AL210 - Appunti integrativi - 6

Prof. Stefania Gabelli - a.a. 2016-2017

Divisibilità in un dominio

Per definire in un anello commutativo unitario una buona teoria della divisibilità, è conveniente assumere che non ci siano zero-divisori, cioè che l'anello sia un dominio.

Dati due elementi x, y di un dominio A, si dice che y *divide* x in A se esiste un elemento $z \in A$ tale che $x = yz$. In tal caso si dice anche che y è un *divisore* o un *fattore* di x in A e che x è un *multiplo* di y. Lo zero di A divide soltanto se stesso ma è diviso da ogni elemento di A, infatti $0x = 0$ per ogni $x \in A$.

Gli elementi invertibili di A sono i divisori dell'unità moltiplicativa di A, denotata con 1. Indicheremo al solito con $\mathcal{U}(A)$ il gruppo moltiplicativo degli elementi invertibili di A.

Si dice che y è *associato* a x in A se esiste un elemento $u \in \mathcal{U}(A)$ tale che $y = ux$. Si verifica subito che questa è una relazione di equivalenza su A e che x e y sono associati se e soltanto se si dividono reciprocamente.

Ogni elemento $x \in A$ è diviso dagli elementi invertibili di A e dai suoi associati. Infatti $x = 1x = u(u^{-1}x)$, per ogni $u \in \mathcal{U}(A)$. Un divisore di x non invertibile e non associato a x si chiama un *divisore proprio* di x.

Notiamo che y divide x se e soltanto se $\langle x \rangle \subseteq \langle y \rangle$. Quindi x e y sono associati se e soltanto se $\langle x \rangle = \langle y \rangle$ e y è un divisore proprio di x se e soltanto se $\langle x \rangle \subsetneq \langle y \rangle \neq A$.

Un elemento x di A si chiama un *elemento irriducibile* se x è non nullo e non invertibile e non ha divisori propri. Un elemento non nullo che ha divisori propri si dice *riducibile*. Un *elemento primo* di A è un elemento x non nullo e non invertibile tale che, scelti comunque $y, z \in A$, quando x divide yz allora x divide y oppure x divide z. Quindi, per induzione su $n \geq 2$, un elemento primo x che divide un prodotto $y_1 y_2 \dots y_n$ divide almeno uno dei fattori y_i.

Proposizione 1 *Sia A un dominio e sia $x \in A$ un elemento non nullo e non invertibile. Allora x è un elemento primo se e soltanto se l'ideale principale $\langle x \rangle$ è un ideale primo.*

Dimostrazione: Segue direttamente dalle definizioni. □

Proposizione 2 *In un dominio A, ogni elemento primo è irriducibile.*

Dimostrazione: Sia $p \in A$ un elemento primo. Se $p = xy$, allora p divide x oppure y. Nel primo caso, p e x sono associati e y è invertibile. Nel secondo caso, p e y sono associati e x è invertibile. Quindi p non ha divisori propri. □

Esempio 3 (1) Gli elementi irriducibili di $\mathbb{Z}$ sono esattamente i numeri primi e i loro opposti e coincidono con gli elementi primi.

(2) Se K è un campo, per la formula del grado, gli elementi invertibili di $K[X]$ sono tutte e sole le costanti non nulle. Dunque un polinomio non costante $f(X) \in K[X]$ è irriducibile se e soltanto se gli unici suoi divisori sono le costanti non nulle ed i polinomi del tipo $cf(X)$, con $c \in K^*$.

Ne segue che un polinomio non nullo $f(X) \in K[X]$ è riducibile su K se e soltanto se $f(X)$ ha un divisore $g(X) \in K[X]$ tale che $1 \leq \deg g(X) < \deg f(X)$. In particolare, se $\deg f(X) = 1$, allora $f(X)$ è irriducibile.

Massimo comune divisore

Se A è un dominio e $x, y \in A$ sono non entrambi nulli, un massimo comune divisore di x e y è un divisore comune di x e y diviso da ogni altro divisore comune. Precisamente, un elemento $d \in A$ è un *massimo comune divisore* di x e y se:

(1) d divide x e y;

(2) Se d' divide x e y, allora d' divide d.

Un massimo comune divisore di x e y, se esiste, non è univocamente determinato. Infatti dalla proprietà (2) segue subito che se $d \in A$ è un massimo comune divisore, lo sono anche tutti gli elementi di A associati a d.

