# Sugli anelli

Francesco Parisio

*Cara Ekaterina,*

In questa lettera vorrò darti una panoramica dell'algebra astratta che ho avuto modo di studiare nei miei tre anni di università: la materia, forse, che mi ha dato più soddisfazione e che più mi ha appassionato. Questo bisogno nasce dalla mia volontà di studiare geometria algebrica, alla cui base vi è una solida e corpulenta dose di algebra commutativa che ho in mente di studiare questo agosto. La mia esperienza dimostra che non v'è modo migliore di capire che spiegare a un altro ciò che hai imparato.

Nelle prossime pagine assumerò qualche rudimento di teoria dei gruppi e una conoscenza basilare delle principali strutture algebriche. Questa lettera è volutamente rivolta a chi ha già studiato l'argomento, e a chi come me l'ha studiato male: non fornirò molti esempi e assumerò che tu sia familiare con l'idea di quozienti, di gruppi, dei teoremi di omomorfismo e del teorema di corrispondenza. Sarò sbrigativo sulle costruzioni formali di alcuni oggetti: vorrò concentrarmi sui risultati algebrici più importanti. Perdona gli errori che potranno nascondersi nelle prossime pagine: ti prego di notificarmeli il prima possibile. Ti auguro, allora, una buona lettura.

## Introduzione

Per iniziare, ti ricordo che un anello è un insieme $R$ non vuoto dotato di due operazioni $+$ e $\cdot$, che contiene almeno due elementi (li denoterò, per comodità, così: 0 e 1) per i quali vale che $(R, +, 0)$ è un *gruppo abeliano* e che $(R, \cdot, 1)$ è un monoide. Come sai, gli insiemi degli elementi invertibili secondo l'operazione di prodotto forma (per definizione!) un gruppo, che indicherò così: $R^\times$. Un sottoanello $S$ di $R$ è un sottoinsieme $S \subset R$ che risulta un sottogruppo additivo con l'operazione $+$ e l'elemento neutro 0 e un sottomonoide moltiplicativo secondo $\cdot$ e 1.

Gli anelli commutativi per cui non esistono divisori dello zero si dicono *domini d'integrità* e ivi vale la legge di cancellazione. Un anello commutativo che ha ogni elemento non nullo invertibile è un *campo*, e chiaramente ogni campo è un dominio: se $F$ è il campo in questione e $a$ è un suo elemento non nullo,

$$\forall b \in F : b \neq 0,\ ab = 0 \quad \text{allora} \quad b = a^{-1}(ab) = 0.$$

Se vale la legge di cancellazione, vuol dire che la funzione $f_\alpha : R \to R$ tale che $f_\alpha : x \mapsto \alpha x$ è sempre iniettiva, per ogni $\alpha \in R - \{0\}$. Anzi, in verità le due proprietà sono equivalenti. Se $R$ è finito, $f_\alpha$ è una bigezione per ogni $\alpha$, quindi $R$ risulta un campo. Infatti,

$$\forall \alpha \in R - \{0\} \quad \exists! y \in R : f_\alpha(y) = \alpha y = 1 = y\alpha \text{ cioè } \alpha \in R^\times.$$

Un ideale di un anello $R$ è un sottoinsieme $\emptyset \neq \mathfrak{m} \subseteq R$ tale che

$$\forall i, j \in \mathfrak{m},\ \forall \alpha, \beta \in R, \quad \alpha i + \beta j \in \mathfrak{m}.$$

Nota che un ideale è, in particolare, un sottogruppo additivo di $R$; e che ogni anello $R$ ha sempre gli ideali $\{0\}$ e $R$. Ad esempio: gli ideali di $\mathbb{Z}$ sono i sottogruppi additivi di $\mathbb{Z}$ con l'operazione di somma. L'argomento che si usa per dimostrarlo è, come al solito, basato sulla divisione euclidea.

Un ideale si dice *principale* se è della forma $\mathfrak{m} = (a) = \{ax : x \in R\}$, per un qualche $a \in R$. Se ci pensi, gli ideali di $\mathbb{Z}$ sono tutti principali. Se gli ideali di un dominio d'integrità sono tutti principali, siamo in presenza di un dominio *a ideali principali* (o un PID – dall'inglese *Principal Ideal Domain*). Nel contesto di anelli commutativi, si può estendere il concetto di

ideale principale a ideale generato da un sottoinsieme $S \subset R$. In tal caso, se ne conosce la struttura: $(S)$ è l'ideale delle *combinazioni lineari* di elementi di $S$ a coefficienti nell'anello $R$. Viene da sé che in assenza di commutatività la struttura $S$ risulta particolarmente complessa.

