NON UNICITÀ DI FATTORIZZAZIONE E SOTTOANELLI DI ANELLI DI POLINOMI.

PAOLO ZANARDO

È universalmente noto che ogni numero intero > 1 si scrive in modo unico come prodotto di numeri primi. I Matematici sanno anche che un'analoga proprietà è soddisfatta dall'anello dei polinomi a coefficienti in un campo, ma che l'unicità di fattorizzazione in prodotto di elementi irriducibili non vale in generale negli anelli commutativi. Lo scopo di questa nota è illustrare vari tipi di fattorizzazioni non uniche di elementi in un anello, tramite esempi di domini di integrità che sono sottoanelli o generalizzazioni di anelli di polinomi. Pur richiedendo solo nozioni di base per essere definiti, si tratta di esempi non ovvi, specialmente quelli finali.

1. Preliminari.

Con R denoteremo un *dominio d'integrità*, ossia un anello commutativo (con $1 \neq 0$) senza divisori dello zero. (Per ogni $a, b \in R \setminus \{0\}$ si ha $ab \neq 0$.)

Un elemento $u \in R$ è *invertibile* se esiste $u' \in R$ tale che $uu' = 1$. R è un *campo* se ogni $0 \neq a \in R$ è invertibile.

Sia $0 \neq a \in R$ *non invertibile*.

(1) a è *irriducibile* se non ha fattori propri, ossia, se $a = bc$ $(b, c \in R)$ allora b oppure c è invertibile.

(2) a è *primo* se soddisfa la seguente proprietà: se a divide bc in R, allora a divide b oppure a divide c.

NB. $a \in R$ primo implica a irriducibile (facile verifica), *ma non viceversa*. Nell'anello R_1 che vedremo fra breve, l'elemento $2 \in R_1$ è irriducibile ma non primo.

DEF. Si dice che R è un *dominio a fattorizzazione unica* (simbolo: UFD) se ogni $0 \neq a \in R$ *non invertibile* è un prodotto $a = x_1 \cdots x_n$, con gli x_i irriducibili, e tale fattorizzazione è (essenzialmente) *unica*, ossia, se $a = y_1 \cdots y_m$ con gli y_j irriducibili, allora $n = m$ e, riordinando gli indici, si ha $x_i = y_i u_i$, con gli u_i *invertibili*. (Naturalmente il prodotto di tali u_i è 1.)

Due fattorizzazioni di $a \in R$ come sopra sono dette *equivalenti*.

Esempio. Negli interi $\mathbb{Z}$ si ha $75 = 3 \cdot 5 \cdot 5 = (-5) \cdot 3 \cdot (-5) = (-3) \cdot (-5) \cdot 5$. La prima e la terza fattorizzazione sono equivalenti.

È facile dimostrare la seguente

Proposition 1.1. *Sia R un UFD. Allora $a \in R$ è irriducibile se e solo se è primo.*

Esempi di UFD: I campi (banalmente, poiché ogni elemento $\neq 0$ è invertibile); gli interi $\mathbb{Z}$; gli anelli di polinomi $K[X]$, a coefficienti nel *campo* K.

Theorem 1.2. *R è un UFD se e solo se $R[X]$ è un UFD.*

Il teorema precedente fornisce ulteriori esempi di UFD: $\mathbb{Z}[X]$, $K[X_1, \ldots, X_m]$, $D_\infty = K[X_n : n > 0]$ (polinomi sul campo K a finite o infinite indeterminate).
Si verifica che D_∞ è un UFD usando il fatto che $D_\infty = \bigcup_{m=1}^{\infty} K[X_1, \ldots, X_m]$.

L'unicità di fattorizzazione è un rilevante argomento di ricerca in Algebra. Un esempio di importante questione in Teoria Algebrica dei Numeri: stabilire quali anelli di interi algebrici sono UFD.

2. L'esempio classico di non UFD.

Consideriamo l'anello $R_1 = \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$.

