Lezione 26

Prerequisiti: Lezione 23.

Un dominio ad ideali principali che non è un dominio euclideo.

Sappiamo già da tempo che ogni dominio euclideo è un PID, ma non abbiamo mai indagato se sia vera l'implicazione contraria, né ci siamo mai imbattuti in un controesempio. In questa lezione ne presentiamo finalmente uno: si tratta dell'anello $D_{\mathbf{Q}(i\sqrt{19})}$ che, in base alla Proposizione 19.20, è $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. Per dimostrare che è un PID si può provare che il suo numero delle classi di ideali è 1 (vedi Proposizione 22.17) come abbiamo fatto nella Lezione 24 per provare che $\mathbf{Z}\left[\sqrt{2}\right]$ è un PID (vedi Esempio 24.6). Esiste però un altro possibile procedimento, basato su un particolare tipo di norma.

Definizione 26.1 Sia A un dominio d'integrità. Si dice *norma di Hasse-Dedekind* su A ogni applicazione $N : A^* \to \mathbf{N}^*$ tale che per ogni $a,b \in A$, $a,b \neq 0$ si ha che $a \in (b)$ oppure esiste $c \in (a,b)$, $c \neq 0$, tale che $N(c) < N(b)$.

Nota La condizione della Definizione 26.1 si può riformulare equivalentemente come segue: per ogni $a,b \in A$, $a,b \neq 0$ esiste $q \in A$ tale che $a = bq$ oppure esistono $q,s \in A$ tali che $sa - bq \neq 0$ e $N(sa - bq) < N(b)$.

Si ha questa interessante caratterizzazione:

Proposizione 26.2 Un dominio d'integrità A è un PID se e solo se ammette una norma di Hasse-Dedekind.

Dimostrazione: Supponiamo che A ammetta una norma di Hasse-Dedekind N. Sia I un ideale non nullo di A. Sia $b \in I$ un elemento non nullo di norma minimale. Sia $a \in I$. Allora $(a,b) \subset I$. Se $a \notin (b)$, allora esisterebbe $c \in (a,b)$, $c \neq 0$ con $N(c) < N(b)$, ma, essendo $c \in I$, ciò contraddirebbe la scelta di b. Quindi $a \in (b)$, e pertanto, per l'arbitrarietà di a, si ha $I = (b)$. Ciò prova che A è un PID.
Viceversa, sia A un PID. Si ponga $N(u) = 1$ per ogni $u \in A$ invertibile e, per ogni $a \in A$ non nullo e non invertibile, $N(a) = 2^n$, se n è il numero dei fattori irriducibili di a (ricordiamo che ogni PID è un UFD). In questo modo abbiamo definito un'applicazione $N : A^* \to \mathbf{N}^*$ che gode della proprietà moltiplicativa. Siano $a,b \in A$, $a,b \neq 0$, sia $c \in A$ tale che $(a,b) = (c)$. Supponiamo che $a \notin (b)$. Allora $(c) = (a,b) \neq (b)$. Essendo $b \in (c)$, si ha che $b = xc$; ma allora x non è invertibile. Segue che $N(b) = N(x)N(c) > N(c)$ (perché?). Ciò prova che N soddisfa anche la Definizione 26.1, e conclude la dimostrazione che N è una norma di Hasse-Dedekind. □

Osservazione 26.3 La valutazione N di un dominio euclideo è una sorta di norma di Hasse-Dedekind. Infatti la condizione della nota vale per $s = 1$. Il significato della Proposizione 26.2 è quindi il seguente: un PID è una sorta di dominio euclideo "più generale", con una norma che soddisfa condizioni "più deboli". Ciò è riassunto nel titolo *Principal Ideal Domains are almost*

Euclidean che John Greene, nel 1997 ha dato all'articolo [Gr] contenente la dimostrazione del "solo se". L'implicazione contraria è invece apparsa nel 1928, per opera di Helmut Hasse (1898-1979) [Ha], che si ispirò agli studi di Richard Dedekind (1831- 1916).

Esempio 26.4 Proviamo che $A = \mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ è un PID, dimostrando che la norma $N = N_{\mathbf{Q}(i\sqrt{19})/\mathbf{Q}}$ definita nella Lezione 23 (rispetto alla base $1, i\sqrt{19}$) è una norma di Hasse-Dedekind su A. Per ogni $a,b \in \mathbf{Z}$ si ha

$$N(a+\frac{1+i\sqrt{19}}{2}b) = N(a+\frac{b}{2}+\frac{b}{2}i\sqrt{19}) = (a+\frac{b}{2})^2 + 19\frac{b^2}{4} = a^2 + ab + \frac{b^2}{4} + 19\frac{b^2}{4} = a^2 + ab + 5b^2.$$