Se $\mathfrak{m}$ e $\mathfrak{n}$ sono due ideali di $R$, la loro intersezione insiemistica e la loro somma

$$\mathfrak{m} + \mathfrak{n} = \{m + n : m \in \mathfrak{m}, n \in \mathfrak{n}\}$$

sono ancora ideali di $R$; dovrebbe, a questo punto, intravedersi una certa analogia tra i sottogruppi di un gruppo e gli ideali di un anello.

Per quanto riguarda gli anelli commutativi, vale un risultato tanto semplice quanto importante: per ogni *anello commutativo* $R$,

$$R \text{ è un campo} \iff R \text{ ha solo due ideali.}$$

Ricorda che se un ideale contiene un elemento invertibile, allora è l'ideale banale $R$, quindi un verso è già dimostrato. Se invece $R$ ha solo due ideali (cioè 0 e $R$), allora ogni elemento non nullo $a$ genera un ideale $(a) = R$. In particolare, esiste $x \in R$ per cui $xa = 1 \in R$, da cui segue $a \in R^\times$. Nota bene che abbiamo usato la commutatività di $R$ proprio nell'ultimo passaggio. Se $R$ non fosse stato abeliano, $xa \neq ax$ in generale, e quindi non si sarebbe potuto concludere allo stesso modo. Per di più, esistono anelli che hanno solo due ideali che non sono campi: l'anello delle matrici $\mathrm{Mat}(2, \mathbb{R})$ ne è un esempio e, come ben sai, non è commutativo. Insomma, l'ipotesi di commutatività è fondamentale in questo risultato.

Dati un anello $R$ e un suo ideale $\mathfrak{m}$, è sempre possibile costruire un anello quoziente $\frac{R}{\mathfrak{m}}$, i cui elementi sono le classi laterali $x + \mathfrak{m}$. Si potrebbe parlare di ideali destri e sinistri, ma divagherei. Il contesto in cui lavoreremo sarà per lo più costituito da anelli commutativi, dove i due concetti sono uguali.

Adesso, ti ricordo brevemente delle proprietà dei morfismi tra anelli. Ti basta sapere che un morfismo da $R$ a $S$ è una funzione $f : R \to S$ che è un morfismo dei gruppi additivi $(R, +)$ in $(S, +)$ e un morfismo dei monoidi moltiplicativi $(R, \cdot)$ in $(S, \cdot)$, dove naturalmente $f(1) = 1$. L'immagine $f[R]$ è un sottoanello di $S$.

Il nucleo di un morfismo si indica con $\ker f = \{x \in R : f(x) = 0\}$ ed è un ideale. In verità, ogni ideale si realizza come nucleo di un qualche morfismo. Se $\mathfrak{m}$ è un ideale di $R$, la mappa di proiezione $p : R \to \frac{R}{\mathfrak{m}}$ definisce un morfismo di anelli di nucleo $\ker p = \mathfrak{m}$! Come avrai già avuto modo di vedere, $\ker f = 0$ se e solo se $f$ è iniettivo. Dovrebbe essere evidente una chiara analogia tra anelli e ideali e gruppi e sottogruppi normali.

**Un esercizio**. Si è visto che l'immagine di sottoanelli per morfismi è ancora un sottoanello. Questa proprietà è vera anche per gli ideali? Sia $f : R \to S$ un morfismo di anelli e siano $\mathfrak{m}$ e $\mathfrak{n}$ due ideali di, rispettivamente, $R$ e $S$. Sebbene $f^{-1}[\mathfrak{n}]$ sia sempre un ideale di $R$, di $f[\mathfrak{m}]$ si può dire lo stesso quando $f$ è suriettivo. Siano $a, b \in \mathfrak{m}$, quindi $f(a), f(b)$ in $f[\mathfrak{m}]$. È chiaro che $f(a - b) = f(a) - f(b) \in f[\mathfrak{m}]$. Se $f$ è suriettivo,

$$yf(a) \overset{\exists x}{=} f(x)f(a) = f(xa) \in f[\mathfrak{m}]$$

per ogni $y \in S$, quindi $f[\mathfrak{m}]$ è ancora un ideale di $S$. Spero di averti potuto introdurre in modo chiaro e sintetico i principali rudimenti con cui lavoreremo in seguito. Nella prossima sezione ti parlerò delle fattorizzazioni, un tema centrale nella teoria degli anelli.

