DOMINI A FATTORIZZAZIONE UNICA

CORSO DI ALGEBRA, A.A. 2012-2013

Nel seguito D indicherà sempre un dominio d'integrità cioè un anello commutativo con unità privo di divisori dello zero. Indicheremo con $U(D)$ l'insieme degli elementi invertibili di D.

Definizione 1. *Siano $a, b \in D$. Diciamo che a* divide *b (o b è* multiplo di *a), e scriviamo $a \mid b$, se esiste $c \in D$ tale che $b = ac$.*

Osservazione 2. *Per ogni $a \in D$, e per ogni $u \in U(D)$ abbiamo che*

(1) *u divide a;*
(2) *a divide u se e solo se $a \in U(D)$.*

Dimostrazione. Abbiamo che

$$a = a \cdot 1_D = a(u \cdot u^{-1}) = u(au^{-1}),$$

quindi vale (a). Se al contrario, a divide u, allora esiste $b \in D$ tale che $u = ab$ e quindi abbiamo che

$$1_D = u \cdot u^{-1} = (ab)u^{-1} = a(bu^{-1})$$

cioè a è invertibile e vale (2). □

Definizione 3. *Siano $a, b \in D \setminus \{0_D\}$. a e b si dicono* associati *se $a \mid b$ e $b \mid a$. In questo caso, a si dice* associato *di b e b si dice* associato *di a.*

Lemma 4. *Due elementi $a, b \in D \setminus \{0_D\}$ sono associati se e solo se esiste un elemento invertibile $u \in D$ tale che $a = ub$.*

Dimostrazione. Supponiamo che a e b siano associati. Allora esistono $c_1, c_2 \in D$ tali che $a = bc_1$ e $b = ac_2$. Sostituendo otteniamo

$$b = ac_2 = bc_1c_2$$

da cui

$$b(1_D - c_1c_2) = 0_D.$$

Poichè per ipotesi $b \neq 0_D$ e D è un dominio d'integrità, deve essere $1_D - c_1c_2 = 0$, da cui segue che $c_1c_2 = 1_D$, cioè c_1 e c_2 sono invertibili. Così $u = c_1$.

Viceversa, se $a = ub$ con u invertibile in D, allora è chiaro che b divide a e analogamente a divide b perchè $b = au^{-1}$. □

Lemma 5. *Siano $a, a' \in D$ associati. Allora*

(1) *se a divide b allora anche a' divide b;*
(2) *se c divide a allora c divide anche a'.*

Dimostrazione. Poichè a e a' sono associati, $a = ua'$ per qualche $u \in U(D)$. a divide b quindi $b = ad$ per qualche $d \in D$. Allora $b = ua'd$, cioè a' divide b.

Ora supponiamo che $c \in D$ divida a. Allora $a = cd$ per qualche $d \in D$. Allora $a' = au^{-1} = cdu^{-1}$, cioè c divide a'. □

Definizione 6. *Un elemento $a \in D$ con $a \neq 0_D$ e $a \notin U(D)$ si dice* primo *se per ogni $c, d \in D$ tali che $a \mid cd$ si ha $a \mid c$ oppure $a \mid d$.*

Un elemento $a \in D$ con $a \neq 0$ e $a \notin U(D)$ si dice irriducibile *se per ogni $b \in D$ tale che $b \mid a$ si ha che b è invertibile oppure $a \mid b$.*

Osservazione 7. *Siano $a, a' \in D$ due elementi associati .*

(1) *a è primo se e solo se a' è primo,*
(2) *a è irriducibile se e solo se a' è irriducibile.*

Dimostrazione. Supponimao che a sia primo e sia $a' = au$ con $u \in U(D)$. Supponiamo che a' divida il prodotto bc con $b, c \in D$. Allora esiste $d \in D$ tale che $bc = a'd = au^{-1}d$. Quindi a divide bc e poichè a è primo, deve essere $a \mid b$ oppure $a \mid c$. Per il Lemma 5 otteniamo che a' divide b o c. Quindi a' è primo.