Nell'impossibilità di privilegiare un particolare massimo comune divisore di due elementi, se d è un *qualsiasi* massimo comune divisore di x e y, si usa scrivere $(x, y) = d$. Se gli unici divisori comuni di x e y sono gli elementi invertibili di A, si scrive $(x, y) = 1$ e si dice che x e y sono elementi *coprimi*.

Lemma 4 *Sia A un dominio. Un elemento $q \in A$, non nullo e non invertibile, è irriducibile se e soltanto se, per ogni $x \in A$, q divide x oppure $(x, q) = 1$.*

Dimostrazione: Poiché gli unici divisori di q sono gli elementi invertibili di A e gli elementi associati a q, se q non divide x, gli unici divisori comuni di x e q sono gli elementi invertibili. Quindi $(x, q) = 1$. □

Diremo che A è un *dominio con il massimo comune divisore* se due qualsiasi elementi non nulli di A hanno un massimo comune divisore.

Proposizione 5 (Lemma di Euclide) *Sia A un dominio con il massimo comune divisore e siano $x, y, z \in A$ elementi non nulli. Se x divide yz e $(x, y) = 1$, allora x divide z.*

Dimostrazione: Si verifica facilmente che $(xz, yz) = z(x, y)$. Allora, se $(x, y) = 1$ e x divide yz, si ha che x divide $(xz, yz) = z(x, y) = z$. □

Corollario 6 *Sia A un dominio con il massimo comune divisore e sia $p \in A$. Allora p è un elemento primo se e soltanto se p è un elemento irriducibile.*

Dimostrazione: Sia p un elemento irriducibile di A e supponiamo che p divida xy. Se p non divide x, allora $(p, x) = 1$ (Lemma 4) e quindi p divide y per il Lemma di Euclide (Proposizione 5). Viceversa, in ogni dominio un elemento primo è irriducibile (Proposizione 2). □

Domini a fattorizzazione unica

Un dominio A si chiama *atomico* se ogni elemento non nullo e non invertibile $x \in A$ può essere fattorizzato nel prodotto di un numero finito di elementi irriducibili (non necessariamente distinti):

$$x = p_1 p_2 \dots p_n, \quad \text{con } p_i \text{ irriducibile per } i = 1, \dots, n.$$

Questa proprietà è garantita dalla condizione della catena ascendente sugli ideali principali. Si dice che un dominio A soddisfa la *condizione della catena ascendente sugli ideali principali* se ogni catena di ideali principali propri di A

$$\langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \dots \subseteq \langle x_i \rangle \subseteq \dots$$

è stazionaria, cioè se esiste un (minimo) intero $n \geq 1$ tale che $\langle x_n \rangle = \langle x_m \rangle$ per $m \geq n$.

Tuttavia è noto che un dominio atomico non soddisfa necessariamente la condizione della catena ascendente sugli ideali principali.

Proposizione 7 *Se A è un dominio che soddisfa la condizione della catena ascendente sugli ideali principali, allora A è atomico.*

Dimostrazione: Supponiamo che la tesi non sia vera e sia $\mathcal{S}$ l'insieme degli ideali principali propri $\langle a \rangle$ di A tali che a non possa essere fattorizzato in elementi irriducibili. Per la condizione della catena ascendente, $\mathcal{S}$ ha un elemento massimale $\langle x \rangle$, perché altrimenti sarebbe possibile costruire una catena infinita di ideali principali generati da elementi di $\mathcal{S}$

$$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \dots \subsetneq \langle x_i \rangle \subsetneq \dots.$$

Poiché x non può essere irriducibile, altrimenti sarebbe banalmente fattorizzabile, possiamo scrivere $x = yz$, con y, z fattori propri di x. Allora

$\langle x \rangle \subsetneq \langle y \rangle$ e $\langle x \rangle \subsetneq \langle z \rangle$. Per la massimalità di $\langle x \rangle$, ne segue che y e z possono essere fattorizzati nel prodotto di un numero finito di elementi irriducibili. Ma allora anche x può essere fattorizzato. Questa è una contraddizione. □

Un dominio A si dice un *dominio a fattorizzazione unica* se soddisfa le due seguenti condizioni:

(1) A è atomico;

(2) Se $x = p_1 \dots p_n = q_1 \dots q_m$ sono due fattorizzazioni dello stesso elemento di A in elementi irriducibili (non necessariamente distinti), allora $n = m$ e gli elementi q_i possono essere rinumerati in modo tale che p_i e q_i siano associati per $i = 1, \dots, n$.

