UNIVERSITÀ DEGLI STUDI DI ROMA TRE

Dipartimento di Matematica e Fisica

Corso di Laurea Magistrale in Matematica

Sintesi della Tesi di Laurea Magistrale in Matematica

Calcolo del Minimo Euclideo di un campo di numeri K

Candidato

Gaja Lombardi

Relatore

Prof. Francesco Pappalardi

Anno Accademico 2012/2013

Maggio 2014

Parole chiave: Algoritmo Euclideo, Minimo Euclideo.

Classificazione MSC2000: 11Y40; 11R04; 12j15; 13F07

Il matematico greco Euclide, che visse intorno al 300 a.C, viene spesso considerato il padre della geometria per l'importante contributo che apportò a quella che oggi viene chiamata Geometria Euclidea. Nonostante la sua opera *Elementi* sia soprattutto conosciuta per i suoi risultati geometrici, questa affronta anche questioni che riguardano la teoria dei numeri. Per esempio il Lemma di Euclide, che conduce poi al Teorema Fondamentale dell'Aritmetica il quale riguarda l'unicità della fattorizzazione in fattori primi, il fatto che i numeri primi siano infiniti e l'Algoritmo Euclideo per trovare il massimo comun divisore tra due numeri interi.
Nel XIX secolo, l'agoritmo Euclideo contribuì al raggiungimento di risultati molto importanti. Il matematico tedesco Peter Gustav Lejeunne Dirichlet (1805-1859) definì l'Algoritmo Euclideo come la base della Teoria dei Numeri. Infatti notò che molti risultati ottenuti tramite l'Algoritmo Euclideo, come per esempio la fattorizzazione unica, continuassero ad essere veri in un qualsiasi altro dominio sul quale valesse l'Algoritmo Euclideo. Richard Dedekind (1831- 1916) utilizzò l'algoritmo per studiare la natura degli interi algebrici e definì il concetto di Dominio Euclideo.
Nel Primo Capitolo definiamo i Domini Euclidei e presentiamo il criterio di Theodore Samuel Motzkin (1908-1970) [23] che stabilisce se, dato un dominio R, esiste una funzione Euclidea da R in $\mathbb{N}$.

Definizione 1.2. Sia R un dominio di integrità e sia W un insieme ben ordinato. Se $\psi : R\backslash\{0\} \longmapsto W$ è un'applicazione tale che per ogni a e $b \in R,\ b \neq 0$, esistono r e $q\ \in R$ tali che $a = bq + r$, dove $r = 0$ oppure $\psi(r) < \psi(b)$, allora ψ si dice **funzione Euclidea su** R o **algoritmo Euclideo su** R. Se sul dominio R è definito un algoritmo Euclideo ψ, diremo che R è un **dominio Euclideo rispetto a** ψ**.**

Un'importante proprietà dei Domini Euclidei è che sono sempre dei domini a ideali principali (PID) i quali sono a loro volta dei domini a fattorizzazione unica (UFD).

Definizione 1.8. Sia K un sottocampo di $\mathbb{C}$. Diremo che K è un **campo di numeri** se è un'estensione di grado finito su $\mathbb{Q}$. Per il Teorema dell'elemento primitivo possiamo sempre scrivere $K = \mathbb{Q}(\theta)$, con $\theta \in \mathbb{C}$.

Definizione 1.9. Sia $\alpha \in \mathbb{C}$, diremo che α è un **intero algebrico** se esiste un polinomio non nullo monico a coefficienti in $\mathbb{Z}$ di cui α è una radice. L'insieme degli interi algebrici forma un anello che indichiamo con $\mathcal{O}$.
Sia K un campo di numeri. Definiamo **l'insieme degli interi algebrici di** K, $\mathcal{O}_K$, come l'insieme costituito dagli interi algebrici contenuti in K, vale a dire

$$\mathcal{O}_K = \mathcal{O} \cap K.$$

Definizione 1.12. Sia K un campo. Un omomorfismo non nullo $\varphi : K \longrightarrow \mathbb{C}$ si dice

immersione.

È tra i risultati fondamentali della Teoria di Galois [21] il fatto che, dato un campo di numeri K tale che $[K : \mathbb{Q}] = n$, esistano esattamente n immersioni di K in $\mathbb{C}$:

$$\sigma_i : K \longrightarrow \mathbb{C} \qquad i = 1, ..., n$$

Definizione 1.15. Sia K un campo di numeri tale che $[K : \mathbb{Q}] = n$ e siano $\sigma_1, \sigma_2, ..., \sigma_n$ le n immersioni di K in $\mathbb{C}$. La **norma di un elemento** $x \in K$ è definita da:

$$N(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Definizione 1.16. Sia K un campo di numeri e sia $\mathcal{O}_K$ il suo anello degli interi algebrici. Diremo che $\mathcal{O}_K$ è **Euclideo rispetto alla norma**[1] se è Euclideo rispetto al valore assoluto della norma, quindi se per ogni $a, b \in \mathcal{O}_K$, con $b \neq 0$, esistono q ed r in $\mathcal{O}_K$ tali che

