

Una introduzione all'Algebra

III. Strutture algebriche

Luca Barbieri Viale

<http://users.unimi.it/barbieri/>

Dipartimento di Matematica "F. Enriques"
Università degli Studi di Milano

© Versione L^AT_EX 2010

⊙ **Attenzione!** Queste pagine raccolgono il terzo capitolo delle note del corso Algebra 1 - *Una introduzione all'Algebra* - di Matematica a Milano. Non intendono essere un testo compiuto ma solo una raccolta di **concetti essenziali** che sono da utilizzare come compendio delle lezioni in aula. Le note complete sono articolate in tre capitoli

- I. Teoria degli Insiemi
- II. Aritmetica
- III. Strutture Algebriche

Paradigma

Assumo note le principali proprietà degli interi, dei razionali e delle congruenze. Abbiamo visto che \mathbb{Z} e $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$ sono dotati di proprietà specifiche deducibili dalle operazioni di somma e prodotto. Vogliamo ora formalizzare queste operazioni per un insieme qualunque e chiederci cosa sono gli “interi” e le “congruenze” in un contesto più ampio.

1 Gruppi

Semigrupperi

Un insieme S con una operazione binaria $\cdot : S \times S \rightarrow S$ ($a, b \mapsto a \cdot b$) associativa ovvero tale che $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per ogni $a, b, c \in S$ si dice semigruppero.
Commutativo se $a \cdot b = b \cdot a$ per ogni $a, b \in S$.

La cardinalità $|S|$ si dice anche ordine del semigruppero. La notazione moltiplicativa $a \cdot b$ è del tutto arbitraria; per semplicità, se non si rischia confusione, denoteremo spesso ab una generica operazione in un semigruppero. Denoteremo anche (S, \cdot) un semigruppero.

Ad esempio, sia X un insieme e sia $X^\circ \stackrel{\text{def}}{=} \{f : X \rightarrow X/f \text{ appl.}\}$. La composizione di applicazioni $\circ : X^\circ \times X^\circ \rightarrow X^\circ$ ($(f, g) \mapsto f \circ g$) determina un semigruppero su X° . Non commutativo, in generale.

Cancellazione

In un semigruppero un elemento $x \in S$ si dice cancellabile a sinistra (risp. a destra) se $xb = xc \Rightarrow b = c$ (risp. $bx = cx \Rightarrow b = c$) per ogni $b, c \in S$. Vale la legge di cancellazione in un semigruppero S se ogni elemento $x \in S$ è cancellabile a destra e a sinistra.

Ad esempio, $(\mathbb{N}, +)$ soddisfa la legge di cancellazione.

Monoide

Un semigruppero (S, \cdot) si dice monoide se esiste un elemento neutro $1 \in S$ tale che $1 \cdot a = a \cdot 1 = a$ per ogni $a \in S$.

Se 1 esiste è unico. Infatti, se $e \cdot a = a \cdot e = a$ per ogni $a \in S$ allora $e \cdot 1 = e = 1$.

Ad esempio, $(X^\circ, \circ, 1_X)$ è un monoide. Anche $(\mathbb{N}, +, 0)$ oppure $(\mathbb{Z}, \cdot, 1)$.

Idempotenti

Un elemento $x \in S$ in un semigruppò (S, \cdot) tale che $x^2 \stackrel{\text{def}}{=} x \cdot x = x$ si dice *idempotente*

Proposizione 1.1 *Sia (S, \cdot) un monoide. Un elemento $e \in S$ cancellabile a sinistra oppure a destra è idempotente se e solo se $e = 1$.*

Dimostrazione: Si ha $e \cdot e = e \cdot 1$ ma anche $e \cdot e = 1 \cdot e$ poichè e idempotente. Siccome e è cancellabile a sinistra o a destra si ha $e = 1$. ⊙

In un monoide che soddisfa la legge di cancellazione non vi sono idempotenti a parte l'elemento neutro.

Invertibili

Sia $(S, \cdot, 1)$ un monoide. Un elemento $a \in S$ si dice *invertibile* se esiste $x \in S$ tale che $x \cdot a = a \cdot x = 1$.

Se tale x esiste è unico: $x \stackrel{\text{def}}{=} a^{-1}$ si dice inverso di a . Infatti, $x = 1x = (x'a)x = x'1 = x'$ se anche $x'a = 1$.

Notare che se $a, b \in S$ sono invertibili anche ab è invertibile. Infatti, $b^{-1}a^{-1}$ è l'inverso.

Gruppo

Si dice *gruppo* un monoide in cui tutti gli elementi sono invertibili. Si dice *gruppo abeliano* se è inoltre commutativo.

Ad esempio, $(\mathbb{Z}, +, 0)$ è un gruppo abeliano.

Proposizione 1.2 *Ogni gruppo soddisfa la legge di cancellazione.*

Dimostrazione: Se $ab = ac$ in un gruppo allora $b = 1b = a^{-1}(ab) = a^{-1}(ac) = 1c = c$, quindi ogni a è cancellabile a sinistra. Analogamente a destra. ⊙

Ad esempio, X° non è un gruppo, in generale. Se $*$ $\in X$ l'applicazione costante $x \mapsto *$ non è cancellabile a sinistra se $|X| > 1$.

Teorema 1.3 *Un monoide finito M è un gruppo se e solo se soddisfa la legge di cancellazione.*

Dimostrazione: Sia $f : M \rightarrow M$ l'applicazione $f(x) \stackrel{\text{def}}{=} ax$ con $a \in M$ fissato. Allora f è iniettiva in quanto vale la legge di cancellazione quindi surgettiva poichè M è finito. Esiste $x \in M$ tale che $f(x) = 1$ ovvero $ax = 1$. Analogamente considerando $g(y) \stackrel{\text{def}}{=} ya$ si ha che esiste $y \in M$ tale che $ya = 1$. Quindi $x = y = a^{-1}$ in quanto $y = y1 = y(ax) = (ya)x = 1x = x$. \odot

Ad esempio, $(\mathbb{Z}_m, +, 0)$ è un gruppo finito. Se $\mathbb{Z}^{\neq 0} \stackrel{\text{def}}{=} \mathbb{Z} - \{0\}$ allora nel monoide abeliano $(\mathbb{Z}^{\neq 0}, \cdot, 1)$ vale la legge di cancellazione ma questo non è un gruppo. Chiaramente $(\mathbb{Q}^{\neq 0}, \cdot, 1)$ è un gruppo. Analogamente, $(\mathbb{Z}_p^{\neq 0}, \cdot, 1)$ è un gruppo se p è primo. Infatti, $ax \equiv_p 1$ ha soluzioni se $(a, p) = 1$.

\odot **Attenzione!** Gli elementi invertibili del monoide $(X^\circ, \circ, 1_X)$ sono le applicazioni bigettive. Sia $S_X \stackrel{\text{def}}{=} \{f : X \rightarrow X/f \text{ bigettiva}\} \subset X^\circ$. Il gruppo $(S_X, \circ, 1_X)$ è il principale esempio di gruppo non commutativo ed è detto gruppo simmetrico. Se $|X| = n$ allora S_X si denota S_n ed è non commutativo se $n > 2$.

Notazione additiva

Per un gruppo abeliano G è spesso conveniente la notazione additiva ovvero si assume l'esistenza di una operazione $+$: $G \times G \rightarrow G$ e un elemento $0 \in G$ tali che

- (a) $a + (b + c) = (a + b) + c$ (associatività)
- (b) $a + b = b + a$ (commutatività)
- (c) $a + b = a + c \Rightarrow b = c$ (cancellazione)
- (d) $2a = a + a$ e per $n \geq 2$ poniamo $na = (n - 1)a + a$
- (e) $a + 0 = a$ (elemento neutro)
- (f) $-a + a = 0$ (inverso)

per ogni $a, b, c \in G$.

2 Anelli

Si dice anello una terna $(A, +, \cdot)$ ovvero un insieme A con due operazioni binarie $+$ e \cdot tali che:

- (a) $(A, +, 0)$ è un gruppo abeliano
 (b) (A, \cdot) è un semigruppso ovvero vale la proprietà associativa

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

e inoltre

- (c) valgono le proprietà distributive

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

per ogni $a, b, c \in A$.

Inoltre, un anello $(A, +, \cdot)$ si dice unitario se possiede l'identità moltiplicativa $1 \in A$ ovvero se $(A, \cdot, 1)$ è un monoide e si dice commutativo se $(A, \cdot, 1)$ è commutativo.