Si usa esprimere la proprietà (2) dicendo che la fattorizzazione in elementi irriducibili è *unica, a meno dell'ordine e di elementi invertibili.*

Esempio 8 (1) Il *Teorema Fondamentale dell'Aritmetica* asserisce che l'anello degli interi $\mathbb{Z}$ è un dominio a fattorizzazione unica. L'esistenza di una fattorizzazione in numeri primi si può dimostrare per induzione sul modulo.

(2) Se A è un dominio a fattorizzazione unica, ogni elemento non nullo di A ha un numero finito di divisori non associati tra loro. Quindi se $\mathcal{U}(A)$ è un insieme finito, ogni elemento non nullo ha un numero finito di divisori.

Infatti, sia $x \in A \setminus \{0\}$. Se $x \in \mathcal{U}(A)$, i suoi divisori sono tutti associati tra di loro, e associati a 1. Se $x \notin \mathcal{U}(A)$ e $x = p_1 \dots p_n$ è una fattorizzazione di x in elementi irriducibili, ogni divisore proprio di x deve essere associato a un elemento del tipo $p_{i_1} \dots p_{i_m}$ con $m \leq n$.

Se A è un dominio a fattorizzazione unica e $x, y \in A$ sono due elementi non nulli e non invertibili, considerando tutti i fattori irriducibili sia di x che di y, possiamo scrivere $x = p_1^{a_1} \dots p_n^{a_n}$ e $y = p_1^{b_1} \dots p_n^{b_n}$, dove $p_1, \dots, p_n$ sono elementi irriducibili distinti e $a_i, b_i \geq 0$, per $i = 1, \dots, n$.

Proposizione 9 *Sia A un dominio a fattorizzazione unica. Allora A è un dominio con il massimo comune divisore. Inoltre, se*

$$x = p_1^{a_1} \dots p_n^{a_n}, \quad y = p_1^{b_1} \dots p_n^{b_n},$$

dove $p_1, \dots, p_n$ sono elementi irriducibili distinti di A e $a_i, b_i \geq 0$, per $i = 1, \dots, n$, si ha $(x, y) = p_1^{m_1} \dots p_n^{m_n}$, dove $m_i := \min\{a_i, b_i\}$, per $i = 1, \dots, n$.

Dimostrazione: È una semplice verifica, osservando che se uno tra gli elementi x e y è invertibile si ha $(x, y) = 1$. □

Teorema 10 *Le seguenti condizioni sono equivalenti per un dominio A:*

(i) *A è un dominio a fattorizzazione unica;*

(ii) *A è atomico e ogni elemento irriducibile di A è un elemento primo;*

(iii) *A è un dominio atomico con il massimo comune divisore;*

(iv) *Ogni elemento non nullo e non invertibile di A si fattorizza in un numero finito di elementi primi;*

Dimostrazione: (i) $\Rightarrow$ (iii) segue dal Proposizione 9.

(iv) $\Rightarrow$ (ii) per il Corollario 6.

(ii) $\Rightarrow$ (i) Supponiamo che $p_1 \dots p_r = q_1 \dots q_s$, dove i p_i e q_j sono elementi irriducibili per $i = 1, \dots, r$ e $j = 1, \dots, s$. Poiché p_1 è un elemento primo di A, allora p_1 divide uno degli elementi q_j. A meno di riordinare i fattori q_j, possiamo supporre che p_1 divida q_1. Allora, essendo p_1 e q_1 entrambi irriducibili, essi devono essere associati, cioè deve essere $q_1 = up_1$, con $u \in \mathcal{U}(A)$. Quindi, cancellando p_1, risulta $p_2 \dots p_r = uq_2 \dots q_s$. Così proseguendo, si ottiene che $r = s$ e, a meno dell'ordine, gli elementi p_i e q_i sono associati per $i = 1, \dots, r$.

(ii) $\Rightarrow$ (iv) è chiaro.

