Teoria Algebrica dei Numeri I

Prof.ssa Ilaria Del Corso

Anno Accademico 2014/2015

Appunti di Carlo Sircana

Indice

Capitolo 1

Anelli degli Interi, Traccia e Discriminante

1.1 Estensioni intere

Siamo ora interessati a studiare le intersezioni dei campi di numeri K, cioè estensioni finite di $\mathbb{Q}$, con il sottoinsieme di $\bar{\mathbb{Q}}$ formato dalle radici di polinomi monici a coefficienti interi, in analogia con quanto viene fatto solitamente in teoria dei campi. Generalizziamo quindi la nozione di elemento algebrico nel caso di estensioni di anelli:

Definizione 1.1. Siano $A \subseteq B$ anelli. $x \in B$ si dice intero su A se esiste un polinomio monico $f \in A[t]$ che si annulla in x.

Discende direttamente dalla definizione che le potenze di un elemento intero sono dipendenti sull'anello. Se $a \in B$ è intero su A, allora definitivamente a^n appartiene all'A-modulo generato dalle potenze a^k con $k \leq n-1$; in particolare questo significa che l'A-modulo $A[a]$ è finitamente generato su A. Diamo ora delle definizioni equivalenti di elemento intero:

Proposizione 1.2. Siano $A \subseteq B$ anelli. Sono equivalenti:

- x è intero su A
- $A[x]$ è un A-modulo finitamente generato.
- Esiste un anello C tale che $A[x] \subseteq C$ e C è finitamente generato su A (come A-modulo)
- Esiste un $A[x]$-modulo fedele M finitamente generato come A-modulo

Dimostrazione.

(1) $\Rightarrow$ (2) Sappiamo che $A[x]$ è generato da $\langle 1, x, x^2, \ldots, x^n \rangle$, dove $n+1$ è il grado di una relazione di dipendenza intera di x su A.

(2) $\Rightarrow$ (3) É sufficiente considerare $C = A[x]$.

(3) $\Rightarrow$ (4) Mostriamo che $M = C$ soddisfa le richieste. Chiaramente C è un $A[x]$-modulo; vogliamo mostrare che è fedele, cioè che $\mathrm{Ann}_{A[x]}(M) = \{0\}$. Notiamo che $a \cdot 1 = a$ per ogni $a \in A[x]$ e dunque l'annullatore è banale.

(4) $\Rightarrow$ (1) Consideriamo l'omomorfismo di A-moduli

$$\begin{array}{rccc} \phi\colon & M & \longrightarrow & M \\ & m & \longmapsto & xm \end{array}$$

Poiché M è fedele, ϕ è non nulla. M è finitamente generato su A e possiamo scegliere dei generatori $M = \langle m_1, \ldots, m_s \rangle$. Possiamo costruire la matrice associata a ϕ, (a_{ij}), rispetto ai generatori scelti e considerarne il polinomio caratteristico $p(t)$. p è monico per definizione e si annulla in ϕ

$$p(\phi)(m) = (\phi^s + \sum b_i \phi^i)m = 0 \ \forall m \in M$$

D'altronde, questo è equivalente a

$$(x^s + \sum b_i x^i)(m) = 0$$

e per fedeltà di M come $A[x]$-modulo, $x^s + \sum b_i x^i = 0$ in B. Questo fornisce una relazione di dipendenza intera di x su A, come voluto.

□

Corollario 1.3. Siano $A \subseteq B$ anelli. Allora B è finitamente generato come A-modulo se e solo se $B = A[x_1, \ldots, x_n]$ è finitamente generato come A-algebra e x_i è intero su A per ogni i.

Dimostrazione. Un'implicazione è ovvia: se B è finitamente generato come A-modulo, lo è come algebra ; inoltre ogni generatore appartiene a B che è finitamente generato come A-modulo. Per il punto 3 della precedente Proposizione è intero.
Viceversa, procediamo per induzione. Se $B = A[x]$, per la Proposizione precedente x è intero e dunque B è finitamente generato su A. Supponiamo vera la tesi per $n-1$ e dimostriamola per n. Per ipotesi induttiva, $B' = A[x_1, \ldots, x_{n-1}]$ è finitamente generato su A e x_n è intero su B'. Quindi B è finitamente generato su B' e di conseguenza B è finitamente generato su A (è generato dai prodotti dei generatori). □

Corollario 1.4. Siano $A \subseteq B$. Allora $C = \{x \in B \mid x \text{ è intero su } A\}$ (chiusura integrale di A in B) è un sottoanello di B che contiene A.

Dimostrazione. Che contenga A è ovvio. Siano $x, y \in C$; mostriamo che $x + y$ e xy appartengono a C. D'altronde, x, y sono interi su A e $A[x, y]$ è un A-modulo finitamente generato. Allora per il punto 3 della Proposizione, tutti i suoi elementi sono interi su A. Dunque $x + y, xy$ sono interi su A. □

Dunque gli elementi di $\bar{\mathbb{Q}}$ che sono interi su $\mathbb{Z}$ formano un anello, $\mathbb{A}$. Lo stesso vale intersecando quest'ultimo con un campo di numeri, $\mathcal{O}_K = K \cap \mathbb{A}$. Chiamiamo questi anelli anelli di interi.

Definizione 1.5. B è intero su A se ogni $x \in B$ è intero su A.
A si dice integralmente chiuso in B se coincide con la sua chiusura integrale in B.
Se A è un dominio, diciamo che A è integralmente chiuso se lo è nel suo campo delle frazioni.

Proposizione 1.6. Se $A \subseteq B$ e $B \subseteq C$ sono estensioni intere, allora $A \subseteq C$ è intera.

Dimostrazione. Sia $\alpha \in C$. Sicuramente α è intero su B, quindi esistono $b_0, b_1 \ldots, b_{n-1} \in B$ tali che:

$$\alpha^n + \sum_{i=0}^{n-1} b_i \alpha^i = 0$$

Sia allora $B' = A[b_0, \ldots, b_{n-1}]$; per costruzione α è intero su B'. Inoltre B' è finitamente generato come A-algebra e i generatori sono interi su A e dunque è finitamente generato come A-modulo. Inoltre $B'[\alpha]$ è finitamente generato su B' perchè α è intero su B'. Dunque $B'[\alpha]$ è un A-modulo finitamente generato. Per la proposizione precedente, α è intero su A. □

Questa proposizione determina la transitività delle estensioni intere.

Corollario 1.7. Sia C la chiusura integrale di A in B. Allora C è integralmente chiusa in B.

Dimostrazione. Se $\alpha \in B$ è intero su C, per transitività è intero anche su A e di conseguenza appartiene anche a C. □

Esempio. Sia $\mathbb{A}$ la chiusura integrale di $\mathbb{Z}$ in $\mathbb{C}$. Sia K un campo di numeri; allora $\mathcal{O}_K = K \cap \mathbb{A}$ è la chiusura integrale di $\mathbb{Z}$ in K. Per il corollario, $\mathcal{O}_K$ è integralmente chiuso in K, che è il suo campo delle frazioni. Chiamiamo $\mathcal{O}_K$ il campo degli interi di K.

Osservazione 1.8. Sia A un UFD. Allora A è integralmente chiuso nel suo campo dei quozienti K. Infatti, sia $\alpha = \beta/\gamma$ un elemento di K; possiamo supporre $(\beta, \gamma) = 1$. Se α è intero su A, esiste una relazione di dipendenza

$$\alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i = 0 \Longrightarrow \frac{\beta^n}{\gamma^n} + \sum_{i=0}^{n-1} a_i \frac{\beta^i}{\gamma^i} = 0$$

da cui segue

$$\beta^n + \sum_{i=0}^{n-1} a_i \beta^i \gamma^{n-i} = 0$$

Dunque $\gamma \mid \beta^n$, da cui $\gamma = 1$. Come voluto, $\alpha \in A$.
Si incontrano facilmente anelli non integralmente chiusi: $\mathbb{Z}[\sqrt{5}]$ è intero su $\mathbb{Z}$ ma non è integralmente chiuso, perché il suo campo dei quozienti è $\mathbb{Q}(\sqrt{5})$ e $\mathcal{O}_K = \mathbb{Z}[1 + \sqrt{5}/2] \supsetneq \mathbb{Z}[\sqrt{5}]$. Invece, l'anello $\mathbb{Z}[\sqrt{-5}]$ è invece integralmente chiuso ma non è UFD. Infatti $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. 2 è irriducibile perché se per assurdo si scrivesse come prodotto

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

passando alle norme si otterrebbe

$$4 = (a^2 + 5b^2)(c^2 + 5d^2)$$

Poichè questi sono elementi di $\mathbb{Z}$, per non essere una fattorizzazione banale entrambi i fattori dovrebbero avere modulo 2. D'altronde $a^2 + 5b^2 = 2$ non ha soluzioni in $\mathbb{Z}$ e quindi 2 è irriducibile. 2 non è primo, perchè $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ ma non divide nessuno dei fattori, perchè

$$\frac{1+\sqrt{-5}}{2} \notin \mathcal{O}_K$$

Proposizione 1.9. Sia A un dominio integralmente chiuso e sia K il suo campo dei quozienti. Allora $\alpha \in \bar{K}$ è intero su A se e solo se il polinomio minimo di α su K appartiene a $A[x]$.

Dimostrazione. Se il polinomio minimo di α su K è a coefficienti in A allora α è intero su A.
Viceversa, sia a intero su A e sia

$$p(t) = t^n + \sum a_i t^i$$

una relazione di interezza di grado minimo. Sia μ_a il polinomio minimo di a su K. Se mostriamo che ogni radice del polinomio minimo μ_a è intera su A, allora il polinomio minimo è a coefficienti in A. Infatti i coefficienti sarebbero combinazioni delle radici e dunque sarebbero elementi interi su A appartenenti a K; ma A è integralmente chiuso in K e dunque sarebbe a coefficienti in A. Questo è chiaro visto che per definizione di polinomio minimo $\mu_a \mid p$ e dunque ogni radice di μ_a è anche radice di p. Di conseguenza p è una relazione di interezza per ogni radice di μ_a da cui la tesi. □

1.2 Traccia e Norma

Introduciamo ora due strumenti per studiare le estensioni di anelli. Sia F/K un'estensione separabile di grado n. Per separabilità dell'estensione, esistono n immersioni $\sigma_1, \ldots, \sigma_n$ di F/K in $\bar{F}$.

Definizione 1.10. Definiamo la traccia $\mathrm{Tr}_{F/K}$

$$\begin{array}{rccc} \mathrm{Tr}_{F/K}: & F & \longrightarrow & K \\ & a & \longrightarrow & \sum_{i=1}^n \sigma_i(a) \end{array}$$

e la norma

$$\begin{array}{rccc} N_{F/K}: & F & \longrightarrow & K \\ & a & \longmapsto & \prod_{i=1}^n \sigma_i(a) \end{array}$$

A priori, le funzioni non sono ben definite perché abbiamo indicato come codominio K; in realtà

Proposizione 1.11. $\mathrm{Tr}_{F/K}$ e $N_{F/K}$ sono ben definite e l'immagine è K.
Se K, F sono campi di numeri e $\alpha \in \mathcal{O}_F$, allora la norma e la traccia appartengono a $\mathcal{O}_K$.

Dimostrazione. Sia $L = K(\alpha)$; allora $[L : K] = d \mid n = [F : K]$. Per separabilità, esistono $\tau_1, \dots, \tau_d$ immersioni di L in $\bar{L}$; per definizione $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{d} \tau_i(\alpha)$ e $N(\alpha) = \prod_{i=1}^{d} \tau_i(\alpha)$ sono elementi di K perchè sono coefficienti del polinomio minimo. In generale, sappiamo che $\mathrm{Tr}_{F/K}(\alpha) = \sum \sigma_i(\alpha)$, ogni τ_i si estende a F in n/d modi e le estensioni sono esattamente le σ_i. Allora $\mathrm{Tr}_{F/K}(\alpha) = (n/d)\,\mathrm{Tr}_{L/K}(\alpha)$. Per la norma, $N_{F/K}(\alpha) = N_{L/K}(\alpha)^{n/d}$. Se α è intero, i coefficienti del polinomio minimo sono in $\mathcal{O}_K$ perché il polinomio minimo di α appartiene a $\mathcal{O}_K[x]$. □

La traccia e la norma soddisfano le formule

$$\mathrm{Tr}(a+b) = \mathrm{Tr}(a) + \mathrm{Tr}(b) \qquad \mathrm{Tr}(\lambda a) = \lambda\,\mathrm{Tr}(a)$$
$$N(ab) = N(a)N(b) \qquad N(\lambda a) = \lambda^n N(a)$$

Proposizione 1.12. Siano $K \subseteq F \subseteq M$ campi. Allora

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{M/F} \quad e \quad N_{M/F} = N_{F/K} \circ N_{M/F}$$

Dimostrazione. Siano $\sigma_1, \dots, \sigma_n$ le immersioni di F/K in $\bar{M}$ e siano $\tau_1, \dots, \tau_m$ le immersioni di M/F in $\bar{M}$. Verifichiamo che le funzioni coincidono su ogni elemento; sia quindi $\alpha \in M$. Per definizione,

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{M/F}(\alpha)) = \mathrm{Tr}_{F/K}\Big(\sum_{j=1}^{m} \tau_j(\alpha)\Big) = \sum_{i=1}^{n} \sigma_i\Big(\sum_{j=1}^{m} \tau_j(\alpha)\Big)$$

Vorremmo distribuire i σ_i sulla somma; purtroppo, i singoli elementi della somma non appartengono a F. Sia allora N la chiusura normale di M su K in una fissata chiusura algebrica $\overline{M}$. Possiamo estendere gli omomorfismi τ_j, σ_i a N, ottenendo $\tilde{\tau_j} \colon N \to N$, $\tilde{\sigma_i} \colon N \to N$ (scegliamo arbitrariamente una delle possibili estensioni). Dunque $\tilde{\tau}_j$ e $\tilde{\sigma}_i$ appartengono al gruppo di Galois $\mathrm{Gal}(N/K)$; posso comporle e $\tilde{\sigma}_i \circ \tilde{\tau}_j$ sono nm elementi del gruppo. Mostriamo che sono distinti; supponiamo che

$$\tilde{\sigma}_i \circ \tilde{\tau}_j = \tilde{\sigma}_h \circ \tilde{\tau}_k$$

Sia $\beta \in F$; allora

$$\tilde{\sigma}_i \circ \tilde{\tau}_j(\beta) = \tilde{\sigma}_h \circ \tilde{\tau}_k(\beta) \Longrightarrow \tilde{\sigma}_i(\beta) = \tilde{\sigma}_h(\beta)$$

perché per ipotesi le immersioni τ_i fissano F; ma dato che l'ultima uguaglianza vale per ogni $\beta \in F$, si ha $i = h$, da cui l'uguaglianza anche di j e k (sono automorfismi, è sufficiente comporre per l'inversa). Allora

$$\begin{aligned}
\mathrm{Tr}_{M/K}(\alpha) &= \sum_{i=1}^{n}\sum_{j=1}^{m} \tilde{\sigma}_i(\tilde{\tau}_j(\alpha)) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{m} \tilde{\sigma}_i(\tau_j(\alpha)) \\
&= \sum_{i=1}^{n} \tilde{\sigma}_i\Big(\sum_{j=1}^{m} \tau_j(\alpha)\Big) \\
&= \sum_{i=1}^{n} \sigma_i(\mathrm{Tr}_{M/F}(\alpha)) \\
&= \mathrm{Tr}_{F/K}(\mathrm{Tr}_{M/F}(\alpha))
\end{aligned}$$

□

Proposizione 1.13. Sia F/K una estensione di campi e sia $\alpha \in F$. Consideriamo l'applicazione φ_α la moltiplicazione per α. Allora vale

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\varphi_\alpha) \qquad\qquad N(\alpha) = \det(\varphi_\alpha)$$

Dimostrazione. Sia $L = K(\alpha)$ e consideriamo la base $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ di L su K. In questa base, la matrice di moltiplicazione per α è la matrice compagna del polinomio minimo di α. Più esplicitamente, detto $\mu_\alpha(x) = \sum a_i x^i$,

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

In particolare, $\det(A) = (-1)^n a_0$ e $\mathrm{Tr}(A) = -a_{n-1}$ e dunque il questo caso si ha l'uguaglianza. Sia ora $x_1, \ldots, x_s$ una base di F su L; allora

$$\mathcal{B} = \{x_1, \alpha x_1, \ldots \alpha^{n-1} x_1, \ldots, x_n, \ldots, \alpha^{n-1} x_s\}$$

è una base di F su K e, ordinata in questo modo, la matrice di moltiplicazione risulta essere una matrice diagonale a blocchi:

$$B = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}$$

Di conseguenza, $\det(B) = \det(A)^s$ e $\mathrm{Tr}(B) = s\,\mathrm{Tr}(A)$, da cui la tesi. □

Sia K un campo di numeri e consideriamo l'anello degli interi $\mathcal{O}_K$; vogliamo studiare il gruppo delle unità $\mathcal{O}_K^*$. La prima osservazione è la seguente:

Proposizione 1.14. $\alpha \in \mathcal{O}_K^*$ se e solo se $N(\alpha) = \pm 1$.

Dimostrazione. Supponiamo dapprima che $\alpha \in \mathcal{O}_K^*$; per definizione esiste β tale che $\alpha\beta = 1$. Applicando la norma, $N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta) = 1$. Entrambi i fattori sono in $\mathbb{Z}$ e dunque $N(\alpha) = \pm 1$ e $N(\beta) = \pm 1$.
Viceversa, supponiamo che α abbia norma unitaria e siano $\sigma_1, \ldots, \sigma_n$ le immersioni di K su $\mathbb{Q}$.

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \prod_{\substack{i=1 \\ \sigma_i \neq \mathrm{Id}}}^{n} \sigma_i(\alpha) = \pm 1$$

Basta mostrare che l'ultimo fattore è intero. D'altronde,

$$\beta = \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha) = \pm \frac{1}{\alpha} \in K$$

e $\prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha)$ è intero su $\mathbb{Z}$, perchè prodotto di interi algebrici (tali elementi hanno lo stesso polinomio minimo di α). □

Per esempio, studiamo il caso $k = \mathbb{Q}(\sqrt{-m})$, con $m > 0$ e libero da quadrati. Sia $\alpha \in \mathcal{O}_k^*$. Allora $N(\alpha) = \pm 1$, cioè $\alpha\bar{\alpha} = \pm 1$ e dunque, se $\alpha = a + b\sqrt{-m}$, $N(\alpha) = a^2 + mb^2$. Gli invertibili sono allora solo le radici dell'unità.

Esempio. Consideriamo ora il campo di numeri $k = \mathbb{Q}(\sqrt{2})$ e il corrispondente anello degli interi $\mathcal{O}_k = \mathbb{Z}[\sqrt{2}]$. Mostriamo che il gruppo degli invertibili è isomorfo a $\mathcal{O}_k^* \simeq \mathbb{Z} \oplus \mathbb{Z}/(2)$. Individuiamo un elemento di ordine infinito. Dato un elemento $\alpha = a + b\sqrt{2} \in \mathcal{O}_k$, la sua norma è $N(\alpha) = a^2 - 2b^2$. Per trovare gli invertibili, in base alla proposizione, è sufficiente trovare gli $\alpha \in \mathcal{O}_k$ tali che $N(\alpha) = 1$. Una soluzione a tale equazione è $\alpha = 1 + \sqrt{2}$ che dunque è invertibile e ha ordine infinito. Mostriamo che $\mathcal{O}_k^* \simeq \langle 1 + \sqrt{2}, -1 \rangle$, cioè che ogni $\epsilon \in O_k^*$ si può scrivere come $\epsilon = \pm(1 + \sqrt{2})^k$. Possiamo supporre $\epsilon > 1$, a meno di prendere il coniugato, e osserviamo che non è possibile che $1 < \epsilon < 1 + \sqrt{2}$. Infatti, sia $\epsilon = x + y\sqrt{2}$. Dato che ϵ è invertibile, ha norma unitaria e dunque

$$(x + y\sqrt{2})(x - y\sqrt{2}) = \pm 1$$

da cui si ottiene $x - y\sqrt{2} \in (-1, 1)$. Sommando ϵ e il suo coniugato arriviamo alla relazione $0 < 2x < 2 + \sqrt{2}$. Di conseguenza, $x = 1$ e $\epsilon = 1 + \sqrt{2}y$; ma per motivi di norma non può esistere un elemento invertibile di questa forma. Dunque $\epsilon > 1 + \sqrt{2}$.
Mostriamo allora che ϵ è della forma voluta. Se $\epsilon \neq (1 + \sqrt{2})^k$ non fosse della forma voluta, allora esisterebbe $k \in \mathbb{N}$ tale che $(1 + \sqrt{2})^k < \epsilon < (1 + \sqrt{2})^{k+1}$. Quindi l'elemento

$$\frac{\epsilon}{(1 + \sqrt{2})^k}$$

sarebbe invertibile e compreso tra 1 e $1 + \sqrt{2}$, da cui un assurdo.

1.3 Caratteri

Definizione 1.15. Sia G un gruppo e K un campo. Un carattere è un omomorfismo di gruppi $\chi \colon G \to K^*$.

Notiamo che in generale la somma di caratteri non è un carattere, ma è comunque una applicazione ben definita a valori in K.

Teorema 1.16 (di indipendenza dei caratteri di Artin)**.** Siano $\chi_1, \ldots, \chi_n$ caratteri distinti a valori in K^*. Allora sono linearmente indipendenti su K.

Dimostrazione. Per assurdo, supponiamo di avere n caratteri $\chi_1, \ldots, \chi_n$ distinti linearmente dipendenti

$$\sum_{i=1}^{n} a_i \chi_i \equiv 0$$

Possiamo supporre che sia la relazione di dipendenza di lunghezza minima. In particolare, ogni coefficiente a_i è non nullo. Per definizione, quindi, per ogni $g \in G$,

$$\sum_{i=1}^{n} a_i \chi_i(g) = 0 \tag{1.1}$$

Sia $h \in G$ tale che $\chi_1(h) \neq \chi_2(h)$ (esiste perchè sono distinti). Applichiamo la relazione a gh:

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_2(h) + \sum a_i\chi_i(g)\chi_i(h) = 0 \tag{1.2}$$

Moltiplicando la relazione 1.1 per $\chi_1(h)$, otteniamo l'equazione

$$\sum a_i\chi_i(g)\chi_1(h) = 0 \tag{1.3}$$

Sottraendo membro a membro le relazioni 1.2 e 1.3, ricaviamo una relazione più corta

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \cdots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) = 0$$

Dunque, è sufficiente mostrare che tale relazione è non banale. Per costruzione, $a_2(\chi_2(h) - \chi_1(h)) \neq 0$ e quindi otteniamo la relazione

$$\sum_{i=2}^{n} a_i(\chi_1(h) - \chi_i(h))\chi \equiv 0$$

e questo è assurdo. □

Vogliamo applicare il teorema alla funzione traccia; la traccia è una applicazione K-lineare da L in K ed è dunque un funzionale; di conseguenza è surgettiva se e solo se non nulla.

Corollario 1.17. Sia L/K una estensione separabile. Allora l'applicazione $\mathrm{Tr}_{L/K}$ è non nulla e dunque surgettiva.

Dimostrazione. Per definizione, la traccia è l'applicazione

$$\mathrm{Tr}_{L/K} = \sum_{i=1}^{n} \sigma_i$$

Dato che ogni σ_i è un omomorfismo di campi, è iniettivo e dunque si può restringere $\sigma_i \colon L^* \to \bar{K}^*$; dunque ogni immersione è un carattere. Per il teorema di indipendenza dei caratteri, dato che le immersioni σ_i sono distinte, otteniamo $\mathrm{Tr}_{L/K} \neq 0$. □

Osservazione 1.18. In realtà vale anche il viceversa, ma serve definire la traccia per estensioni non separabili.

Consideriamo ora l'applicazione bilineare

$$\begin{array}{ccc} L \times L & \to & K \\ (x, y) & \mapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

Notiamo che è non degenere, in quanto fissato un elemento $x \in L$ esiste sempre $y \in L$ tale che $\mathrm{Tr}(xy) \neq 0$. Infatti, esiste $z \in L$ tale che $\mathrm{Tr}(z) \neq 0$ e dunque è sufficiente scegliere $y = x^{-1}z$. Tale applicazione induce l'isomorfismo tra L e il suo duale L^*

$$\begin{array}{cccc} \phi & L & \longrightarrow & L^* \\ & x & \longmapsto & \mathrm{Tr}(x\,\cdot) \end{array}$$

Sia $\alpha_1, \ldots, \alpha_n$ una base di L; chiamo $f_1, \ldots f_n \in L^*$ la sua base duale determinata dalla proprietà che

$$f_i(\alpha_j) = \delta_{ij}$$

Per ogni i, chiamiamo $\beta_i = \phi^{-1}(f_i)$ e vale $\mathrm{Tr}_{L/K}(\alpha_i\beta_j) = \delta_{ij}$.

Definizione 1.19. Sia M un A-modulo finitamente generato. M si dice libero se esiste n tale che $M \simeq A^n$.
Definiamo tale n come rango del modulo n.

Ogni modulo libero ammette per definizione una base di n elementi. Nonostante questo valga per gli spazi vettoriali, non è vero sottomodulo di un modulo libero non è libero. Per esempio, dato A un anello, se ogni ideale fosse libero, allora $I = (a)$; per trovare un controesempio è sufficiente allora considerare un anello non a ideali principali, per esempio $\mathbb{Z}[x]$. Per i PID valgono però il seguente:

Teorema 1.20. Sia A un PID e sia F un A-modulo libero. Allora ogni sottomodulo M di F è libero e $\mathrm{rk}(M) \leq \mathrm{rk}(F)$.

Teorema 1.21. Sia A un PID, sia F un A-modulo libero finitamente generato e sia M un suo sottomodulo. Allora esiste una base $\mathcal{B}$ di F (che d'ora in poi chiameremo base diagonale), $e_1, \dots e_n \in \mathcal{B}$ e $a_1, \dots a_n \in A$ tali che

- $a_1 e_1, \dots, a_n e_n$ sia una base di M
- $a_i \mid a_{i+1}$ per ogni i.

Inoltre $(a_1), \dots (a_n)$ sono univocamente determinati.

Corollario 1.22. Sia A un PID e sia M un A-modulo finitamente generato. Allora M è isomorfo a

$$A^r \bigoplus \left(\oplus_{i=1}^{r} {}^{A}\!/_{(a_i)} \right)$$

dove $a_i \mid a_{i+1}$ e r e (a_i) sono univocamente determinati.

Parziale. Dato che M è finitamente generato, esiste un omomorfismo surgettivo $A^n \to M$; per i teoremi di isomorfismo,

$$M \simeq {}^{A^n}\!/_{R}$$

dove R è il nucleo dell'omomorfismo $A^n \to M$ indotto dalla scelta di un insieme di generatori. Dato che A è PID, R è libero ed esiste una base diagonale come nel teorema 1.21. Detta $\mathcal{B} = \{w_1, \dots w_n\}$ tale base, ricaviamo una base $\mathcal{D} = \{a_1 w_1, \dots, a_s w_s\}$. Dunque

$$ {}^{A^n}\!/_{R} \simeq A^{n-s} \oplus \left(\bigoplus_{i=1}^{s} {}^{A}\!/_{(a_i)} \right)$$

□

Struttura di $\mathcal{O}_k$ Utilizzando questi risultati, possiamo dimostrare il seguente enunciato sulla struttura additiva degli anelli di interi:

Teorema 1.23. Sia k un campo dei numeri e supponiamo $[k : \mathbb{Q}] = n$. Allora $\mathcal{O}_k$ è uno $\mathbb{Z}$-modulo libero di rango n.

Dimostrazione. Mostriamo che esistono due $\mathbb{Z}$-moduli A, B tali che $A \subseteq \mathcal{O}_k \subseteq B$ e che A, B siano liberi di rango n. Se esistessero, infatti,

- $\mathcal{O}_k$ sarebbe libero perchè sottomodulo del modulo libero B su $\mathbb{Z}$, che è un PID (per il teorema 1.20).
- $\mathcal{O}_k \subseteq B$ avrebbe rango $\leq n$ perché contenuto in B
- $\mathcal{O}_k \supseteq A$ avrebbe rango $\geq n$ perché contiene A

e dunque la tesi seguirebbe.
Costruiamo prima A. Per il teorema dell'elemento primitivo, esiste $\alpha \in K$ tale che $K = \mathbb{Q}(\alpha)$. Possiamo supporre, a meno di moltiplicazione per un elemento di $\mathbb{Z}$, che $\alpha \in \mathcal{O}_k$ sia intero su $\mathbb{Z}$. Di conseguenza $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_k$ e possiamo scegliere $\mathbb{Z}[\alpha] = A$. Infatti, $1, \alpha, \ldots, \alpha^{n-1}$ sono generatori su $\mathbb{Z}$ di A e sono indipendenti su $\mathbb{Z}$ (lo sono su $\mathbb{Q}$).
Costruiamo ora B. Sia $\alpha_1, \ldots, \alpha_n$ una $\mathbb{Q}$-base di k; posso supporre che $\alpha_i \in \mathcal{O}_k$ sia intero su $\mathbb{Z}$ per ogni i. Sia $\beta_1, \ldots, \beta_k$ la sua base duale. Mostriamo che, detto $B = \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}}$, vale $\mathcal{O}_k \subseteq B$. Sia $\alpha \in \mathcal{O}_k$; sicuramente α si scrive come combinazione dei β_i

$$\alpha = \sum x_i \beta_i \quad x_i \in \mathbb{Q}$$

perchè $\beta_1, \ldots, \beta_n$ sono una base su $\mathbb{Q}$. Consideriamo l'elemento $\alpha\alpha_j$; questo si scrive come

$$\alpha\alpha_j = \sum x_i \beta_i \alpha_j \in \mathcal{O}_k$$

Applicando la funzione traccia $\mathrm{Tr}_{k/\mathbb{Q}}$ otteniamo

$$\mathrm{Tr}(\alpha\alpha_j) = \sum x_i \,\mathrm{Tr}(\beta_i\alpha_j) = x_j \,\mathrm{Tr}(\beta_j\alpha_j) = x_j$$

e dunque $x_j \in \mathbb{Z}$ perché la traccia di un elemento intero sta in $\mathbb{Z}$, da cui $\alpha \in B$. □

Come conseguenza del teorema, possiamo dare la seguente definizione:

Definizione 1.24. Una base intera di k su $\mathbb{Q}$ è una qualsiasi $\mathbb{Z}$ base di $\mathcal{O}_k$.

Segue direttamente dalla definizione che se $\alpha_1, \ldots, \alpha_n$ è una base intera allora k è generato su $\mathbb{Q}$ da quest'ultima. Notiamo che il teorema è vero solo per estensioni $k/\mathbb{Q}$ ma lo stesso non vale per estensioni relative. Infatti, se $\mathcal{O}_k, \mathcal{O}_F$ sono $\mathbb{Z}$-moduli liberi, $\mathcal{O}_F$ non è libero su $\mathcal{O}_k$ perché in generale $\mathcal{O}_k$ può non essere un PID.

1.4 Discriminante

Introduciamo ora un invariante di un campo di numeri; consideriamo quindi un'estensione F/K di campi di numeri di grado n (o più in generale, un'estensione finita separabile). Siano $\sigma_1, \ldots, \sigma_n$ le immersioni di F/K in $\overline{F}$.

Definizione 1.25. Siano $\alpha_1, \ldots, \alpha_n \in F$. Definiamo il *discriminante* come

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

dove la matrice $(\sigma_i(\alpha_j))$ è la seguente:

$$(\sigma_i(\alpha_j))_{i,j} = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}$$

Segue dalla definizione che il discriminante sia invariante per l'ordine delle immersioni e degli α_i. Il seguente teorema collega il discriminante alla funzione traccia:

Teorema 1.26. Sia F/K un'estensione di campi di numeri e siano $\alpha_1, \dots, \alpha_n$ elementi di F. Allora

$$\mathrm{disc}_{F/K}\{\alpha_1, \dots, \alpha_n\} = \det(\mathrm{Tr}_{F/K}(\alpha_i\alpha_j))_{i,j}$$

In particolare, il discriminante è un elemento di K e se $\alpha_j \in \mathcal{O}_F$ è intero su $\mathbb{Z}$ per ogni j, allora il discriminante appartiene a $\mathcal{O}_K$.

Dimostrazione. Sia $A = (\sigma_i(\alpha_j))_{i,j}$ la matrice del discriminante. Per definizione,

$$\begin{aligned}\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) &= \det(A)^2 \\ &= \det(A^2) \\ &= \det(A^t A)\end{aligned}$$

L'elemento in posizione i, j della matrice $A^t A$ è

$$(A^t A)_{i,j} = \sum_{k=0}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=0}^{n} \sigma_k(\alpha_i\alpha_j) = \mathrm{Tr}(\alpha_i\alpha_j)$$

da cui la tesi. □

Teorema 1.27. Sia F/K una estensione di campi di numeri e siano $\alpha_1, \dots, \alpha_n \in F$. Allora

$$\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = 0 \iff \{\alpha_1, \dots, \alpha_n\} \text{ è linearmente dipendente su } K$$

Dimostrazione. Se $\alpha_1, \dots, \alpha_n$ sono linearmente indipendenti, allora le colonne della matrice sono linearmente dipendenti e viceversa. □

Il teorema appena enunciato spinge a considerare solo basi di F come K-spazio vettoriale.

Teorema 1.28. Sia $F = K(\alpha)$ un'estensione finita di K. Allora

$$\begin{aligned}\mathrm{disc}_{F/K}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) &= \prod_{1 \le r < s \le n} (\sigma_s(\alpha) - \sigma_r(\alpha))^2 \\ &= (-1)^{\frac{n(n-1)}{2}} N_{F/K}(\mu'_\alpha(\alpha))\end{aligned}$$

Dimostrazione. La matrice del discriminante

$$\begin{pmatrix} 1 & \sigma_1(\alpha) & \dots & \sigma_1(\alpha)^{n-1} \\ \vdots & & & \vdots \\ 1 & \sigma_n(\alpha) & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix}$$

è una matrice di Vandermonde e dunque ha come determinante (si può mostrare per induzione, sviluppando il determinante con la formula di Laplace) $\prod_{1 \le s < r \le n}(\sigma_s(\alpha) - \sigma_r(\alpha))$. Notiamo che

$$\prod_{1 \le r < s \le n} (\sigma_s(\alpha) - \sigma_r(\alpha))^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{r \ne s} (\sigma_s(\alpha) - \sigma_r(\alpha))$$

Il polinomio minimo μ_α di α ha come radici i coniugati di α tramite le immersioni:

$$\mu_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$$

e la sua derivata è

$$\mu'_\alpha(x) = \sum_{i=1}^{n}\prod_{j\neq i}(x - \sigma_j(\alpha))$$

Valutando la derivata in α e calcolando la norma otteniamo

$$\begin{aligned} N(\mu'_\alpha(\alpha)) &= \prod_{l=1}^{n}\sigma_l(\mu'_\alpha(\alpha)) \\ &= \prod \mu'_\alpha(\sigma_l(\alpha)) \\ &= \prod_l \prod_{j\neq l}(\sigma_l(\alpha) - \sigma_j(\alpha)) \\ &= \prod_{j\neq l}(\sigma_l(\alpha) - \sigma_j(\alpha)) \end{aligned}$$

da cui la tesi. □

Indicheremo con $\operatorname{disc}\alpha$ il discriminante della base $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

Esempio.

- Vediamo come applicare il teorema nel caso delle estensioni ciclotomiche. Chiamiamo $\zeta = \zeta_n$. Sappiamo allora che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ e una $\mathbb{Q}$-base di $\mathbb{Q}(\zeta)$ è data dalle potenze $\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\}$. Calcoliamo il discriminante $\operatorname{disc}(\zeta)$; per la formula appena mostrata,

  $$\operatorname{disc}(\zeta) = (-1)^{\frac{\phi(n)(\phi(n)-1)}{2}} N(\mu'(\zeta))$$

  Il polinomio $p(x) = x^m - 1$ si annulla in ζ e dunque il polinomio minimo di ζ divide p, cioè $x^m - 1 = \mu(x)g(x)$. Valutando in ζ, si ha che $m\zeta^{m-1} = \mu'(\zeta)g(\zeta) + \mu(\zeta)g'(\zeta) = \mu'(\zeta)g(\zeta)$. Passando alle norme,

  $$N(m)N(\zeta)^{m-1} = N(\mu'(\zeta))N(g(\zeta))$$

  Dato che $N(m) = m^{\phi(m)}$ e che $N(\zeta)^{m-1} = 1$, si ha

  $$m^{\phi(m)} = N(\mu'(\zeta))N(g(\zeta))$$

  Di conseguenza, dato che $N(g(\zeta)) \in \mathbb{Z}$ (le sue radici sono radici dell'unità e dunque elementi interi su $\mathbb{Z}$), si ha che $N(\mu'(\zeta)) \mid m^{\phi(m)}$.

