Un dominio ad ideali principali, non euclideo

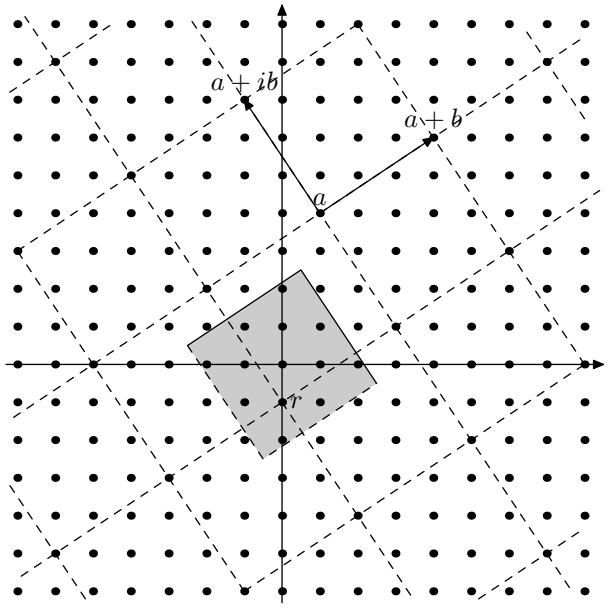
È ben noto che i domini euclidei sono dei particolari domini ad ideali principali ma non è facile trovare nei testi standard di algebra degli esempi di domini ad ideali principali che non siano anche euclidei, esempi che a volte si trovano sotto forma di esercizio in testi di teoria dei numeri (ad esempio sono due esercizi nel libro di Borevich e Shafarevich). Qui sotto è descritto l'esempio costituito dall'anello degli interi del corpo $\mathbb{Q}(\sqrt{-19})$, assieme a qualche richiamo ed esempio sugli anelli euclidei. Lo stesso esempio si può trovare come esercizio nella pagina web di Mark V. Sapir (`www.math.vanderbilt.edu/~msapir/283/rings4.pdf`).

Richiamo. [Anelli Euclidei] L'algoritmo di divisione euclidea è un buon strumento per studiare la struttura dell'anello $\mathbb{Z}$ degli interi razionali. Questa struttura è comune anche ad altri anelli. Ricordiamo quindi la seguente

Definizione. Un anello R si dice *euclideo* se ad ogni elemento $a \neq 0$ si può associare un intero $g(a) \geq 0$ (il *grado* di a) in modo che

(a) $g(ab) \geq g(a)$, qualunque siano $a \neq 0 \neq b$;
(b) dati $b \neq 0$ ed $a \in R$ esistono q ed r in R tali che $a = bq + r$, ove $r = 0$ oppure $g(r) < g(b)$.

Oltre all'anello degli interi razionali, in cui può essere presa come funzione grado il valore assoluto (o il suo quadrato), un altro esempio di anello euclideo è l'anello dei polinomi in una variabile, a coefficienti in un corpo C, ove la *funzione grado* di cui si parla nella definizione è proprio il grado del polinomio.



Come ulteriore esempio, vogliamo mostrare che l'anello $\mathbb{Z}[i]$ degli interi di Gauss è un anello euclideo. Gli *interi di Gauss* sono i numeri complessi del tipo $a_1 + ia_2$ con $a_1, a_2 \in \mathbb{Z}$ e la funzione grado è il quadrato della restrizione a $\mathbb{Z}[i]$ del valore assoluto complesso. La condizione (a) è ovviamente soddisfatta e dobbiamo quindi esibire un algoritmo di divisione con resto. Dati $a, b \in \mathbb{Z}[i]$, con $b \neq 0$, tutti i numeri del tipo $a - bx$, al variare di $x \in \mathbb{Z}[i]$, formano un reticolo quadrato, passante per a ed avente lato di lunghezza $|b|$. I punti z del reticolo con $|z|^2 < |b|^2$, sono al più quattro, ma uno solo tra questi è contenuto nell'insieme $D_b \cap \mathbb{Z}[i]$, ove D_b è l'insieme dei numeri complessi

$$D_b = \left\{ (x+iy)b \in \mathbb{C} \;\middle|\; x, y \in (-\tfrac{1}{2}, \tfrac{1}{2}] \right\}$$

dunque esistono e sono unici $r \in D_b$ e $q \in R$ tali che $a = bq + r$.

Si veda ad esempio il disegno a lato, ove $a = 1 + 4i$ e $b = 3 + 2i$ (quindi $q = 1 + i$ ed $r = -i$) e si sono uniti con linee tratteggiate tutti i punti del tipo $a + xb$ al variare di $x \in \mathbb{Z}[i]$.

I punti contenuti nella regione evidenziata in grigio (o eventualmente appartenenti al bordo non tratteggiato) sono l'insieme D_b e si osservi che questi punti sono dei rappresentanti degli elementi dell'anello delle classi resto modulo b, ovvero $\mathbb{Z}[i]/b\mathbb{Z}[i]$. In particolare, notiamo che in questo caso gli elementi di D_b sono esattamente $13 = |3 + 2i|^2$.