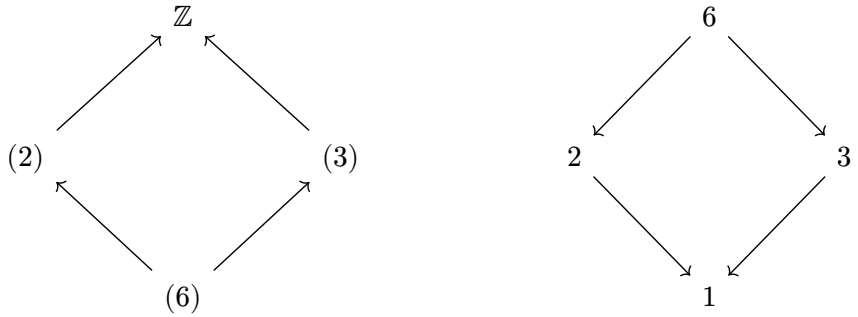
## Fattorizzazioni

Data l'importanza di questo argomento, sarò meno sbrigativo. *Sia $R$ un dominio di integrità*: è il minimo che richiedo per costruire un po' di teoria. Adotterò la seguente notazione: per ogni elemento $a$, indicherò con $\mathfrak{a}$ l'ideale $(a)$.

- Un elemento $a$ divide $b$ se $\exists x \in R : b = ax$ o, equivalentemente, se $\mathfrak{b} \subset \mathfrak{a}$.
- Due elementi $a$ e $b$ si dicono associati se si dividono a vicenda, dunque se e solo se $\mathfrak{a} = \mathfrak{b}$.

La relazione di divisione e quella di inclusione tra gli ideali principali è, se vuoi, *contravariante*: $a \mid b$ vuol dire che $\mathfrak{b} \subset \mathfrak{a}$. Nella pratica, se consideriamo un insieme di ideali principali di $R$, i reticoli di inclusione tra gli ideali e quelli di divisione in un insieme di loro rappresentanti sono uno il duale dell'altro.

Questo schema può aiutarti a visualizzare meglio questo concetto.




Vediamo allora cosa vuol dire per un elemento essere irriducibile oppure primo.

### Elementi irriducibili e ideali massimali

Un elemento $a$ si dice *irriducibile* se non è nullo e se *non ha divisori propri*. Un ideale $K$ è *massimale* se non esistono ideali propri $J$ per cui

$$K \subset J \subset R.$$

Le condizioni che $a$ sia irriducibile e che $\mathfrak{a}$ sia massimale sono simili, e *sono equivalenti nel caso di un PID*. In generale, ogni ideale principale massimale induce un elemento irriducibile. Sia $\mathfrak{a}$ massimale. Se $b$ è un divisore di $a$, $\mathfrak{a} \subset \mathfrak{b} \subset R$, e per massimalità $b$ è associato a $a$ oppure è invertibile, quindi $a$ non ha divisori propri. Viceversa, sia $R$ un PID e sia $a$ un elemento irriducibile di $R$. Allora, per ogni ideale $J$ esiste un generatore $b$ per cui $J = \mathfrak{b}$. Se $\mathfrak{b}$ contiene $\mathfrak{a}$, allora $b \mid a$, cioè esiste $x \in R$ per cui $a = bx$. Poiché $a$ è irriducibile, $b$ è invertibile e $x$ è associato a $a$ o viceversa. In entrambi i casi, $\mathfrak{b} = R$ oppure $\mathfrak{b} = \mathfrak{a}$, quindi $\mathfrak{a}$ è massimale.

Nella dimostrazione precedente, l'ipotesi che $R$ sia un PID è essenziale, perché in questo contesto gli ideali principali esauriscono tutti gli ideali dell'anello. Se non si suppone che $R$ sia un PID, vale solo che è "massimale per ideali principali", nel senso che non esistono ideali principali $\mathfrak{p}$ di modo che l'inclusione $K \subset \mathfrak{p} \subset R$ sia propria. In nessun modo, però, questa condizione implica l'essere massimale! Ti proporrei un controesempio, ma mi serve qualche strumento in più: lo troverai alla fine di questo capitolo, contrassegnato con un carino (♡).

### Primalità

Un elemento $a$ non nullo e non invertibile si dice *primo* se, ogni volta che divide un prodotto, divide uno dei due fattori. Un ideale $\mathfrak{m}$ è primo se

$$(ab) \subset \mathfrak{m} \implies \mathfrak{a} \subset \mathfrak{m} \text{ oppure } \mathfrak{b} \subset \mathfrak{m}.$$

L'insieme degli ideali primi di $R$ è detto "spettro" di $R$ e si denota con $\mathrm{Spec}(R)$. In questo caso, $a$ primo e $\mathfrak{a}$ primo sono equivalenti su domini di integrità.

