Gli anelli degli interi algebrici in campi di numeri sono noetheriani

GIOVANNI CUTOLO

1.

1.1. **Richiami e discriminanti.** Fissiamo alcune notazioni. Indichiamo con $\overline{\mathbb{Z}}$ la chiusura intera di $\mathbb{Z}$ in $\mathbb{C}$; ovviamente $\overline{\mathbb{Z}}$ è contenuto nella chiusura agebrica $\overline{\mathbb{Q}}$ di $\mathbb{Q}$ in $\mathbb{C}$. L'anello $\overline{\mathbb{Z}}$ è noto come l'*anello degli interi algebrici*. Sia poi K un campo di numeri, vale a dire: una estensione di grado finito n del campo $\mathbb{Q}$. Come sappiamo dai corsi elementari di teoria dei campi, K è necessariamente un'estensione algebrica di $\mathbb{Q}$ ed è quindi immergibile in $\overline{\mathbb{Q}}$; senza perdere in generalità possiamo dunque assumere che K sia un sottocampo di $\overline{\mathbb{Q}}$, dunque di $\mathbb{C}$. Poniamo $Z_K := K \cap \overline{\mathbb{Z}}$, questo è l'*anello degli interi algebrici di* K. Vogliamo qui provare che questo anello è noetheriano. Aggiungendo l'informazione che questo anello è integralmente chiuso ed ha dimensione 1, si potrà concludere che Z_K è un anello di Dedekind.

Un importante risultato (sulle estensioni finite separabili di campi) garantisce che esistono esattamente n omomorfismi di campi da K a $\overline{\mathbb{Q}}$. Per omomorfismo di campi intendiamo un omomorfismo di anelli unitari tra due campi; dunque gli omomorfismi di campi sono certamente non nulli e di conseguenza sono tutti monomorfismi. Il sottocampo di $\overline{\mathbb{Q}}$ generato dalle immagini di questi monomorfismi è la *chiusura normale* di K (rispetto a $\mathbb{Q}$), che indichiamo con N. Chiaramente (sempre in conseguenza di risultati elementari della teoria dei campi) anche N ha grado finito su $\mathbb{Q}$. Abbiamo così esattamente n omomorfismi (di campi) da K a N, indichiamoli come σ_1, $\sigma_2, \ldots, \sigma_n$ e chiamiamo S l'insieme da essi costituito. Notiamo esplicitamente che ciascuno dei σ_i fissa (cioè manda in se stesso) ogni elemento di $\mathbb{Q}$. Dunque i σ_i sono anche monomorfismi di estensioni di campi (dall'estensione $K/\mathbb{Q}$ all'estensione $N/\mathbb{Q}$), cioè monomorfismi di $\mathbb{Q}$-algebre da K a N.

Ora, N è quella che si chiama un'estensione di Galois di $\mathbb{Q}$. Vediamo cosa significhi ciò, limitandoci allo stretto necessario per i nostri scopi. Come già affermato in riferimento a K, esistono esattamente $m := [N : \mathbb{Q}] = \dim_{\mathbb{Q}} N$ omomorfismi di campi da N a $\overline{\mathbb{Q}}$. A differenza di quanto accade per K, però, questi omomorfismi (che, ricordiamo, sono iniettivi) hanno tutti per immagine N. Abbiamo così esattamente m automorfismi del campo N. Indichiamo con G il gruppo da essi costituito: $G = \operatorname{Aut} N$ (questo è quello che si chiama il gruppo di Galois dell'estensione $N/\mathbb{Q}$). Uno dei risultati fondamentali della teoria di Galois assicura che $\mathbb{Q}$ è precisamente il campo degli elementi fissati da G, cioè che, per ogni $a \in N$, si ha $a \in \mathbb{Q} \iff (\forall g \in G)(a^g = a)$.

Esiste uno stretto legame tra gli omomorfismi $\sigma_i \colon K \to N$ e gli elementi di G. Infatti, per il cosiddetto teorema di prolungamento, ciascuno dei σ_i è una restrizione di un automorfismo di N. Detto diversamente, l'applicazione $G \to S$ che ad ogni $g \in G$ associa la restrizione $g_{\restriction K}$ di g a K è suriettiva.

