Appunti di Teoria Algebrica dei Numeri 1

Giacomo Mezzedimi

20 settembre 2015

Indice

Introduzione

Questi appunti nascono durante il secondo semestre dell'anno accademico 2014/2015, periodo nel quale io ho seguito il corso della professoressa Del Corso; seguono abbastanza fedelmente le lezioni tenute dalla professoressa, e il testo di riferimento é il libro "Number Fields" di Marcus (in particolare i primi 5 capitoli).
Gli esercizi presenti sono stati quasi tutti svolti in classe, e tutti sono presi dal libro di Marcus; altri testi utilizzati (molto piú marginalmente) sono stati "Algebraic Theory of Numbers" di Samuel, "Elementary and Analytic Theory of Algebraic Numbers" di Narkiewicz e "Introduction to Cyclotomic Fields" di Washington.
I paragrafi 6.4 e 6.5 sono gli unici non svolti in classe e contengono la risoluzione di alcuni esercizi del Marcus che portano a una dimostrazione del teorema di Kronecker e Weber.
Avendo io stesso studiato su questi appunti, **dovrebbero** essere abbastanza sgombri da errori, ma chiedo a chiunque usi questi appunti di segnalarmi qualsiasi tipo di errore presente, ad esempio per mail (*mezzedimi@mail.dm.unipi.it*).
Questi appunti si trovano sulla mia pagina web *http://poisson.phc.unipi.it/~mezzedimi/*.

Giacomo Mezzedimi

1 Richiami di teoria e prime definizioni

1.1 Richiami di teoria di Galois

Nel seguito siano $K \subset F$ campi.

Definizione 1.1.1. $\alpha \in F$ si dice **algebrico** su K se $\exists f(x) \in K[x]$, $f(x) \neq 0$ tale che $f(\alpha) = 0$.
$f(x)$ si dice **relazione di dipendenza algebrica** di α.
F si dice **algebrico** su K se tutti gli $\alpha \in F$ sono algebrici su K.

Definizione 1.1.2. F/K si dice **finita** se $[F : K] < +\infty$.

Osservazione. Estensione finita $\Rightarrow$ algebrica. Il viceversa é falso in generale (ad esempio con $\overline{\mathbb{Q}}$).
Peró estensione algebrica e finitamente generata $\Rightarrow$ finita.

Definizione 1.1.3. $\alpha \in F$ si dice **separabile** su K se $\mu_\alpha(x)$ é separabile, cioé ha tutte radici semplici in un campo spezzamento (ad esempio $\overline{K}$).

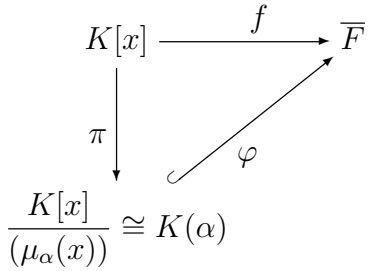
Esempi.
1. $\text{char}(K) = 0 \Rightarrow$ tutte le estensioni sono separabili.
2. $K = \mathbb{F}_{p^n} \Rightarrow$ ogni estensione finita di K é separabile.

   Dimostrazione. $\left(\mu_\alpha(x), (\mu_\alpha(x))'\right) \in K[x]$, ma $\mu_\alpha(x)$ é irriducibile, dunque se $\left(\mu_\alpha(x), (\mu_\alpha(x))'\right) \neq 1$, allora $\left(\mu_\alpha(x), (\mu_\alpha(x))'\right) = \mu_\alpha(x)$.
   Ma $\deg\left((\mu_\alpha(x))'\right) < \deg\left(\mu_\alpha(x)\right)$, dunque $(\mu_\alpha(x))' = 0$.
   Ma poiché i polinomi di $\mathbb{F}_{p^n}$ che hanno derivata 0 sono tutti potenze p-esime, allora $\mu_\alpha(x)$ non é irriducibile, assurdo. □

Osservazione. $K = \mathbb{F}_p(t)$, $x^p - t \in K[x]$ é irriducibile (per il lemma di Gauss), e se $\alpha \in \overline{K}$ tale che $\alpha^p = t \Rightarrow x^p - t = x^p - \alpha^p = (x - \alpha)^p$, dunque α non é separabile.

Da ora in poi considereremo solo estensioni finite e separabili, per cui vale il teorema dell'elemento primitivo.

Osservazione. Se $F = K(\alpha)$, data $\sigma : K \to \overline{F}$, quanti sono gli omomorfismi $\varphi : F \to \overline{F}$ che estendono σ, cioé $\varphi_{|K} = \sigma$?
Sicuramente questi omomorfismi sono immersioni, poiché il dominio é un campo e $\text{Ker}(\varphi)$ é un ideale.
Lo scopo non é altro che contare gli omomorfismi $f : K[x] \to \overline{F}$ tali che $\text{Ker}(f) = (\mu_\alpha(x))$, poiché:



Se $f : K[x] \to \overline{F}$ é tale che $f(k) = \sigma(k)$ e $f(x) = \beta$, allora:

$$f : p(x) = \sum_i a_i x^i \longrightarrow \sum_i \sigma(a_i)\beta^i = (\sigma p)(\beta),$$

dunque $\forall \beta \in \overline{F}$, f é un ben definito omomorfismo di anelli.
Per passare al quoziente, si deve avere che $f(\mu_\alpha(x)) = 0$, cioé $(\sigma\mu_\alpha)(\beta) = 0$.

Se $\sigma = id \Rightarrow f(\mu_\alpha(x)) = \mu_\alpha(\beta) = 0$, cioé x deve essere mappato in una radice del polinomio minimo di α.
Ma allora il numero di immersioni $F \hookrightarrow \overline{F}$ coincide con il numero di radici distinte di $\mu_\alpha(x)$, che a sua volta coincide con $[K(\alpha) : K]$ in quanto separabile.
Se $\sigma \neq id$, la situazione sostanzialmente non cambia, poiché $\sigma(\mu_\alpha(x))$ rimane un polinomio irriducibile con deg $(\mu_\alpha(x))$ radici distinte.

Osservazione. Se $F \overset{m}{\supset} L \overset{n}{\supset} K$, abbiamo appena visto che esistono n estensioni dell'inclusione $K \hookrightarrow \overline{F}$ a L.
Analogamente esistono mn estensioni dell'inclusione $K \hookrightarrow \overline{F}$ a F.
In particolare, se $\sigma_1, \ldots, \sigma_n$ sono le estensioni di L/K, $\forall i\ \exists \tau_{i_1}, \ldots, \tau_{i_m}$ estensioni di σ_i a F (che dunque generano le mn immersioni di F/K).

Definizione 1.1.4. F/K si dice **normale** se $\forall \varphi : F \to \overline{F}$ tale che $\varphi_{|K} = id$, $\varphi(F) = F$.
Equivalentemente, F/K é normale $\iff$ F é campo di spezzamento di $\mu_\alpha(x)$ $\forall \alpha \in F$.

Definizione 1.1.5. F/K si dice **di Galois** se é normale e separabile. In questo caso si denota $\mathrm{Gal}(F/K) := \{\varphi : F \to \overline{F} | \varphi_{|K} = id\}$ il **gruppo di Galois**.

Osservazione. Per quanto detto prima, $|\mathrm{Gal}(F/K)| = [F : K]$.

Osservazione. $\mathbb{Q}(\zeta_n)$ é un'estensione di Galois con $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ abeliano, dunque per la corrispondenza di Galois ogni estensione intermedia $\mathbb{Q} \subset E \subset \mathbb{Q}(\zeta_n)$ é di Galois su $\mathbb{Q}$. Inoltre si hanno le relazioni:

- $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{[n,m]})$;
- $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{(n,m)})$.

Dimostrazione. Le due dimostrazioni sono analoghe; vediamo la prima.
L'inclusione $\supseteq$ é ovvia; inoltre per Bezout $(n, m) = d \Rightarrow an + bm = d \Rightarrow \zeta_n^b \zeta_m^a = e^{\frac{2\pi i b}{n}} e^{\frac{2\pi i a}{m}} = e^{\frac{2\pi i (an+bm)}{nm}} = e^{\frac{2\pi i}{[n,m]}}$. □

Infine osserviamo che se m é dispari, allora $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$; inoltre, se m é pari, i $\mathbb{Q}(\zeta_m)$ sono tutti distinti.

1.2 Richiami di algebra commutativa

Nel seguito indicheremo con A un anello commutativo con 1.

Definizione 1.2.1. Un **A-modulo** é una coppia (M, φ), dove M é un gruppo abeliano e $\varphi : A \to \mathrm{End}(M)$ tale che $a \to \varphi_a$ (moltiplicazione per a) é un omomorfismo di anelli.

Osservazioni.
- K campo $\Rightarrow$ un K-modulo é un K-spazio vettoriale.
- $I \subset A$ ideale $\Rightarrow$ I é un A-modulo.
- A é $\mathbb{Z}$-modulo $\iff$ $A = G$ gruppo abeliano.
  Infatti $\forall G$ gruppo, é ben definito l'omomorfismo:

$$\begin{array}{ccc} \mathbb{Z} \times G & \longrightarrow & G \\ (m, g) & \longrightarrow & \underbrace{g + \ldots + g}_{m \text{ volte}} \end{array}$$

Osservazione. Nei moduli in generale non esiste una base; ad esempio $\mathbb{Z}/n\mathbb{Z}$ come $\mathbb{Z}$-modulo non ha base, poiché tutti i suoi elementi sono di torsione.
Allo stesso modo, $\mathbb{Z} = \langle 1 \rangle$ e $\mathbb{Z} = \langle 2, 3 \rangle$, e sono insiemi minimali di generatori, ma hanno cardinalitá diversa.

Definizione 1.2.2. Si dice che M é generato da S su A (e si scrive $M = \langle S \rangle_A$) se $M = \left\{ \sum_{i=1}^{n} a_i s_i | a_i \in A, s_i \in S, n \in \mathbb{N} \right\}$.

Definizione 1.2.3. Un modulo M si dice finitamente generato su A se $M = \langle s_1, \ldots, s_n \rangle_A$.

Osservazione. Se M é un A-modulo finitamente generato, $M = \langle m_1, \ldots, m_n \rangle_A$, allora l'omomorfismo $\varphi : A^n \to M$ tale che $e_i \to m_i$ é surgettivo e dunque $M \cong \frac{A^n}{\mathrm{Ker}(\varphi)}$.

Definizione 1.2.4. M A-modulo, $x \in M$. Si definisce **annullatore di** x l'ideale $\mathrm{Ann}(x) = \{a \in A | ax = 0\} \subset A$.
Inoltre si definisce **annullatore di** M l'ideale $\mathrm{Ann}(M) = \{a \in A | am = 0 \ \forall m \in M\}$.

Definizione 1.2.5. M A-modulo si dice **fedele** se $\mathrm{Ann}(M) = \{0\}$.

Definizione 1.2.6. $A \subseteq B$ anelli. $\alpha \in B$ si dice **intero** su A se $\exists f \in A[x]$ monico tale che $f(\alpha) = 0$ (cioé $\alpha^n + a_1 \alpha^{n-1} + \ldots + a_n = 0$ per certi $a_1, \ldots, a_n$, cioé $\alpha^n \in \langle \alpha^{n-1}, \ldots, 1 \rangle_A$).

Proposizione 1.2.1. *$A \subseteq B$ anelli, $x \in B$. Sono fatti equivalenti:*

1. *x é intero su A*
2. *$A[x]$ é un A-modulo finitamente generato*
3. *$\exists C$ anello tale che $A[x] \subseteq C$ e C é finitamente generato come A-modulo*
4. *$\exists M$ $A[x]$-modulo fedele finitamente generato come A-modulo.*

Dimostrazione. 1) $\Rightarrow$ 2) $A[x] = \langle 1, \ldots, x^{n-1} \rangle_A$.

2) $\Rightarrow$ 3) Basta considerare $C = A[x]$.

3) $\Rightarrow$ 4) $M = C$ va bene, poiché C é un $A[x]$-modulo (in quanto contiene $A[x]$ ed é un A-modulo) e $Ann_{A[x]}(C) = \{a(x) \in A[x] | a(x) \cdot c = 0 \ \forall c \in C\} = \{0\}$, poiché $1 \in C \Rightarrow a(x) \cdot 1 = 0 \Rightarrow a(x) = 0$.

