Calcolo di una base intera per un campo di numeri

Carlo Sircana

21 novembre 2015

1 Introduzione

In questo seminario, illustreremo un algoritmo per il calcolo di una base intera di un anello di interi. Più precisamente, considereremo un campo K che sia un'estensione finita di $\mathbb{Q}$; un tale campo viene solitamente detto campo di numeri. In analogia con la nozione di elemento algebrico, si considerano gli elementi di K interi su $\mathbb{Z}$, ossia elementi che sono radici di un polinomio monico a coefficienti in $\mathbb{Z}$. Tale insieme eredita in maniera naturale una struttura di anello, che indicheremo con $\mathcal{O}_K$; inoltre è un dominio, in quanto sottoanello di un campo, e per la richiesta finitezza di K su $\mathbb{Q}$ è anche noetheriano (per il teorema della base di Hilbert). Dato che per definizione $\mathcal{O}_K$ è intero su $\mathbb{Z}$, ha dimensione di Krull 1 ed è integralmente chiuso. Di conseguenza, è un dominio di Dedekind; questi sono una naturale generalizzazione degli UFD, in quanto sono caratterizzati dal seguente:

Teorema 1.1. Sia A un dominio. A è un dominio di Dedekind se e solo se ogni ideale non nullo di A si scrive in modo unico come prodotto finito di ideali primi.

Siamo più interessati a studiare la natura di $\mathbb{Z}$-modulo di $\mathcal{O}_K$. Vale infatti che $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo finito e, dato che $\mathbb{Z}$ è un PID, il seguente

Teorema 1.2. Sia K un campo di numeri e sia $n = [K : \mathbb{Q}]$. Allora $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo libero di rango n.

Una base intera di $\mathcal{O}_K$ è una base di $\mathcal{O}_K$ come $\mathbb{Z}$-modulo e scopo di questo seminario è trovare un metodo per il calcolo di un tale insieme di generatori. La dimostrazione classica del teorema non fornisce infatti un metodo esplicito per il calcolo di una base intera, ma si limita a individuare due moduli liberi di rango n M, N tali che $M \subseteq \mathcal{O}_K \subseteq N$.

Esempio. Consideriamo $K = \mathbb{Q}(\sqrt{5})$. Chiaramente, $\mathcal{O}_K \supseteq \mathbb{Z}[\sqrt{5}]$; in realtà, anche l'elemento

$$\alpha = \frac{1+\sqrt{5}}{2}$$

è intero su $\mathbb{Z}$, in quanto il suo polinomio minimo è $\mu_\alpha(t) = t^2 - t - 1$. Infatti, si può dimostrare che

$$\mathcal{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big]$$

2 Discriminante

Innanzitutto, è necessario trovare un criterio per determinare quando degli elementi di $\mathcal{O}_K$ formino una base intera. Per questo, è utile studiare un invariante numerico: il discriminante.

Definizione 2.1. Sia K un campo di numeri di grado n su $\mathbb{Q}$ e consideriamo le immersioni di K in $\mathbb{C}$ $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$. Dati $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, definiamo il discriminante di $\alpha_1, \ldots, \alpha_n$ come

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j)_{i,j})^2$$

Una definizione equivalente è la seguente: il discriminante è il determinante della matrice delle tracce dei prodotti degli elementi

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det((\operatorname{Tr}(\alpha_i \alpha_j))_{i,j})$$

Osservazione 2.2. Chiaramente, dato che le immersioni sono omomorfismi, il discriminante è non nullo se e solo se gli elementi α_i sono linearmente indipendenti su $\mathbb{Q}$; inoltre, dalla caratterizzazione della matrice delle tracce, il discriminante di elementi interi appartiene a $\mathbb{Z}$.

Per lo studio di una base intera, è interessante capire come varia il discriminante al variare di una base di K come $\mathbb{Q}$-spazio vettoriale. Siano $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ due basi di K come $\mathbb{Q}$-spazi vettoriali. Possiamo allora esprimere ogni α_i come combinazione dei β_j a coefficienti in $\mathbb{Q}$:

$$\alpha_i = \sum_{j=1}^{n} m_{ij} \beta_j$$

Dato che le immersioni σ_i sono omomorfismi, detta $M = (m_{ij})$ la matrice dei coefficienti, otteniamo

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det M^2 \operatorname{disc}(\beta_1, \ldots, \beta_n)$$

In particolare, se $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ sono basi intere, hanno lo stesso discriminante in quanto le matrici invertibili a coefficienti interi hanno determinante ± 1. Dunque

Definizione 2.3. Il discriminante di K $\operatorname{disc}(K)$ è il discriminante di una qualsiasi base intera di $\mathcal{O}_K$.

In particolare, abbiamo un utile criterio per stabilire se un'insieme di elementi formi una base intera:

Proposizione 2.4. Sia K un campo di numeri e siano $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ elementi interi. Allora $\alpha_1, \ldots, \alpha_n$ è una base intera di $\mathcal{O}_K$ se e solo se $\operatorname{disc}(K) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

Osservazione 2.5. Notiamo che la formula del cambio di base può essere raffinata. Sia M un sottomodulo libero di $\mathcal{O}_K$ di rango n; allora

$$\operatorname{disc}(M) = \left| \mathcal{O}_K / M \right| \operatorname{disc}(K)$$

dove con $\operatorname{disc}(M)$ abbiamo indicato il discriminante di una qualsiasi base di M.