**Domini a fattorizzazione unica**

Ti ricordo una definizione: un dominio di integrità $R$ è un *dominio a fattorizzazione unica* (UFD – dall'inglese *Unique Factorisation Domain*) se ogni elemento non nullo di $R$ ammette una scomposizione *essenzialmente unica* in fattori irriducibili. Per il teorema fondamentale dell'aritmetica, $\mathbb{Z}$ è un UFD.

Ti introduco all'argomento con la seguente osservazione: *in ogni dominio di integrità, ogni elemento primo è pure irriducibile.* Infatti, se $a \in R$ e $m$ è un suo divisore, si ha $m \mid a$, cioè esiste $n$ per cui $a = mn$. Per primalità, si realizza solo una tra le seguenti possibilità. Se $a \mid m$, allora $a$ e $m$ sono associati, quindi $m$ non è un divisore proprio. Se $a \mid n$, $m$ è invertibile (basta osservare che in tal caso esiste un $t \in R$ per cui $a = mta$, quindi $1 = mt$, e siccome siamo in un dominio di integrità…), quindi $m$ è una unità. Di conseguenza, $a$ è irriducibile. Si può mostrare qualcosa di simile passando agli ideali principali. In tal caso, è facile vedere – ragionando sull'inclusione degli ideali principali, anziché sulla divisione dei loro rappresentanti – che non esistono ideali *principali* $\mathfrak{e}$ per cui le inclusioni $\mathfrak{a} \subset \mathfrak{e} \subset R$ siano proprie. Questo, tuttavia, *non* implica che $\mathfrak{a}$ sia massimale. Se però ogni ideale è principale, questo è ciò che abbiamo appena asserito: l'ipotesi chiave è che $R$ sia un PID. L'argomento, se vuoi, è identico a quello esibito poco fa, nella sezione sugli elementi irriducibili – non trovi? Come conseguenza, in un PID ogni ideale primo è pure massimale. Come vedremo, tuttavia, i due concetti sono ben diversi in domini UFD.

È di grande importanza il seguente teorema, che dimostreremo nel dettaglio.

**Teorema di caratterizzazione degli UFD** Un dominio d'integrità $R$ è un dominio a fattorizzazione unica se e solo se ogni elemento irriducibile è primo e se ogni catena ascendente di ideali *principali* è stazionaria.

Ti ricordo che una catena di ideali $I_1 \subset I_2 \subset ...$ è stazionaria se esiste un indice $k$ per cui, per ogni $\ell > k$, $I_\ell = I_k$. Questo ha, come conseguenza, il fatto che ogni catena $... \mid a_2 \mid a_1$ si stabilizza. In altre parole, non si può dividere all'infinito: a un certo punto, trovo un elemento finale nel processo di divisione. Non deve essere intuitivo il perché le due condizioni siano equivalenti, ma dovrebbe essere immediato (e affascinante!) la somiglianza tra ACC (*Ascending Chain Condition*) e la possibilità di fattorizzare in un dominio.

**Dimostrazione** *Ti spiego, anzitutto, come mai in un UFD ogni elemento irriducibile è primo.* Sia $a \in R$ tale che $a \mid hk$. Se uno tra $h$ o $k$ è invertibile, allora $a$ divide l'altro fattore, quindi è fatta. Qualora $h$ e $k$ non siano invertibili, siamo certi che non siano nulli perché $a$ non lo è (ti ricordo, a proposito, che $R$ è un dominio). Allora, $h$ e $k$ si fattorizzano come, rispettivamente, $h_1...h_n$ e $k_1...k_m$. Esiste un certo $b$ per cui

$$ab = h_1...h_nk_1...k_m \text{ e quindi } ab_1...b_\ell = h_1...h_nk_1...k_m$$

per una fattorizzazione $b_1...b_\ell$ di $b$. Ma ora, abbiamo uguagliati due prodotti di irriducibili: $a$ deve necessariamente dividere uno tra gli $h_1, ...h_n$ o tra i $k_1, ...k_m$. In entrambi i casi, $a$ divide $h$ o $k$, quindi $a$ è primo.