4) $\Rightarrow$ 1) Sia $\phi : M \to M \in \mathrm{End}(M) | m \to xm$ la moltiplicazione per x (che é definita perché M é un $A[x]$-modulo).
M é finitamente generato su A, dunque $M = \langle m_1, \ldots, m_s \rangle_A$; in particolare, $\phi(m_i) = xm_i = \sum_{j=1}^{s} a_{ij} m_j$.
Condidero la matrice (a_{ij}); il suo polinomio caratteristico é $t^s + b_1 t^{s-1} + \ldots + b_s = 0$, con $b_i \in A$ perché le entrate della matrice stanno in A, da cui $\phi^s + b_1 \phi^{s-1} + \ldots + b_s \equiv 0$.
Dunque $(x^s + b_1 x^{s-1} + \ldots + b_s)m = 0 \ \forall m \in M$, ma M é fedele $\Rightarrow x^s + b_1 x^{s-1} + \ldots + b_s = 0$, cioé x é intero su A.

□

Corollario 1.2.2. *$A \subseteq B$ anelli. B é finitamente generato come A-modulo $\iff$ $B = A[x_1, \ldots, x_n]$, con x_i intero su A $\forall i$.*

Dimostrazione. $\Rightarrow$) Se $B = \langle x_1, \ldots, x_n \rangle_A \Rightarrow B = A[x_1, \ldots, x_n]$.
Inoltre $x_i \in B \ \forall i$ e B é un anello finitamente generato $\Rightarrow$ per il punto 3) della precedente proposizione si ha la tesi.

$\Leftarrow$) Procediamo per induzione su n.
Se $n = 1$ la tesi segue per il punto 2) della precedente proposizione.
Se invece $B' = A[x_1, \ldots, x_{n-1}]$, é finitamente generato su A per ipotesi induttiva e $B = B'[x_n]$, ma x_n é intero su A e dunque su $B' \Rightarrow B$ é finitamente generato su B', che é finitamente generato su $A \Rightarrow$ é finitamente generato su A (in quanto i generatori sono i possibili prodotti dei due insiemi di generatori).

□

Definizione 1.2.7. $A \subseteq B$ anelli. Si definisce **chiusura integrale di A in B** l'insieme $\{x \in B | x \text{ é intero su } A\}$.

Corollario 1.2.3. *La chiusura integrale é un anello (e dunque un sottoanello di B che contiene A).*

Dimostrazione. Siano x, y nella chiusura integrale, cioé x, y interi su A. Allora $A[x, y]$ é un A-modulo finitamente generato per il precedente corollario $\Rightarrow$ per il punto 3) della proposizione **1.2.1** i suoi elementi sono interi su A (e dunque in particolare $x + y$ e xy). □

Definizione 1.2.8.

- B si dice **intero** su A se tutti i suoi elementi sono interi su A.
- A si dice **integralmente chiuso** in B se gli elementi interi di B sono tutti e soli gli elementi di A.
- A dominio si dice **integralmente chiuso** se lo é nel suo campo delle frazioni.

Proposizione 1.2.4 (Transitivitá della dipendenza integrale)**.** *$A \subseteq B \subseteq C$ interi $\Rightarrow$ C é intero su A.*

Dimostrazione. $\alpha \in C \Rightarrow \exists b_1, \ldots, b_n \in B$ tali che $\alpha^n + b_1\alpha^{n-1} + \ldots + b_n = 0 \Rightarrow$ se $B' = A[b_1, \ldots, b_n]$, α é intero su B', che é finitamente generato come A-algebra con elementi interi e dunque é finitamente generato come A-modulo.
D'altra parte $B'[\alpha]$ é finitamente generato su B', poiché α é intero su $B' \Rightarrow B'[\alpha]$ é finitamente generato come A-modulo $\Rightarrow \alpha$ é intero su A. □

Corollario 1.2.5. *La chiusura integrale C di A su B é integralmente chiusa su B.*

Dimostrazione. $\alpha \in B$ intero su C é intero anche su A perché C é intero su A e vale la proposizione precedente. □

Proposizione 1.2.6. *A UFD $\Rightarrow$ A integralmente chiuso.*

Dimostrazione. Sia K il campo delle frazioni di A. $\alpha = \frac{\beta}{\gamma} \in K$ intero, $\beta, \gamma \in A$, $(\beta, \gamma) = 1$.
$\exists a_1, \ldots, a_n \in A$ tali che $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0 \Rightarrow \frac{\beta^n}{\gamma^n} + a_1\frac{\beta^{n-1}}{\gamma^{n-1}} + \ldots + a_n = 0 \Rightarrow$ $\beta^n + a_1\beta^{n-1}\gamma + \ldots + a_n\gamma^n = 0 \Rightarrow \gamma | \beta^n$, ma $(\gamma, \beta) = 1$, dunque $\gamma = 1$. □

Osservazioni.

1. $\mathbb{Z}[\sqrt{5}]$ é intero su $\mathbb{Z}$ e il suo campo delle frazioni é $K = \mathbb{Q}(\sqrt{5})$.
   Peró non é integralmente chiuso, perché vedremo nella prossima sezione che la sua chiusura integrale é $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{5}]$.
2. Integralmente chiuso $\not\Rightarrow$ UFD.
   Infatti vedremo che $\mathbb{Z}[\sqrt{-5}]$ é integralmente chiuso, ma non é UFD perché $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ sono fattorizzazioni distinte di 6.

Proposizione 1.2.7. *A dominio integralmente chiuso, K il suo campo delle frazioni.*
$\alpha \in \overline{K}$ é intero su $A \iff \mu_\alpha(x) \in A[x]$, con μ_α polinomio minimo di α su K.

Dimostrazione. L'implicazione $\Leftarrow$ é del tutto ovvia, dunque vediamo l'altra.
Se $\overline{A}$ é la chiusura integrale di A in $\overline{K}$, e $\alpha \in \overline{A}$, allora anche $\sigma(\alpha) \in \overline{A}\ \forall \sigma : K(\alpha) \to \overline{K} | \sigma_{|K} = id$.
Infatti la stessa equazione di dipendenza intera di α vale anche per $\sigma(\alpha)$, poiché $\sigma_{|A} = id$.
Dunque $\mu_\alpha(x) = \prod_\sigma (x - \sigma(\alpha)) \in K[x] \cap \overline{A}[x]$, ma $K \cap \overline{A} = A$ perché A é integralmente chiuso $\Rightarrow K[x] \cap \overline{A}[x] = A[x]$. □

Definizione 1.2.9. *M A-modulo finitamente generato si dice* **libero** se $\exists n | M \cong A^n$. *n si dice* **rango** di M e si indica $\mathrm{rk}(M)$.

<u>*Osservazione*</u>. Ogni modulo libero di rango n ammette una base di n elementi.

<u>*Osservazione*</u>. In generale non é vero che ogni sottomodulo di un modulo libero é libero.
Ad esempio A é libero su se stesso, ma se tutti i suoi sottomoduli, cioé i suoi ideali, fossero liberi, avrebbero al piú un generatore, cioé A sarebbe un PID, che é falso in generale.

Teorema 1.2.8. *A PID, F A-modulo libero. Allora ogni sottomodulo M di F é libero e* $\mathrm{rk}(M) \leq \mathrm{rk}(F)$.

Teorema 1.2.9. *A PID, F A-modulo libero e M un suo sottomodulo finitamente generato. Allora $\exists$ una base $\mathscr{B}$ di F su A, $\exists e_1, \dots, e_n \in \mathscr{B}$, $a_1, \dots, a_n \in A$ tali che:*

1. *$\{a_1 e_1, \dots, a_n e_n\}$ é una A-base di M*
2. *$a_i | a_{i+1} \quad \forall i$.*

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

Corollario 1.2.10 (Teorema di struttura per moduli finitamente generati su PID)**.** *M A-modulo finitamente generato, A PID. Allora $M \cong A^r \oplus \frac{A}{(a_1)} \oplus \dots \oplus \frac{A}{(a_1)}$, con $a_i | a_{i+1} \quad \forall i$ e gli a_i sono univocamente determinati.*

Dimostrazione. M finitamente generato $\Rightarrow M \cong \frac{F}{R}$, con F A-modulo libero e $R \subseteq F$ sottomodulo. Ma allora R é libero ed $\exists \mathscr{B} = \{\omega_1, \dots, \omega_m\}$ base di F tale che $\{a_1\omega_1, \dots, a_n\omega_n\}$ é una base diagonale di R, con $n \leq m$.
$F = \omega_1 A \oplus \dots \oplus \omega_m A$ e $R = a_1\omega_1 A \oplus \dots \oplus a_n\omega_n A$ implicano la tesi. □

1.3 Prime definizioni e proprietá

Definizione 1.3.1. Definiamo **campo di numeri** un'estensione finita (e quindi semplice) di $\mathbb{Q}$, cioé $\mathbb{Q}(\alpha)$ con α algebrico su $\mathbb{Q}$.

<u>*Esempi.*</u> 1. $\mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z}$ libero da quadrati; queste sono tutte e sole le estensioni quadratiche di $\mathbb{Q}$ (e la lista non é ridondante).

Dimostrazione. Se $K \supset \mathbb{Q}$, $[K : \mathbb{Q}] = 2$, allora $K = \mathbb{Q}(\alpha)$, con α radice di un polinomio irriducibile di grado 2 con Δ non quadrato, cioé $K = \mathbb{Q}(\sqrt{\Delta})$.
m puó essere libero da quadrati perché, se $m = l^2 m'$, allora $\mathbb{Q}(m) = \mathbb{Q}(m')$.
Infine posso supporre $m \in \mathbb{Z}$, poiché se $m = \frac{r}{s}$, $\mathbb{Q}\left(\sqrt{\frac{r}{s}}\right) = \mathbb{Q}(\sqrt{rs})$.
Vediamo infine che $mn = r^2 \iff \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$, con $m, n \in \mathbb{Z}$ liberi da quadrati:
$\Rightarrow$) ovvia
$\Leftarrow$) $\sqrt{m} \in \mathbb{Q}(\sqrt{n}) \Rightarrow \sqrt{m} = \alpha + \beta\sqrt{n}$, $a, b \in \mathbb{Z} \Rightarrow m = \alpha^2 + \beta^2 n + 2\alpha\beta\sqrt{n} \Rightarrow \alpha\beta = 0$, ma se $\beta = 0 \Rightarrow m$ é un quadrato, assurdo, dunque $\alpha = 0$ e $\sqrt{m} = \beta\sqrt{n}$, cioé $m = \beta^2 n$, cioé $mn = \beta^2 n^2$. □

2. Le estensioni ciclotomiche $\mathbb{Q}(\zeta_n)$.

Definizione 1.3.2. $\alpha \in \mathbb{C}$ (o meglio $\alpha \in \overline{\mathbb{Q}}$) si dice **intero algebrico** se $\exists f \in \mathbb{Z}[x]$ monico tale che $f(\alpha) = 0$.

Osservazione. α intero algebrico $\Rightarrow$ α algebrico.

Definizione 1.3.3. $\mathbb{A} := \{\alpha \in \mathbb{C} | \alpha \text{ é intero algebrico}\}$.

Osservazione. $\mathbb{A}$ é un anello per il corollario **1.2.3**.

Definizione 1.3.4. $\mathscr{O}_K := \mathbb{A} \cap K$, con K campo di numeri, é detto **anello degli interi** di K.

Osservazione. $\mathscr{O}_K$ é un anello, in quanto intersezione di anelli; inoltre é un dominio, in quanto é contenuto in un campo.

Osservazione. In generale é falso che $\mathbb{Q}(\alpha) \cap \mathbb{A} = \mathbb{Z}[\alpha]$, ma affinché valga l'inclusione $\mathbb{Q}(\alpha) \cap \mathbb{A} \supset \mathbb{Z}[\alpha]$, é condizione necessaria che α sia un intero algebrico.
In realtá é anche condizione sufficiente, poiché $\mathbb{Z} \subset \mathscr{O}_K$, con $K = \mathbb{Q}(\alpha)$, e $\alpha \in \mathscr{O}_K \Rightarrow \mathscr{O}_K \supset \mathbb{Z}[\alpha]$.

Proposizione 1.3.1. *$\alpha \in \mathbb{C}$ algebrico su $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$. $\exists d \in \mathbb{Z}$ tale che $d\alpha$ é un intero algebrico.*

Dimostrazione. $\mu_\alpha(x) \in \mathbb{Q}[x]$ polinomio minimo di α, $\mu_\alpha(x) = x^n + a_1 x^{n-1} + \ldots + a_n$.
Sia $d \in \mathbb{Z}$ tale che $d \cdot a_i \in \mathbb{Z}\ \forall i$; allora $d \cdot \mu_\alpha(x) \in \mathbb{Z}[x]$.

$$d^n \mu_\alpha(\alpha) = d^n \alpha^n + (da_1) d^{n-1} \alpha^{n-1} + \ldots + (d^{n-1} a_{n-1}) d\alpha + d^n a_0 = f(d\alpha),$$

con $f(x)$ monico e $f(x) \in \mathbb{Z}[x]$.
Per avere la tesi basta osservare che $\mathbb{Q}(\alpha) = \mathbb{Q}(d\alpha)$. □

Osservazione. Dunque tutti i campi di numeri sono del tipo $\mathbb{Q}(\alpha)$, con α intero algebrico. Dunque d'ora in poi considereremo ogni campo di numeri come $\mathbb{Q}(\alpha)$, con α un intero algebrico.