Siano $\alpha, \beta \in A$ non nulli tali che β non divide α. Proviamo che esistono $s,t \in A$ tali che $s\alpha - t\beta \neq 0$ e $N(s\alpha - t\beta) < N(\beta)$, ossia, data la moltiplicatività della norma N (vedi la Proposizione 23.4), tali che

$$N(s\alpha\beta^{-1} - t) < N(1) = 1. \qquad (1)$$

Osserviamo che $\alpha\beta^{-1} \in \mathbf{Q}(i\sqrt{19})$ che, in base alla Proposizione 20.5, è il campo dei quozienti di A; inoltre, per ipotesi, $\alpha\beta^{-1} \notin A$. Possiamo quindi scrivere

$$\alpha\beta^{-1} = \frac{a+bi\sqrt{19}}{c}, \quad \text{con } a,b,c \in \mathbf{Z} \text{ coprimi, } c > 1.$$

In base al Lemma di Bézout, esistono $x,y,z \in \mathbf{Z}$ tali che $ax + by + cz = 1$. Siano $q,r \in \mathbf{Z}$ tali che $ay - 19bx = cq + r$, con $|r| \leq \left[\frac{c}{2}\right]$. Sia $s = y + xi\sqrt{19}$, e $t = q - zi\sqrt{19}$. Allora

$$0 < N(s\alpha\beta^{-1} - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} \leq \frac{\left[\frac{c}{2}\right]^2 + 19}{c^2},$$

e quindi vale (1) se $c \geq 5$. Consideriamo separatamente i restanti casi.
Sia $c = 2$. Allora *a,b* non sono entrambi pari (per rispettare la condizione di coprimalità), ma non possono essere nemmeno entrambi dispari, perché altrimenti $\alpha\beta^{-1} \in A$. Quindi uno tra *a,b* è pari, l'altro è dispari. Segue che $t = \frac{a-1+bi\sqrt{19}}{2} \in A$; un rapido calcolo mostra che questo numero, insieme a $s = 1$, verifica (1).
Sia ora $c = 3$. Allora 3 non può dividere entrambi *a,b*. Segue che $a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 3$. Sia *q* il quoziente della divisione di $a^2 + 19b^2$ per 3. Allora (1) è verificata da $s = a - bi\sqrt{19}$, $t = q$.
Sia infine $c = 4$. Allora *a,b* non sono entrambi pari. Se uno è pari, e l'altro è dispari, allora $a^2 + 19b^2$ è dispari. Sia *q* il quoziente della divisione di $a^2 + 19b^2$ per 4. Allora (1) è soddisfatta da $s = a - bi\sqrt{19}$, $t = q$. Se *a,b* sono entrambi dispari, allora si può prendere $s = \frac{a-bi\sqrt{19}}{2}, t = q$, ove *q* è il quoziente della divisione di $a^2 + 19b^2$ per 8.

Il nostro prossimo obiettivo è dimostrare che A non è un dominio euclideo. A tal fine sarà utile dare un nuovo criterio necessario (che sia diverso da quello di essere un PID, inapplicabile in questo caso). Esso sarà basato sulla seguente nozione:

Definizione 26.5 Un elemento non nullo e non invertibile a di un dominio d'integrità A si dice un *divisore laterale universale* se per ogni $x \in A$ esiste un elemento nullo o invertibile y tale che a divida $x - y$.

Proposizione 26.6 Un dominio euclideo che non è un campo possiede un divisore laterale universale.

Dimostrazione: Sia A un dominio euclideo (non un campo) rispetto alla valutazione N. Sia a un elemento non nullo e non invertibile tale che $N(a)$ sia minimale. Per ogni $x \in A$ esistono $q, r \in A$ tali che $x = aq + r$ e $r = 0$ oppure $r \neq 0$ e $N(r) < N(a)$. Nel secondo caso r è invertibile. Ciò prova che a è un divisore laterale universale. □

Esempio 26.7 Proviamo che $A = \mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ non è un dominio euclideo dimostrando che non possiede alcun divisore laterale universale. Come stabilito dal Corollario 23.15, gli elementi invertibili di A sono quelli di norma 1, ovvero 1 e –1. Supponiamo per assurdo che esista un divisore laterale universale $\alpha \in A$. Applicando la Definizione 26.5 a $x = 2$, segue che α divide 2 oppure 3. Considerando le norme di questi elementi, è facile vedere che 2 (che ha norma 4) e 3 (che ha norma 9) ammettono solo i divisori interi banali. Quindi $\alpha \in \{2, -2, 3, -3\}$. Ogni multiplo di 2 (o –2) ha norma multipla di 4. Se 2 (o –2) fosse un divisore laterale universale, allora dividerebbe $\frac{1+i\sqrt{19}}{2}$ oppure $\frac{1+i\sqrt{19}}{2} \pm 1$. Ma ciò è impossibile, perché questi tre elementi hanno tutti norma dispari. Analogamente si vede che nessuno di questi è multiplo di 3 (o –3). □

Nota Una trattazione alternativa dell'argomento di questa lezione è contenuta nell'articolo *A Principal Ideal Domain That is Not a Euclidean Domain*, di Oscar A. Cámpoli, pubblicato su *American Mathematical Monthly* **95** (1988), pagg. 868-871, ed accessibile all'indirizzo:
https://www.jstor.org/stable/2322908?seq=1#page_scan_tab_contents