*Vediamo allora, per quale motivo ogni UFD soddisfa l'ACCP, ovverosia, ogni catena ascendente di ideali principali è stazionaria.* Sia $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ una catena ascendente di ideali e siano $a_1, a_2, ...$ i loro generatori. Sia ora $\prod_i f_i^{s_i}$ una fattorizzazione di $a_1$, dove $s_i$ sono esponenti

naturali. Siccome $a_2 \mid a_1$, la fattorizzazione di $a_2$ è della forma $\prod_i f_i^{\sigma_i}$ dove $\sigma_i \leq s_i$. Essendo i fattori $f_i$ finiti, le inclusioni proprie della catena $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ possono essere al più $\sum_i s_i$. L'unica possibilità è che la catena sia stazionaria.

*Viceversa, ti faccio vedere che un dominio che soddisfa ACCP è un dominio a fattorizzazione, non necessariamente unica.* Intanto, preso un qualsiasi $a$ non nullo e non invertibile, esiste un irriducibile $\beta_1$ che divide $a$. Puoi costruire una catena ascendente nel seguente modo: se $a$ è irriducibile, hai finito; ma se $a = a_1$ non lo è, esiste un fattore $a_2$ che divide $a_1$, cioè $\mathfrak{a}_1 \subset \mathfrak{a}_2$. Se tu non potessi trovare un elemento irriducibile, la catena non si arresterebbe: assurdo!

Nello stesso spirito, cerchiamo una fattorizzazione di $a$. Sappiamo che esiste un irriducibile $\beta_1$ che lo divide: allora $a = \beta_1 a_1$. Si applica l'argomento a $a_1$ e si trova $\beta_2$ tale che $a = \beta_1\beta_2 a_2$. L'idea è chiara: ancora una volta, questo procedimento deve arrestarsi, pena la costruzione di una catena ascendente di ideali principali $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ che non si arresta.

*Supponi, finalmente, che un dominio a fattorizzazione abbia ogni irriducibile primo.* Siamo riusciti a costruire due fattorizzazioni $\beta_1...\beta_n = \gamma_1...\gamma_m$ di $a$. Come dimostreresti che sono essenzialmente uniche? Io procedo così: siccome è irriducibile, è pure primo, quindi $\beta_1$ divide, senza perdita di generalità, $\gamma_1$: sono associati, essendo entrambi irriducibili. Perciò, a meno di invertibili, $\beta_2...\beta_n = \gamma_2...\gamma_m$. Allora, possiamo supporre che esista un $\ell < m$ per cui $1 = \gamma_\ell...\gamma_m$. Siamo in un dominio commutativo, dunque i fattori rimanenti sono tutti invertibili: questo è assurdo perché $\gamma_1...\gamma_m$ sono tutti irriducibili. Di conseguenza, $n = m$ e le fattorizzazioni sono uguali. ■

La dimostrazione del teorema dovrebbe farti venire in mente che anche se non si è in presenza un dominio dove il concetto di primo e irriducibile coincidono, finché vale la condizione ACCP, siamo certi di essere in un *dominio a fattorizzazione* (FD in inglese, da Factorisation Domain). Questa distinzione non è utile ai nostri scopi, ma serve a rafforzare l'idea che:

- l'ipotesi di ACCP è equivalente al *poter* fattorizzare,
- l'ipotesi che primi e irriducibili siano uguali equivale all'*unicità* della fattorizzazione.

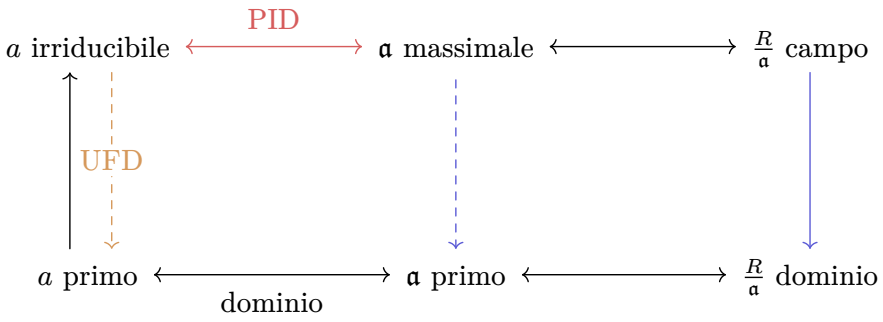
## Quozienti e PID

Un breve inciso sui quozienti di anelli. C'è un legame notevole tra la primalità e la massimalità dell'ideale $\mathfrak{m}$ di $R$ e le qualità del suo quoziente. Denotiamo con $Q$ il quoziente $\frac{R}{\mathfrak{m}}$.