Corollario 1.3.2. *Se $K = \mathbb{Q}(\alpha)$, il campo quoziente di $\mathscr{O}_K$ é K.*

Dimostrazione. Ovviamente, posto L il campo quoziente di $\mathscr{O}_K$, $L \subset K$, poiché $K \supset \mathscr{O}_K$ ed é un campo.
Ma $\mathbb{Z}[\alpha] \subset \mathscr{O}_K$, dunque $K \subset L$. □

Osservazione. Dunque $\mathscr{O}_K$ é integralmente chiuso.

Proposizione 1.3.3. *$\alpha \in \mathbb{C}$ é un intero algebrico $\iff$ $\mu_\alpha(x) \in \mathbb{Z}[x]$.*

Dimostrazione. $\Leftarrow$) ovvia
$\Rightarrow$) Per definizione $\exists f \in \mathbb{Z}[x]$ monico tale che $f(\alpha) = 0$.
Sia f di grado minimo tra i polinomi con questa proprietá. Dico che f é irriducibile su $\mathbb{Q}$ (o su $\mathbb{Z}$); questo basterebbe per giungere alla tesi.
Se per assurdo $f = gh$ in $\mathbb{Q}[x]$, allora $f = g'h'$ in $\mathbb{Z}[x]$ per il lemma di Gauss, e g', h' sono monici a meno di moltiplicare per -1, poiché il termine di grado massimo di $g'h'$ é 1 e dunque i termini di grado massimo di g' e h' stanno in $\mathbb{Z}^* = \{\pm 1\}$.
$0 = f(\alpha) = g'(\alpha)h'(\alpha)$, dunque $g'(\alpha) = 0 \vee h'(\alpha) = 0$, assurdo, per la minimalitá del grado di f. □

Osservazione. $\mathscr{O}_{\mathbb{Q}} = \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, infatti $\alpha = \frac{r}{s}$ é un intero algebrico $\iff$ $\mu_\alpha(x) = x - \alpha \in \mathbb{Z}[x] \iff \alpha \in \mathbb{Z}$.

Proposizione 1.3.4. *$m \in \mathbb{Z}$ libero da quadrati. Allora:*

$$\mathbb{Q}(\sqrt{m}) \cap \mathbb{A} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{se } m \equiv 2,3 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{se } m \equiv 1 \ (4) \end{cases}$$

Dimostrazione. Sia $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ di grado 2, cioé $b \neq 0$. $\alpha \in \mathbb{A} \iff \mu_\alpha(x) \in \mathbb{Z}[x]$.
$\mu_\alpha(x) = x^2 - 2ax + a^2 - b^2 m \in \mathbb{Z}[x] \Rightarrow a = \frac{r}{s}$, $(r,s) = 1$ e $2a \in \mathbb{Z}$, cioé $s|2$, cioé $s \in \{1,2\}$.
Se $s = 1$, allora $a \in \mathbb{Z}$, dunque anche $b^2 m \in \mathbb{Z}$. Ma m é libero da quadrati, dunque non puó cancellare il denominatore di b^2, quindi $b \in \mathbb{Z}$.
Perció gli elementi di $\mathbb{Z}[\sqrt{m}]$ sono interi e se $s = 1$ non ce ne sono altri.
Se invece $s = 2$, allora $a = \frac{r}{2}$, perció, posto $b = \frac{u}{t}$:

$$a^2 - b^2 m = \frac{r^2}{4} - \frac{u^2}{t^2} m = \frac{t^2 r^2 - 4mu^2}{4t^2} \in \mathbb{Z} \iff 4t^2 | t^2 r^2 - 4mu^2.$$

Dunque:

$$r^2 t^2 - 4mu^2 \cong r^2 t^2 \cong 0 \quad (4),$$

ma $(r,2) = 1$, dunque $2|t$. Poniamo $t = 2k$.
$t^2 | r^2 t^2 - 4mu^2 \Rightarrow 4u^2 m \equiv 0 \ (4k^2) \Rightarrow u^2 m \equiv 0 \ (k^2)$, ma m é libero da quadrati, dunque $k^2 | u^2$, cioé $k|u$.
Ma $b = \frac{u}{2k}$ e $(u, 2k) = 1 \Rightarrow k = 1 \Rightarrow t = 2$.
Vediamo se nel caso $s = 2$ la condizione $t = 2$ é anche sufficiente:

$$\alpha = \frac{r}{2} + \frac{u}{2}\sqrt{m} \in \mathscr{O}_K \Rightarrow a^2 - b^2 m = \frac{4r^2 - 4u^2 m}{4 \cdot 4} \in \mathbb{Z} \Rightarrow r^2 - u^2 m \equiv 0 \ (4) \iff r^2 \equiv u^2 m \ (4),$$

ma $(r,2) = 1$, $(u,2) = 1 \Rightarrow m \equiv 1 \ (4)$.
Dunque, se $m \not\equiv 1 \ (4)$, il caso $s = 2$ non dá nuovi interi e quindi $\mathscr{O}_K = \mathbb{Z}[\sqrt{m}]$.
Se $m \equiv 1 \ (4)$, ci sono anche gli elementi del tipo $\frac{r}{2} + \frac{u}{2}\sqrt{m}$, con r, u dispari, cioé $r = 1 + 2l$, $u = 1 + 2h \Rightarrow \frac{r}{2} + \frac{u}{2}\sqrt{m} = l + h\sqrt{m} + \frac{1+\sqrt{m}}{2}$, da cui $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. □

Esempi. Al variare di K fra i campi di numeri, la cardinalitá degli invertibili di $\mathscr{O}_K$ puó essere finita o infinita.

1. $K = \mathbb{Q}(\sqrt{-m})$, con $m > 0$. Allora, se $m = 1$, $\mathscr{O}_K^* = \{\pm 1, \pm i\}$, se $m = 3$, $\mathscr{O}_K^* = \left\{\pm 1, \pm\frac{1 \pm \sqrt{-3}}{2}\right\}$, se $m \neq 1, 3$, $\mathscr{O}_K^* = \{\pm 1\}$.

   Dimostrazione. Sia $-m \equiv 2,3 \ (4)$. $\mathscr{O}_K = \mathbb{Z}[\sqrt{-m}] \Rightarrow$ se $\alpha \in \mathscr{O}_K^*$, $\alpha = a + b\sqrt{-m}$, e $\exists \beta \in \mathscr{O}_k$ tale che $\alpha\beta = 1$.
   Prendendo la norma $\mathrm{N} = \|\cdot\|^2$, si ha:

   $$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta) = 1 \Rightarrow \mathrm{N}(\alpha) = a^2 + b^2 m | 1 \Rightarrow a^2 + b^2 m = 1,$$

   poiché é positivo.
   Se $m > 1 \Rightarrow b = 0 \Rightarrow a = \pm 1 \Rightarrow \alpha = \pm 1$.
   Se $m = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow a = \pm 1$, $b = 0 \vee a = 0$, $b = \pm 1$.
   Sia invece $-m \equiv 1 \ (4)$. $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-m}}{2}\right]$.
   $\alpha = a + b\sqrt{-m} \in \mathscr{O}_K^* \Rightarrow$ come prima dobbiamo risolvere $a^2 + mb^2 = 1$.
   Ora $a = \frac{c}{2}$ e $b = \frac{d}{2}$, con $b, d \in \mathbb{Z} \Rightarrow c^2 + md^2 = 4$.
   Se $m > 4 \Rightarrow d = 0 \Rightarrow c = \pm 2$.
   Se $m = 3 \Rightarrow d = 0$, $c = \pm 2 \vee d = \pm 1$, $c = \pm 1$ (sono le radici terze dell'unitá). □

2. $K = \mathbb{Q}(\sqrt{2})$. Allora $\mathscr{O}_K^* \cong \mathbb{Z} \oplus \{\pm 1\}$; in particolare $|\mathscr{O}_K^*| = +\infty$.

Dimostrazione. Bisogna risolvere l'equazione $a^2 - 2b^2 = \pm 1$. $\alpha = 1+\sqrt{2}$ la risolve, dunque $(1+\sqrt{2})^\gamma \in \mathscr{O}_K^*$ $\forall \gamma \in \mathbb{Z}$ e le potenze sono tutte distinte perché $\|1+\sqrt{2}\| > 1$.
Dico che $\varepsilon \in \mathscr{O}_K^* \Rightarrow \varepsilon = \pm(1+\sqrt{2})^\gamma$, $\gamma \in \mathbb{Z}$ (e avrei la tesi).
Se $\varepsilon \neq \pm 1$, considero $\varepsilon > 1$ (poiché altrimenti considererei $\overline{\varepsilon} > 1$); voglio vedere che non é possibile che sia $1 < \varepsilon < 1 + \sqrt{2}$.
$\varepsilon = x + y\sqrt{2}$, e $-1 < \overline{\varepsilon} < 1$; ma:

$$\begin{cases} 1 < x + y\sqrt{2} < 1 + \sqrt{2} \\ -1 < x - y\sqrt{2} < 1 \end{cases} \Rightarrow 0 < 2x < 2 + \sqrt{2} \Rightarrow x = 1,$$

poiché $x, y \in \mathbb{Z} \Rightarrow \varepsilon = 1 + y\sqrt{2}$, ma $1 < \varepsilon < 1 + \sqrt{2}$, assurdo.
Se fosse $\varepsilon \neq (1+\sqrt{2})^\gamma$ $\forall \gamma$, allora $\exists k$ tale che $(1+\sqrt{2})^k < \varepsilon < (1+\sqrt{2})^{k+1}$.
Ma allora si avrebbe $\varepsilon \cdot (1+\sqrt{2})^{-k} \in \mathscr{O}_K^*$, $1 < \varepsilon \cdot (1+\sqrt{2})^{-k} < 1 + \sqrt{2}$, assurdo. □

2 Traccia, norma, discriminante e loro conseguenze

2.1 Traccia e norma

Definizione 2.1.1. Sia F/K un'estensione separabile di grado n, e siano $\sigma_1, \dots, \sigma_n$ le immersioni di F/K. Si definisce **traccia di** F/K:

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

e **norma di** F/K:

$$\begin{array}{rccc} \mathrm{N}_{F/K}: & F & \longrightarrow & K \\ & \alpha & \longrightarrow & \prod_{i=1}^{n} \sigma_i(\alpha) \end{array} .$$

Osservazione. A prima vista sembra che le precedenti applicazioni non siano ben definite, in quanto a priori il codominio é F; per questo ci viene in aiuto il seguente risultato:

Proposizione 2.1.1. *Traccia e norma sono ben definite e, se K, F sono campi di numeri e $\alpha \in \mathscr{O}_F \Rightarrow \mathrm{Tr}_{F/K}(\alpha), \mathrm{N}_{F/K}(\alpha) \in \mathscr{O}_K$.*

Dimostrazione. Il caso $F = K(\alpha)$ é particolarmente semplice, poiché $\mathrm{Tr}_{F/K}(\alpha)$ e $\mathrm{N}_{F/K}(\alpha)$ non sono altro che il secondo e l'ultimo coefficiente del polinomio minimo di α, e perció stanno in K.
In generale, sia $\alpha \in F$ e $L = K(\alpha) \subset F$, $[L : K] = d | n$; denotiamo con $\tau_1, \dots, \tau_d$ le immersioni di L/K.
Allora $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{d} \tau_i(\alpha) \in K$, per quanto visto nel primo caso.
Ma ogni τ_i si estende a $\frac{n}{d}$ immersioni di F/K, e tramite queste immersioni $\alpha \to \tau_i(\alpha)$, dunque:

$$\mathrm{Tr}_{F/K}(\alpha) = \frac{n}{d}(\tau_1(\alpha) + \ldots + \tau_d(\alpha)) = \frac{n}{d} \cdot \mathrm{Tr}_{L/K}(\alpha) \in K.$$

Analogamente $\mathrm{N}_{F/K}(\alpha) = \big(\mathrm{N}_{L/K}(\alpha)\big)^{\frac{n}{d}}$.
Infine, se $\alpha \in \mathscr{O}_F \Rightarrow \alpha \in \mathscr{O}_F \cap L = \mathscr{O}_L$, perció $\mathrm{Tr}_{F/K}(\alpha), \mathrm{N}_{F/K}(\alpha) \in \mathscr{O}_K$, in quanto $\mu_\alpha(x) \in \mathscr{O}_K[x]$. □

Proposizione 2.1.2. *La traccia é K-lineare, cioé:*

$$\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta) \quad \forall \alpha, \beta \in F$$

$$\mathrm{Tr}_{F/K}(\lambda\alpha) = \lambda \, \mathrm{Tr}_{F/K}(\alpha) \qquad \forall \alpha \in F, \lambda \in K.$$

Invece la norma é moltiplicativa, cioé:

$$\mathrm{N}_{F/K}(\alpha\beta) = \mathrm{N}_{F/K}(\alpha) \, \mathrm{N}_{F/K}(\beta) \quad \forall \alpha, \beta \in F$$

$$\mathrm{N}_{F/K}(\lambda\alpha) = \lambda^n \, \mathrm{N}_{F/K}(\alpha) \qquad \forall \alpha \in F, \lambda \in K.$$

Proposizione 2.1.3. *$K \subset F \subset M$ campi. Allora:*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{M/F} \qquad e \qquad \mathrm{N}_{M/K} = \mathrm{N}_{F/K} \circ \mathrm{N}_{M/F}$$

Dimostrazione. Siano $\sigma_1, \dots, \sigma_n$ le immersioni di F/K; siano inoltre $\tau_1, \dots, \tau_m$ le immersioni di M/F. $\alpha \in M$.