Per il calcolo del discriminante si usa raramente la definizione, in quanto richiede il calcolo di un determinante e il calcolo di tracce di elementi. La seguente proposizione fornisce un metodo alternativo e più facile:

Proposizione 2.6. Sia $K = \mathbb{Q}(\alpha)$, dove $\alpha \in \mathcal{O}_K$ è un elemento intero su $\mathbb{Z}$ di grado n. Sia $\mu_\alpha(x) \in \mathbb{Z}[x]$ il suo polinomio minimo. Allora

$$\operatorname{disc}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = N_{K/\mathbb{Q}}(\mu'_\alpha(\alpha)) = \operatorname{disc}(\mu_\alpha)$$

Esempio. Le ultime due proposizioni permettono di dimostrare che, nell'esempio 1, l'insieme $\{1, \alpha\}$ forma effettivamente una base intera. Infatti

$$\operatorname{disc}(\alpha) = N_{K/\mathbb{Q}}(\mu'_\alpha(\alpha)) = N_{K/\mathbb{Q}}(\sqrt{5}) = -5$$

e dunque, dato che α è intero e che 5 è libero da quadrati, $1, \alpha$ è una base intera.

3 La forma normale di Hermite

Definizione 3.1. Sia M una matrice $n \times m$ a coefficienti in $\mathbb{Z}$. Diciamo che M è in forma normale di Hermite se

- Le prime r colonne sono nulle, $r \leq m$
- Esiste $f\colon \{r+1, \dots, m\} \to \{1, \dots, m\}$ strettamente crescente tale che $m_{f(i),i} > 0$, $m_{i,j} = 0$ se $i > f(j)$ e $0 \leq m_{i,j} \leq m_{f(j),j}$ se $i < f(j)$.

$$\begin{pmatrix} 0 & 0 & \dots & 0 & * & * & \dots & * \\ 0 & 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & \dots & * \end{pmatrix}$$

Chiaramente la forma di Hermite esiste e la dimostrazione è un sottoprodotto dell'esistenza della forma normale di Smith. La forma normale di Hermite è però molto meno costosa in termini computazionali; inoltre rende facilmente risolubili i sistemi lineari e in più è unica, dato che abbiamo imposto la positività degli elementi non nulli. Riportiamo comunque lo pseudocodice dell'algoritmo per il calcolo della forma normale. Supponiamo quindi di avere in input una matrice M $m \times n$ a coefficienti interi. Indicheremo con M_i le colonne di M.

1. Inizializzare $i = m$, $j = n$ e $l = 1$ se $m \leq n$, altrimenti $l = m - n + 1$
2. Se $m_{ij} = 0$ per $j < k$ e $m_{ik} < 0$, allora $M_i = -M_i$ e andare a 6.
3. Scegliere l'elemento m_{ij} con $j \leq k$ di valore assoluto minimo. Detto m_{ij_0} tale elemento, scambiare M_{j_0} e M_k.
4. Se $m_{ik} < 0$, scambiare M_k con $-M_k$.
5. Per $j = 1, \dots, k-1$, porre $s_j = \lfloor m_{ij}/m_{ik} \rfloor$ e sostituire $M_j = M_j - s_j M_k$. Tornare a 2.

6. Se $m_{ik} = 0$, porre $k = k + 1$ e andare al passo 7. Altrimenti, porre $t_j = \lfloor m_{ij}/m_{ik} \rfloor$ e sostituire $M_j = M_j - t_j M_k$ per $k > j$.

7. Se $i = l$, terminare l'algoritmo. Altrimenti, porre $i = i - 1$ e $k = k - 1$ e andare a 6.

Notiamo che l'algoritmo termina perché il valore assoluto degli elementi scelti a ogni iterazione al passo 3 è decrescente. Inoltre la matrice in output è per definizione in forma normale di Hermite e ogni operazione coincide con la moltiplicazione a sinistra per una matrice invertibile e dunque l'algoritmo è corretto. Un'utile applicazione della forma normale di Hermite è che permette di trovare in maniera elementare il nucleo dell'applicazione lineare indotta dalla matrice. Infatti

Proposizione 3.2. Sia A una matrice $m \times n$ a coefficienti interi, sia $B = AU$ la sua forma normale di Hermite. Allora il nucleo di A ha come base le prime r colonne di U, dove r è il numero di colonne nulle di B.

Dimostrazione. Un contenimento è ovvio. Sia allora $x \in \mathrm{Ker}(A)$. Dunque $AUx = 0$. Detto $y = Ux$, $Ay = 0$ e questo accade se e solo se le ultime $n - r$ conponenti di y sono nulle, da cui la tesi. □

4 Il teorema di Pohst-Zassenhaus e il criterio di Dedekind

Per procedere al calcolo di una base intera, partiremo quindi da un elemento primitivo α che sia anche intero su $\mathbb{Z}$ e modificheremo la $\mathbb{Q}$-base di K data dalle sue potenze per ottenere quanto voluto. Nei vari passi dell'algoritmo otterremo quindi diversi anelli interi su $\mathbb{Z}$, sottomoduli di $\mathcal{O}_K$ di rango n su $\mathbb{Z}$.