Sia $a + i\sqrt{5}b \in R_1$. La sua norma come numero complesso è $N(a+i\sqrt{5}b) = a^2 + 5b^2$. Cerchiamo ora gli elementi invertibili di R_1. Sia $u + i\sqrt{5}v$ invertibile in R_1; il suo inverso è il suo coniugato in $\mathbb{C}$. Allora la sua norma $N(u+i\sqrt{5}v) = u^2+5v^2 = 1$, essendo la norma moltiplicativa. Di conseguenza $u + iv = \pm 1$.

$\mathbb{Z}[i\sqrt{5}]$ *non* è a fattorizzazione unica. Infatti

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 1 + (\sqrt{5})^2$$

sono due fattorizzazioni non equivalenti di 6 in fattori irriducibili (*non primi!*). Da $N(2) = 4$, $N(3) = 9$, $N(1 \pm i\sqrt{5}) = 6$, segue che $2, 3, 1 \pm i\sqrt{5}$ non sono prodotti di due elementi non invertibili, essendo la norma moltiplicativa, e quindi sono tutti irriducibili. (Se $\alpha, \beta \in R_1$ non sono interi $N(\alpha\beta) \geq 25$.)

Inoltre, per esempio, $(1 \pm i\sqrt{5})/2 \notin \mathbb{Z}[i\sqrt{5}]$, quindi le due fattorizzazioni di 6 non possono essere equivalenti.

L'anello R_1 fornisce altre fattorizzazioni interessanti. Usando le definizioni, si prova direttamente che 11 è un elemento primo di R_1, da cui si ricava che $22 = 2 \cdot 11$ è l'unica fattorizzazione di $22 \in R_1$; quindi 22 si fattorizza in modo unico come prodotto di elementi irriducibili di R_1, ma *non ammette* una fattorizzazione in prodotto di primi, come avviene negli UFD. Infatti 2 non è primo in R_1.

Notiamo che 11 è il più piccolo intero positivo a essere primo in R_1. Infatti $2, 3$ non sono primi, 5 non è irriducibile, e le fattorizzazioni $14 = 2 \cdot 7 = (3+i\sqrt{5})(3-i\sqrt{5})$ mostrano che neppure 7 è primo in R_1.

3. Sottoanelli di anelli di polinomi

Dato un campo K, consideriamo i polinomi su K privi del termine di grado 1.

$$R_2 = K + X^2K[X] = K[X^2, X^3] \subset K[X].$$

Ovviamente R_2 è un sottoanello di $K[X]$. Notiamo che $u \in R_2$ è invertibile se e solo se $0 \neq u \in K$.

Consideriamo $f = X^2, g = X^3$, elementi di R_2. L'uguaglianza

$$X^6 = f \cdot f \cdot f = g \cdot g$$

fornisce due fattorizzazioni non equivalenti di X^6. Infatti f, g sono irriducibili in R_2 (almeno un divisore proprio non invertibile di f o g dovrebbe essere X, ma $X \notin R_2$) e i due prodotti hanno un numero diverso di fattori.

Notiamo che da $R_2 \subset K[X]$ segue che ogni $a \in R$ non invertibile è prodotto di irriducibili. Analogamente, ogni $r \in R_1 = \mathbb{Z}[i\sqrt{5}]$ non invertibile è prodotto di irriducibili, essendo la norma moltiplicativa. Questa proprietà, apparentemente così spontanea, non vale in generale, neppure in anelli semplici come quello che segue.

OSS. Un UFD R non contiene elementi $a \neq 0$ *infinitamente divisibili*, ossia tali che per ogni $n > 0$ esistono $b_1, \ldots, b_n \in R$ *non invertibili* tali che $b_1 \cdots b_n$ divide a in R.

Consideriamo i polinomi a coefficienti in $\mathbb{Q}$ con termine noto in $\mathbb{Z}$.

$$R_3 = \mathbb{Z} + X\mathbb{Q}[X] \subset \mathbb{Q}[X].$$

Ovviamente R_3 è un anello; 1, -1 sono gli unici invertibili.

Sia $p \in \mathbb{Z} \subset R_3$ numero primo. Allora p è irriducibile in R_3. Per ogni $n > 0$ si ha $X/p^n \in R_3$, per cui $X = p^n(X/p^n)$ è infinitamente divisibile. Quindi R_2 non è un UFD.