Notare che dalla distributività si ha che $a \cdot 0 = 0 \cdot a = 0$ per ogni $a \in A$. Quindi $1 = 0$ in A se e solo se $A = \{0\}$ è l'anello nullo.

Ad esempio, $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_m, +, \cdot)$ sono anelli commutativi con identità. Le matrici quadrate $(M_n(A), +, \cdot)$ con entrate in un anello A e rispetto alle operazioni di somma di matrici e prodotto righe per colonne sono un anello non commutativo (se $n \geq 2$) anche se A è commutativo.

Notare che ogni gruppo abeliano $(G, +, 0)$ si può considerare come un anello in cui $a \cdot b = 0$ per ogni $a, b \in G$. In particolare, la struttura di anello non è unica come d'altra parte non è unica la struttura di gruppo.

Dominio

Sia A un anello commutativo unitario e sia $A^{\neq 0} \stackrel{\text{def}}{=} A - \{0\}$. L'anello A si dice dominio se $(A^{\neq 0}, \cdot, 1)$ è un monoide che soddisfa la legge di cancellazione. In particolare, se $a \neq 0$ e $b \neq 0$ allora $a \cdot b \neq 0$ in A .

Al contrario, diciamo che un elemento $a \in A^{\neq 0}$ di un anello qualunque è uno zero-divisore se esiste $b \in A^{\neq 0}$ tale che $a \cdot b = 0$. Se l'anello non è commutativo a è zero-divisore sinistro e b è zero-divisore destro. In questo caso, $a \cdot b \notin A^{\neq 0}$ e dunque $A^{\neq 0}$ non è chiuso rispetto al prodotto in A . Inoltre, siccome $a \cdot b = 0 = a \cdot 0$ ma $b \neq 0$ si ha che a non è cancellabile a sinistra.

Lemma 2.1 *Sia A anello e $a \in A$. Se $a \neq 0$ non è zero-divisore sinistro allora è cancellabile a sinistra ovvero*

$$ab = ac \Rightarrow b = c$$

per ogni $b, c \in A$. Analogamente a destra.

Dimostrazione: Se $ab = ac$ allora $a(b - c) = 0$ da cui $b = c$ se a non è zero-divisore sinistro. \odot

Proposizione 2.2 *Un anello commutativo unitario non nullo è un dominio se e solo se non ha zero-divisori.*

Dimostrazione: Infatti, dal lemma segue che se A non ha zero-divisori allora $(A^{\neq 0}, \cdot, 1)$ è un monoide che soddisfa la legge di cancellazione. \odot

Ad esempio, $A = \mathbb{Z}$ è un dominio, mentre $A = \mathbb{Z}_m$ ha zero-divisori se m non è primo.

Campo

Un anello A si dice *corpo* se $(A^{\neq 0}, \cdot, 1)$ è un gruppo. Si dice *campo* se tale gruppo è commutativo.

Ad esempio, $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi ma anche \mathbb{Z}_p con p primo. Notare che il più piccolo campo è $\mathbb{Z}_2 = \{0, 1\}$ che ha due elementi.

Dato un anello A unitario possiamo considerare $A^* \stackrel{\text{def}}{=} \{a \in A \mid a \text{ invertibile}\}$ il sottoinsieme degli elementi con inverso moltiplicativo. Si ha che $(A^*, \cdot, 1)$ è un gruppo. Inoltre A è un corpo se e solo se $A^* = A^{\neq 0}$.

Proposizione 2.3 *Se A è un campo allora è un dominio.*

Dimostrazione: Basta osservare che $a \in A^*$ invertibile non è zero divisore. Infatti, se $ab = 0$ allora $a^{-1}ab = 0$ e quindi $b = 0$. \odot

Lemma 2.4 *Se A è un anello commutativo finito non-nullo e senza zero-divisori allora A è un campo.*

Dimostrazione: Sia $a \neq 0$ e sia $f : A \rightarrow A$ definita da $f(x) \stackrel{\text{def}}{=} ax$. Siccome a è cancellabile si ha che f è iniettiva quindi surgettiva poichè A finito. Quindi esiste $e \in A$ tale che $ae = a$. Dato $b \in A$ esiste $c \in A$ tale che $ac = b$ ma anche $ca = b$ poichè A è commutativo. Dunque $cae = be$ ovvero $b = be$. In conclusione $e = 1$ è l'identità moltiplicativa e $f^{-1}(1) = a^{-1}$ è l'inverso. \odot

Corollario 2.5 *Un anello finito è un campo se e solo se è un dominio.*

Sottoanello

Sia $(G, +, 0)$ un gruppo. Un sottogruppo $H \subseteq G$ è un sottoinsieme non vuoto tale che

$$(1) \quad a, b \in H \Rightarrow a + b \in H$$

$$(2) \quad a \in H \Rightarrow -a \in H$$

siano soddisfatte per ogni $a, b \in H$. Chiaramente anche $0 \in H$ in quanto $-a + a = 0$.

Ad esempio, $G = \mathbb{Z}$ e $H = m\mathbb{Z} \stackrel{\text{def}}{=} \{mn \mid n \in \mathbb{Z}\}$ per $m \in \mathbb{N}$.

Lemma 2.6 *Se $H \subseteq \mathbb{Z}$ è un sottogruppo allora $H = n\mathbb{Z}$ per qualche $n \in \mathbb{N}$.*

Dimostrazione: Se $H = \{0\}$ si ha $n = 0$. Se $H \neq \{0\}$ sia $n \in H$ con $n > 0$ minimo (deve esistere in quanto $h \in H$, $h \neq 0$ implica $-h \in H$ e \mathbb{N} è ben ordinato). Dunque $n\mathbb{Z} \subseteq H$. Inoltre dato $x \in H$ si ha che $x = qn + r$ con $r < n$. Quindi $r = x - qn \in H$ e dunque $r = 0$ poichè n è minimo tra gli elementi positivi. ◊

Sia A un anello. Un sottoinsieme $B \subseteq A$ si dice sottoanello se

$$(1) \quad B \text{ è un sottogruppo di } (A, +, 0)$$

$$(2) \quad a, b \in B \Rightarrow a \cdot b \in B$$

$$(3) \quad 1 \in A \Rightarrow 1 \in B$$

L'intersezione arbitraria di sottoanelli è un sottoanello.

Ad esempio, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{C}$ sottoanelli. Notare che l'anello nullo non è un sottoanello di \mathbb{Z} e \mathbb{Z} è il più piccolo sottoanello di \mathbb{C} . Infatti, dato A con $1 \in A$ si ha che $A^\dagger \stackrel{\text{def}}{=} \{n1 \mid n \in \mathbb{Z}\}$ è un sottoanello di A contenuto in tutti i sottoanelli di A . Se A^\dagger è infinito si dice che A ha caratteristica zero mentre se A^\dagger è finito si dice che A ha caratteristica positiva e si denota $\text{char}(A) \stackrel{\text{def}}{=} |A^\dagger|$. In particolare, $\text{char}(\mathbb{Z}_m) = m$.

Sottoanello generato da un sottoinsieme

Sia $A \subseteq B$ sottoanello commutativo unitario e sia $b \in B$. Ad esempio, $\mathbb{Z} \subset \mathbb{C}$ e $\alpha \in \mathbb{C}$. Costruiamo il più piccolo sottoanello di B contenente A e b . Se $a \in A$ dunque $b, b^2, b^3, \dots, ab, ab^2, \dots$ e loro somme saranno tutti suoi elementi. In generale, tutte le espressioni $a_0 + a_1b + a_2b^2 + \dots + a_nb^n$ saranno

tutti suoi elementi per ogni $a_i \in A$ con $i = 0, \dots, n$. Con le operazioni indotte da B l'insieme $A[b]$ di tali espressioni è chiaramente un sottoanello di B . Chiaramente $A[b]$ è contenuto in tutti i sottoanelli di B contenenti A e b . Ad esempio, abbiamo dunque costruito anelli $\mathbb{Z}[\alpha]$ per ogni $\alpha \in \mathbb{C}$. In particolare, per $\alpha = i$ tale che $i^2 = -1$ otteniamo gli interi di Gauss ovvero

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

Per $S \subseteq B$ un sottoinsieme arbitrario, il più piccolo sottoanello di B contenente A e S è l'anello $A[S]$ che ammette una descrizione del tutto analoga.