Definizione 4.1. Sia K un campo di numeri di grado n su $\mathbb{Q}$. Un ordine è un sottoanello di K che ha rango n come modulo su $\mathbb{Z}$.

Dalla definizione, è chiaro allora che l'anello degli interi $\mathcal{O}_K$ non sia altro che l'ordine massimo. L'idea è allora quella di trovare ordini sempre più grandi fino ad ottenere $\mathcal{O}_K$. Il primo problema è però quello di capire quando si è arrivati a una base intera. La risposta ci viene data dal teorema di Pohst-Zassenhaus, che fornisce un metodo per capire quali fattori del discriminante dell'ordine intermedio siano sovrabbondanti.

Definizione 4.2. Sia $\mathcal{O}$ un ordine di K e sia $p \in \mathbb{Z}$ un primo. Diciamo che $\mathcal{O}$ è p-massimale se $p \nmid [\mathcal{O}_K : \mathcal{O}]$.
Definiamo il p-radicale $I_p \subseteq \mathcal{O}$ come il radicale dell'estensione $p\mathcal{O}$ di p.

Il p-radicale è facilmente caratterizzabile:

Proposizione 4.3. Sia $\mathcal{O}$ un ordine di K. I_p coincide con il prodotto di tutti i primi di $\mathcal{O}$ che contengono $p\mathcal{O} \subseteq \mathcal{O}$, che sono in numero finito.

Dimostrazione. Notiamo che, dato che le estensioni intere preservano la dimensione di Krull, si ha $\dim(X) = 1$. Di conseguenza, due primi non nulli distinti sono comassimali e per il teorema cinese del resto

$$I_p = \bigcap_{\substack{P \in \mathrm{Spec}(\mathcal{O}) \\ P \supseteq p\mathcal{O}}} P = \prod_{\substack{P \in \mathrm{Spec}(\mathcal{O}) \\ P \supseteq p\mathcal{O}}} P$$

Basta allora mostrare che questi primi sono in numero finito. Per questo, basta utilizzare la fattorizzazione unica nei domini di Dedekind e notare che i primi dell'intersezione devono coincidere con la contrazione dei primi Q_i sopra p in $\mathcal{O}_K$, dato che $\mathcal{O}_K$ è intero su $\mathcal{O}$. □

Teorema 4.4 (Pohst-Zassenhaus)**.** Consideriamo un campo di numeri K di grado n su $\mathbb{Q}$. Sia $\mathcal{O}$ un ordine di K e sia $p \in \mathbb{Z}$ un primo. Sia

$$\mathcal{O}' = \{x \in K \mid xI_p \subseteq I_p\}$$

Vale una e una sola delle seguenti:

- $\mathcal{O} = \mathcal{O}'$ e $\mathcal{O}$ è p-massimale
- $p \mid [\mathcal{O}' : \mathcal{O}] \mid p^n$

Dimostrazione. Notiamo intanto che $\mathcal{O}'$ è un anello contenente $\mathcal{O}$ dato che I_p è un ideale. Inoltre, dato che $p \in I_p$, per ogni $x \in \mathcal{O}'$ si ha $xp \in I_p$ e dunque i contenimenti

$$\mathcal{O} \subseteq \mathcal{O}' \subseteq \frac{1}{p}\mathcal{O}$$

Di conseguenza $\mathcal{O}'$ è un modulo libero di rango n su $\mathbb{Z}$. Inoltre, ogni elemento del quoziente $\mathcal{O}'/\mathcal{O}$ ha ordine al più p e dunque $[\mathcal{O}' : \mathcal{O}] \mid p^n$. Rimane allora da dimostrare solo che se $\mathcal{O} = \mathcal{O}'$ allora $\mathcal{O}$ è p-massimale. Consideriamo l'insieme

$$\mathcal{O}_p = \{x \in \mathcal{O}_K \mid \exists j \geq 1 \; p^j x \in \mathcal{O}\}$$

Chiaramente $\mathcal{O} \subseteq \mathcal{O}_p$ e $\mathcal{O}_p$ è un ordine, in quanto è un sottoanello di $\mathcal{O}_K$ che contiene $\mathcal{O}$. Inoltre $\mathcal{O}_p$ è p-massimale; se infatti $p \mid [\mathcal{O}_K : \mathcal{O}_p]$, per il teorema di Cauchy esisterebbe $x \in \mathcal{O}_K \setminus \mathcal{O}_p$ tale che $px \in \mathcal{O}_p$ e dunque per definizione $x \in \mathcal{O}_p$, da cui un assurdo.
Quindi è sufficiente mostrare che $\mathcal{O} = \mathcal{O}' = \mathcal{O}_p$. Supponiamo per assurdo che $\mathcal{O}_p \not\subseteq \mathcal{O}$. Per ipotesi, abbiamo che:

- $\mathcal{O}_p$ è finitamente generato su $\mathbb{Z}$; scelti dei generatori $s_1, \ldots, s_n$, per definizione esiste $k \in \mathbb{N}$ tale che $p^k s_i \in \mathcal{O}$ e dunque $p^k \mathcal{O}_p \subseteq \mathcal{O}$.
- $\mathcal{O}$ è noetheriano e dunque esiste $s \in \mathbb{N}$ tale che $I_p^s \subseteq p\mathcal{O}$.