In un anello euclideo ogni ideale proprio è principale ed è generato da un qualunque suo elemento non nullo di grado minimo.

Vogliamo dimostrare che l'anello degli interi dell'estensione $\mathbb{Q}(\sqrt{-19})$ è un dominio ad ideali principali, ma non è un anello euclideo. Stiamo parlando dell'anello D formato dai numeri complessi del tipo $a + b\alpha$, ove $a, b \in \mathbb{Z}$ ed $\alpha = \frac{1+\sqrt{-19}}{2}$. È facile verificare che la restrizione a D del quadrato del valore assoluto complesso definisce una funzione (*norma*) $N : D \to \mathbb{Z}_{\geq 0}$, ove $N(a + b\alpha) = a^2 + ab + 5b^2$. Inoltre la restrizione a D della coniugazione complessa definisce un automorfismo di D e gli unici elementi invertibili di D sono ± 1.

Cominciamo con un'osservazione generale (attribuita a Dedekind ed Hasse) che stabilisce una condizione sufficiente affinché un dominio sia ad ideali principali.

Proposizione. *Sia R un dominio di integrità. Se esiste una funzione $N : R \to \mathbb{Z}_{\geq 0}$ tale che*
(a) $N(x) > 0$ per ogni $x \neq 0$;
(b) dati x, y, diversi da zero e con $N(x) > N(y)$, allora o y divide x, oppure esistono $s, t \in R$ tali che $0 < N(sx - ty) < N(y)$; allora R è un dominio ad ideali principali.

dim. Gli ideali banali sono chiaramente principali. Sia I un ideale non banale di R e consideriamo un elemento $y \neq 0$ di I su cui la funzione N assuma il valore minimo. Dato un qualunque altro elemento x di I, necessariamente y deve dividere x perché altrimenti l'elemento $sx - ty$ del punto (b) apparterrebbe ad I, contraddicendo il fatto che il valore assunto su y da N sia il minimo. Dunque $I = yR$. **CVD** □

Dimostriamo che la funzione norma, N, definita su D, soddisfa alle condizioni della Proposizione precedente e quindi che D è un dominio ad ideali principali.

La condizione (a) è soddisfatta, essendo $|ab| < a^2 + 5b^2$ per ogni coppia $(a, b) \neq (0, 0)$ in $\mathbb{Z}^2$. La verifica della condizione (b) richiede un ragionamento più articolato. Per prima cosa, osserviamo che, la funzione norma su D (e sul suo corpo dei quozienti $\mathbb{Q}(\sqrt{-19})$) è moltiplicativa e quindi $0 < N(sx - ty) < N(y)$ se, e solo se, $0 < N(s\frac{x}{y} - t) < 1$. Supponiamo ora di avere due elementi x, y di D, con $N(x) > N(y) > 0$, e che y non divida x. Allora $\dfrac{x}{y} = \dfrac{a + b\sqrt{-19}}{c}$ con a, b, c interi, relativamente primi, e $c > 1$. Siano p, q, r interi tali che $ap + bq + cr = 1$ e, tramite l'algoritmo euclideo (in $\mathbb{Z}$), sia $aq - 19bp = uc + v$ con u, v interi e $|v| \leq c/2$. Allora, posto $s = q + p\sqrt{-19}$ e $t = u - r\sqrt{-19}$, si ha

$$s\frac{x}{y} - t = \frac{a + b\sqrt{-19}}{c}(q + p\sqrt{-19}) - (u - r\sqrt{-19}) = \frac{(aq - 19bp - uc) + (ap + bq + cr)\sqrt{-19}}{c} = \frac{v + \sqrt{-19}}{c}$$