Anello quoziente

Dato $H \subseteq G$ sottogruppo di un gruppo (abeliano) $(G, +, 0)$ e $x, y \in G$ possiamo definire una relazione

$$x \simeq y \Leftrightarrow x - y \in H$$

Ad esempio, se $H = m\mathbb{Z}$ e $G = \mathbb{Z}$ allora $x \simeq y$ è la relazione di congruenza $x \equiv_m y$. In generale, è facile verificare che \simeq è una relazione di equivalenza su G . Siccome G è abeliano possiamo considerare l'insieme quoziente $G/\simeq \stackrel{\text{def}}{=} \{[g] \mid g \in G\}$ con la somma indotta

$$[g] + [g'] \stackrel{\text{def}}{=} [g + g']$$

Infatti, $g - h \in H$ e $g' - h' \in H$ implica $(g - h) + (g' - h') = (g + g') - (h + h') \in H$. Il gruppo quoziente $(G/\simeq, +, [0])$ si denota semplicemente G/H . Ad esempio, $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Ideale

In un anello A un sottogruppo additivo $I \subseteq A$ si dice ideale sinistro (risp. destro) se $a \in A$ $x \in I \Rightarrow ax \in I$ (risp. se $a \in A$ $x \in I \Rightarrow xa \in I$). Ideale bilatero se destro e sinistro: ovviamente se l'anello è commutativo si ha che sinistro \Leftrightarrow destro \Leftrightarrow bilatero.

Ad esempio, $I = m\mathbb{Z}$ sono tutti e soli gli ideali di $A = \mathbb{Z}$. Mentre $\mathbb{Z} \subset \mathbb{Q}$ è un sottoanello che non è ideale. Il gruppo quoziente \mathbb{Q}/\mathbb{Z} non eredita una struttura di anello (perchè !?).

Se $I \subseteq A$ è un ideale di un anello commutativo il gruppo quoziente A/I eredita il prodotto

$$[a] \cdot [b] \stackrel{\text{def}}{=} [a \cdot b]$$

Infatti, $[a] = [a']$ ovvero $a - a' \in I$ quindi $ab - a'b \in I$ (in quanto I ideale) ovvero $[ab] = [a'b]$ in A/I . Se A non è commutativo questo avviene se I è

bilatero poichè bisogna anche mostrare che $[b] = [b']$ implica $[ab] = [ab']$ in A/I . Se A è commutativo unitario anche A/I è commutativo unitario. Si dice che $(A/I, \cdot, [1])$ è la struttura di anello quoziente sul gruppo quoziente A/I .

Osserviamo infine che l'intersezione arbitraria di ideali è un ideale. Inoltre, dati I e J ideali di A si ha che la somma $I + J \stackrel{\text{def}}{=} \{a + b \mid a \in I, b \in J\}$ è ancora un ideale.

Dominio a ideali principali

Dato un sottoinsieme $S \subseteq A$, l'ideale (sinistro) generato da S è semplicemente l'insieme di tutte le combinazioni lineari di elementi di S a coefficienti in A ovvero

$$\mathcal{I}(S) \stackrel{\text{def}}{=} \left\{ \sum_{i=0}^k a_i s_i \mid a_i \in A, s_i \in S \right\}$$

Si ha che $\mathcal{I}(S)$ è il più piccolo ideale di A contenente S . Ad esempio, se I e J sono ideali di A e $S = I \cup J$ allora $\mathcal{I}(S) = I + J$.

Per $S = \{a\}$ si ha che $\mathcal{I}(S) = \{xa \mid x \in A\}$ si denota Aa oppure, se A è commutativo, anche (a) e si chiama ideale principale generato da $a \in A$. Un dominio A si dice a ideali principali (P.I.D.) se ogni ideale I di A è principale. Ad esempio, $A = \mathbb{Z}$ è un P.I.D.

Omomorfismo

Osserviamo che l'applicazione $\pi : A \rightarrow A/I, a \mapsto [a] \stackrel{\text{def}}{=} \pi(a)$ (proiezione sul quoziente) è tale che $[a + a'] = [a] + [a']$, $[aa'] = [a][a']$ e $[1] = 1$ in A/I .

Diciamo che un omomorfismo di anelli è un'applicazione $f : A \rightarrow B$ tra anelli $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ tale che

- (1) $f(a +_A a') = f(a) +_B f(a')$
- (2) $f(a \cdot_A a') = f(a) \cdot_B f(a')$
- (3) $1_A \in A, 1_B \in B \Rightarrow f(1_A) = 1_B$

per ogni $a, a' \in A$. Notiamo che dalla (1) segue che

$$(1.1) \quad f(0_A) = 0_B$$

$$(1.2) \quad f(-a) = -f(a)$$

$$(1.3) \quad f(na) = nf(a)$$

per ogni $a \in A$ e $n \in \mathbb{Z}$. Infatti, $f(0_A) = f(0_A) +_B f(0_A)$ e basta usare la legge di cancellazione in $(B, +_B, 0_B)$ e inoltre $0_B = f(a +_A -a) = f(a) +_B f(-a)$ e si sfrutta l'unicità dell'inverso in $(B, +_B, 0_B)$.

Notiamo che se $A = \mathbb{Z}$ allora $f : \mathbb{Z} \rightarrow B$ che verifica (1) è completamente determinato da $f(1) \in B$ in quanto dalla (1.3) si ha $f(n) = nf(1)$ per ogni $n \in \mathbb{Z}$. Dunque se B è (commutativo) unitario allora esiste un unico omomorfismo $f : \mathbb{Z} \rightarrow B$ detto omomorfismo caratteristico in quanto $f(1) = 1_B$.

Un isomorfismo di anelli è un omomorfismo bigettivo. In generale, ad ogni $f : A \rightarrow B$ omomorfismo possiamo associare immagine $\text{Im } f \stackrel{\text{def}}{=} f(A)$ e nucleo $\text{Ker } f \stackrel{\text{def}}{=} \{a \in A \mid f(a) = 0\}$.

Lemma 2.7 $\text{Ker } f$ è ideale (bilatero) di A e $\text{Im } f$ è sottoanello di B .

Dimostrazione: Per vedere che $f(A) = \{f(a) \mid a \in A\}$ sia un sottoanello e che $\text{Ker } f$ sia un sottogruppo basta usare la definizione di omomorfismo. Inoltre, se $a \in A$ e $x \in \text{Ker } f$ ovvero $f(x) = 0$ allora $ax \in \text{Ker } f$ in quanto $f(ax) = f(a)f(x) = f(a)0 = 0$. ◊

Notare che se $f : A \rightarrow B$ è un omomorfismo di anelli unitari $\text{Ker } f$ è un sottoanello se e solo $1 \in \text{Ker } f$ e questo equivale a $B = 0$. D'altra parte $\text{Im } f$ non è un ideale, in generale. Osserviamo che la relazione di equivalenza \sim_f associata ad f è tale che $x \sim_f y \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x-y) = 0 \Leftrightarrow x-y \in \text{Ker } f$. In particolare, f iniettivo $\Leftrightarrow \text{Ker } f = 0$. Si ha dunque che:

Teorema 2.8 Dato $f : A \rightarrow B$ omomorfismo di anelli si ha che l'anello quoziente $A/\text{Ker } f$ è canonicamente isomorfo al sottoanello $\text{Im } f \subset B$ ovvero si ha la fattorizzazione canonica

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\text{Ker } f \\ & \searrow f & \downarrow \bar{f} \\ & & B \end{array}$$

con \bar{f} iniettiva e $A/\text{Ker } f \cong \text{Im } f = \text{Im } \bar{f}$.

Ad esempio, il sottoanello $B^\dagger = \{n1 \mid n \in \mathbb{Z}\} \subseteq B$ è l'immagine di $f : \mathbb{Z} \rightarrow B$ omomorfismo caratteristico: si ha che $B^\dagger \cong \mathbb{Z}$ oppure $B^\dagger \cong \mathbb{Z}_m$ visti come sottoanelli di B a seconda che B sia di caratteristica zero o positiva. Se B è un dominio allora m deve essere un primo.