- *$Q$ è un dominio integrale se e solo se $\mathfrak{m}$ è primo.* Se scrivi le definizioni, ti accorgi subito della banalità della faccenda, quindi non ti tedio. Di natura leggermente diversa è il seguente risultato.
- *$Q$ è un campo se e solo se $\mathfrak{m}$ è massimale.* Bisogna che tu ricordi il teorema di omomorfismo e il teorema di corrispondenza per gli anelli. Se hai qualche rudimento di teoria dei gruppi, la mia spiegazione non dovrebbe risultarti troppo difficile: l'ideale $\mathfrak{m}$ è massimale se e solo se gli unici ideali di $Q$ sono 0 e $Q$, se e solo se $Q$ è un campo.

Ti ho già introdotto ai PID: sono strutture che non incontreremo spesso in geometria algebrica, ma sono importanti: devi sapere che ogni PID è anche un UFD. Lo verifichiamo con la caratterizzazione che abbiamo appena dimostrato.

Anzitutto, in un PID ogni irriducibile è pure primo, come rende evidente la seguente catena di implicazioni.




Basta allora dimostrare che in un PID vale la ACCP (che è equivalente a ACC). Prendi una catena di ideali $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ e considera $I = \cup_i \mathfrak{a}_i$. L'insieme $I$ è un ideale, e in particolare è principale: $I = \mathfrak{b} = (b)$ per un certo $b$ in $R$, che può essere preso non invertibile (siccome $I \neq R$). Ora, $\exists i \in \mathbb{N} : b \in \mathfrak{a}_i$, quindi per ogni $\ell > i$, si ha $\mathfrak{a}_\ell = \mathfrak{b}$, quindi la catena è stazionaria.

**Esempio (♡).** Ricordi la questione sugli elementi massimali e irriducibili? Avevamo dimostrato che *un elemento $a$ è irriducibile se e solo se $\mathfrak{a}$ è massimale per ideali principali.* Nei PID, essere massimale per ideali principali è del tutto equivalente all'essere massimale, ma questo non è naturalmente vero per altre strutture. Se non sei convinto, ecco un controesempio: prendi $\mathbb{Z}$ e considera il suo anello di polinomi $\mathbb{Z}[X]$. L'ideale $(3)$ è primo (in effetti, 3 è primo in $\mathbb{Z}$… tornerò su questo punto più tardi) ma non risulta massimale: ad esempio, $(X, 3)$ non coincide con $\mathbb{Z}[X]$ ma neppure con $(3)$. Peraltro, $(X, 3)$ è massimale, poiché $\frac{\mathbb{Z}[X]}{(X,3)}$ è isomorfo al campo $\mathbb{F}_3$. Tuttavia, $(3)$ è ovviamente "massimale per ideali principali", nel senso che ogni ideale principale che contiene $(3)$ collassa su $(3)$ oppure su $\mathbb{Z}[X]$. Non a caso, le uniche possibilità per tale ideale sono $(3)$ oppure $(1) = \mathbb{Z}[X]$.

L'ultimo passaggio potrebbe non esserti chiaro: dopo la breve (ma doverosa) parentesi sui domini euclidei, tornerò a parlarti dei polinomi più nel dettaglio.

## Domini euclidei

Un dominio euclideo è un dominio $E$ dotato di una funzione di *valutazione*

$$v : E - \{0\} \to \mathbb{N}$$

che soddisfa le seguenti proprietà: per ogni $a, b \in E$ con $b \neq 0$ esistono $q, r \in E$ tali che

$$a = bq + r$$
$$r = 0 \text{ oppure } v(r) < v(b).$$

Questa proprietà generalizza a tutti gli effetti la divisione euclidea su $\mathbb{Z}$ (in effetti, $\mathbb{Z}$ è un dominio euclideo con la funzione di valutazione *valore assoluto*). Non è difficile provare che ogni dominio euclideo è anche un PID e lo si fa dimostrando che, per ogni ideale $I$ di $E$, $I = \mathfrak{b}$, dove $b \in I$ è un elemento dell'ideale con valutazione minima tra tutti gli elementi di $I$.

Tra tutte le strutture algebriche che abbiamo visto, solo i campi sono stati trattati in maniera marginale. Ti ricordo che $\mathbb{Z}$ è un dominio euclideo, ma non è un campo: forse, essere campo sembra essere una condizione più forte dell'essere euclideo… ma infatti, se $F$ è un campo, per ogni due $a \in F, b \in F^\times$, possiamo sempre scrivere

$$a = b(b^{-1}a) + 0.$$

Da questo, dovrebbe esserti chiaro che ogni campo è anche un dominio euclideo!