- Nel caso particolare $m = p^k$, $N(\mu'(\zeta_m)) \mid p^{k\phi(p^k)}$ e dunque la norma è una potenza di p.

- Se $m = p$, sappiamo che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ e $\mu(x)(x - 1) = x^p - 1$. Allora $N(\mu'(\zeta))N(\zeta - 1) = p^{p-1}$. Il polinomio minimo di $\zeta - 1$ è $\mu_{\zeta-1} = \mu_\zeta(x + 1) = \sum_{i=0}^{p-1}(x + 1)^i$ e dunque ha termine noto p. Di conseguenza, $N(\zeta - 1) = p$ e

  $$\operatorname{disc}(\zeta) = (-1)^{\frac{(p-1)(p-2)}{2}} N(\zeta) = (-1)^{\frac{(p-1)}{2}} p^{p-2}$$

Cambio di base Sia F/K un'estensione finita di campi di numeri e siano $\alpha_1, \dots \alpha_n$ e $\beta_1, \dots, \beta_n$ due basi di F come K-spazio vettoriale. Sappiamo che possiamo esprimere ogi β_i in modo unico come combinazione lineare degli α_i,

$$\beta_i = \sum a_{ij}\alpha_j$$

cioè esiste una matrice M tale che $M\alpha_i = \beta_i$ per ogni indice i. Denotiamo con $\Sigma(\alpha)$ la matrice $(\sigma_i(\alpha_j))_{i,j}$, dove le σ_i sono le immersioni di F/K in $\overline{F}$. Allora $\mathrm{disc}_{F/K}(\alpha) = \det(\Sigma(\alpha))^2$ e $\mathrm{disc}(\beta) = \det(\Sigma(\beta))^2$ e quindi, dato che le σ_i sono omomorfismi,

$$\Sigma(\beta) = M\Sigma(\alpha)$$

Otteniamo la relazione $\det M^2 \det(\Sigma(\alpha))^2 = \det(\Sigma(\beta))^2$.
Consideriamo il caso particolare di due basi intere di $\mathcal{O}_K$. La relazione impone che i discriminanti siano uguali, perchè la matrice M manda una base in una base e quindi è invertibile (le matrici di $GL(\mathbb{Z})$ hanno determinante ± 1). Abbiamo così dimostrato che

Proposizione 1.29. Siano $\mathcal{B}, \mathcal{B}'$ due basi intere di K. Allora

$$\mathrm{disc}(\mathcal{B}) = \mathrm{disc}(\mathcal{B}')$$

Il discriminante di una base intera è un invariante del campo.

Definiamo allora

$$\mathrm{disc}(K) \coloneqq \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$$

dove $\alpha_1, \dots, \alpha_n$ è una base intera.

Esempio (Discriminante di estensioni quadratiche). Consideriamo l'estensione quadratica $\mathbb{Q}(\sqrt{m})$ con m libero da quadrati. Sappiamo che

$$\mathcal{O}_k = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & m \equiv 1 \pmod 4 \end{cases}$$

Se $m \equiv 2,3 \pmod 4$, allora

$$\mathrm{disc}(K) = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = 4m$$

Se invece $m \equiv 1 \pmod 4$ otteniamo $\mathrm{disc}(K) = m$.

Definizione 1.30. Sia $X \subseteq k$ uno $\mathbb{Z}$-modulo di rango n generato da $X = \langle \alpha_1, \dots, \alpha_n \rangle$ elementi linearmente indipendenti su $\mathbb{Q}$. Definiamo

$$\mathrm{disc}(X) \coloneqq \mathrm{disc}_{k/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$$

Per quanto visto, due basi diverse di uno $\mathbb{Z}$-modulo forniscono lo stesso discriminante. Consideriamo $Y \subseteq X \subseteq K$ $\mathbb{Z}$-moduli di rango n e siano $\{y_i\}_{i=1}^n$ una base per Y e $\{\alpha_i\}_{i=1}^n$ una base di X. Allora $\mathrm{disc}(Y) = \det M^2 \,\mathrm{disc}(X)$, dove M è la matrice tale che $M\alpha_i = y_i$. Per la forma normale di Smith, possiamo

supporre di avere una base diagonale per X, Y. In questo caso, la matrice M diventa

$$M = \begin{pmatrix} a_0 & & & \\ & a_1 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$$

Dunque $\det M^2 = (a_1, \dots, a_n)^2$. Nel quoziente,

$$X/Y \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}$$

Di conseguenza, $\left|X/Y\right| = \prod_{i=1}^{n} a_i$.
Se $Y \subseteq X$ sono $\mathbb{Z}$ moduli di rango n, dove $n = [k : \mathbb{Q}]$, si ottiene

$$\operatorname{disc}(Y) = [X : Y]^2 \operatorname{disc}(X)$$

Questo permette di relazionare il discriminante di α con quello di $\mathcal{O}_k$, con $k = \mathbb{Q}(\alpha)$. Sicuramente $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_k$ e per quanto appena detto il discriminante di α può essere espresso come

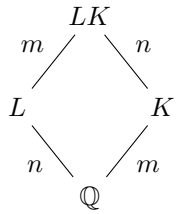
$$\operatorname{disc}(\alpha) = \left|\mathcal{O}_k/\mathbb{Z}[\alpha]\right|^2 \operatorname{disc}(\mathcal{O}_k) \tag{1.4}$$

Questo fornisce un criterio per stabilire se $\mathcal{O}_k = \mathbb{Z}[\alpha]$. Infatti, se $\operatorname{disc}(\alpha)$ è libero da quadrati, abbiamo necessariamente l'uguaglianza.

Definizione 1.31. Sia $\alpha \in K$ un elemento intero e supponiamo che $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$; $\mathbb{Z}[\alpha]$ è generato da $1, \alpha, \dots, \alpha^{n-1}$. Definiamo l'indice di α in $\mathcal{O}_K$ come

$$\operatorname{ind}(\alpha) \coloneqq \left|\mathcal{O}_K/\mathbb{Z}[\alpha]\right|$$

Segue direttamente dalla definizione che $\operatorname{ind}(\alpha)\mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$ e quindi $\mathcal{O}_K \subseteq \frac{1}{\operatorname{ind}(\alpha)}\langle 1, \alpha, \dots, \alpha^{n-1}\rangle$.
Studiamo ora il comportamento del discriminante rispetto alle estensioni di campi. Siano L, K campi di numeri e supponiamo che le estensioni siano linearmente disgiunte, cioè $[LK : K] = [L : \mathbb{Q}]$.



Fissiamo $\mathcal{B} = \{v_i\}$ una base di L su $\mathbb{Q}$ e $\mathcal{D} = \{w_j\}$ una base di K su $\mathbb{Q}$; allora $\{v_i\}$ è una K base per LK su K (genera 1 ed è un anello). Quindi $\{v_i w_j\}$ è una $\mathbb{Q}$-base di LK.
Studiamo il caso in cui $\mathcal{D}$, $\mathcal{B}$ sono basi intere di $\mathcal{O}_L$ e O_K. Allora $\{v_i w_j\}$ non è una base intera di $\mathcal{O}_{LK}$; per esempio

Esempio. Sia $L = \mathbb{Q}(\sqrt{3})$ e $K = \mathbb{Q}(\sqrt{7})$; allora $LK = M = \mathbb{Q}(\sqrt{3}+\sqrt{7})$ per motivi di grado. Invece,

$$\mathcal{O}_L = \mathbb{Z}[\sqrt{3}] \qquad\qquad \mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$$

e $\mathcal{O}_L\mathcal{O}_K \neq \mathcal{O}_M$ perché

$$\frac{\sqrt{3}+\sqrt{7}}{2} \in \mathcal{O}_M \setminus \mathcal{O}_L\mathcal{O}_K$$

Chiaramente non appartiene a $\mathcal{O}_L\mathcal{O}_K$; calcolando il polinomio minimo si ottiene che è intero.

In ogni caso, otteniamo una base di $\mathcal{O}_L\mathcal{O}_K$. È chiaro che $\{v_iw_j\}$ siano linearmente indipendenti; inoltre, dato che

$$\mathcal{O}_L\mathcal{O}_K = \left\{\sum \gamma_a\rho_a \mid \gamma_a \in \mathcal{O}_L \ \rho_a \in \mathcal{O}_k\right\}$$

generano $\mathcal{O}_M$ su $\mathbb{Q}$.

Teorema 1.32. Siano L, K tali che $[L : \mathbb{Q}][K : \mathbb{Q}] = [LK : \mathbb{Q}]$ e sia $d = (\operatorname{disc}(K), \operatorname{disc}(L))$. Allora

$$\mathcal{O}_{LK} \subseteq \frac{1}{d}\mathcal{O}_L\mathcal{O}_K$$

In particolare se $d = 1$ abbiamo l'uguaglianza.

Dimostrazione. Sia $\alpha \in \mathcal{O}_{LK}$ e siano $\mathcal{B} = \{\alpha_i\}_{i=1}^n$ e $\mathcal{B}' = \{\beta_i\}_{i=1}^m$ due basi rispettivamente di $\mathcal{O}_L$ e $\mathcal{O}_K$. Allora α si scrive nei termini della base $\{\alpha_i\beta_j\}$ con coefficienti razionali:

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j \quad m_{ij}, r \in \mathbb{Z}$$

con $\gcd(r, \gcd(m_{ij})) = 1$. Per dimostrare il teorema, è sufficiente verificare che $r \mid d$; basta mostrare che $r \mid \operatorname{disc} K$ e $r \mid \operatorname{disc} L$. Scriviamo α nella forma

$$\alpha = \sum_i x_i\alpha_i \quad x_i = \sum_j \frac{m_{ij}}{r}\beta_j \quad \in K$$

Mostriamo ora che $\operatorname{disc}(L)x_i \in \mathbb{A}$. Da questo seguirà infatti che $\operatorname{disc}(L)x_i \in \mathbb{A} \cap K = \mathcal{O}_K$ e dunque $r \mid \operatorname{disc}(L)$. Simmetricamente, varrà $r \mid \operatorname{disc}(K)$, da cui la tesi. Siano ora $\sigma_1, \dots, \sigma_n$ le immersioni di $L/\mathbb{Q}$ e siano $\tilde{\sigma}_1, \dots, \tilde{\sigma}_n$ le immersioni di LK/K; possiamo anche supporre che $\tilde{\sigma}_i|_L = \sigma_i$. Se infatti per assurdo $\tilde{\sigma}_i|_L = \tilde{\sigma}_j|_L$, allora coinciderebbero sia su L che su K e quindi su tutto il composto LK. Dall'equazione

$$\alpha = \sum_i x_i\alpha_i$$

applicando le $\tilde{\sigma}_i$ otteniamo un sistema lineare (in cui le incognite sono le x_i):

$$\begin{cases} \sum_i x_i\tilde{\sigma}_1(\alpha_i) = \tilde{\sigma}_1(\alpha) \\ \vdots \\ \sum_i x_i\tilde{\sigma}_n(\alpha_i) = \tilde{\sigma}_n(\alpha) \end{cases}$$

Notiamo che la matrice del sistema è $A = (\tilde{\sigma}_i(\alpha_j))$ e dunque, detto $\delta := \det(A)$ il suo determinante, si ha $\mathrm{disc}(L) = \delta^2$. In particolare, il sistema ha soluzione e per Cramer otteniamo

$$x_i = \frac{\det(A^i)}{\delta}$$

dove A^i è la matrice ottenuta sostituendo l'i-esima colonna con il vettore dei termini noti $(\tilde{\sigma}_i(\alpha))$. Ogni entrata di $a_{ij} \in \mathbb{A}$ è intera su $\mathbb{Q}$ e quindi dalla relazione $\det(A^i) = x_i\delta$ otteniamo $\mathrm{disc}(L)x_i = \delta^2 x_i = \delta(\delta x_i) \in \mathbb{A} \cap K = \mathcal{O}_K$, come voluto. □

Il teorema ci permette di caratterizzare gli anelli interi delle estensioni ciclotomiche.

Osservazione 1.33. Consideriamo l'estensione ciclotomica $K = \mathbb{Q}(\zeta_p)$ con $p \in \mathbb{Z}$ un primo. Allora

$$N_{K/Q}(1 - \zeta_{p^l}) = \prod_{(k,p)=1} (1 - \zeta_{p^l}^k) = p$$

Infatti, il polinomio minimo di ζ_{p^l} è

$$\mu_{\zeta_{p^l}}(x) = \frac{x^{p^l} - 1}{x^{p^{l-1}} - 1} = \prod_{(k,p)=1} (x - \zeta^k) = (x^{p^{l-1}})^{p-1} + \cdots + x^{p^{l-1}} + 1$$

e ponendo $x' = 1 - x$ si ottiene il polinomio minimo di $1 - \zeta_{p^l}$. Il termine noto di quest'ultimo, che coincide con la norma, è proprio p, come voluto.

Lemma 1.34. Sia $p \in \mathbb{Z}$ un primo e sia $m = p^l$. Allora $\mathbb{Q}(\zeta_m) \cap \mathbb{A} = \mathbb{Z}[\zeta_m]$.

Dimostrazione. Sia $k = \mathbb{Q}(\zeta_m)$. Sappiamo che vale in contenimento $\mathcal{O}_k \supseteq \mathbb{Z}[\zeta_m] = \mathbb{Z}[1 - \zeta]$. Mostriamo l'uguaglianza. Sia $n = \phi(p^l)$ e $d = \mathrm{disc}(\zeta) = \mathrm{disc}(1 - \zeta)$. Abbiamo già osservato che

$$\mathbb{Z}[1 - \zeta] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbb{Z}[1 - \zeta]$$

Dunque, dato $\alpha \in \mathcal{O}_k$, possiamo scrivere

$$\alpha = \frac{m_1 + m_2(1 - \zeta) + \cdots + m_n(1 - \zeta)^{n-1}}{d} \qquad m_i \in \mathbb{Z}$$

dove $d = \mathrm{disc}(\zeta) \mid p^{ln}$. Se per assurdo $\mathcal{O}_K \neq \mathbb{Z}[1 - \zeta]$, allora esisterebbe $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}[1 - \zeta]$ con non tutti gli m_i divisibili per p. Dunque potremmo trovare $\beta \in \mathcal{O}_k$ tale che

$$\beta = \frac{m_i(1 - \zeta)^{i-1} + \cdots + m_n(1 - \zeta)^{n-1}}{p}$$

con $p \nmid m_i$, che otteniamo da α moltiplicando per una opportuna potenza di p e sottraendo elementi di $\mathbb{Z}[1 - \zeta]$. Per l'osservazione 1.33, otteniamo

$$N_{K/Q}(1 - \zeta_{p^l}) = \prod_{(k,p)=1} (1 - \zeta_{p^l}^k) = p$$

e dato che $(1-\zeta) \mid (1-\zeta^k)$ in $\mathcal{O}_K$ per ogni $k \in \mathbb{N}$, dividendo per $(1-\zeta)^n$ ricaviamo

$$\prod_{(k,p)=1} \frac{(1-\zeta^k)}{(1-\zeta)} = \frac{p}{(1-\zeta)^n}$$

In questo modo, ogni elemento del prodotto appartiene a $\mathbb{Z}[1-\zeta]$ e dunque lo stesso vale per il secondo membro dell'uguaglianza. Di conseguenza,

$$\beta \frac{p}{(1-\zeta)^i} = \frac{m_i}{(1-\zeta)} + f$$

dove $f \in \mathbb{Z}[\zeta]$. Calcoliamo ora la norma:

$$N_{K/\mathbb{Q}}\Big(\frac{m_i}{(1-\zeta)}\Big) = \frac{N(m_i)}{N(1-\zeta)} = \frac{m_i^n}{p}$$

che appartiene a $\mathbb{Z}$ perché $\frac{m_i}{(1-\zeta)} \in \mathcal{O}_K$. Ciò è assurdo perché avevamo supposto $p \nmid m_i$, da cui la tesi. □

Teorema 1.35. $\mathbb{Q}(\zeta_m) \cap \mathbb{A} = \mathbb{Z}[\zeta_m]$.

Dimostrazione. Sia $K = \mathbb{Q}(\zeta_m)$. Procediamo ora per induzione su m. Il caso $m = 2$ è ovvio. Supponiamo che $\mathcal{O}_{\mathbb{Q}(\zeta_{m'})} = \mathbb{Z}[\zeta_{m'}]$ per ogni $m' < m$. Possiamo distinguere due casi:

$$m = \begin{cases} p^l \\ m_1 m_2 \quad (m_1, m_2) = 1 \end{cases}$$

Abbiamo già trattato il primo caso nel lemma precedente. Nel secondo caso, siano $K_i = \mathbb{Q}(\zeta_{m_i})$. Allora, per il teorema 1.32,

$$\mathcal{O}_K \subseteq \frac{1}{d} \mathcal{O}_{K_1} \mathcal{O}_{K_2}$$

dove $d = (d_1, d_2)$. Basta mostrare che $d = 1$ per avere l'uguaglianza, perché l'altro contenimento è ovvio. Per quanto visto nell'esempio 1.4, vale $d_i | m_i^{\phi(m_i)}$ e dunque $(d_1, d_2) = 1$. Di conseguenza,

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}] = \mathbb{Z}[\zeta_m]$$

dove l'ultima uguaglianza vale perché $(m_1, m_2) = 1$. □

Corollario 1.36. Sia $p \in \mathbb{Z}$ un primo. Allora

$$\sqrt{\operatorname{disc}(\zeta_p)} \in \mathbb{Q}(\zeta_p)$$

Dimostrazione. In base al teorema appena dimostrato, $1, \zeta_p, \ldots, \zeta_p^{p-1}$ è una base intera di $\mathcal{O}_K$ e, per il teorema 1.28, vale

$$\operatorname{disc}(\mathbb{Q}(\zeta_p)) = \operatorname{disc}(\zeta) = \prod_{1 \le r < s \le n} (\sigma_s(\zeta) - \sigma_r(\zeta))^2$$

Di conseguenza,

$$\sqrt{\operatorname{disc}(\mathbb{Q}_{\zeta_p})} = \sqrt{\prod_{1 \le r < s \le n} (\sigma_s(\zeta) - \sigma_r(\zeta))^2} = \prod_{1 \le r < s \le n} |\sigma_s(\zeta) - \sigma_r(\zeta)| \in \mathbb{Q}(\zeta_p)$$

□

Enunciamo i seguenti teoremi senza dimostrazione:

Teorema 1.37. Sia $K = \mathbb{Q}(\alpha)$, con $\alpha \in \mathcal{O}_K$. Allora esiste una base intera di K della forma

$$1, \frac{f_1(\alpha)}{d_1} \dots \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

dove $\deg(f_i) = i$, $f_i \in \mathbb{Z}[x]$ polinomi monici e $d_i \mid d_{i+1}$. Inoltre i d_i sono univocamente determinati e $d_1 d_2 \dots d_{n-1} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

Proposizione 1.38. Sia $K = \mathbb{Q}(\alpha)$ con $\alpha \in \mathcal{O}_K$. Nella notazione del precedente teorema,

- $\operatorname{disc}(\alpha) = (d_1 \dots d_{n-1})^2 \operatorname{disc}(K)$
- $\mathcal{O}_K/\mathbb{Z}[\alpha]$ ha cardinalità $d_1 \dots d_{n-1}$
- Se $i + j < n$, allora $d_i d_j \mid d_{i+j}$
- Se $i < n$, allora $d_1^i \mid d_i$ e in particolare $d_1^{n(n-1)} \mid \operatorname{disc}(\alpha)$

Dimostrazione.

- Per il teorema precedente, possiamo trovare una base intera di $\mathcal{O}_K$ del tipo

  $$\mathcal{B} = \left\{1, \frac{f_1(\alpha)}{d_1} \dots \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\}$$

  Scriviamo la matrice di cambiamento di base M tra questa e la base $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. La matrice che si ottiene è triangolare superiore, con elementi diagonali $1/d_i$. Di conseguenza $\det M = 1/(d_1 \dots d_{n-1})$. Utilizzando la formula 1.4, si ottiene proprio

  $$\operatorname{disc}(\alpha) = (d_1 \dots d_{n-1})^2 \operatorname{disc}(K)$$

- Segue direttamente dalla formula 1.4 e il punto precedente.

- Notiamo che lo span su $\mathbb{Q}$ dei primi k elementi di $\mathcal{B}$ coincide con lo span di $1, \alpha, \dots, \alpha^{k-1}$. Consideriamo allora l'elemento

  $$\beta = \frac{f_j(\alpha)}{d_j} \frac{f_i(\alpha)}{d_i}$$

  Questo è un polinomio di grado $i + j$ con termine di testa $1/d_i d_j$. Il coefficiente dell'$i+j$-esimo vettore di $\mathcal{B}$ appartiene a $\mathbb{Z}$ e dunque otteniamo la relazione voluta sui d_i.

- Come nel punto precedente, considerando l'elemento

  $$\gamma = \frac{f_1(\alpha)^i}{d_1^i}$$

  Il caso particolare segue da questo e dalla formula del punto 1.

□

Proposizione 1.39. Sia $\alpha \in \mathbb{A}$ e sia $K = \mathbb{Q}(\alpha)$. Sia μ_α il polinomio minimo di α; supponiamo che sia di Eisenstein rispetto a un primo $p \in \mathbb{Z}$. Allora

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] = \mathrm{ind}(\alpha)$$

Dimostrazione. Dato che il polinomio minimo μ_α

$$\mu_\alpha = x^n + \sum a_{n-i} x^i$$

è di Eisenstein rispetto a p, si ha $p \mid a_i$ per ogni indice i e $p^2 \nmid a_n$. Notiamo che

$$\frac{\alpha^n}{p} \in \mathbb{Z}[\alpha] \qquad\qquad N_{K/\mathbb{Q}}(\alpha) = a_n$$

Supponiamo per assurdo che $p \mid \mathrm{ind}(\alpha)$. Allora, per il teorema di Cauchy (applicato al quoziente $\mathcal{O}_K/\mathbb{Z}[\alpha]$), esiste $\xi \in \mathcal{O}_k \setminus \mathbb{Z}[\alpha]$ tale che $p\xi \in \mathbb{Z}[\alpha]$. Possiamo scrivere ξ in termini della base di $\mathbb{Z}[\alpha]$ in questo modo

$$\xi = \frac{1}{p}(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1})$$

dove non tutti i $b_i \equiv 0 \pmod p$. A meno di sottrarre elementi in $\mathbb{Z}[\alpha]$, possiamo supporre che

$$\xi = \frac{b_j\alpha^j + \cdots + b_{n-1}\alpha^{n-1}}{p}$$

con $p \nmid b_j$. Consideriamo ora l'elemento

$$\beta = \frac{b_j\alpha^{n-1}}{p} = \alpha^{n-1-j}\xi - \frac{\alpha^n}{p}x$$

dove $x \in \mathbb{Z}[\alpha]$; notiamo che $\beta \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$. Calcoliamo la norma di $p\beta$.

$$p^n N(\beta) = N(p\beta) = N(b_j\alpha^{n-1}) = b_j^n N(\alpha)^{n-1} \equiv 0 \pmod{p^n}$$

Dato che $b_j \not\equiv 0 \pmod p$, necessariamente $N(\alpha)^{n-1} \equiv 0 \pmod{p^n}$, cioè $a_n^{n-1} \equiv 0 \pmod{p^n}$. Questo è però assurdo perché il polinomio minimo μ_α è di p-Eisenstein. □

Estensioni Cubiche Pure Sia K un'estensione cubica pura di $\mathbb{Q}$, cioè $K = \mathbb{Q}(\sqrt[3]{m})$ con $m = ab^2$ e a, b relativamente primi e liberi da quadrati. Dato che $\mathbb{Q}(\sqrt[3]{a^2b}) = \mathbb{Q}(\sqrt[3]{ab^2})$, possiamo supporre che 3 non sia un fattore di b. Sia $\alpha \in \mathbb{A}$ tale che $\alpha^3 = m$. Dall'equazione 1.4,

$$\mathrm{disc}(\alpha) = \left|\mathcal{O}_k/\mathbb{Z}[\alpha]\right|^2 \mathrm{disc}(K)$$

D'altro canto, per la proposizione 1.28,

$$\mathrm{disc}(\alpha) = -N(\mu'(\alpha)) = 3^3m^2 = -27a^2b^4$$

Notiamo che se $p \mid a$, allora $x^3 - ab^2$ è di p-Eisenstein. Allora, per la proposizione 1.39, $p \nmid \left|\mathcal{O}_K/\mathbb{Z}[\alpha]\right|$ e $a^2, 3 \mid \mathrm{disc}(K)$.
Consideriamo ora il generatore $m' = a^2b = \beta^3$. Allora

$$\mathrm{disc}(\beta) = -27a^4b^2$$

e il polinomio minimo è di p-Eisenstein per ogni primo che divide b; dunque $b^2 \mid \operatorname{disc}(K)$. Dunque

$$3, a^2, b^2 \mid \operatorname{disc}(K) \mid (\operatorname{disc}(\alpha), \operatorname{disc}(\beta)) = 27a^2b^2$$

Utilizzando il teorema 1.37, sappiamo che possiamo trovare una base intera del tipo

$$\mathcal{B} = \left\{1, \frac{\alpha + p}{d_1}, \frac{\alpha^2 + s\alpha + t}{d_2}\right\}$$

e per la proposizione 1.38 vale $d_1 = 1$. Infatti

$$27a^2b^4 = d_1^2 d_2^2 \operatorname{disc}(K)$$

e il primo membro non può contenere seste potenze per come abbiamo scelto m. Dunque possiamo scegliere una base intera della forma

$$\mathcal{B} = \left\{1, \alpha, \frac{\alpha^2 + s\alpha + t}{d_2}\right\}$$

Inoltre la relazione sui discriminanti è semplificata:

$$27a^2b^4 = d_2^2 \operatorname{disc}(K)$$

Per terminare basta determinare il terzo elemento della base intera $\mathcal{B}$. Distinguiamo ora alcuni casi:

- Se $3 \mid m$, allora $x^3 - m$ è di 3-Eisenstein e dunque $3 \nmid \operatorname{ind}\alpha$ per la proposizione 1.39 quindi $27 \mid \operatorname{disc}(K)$. Di conseguenza $1, \alpha, \alpha^2/b$ è una base intera e $\operatorname{disc}(K) = 27a^2b^2$.

- Se $m \not\equiv \pm 1 \pmod 9$, possiamo ricondurci al caso precedente, considerando l'elemento $\gamma = \alpha - m$. Il suo polinomio minimo di è

  $$\mu_\gamma(x) = x^3 + 3x^2m + 3xm^2 + m^3 - m$$

  e tale polinomio in questo caso è di 3-Eisenstein. Di conseguenza possiamo ripetere il ragionamento del punto precedente ($\operatorname{disc}(\gamma) = \operatorname{disc}(\alpha)$ perché generano lo stesso $\mathbb{Z}$-modulo) e quindi $\operatorname{disc}(K) = 27a^2b^2$.

- Se $m \equiv +1 \pmod 9$,per quanto dimostrato fino ad ora, $\operatorname{disc}(K) = 3a^2b^2$ oppure $\operatorname{disc}(K) = 27a^2b^2$. Proviamo allora a vedere se sia possibile completare la base intera con un elemento del tipo

  $$\beta = \frac{\alpha^2 + s\alpha + t}{3} \qquad\qquad s, t \in \{0, 1, -1\}$$

  Si osserva che $\gamma = \frac{\alpha^2+\alpha+1}{3}$ è intero con polinomio minimo

  $$\mu(x) = x^3 - x^2 - \frac{m-1}{3}x - \frac{(m-1)^2}{27}$$

  Di conseguenza il discriminante è $3a^2b^2$ e una base intera $\{1, \alpha, \gamma\}$.

- Se $m \equiv -1 \pmod 9$ valgono le stesse osservazioni del punto precedente e si ottiene che $\delta = \frac{\alpha^2-\alpha+1}{3}$ è intero con polinomio minimo

$$\mu(x) = x^3 - x^2 + \frac{m+1}{3}x - \frac{(m+1)^2}{27}$$

  Di conseguenza il discriminante è $3a^2b^2$ e una base intera $\{1, \alpha, \delta\}$.

Teorema 1.40 (Kronecker-Weber)**.** Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in una estensione ciclotomica.

Studiamo un caso particolare del teorema di Kronecker-Weber: le estensioni quadratiche di $\mathbb{Q}$, cioè le estensioni del tipo $\mathbb{Q}(\sqrt{m})$.

Proposizione 1.41. Sia $m \in \mathbb{Z}$ un intero libero da quadrati. Allora

$$\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_d)$$

dove $d = \operatorname{disc}(\mathbb{Q}(\sqrt{m}))$.

Dimostrazione. Notiamo che, come conseguenza del corollario 1.36, vale

$$\begin{cases} \sqrt{-p} \in \mathbb{Q}(\zeta_p) & p \equiv 1 \pmod 4 \\ \sqrt{p} \in \mathbb{Q}(\zeta_p) & p \equiv 3 \pmod 4 \end{cases}$$

Scomponiamo m in fattori irriducibili

$$m = p_1 \dots p_a q_1 \dots q_b$$

dove $p_i \equiv 1 \pmod 4$ e $q_i \equiv 3 \pmod 4$.

- Supponiamo $m \equiv 1 \pmod 4$ e mostriamo che $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_m)$. Allora

$$m = p_1 \dots p_a (-q_1) \dots (-q_b)$$

  perché, per la scelta della classe di resto $\pmod 4$, il numero di primi q_i deve essere pari. Dunque

$$\sqrt{m} = \sqrt{p}_1 \dots \sqrt{p}_a \sqrt{-q_1} \dots \sqrt{-q_b} \in \mathbb{Q}(\zeta_m)$$

  dato che $\mathbb{Q}(\zeta_{p_i}) \subseteq \mathbb{Q}(\zeta_m)$ e $\mathbb{Q}(\zeta_{q_i}) \subseteq \mathbb{Q}(\zeta_m)$.

- Se $m \equiv 2 \pmod 4$,

$$m = \pm 2 p_1 \dots p_a q_1 \dots q_b$$

  e $\sqrt{m} \in \mathbb{Q}(\zeta_{4m})$ visto che $8 \mid 4m$.

- Se $m \equiv 3 \pmod 4$, possiamo ignorare i segni perché $\sqrt{-1} \in \mathbb{Q}(\zeta_{4m})$ e dunque $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{4m})$.

□

Proposizione 1.42. Sia $\zeta = \zeta_n$ una radice n-esima primitiva dell'unità. Allora $\mathcal{O}_F := \mathbb{Q}(\zeta + \bar{\zeta}) \cap \mathbb{A} = \mathbb{Z}[\zeta + \bar{\zeta}]$

Dimostrazione. Notiamo preliminarmente che $\mathbb{Z}[\zeta + \bar{\zeta}] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$. Infatti $\zeta + \bar{\zeta} \in \mathbb{Q}(\zeta)$ e dunque $\mathbb{Q}(\zeta + \bar{\zeta}) \subseteq \mathbb{Q}(\zeta)$. Non vale l'uguaglianza perché $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \bar{\zeta})] = 2$: infatti il polinomio minimo di ζ su $\mathbb{Q}(\zeta + \bar{\zeta})$ ha grado due ed è $x^2 - (\zeta - \bar{\zeta})x + 1$). Dunque $\mathbb{Z}[\zeta + \bar{\zeta}] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$.
Sia $F = \mathbb{Q}(\zeta + \bar{\zeta})$; mostriamo che $\mathbb{Z}[\zeta + \bar{\zeta}] \supseteq \mathcal{O}_F$. Per quanto detto, $\mathbb{Z}[\zeta + \bar{\zeta}]$ ha come base l'insieme

$$1, (\zeta + \bar{\zeta}), \dots (\zeta + \bar{\zeta})^{\frac{\phi(n)}{2} - 1}$$

Supponiamo per assurdo esista $\alpha \in \mathcal{O}_F \setminus \mathbb{Z}[\zeta + \bar{\zeta}]$; allora possiamo scrivere α in termini della $\mathbb{Q}$-base di F

$$\alpha = a_0 + a_1(\zeta + \bar{\zeta}) + \cdots + a_N(\zeta + \bar{\zeta})^N$$

dove $N \leq \frac{\phi(n)}{2} - 1$ e possiamo assumere senza perdità di generalità che $a_N \notin \mathbb{Z}$. Moltiplicando α per ζ^N otteniamo

$$\zeta^N \alpha = a_N + \cdots + a_N \zeta^{2N}$$

(il termine noto e il coefficiente direttore sono uguali) è un polinomio in ζ. $a_N\zeta$ è scritto in termini della $\mathbb{Z}$-base $1, \dots, \zeta^{\phi(n)-1}$ di $\mathbb{Z}[\zeta]$, perchè $2N \leq \phi(n) - 2 < \phi(n) - 1$. Dato che $\alpha\zeta^N \in \mathbb{Z}[\zeta]$, i coefficienti devono appartenere a $\mathbb{Z}$ e dunque $a_N \in \mathbb{Z}$, da cui un assurdo. □

Capitolo 2

Fattorizzazione di Ideali

2.1 Domini di Dedekind

Definizione 2.1. Sia M un A-modulo. M si dice noetheriano se verifica una delle seguenti equivalenti:

- Ogni famiglia non vuota di sottomoduli di M ammette un elemento massimale.
- Ogni catena ascendente di sottomoduli di M è stazionaria.
- Ogni sottomodulo di M è finitamente generato.

Un anello A si dice noetheriano se lo è come A-modulo, cioè se queste proprietà valgono sugli ideali di A.

Esempio. Se $A = K[x_1, \dots]$, allora A non è un anello noetheriano, perché l'ideale delle indeterminate $(x_1, x_2, x_3, \cdots)$ non è finitamente generato e ogni x_i è irriducibile. Notiamo che questo significa che in generale non è detto che un sottomodulo di un modulo finitamente generato sia finitamente generato.

Definizione 2.2. Un dominio di Dedekind R è un dominio di integrità tale che:

- R è noetheriano.
- $\dim(R) = 1$.
- R è integralmente chiuso.

Proposizione 2.3. Se R è un PID, allora R è un dominio di Dedekind.

Dimostrazione. Ogni ideale di R è principale e dunque R è noetheriano; in un PID ogni primo non nullo è massimale e dunque $\dim(R) = 1$. Inoltre, un PID è in particolare un UFD e quindi è integralmente chiuso. □

Lemma 2.4. Sia K un campo di numeri e sia $0 \neq I \subseteq \mathcal{O}_K$ un ideale. Allora

$$\left|\mathcal{O}_K/I\right| < \infty$$

Dimostrazione. Sia $\alpha \in I$. Allora $N(\alpha) = \alpha\beta \in \mathbb{Z}$ e β è un intero algebrico. Chiamiamo $N(\alpha) = m$; dalla relazione segue che

$$\beta = \frac{m}{\alpha}$$

dunque $\beta \in \mathcal{O}_K$ e $m = \alpha\beta \in I$. Valgono i contenimenti

$$(m) \subseteq I \subseteq \mathcal{O}_K$$

Dato che $\mathcal{O}_K$ può essere visto come $\mathbb{Z}$-modulo libero di rango n, si ha

$$\left|\mathcal{O}_K/(m)\right| = m^n$$

Per il secondo teorema di omomorfismo,

$$[\mathcal{O}_K : I][I : (m)] = [\mathcal{O}_K : (m)] = m^n$$

e dunque ha indice finito. □

Dimostrazione alternativa. Per ipotesi, l'inclusione $\mathbb{Z} \to \mathcal{O}_K$ è un omomorfismo intero. Allora anche

$$\mathbb{Z}/I \cap \mathbb{Z} \longrightarrow \mathcal{O}_K/I$$

è un omomorfismo intero. In particolare, $\mathcal{O}_K/I$ è uno $\mathbb{Z}/I$-modulo finitamente generato e dunque è finito. □

Proposizione 2.5. Sia K un campo di numeri, $[K\colon \mathbb{Q}] = n$. Allora $\mathcal{O}_K$ è un dominio di Dedekind.