3 Polinomi

Sia A anello commutativo unitario. Un polinomio in X a coefficienti in A è una espressione formale $p(X) \stackrel{\text{def}}{=} a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ con $a_i \in A$,

inteso che due tali espressioni $p(X) = a_0 + a_1X + \cdots + a_nX^n$ e $q(X) = b_0 + b_1X + \cdots + b_mX^m$ coincidano, ovvero $p(X) = q(X)$, se $a_i = b_i$ in A . Più precisamente, possiamo riscrivere $p(X)$ mediante una successione $(a_0, a_1, a_2, \dots, a_n, 0, \dots)$ tale che $a_i \neq 0$ per un numero finito di indici $i \in \mathbb{N}$. In questo modo $a \in A$ si riscrive come $(a, 0, \dots)$ e si ha che $X \stackrel{\text{def}}{=} (0, 1, 0, \dots)$, $X^2 \stackrel{\text{def}}{=} (0, 0, 1, 0, \dots)$, etc. Ad esempio, $1 + X + X^2 = (1, 1, 1, 0, \dots)$. Chiaramente $(a_0, a_1, a_2, \dots, a_n, 0, \dots) = (b_0, b_1, b_2, \dots, b_m, 0, \dots)$ se e solo se $a_i = b_i$ in A . Sia dunque

$$A[X] \stackrel{\text{def}}{=} \{p(X) \mid p(X) \text{ polinomio}\}$$

Definiamo la somma di due polinomi $p(X) = (a_0, a_1, a_2, \dots, a_n, 0, \dots)$ e $q(X) = (b_0, b_1, b_2, \dots, b_m, 0, \dots)$ mediante

$$p(X) + q(X) \stackrel{\text{def}}{=} (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, \dots)$$

e il prodotto $p(X) \cdot q(X)$ come segue

$$(a_0, a_1, a_2, \dots, a_n, 0, \dots) \cdot (b_0, b_1, b_2, \dots, b_m, 0, \dots) \stackrel{\text{def}}{=} (c_0, c_1, \dots, c_i, \dots, 0)$$

dove $c_0 \stackrel{\text{def}}{=} a_0b_0$, $c_1 = a_0b_1 + a_1b_0$ e

$$c_i = \sum_{j+k=i} a_j b_k$$

In particolare, per $a \in A$ si ha che $a \cdot q(X) = (ab_0, ab_1, ab_2, \dots, ab_m, 0, \dots)$. Dunque $1 \in A$ risulta unità anche di $A[X]$. Inoltre, $X \cdot X = X^2$, etc. Non è difficile verificare che $(A[X], +, \cdot)$ è un anello commutativo unitario detto *anello dei polinomi* a coefficienti in A . Infine, $A \rightarrow A[X] \ a \mapsto (a, 0, \dots)$ è un omomorfismo di anelli iniettivo che identifica A con un sottoanello di $A[X]$. Se $f : A \rightarrow B$ è un omomorfismo di anelli allora si ha un'unica estensione di f agli anelli di polinomi $f : A[X] \rightarrow B[X]$ tale che $X \mapsto X$, l'omomorfismo così definito

$$(a_0, a_1, a_2, \dots, a_n, 0, \dots) \mapsto (f(a_0), f(a_1), f(a_2), \dots, f(a_n), 0, \dots)$$

Infine si ha:

Lemma 3.1 (Principio di sostituzione) *Sia B un anello commutativo unitario e sia $A \subset B$ un sottoanello di B . Dato $b \in B$ esiste un unico omomorfismo $f_b : A[X] \rightarrow B \ X \mapsto b$ ovvero tale che $f_b(a) \stackrel{\text{def}}{=} a$ per ogni $a \in A$ e $f_b(X) \stackrel{\text{def}}{=} b$.*

Dimostrazione: Supponiamo che esista un omomorfismo $f : A[X] \rightarrow B$ tale che $f(a) = a$ per ogni $a \in A$ e $f(X) = b$. Dunque $f(X^2) = b^2$, etc. $f(X^k) = b^k$ per ogni $k \geq 0$. Inoltre, per $p(X) = a_0 + a_1X + \cdots + a_nX^n$ si ha

che $f(p(X)) = a_0 + a_1b + \cdots + a_nb^n$. Dunque f è unicamente determinato da $f(a) = a$ per ogni $a \in A$ e $f(X) = b$. Basta dunque verificare che

$$a_0 + a_1X + \cdots + a_nX^n \longmapsto a_0 + a_1b + \cdots + a_nb^n$$

sia un omomorfismo ma questo è evidente. Ad esempio si vede facilmente che

$$p(X)q(X) = \sum a_ib_jX^{i+j} \longmapsto \sum a_ib_jb^{i+j} = \left(\sum a_ib^i\right) \cdot \left(\sum b_jb^j\right)$$

dove $p(X) = a_0 + a_1X + \cdots + a_nX^n$ e $q(X) = b_0 + b_1X + \cdots + b_mX^m$. \odot

L'omomorfismo f_b del lemma precedente che associa ad un polinomio $p(X)$ il suo valore $p(b)$ in $b \in B$ ha come immagine $\text{Im } f_b$ l'anello $A[b]$ e nucleo $\text{Ker } f_b$ l'ideale dei polinomi $p(X)$ tali che $p(b) = 0$. Mediante il teorema di fattorizzazione si ha il seguente:

Corollario 3.2 *Sia $A \subseteq B$ un sottoanello di B commutativo unitario e $b \in B$. Il sottoanello $A[b] \subseteq B$ è canonicamente isomorfo all'anello quoziente di A modulo l'ideale dei polinomi che si annullano in b .*

In particolare, con $B = A[Y]$ e $b = Y$ si ha che f_Y è iniettivo; dunque, f_Y è l'unico isomorfismo $A[X] \cong A[Y]$ che è l'identità su A . D'altra parte, se $B = A$ e $b = 0$ si ha che $A[0] = A$ e dunque $A = A[X]/(X)$.

Divisione di polinomi

Dato un polinomio $p \in A[X]$ non nullo sia $p(X) = a_0 + a_1X + \cdots + a_nX^n$ diciamo che il grado di $p(X)$ è n se $a_n \neq 0$ e $a_i = 0$ per $i > n$. Denotiamo $\deg p$ il grado. Inoltre, a_n è detto coefficiente direttivo e il polinomio si dice monico se $a_n = 1$.

Proposizione 3.3 *Se A è un dominio allora $A[X]$ è un dominio.*

Dimostrazione: Se $p, q \in A[X]$ sono non nulli allora $\deg(p \cdot q) = \deg p + \deg q$. Infatti, sia $p(X) = a_nX^n + \cdots$ di grado n e sia $q(X) = b_mX^m + \cdots$ di grado m . Dunque $a_n \neq 0$ e $b_m \neq 0$ da cui $a_nb_m \neq 0$ in quanto A è un dominio. Dunque $p(X)q(X) = a_nb_mX^{n+m} + \cdots$ e $\deg(p \cdot q) = n + m$. \odot

In particolare, se $A = k$ è un campo allora $k[X]$ è un dominio. Analogamente $p(X) \in k[X]$ invertibile implica $p(X) \in k^{\neq 0}$ e quindi $k[X]$ non è un campo.

Teorema 3.4 Siano $f(X), g(X) \in A[X]$ e supponiamo che il coefficiente direttivo di $g(X)$ sia invertibile in A . Allora

$$f(X) = q(X)g(X) + r(X)$$

con $r(X) = 0$ oppure $\deg r < \deg g$.

Dimostrazione: Se $f = 0$ allora $q = r = 0$. Sia $f(X) = a_n X^n + \dots$ di grado n e sia $g(X) = b_m X^m + \dots$ di grado m . Se $n = \deg f < m = \deg g$ allora $f(X) = r(X)$ e $q(X) = 0$. Se $n = \deg f \geq m = \deg g$ procediamo per induzione su $n \geq 0$. Se $n = m = 0$ ovvero $f(X) = a_0, g(X) = b_0 \in A^*$ allora $a_0 = a_0 b_0^{-1} b_0, q(X) = a_0 b_0^{-1}, r(X) = 0$. Possiamo dunque applicare l'ipotesi induttiva a tutti i gradi k di polinomi f' tali che $k < n$. Sia

$$f'(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X)$$

da cui $f'(X) = a_n X^n - (a_n b_m^{-1} X^{n-m})(b_m X^m) + \dots$ ha grado $\leq n - 1$ quindi $f'(X) = q'(X)g(X) + r'(X)$ e sostituendo

$$f(X) = (q'(X) + a_n b_m^{-1} X^{n-m})g(X) + r'(X)$$

da cui $q(X) = q'(X) + a_n b_m^{-1} X^{n-m}$ e $r(X) = r'(X)$. \odot

In generale, si dice che $g(X)$ divide $f(X)$ se $r(X) = 0$. Se ad esempio, si considera $a \in A, f(X) \in A[X]$ è tale che $f(a) = 0$ se e solo se $X - a$ divide $f(X)$: basta scrivere $f(X) = q(X)(X - a) + r(X)$ da cui $r(X) = f(a) \in A$.

In particolare in $k[X]$ con k campo si ha che per ogni $f(X), g(X) \in k[X]$ con $g(X) \neq 0$ possiamo sempre scrivere $f(X) = q(X)g(X) + r(X)$ con $r(X) = 0$ oppure $\deg r < \deg g$.