$$a = bq + r \text{ dove } r = 0 \text{ oppure } |N(r)| < |N(b)|.$$

In Europa agli inizi del 1800 molti matematici si domandarono quali fossero i campi di numeri K il cui anello degli interi algebrici $\mathcal{O}_K$ fosse un dominio Euclideo. In particolare si chiesero quali $\mathcal{O}_K$ fossero Euclidei rispetto al valore assoluto della norma. Mentre i matematici tedeschi, quali Gauss, Jacobi e Kummer, si occuparono di questa questione per cercare di generalizzare la Legge di Reciprocità Quadratica di Gauss per potenze più alte, i matematici francesi invece, quali Cauchy e Liouville, se ne occuparono per dimostrare l'Ultimo Teorema di Fermat. Entrambi questi approcci richiedevano che $\mathcal{O}_K$ fosse a fattorizzazione unica (UFD). Chiaramente se $\mathcal{O}_K$ è Euclideo è anche UFD.
Era noto che $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$ fossero Euclidei rispetto alla norma. Nel 1893 furono aggiunti alla lista anche $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$ e $\mathbb{Q}(\sqrt{-11})$. Oltre a questi campi, esistono solo altri quattro campi quadratici immaginari ($\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ e $\mathbb{Q}(\sqrt{-163})$) il cui anello degli interi algebrici $\mathcal{O}_K$ è un PID. Nel 1949 Motzkin [23] non soltanto dimostrò che questi quattro campi non sono Euclidei rispetto alla norma, ma che non sono Euclidei per nessun algoritmo a valori in $\mathbb{N}$, vale a dire che, nel caso in cui $\mathcal{O}_K$ è uno tra $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, $\mathbb{Z}[\frac{1+\sqrt{-43}}{2}]$, $\mathbb{Z}[\frac{1+\sqrt{-67}}{2}]$ e $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$, non esiste un algoritmo Euclideo $\psi : \mathcal{O}_K \setminus \{0\} \longrightarrow \mathbb{N}$. Motzkin in un certo senso fu innovativo, perché formulò un criterio per trovare, nel caso fosse esistita, una funzione Euclidea su un dominio che fosse diversa dalla norma. Fino ad allora, infatti, si pensava che la norma fosse l'unica funzione Euclidea possibile. Proprio perché Motzkin fornì un metodo per caratterizzare i domini Euclidei, abbiamo ritenuto importante riportare il suo criterio in questa tesi.
Nel Primo Capitolo, quindi, viene riportato il criterio di Motzkin [23] e si dà un accenno al criterio di Harper [16], che altro non è che una variante del criterio di Motzkin. La

[1] O più semplicemente diremo che K è Euclideo rispetto alla norma.

particolarità del criterio di Motzkin è che non soltanto stabilisce se esiste o meno un algoritmo Euclideo sul dominio in questione, ma ne costruisce addirittura uno. In particolare tramite il criterio di Motzkin si costruisce il "più piccolo" algoritmo Euclideo a valori in $\mathbb{N}$. Questo rappresenta un risultato importante perché permette di trovare degli esempi di domini Euclidei per i quali non esiste una funzione Euclidea che assuma valori in $\mathbb{N}$.

Definizione 1.26. (Costruzione di Motzkin) Sia R un dominio, poniamo $A_0 := \{0\} \cup R^*$, dove con R^* indichiamo l'insieme costituito dalle unità di R. Siano

$$A_i = \{a \in R \ : \ \forall x \in R, \ \exists \ y \in A_{i-1} \text{ t.c. } x - y \in (a)\}$$

per ogni $i > 0$, e sia $A = \bigcup_{i=0}^{\infty} A_i$. Questa successione di insiemi A_i si chiama **Costruzione di Motzkin** relativa al dominio R. Inoltre se $A = R$ definiamo la funzione

$$\begin{aligned} \phi_R : R &\longmapsto \mathbb{N} \\ x &\longmapsto \phi_R(x) = \begin{cases} i & \text{se } x \in A_i \backslash A_{i-i} \text{ e } x \neq 0 \\ 0 & \text{se } x = 0 \end{cases} \end{aligned}$$

Teorema 1.28.(Motzkin) *Sia R un dominio e sia $(A_i)_{i\geq 0}$ la successione di insiemi data dalla costruzione di Motzkin della Definizione 1.26. Posto*

$$A = \bigcup_{i=0}^{\infty} A_i,$$

se $A = R$ allora la funzione ϕ_R della Definizione 1.26 è una funzione Euclidea da R in $\mathbb{N}$.

Definizione 1.30. Sia R un dominio Euclideo e sia W un insieme ben ordinato. Definiamo la funzione

$$\begin{aligned} \phi_W : R &\longmapsto W \\ a &\longmapsto \phi_W(a) := \inf_{\varrho} \varrho(a) \end{aligned}$$

al variare degli algoritmi Euclidei $\varrho : R \longmapsto W$. Diremo che ϕ_W è **l'algoritmo minimo** da R a W.

Si dimostra che se R è un dominio sul quale è definito un algoritmo Euclideo da R in $\mathbb{N}$, l'algoritmo ϕ_R, costruito tramite la costruzione di Motzkin, è l'algoritmo Euclideo minimo da R a $\mathbb{N}$.

Teorema 1.32. *Sia R un dominio per il quale esista un algoritmo Euclideo $\varrho : R \longmapsto \mathbb{N}$. Allora l'algoritmo ϕ_R della Definizione 1.26 è l'algoritmo minimo da R a $\mathbb{N}$. In altre parole*

$\phi_R = \phi_{\mathbb{N}}$.