Dimostrazione elementare. Chiaramente $\mathcal{O}_K$ è un dominio, perché sottoanello di un campo. Mostriamo la noetherianità, cioè che ogni ideale è finitamente generato. Dato che $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo libero di rango n, ogni suo sottomodulo è libero; dunque I è uno $\mathbb{Z}$-modulo libero di rango $\leq n$. In particolare, è finitamente generato.
Mostriamo che ha dimensione 1. Sia $p \subseteq \mathcal{O}_K$ un primo non nullo; vogliamo mostrare che p è massimale. Per il lemma 2.4,

$$A = \mathcal{O}_K/p$$

è un dominio finito e quindi è un campo. Da questo discende la massimalità di p.
Inoltre $\mathcal{O}_K$ è integralmente chiuso per definizione (è la chiusura integrale di $\mathbb{Z}$ in K). □

Dimostrazione mediante teoremi di Cohen-Seidenberg. $\mathcal{O}_K$ è la chiusura integrale di $\mathbb{Z}$ in K e dunque è un dominio di integrità, è integralmente chiuso per definizione. Le estensioni intere mantengono la dimensione e dunque ha dimensione 1 ($\mathbb{Z}$ è PID). Inoltre è noetheriano per il teorema della base di Hilbert, perché $\mathcal{O}_K$ è finitamente generato come modulo su $\mathbb{Z}$ e dunque in particolare lo è come algebra. □

Lemma 2.6. Sia A un anello noetheriano. Allora ogni ideale non nullo contiene un prodotto finito di ideali primi.

Dimostrazione. Consideriamo l'insieme

$$\mathcal{F} = \{0 \neq I \subseteq A \mid I \text{ non contiene un prodotto di ideali primi}\}$$

e supponiamo per assurdo che $\mathcal{F}$ sia non vuoto. Per noetherianità, esiste un elemento massimale J di $\mathcal{F}$. J non è un ideale primo e quindi esistono $x, y \in A$ tali che $xy \in J$ ma $x, y \notin J$. Allora gli ideali $J + (x)$ e $J + (y)$ contengono un prodotto di ideali primi e

$$J \supseteq (J + (x))(J + (y)) \supseteq P_1 \dots P_r Q_1 \dots Q_s$$

dove $J + (x) \supseteq P_1 \dots P_r$ e $J + (y) \supseteq Q_1 \dots Q_s$. □

Dimostrazione alternativa. Il radicale di I è intersezione di finiti primi per noetherianità e in un anello noetheriano ogni ideale contiene una potenza del suo radicale. □

Definizione 2.7. Sia A un dominio e sia K il campo dei quozienti di A. Un A-modulo $I \subseteq K$ si dice ideale frazionario se esiste $d \in A$ non nullo tale che $dI \subseteq A$

Proposizione 2.8. Sia $I \subseteq K$ un A-modulo finitamente generato. Allora I è un ideale frazionario.
Viceversa, se A è noetheriano e I è un ideale frazionario di A, allora I è finitamente generato come A-modulo.

Dimostrazione. La prima implicazione è ovvia: è sufficiente prendere un insieme di generatori finito e scegliere come d il prodotto dei denominatori. Viceversa, $dI \subseteq A$ è finitamente generato e dunque I sarà generato dai generatori di dI divisi per d. □

L'insieme degli ideali frazionari è un monoide; infatti se I, J sono ideali frazionari di A, l'ideale

$$IJ \coloneqq \langle ij \mid i \in I,\ j \in J \rangle$$

è un ideale frazionario: se $aI \subseteq A$ e $bJ \subseteq A$, allora $abIJ \subseteq A$. Vogliamo mostrare che in realtà è un gruppo; definiamo l'ideale inverso come

$$I^{-1} \coloneqq \{x \in K \mid xI \subseteq A\}$$

Proposizione 2.9.

1. I^{-1} è un ideale frazionario di A
2. $II^{-1} \subseteq A$
3. Se I, J sono ideali frazionari e $IJ = A$, allora $J = I^{-1}$ e $I = J^{-1}$.

Dimostrazione. Chiaramente $II^{-1} \subseteq A$, da cui (2). Da questo segue anche (1): infatti preso $a \in I$ non nullo, $aI^{-1} \subseteq A$. Se $IJ = A$, allora $J \subseteq I^{-1}$. D'altra parte, $A = IJ \subseteq II^{-1} \subseteq A$ e dunque abbiamo $IJ = II^{-1}$ da cui segue l'altro contenimento. □

Definizione 2.10. Sia I un ideale frazionario non nullo. I si dice invertibile se $II^{-1} = A$.

Teorema 2.11. Sia A un dominio di Dedekind. Allora ogni ideale massimale di A è invertibile.

Dimostrazione. Sia $m \subseteq A$ un ideale massimale; vogliamo mostrare l'uguaglianza $mm^{-1} = A$. Sicuramente $m^{-1} \supseteq A$ perchè per definizione contiene 1. Allora

$$m \subseteq mm^{-1} \subseteq A$$

Inoltre sappiamo che mm^{-1} è un ideale di A. Per massimalità di m, $mm^{-1} = m$ oppure $mm^{-1} = A$. Supponiamo per assurdo che $mm^{-1} = m$ e mostriamo che questo implica allora $m^{-1} = A$. Per questo, basta mostrare che se $x \in m^{-1}$, allora $x \in A$.
Sia $x \in m^{-1}$. Allora

$$xm \subseteq m \Rightarrow x^n m \subseteq m \ \forall n \in \mathbb{N}$$

Di conseguenza, dato $d \in m$, si ha $x^n d \in m$ per ogni n, cioè $x^n \in d^{-1}m$ per ogni n da cui

$$A[x] \subseteq d^{-1}A$$

Di conseguenza $A[x]$ è finitamente generato su A perché sottomodulo di $d^{-1}A$ e dunque x è intero su A. Ma A è integralmente chiuso e quindi $m^{-1} = A$. Questo è assurdo perché, dato $a \in m$, aA è un ideale non nullo di un anello noetheriano e dunque contiene un prodotto $P_1, \dots, P_r$ di ideali primi. Possiamo supporre che r sia minimo e

$$m \supseteq aA \supseteq P_1 \dots P_r \Rightarrow m = P_1 \text{ per scansamento}$$

Sia $I = P_2 \dots P_r$. Allora $aA \not\supset I$ e $aA \supseteq mI$. Allora esiste $\alpha \in I$ tale che $\alpha \notin aA$.

$$a^{-1}\alpha m \subseteq A$$

e dunque $a^{-1}\alpha \in m$, da cui un assurdo. □

Riassumendo, nel caso dei domini di Dedekind, $\mathcal{I}(R)$, l'insieme degli ideali frazionari, è un monoide rispetto al prodotto e ogni ideale di R è invertibile. Se consideriamo un ideale P^n, con P ideale primo di R, allora P^n è invertibile, perché

$$P^n P^{-n} = (PP^{-1})^n = R$$

Corollario 2.12. Siano $P_1, \dots, P_r$ ideali primi di un dominio di Dedekind R e siano $e_1, \dots, e_r \in \mathbb{Z}$. Allora

$$I = P_1^{e_1} \dots P_r^{e_r}$$

è invertibile.

Dimostrazione. I è frazionario, perché gli ideali frazionari sono chiusi rispetto al prodotto. Mostriamo che

$$I^{-1} = P_1^{-e_1} \dots P_r^{-e_r}$$

è invertibile, ma questo è ovvio per commutatività e per quanto mostrato. □

Teorema 2.13. Sia R un dominio di Dedekind. Ogni ideale frazionario di R si scrive in modo unico come prodotto di ideali primi.

$$I = P_1^{e_1} \dots P_r^{e_r}$$

Inoltre, se $I \subseteq R$, allora $e_i \geq 0$.

Dimostrazione. Mostriamo che se $I \subseteq R$, allora $I = P_1^{e_1} \dots P_r^{e_r}$ con $e_i \geq 0$. Da questo segue il caso generale; se I è un ideale frazionario e $dI \subseteq R$, allora $I = (d)^{-1} dI$.
Consideriamo l'insieme

$$\mathcal{F} = \{I \subseteq R \mid I \text{ non si scrive come prodotto di ideali primi}\}$$

Supponiamo per assurdo che $\mathcal{F}$ sia non vuoto; per noetherianità esisterebbe un elemento massimale J che non è primo. J è allora contenuto in un ideale massimale P, che ammette inverso P^{-1}. Allora

$$J \subseteq P^{-1}J \subseteq PP^{-1} = R$$

dove il primo contenimento si ha perché $P^{-1} \supseteq R$.
Mostriamo che $J \subsetneq JP^{-1}$. Se fosse $J = JP^{-1}$, esisterebbe $x \in P^{-1}$ tale che

$$xJ \subseteq J \qquad\qquad x^n J \subseteq J$$

Dunque se $d \in J$, $dx^n \in J$ e quindi $R[x] \subseteq d^{-1}R$ che implicherebbe $x \in R$ dato che R è integralmente chiuso. Quindi $P^{-1} \subseteq R$, cioè $P^{-1} = R$. Ma allora $R = PP^{-1} = PR = P$, da cui un assurdo.
Allora $J \subsetneq P^{-1}J$ e quest'ultimo si fattorizza per massimalità di J. Possiamo allora scrivere

$$P^{-1}J = P_1^{e_1} \dots P_r^{e_r}$$

da cui $J = PP_1^{e_1} \dots P_r^{e_r}$ e questo conclude l'esistenza.
Mostriamo ora l'unicità. Supponiamo

$$\prod_{p \in P} p^{e_p} = \prod_{p \in P} p^{a_p}$$

dove P è l'insieme degli ideali primi e e_p, a_p quasi tutti nulli. Allora

$$P_1^{b_1} \dots P_r^{b_r} = Q_1^{c_1} \dots Q_t^{c_t}$$

con $c_i > 0$, $b_i > 0$ e $P_i \neq Q_j$ per ogni i, j. In particolare $P_1^{b_1} \supseteq Q_1^{c_1} \dots Q_t^{c_t}$ e per scansamento $P_1 = Q_i$, assurdo. Dunque le due fattorizzazioni coincidono. □

Corollario 2.14. Gli ideali frazionari formano un gruppo.

Chiamiamo il gruppo degli ideali frazionari $\mathcal{F}(R)$, che è un gruppo abeliano libero per unicità della fattorizzazione. Studieremo il quoziente di $\mathcal{F}(R)$ per gli ideali principali, il gruppo delle classi di ideali.

$$Cl(K) := {}^{\mathcal{F}(K)}\!/_{\mathcal{P}(K)}$$

Dato $I \subseteq \mathcal{O}_k$, consideriamo la sua fattorizzazione $I = p_1^{e_1} \dots p_t^{e_t}$. Indichiamo con $e_i = e_{p_i}(I)$ la massima potenza di p che compare nella fattorizzazione di I.

In particolare, l'unicità della fattorizzazione fornisce la buona definizione della mappa

$$\begin{array}{rccc} e_p\colon & \mathcal{F}(K) & \longrightarrow & \mathbb{Z} \\ & I & \longmapsto & e_p(I) \end{array}$$

che è una valutazione. In particolare

- $e_p(IJ) = e_p(I) + e_p(J)$
- $I \subseteq \mathcal{O}_k \iff e_p(I) \geq 0$ per ogni $p \in \mathrm{Spec}(\mathcal{O}_k)$
- Se $I \subseteq J$, allora $e_p(I) \geq e_p(J)$ (perché $I \subseteq J \iff IJ^{-1} \subseteq \mathcal{O}_k$)
- $I \mid J$ (cioè $\exists L \subseteq \mathcal{O}_k$ tale che $J = IL$) $\iff J \subseteq I$. Infatti, se $JI^{-1} \subseteq \mathcal{O}_k$, allora $I(I^{-1}J) = J$ e dunque $I \mid J$.

Si può anche definire il massimo comune divisore e il minimo comune multiplo. Si verifica che essi possono essere trovati nel modo solito a partire dalla fattorizzazione.

Esempio. Se I, J sono ideali frazionari, $\gcd(I, J) = I + J$. Basta mostrare che $I + J \mid I$, $I + J \mid J$ e che se $L \mid I$ e $L \mid J$, allora $L \mid I + J$. Questo è chiaro perchè $I, J \subseteq I + J$ e se $I, J \subseteq L$, allora $I + J \subseteq L$ e dunque $L \mid I + J$.

Proposizione 2.15. Sia $I \subseteq \mathcal{O}_k$. Allora $\forall \alpha \in I$ esiste $\beta \in I$ tale che $I = (\alpha, \beta)$.

Dimostrazione. Notiamo che $I = (\alpha, \beta)$ se e solo se $I = \gcd(\alpha, \beta)$ e dunque è sufficiente mostrare quest'ultima condizione. I ammette una fattorizzazione in ideali primi

$$I = \prod_{i=1}^{n} Q_i^{e_i}$$

Se $\alpha \in I$, allora $(\alpha) \subseteq I$ e dunque $I \mid (\alpha)$.

$$(\alpha) = J_1 \prod_{i=1}^{n} Q_i^{a_i}$$

con $a_i \geq e_i$ e $Q_i \nmid J_1$. Dunque, se β esiste,

$$(\beta) = J_2 \prod_{i=1}^{n} Q_i^{s_i}$$

dove $Q_i \nmid J_2$ e $\min(s_i, a_i) = e_i$. Mostriamo che un tale elemento β esiste per il Teorema Cinese del Resto. Imponiamo che $\beta \in Q_i^{e_i} \setminus Q_i^{e_i+1}$ e $\beta \notin J_1$. Consideriamo per ogni i un β_i tale che $\beta_i \in Q_i^{e_i} \setminus Q_i^{e_i+1}$.

$$\begin{cases} \beta \equiv \beta_i & (\mathrm{mod}\ Q_i^{e_i+1}) \\ \beta \equiv 1 & (\mathrm{mod}\ J_2) \end{cases}$$

e questo ha soluzione per il teorema cinese. □

Proposizione 2.16. $\mathcal{O}_k$ è PID se e solo se $\mathcal{O}_k$ è UFD.

Dimostrazione. Una implicazione è ovvia. Mostriamo la contronominale dell'altra. Supponiamo quindi che $\mathcal{O}_k$ non sia PID. Allora esiste $P \subseteq \mathcal{O}_k$ ideale primo non principale.

$$\mathcal{F} = \{I \subseteq \mathcal{O}_k \mid PI \text{ è principale}\}$$

Notiamo che $\mathcal{F}$ è non vuoto perché $P^{-1} \subseteq \frac{\mathcal{O}_k}{d}$, con $d \in \mathcal{O}_k$. Quindi

$$P(dP^{-1}) = d(PP^{-1}) = (d)$$

Per noetherianità, $\mathcal{F}$ ammette un elemento massimale. Sia $M \in \mathcal{F}$ un tale elemento, cioé $PM = (\alpha)$. Mostriamo che α è irriducibile.

$$\alpha = \beta\gamma \Rightarrow (\alpha) = (\beta)(\gamma) = PM$$

Supponiamo $\beta = PL$; allora $L \mid M$ e $M \subseteq L$. Per massimalità di L, $M = L$ e dunque $\alpha \sim \beta$ da cui α irriducibile.
Mostriamo che α non è primo. Dato che $\alpha = PM$, sia $\beta \in P \setminus (\alpha)$ e $\gamma \in M \setminus \alpha$; esistono perché hanno una fattorizzazione diversa. Ma $\beta\gamma \in PM = (\alpha)$. □

Dimostrazione alternativa. È sufficiente mostrare che ogni primo non nullo P di $\mathcal{O}_k$ è principale. Sia $f \in P$ un elemento non nullo; f ammette una fattorizzazione in irriducibili

$$f = q_1 \dots q_k$$

e per primalità dell'ideale uno di questi fattori appartiene a P. Senza perdità di generalità possiamo supporre $q_1 \in P$. Allora (q_1) genera un ideale primo contenuto in P. Ma $\mathcal{O}_k$ ha dimensione 1 e dunque $P = (q_1)$, da cui la tesi. □

Una dimostrazione alternativa della fattorizzazione unica In realtà è possibile dare una definizione differente dei domini di Dedekind:

Definizione 2.17. Sia A un dominio noetheriano. A è un dominio di Dedekind se A_p è un dominio a valutazione discreta per ogni p primo non nullo di A.

Le definizioni date sono equivalenti; dimostrare che quest'ultima definizione implica la prima è facile, in quanto essere integralmente chiuso è una proprietà locale. Il viceversa è più complicato e dunque non lo dimostriamo. Questa definizione rende più agevole la dimostrazione della proprietà di fattorizzazione unica. Infatti essere invertibile è una proprietà locale:

Proposizione 2.18. Sia A un dominio e sia I un ideale frazionario. Allora

1. I_p è frazionario per ogni primo $p \subseteq A$
2. I è invertibile se e solo se I_p è invertibile per ogni primo $p \subseteq A$

Dimostrazione.

1. Sia $d \in A$ tale che $dI \subseteq A$. Allora
$$\frac{d}{1} I_p \subseteq A_p$$
2. Se I è invertibile, allora $II^{-1} = A$. Localizzando, si ottiene $I_p I_p^{-1} = A_p$. Viceversa, supponiamo $I_p I_p^{-1} = A_p$ per ogni primo $p \subseteq A$ e sia $J = II^{-1} \subseteq A$. Allora $J_p = I_p I_p^{-1} = A_p$, cioè $J \not\subset p$ per ogni primo p. Di conseguenza, $J = A$ da cui la tesi.

□

Lemma 2.19. Sia A un dominio a valutazione discreta. Allora ogni ideale frazionario di A è invertibile.

Dimostrazione. Sia I un ideale frazionario di A e sia $d \in A$ tale che $dI \subseteq A$. Se $dI = A$, allora $(d) = I^{-1}$. Supponiamo allora che $(a) = dI \subseteq m$, dove $m = (x)$ è l'ideale massimale di A. Allora

$$a^{-1}dI \subseteq a^{-1}(a)$$

e $1 \in a^{-1}(a)$. Di conseguenza, detto $J = (a^{-1}d)$, $IJ \supseteq A$ e l'altro contenimento è ovvio. □

Teorema 2.20. Sia A un dominio di Dedekind. Ogni ideale frazionario è invertibile.

Dimostrazione. Sia I un ideale frazionario. Allora per ogni p primo di A I_p è un ideale frazionario di A_p e dunque per il lemma invertibile. Di conseguenza, I_p è invertibile per ogni primo p e quindi I è invertibile. □

2.2 Grado di Inerzia e Indice di Ramificazione

Siano $K \subseteq F$ campi di numeri e sia I un ideale frazionario. Abbiamo visto che I ammette una fattorizzazione

$$I = \prod Q_i^{e_i}$$

dove ogni Q_i è un ideale di $\mathcal{O}_F$ e $e_i \in \mathbb{Z}$. Sia $P \subseteq \mathcal{O}_K$ un ideale primo. Vogliamo ora studiare come si comporta la fattorizzazione dell'estensione

$$P\mathcal{O}_F = \prod P_i^{a_i}$$

Mostreremo che gli esponenti che compaiono nella fattorizzazione devono rispettare alcune formule.

Definizione 2.21. Sia $Q \subseteq \mathcal{O}_F$. Diciamo che P sta sotto Q se P è la contrazione di Q in $\mathcal{O}_K$; nello stesso caso, diciamo che Q sta sopra P.

Per ogni Q ideale di $\mathcal{O}_F$, esiste un unico primo che sta sotto Q. Invece,

Proposizione 2.22. Sia P un primo di $\mathcal{O}_K$. Allora l'insieme dei primi di $\mathcal{O}_F$ sopra P coincide con l'insieme dei primi nella fattorizzazione di $P\mathcal{O}_F$.

Dimostrazione. Innanzitutto, mostriamo che $P\mathcal{O}_F$ è un ideale proprio. Sicuramente $P^{-1} \supsetneq \mathcal{O}_K$; sia quindi $x \in P^{-1} \setminus \mathcal{O}_K$. Allora

$$(xP)\mathcal{O}_F \subseteq \mathcal{O}_K\mathcal{O}_F \subseteq \mathcal{O}_F$$

Se $P\mathcal{O}_F = \mathcal{O}_F$, allora $x = x1 \in \mathcal{O}_F$ e dunque $x \in \mathcal{O}_F \cap K = \mathcal{O}_K$, da cui un assurdo.
Mostriamo ora che i due insiemi dell'enunciato coincidono. $P\mathcal{O}_F$ ammette una fattorizzazione in ideali primi di $\mathcal{O}_F$:

$$P\mathcal{O}_F = \prod Q_i^{e_i} \subseteq Q_i$$

Allora $Q_i \cap \mathcal{O}_K \supseteq P$ e dunque vale l'uguaglianza perché $\dim(\mathcal{O}_K) = 1$. Viceversa, se $Q \cap \mathcal{O}_K = P$, allora $P\mathcal{O}_F \subseteq Q$ e quindi $Q = Q_i$ per un certo i. □

Una facile e importante conseguenza della proposizione è che i primi sopra un ideale P sono in numero finito.

Definizione 2.23. Sia P un ideale primo di $\mathcal{O}_K$ e sia $P\mathcal{O}_F = \prod Q_i^{e_i}$ la fattorizzazione della sua estensione in $\mathcal{O}_F$. Definiamo l'indice di ramificazione di Q_i in P come

$$e_i = e(Q_i \mid P) = e_{Q_i}(P\mathcal{O}_F)$$

Sia Q_i uno dei primi sopra P. Allora

$$A = \mathcal{O}_F \big/ Q_i$$

è un campo. Possiamo considerare la composizione

$$\mathcal{O}_K \longrightarrow \mathcal{O}_F \longrightarrow A$$

che ha come nucleo la contrazione di Q_i, cioé P. Di conseguenza $\mathcal{O}_K \big/ P$ è un sottocampo di $\mathcal{O}_F \big/ Q_i$.

Definizione 2.24. Definiamo grado di inerzia di Q_i su P come il grado dell'estensione di campi

$$\left[\mathcal{O}_F \big/ Q_i : \mathcal{O}_K \big/ P\right] = f(Q_i \mid P) = f_i$$

Proposizione 2.25. Sia $[K : \mathbb{Q}] = n$ e sia $x \in K$. Allora

$$N_{K/\mathbb{Q}}(x) = \left|\mathcal{O}_K \big/ x\mathcal{O}_K\right|$$

Dimostrazione. Dall'equazione 1.4,

$$\operatorname{disc}_{K/\mathbb{Q}}(x\mathcal{O}_K) = \left|\mathcal{O}_K \big/ x\mathcal{O}_K\right|^2 \operatorname{disc} \mathcal{O}_k$$

Inoltre, per il teorema 1.21 esiste una base diagonale $e_1, \dots, e_n$ di $\mathcal{O}_K$ tale che $xe_1, \dots, xe_n$ sia una base di $x\mathcal{O}_K$.

$$\operatorname{disc}(xe_1, \dots, xe_n) = \det(\varphi_x)^2 \operatorname{disc}(e_1, \dots, e_n)$$

dove φ_x è la matrice che rappresenta l'applicazione di moltiplicazione per x. Si conclude perché $|\det(\varphi_x)| = N(x)$. □

Definizione 2.26. Sia $I \subseteq \mathcal{O}_K$. Definiamo

$$N(I) \coloneqq \left|\mathcal{O}_K \big/ I\right|$$

Il teorema precedente si riformula dicendo che

$$|N_{K/\mathbb{Q}}(x)| = N(x\mathcal{O}_K)$$

Il lemma 2.4 implica che la norma di un ideale è finita, il teorema seguente mostra che la norma è moltiplicativa.

Proposizione 2.27. Siano I, J ideali di $\mathcal{O}_k$. Allora

$$N(IJ) = N(I)N(J)$$

Dimostrazione.

$$N(IJ) = \left|\mathcal{O}_k/IJ\right| \qquad\qquad N(I) = \left|\mathcal{O}_k/I\right|$$

Se I, J sono comassimali, la tesi segue dal teorema cinese del resto. Quindi è sufficiente vedere che $N(P)^d = N(P^d)$ per ogni ideale primo P; infatti basta considerare la fattorizzazione e applicare il teorema cinese del resto.

$$N(P^n) = \left|\mathcal{O}_k/P^n\right| \stackrel{?}{=} \left|\mathcal{O}_k/P\right|^n$$

Consideriamo la catena di ideali

$$P^n \subsetneq P^{n-1} \subsetneq \cdots \subsetneq P \subsetneq \mathcal{O}_K$$

Allora

$$\left|\mathcal{O}_K/P^m\right| = \prod \left|P^i/P^{i+1}\right|$$

Mostriamo che che $|P^i/P^{i+1}| = |\mathcal{O}_K/P|$. Consideriamo l'applicazione

$$\begin{array}{rccc} \phi\colon & \mathcal{O}_k & \longrightarrow & P^i/P^{i+1} \\ & \alpha & \longrightarrow & x\alpha + P^{i+1} \end{array}$$

dove $x \in P^i \setminus P^{i+1}$. Questo è un omomorfismo di $\mathbb{Z}$-moduli. Il nucleo è proprio P

$$\mathrm{Ker}(\phi) = \{\alpha \in \mathcal{O}_k \mid x\alpha \in P^{i+1}\} = P$$

e dunque passa al quoziente $\mathcal{O}_k/P \to P^i/P^{i+1}$. Mostriamo allora la surgettività; da questo seguirebbe la tesi. D'altronde,

$$\phi(\mathcal{O}_k) = \left(x\mathcal{O}_k + P^{i+1}\right)/P^{i+1} = P^i/P^{i+1}$$

□

Teorema 2.28. Sia $[F\colon K] = n$ un'estensione di campi di numeri. Sia $P \subseteq \mathcal{O}_K$ un ideale primo e consideriamo la fattorizzazione dell'estensione

$$P\mathcal{O}_F = \prod_{i=1}^{r} Q_i^{e_i}$$

Allora vale

$$\sum_{i=1}^{r} e_i f_i = [F\colon K]$$

Dimostrazione. Per moltiplicatività della norma (proposizione 2.27),

$$N(P\mathcal{O}_F) = \prod_{i=1}^{r} N(Q_i)^{e_i}$$

Per definizione di grado di inerzia,

$$N(Q_i) = \left|\mathcal{O}_F/Q_i\right| = \left|\mathcal{O}_k/P\right|^{f_i} = N(P)^{f_i}$$

e dunque otteniamo la relazione

$$N(P\mathcal{O}_F) = N(P)^{\sum_{i=1}^{n} e_i f_i}$$

Basta mostrare allora che $N(P\mathcal{O}_F) = N(P)^n$.
Se $K = \mathbb{Q}$, $P = (p)$ con $p \in \mathbb{Z}$, allora

$$N(P\mathcal{O}_f) = \left|N_{F/\mathbb{Q}}(p)\right| = p^n \tag{2.1}$$

e dunque avremmo concluso.
Nel caso generale, abbiamo l'inclusione

$$\mathcal{O}_K/P \longrightarrow \mathcal{O}_F/P\mathcal{O}_F$$

e questo rende $\mathcal{O}_F/P\mathcal{O}_F$ uno spazio vettoriale. Basta allora mostrare che

$$\dim_{\mathcal{O}_K/p} \mathcal{O}_F/P\mathcal{O}_F = n$$

Verifichiamo che valgono le due disuguaglianze. Mostriamo prima che dati $n+1$ elementi, questi sono sempre linearmente dipendenti; questo darebbe la disuguaglianza $\leq$. Siano $\alpha_1, \ldots, \alpha_{n+1} \in O_F$; sono linearmente dipendenti su K e dunque lo sono anche su $\mathcal{O}_K$. Di conseguenza, esistono $b_1, \ldots, b_{n+1} \in O_K$ non tutti nulli tali che

$$\sum_{i=1}^{n+1} b_i \alpha_i = 0$$

Vorremmo ora ridurre modulo P tale relazione, ma bisogna prima sincerarsi che non tutti i b_i stiano in $P\mathcal{O}_k$. In particolare, mostriamo che i b_i possono essere scelti in modo che esista j tale che $b_j \notin P$. Consideriamo l'ideale $B = (b_1, \ldots, b_{n+1})$. Tale ideale è invertibile (perché non tutti i b_i sono nulli) e dunque esiste $b \in B^{-1}$ tale che $bB \not\subseteq P\mathcal{O}_K$. A meno di cambiare $b_1, \ldots, b_{n+1}$ con bb_i possiamo supporre che almeno uno dei b_i non stia in P. Di conseguenza

$$\dim_{\mathcal{O}_K/p} \mathcal{O}_F/P\mathcal{O}_F \leq n$$

Sia ora $m = [K\colon \mathbb{Q}]$ e sia $n = [F\colon K]$ e sia p la contrazione di P a $\mathbb{Z}$. Estendiamo p a $\mathcal{O}_K$ e a $\mathcal{O}_F$

$$p\mathcal{O}_K = \prod_{i=1}^{s} P_i^{\epsilon_i} \qquad\qquad p\mathcal{O}_F = \prod_{i=1}^{s} (P_i\mathcal{O}_K)^{\epsilon_i}$$

Passando alle norme, per l'equazione 2.1,

$$p^{nm} = \prod N(P_i\mathcal{O}_F)^{\epsilon_i} = \prod (N(P_i)^{n_i})^{\epsilon_i}$$

con $n_i \leq n$ per quanto già mostrato all'inizio della dimostrazione. Dato che

$$N(P_i) = p^{f(P_i|p)}$$

si ottiene

$$p^{nm} = p^{\sum f(P_i|p)n_i\epsilon_i} = p^{\sum n_i(\epsilon_i f(P_i|p))} \leq p^{n\sum \epsilon_i f(P_i|p)} \leq p^{nm}$$

e vale l'uguaglianza se e solo se $n = n_i$ per ogni i. □

Proposizione 2.29 (moltiplicatività del grado di inerzia e dell'indice di ramificazione)**.** Consideriamo una torre di estensioni di campi di numeri

$$\begin{array}{cc} \mathbb{Q} & \mathbb{Z} \\ | & \\ K & \mathcal{O}_K \\ | & \\ F & \mathcal{O}_F \\ | & \\ L & \mathcal{O}_L \end{array}$$

Sia P un primo di $\mathcal{O}_K$ e siano $Q \subseteq \mathcal{O}_F$ un primo su P e $U \subseteq \mathcal{O}_L$ un primo su Q. Allora

$$e(U|P) = e(U|Q)e(Q|P) \qquad\qquad f(U|P) = f(U|Q)f(Q|P)$$

Dimostrazione. Scriviamo le fattorizzazioni:

$$P\mathcal{O}_F = \prod_{i=1}^{n} Q_i^{s_i} \qquad\qquad Q_i\mathcal{O}_L = \prod_{j=1}^{m_i} U_{i,j}^{t_{i,j}}$$

Otteniamo allora

$$P\mathcal{O}_L = (P\mathcal{O}_F)\mathcal{O}_L = \prod Q_i^{s_i}\mathcal{O}_L = \prod_{i=1}^{n}(Q_i\mathcal{O}_L)^{e(Q_i|P)} = \prod_{i=1}^{n}\prod_{j=1}^{m_i} U_{i,j}^{e(U_{i,j}|Q_i)e(Q_i|P)}$$

da cui $e(U_{i,j}|Q_i)e(Q_i|P) = e(U_i|P)$ per unicità della fattorizzazione, come voluto. Per quanto riguarda il grado di inerzia, vogliamo mostrare che

$$\left[\mathcal{O}_F/U_{i,j} : \mathcal{O}_K/P\right] = \left[\mathcal{O}_F/U_{i,j} : \mathcal{O}_L/Q_i\right]\left[\mathcal{O}_L/Q_i : \mathcal{O}_K/P\right]$$

e questo segue dal teorema sul grado nelle torri di estensione.

□

Vogliamo ora studiare il comportamento dell'estensioni di ideali quando L/K è un'estensione di Galois. In questo caso, il gruppo di Galois $G = \mathrm{Gal}(L/K)$ agisce sugli ideali primi di $\mathcal{O}_L$. In particolare, l'azione è transitiva:

Proposizione 2.30. Sia $P \subseteq \mathcal{O}_K$ un ideale primo. Allora G agisce transitivamente sui primi sopra P.

Dimostrazione. Scriviamo la fattorizzazione:

$$P\mathcal{O}_L = \prod_{i=1}^{n} Q_i^{e_i}$$

Applicando $\sigma \in G$, otteniamo

$$\underbrace{\sigma(P)\mathcal{O}_L}_{=P\mathcal{O}_L} = \prod_{i=1}^{n} \sigma(Q_i)^{e_i}$$

dove P viene fissato perché $P \subseteq \mathcal{O}_K \subseteq K = \mathrm{Fix}(G)$. Di conseguenza, per unicità di fattorizzazione,

$$\{Q_1, \dots, Q_n\} = \{\sigma(Q_1), \dots, \sigma(Q_n)\}$$

Mostriamo che l'azione è transitiva. Siano Q, Q' primi sopra P. Procediamo per assurdo e supponiamo che $\sigma(Q) \neq Q'$ per ogni $\sigma \in G$. Allora esiste $\alpha \in Q'$ tale che $\alpha \notin \sigma(Q)$ per ogni σ. Se infatti $\cup\sigma(Q) \supseteq Q'$, per il lemma di scansamento esisterebbe $\bar{\sigma} \in G$ tale che $\bar{\sigma}(Q) = Q'$. Applicando la norma a α, $N(\alpha) \in Q' \cap \mathcal{O}_K = P$. Ma $\sigma(\alpha) \notin Q$ per ogni σ e dunque

$$\prod \sigma(\alpha) = N(\alpha) \in P \subseteq Q$$

da cui un assurdo. □

Corollario 2.31. Sia L/K un'estensione di Galois. Allora

$$P\mathcal{O}_L = (\prod_i Q_i)^e$$

Gli indici di ramificazione e di inerzia non dipendono da i.

Dimostrazione. Siano $i \neq j$. Allora esiste $\sigma \in G$ tale che $\sigma(Q_i) = Q_j$ e per unicità di fattorizzazione ogni esponente deve essere uguale. Mostriamo ora l'enunciato sugli indici di inerzia. Consideriamo il diagramma commutativo

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/Q_i & \to & \mathcal{O}_L/Q_j \end{array}$$

dove $Q_j = \sigma(Q_i)$. La mappa tra i quozienti è un isomorfismo e questo dimostra l'enunciato. □

Vediamo le applicazioni di questi risultati. Nel caso $n = 2$, possiamo avere 3 tipi di fattorizzazioni:

$$P\mathcal{O}_L = \begin{cases} Q_1Q_2 & e = f = 1 \\ Q & f = 2\ e = 1 \\ Q^2 & e = 2\ f = 1 \end{cases}$$

Per $n = 3$, le fattorizzazioni possibili sono le seguenti:

$$P\mathcal{O}_L = \begin{cases} Q_1Q_2Q_3 & e_i = f_i = 1 \\ Q_1Q_2 & f_1 = 2\ f_2 = 1 \\ Q & f = 3 \\ Q_1^2Q_2 & f = 1 \\ Q^3 & \end{cases}$$

Gli spezzamenti non sono però tutti realizzabili; per esempio se L/K è di Galois, non è possibile che $P\mathcal{O}_L = Q_1Q_2$ o $P\mathcal{O}_L = Q_1^2Q_2$.

Sia $L = K(\alpha)$ un campo di grado n su K e $\tilde{L}$ la chiusura normale di L con gruppo di Galois $G = \mathrm{Gal}(\tilde{L}/K)$. Il gruppo G si immerge in S_n tramite l'azione sui coniugati di α, ad ogni elemento $g \in G$ si può associare il vettore di interi $(g_1, g_2, \ldots, g_k)$ dove g_i sono le lunghezze dei cicli di g in S_n ordinate in modo decrescente. Si considerano i punti fissi di g come cicli di lunghezza uno, quindi si ha $\sum_{i=1}^{k} g_i = n$. Il vettore non dipende dall'immersione scelta quindi possiamo definire il tipo di g come il vettore $(g_1, \ldots, g_k)$.

Se un primo p che non ramifica in $\mathcal{O}_L$ possiamo definire il suo tipo come il vettore $(f_1, f_2, \ldots, f_r)$ con gli f_i ordinati in modo decrescente. Anche in questo caso si ha $\sum_{i=1}^{r} f_i = n$. Dato che solo un numero finito di primi ramifica possiamo enunciare il seguente risultato, senza dimostrazione:

Teorema 2.32 (di densità di Chebotarev)**.** Sia $L/\mathbb{Q}$ un'estensione finita e sia $G = \mathrm{Gal}(\tilde{L}/\mathbb{Q})$, dove $\tilde{L}$ è la chiusura normale.

$$d\{p \in \mathbb{Z} \mid p\mathcal{O}_L \text{ ha fattorizzazione di tipo } F\} = \frac{\{\sigma \in G < S_n \mid \sigma \text{ di tipo } F\}}{|G|}$$

Con densità d intendiamo

$$d(X) = \lim_{n\to\infty} \frac{X \cap \{1, \ldots, n\}}{\mathcal{P}_n}$$

Dove $\mathcal{P}_n$ si intende il numero di primi minori o uguali a n. Per un insieme qualsiasi il limite potrebbe non esistere, il teorema ne afferma anche l'esistenza.