Come conseguenza di questi due punti $I_p^{ks}\mathcal{O}_p \subseteq \mathcal{O}$. Sia n il massimo indice per il quale $I_p^n \mathcal{O}_p \not\subseteq \mathcal{O}$ e sia $x \in I_p^n \mathcal{O}_p \setminus \mathcal{O}$. Notiamo che $xI_p \subseteq \mathcal{O}$; inoltre, se $y \in I_p$, $(xy)^{ks+1} = x^{ks+1}y^{ks+1} \in I_p(I_p^{ks}\mathcal{O}_p) \subseteq I_p\mathcal{O} = I_p$. Dato che I_p è radicale e $xy \in \mathcal{O}$, $xy \in I_p$ e dunque $xI_p \subseteq I_p$. Per definizione si ha allora $x \in \mathcal{O}' = \mathcal{O}$, da cui un assurdo. □

Dunque, nel corso dell'algoritmo, partiremo dall'ordine $\mathbb{Z}[\alpha]$, dove α è un elemento intero primitivo per K. Di questo ordine, è facilmente calcolabile il discriminante, per esempio calcolando il discriminante del polinomio minimo; possiamo allora fattorizzarlo $\operatorname{disc}(\alpha) = DF^2$, con D libero da quadrati. Per la formula di cambio di base del discriminante, sappiamo infatti che il discriminante di un sottordine differisce solo per fattori quadratici. A questo punto si considerano i primi che dividono F. Il problema è capire quali di questi primi non compaia nel discriminante e questo si può studiare, come visto nel teorema di Pohst-Zassenhaus, considerando l'ordine $\mathcal{O}'$. Occupiamoci ora di elaborare un metodo per il calcolo di $\mathcal{O}'$. Il seguente lemma fornisce un buon metodo:

Lemma 4.5. Con la notazione del precedente teorema, sia U il nucleo dell'applicazione

$$\begin{array}{rccc} \varphi\colon & \mathcal{O} & \longrightarrow & \operatorname{End}\left({}^{I_p}\!/_{p\mathcal{I}_p}\right) \\ & \alpha & \longmapsto & (\bar{\beta} \mapsto \bar{\alpha}\bar{\beta}) \end{array}$$

Allora $\mathcal{O}' = \frac{1}{p}U$.

Dimostrazione. Sia $x \in U$. Allora, dato che x induce per moltiplicazione l'endomorfismo nullo sul quoziente, si ha $xI_p \subseteq p\mathcal{I}_p$, da cui $\frac{x}{p}I_p \subseteq I_p$. Per definizione allora $x/p \in \mathcal{O}'$, da cui un contenimento. Per l'altro, notiamo preliminarmente che, dato che $p \in I_p$, $p\mathcal{O}' \subseteq \mathcal{O}$. Sia allora $x \in \mathcal{O}'$. Per definizione, $xI_p \subseteq I_p$; moltiplicando per p, $xpI_p \subseteq p\mathcal{I}_p$ e dunque $xp \in U$. Di conseguenza, $x \in U/p$, come volevasi dimostrare. $\square$

Abbiamo ridotto il calcolo di $\mathcal{O}'$ a un problema di algebra lineare. In primis, abbiamo necessità di un algoritmo per il calcolo del radicale I_p. Questo problema si risolve prima modulo p, notando che $\mathcal{O}/p\mathcal{O}$ è uno spazio vettoriale di dimensione finita sul quale può essere definito l'omomorfismo di Frobenius:

Proposizione 4.6. Consideriamo un campo di numeri K di grado n su $\mathbb{Q}$. Siano $\mathcal{O}$ un ordine di K e $p \in \mathbb{Z}$ un primo. Detto $R = \mathcal{O}/p\mathcal{O}$, il nilradicale di R coincide con il nucleo dell'omomorfismo $x \mapsto x^{p^j}$, dove $p^j \geq n$.

Dimostrazione. Chiaramente, un elemento nel nucleo appartiene al nilradicale, in quanto $x^{p^j} = 0$. Viceversa, sia $x \in \mathfrak{N}(R)$. x induce per moltiplicazione un endomorfismo φ_x di $\mathbb{F}_p$-spazi vettoriali su R che necessariamente è nilpotente. Dunque tutti gli autovalori di φ_x sono nulli e il suo polinomio caratteristico è $p(t) = t^n$. Di conseguenza, $x^n = 0$ e dunque, visto che $p^j \geq n$, $x^{p^j} = 0$. $\square$