Abbiamo visto le proprietà dei principali domini integri commutativi. Questo schema potrebbe aiutarti a visualizzare meglio le catene di implicazioni che abbiamo dimostrato.

Domini Integri ⟵ UFD ⟵ PID ⟵ Domini Euclidei ⟵ Campi

## Anelli di polinomi

Stavolta, non procederò con definizioni formali. Piuttosto, assumerò che tu sappia cosa sia un polinomio e in che modo possiamo definire il prodotto tra due polinomi. L'insieme dei polinomi nell'incognita $X$ con coefficienti nell'anello $A$ si indica con $A[X]$, ed è anch'esso un anello con le operazioni di somma e prodotto canoniche. Anelli di polinomi in $A$ di più variabili possono essere definiti in modo "ricorsivo" come $A[X,Y] = (A[X])[Y]$ (questo richiederebbe una dimostrazione rigorosa, ma penso che sia più che opportuno ometterla).

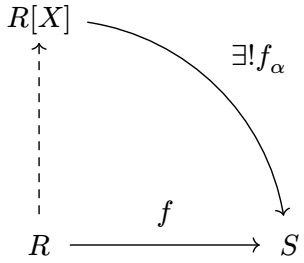
D'ora in poi, $R$ *sarà un dominio integro*. In questo caso, non è difficile vedere che $R[X]$ è un dominio integro e vale che $\deg(fg) = \deg f + \deg g$. Inoltre, se $f, g \in R[X]$ sono invertibili, allora necessariamente

$$1 = fg \implies 0 = \deg f + \deg g \implies 0 = \deg f = \deg g.$$

Ne consegue che $R^\times = (R[X])^\times$. Uno strumento importantissimo nell'ambito dei polinomi è il *principio di sostituzione*. Consideriamo un morfismo di anelli $f : R \to S$, e sia $\alpha \in S$. Allora esiste un unico morfismo $f_\alpha : R[X] \to S$ tale che

$$f_\alpha(x) = f(x) \text{ per ogni } x \in R \text{ e che}$$
$$f_\alpha(X) = \alpha.$$

Quello che ci dice il teorema è, se vogliamo, intuitivo: se voglio estendere $f$ in modo che "$f(X) = \alpha$", v'è un unico modo! Un diagramma potrebbe aiutarti a visualizzare questo risultato:




Un applicazione di questo teorema permette di definire un esempio altrettanto importante di dominio euclideo. Considera l'immersione degli interi nei complessi $f : \mathbb{Z} \to \mathbb{C}$. Sia $\alpha = i$ l'unità immaginaria. Esiste un unico morfismo $f_i : \mathbb{Z}[X] \to \mathbb{Z}[i]$ tale che $f_i(X) = i$. L'immagine di $f_i$ è l'anello $\mathbb{Z}[i]$ degli *interi di Gauss*. Il fatto che questo sia un dominio euclideo non è del tutto banale, ma la sua dimostrazione non rientra tra gli scopi di questa lettera: la puoi trovare, comunque, in qualsiasi libro di Algebra. La valutazione di $\mathbb{Z}[i]$ è $N(\alpha + i\beta) = \alpha^2 + \beta^2$, ovvero la norma nel campo complesso al quadrato.

Com'è noto dalle scuole superiori, tra polinomi si può dividere. V'è un teorema che regolamenta questa divisione e che ci dice quando è possibile eseguirla. Non mi addentrerò in conti: ti basta sapere che se il coefficiente direttivo è invertibile, allora si può eseguire la divisione euclidea per qualsiasi polinomio di $R[X]$ (questo risultato vale per anelli che non sono domini integri). Chiaramente, se $F$ è un campo, questo risultato ci dice che $F[X]$ è un dominio euclideo (con valutazione $v = \deg$, naturalmente).