Esempio 1.34. Consideriamo il dominio $\mathbb{Z}[\sqrt{-5}]$. Vogliamo dimostrare non soltanto che la norma non è una funzione Euclidea su $\mathbb{Z}[\sqrt{-5}]$ ma che non esiste una funzione Euclidea da $\mathbb{Z}[\sqrt{-5}]$ in $\mathbb{N}$.
Supponiamo per assurdo che il valore assoluto della norma sia un algoritmo Euclideo su $\mathbb{Z}[\sqrt{-5}]$. Siano R_i gli insiemi

$$R_i = \{0\} \cup \{\alpha \in \mathbb{Z}[\sqrt{-5}] : |N(\alpha)| \leq i\}.$$

Nella dimostrazione del Teorema 1.32 dimostreremo per induzione che gli insiemi $R_i \subseteq A_i$ per ogni $i \geq 0$, dove gli insiemi A_i sono come nella Definizione 1.26. Avremo
$R_0 = \{0\}$;
$R_1 = \{0, \pm 1\}$
$R_2 = \{0, \pm 1\}$
$R_3 = \{0, \pm 1\}$.
Sappiamo che $A_0 = \{0, \pm 1\}$. Vogliamo determinare A_1. Per quanto detto sopra, $R_1 \subseteq A_1$, ma poiché $R_1 = R_2 = R_3$, allora $R_3 \subseteq A_1$. Quindi in $A_1 \backslash A_0$ ci sono elementi il cui valore assoluto della norma è minore di 3. Ma gli unici elementi $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tali che $a^2 + 5b^2 \leq 3$ sono 0 e ± 1.Quindi $A_1 = A_0$ e $A_1 \backslash A_0 = \emptyset$. Questo implica che $A = \{0, \pm 1\}$ e che $\mathbb{Z}[\sqrt{-5}] \neq A$. Ma allora $\mathbb{Z}[\sqrt{-5}]$ non possiede un algoritmo Euclideo a valori in $\mathbb{N}$, in particolare non è Euclideo rispetto alla norma.

Nel Secondo Capitolo vengono introdotti dei nuovi concetti: quello del Minimo Euclideo (relativo alla norma) e del Minimo non Omogeneo, i quali rappresentano un criterio efficace per verificare se $\mathcal{O}_K$ sia Euclideo rispetto alla norma. Queste costanti furono inizialmente studiate proprio per la loro relazione a questo problema [18]. Infatti quando il Minimo Euclideo è strettamente minore di 1, il campo di numeri K in questione è Euclideo rispetto alla norma cioè il suo anello degli interi algebrici $\mathcal{O}_K$ ammette un algoritmo di divisione Euclidea ed è, quindi, un PID e di conseguenza anche un UFD. Tra gli articoli più importanti che trattano di questo argomento ricordiamo sicuramente quelli di F. Lemmermeyer [18], J. P. Cerri [5], [6] e quello di M. Elia e J. Carmelo [11].
Sia K un campo di numeri, $\mathcal{O}_K$ il suo anello degli interi algebrici e sia N la norma definita su K (Definizione 2.5).

Teorema 1.17. *$\mathcal{O}_K$ è Euclideo rispetto alla norma se e soltanto se per ogni $\xi \in K$, esiste $\gamma \in \mathcal{O}_K$ tale che $|N(\xi - \gamma)| < 1$.*

Definizione 2.7. Sia $\xi \in K$. Il **Minimo Euclideo di** ξ (relativo alla norma)[2] è il

[2]Il termine originario inglese è "local Euclidean minimum". Il termine "Minimo Euclideo di ξ" è una mia traduzione.

numero reale non negativo

$$m_K(\xi) = \inf\{|N(\xi - \gamma)| : \gamma \in \mathcal{O}_K\}$$

. **Proposizione 2.8.** *$m_K(\xi)$ ha le seguenti proprietà:*

1. *per ogni $(\xi, \gamma, \epsilon) \in K \times \mathcal{O}_K \times \mathcal{O}_K^*$, $m_K(\epsilon\xi - \gamma) = m_K(\xi)$;*
2. *per ogni $\xi \in K$, esiste $\gamma \in \mathcal{O}_K$ tale che $m_K(\xi) = |N(\xi - \gamma)|$;*
3. *per ogni $\xi \in K$, $m_K(\xi) \in \mathbb{Q}$. Inoltre $m_K(\xi) = 0$ se e solo se $\xi \in \mathcal{O}_K$.*

Dalla Proposizione 2.8 (1) si deduce che preso un elemento ξ del campo di numeri K, $m_K(\xi) = m_K(\xi - \gamma)$ per ogni $\gamma \in \mathcal{O}_K$. Questo significa che il Minimo Euclideo locale $m_K(\xi)$ dipende soltanto dalla classe di ξ in $K/\mathcal{O}_K$. Il Minimo Euclideo locale permette di riformulare il concetto di campo Euclideo rispetto alla norma, infatti, per il Teorema 1.17, un campo di numeri K è Euclideo rispetto alla norma se e soltanto se per ogni $\xi \in K$ esiste $\gamma \in \mathcal{O}_K$ tale che $|N(\xi - \gamma)| < 1$ ma questo equivale a verificare che per ogni $\xi \in K$, $m_K(\xi) < 1$. Per questo motivo definiamo:

Definizione 2.9.. Il **Minimo Euclideo di** K (rispetto alla norma) è il numero positivo reale

$$M(K) = \sup\{m_K(\xi) : \xi \in K\}.$$

Abbiamo potuto fornire questa definizione perché si dimostra in [6] che m_K è limitata e quindi $M(K)$ è finito.