Supponiamo ora che a sia irriducibile. Per mostrare che a' è irriducibile supponiamo che $b \in D$ divida a'. Allora, per il Lemma 5, b divide anche a che è irriducibile. Quindi o b è invertibile oppure b divide a. In questo ultimo caso b divide a', di nuovo per il Lemma 5. □

Lemma 8. *Sia D un dominio. Se $a \in D$ è primo, allora a è irriducibile.*

Dimostrazione. Supponiamo che $b \in D$ sia un divisore di a. Mostriamo che o a divide b oppure b è invertibile. Abbiamo che esiste $c \in D$ tale che $a = bc$. Quindi a divide bc e poichè per ipotesi a è primo, deve essere che a divide b oppure a divide c. Se a divide b, abbiamo finito. Se invece a divide c, allora $c = ad$ per qualche $d \in D$ e così

$$a = bc = b(ad) = a(bd).$$

Segue che $a(1_D - bd) = 0$. Poichè a è primo, $a \neq 0_D$. Essendo D un dominio d'integrità deve essere $1_D - bd = 0$, da cui $bd = 1_D$. Quindi b (e anche c) è invertibile. □

Definizione 9. *Siano $a, b \in D$. Diremo che b è un* divisore proprio *di a se*

(1) *b divide a;*
(2) *b non è invertibile e b non è associato di a.*

Diremo che $a = bc$ è una fattorizzazione propria *di a se b e c sono divisori propri di a.*

Definizione 10. *Un dominio D si dice* dominio a fattorizzazione unica *(UFD) se ogni elemento di D diverso da zero e non invertibile si scrive come prodotto di elementi irriducibili in modo unico a meno dell'ordine e a meno di associati, cioè:*

(1) *per ogni $a \in D \setminus (\{0_D\} \cup U(D))$ esistono elementi irriducibili $p_1, \ldots, p_r$ taliche $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r$;*
(2) *se $p_1, \ldots p_r$, $q_1, \ldots, q_s$ sono elementi irriducibili tali che*

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

allora $r = s$ ed esiste una permutazione σ degli indici $1, \ldots, s$ tale che, per ogni $i \in \{1, \ldots, r\}$, p_i è associato di $q_{\sigma(i)}$.

Definizione 11. *Un dominio D si dice* dominio a ideali principali (PID) *se ogni ideale di D è principale, cioè è del tipo $aD = \{ad \mid d \in D\}$.*

Scriveremo (a) al posto di aD. L'elemento a si dice generatore *dell'ideale (a).*

Esempio. $\mathbb{Z}$ è un dominio a ideali principali: infatti sappiamo che i suoi ideali sono tutti e soli gli $n\mathbb{Z}$ al variare di $n \in \mathbb{N}$.

Osservazione 12. *Sia D un dominio a ideali principali e I un ideale di D. Allora tutti gli ideali dell'anello quoziente D/I sono principali. Non è vero invece in generale che D/I sia un dominio.*

Dimostrazione. Per il teorema di corridspondenza sappiamo che gli ideali di D/I sono tutti del tipo J/I con J ideale di J contenente I. Ma allora $J = (a)$ per qualche $a \in D$ e quindi

$$J/I = \{I + ar \mid r \in D\} = (I + a).$$

In generale D/I non è un dominio, ad esempio con $D = \mathbb{Z}$ e $I = n\mathbb{Z}$ se n non è un numero primo. □

Lemma 13. *Siano $a, b, a' \in D$ dominio d'integrità qualsiasi. Allora*

(1) *a divide b se e solo se $(b) \subseteq (a)$;*
(2) *a e a' sono associati se e solo se $(a) = (a')$.*

Dimostrazione. Se a divide b, allora esiste $c \in D$ tale che $b = ac$. Allora $b \in (a)$ da cui segue subito che $(b) \subseteq (a)$. Viceversa, se $(b) \subseteq (a)$, allora in particolare $b \in (a)$ e quindi b è un multiplo di a.

Per il punto (1), $(a) = (a')$ se e solo se a divide a' e a' divide a, cioè a e a' sono associati. □

Definizione 14. *Un dominio D si dice* dominio euclideo *se esiste una funzione*

$$\delta : D \setminus \{0_D\} \longrightarrow \mathbb{N}$$

con la proprietà che per ogni $a, b \in D$ con $b \neq 0_D$ esistono $q, r \in D$ tali che

$$a = bq + r$$

con $r = 0_D$ oppure $\delta(r) < \delta(b)$.