Per esempio, per $n = 3$, supponiamo $\mathrm{Gal}(\tilde{L}/\mathbb{Q}) = S_3$. Allora

densità	*classe di coniugio*	*tipo*
$d\{p \mid p\mathcal{O}_L = P_1P_2P_3\} = \frac{1}{6}$	Id	$(1,1,1)$
$d\{p \mid p\mathcal{O}_L = P_1P_2\} = \frac{1}{2}$	2-*cicli*	$(2,1)$
$d\{p \mid p\mathcal{O}_L = P\} = \frac{1}{3}$	3-*cicli*	(3)

Teorema 2.33. Sia $p \in \mathbb{Z}$. Allora p è ramificato in K se e solo se $p \mid \mathrm{disc}(K)$.

Mostriamo per il momento solo l'implicazione $\Rightarrow$, l'altra implicazione sarà dimostrata nel teorema 3.15.

Dimostrazione. Sia $p \in \mathbb{Z}$ un primo e supponiamo che $p\mathcal{O}_K$ sia ramificato. La fattorizzazione sarà allora del tipo

$$p\mathcal{O}_K = PI$$

con $e(P|p) \geq 2$. Sia $\alpha_1, \ldots, \alpha_n$ base intera di $\mathcal{O}_K$; per definizione $\mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. Vogliamo mostrare che $p \mid \mathrm{disc}(K)$; per mostrare che vale questa relazione di divisibilità, è più comodo cambiare base in modo che il discriminante non cambi per un fattore p. Dato che $e(P|p) \geq 2$, esiste un elemento $\alpha \in I$ tale che $\alpha \notin p\mathcal{O}_K$; notiamo allora che α appartiene a ogni primo sopra p di $\mathcal{O}_K$ ma non a $p\mathcal{O}_K$. In termini della base intera,

$$\alpha = \sum_{i=1}^{n} m_i\alpha_i \quad m_i \in \mathbb{Z}$$

il fatto che $\alpha \notin p\mathcal{O}_K$ è equivalente alla condizione che esista un indice i tale che $p \nmid m_i$. Senza perdita di generalità possiamo supporre $i = 1$. Allora

$$\operatorname{disc}(\alpha, \alpha_2, \dots \alpha_n) = (m_1)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)$$

perché la matrice di cambiamento di base è una matrice triangolare con elementi diagonali tutti 1 eccetto il primo (che è proprio m_1). Dunque $p \mid \operatorname{disc}(K)$ se e solo se $p \mid \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$. Siano $\sigma_1, \dots, \sigma_n$ le immersioni di K in $\mathbb{C}$ e sia L la chiusura normale di K su $\mathbb{Q}$. Per definizione,

$$\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \vdots & & & \vdots \\ \sigma_n(\alpha) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

Siano $\tilde{\sigma}_1, \dots, \tilde{\sigma}_n$ le estensioni di $\sigma_1, \dots, \sigma_n$ a L. Siano $Q_1, \dots, Q_s \subseteq \mathcal{O}_L$ tutti e soli i primi sopra p. Allora α appartiene a Q_i per ogni i dato che α appartiene a ogni primo sopra p in $\mathcal{O}_K$.

$$\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det \begin{pmatrix} \tilde{\sigma}_1(\alpha) & \tilde{\sigma}_1(\alpha_2) & \dots & \tilde{\sigma}_1(\alpha_n) \\ \vdots & & & \vdots \\ \tilde{\sigma}_n(\alpha) & \tilde{\sigma}_n(\alpha_2) & \dots & \tilde{\sigma}_n(\alpha_n) \end{pmatrix}^2$$

Ogni elemento della prima colonna della matrice appartiene a tutti i primi $Q_i \subseteq \mathcal{O}_L$ sopra P. Di conseguenza, $\operatorname{disc}(K) \in \mathbb{Z} \cap (\cap Q_i) \subseteq p\mathbb{Z}$, come voluto. □

Corollario 2.34. Sia $K = \mathbb{Q}(\alpha)$ con α intero su $\mathbb{Z}$. Se $p \nmid N(\mu'_\alpha(\alpha))$, allora p non è ramificato in K.

Corollario 2.35. Supponiamo L/K sia un'estensione finita. Allora solo un numero finito di primi di K ramifica in L.

Dimostrazione. Per $K = \mathbb{Q}$ coincide con il teorema. Sia ora $P \subseteq \mathcal{O}_K$ un primo ramificato in L. Allora $p = P \cap \mathbb{Z}$ è ramificato in L per moltiplicatività dell'indice di ramificazione. Il corollario segue, dato che i primi di $\mathbb{Z}$ che dividono il discriminante $p \mid \operatorname{disc}(L)$ sono in numero finito e i primi di $\mathcal{O}_K$ sopra i divisori del discriminante sono anch'essi in numero finito. □

Il teorema può anche essere raffinato: Sia K/L un'estensione di campi di numeri e sia P un primo di $\mathcal{O}_K$. Sappiamo che $\mathcal{O}_L/P\mathcal{O}_L$ è uno spazio vettoriale di dimensione n su $\mathcal{O}_K/P$. Infatti, per il teorema cinese del resto,

$$\mathcal{O}_L \big/ P\mathcal{O}_L = \mathcal{O}_L \big/ Q_1^{e_1} \dots Q_r^{e_r} = \prod_{i=1}^{r} \mathcal{O}_L \big/ Q_i^{e_i}$$

e, come spazio vettoriale, $\mathcal{O}_L/Q_i^{e_i} \simeq (\mathcal{O}_L/Q_i)^{e_i}$.

Proposizione 2.36. Sia $\mathcal{B}_i = \{b_1^{(i)}, \dots, b_{f_i}^{(i)}\}$ una $\mathcal{O}_K/P$-base di $\mathcal{O}_L/Q_i$. Per ogni $i = 1, \dots, r$ e per ogni $j = 1, \dots, e_i$ scegliamo un elemento

$$\alpha_{i,j} \in (Q_i^{j-1} \setminus Q_i^j) \cap \Big(\bigcap_{h \neq i} Q_h^{e_h} \Big)$$

Allora l'insieme $\{\alpha_{ij} b_\lambda^{(i)}\}_{i,j,\lambda}$ è una base di $\mathcal{O}_L/P\mathcal{O}_L$ su $\mathcal{O}_K/P$.

Dimostrazione. Consideriamo una combinazione lineare nulla modulo $P\mathcal{O}_L$

$$\sum_{i,j,\lambda} s_{ij\lambda}\alpha_{ij}b_\lambda^{(i)} = 0 \pmod{P\mathcal{O}_L}$$

Mostriamo che ogni $a_{ij\lambda} \equiv 0 \pmod{P\mathcal{O}_L}$. Supponiamo $P\mathcal{O}_L = \prod Q_j^{e_j}$. Per ogni primo Q_t della fattorizzazione di $P\mathcal{O}_L$, vale

$$\sum_{i,j,\lambda} s_{ij\lambda}\alpha_{ij}b_\lambda^{(i)} \equiv 0 \pmod{Q_t}$$

Dato che per $i \neq t$ abbiamo per ipotesi $\alpha_{ij} \in Q_t$, otteniamo la somma

$$\sum_{j,\lambda} s_{tj\lambda}\alpha_{tj}b_\lambda^{(t)} = 0 \pmod{Q_t}$$

Ma $\alpha_{tj} \in Q_t^{j-1}$ e dunque rimane nella somma solo $j = 1$,

$$\alpha_{t1}\sum_{\lambda} s_{t1\lambda}b_\lambda^{(t)} \equiv 0 \pmod{Q_t}$$

Dato che $\alpha_{t1} \notin Q_t$ e Q_t è primo, otteniamo

$$\sum_{\lambda} s_{t1\lambda}b_\lambda^{(t)} \equiv 0 \pmod{Q_t}$$

e dato che i $b_\lambda^{(t)}$ sono una base, i coefficienti sono nulli. Se $Q_t^2 | P\mathcal{O}_L$, consideriamo la congruenza modulo Q_t^2 e otteniamo che anche i coefficienti $s_{t2\lambda} = 0 \pmod{P}$ e così via. Iterando, si ottiene la tesi. □

Proposizione 2.37. Sia $K = \mathbb{Q}$, L un campo di numeri e $P = p\mathbb{Z}$.

1. Se $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ sono indipendenti modulo $p\mathcal{O}_L$, allora $p \nmid |\mathcal{O}_L/G|$, dove $G = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}}$.
2. $p^k \mid \operatorname{disc}(L)$ per $k = n - \sum_{i=1}^r f_i = \sum_{i=1}^r (e_i - 1)f_i$

Dimostrazione.

1. Se per assurdo $p \mid |\mathcal{O}_L/G|$, allora esisterebbe $\beta \in \mathcal{O}_L \setminus G$ tale che $p\beta \in G$.

   $$p\beta = \sum_{i=1}^n \lambda_i\alpha_i \quad \lambda_i \in \mathbb{Z}$$

   Dato che $\beta \notin G$, esiste un indice i tale che $p \nmid \lambda_i$; altrimenti potremmo dividere ogni coefficiente per p e trovare β. D'altronde, riducendo modulo $p\mathcal{O}_L$,

   $$\sum \lambda_i\alpha_i = 0 \pmod{p\mathcal{O}_L}$$

   e per indipendenza $\lambda_i \equiv 0 \pmod{p}$, contro le ipotesi. Dunque $p \nmid |\mathcal{O}_L/G|$.

2. Da punto 1 segue che se $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ sono indipendenti modulo p, $p^k \mid \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ se e solo se $p^k \mid \operatorname{disc}(\mathcal{O}_L)$. Basta allora mostrare che $p^k \mid \operatorname{disc}(\gamma_1, \dots, \gamma_n)$, dove i $\gamma_i \in \mathcal{O}_L$ sono indipendenti modulo p. Per la proposizione precendente, possiamo trovare una base del tipo $\alpha_{ij} b_\lambda^{(i)}$; calcoliamo allora il discriminante di tali elementi. Per farlo, utilizziamo la matrice delle tracce.

$$p^k \mid \operatorname{disc}(\gamma_1, \dots, \gamma_n) = \det(\operatorname{Tr}(\gamma_l \gamma_m))$$

Sia $\tilde{L}$ la chiusura di Galois di L/K; osserviamo che $\alpha_{ij} b_\lambda^{(i)} \alpha_{i'j'} b_{\lambda'}^{(i')} \in Q$ per ogni primo Q di $\mathcal{O}_{\tilde{L}}$ sopra p e per ogni $j > 1$. In questo caso, avremmo concluso perché

$$\operatorname{Tr}(\alpha_{ij} b_\lambda^{(i)} \alpha_{i'j'} b_{\lambda'}^{(i')}) \in p \qquad \forall\, j > 1$$

Per la scelta degli α_{ij}, questo è vero esattamente per $\sum (e_i - 1) f_i$ indici (gli elementi $\alpha_{i,1}$ non appartengono a Q_i) e per multilinearità del determinante otteniamo la tesi.

□

2.3 Il Teorema di Kummer

Definizione 2.38. Sia F/K un'estensione di campi di numeri e sia $P \subseteq \mathcal{O}_K$ un primo. A seconda della fattorizzazione dell'estensione $P\mathcal{O}_F$, diremo che

- P è totalmente ramificato se $P\mathcal{O}_F = Q^n$
- P è inerte se $P\mathcal{O}_F = Q$
- P si spezza completamente se $P\mathcal{O}_F = Q_1 \dots Q_n$ (cioè $f_i = e_i = 1$).

Per l'elemento primitivo, possiamo supporre $F = K(\alpha)$ con α intero. Sia T il polinomio minimo di α su $\mathcal{O}_K$: sappiamo che $\deg(T) = n = [F : K]$. Sia P un primo di $\mathcal{O}_K$ e sia $\bar{T}$ la proiezione di T su $\mathcal{O}_K/P$. Supponiamo $\bar{T}$ si fattorizzi modulo P

$$\bar{T}(x) = \prod \bar{T}_i^{e_i}$$

Il teorema di Kummer lega tale fattorizzazione alla fattorizzazione dell'estensione:

Teorema 2.39 (di Kummer)**.** Sia $p = P \cap \mathbb{Z}$ e supponiamo $p \nmid |\mathcal{O}_F/\mathcal{O}_K[\alpha]| = \operatorname{ind}(\alpha)$. Allora

$$P\mathcal{O}_F = \prod_{i=1}^{r} Q_i^{e_i}$$

dove gli e_i e r sono quelli della fattorizzazione di $\bar{T}$ e

$$\left[\mathcal{O}_F \big/ Q_i : \mathcal{O}_K \big/ P \right] = \deg(\bar{T}_i)$$

Inoltre $Q_i = (P, T_i(\alpha))$ dove T_i è uno dei qualsiasi sollevamenti monici di $\bar{T}_i$ in $\mathcal{O}_K[x]$.

Il teorema fornisce un metodo per la fattorizzazione di estensioni di primi. Purtroppo esistono estensioni tale che ogni elemento intero ha indice divisibile per uno stesso primo di $\mathbb{Z}$; vedremo un esempio.

Osservazione 2.40. Sappiamo che detti $f_i = \deg(T_i)$, sappiamo che $\deg T = n = \sum e_i f_i$ e questo torna con l'enunciato

Dimostrazione. Sia $Q_i = (P, T_i(x))$. Il teorema segue dai seguenti:

1. Per ogni indice i, o $\mathcal{O}_F/Q_i$ è un campo e $[\mathcal{O}_F/Q_i : \mathcal{O}_K/P] = \deg T_i$ o $\mathbb{Q}_i = \mathcal{O}_F$.
2. Per ogni indice i, j, $Q_i + Q_j = \mathcal{O}_F$
3. $P\mathcal{O}_F \mid \prod Q_i^{e_i}$

Infatti, sappiamo che i Q_i o sono primi non nulli o sono ideali banali. Supponiamo in particolare che $Q_1, \dots Q_s$ siano primi e $Q_{i+1} \dots Q_r = \mathcal{O}_F$. Allora $P\mathcal{O}_F \mid Q_1^{e_1} \dots Q_s^{e_s}$. Ne segue che $P\mathcal{O}_F = Q_1^{d_1} \dots Q_s^{d_s}$ con $e_i \geq d_i \geq 0$ per ogni i. Da questa fattorizzazione, $n = \sum_{i=1}^{s} d_i f_i = \sum_{i=1}^{r} e_i f_i$. Ma visto che le somme sono di numeri positivi e sono uguali, ogni termine deve essere uguale e dunque $s = r$ e $e_i = d_i$. Mostriamo ora i tre punti.

1. Consideriamo
$$F_i = {}^{\mathcal{O}_K}\!\diagup_{P[x]}\!\diagup_{(\bar{T}_i(x))}$$
Questo è un campo e $[F_i \colon \mathcal{O}_K/P] = \deg \bar{T}_i = f_i$. Osserviamo che la composizione φ data da $\mathcal{O}_K[x] \to \mathcal{O}_K/P[x] \to F_i$ è surgettiva e ha come nucleo
$$\mathrm{Ker}(\varphi) = \{a \in \mathcal{O}_K[x] \mid \bar{a}(x) \in (\bar{T}_i)\} = (P, T_i(x))$$
dove $T_i(x)$ è un qualsiasi sollevamento monico. Chiaramente vale $\supseteq$. Viceversa, se $\bar{a}(x)$ sta nel nucleo, possiamo dividere per $T_i(x)$ e
$$a(x) = q(x)T_i(x) + \underbrace{r(x)}_{\in P\mathcal{O}_K[x]}$$
Dunque $\mathcal{O}_K[x]/(P, T_i(x)) \simeq F_i$. Di conseguenza $Q_i = (P, T_i(x))$ è un ideale primo. Si poteva vedere questo punto anche con il secondo teorema di omomorfismo o per motivi dimensionali.
Consideriamo ora la composizione ψ
$$\begin{array}{ccccc} \mathcal{O}_K[x] & \longrightarrow & \mathcal{O}_K[\alpha] & \longrightarrow & \mathcal{O}_F/Q_i \\ x & \longmapsto & \alpha & \longmapsto & \alpha + Q_i \end{array}$$
Il nucleo è
$$\mathrm{Ker}(\psi) = \{a \in \mathcal{O}_K[x] \mid a(\alpha) \in Q_i\}$$
Sicuramente $\mathrm{Ker}(\psi) \supseteq P$ e $\mathrm{Ker}(\psi) \supseteq T_i(x)$ e dunque contiene $(P, T_i(x))$; questo è un ideale massimale perché il quoziente è un campo. Di conseguenza, $\mathrm{Ker}(\psi)$ può essere solo
$$\mathrm{Ker}(\psi) = \begin{cases} \mathcal{O}_K[x] \\ (P, T_i(x)) = Q_i \end{cases}$$

Mostriamo che ψ è surgettiva. Per definizione

$$\mathrm{Im}(\psi) = \{a(\alpha) + Q_i\} = \mathcal{O}_K[\alpha] + Q_i \stackrel{?}{=} \mathcal{O}_F$$

Per mostrare l'uguaglianza, facciamo vedere che $\mathcal{O}_K[\alpha] + Q_i$ ha indice 1 o equivalentemente che l'indice non è divisibile per nessun primo $p \in \mathbb{Z}$. Valgono i contenimenti

$$\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_K[\alpha] + p\mathcal{O}_F \subseteq \mathcal{O}_F \qquad p\mathcal{O}_F \subseteq \mathcal{O}_k[\alpha] + p\mathcal{O}_F \subseteq \mathcal{O}_F$$

Dunque

$$\left|\mathcal{O}_F/(\mathcal{O}_k[\alpha] + p\mathcal{O}_F)\right| \text{ divide } \left(\left|\mathcal{O}_F/\mathcal{O}_K[\alpha]\right|, \left|\mathcal{O}_F/p\mathcal{O}_F\right|\right)$$

Sappiamo che il secondo termine del massimo comune divisore è una potenza di p (esattamente $p^{[F:\mathbb{Q}]}$), mentre l'altro non è divisibile per p per ipotesi. Dunque otteniamo le uguaglianza cercate e ψ è surgettiva. Da questo segue allora che il nucleo $\mathrm{Ker}(\psi)$ non può essere tutto l'anello, cioè $\mathrm{Ker}(\psi) = Q_i$. Per il primo teorema di omomorfismo,

$$F_i = \mathcal{O}_K[x]/(P, T_i(x)) \simeq \mathcal{O}_F/Q_i$$

e abbiamo visto che F_i ha grado $f_i = \deg(T_i)$ su $\mathcal{O}_K/P$, da cui segue il punto 1.

2. Mostriamo la comassimalità. Sappiamo che in $\mathcal{O}_k/P[x]$ $(\bar{T}_i, \bar{T}_j) = 1$ e dunque $Q_i \neq Q_j$; dato che entrambi sono ideali primi in un anello di Dedekind, sono anche comassimali. Alternativamente, per Bezout si ha

$$\bar{a}(x)\bar{T}_i(x) + \bar{b}(x) + \bar{T}_j(x) = \bar{1}$$

cioè, come congruenza,

$$a(x)T_i(x) + b(x)T_j(x) = 1 + P\mathcal{O}_K[x]$$

Valutando in α, otteniamo

$$a(\alpha)T_i(\alpha) + b(\alpha)T_j(\alpha) \in 1 + P\mathcal{O}_K[\alpha] \subseteq 1 + P\mathcal{O}_F$$

e quindi $1 \in (P, T_i(\alpha), T_j(\alpha)) = Q_i + Q_j$.

3. Mostriamo che $P\mathcal{O}_F \mid \prod Q_i^{e_i}$, cioè

$$P\mathcal{O}_F \supseteq Q_1^{e_1} \dots Q_r^{e_r} = \prod_{i=1}^{r} (P, T_i(\alpha))^{e_i}$$

Notiamo che vale

$$\prod_{i=1}^{r} (P, T_i(\alpha))^{e_i} \subseteq (P, T_1(\alpha)^{e_1} \dots T_r(\alpha)^{e_r})$$

Se mostriamo che quest'ultimo è contenuto in $P\mathcal{O}_F$, a maggior ragione lo sarà $\prod Q_i^{e_i}$. Dato che $T(x) = \prod T_i(x)^{e_i} \pmod P$, si ottiene

$$T(\alpha) - \prod T_i(\alpha)^{e_i} \in P\mathcal{O}_F$$

Inoltre $T(\alpha) = 0$ da cui $\prod T_i(\alpha)^{e_i} \in P\mathcal{O}_F$ e quindi la tesi.

□

Possiamo ora enunciare e dimostrare un corollario della proposizione 1.39

Corollario 2.41. Sia $K = \mathbb{Q}(\alpha)$ e supponiamo che μ_α sia p-Eisenstein. Allora $p\mathcal{O}_K = Q^n$ è totalmente ramificato in K.

Dimostrazione. Per la proposizione 1.39, $p \nmid \mathrm{ind}(\alpha)$ e si può utilizzare il teorema di Kummer con il polinomio μ_α. Dato che il polinomio è di p-Eisenstein, $\mu_\alpha \equiv x^n \pmod p$ da cui la tesi. □

Applichiamo ora il teorema alle estensioni quadratiche e a quelle ciclotomiche.

Fattorizzazione nelle estensioni quadratiche Studiamo il caso di $\mathbb{Q}(\sqrt{m})$, con m libero da quadrati. Sappiamo che

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2,3 \pmod 4 \quad \mathrm{disc}(K) = 4m \\ \mathbb{Z}[1+\sqrt{m}/2] & m \equiv 1 \pmod 4 \quad \mathrm{disc}(K) = m \end{cases}$$

Mostriamo che

- se $p \mid m$,
$$p\mathcal{O}_K = (p, \sqrt{m})^2$$
- se p è dispari e $p \nmid m$, allora
$$p\mathcal{O}_K = \begin{cases} (p, n-\sqrt{m})(p, n+\sqrt{m}) & m \equiv n^2 \pmod p \\ (p) & m \not\equiv \square \pmod p \end{cases}$$
- se $p = 2$ e $p \nmid m$
$$2\mathcal{O}_K = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod 4 \\ (2, 1+\sqrt{m}/2)(2, 1-\sqrt{m}/2) & m \equiv 1 \pmod 8 \\ (2) & m \equiv 5 \pmod 8 \end{cases}$$

Sia $T(x) = x^2 - m$; fattorizziamolo modulo p:

$$T(x) \equiv x^2 - m \pmod p$$

- Se $p \mid m$, allora $T \equiv x^2 \pmod p$ e dunque $p\mathcal{O}_K = (p, \sqrt{m})^2$.
- Se $p \nmid m$ e $m = n^2$ è un quadrato, otteniamo $T(x) = (x-n)(x+n)$ da cui $p\mathcal{O}_K = (p, \sqrt{m} - n)(p, \sqrt{m} + n)$.
- Se $m \neq n^2$, allora T è irriducibile modulo p e $p\mathcal{O}_K = (p)$.

Rimane il caso $p = 2$.

- Se $p \mid m$, $m \equiv 2 \pmod 4$, possiamo ancora fattorizzare $T(x)$ e quindi $T(x) \equiv x^2$ e $2\mathcal{O}_K = (2, \sqrt{m})^2$.
- Se $m \equiv 3 \pmod 4$, si ha $T(x) = (x+1)^2$ e $2\mathcal{O}_K = (2, \sqrt{m}+1)^2$.

- Se $m \equiv 1 \pmod 4$, allora scegliamo il polinomio $H(x)$ come il polinomio minimo di $1 + \sqrt{m}/2$, che è

$$H(x) = x^2 - x + \frac{1-m}{4}$$

Otteniamo i sottocasi:

  - Se $m \equiv 1 \pmod 8$, allora $H(x) \equiv x^2 + x \pmod 2$ e dunque $2\mathcal{O}_K = (2, 1 + \sqrt{m}/2)(2, 1 - \sqrt{m}/2)$.
  - Se $m \equiv 5 \pmod 8$, allora $H(x) \equiv x^2 + x + 1 \pmod 2$ e dunque è irriducibile. Di conseguenza, $2\mathcal{O}_K = (2)$ è inerte.

Fattorizzazione nelle estensioni ciclotomiche

Studiamo il caso delle estensioni ciclotomiche $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta)$. Dato che queste sono estensioni di Galois, troveremo gradi di inerzia e di ramificazione tutti uguali.

Proposizione 2.42. Sia $p \in \mathbb{Z}$ un primo e supponiamo $m = p^k n$ con $(n, p) = 1$. Allora

$$p\mathcal{O}_K = \prod_{i=1}^{r} Q_i^e$$

dove $e = \phi(p^k)$, $f = ord^*_{\mathbb{Z}_n} p$ e $ref = \phi(m)$.

Dimostrazione. Consideriamo dapprima il caso $m = p^k$. Allora

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(p^k)$$

Mostriamo che p è totalmente ramificato. Sappiamo che il polinomio minimo $\mu \mid x^{p^k} - 1 = \mu(x)g(x)$ e che $\mathcal{O}_K = \mathbb{Z}[\zeta]$. D'altronde, $x^m - 1$ è una potenza p-esima modulo p e dunque $\mu \equiv (x-1)^{\phi(p^k)} \pmod p$. Abbiamo ottenuto in questo caso

$$p\mathcal{O}_K = Q^{\phi(p^k)}$$

Con $Q = (1-\zeta)$. Se $(m, p) = 1$, abbiamo ancora $\mu \mid x^m - 1$, che ha radici semplici modulo p per il criterio della derivata. Di conseguenza μ ha radici semplici e p non ramifica. Potevamo dedurre questo anche dal fatto che $p \nmid \operatorname{disc}(K)$, che è una potenza di m. Inoltre,

$$\mathcal{O}_K \big/ Q_i = \mathbb{Z}[\zeta] \big/ Q_i = \mathbb{F}_p[\bar{\zeta}_m]$$

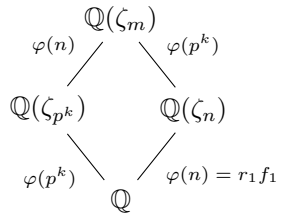
e quindi

$$\left[\mathcal{O}_K \big/ Q_i : \mathbb{F}_p\right] = \deg \underbrace{\mu_{\bar{\zeta}}}_{\in \mathbb{F}_p[x]}$$

Notiamo che $\bar{\zeta}$ è una radice n-esima primitiva dell'unità in $\overline{\mathbb{F}}_p$ e dunque

$$\mathbb{F}_p[\bar{\zeta}] = \mathbb{F}_{p^k}$$

dove $k = ord_{\mathbb{Z}/n\mathbb{Z}^*_n} p$.
Nel caso generale, sia $m = p^k n$ con $(n, p) = 1$. Consideriamo il diagramma



con gradi delle estensioni indicati vicino alle frecce. Sappiamo che

$$p\mathcal{O}_L = (Q_1 \dots Q_r)^e$$

con $fer = \phi(p^k)\phi(n)$ e la moltiplicatività nelle torri fornisce

- $\phi(p^k) \leq e$ perché $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})} = (p, 1-\zeta_{p^k})^{\phi(p^k)}$.
- $\phi(n) \leq rf$ dall'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$.
- $f_1 = \mathrm{ord}_{\mathbb{F}_p^*} n \mid f$

Di conseguenza $e = \phi(p^k)$ e $rf = \phi(n)$. Visto che $f_1 \leq f$, $r_1 \leq r$ e $f_1 r_1 = \phi(n)$ si hanno le uguaglianze $f_1 = f$ e $r = r_1$, come voluto. □

Il teorema di Kummer purtroppo non funziona in tutti i casi. Se l'anello degli interi è monogenico, allora è sempre possibile utilizzarlo, perché l'indice del generatore è banalmente 1. Esistono però casi in cui l'anello degli interi non è monogenico. In questo caso, si potrebbe pensare di cambiare generatore e procedere nel modo seguente:

- Sia $\alpha \in \mathcal{O}_K$ e sia $k = \mathrm{ind}(\alpha)$
- Se $p \nmid k$, usiamo il polinomio minimo di α
- Se $p \mid k$, cerchiamo $\beta \in \mathcal{O}_K$ tale che $p \nmid \mathrm{ind}(\beta)$

Purtroppo, non sempre esiste un tale β; infatti è possibile che l'indice di ogni elemento sia divisibile per uno stesso primo p.

Definizione 2.43. Sia K un campo di numeri e supponiamo $[K : \mathbb{Q}] = n$. Definiamo

$$\mathrm{ind}(K) = \gcd\{\mathrm{ind}(\alpha) \mid \alpha \in \mathcal{O}_K \text{ di grado } n\}$$

Ci poniamo quindi i seguenti problemi:

Esiste un'estensione $K/\mathbb{Q}$ tale che $\mathrm{ind}(K) = 1$ e $\mathcal{O}_K$ non sia monogenico?
Esiste un'estensione $K/\mathbb{Q}$ tale che $\mathrm{ind}(K) > 1$?

Esempio. Sia $K = \mathbb{Q}(\sqrt[3]{m})$, con $m = ab^2$ e $(a, b) = 1$. Allora $\mu_\alpha = x^3 - m$. Supponiamo $m \not\equiv \pm 1 \pmod 9$; abbiamo visto nel paragrafo 1.4 che in questo caso $\mathrm{disc}(K) = -27a^2b^2$ e $1, \alpha, \frac{\alpha^2}{b}$ è una base intera. Mostriamo che $\mathrm{ind}(K) = 1$.

$$\mathrm{ind}(\alpha) = \left(\frac{\mathrm{disc}(\alpha)}{\mathrm{disc}(K)}\right)^{\frac{1}{2}} = b$$

$$\mathrm{ind}\left(\frac{\alpha^2}{b}\right) = \left(\frac{\mathrm{disc}(\alpha^2/b)}{\mathrm{disc}(K)}\right)^{\frac{1}{2}} = a$$

e dunque $\mathrm{ind}(K) = 1$.
Mostriamo che non esistono interi di indice 1. Sia $w \in \mathcal{O}_K$. Allora

$$w = x + y\alpha + z\frac{\alpha^2}{b}$$

con $x, y, z \in \mathbb{Z}$. Notiamo che $\mathrm{ind}(w) = \mathrm{ind}(w - x)$, perché generano lo stesso $\mathbb{Z}$-modulo e dunque hanno lo stesso discriminante. Dunque possiamo supporre

$$w = y\alpha + z\frac{\alpha^2}{b} \qquad\qquad w^2 = y^2\alpha^2 + 2yzab + z^2a\alpha$$

Calcoliamo l'indice di w rispetto alla base $1, \alpha, \alpha^2/b$.

$$\mathrm{ind}(w) = \left|\det \begin{pmatrix} 1 & 0 & 2yzab \\ 0 & y & z^2a \\ 0 & z & by^2 \end{pmatrix}\right| = |y^3b - z^3a|$$

Mostriamo che esistono $a, b \in \mathbb{Z}$ tali che

- $ab^2 \not\equiv \pm 1 \pmod 9$
- $y^3b - z^3a \neq \pm 1 \quad \forall y, z \in \mathbb{Z}$

Scegliamo $a = 7$, $b = 5$. La prima condizione è banalmente soddisfatta. D'altronde, la seconda equazione non ha soluzione in $\mathbb{Z}$ perché non ha soluzioni modulo 7. Infatti,

$$5y^3 \equiv \pm 1 \pmod 7$$

gli unici cubi modulo 7 sono ± 1.

Esempio (Dedekind). Mostriamo che esiste un'estensione $[K : \mathbb{Q}] = 3$ con $\mathrm{ind}(K) = 2$. Consideriamo il polinomio $\mu_\alpha(x) = x^3 - x^2 - 2x - 8$; questo è irriducibile su $\mathbb{Q}$ perché non ha radici e dunque $K = \mathbb{Q}(\alpha)$ ha grado 3 su $\mathbb{Q}$. Il discriminante di α

$$\mathrm{disc}(\alpha) = \mathrm{disc}(\mu(\alpha)) = N(\mu'_\alpha(\alpha)) = -4 \cdot 503$$

Per la formula di cambio di base 1.4, $\mathrm{disc}(\alpha)$ coincide con $\mathrm{disc}(K)$ a meno di un quadrato; dunque l'unico fattore eliminabile è un 2. In realtà, $\mathrm{disc}(K) = -503$. Infatti, sia

$$\beta = \frac{\alpha^2 + \alpha}{2}$$

Allora $\text{disc}(1, \alpha, \beta) = -503$ ma va verificato che β sia intero, che si vede calcolando il polinomio minimo. Infatti,

$$\begin{aligned} \alpha^3 - \alpha^2 - 2\alpha - 8 = 0 &\iff \alpha^3 + \alpha^2 - 2\alpha^2 - 2\alpha - 8 = 0 \\ &\iff \alpha(2\beta) - 4\beta - 8 = 0 \\ &\iff \alpha = \frac{2\beta + 4}{\beta} \end{aligned}$$

Sostituendo quest'ultima uguaglianza nel polinomio minimo di α e moltiplicando per β^3, otteniamo

$$(2\beta + 4)^3 - \beta(2\beta + 4)^2 - 2\beta^2(2\beta + 4) - 8\beta^3 = 0$$

Svolgendo, si arriva alla relazione

$$\beta^3 - 3\beta^2 - 10\beta - 8 = 0$$

e quindi β è intero.
Sia $\xi = b\alpha + c\beta$ un elemento generico; allora

$$\xi^2 = (6c^2 + 8bc) + (2c^2 - b)\alpha + (2b^2 + 3c^2 + 4bc)\beta$$

Calcoliamo $\text{ind}(\xi)$ e mostriamo che è divisibile per 2.

$$\text{ind}(\xi) = \left| \det \begin{pmatrix} 1 & 0 & 6c^2 + 8bc \\ 0 & b & 2c^2 - b^2 \\ 0 & c & 2b^2 + 3c^2 + 4b \end{pmatrix} \right| \equiv bc^2 + b^2c \equiv bc(b + c) \equiv 0 \pmod 2$$

Dunque l'indice di ogni elemento è divisibile per 2 e $\text{ind}(K) \equiv 0 \pmod 2$. Dato che $\text{ind}(\alpha) = 2$, si ha l'uguaglianza $\text{ind}(K) = 2$. Di conseguenza, $\mathcal{O}_K$ non è monogenico e $2\mathcal{O}_K$ non si fattorizza con il teorema di Kummer. Si poteva anche scoprire in un altro modo. Infatti vale

$$2\mathcal{O}_K = P_1 P_2 P_3$$

ma non esistono 3 polinomi distinti di grado 1 in $\mathbb{F}_2[x]$.

Lemma 2.44. Sia $f \in \mathbb{Z}[x]$ un polinomio di grado positivo. Allora esistono infiniti primi $p \in \mathbb{Z}$ tali che f ha una radice modulo p.

Dimostrazione. Notiamo che se f ha una radice in $\mathbb{Z}$, l'enunciato è ovvio; possiamo quindi supporre che f non abbia radici in $\mathbb{Z}$. Supponiamo $f(0) = 1$; mostreremo poi che possiamo sempre ricondurci a questo caso. Procediamo per assurdo e supponiamo che l'insieme $\{p_1, \ldots, p_r\}$ sia l'insieme dei primi per il quale f ha una radice modulo p. Sia $n > p_i$ per ogni i e consideriamo $f(n!)$. Per quanto supposto, $f(n!) \neq 0$ e possiamo assumere che sia diverso da ± 1 a meno di scegliere un n più grande, dato che i polinomi sono illimitati all'infinito. Sia allora p un primo tale che $p \mid f(n!)$; allora $p \neq p_i$ per ogni i. Infatti $p_i \nmid f(n!)$ perché $p_i \mid n!$ ma $p_i \nmid 1$.
Nel caso generale, possiamo considerare il polinomio

$$g(x) = \frac{f(xf(0))}{f(0)} \in \mathbb{Z}[x]$$

e ripetere il ragionamento. □

Proposizione 2.45. Sia $K \subseteq L$ campi di numeri. Allora esistono infiniti primi di K che si spezzano completamente in L.

Dimostrazione.