Proposizione 2.12. *Il valore di $M(K)$ fornisce importanti informazioni:*

1. *Se $M(K) < 1$, K è Euclideo rispetto alla norma.*
2. *Se $M(K) > 1, K$ non è Euclideo rispetto alla norma.*
3. *Se $M(K) = 1$, non possiamo dire niente a meno che non esista un elemento $\xi \in K$ tale che $M(K) = m_K(\xi)$; in questo caso K non è Euclideo rispetto alla norma.*

Esempio 2.35. Si dimostra ([17]) che il minimo Euclideo $M(K)$ di un campo quadratico immaginario $K = \mathbb{Q}(\sqrt{-m})$ rispetto alla norma è:

$$M(K) = \begin{cases} \frac{|m|+1}{4}, & \text{se } \mathcal{O}_K = \mathbb{Z}[\sqrt{-m}] \\ \frac{(|m|+1)^2}{16m}, & \text{se } \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-m}}{2}]. \end{cases}$$

Calcolando il Minimo Euclideo nei casi in cui $m = 1, 2, 3, 7, 11$ otteniamo rispettivamente $M(K) = \frac{1}{2},\ \frac{3}{4},\ \frac{1}{3},\ \frac{4}{7},\ \frac{9}{11}$ che sono tutti minori strettamente di 1. Infatti $K = \mathbb{Q}(\sqrt{-m})$ è Euclideo rispetto alla norma se e solo se $m = 1, 2, 3, 7, 11$ ([18], Proposizione 4.1). Prendiamo per esempio $K = \mathbb{Q}(\sqrt{-5})$, allora $M(K) = \frac{3}{2}$ che è maggiore di uno quindi K

non è Euclideo rispetto alla norma.
Nel caso quadratico reale non si ha invece un'uguaglianza per $M(K)$, ma si hanno comunque buone stime. Sia K un campo quadratico reale e sia d il suo discriminante, si ha

$$\frac{\sqrt{d}}{16+6\sqrt{6}} \leq M(K) \leq \frac{1}{4}\sqrt{d}$$

(si veda Proposizione 2.33). Anche in questo caso se calcoliamo il Minimo Euclideo di K con $K = \mathbb{Q}(\sqrt{m})$, con $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$, otteniamo $M(K)<1$. Quindi, per questi valori di m, K è Euclideo rispetto alla norma. Questo risultato era prevedibile perchè nel caso quadratico reale $K = \mathbb{Q}(\sqrt{m})$, K è Euclideo rispetto alla norma se e soltanto se $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ ([18], Teorema 4.4).

Il problema relativo al Minimo Euclideo $M(K)$ è che può risultare difficile calcolarlo. Per ovviare a questo problema si introduce una nuova "norma" definita su tutto $\mathbb{R}^n$ tramite la quale è possibile definire il Minimo Non Omogeneo di K, $M(\overline{K})$, che ci sarà utile per il calcolo del Minimo Euclideo $M(K)$.
Sia n il grado di K su $\mathbb{Q}$ allora, per quanto detto prima, esistono esattamente n immersioni σ_i di K in $\mathbb{C}$. Scriviamo $n = r_1+2r_2$ e $r = r_1+r_2-1$, dove r_1 e $2r_2$ indicano rispettivamente il numero di immersioni reali ed il numero di immersioni complesse di K in $\mathbb{C}$. Il Teorema di Dirichlet sulle unità ([22], p.114), afferma che l'insieme degli elementi invertibili di $\mathcal{O}_K$, $\mathcal{O}_K^*$, è un gruppo moltiplicativo generato dalle radici dell'unità contenute in K e da r unità fondamentali $(\epsilon_i)_{1\leq i\leq r}$ dove $r = r_1 + r_2 - 1$ è il rango di $\mathcal{O}_K^*$. Rinumeriamo le immersioni σ_i in modo tale che σ_i, $1 \leq i \leq r_1$ siano le r_1 immersioni reali di K in $\mathbb{C}$ e σ_i con $r_1+1 \leq i \leq 2r_2+r_1 = n$ siano invece le $2r_2$ immersioni complesse di K in $\mathbb{C}$ le quali sono a due a due coniugate, quindi tali che $\sigma_{r_2+i} = \overline{\sigma_i}$ per ogni $r_1 + 1 \leq i \leq r_1 + r_2$. Sia

$$\begin{aligned} \Phi : K &\to \mathbb{R}^n \\ \xi &\mapsto (\sigma_1(\xi), ..., \sigma_{r_1}(\xi),\ \mathcal{R}\sigma_{r_1+1}(\xi), ..., \mathcal{R}\sigma_{r_1+r_2}(\xi), \mathcal{I}\sigma_{r_1+1}(\xi), ..., \mathcal{I}\sigma_{r_1+r_2}(\xi)) \end{aligned} \tag{2.1}$$

dove $\mathcal{R}$ e $\mathcal{I}$ rappresentano rispettivamente la parte reale e la parte immaginaria di un elemento di $\mathbb{C}$. Affinchè Φ possa essere un omomorfismo non nullo di K in $\mathbb{R}^n$, è necessario estendere il prodotto definito su K ad $\mathbb{R}^n$ in questo modo: siano $x = (x_i)_{1\leq i\leq n}$ e $y = (y_i)_{1\leq i\leq n}$ appartenenti a $\mathbb{R}^n$, allora $x \cdot y := (z_i)_{1\leq i\leq n}$ dove

$$z_i = \begin{cases} x_i y_i & \text{se } 1 \leq i \leq r_1 \\ x_i y_i - x_{i+r_2} y_{i+r_2} & \text{se } r_1 < i \leq r_1 + r_2 \\ x_{i-r_2} y_i + x_i y_{i-r_2} & \text{se } r_1 + r_2 < i \leq n. \end{cases} \tag{2.2}$$

e per praticità introduciamo $H = K \otimes_{\mathbb{Q}} \mathbb{R}$ che identifichiamo con $\mathbb{R}^n$ e sul quale è definito

il prodotto (2.2). Possiamo estendere la norma ad H tramite la funzione $\mathcal{N}$

$$\begin{aligned} \mathcal{N} : H &\to \mathbb{R} \\ x = (x_i)_{1\le i\le n} &\to \prod_{i=1}^{r_1} x_i \prod_{i=r_1+1}^{r_1+r_2} (x_i^2 + x_{i+r_2}^2). \end{aligned} \tag{2.6}$$