Sia ora $\underline{b} = (b_1, b_2, \ldots, b_n)$ una $\mathbb{Q}$-base (ordinata) di K, cioè una base di K visto come $\mathbb{Q}$-spazio vettoriale. Ad essa associamo la matrice (a termini in N)

$$D_{\underline{b}} := (b_j^{\sigma_i}) = \begin{pmatrix} b_1^{\sigma_1} & b_2^{\sigma_1} & \ldots & b_n^{\sigma_1} \\ b_1^{\sigma_2} & b_2^{\sigma_2} & \ldots & b_n^{\sigma_2} \\ \vdots & \vdots & \ldots & \vdots \\ b_1^{\sigma_n} & b_2^{\sigma_n} & \ldots & b_n^{\sigma_n} \end{pmatrix},$$

le cui righe sono le immagini della base $\underline{b}$ mediante gli omomorfismi σ_i. Per ogni $g \in G$, possiamo considerare la trasformata di $D_{\underline{b}}$ mediante g, cioè la matrice $D_{\underline{b}}^g := ((b_j^{\sigma_i})^g)$. Vogliamo provare che $D_{\underline{b}}^g$ si ottiene da $D_{\underline{b}}$ con una permutazione delle righe. Per ogni $i \in \{1, 2, \ldots, n\}$, sia h uno degli elementi di G tale che $\sigma_i = h_{\restriction K}$. Ovviamente $(hg)_{\restriction K} \in S$; chiamiamo i_g l'unico elemento di $\{1, 2, \ldots, n\}$ tale che $(hg)_{\restriction K} = \sigma_{i_g}$. Per ogni $b \in K$, abbiamo $b^{\sigma_{i_g}} = b^{hg} = (b^{\sigma_i})^g$. Questo mostra, tra l'altro, che la definizione di i_g non dipende dalla scelta di h tra gli elementi di N la cui restrizione a K sia σ_i.

Abbiamo così definito un'applicazione $\alpha_g\colon i \mapsto i_g$ di $\{1,2,\dots,n\}$ in sé. Questa applicazione è biettiva: come infatti si verifica subito, la sua inversa è l'applicazione $\alpha_{g^{-1}}$ costruita a partire da g^{-1} piuttosto che g. Dunque, $\alpha_g \in \mathbb{S}_n$. Torniamo alla matrice $D^g_{\underline{b}}$. Per ogni $i \in \{1,2,\dots,n\}$, la sua i-esima riga è $((b_1^{\sigma_i})^g, (b_2^{\sigma_i})^g, \dots, (b_n^{\sigma_i})^g)$, ovvero $(b_1^{\sigma_{i_g}}, b_2^{\sigma_{i_g}}, \dots, b_n^{\sigma_{i_g}})$, la riga i_g-esima di $D_{\underline{b}}$. Dunque, effettivamente, $D^g_{\underline{b}}$ si ottiene da $D_{\underline{b}}$ permutandone le righe, precisamente tramite la permutazione α_g^{-1}. Di conseguenza, detto d il determinante $|D_{\underline{b}}|$ (che, ricordiamo, appartiene a N), abbiamo $d^g = |D^g_{\underline{b}}| \in \{d, -d\}$. Ulteriore conseguenza è che d^2 è fissato da ogni elemento di G. Per quanto richiamato prima, questo significa che $d^2 \in \mathbb{Q}$. Questo numero razionale d^2 ha un ruolo molto importante nella teoria algebrica dei numeri; esso prende il nome di *discriminante* della base $\underline{b}$, lo si indica con $\Delta(\underline{b})$.

Abbiamo dimostrato che il discriminante di una base è un numero razionale; dimostreremo ora che questo numero è diverso da zero. Per farlo, richiamiamo un altro risultato fondamentale della teoria dei campi, noto come Lemma di Dedekind: se E ed F sono campi arbitrari, ogni insieme di omomorfismi di campi da E ad F è linearmente indipendente su F. Chiariamo questo enunciato. Stiamo considerando la consueta struttura di anello sull'insieme F^E delle applicazioni da E a F (le operazioni di addizione e moltiplicazione sono le corrispondenti operazioni puntuali) in cui immergiamo F tramite le applicazioni costanti (cioè identifichiamo ciascun elemento $a \in F$ con l'applicazione costante a da E a F). In questo modo F^E si struttura come F-algebra, quindi in particolare come F-spazio vettoriale. Dunque, l'addizione interna in questo spazio vettoriale è l'operazione di addizione puntuale e il prodotto esterno è definito da $\sigma a\colon e \in E \mapsto e^\sigma a \in F$ per ogni $\sigma \in F^E$ e $a \in F$. Bene, se A è un qualsiasi insieme di omomorfismi (di campi) da E a F, allora A è un sottoinsieme di questo F-spazio vettoriale F^E; il Lemma di Dedekind assicura, appunto, che questo sottoinsieme A è linearmente indipendente.