Esempi. L'anello $\mathbb{Z}$ è un dominio euclideo con $\delta(z) = |z|$.

Se F è un campo, l'anello dei polinomi $F[x]$ è un dominio euclideo con $\delta(p)$ uguale al grado del polinomio p.

Teorema 15. *Ogni dominio euclideo è un dominio e ideali principali.*

Dimostrazione. Sia D un dominio euclideo rispetto alla funzione δ. Sia I un ideale di D. Vogliamo mostrare che I è principale, cioè esiste un elemento $a \in D$ tale che $I = (a)$.

Se $I = \{0_D\}$ basta prendere $a = 0_D$. Supponiamo quindi che $I \neq \{0_D\}$. Allora l'insieme

$$\mathcal{S} = \{\delta(i) \mid i \in I \setminus \{0_D\}\}$$

è un sottoinsieme non vuoto di $\mathbb{N}$. Poichè $\mathbb{N}$ soddisfa la condizione del minimo, $\mathcal{S}$ contiene un elemento minimo n. Sia $a \in I \setminus \{0_D\}$ tale che $\delta(a) = n$. Poichè $a \in I$ e I è un ideale di D, abbiamo che $(a) = aD \subseteq I$.

Viceversa, se $x \in I$ possiamo fare la divisione di x per a ottenendo $x = aq + r$ con $q, r \in D$ e $r = 0_D$ oppure $\delta(r) < \delta(a)$. Ma $r = x - aq \in I$, quindi $\delta(r) \in \mathcal{S}$

e per la minimalità di $n = \delta(a)$ in $\mathcal{S}$ deve essere $\delta(r) \geq \delta(a)$. Quindi $r = 0_D$ e $x = aq \in (a)$. Così $I \subseteq (a)$. Pertanto $I = (a)$. □

Lemma 16. *In un dominio a ideali principali ogni catena ascendente di ideali è stazionaria cioè se*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

è una catena di ideali, allora esiste un $n \in \mathbb{N}$ tale che $I_n = I_{n+i}$ per ogni $i \geq 1$.

Dimostrazione. Sia $I_1 \subseteq I_2 \subseteq \ldots I_k \subseteq \ldots$ una catena ascendente di ideali e poniamo

$$U = \bigcup_i I_i.$$

Mostriamo che U è un ideale di D. Siano $a, b \in U$. Allora esistono due indici h, k tali che $a \in I_h$ e $b \in I_k$. Se $l \in \mathbb{N}$ è maggiore di h e di k, abbiamo che $a, b \in I_l$ e quindi $a - b \in I_l \subseteq U$ e per ogni $d \in D$ il prodotto ad sta in I_l perchè I_l è un ideale di D. Quindi U è un ideale di D.

Poichè per ipotesi tutti gli ideali di D sono principali, esiste $e \in D$ tale che $U = (e)$. Ora $e \in U$ e quindi esiste $n \in \mathbb{N}$ tale che $e \in I_n$. Così per ogni $i \geq 0$ abbiamo che

$$U = (e) \subseteq I_n \subseteq I_{n+i} \subseteq U.$$

Quindi $U = I_n = I_{n+i}$, per ogni $i \geq 0$. □

Definizione 17. *Siano $a, b \in D$. Un* massimo comun divisore *di a e b è un elemento $d \in D$ tale che*

(1) *d divide a e d divide b;*
(2) *se c divide a e c divide b allora c divide d.*

Indicheremo un massimo comun divisore tra a e b con (a, b). Si osservi che il massimo comun divisore non è necessariamente unico, anzi in genere non lo è perchè si verifica facilmente che se d è un massimo comun divisore di a e b, allora anche ogni associato di d lo è. Viceversa, dalla definizione segue subito che due massimi comuni divisori i a e b sono sempre associati.