Con abuso di notazione, diremo che $\mathcal{N}$ è la norma in $H \simeq \mathbb{R}^n$, anche se non è una norma vera e propria, in quanto $\mathcal{N}(x) = 0$ non implica necessariamente che $x = 0$. Questa nuova funzione $\mathcal{N}$, è una funzione moltiplicativa, quindi per ogni $x, y \in H,\ \mathcal{N}(x \cdot y) = \mathcal{N}(x)\mathcal{N}(y)$. Si nota, inoltre, che per ogni $\xi \in K,\ N(\xi) = \mathcal{N}(\Phi(\xi))$, vale a dire:

$$\mathcal{N}|_{\Phi(K)} = N$$

dove con N indichiamo la norma da K in $\mathbb{R}$ (Definizione 1.15).
Poiché un campo di numeri K è Euclideo rispetto alla norma se e solo se per ogni $\xi \in K$ esiste un elemento $z \in \mathcal{O}_K$ tale che $|N(\xi - z)| < 1$ (Teorema 1.17), allora $\mathcal{O}_K$ è Euclideo rispetto alla norma se e solo se $|\mathcal{N}(\Phi(\xi - z))| < 1$ ma questo accade se e solo se $|\mathcal{N}(\Phi(\xi) - \Phi(z))| < 1$. Quindi, affinché K risulti Euclideo, è sufficiente che per ogni $x \in \mathbb{R}^n$ esista un $z \in \mathcal{O}_K$ tale che

$$|\mathcal{N}(x - \Phi(z))| < 1. \tag{2.7}$$

Ricordando che un sottogruppo discreto di rango n di $\mathbb{R}^n$ si chiama **reticolo** di $\mathbb{R}^n$, dimostreremo che $\Phi(\mathcal{O}_K)$, dove Φ è definita in (2.1), è un reticolo di $\mathbb{R}^n \simeq H$. Sia $\mathcal{F} = \{x \in H \mid x = \sum_{i=1}^n e_i\alpha_i \text{ dove } 0 \le \alpha < 1\}$ il dominio fondamentale del reticolo $\Phi(\mathcal{O}_K)$, dove $(e_i)_{1\le i\le n}$ è una $\mathbb{Z}$-base di $\Phi(\mathcal{O}_K)$, allora ogni elemento di $\mathbb{R}^n$ è congruo, modulo $\Phi(\mathcal{O}_K)$, ad un unico punto del dominio fondamentale $\mathcal{F}$. Quindi una condizione sufficiente affinché $\mathcal{O}_K$ sia Euclideo rispetto alla norma è che per ogni $x \in \mathcal{F}$ esista un elemento $Z \in \Phi(\mathcal{O}_K)$ tale che $|\mathcal{N}(x - Z)| < 1$. Per questo motivo si definisce il Minimo non Omogeneo che è l'equivalente del Minimo Euclideo $M(K)$ in $\mathbb{R}^n$ e rispetto alla norma $\mathcal{N}$.

Definizione 2.17. Sia $x \in H$. Il **Minimo Non Omogeneo di** x è il numero reale

$$m_{\overline{K}}(x) := \inf_{\gamma\in\mathcal{O}_K} |\mathcal{N}(x - \Phi(\gamma))|$$

dove Φ è l'applicazione definita in (2.1).

Proposizione 2.18 (1). *La mappa $m_{\overline{K}}$ è tale che per ogni $(x, Z, \epsilon) \in H \times \Phi(\mathcal{O}_K) \times \mathcal{O}_K^*,\ m_{\overline{K}}(x) = m_{\overline{K}}(\Phi(\epsilon) \cdot x - Z)$, dove con $\mathcal{O}_K^*$ indichiamo il gruppo delle unità di $\mathcal{O}_K$.*

In particolare, considerato $x \in H$, $m_{\overline{K}}(x) = m_{\overline{K}}(x - Z)$ per ogni $Z \in \Phi(\mathcal{O}_K)$. Quindi, come il Minimo Euclideo locale $m_K(\xi)$ dipende solo dalla classe di ξ in $K/\mathcal{O}_K$, così, considerato $x \in H$, il Minimo Non Omogeneo locale $m_{\overline{K}}(x)$ dipende solo dalla classe di x

in $H/\Phi(\mathcal{O}_K)$. Per la dimostrazione si veda [5]. Poiché in [5] si dimostra, inoltre, che $m_{\overline{K}}$ è limitata, allora è possibile dare la seguente definizione.

Definizione 2.19. Chiameremo il **Minimo Non Omogeneo di** K, e lo indicheremo con $M(\overline{K})$, il numero reale positivo

$$M(\overline{K}) = \sup\{m_{\overline{K}}(x) : x \in H\}.$$

Dalla definizione segue che $M(K) \leq M(\overline{K})$. In realtà Barnes e Swinnerton-Dyer [1] dimostrarono che $M(K) = M(\overline{K}) \in \mathbb{Q}$ nel caso in cui K è un campo quadratico reale; F. J. van der Linden [28] giunse alle stesse conclusioni nel caso più generale in cui il rango di $\mathcal{O}_K^*$ è $r = 1$. Queste considerazioni suggerirono delle congetture riguardanti i campi di numeri K con rango $r \geq 1$:
(1) $M(K) = M(\overline{K})$;
(2) $M(K)$, e quindi anche $M(\overline{K})$, è sempre razionale.
Nel 2005 J. P. Cerri [6] riuscì a dimostrare entrambe queste congetture. Possiamo quindi concludere che:

Corollario 2.23. *Per ogni campo di numeri K si ha $M(K) = M(\overline{K})$.*

Quindi per conoscere il valore del Minimo Euclideo di un campo di numeri K, calcolaremo il Minimo Euclideo non omogeneo $M(\overline{K})$.
Negli ultimi due capitoli spieghiamo come si calcola $M(K) = M(\overline{K})$, illustrando un algoritmo che calcoli il Minimo Euclideo di K. In particolare nel terzo capitolo forniamo una serie di algoritmi preliminari che saranno necessari per la costruzione dell'algoritmo principale che viene presentato, invece, nell'ultimo capitolo. Ricordiamo che per ogni $\xi \in K$ $N(\xi) = \mathcal{N}(\Phi(\xi))$, quindi

$$m_K(\xi) = m_{\overline{K}}(\Phi(\xi))$$

dove m_K e $m_{\overline{K}}$ rappresentano rispettivamente il Minimo Euclideo locale (Definizione 2.7) ed il Minimo non omogeneo locale (Definizione 2.17) e Φ è l'applicazione definita in (2.1). La strategia è la seguente.
Supponiamo di avere un'idea del valore esatto di $M(K)$ che denotiamo con k. L'idea è quella di dimostrare che $m_K(\xi) = m_{\overline{K}}(\Phi(\xi)) < k$ a meno di un numero finito di punti $(\xi_i)_{1\leq i\leq l} \in K$. Se esiste qualche i per cui $m_K(\xi_i) \geq k$, allora $M(K) = \max_{1\leq i\leq l} m_K(\xi_i)$. Poiché, però, per la Proposizione 2.18, $m_{\overline{K}}$ è definita modulo $\Phi(\mathcal{O}_K)$, e ricordando che $\Phi(\mathcal{O}_K)$ è un reticolo di $\mathbb{R}^n$, è sufficiente lavorare su $\mathcal{F}$, il dominio fondamentale del reticolo $\Phi(\mathcal{O}_K)$. Quindi supponiamo che k sia la nostra supposizione sul valore di $M(K)$, allora se $m_{\overline{K}}(x_i) < k$ a meno di un numero finito di punti $(x_i)_{1\leq i\leq l} = (\Phi(\xi_i))_{1\leq i\leq l}$ del dominio fondamentale $\mathcal{F}$ ed esiste quindi qualche i per cui $m_{\overline{K}}(x_i) \geq k$ allora $M(\overline{K}) = \max_{1\leq i\leq l} m_{\overline{K}}(x_i) = \max_{1\leq i\leq l} m_K(\xi_i) = M(K)$. La prima cosa che si fa è quella di ricoprire il dominio fondamentale $\mathcal{F}$ tramite dei parallelepipedi n-dimensionali di cui

diamo di seguito la definizione.

Definizione 3.8. Un n**-parallelepipedo** (o più semplicemente parallelepipedo) $\mathcal{P}$ di centro $c = (c_1, ..., c_n)$ e raggio $h = (h_1, ..., h_n) \in (\mathbb{R}_{>0})^n$ è l'insieme

$$\mathcal{P} = \{(x_1, ..., x_n) \in H,\ \forall\ 1 \leq i \leq n,\ |c_i - x_i| < h_i\}.$$

Lo scopo è quello di determinare una famiglia $\{\mathcal{P}_i\}_{i \in I}$ di n-parallelepipedi tali che $\mathcal{F} \subseteq \bigcup_{i \in I} \mathcal{P}_i$. Il procedimento tramite il quale si ottengono certi parallelepipedi è descritto in dettaglio in [5]. Una volta determinato un ricoprimento del dominio fondamentale tramite parallelepipedi, si eliminano tutti quei parallelepipedi $\mathcal{P}$ all'interno dei quali $m_{\overline{K}}(x) < k$ per ogni $x \in \mathcal{P}$.

Definizione 3.9. Sia $\mathcal{P}$ un n-parallelepipedo e $k > 0$. Se esiste un elemento $z \in \Phi(\mathcal{O}_K)$ tale che, per ogni $x \in \mathcal{P}$, $|\mathcal{N}(x - z)| < k$, si dice che $\mathcal{P}$ è **assorbito da** z.

I parallelepipedi che vengono quindi eliminati dal ricoprimento di $\mathcal{F}$ sono tutti quei parallelepipedi $\mathcal{P}$ che vengono assorbiti da un elemento $z \in \Phi(\mathcal{O}_K)$, grazie al criterio fornito dal seguente Lemma:

Lemma 3.11. *Sia $\mathcal{P}$ un parallelepipedo di centro $c = (c_1, ..., c_n)$ e passo $h = (h_1, .., h_n)$. $\mathcal{P}$ è assorbito da $z = (z_1, ..., z_n) \in \Phi(\mathcal{O}_K)$ se*

$$\prod_{i=1}^{r_1} (|c_i - z_i| + h_i) \prod_{i=r_1+1}^{r_1+r_2} \left((|c_i - z_i| + h_i)^2 + (|c_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 \right) < k.$$

Quindi per ogni parallelepipedo $\mathcal{P}$ che ricopre il dominio fondamentale si considera una lista di interi $\mathcal{L} \subseteq \Phi(\mathcal{O}_K)$. Se esiste un elemento $z \in \mathcal{L}$ tale che l' ipotesi del Lemma 3.11 è verificata, allora il parallelepipedo $\mathcal{P}$ viene scartato. Questo procedimento prende il nome di **Test di assorbimento**. I parallelepipedi che non vengono scartati tramite il Test di assobimento si dicono **parallelepipedi problematici**. Notiamo che all'interno di questi parallelepipedi problematici potrebbero esserci dei punti $x \in \mathcal{F}$ tali che $m_{\overline{K}}(x) \geq k$. Per capire meglio però la natura degli elementi appartenenti ai parallelepipedi problematici rimasti, si analizza l'azione del gruppo delle unità su H