Vien da sé che, per studiare la divisibilità in questo ambiente, si usano i teoremi che abbiamo già introdotto prima. Vedere che un polinomio $f$ è irriducibile in $R[X]$ è del tutto equivalente a dimostrare che il quoziente $\frac{R[X]}{\mathfrak{f}}$ sia un campo, per esempio. Vale un discorso analogo per quanto riguarda la primalità. Siccome $R[X]$ è un'estensione di $R$, è naturale chiedersi se sussistano delle relazioni tra gli elementi irriducibili o primi di $R$ e quelli di $R[X]$. È sempre vero, ad esempio, che se $a \in R$ è irriducibile in $R$, lo è anche in $R[X]$? La risposta è affermativa, nel senso che *ogni irriducibile di $R$ lo è anche in $R[X]$*.
Per vederlo, il modo più semplice che mi è venuto in mente è confrontare i gradi. Se $p \in R$ è irriducibile in $R$, allora lo è necessariamente anche in $R[X]$: per la proprietà dei gradi, un elemento $r$ che è un divisore proprio di $p$ è tale che $\deg r = 0 = \deg p$. Di conseguenza, gli unici divisori propri di $p$, se esistono, sono da ricercare tra gli elementi di $R$, dunque l'irriducibilità in $R[X]$.

Ci aspettiamo che la struttura di $R[X]$ dipenda in qualche modo da quella di $R$. Come ti ho fatto vedere all'inizio, la proprietà di integralità è abbastanza robusta: $R[X]$ è un dominio integro se e solo se $R$ lo è. Il risultato è decisamente facile da dimostrare. Di diversa natura è invece il seguente: *$R$ è un UFD se e solo se $R[X]$ è un UFD*, la cui dimostrazione usa qualche fatto che non ho avuto modo di mostrarti e che quindi ometto.

Riprendiamo in mano l'esempio (♡). Se ricordi bene, nelle scorse righe, ho sfruttato il fatto che $(3)$ fosse primo in $\mathbb{Z}$ per dire che $(3)$ lo è in $\mathbb{Z}[X]$. In generale, la relazione di primalità su $R$ non passa agli anelli di polinomi di $R[X]$: è una condizione piuttosto forte. Tuttavia, osserva: $\mathbb{Z}$ è un UFD, quindi anche $\mathbb{Z}[X]$ lo è, e allora primi e irriducibili coincidono. Siccome $3$ è irriducibile in $\mathbb{Z}$, lo è anche in $\mathbb{Z}[X]$, quindi $(3)$ è un ideale *primo* di $\mathbb{Z}[X]$.

Se ricordi qualche nozione di teoria della computazione, questo finale inciso può essere interessante. Ho detto che la condizione di irriducibilità è più debole di quella di primalità: per stressare su questo fatto, ti porto questo esempio. Il problema PRIME che decide su $\mathbb{N}$ l'insieme dei numeri primi è un problema decidibile, nel senso che esiste un algoritmo che ne calcola la funzione caratteristica. Se `n` è il numero naturale in input,

```
predicate is_prime(n: int) {
    for i in 2..(n/2) {
      if n % i == 0:
        return false;
    }
    return true;
}
```

fornisce una procedura che decide l'insieme dei numeri primi (in tempo esponenziale). Il predicato `is_prime` decide l'insieme dei numeri primi perché la condizione di irriducibilità – che è quella che il predicato controlla, nella realtà – è equivalente a quella di primalità. Se fossimo stati in un dominio arbitrario, le due proprietà non sarebbero state uguali, dunque decidere l'insieme dei primi in $R$ sarebbe stato un gran problema: avremmo dovuto controllare tutti gli elementi di $R$. A meno di trovare modi più furbi, nel caso di $\#R = \infty$, l'algoritmo per *forza bruta* termina se `n` è primo, ma non termina mai se `n` non lo è!

## In conclusione

Cara amica, dopo tutte queste pagine, spero tu sia arrivata sana e salva fino a qui. Vedi, l'algebra per me è stata inizialmente una grande sofferenza. Non ti mento che l'esame di Algebra I mi è andato particolarmente male: un misero diciotto. Come vendetta, ho deciso di scrivere queste

pagine proprio sulla parte più antipatica del programma – o almeno, quella che al tempo ritenevo tale! Se sono stato capace di scrivere queste pagine, è grazie allo sforzo e passione di svariati mesi. In fondo, il mio professore di matematica aveva ragione a dirmi che ci sarebbe voluto del tempo perché tutto potesse diventarmi più naturale.

Nella busta, dovresti aver ricevuto, oltre a queste pagine, una cartolina di Firenze. Quello che vedi dietro di me è il duomo, finito negli anni '30 del 1400. È impressionante, non trovi? Il giorno in cui ho scattato quella fotografia era particolarmente felice e spensierato e ho bei ricordi di quel giro in centro. Quando tornerai qua in Italia? Io e Paolo ti aspettiamo!

Intanto, ti auguro il meglio.

*per Ekaterina Perelmanova,*

*da Francesco.*

*Firenze, 21 luglio 2026*