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

Sia N la chiusura normale di M/K (cioé il composto dei coniugati di M) e siano $\widetilde{\sigma_1}, \dots, \widetilde{\sigma_n}$, $\widetilde{\tau_1}, \dots, \widetilde{\tau_m}$ estensioni delle σ_i e τ_j a N. $\widetilde{\sigma_i}, \widetilde{\tau_j} \in \mathrm{Gal}(N/K)\ \forall i, j$.
Dico che $\{\widetilde{\sigma_i} \circ \widetilde{\tau_j}\}_{i,j}$ sono mn elementi distinti su M in $\mathrm{Gal}(N/K)$ (cioé $(\widetilde{\sigma_i} \circ \widetilde{\tau_j})_{|M}$ al variare di i, j sono le immersioni di M/K).
Supponiamo $(\widetilde{\sigma_i} \circ \widetilde{\tau_j})_{|M} = (\widetilde{\sigma_h} \circ \widetilde{\tau_k})_{|M}$; allora, se $F = K(\beta)$:

$$\widetilde{\sigma_i}\big(\underbrace{\widetilde{\tau_j}(\beta)}_{=\beta}\big) = \widetilde{\sigma_h}\big(\underbrace{\widetilde{\tau_k}(\beta)}_{=\beta}\big) \Rightarrow \sigma_i(\beta) = \sigma_h(\beta),$$

poiché $\sigma_i = \widetilde{\sigma_i}$, $\sigma_h = \widetilde{\sigma_h}$ su F.
Dunque le σ_i coincidono su β oltre che su K, cioé coincidono su $F \Rightarrow i = h$, poiché su F sono tutte distinte.
Quindi $\widetilde{\sigma_i} = \widetilde{\sigma_h}$, ma essendo elementi del gruppo di Galois sono invertibili, perció $\widetilde{\tau_j}_{|M} = \widetilde{\tau_k}_{|M} \Rightarrow \tau_j = \tau_k \Rightarrow j = k$ per lo stesso ragionamento precedente.
Allora:

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i,j} \big(\widetilde{\sigma_i} \circ \widetilde{\tau_j}(\alpha)\big) = \sum_{i,j} \widetilde{\sigma_i}\big(\widetilde{\tau_j}(\alpha)\big) = \sum_i \widetilde{\sigma_i}\Bigg(\underbrace{\sum_j \tau_j(\alpha)}_{=\mathrm{Tr}_{M/F}(\alpha) \in F}\Bigg) =$$

$$= \sum_i \sigma_i\big(\mathrm{Tr}_{M/F}(\alpha)\big) = \mathrm{Tr}_{F/K}\big(\mathrm{Tr}_{M/F}(\alpha)\big).$$

Per la norma il ragionamento é del tutto analogo. □

Lasciamo al lettore la dimostrazione di questo semplice fatto, che ci servirá in seguito:

Esercizio. *F/K estensione, $\alpha \in F$, $\varphi_\alpha : \begin{matrix} F & \to & F \\ a & \to & \alpha a \end{matrix}$. Sia $M_\alpha = [\varphi_\alpha]$ la matrice associata a φ_α in una qualunque base. Allora $\mathrm{Tr}_{F/K}(\alpha) = \mathrm{tr}\, M_\alpha$ e $\mathrm{N}_{F/K}(\alpha) = \det M_\alpha$.*
(Suggerimento: si lavori prima con una base del tipo $\{1, \alpha, \dots, \alpha^{n-1}\}$. Poi si consideri $F \supseteq K(\alpha) \supseteq K$ e si crei una base di F/K del tipo $\{\alpha^i b_j\}$, $i = 0, \dots, d-1$, $j = 1, \dots, \frac{n}{d}$. Allora $\mathrm{Tr}_{F/K}(\alpha) = \frac{n}{d}(\sigma_1(\alpha) + \dots + \sigma_d(\alpha)) = \mathrm{tr}(M\alpha)$.)

<u>*Osservazione*</u>. $\alpha \in \mathscr{O}_K$. Allora $\alpha \in \mathscr{O}_K^* \iff \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Dimostrazione. $\Rightarrow$) $\exists \beta$ tale che $\alpha\beta = 1 \Rightarrow \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathrm{N}_{K/\mathbb{Q}}(\beta) = 1$, ma α é intero $\Rightarrow \mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}^* = \{\pm 1\}$.

$\Leftarrow$) $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_\sigma \sigma(\alpha) = \alpha \cdot \prod_{\sigma \neq id} \sigma(\alpha) = \pm 1$.
Se $\beta = \prod_{\sigma \neq id} \sigma(\alpha)$, $\beta = \pm\frac{1}{\alpha} \in K$ perché inverso di un elemento di K; ma $\beta \in \mathbb{A}$, poiché α intero $\Rightarrow \sigma(\alpha)$ intero $\forall \sigma \Rightarrow \beta \in K \cap \mathbb{A} = \mathscr{O}_K$.

□

<u>*Osservazione*</u>. $\mathscr{O}_K$ é un anello che contiene $\mathbb{Z}$, dunque é uno $\mathbb{Z}$-modulo, cioé un gruppo abeliano.

Definizione 2.1.2. G gruppo, K campo. Si definisce **carattere** di G in K un omomorfismo $\chi : G \to K^*$.

<u>*Osservazione*</u>. É ben definita la somma di due caratteri, poiché si sfrutta la somma definita su K. Peró in generale la somma di due caratteri non é un carattere.

Teorema 2.1.4 (di indipendenza dei caratteri di Artin)**.** *Caratteri distinti sono linearmente indipendenti su K (o su un qualunque campo $\supset K$).*

Dimostrazione. Supponiamo per assurdo che $\exists \chi_1, \ldots, \chi_n$ caratteri distinti linearmente dipendenti, cioé $a_1\chi_1 + \ldots + a_n\chi_n \equiv 0$. Suppongo n minimo con questa proprietá (e dunque $a_i \neq 0$ $\forall i$, altrimenti lo potrei togliere).
Allora $\forall g \in G$, $a_1\chi_1(g) + \ldots + a_n\chi_n(g) = 0$. Sia $h \in G$ tale che $\chi_1(h) \neq \chi_2(h)$, che esiste perché $\chi_1 \neq \chi_2$. Allora:

$$0 = a_1\chi_1(gh) + \ldots + a_n\chi_n(gh) = a_1\chi_1(g)\chi_1(h) + \ldots + a_n\chi_n(g)\chi_n(h).$$

Moltiplicando la relazione di dipendenza lineare per $\chi_1(h)$ si ha:

$$0 = a_1\chi_1(g)\chi_1(h) + \ldots + a_n\chi_n(g)\chi_1(h).$$

Sottraendo le due equazioni:

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \ldots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) = 0 \quad \forall g \in G,$$

assurdo, poiché ho ottenuto una combinazione lineare non nulla (in quanto $\chi_2(h) - \chi_1(h) \neq 0$) di lunghezza $< n$. □

Corollario 2.1.5. *L/K separabile $\Rightarrow$ $\mathrm{Tr}_{L/K} : L \to K$ é surgettiva (in realtá vale anche il viceversa).*

Dimostrazione. $\mathrm{Tr}_{L/K}$ é K-lineare fra due K-spazi vettoriali, e il codominio ha dimensione 1 su K, dunque $\mathrm{Tr}_{L/K}$ é surgettiva $\iff$ é non nulla.
$\mathrm{Tr}_{L/K} = \sum_{i=1}^{n} \sigma_i$, e $\sigma_i : L \to K$ é iniettiva, dunque la posso restringere a $\sigma_i : L^* \to K^*$ $\forall i$; ma allora i σ_i sono caratteri distinti e la tesi segue per il teorema precedente. □

<u>*Osservazione*</u>. $\begin{array}{ccc} L \times L & \to & K \\ (x,y) & \to & \mathrm{Tr}_{L/K}(xy) \end{array}$ é bilineare e non degenere (perché l'applicazione ψ_x : $\begin{array}{ccc} L & \to & K \\ y & \to & \mathrm{Tr}_{L/K}(xy) \end{array}$ non é mai nulla per il corollario precedente).
Dunque esiste una base duale:

$$\begin{array}{rccc} \psi : & L & \longrightarrow & \widehat{L} = \mathrm{Hom}(L,K) \\ & x & \longrightarrow & \psi_x \end{array}$$

é lineare e iniettiva perché l'applicazione bilineare é non degenere (e quindi surgettiva per dimensione).

Corollario 2.1.6. *$\psi : L \to \widehat{L}$ é un isomorfismo di K-spazi vettoriali.*

<u>*Osservazione*</u>. Sia $\alpha_1, \ldots, \alpha_n$ una K-base di L. Sia $f_1, \ldots, f_n$ la sua base duale (cioé $f_i \in \widehat{L}$, $f_i(\alpha_j) = \delta_{ij}$).
Queste f_i sono tracce, perché ψ é surgettiva $\Rightarrow \forall i \quad \exists \beta_i \in L | f_i = \psi_{\beta_i}$.
$\beta_1, \ldots, \beta_n$ sono linearmente indipendenti, poiché hanno immagini linearmente indipendenti.

Definizione 2.1.3. Secondo la notazione precedente, $\{\beta_1, \ldots, \beta_n\}$ base di L si chiama **base duale** di $\{\alpha_1, \ldots, \alpha_n\}$ e ha la proprietá che $\mathrm{Tr}_{L/K}(\alpha_i\beta_j) = \delta_{ij}$.

Teorema 2.1.7 (Struttura additiva di $\mathscr{O}_K$)**.** *$[K : \mathbb{Q}] = n$. $\mathscr{O}_K$ é uno $\mathbb{Z}$-modulo libero di rango n.*

Dimostrazione. Sicuramente $\mathscr{O}_K$ é uno $\mathbb{Z}$-modulo.
Se troviamo A, B gruppi abeliani liberi di rango n tali che $A \subseteq \mathscr{O}_K \subseteq B$, avremmo la tesi.

A) $\exists \alpha \in K$ tale che $K = \mathbb{Q}(\alpha)$. Posso supporre che $\alpha \in \mathscr{O}_K$.
$\mathbb{Z}[\alpha] \subseteq \mathscr{O}_K$. Dico che $A = \mathbb{Z}[\alpha]$ va bene.
$\{1, \alpha, \dots, \alpha^{n-1}\}$ sono i generatori su $\mathbb{Z}$ di $\mathbb{Z}[\alpha]$ e sono indipendenti su $\mathbb{Q}$, cioé su $\mathbb{Z}$, dunque sono una base e $\mathrm{rk}(\mathbb{Z}[\alpha]) = n$.

B) Sia $\{\alpha_1, \dots, \alpha_n\}$ una $\mathbb{Q}$-base di K, con $\alpha_i \in \mathscr{O}_K \ \forall i$. Sia $\{\beta_1, \dots, \beta_n\}$ la base duale.
Dico che, se $B = \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}}$, $\mathscr{O}_K \subseteq B$ (e ovviamente $\mathrm{rk}(B) = n$).
Sia $\alpha \in \mathscr{O}_K$. $\alpha = \sum_i x_i \beta_i$, con $x_i \in \mathbb{Q}$. Voglio vedere che $x_i \in \mathbb{Z}$.
$\mathscr{O}_K \ni \alpha\alpha_j = \sum_i x_i \beta_i \alpha_j$. Applicando la traccia:

$$\mathbb{Z} \ni \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\alpha_j) = \sum_i x_i \cdot \mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\alpha_j) = \sum_i x_i \cdot \delta_{ij} = x_j \quad \forall j.$$

□

Definizione 2.1.4. Si definisce **base intera** di $K/\mathbb{Q}$ una $\mathbb{Z}$-base di $\mathscr{O}_K$.