Il Lemma di Dedekind permette di provare che le righe della matrice $D_{\underline{b}}$ sono linearmente indipendenti tra loro. Siano infatti $\alpha_1, \alpha_2, \dots, \alpha_n \in N$ tali che, per ogni $j \in \{1,2,\dots,n\}$, si abbia $0 = \sum_{i=1}^n b_j^{\sigma_i}\alpha_i = b_j^{\sum_{i=1}^n \sigma_i\alpha_i}$. Ora, $\sum_{i=1}^n \sigma_i\alpha_i$ (che non è, in generale un omomorfismo di campi) è sicuramente un omomorfismo di $\mathbb{Q}$-spazi vettoriali da K a N; il fatto che si annulli su tutti gli elementi di una $\mathbb{Q}$-base di K garantisce che è l'endomorfismo nullo. Dunque $\sum_{i=1}^n \sigma_i\alpha_i = 0$. Ma, per il Lemma di Dedekind, S è linearmente dipendente su N, quindi $\alpha_i = 0$ per ogni $i \in \{1,2,\dots,n\}$. Abbiamo così dimostrato l'indipendenza tra le righe di $D_{\underline{b}}$, quindi $D_{\underline{b}}$ non è degenere, ovvero $|D_{\underline{b}}| \neq 0$. Concludiamo così:

Lemma 1.1.1. *Il discriminante di una qualsiasi $\mathbb{Q}$-base di un campo di numeri è un numero razionale diverso da 0.*

1.2. **Noetherianità.** Se ora $\underline{b}$ è una $\mathbb{Q}$-base di K costituita da interi algebrici (e ricordiamo che esistono in K basi siffatte), il discriminante $\Delta(\underline{b})$ è un intero algebrico (osserviamo infatti che ciascuno dei σ_i manda interi algebrici in interi algebrici), quindi $0 \neq \Delta(\underline{b}) \in \mathbb{Z}$. Tra le $\mathbb{Q}$-basi di K costituite da interi algebrici, possiamo allora selezionarne una, chiamiamola ancora $\underline{b} = (b_1, b_2, \dots, b_n)$, tale che $|\Delta(\underline{b})|$ abbia il minimo valore possibile. Vogliamo provare che allora Z_K è il sottogruppo di $(K,+)$ generato da $\{b_1, b_2, \dots, b_n\}$. Supponiamo che ciò non accada, e sia $c \in Z_K \smallsetminus \langle b_1, b_2, \dots, b_n\rangle$. Allora (ricordiamo che $\underline{b}$ è una $\mathbb{Q}$-base di K) esistono, univocamente determinati, $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{Q}$ tali che $c = \sum_{i=1}^n \lambda_i b_i$, ma almeno uno dei λ_i non è in $\mathbb{Z}$. A meno di riordinare la base $\underline{b}$, se necessario, possiamo assumere $\lambda_1 \notin \mathbb{Z}$. Esiste un intero ℓ tale che $\ell < \lambda_1 < \ell + 1$; a meno di sostituire c con $c - \ell b_1$ $(\in Z_K)$, possiamo ulteriormente assumere $\ell = 0$, cioè $0 < \lambda_1 < 1$. Ora, anche $\underline{b}' := (c, b_2, \dots, b_n)$ è una $\mathbb{Q}$-base di K costituita da interi algebrici, ed abbiamo

$$D_{\underline{b}'} = D_{\underline{b}} \left(\begin{array}{c|ccc} \lambda_1 & 0 & \cdots & 0 \\ \hline \lambda_2 & & & \\ \vdots & & I_{n-1} & \\ \lambda_n & & & \end{array}\right)$$

(dove naturalmente I_{n-1} è la matrice identica di rango $n-1$). Allora $|D_{\underline{b}'}| = |D_{\underline{b}}|\lambda_1$ e quindi $|\Delta(\underline{b}')| = |\Delta(\underline{b})|\lambda_1^2 < |\Delta(\underline{b})|$, in contraddizione con la scelta di $\underline{b}$. Abbiamo così provato che $(Z_K,+) = \langle b_1, b_2, \dots, b_n\rangle$ è un gruppo abeliano finitamente generato (in effetti: un gruppo abeliano libero di rango n), quindi a condizione massimale. Da ciò, ovviamente, segue che Z_K è un anello noetheriano. □