Sia allora $\omega_1, \ldots, \omega_n$ la base corrispondente alla forma normale di Hermite di $\mathcal{O}$ rispetto a $1, \alpha, \ldots, \alpha^{n-1}$. Gli elementi $\bar{\omega}_1, \ldots, \bar{\omega}_n$ sono una $\mathbb{F}_p$-base di R e scelto j come nella proposizione, possiamo trovare dei coefficienti $a_{ij} \in \mathcal{O}$ tali che

$$\bar{\omega}_i^{p^j} = \sum_{j=1}^{n} \bar{a}_{ij}\bar{\omega}_j$$

Per farlo, basta rappresentare il primo membro come polinomio in α e, dato che la matrice degli ω_i è triangolare, passare dalla scrittura in base α a quella in base ω è poco oneroso. Detta allora $\bar{A}$ la matrice degli $\bar{a}_{ij}$, per la proposizione precedente il nilradicale coincide con il nucleo della matrice. Per eliminazione

gaussiana, possiamo allora trovare $\bar{s}_1, \dots, \bar{s}_l$ base del del nucleo data dall'applicazione. Per calcolare il radicale di $p\mathcal{O}$ è allora sufficiente trovare la controimmagine del nilradicale, che è sicuramente generata da $s_1, \dots, s_l$ e $p\omega_1, \dots, p\omega_n$. Per estrarne una base è allora sufficiente applicare alla matrice che ha come colonne i vettori $s_1, \dots, s_l, p\omega_1, \dots, p\omega_n$ (scritti rispetto alla base $1, \alpha, \dots, \alpha^{n-1}$) l'algoritmo di riduzione di Hermite e considerare i vettori corrispondenti alle colonne non nulle della matrice così ottenuta.

In questo modo abbiamo trovato una base di I_p e di $I_p/p\mathcal{O}$. Per trovare una base di $I_p/p\mathcal{I}_p$, è sufficiente considerare la base di I_p trovata e prenderne le immagini nel quoziente. Trovata una base $\bar{\beta}_1, \dots, \bar{\beta}_n$ di I_p/pI_p, sappiamo che una base di $\mathrm{End}(I_p/pI_p)$ è data dalle matrici E_{ij} tali che

$$(E_{ij})_{sk} = \delta_{is}\delta_{jk}$$

dove in questo caso δ è il delta di Kronecker. Vogliamo trovare il nucleo U del lemma; per questo, costruiamo la matrice dell'applicazione φ. È conveniente calcolare prima la matrice corrispondente alla mappa sul quoziente $\tilde{\varphi}\colon \mathcal{O}/p\mathcal{O} \to \mathrm{End}(I_p/pI_p)$ vista come applicazione di $\mathbb{F}_p$-spazi vettoriali. Per questo, è sufficiente trovare gli elementi $\bar{a}_{i,j,k} \in \mathbb{F}_p$ tali che

$$\bar{\omega}_i\bar{\beta}_j = \sum_{k=1}^{n} \bar{a}_{i,j,k}\bar{\beta}_k$$

Per riduzione Gaussiana, dato che $\mathbb{F}_p$ è un campo, si può così trovare una base $\bar{v}_1, \dots, \bar{v}_k$ del nucleo di $\tilde{\varphi}$. Per ottenere U, si applica l'algoritmo di riduzione di Hermite alla matrice

$$\begin{pmatrix} v_1 \,\big|\, & \dots & \big|\, v_k \,\big|\, p\omega_1 \,\big|\, & \dots & \big|\, p\omega_n \end{pmatrix}$$

Dividendo allora la base così ottenuta per p, si ricava una base di $\mathcal{O}'$, come voluto.

4.1 Il criterio di Dedekind

Il metodo appena elaborato risulta abbastanza pesante, in quanto prende in considerazione i primi che dividono il discriminante rispetto al quale $\mathbb{Z}[\alpha]$ è massimale. Per evitare questi, si usa solitamente il criterio di Dedekind:

Teorema 4.7 (Dedekind)**.** Sia K un campo di numeri e sia $\alpha \in K$ un elemento primitivo intero. Sia $\mu_\alpha \in \mathbb{Z}[x]$ il polinomio minimo di α e sia $p \in \mathbb{Z}$ un primo. Consideriamo la fattorizzazione in irriducibili di μ_α in $\mathbb{F}_p[x]$

$$\bar{\mu}_\alpha(x) = \prod_{i=1}^{r} \bar{t}_i(x)^{e_i}$$

con $(t_i, t_j) = 1$ se $i \neq j$. Sia $g(x) \in \mathbb{Z}[x]$ il polinomio

$$g(x) = \prod_{i=1}^{r} t_i(x)$$

dove t_i è un sollevamento monico di $\bar{t}_i$. Allora

1. Il p-radicale I_p è dato da

$$I_p = (p, g(\alpha)) \subseteq \mathbb{Z}[\alpha]$$

2. Sia $h \in \mathbb{Z}[x]$ un sollevamento monico di $\bar{\mu}_\alpha/\bar{g}$ e consideriamo il polinomio

$$f(x) = \frac{h(x)g(x) - \mu_\alpha(x)}{p}$$

Sia $U \in \mathbb{Z}[x]$ un sollevamento monico di $\bar{\mu}_\alpha/(\bar{f}, \bar{g}, \bar{h})$. Allora

$$\mathcal{O}' = \{x \in K \mid xI_p \subseteq I_p\} = \mathbb{Z}[\alpha] + \frac{1}{p}U(\alpha)\mathbb{Z}[\alpha]$$

Inoltre, detto $m = \deg(\bar{f}, \bar{g}, \bar{h})$, si ha $[\mathcal{O}' : \mathbb{Z}[\alpha]] = p^m$.