(iv) $\Rightarrow$ (ii) A è atomico, perché gli elementi irriducibili sono primi Proposizione 2. Sia q un elemento non nullo e non invertibile di A. Se $q = p_1 \dots p_n$ si fattorizza in $n \geq 2$ elementi primi allora q non è irriducibile. Quindi ogni elemento irriducibile è primo. □

Domini di Bezout e a ideali principali

Se $d = (x, y)$ è un massimo comune divisore di x e y ed è possibile scrivere $d = ax + by$ per opportuni $a, b \in A$, questa espressione si chiama una *identità di Bezout* per d.

Proposizione 11 *Dati due elementi non nulli x, y di un dominio A, le seguenti condizioni sono equivalenti:*

(i) *$\langle x, y \rangle =: \langle d \rangle$ è un ideale principale;*

(ii) *$(x, y) = d$ e $d = ax + by$, per opportuni a, $b \in A$ (cioè esiste un massimo comune divisore di x e y ed una identità di Bezout per esso).*

Dimostrazione: Ricordiamo che d divide x e y se e soltanto se $\langle x, y \rangle \subseteq \langle d \rangle$.

(i) $\Rightarrow$ (ii) Se $\langle x, y \rangle = \langle d \rangle$, d divide x, y e $d = ax + by$, per a, $b \in A$. Dunque ogni d' che divide x e y divide d e segue che $(x, y) = d$.

(ii) $\Rightarrow$ (i) Se $(x, y) = d$, $\langle x, y \rangle \subseteq \langle d \rangle$ e se $d = ax + by$, $\langle d \rangle \subseteq \langle x, y \rangle$. □

Un dominio si dice *a ideali principali* se ogni suo ideale è principale. Inoltre, un dominio che soddisfa le condizioni equivalenti della Proposizione

11 si chiama un *dominio di Bezout*. Dunque, per induzione sul numero dei generatori, un dominio A è di Bezout se e soltanto se ogni ideale finitamente generato è principale.

Corollario 12 *Se A è un dominio a ideali principali, allora A è un dominio di Bezout.*

Proposizione 13 *Sia A un dominio in cui ogni ideale primo è principale (in particolare un dominio a ideali principali) e sia $p \in A$ un elemento non nullo e non invertibile. Le seguenti condizioni sono equivalenti:*

(i) *$\langle p \rangle$ è un ideale massimale;*

(ii) *$\langle p \rangle$ è un ideale primo;*

(iii) *p è un elemento primo di A;*

(iv) *p è un elemento irriducibile di A.*

Dimostrazione: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) sono sempre vere.

(iv) $\Rightarrow$ (i) Sia p un elemento irriducibile di A e sia $M := \langle q \rangle$ un ideale massimale tale che $p \in M$. Allora q divide p e q non è invertibile. Dunque q è associato a p e ne segue che $\langle p \rangle = \langle q \rangle = M$ è un ideale massimale. $\square$

Proposizione 14 *Un dominio a ideali principali è un dominio a fattorizzazione unica.*

Dimostrazione: Sia A un dominio a ideali principali. Poiché ogni elemento irriducibile di A è primo (Proposizione 13), per il Teorema 10, basta far vedere che A soddisfa la condizione della catena ascendente sugli ideali principali. Sia

$$\langle x_1 \rangle \subseteq \langle x_2 \rangle \subseteq \ldots \subseteq \langle x_i \rangle \subseteq \ldots$$

una catena di ideali principali e sia $I := \bigcup_{i \geq 1} \langle x_i \rangle$. Si vede facilmente che I è un ideale di A e quindi I è principale per ipotesi. Se $I = \langle x \rangle$, per definizione $x \in \langle x_n \rangle$ per qualche $n \geq 1$. Ne segue che $I = \langle x_n \rangle = \langle x_m \rangle$ per $m \geq n$. $\square$

Esempio 15 **(1)** Se A è un dominio a fattorizzazione unica, per il così detto *Lemma di Gauss*, ogni anello di polinomi su A è un dominio a fattorizzazione unica. In particolare ogni anello di polinomi a coefficienti in un campo o nell'anello degli interi $\mathbb{Z}$ è un dominio a fattorizzazione unica.

(2) L'anello dei polinomi $\mathbb{Z}[X]$ non è a ideali principali, anche se lo è $\mathbb{Z}$.

Ad esempio, si può verificare facilmente che l'ideale $I := \langle 2, X \rangle$, formato dai polinomi con termine noto pari non è principale. Infatti un suo generatore $f(X)$ dovrebbe dividere sia 2 che X. Allora $f(X) = 1$, mentre $1 \notin I$.