$$\begin{cases} \mathcal{O}_K^* \times H \to H \\ (\epsilon, x) \to \Phi(\epsilon) \cdot x \end{cases} \tag{3.1}$$

dove $\mathcal{O}_K^*$ è il gruppo moltiplicativo delle unità di $\mathcal{O}_K$ che è dato dal prodotto diretto tra un gruppo ciclico finito generato dalle radici delle unità contenute in K ed un infinito gruppo libero di rango $r = r_1 + r_2 - 1$, che è isomorfo al prodotto diretto di r copie del gruppo additivo $\mathbb{Z}$ (Teorema sulle unità di Dirichlet, [22] p.114). Per la Proposizione 2.18 (1),

possiamo dedurre che $m_{\overline{K}}$ è costante sugli elementi appartenenti alla stessa orbita. Infatti, sia $x \in H$ e sia $y \in \mathrm{Orb}(x) = \{\Phi(\epsilon) \cdot x \ : \ \epsilon \in \mathcal{O}_K^*\}$. Si ha che

$$m_{\overline{K}}(y) = m_{\overline{K}}(\Phi(\epsilon) \cdot x) = m_{\overline{K}}(x).$$

Si dimostra inoltre che $\mathrm{Orb}(x)$ è finita se e soltanto se $x \in \Phi(K)$. Sia $\epsilon \in \mathcal{O}_K^*$, poniamo $\nu = (\nu_i)_{1 \le i \le n} = \Phi(\epsilon)$, dove Φ è definita in (2.1). Consideriamo un parallelepipedo problematico $\mathcal{P}$ e la sua immagine mediante l'azione dell'unità $\epsilon \in \mathcal{O}_K^*$, consideriamo, cioè:

$$\Phi(\epsilon) \cdot \mathcal{P} = \nu \cdot \mathcal{P} = \{\nu \cdot x, \ x \in \mathcal{P}\}.$$

Anche $\nu \cdot \mathcal{P}$ è un parallelepipedo, le cui facce sono ortogonali agli assi di $\mathbb{R}^n$ ed è contenuto in un dominio $\mathcal{B} \subseteq H$. A questo punto vogliamo traslare il parallelepipedo $\nu \cdot \mathcal{P} \subseteq \mathcal{B}$ in $\mathcal{F}$ tramite un vettore cosiddetto di traslazione.

Definizione 3.14. Un elemento $z \in \Phi(\mathcal{O}_K)$ si dice **vettore di traslazione** di $\mathcal{B}$ in $\mathcal{F}$ se $(\mathcal{B} - z) \cap \mathcal{F} \neq \emptyset$.

Si controlla se il traslato di $\nu \cdot \mathcal{P}$ nel dominio fondamentale $\mathcal{F}$ sia contenuto nell'insieme $\{x \in \mathcal{F} \ : \ m_{\overline{K}}(x) < k\}$. Se così fosse per ogni $x \in \mathcal{P}$ si avrebbe $m_{\overline{K}}(x) = m_{\overline{K}}(\nu \cdot x - z_x) < k$, quindi $\mathcal{P}$ può essere scartato. Supponiamo che $\{\mathcal{Q}^{(i)}, \ 1 \le i \le l\}$ sia un ricoprimento di $\mathcal{F}$, tale che per ogni $1 \le i \le l$, $\mathcal{Q}^{(i)}$ sia un parallelepipedo di centro $c^{(i)}$ e raggio $h^{(i)}$. Supponiamo che esista un intero $1 \le m \le l$ tale che per ogni $m < i \le l$, il parallelepipedo $\mathcal{Q}^{(i)}$ sia assorbito da qualche intero (questo vuol dire che i primi m parallelepipedi $\mathcal{Q}^{(i)}$ sono tutti problematici).

Lemma 3.15. *Sia $\{z^{(j)}, 1 \le j \le k\} \subseteq \Phi(\mathcal{O}_K)$ la lista di vettori di traslazione di $\mathcal{B}$ in $\mathcal{F}$. Se per ogni $1 \le j \le k, \ 1 \le i \le m$, $(\mathcal{B} - z^{(j)}) \cap \mathcal{Q}^{(i)} = \emptyset$, allora $\mathcal{P}$ può essere scartato dalla lista dei parallelepipedi problematici.*

Questo procedimento prende il nome di **Test delle unità**. Diamo ora alcune definizioni.

Definizione 3.25. Un camminio infinito $(v_i)_{i \ge 0}$ si dice **fondamentalmente periodico** se esistono interi razionali $r \ge 0, \ p \ge 1$ tali che

$$\text{per ogni } \ i \ge r, \ v_{i+p} = v_i.$$

Definizione 3.26. Un grafo orientato $\mathcal{G}$ si dice **conveniente** se ogni cammino infinito di $\mathcal{G}$ è fondamentalmente periodico.

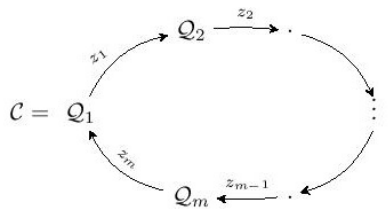
Equivalentemente un grafo è conveniente se ogni coppia di cicli semplici del grafo $\mathcal{G}$

non ha vertici in comune. In che modo colleghiamo questa nuova nozione di grafo conveniente con i parallelepipedi problematici $(\mathcal{Q}_i)_{1\leq i\leq m}$ che rimangono in seguito ad aver applicato il Test delle unità?
Costruiamo un grafo orientato $\mathcal{G}$ i cui vertici siano proprio i parallelepipedi problematici $(\mathcal{Q}_i)_{1\leq i\leq m}$ ed in cui gli archi orientati siano

$$\mathcal{Q}_i \xrightarrow{z} \mathcal{Q}_j$$

se $(\Phi(\epsilon)\cdot\mathcal{Q}_i - z)\cap\mathcal{Q}_j \neq \emptyset$, per qualche $z\in\Phi(O_K)$. Questo è un grafo conveniente $\mathcal{G}$ e possiede dei cicli semplici che denotiamo con $(\mathcal{C}_i)_{1\leq i\leq l}$.