Dimostrazione.

1. Notiamo che $p \in I_p$ per definizione. Inoltre, $\bar{\mu}_\alpha(x) \mid \bar{g}(x)^n$ e dunque $g(\alpha) = 0 \pmod{p\mathbb{Z}[\alpha]}$, da cui il contenimento

$$I_p \supseteq (p, g(\alpha))$$

Per mostrare l'altro contenimento, notiamo che se $\bar{g} \in F_p[x]$ è tale che $\bar{g}(\alpha) = 0$, allora $\bar{\mu}_\alpha \mid \bar{g}$. Infatti, se $\bar{g}(\alpha) = 0$, allora esiste $s \in \mathbb{Z}[x]$ tale che $g(\alpha) + ps(\alpha) = 0$. Di conseguenza,

$$\mu_\alpha(x) \mid g(x) + ps(x) \implies \bar{\mu}_\alpha \mid \bar{g}$$

Sia allora $x \in I_p$. Per definizione di ideale radicale, esiste $n \in \mathbb{N}$ tale che $x^n \in p\mathbb{Z}[\alpha]$. Sia $A \in \mathbb{Z}[x]$ il polinomio tale che $A(\alpha) = x$. Allora $A^n(\alpha) = 0 \pmod{p\mathbb{Z}[\alpha]}$ e dunque $\bar{\mu}_\alpha \mid \bar{A}^n$, da cui $\bar{t}_i \mid \bar{A}$ per irriducibilità di $\bar{t}_i$. Abbiamo allora ottenuto che $\bar{g} \mid \bar{A}$ da cui $x \in p\mathbb{Z}[\alpha] + g(\alpha)\mathbb{Z}[\alpha]$.

2. Abbiamo necessità di un lemma:

Lemma 4.8. Sia $A \in \mathbb{Z}[x]$ un polinomio e consideriamo l'elemento $x = A(\alpha)/p \in Z[\alpha]$. Sia $\bar{k} = \bar{g}/(\bar{f}, \bar{g})$ e sia k un suo sollevamento monico. Allora $xg(\alpha) \in I_p$ se e solo se $\overline{hk} \mid \bar{A}$.

Dimostrazione del lemma. Per quanto fatto vedere, $xg(\alpha) \in I_p$ se e solo se esistono due polinomi $q, r \in \mathbb{Z}[x]$ tali che

$$A(\alpha)g(\alpha) = p^2 q(\alpha) + pg(\alpha)r(\alpha)$$

Dato che μ_α è il polinomio minimo di α, questo è equivalente a dire che esiste un $s \in \mathbb{Z}[x]$ tale che

$$A(x)g(x) = p^2 q(x) + pg(x)r(x) + s(x)\mu_\alpha(x)$$

Riduciamo quest'equazione modulo p; allora $\bar{A}(x) = \bar{s}(x)\bar{h}(x)$. Di conseguenza, possiamo scrivere

$$A(x) = s(x)h(x) + pz(x) \tag{1}$$

Sostituendo, otteniamo

$$s(x)h(x)g(x) + pz(x)g(x) = p^2q(x) + pg(x)r(x) + s(x)\mu_\alpha(x)$$

Raccogliendo $s(x)$, si arriva alla relazione

$$s(x)(h(x)g(x) - \mu_\alpha(x)) = p^2q(x) + pg(x)(r(x) - z(x))$$

Chiamando $r(x) - z(x) = b(x)$ e notando che $h(x)g(x) - \mu_\alpha(x)$ è proprio il polinomio $pf(x)$ definito nell'enunciato del teorema, si ha

$$s(x)f(x) = pq(x) + g(x)b(x)$$

Questa relazione implica che $\bar{g} \mid s(x)f(x)$ e dunque, preso k come nella definizione del teorema, $\bar{k}(x) \mid \bar{s}(x)$. Ancora una volta, esistono $c(x), d(x) \in \mathbb{Z}[x]$ tale che $s(x) = k(x)d(x) + pc(x)$. Riassumendo, dall'equazione 1, $xg(\alpha) \in I_p$ se e solo se esistono dei polinomi (con abuso di notazione) q, r tali che

$$A(x) = h(x)k(x)q(x) + pr(x)$$

e questo accade se e solo se $\overline{hk} \mid \bar{A}$, come voluto. □

Siamo allora pronti per dimostrare la seconda parte del teorema. Per definizione, $x \in \mathcal{O}'$ se e solo se $xI_p \subseteq I_p$. Chiaramente è sufficiente testare questo sui generatori e dunque $x \in \mathcal{O}'$ se e solo se $px \in I_p$ e $xg(\alpha) \in I_p$. Per quanto visto fino ad ora, è allora sufficiente mostrare che $\bar{g} \mid \bar{A}$ ($\Rightarrow$ $px \in I_p$) e che $\overline{hk} \mid \bar{A}$ ($\Rightarrow$ $xg(\alpha) \in I_p$). Le condizioni richieste sono equivalenti a $\operatorname{lcm}(\bar{g}, \overline{hk}) \mid \bar{A}$. Per le proprietà del minimo comune multiplo,

$$\operatorname{lcm}(\bar{g}, \overline{hk}) = \bar{k}\operatorname{lcm}(\gcd(\bar{f}, \bar{g}), \bar{h}) = \frac{\bar{g}}{(\bar{f}, \bar{g})}\frac{\bar{h}(\bar{f}, \bar{g})}{(\bar{h}, \bar{f}, \bar{g})} = \frac{\bar{\mu}_\alpha}{(\bar{f}, \bar{g}, \bar{h})} = \bar{U}$$