D'altra parte, sia $h \in R_3$, $h \notin X\mathbb{Q}[X]$. Allora $h = m + Xf = m(1 + Xg)$, ove $g = f/m$. Usando questa scrittura di h e la fattorizzazione unica in $\mathbb{Q}[X]$, si prova senza troppa fatica la seguente

Proposition 3.1. *(i) Gli elementi irriducibili di R_3 sono primi.*
(ii) Ogni $h \in R_3 \setminus X\mathbb{Q}[X]$ si scrive in modo unico come prodotto di elementi irriducibili di R_3.
(iii) $X\mathbb{Q}[X]$ contiene tutti e soli gli elementi infinitamente divisibili di R_3.

La proposizione mostra che R_3 è "vicino" a essere un UFD, nel senso che i suoi elementi che non sono infinitamente divisibili si fattorizzano *in modo unico* come prodotto di primi.

4. Altri Esempi

Ricordiamo la definizione di ideale di un anello. $I \subset R$ è un *ideale* (proprio) di R se:
$1 \notin I$; $ra \in I$ per ogni $r \in R$, $a \in I$; se $a, b \in I$ allora $a + b \in I$.

R è detto *dominio a ideali principali* (simbolo: PID) se ogni ideale di R è principale, ossia della forma aR per un opportuno $a \in R$.

Theorem 4.1. *Un dominio a ideali principali è un UFD.*

Esempi di PID: $\mathbb{Z}$, $K[X]$.

Diamo ora un esempio di anello V la cui definizione appare inusuale e molto più complicata rispetto a quelle di R_2 e R_3, ma che in realtà ha una struttura molto semplice, da cui derivano fattorizzazioni immediate dei suoi elementi.

Sia K campo, X, Y indeterminate. Consideriamo l'anello

$$D = K[X, Y] \subset K(X, Y) = F,$$

ove F è il campo delle frazioni di D. Se $f \in D$, $\delta(f)$ denota il *grado* del polinomio f; se $f/g \in F$ definiamo il grado $\delta(f/g) = \delta(f) - \delta(g)$.

Sia

$$V = \{f/g \in F : \delta(f/g) \leq 0\}.$$

Si noti che V è un sottoanello di F, poiché

$$\delta(ab) = \delta(a) + \delta(b)\ ,\ \delta(a + b) \leq \max\{\delta(a), \delta(b)\}.$$

Dato che ogni $f \in D \setminus K$ ha grado > 0, si ha $D \cap V = K$.
Notiamo che $u \in V$ è invertibile se e solo se $\delta(u) = 0$. Per esempio $\frac{X^2+1}{XY-X+Y}$ è invertibile. Inoltre $1/f \in V$ per ogni $0 \neq f \in D$, quindi F è il campo delle frazioni anche di V.

Si vede subito che $\mathfrak{M} = \{r \in V : \delta(r) < 0\}$ è un ideale di V. Ovviamente $\mathfrak{M}$ contiene ogni altro ideale di V, quindi è l'unico ideale massimale.

Si ha $\mathfrak{M} = \frac{1}{X}V$. Basta verificare che $\mathfrak{M} \subseteq \frac{1}{X}V$. Infatti, se $a \in \mathfrak{M}$, allora $\delta(a) = -m < 0$, e si ha

$$a = (1/X)(aX) \quad \text{ove } \delta(aX) = -m + 1 \leq 0.$$

Quindi $aX \in V$ da cui $a \in \frac{1}{X}V$.

Notiamo che $1/X$ è irriducibile in V, poiché $\delta(1/X) = -1$, e il prodotto di due elementi non invertibili di V ha grado ≤ -2.

Si ha anche $\mathfrak{M} = \frac{1}{Y}V$ poiché $1/Y = (1/X)(X/Y)$, e $\delta(X/Y) = 0$, per cui X/Y è invertibile. In effetti, $\mathfrak{M} = bV$ se e solo se $\delta(b) = -1$.

