Un PID non Euclideo

17 marzo 2016

1 Introduzione

In una serie di esercizi determineremo, in modo esplicito, un esempio di PID che non è un anello euclideo. La dimostrazione che presentiamo è presa da una serie analoga di esercizi sviluppata da G. Bergman. Potete trovare altro materiale interessante nella sua pagina web, all'indirizzo `math.berkeley.edu/~gbergman`.

2 Esempio di PID non euclideo

Lo scopo di queste note è di dimostrare il seguente teorema.

Teorema 2.1. *Sia* $\alpha = \dfrac{1+\sqrt{-19}}{2} \in \mathbb{C}$ *e sia* $R = \mathbb{Z}[\alpha]$ *il sottoanello di* $\mathbb{C}$ *generato da* α*. Allora* R *è un PID, ma non è un anello euclideo.*

La dimostrazione del Teorema 2.1 sarà ottenuta tramite una serie di esercizi.

Definizione 2.2. L'*anello degli interi algebrici* di un campo K, denotato con $\mathcal{O}_K$ è l'anello formato dagli elementi $x \in K$ tali che x è radice di un polinomio *monico* a coefficienti interi.

Sia K un *campo di numeri* e cioè un sottocampo del campo dei numeri complessi $\mathbb{C}$, che contiene $\mathbb{Q}$, e tale che ogni suo elemento sia algebrico su $\mathbb{Q}$. Allora ogni elemento di K è radice di un polinomio a coefficienti razionali e, cancellando i denominatori, possiamo supporre che il polinomio sia a coefficienti interi.

Corollario 2.3. *L'anello degli interi di* K *è un UFD.*

Dimostrazione. Ogni PID è un UFD.[1] □

Esercizio 2.4. Dimostrare che l'insieme $\mathcal{O}_K$ è un anello.

Suggerimento: Non è immediato dalla definizione che l'insieme $\mathcal{O}_K$ sia chiuso rispetto alla somma e al prodotto. Per una dimostrazione, vedere [AM], Capitolo 5 fino al Corollario 5.3.

Esercizio 2.5. L'anello R è di *interi algebrici*.

[1] Questa proprietà non è quasi mai vera per gli anelli di interi di campi di numeri e anzi un problema importante in Teoria dei Numeri è determinare di quanto la fattorizzazione unica fallisca in un campo di numeri.

Esercizio 2.6. Dimostrare che l'anello $R = \mathbb{Z}[\alpha]$ è l'anello degli interi del campo $K = \mathbb{Q}(\sqrt{-19})$.

Questo esercizio mostra che l'anello $R = \mathbb{Z}[\alpha]$ **non è un esempio isolato**, ma appartiene ad una classe importante di anelli.

2.1 R non è euclideo

Notazione 2.7. *Con la notazione $\bar{x}$ indichiamo il coniugato del numero complesso x.*

Esercizio 2.8. Verificare che:

1. $\alpha^2 - \alpha + 5 = 0$ (questo dimostra che α è un intero algebrico);
2. $R = \{m + n\alpha \mid m, n \in \mathbb{Z}\} = \{m + n\bar{\alpha} \mid m, n \in \mathbb{Z}\}$;
3. $x \mapsto |x|^2 = x \cdot \bar{x}$ è una funzione (definita su R) a valori interi, non negativi, e rispetta il prodotto.

Esercizio 2.9. Determinare l'estremo inferiore dell'insieme dei valori assoluti della parte immaginaria di tutti gli elementi di R non reali (cioè con parte immaginaria non nulla).

Esercizio 2.10. Dimostrare che se $x \in R$ è invertibile allora $|x|^2 = 1$ e che gli unici elementi invertibili di R sono 1 e -1.

Supponiamo ora che l'anello R sia euclideo, e sia δ la valutazione euclidea. Fra tutti gli elementi non invertibili di $R \setminus \{0\}$ scegliamo t in modo da minimizzare $\delta(t)$.

Esercizio 2.11. Dimostrare che $R/(t)$ è formato dalle immagini di 0 e dalle immagini degli elementi invertibili di R, e quindi è un anello di cardinalità minore o uguale a 3.

Esercizio 2.12. Dimostrare che l'equazione $x^2 - x + 5 = 0$ non ha soluzioni in nessun anello di cardinalità minore o uguale a 3. **Dedurre che R non è un anello euclideo**.

Suggerimento: Ricordiamo che abbiamo appena dimostrato che $\alpha\overline{\alpha} = 5$ e che $\alpha^2 = \alpha - 5$. Inoltre sappiamo che le unità di R sono solo ± 1, mentre 2 e 3 sono irriducibili in R.

Ora con queste ipotesi dimostriamo per assurdo che R non è Euclideo.

Supponiamo che esista una funzione d euclidea per R e sia $m \in R$ che minimizza questa funzione con $m \neq 0$ e m non un'unità.