Domini euclidei

Una classe importante di domini a ideali principali (e quindi a fattorizzazione unica) è data dai domini euclidei.

Una *funzione euclidea* su dominio A è un'applicazione $\phi : A \setminus \{0\} \longrightarrow \mathbb{N}$ tale che, per ogni a, $b \in A \setminus \{0\}$:

(1) Se a divide b, allora $\phi(a) \leq \phi(b)$;

(2) (Divisione euclidea) esistono q, $r \in A$ (detti rispettivamente *quoziente* e *resto*) tali che $a = bq + r$ e $r = 0$ oppure $\phi(r) < \phi(b)$.

Se sul dominio A esiste una funzione euclidea ϕ, A si chiama un *dominio euclideo rispetto a* ϕ.

Esempio 16 (1) L'anello degli interi $\mathbb{Z}$ è euclideo rispetto al modulo, l'anello dei polinomi $K[X]$ a coefficienti in un campo è euclideo rispetto al grado

(2) L'anello degli *interi di Gauss* $\mathbb{Z}[i]$ è euclideo rispetto alla norma complessa.

Per effettuare la divisione di α per β si può procedere nel modo seguente. Posto $\eta := \alpha/\beta$, se $\eta \notin \mathbb{Z}[i]$, si cerca $\delta \in \mathbb{Z}[i]$ tale che $|N(\eta - \delta)| < 1$. Allora $\eta = \delta + (\eta - \delta)$ e, moltiplicando per β, si ottiene $\alpha = \delta\beta + (\eta - \delta)\beta$. Inoltre $\rho := (\eta - \delta)\beta = \alpha - \delta\beta \in \mathbb{Z}[i]$ e $|N(\rho)| = |N(\eta - \delta)||N(\beta)| < |N(\beta)|$.

(3) Il resto della divisione euclidea non è sempre unico. Anzi, si può dimostrare che il resto è unico se e soltanto se A è isomorfo ad un anello di polinomi $K[X]$, mentre esistono al più soltanto due resti se e soltanto se A è isomorfo a $\mathbb{Z}$.

Proposizione 17 *Un dominio euclideo A è a ideali principali. Precisamente, ogni ideale non nullo $I \subseteq A$ è principale, generato da un elemento di valutazione minima.*

Dimostrazione: Sia $I \subseteq A$ non nullo. Allora il sottoinsieme $\{\phi(x)\,;\ 0 \neq x \in I\}$ di $\mathbb{N}$ è non vuoto e perciò esiste un elemento non nullo $a \in I$ di valutazione minima $\phi(a)$. Per ogni elemento non nullo $y \in I$, possiamo scrivere $y = aq + r$. Poiché $r \in I$, non può essere $\phi(r) < \phi(a)$; quindi $r = 0$ e y è un multiplo di a. □

Proposizione 18 *Sia A un dominio euclideo rispetto alla funzione ϕ e sia $x \in A \setminus \{0\}$. Allora:*

(1) $\phi(x) \geq \phi(1)$.

(2) *Se y divide x e $\phi(x) = \phi(y)$, allora x e y sono associati.*

(3) *x è invertibile se e soltanto se $\phi(x) = \phi(1)$.*

Dimostrazione: (1) Poiché $x = x1$, si ha $\phi(x) = \phi(x1) \geq \phi(1)$.

(2) Sia $y = xz$. Poiché $y \in \langle x \rangle$, se $\phi(y) = \phi(x)$, allora y ha valutazione minima nell'ideale $\langle x \rangle$. Dunque y genera l'ideale $\langle x \rangle$ ed è per questo associato a x.