Lemma 18. *Siano $a, b \in D$ con a irriducibile. Se a non divide b, allora 1_D è un massimo comun divisore di a e b.*

Dimostrazione. Poniamo $d = (a, b)$. Allora d divide a e poichè a è irriducibile abbiamo che a e d sono associati oppure d è invertibile. Poichè d divide b ma a non divide b, dal Lemma 5 segue che a non è associato di d. Quindi d è invertibile. Poichè ogni associato di d è un massimo comun divisore di a e b, otteniamo la tesi. □

Teorema 19. *Sia D un dominio a ideali principali. Per ogni $a, b \in D \setminus \{0_D\}$ esiste un massimo comun divisore. Inoltre, se $d = (a, b)$, allora esistono $x, y \in D$ tali che $d = ax + by$.*

Dimostrazione. Siano $a, b \in D \setminus \{0_D\}$. Allora $(a) + (b) = \{r + s \mid r \in (a), s \in (b)\}$ è un ideale di D e quindi è principale. Sia $d \in D$ tale che $(a) + (b) = (d)$. Allora $(a) \subseteq (d)$ e $(b) \subseteq (d)$ e quindi il Lemma 13 implica che d divide a e b.

Sia ora c un divisore di a e b. Allora sempre per il Lemma 13, $(a) \subseteq (c)$ e $(b) \subseteq (d)$, da cui segue che $(d) = (a) + (b) \subseteq (c)$ e quindi c divide d. Pertanto d è un massimo comun divisore di a e b.

Infine, poichè $d \in (a) + (b)$, d si scrive come somma di un elemento di (a) e di un elemento di (b), ovvero esistono $x, y \in D$ tali che $d = ax + by$. □

Lemma 20. *In un dominio a ideali principali ogni elemento irriducibile è primo.*

Dimostrazione. Sia D un dominio a ideali principali e sia q un elemento irriducibile di D. Supponiamo che q divida il prodotto ab, $a, b \in D$ e q non divida a. Mostriamo che q divide b. Poichè q divide ab abbiamo $ab = qt$ per qualche $t \in D$. Poichè q non divide a, il Lemma 18 implica che $1_D = (q, a)$ e per il Teorema 19 esistono $x, y \in D$ tali che $1_D = qx + ay$. Allora moltiplicando per b otteniamo

$$b = bqx + aby = qbx + qty = q(bx + ty),$$

da cui q divide b. Pertanto q è primo in D. □

Teorema 21. *Ogni dominio a ideali principali è un dominio a fattorizzazione unica.*

Dimostrazione. Sia D un dominio a ideali principali. Sia $\mathcal{A}$ l'insieme degli elementi di D non nulli e non invertibili che non si possono scrivere come prodotto di elementi irriducibili. Mostriamo che $\mathcal{A} = \emptyset$. Supponiamo per assurdo che $\mathcal{A} \neq \emptyset$ e sia $a_1 \in \mathcal{A}$. Allora $a_1 \neq 0$ non è invertibile e non è irriducibile e quindi esistono $b, c \in D$ tali che $a_1 = bc$ è una fattorizzazione propria di a. Allora b, c sono diversi da zero, non sono invertibili e almeno uno tra i due non è prodotto di irriducibili, perchè altrimenti anche a_1 lo sarebbe. Chiamiamo a_2 quello tra b e c che non è prodotto di irriducibili. Allora $a_2 \in \mathcal{A}$ e, ripetendo il ragionamento per a_2 al posto di a_1, troviamo $a_3 \in \mathcal{A}$ tale che a_3 divide a_2 e non è associato ad a_2. Procedendo in questo modo possiamo costruire una successione infinita a_i di elementi di D tali che per ogni $i \geq 1$

$$a_i \text{ divide } a_{i+1} \text{ ma } a_i \text{ e } a_{i+1} \text{ non sono associati.}$$

Per il Lemma 13 otteniamo così una catena ascendente di ideali

$$(a_1) \subset (a_2) \subset \ldots \subset (a_k) \subset \ldots$$

che non è stazionaria perchè tutte le inclusioni sono proprie. Questo contraddice il Lemma 16 e quindi deve essere $\mathcal{A} = \emptyset$.

Vediamo ora l'uncità della decomposizione in prodotto di irriducibili. Supponiamo che

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = a = q_1 \cdot q_2 \cdot \ldots \cdot q_s \tag{1}$$

con p_i e q_i irriducibili per ogni i. Dobbiamo mostrare che $r = s$ ed esiste una permutazione α degli indici $1, \ldots, r$ tale che, per ogni $i \in \{1, \ldots r\}$, p_i e $q_{\alpha(i)}$ sono associati. Procediamo per induzione su r. Se $r = 1$, allora $a = p_1$ è irriducibile e quindi gli unici suoi divisori sono gli invertibili e i suoi associati. Pertanto deve essere $s = 1$ e $q_1 = p_1$. Sia ora $r > 1$ e supponiamo che la tesi sia vera per $r - 1$.