M
$|$
L
$|$
K
$|$
$\mathbb{Q}$

Consideriamo la torre $M \supseteq L \supseteq K \supseteq \mathbb{Q}$ con $M/\mathbb{Q}$ di Galois, $M = \mathbb{Q}(\alpha)$ con $\alpha \in \mathbb{A}$. Sia $\mu_\alpha \in \mathbb{Z}[x]$ il polinomio minimo di α. Per il teorema di Kummer 2.39, tutti i primi $p \in \mathbb{Z}$ che non dividono l'indice di α si fattorizzano come μ_α modulo p. Sia

$$\mathcal{P}_M = \{p \in \mathbb{Z} \mid \exists U \subseteq \mathcal{O}_M \;\; U \mid p \;\; f(U|p) = 1\}$$

Per il lemma precedente 2.44 e per il teorema di Kummer 2.39, $\mathcal{P}_M$ è infinito. Sia $p \in \mathcal{P}_M$; l'estensione di p in $\mathcal{O}_M$ si fattorizza

$$p\mathcal{O}_M = (U_1 \dots U_s)^e \qquad\qquad f(U_i|p) = 1$$

con $es = [M : \mathbb{Q}]$. Notiamo che i primi ramificati sono in numero finito per il corollario 2.35. Allora

$$|\mathcal{P}_M| - |\{\text{primi ramificati}\}| = \infty$$

e questi sono proprio i primi cercati. Dunque esistono infiniti primi di $\mathbb{Z}$ che si spezzano completamente in M. Sia ora P un primo di $\mathcal{O}_K$; per la formula della torre di estensione, dato che $P\mathcal{O}_M$ si spezza completamente, anche $P\mathcal{O}_L$ si spezza completamente. □

Corollario 2.46 (Dirichlet, forma debole)**.** Per ogni intero m esistono infiniti primi p tali che $p \equiv 1 \pmod{m}$.

Dimostrazione. Sia $K = \mathbb{Q}(\zeta_m)$. Allora esistono infiniti primi di $\mathbb{Z}$ che si spezzano completamente in $\mathcal{O}_K$. Per definizione, p si spezza completamente se e solo se $e = f = 1$. Ma $f = 1$ implica $p \equiv 1 \pmod{m}$ per la proposizione 2.42. □

Esempio. Consideriamo $K = \mathbb{Q}(\zeta_7)$ e studiamo l'estensione dei primi in questo caso. Sappiamo che il primo 7 è totalmente ramificato per 2.42 e quindi

$$7\mathcal{O}_K = P^6$$

Per gli altri primi, possiamo utilizzare il teorema di Kummer. Dunque

$$p\mathcal{O}_K = \begin{cases} Q & f = 6 \quad p^6 \equiv 1 \pmod{6} \\ Q_1Q_2 & f = 3 \quad p^3 \equiv 1 \pmod{6} \\ Q_1Q_2Q_3 & f = 2 \quad p^2 \equiv 1 \pmod{6} \\ Q_1 \dots Q_6 & f = 1 \quad p \equiv 1 \pmod{6} \end{cases}$$

Il teorema di Chebotarev fornisce

$$d(\{p \in \mathbb{Z} \mid p\mathcal{O}_K = Q_1Q_2Q_3\}) = \frac{|\{\text{cicli di tipo } 2+2+2\}|}{|G|} = \frac{1}{6}$$

Notiamo che questo dipende dall'immersione: se avessimo realizzato il gruppo di Galois come $\mathbb{Z}_2 \times \mathbb{Z}_3$, il risultato sarebbe stato diverso; il teorema di Chebotarev richiede di utilizzare un elemento primitivo. L'immersione di G in S_n data dal teorema di Cayley risolve questo problema.

Capitolo 3

Estensioni Normali

3.1 Gruppo di Decomposizione e Gruppo di Inerzia

Sia L/K un'estensione normale e sia G il gruppo di Galois di L su K. Sappiamo che G agisce su L e sull'anello degli interi $\mathcal{O}_L$. Sia Q un ideale primo di $\mathcal{O}_L$. L'azione sugli ideali primi fornisce il diagramma commutativo

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/\mathrm{Ker}(\phi) & \xrightarrow[\bar{\sigma}]{} & \mathcal{O}_L/Q \end{array}$$

Notiamo che $\mathrm{Ker}(\phi) = \sigma^{-1}(Q)$ e dunque ogni primo che sta sotto $\sigma^{-1}(Q)$ sta sotto Q.
Studiamo il caso particolare in cui $\sigma^{-1}(Q) = Q$.

Definizione 3.1. Lo stabilizzatore di Q in G si chiama gruppo di decomposizione.

$$D(Q|P) = \{\sigma \in G \mid \sigma(Q) = Q\} = \mathrm{Stab}_G(Q)$$

In questo caso particolare,

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/Q & \xrightarrow[\bar{\sigma}]{} & \mathcal{O}_L/Q \end{array}$$

l'omomorfismo indotto sui campi residui risulta essere un automorfismo e dunque è un elemento del gruppo di Galois $\bar{\sigma} \in \mathrm{Gal}(\mathcal{O}_L/Q/\mathcal{O}_K/P) = \bar{G}$. Possiamo definire un'applicazione

$$\begin{array}{rccc} \psi\colon & D(Q|P) & \longrightarrow & \bar{G} \\ & \sigma & \longmapsto & \bar{\sigma} \end{array}$$

In generale tale applicazione non è iniettiva, ma ha come nucleo

$$\begin{aligned}\mathrm{Ker}(\psi) &= \{\sigma \in D(Q|P) \mid \bar{\sigma}(\bar{\alpha}) = \bar{\alpha} \ \ \forall \alpha \in \mathcal{O}_L\} \\ &= \{\sigma \in D(Q|P) \mid \sigma(\alpha) \equiv \alpha \pmod{Q} \ \forall \alpha \in \mathcal{O}_L\}\end{aligned}$$

Definizione 3.2. Chiamiamo il nucleo di ψ gruppo di inerzia e lo denotiamo con $E(Q|P)$.

Dunque

$$D(Q|P)/E(Q|P) \longrightarrow \bar{G} = \mathrm{Gal}\left(\mathcal{O}_L/Q \Big/ \mathcal{O}_K/P\right)$$

Di conseguenza, E è un sottogruppo normale e

$$\left|D/E\right| \, |f(Q|P)$$

Per il teorema di corrispondenza di Galois, possiamo associare a questi sottogruppi dei sottocampi:

$$\begin{array}{cc} L & Q \\ | & | \\ L_E & Q_E = Q \cap \mathcal{O}_{L_E} \\ | & | \\ L_D & Q_D = Q \cap \mathcal{O}_{L_D} \\ | & | \\ K & P = Q \cap \mathcal{O}_K \end{array}$$

Supponiamo $[L : K] = n$ e sia Q un primo di $\mathcal{O}_L$ sopra P. Chiamiamo e l'indice di ramificazione, f il grado di inerzia di Q su P e r il numero di primi distinti che compaiono nella fattorizzazione di $P\mathcal{O}_L$. Siano Q_D e Q_E le contrazioni di Q rispettivamente a L_D e L_E. Studiamo gli indici di ramificazione e il grado di inerzia di tali primi.

$$\begin{array}{ccccc} & & & \textit{indice di ramificazione} & \textit{grado di inerzia} \\ L & & Q & & \\ | \, e & & | & e & 1 \\ L_E & & Q_E = Q \cap \mathcal{O}_{L_E} & & \\ | \, f & & | & 1 & \mathrm{f} \\ L_D & & Q_D = Q \cap \mathcal{O}_{L_D} & & \\ | \, r & & | & 1 & 1 \\ K & & P = Q \cap \mathcal{O}_K & & \end{array}$$

- Mostriamo che $[L_D : K] = r$. Per corrispondenza di Galois, sappiamo che questo è uguale a $[G : D] = [G : \mathrm{Stab}_G(Q)] = |\,\mathrm{Orb}_G(Q)| = r$ perchè l'azione del gruppo di Galois sui primi sopra P è transitiva.
- Mostriamo ora che $f(Q|Q_E) = 1$. Per definizione,

$$f(Q|Q_E) = \left[\mathcal{O}_L/Q : \mathcal{O}_{L_E}/Q_E\right]$$

Per il teorema dell'elemento primitivo, esiste un elemento $\bar{\alpha} \in \mathcal{O}_L/Q$ tale che $\mathcal{O}_L/Q = \mathcal{O}_{L_E}/Q_E(\bar{\alpha})$. Mostriamo allora che il polinomio minimo di $\bar{\alpha}$ è lineare. Consideriamo il polinomio

$$g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha))$$

dove $\alpha \in \mathcal{O}_L$ è un elemento che si proietta su $\bar{\alpha}$. Notiamo che $g \in \mathcal{O}_{L_E}[x]$ perché è fissato da E per definizione. Riducendo modulo Q_E, otteniamo

$$\bar{g}(x) = \prod (x - \bar{\sigma}(\bar{\alpha})) = (x - \bar{\alpha})^{|E|}$$

per definizione di gruppo di inerzia. Il polinomio minimo di $\bar{\alpha}$ su $\mathcal{O}_{L_E}/Q_E$ deve dividere $\bar{g}(x)$ e deve essere irriducibile; di conseguenza $\mu_{\bar{\alpha}} = (x - \bar{\alpha})$ e dunque $f(Q|Q_E) = 1$.

Osserviamo che Q è l'unico primo di $\mathcal{O}_L$ sopra Q_D. Infatti, $\mathrm{Gal}(L/L_D) = D$ agisce transitivamente sui primi di $\mathcal{O}_L$ sopra Q_D; ma per ogni $\sigma \in D$ $\sigma(Q) = Q$ e dunque esiste un unico primo di $\mathcal{O}_L$ sopra Q_D dato che l'azione è transitiva.

- Come conseguenza, vale

  $$[L : L_D] = e(Q|Q_D)f(Q|Q_D)r(Q|Q_D) = e(Q|Q_D)f(Q|Q_D)$$

  e d'altro canto, $[L : L_D] = ef$ perché $n = ref$ e abbiamo già mostrato che $[L_D : K] = r$.

- Mostriamo che $e(Q|Q_D) = e$ e $f(Q|Q_D) = f$. Q_D si fattorizza $Q_D\mathcal{O}_L = Q^{e(Q|Q_D)}$ e dunque si ha l'uguaglianza cercata. Da questo segue anche che $f(Q_E \mid Q_D) = f$ e dunque $[G : D] = f$.

Una conseguenza di tutto ciò è il seguente:

Corollario 3.3. $D/E \simeq \bar{G}$ e dunque è ciclico di ordine f.

Osservazione 3.4.

- Notiamo che abbiamo mostrato che $Q_D\mathcal{O}_L = Q^e$. In particolare Q è l'unico primo di $\mathcal{O}_L$ sopra Q_D.

- Q_D è non ramificato e ha grado di inerzia 1 su P. Dunque $P\mathcal{O}_{L_D} = Q_D I$, dove Q_D non compare in I.

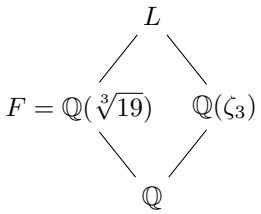
- Q_E è totalmente ramificato in $\mathcal{O}_L$, cioè $Q_E\mathcal{O}_L = Q^e$

- Q_E non è ramificato su P, perché $e(Q_E|P) = 1$. In particolare, non è detto che $P\mathcal{O}_{L_D} = Q_{D_1} \dots Q_{D_R}$, cioè non è detto che P si spezzi completamente in L_D. Infatti, se $Q'|P$, allora $\sigma(Q) = Q'$ e $D(\sigma(Q)|P) = \sigma D(Q|P)\sigma^{-1}$. La stessa cosa vale per E, cioè $E(\sigma(Q)|P) = \sigma E(Q|P)\sigma^{-1}$. La teoria di Galois dice che

  $$L_{\sigma D \sigma^{-1}} = \sigma L_D$$

  Dunque se $D \trianglelefteq G$, L_D è il campo di decomposizione di tutti i primi di $\mathcal{O}_L$ sopra P e dunque $P\mathcal{O}_{L_D}$ si spezza completamente.

Esempio. Consideriamo il campo $L = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$, che è normale perché campo di spezzamento su $\mathbb{Q}$ del polinomio $x^3 - 19$ e il suo gruppo di Galois $\mathrm{Gal}(L/\mathbb{Q}) = S_3$. Mostriamo che $3\mathcal{O}_L = (Q_1Q_2Q_3)^2$.



Intanto, notiamo che $3\mathcal{O}_{\mathbb{Q}(\zeta_3)} = P^2$. Invece, dato che $19 \equiv 1 \pmod 9$, $\mathrm{disc}_{\mathbb{Q}} F = -3 \cdot 19^2$ per 1.4. Dunque 3 ramifica e vi sono 2 possibilità

$$3\mathcal{O}_F = \begin{cases} Q^3 \\ Q^2Q' \end{cases}$$

Il primo caso non si verifica perché $3^{3-1} \nmid \mathrm{disc}\, F$ per la proposizione 2.37. Quindi $2 \mid e(Q_1|3)$ per moltiplicatività nelle torri e dunque può essere 2 o 6. D'altronde non può ramificare totalmente perché non lo è in $\mathcal{O}_F L$ e di conseguenza $e = 2$, $r = 3$ e $f = 1$. Calcoliamo gruppi di decomposizione e di inerzia relativi a Q_1, Q_2, Q_3. Notiamo che dato che $f = 1$ questi coincidono. Le sottoestensioni di grado 3 sono

$$L_{D_1} = \mathbb{Q}(\sqrt[3]{19}) \qquad L_{D_2} = \mathbb{Q}(\zeta_3 \sqrt[3]{19}) \qquad L_{D_3} = \mathbb{Q}(\zeta_3^2 \sqrt[3]{19})$$

e per corrispondenza sono i campi di inerzia dei primi.

Sia L/K estensione di Galois e sia Q in $\mathcal{O}_L$. Abbiamo visto che se Q, Q' sono primi sopra P, Q, Q' sono coniugati tramite un automorfismo del gruppo di Galois e dunque i rispettivi gruppi di decomposizione e di inerzia sono coniugati.

Osservazione 3.5. Se $D(Q|P)$ è un sottogruppo normale di G, allora P si spezza completamente in L_D. Infatti, la normalità di questo sottogruppo implica che L_D è il campo di decomposizione di ogni primo Q' di $\mathcal{O}_L$ sopra P, per la formula $D(\sigma(Q)|P) = \sigma D(Q|P)\sigma^{-1}$. Per ogni primo Q di $\mathcal{O}_{L_D}$ sopra P, Q_D ha indice di ramificazione $e = 1$ e grado di inerzia $f = 1$ e dunque P si spezza completamente.

Questa osservazione è utile per trovare un sottocampo di L su cui un primo si spezza completamente; vorremmo ora mostrare che vale anche il viceversa. Consideriamo delle estensioni

$$K \subseteq K' \subseteq L$$

con L/K di Galois. Sia Q un primo di $\mathcal{O}_L$ e siano P' e P le contrazioni rispettivamente a K' e K. Per corrispondenza, $K' = L^H$, con $H < G$ e $\mathrm{Gal}(L/K') = H$. Allora

$$D(Q|P') = \{\sigma \in H \mid \sigma Q = Q\} = D(Q|P) \cap H$$
$$E(Q|P') = E(Q|P) \cap H$$

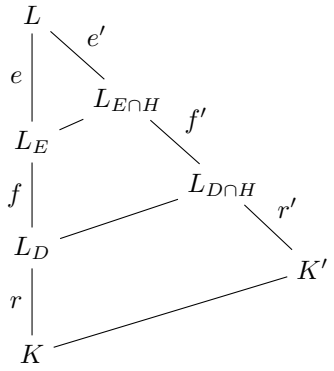
In teoria di Galois, l'intersezione corrisponde al composto e dunque

$$L_{E \cap H} = L_E K' \qquad L_{D \cap H} = L_D K'$$

Teorema 3.6.

1. L_D è il più grande campo intermedio K' tale che $f(P'|P) = e(P'|P) = 1$.
2. L_D è il più piccolo campo intermedio K' tale che in $\mathcal{O}_L$ esista un unico primo sopra P'.
3. L_E è il più grande campo intermedio K' tale che P' è non ramificato su P.
4. L_E è il più piccolo campo intermedio K' tale che Q è totalmente ramificato su P'.

Dimostrazione. Per quanto visto, tali campi hanno le proprietà richieste. Mostriamo la minimalità e la massimalità.



1. Sia K' un campo tale che $f(P'|P) = f' = 1$ e $e(P'|P) = e' = 1$, dove P' è un primo di $\mathcal{O}_{K'}$ sopra P. Allora $e' = e$ e $f' = f$. Dato che vale il contenimento $L_{D\cap H} \supseteq L_D$ e $ef = e'f'$, allora deve valere l'uguaglianza $L_{D\cap H} = L_D$, perché $[L : L_D] = [L : L_{D\cap H}]$. Di conseguenza, $L_D \supseteq K'$.
2. Sia K' un campo tale che in $\mathcal{O}_L$ ci sia un unico primo sopra P', cioè $r' = 1$. Allora $K' = L_D K'$ e dunque $L_D \subseteq K'$.
3. Per ipotesi, $e(P'|P) = 1$ e dunque $e = e'$. Quindi $[L : L_E] = [L : L_{E\cap H}]$ e $K' \subseteq L_E$.
4. Q è totalmente ramificato su P' se e solo se $f' = r' = 1$, cioè $L_E K' = K'$, cioè $L_E \subseteq K'$.

□

Corollario 3.7. Il gruppo di decomposizione è un sottogruppo normale di G $D \trianglelefteq G$ se e solo se P si spezza completamente in L_D.

Dimostrazione. Abbiamo già visto che se il gruppo di decomposizione è normale P si spezza completamente in L_D nell'osservazione 3.5; mostriamo il viceversa. Supponiamo quindi che P si spezzi completamente in L_D. Questo è equivalente a dire che L_D contiene tutti i campi di decomposizione dei primi Q su P. Allora per ogni Q' sopra P, $L_{D'} \supseteq L_D$ e dunque, dato che sono tutti coniugati, $L_{D'} = L_D$, da cui $D = D'$ e quindi $D \trianglelefteq G$, perché invariante per coniugio. □

Corollario 3.8. Supponiamo che il gruppo di decomposizione $D \trianglelefteq G$ sia un sottogruppo normale del gruppo di Galois. Allora P si spezza completamente in K' se e solo se $K' \subseteq L_D$.

Proposizione 3.9. Sia L/K un'estensione normale e sia $P \subseteq \mathcal{O}_K$ un primo.

1. Se P è inerte, G è ciclico.
2. Se P è totalmente ramificato in ogni campo intermedio ma non in L, allora G è ciclico di ordine p.

3. Se ogni campo intermedio K' K' ha un unico primo sopra P ma per L non vale, allora G è ciclico di ordine primo.

4. Se P è non ramificato in K' per ogni campo intermedio ma è ramificato in L, allora esiste H sottogruppo minimo di G (non banale) e H è normale.

5. Se P si spezza completamente in ogni K' ma non in L, allora esiste un sottogruppo minimo e trovare un esempio in cui questo succede.

6. Se P è inerte in ogni campo intermedio ma non in L, allora G è ciclico di ordine potenza di un primo.

Dimostrazione.

1. Basta notare che $L_E = L$, $L_D = K$ e $D/E = G$ è ciclico.

2. Se $fr > 1$, $0 \lneq E \lneq G$ e quindi L_E è una sottoestensione propria di L. D'altronde, per la caratterizzazione della proposizione precendete, $e(P_E|P) = 1$. Per ipotesi però P ramifica totalmente in L_E, da cui un assurdo. Dunque non esistono sottoestensioni proprie L e per corrispondenza G non ha sottogruppi propri. Di conseguenza, il gruppo di Galois è ciclico di ordine primo.

3. Basta ripetere il ragionamento di 2. con il gruppo di inerzia.

4. Se P è ramificato in L, $L \supsetneq L_E$ e quindi E è un sottogruppo proprio non banale. Dato che P è non ramificato in K' per ogni campo intermedio K', si ottiene $K' \subseteq L_E$. Per corrispondenza, ogni sottogruppo proprio contiene E da cui la tesi.

5. Per mostrare l'enunciato, basta ripetere il ragionamento di 4. utilizzando il gruppo di inerzia. Mostriamo un esempio; sia $L = \mathbb{Q}(\zeta_5)$, che ha come unica sottoestensione $\mathbb{Q}(\sqrt{5})$. Sappiamo che l'unico primo ramificato può essere è 5 e dunque per tutti gli altri $e = 1$. Cerchiamo quindi un primo $p \in \mathbb{Q}$ tale che $f = 2$ e in tal caso $r = 2$ e dunque nel campo intermedio necessariamente tale primo si spezzerebbe completamente. Cerchiamo allora $q \in \mathbb{Z}$ tale che
$$q^2 \equiv 1 \pmod 5$$
per esempio $q = 19$.

6. Per definizione, P è non ramificato in K' per ogni campo intermedio K' e in L vale o $e > 1$ (e dunque possiamo applicare 4.) oppure $r > 1$ (e dunque possiamo utilizzare 3). Il secondo caso è ovvio, supponiamo allora $e > 1$. Allora G ha un sottogruppo minimo H non banale e di conseguenza G ha cardinalità p^n. H corrisponde a un sottocampo intermedio massimale K' e per ipotesi P è inerte in K'. Allora il gruppo di Galois $\mathrm{Gal}(K'/K) \simeq G/H$ è ciclico. D'altronde in un p-gruppo il centro è non banale e dunque $Z(G) \supseteq H$. Per corrispondenza allora $G/Z(G)$ è ciclico e quindi G è abeliano. Utilizzando ancora una volta il teorema di corrispondenza, otteniamo allora che G è ciclico.

□

Esempio. Consideriamo $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ con gruppo $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Supponiamo che P sia ramificato in ogni sottoestensione quadratica

$$K_1 = \mathbb{Q}(\sqrt{m}) \qquad K_2 = \mathbb{Q}(\sqrt{n}) \qquad K_3 = \mathbb{Q}(\sqrt{mn})$$

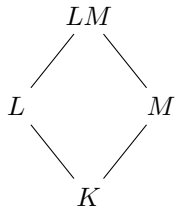
Per la proposizione, P è totalmente ramificato in L; troviamo un esempio di un primo che realizza questa situazione. Se $m \equiv 2 \pmod 4$ e $n \equiv 3 \pmod 4$, 2 è ramificato in tutte le estensioni perché divide il discriminante e dunque questo è un esempio.
Supponiamo ora che P si spezzi completamente in K_i per ogni i; allora in L si spezza completamente. Per trovare un esempio, scegliamo ancora $p = 2$ e consideriamo il polinomio

$$T(x) = x^2 + x + (1 - m)/4$$

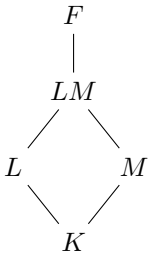
Per Kummer, se scegliamo $17, 33, 2$ si spezza completamente in ogni sottoestensione e in K.
Se P è inerte per ogni K_i, allora per quanto visto il gruppo di Galois sarebbe ciclico e dunque P non può essere inerte.
Troviamo ora esempi in cui $P\mathcal{O}_L = Q_1Q_2$, $P\mathcal{O}_L = Q_1^2Q_2^2$ e $P\mathcal{O}_L = Q^2$.

$$\begin{cases} P\mathcal{O}_L = Q_1Q_2 & P = (2) \quad L = \mathbb{Q}(\sqrt{5}, \sqrt{17}) \\ P\mathcal{O}_L = Q_1^2Q_2^2 & P = (2) \quad L = \mathbb{Q}(\sqrt{2}, \sqrt{17}) \\ P\mathcal{O}_L = Q^2 & P = (2) \quad L = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \end{cases}$$

Teorema 3.10. Sia P un primo di $\mathcal{O}_K$ non ramificato sia in L che in M. Allora P è non ramificato in LM.



Inotre, se P si spezza completamente in L e in M, allora P si spezza completamente nel composto.



Dimostrazione. Sia $P' \subseteq \mathcal{O}_{LM}$ un primo sopra $P \subseteq \mathcal{O}_K$. Consideriamo F la chiusura normale di LM su K e sia Q un primo di $\mathcal{O}_F$ sopra P'. Sia F_E il campo di inerzia di Q su P. Dato che $L, M \subseteq F_E$ per la proprietà 3 del teorema 3.6, lo stesso vale per il composto $LM \subseteq F_E$ e dunque $e(P'|P) \mid e(Q_E|P) = 1$. Di conseguenza, dato che questo vale per ogni primo $Q \subseteq \mathcal{O}_F$ sopra P, lo stesso vale per ogni primo $P' \subseteq \mathcal{O}_{LM}$ da cui il primo asserto. Supponiamo ora che P si spezzi completamente in $\mathcal{O}_L$ e in $\mathcal{O}_M$ e sia $Q \subseteq \mathcal{O}_F$ un primo sopra p. Allora $L \subseteq F_D$ e $M \subseteq F_D$ e dunque $LM \subseteq F_D$. Dato che questo vale per ogni primo $Q \subseteq \mathcal{O}_F$ sopra P, si ha $LM \subseteq \cap_{Q|P} F_D$. Dunque P si spezza completamente in LM, come voluto. □

Corollario 3.11. Sia L/K un'estensione e sia $\tilde{L}$ la sua chiusura normale. Sia P un primo di $\mathcal{O}_K$. Allora P è ramificato in L se e solo se P è ramificato in $\tilde{L}$.

Dimostrazione. Per moltiplicatività dell'indice di ramificazione nelle torri di estensione, si ha che se P è ramificato in L allora è ramificato in $\tilde{L}$. Viceversa, supponiamo che P non sia ramificato in L. Siano σ_i le immersioni di L in $\bar{L}$ che fissano K; allora P non è ramificato in $\sigma_i(L)$ per ogni indice i. Per il teorema precedente, P non è ramificato nel composto dei $\sigma_i(L)$, che coincide con $\tilde{L}$, da cui la tesi. □

3.2 Reciprocità Quadratica

Consideriamo il caso di un'estensione ciclotomica, quindi $L = \mathbb{Q}(\zeta_p)$. Dato $q \in \mathbb{Z}$ un primo diverso da p, sappiamo dal teorema 2.42 che $f = \mathrm{ord}_{\mathbb{F}_p^*} q$, $r = (p-1)/f$ e $e = 1$.

$$\begin{array}{c} L \\ e \,\big|\, \\ L_E \\ f \,\big|\, \\ L_D \\ r \,\big|\, \\ \mathbb{Q} \end{array}$$

In questo caso, il gruppo di Galois dell'estensione è ciclico e quindi esiste un unico sottogruppo di ordine d per ogni d che divide l'ordine del gruppo. Per il teorema di corrispondenza di Galois, esiste quindi per ogni d che divide $p-1$ un unico sottocampo di $\mathbb{Q}(\zeta_p)$ di grado d su $\mathbb{Q}$, che chiamiamo F_d.

Teorema 3.12. Siano $p, q \in \mathbb{Z}$ primi distinti e sia $d \mid p-1$. Allora q si spezza completamente in F_d se e solo se q è una potenza d-esima modulo p.

Dimostrazione. Per il corollario 3.8, q si spezza completamente in F_d se e solo se $F_d \subseteq F_r$ e questo accade se e solo se $d \mid r$. Inoltre, q è una potenza d-esima modulo p se e solo se $q^{p-1/d} = 1$ in $\mathbb{F}_p$. Supponiamo dapprima che $d \mid r$. Allora

$$\mathrm{ord}_{\mathbb{F}_p^*} q = f = \frac{p-1}{r} \;\Big|\; \frac{p-1}{d}$$

cioè $q^{\frac{p-1}{d}} = 1$. Viceversa, supponiamo che $q^{p-1/d} = 1$ in $\mathbb{F}_p$. Sia ξ un generatore di $\mathbb{F}_p^*$ e supponiamo $\xi^a = q$. Allora

$$f = \mathrm{ord}_{\mathbb{F}_p^*}(q) \;\Big|\; \frac{p-1}{d}$$

D'altronde $f = (p-1)/r$ e dunque la relazione di divisibilità ottenuta si traduce proprio in $d \mid r$, come voluto. □

Definizione 3.13. Sia $p \in \mathbb{Z}$ un primo e sia $n \in \mathbb{Z}$ tale che $p \nmid n$. Definiamo il simbolo di Legendre

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & n \equiv \square \pmod p \\ -1 & \text{altrimenti} \end{cases}$$

Teorema 3.14 (Legge di reciprocità quadratica)**.** Siano p, q primi distinti dispari. Allora

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & p \equiv q \equiv 3 \pmod 4 \end{cases}$$

mentre

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

Dimostrazione. Sappiamo che $(q/p) = 1$ se e solo se q è un quadrato modulo p se e solo se q si spezza completamente in F_2, l'unica estensione di grado 2 di $\mathbb{Q}(\zeta_p)$, che è $\mathbb{Q}(\sqrt{\pm p})$.

- Supponiamo $p \equiv 1 \pmod 4$. Allora $F_2 = \mathbb{Q}(\sqrt{p})$ e $\mathcal{O}_{F_2} = \mathbb{Z}[(1+\sqrt{p})/2]$.
  - Se $q \neq 2$, sappiamo che $\operatorname{ind}(\sqrt{p}) = 2$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ e in particolare non è divisibile per p. Possiamo allora applicare il teorema di Kummer e $x^2 - p$ si spezza in fattori lineari se e solo se p è un quadrato modulo q, cioè se e solo se $(p/q) = 1$.
  - Se $q = 2$, utilizziamo il polinomio $x^2 + x + (p-1)/4$. 2 si spezza completamente in F_2 se e solo se $p - 1 \equiv 0 \pmod 8$.
- Se $p \equiv 3 \pmod 4$, $F_2 = \mathbb{Q}(\sqrt{-p})$ e ancora $\mathbb{Z}[\sqrt{-p}] \subseteq \mathbb{Z}[(1+\sqrt{-p})/2]$.
  - Se $q \neq 2$, $x^2 + p$ si spezza completamente modulo q se e solo se $-p$ è un quadrato modulo q.
    - Se $q \equiv 1 \pmod 4$, -1 è un quadrato $\pmod q$. Quindi p è un quadrato modulo q se e solo se lo è $-p$. Ma $-p \equiv 1 \pmod 4$ e dunque $-p$ è un quadrato modulo q se e solo se q è un quadrato modulo p per quanto già visto.
    - Se $q \equiv 3 \pmod 4$, $-p$ è un quadrato modulo q se e solo se p non è un quadrato modulo q. Quindi $(q/p) = 1$ se e solo se $(p/q) = -1$.
  - Se $q = 2$, 2 è un quadrato modulo p se e solo se 2 si spezza completamente in F_2. Per vedere questo, utilizziamo il teorema di Kummer con il polinomio
    $$f(x) = x^2 + x + \frac{1+p}{4}$$
    Ridotto modulo 2, f si spezza se e solo se $(1+p)/4 \equiv 0 \pmod 2$, cioè $1 + p \equiv 0 \pmod 8$. Dunque 2 è un quadrato modulo p se e solo se $p \equiv -1 \pmod 8$.

□

Teorema 3.15. Sia K un campo di numeri e sia p un primo. Se $p \mid \operatorname{disc}(K)$, allora p è ramificato in $\mathcal{O}_K$.

Dimostrazione. Per prima cosa, riformuliamo l'ipotesi di divisibiltà del discriminante per il primo p. Sia $\alpha_1, \dots \alpha_n$ una base intera di $\mathcal{O}_K$.

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

Il determinante è nullo modulo p e dato che questo commuta con la proiezione, possiamo ridurci a mostrare che

$$\overline{\operatorname{disc}(K)} = \det(\operatorname{Tr}(\overline{\alpha_i \alpha_j})) = 0$$

Se il determinante è nullo, la matrice non è invertibile e possiamo trovare una combinazione lineare nulla delle colonne. Esistono allora $m_1, \dots, m_n$ non tutti nulli modulo p tali che $\sum_{i=1}^{n} m_i \operatorname{Tr}(\alpha_i \alpha_j) = 0$ per ogni j modulo p. Dato che la traccia è lineare, consideriamo l'elemento

$$\alpha = \sum_{i=1}^{n} m_i \alpha_i$$

e dunque

$$\operatorname{Tr}(\alpha \alpha_j) = 0 \pmod{p}$$

per ogni j. Dunque $\operatorname{Tr}(\alpha \mathcal{O}_K) \subseteq p\mathbb{Z}$ e $\alpha \notin p\mathcal{O}_K$ perché non tutti gli m_i sono divisibili per p.
Supponiamo per assurdo che p sia non ramificato. Allora

$$p\mathcal{O}_K = P_1 \dots P_r$$

Dato che $\alpha \notin p\mathcal{O}_K$, esiste $P = P_i$ tale che $\alpha \notin P$. Sia L la chiusura normale di K su $\mathbb{Q}$. Dato che p è non ramificato in $\mathcal{O}_K$, non è ramificato in $\mathcal{O}_L$ per il corollario 3.11. Sia $Q \subseteq \mathcal{O}_L$ un primo sopra P; notiamo che Q non contiene α.

$$\begin{aligned} \operatorname{Tr}_{L/\mathbb{Q}}(\alpha \mathcal{O}_L) &= \operatorname{Tr}_{K/\mathbb{Q}}(\operatorname{Tr}_{L/K}(\alpha \mathcal{O}_L)) \\ &= \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \operatorname{Tr}_{L/K}(\mathcal{O}_L)) \\ &\subseteq \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \mathcal{O}_K) \\ &\subseteq p\mathbb{Z} \end{aligned}$$

Sia $\beta \in \mathcal{O}_L$ tale che $\beta \notin Q$ e $\beta \in Q'$ per ogni $Q' \mid p$, $Q' \neq Q$. Per ogni $\gamma \in \mathcal{O}_L$,

$$\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\gamma) \in p\mathbb{Z} \subseteq Q$$

Inoltre, dato $\sigma \in \operatorname{Gal}(L/\mathbb{Q}) \setminus D(Q|p)$, vale $\sigma(\alpha\beta\gamma) \in Q$. Infatti questo è equivalente a dire che $\alpha\beta\gamma \in \sigma^{-1}Q \neq Q$ e $\beta \in \sigma^{-1}Q$ per costruzione. Per quanto detto,

$$\operatorname{Tr}(\alpha\beta\gamma) = \sum_{\sigma \in G} \sigma(\alpha\beta\gamma) \in p\mathbb{Z} \subseteq Q$$

Spezzando la somma, quindi

$$\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) + \sum_{\sigma \in G \setminus D} \sigma(\alpha\beta\gamma) \in Q$$

e per quanto detto la seconda somma appartiene a Q e di conseguenza anche la prima vi appartiene. Dunque, riducendo modulo Q,

$$\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) \in Q \Longrightarrow \sum_{\bar{\sigma} \in \bar{D}} \bar{\sigma}(\overline{\alpha\beta\gamma}) = 0$$

Dato che il primo è non ramificato, $\bar{D} = \bar{G} = \mathrm{Gal}(\mathcal{O}_L/Q, \mathbb{Z}/p\mathbb{Z})$. Quindi

$$\sum_{\bar{\sigma}\in\bar{G}} \bar{\sigma}(\overline{\alpha\beta\gamma}) = 0 \quad \forall\gamma \in \mathcal{O}_L$$

Dato che $\overline{\alpha\beta} \neq 0$ (non appartengono a Q),

$$\sum_{\sigma\in\bar{G}} \sigma(\bar{x}) = 0$$

per ogni $x \in \mathcal{O}_L/Q$ e questo è assurdo per il teorema di indipendenza dei caratteri 1.16. □

3.3 Automorfismo di Frobenius

Sia L/K un'estensione di Galois con gruppo di Galois G e sia $P \subseteq \mathcal{O}_K$ un primo non ramificato in $\mathcal{O}_L$. Sia Q un primo di $\mathcal{O}_L$ sopra P; dato che il primo P è non ramificato, necessariamente $E(Q|P) = 0$ e il gruppo di Galois dell'estensione dei campi residui è per definizione $D(Q|P)$.

$$\mathrm{Gal}\left(\mathcal{O}_L/Q \big/ \mathcal{O}_K/P\right) \simeq D(Q|P)$$

Dato che i campi in questione sono finiti, tale gruppo è ciclico. Infatti, $\mathcal{O}_K/P \simeq \mathbb{F}_q$, dove $q = N(P)$ e $[\mathcal{O}_L/Q : \mathcal{O}_K/P] = f$ e dunque $\mathcal{O}_L/Q = \mathbb{F}_{q^f}$. Sappiamo che l'automorfismo di Frobenius

$$\begin{array}{rccc} \eta\colon & \mathcal{O}_L/Q & \longrightarrow & \mathcal{O}_L/Q \\ & x & \longmapsto & x^{N(P)} \end{array}$$

genera il gruppo di Galois dell'estensione. Dato che $D(Q|P) \simeq \bar{G}$, esiste un unico elemento di $D(Q|P)$ che al quoziente diventa l'automorfismo di Frobenius dell'estensione. Chiamiamo questo elemento automorfismo di Frobenius di $Q|P$ e lo denotiamo con $\phi(Q|P)$. Notiamo che per definizione

$$\phi(Q|P)(x) \equiv x^{\|P\|} \pmod{Q}$$

Osservazione 3.16.