4 Anelli euclidei

Sia A un anello commutativo unitario e siano $a \in A^{\neq 0}$ e $b \in A$. Diciamo che a divide b in A se $b = ac$ per qualche $c \in A$. Sinteticamente scriviamo $a|b$ in questo caso. Osserviamo subito che se $a|b, b|a$ e a oppure b non sono zero-divisori allora $b = ac$ e $a = bc^{-1}$ con $c \in A^*$ invertibile. Infatti, se $b = ac$ e $a = bd$ allora $a = acd$ e dunque $a(1 - cd) = 0$ oppure $b = bdc$ e dunque $b(1 - dc) = 0$. Viceversa, se $b = ac$ con $c \in A^*$ invertibile allora $a|b$ e $b|a$.

Sia A un dominio e $a, b, c \in A^{\neq 0}$:

- a e b si dicono associati se $a|b$ e $b|a$
- $a \notin A^*$ si dice irriducibile se $a = bc \Rightarrow b \in A^*$ oppure $c \in A^*$

- $a \notin A^*$ si dice *primo* se $a|bc \Rightarrow a|b$ oppure $a|c$

Denotiamo $a \sim b$ due elementi associati di A . La relazione \sim è una relazione di equivalenza e le classi di equivalenza sono $[a] = \{ac \mid c \in A^*\}$.

Lemma 4.1 *In un dominio ogni primo è irriducibile.*

Dimostrazione: Se $a = bc$ e $a|b$ allora $a = adc$ e quindi $dc = 1$. ⊙

Ad esempio, sia $A = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ sottoanello dunque dominio. Si vede facilmente che $A^* = \{\pm 1\}$ e dunque $\pm a$ sono i soli associati di a in A . Abbiamo che $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Si ha che 2 è irriducibile ma non è primo in A in quanto 2 non divide $1 \pm \sqrt{-5}$.

Dominio a fattorizzazione unica

Un dominio A si dice a *fattorizzazione unica* (U.F.D.) se tutti gli elementi non invertibili $a \notin A^*$ si possono scrivere come prodotto

$$a = a_1 \cdots a_n$$

con a_i irriducibile e in modo unico a meno di associati. L'unicità significa che

$$a = a_1 \cdots a_n = b_1 \cdots b_m$$

implica che $n = m$ e $a_i \sim b_j$ sono coppie di associati. Ad esempio, $A = \mathbb{Z}$ è un U.F.D. mentre $A = \mathbb{Z}[\sqrt{-5}]$ non lo è.

Lemma 4.2 *In un U.F.D. ogni irriducibile è primo.*

Dimostrazione: Supponiamo $p|ab$ con a, b non invertibili e p irriducibile. Dunque $p|a_1 \cdots a_n b_1 \cdots b_m$ ovvero $a_1 \cdots a_n b_1 \cdots b_m = pc$ e quindi $p \sim a_i$ oppure $p \sim b_j$ per qualche i o j per l'unicità della fattorizzazione in irriducibili. In conclusione, $p|a_i$ ma $a_i|a$ dunque $p|a$ oppure $p|b_j$ ma $b_j|b$ dunque $p|b$. ⊙

Lemma 4.3 *Se in un dominio A si ha che:*

- (a) *ogni irriducibile è primo e*
- (b) *ogni $a \notin A^*$ si scrive come $a = a_1 \cdots a_n$ con a_i irriducibili*

allora tale fattorizzazione è unica a meno di associati ovvero A è un U.F.D.

Dimostrazione: Sia $a = p_1 \cdots p_n = q_1 \cdots q_m$ e procediamo per induzione su $n \geq 1$. Se $a = p_1 = q_1 \cdots q_m$ allora a è irriducibile dunque $m = 1$ poichè q_j sono irriducibili $q_j \notin A^*$. Se $n > 1$ allora $p_1 | q_1 \cdots q_m$ dunque $p_1 | q_k$ per qualche $k \geq 1$ poichè p_1 è primo. Siccome q_k è irriducibile non ha divisori propri e quindi $p_1 \sim q_k$. Per ipotesi induttiva $p_2 \cdots p_n$ è unico a meno di associati e quindi $p_i \sim q_j$ per ogni $i, j \geq 1$. \odot

In conclusione, in A anello U.F.D. si ha che la nozione di irriducibile e primo coincidono. Inoltre, scegliendo una volta per tutte i rappresentanti p_i nelle classi di equivalenza degli associati si ha che ogni $a \notin A^*$ si scrive in modo unico

$$a = cp_1^{n_1} \cdots p_k^{n_k}$$

con p_i primi, $n_i \in \mathbb{N}$ e $c \in A^*$.

Massimo comun divisore

Sia A un dominio e $a, b, c \in A^{\neq 0}$: $d \in A^{\neq 0}$ è un massimo comun divisore (M.C.D.) di a e b se $d|a$, $d|b$ e se $c|a$ e $c|b$ allora $c|d$. Denotiamo $d \stackrel{\text{def}}{=} (a, b)$ un M.C.D. di a e b . Osserviamo subito che d è unico a meno di associati: se $d' = (a, b)$ è un altro M.C.D. allora $d|d'$ e $d'|d$ ovvero $d \sim d'$.

In un dominio A due elementi $a, b \in A^{\neq 0}$ si dicono coprimi se $1 = (a, b)$. Ad esempio, se $a \in A^*$ oppure $b \in A^*$ allora $(a, b) = 1$. Infatti, se $a \in A^*$ allora $a|1$ e $a|b$ in quanto $b = a(a^{-1}b)$.

Proposizione 4.4 *Se A è U.F.D. allora $d = (a, b)$ esiste per ogni $a, b \in A^{\neq 0}$.*

Dimostrazione: Siano $a, b \notin A^*$ e sia $a = cp_1^{n_1} \cdots p_r^{n_r}$ e $b = c'p_1^{m_1} \cdots p_s^{m_s}$. Poniamo $d = p_1^{l_1} \cdots p_t^{l_t}$ dove $l_i = \min(n_i, m_i)$. Non è difficile vedere che $d = (a, b)$. \odot

Proposizione 4.5 *Se A è P.I.D. allora $d = (a, b)$ esiste per ogni $a, b \in A^{\neq 0}$ e inoltre $d = ra + sb$ per qualche $r, s \in A^{\neq 0}$.*

Dimostrazione: Siano (a) e (b) gli ideali principali generati da $a, b \notin A^*$. Allora $(a) + (b) \stackrel{\text{def}}{=} \{ra + sb \mid r, s \in A\} = \mathcal{I}(S)$ con $S = \{a, b\}$ è un ideale. Siccome A è P.I.D. si ha che $(a) + (b) = (d)$ è principale, $(a) \subseteq (d)$ e $(b) \subseteq (d)$, dunque $a \in (d)$ e $b \in (d)$ ovvero $d|a$ e $d|b$. Inoltre $d = ra + sb \in (a) + (b)$. Infine, se $c|a$ e $c|b$ allora $c|d$. \odot

Traduzione in termini di ideali

In un dominio A qualunque:

- $a|b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$
- $a \sim b \Leftrightarrow (a) = (b)$
- $a \in A^* \Leftrightarrow (a) = (1) = A$
- a irriducibile $\Leftrightarrow (a) \neq (1)$ e se $(a) \subseteq (b)$ allora $(b) = (1)$ oppure $(a) = (b)$
- p primo $\Leftrightarrow (p) \neq (1)$ e se $ab \in (p)$ allora $a \in (p)$ oppure $b \in (p)$

Sempre in termini di ideali si ha che (d) l'ideale generato dal massimo comun divisore $d = (a, b)$ è il più piccolo ideale principale contenente a e b . Infatti, l'ideale somma $(a) + (b)$ è il più piccolo ideale contenente gli elementi a e b e quindi $(a) + (b) \subseteq (d)$ e inoltre se $(a) + (b) \subseteq (c)$ allora $(d) \subseteq (c)$ in quanto $c|d$ dalla definizione di massimo comun divisore.

Osserviamo che l'ideale somma esiste sempre, mentre, in generale, l'esistenza del più piccolo ideale principale contenente l'ideale somma dipende fortemente da proprietà specifiche dell'anello. In un anello qualunque, si denota spesso $(a, b) \stackrel{\text{def}}{=} (a) + (b)$ l'ideale somma.

P.I.D. \Rightarrow U.F.D.