Osservazione. $\{\alpha_1, \dots, \alpha_n\}$ base intera, cioé $\mathscr{O}_K = \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}} \Rightarrow K = \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Q}}$ (ma ovviamente non é vero il viceversa).

Osservazione. $\mathbb{Z} \subseteq F \subseteq K$. In generale $\mathscr{O}_K$ non é libero su $\mathscr{O}_F$.
Inoltre in generale $\mathscr{O}_F$ non é PID.

2.2 Discriminante

Nel seguito denoteremo con F/K un'estensione di campi di numeri, $[F : K] = n$, e con $\sigma_1, \dots, \sigma_n$ le immersioni di F/K.

Definizione 2.2.1. $\alpha_1, \dots, \alpha_n \in F$. Definiamo **discriminante** di $\alpha_1, \dots, \alpha_n$
$\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$.

Teorema 2.2.1. $\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = \det\big(\mathrm{Tr}_{F/K}(\alpha_i\alpha_j)\big)$.
In particolare, $\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) \in K$ *e se* $\alpha_j \in \mathscr{O}_F \ \forall j \Rightarrow \mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) \in \mathscr{O}_K$.

Dimostrazione. $\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det\big({}^t(\sigma_i(\alpha_j))\big) \cdot \det(\sigma_i(\alpha_j)) =$
$\det\big({}^t(\sigma_i(\alpha_j))(\sigma_i(\alpha_j))\big) = \det\big(\mathrm{Tr}_{F/K}(\alpha_i\alpha_j)\big)$. □

Teorema 2.2.2. $\mathrm{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = 0 \iff \alpha_1, \dots, \alpha_n$ *sono linearmente dipendenti su* K.

Dimostrazione. Poiché le σ_i sono iniettive, $\det(\sigma_i(\alpha_j)) = 0 \iff \exists a_1, \dots, a_n$ non tutti nulli tali che $\sum_j a_j\sigma_i(\alpha_j) \ \forall i \iff \sigma_i\big(\sum_j a_j\alpha_j\big) = 0 \ \forall i \iff \sum_j a_j\alpha_j = 0$. □

Teorema 2.2.3. $F = K(\alpha)$. *Allora, se* $\mu_\alpha(x)$ *é il polinomio minimo di* α*:*

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

Dimostrazione. Per definizione di discriminante:

$$\mathrm{disc}_{F/K}(1, \alpha, \dots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \dots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \dots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 = \prod_{1 \le r < s \le n} (\sigma_s(\alpha) - \sigma_r(\alpha))^2,$$

poiché é una matrice di Vandermonde.
Ora:

$$\prod_{1\le r<s\le n}(\sigma_s(\alpha)-\sigma_r(\alpha))^2=\prod_{r\neq s}(\sigma_s(\alpha)-\sigma_r(\alpha))\cdot(-1)^{\binom{n}{2}},$$

poiché $\binom{n}{2}$ é il numero di scambi di segno che vengono fatti.
Poiché $\mu_\alpha(x)=\prod_{i=1}^n(x-\sigma_i(\alpha))\Rightarrow\mu'_\alpha(x)=\sum_{i=1}^n\prod_{j\neq i}(x-\sigma_j(\alpha))$, dunque:

$$\mathrm{N}_{F/K}(\mu'_\alpha(\alpha))=\prod_{l=1}^n\sigma_l(\mu'_\alpha(\alpha))=\prod_{l=1}^n\mu'_\alpha(\sigma_l(\alpha))=\prod_{l=1}^n\prod_{j\neq l}(\sigma_l(\alpha)-\sigma_j(\alpha))=\prod_{r\neq s}(\sigma_r(\alpha)-\sigma_s(\alpha)),$$

da cui la tesi. □

Esempi. Vediamo alcuni esempi nel caso delle estensioni ciclotomiche.

1. $m\in\mathbb{Z}$, $K=\mathbb{Q}(\zeta_m)$, $[K:\mathbb{Q}]=\phi(m)$. $\{1,\zeta_m,\dots,\zeta_m^{\phi(m)-1}\}$ é una $\mathbb{Q}$-base di K. Denotiamo $\mathrm{disc}_{K/\mathbb{Q}}(\zeta_m):=\mathrm{disc}_{K/\mathbb{Q}}(1,\zeta_m,\dots,\zeta_m^{\phi(m)-1})$.
   Per quanto appena visto, $\mathrm{disc}_{K/\mathbb{Q}}(\zeta_m)=(-1)^{\frac{n(n-1)}{2}}\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_m))$, dove $\mu(x)$ é il polinomio minimo di ζ_m.
   Ora:

   $$x^m-1=\mu(x)g(x)\Rightarrow mx^{m-1}=\mu'(x)g(x)+\mu(x)g'(x)\Rightarrow m\zeta_m^{m-1}=\mu'(\zeta_m)g(\zeta_m)\Rightarrow$$
   $$\Rightarrow\mathrm{N}_{K/\mathbb{Q}}(m)\,\mathrm{N}_{K/\mathbb{Q}}(\zeta_m)^{m-1}=\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_m))\,\mathrm{N}_{K/\mathbb{Q}}(g(\zeta_m)).$$

   Ma $\mathrm{N}_{K/\mathbb{Q}}(m)=m^{\phi(m)}$ e $\mathrm{N}_{K/\mathbb{Q}}(\zeta_m)=\pm1$, poiché é un'unitá, dunque $\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_m))\,\mathrm{N}_{K/\mathbb{Q}}(g(\zeta_m))=\pm m^{\phi(m)}$, da cui $\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_m))|m^{\phi(m)}$ (poiché $\mathrm{N}_{K/\mathbb{Q}}(g(\zeta_m))\in\mathbb{Z}$ in quanto $g(\zeta_m)$ é un intero in K).

2. Se $m=p^k$, con p primo, allora $\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_m))|p^{k\phi(p^k)}$, cioé é una potenza di p.

3. Se $m=p$ primo, $x^p-1=\mu(x)(x-1)\Rightarrow p\zeta_p^{p-1}=\mu'(\zeta_p)(\zeta_p-1)\Rightarrow\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_p))\,\mathrm{N}_{K/\mathbb{Q}}(\zeta_p-1)=p^{\phi(p)}=p^{p-1}$ (poiché $\mathrm{N}_{K/\mathbb{Q}}(\zeta_p)=1$ in quanto é il termine noto del suo polinomio minimo).
   Il polinomio minimo di ζ_p-1 si trova per traslazione da $\mu_{\zeta_p}(x)$:

   $$\mu_{\zeta_p-1}(x)=\mu_{\zeta_p}(x+1)=(x+1)^{p-1}+\ldots+(x+1)+1=xq(x)+p,$$

   dunque $\mathrm{N}_{K/\mathbb{Q}}(\zeta_p-1)=p$. Ma allora $\mathrm{N}_{K/\mathbb{Q}}(\mu'(\zeta_p))=p^{p-2}$, da cui $\mathrm{disc}_{K/\mathbb{Q}}(\zeta_p)=(-1)^{\frac{(p-1)(p-2)}{2}}p^{p-2}=(-1)^{\frac{p-1}{2}}p^{p-2}$.

Osservazione. $\mathscr{A}=\{\alpha_1,\dots,\alpha_n\}$, $\mathscr{B}=\{\beta_1,\dots,\beta_n\}$ basi di F/K. $\forall i$, $\beta_i=\sum_{j=1}^n a_{ij}\alpha_j$, cioé $\exists M$ tale che $M\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}$.
$\mathrm{disc}_{F/K}(\alpha_1,\dots,\alpha_n)=\det(\Sigma(\alpha))^2$, dove $\Sigma(\alpha)=(\sigma_i(\alpha_j))$.
Analogamente, $\mathrm{disc}_{F/K}(\beta_1,\dots,\beta_n)=\det(\Sigma(\beta))^2$.
$\Sigma(\beta)=M\cdot\Sigma(\alpha)$, dunque $\det(\Sigma(\beta))^2=\det(M)^2\det(\Sigma(\alpha))^2$.
Se $\mathscr{A}$ e $\mathscr{B}$ sono basi intere, allora $M\in\mathfrak{M}(n,\mathbb{Z})$, ma M é invertibile, poiché posso scrivere gli α_i come combinazione lineare dei β_j, perció $\det(M)\in\mathbb{Z}^*=\{\pm1\}$, cioé $\det(M)^2=1$.
Quindi $\mathrm{disc}_{F/K}(\alpha_1,\dots,\alpha_n)=\mathrm{disc}_{F/K}(\beta_1,\dots,\beta_n)$. In conclusione, il discriminante di $K/\mathbb{Q}$ di una base intera é un invariante di K; denotiamo dunque $\mathrm{disc}(K):=\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1,\dots,\alpha_n)$, con $\{\alpha_1,\dots,\alpha_n\}$ base intera di $K/\mathbb{Q}$.

Esempio. $K = \mathbb{Q}(\sqrt{m})$, con m libero da quadrati. Allora:

$$\operatorname{disc}(K) = \begin{cases} 4m & \text{se } m \equiv 2,3 \ (4) \\ m & \text{se } m \equiv 1 \ (4) \end{cases}.$$

Infatti le immersioni di $K/\mathbb{Q}$ sono $\sqrt{m} \to \pm\sqrt{m}$, da cui:

$$\operatorname{disc}(K) = \begin{cases} \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = 4m & \text{se } m \equiv 2,3 \ (4) \\ \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = m & \text{se } m \equiv 1 \ (4) \end{cases}$$

Osservazione. Se $Y \subset X \subset K$, con X, Y $\mathbb{Z}$-moduli di rango $n = [K : \mathbb{Q}]$, $\exists\{x_1, \dots, x_n\}$ $\mathbb{Z}$-base di X, $\exists a_1, \dots, a_n \in \mathbb{Z}$ tali che $\{a_1x_1, \dots, a_nx_n\}$ é $\mathbb{Z}$-base di Y.
Se $M = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$, $M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_1x_1 \\ \vdots \\ a_nx_n \end{pmatrix}$ e $\det(M)^2 = (a_1 \cdot \ldots \cdot a_n)^2$. Notiamo che $\frac{X}{Y}$ é un gruppo abeliano e $\frac{X}{Y} \cong \frac{x_1\mathbb{Z} \oplus \ldots \oplus x_n\mathbb{Z}}{a_1x_1\mathbb{Z} \oplus \ldots \oplus a_nx_n\mathbb{Z}} \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_n\mathbb{Z}$, da cui $\left|\frac{X}{Y}\right| = a_1 \cdot \ldots \cdot a_n$.
Poiché $\operatorname{disc}(Y) = \operatorname{disc}(a_1x_1, \dots, a_nx_n) = \det(M)^2 \operatorname{disc}(x_1, \dots, x_n) = \operatorname{disc}(X)$, concludiamo che:

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

Corollario 2.2.4. *$K = \mathbb{Q}(\alpha)$, α intero. Allora:*

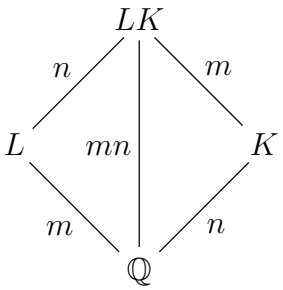
$$\operatorname{disc}(\alpha) = \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right|^2 \operatorname{disc}(\mathscr{O}_K).$$

Definizione 2.2.2. $K = \mathbb{Q}(\alpha)$, α intero. Si definisce **indice di** α, $\operatorname{ind}(\alpha) := \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right|$.