Dividiamo 2 per m:

$$2 = mq + r, \text{ con } d(r) < d(m) \text{ o } r = 0,$$

allora $r = 0, 1, -1$. Se $r = 0$ allora $m \mid 2$, perciò $m = \pm 2$ poiché 2 è irriducibile e m non è un'unità. Analogamente se $r = -1$ allora $m = \pm 3$. Il caso $r = 1$ non può succedere altrimenti $m \mid 1$ e m sarebbe un'unità.

Ora dividiamo α per m:

$$\alpha = mq' + r', \text{ con } d(r') < d(m) \text{ o } r' = 0.$$

Ancora $r' = 0, 1, -1$, quindi uno tra $\alpha, \alpha+1, \alpha-1$ deve essere divisibile per m. Ma abbiamo detto prima che $m = \pm 2$ o $m = \pm 3$ ed è facile vedere che nessuno di questi quozienti è in R.

Questa contraddizione mostra che R non è Euclideo per nessuna funzione Euclidea.

2.2 R è un PID

Sia I un ideale non nullo di R, e sia $x \in I$ un elemento non nullo di valore assoluto minimo, cioè che minimizza l'intero $x \cdot \bar{x}$. Dimostreremo che $I = (x)$ e quindi che I è principale. Stiamo quindi usando la funzione $x \mapsto x \cdot \bar{x}$ al posto della valutazione euclidea.

Il numero complesso x ha inverso $x^{-1} \in \mathbb{C}$ e poniamo

$$J = x^{-1}I = \{y \in \mathbb{C} \mid y = x^{-1}b,\ b \in I\} = \{y \in \mathbb{C} \mid yx \in I\}$$

Definizione 2.13. Sia A un anello. Un *A-modulo sinistro* M è un gruppo abeliano $(M, +)$ su cui è definita un'operazione $A \times M \to M$ tale che

1. $a(v + w) = av + aw$ per ogni $a \in A$, $v, w \in M$;
2. $(a + b)v = av + bv$ per ogni $a, b \in A$, $v \in M$;
3. $(ab)v = a(bv)$ per ogni $a, b \in A$, $v \in M$.

Un *A-modulo destro* M è un gruppo abeliano $(M, +)$ su cui è definita un'operazione $M \times A \to M$ tale che

1. $(v + w)a = va + wa$ per ogni $a \in A$, $v, w \in M$;
2. $v(a + b) = va + vb$ per ogni $a, b \in A$, $v \in M$;
3. $v(ab) = (va)b$ per ogni $a, b \in A$, $v \in M$.

Se l'anello A è commutativo allora le nozioni di A-modulo destro e A-modulo sinistro coincidono. In tal caso parleremo solo di A-modulo.

Esercizio 2.14. Dimostrare che:

1. $R \subseteq J$,
2. J è un R-modulo,
3. se $a \in J$, $a \neq 0$ allora $|a| \geq 1$.

Da queste proprietà dedurremo che $J = R$, e quindi $I = (x)$.

Esercizio 2.15. Sia $a \in J$. Se esiste $b \in R$ per cui $|a - b| < 1$ allora $a \in R$.

Quindi gli elementi di $J \setminus R$ devono essere "lontani" dagli elementi di R. La versione quantitativa di questo enunciato (versione che si deduce dall'esercizio precedente) è:

Esercizio 2.16. Se $a = m + ni \in J \setminus R$, allora

$$\left| n - k\frac{\sqrt{19}}{2} \right| > \frac{\sqrt{3}}{2}, \qquad \forall k \in \mathbb{Z}$$

Osservazione: n è la parte immaginaria di a, e non è necessariamente un numero intero. Disegnare con cura, nel piano complesso, gli elementi di R, e le zone dove, secondo l'Esercizio 2.15, gli elementi di $J \setminus R$ non possono stare. Usando il disegno come ispirazione, trovare una dimostrazione della diseguaglianza[2].

Esercizio 2.17. Dimostrare che, se $J \setminus R$ è non vuoto, deve contenere un elemento $y = m + ni$ tale che

$$-\frac{1}{2} < m \leq \frac{1}{2}, \quad \text{e} \quad \frac{\sqrt{3}}{2} \leq n \leq \frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}.$$

Esercizio 2.18. Dimostrare che, se y è l'elemento trovato nell'esercizio precedente, il numero $2y$ ha parte immaginaria troppo vicina a $\sqrt{19}/2$ per poter appartenere a $J \setminus R$. Concludere che $y = \alpha/2$ oppure $-\bar{\alpha}/2$ e quindi $\alpha \cdot \bar{\alpha}/2 \in J$.

Esercizio 2.19. Calcolare $\alpha \cdot \bar{\alpha}/2$ e ottenere una contraddizione. Concludere che $J = R$ e quindi I è un ideale principale, e perciò R **è un PID**.

Riferimenti bibliografici

[AM] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison–Wesley, 1969

[2] `www.math.unipd.it/~candiler/didafiles/pid.pdf`