Teorema 3.29. *Sia $\mathcal{C}$ un ciclo semplice di $\mathcal{G}$. Siano $\mathcal{Q}_1,..,\mathcal{Q}_m$ i vertici di $\mathcal{C}$ e siano m gli elementi $z_1=\Phi(Z_1),...,z_m=\Phi(Z_m)$ di $\Phi(\mathcal{O}_K)$ tali che*



Allora, se definiamo $\Omega_{\mathcal{C}}=\sum_{j=0}^{m}\epsilon^j z_{m-j}\in\mathcal{O}_K$, $\xi_{\mathcal{C}}=\frac{\Omega_{\mathcal{C}}}{\epsilon^m-1}$ e $t=\Phi(\xi_{\mathcal{C}})$, avremo che per ogni $x\in\bigcup_{i=1}^{m}\mathcal{Q}_i$ tale che $m_{\overline{K}}(x)\geq k$,

1. *$k\leq m_{\overline{K}}(x)\leq m_{\overline{K}}(t)$,*
2. *se $x\in\Phi(K)$, allora $x=t$.*

Tramite questo Teorema è possibile associare ad ogni ciclo semplice $\mathcal{C}$ di $\mathcal{G}$ un punto $t\in\Phi(K)$ tale che per ogni elemento x nelle regioni descritte dai vertici di $\mathcal{C}$, $m_{\overline{K}}(x)\leq m_{\overline{K}}(t)$ e $k<m_{\overline{K}}(t)$. Ricordando che $m_{\overline{K}}$ è costante sugli elementi appartenenti alla stessa orbita rispetto all'azione (3.1) e che l'orbita di un elemento di $\Phi(K)$ è sempre finita, allora ogni elemento t_i appartenente all'orbita di t è tale che $m_{\overline{K}}(t_i)=m_{\overline{K}}(t)>k$. Quindi avremmo trovato un numero finito di elementi $t\in\mathcal{F}$ tali che $m_{\overline{K}}(t)>k$. Per il Teorema 3.29 ad ogni ciclo $\mathcal{C}$ del grafo $\mathcal{G}$ possiamo associare un elemento $t\in\Phi(\mathcal{O}_K)$. Sia $m(\mathcal{C})=m_{\overline{K}}(t)=m_{\overline{K}}(t_i)$ per ogni $t_i\in\mathrm{Orb}(t)$. Il più grande valore di $m_{\mathcal{C}}$ al variare di tutti i cicli semplici del grafo $\mathcal{G}$ è il valore del Minimo Euclideo $M(K)$.
Ricapitolando: ad ogni passo si considerano 3 numeri reali $k_0,\ k,\ k_1$, tali che

1. $k_0 < k < k_1$,
2. $M(K) < k_1$,
3. $k_0 < M(K)$, con molta probabilità.

Dopodiché applichiamo il test di assorbimento (Algoritmo 3.4) ed il test delle unità (Algoritmo 3.5) per qualche k tale che $k_0 < k < k_1$. Se con questo procedimento

riusciamo a scartare tutti i parallelepipedi problematici, allora $M(K) < k$, e possiamo reiniziare il procedimento ponendo $k_1 = k$. In caso contrario, non possiamo essere certi che $k < M(K)$. Tuttavia proviamo a costruire un grafo conveniente, e se questo tentativo fallisce, riapplichiamo i test di assorbimento e quello delle unità con $k_0 = k$, in modo tale che, con molta probabilità, $k_0 < M(K)$.
Questo algoritmo richiede un valore iniziale $\mathcal{K}$ per k, e poiché il test di assorbimento può essere molto lungo nel caso in cui rimangano molti parallelepipedi problematici, allora scegliamo un grande valore per $\mathcal{K}$.
Una volta fissati i valori k_0 e k_1, in che modo scegliamo k?
Sia $d \in (0, 1)$ e si ponga $k = (1 - d)k_0 + dk_1$. Si decide un il criterio secondo il quale termineremo il taglio dei parallelepipedi e l'applicazione del test di assorbimento e quello delle unità. In pratica, si fissa un intero $\mathcal{I}$ e se dopo $\mathcal{I}$ tagli consecutivi il numero di parallelepipedi problematici non subisce una variazione, allora ci fermiamo. L'algoritmo fallisce nel caso non si riesca a costruire un grafo conveniente. In questo caso, esiste un valore di soglia, k_2, tale che:

- se $k > k_2$ allora tutti i problemi vengono "assorbiti",
- se $k < k_2$, rimangono alcuni problemi e non si riesce a trovare un grafo conveniente.

In questo modo k_0 e k_1 sarebbero vicini a k_2. Per evitare che l'algoritmo non termini più, si fissa un valore $\varepsilon > 0$ tale che se $k_1 - k_0 < \varepsilon$, allora l'algoritmo termina restituendo "failure". In un certo senso ε rappresenta la precisione del test di assorbimento. Nel caso riuscissimo a trovare un grafo conveniente rispetto al valore k, potremmo usare k_1 come maggiorazione dall'alto di $M(K)$ per calcolare il Minimo Euclideo Locale dei punti associati ai cicli semplici. Inoltre, se in un qualsiasi momento otteniamo $k_1 < 1$, allora possiamo concludere che K è Euclideo rispetto alla norma.