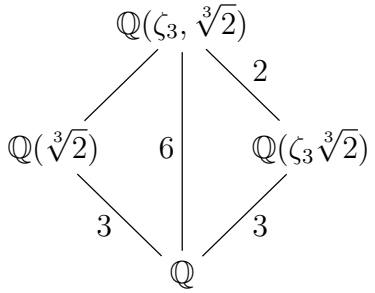
Osservazione. Se $\operatorname{disc}(\alpha)$ é libero da quadrati, allora $\operatorname{ind}(\alpha) = 1$, cioé $\mathbb{Z}[\alpha] = \mathscr{O}_K$.
Osservazione. $\operatorname{ind}(\alpha)$ é finito, dunque gli elementi di $\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}$ hanno ordine divisore di $\operatorname{ind}(\alpha)$; in altre parole, $\operatorname{ind}(\alpha) \cdot \frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]} = \overline{0}$, cioé $\operatorname{ind}(\alpha) \cdot \mathscr{O}_K \subseteq \mathbb{Z}[\alpha]$.
Dunque:

$$\mathscr{O}_K \subseteq \frac{1}{\operatorname{ind}(\alpha)} \langle 1, \alpha, \dots, \alpha^{n-1} \rangle_{\mathbb{Z}}.$$

Osservazione. Sia dato il diagramma di estensioni di campi:



Allora segue che $L \cap K = \mathbb{Q}$, poiché se si avesse un'intersezione piú grande, si avrebbe che $[LK : K] < m$. (Il viceversa é falso; un controesempio puó essere:



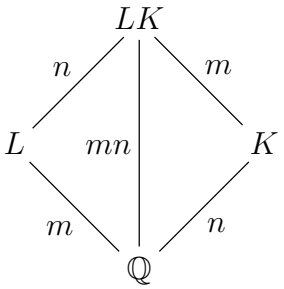
in quanto $\mathbb{Q}(\zeta_3\sqrt[3]{2}) \cap \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}$.) Supponiamo che $\mathscr{B}_L = \{v_1, \dots, v_m\}$ sia una $\mathbb{Q}$-base di L e che $\mathscr{B}_K = \{w_1, \dots, w_n\}$ sia una $\mathbb{Q}$-base di K. Allora $\mathscr{B}_L$ é una K-base di LK.

Dimostrazione. $L = \langle v_1, \dots, v_m\rangle_{\mathbb{Q}} \Rightarrow L \subseteq \langle v_1, \dots, v_m\rangle_K \subseteq LK$.
$K \subseteq \langle v_1, \dots, v_m\rangle_K$, poiché $1 \in \langle v_1, \dots, v_m\rangle_{\mathbb{Q}} \subseteq \langle v_1, \dots, v_m\rangle_K$; inoltre $\langle v_1, \dots, v_m\rangle_K$ é un anello poiché $\forall i, j$, $v_i + v_j, v_i v_j \in \langle v_1, \dots, v_m\rangle_{\mathbb{Q}} \subseteq \langle v_1, \dots, v_m\rangle_K$.
Ma l'anello $\langle v_1, \dots, v_m\rangle_K$ contiene L e K, quindi contiene LK, cioé $\langle v_1, \dots, v_m\rangle_K \supseteq LK$. □

Di conseguenza $\mathscr{B}_{LK} = \{v_i w_j\}_{\substack{1\le i\le m\\ 1\le j\le n}}$ é una $\mathbb{Q}$-base di LK.
Inoltre, se $\mathscr{B}_L$ e $\mathscr{B}_K$ sono basi intere, $\mathscr{B}_{LK}$ é base intera di $\mathscr{O}_L\mathscr{O}_K \subseteq \mathscr{O}_{LK}$ (in generale $\mathscr{O}_L\mathscr{O}_K \subsetneq \mathscr{O}_{LK}$; si veda l'esempio seguente).
Infatti gli elementi di $\mathscr{B}_{LK}$ sono indipendenti e generano, in quanto $\mathscr{O}_L\mathscr{O}_K = \left\{\sum \gamma_a\rho_b | \gamma_a \in \mathscr{O}_L, \rho_b \in \mathscr{O}_K\right\}$.

Esempio. Nelle notazioni precedenti, $\mathscr{B}_L$ e $\mathscr{B}_K$ basi intere $\not\Rightarrow \mathscr{B}_{LK}$ base intera.
Sia $L = \mathbb{Q}(\sqrt{3})$, $K = \mathbb{Q}(\sqrt{7})$. $LK = \mathbb{Q}(\sqrt{3})\mathbb{Q}(\sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$, poiché le immersioni di $LK/\mathbb{Q}$ mappano $\sqrt{3} + \sqrt{7} \to \pm\sqrt{3} \pm \sqrt{7}$, che sono distinti e dunque $\sqrt{3} + \sqrt{7}$ ha grado 4 su $\mathbb{Q}$.
$3, 7 \equiv 3\ (4)$, dunque $\mathscr{O}_L = \mathbb{Z}[\sqrt{3}]$ e $\mathscr{O}_K = \mathbb{Z}[\sqrt{7}]$; ma allora $\mathscr{O}_L\mathscr{O}_K = \mathbb{Z}[\sqrt{3}]\mathbb{Z}[\sqrt{7}] \subsetneq \mathscr{O}_{LK}$, in quanto $\frac{\sqrt{3}+\sqrt{7}}{2} \notin \mathscr{O}_L\mathscr{O}_K$, ma $\frac{\sqrt{3}+\sqrt{7}}{2} \in \mathscr{O}_{LK}$ perché $x^4 - 5x^2 + 1$ é il suo polinomio minimo.

Teorema 2.2.5. *Consideriamo il diagramma di estensioni di campi:*



Sia $\{\alpha_i\}$ una $\mathbb{Z}$-base di $\mathscr{O}_K$ e sia $\{\beta_j\}$ una $\mathbb{Z}$-base di $\mathscr{O}_L$.
Detto $d = (\mathrm{disc}(K), \mathrm{disc}(L))$, si ha che $\mathscr{O}_{LK} \subseteq \frac{1}{d}\mathscr{O}_L\mathscr{O}_K$.

Dimostrazione. Per le osservazioni precedenti, $\{\alpha_i\beta_j\}$ é una $\mathbb{Q}$-base di LK, dunque $\alpha \in \mathscr{O}_{LK} \Rightarrow \alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j$, con $m_{ij} \in \mathbb{Z}$ e r piú piccolo possibile. In particolare, $\gcd(r, \gcd(m_{ij})) = 1$.
Se dimostro che $r|d$ ho la tesi. Equivalentemente, posso dimostrare che $r|d_K := \mathrm{disc}(K)$ e $r|d_L := \mathrm{disc}(L)$.
Poniamo $x_i = \sum_j \frac{m_{ij}}{r}\beta_j \in L$; allora $\alpha = \sum_i x_i\alpha_i$.
Evidentemente $r|d_K \iff d_K x_i \in \mathscr{O}_L$, poiché r é stato preso minimo.
Siano $\sigma_1, \dots, \sigma_n$ le immersioni di $K/\mathbb{Q}$ e $\widetilde{\sigma_1}, \dots, \widetilde{\sigma_n}$ le immersioni di LK/L. $\widetilde{\sigma}_{i|K} \neq \widetilde{\sigma}_{j|K}\ \forall i \neq j$, in quanto se coincidessero su K, coinciderebbero su LK perché $\widetilde{\sigma}_{i|L} = id\ \forall i$.
Dunque rinumero le $\widetilde{\sigma}_i$ in modo che $\widetilde{\sigma}_{i|K} = \sigma_i\ \forall i$.
$\widetilde{\sigma}_j(\alpha) = \sum_i x_i\widetilde{\sigma}_j(\alpha_i) = \sum_i x_i\sigma_j(\alpha_i)\ \forall j$, quindi ho un sistema di n equazioni in n incognite associato alla matrice

$$M = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix}$$

del discriminante, perció $\det(M) = \delta$, con $\delta^2 = d_K$.
Risolvendo con Cramer, $x_i = \frac{\det(M_i)}{\delta}$, con M_i a entrate intere, poiché gli α_i sono interi e i coniugati di elementi interi sono interi, dunque $x_i = \frac{\beta_i}{\delta}$, $\beta_i, \delta \in \mathbb{A}$.
Ora $d_K x_i = \delta^2 x_i = \delta\beta_i \in \mathbb{A}$, ma $d_K x_i \in L \Rightarrow d_K x_i \in \mathscr{O}_L$.
Mostrare che $r|d_L$ é del tutto analogo. □

Teorema 2.2.6. $\mathbb{Q}(\zeta_m) \cap \mathbb{A} = \mathbb{Z}[\zeta_m]$

Dimostrazione. Poniamo $\zeta = \zeta_m$, $K = \mathbb{Q}(\zeta)$.
Trattiamo prima il caso $m = p^l$.
Innanzitutto notiamo che $\mathrm{N}_{K/\mathbb{Q}}(1-\zeta) = \prod_{(k,p)=1}(1-\zeta^k) = p$; infatti:

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

dunque $\prod_{(k,p)=1}(1-\zeta^k) = \mu_\zeta(1) = p$.
Visto che $\mathscr{O}_K \supseteq \mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, lavoriamo con quest'ultima; vorremmo dimostrare che $\mathscr{O}_K \subseteq \mathbb{Z}[1-\zeta]$. Poniamo $n = \phi(p^l)$.
$d = \mathrm{disc}(1-\zeta) = \mathrm{disc}(\zeta) = p^t$, poiché basi intere dello stesso $\mathbb{Z}$-modulo hanno lo stesso discriminante; sappiamo che $\mathbb{Z}[1-\zeta] \subseteq \mathscr{O}_K \subseteq \frac{1}{d}\mathbb{Z}[1-\zeta]$ (in quanto $\mathrm{ind}(\zeta)|\,\mathrm{disc}(\zeta)$), dunque $\forall \alpha \in \mathscr{O}_K$, $\alpha = \frac{m_1+m_2(1-\zeta)+\ldots+m_n(1-\zeta)^{n-1}}{d}$, con $m_i \in \mathbb{Z}$.
Se per assurdo $\mathscr{O}_K \supsetneqq \mathbb{Z}[1-\zeta] \Rightarrow \exists \alpha \in \mathscr{O}_K$, $\alpha \notin \mathbb{Z}[1-\zeta]$, cioé nella scrittura precedente di α, la massima potenza di p che divide il numeratore é $s < t$.
Dunque moltiplico α per $p^{\gamma-1}$, dove $\gamma = t - s$ e gli tolgo gli addendi che stanno in $\mathbb{Z}[1-\zeta]$, ottenendo $\beta = \frac{m_i(1-\zeta)^{i-1}+\ldots+m_n(1-\zeta)^{n-1}}{p}$ (dove gli m_j non sono necessariamente uguali a quelli di α).
Per costruzione, $\beta \in \mathscr{O}_K$, ma $\beta \notin \mathbb{Z}[1-\zeta]$; in particolare $p \nmid m_i$.
Sicuramente $\forall k \geq 1$ $(1-\zeta)|(1-\zeta^k)$ in $\mathbb{Z}[1-\zeta]$, e quindi per l'osservazione iniziale:

$$p = (1-\zeta)^n \prod_{(k,p)=1} \frac{1-\zeta^k}{1-\zeta} \Rightarrow \frac{p}{(1-\zeta)^n} \in \mathbb{Z}[1-\zeta].$$

Poiché $i \leq n$, $\frac{p}{(1-\zeta)^i} \in \mathbb{Z}[1-\zeta]$, dunque:

$$\mathscr{O}_K \ni \beta\frac{p}{(1-\zeta)^i} = \frac{m_i}{1-\zeta} + \underbrace{r(1-\zeta)}_{\in\mathbb{Z}[1-\zeta]},$$

da cui $\frac{m_i}{1-\zeta} \in \mathscr{O}_K$.
Ma allora:

$$\mathbb{Z} \ni \mathrm{N}_{K/\mathbb{Q}}\Big(\frac{m_i}{1-\zeta}\Big) = \frac{\mathrm{N}_{K/\mathbb{Q}}(m_i)}{\mathrm{N}_{K/\mathbb{Q}}(1-\zeta)} = \frac{m_i^n}{p},$$

assurdo, perché $p \nmid m_i$.
Passiamo ora al caso generale: procediamo per induzione II su m, essendo il caso $m = 2$ del tutto ovvio.
Se $m > 2$, $m = \begin{cases} p^l & \text{giá visto} \\ m_1 m_2 & \text{con } (m_1, m_2) = 1 \end{cases}$.
Se $K_i = \mathbb{Q}(\zeta_{m_i})$, $i = 1, 2$, e $K = \mathbb{Q}(\zeta_m)$, allora $\mathscr{O}_{K_i} = \mathbb{Z}[\zeta_{m_i}]$, $i = 1, 2$ per ipotesi induttiva.
Se $d_i = \mathrm{disc}(K_i)$, $i = 1, 2$, $d = (d_1, d_2)$, allora $\mathscr{O}_{K_1}\mathscr{O}_{K_2} \subseteq \mathscr{O}_K \subseteq \frac{1}{d}\mathscr{O}_{K_1}\mathscr{O}_{K_2}$; osservo che $d = 1$, infatti $d_i | m_i^{\phi(m_i)}$ e $(m_1, m_2) = 1$.
Ma allora $\mathscr{O}_K = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}] = \mathbb{Z}[\zeta_m]$ (l'ultima uguaglianza si dimostra con Bezout in analogia a $\mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2}) = \mathbb{Q}(\zeta_m)$). □

Enunciamo il seguente teorema senza dimostrazione, che ci potrá essere utile:

Teorema 2.2.7. *$K = \mathbb{Q}(\alpha)$, α intero. Allora esiste una base intera di K della forma $\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\}$, dove $f_i(x) \in \mathbb{Z}[x]$ monico, $\deg(f_i) = i$ $\forall i$, con $d_1|\ldots|d_{n-1}$ tali che $d_1 \cdot \ldots \cdot d_{n-1} = [\mathscr{O}_K : \mathbb{Z}[\alpha]]$.*
Inoltre i d_i sono univocamente determinati.