Sia $z \in F$. Da $\delta(z) = -\delta(1/z)$, si ricava che, per ogni $z \in F$, si ha $z \in V$ oppure $1/z \in V$. Questa proprietà mostra che V è un *dominio di valutazione*.
(Non insistiamo su questa nozione: per approfondirla si può consultare internet.)

Gli ideali di V formano una catena:

$$\mathfrak{M} = \frac{1}{X}V \supset \frac{1}{X^2}V \supset \cdots \supset \frac{1}{X^n}V \supset \dots$$

La dimostrazione è facile: ogni ideale $0 \neq I$ di V è generato dalla minima potenza di $1/X$ che esso contiene. Quindi V è un PID; in particolare V è un UFD.

In effetti, se $0 \neq t \in V$ non è invertibile (ovvero $t \in \mathfrak{M}$), si ha $\delta(t) = -n < 0$ e allora

$$t = \frac{1}{X^n}(X^n t)$$

è la fattorizzazione unica di t in V; infatti $X^n t \in V$ è invertibile, avendo grado zero.

Abbiamo quindi concluso che V ha una struttura di ideali molto semplice, da cui si ricava subito la fattorizzazione unica di ogni suo elemento.

Estendiamo ora, in modo molto naturale, l'usuale nozione di polinomio.

Sia $\mathbb{Q}_{>0}$ l'insieme dei razionali > 0. Definiamo i *polinomi su K a esponenti razionali > 0*,

$$D = K[X, \mathbb{Q}_{>0}] = \{a_0 + \sum_{i\geq 1} a_i X^{q_i} : a_0, a_i \in K, q_i \in \mathbb{Q}_{>0}\},$$

ove le somme sono finite, $0 < q_1 < q_2 < \dots$, e valgono le solite regole delle potenze $X^q X^r = X^{q+r}$, $(X^q)^r = X^{qr}$ e della moltiplicazione fra polinomi.

Un elemento $u \in K[X, \mathbb{Q}_{>0}]$ è invertibile se e solo se $0 \neq u \in K$.

Poichè ogni $f \in D$ è un polinomio in $X^{1/k}$ per un opportuno $k > 0$, si ha $D = K[X^{1/n} : n > 0]$.

Notiamo che D non è un UFD, poiché, per esempio, $X = (X^{1/n})^n$ per ogni $n > 0$, quindi X è infinitamente divisibile in D. Tuttavia è più interessante il seguente sottoanello di D, che presenta fattorizzazioni non uniche di un tipo non ancora esaminato.

Definiamo

$$R_4 = \{a_0 + \sum_{i\geq 1} a_i X^{q_i} \in D : q_1 \geq 1\} = K + XD.$$

Quindi R_4 è il sottoanello di D i cui polinomi non contengono nella loro espressione alcun X^r con $0 < r < 1$.

Si verifica che:

(1) X^q è irriducibile in R_4 per ogni $1 \leq q < 2$;

(2) $X^2 = X \cdot X$ è l'unica fattorizzazione di X^2 in elementi irriducibili di R_4;

(3) le potenze del tipo X^{2+s} con $0 < s < 1$ ammettono *infinite fattorizzazioni non equivalenti in prodotto di due irriducibili*, del tipo

$$X^{2+s} = X^{1+a} X^{1+b}$$

ove $0 \leq a, b < 1$ e $a + b = s$; tali elementi *non* sono prodotti di almeno 3 irriducibili.

Dal fatto che $X^q \in R_4$ implica $q \geq 1$, segue facilmente che R_4 non contiene elementi infinitamente divisibili.

Notiamo che i precedenti domini d'integrità R_1 e R_2 non contengono elementi soddisfacenti la proprietà (3). (A maggior ragione V, essendo un UFD, non contiene elementi di questo tipo.)

Altre proprietà di fattorizzazione si possono trovare per gli X^r con $r \geq 3$. Per esempio, $X^3 = X \cdot X \cdot X = X^{1+a}X^{1+b}$ $(a + b = 1)$ ha un'unica fattorizzazione in tre irriducibili e infinite fattorizzazioni in due irriducibili.