(3) Se x è invertibile, allora $xz = 1$ e $\phi(1) = \phi(xz) \geq \phi(x)$. Quindi per (1) vale l'uguaglianza. Il viceversa segue da (2) per $y = 1$. □

Osservazione 19 Se A è un dominio euclideo, un massimo comune divisore di due elementi $x, y \in A$ si può calcolare con l'*algoritmo euclideo delle divisioni successive*. Precisamente, se

$$\begin{aligned}
x &= yq_1 + r_1\,, & r_1 &= 0 \text{ oppure } \phi(r_1) < \phi(x);\\
y &= r_1q_2 + r_2\,, & r_2 &= 0 \text{ oppure } \phi(r_2) < \phi(r_1);\\
&\cdots\cdots & &\cdots\cdots\\
r_{n-2} &= r_{n-1}q_n + r_n\,, & r_n &= 0 \text{ oppure } \phi(r_n) < \phi(r_{n-1});\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Allora un massimo comune divisore $d := (x, y)$ è l'ultimo resto non nullo r_n (notiamo che il procedimento ha termine perché $\phi(x) > \phi(r_1) > \phi(r_2) > \ldots$ è una successione strettamente decrescente di interi positivi).

Inoltre, dalla successione di uguaglianze:

$$\begin{aligned}
r_n &= r_{n-2} - q_nr_{n-1};\\
r_{n-1} &= r_{n-3} - q_{n-1}r_{n-2};\\
&\cdots\cdots
\end{aligned}$$

per sostituzioni successive, si ottiene esplicitamente una identità di Bezout per d.

Quozienti di domini a ideali principali

Se A è un dominio a ideali principali e $a \in A$, le proprietà dell'anello quoziente $\frac{A}{\langle a \rangle}$ sono determinate dalla fattorizzazione dell'elemento a.

Intanto ricordiamo che gli ideali di $\frac{A}{\langle a \rangle}$ sono in corrispondenza biunivoca con gli ideali di A contenenti a. Se A è a ideali principali, tali ideali sono tutti principali, generati da un divisore di a (anche se $\frac{A}{\langle a \rangle}$ non è un dominio) e dunque gli ideali $\frac{A}{\langle a \rangle}$ sono tutti principali generati dalle classi modulo l'ideale $\langle a \rangle$ dei divisori dell'elemento a.

Precisamente, se $a = p^{e_1} \ldots p^{e_n}$ è la fattorizzazione di a in elementi primi distinti, tutti e soli gli ideali di $\frac{A}{\langle a \rangle}$ sono quelli generati dalle classi modulo $\langle a \rangle$ degli elementi $p^{a_1} \ldots p^{a_n}$ con $0 \leq a_i \leq e_i$. In particolare, gli ideali massimali sono quelli generati dalle classi dei p_i e $\frac{A}{\langle a \rangle}$ è un campo se e soltanto se $a = p$ è primo.

Notiamo anche che gli ideali $Q_i := \langle p_i^{e_i} \rangle$ e $Q_j := \langle p_j^{e_j} \rangle$ sono coprimi per $i \neq j$ e, per il Teorema Cinese dei Resti, si ha un isomorfismo:

$$\frac{A}{\langle a \rangle} \longrightarrow \frac{A}{Q_i} \times \cdots \times \frac{A}{Q_n}, \quad x + \langle a \rangle \to (x + Q_1, \ldots, x + Q_n).$$

Riguardo alla divisibilità in $\frac{A}{\langle a \rangle}$, abbiamo che ogni classe $\overline{x} := x + \langle a \rangle \in \frac{A}{\langle a \rangle}$ è invertibile oppure è uno zero-divisore. Questo dipende dall'esistenza di una identità di Bézout. Infatti, sia $d = (x, a)$ un massimo comune divisore di x e a e sia $d = \alpha x + \beta a$ una identità di Bézout. Allora $\overline{d} = \overline{\alpha x}$.

Se x e a sono coprimi, scegliendo $d = 1$, si ha $\overline{1} = \overline{\alpha x}$; quindi $\overline{x}$ è invertibile in $\frac{A}{\langle a \rangle}$, con inverso $\overline{\alpha}$. Questo accade se e soltanto se p_i non divide a per ogni $i = 1, \ldots, n$.

Se invece d non è invertibile, scrivendo $a = a'd$, $x = x'd$, abbiamo $xa' = x'da' = x'a$, da cui $\overline{x}\overline{a'} = \overline{0}$. Poiché a e a' non sono associati, si ha che $a' \notin \langle a \rangle$, dunque $\overline{a'} \neq \overline{0}$ e $\overline{x}$ è uno zerodivisore in $\frac{A}{\langle a \rangle}$.