Abbiamo che p_1 divide il prodotto $q_1 \cdot q_2 \cdot \ldots \cdot q_s$. Per il Lemma 20, p_1 è primo e quindi esiste $h \in \{1, \ldots, s\}$ tale che p_1 divide q_h. Essendo q_h irriducibile, $q_h = up_1$ per qualche $u \in U(D)$. Sia $\beta \in S_s$ una permutazione tale che $\beta(1) = h$. Allora dall'uguaglianza in (1) segue che

$$p_1(p_2 \cdot \cdots \cdot p_r - uq_{\beta(2)} \cdot \cdots \cdot q_{\beta(s)}) = 0_D$$

da cui otteniamo

$$p_2 \cdot \cdots \cdot p_r = uq_{\beta(2)} \cdot \cdots \cdot q_{\beta(s)}$$

perchè D è un dominio e $p_1 \neq 0_D$. A questo punto, per l'ipotesi induttiva, $r = s$ ed esiste una permutazione τ degli indici $\{\beta(2), \ldots, \beta(r)\}$ tale che p_2 è associato a $uq_{\tau\beta(2)}$ e p_i è associato a $q_{\tau\beta(i)}$ per ogni $i \in \{3, \ldots, r\}$. Sia $\alpha \in S_r$ la permutazione così definita:

$$\alpha(1) = h, \quad \alpha(i) = \tau\beta(i) \text{ per } i = 2, \ldots, r.$$

Allora per ogni $i \in \{1, \ldots r\}$, p_i e $q_{\alpha(i)}$ sono associati, come voluto. □

Si noti che è molto difficile trovare esempi di domini fattoriali che non siano domini a ideali principali.

Definizione 22. *Siano $a, b \in D$. Un* minimo comune multiplo *di a e b è un elemento $m \in D$ (che indicheremo con $[a, b]$) tale che*

(1) *a divide m e b divide m;*
(2) *se a divide c e b divide c allora m divide c.*

Lemma 23. *Sia D un dominio fattoriale. Per ogni $a, b \in D \setminus \{0_D\}$ esistono (a, b) e $[a, b]$.*

Dimostrazione. Siano

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \text{ e } b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$$

le fattorizzazioni in irriducibili distinti di a e b, dove gli esponenti α_i e β_i sono interi non negativi, eventualmente nulli se p_i non divide a o b. Si verifica facilmente che

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_r^{\min\{\alpha_r, \beta_r\}}$$

e

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_r^{\max\{\alpha_r, \beta_r\}}.$$

□

Concludiamo con una caratterizzazione degli ideali massimali di un dominio a ideali principali.

Lemma 24. *Sia D un dominio a ideali principali e sia $a \in D$. Allora (a) è un ideale massimale se e solo se a è un elemento irriducibile.*

Dimostrazione. Supponiamo che a sia irriducibile. Sia I un ideale di D tale che $(a) \subset I \subseteq D$. Mostriamo che $I = D$. Poichè tutti gli ideali di D sono principali, esiste $b \in D$ tale che $I = (b)$. Per il Lemma 13, $(a) \subset I$ implica che b divide a ma b non è associato di a. Chiaramente $b \neq 0_D$ perchè $I \neq \{0_D\}$. Ma allora, poichè a è irriducibile, b deve essere invertibile. Ciò implica $I = (b) = D$.

Viceversa, supponiamo che (a) sia un ideale massimale. Supponiamo che $0_D \neq b \in D \setminus U(D)$ sia un divisore di a. Allora (b) è un ideale non nullo, diverso da D (perchè b non è invertibile) e contenente (a) per il Lemma 13. Poichè (a) è un

ideale massimale, segue che $(b) = (a)$. Il Lemma 13 implica che b è associato di a. Quindi a è irriducibile. □

Corollario 25. *Sia D un dominio a ideali principali. $a \in D$ è irriducibile se e solo se $D/(a)$ è un campo.*

Dimostrazione. Sappiamo che l'anello quoziente $D/(a)$ è un campo se e solo se (a) è un ideale massimale. Dal Lemma 24 segue la tesi. □