- Quest'ultima proprietà individua un unico elemento di G. Infatti un tale elemento deve appartenere a $D(Q|P)$ e sul quoziente deve agire come il Frobenius.
- Se $\sigma \in G$, allora $\phi(\sigma Q|P) = \sigma\phi(Q|P)\sigma^{-1}$. Quindi ogni primo $P \subseteq \mathcal{O}_K$ non ramificato in $\mathcal{O}_L$ individua un'unica classe di coniugio di elementi di G.
- Se $\mathrm{ord}(\phi(Q|P)) = f$, allora $[\mathcal{O}_L/Q : \mathcal{O}_K/P] = f$ e quindi l'automorfismo di Frobenius individua il tipo di spezzamento di $P\mathcal{O}_L$.

Come conseguenza di questa osservazione, abbiamo la corrispondenza

$$\begin{array}{ccc} \{P \subseteq \mathcal{O}_K \mid P\mathcal{O}_L \text{ è non ramificato}\} & \longrightarrow & \{\text{classi di coniugio di } G\} \\ P & \longmapsto & cl(\phi(Q|P)) \end{array}$$

che a un primo associa la classe di coniugio di $\phi(Q|P)$, dove Q è un qualsiasi primo sopra P. Se G è abeliano, la mappa si semplifica

$$P \longmapsto \phi(P)$$

perché non dipende da Q (il coniugio agisce banalmente). In questo caso

$$\phi(\alpha) \equiv \alpha^{N(P)} \pmod{Q}\ \forall Q \Longrightarrow \phi(\alpha) \equiv \alpha^{N(P)} \pmod{P\mathcal{O}_L}$$

Esempio.

- Sia $K = \mathbb{Q}(\sqrt{m})$; in tal caso, $G = \{\pm \mathrm{Id}\}$. In questo caso, la mappa diventa semplicemente

  $$\{p \in \mathbb{Z} \mid p \nmid \mathrm{disc}(K)\} \longmapsto G$$

  In $\mathcal{O}_K$,

  $$p\mathcal{O}_K = \begin{cases} PQ & \text{se } f = 1 \longrightarrow \mathrm{Id} \quad m \equiv \square \pmod{p} \\ P & \text{se } f = 2 \longrightarrow -\mathrm{Id} \quad m \not\equiv \square \pmod{p} \end{cases}$$

- Sia $L = \mathbb{Q}(\zeta_m)$; sappiamo che $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$ e coincide con l'insieme $\{\sigma_i \mid (i,m) = 1\}$ con $\sigma_i(\zeta) = \zeta^i$. Cerchiamo l'automorfismo di Frobenius relativo a un primo p; dato che p non deve essere ramificato, necessariamente $(p,m) = 1$. L'automorfismo di Frobenius sarà allora un σ_i tale che

  $$\phi(\zeta) = \zeta^p \pmod{p\mathcal{O}_L} \Rightarrow \zeta^i \equiv \zeta^p \pmod{p\mathcal{O}_L} \Rightarrow \zeta^{p-i} \equiv 1 \pmod{p\mathcal{O}_L}$$

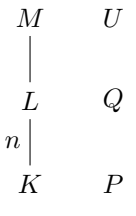
  Dunque $i \equiv p \pmod{m}$ e $\phi = \sigma_i$ dove i è la classe di resto di p modulo m. La condizione imposta è necessaria e individua un solo automorfismo; dato che il Frobenius esiste deve coincidere con questo.

Vale il seguente teorema

Teorema 3.17 (Artin)**.** Ogni $\sigma \in \mathrm{Gal}(L/K)$ è Frobenius di infiniti primi.

Nel caso delle estensioni ciclotomiche implica che per ogni i esistono infiniti primi p tali che $p \equiv i \pmod{m}$.

Consideriamo ora il caso di estensioni non normali. Sia K un campo e sia L un'estensione di grado n di K. Data M una estensione normale di L su K, sia P un primo di $\mathcal{O}_K$ e chiamiamo Q, U primi sopra P rispettivamente in $\mathcal{O}_L$ e $\mathcal{O}_M$, che supponiamo essere non ramificati. Siano $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$, $\phi = \phi(U|P)$ l'automorfismo di Frobenius e consideriamo l'insieme X delle classi laterali di H in G. L'automorfismo di Frobenius agisce in maniera naturale sulle classi laterali destre per moltiplicazione a destra:



$$\begin{array}{ccc} \langle\phi\rangle & \longrightarrow & S(X) \\ \phi & \longmapsto & \{H\sigma \longmapsto H\sigma\phi\} \end{array}$$

Di conseguenza, le orbite sono del tipo

$$\mathrm{Orb}(H\sigma) = \{H\sigma, H\sigma\phi, \dots H\sigma\phi^{m-1}\}$$

Le orbite di questa azione sono profondamente legate alla fattorizzazione di P:

Teorema 3.18. Sia M/K un'estensione di Galois, sia L un campo intermedio, sia $P \subseteq \mathcal{O}_K$ un primo non ramificato in M e sia $\phi = \phi(U|P)$ l'automorfismo di Frobenius, dove $U \subseteq \mathcal{O}_M$ è un primo sopra P. Detto X l'insieme delle classi laterali destre del sottogruppo $H < G$ corrispondente a L, siano $m_1, \dots, m_r$ le lunghezze delle orbite degli elementi di X sotto l'azione di ϕ. Allora P si fattorizza in L come

$$P\mathcal{O}_L = Q_1 \dots Q_r$$

con $f(Q_i|P) = m_i$. Inoltre, se $\mathrm{Orb}(H\sigma_i) = \{H\sigma_i, \dots H\sigma_i\phi^{m_i-1}\}$, allora $Q_i = \sigma_i U \cap \mathcal{O}_L$.

Dimostrazione. Siano $\mathrm{Orb}(H\sigma_1), \dots, \mathrm{Orb}(H\sigma_s)$ tutte le orbite (senza ripetizioni). Preliminarmente, notiamo che i Q_i sono primi di $\mathcal{O}_L$ perché sono contrazione di primi di $\mathcal{O}_M$. Mostriamo che sono tutti distinti tra loro. Se per assurdo $Q_i = Q_j$, allora $\sigma_i U$ e $\sigma_j U$ sarebbero due primi sopra Q_i. Notiamo che H agisce transitivamente sull'insieme dei primi sopra un fissato primo di $\mathcal{O}_L$. Di conseguenza, esiste $\tau \in H$ tale che $\tau\sigma_i U = \sigma_j U$, cioè $\sigma_j^{-1}\tau\sigma_i \in D(U|P) = \langle\phi\rangle$. Dunque

$$\sigma_j^{-1}\tau\sigma_i = \phi^l \implies \tau\sigma_i = \sigma_j\phi^l \implies H\sigma_i = H\sigma_j\phi^l \implies H\sigma_i \in \mathrm{Orb}(H\sigma_j)$$

e dunque i Q_i sono primi distinti. Di conseguenza, $Q_1 \dots Q_s \mid P\mathcal{O}_L$. Sia f_i il grado di inerzia di Q_i. Se mostriamo che $\sum f_i = n$ allora $P\mathcal{O}_L = Q_1 \dots Q_s$. Per questo, è sufficiente che $m_i \le f_i$ per ogni i. Infatti m_i è la lunghezza dell'i-esima orbita e $n = \sum m_i \le \sum f_i \le n$, da cui seguirebbe l'uguaglianza.
Dato che le orbite sono del tipo

$$\mathrm{Orb}(H\sigma_i) = \{H\sigma_i, \dots, H\sigma_i\phi^{m_i}\}$$

ci basta mostrare che $H\sigma_i\phi^{f_i} = H\sigma_i$ o equivalentemente che $\sigma_i\phi^{f_i}\sigma_i^{-1} \in H$. Mostriamo che $\phi(\sigma_i(U)|Q_i) = \phi(\sigma_i(U)|P)^{f_i}$. Per l'osservazione 3.16, $\phi(\sigma_i(U)|Q_i)$ è l'unico automorfismo tale che $\phi(\sigma_i(U)|Q_i)(x) \equiv x^{N(Q_i)} \pmod{\sigma_i(U)}$

$$\phi(\sigma_i(U)|P)^{f_i}(x) \equiv x^{N(P)^{f_i}} \pmod{\sigma_i^{-1}(U)}$$

e notiamo che $N(P)^{f_i} = N(Q_i)$. Per unicità dell'automorfismo di Frobenius, $\phi(\sigma_i(U)|Q_i) = \phi(\sigma(U)|P)^{f_i}$. Dunque per ogni $\sigma \in G$

$$H \ni \phi(\sigma^{-1}(U)|Q) = \sigma\phi^{f_i}\sigma^{-1}$$

da cui la tesi. □

Esempio. Sia $m \in \mathbb{Z}$ un non quadrato e sia $K = \mathbb{Q}(\sqrt[4]{m})$. Consideriamo la sua chiusura normale $L = K(i)$; sappiamo che $\mathrm{Gal}(L/\mathbb{Q}) = D_4$. Chiamiamo $\alpha, i\alpha, -\alpha, -i\alpha$ le radici del polinomio $x^4 - m$. Mostriamo che $\mathrm{Gal}(L/\mathbb{Q}) = \langle(2,4),(1,2,3,4)\rangle$. Consideriamo l'automorfismo

$$\sigma(\alpha) = i\alpha \qquad\qquad \sigma(i) = i$$

Allora σ individua un 4-ciclo, che con la numerazione data è $(1,2,3,4)$. La trasposizione è invece data da

$$\tau(\alpha) = \alpha \qquad\qquad \tau(i) = -i$$

Supponiamo ora che $p \in \mathbb{Z}$ sia un primo dispari tale che $p \nmid m$; mostriamo che p è non ramificato in L. Dato che L è il composto di K e $\mathbb{Q}(i)$ e p non ramifica in $\mathbb{Q}(i)$ perché $\text{disc}(\mathbb{Q}(i)) = 2$, per la proposizione 3.10 basta vedere che p non è ramificato in K. Dato che $\text{disc}(K) \mid \text{disc}(\sqrt[4]{m})$, è sufficiente che p non divida il discriminante di $\sqrt[4]{m}$. D'altronde,

$$\mu(x) = x^4 - m \qquad \mu'(x) = 4x^3 \qquad \mu'(\alpha) = 4\alpha^3$$

e dunque $N(\mu'(\alpha)) = 4^4 m^3$; dato che per ipotesi $p \nmid 2m$, $p \nmid \text{disc}(\sqrt[4]{m})$ e dunque è non ramificato.
Sia ora $Q \subseteq \mathcal{O}_L$ tale che $Q \mid p$ e tale che $\phi(Q|p) = \tau$. Utilizzando il teorema, mostriamo ora che

$$p\mathcal{O}_K = P_1 P_2 P_3$$

In questo caso, $H = \langle \tau \rangle$ e $K = L^H$. Facciamo agire τ sull'insieme X delle classi laterali destre di H, che sono $\{H, H\sigma, H\sigma^2, H\sigma^3\}$.

$$\begin{array}{ccc} \langle \tau \rangle & \longrightarrow & S(X) \\ \tau & \longmapsto & \varphi_\tau \end{array}$$

dove $\varphi_\tau(H) = H\tau = H$. L'azione di τ individua le orbite

$$\{H\}, \{H\sigma^2\}, \{H\sigma, H\sigma^3\}$$

e dunque

$$p\mathcal{O}_K = P_1 P_2 P_3$$

dove $P_1 = Q \cap \mathcal{O}_L$, $P_2 = \sigma^2(Q) \cap \mathcal{O}_L$ e $P_3 = \sigma(Q) \cap \mathcal{O}_L$.
Supponiamo invece $\phi(Q|p) = \sigma$. Allora $X = \{H, H\sigma, H\sigma^2, H\sigma^3\}$ e dunque p è inerte $p\mathcal{O}_K = P$.

3.4 Differente

Sia R un dominio di Dedekind e sia K il suo campo dei quozienti. Consideriamo un'estensione di campi L/K finita e separabile e sia $S = \bar{R}$ la chiusura integrale. Supponiamo che per ogni ideale I di R R/I sia finito (proprietà delle norme finite) e che $\text{Cl}(K)$ sia finito. Sappiamo che gli ideali frazionari $\mathcal{F}(L)$ di L formano un gruppo, generato dagli ideali interi $\mathcal{I}(L)$ di L. L'estensione di campi induce una mappa

$$i_{L/K}\colon \quad \begin{array}{ccc} \mathcal{F}(K) & \longrightarrow & \mathcal{F}(L) \\ I & \longmapsto & IS \end{array}$$

che è un omomorfismo iniettivo di gruppi (l'estensione $\mathcal{O}_K \to \mathcal{O}_L$ intera e dunque l'estensione di un ideale primo è proprio) e inoltre $i_{L/K}(\mathcal{I}(K)) \subseteq \mathcal{I}(L)$.
In realtà, è possibile anche trovare una applicazione che agisce nel verso opposto: l'applicazione norma. Tale mappa si definisce sull'insieme dei primi

$$N_{L/K}\colon \quad \begin{array}{ccc} \mathcal{F}(L) & \longrightarrow & \mathcal{F}(K) \\ Q & \longmapsto & N_{L/K}(Q) = P^{f(Q|P)} \end{array}$$

e si estende per linearità dato che gli ideali primi sono generatori liberi.

Definizione 3.19. Sia I un ideale frazionario di L. Chiamiamo

$$I^* = \{x \in L \mid \mathrm{Tr}_{L/K}(xI) \subseteq R\}$$

il duale di I o codifferente.

Proposizione 3.20.

- Sia $I \in \mathcal{F}(L)$: allora $I^* \in \mathcal{F}(L)$ e $I \cdot I^* = S^*$.
- Se $I \in \mathcal{I}(S)$, allora $(I^*)^{-1} \in \mathcal{I}(S)$.

Dimostrazione.

- Chiaramente I^* è un S-modulo non banale; infatti dato che I è un ideale frazionario esiste $0 \neq a \in S$ tale che $aI \subseteq S$ e quindi $\mathrm{Tr}(aI) \subseteq \mathrm{Tr}(S) \subseteq R$. Mostriamo che I^* è un ideale frazionario, cioè che esiste $d \in S$ tale che $dI^* \subseteq S$. Consideriamo l'elemento

  $$d = b \det(\mathrm{Tr}(w_i w_j))$$

  e verifichiamo che soddisfa le condizioni, dove $w_1, \ldots, w_n \in S$ è una K-base di L di elementi interi e dove b è un elemento di $I \cap R$ diverso da 0. Tale b esiste perché $aI \subseteq I \cap S$ e preso un elemento $c \in aI$ si ha $N_{L/K}(c) \in I \cap R$.
  Sia $x \in I^*$. Allora

  $$x = \sum_{j=1}^{n} c_j w_j$$

  Notiamo che $bw_i \in I$ per ogni i e quindi

  $$\mathrm{Tr}_{L/K}(\underbrace{x}_{I^*}\underbrace{bw_i}_{I}) \in R$$

  Per linearità della traccia,

  $$\mathrm{Tr}_{L/K}(bxw_i) = b\sum_{j=1}^{n} c_j \,\mathrm{Tr}_{L/K}(w_j w_i)$$

  Questo ci fornisce n equazioni; risolvendo con Cramer si ottiene

  $$bc_i = \frac{\det A_i}{\det(\mathrm{Tr}(w_i w_j))}$$

  Dato che $\det(A_i) \in R$, $b\det(\mathrm{Tr}(w_i w_j))c_i = dc_i \in R$. Di conseguenza $dx \in S$ e $dI^* \subseteq S$.
  Notiamo inoltre che

  $$\begin{aligned} a \in I^* &\iff \mathrm{Tr}_{L/K}(aI) \subseteq R \\ &\iff \mathrm{Tr}_{L/K}(aIS) \subseteq R \\ &\iff aI \in S^* \\ &\iff a \in I^{-1}S^* \end{aligned}$$

  Dunque $I^* = I^{-1}S^*$ e dunque $II^* = II^{-1}S^* = S^*$.

- Se $I \subseteq S$, $S \subseteq I^*$ perché $\mathrm{Tr}(IS) \subseteq \mathrm{Tr}(S) \subseteq R$. Allora $(I^*)^{-1} \subseteq S^{-1} = S$ e $(I^*)^{-1}$ è intero.

□

Definizione 3.21. Sia $I \in \mathcal{F}(L)$. Definiamo il differente di I come

$$\mathcal{D}_{L/K}(I) \coloneqq (I^*)^{-1}$$

Definiamo il differente di L/K come

$$\mathcal{D}_{L/K} \coloneqq \mathcal{D}_{L/K}(S)$$

Notiamo che se I è un ideale intero, allora $\mathcal{D}_{L/K}(I) \subseteq S$ e dunque il differente è un ideale intero.

Teorema 3.22.

1. Se I è un ideale frazionario, $\mathcal{D}_{L/K}(I) = I\mathcal{D}_{L/K}$
2. Se $M \supseteq L \supseteq K$, allora $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$
3. Se L/K è normale, $\mathcal{D}_{L/K}$ è invariante per l'azione di $\mathrm{Gal}(L/K)$.
4. Se I è un ideale frazionario di K, per ogni J ideale frazionario di L vale
$$\mathrm{Tr}_{L/K}(J) \subseteq I \iff J \subseteq I\mathcal{D}_{L/K}^{-1}$$

Dimostrazione.

1. Mostriamo che
$$(\mathcal{D}_{L/K}(I))^{-1} I \mathcal{D}_{L/K} = S$$
Per definizione, il primo membro è uguale a
$$I^* I \mathcal{D}_{L/K} = S^* S^{*^{-1}} = S$$

2. Sia W la chiusura integrale di S in M. Allora
$$\begin{aligned}\mathrm{Tr}_{M/K}((\mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1})W) &= \mathrm{Tr}_{L/K}\,\mathrm{Tr}_{M/L}(\mathcal{D}_{L/K}^{-1}(\mathcal{D}_{M/L}^{-1}W)) \\ &= \mathrm{Tr}_{L/K}(\mathcal{D}_{L/K}^{-1}\,\mathrm{Tr}_{M/L}(\mathcal{D}_{M/L}^{-1}W)) \\ &= \mathrm{Tr}_{L/K}(\mathcal{D}_{L/K}^{-1}\,\mathrm{Tr}_{M/L}(W^*W)) \\ &\subseteq \mathrm{Tr}_{L/K}(\mathcal{D}_{L/K}^{-1}S) \\ &\subseteq R\end{aligned}$$
Dunque
$$\mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1} \subseteq \mathcal{D}_{M/K}^{-1}$$
Viceversa,
$$\mathrm{Tr}_{L/K}\underbrace{\mathrm{Tr}_{M/L}(\mathcal{D}_{M/K}^{-1}W)}_{\subseteq \mathcal{D}_{L/K}^{-1}} = \mathrm{Tr}_{M/K}(\mathcal{D}_{M/K}^{-1}W) \subseteq R$$
Dunque
$$\mathcal{D}_{L/K}\,\mathrm{Tr}_{M/L}(\mathcal{D}_{M/K}^{-1}W) \subseteq S$$
e
$$\mathcal{D}_{L/K}\mathcal{D}_{M/K}^{-1} \subseteq \mathcal{D}_{M/L}^{-1}$$

3. Siano $\sigma \in G$. Se mostriamo che $\mathcal{D}_{L/K}^{-1}$ è invariante per l'azione di G, allora lo è anche $\mathcal{D}_{L/K}$. Siano $x \in S^*$ e $y \in S$. Allora

$$\mathrm{Tr}(\sigma(x)y) = \mathrm{Tr}(x\sigma^{-1}(y)) \in S$$

da cui l'invarianza.

4. Basta notare che

$$\begin{aligned}
\mathrm{Tr}_{L/K}(J) \subseteq I &\iff I^{-1}\,\mathrm{Tr}_{L/K}(J) \subseteq R \\
&\iff \mathrm{Tr}_{L/K}(I^{-1}J) \subseteq R \\
&\iff \mathrm{Tr}_{L/K}(I^{-1}JS) \subseteq R \\
&\iff I^{-1}J \subseteq \mathcal{D}_{L/K}^{-1} \\
&\iff J \subseteq I\mathcal{D}_{L/K}^{-1}
\end{aligned}$$

□

Corollario 3.23. Il differente $\mathcal{D}_{L/K}^{-1}$ è il più grande ideale frazionario di S tale che ogni suo elemento ha traccia in R.

Sappiamo che l'applicazione traccia, nel caso di estensioni separabili, è surgettiva. La restrizione all'anello degli interi, non lo è.

Esempio. Sia $K = \mathbb{Q}$ e $L = \mathbb{Q}(i)$. Allora $R = \mathbb{Z}$ e $S = \mathbb{Z}[i]$. Notiamo che

$$\mathrm{Tr}_{L/K}(a + ib) = 2a$$

e dunque $\mathrm{Tr}_{L/K}(\mathbb{Z}[i]) = 2\mathbb{Z}$. Il codifferente

$$\begin{aligned}
\mathcal{D}_{L/K}^{-1} = S^* &= \{a + ib \in \mathbb{Q}(i) \mid \mathrm{Tr}_{L/K}((a+ib)\mathbb{Z}[i]) \subseteq \mathbb{Z}\} \\
&= \mathcal{D}_{L/K}^{-1} = \frac{\mathbb{Z}[i]}{2}
\end{aligned}$$

Corollario 3.24.

$$\mathrm{Tr}_{L/K}(S) = \mathrm{mcm}\left\{I \subseteq R\colon IS \mid \mathcal{D}_{L/K}\right\}$$

Dimostrazione. Applichiamo il punto 4 con $J = S$. Allora

$$\mathrm{Tr}_{L/K}(S) \subseteq I \iff S \subseteq I\mathcal{D}_{L/K}^{-1} \iff \mathcal{D}_{L/K} \subseteq IS$$

da cui la tesi. □

Corollario 3.25. $\mathrm{Tr}_{L/K}$ è surgettiva se e solo se $\mathcal{D}_{L/K}$ non ha divisori propri in $i_{L/K}(\mathcal{I}(R))$.

Consideriamo ora il caso particolare di un campo di numeri su $\mathbb{Q}$. Vale la seguente:

Proposizione 3.26. Sia L un'estensione di $\mathbb{Q}$ e sia $I \in \mathcal{F}(L)$. Sia $a_1, \ldots, a_n$ una $\mathbb{Z}$-base di I e sia $b_1, \ldots, b_n$ la sua base duale. Allora

- $I^* = \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}}$

- $N_{L/\mathbb{Q}}(\mathcal{D}_{L/\mathbb{Q}}(I)) = N_{L/\mathbb{Q}}(I)|\operatorname{disc}(L)|$. In particolare, per $I = \mathcal{O}_L$, vale $N_{L/\mathbb{Q}}(\mathcal{D}_{L/\mathbb{Q}}) = |\operatorname{disc}(L)|$

Dimostrazione. Preliminarmente, notiamo che $a_1, \dots, a_n$ è anche una $\mathbb{Q}$-base di L e dunque lo stesso vale per $b_1, \dots, b_n$. Sia $x \in I^*$; possiamo allora scriverlo in termini della base duale:

$$x = \sum_{i=1}^{n} \lambda_i b_i$$

dove $\lambda_i \in \mathbb{Q}$. Mostriamo che in realtà $\lambda_i \in \mathbb{Z}$. Per definizione,

$$\begin{aligned} x \in I^* &\iff \operatorname{Tr}_{L/\mathbb{Q}}(xI) \subseteq \mathbb{Z} \\ &\iff \operatorname{Tr}(xa_j) \in \mathbb{Z} \ \ \forall j \\ &\iff \textstyle\sum_{i=1}^{n} \lambda_i \underbrace{\operatorname{Tr}(b_i a_j)}_{=\delta_{i,j}} = \lambda_j \in \mathbb{Z} \end{aligned}$$

e dunque ogni $\lambda_i \in \mathbb{Z}$.
Mostriamo ora il secondo e il terzo punto. Poiché $\mathcal{D}_{L/\mathbb{Q}}(I) = I\mathcal{D}_{L/\mathbb{Q}}$, vale

$$N(\mathcal{D}_{L/\mathbb{Q}}(I)) = N(I)N(\mathcal{D}_{L/\mathbb{Q}})$$

e dunque è sufficiente dimostrare il caso particolare $I = \mathcal{O}_L$. Sia $w_1, \dots, w_n$ una base intera e sia $b_1, \dots, b_n$ la sua base duale. Allora

$$\mathcal{O}_L = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}} \quad \mathcal{D}_{L/\mathbb{Q}}^{-1} = \mathcal{O}_L^* = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}}$$

Sia $m \in \mathbb{Z}$ tale che $mb_i \in \mathcal{O}_L$ per ogni i; detto $c_i = mb_i$, si ha che $I = m\mathcal{D}_{L/\mathbb{Q}}^{-1} \subseteq \mathcal{O}_L$ è generato su $\mathbb{Z}$ dai c_i. Sappiamo che

$$m^{2n} \operatorname{disc}(b_1, \dots, b_n) = \operatorname{disc}(c_1, \dots, c_n) = N(I)^2 \operatorname{disc}(L)$$

Ma $N(I) = m^n N(\mathcal{D}_{L/\mathbb{Q}})^{-1}$ e dunque

$$N_{L/\mathbb{Q}}(\mathcal{D}_{L/\mathbb{Q}})^2 = \frac{\operatorname{disc}(L)}{\operatorname{disc}(b_1, \dots, b_n)}$$

D'altronde, $\operatorname{disc}(b_1, \dots, b_n) = \operatorname{disc}(L)^{-1}$. Infatti,

$$\begin{aligned} \operatorname{disc}(b_1 \dots b_n) &= \det((\sigma_i(b_j))_{i,j}^t (\sigma_i(b_j))_{i,j}) \\ \operatorname{disc}(L) &= \det((\sigma_i(w_j))_{i,j}^t (\sigma_i(w_j))_{i,j}) \end{aligned}$$

Il prodotto $(\sigma_i(b_j))_{i,j}(\sigma_i(w_j))_{i,j}^t$ è l'identità:

$$\sum_{k=0}^{n} \sigma_k(b_i)\sigma_k(w_j) = \delta_{i,j}$$

da cui la relazione sui discriminanti. Di conseguenza

$$N_{L/\mathbb{Q}}(\mathcal{D}_{L/\mathbb{Q}})^2 = \operatorname{disc}(L)^2$$

da cui la tesi. □

Definizione 3.27. Sia L/K un'estensione di campi. Definiamo il discriminante di L su K come $\mathrm{disc}(L/K) = N_{L/K}(\mathcal{D}_{L/K})$.

Segue dalla definizione che il discriminante è un ideale di K.

Proposizione 3.28. Sia $M \supseteq L \supseteq K$ una torre di estensioni. Allora

$$\mathrm{disc}(M/K) = N_{L/K}(\mathrm{disc}(M/L))(\mathrm{disc}(L/K))^{[M:L]}$$

Dimostrazione. Dato che

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$$

applicando la norma $N_{M/K}$ a questa relazione otteniamo

$$\begin{aligned}\mathrm{disc}(M/K) &= N_{L/K}N_{M/L}(\mathcal{D}_{M/L}\mathcal{D}_{L/K}) \\ &= N_{L/K}(N_{M/L}(\mathcal{D}_{M/L})N_{M/L}(\mathcal{D}_{L/K})) \\ &= N_{L/K}(\mathrm{disc}(M/L))N_{L/K}(\mathcal{D}_{L/K})^{[M:L]} \\ &= N_{L/K}(\mathrm{disc}(M/L))\,\mathrm{disc}(L/K)^{[M:L]}\end{aligned}$$

□

Consideriamo il caso $K = \mathbb{Q}$. Dalla fattorizzazione di $\mathrm{disc}(M)$ possiamo dedurne i gradi di possibili estensioni intermedie. Infatti, se $\mathbb{Q} \subsetneq L \subsetneq M$ dimostreremo che $\mathrm{disc}(L) \neq 1$ e per quanto visto vale $\mathrm{disc}(L)^{[M:L]} | \,\mathrm{disc}(M)$. Enunciamo ora il seguente teorema senza dimostrazione:

Teorema 3.29. Sia P un primo di R e sia $PS = Q^eI$, con $(Q, I) = 1$. Allora $Q^{e-1} \mid \mathcal{D}_{L/K}$. In tal caso, se inoltre $(e, N_{L/K}(Q)) = 1$, allora $Q^e \nmid \mathcal{D}_{L/K}$.

Il teorema ha come importante conseguenza il seguente:

Corollario 3.30.

- $Q \subseteq S$ è ramificato su P se e solo se $Q \mid \mathcal{D}_{L/K}$
- $P \subseteq R$ è ramificato in S se e solo se $P \mid \mathrm{disc}(L/K)$

Proposizione 3.31. Siano $K_1/K, K_2/K$ estensioni di campi e sia $L = K_1K_2$ il composto. Sia $P \subseteq R$. Allora

$$P \mid \mathrm{disc}(L/K) \iff P \mid \mathrm{disc}(K_1/K)\,\mathrm{disc}(K_2/K)$$

Dimostrazione.

$\Rightarrow$ Per ipotesi, P è ramificato in L/K. Se per assurdo valesse la relazione $P \nmid \mathrm{disc}(K_1/K)\,\mathrm{disc}(K_2/K)$ allora P non sarebbe ramificato in K_1 e in K_2 ma allora non sarebbe ramificato nel composto.

$\Leftarrow$ Supponiamo che $P \mid \mathrm{disc}(K_1/K)$; allora P è ramificato in K_1. Per moltiplicatività dell'indice di ramificazione, P è ramificato in L, da cui la tesi.

□

Corollario 3.32. Sia L/K un'estensione di campi e sia M la chiusura normale. Allora $\operatorname{disc}(M/K)$ e $\operatorname{disc}(L/K)$ hanno gli stessi primi nella fattorizzazione.

Dimostrazione. Sappiamo che P è ramificato in L se e solo se P è ramificato in M e dunque segue la tesi. □

Consideriamo $\mathbb{Q} \subseteq K \subseteq L$. Sia Q un primo di L e siano P, p le sue contrazioni. Allora $(e, N_{L/K}(Q)) = 1 \iff (e, p) = 1$ e dunque possiamo distinguere dal teorema due casi

Definizione 3.33. Diciamo che Q ha ramificazione tame su P se $p \nmid e(Q|P)$. P ha ramificazione tame in S se $PS = Q_1^{e_1} \dots Q_r^{e_r}$ e $p \nmid e_i$ per ogni i. Diciamo che Q ha ramificazione wild su P se $p \mid e_i$ per ogni i.

Corollario 3.34. Se Q è tame su P, allora $\operatorname{Tr}_{L/K}(S) \not\subset P$. Se per ogni primo P di R esiste Q con ramificazione tame su P, allora $\operatorname{Tr}_{L/K}(S) = R$.

Dimostrazione. Sappiamo che $\operatorname{Tr}_{L/K}(S) \subseteq P$ se e solo se $PS \mid \mathcal{D}_{L/K}$.

$$PS = Q^e I \quad (I, Q) = 1$$

Ma $Q^e \nmid \mathcal{D}_{L/K}$ e dunque $PS \nmid \mathcal{D}_{L/K}$. □

Esempio. Abbiamo visto che nel caso $L = \mathbb{Q}(i)$,

$$\operatorname{Tr}_{L/\mathbb{Q}}(\mathbb{Z}[i]) = 2\mathbb{Z}$$

e $\mathcal{D}_{L/\mathbb{Q}} = 2$. Sappiamo effettivamente che $(2) = (1-i)^2$ ha ramificazione wild perché $2 \mid e = 2$.

Assumiamo il teorema

Teorema 3.35. Se $K \supseteq \mathbb{Q}$, allora $|\operatorname{disc}(K)| > 1$. In particolare, esiste $p \in \mathbb{Z}$ ramificato in K.

Il teorema non si può estendere: se $L \supsetneq K \supsetneq \mathbb{Q}$, non è detto che in L/K ci siano primi ramificati.

Esempio. Consideriamo $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, $K_a = \mathbb{Q}(\sqrt{a})$ e $K_b = \mathbb{Q}(\sqrt{b})$. Sia $a \equiv b \equiv 1 \pmod 4$ con $(a, b) = 1$. Sappiamo che

- p ramifica in L se e solo se P ramifica in almeno una delle estensioni intermedie.
- p ramifica in L se e solo se $p \mid a$ o $p \mid b$.

Supponiamo $p \mid a$ (allora $p \nmid b$). Allora

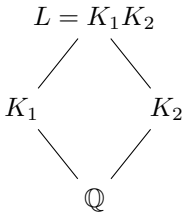
$$p\mathcal{O}_a = P^2 \qquad p\mathcal{O}_b = \begin{cases} Q & f = 2 \\ Q_1 Q_2 \end{cases}$$

Di conseguenza,

$$p\mathcal{O}_L = \begin{cases} U^2 & f = 2 \\ U_1^2 U_2^2 & f = 1 \end{cases}$$

Mostriamo che L/K_{ab} non ha primi ramificati. Sia U un primo di $\mathcal{O}_L$. Se U è ramificato su K_{ab}, allora U è ramificato su $\mathbb{Q}$. Quindi $U \cap \mathbb{Z} = p \mid a$ e $\mathcal{O}_{ab} = Q^2$.

Consideriamo il caso di estensioni linearmente disgiunte e supponiamo che $(\mathrm{disc}(K_1), \mathrm{disc}(K_2)) = 1$.



In questo caso, vale il teorema 1.32; in realtà il teorema può essere raffinato:

Teorema 3.36. Consideriamo delle estensioni $K_i/\mathbb{Q}$, con $[K_i : \mathbb{Q}] = n_i$ e chiamiamo $d_i = \mathrm{disc}(K_i)$, con $i = 1, 2$. Se $(d_1, d_2) = 1$ e $L = K_1K_2$ si ha

1. $[L : \mathbb{Q}] = n_1n_2$
2. $\mathrm{disc}(L) = d_1^{n_2}d_2^{n_1}$
3. Se $\{w_i\}_i$ è una base intera di K_1 e $\{v_j\}_j$ è una base intera di K_2, allora $\{w_iv_j\}_{i,j}$ è una base intera di L.

Dimostrazione.

1. Sia $K_1 = \mathbb{Q}(a)$ e sia μ il suo polinomio minimo su $\mathbb{Q}$. Sia K la chiusura normale di $K_1/\mathbb{Q}$, il campo di spezzamento di μ. Sappiamo che $d(K)$ ha gli stessi fattori primi di d_1 e dunque $(d(K), d_2) = 1$. Notiamo che $L = K_2(a)$. Allora

   $$[L : \mathbb{Q}] = [K_2(a) : K_2][K_2 : \mathbb{Q}] = \deg(g)n_2$$

   dove g è il polinomio minimo di a su K_2. Chiaramente $g \mid \mu$: la tesi equivale a mostrare che $g = \mu$. Sia $k = K \cap K_2$ e notiamo che $g \in k[x]$. Dato che $k \subseteq K$, si ha $d(k) \mid d(K)$; analogamente $d(k) \mid d_2$ e dato che questi sono coprimi si ha $d(k) = 1$, cioè $k = \mathbb{Q}$. Quindi $g \in \mathbb{Q}[x]$ e $g = \mu$.

3. Segue da quanto mostrato nel teorema 1.32 e nel punto 1.

2. Per il punto 3, $\mathrm{disc}(L) = \mathrm{disc}(w_iv_j)$. Dette σ_i le immersioni di K_1 su $\mathbb{Q}$ e τ_j le immersioni di K_2 su $\mathbb{Q}$ le estendiamo a K_1K_2 e le rinominiamo $\tilde{\sigma}_i$ e $\tilde{\tau}_j$. Allora

   $$\mathrm{disc}(L) = \det(\tilde{\sigma}_h\tilde{\tau}_l(w_iv_j))^2 = \det(\sigma_h(w_i)\tau_l(v_j))^2$$

   Inoltre,

   $$\mathrm{disc}(K_1) = \det(\sigma_k(w_i))^2 \qquad \mathrm{disc}(K_2) = \det(\tau_l(v_j))^2$$

   La matrice del discriminante di L è il prodotto di Kronecker di quest'ultima, da cui la tesi.

