrità 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  $b$  è anche un divisore di  $d$ . Se  $1$  è un massimo comune divisore di  $a$  e  $b$ , allora  $a$  e  $b$  si dicono *coprime*.

**ESERCIZIO 22** Provare che due elementi di  $D$  risultano entrambi massimo comune divisore di  $a$  e  $b$  se, e soltanto se, sono associati.

**ESERCIZIO 23** *Provare che, se un massimo comune divisore di due elementi  $a, b$  di  $D$  è invertibile, allora  $a$  e  $b$  sono coprime.*

## massimo comune divisore negli anelli principali

**TEOREMA 24** *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*

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

**DIM.** 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  $d = xa + yb$ , con  $x, y$  opportuni elementi di  $D$ . Abbiamo allora che  $d$  è un divisore comune di  $a$  e  $b$  in quanto  $a$  e  $b$ , appartenendo a  $(d)$ , sono multipli di  $d$ . D'altra parte, se  $c$  è un divisore comune di  $a$  e  $b$ , allora  $c$  divide  $xa + yb = d$  e l'asserto è completamente provato.

**COROLLARIO 25** *Siano  $D$  un anello principale e  $a, b$  due suoi elementi non nulli. Allora un elemento  $d \in D$  è un massimo comune divisore di  $a$  e  $b$  se, e solo se,  $d$  è un generatore dell'ideale  $(a, b)$ .*

**ESERCIZIO 26** *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  $(a) \cap (b)$ .*