Un ideale $I \subset A$ di un anello (commutativo unitario) qualunque A si dice

- ideale primo se $I \neq A$ e dati $a, b \in A$ tali che $ab \in I$ allora $a \in I$ oppure $b \in I$
- ideale massimale se $I \neq A$ e dato J ideale di A tale che $I \subseteq J$ allora $J = A$ oppure $J = I$.

Un anello con un unico ideale massimale si dice anello locale. Ad esempio, $I = (0)$ primo se e solo se A dominio e $I = (0)$ massimale se e solo se A campo; ogni campo è un anello locale e \mathbb{Z}_4 è un anello locale che non è un campo. Si ha sempre che:

Lemma 4.6 *In un anello commutativo unitario A ogni ideale I massimale è primo. Inoltre, il quoziente A/I è un campo se e solo se $I \subset A$ è massimale.*

Dimostrazione: Infatti, se $ab \in I$ e $a \notin I$ allora $I \subsetneq (a) + I = A$ se I massimale. Dunque, $1 = ra + x$ con $r \in A$ e $x \in I$ ma allora $b = rab + bx \in I$ in quanto $rab \in I$ e $bx \in I$. Inoltre $[r] = [a]^{-1}$ in A/I . Infine, sia ora J ideale

di A tale che $I \subsetneq J$. Esiste dunque $a \in J - I$ ma se A/I è un campo allora $1 = ra + x$ con $r \in A$ e $x \in I$ dunque $ra \in J$ e $x \in J$ da cui $1 \in J$. \odot

Sia ora $I = (p)$ un ideale principale di A dominio. Osserviamo che (p) è un ideale primo non nullo se e solo se p è un elemento primo in A . Inoltre, se (p) è un ideale massimale allora p è irriducibile ma non viceversa, in generale.

Proposizione 4.7 *Se A è P.I.D. allora $I = (p)$ ideale non nullo è primo se e solo se massimale ovvero un elemento $p \in A^{\neq 0}$ è irriducibile se e solo se è primo.*

Dimostrazione: Infatti, se ogni ideale è principale, si ha che p irriducibile $\Rightarrow (p)$ ideale massimale. Abbiamo dunque che (p) primo $\Rightarrow p$ primo $\Rightarrow p$ irriducibile $\Rightarrow (p)$ massimale $\Rightarrow (p)$ primo. \odot

Corollario 4.8 *Sia I ideale non nullo in A P.I.D. Se A/I è un dominio allora è un campo.*

Teorema 4.9 *Se A è P.I.D. allora A è U.F.D.*

Dimostrazione: Basta vedere che per ogni $a \notin A^*$ esiste una fattorizzazione $a = b_1 \cdots b_n$ con b_i irriducibili, in quanto ogni irriducibile è primo, questa fattorizzazione è unica. Supponiamo che a sia riducibile $a = a_1 b_1$ e sia anche $a_1 = a_2 b_2$ riducibile, dunque $a = b_1 b_2 a_2$, etc. ovvero $(a) \subset (a_1) \subset (a_2) \subseteq \cdots$. Continuando a decomporre a in fattori irriducibili per mostrare che il processo termina in numero finito di passi e dunque si ha $a = b_1 \cdots b_n$ con b_i irriducibili mostriamo che ogni catena di ideali $(a) \subset (a_1) \subset (a_2) \subseteq \cdots$ con $a_i \notin A^*$ è stazionaria ovvero che esiste k tale che $(a_k) = (a_{k+1}) = \cdots$. Sia $I = \cup (a_i)$ l'unione di tutti gli ideali (a_i) . Siccome $\{(a_i)\}$ è una catena di ideali si ha che I è un ideale. In quanto A è P.I.D. si ha che $I = (b)$. Dunque esiste k tale che $b \in (a_k)$ e $b \notin A^*$. In conclusione $I = (b) \subseteq (a_k)$ e quindi $I = (a_k) = (a_{k+1}) \cdots$. \odot

\odot **Attenzione!** Consideriamo $A[X]$ l'anello dei polinomi e sia $a \in A^{\neq 0}$. Sia $(a, X) \stackrel{\text{def}}{=} (a) + (X)$ l'ideale generato da a e X in $A[X]$. Se $(a, X) = (f(X))$ è principale allora $f(X) = b \in A$ in quanto $a \in (f(X))$ e inoltre $b \in A^*$ in quanto $X \in (b)$ e dunque $(a, X) = A$. In particolare, $1 \in (a, X)$ e quindi $a \in A^*$. Se A è un dominio che non è un campo allora $A[X]$ è un dominio che non è a ideali principali; inoltre, X è irriducibile ma (X) non è massimale.

Ad esempio, se $A = \mathbb{Z}$ allora $\mathbb{Z}[X]$ non è P.I.D. D'altra parte se $A = k$ campo in $k[X]$ ogni ideale non nullo I è principale: infatti, se $f(X) \in I$ è un polinomio di grado minimo in I allora la divisione di polinomi mostra che è un generatore $I = (f(X))$.

Divisione euclidea

Sia A un dominio. Un'applicazione $\delta : A^{\neq 0} \rightarrow \mathbb{N}$ tale che $\delta(ab) \geq \delta(a)$ si dice norma su A . Un anello euclideo è una coppia (A, δ) dove A è un dominio e δ è una norma su A tali che per ogni $a \in A$ e $b \in A^{\neq 0}$ si ha

$$a = qb + r$$

per qualche $q, r \in A$ con $r = 0$ oppure $\delta(r) < \delta(b)$. Ecco alcuni esempi di anelli euclidei:

- $A = \mathbb{Z}$ e $\delta(z) = |z|$ il valore assoluto dell'intero $z \in \mathbb{Z}^{\neq 0}$ per la ben nota divisione euclidea in \mathbb{Z}
- $A = k[X]$ con k campo e $\delta = \deg$ il grado per la divisione di polinomi in $k[X]$
- $A = K$ campo e δ costante in quanto $a|b$ e $b|a$ per ogni $a, b \in A^{\neq 0}$
- $A = \mathbb{Z}[i]$ gl'interi di Gauss e $\delta(z) = \|z\|^2 \stackrel{\text{def}}{=} a^2 + b^2$ per $z = a + ib \in \mathbb{Z}[i]$ si verifica che è un anello euclideo.

Osserviamo che in un dominio A con norma δ si ha che $\delta(a) \geq \delta(1)$ per ogni $a \in A^{\neq 0}$ e se $a \in A^*$ allora $\delta(a) = \delta(1)$; infatti, in questo caso anche $\delta(a) \leq \delta(aa^{-1}) = \delta(1)$. Se inoltre (A, δ) è euclideo allora vale anche il viceversa ovvero $\delta(a) > \delta(1)$ per ogni $a \notin A^*$. Basta osservare che se $b|a$ e $\delta(a) = \delta(b)$ allora $a|b$. Infatti, se $a = bc$, $b = aq + r$ e $r \neq 0$ si ha $r = b(1 - qc)$ e quindi $\delta(r) < \delta(a) = \delta(b)$ e $\delta(r) \geq \delta(b)$.

In particolare, (A, δ) euclideo con $\delta(a) = \delta(1)$ costante per ogni $a \in A$ è necessariamente un campo.

Teorema 4.10 *Se (A, δ) è euclideo allora A è P.I.D. Se A è un anello locale vale anche il viceversa.*

Dimostrazione: Sia (A, δ) euclideo. Sia $I \neq (0), (1)$ ideale proprio non nullo. Sia $a_0 \in I$ tale che $a_0 \neq 0$ e $\delta(a_0) > \delta(1)$ minimo di $\{\delta(a) \mid a \in I\} \subset \mathbb{N}$. Mostriamo che $I = (a_0)$. Sia $a \in I$ e scriviamo $a = a_0q + r$. Dunque $r = a - a_0q \in I$ da cui $r = 0$ altrimenti $\delta(r) < \delta(a_0)$ contraddice la minimalità di a_0 .

Supponiamo che A sia un anello locale che è anche P.I.D. Se A è un campo e dunque $A^* = A^{\neq 0}$ poniamo $\delta = 0$ costante. Altrimenti, sia dunque (p) l'unico primo non nullo di A . Siccome A è U.F.D. ogni elemento $a \in A^{\neq 0}$ si scrive $a = cp^n$ con $c \in A^*$. Definiamo $\delta : A^{\neq 0} \rightarrow \mathbb{N}$ $a = cp^n \mapsto n$ e dunque $\delta(a) = 0$ per ogni $a \in A^*$ e per $a \notin A^*$ il valore $\delta(a) = n > 0$ è unicamente determinato. Sia $b \in A^{\neq 0}$ e sia $b = c'p^m$ con $c' \in A^*$. Siccome $\delta(ab) = \delta(a) + \delta(b)$ si ha che δ è una norma su A . Infine, si ha che $a|b$ oppure $b|a$ in quanto $m \geq n$ oppure $n \geq m$. Se $n \geq m$ si ha $a = bq$ con $q = c''p^{n-m}$ ed $r = 0$ mentre se $m > n$ si ha $a = r$ e $q = 0$. \odot

Ecco un esempio di anello locale che è anche P.I.D.