□

Capitolo 4

Gruppo delle Classi e Teorema di Dirichlet

4.1 Gruppo delle Classi

Sia K un campo di numeri. Abbiamo visto nella sezione 2.1 che l'insieme degli ideali frazionari $\mathcal{F}(K)$ è un gruppo abeliano libero generato dagli ideali primi di $\mathcal{O}_K$. Il quoziente per il sottogruppo $\mathcal{P}(K)$ degli ideali principali

$$\mathrm{Cl}(K) = {}^{\mathcal{I}(K)}\!\diagup_{\mathcal{P}(K)}$$

è il gruppo delle classi. Siamo ora interessati a studiare questo gruppo; in particolare vogliamo dimostrare il seguente:

Teorema 4.1. Sia K un campo di numeri. Allora $\mathrm{Cl}(K)$ è finito.

Osservazione 4.2.

- $\mathrm{Cl}(K) = 0$ se e solo se $\mathcal{O}_K$ è UFD.
- Per ogni $C \in \mathrm{Cl}(K)$ esiste un ideale intero I di $\mathcal{O}_K$ tale che $I \in C$. Infatti, per ogni $J \in C$ e per ogni $d \in \mathcal{O}_K$ si ha $J \simeq dJ$. Dunque ogni classe è rappresentato da ideali interi.

Per dimostrare il teorema, abbiamo prima bisogno di una stima sulla norma degli ideali interi.

Proposizione 4.3. Sia K un campo di numeri. Esiste una costante $\lambda \in \mathbb{R}$ tale che per ogni I ideale di $\mathcal{O}_K$ esiste $\alpha \in I$ per il quale $N(\alpha) \leq \lambda N(I)$.

Dimostrazione. Sia $\alpha_1, \ldots, \alpha_n$ una base intera di $K/\mathbb{Q}$ e siano σ_i le immersioni in $\overline{K}$. Mostriamo che

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

soddisfa la tesi. Sia I un ideale di $\mathcal{O}_K$. La successione $a_m = m^n$ è crescente e illimitata, esiste $m \in \mathbb{N}$ tale che

$$m^n \leq N(I) \leq (m+1)^n$$

Consideriamo gli $(m+1)^n$ elementi di $\mathcal{O}_K$

$$\sum_{j=1}^{n} m_j \alpha_j \quad 0 \leq m_j \leq m$$

Dato che la norma di un ideale coincide con la cardinalità del quoziente, almeno due di questi elementi hanno la stessa proiezione in $\mathcal{O}_K/I$, cioè appartengono alla stessa classe laterale di I. La differenza di tali elementi è un elemento $\alpha \in I \setminus \{0\}$ tale che

$$\alpha = \sum \bar{m}_j \alpha_j \quad |\bar{m}_j| \leq m$$

Allora

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\alpha)| &= |\prod_{i=1}^{n} \sigma_i(\sum m_j \alpha_j)| \\
&= |\prod_i \sum_j \bar{m}_j \sigma_i(\alpha_j)| \\
&\leq \prod_i \sum_j |\bar{m}_j||\sigma_i(\alpha_j)| \\
&\leq m^n \underbrace{\prod_i \sum_j |\sigma_i(\alpha_j)|}_{=\lambda} \\
&\leq \lambda N(I)
\end{aligned}$$

□

Corollario 4.4. Ogni classe di ideali $C \in \mathrm{Cl}(K)$ contiene un ideale $J \subseteq \mathcal{O}_K$ con $N(J) \leq \lambda$.

Dimostrazione. Sia $C \in \mathrm{Cl}(K)$ e sia $I \in C^{-1}$. Per la proposizione precedente, esiste $\alpha \in I$ tale che $|N(\alpha)| \leq \lambda N(I)$. Dato che $\alpha \in I$, si ha $I \mid (\alpha)$ e dunque $(\alpha) = IJ$, con J ideale intero. Allora $J \in C^{-1^{-1}} = C$. Per moltiplicatività della norma,

$$N(I)N(J) \leq \lambda N(I) \Longrightarrow N(J) \leq \lambda$$

□

Dunque ogni classe di ideali può essere rappresentata da un primo con norma limitata. Siamo allora pronti a dimostrare il teorema:

Dimostrazione del Teorema 4.1. Mostriamo che che il gruppo delle classi è finito; mostriamo in particolare che esiste solo un numero finito di ideali di norma limitata. Sia J un ideale intero di $\mathcal{O}_K$ e sia

$$J = P_1^{n_1} \dots P_s^{n_s}$$

la sua fattorizzazione. Allora la sua norma è

$$N(J) = N(P_1)^{n_1} \dots N(P_s)^{n_s} = \prod_{i=1}^{s} p_i^{f_i n_i}$$

dove $p_i = P_i \cap \mathbb{Z}$ e $f_i = f(P_i|p_i)$.

$$N(J) \leq \lambda \iff \prod_{i=1}^{s} p_i^{f_i n_i} \leq \lambda$$

In particolare, deve valere $p_i \leq \lambda$ per ogni i e dunque i primi P_i sono in numero finito, perché sono al più i primi che compaiono nella fattorizzazione di $p\mathcal{O}_K$. Allo stesso modo gli esponenti sono limitati e dunque J si deve fattorizzare con primi in un insieme finito e esponenti limitati. Di conseguenza, esistono solo finiti J con questa proprietà. □

Esempio. Calcoliamo $\mathrm{Cl}(K)$, con $K = \mathbb{Q}(\sqrt{-5})$. Sappiamo che in questo caso $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ e $d_K = -20$. Seguiamo il procedimento dato dalla dimostrazione; troviamo λ come nella proposizione. Scelta la base intera $\mathcal{B} = \{1, \sqrt{-5}\}$, si ha

$$\lambda = (1 + |\sqrt{-5}|)(1 + |-\sqrt{-5}|) = (1 + \sqrt{5})^2 < 11$$

Quindi, per il corollario, ogni classe di ideali contiene un ideale J con norma di $J \leq 10$. In particolare, possono comparire come rappresentanti solo primi che compaiono nella fattorizzazione di estensioni dei primi $2, 3, 5, 7$. Utilizzando 2.3, otteniamo

$$2\mathcal{O}_K = P^2 = (2, 1 + \sqrt{-5})^2 \qquad 3\mathcal{O}_K = P_1P_2 \quad f_i = 1$$
$$5\mathcal{O}_K = (\sqrt{-5})^2 \qquad 7\mathcal{O}_K = Q_1Q_2$$

Quindi $\mathrm{Cl}(K) = \langle [P], [P_1], [P_2], [Q_1], [Q_2] \rangle$. Studiamo le relazioni.
Notiamo che non esiste α tale che $N(\alpha) \leq 2$ e dunque P non è principale, da cui $\mathrm{Cl}(K) \neq \{\mathrm{Id}\}$. Inoltre, dato che P^2 è principale, $\mathrm{ord}[P] = 2$ e dunque $2 \mid |\mathrm{Cl}(K)|$. Non esiste neanche α tale che $N(\alpha) = 3$ e dunque P_1, P_2 non sono principali. Si ha però $[P_1] = -[P_2]$ perché $P_1P2 = (3)$ che è principale. Osserviamo inoltre che $N(1 + \sqrt{-5}) = 6$ e quindi $(1 + \sqrt{-5}) = PP_1$; di conseguenza, $[P] = [P_1] = [P_2]$. Non esiste neanche $\alpha \in \mathcal{O}_K$ tale che $N(\alpha) = 7$ e dunque Q_1, Q_2 non sono principali. Sia $\beta = 3 + \sqrt{-5}$; allora $N(\beta) = 14$ e dunque $(\beta) = Q_1P$ e quindi $[Q_1] = [P]^{-1} = [P]$. Di conseguenza, $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$.

L'esempio mostra l'importanza di trovare una costante λ migliore, in modo da dover esaminare meno casi. Le dimostrazioni dei teoremi forniscono infatti un metodo costruttivo per determinare il gruppo delle classi.

Definizione 4.5. Sia $H \subseteq \mathbb{R}^n$ un sottogruppo. H si dice discreto se per ogni $K \subseteq \mathbb{R}^n$ compatto $|H \cap K| < \infty$

Esempio.

- $\mathbb{Z}^n$ è un sottogruppo discreto.
- $\mathbb{Z}^r \times \{0\}^{n-r}$ è discreto.
- Siano $v_1, \ldots, v_r$ elementi linearmente indipendenti. Allora $H = \langle v_1, \ldots, v_r \rangle_{\mathbb{Z}}$ è un sottogruppo discreto.

In realtà questi esauriscono tutti i possibili esempi:

Proposizione 4.6. Sia H un sottogruppo discreto di $\mathbb{R}^n$. Allora esistono $v_1, \ldots, v_r \in \mathbb{R}^n$ linearmente indipendenti tali che $H = \langle v_1, \ldots, v_r \rangle_{\mathbb{Z}}$.

Dimostrazione. Siano $e_1, \dots, e_r \in H$ un insieme massimale di elementi linearmente indipendenti su $\mathbb{R}$. Sia $x \in H$; allora x è dipendente su $\mathbb{R}$ e dunque esistono $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tali che

$$x = \sum_{i=1}^{r} \lambda_i e_i$$

Consideriamo l'inviluppo convesso di $e_1, \dots, e_n$:

$$P = \Big\{ \sum_{i=1}^{r} a_i e_i \mid 0 \leq a_i \leq 1 \Big\}$$

P è un compatto e dunque $P \cap H$ è finito. Per ogni $j \in \mathbb{Z}$, sia

$$x_j = jx - \sum_{i=1}^{r} \lfloor j\lambda_i \rfloor e_i = \sum (j\lambda_i - \lfloor j\lambda_i \rfloor) e_i \tag{4.1}$$

Notiamo che $jx \in H$ e $\lfloor j\lambda_i \rfloor e_i$ appartengono ad H perché sono multipli interi di elementi di H. Di conseguenza $x_j \in P \cap H$ per ogni $j \in \mathbb{N}$. Dato che $\mathbb{Z}$ è infinito e $P \cap H$ è finito, esistono $j, h \in \mathbb{N}$ tali che $x_j = x_h$ e quindi si ha dalla 4.1

$$(j-h)\lambda_i = \lfloor j\lambda_i \rfloor - \lfloor h\lambda_i \rfloor$$

dove abbiamo utilizzato il fatto che gli e_i siano linearmente indipendenti. Dunque $\lambda_i \in \mathbb{Q}$ per ogni i e H è generato su $\mathbb{Z}$ dagli e_i e dagli elementi di $P \cap H$, che sono combinazioni razionali degli e_i. Sia $d \in \mathbb{Z}$ il minimo comune multiplo dei denominatori dei coefficienti delle combinazioni lineari che danno i finiti elementi di $P \cap H$. Allora abbiamo i contenimenti

$$\langle e_1, \dots, e_r \rangle_{\mathbb{Z}} \subseteq H \subseteq \frac{1}{d} \langle e_1, \dots, e_r \rangle_{\mathbb{Z}}$$

da cui segue che H è libero di rango r, da cui la tesi. □

Definizione 4.7. Un sottogruppo discreto di $\mathbb{R}^n$ di rango n si chiama reticolo.

Notiamo che Λ è un reticolo di $\mathbb{R}^n$ se e solo se Λ è uno $\mathbb{Z}$ -modulo generato da una base di $\mathbb{R}^n$. Ad ogni reticolo possiamo associare l'inviluppo convesso dato da una sua base. Più precisamente, dato Λ un reticolo, $\Lambda = \langle e_1, \dots e_n \rangle_{\mathbb{Z}}$. Sia $e = (e_1, \dots, e_n)$. Chiamiamo

$$P_e = \Big\{ \sum_{i=1}^{n} \alpha_i e_i \;\Big|\; 0 \leq \alpha_i \leq 1 \;\; \alpha_i \in \mathbb{R} \Big\}$$

il dominio fondamentale. Questo dipende dalla base scelta; la sua misura di Lebesgue è però invariante.

Lemma 4.8. La misura di Lebesgue del dominio fondamentale non dipende dalla base scelta, ma solo da Λ.

Dimostrazione. La misura del dominio fondamentale rispetto a una base e è

$$\mu(P_e) = |\det(e_1, \dots, e_n)|$$

Data una base v, si ha

$$\mu(P_v) = |\det(v_1, \ldots, v_n)|$$

La matrice di cambiamento di base M fornisce

$$\mu(P_v) = |\det M|\mu(P_e)$$

Ma M è una matrice di cambiamento di base di uno $\mathbb{Z}$-modulo e dunque deve avere determinante ± 1. □

Definizione 4.9. Definiamo il volume del reticolo Λ come $\mathrm{Vol}(\Lambda) = \mu(P_e)$, dove e è una qualsiasi base di Λ.

Teorema 4.10 (di Minkowski)**.** Sia Λ un reticolo di $\mathbb{R}^n$ e sia S un sottoinsieme di $\mathbb{R}^n$ Lebesgue-misurabile tale che

$$\mu(S) > \mathrm{Vol}(\Lambda)$$

Allora esistono $x, y \in S$ distinti tali che $0 \neq x - y \in \Lambda$.

Dimostrazione. Sia $e_1, \ldots, e_n$ una base del reticolo e sia P_e il suo dominio fondamentale. Scriviamo

$$S = \bigcup_{\lambda \in \Lambda} S \cap (\lambda + P_e)$$

Λ è numerabile e quindi $\mu(S) = \sum \mu(S \cap \lambda + P_e)$. Dato che la misura di Lebesgue è invariante per traslazione

$$\mu(S \cap \lambda + P_e) = \mu(-\lambda + S \cap P_e)$$

e si ottiene $\mu(S) = \sum \mu((S - \lambda) \cap P_e)$ D'altronde gli insiemi

$$\{-\lambda + S \cap P_e\}_{\lambda \in \Lambda}$$

non possono essere tutti disgiunti perché la somma delle misure è $\mu(S)$ e sono tutti contenuti in P_e, che per ipotesi ha misura minore di $\mu(S)$. Esistono allora $\lambda_1, \lambda_2 \in \Lambda$ distinti tali che

$$(-\lambda_1 + S) \cap (-\lambda_2 + S) \cap P_e \neq \emptyset$$

e dunque esistono $x, y \in S$ tali che $-\lambda_1 + x = -\lambda_2 + y$ da cui la tesi. □

Corollario 4.11. Sia Λ un reticolo di $\mathbb{R}^n$. Supponiamo che S sia misurabile, convesso e simmetrico rispetto a 0. Supponiamo inoltre che valga una delle seguenti

1. $\mu(S) > 2^n \mathrm{Vol}(\Lambda)$
2. $\mu(S) \geq 2^n \mathrm{Vol}(\Lambda)$ e S compatto

Allora $S \cap \Lambda$ contiene un punto diverso da 0.

Dimostrazione. Supponiamo valga la prima condizione. Sia $S' = \frac{1}{2}S$; allora S' soddisfa le ipotesi di Minkowski. Dunque esistono $x, y \in S'$ distinti tali che $0 \neq x - y \in \Lambda$. Siano $x' = 2x \in S$ e $y' = -2y \in S$ (stiamo sfruttando che S sia simmetrico rispetto all'origine) ; allora per convessità di S,

$$x - y = \frac{1}{2}x' + \frac{1}{2}y' \in S \cap \Lambda$$

da cui la tesi.
Supponiamo ora valga seconda condizione e sia $S_n = (1 + \frac{1}{n})S$. Allora S_n soddifa le ipotesi del primo punto di questo corollario e dunque per ogni $n \in \mathbb{N}$ esiste $x_n \in S_n$ tale che $x_n \in \Lambda \cap H$. Dato che S è compatto, esiste una sottosuccessione x_{n_k} convergente. Sia $x = \lim x_{n_k}$; allora, dato che Λ e S sono chiusi, $x \in \Lambda \cap H$. □

Sfruttiamo ora la teoria svolta sui reticoli e troviamo una immersione di un campo di numeri in $\mathbb{R}^n$. Sia K un campo di numeri di grado n su $\mathbb{Q}$ e siano σ_i le immersioni in $\mathbb{C}$. Consideriamo il coniugio ϵ in $\mathbb{C}$; dato che queste sono tutte e sole le immersioni in $\mathbb{C}$, per ogni indice i esiste j tale che $\sigma_j = \epsilon \circ \sigma_i$. Inoltre

$$\epsilon \circ \sigma_i = \sigma_i \iff \sigma_i(K) \subseteq \mathbb{R}$$

Possiamo allora enumerare le immersioni reali con $\sigma_1, \dots, \sigma_r \colon K \to \mathbb{R}$ e quelle a valori nei complessi con $\sigma_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \dots, \bar{\sigma}_{r+s} \colon K \to \mathbb{C}$.

Osservazione 4.12. Se $K/\mathbb{Q}$ è un'estensione di Galois, ci sono due casi:

- Se $K \subseteq \mathbb{R}$ si ha $n = r$.
- Se $K \not\subseteq \mathbb{R}$ si ha $n = 2s$.

Consideriamo allora l'immersione di K

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{R}^r \times \mathbb{C}^s \\ x & \longrightarrow & (\sigma_1(x), \dots, \sigma_r(x), \sigma_{r+1}(x), \dots, \sigma_{r+s}(x)) \end{array}$$

Componendo con parte reale e parte immaginaria, otteniamo una immersione in $\mathbb{R}^n$

$$\begin{array}{rccc} \sigma \colon & K & \longrightarrow & \mathbb{R}^n \\ & x & \longmapsto & (\sigma_1(x), \dots, \sigma_r(x), \Re\sigma_{r+1}(x), \Im\sigma_{r+1}(x), \dots) \end{array}$$

σ è un omomorfismo iniettivo e quindi è una immersione di K in $\mathbb{R}^n$.

Proposizione 4.13. Sia $M = \langle x_1, \dots, x_n \rangle$ uno $\mathbb{Z}$-modulo libero di rango n contenuto in K. Allora $\sigma(M)$ è il reticolo di $\mathbb{R}^n$ e

$$\mathrm{Vol}(M) = 2^{-s}\sqrt{|\operatorname{disc}(M)|}$$

Dimostrazione. Notiamo che $\sigma(M) = \langle \sigma(x_1), \dots, \sigma(x_n) \rangle$; basta mostrare che tale reticolo ha volume diverso da 0. Il volume di un inviluppo convesso è il determinante della matrice dei vettori che lo generano e dunque

$$\mathrm{Vol}(\sigma(M)) = |\det(\sigma(x_1), \dots, \sigma(x_n))|$$

Notiamo che l'i-esima colonna di questa matrice è

$$\begin{pmatrix} \sigma_1(x_i) \\ \vdots \\ \sigma_r(x_i) \\ \Re\sigma_{r+1}(x_i) \\ \Im\sigma_{r+1}(x_i) \\ \vdots \end{pmatrix}$$

Cambiamo base per ottenere la matrice del discriminante, utilizzando le formule

$$\Re(z) = \frac{1}{2}(z + \bar{z}) \qquad\qquad \Im(z) = \frac{1}{2i}(z - \bar{z})$$

Otteniamo così la matrice del discriminante a meno di un fattore 2^{-s} e dunque

$$\mathrm{Vol}(\sigma(M)) = \det(\sigma(x_1), \dots, \sigma(x_n)) = 2^{-s} |\det(\sigma_i(x_j))| = 2^{-s}\sqrt{|\operatorname{disc}(M)|}$$

□

Corollario 4.14. Sia $I \neq 0$ un ideale di $\mathcal{O}_K$. Allora

$$\mathrm{Vol}(\sigma(I)) = 2^{-s} N(I) \sqrt{|\operatorname{disc}(K)|}$$

Inoltre,

$$\mathrm{Vol}(\sigma(\mathcal{O}_K)) = 2^{-s}\sqrt{|\operatorname{disc}(K)|}$$

Teorema 4.15. Sia $[K : \mathbb{Q}] = r + 2s = n$, sia $d = \operatorname{disc}(K)$ e sia $I \neq 0$ un ideale di $\mathcal{O}_K$. Allora esiste $x \in I$ tale che

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |d|^{\frac{1}{2}} N(I)$$

Dimostrazione. Sia $t \in \mathbb{R}^+$ e consideriamo l'insieme

$$B_t = \left\{ (y, z) \in \mathbb{R}^r \times \mathbb{C}^s \,\middle|\, \sum_{i=1}^{r} |y_i| + 2 \sum_{j=1}^{s} |z_j| \leq t \right\}$$

B_t è convesso e simmetrico rispetto all'origine. La misura di tale insieme è

$$\mu(B_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

Scegliamo t tale che $\mu(B_t) = 2^n \,\mathrm{Vol}(\sigma(I))$; dalle equazioni ricaviamo

$$t^n = 2^{n-r} \pi^{-s} n! |d|^{\frac{1}{2}} N(I)$$

da cui otteniamo il valore voluto di t. Per il teorema di Minkowski, esiste $x \in I \setminus \{0\}$ tale che $\sigma(x) \in B_t$. Calcoliamone la norma:

$$\begin{aligned}
|N(x)| &= \prod_{i=1}^{n} |\sigma_i(x)| \\
&= \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=1}^{s} |\sigma_{r+j}(x)|^2 \\
&\leq \left(\frac{1}{n} \sum_{i=1}^{r} |\sigma_i(x)| + \frac{2}{n} \sum_{j=1}^{s} |\sigma_{r+j}(x)| \right)^n && \text{disuguaglianza media aritmetica-geometrica} \\
&\leq \frac{t^n}{n^n} && \sigma(x) \in B_t \\
&= \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s |d|^{\frac{1}{2}} N(I) && \text{dalla relazione } n = r + 2s
\end{aligned}$$

□

Notiamo che a priori bisognerebbe conoscere il discriminante del campo; di solito si utilizzano maggiorazioni, calcolando il discriminante di un singolo elemento intero.

Corollario 4.16 (Costante di Minkowski)**.** Ogni classe di ideali $C \in \mathrm{Cl}(K)$ contiene un ideale I tale che

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s |d|^{\frac{1}{2}}$$

Esempio. Riprendiamo l'esempio $K = \mathbb{Q}(\sqrt{-5})$. In questo caso, la costante di Minkowski è

$$\frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s |d|^{\frac{1}{2}} = \frac{2}{4} \frac{4}{\pi} \sqrt{20} < 3$$

e dunque avremmo dovuto considerare solo $p = 2$.

Corollario 4.17. Sia $[K : \mathbb{Q}] = n \geq 2$ e sia $d = \mathrm{disc}(K)$. Allora

$$|d| \geq \frac{\pi}{3} \left(\frac{3\pi}{4} \right)^{n-1}$$

Equivalentemente,

$$\frac{n}{\log |d|} \leq k$$

dove k è una costante assoluta.

Dimostrazione. Sappiamo che

$$1 \leq N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^n |d|^{\frac{1}{2}}$$

Di conseguenza,

$$|d|^{\frac{1}{2}} \geq \left(\frac{\pi}{4} \right)^n \frac{n^n}{n!}$$

Elevando al quadrato,

$$|d| \geq \left(\frac{\pi}{4}\right)^{2n} \frac{n^{2n}}{n!^2} \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{n!^2} = a_n$$

Mostriamo per induzione che

$$a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

Per $n = 2$, è ovvio; supponiamo la tesi vera per n e dimostriamo che vale per $n+1$.

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4}\frac{(n+1)^{2(n+1)}}{(n+1)^2 n!^2}\frac{n!^2}{n^{2n}} \\ &= \frac{\pi}{4}\Big(1+\frac{1}{n}\Big)^{2n} \\ &\geq \frac{3\pi}{4}\end{aligned}$$

Dunque

$$a_{n+1} \geq \frac{3\pi}{4} a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n}$$

□

Corollario 4.18. Se $K \supsetneq \mathbb{Q}$, $|\operatorname{disc}(K)| > 1$.

Teorema 4.19 (di Hermite)**.** Esistono solo un numero finito di campi di numeri di discriminante assegnato.

Dimostrazione. Fissiamo $d \in \mathbb{N}$; se $|\operatorname{disc}(K)| = d$, allora $[K : \mathbb{Q}] \leq h \log(d)$ e dunque il grado su $\mathbb{Q}$ di un campo con discriminante d è limitato. Dividiamo le immersioni in r reali e $2s$ immersioni complesse; è allora sufficiente mostrare che, comunque fissati r, s e d, la cardinalità dell'insieme

$$\{K \mid [K:\mathbb{Q}] = n = r + 2s \;\; |\operatorname{disc}(K)| = d\}$$

è finita. Consideriamo l'insieme

$$B = \begin{cases} \{(y,z) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_1| \leq A \;\; |y_i| \leq \frac{1}{2} \quad |z_j| \leq \frac{1}{2}\} & \text{se } r > 0 \\ \{z \in \mathbb{C}^s \mid |z_1 - \bar{z}_1| \leq C \;\; |z_1 + \bar{z}_1| \leq \frac{1}{2} \;\; |z_i| \leq \frac{1}{2}\} & \text{altrimenti} \end{cases}$$

Scegliamo le costanti A, C tali che

$$\mu(B) = 2^n \operatorname{Vol}(\sigma\mathcal{O}_K) = 2^n 2^{-s} d^{1/2}$$

Svolgiamo i conti: se $r > 0$

$$\mu(B) = 2A\left(\frac{\pi}{4}\right)^{s}$$

e dunque

$$A = \frac{2^{r-s-1}}{\pi^s} d^{1/2}$$

Allo stesso modo è possibile scegliere la costante C. Notiamo che B è compatto, convesso e simmetrico rispetto a 0 e dunque per il teorema di Minkowski esiste $x \in \mathcal{O}_K$ tale che $\sigma(x) \in B$. Mostriamo che x è un elemento primitivo per l'estensione $K/\mathbb{Q}$. Chiaramente $\mathbb{Q}(x) \subseteq K$. Mostriamo che x ha tutti i coniugati distinti; equivalentemente, che $\sigma_1(x) \neq \sigma_i(x)$ per ogni i. Notiamo che $x \in \mathcal{O}_K$ e dunque $|N(x)| \geq 1$. Supponiamo $r > 0$. Dato che $\sigma(x) \in B$, le componenti dalla seconda all'ultima sono limitate $|\sigma_i(x)| \leq 1/2$ e otteniamo allora $\sigma_1(x) > 1$ e dunque $\sigma_1(x) \neq \sigma_i(x)$. Il caso $r = 0$ è analogo; abbiamo allora mostrato che fissati r, s, d, K è generato da un intero $x \in \mathcal{O}_K$ tale che $\sigma(x) \in B$. Gli interi $x \in \mathcal{O}_K$ tali che $\sigma(x) \in B$ sono però in numero finito. Infatti, se $\sigma(x) \in B$, x ha tutti i coniugati di modulo limitato. Allora i coefficienti di μ_x sono limitati in quanto i coefficienti sono combinazione finita delle radici e $\mu_x \in \mathbb{Z}[x]$. Di conseguenza esistono finiti polinomi di cui un tale elemento può essere radice, da cui la tesi. □

4.2 Teorema delle Unità di Dirichlet

Studiamo la struttura di gruppo degli invertibili di un anello di interi. Sappiamo che certamente $\{\pm 1\}$ è contenuto in questi ma ne possono esistere altri, come abbiamo visto nell'esempio 1.2. Sia allora K un campo di numeri e supponiamo che abbia r immersioni reali $\sigma_1, \dots \sigma_r \colon K \to \mathbb{R}$ e $2s$ immersioni complesse $\sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}$. Vale allora il seguente:

Teorema 4.20 (di Dirichlet)**.** $\mathcal{O}_K^*$ è isomorfo a $\mathbb{Z}^{r+s-1} \oplus T$, dove T è ciclico, finito ed è composto dalle radici dell'unità in $\mathcal{O}_K$.

Notiamo che come conseguenza,

$$\mathcal{O}_K \diagup_T \simeq \mathbb{Z}^{r+s-1}$$

è un gruppo abeliano libero, generato da $\langle \epsilon_1, \dots, \epsilon_{r+s-1} \rangle$. Dei generatori della parte libera vengono detti *unità fondamentali.*
Il teorema si divide in 3 parti:

1. Dimostrare che $\mathcal{O}_K^*$ è finitamente generato
2. Mostrare che il sottomodulo di torsione è del tipo $\{\alpha \in K \mid \exists d \in \mathbb{N}\ \alpha^d = 1\}$
3. Dimostrare che il rango di $\mathcal{O}_K^*$ è esattamente $r + s - 1$

Iniziamo con la prima parte. Consideriamo l'omomorfismo di gruppi, detta mappa logaritmica:

$$\begin{array}{rccccc} L\colon & K^* & \longrightarrow & \mathbb{R}^r \times \mathbb{C}^s & \longrightarrow & \mathbb{R}^{r+s} \\ & x & \longmapsto & (\sigma_1(x), \dots, \sigma_{r+s}(x)) & \longmapsto & (\log|\sigma_1(x)|, \dots, \log|\sigma_{r+s}(x)|) \end{array}$$

Notiamo che se B è un compatto in $\mathbb{R}^{r+s}$, l'insieme

$$B' = \{x \in \mathcal{O}_K^* \mid L(x) \in B\}$$

è finito. Sia infatti $x \in B'$; dato che B è compatto, è limitato e dunque esiste $\alpha \in \mathbb{R}$ tale che $|\log|\sigma_i(x)|| \leq \alpha$ per ogni i. Allora i coniugati di x hanno modulo

limitato e dunque vi sono un numero finito di polinomi del quale può essere radice. Di conseguenza, il nucleo $\mathrm{Ker}(L|_{\mathcal{O}_K^*})$ è finito, dato che è controimmagine del compatto 0; notiamo che è costituito dall'insieme $\{x \in \mathcal{O}_K^* \mid \exists t \in \mathbb{N} \;\; x^t = 1\}$. Intanto, $\mathrm{Ker}(L|_{\mathcal{O}_K^*})$ è ciclico perché sottogruppo moltiplicativo finito di un campo e dunque vale un contenimento. D'altra parte, se $x \in \mathcal{O}_K^*$ tale che $x^t = 1$, allora $|\sigma_i(x)| = 1$ e dunque $L(x) = 0$.
Abbiamo mostrato quindi che $L(\mathcal{O}_K^*)$ è un sottogruppo discreto di $\mathbb{R}^{r+s}$, perché interseca ogni compatto in un numero finito di punti per il ragionamento fatto sopra. Per il teorema 4.6, $L(\mathcal{O}_K^*)$ è uno $\mathbb{Z}$-modulo libero finitamente generato di rango $d \leq r + s$. Consideriamo la successione esatta

$$0 \to T \longrightarrow \mathcal{O}_K^* \longrightarrow L(\mathcal{O}_K^*) \to 0$$

Dunque $\mathcal{O}_K^* \simeq L(\mathcal{O}_K^*) \oplus T$ perchè $L(\mathcal{O}_K^*)$ è un modulo proiettivo.
Abbiamo così mostrato i primi due punti del teorema; rimane l'ultimo. Mostriamo ora che vale $d \leq r + s - 1$; consideriamo l'iperpiano (che per definizione ha dimensione $n - 1$)

$$W = \Big\{(x, y) \in \mathbb{R}^r \times \mathbb{R}^s \Big| \sum_{i=1}^{r} x_i + 2\sum_{j=1}^{s} y_j = 0\Big\}$$

Mostriamo che $L(\mathcal{O}_K^*) \subseteq W$; se $x \in \mathcal{O}_K^*$, allora vale

$$1 = |N(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=1}^{s} |\sigma_{r+j}(x)|^2$$

e applicando i logaritmi si ha la tesi.
La disuguaglianza restante è la parte più ostica del teorema. La dimostrazione passa per alcuni lemmi; vogliamo trovare $r + s - 1$ vettori linearmente indipendenti. L'idea è trovare per ogni $k = 1, \ldots, r + s$ un vettore nell'immagine con componenti negative per ogni $i \neq k$ e componente k-esima positiva.

Lemma 4.21. Sia $k \in \mathbb{N}$ tale che $1 \leq k \leq r + s$. Per ogni $\alpha \in \mathcal{O}_K \setminus \{0\}$ esiste $\beta \in \mathcal{O}_K$ di norma limitata

$$|N(\beta)| \leq \Big(\frac{2}{\pi}\Big)^s \sqrt{|\operatorname{disc}(K)|}$$

tale che se $L(\alpha) = (\alpha_i)$ e $L(\beta) = (\beta_i)$, si ha $\beta_i < \alpha_i$ per ogni $i \neq k$.

Dimostrazione. Consideriamo l'insieme

$$B = \{(y, z) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \leq c_i \; |z_j| \leq c_{r+j}\}$$

dove gli elementi c_i sono scelti in modo che

$$0 < c_i < e^{a_i} \quad \forall i \neq k$$

Per quanto riguarda c_k, lo scegliamo in modo da regolare il volume di B e applicare il teorema di Minkowski:

$$\mu(B) = 2^r c_1 \ldots c_r \pi^s c_{r+1}^2 \ldots c_{r+s}^2 = 2^{n-s} \sqrt{|\operatorname{disc}(K)|}$$

da cui ricaviamo univocamente c_k. Dunque $\mu(B) = 2^n \operatorname{Vol}(\sigma\mathcal{O}_K)$ e B è compatto. Per il teorema di Minkowski, esiste un elemento $\beta \in \mathcal{O}_K \setminus \{0\}$ tale che $\sigma(\beta) \in B$. Per definizione di B,

$$|\sigma_i(\beta)| \leq c_i < e^{a_i} \Rightarrow \log|\sigma_i(\beta)| < a_i$$

per ogni $i \neq k$. Di conseguenza otteniamo la disuguaglianza richiesta sulla norma:

$$|N(\beta)| \leq c_1 \dots c_r c_{r+1}^2 \dots c_{r+s}^2 = \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

□

Tramite applicazione iterata del lemma riusciamo a ottenere i vettori cercati:

Lemma 4.22. Sia $k \in \mathbb{N}$ compreso tra $1 \leq k \leq r+s$. Allora esiste $u_k \in \mathcal{O}_K^*$ tale che, posto $L(u_k) = (x_1, \dots, x_{r+s})$, si ha $x_i < 0$ per ogni $i \neq k$.

Dimostrazione. Sia $\alpha_0 \in \mathcal{O}_K$; applicando il lemma, si calcolano induttivamente $\alpha_{j+1} \in \mathcal{O}_k \setminus \{0\}$ con norma

$$N((\alpha_j)) = |N(\alpha_j)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

Dato che gli ideali di norma limitata sono in numero finito, esistono $l > \lambda$ tali che $(\alpha_\lambda) = (\alpha_l)$. Per costruzione,

$$\log|\sigma_i(\alpha_l)| \leq \log|\sigma_i(\alpha_\lambda)| \quad \forall i \neq k$$

Allora esiste $u_k \in \mathcal{O}_K^*$ tale che $\alpha_l = u_k \alpha_\lambda$ e dunque

$$\log|\sigma_i(u_k)| < 0 \ \ \forall i \neq k$$

□

Dato che se $u_k \in \mathcal{O}_k^*$ $N(u_k) = \pm 1$, necessariamente la componente k-esima è maggiore di 0 e la somma delle componenti, dopo aver dimezzato la ultime s componenti, è 0. Abbiamo allora ottenuto gli elementi $u_1, \dots, u_{r+s}$ che cercavamo. $r+s-1$ di questi sono linearmente indipendenti per il seguente:

Lemma 4.23. Sia $A = (a_{ij})$ una matrice $n \times n$ a coefficienti complessi. Supponiamo che sia positiva sulla diagonale e negativa altrove e che la somma di ogni colonna o di ogni riga sia zero. Allora $\operatorname{rk}(A) = n-1$.

Dimostrazione. Chiaramente, a meno di trasporre, possiamo supporre che la somma di ogni riga sia 0. Allora $\operatorname{rk}(A) \leq n-1$, perché il vettore con ogni componente 1 sta nel nucleo di A. D'altronde, il minore principale di taglia $n-1$ è una matrice fortemente dominante diagonale e dunque è invertibile per il teorema di Gershgorin. □

e questo termina la dimostrazione. Vediamo ora alcuni esempi:

Campi quadratici immaginari Consideriamo i campi quadratici immaginari $K = \mathbb{Q}(\sqrt{-d})$. Si ha $r = 0$ e $s = 1$ e dunque $\mathcal{O}_K^*$ è ciclico finito, formato dalle radici dell'unità contenute nel campo. In particolare, dato che $\phi(n) \leq 2$ solo se $n = 2, 3, 4, 6$, si ha che gli uniche estensioni in cui $\mathcal{O}_K^* \neq \{\pm 1\}$ sono $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_6]$.