Quozienti di domini euclidei

Se A è euclideo, con valutazione ϕ, possiamo dividere ogni elemento x per a, ovvero scrivere $x = qa + r$, con $r = 0$ oppure $\phi(r) < \phi(a)$. Posto al solito $\overline{x} := x + \langle a \rangle$, poiché $\overline{x} = \overline{r}$, ogni classe modulo $\langle a \rangle$ può essere rappresentata da un elemento con valutazione minore strettamente di quella di a. Ovvero

$$\frac{A}{\langle a \rangle} = \{\overline{x}\,;\ x = 0 \text{ oppure } \phi(x) < \phi(a)\}.$$

Inoltre una identità di Bézout si può calcolare con l'Algoritmo Euclideo delle divisioni successive. Questo semplifica il calcolo degli inversi in $\frac{A}{\langle a \rangle}$.

Esempio 20 **(1)** Se K è un campo, l'anello dei polinomi $K[X]$ è euclideo rispetto al grado. Dunque, dato un polinomio non costante $p(X)$ risulta

$$\frac{K[X]}{\langle p(X) \rangle} = \{\overline{f(X)}\,;\ f(X) = 0 \text{ oppure } \deg f(X) < \deg p(X)\}.$$

Notiamo che, date due costanti $a, b \in K$, $a - b \in \langle p(X) \rangle$ se e soltanto se $a - b = 0$, cioè $a = b$. Perciò si ha un isomorfismo iniettivo

$$K \longrightarrow \frac{K[X]}{\langle p(X) \rangle}; \quad a \mapsto \overline{a} := a + \langle p(X) \rangle.$$

Ne segue che K e l'anello quoziente $\frac{K[X]}{\langle p(X) \rangle}$ hanno stessa caratteristica. Tale caratteristica è uguale a zero oppure è prima.

(2) Se $p(X) := \sum a_i X^i \in K[X]$ è irriducibile, come visto sopra, $F := \frac{K[X]}{\langle p(X) \rangle}$ è un campo contenente isomorficamente K. Dunque, identificando le

costanti di K con le loro classi in F, ogni polinomio $f(X) \in K[X]$ è anche un polinomio a coefficienti in F.

Inoltre, posto $\alpha := \overline{X}$, se $f(X) = \sum c_i X^i$, risulta

$$\overline{f(X)} = \overline{\sum c_i X^i} = \sum \overline{c_i}\,\overline{X^i} = \sum \overline{c_i}\,\overline{X}^i = \sum c_i \alpha^i.$$

In questo modo, si vede che il polinomio $p(X)$ non è più irriducibile su F, perché ha una radice in F. Infatti

$$\overline{0} = \overline{p(X)} = \sum c_i \alpha^i.$$

Dunque $\alpha \in F$ è una radice di $p(X)$. Inoltre, poiché $\overline{f(X)} = \overline{0}$ se e soltanto se $f(X) \in \langle p(X) \rangle$ se e soltanto se $p(X)$ divide $f(X)$, abbiamo che $f(\alpha) = 0$ se e soltanto se $p(X)$ divide $f(X)$.

Ne segue che F è uno spazio vettoriale su K di dimensione n, infatti, con le notazioni precedenti,

$$F := \frac{K[X]}{\langle p(X) \rangle} = \{\overline{f(X)}\,;\ f(X) = 0 \text{ oppure } \deg f(X) < n\} = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, c_i \in K\}.$$

Allora $1, \alpha, \ldots, \alpha^{n-1}$ generano F su K. Inoltre essi sono anche linearmente indipendenti su K, perché se $f(\alpha) = 0$, con $f(X) \in K[X]$ non nullo, deve essere in particolare $\deg f(X) \geq n$.

(3) Se K è un campo finito, i polinomi di grado fissato su K sono in numero finito. Dunque l'anello quoziente $\frac{K[X]}{\langle p(X) \rangle}$ ha un numero finito di elementi. In particolare, se $p(X)$ è irriducibile, il campo $F := \frac{K[X]}{\langle p(X) \rangle}$ è finito e contiene il sottocampo fondamentale con p elementi $\mathbb{F}_p$, dove p è la caratteristica di K.

Poiché poi F è uno spazio vettoriale su K di dimensione $n = \deg p(X)$, F ha $|K|^n$ elementi. In particolare, se $K = \mathbb{F}_p$, F ha p^n elementi.