- $A = \mathbb{Z}_{(p)} \stackrel{\text{def}}{=} \{a/b \in \mathbb{Q} \mid (b, p) = 1\}$ per un primo p fissato. Si ha che $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ è un sottoanello dunque un dominio. Se $a/b \in \mathbb{Z}_{(p)}$ è tale che $(a, p) = 1$ allora $b/a \in \mathbb{Z}_{(p)}$ e viceversa. Dunque $a/b \notin \mathbb{Z}_{(p)}^*$ implica che $p|a$. Denotiamo $(p/1) = \{a/b \in \mathbb{Q} \mid (b, p) = 1 \ p|a\}$ l'ideale principale generato da p in $\mathbb{Z}_{(p)}$. Sia $I \neq (1)$ ideale, per $a/b \in I$ dunque $p|a$ e $I \subseteq (p/1)$. Se $I \neq (0), (p/1)$ sia $k > 1$ minimo tale che $p^k|a$. Si ha dunque che $I = (p^k/1) = \{a/b \in \mathbb{Q} \mid (b, p) = 1 \ p^k|a\}$ è principale. Dunque $\mathbb{Z}_{(p)}$ è P.I.D. e $I = (p^k/1)$ è primo se e solo se p^k irriducibile in $\mathbb{Z}_{(p)}$ ovvero $k = 1$. In conclusione, $I = (p/1)$ è l'unico massimale di $\mathbb{Z}_{(p)}$.

\odot **Attenzione!** Sia $A = \mathbb{Z}[\alpha] \subset \mathbb{C}$. Se $\alpha = \sqrt{-n}$ con $n \geq 1$ allora $\mathbb{Z}[\alpha]$ è sempre un dominio con norma moltiplicativa indotta dalla norma usuale in \mathbb{C} ma, in generale, non U.F.D. e dunque non P.I.D. Se $\alpha = (1 + \sqrt{-19})/2$ si ha che $\mathbb{Z}[\alpha]$ è P.I.D. ma non euclideo (non è ovvio mostrarlo!). Quest'ultimo è l'anello degli "interi algebrici" nel campo di numeri $\mathbb{Q}(\sqrt{-19})$.

Appendici: Lemma di Gauss e Interi Algebrici

A Lemma di Gauss

Abbiamo visto che $\mathbb{Z}[X]$ non è P.I.D. dunque non è euclideo nonostante \mathbb{Z} sia euclideo; si vede però che $\mathbb{Z}[X]$ è U.F.D. In generale, si dimostra:

Teorema A.1 *Se A è U.F.D. allora $A[X]$ è U.F.D.*

Un altro esempio di U.F.D. non P.I.D. è dunque l'anello di polinomi in $n \geq 2$ variabili definito per induzione

$$k[X_1, X_2, \dots, X_n] \stackrel{\text{def}}{=} k[X_1, X_2, \dots, X_{n-1}][X_n]$$

a coefficienti in k campo.

Se A è U.F.D. diciamo che un polinomio $p(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$ è primitivo se i coefficienti $a_0, \dots, a_n \in A$ non hanno fattori comuni che non siano invertibili. In altre parole se $c(p) \stackrel{\text{def}}{=} (a_0, \dots, a_n)$ è un massimo comun divisore si ha $p(X)$ primitivo se e solo se $c(p) \sim 1$. Ad esempio, ogni polinomio monico è primitivo ma non viceversa. Se $A = k$ campo ogni polinomio $p(X) \in k[X]$ si scrive $p(X) = cp'(X)$ con $c \in k$ e $p'(X)$ monico: questo non è vero in generale. Se $A = \mathbb{Z}$ possiamo al più richiedere che il coefficiente direttivo di un polinomio primitivo sia positivo.

Dimostriamo il Teorema precedente nel caso di $A = \mathbb{Z}$

Lemma A.2 *Ogni polinomio non nullo $p(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$ si scrive in modo unico $p(X) = cp'(X)$ dove $c \in \mathbb{Q}$ e $p'(X) \in \mathbb{Z}[X]$ è primitivo. Inoltre, $p(X) \in \mathbb{Z}[X]$ se e solo se $c \in \mathbb{Z}$ e $p(X)$ è primitivo se e solo se $c = 1$.*

Dimostrazione: Si ha $ap(X) \in \mathbb{Z}[X]$ dove a è il minimo comune multiplo dei denominatori di $a_i \in \mathbb{Q}$. Si ha $bp'(X) = ap(X)$ dove b è il massimo comun divisore dei coefficienti di $ap(X)$ preso con segno concorde con quello del coefficiente direttivo di $p(X)$. Quindi $c \stackrel{\text{def}}{=} b/a$. \odot

Lemma A.3 (Lemma di Gauss) *Un prodotto di polinomi primitivi in $\mathbb{Z}[X]$ è primitivo.*

Dimostrazione: Sia $h = fg$ con f, g primitivi. Sia $p \in \mathbb{Z}$ un primo e sia

$$\rho_p : \mathbb{Z}[X] \rightarrow \mathbb{Z}_p[X] \quad a_mX^m + \dots + a_0 \mapsto \bar{a}_mX^m + \dots + \bar{a}_0$$

l'omomorfismo surgettivo di anelli di polinomi indotto da $\rho_p : \mathbb{Z} \rightarrow \mathbb{Z}_p$ ovvero dalla riduzione modulo p dei coefficienti. Siccome $\mathbb{Z}_p[X]$ è un dominio il nucleo di $\rho_p : \mathbb{Z}[X] \rightarrow \mathbb{Z}_p[X]$ è un ideale primo e si tratta dell'ideale dei polinomi per cui p divide i coefficienti

$$\text{Ker } \rho_p = (p)[X] \stackrel{\text{def}}{=} \{a_m X^m + \cdots + a_0 \in \mathbb{Z}[X] \mid a_i \in (p)\}$$

Siccome f e g sono primitivi $f, g \notin (p)[X]$ ma $(p)[X]$ è primo e dunque $h = fg \notin (p)[X]$. In conclusione, $h \notin (p)[X]$ per ogni primo $p \in \mathbb{Z}$ e dunque h è primitivo. \odot

Lemma A.4 *Ogni irriducibile in $\mathbb{Z}[X]$ è primo.*

Dimostrazione: Sia $f \in \mathbb{Z}[X]$ irriducibile. Mostriamo che (f) è un ideale primo. Sia $gh \in (f)$ e scriviamo $g = cg' \in \mathbb{Z}[X]$ e $h = dh' \in \mathbb{Z}[X]$ con g', h' primitivi dunque $g'h'$ primitivo. Osserviamo che: se $f = p \in \mathbb{Z}$ è un primo allora qualche coefficiente di $g'h'$ sia $a \in \mathbb{Z}$ non è divisibile per p ma $p|gh$ implica $p|cda$ e dunque $p|c$ oppure $p|d$ ovvero $g \in (f)$ oppure $h \in (f)$; se f è un polinomio primitivo che è irriducibile in $\mathbb{Q}[X]$ allora (f) è primo in $\mathbb{Q}[X]$ e dunque $f|g$ oppure $f|h$ in $\mathbb{Q}[X]$. Basta dunque mostrare che:

- (i) se $f \in \mathbb{Z}[X]$ è irriducibile allora f è un primo in \mathbb{Z} oppure è un polinomio primitivo che è irriducibile in $\mathbb{Q}[X]$
- (ii) se $f, g \in \mathbb{Z}[X]$ con f primitivo e $f|g$ in $\mathbb{Q}[X]$ allora $f|g$ in $\mathbb{Z}[X]$.

Per vedere (ii) sia $g = fq$, $q \in \mathbb{Q}[X]$ scriviamo $q = tq'$ con q' primitivo e dunque fq' primitivo, $g = tfq' \in \mathbb{Z}[X]$ da cui $t \in \mathbb{Z}$ e quindi $q \in \mathbb{Z}[X]$.