Di conseguenza, $\bar{U} \mid \bar{A}$ da cui $\mathcal{O}' = \mathbb{Z}[\alpha] + \frac{U(\alpha)}{p}\mathbb{Z}[\alpha]$. Inoltre, un sistema di rappresentanti per $\mathcal{O}'$ modulo $p\mathbb{Z}[\alpha]$ è formato dai polinomi della forma $a(x)U(x)/p$ al variare di a tra i polinomi di grado $< \deg(\mu_\alpha) - \deg(U) = m$, da cui la tesi.

□

Corollario 4.9. $\mathbb{Z}[\alpha]$ è p-massimale se e solo se $(\bar{f}, \bar{g}, \bar{h}) = 1$ in $\mathbb{F}_p[x]$.

Notiamo che possiamo applicare il criterio di Dedekind una sola volta per ogni primo p che divide il discriminante di $\mathbb{Z}[\alpha]$.Se dopo aver applicato il criterio p^2 dividesse ancora il discriminante di $\mathcal{O}$, dovremmo necessariamente ricorrere al teorema di Pohst-Zassenhaus. D'altronde, questo criterio è computazionalmente fondamentale, perché fornisce un modo semplice per scartare dalla coda i primi di $\mathbb{Z}$ che compaiono effettivamente nel discriminante.

5 Descrizione dell'algoritmo

Supponiamo quindi di avere in input un polinomio $T \in \mathbb{Z}[x]$, che sia il polinomio minimo di un elemento θ intero su $\mathbb{Z}$ e che sia un elemento primitivo per il campo di numeri K. In output, restituiremo una base intera di $\mathcal{O}_K$.

1. Porre $\omega_i = \theta^{i-1}$ per $i = 1, \ldots, n$
2. Calcolare il discriminante $\mathrm{disc}(\theta)$ mediante il calcolo del risultante $\mathrm{Ris}(T, T')$.
3. Fattorizzare $\mathrm{disc}(\theta) = DF^2$, con D libero da quadrati e con fattori a due a due coprimi.
4. Se $F = 1$, terminare l'algoritmo e restituire in output la base intera $\omega_1, \ldots, \omega_n$.
5. Sia $p \in \mathbb{Z}$ il più piccolo primo che divide F.
6. Fattorizzare T modulo p

$$\bar{T}(x) = \prod_{i=1}^{r} \bar{t}_i(x)^{e_i}$$

   e porre

$$g(x) = \prod t_i(x)h(x) = T(x)/g(x) \qquad f(x) = \frac{g(x)h(x) - T(x)}{p}$$

7. Calcolare $\bar{Z} = (\bar{f}, \bar{g}, \bar{h}) \in \mathbb{F}_p[x]$ e $\bar{U} = \bar{T}/\bar{Z}$.
8. Se $\deg(Z) = 0$, allora $\mathcal{O}$ è p-massimale, rimuovere p tra i divisori di F e tornare a 4.
9. Se $\deg(Z) > 0$, sia v_i il vettore dato dall'espressione di $\omega_i U(\theta)$ in base $1, \ldots, \theta^{n-1}$ per $i = 1, \ldots, m$ e v_{m+j} come il vettore corrispondente a $p\omega_j$ per $j = 1, \ldots, n$.
10. Applicare l'algoritmo di riduzione di Hermite alla matrice data dai vettori v_i e sia H la matrice corrispondente alle ultime n colonne ottenute dopo la riduzione.
11. Porre $\omega_i = H_i$, dove H_i è l'elemento corrispondente alla i-esima colonna di H.
12. Se $p^{m+1} \nmid F$, allora l'ordine ottenuto è p-massimale, quindi rimuovere p tra i divisori di F e tornare a 4.
13. Sia q la più piccola potenza di p tale che $q \geq n$. Calcolare la matrice A a coefficienti in $\mathbb{F}_p$ tale che

$$\omega_j^q = \sum_{i=1}^{n} a_{i,j}\omega_i$$

   Calcolare una base del nucleo di A $\bar{\beta}_1, \ldots, \bar{\beta}_k \subseteq I_p/p\mathcal{O}$
14. Completare $\bar{\beta}_1, \ldots, \bar{\beta}_k$ a base di $\mathcal{O}/p\mathcal{O}$

15. Porre $\alpha_i = \beta_i$ per $i = 1, \dots, k$ e $\alpha_i = p\beta_i$ per $i = k+1, \dots, n$, dove β_i è un sollevamento di $\bar{\beta}_i$ a $\mathcal{O}$.