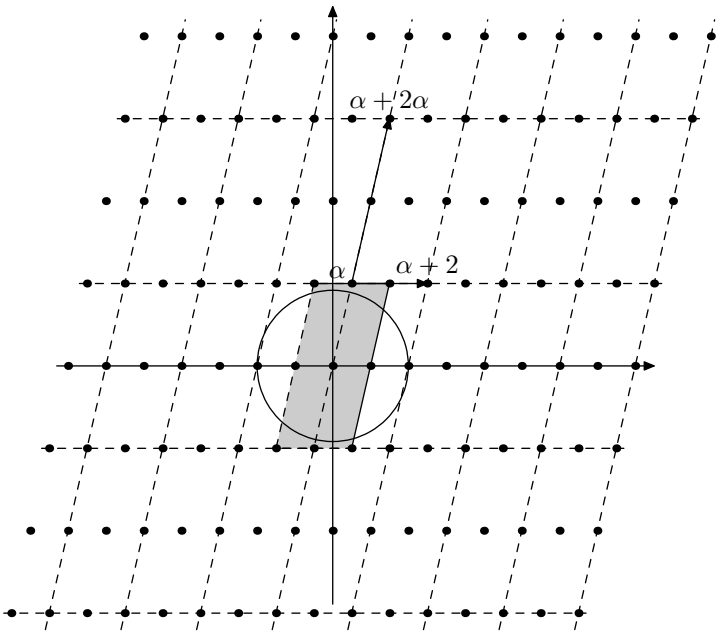
e la norma di questo numero è $\dfrac{v^2 + 19}{c^2} > 0$, che è minore di 1 se $c \geq 5$. Nei casi rimanenti ($c = 2, 3, 4$) bisogna dimostrare che si possono scegliere degli interi p, q, r tali che $ap + bq + cr = 0$ ed $aq - 19bp \notin c\mathbb{Z}$, dopo di che u, v, s e t sono definiti come sopra e la norma di $s\frac{x}{y} - t$ è compresa tra 0 ed 1. Passando all'anello quoziente $\mathbb{Z}/c\mathbb{Z}$, si tratta di dimostrare che il sistema $\begin{cases} ap + bq = 0 \\ -19bp + aq = d \end{cases}$, nelle incognite p e q, ha soluzione per un qualche $d \neq 0$. Se $c = 2$, possiamo supporre che a e b non siano congrui tra loro modulo 2, perché altrimenti $\frac{x}{y}$ apparterrebbe a D. Sotto tali ipotesi, il determinante della matrice dei coefficienti, $a^2 + 19b^2$, non è nullo e quindi il sistema ha soluzioni. Analogamente il determinante non è nullo per $c = 3$. Per $c = 4$, possiamo supporre che a e b non siano entrambi pari perché a, b e c non possono avere fattori comuni. Dunque, il determinante non si annulla se a non è congruo a $\pm b$ modulo 4. Supponiamo, ad esempio che $a \equiv b \equiv 1 \mod 4$, alora $\frac{x}{y} = \frac{\alpha}{2} + d$ per qualche $d \in D$ e quindi, posto $s = \bar{\alpha}$ e $t = \bar{\alpha}d + 2$, si ottiene $s\frac{x}{y} - t = \frac{1}{2}$ che è quanto volevamo. Nei casi rimanenti si ragiona in modo analogo.

Mettiamo in evidenza una proprietà degli anelli euclidei.

Proposizione. *Sia R un anello euclideo, allora esiste un elemento s, diverso da zero e non invertibile, con la proprietà che, per ogni elemento x di R esiste un elemento $z \in R^\times \cup \{0\}$, tale che s divida $x - z$.*

dim. Sia g la funzione grado del dominio R, e sia s un elemento di $R \setminus (R^\times \cup \{0\})$ di grado minimo. Dato un generico elemento x di R, applicando la divisione euclidea, si ha $x = sy + z$ con $z = 0$, oppure $g(z) < g(s)$, dunque, se z è diverso da zero, allora deve essere invertibile, per la minimalità del grado di s e quindi s è uno degli elementi cercati. **CVD** □

Si conclude osservando che non può esistere in D un elemento s del tipo descritto nella Proposizione precedente. Infatti, se s fosse un tale elemento, presi $x = 2$ ed $x = 3$, si avrebbe $s \in \{\pm 2, \pm 3\}$, perché 2 e 3 sono irriducibili in D, ma nessuna di queste possibilità è accettabile per $x = \alpha$, e quindi D non è un anello euclideo.



Da ultimo vogliamo osservare che si sarebbe potuto definire una "divisione con resto" in D in modo analogo a quanto fatto negli interi di Gauss. Ovvero, dati a e b in D, si sarebbero potuti considerare gli insiemi $S_a = \{\, a + bx \mid x \in D \,\}$ e $D_b = \left\{\, (x + y\alpha)b \;\middle|\; x, y \in (-\tfrac{1}{2}, \tfrac{1}{2}] \,\right\}$ e prendere come "resto della divisione" l'unico elemento dell'intersezione $S_a \cap D_b = \{r\}$; ma, a differenza del caso degli interi di Gauss, in D non abbiamo alcuna garanzia che il numero r così determinato abbia norma minore di $N(b)$.

Si veda ad esempio il disegno qui a fianco, in cui $a = \alpha$, $b = 2$. I punti di S_a sono all'incrocio di linee tratteggiate, mentre D_b è evidenziato in grigio e comprende la parte di bordo non tratteggiata. L'intersezione è costituita dal punto $r = \alpha$, che si trova al di fuori del cerchio dei numeri complessi di norma uguale alla norma di b.

Da questa osservazione potremmo concludere che la funzione N non può essere presa come "grado" in D, ma non sapremmo dire nulla sull'esistenza di una diversa funzione che renda D euclideo. Discende dall'ultima Proposizione e dalle successive considerazioni il fatto che non può esistere una funzione grado che renda D euclideo.