Per vedere (i) sia $f = zf' \in \mathbb{Z}[X]$ irriducibile dunque $f' = 1$ oppure $z = \pm 1$. Se $f' = 1$ allora $f = p$ è un primo in \mathbb{Z} . Se $z = \pm 1$ allora $\pm f$ è primitivo irriducibile in $\mathbb{Z}[X]$ e dunque in $\mathbb{Q}[X]$. \odot

Lemma A.5 *Ogni polinomio non nullo $p(X) \in \mathbb{Z}[X]$ si scrive*

$$p(X) = \pm p_1 \cdots p_m q_1(X) \cdots q_n(X)$$

dove p_i sono primi in \mathbb{Z} e $q_j \in \mathbb{Z}[X]$ sono polinomi primitivi irriducibili in $\mathbb{Z}[X]$.

Dimostrazione: Sia $p = cp'$ con p' primitivo. Se p' è irriducibile basta fattorizzare c e si ha la tesi. Altrimenti fattorizziamo anche $p' = q_1 q_2$ dove $q_1, q_2 \in \mathbb{Z}[X]$ sono ancora primitivi (in quanto p' è primitivo). Si ha che $\deg(p) = \deg(p')$ ma $\deg(q_i) < \deg(p')$ e continuando a fattorizzare il grado

dei polinomi q_i decresce e quindi ha un minimo > 0 e si ottiene la fattorizzazione. \odot

Da questi ultimi due lemmi segue che $\mathbb{Z}[X]$ è U.F.D.

B Interi algebrici

Un numero complesso $\alpha \in \mathbb{C}$ è detto algebrico se è radice di un polinomio non nullo a coefficienti razionali ovvero se esiste $p(X) \in \mathbb{Q}[X]$ tale che $p(\alpha) = 0$. Chiaramente, se α è algebrico possiamo sempre trovare anche $p'(X) \in \mathbb{Z}[X]$ primitivo tale che $p'(\alpha) = 0$ (basta considerare $p = cp'$ con $c \in \mathbb{Q}$). Altrimenti, se α non è algebrico, si dice trascendente ovvero nel caso in cui tale polinomio non esista. Ad esempio, ogni numero razionale $b/a \in \mathbb{Q}$ con $(a, b) = 1$ è radice del polinomio primitivo $p'(X) = aX - b \in \mathbb{Z}[X]$ mentre $\pi \in \mathbb{C}$ è trascendente. Diciamo infine che α è un intero algebrico se esiste un polinomio $p(X) \in \mathbb{Z}[X]$ monico tale che $p(\alpha) = 0$. In generale, se $A \subset B$ è un sottoanello di B si dice che $\alpha \in B$ è intero su A se soddisfa una equazione in B

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \quad a_i \in A$$

a coefficienti in A . Se $A = \mathbb{Z}$ e $B = \mathbb{C}$ si ha la definizione d'intero algebrico. Ad esempio, le radici n -esime dell'unità sono interi algebrici in quanto sono radici del polinomio monico $p(X) = X^n - 1$.

In altre parole sia $\alpha \in \mathbb{C}$ e sia $f_\alpha : \mathbb{Q}[X] \rightarrow \mathbb{C}$ l'omorfismo che associa ad un polinomio $p(X) \in \mathbb{Q}[X]$ il suo valore $p(\alpha)$ ovvero

$$p(X) = a_n X^n + \cdots + a_1 X + a_0 \mapsto p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

Si ha che $\text{Im } f_\alpha = \mathbb{Q}[\alpha] \subset \mathbb{C}$ è un dominio e dunque $\text{Ker } f_\alpha$ è un ideale primo. Se $\text{Ker } f_\alpha \neq 0$ allora α è algebrico e viceversa. In effetti, siccome $\mathbb{Q}[X]$ è P.I.D. si ha inoltre che $\text{Ker } f_\alpha = (p(X))$. Se $p(X) \neq 0$ allora $p(X)$ è irriducibile e $\mathbb{Q}[\alpha]$ è un campo che coincide con $\mathbb{Q}(\alpha)$ il più piccolo campo contenente \mathbb{Q} ed α . Inoltre se $p(X)$ ha grado n allora $1, \alpha, \dots, \alpha^{n-1}$ sono una base di $\mathbb{Q}[\alpha]$ come \mathbb{Q} -spazio vettoriale. Se $p(X) = 0$ ovvero α trascendente si ha $\mathbb{Q}[X] \cong \mathbb{Q}[\alpha]$. In generale, un sottocampo K di \mathbb{C} si dice campo di numeri algebrici se tutti i suoi elementi sono algebrici. Ad esempio, se α è algebrico, non è difficile vedere che $K = \mathbb{Q}(\alpha)$ è un campo di numeri algebrici.

Il generatore non nullo $p(X)$ di $\text{Ker } f_\alpha$ è un polinomio di grado minimo che ha α come radice ed è unico a meno di associati: possiamo scegliere $p'(X) \sim p(X)$ primitivo e irriducibile in $\mathbb{Z}[X]$. Si ha:

Lemma B.1 $\mathbb{Z}[X]/(p'(X)) \cong \mathbb{Z}[\alpha]$.

Dimostrazione: Se consideriamo l'analogo omomorfismo $f_\alpha : \mathbb{Z}[X] \rightarrow \mathbb{C}$ che associa ad un polinomio il suo valore in α si ha $\text{Im } f_\alpha = \mathbb{Z}[\alpha]$ e dunque basta mostrare che $\text{Ker } f_\alpha = (p'(X))$. Infatti, se $g \in \mathbb{Z}[X]$ con $g(\alpha) = 0$ allora $p' \mid g$ in $\mathbb{Q}[X]$ ma allora $p' \mid g$ in $\mathbb{Z}[X]$, come abbiamo visto, in quanto p' è primitivo. \odot

Come conseguenza si ha:

Teorema B.2 *Un numero algebrico $\alpha \in \mathbb{C}$ è un intero algebrico se e solo se il suo polinomio $p'(X) \in \mathbb{Z}[X]$ primitivo irriducibile è monico.*

Dimostrazione: Infatti, se $p'(X)$ non è monico nessun suo multiplo in $\mathbb{Z}[X]$ può essere monico. \odot

Sia K un campo di numeri algebrici. Si mostra che

$$\mathcal{O}_K \stackrel{\text{def}}{=} \{z \in K \mid z \text{ intero su } \mathbb{Z}\}$$

è un anello e si dice anello degli interi del campo K . Ecco i due esempi paradigmatici:

- Se $K = \mathbb{Q}$ allora $\mathcal{O}_K = \mathbb{Z}$ sono gli interi. Per $z = b/a \in \mathbb{Q}$ con $(a, b) = 1$ ha polinomio primitivo irriducibile $p'(X) = aX - b \in \mathbb{Z}[X]$ che è monico se e solo se $z \in \mathbb{Z}$.
- Se $K = \mathbb{Q}(i)$ allora $\mathcal{O}_K = \mathbb{Z}[i]$ sono gli interi di Gauss. Per $\alpha \in \mathbb{Q}(i)$ ha polinomio $p(X) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha}$ e gli interi sono tutti e soli $\alpha \in \mathbb{Z}[i]$. Infatti se $\alpha = s + it$ con $s, t \in \mathbb{Q}$ allora $\alpha^2 - 2s\alpha + s^2 + t^2 = 0$. Se $t, s \in \mathbb{Z}$ allora $-2s, s^2 + t^2 \in \mathbb{Z}$; inoltre, $\alpha \in \mathbb{Q}(i)$ è intero su \mathbb{Z} solo se $p(X)$ ha coefficienti interi e quindi $s, t \in \mathbb{Z}$ (perchè!).

\odot **Attenzione!** Non farsi ingannare da ingenue analogie nel dire che un numero algebrico sia un intero o meno! Ad esempio, $\alpha = (-1 + \sqrt{-3})/2$ è un intero algebrico. Infatti, $\alpha^2 + \alpha + 1 = 0$ e inoltre $\mathbb{Z}[\alpha]$ sono tutti interi (detti di Eisenstein). Infatti, $\zeta \in \mathbb{Q}(\alpha)$ ha sempre polinomio $p(X) = X^2 - (\zeta + \bar{\zeta})X + \zeta\bar{\zeta}$. Sia $\zeta = s + at$ allora $\zeta^2 - (2s - t)\zeta + s^2 - st + t^2 = 0$. Se $\zeta \in \mathbb{Z}[\alpha]$ allora $-2s + t, s^2 - st + t^2 \in \mathbb{Z}$. Un altro esempio è anche $\zeta = 1 + \alpha = (1 + \sqrt{-3})/2$ che è dunque un intero algebrico. Se però $\alpha = (1 + \sqrt{2})/2$ allora $4\alpha^2 - 4\alpha - 1 = 0$ ma questo non è un intero algebrico.