16. Calcolare $c_{i,j,k} \in \mathbb{F}_p$ che soddisfano la relazione

$$\omega_k \alpha_j = \sum_{i=1}^{n} c_{i,j,k} \alpha_i \pmod p$$

e sia C la corrispondente matrice $n^2 \times n$.

17. Calcolare una base del nucleo di C $\bar{\gamma}_1, \dots, \bar{\gamma}_m$

18. Porre $v_i = \gamma_i$ per $i = 1, \dots, m$ e $v_{m+j} = p\omega_j$ per $j = 1, \dots, n$.

19. Applicare l'algoritmo di riduzione di Hermite alla matrice M $n \times (n+m)$ avente come colonne i vettori v_i.

20. Porre $\omega_i' = N_i/p$, dove N_i è l'elemento corrispondente all'i-esima colonna della matrice ottenuta dalla riduzione dello scorso punto.

21. Se $\omega_i = \omega_i'$ per ogni i, rimuovere il fattore p da F e tornare a 4.

22. Porre $\omega_i = \omega_i'$ e tornare al passo 13.

Chiaramente l'algoritmo può essere migliorato; in certi casi può essere utile per esempio il seguente:

Teorema 5.1. Sia $K = \mathbb{Q}(\alpha)$ un campo di numeri con $\alpha \in \mathcal{O}_K$ e sia μ_α il polinomio minimo di α. Se μ_α è di p-Eisenstein, allora

$$p \nmid \left| \mathcal{O}_K / \mathbb{Z}[\alpha] \right|$$

Questo permette di non considerare tutti i primi che dividono il discriminante quadraticamente e per i quali μ_α è di p-Eisenstein.

Esempio. Consideriamo il campo $K = \mathbb{Q}(\alpha)$, con $\alpha = \sqrt[3]{12}$. Notiamo che

$$\operatorname{disc}(\alpha) = N(\mu'(\alpha)) = 2^4 3^5$$

Dunque applichiamo il criterio di Dedekind per $p = 2, 3$.

- Se $p = 3$, fattorizziamo μ modulo 3, ottenendo

$$\mu \equiv x^3 \pmod 3$$

da cui $g(x) = x$ e $h(x) = x^2$. Dunque $f(x) = 4$ da cui $(\bar{f}, \bar{g}, \bar{h}) = 1$ e dunque $\mathbb{Z}[\alpha]$ è 3-massimale.

- Se $p = 2$, vale

$$\mu \equiv x^3 \qquad g(x) = x \qquad h(x) = x^2 \qquad f(x) = 6$$

Di conseguenza, $(\bar{f}, \bar{g}, \bar{h}) = x$ e $U(x) = x^2$. Dunque otteniamo una nuova candidata base intera

$$\mathcal{O}' = \mathbb{Z}[\alpha] + \frac{\alpha^2}{2}\mathbb{Z}[\alpha] = \langle 1, \alpha, \frac{\alpha^2}{2} \rangle$$

Purtroppo non siamo ancora certi della massimalità di $\mathcal{O}'$. Dobbiamo allora continuare ad eseguire l'algoritmo. Dobbiamo quindi costruire la matrice dell'omomorfismo di Frobenius $\alpha \to \alpha^4$ sulla riduzione modulo 2. Dato che $\alpha^3 \equiv 0 \pmod 2$, la matrice corrispondente è

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

e dunque $I_p = \langle \alpha, \alpha^2/2, 2, 2\alpha, \alpha^2 \rangle = \langle 2, \alpha, \alpha^2/2 \rangle$. Costruiamo allora la matrice corrispondente all'applicazione $\tilde{\varphi} \colon \mathcal{O}/p\mathcal{O} \to \mathrm{End}(I_p/pI_p)$. Allora

$$\begin{array}{ccccc} & 2 \mapsto 2 & & 2 \mapsto 2\alpha & & 2 \mapsto \alpha^2 \\ \cdot 1 & \alpha \mapsto \alpha & \cdot\alpha & \alpha \mapsto \alpha^2 & \cdot\frac{\alpha^2}{2} & \alpha \mapsto \frac{\alpha^3}{2} = 2 \cdot 3 \\ & \frac{\alpha^2}{2} \mapsto \frac{\alpha^2}{2} & & \frac{\alpha^2}{2} \mapsto \frac{\alpha^3}{2} = 2 \cdot 3 & & \frac{\alpha^2}{2} \mapsto \frac{\alpha^4}{4} = 3\alpha \end{array}$$

La matrice corrispondente in $\mathbb{F}_p$ è

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Dunque $\bar{U} = 0$. Di conseguenza $U = \langle 2, 2\alpha, \alpha^2 \rangle$, da cui $\mathcal{O}'' = \langle 1, \alpha, \alpha^2/2 \rangle$, da cui $\mathcal{O}' = \mathcal{O}''$. L'algoritmo termina restituendo il output la base intera:

$$\mathcal{O}_K = \langle 1, \alpha, \frac{\alpha^2}{2} \rangle$$

Chiaramente l'algoritmo, con piccole modifiche, può restituire in output anche il discriminante del campo, che in questo caso è $\mathrm{disc}(K) = 27 \cdot 4 \cdot 3$.