Cerchiamo ora un dominio d'integrità che non sia un campo e che *non contenga elementi irriducibili*.

Sia $F_p = \mathbb{Z}/p\mathbb{Z}$. Ricordiamo che $a^p = a$ per ogni $a \in F_p$. Inoltre, per il celebre endomorfismo di Frobenius, se un anello R ha caratteristica p, e $a, b \in R$, allora $(a + b)^p = a^p + b^p$.

Verifichiamo che

$$R_5 = F_p[X, \mathbb{Q}_{>0}]$$

non contiene elementi irriducibili.

Ricordiamo che $0 \neq u \in R_5$ è invertibile se e solo se $u \in F_p$.

Sia $f = a_0 + a_1X^{q_1} + \cdots + a_nX^{q_n} \in R_5 \setminus F_p$; si ha

$$(a_0 + a_1X^{q_1/p} + \cdots + a_nX^{q_n/p})^p = a_0 + a_1X^{q_1} + \cdots + a_nX^{q_n}.$$

Concludiamo che ogni $0 \neq f \in R_5$ non invertibile è una potenza p-esima in R_5, quindi non è irriducibile. Ovviamente f è infinitamente divisibile, quindi R_5 non è un UFD.

CURIOSITÀ. Consideriamo il seguente insieme di numeri reali

$$E = \{a_0 + a_1\pi^{q_1} + a_2\pi^{q_2} + \cdots + a_n\pi^{q_n} : n > 0\}$$

al variare di $a_0, a_i \in \mathbb{Q}$ e $q_i \in \mathbb{Q}_{>0}$; π è pi-greco.

Allora E è un dominio d'integrità isomorfo a $D = \mathbb{Q}[X, \mathbb{Q}_{>0}]$.

Infatti la mappa $\phi : D \to E$

$$\phi : a_0 + a_1X^{q_1} + \cdots + a_nX^{q_n} \mapsto a_0 + a_1\pi^{q_1} + \cdots + a_n\pi^{q_n}$$

è un isomorfismo, essendo π trascendente su $\mathbb{Q}$. (Ossia: π non è radice di alcun polinomio a coefficienti razionali.)

Più in generale, se $K \subset \mathbb{R}$ è un'estensione algebrica di $\mathbb{Q}$, per la trascendenza di π si conclude facilmente che $\mathbb{R}$ contiene copie isomorfe degli anelli di polinomi a esponenti razionali sul campo K e dei loro sottoanelli del tipo di R_4. Per lo stesso motivo i reali contengono anche copie di R_2 e R_3; infine $V \subset \mathbb{R}$, se per X e Y scegliamo due numeri reali *algebricamente indipendenti* su $\mathbb{Q}$. (Ossia: la coppia (X, Y) non annulla alcun polinomio in due variabili a coefficienti in $\mathbb{Q}$.)

5. EXTRA

L'esempio finale si distacca dai precedenti, in quanto fa uso della nozione di anello quoziente modulo un ideale. Gli anelli quoziente sono una fonte copiosa di esempi di fattorizzazioni non uniche.

Nelle notazioni precedenti, consideriamo l'anello $D = K[X, Y, Z^{1/n} : n > 0]$.

Notiamo che $XY - Z$ è un elemento primo di D. Di conseguenza l'ideale principale $J = (XY - Z)D$ è un *ideale primo* di D (ossia se $f \notin J$ e $g \notin J$ allora $fg \notin J$, per tutti gli $f, g \in D$).

Essendo J ideale primo, l'anello quoziente $R_6 = D/J$ è un dominio d'integrità.

Siano $x = X + J$, $y = Y + J$, $z^{1/n} = Z^{1/n} + J$ $(n > 0)$ le classi laterali mod J. Si verifica facilmente che

(i) x, y sono irriducibili in R_6;

(ii) per ogni $n > 0$,

$$z = xy, \quad z = (z^{1/n})^n.$$

Quindi l'elemento z è prodotto di due irriducibili in R_6, ma è anche infinitamente divisibile in R_6.

Con le fattorizzazioni può succedere di tutto!