Ad esempio, il polinomio $p(X) = X^3 + X^2 + 1 \in \mathbb{F}_2$ è irriducibile, dunque

$$F := \frac{\mathbb{F}_2[X]}{\langle p(X) \rangle} = \{\overline{f(X)}\,;\ f(X) \in \mathbb{F}_2[X], f(X) = 0 \text{ oppure } \deg f(X) \leq 2\} = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

è un campo con $8 = 2^3$ elementi.

(4) I quozienti dell'anello $\mathbb{Z}[i]$ hanno sempre un numero finito di elementi. Infatti, gli interi di Gauss di norma limitata sono in numero finito e dato $\alpha \in Z[i]$, risulta

$$A := \frac{\mathbb{Z}[i]}{\langle \alpha \rangle} = \{\beta + \langle \alpha \rangle\,;\ N(\beta) < N(\alpha)\}.$$

Notando che $n := N(\alpha) = \alpha\overline{\alpha} \in \langle\alpha\rangle$ (dove $\overline{\alpha}$ è il coniugato complesso di α), si vede che $n(\beta + \langle\alpha\rangle) = n\beta + \langle\alpha\rangle = \overline{0}$. Dunque la caratteristica dell'anello quoziente A divide n.

In particolare, se $N(\alpha) = p$ è un numero primo, α è irriducibile (perché la norma è moltiplicativa) e A è un campo finito di caratteristica p.

Vedremo nel prossimo esempio che, se $N(\alpha) = p$, A è isomorfo a $\mathbb{F}_p$. Più in generale, è possibile dimostrare che A ha $n := N(\alpha)$ elementi.

(5) Sia $p \in \mathbb{Z}$ un numero primo. Si verifica facilmente che si ha un isomorfismo

$$\frac{\mathbb{Z}[i]}{\langle p\rangle} \longrightarrow \frac{\mathbb{F}_p[X]}{\langle X^2 + [1]\rangle}\,; \quad a + bi + \langle p\rangle \to [a] + [b]X + \langle X^2 + [1]\rangle.$$

Poiché $\dfrac{\mathbb{F}_p[X]}{(X^2 + [1])} = \{\overline{a + bX}\,;\ a, b \in \mathbb{F}_p\}$, l'anello $A := \dfrac{\mathbb{Z}[i]}{\langle p\rangle}$ ha p^2 elementi. Inoltre A ha caratteristica p, perché contiene isomorficamente $\mathbb{F}_p$.

Osserviamo che $A := \dfrac{\mathbb{Z}[i]}{\langle p\rangle}$ è un campo se e soltanto se p è irriducibile in $\mathbb{Z}[i]$, se e soltanto se il polinomio $X^2 + 1$ è irriducibile modulo p.

Inoltre p è riducibile in $\mathbb{Z}[i]$ se e soltanto se esistono interi di Gauss di norma p. In questo caso, se $N(\alpha) = p$, si ha $p = \alpha\overline{\alpha}$ (dove $\overline{\alpha}$ è il coniugato complesso di α) e

$$\frac{\mathbb{Z}[i]}{\langle p\rangle} \longrightarrow \frac{\mathbb{Z}[i]}{\langle\alpha\rangle} \times \frac{\mathbb{Z}[i]}{\langle\overline{\alpha}\rangle}$$

dove $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$ e $\dfrac{\mathbb{Z}[i]}{\langle\overline{\alpha}\rangle}$ sono campi isomorfi a $\mathbb{F}_p$.

Per verificare quest'ultima osservazione, notiamo che si ha una suriezione

$$\varphi : \frac{\mathbb{Z}[i]}{\langle p\rangle} \longrightarrow \frac{\mathbb{Z}[i]}{\langle\alpha\rangle}\,; \quad \beta + \langle p\rangle \mapsto \beta + \langle\alpha\rangle.$$

Quindi l'ordine di $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$ divide l'ordine di $\dfrac{\mathbb{Z}[i]}{\langle p\rangle}$, che come visto sopra è uguale a p^2. Dunque $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$ può avere ordine p oppure p^2. Siccome $\alpha \notin \langle p\rangle$, perché $p = \alpha\overline{\alpha}$ e $\overline{\alpha}$ non è invertibile, il nucleo di φ è non nullo. Quindi φ non è un isomorfismo e $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$ ha p elementi.

Analogamente, scambiando α con $\overline{\alpha}$ si vede che anche $\dfrac{\mathbb{Z}[i]}{\langle\overline{\alpha}\rangle}$ ha p elementi.