Campi quadratici reali Consideriamo $K = \mathbb{Q}(\sqrt{d})$, con $d > 0$. Chiaramente $r = 2$ e $s = 0$ e

$$\mathcal{O}_K^* \simeq \{\pm 1\} \oplus \mathbb{Z}$$

Proviamo a calcolare l'unità fondamentale. Sia α una unità; allora solo una tra $\pm\alpha$, $\pm\alpha^{-1}$ è maggiore di 1. Dunque in $\mathcal{O}_K^*$ esiste un'unica unità fondamentale maggiore di 1. Notiamo che $\mathcal{O}_K = \mathbb{Z}[w]$ con

$$\begin{cases} w = \sqrt{d} & d \equiv 2, 3 \pmod 4 \\ w = \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \end{cases}$$

Sia $\alpha = a + bw \in \mathcal{O}_K^*$. Dato che $N(\alpha) = \pm 1$ e la norma cresce al crescere di a, b, si ha che l'unità fondamentale di modulo maggiore di 1 è quella in cui $a > 0$, $b > 0$, eccetto per $d = 5$. In questo caso infatti l'unità fondamentale si trova facilmente ed è proprio w. Dunque, un algoritmo naive per trovare un'unità fondamentale è quello di considerare la successione $\{b^2 d\}_b$ e trovare il più piccolo $b \in \mathbb{B}$ tale che $b^2 d \pm 1$ è un quadrato.
Un metodo più rapido è basato sul seguente teorema, che enunciamo senza dimostrazione:

Teorema 4.24. Sia $\xi \in \mathbb{R}^+$. Siano $x, y \in \mathbb{N}$ coprimi tali che

$$\left| \xi - \frac{x}{y} \right| < \frac{1}{2y^2}$$

Allora $\frac{x}{y}$ è uno dei convergenti (somme parziali) della frazione continua di ξ.

Cerchiamo di utilizzare questo teorema. Sia $\epsilon = a + bw$ l'unità fondamentale di modulo ≥ 1. Allora

$$|\sigma(\epsilon)| = \frac{1}{\epsilon} = \frac{1}{a + bw}$$

Supponiamo $d \equiv 1 \pmod 4$ e $d \neq 5$ (questo caso l'abbiamo già risolto). Allora

$$\left| \frac{a}{b} + \sigma(w) \right| = \frac{1}{b^2(\frac{a}{b} + \frac{1+\sqrt{d}}{2})} < \frac{1}{2b^2}$$

Dunque è sufficiente cercare i coefficienti a, b di ϵ tra i convergenti della frazione continua di $-\sigma(w)$. Se invece $d \equiv 2, 3 \pmod 4$, notiamo che

$$a^2 - b^2 d = \pm 1 \Rightarrow a^2 = \pm 1 + b^2 d \geq b^2 d - 1 \geq b^2(d - 1)$$

e dunque come prima

$$\left| \frac{a}{b} + \sigma(w) \right| = \frac{1}{b(a + b\sqrt{d})} = \frac{1}{b^2(\frac{a}{b} + \sqrt{d})} < \frac{1}{b^2(\sqrt{d-1} + \sqrt{d})} < \frac{1}{2b^2}$$

Anche in questo caso, è sufficiente trovare i convergenti di $-\sigma(w)$. Il primo convergente con norma unitaria fornisce i coefficienti dell'unità fondamentale.

Esempio. Sia $K = \mathbb{Q}(\sqrt{41})$. Allora $w = \frac{1+\sqrt{41}}{2}$ e $-\sigma(w) = \frac{\sqrt{41}-1}{2}$. Indichiamo con k l'iterazione dell'algoritmo, con c_k il k-esimo approssimante, con p_k e d_k rispettivamente il numeratore e il denominatore del k-esimo convergente, mentre l'ultima riga è la norma della soluzione parziale data dall'algoritmo.

k	0	1	2	3	4
c_k	2	1	2	2	1
$p_k = c_k p_{k-1} + p_{k-2}$	2	3	8	19	27
$d_k = c_k q_{k-1} + q_{k-2}$	1	1	3	7	10
$N(p_k + wq_k)$	-4	2	-2	4	-1

da cui $\epsilon = 27 + 10w$.

4.3 Un'introduzione alla Class Field

Cominciamo questa sezione con un esempio:

Esempio. Consideriamo il campo di numeri $K = \mathbb{Q}(\sqrt{-21})$ e calcoliamo il gruppo delle classi. Dato che $-21 \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-21}]$ e il suo discriminante è

$$\operatorname{disc}(K) = -4 \cdot 21$$

L'estensione è immaginaria e dunque $r = 0$, $s = 1$.

Osservazione 4.25. Notiamo che 2 ha ramificazione wild, mentre $3, 7$ hanno ramificazione tame. Infatti, per motivi di grado dell'estensione $3, 7$ non possono dividere l'indice di ramificazione; invece $2\mathcal{O}_K = P^2$ dal teorema di Kummer e $e(Q|2) = 2$.

Calcoliamo la costante di Minkowski:

$$\frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\operatorname{disc}(K)|} = \frac{4}{\pi}\sqrt{21} < 6$$

Per calcolare il gruppo delle classi, possiamo allora cercare i generatori tra gli ideali primi che compaiono nella fattorizzazione dei primi di $\mathbb{Z}$ di norma ≤ 5.

$$2\mathcal{O}_K = P^2 \qquad 3\mathcal{O}_K = Q^2 \qquad 5\mathcal{O}_K = Q_1 Q_2$$

Notiamo che la fattorizzazione di $2, 3$ è immediata perché sono ramificati (dividono il discriminante); per quanto riguarda $p = 5$, è sufficiente utilizzare il teorema di Kummer sul polinomio $T(x) = x^2 + 21 \equiv x^2 - 4 = (x + 2)(x - 2)$. Studiamo ora l'ordine dei primi che compaiono nelle fattorizzazioni.

- P non può essere principale per motivi di norma:

  $$N(a + \sqrt{-21}b) = a^2 + 21b^2 \neq 2 \quad \forall a, b \in \mathbb{Z}$$

  Inoltre $P^2 = (2)$ e dunque $\operatorname{ord}(P) = 2$.

- Anche Q non può essere principale per motivi di norma. Inoltre $N(PQ) = 6$ e tale ideale non è principale, da cui $[P] \neq [Q]$.

- Per Q_1 e Q_2, vale sicuramente la relazione $[Q_1] = [Q_2]^{-1}$ e non possono essere principali in quanto non esiste un elemento con norma 5. Notiamo che $N(Q_1^2) = 25$ e dunque $Q_1^2 = (2 + \sqrt{-21})$ da cui $\operatorname{ord}(Q_1) = 2$.

Allora abbiamo ridotto i generatori a

$$\operatorname{Cl}(K) = \langle [P], [Q], [Q_1] \rangle$$

Notiamo che $N(PQQ_1) = 30$ ed è un ideale principale, da cui $\operatorname{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposizione 4.26. Sia K un campo di numeri e sia $I \subseteq \mathcal{O}_K$ un ideale.

- Esiste un'estensione L di K tale che $I\mathcal{O}_L$ sia principale.
- Esiste un'estensione L di K tale che per ogni $J \subseteq \mathcal{O}_K$ $J\mathcal{O}_L$ sia principale.

Dimostrazione.

- Dato che il gruppo delle classi è finito, esiste $m \in \mathbb{N}$ tale che $I^m = (\alpha)$. Consideriamo allora il campo $L = K(\sqrt[m]{\alpha})$ e mostriamo che

$$I\mathcal{O}_L = (\sqrt[m]{\alpha})$$

  Notiamo che

$$(I\mathcal{O}_L)^m = I^m\mathcal{O}_L = (\alpha)\mathcal{O}_L \qquad (\sqrt[m]{\alpha})^m\mathcal{O}_L = (\alpha)$$

  Per il teorema di fattorizzazione unica, $I\mathcal{O}_L = (\sqrt[m]{\alpha})$.

- Sia $\mathrm{Cl}(K) = \{[I_1], \dots, [I_d]\}$. Dato che il gruppo delle classi è finito, per ogni i esiste $m_i \in \mathbb{N}$ tale che $I^{m_i} = (\alpha_i)$. Detto $L = K(\sqrt[m_1]{\alpha_1}, \dots, \sqrt[m_d]{\alpha_d})$, mostriamo che per ogni $J \in \mathcal{O}_K$ $J\mathcal{O}_L$ è principale. Per il punto precedente, $I_j\mathcal{O}_L$ è principale; per ogni altro ideale J, $J = (\beta)I_i$ da cui

$$J\mathcal{O}_L = (\beta)I_i\mathcal{O}_L = (\beta\sqrt[m_i]{I_i})$$

□

Riprendiamo ora l'esempio:

Esempio. Sia $K = \mathbb{Q}(\sqrt{-21})$. Abbiamo visto che $\mathrm{Cl}(K) = \langle[P]\rangle \times \langle[Q]\rangle$. Per quanto visto nella proposizione,

$$L = K(\sqrt{2}, \sqrt{3})$$

è un'estensione di K nella quale tutti i primi di $\mathcal{O}_K$ si estendono a ideali principali.

Notiamo che nell'esempio

$$\mathrm{Gal}\left(L/K\right) \simeq \mathrm{Cl}(K)$$

Questo è legato al teorema della Class Field:

Definizione 4.27. Sia K un campo di numeri e sia L una sua estensione e siano $\sigma_i \colon K \to \mathbb{R}$ le immersioni reali di K. Diciamo che i primi infiniti di K non ramificano se per ogni $\tau \colon L \to \mathbb{C}$ tale che $\tau|_K = \sigma_i$, allora $\tau(L) \subseteq \mathbb{R}$.
Chiamiamo Hilbert Class Field la massima estensione abeliana H non ramificata di K per la quale non ramificano neanche i primi infiniti.

Teorema 4.28 (della Class Field globale)**.** Sia K un campo di numeri e sia H il suo Hilbert Class Field. Allora $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}(K)$.

Idea di dimostrazione. Consideriamo la mappa di Artin

$$\mathcal{I}(K) \quad \longrightarrow \quad \mathrm{Gal}\left(H/K\right)$$

che estende moltiplicativamente la mappa di Frobenius, cioè

$$\prod P_i^{e_i} \longmapsto \prod \phi(P_i)^{e_i}$$

La dimostrazione consiste nel mostrare che tale mappa passa al quoziente sui primi principali e che diventa un isomorfismo sul quoziente. □

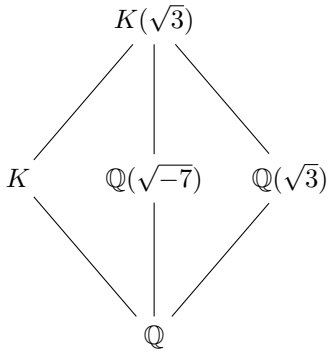
Teorema 4.29 (dell'ideale principale)**.** In H, ogni ideale di K diventa principale.

Sorge ora spontaneo chiedersi se il campo trovato nell'esempio fosse proprio l'Hilbert Class Field:

Esempio. Sia $K = \mathbb{Q}(\sqrt{-21})$ e sia $L = K(\sqrt{2}, \sqrt{3})$. Abbiamo visto che

$$\mathrm{Gal}\left(L/K\right) \simeq \mathrm{Cl}(K)$$

e in L tutti gli ideali di K son principali. Questa non può essere l'Hilbert Class Field H perché 2 ramifica in L. 2 è ramificato in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ per il discriminante. Costruiamo allora H; dato che K ha solo immersioni immaginarie, non dobbiamo preoccuparci della condizione sulla ramificazione infinita. Sia $L = K(\sqrt{3})$; notiamo che



$$K(\sqrt{3})/K$$

è non ramificata. Ricordiamo che se un primo è totalmente ramificato nel composto allora lo è anche in tutti i sottocampi. Notiamo però che

$$\mathrm{disc}(K) = -4 \cdot 21 \quad \mathrm{disc}(\mathbb{Q}(\sqrt{3})) = 4 \cdot 3$$
$$\mathrm{disc}(\mathbb{Q}(\sqrt{-7})) = -7$$

Dunque 2 non può essere totalmente ramificato in L perché non è ramificato in $\mathbb{Q}(\sqrt{7})$. Lo stesso vale per i primi 7 e 3 e dunque nessun primo che è totalmente ramificato in K è totalmente ramificato in L. Una dimostrazione alternativa di questo si basa sul discriminante. Notiamo che

$$K(\sqrt{3}) = \underbrace{\mathbb{Q}(\sqrt{3})}_{K_1}\underbrace{\mathbb{Q}(\sqrt{-7})}_{K_2}$$

e $\mathrm{disc}(K_1) = 12$, $\mathrm{disc}(K_2) = -7$. Dato che sono coprimi, possiamo applicare la formula sui discriminanti nelle torri da cui si ottiene $\mathrm{disc}(K(\sqrt{3})/K) = 1$. Con analoghe argomentazioni, possiamo mostrare che $K(i)$ è non ramificata su K. Allora $H \supseteq K(i, \sqrt{3})$; d'altronde hanno lo stesso grado per il teorema della Class Field e dunque si ha l'uguaglianza.

4.4 Campi Ciclotomici

Consideriamo un campo ciclotomico $K = \mathbb{Q}(\zeta_n)$. Tali estensioni sono sempre immaginarie, cioè ogni immersione $\tau\colon K \to \mathbb{C}$ ha immagine non contenuta in $\mathbb{R}$. Possiamo individuare allora un sottocampo $K^+ = K \cap \mathbb{R}$. Vogliamo relazionare gli invertibili dell'anello degli interi di K e K^+.

Osservazione 4.30. Se $n = p^m$, allora

$$p\mathcal{O}_K = P^{\phi(p^m)}$$

e $P = (1-\zeta)$; infatti applicando il teorema di Kummer si ottiene $P = (p, 1-\zeta)$ e $N(1-\zeta) = p$ e dunque $p \in (1-\zeta)$.
Se invece $n = \prod p_j^{m_j}$ non è potenza di un primo, allora $1-\zeta$ è un'unità. Infatti,

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = \prod_{i=1}^{n-1}(x - \zeta^i)$$

e valutando in 1,

$$n = \prod_{i=1}^{n-1}(1 - \zeta^i) \tag{4.2}$$

Possiamo scrivere tale relazione per ogni p_j

$$p_j^{m_j} = \prod_{i=1}^{p_j^{m_j}-1} (1 - \zeta_{p^m}^i)$$

Notiamo che $\zeta_{p^m}^i = \zeta_n^{\frac{n}{p^m} i}$, da cui, sostituendo nela relazione 4.2,

$$1 = \prod_{(i,n)=1} (1 - \zeta_n^i) = N(1-\zeta)$$

Per il teorema di Dirichlet, gli invertibili dell'anello degli interi di $K = \mathbb{Q}(\zeta_n)$ sono

$$E = \mathcal{O}_K^* = \underbrace{\langle \pm\zeta_n \rangle}_{=W} \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1}$$

Per quanto riguarda la parte reale dell'estensione, otteniamo invece

$$E^+ = \mathcal{O}_{K^+}^* = \langle \pm 1 \rangle \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1}$$

Lemma 4.31. Sia α un intero algebrico tale che α e ogni suo coniugato abbia valore assoluto 1. Allora α è una radice dell'unità.

Il lemma non è ovvio, per esempio

Esempio.

$$\alpha = \frac{3}{5} + i\frac{4}{5} \notin \mathbb{Z}[i]$$

e ogni suo coniugato ha valore assoluto 1. D'altronde, non è una radice dell'unità.

Dimostrazione. Consideriamo l'insieme $S = \{\alpha^h\}_{h\geq 1}$, formato dalle potenze di α. Ogni elemento di S ha la stessa proprietà di α: sono interi algebrici e ogni coniugato ha valore assoluto 1. Inoltre, in K ci sono solo un numero finito di elementi con tale proprietà. Infatti, un tale elemento ha grado su $\mathbb{Q}$ limitato perché appartiene a K e i coefficienti del polinomio minimo devono essere interi e limitati, perché sono combinazione dei coniugati. Di conseguenza, esistono h, k tale che

$$\alpha^h = \alpha^k \Longrightarrow \alpha^{h-k} = 1$$

da cui la tesi. □

Teorema 4.32. Sia $K = \mathbb{Q}(\zeta_n)$ e siano E, E^+ i gruppi delle unità rispettivamente di $\mathcal{O}_K, \mathcal{O}_{K^+}$ come sopra.

$$E = \mathcal{O}_K^* = \underbrace{\langle \pm\zeta_n \rangle}_{=W} \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1} \qquad E^+ = \mathcal{O}_{K^+}^* = \langle \pm 1 \rangle \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1}$$

Allora vale

$$[E : E^+W] = Q = \begin{cases} 1 & \text{se } n = p^\alpha \\ 2 & \text{altrimenti} \end{cases}$$

Dimostrazione. Consideriamo la mappa

$$\begin{array}{rccc} \phi\colon & E & \longrightarrow & W \\ & e & \longmapsto & \frac{e}{\bar{e}} \end{array}$$

ϕ è ben definita, perché $\frac{e}{\bar{e}}$ è una radice dell'unità per il lemma precedente. Infatti

$$\left|\frac{e}{\bar{e}}\right| = 1 \qquad \sigma\left(\frac{e}{\bar{e}}\right) = \frac{\sigma(e)}{\sigma(\bar{e})} = \frac{\sigma(e)}{\overline{\sigma(e)}} = 1$$

Notiamo che il coniugio (complesso) commuta con σ perché il gruppo di Galois $\mathrm{Gal}(K/\mathbb{Q})$ è abeliano. Consideriamo allora il quoziente $\pi\colon W \to W/W^2$ e la composizione $\psi = \pi \circ \phi$. Notiamo che W/W^2 ha ordine 2 perché quoziente di un gruppo ciclico per il suo sottogruppo dei quadrati.
Mostriamo ora che $\mathrm{Ker}(\psi) = E^+W$. Infatti, se $\zeta \in W$ e $e \in E^+$, allora

$$\phi(\zeta e) = \frac{\zeta e}{\overline{\zeta e}} = \frac{\zeta e}{\bar{\zeta} e} = \frac{\zeta^2}{\zeta\bar{\zeta}} = \zeta^2$$

perché le radici dell'unità hanno modulo uno, da cui il contenimento $\mathrm{Ker}(\psi) \supseteq E^+W$.
Viceversa, se $e \in \mathrm{Ker}(\psi)$, allora $\phi(e) = \zeta^2 \in W^2$ e dunque coniugando otteniamo un elemento reale. Dividiamo in due casi:

- Se $n = p^\alpha$ con $p \neq 2$, allora
$$\frac{e}{\bar{e}} = \pm\zeta^a$$
Se per assurdo $e = -\zeta^a\bar{e}$, allora
$$e = \sum a_i\zeta^i \equiv \sum a_i \pmod{1-\zeta}$$

e analogamente

$$\bar{e} = \sum a - i\bar{\zeta}^i \equiv \sum a_i \pmod{1-\zeta}$$

Da questo seguirebbe che $e = -\bar{e} \pmod{1-\zeta}$ da cui $2\zeta \equiv 0 \pmod{1-\zeta}$ e dunque un assurdo.

- Se $p = 2$ e $n = 2^m$, supponiamo per assurdo che esista $e \in E$ tale che $e/\bar{e} \notin W^2$. Allora $e/\bar{e} = \zeta$, dove ζ è una radice 2^m-esima primitiva di 2. Notiamo che

$$N_{K/\mathbb{Q}(i)}(\zeta) = \zeta^a \qquad a = \sum_{\substack{0<b<2^m \\ b\equiv 1 \pmod 4}} b \equiv 2^{m-2} \pmod{2^{m-1}}$$

Allora $N(\zeta) = \pm i$. D'altronde,

$$\pm i = N(\zeta) = \frac{N(e)}{\overline{N(e)}}$$

e questo è assurdo perché $N_{K/\mathbb{Q}(i)}(e) = \pm 1, \pm i$.

- Se n non è potenza di un primo, $1-\zeta_n$ è una unità e

$$\frac{1-\zeta_n}{1-\bar{\zeta}_n} = \frac{\zeta_n}{\zeta_n}\frac{1-\zeta_n}{1-\bar{\zeta}_n} = \frac{\zeta_n(1-\zeta_n)}{(\zeta_n - \zeta_n\bar{\zeta}_n)} = \frac{\zeta_n(1-\zeta_n)}{(\zeta_n - 1)} = -\zeta_n$$

Notiamo che $-\zeta_n \notin W^2$; se infatti stesse in W^2, allora $-\zeta_n = (\pm\zeta_n^r)^2 = \zeta_n^{2r}$. Di conseguenza,

$$\zeta^{2r-1} = -1$$

Se $2\|n$, si ripete il ragionamento con $n/2$ dato che $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$; se invece $4 \mid n$, allora

$$\frac{n}{2} \equiv 2r - 1 \pmod{n}$$

da cui $n/2 = -1 \pmod 2$ mentre $n \equiv 0 \pmod 4$ da cui un assurdo.

□

Teorema 4.33. Sia $K = \mathbb{Q}(\zeta_n)$ e consideriamo i gruppi delle classi $C = \mathrm{Cl}(K)$ e $C^+ = \mathrm{Cl}(K^+)$. Allora $C^+ \hookrightarrow C$.

Dimostrazione. L'inclusione $K^+ \to K$ induce l'applicazione di estensione di ideali sul gruppo degli ideali frazionari

$$\begin{array}{ccc} \mathcal{F}(K^+) & \longrightarrow & \mathcal{F}(K) \\ I & \longmapsto & I\mathcal{O}_K \end{array}$$

Tale applicazione passa al quoziente sul gruppo delle classi. Infatti, se $I \subseteq \mathcal{O}_{K^+}$ e $I\mathcal{O}_K = (\alpha)$, allora

$$I = \bar{I} \Longrightarrow (1) = {}^{I\mathcal{O}_K}\!/_{\bar{I}\mathcal{O}_K} = \left(\frac{\alpha}{\bar{\alpha}}\right)$$

da cui $\alpha/\bar{\alpha}$ è un'unità di valore assoluto 1; dato che questo vale per tutte le estensioni ($\mathrm{Gal}(K/\mathbb{Q})$ è abeliano), otteniamo che $\alpha/\bar{\alpha}$ è una radice dell'unità.

Se n non è una potenza di p, allora, con la notazione del teorema precedente, $\phi(E) = W$ e dunque esiste $e \in E$ tale che $e/\bar{e} = \bar{\alpha}/\alpha$. Allora

$$e\alpha = \overline{e\alpha} \in E^+$$

e dunque $I\mathcal{O}_K = (\alpha) = (e\alpha)$ e quest'ultimo è reale. Dunque $I = (e\alpha)$ per unicità della fattorizzazione. Se $n = p^a$, chiamiamo $\pi = \zeta_{p^a} - 1$. Allora

$$\frac{\pi}{\bar{\pi}} = -\zeta_{p^a}$$

e $W = \langle -\zeta_{p^a} \rangle$. Allora

$$\frac{\bar{\alpha}}{\alpha} \in W \Rightarrow \frac{\bar{\alpha}}{\alpha} = \frac{\pi^d}{\bar{\pi}^d}$$

Mostriamo che d è pari; in tal caso, $\bar{\alpha}/\alpha \in W^2$ e concludo come prima che $\bar{\alpha}/\alpha = e/\bar{e}$ da cui $\alpha e \in \mathcal{O}_{K^+}$. Notiamo che

$$v_\pi(\alpha) = v_\pi(I)$$

e dunque è pari perché se $I = P^x J$ (I è l'unico ideale di $\mathcal{O}_{K^+}$ che sta sopra p), allora $I\mathcal{O}_K = Q^{2x}(J\mathcal{O}_K)$. Di conseguenza,

$$v_\pi(\pi^d \alpha) \equiv 0 \pmod 2$$

e

$$d = v_\pi(\pi^d) = v_\pi(\alpha\pi^d) - v_\pi(\alpha)$$

da cui d pari. □

Definizione 4.34. Un campo K si dice CM se K è totalmente immaginario e K è un'estensione quadratica di un campo K^+ con K^+ totalmente reale.

Per esempio, $\mathbb{Q}(\zeta_n)$ è CM. In generale, per costruire campi CM, è sufficiente costruire un'estensione totalmente reale K^+; dato allora α tale che $\sigma(\alpha) < 0$, un campo CM è $K^+(\sqrt{\alpha})$. Se K è non reale e $K/\mathbb{Q}$ è abeliana, allora K è sicuramente CM e K^+ è il fissato dal coniugio. Un esempio di campo non CM è

$$K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$$

K è totalmente immaginario, $K/\mathbb{Q}$ è di Galois ma non abeliano, ma K^+ non è totalmente reale.
Nei campi CM, il coniugio commuta con le immersioni e dunque il primo teorema che abbiamo visto vale. Invece, non è vero che C^+ si immerga in C, ma vale il seguente:

Teorema 4.35. Sia K un campo CM, sia $h = |\operatorname{Cl}(K)|$ e sia $h^+ = |\operatorname{Cl}(K^+)|$. Allora $h^+ \mid h$.

In generale però non si ha un'immersione:

Esempio. Sia $K = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$. Allora $K^+ = \mathbb{Q}(\sqrt{10})$. L'ideale $I = (2, \sqrt{10}) \subseteq \mathcal{O}_{K^+}$ è tale che $2\mathcal{O}_K = I^2$ e non è principale perché in $\mathcal{O}_{K^+}$ non ci sono elementi di norma 2. D'altronde,

$$I\mathcal{O}_K = (\sqrt{-2})$$

e dunque non si può avere l'immersione.

4.5 Anelli di Gruppo

Definizione 4.36. Sia A un anello commutativo con identità e G un gruppo finito. Definiamo l'anello di gruppo come l'anello (non commutativo)

$$A[G] = \{\sum a_g g \mid g \in G \ a_g \in A\}$$

con le operazioni

$$\Big(\sum_{g\in G} a_g g\Big) + \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G}(a_g + b_g)g \quad \Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{g\in G} b_g g\Big) = \sum_{g,h\in G}(a_g b_g)(gh)$$

Esempio.

- Sia K un campo e sia L/K un'estensione finita di Galois. Detto $G = \mathrm{Gal}(L/K)$, consideriamo l'anello di gruppo $K[G]$. Allora L è un $K[G]$-modulo
$$\Big(\sum_{g\in G} \lambda_g g\Big)(\alpha) = \sum \lambda_g g(\alpha)$$
- Sia L/K un'estensione di campi di numeri di Galois. Allora $\mathcal{O}_L$ è un $\mathcal{O}_K[G]$-modulo.

Vogliamo quindi approfondire questi esempi e studiare le strutture di modulo. Di centrale importanza è il seguente teorema di teoria di Galois:

Teorema 4.37 (della base normale)**.** Sia L/K un'estensione finita di Galois di gruppo di Galois G, allora esiste $\alpha \in L$ tale che $\{\sigma(\alpha)\}_{\sigma\in G}$ è una base di L/K.

Dal teorema segue direttamente la seguente definizione:

Definizione 4.38. Sia L/K un'estensione di Galois. Una base di L/K data dai coniugati di un elemento si dice base normale.

Corollario 4.39. Sia L/K un'estensione di Galois e sia $G = \mathrm{Gal}(L/K)$. Allora L è un $K[G]$-modulo libero di rango 1.

Dimostrazione. Basta notare che, preso α come nel teorema,

$$K[G]\alpha = \Big\{\sum \lambda_\sigma \sigma(\alpha) \mid \lambda_\sigma \in K\Big\} = \langle\{\sigma(\alpha)\}_{\sigma\in G}\rangle_K$$

□

Abbiamo così un risultato concreto per quanto riguarda l'anello di gruppo di un'estensione L/K. Ci poniamo ora il problema della struttura di $\mathcal{O}_L$ come $\mathcal{O}_K[G]$-modulo. In generale, $\mathcal{O}_L$ non è libero perché $\mathcal{O}_L$ non è libero su $\mathcal{O}_K$. Se $\mathcal{O}_L = \mathcal{O}_K[H]\alpha$, allora $\{\sigma(\alpha)\}$ sarebbe una base intera. Concentriamoci ora sul caso $K/\mathbb{Q}$. Anche in questo caso in generale è falso:

Esempio. Sia $K = \mathbb{Q}(i)$ e $\mathcal{O}_K = \mathbb{Z}[i]$. Sia $\alpha = a + ib \in \mathbb{Z}[i]$; allora

$$\mathbb{Z}[G]\alpha = \{c\alpha + d\bar{\alpha}\} = \{c(a+ib) + d(a-ib)\} = \{a(c+d) + ib(c-d)\}$$

e un elemento tra $1, -1$ non appartiene a questo insieme.

Definizione 4.40. Diciamo che $\mathcal{O}_L$ ha una base normale intera (NIB) su K se esiste $\alpha \in L$ tale che $\mathcal{O}_L = \mathcal{O}_K[G]\alpha$. In tal caso, α si chiama generatore di una base intera.

Definizione 4.41. L/K estensione di campi di numeri. Sia $P \subseteq \mathcal{O}_K$ e consideriamo la sua fattorizzazione $P\mathcal{O}_L = \prod Q_i^{e_i}$. Q è tame su P se $p = P \cap \mathbb{Z} \nmid e(Q|P)$. P è tame su L se $p \nmid e(Q|P)$ per ogni Q sopra P. L'estensione si dice tame se per ogni $P \subseteq \mathcal{O}_K$ P è tame in L.

I primi non ramificati sono tame in automatico.

Teorema 4.42. Sia L/K un'estensione di Galois di gruppo G. Sono equivalenti:

1. L/K ha solo ramificazione tame
2. $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$
3. $\mathcal{O}_L$ è $\mathcal{O}_K[G]$-proiettivo

Dimostrazione. Mostriamo solo l'equivalenza delle prime due condizioni. Ricordiamo che $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = mcm\{I \subseteq \mathcal{O}_K \mid I\mathcal{O}_L | \mathcal{D}_{L/K}\}$ e che $\sigma(\mathcal{D}_{L/K}) = \mathcal{D}_{L/K}$ per ogni $\sigma \in \mathrm{Gal}(L/K)$.

(1) $\Rightarrow$ (2) Basta mostrare che per ogni primo $P \subseteq \mathcal{O}_K$ vale $\mathrm{Tr}_{L/K}(\mathcal{O}_K) \not\subseteq P$. Se $\mathrm{Tr}_{L/K}(\mathcal{O}_K) \subseteq P$, allora $P\mathcal{O}_L \mid \mathcal{D}_{L/K}$.

$$P\mathcal{O}_L = (Q_1 \dots Q_r)^e \mid \mathcal{D}_{L/K} \Rightarrow Q_i^e \mid \mathcal{D}_{L/K}$$

e questo è assurdo perché L/K ha solo ramificazione tame.

(2) $\Rightarrow$ (1) Supponiamo che esista $P \subseteq \mathcal{O}_K$ tale che $P\mathcal{O}_L = (Q_1 \dots Q_r)^e$ e esista i tale che $Q_i^e \mid \mathcal{D}_{L/K}$. Per transitività dell'azione del gruppo di Galois e per invarianza del differente per l'azione, questo vale allora per ogni i e dunque $P\mathcal{O}_L \mid \mathcal{D}_{L/K}$. Di conseguenza, $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq P$, da cui un assurdo.

□

Proposizione 4.43. Se L/K ha una base normale intera, allora L/K è tame.

Dimostrazione. Basta mostrare che la traccia è surgettiva. Sia $x \in \mathcal{O}_K$ e sia $G = \mathrm{Gal}(L/K)$; sappiamo che $\mathcal{O}_L = \mathcal{O}_K[G]\alpha$ e dunque

$$x = \sum a_g g(\alpha)$$

Notiamo che $x \in O_K$ se e solo se per ogni $\tau \in G$, $\tau(x) = x$, cioé

$$\sum a_g g(\alpha) = \sum a_{\tau^{-1}g} g(\alpha)$$

Dato che i $g(\alpha)$ sono una base, $a_g = a_{\tau^{-1}g}$ e dunque $a_g = a$ per ogni $g \in G$. Allora

$$x \in \mathcal{O}_K \iff x = a\,\mathrm{Tr}(\alpha)$$

e dunque l'estensione è tame. □

Sono stati dati esempi di $K[Q_8]$-moduli proiettivi (quaternioni) di rango 1 non liberi. Focalizziamoci ora sulle estensioni ciclotomiche tame hanno sempre una base normale intera.

Proposizione 4.44. Sia $L/\mathbb{Q}$ un'estensione di Galois con una base normale intera con generatore α. Allora per ogni $K/\mathbb{Q}$ estensione intermedia di Galois, $K/\mathbb{Q}$ ha una base normale intera generata da $\beta = \mathrm{Tr}_{L/K}(\alpha)$.

Dimostrazione. Sia $G = \mathrm{Gal}(L/\mathbb{Q})$ e sia $H \trianglelefteq G$ il sottogruppo tale che $L^H = K$. Dato $x \in \mathcal{O}_L$,

$$x = \sum a_g g(\alpha)$$

Si ha che $x \in \mathcal{O}_K$ se e solo se $hx = x$ per ogni $h \in H$ e dunque

$$\sum a_g g(\alpha) = \sum a_{h^{-1}g} g(\alpha)$$

da cui $a_{h^{-1}g} = a_g$ per ogni $h \in H$. Di conseguenza i coefficienti a_g sono costanti sulle classi laterali sinistre di H:

$$\begin{aligned} x = \sum_g a_g g(\alpha) &= \sum_{i=1}^{d} \sum_{h \in H} a_{hg_i} h g_i(\alpha) \\ &= \sum_{i=1}^{d} a_{g_i} \sum_{h \in H} h g_i(\alpha) \\ &= \sum_{i=1}^{d} a_{g_i} \sum_{h \in H} g_i g_i^{-1} h g_i(\alpha) \\ &= \sum_{i=1}^{d} a_{g_i} \sum_{h \in H} g_i h(\alpha) \\ &= \sum_{i=1}^{d} a_{g_i} g_i(\mathrm{Tr}(\alpha)) \\ &= \sum_{\sigma \in G/H} a_\sigma \sigma(\beta) \end{aligned}$$

da cui la tesi. □

Proposizione 4.45. Siano $K_i/\mathbb{Q}$ estensioni di campi di Galois con una base normale intera generata da α_i e supponiamo che i discriminanti $(d(K_i), d(K_j)) = 1$ siano a due a due coprimi. Allora il composto $L = K_1 \dots K_m$ ha una base normale intera generata da $\alpha_1 \dots \alpha_n$.

Dimostrazione. Per quanto già visto,

$$\{\sigma^{(1)}(\alpha_1) \dots \sigma^{(m)}(\alpha_m)\}$$

è una base intera del composto. D'altronde,

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \prod_{i=1}^{m} \mathrm{Gal}(K_i/\mathbb{Q})$$

da cui la tesi. □

Corollario 4.46. Sono equivalenti:

1. $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ha una base normale intera
2. m è libero da quadrati
3. $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ è tame

Dimostrazione. Supponiamo che m sia squarefree, $m = p_1 \dots p_r$. Notiamo che

$$\mathbb{Q}(\zeta_p)/\mathbb{Q}$$

ha una base normale intera, data da $\{\zeta, \dots, \zeta^p\}$ e generata da ζ_p. Inoltre $\mathrm{disc}(\mathbb{Q}(\zeta_p)) = p^\alpha$. Di conseguenza, i discriminanti sono a due a due coprimi e dunque possiamo applicare la proposizione precendente. Viceversa, supponiamo che esista $p \in \mathbb{Z}$ tale che $p^2 \mid m$. Allora

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{p^2}) \subseteq \mathbb{Q}(\zeta_m)$$

Per la proposizione. basta allora mostrare che $\mathbb{Q}(\zeta_{p^2})$ non ha una base intera e questo è vero perché tale estensione non è tame. Infatti, il primo p ha ramificazione wild in $\mathbb{Q}(\zeta_{p^2})$:

$$p\mathbb{Z}[\zeta_{p^2}] = P^{\phi(p^2)}$$

e $p \mid \phi(p^2)$. □

Per le estensioni abeliane, si può utilizzare il teorema di Kronecker-Weber:

Teorema 4.47. Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in una estensione ciclotomica.

e vale il seguente:

Teorema 4.48 (Hilbert-Spaiser)**.** Se $K/\mathbb{Q}$ abeliana è tame allora $K \subseteq \mathbb{Q}(\zeta_m)$ con m squarefree.

grazie al quale si riesce a dire che $\mathcal{O}_K$ ha una base normale intera anche in questi casi. Il teorema di Hilbert-Spaiser non può però essere ampliato: $\mathbb{Q}$ è l'unico campo con tale proprietà.