Il seguente risultato, di capitale importanza nella teoria dei numeri globale, viene enunciato senza dimostrazione, che non puó essere affrontata a questo livello:

Teorema 2.2.8 (di Kronecker-Weber)**.** *Ogni estensione abeliana di $\mathbb{Q}$ é contenuta in un'estensione ciclotomica.*

Affrontiamo peró come esercizio un caso molto particolare del teorema di Kronecker-Weber, quello delle estensioni quadratiche:

Esercizio. *Ogni estensione quadratica di $\mathbb{Q}$ é contenuta in un'estensione ciclotomica.*

Dimostrazione. $K = \mathbb{Q}(\sqrt{m})$, con m libero da quadrati.
Dimostro che $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_d)$, dove $d = \mathrm{disc}(\mathbb{Q}(\sqrt{m}))$, cioé $d = \begin{cases} 4m & \text{se } m \equiv 2,3 \quad (4) \\ m & \text{se } m \equiv 1 \quad (4) \end{cases}$.
Vediamo innanzitutto il caso $m = p$ primo.
Per il teorema precedente, $\{1, \zeta_p, \dots, \zeta_p^{p-1}\}$ é una base intera di K, ma $\sqrt{\pm p^{p-2}} = \sqrt{\mathrm{disc}(\zeta_p)} \in K$, da cui $\sqrt{\pm p} \in K$ se $p \equiv \pm 1$ (4).
Passiamo ora al caso generale: notiamo che, se $p_i \equiv 1$ (4), $q_j \equiv -1$ (4):

$$m = \begin{cases} \pm p_1 \cdot \ldots \cdot p_a \cdot q_1 \cdot \ldots \cdot q_b & \text{se } m \equiv 1,3 \quad (4) \\ \pm 2p_1 \cdot \ldots \cdot p_a \cdot q_1 \cdot \ldots \cdot q_b & \text{se } m \equiv 2 \quad (4) \end{cases}.$$

Se $m \equiv 1$ (4), voglio vedere che $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_m)$.
$m = \pm p_1 \cdot \ldots \cdot p_a \cdot q_1 \cdot \ldots \cdot q_b = p_1 \cdot \ldots \cdot p_a \cdot (-q_1) \cdot \ldots \cdot (-q_b)$, poiché b pari $\iff m > 0$, dunque $\sqrt{m} = \sqrt{p_1} \cdot \ldots \cdot \sqrt{p_a} \cdot \sqrt{-q_1} \cdot \ldots \cdot \sqrt{-q_b} \in \mathbb{Q}(\zeta_m)$, poiché $\sqrt{p_i} \in \mathbb{Q}(\zeta_{p_i}) \subseteq \mathbb{Q}(\zeta_m)$ e $\sqrt{-q_j} \in \mathbb{Q}(\zeta_{q_j}) \subseteq \mathbb{Q}(\zeta_m)$.
Se $m \equiv 3$ (4), voglio vedere che $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{4m})$.
Ma $i \in \mathbb{Q}(\zeta_{4m})$ e $\sqrt{-m} = i\sqrt{m} \in \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{4m})$, quindi $\sqrt{m} = -i\sqrt{-m} \in \mathbb{Q}(\zeta_{4m})$.
Se $m \equiv 2$ (4), voglio vedere che $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{4m})$.
$8|4m$, quindi $i, \sqrt{2} \in \mathbb{Q}(\zeta_{4m})$; ragionando come nel caso precedente, ci si riconduce al primo caso e si ottiene la tesi.
(Si puó notare che, se $d < \mathrm{disc}(\mathbb{Q}(\zeta_m))$, in generale non é vero che $\sqrt{m} \in \mathbb{Q}(\zeta_d)$.) □

Esercizio. $\mathbb{Q}(\zeta_n + \overline{\zeta_n}) \cap \mathbb{A} = \mathbb{Z}[\zeta_n + \overline{\zeta_n}]$.

Dimostrazione. Scriveremo per semplicitá $\zeta = \zeta_n$.

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \Big| \, 2 \\ \mathbb{Q}(\zeta + \overline{\zeta}) = F \\ \Big| \, \frac{\phi(n)}{2} \\ \mathbb{Q} \end{array}$$

$[\mathbb{Q}(\zeta) : F] = 2$, infatti $[\mathbb{Q}(\zeta) : F] \geq 2$ in quanto $F \subseteq \mathbb{R}$, e $[\mathbb{Q}(\zeta) : F] \leq 2$ in quanto ζ si annulla in $(x-\zeta)(x-\overline{\zeta}) = x^2 - (\zeta+\overline{\zeta})x + 1 \in F[x]$.

$\left\{1, \zeta + \overline{\zeta}, \dots, (\zeta + \overline{\zeta})^{\frac{\phi(n)}{2}-1}\right\}$ é una $\mathbb{Q}$-base di F (si vede che sono indipendenti sviluppando le potenze e usando che $\overline{\zeta} = \zeta^{-1}$).
Se per assurdo $\mathscr{O}_F \supsetneq \mathbb{Z}[\zeta + \overline{\zeta}]$, $\exists \alpha \in \mathscr{O}_F \backslash \mathbb{Z}[\zeta + \overline{\zeta}]$, $\alpha = a_0 + a_1(\zeta + \overline{\zeta}) + \ldots + a_N(\zeta + \overline{\zeta})^N$, con $N \leq \frac{\phi(n)}{2} - 1$.
Scelgo α in modo che $a_N \notin \mathbb{Z}$; ma allora, sfruttando il fatto che $\overline{\zeta} = \zeta^{-1}$, si ha:

$$\mathscr{O}_F \ni \beta = \zeta^N \alpha = a_N + \underbrace{r(\zeta)}_{\in \mathbb{Q}[\zeta]} + a_N \zeta^{2N}.$$

$\beta \in \mathscr{O}_F$ é scritto in termini della $\mathbb{Z}$-base $\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\}$ di $\mathbb{Z}[\zeta]$, poiché $2N \leq \phi(n) - 2 \leq \phi(n) - 1$, dunque i coefficienti stanno in $\mathbb{Z}$, assurdo. □

Proposizione 2.2.9. *$K = \mathbb{Q}(\alpha)$, α intero, $\mu_\alpha(x) \in \mathbb{Z}[x]$ polinomio minimo di α.*
Supponiamo che μ_α sia p-Eisenstein (cioé di Eisenstein rispetto al primo p); allora $p \nmid \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right| = \operatorname{ind}_K(\alpha)$.

Dimostrazione. $\mu_\alpha(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, cioé $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$.
Inoltre $p|a_i \quad \forall i$, ma $p^2 \nmid a_n = \mathrm{N}_{K/\mathbb{Q}}(\alpha)$; allora $\frac{\alpha^n}{p} \in \mathbb{Z}[\alpha] \subseteq \mathscr{O}_K$.
Se per assurdo $p|\operatorname{ind}_K(\alpha) \Rightarrow \exists \xi \in \frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}$ di ordine p, cioé $\exists \xi \in \mathscr{O}_K \backslash \mathbb{Z}[\alpha]$ tale che $p\xi \in \mathbb{Z}[\alpha]$.
$\xi = \frac{1}{p}(b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1})$, con non tutti i $b_i \equiv 0 \quad (p)$ (altrimenti $\xi \in \mathbb{Z}[\alpha]$).
A meno di sottrarre elementi $\in \mathbb{Z}[\alpha]$, scrivo $\xi = \frac{b_j\alpha^j + \ldots + b_{n-1}\alpha^{n-1}}{p}$, con $p \nmid b_j$ (cioé j é il primo indice tale che $p \nmid b_j$).
Sia $\beta = \frac{b_j\alpha^{n-1}}{p} = \alpha^{n-1-j}\xi - \frac{\alpha^n}{p}\underbrace{r(\alpha)}_{\in\mathbb{Z}[\alpha]} \in \mathscr{O}_K$; $p\beta \in \mathbb{Z}[\alpha]$.
$\mathrm{N}_{K/\mathbb{Q}}(p\beta) = p^n \mathrm{N}_{K/\mathbb{Q}}(\beta)$ e $\mathrm{N}_{K/\mathbb{Q}}(p\beta) = \mathrm{N}_{K/\mathbb{Q}}(b_j\alpha^{n-1}) = b_j^n \mathrm{N}_{K/\mathbb{Q}}(\alpha)^{n-1}$, ma $\mathrm{N}_{K/\mathbb{Q}}(\beta)$ é intero, dunque $b_j^n \mathrm{N}(\alpha)^{n-1} \equiv 0 \quad (p^n)$.
Ma $b_j \in (\mathbb{Z}/p\mathbb{Z})^*$, quindi $\mathrm{N}(\alpha)^{n-1} \equiv 0 \quad (p^n)$, cioé $p^n|\mathrm{N}(\alpha)^{n-1}$, assurdo perché $p^2 \nmid a_n$. □

<u>*Osservazione*</u>. La precedente proposizione é molto utile, poiché, sapendo che $\operatorname{disc}(\alpha) = \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right|^2 \operatorname{disc}(K)$, permette di decidere quali primi di $\operatorname{disc}(\alpha)$ passano nella fattorizzazione di $\operatorname{disc}(K)$.

Esercizio (Marcus, n° 41, pag. 49)**.** *$K = \mathbb{Q}(\sqrt[3]{m})$, m libero da cubi, $m = ab^2$, $(a, b) = 1$.*
Posso supporre che $3|m \Rightarrow 3|a$ a meno di scambiare m con $m' = a^2b$ (e $\mathbb{Q}(\sqrt[3]{m}) = \mathbb{Q}(\sqrt[3]{m'})$).
Allora:

$$\operatorname{disc}(K) = \begin{cases} -3a^2b^2 & \text{se } m \equiv \pm 1 \quad (9) \\ -27a^2b^2 & \text{se } 3|m \vee m \not\equiv \pm 1 \quad (9) \end{cases}$$

Dimostrazione. Sia α tale che $\alpha^3 = m$.
$\operatorname{disc}(\alpha) = -\mathrm{N}_{K/\mathbb{Q}}(\mu'(\alpha)) = -\mathrm{N}_{K/\mathbb{Q}}(3\alpha^2) = -3^3m^2 = -27a^2b^4$. $\forall p|a$, $x^3 - ab^2$ é p-Eisenstein $\Rightarrow p \nmid \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right|$, cioé $a^2|\operatorname{disc}(K)$.
Inoltre $3|\operatorname{disc}(K)$, poiché il fattore $\left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right|^2$ contiene solo quadrati.
Analogamente a prima, se al posto di m uso m', e $\beta^3 = m' = a^2b$ (cioé $\beta = \frac{\alpha^2}{b}$), $\operatorname{disc}(\beta) = -27a^4b^2$ e il polinomio $x^3 - a^2b$ é p-Eisenstein $\forall p|b$, dunque $b^2|\operatorname{disc}(K)$.
Riassumendo, si ha che $\operatorname{disc}(K) = -3a^2b^2$ o $\operatorname{disc}(K) = -27a^2b^2$.
Se $3|m \Rightarrow 3|a \Rightarrow 3 \nmid \left|\frac{\mathscr{O}_K}{\mathbb{Z}[\alpha]}\right| \Rightarrow \operatorname{disc}(K) = -27a^2b^2$ e $\{1, \alpha, \beta\}$ é una base intera, con $\beta = \frac{\alpha^2}{b}$, in quanto $\operatorname{disc}(1, \alpha, \beta) = \frac{1}{b^2}\operatorname{disc}(\alpha) = -27a^2b^2$.
Se invece $3 \nmid m$, e $m \not\equiv \pm 1 \quad (9)$, sia $\gamma = \alpha - m$; il polinomio minimo di γ, $\mu_\gamma(x) = \mu_\alpha(x+m) = (x+m)^3 - m = x^3 + 3x^2 + 3xm^2 + m^3 - m$ é 3-Eisenstein, dunque $\operatorname{disc}(K) = -27a^2b^2$.
Inoltre $\{1, \alpha, \beta\}$ é una base intera.
Se $m \equiv \pm 1 \quad (9)$, sia $\delta = \frac{1 \pm \alpha + \alpha^2}{3}$; $\delta \in \mathscr{O}_K$, poiché $\delta^2 = \frac{1+\alpha^2+m\alpha\pm 2\alpha \pm 2m + 2\alpha^2}{9} = \frac{(1\pm 2m) + (\pm 2 + m)\alpha + 3\alpha^2}{9} = 3\delta + 2k \pm k\alpha$, dove $m = \pm 1 + 9k$, dunque $\delta^2 - 3\delta$ é un intero e perció δ é un intero.
Le immersioni di $K/\mathbb{Q}$ sono $\alpha \to \alpha\zeta_3^e$, $e = 0, 1, 2$, quindi:

$$\operatorname{disc}(1, \beta, \delta) = \det \begin{pmatrix} 1 & \beta & \frac{1+\alpha+\alpha^2}{3} \\ 1 & \zeta_3^2\beta & \frac{1+\alpha\zeta_3+\alpha^2\zeta_3^2}{3} \\ 1 & \zeta^3\beta & \frac{1+\alpha\zeta_3^2+\alpha^2\zeta_3}{3} \end{pmatrix}^2 = \frac{1}{9}\det \begin{pmatrix} 1 & \beta & 1+\alpha+\alpha^2 \\ 0 & (\zeta_3^2-1)\beta & (\zeta_3-1)\alpha + (\zeta_3^2-1)\alpha^2 \\ 0 & (\zeta_3-1)\beta & (\zeta_3^2-1)\alpha + (\zeta_3-1)\alpha^2 \end{pmatrix}^2 =$$

$$\frac{1}{9}\big((\zeta_3^2-1)^2\alpha\beta - (\zeta_3-1)^2\alpha\beta\big)^2 = \Big(\frac{m}{b}\zeta_3(1-\zeta_3)\Big)^2 = -3a^2b^2,$$

da cui necessariamente $\{1, \beta, \delta\}$ é una base intera e $\text{disc}(K) = -3a^2b^2$. In alternativa si poteva calcolare $\text{disc}(1, \beta, \delta)$ come $\det(M)^2 \text{disc}(\alpha)$ con M matrice del cambiamento di base:

$$M = \begin{pmatrix} 1 & 0 & \frac{1}{3} \\ 0 & 0 & \pm\frac{1}{3} \\ 0 & \frac{1}{b} & \frac{1}{3} \end{pmatrix},$$

da cui $\det(M)^2 = \frac{1}{9b^2} \Rightarrow \text{disc}(1, \beta, \delta) = -3a^2b^2$. □

Esercizio (Criterio di Stickelberger)**.** *K campo di numeri. Allora* $\text{disc}(K) \equiv 0, 1 \pmod 4$.

Dimostrazione. Sia $\{\alpha_1, \dots, \alpha_n\}$ una base intera di K e siano $\sigma_1, \dots, \sigma_n$ le immersioni di $K/\mathbb{Q}$. Sappiamo che $\text{disc}(K) = \det(\sigma_i(\alpha_j))^2$.

$$\det(\sigma_i(\alpha_j))^2 = \sum_{\pi \in \mathcal{A}_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(a_i) - \sum_{\pi \in \mathcal{S}_n \setminus \mathcal{A}_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(a_i) := P - N.$$

Visto che $(P-N)^2 = (P+N)^2 - 4PN$, per avere la tesi mi basta mostrare che $P+N, PN \in \mathbb{Z}$. Sicuramente $P + N, PN \in \mathbb{A}$. Vediamo che stanno in $\mathbb{Q}$.
Sia $L = \widetilde{K}$ la chiusura normale. Mi basta vedere che $\phi(P + N) = P + N$ e $\phi(PN) = PN$ $\forall \phi \in \text{Gal}(L/\mathbb{Q})$. Sia dunque $\phi \in \text{Gal}(L/\mathbb{Q})$.
$\sigma_i(K) \subseteq L$ $\forall i$, poiché σ_i si estende a $\widetilde{\sigma}_i$ in L tale che $\widetilde{\sigma}_i(L) = L$; ma allora $\forall i$, $\phi \circ \sigma_i : K \hookrightarrow \mathbb{C}$ é un'immersione di $K/\mathbb{Q}$, diciamo $\sigma_{\tau(i)}$. $\tau : \{1, \dots, n\} \to \{1, \dots, n\}$ é dunque una permutazione. Distinguiamo due casi:

$\tau \in \mathcal{A}_n$: $\tau(\mathcal{A}_n) = \mathcal{A}_n$ e $\tau(\mathcal{S}_n \setminus \mathcal{A}_n) = \mathcal{S}_n \setminus \mathcal{A}_n$, dunque:

$$\phi(P) = \phi\left(\sum_{\pi \in \mathcal{A}_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(a_i)\right) = \sum_{\pi \in \mathcal{A}_n} \prod_{i=1}^{n} \underbrace{\phi \circ \sigma_{\pi(i)}}_{=\sigma_{\tau\circ\pi(i)}}(a_i) = \sum_{\pi \in \tau(\mathcal{A}_n) = \mathcal{A}_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(a_i) = P.$$

Analogamente $\phi(N) = N$.

$\tau \notin \mathcal{A}_n$: Il caso é sostanzialmente analogo al precedente perché $\tau(\mathcal{A}_n) = \mathcal{S}_n \setminus \mathcal{A}_n$ e $\tau(\mathcal{S}_n \setminus \mathcal{A}_n) = \mathcal{A}_n$, quindi con calcoli simili viene che $\phi(P) = N$ e $\phi(N) = P$.

□

3 Fattorizzazione di ideali primi in estensioni di campi

3.1 Domini di Dedekind

Definizione 3.1.1. M A-modulo si dice **noetheriano** se verifica le seguenti condizioni equivalenti:

1. Ogni famiglia non vuota di sottomoduli di M ammette un elemento massimale
2. Ogni catena ascendente di sottomoduli di M é stazionaria
3. Ogni sottomodulo di M é finitamente generato.

Definizione 3.1.2. A anello si dice **noetheriano** se lo é come A-modulo.

Esempio. $A = K[x_1, x_2, \ldots]$ non é un anello noetheriano poiché $(x_1, x_2, \ldots)$ non é finitamente generato.

Definizione 3.1.3. Un **dominio di Dedekind** R é un dominio d'integritá tale che:

1. É noetheriano
2. Ogni ideale primo non nullo é massimale (ed esiste un ideale primo non nullo); in altre parole $\dim(R) = 1$
3. É integralmente chiuso nel suo campo delle frazioni.

Proposizione 3.1.1. *R PID $\Rightarrow$ R dominio di Dedekind.*

Dimostrazione. Sicuramente é noetheriano, ogni ideale primo é massimale e PID $\Rightarrow$ UFD $\Rightarrow$ integralmente chiuso. □

Lemma 3.1.2. $(0) \neq I \subseteq \mathscr{O}_K \Rightarrow \left|\frac{\mathscr{O}_K}{I}\right| < +\infty$. *Dunque ogni ideale di $\mathscr{O}_K$ é uno $\mathbb{Z}$-modulo libero di rango n.*

Dimostrazione. $0 \neq \alpha \in I$. $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha\beta$ per un certo $\beta \in \mathbb{A}$ (poiché é prodotto di coniugati di un elemento algebrico).
$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = m \in \mathbb{Z} \Rightarrow \beta = \frac{m}{\alpha} \in K \Rightarrow \beta \in \mathbb{A} \cap K = \mathscr{O}_K \Rightarrow m = \alpha\beta \in I$.
Allora $(m) \subseteq I \subseteq \mathscr{O}_K$ e $\left|\frac{\mathscr{O}_K}{(m)}\right| = m^n$, poiché $\{x_1, \ldots, x_n\}$ $\mathbb{Z}$-base di $\mathscr{O}_K \Rightarrow \{mx_1, \ldots, mx_n\}$ $\mathbb{Z}$-base di (m).
Dunque per la formula delle torri $[\mathscr{O}_K : I][I : (m)] = [\mathscr{O}_K : (m)] = m^n$, da cui $[\mathscr{O}_K : I] | m^n$. □

Teorema 3.1.3. $[K : \mathbb{Q}] = n \Rightarrow \mathscr{O}_K = K \cap \mathbb{A}$ *é un dominio di Dedekind.*

Dimostrazione. Ovviamente é un dominio in quanto sottoinsieme di un campo. Dimostriamo le tre condizioni:

1. Sia $I \subseteq \mathscr{O}_K$ ideale. $\mathscr{O}_K$ é uno $\mathbb{Z}$-modulo libero di rango n, $\mathbb{Z}$ é PID, quindi I é uno $\mathbb{Z}$-modulo libero di rango $\leq n$, cioé $I = \langle x_1, \ldots, x_k \rangle_{\mathbb{Z}}$, cioé $I = (x_1, \ldots, x_k)$.
2. Sia $(0) \neq P \subset \mathscr{O}_K$ primo. $\frac{\mathscr{O}_K}{P}$ é un dominio, ma per il lemma é finito, dunque é un campo.
3. Giá visto.

□

Lemma 3.1.4. *A dominio noetheriano. Ogni ideale non nullo di A contiene un prodotto di ideale primi.*

Dimostrazione. Sia $\mathcal{F} = \{(0) \neq I \subsetneq A | I \text{ non contiene un prodotto di primi}\}$. Se per assurdo $\mathcal{F} \neq \emptyset$, $\exists J \subset \mathcal{F}$ elemento massimale per noetherianitá.
J non é primo (altrimenti conterrebbe se stesso primo), quindi $\exists x, y \in A$ tali che $xy \in J$ ma $x, y \notin J$.
$J + (x), J + (y) \supsetneq J \Rightarrow J + (x), J + (y) \notin \mathcal{F} \Rightarrow J + (x) \supseteq P_1 \cdot \ldots \cdot P_r$ e $J + (y) \supseteq Q_1 \cdot \ldots \cdot Q_t$ ideali primi.
Ma questo é assurdo, poiché $J = J + (xy) \supseteq (J + (x))(J + (y)) \supseteq P_1 \cdot \ldots \cdot P_r \cdot Q_1 \cdot \ldots \cdot Q_t$. □

Definizione 3.1.4. A dominio, $K = K(A)$ campo delle frazioni. Un A-modulo $I \subseteq K$ si dice **ideale frazionario** se $\exists 0 \neq d \in A$ tale che $dI \subseteq A$ (o equivalentemente $I \subseteq \frac{1}{d}A$).

Proposizione 3.1.5. *$I \subseteq K$ finitamente generato come A-modulo $\Rightarrow I$ é ideale frazionario.*

Dimostrazione. Se $I = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle_A$, $d = b_1 \cdot \ldots \cdot b_n$ mi dá la tesi. □

Proposizione 3.1.6. *A noetheriano, I ideale frazionario di $A \Rightarrow I$ é finitamente generato.*

Dimostrazione. $\exists d$ per cui dI é finitamente generato per noetherianitá da $\{x_1, \ldots, x_k\}$; ma allora $I = \langle \frac{x_1}{d}, \ldots, \frac{x_k}{d} \rangle_A$. □

<u>*Osservazione*</u>. I, J ideali frazionari di $A \Rightarrow IJ$ é ideale frazionario di A.
Infatti $aI \subseteq A$, $bJ \subseteq A \Rightarrow abIJ \subseteq A$.

Definizione 3.1.5. A dominio, $K = K(A)$, $I \neq (0)$ ideale frazionario. Definiamo **inverso** di I l'insieme $I^{-1} = \{x \in K | xI \subseteq A\}$.

Lemma 3.1.7. *I^{-1} é un A-modulo.*

Dimostrazione. Se $x, y \in I^{-1}$ e $\lambda \in A$, evidentemente $x + y \in I^{-1}$ e $\lambda x \in I^{-1}$. □

Proposizione 3.1.8.
- $II^{-1} \subseteq A$
- *I^{-1} é un ideale frazionario di A*
- *I, J ideali frazionari di A e $IJ = A \Rightarrow J = I^{-1}$ e $I = J^{-1}$.*

Dimostrazione.
- Ovvio
- I^{-1} é un A-modulo e se $0 \neq a \in I$, $aI^{-1} \subseteq A$.
- Se $IJ = A$, sicuramente $J \subseteq I^{-1}$. Ma $A = IJ \subseteq II^{-1} \subseteq A$, dunque ci sono uguaglianze e $IJ = II^{-1}$, da cui $I^{-1} = J$ (poiché $I^{-1}IJ = I^{-1}II^{-1}$ e $II^{-1} = A$).

□

Definizione 3.1.6. $I \neq (0)$ ideale frazionario si dice **invertibile** se $II^{-1} = A$.

Teorema 3.1.9. *R dominio di Dedekind. Allora gli ideali massimali di R sono invertibili.*

Dimostrazione. $M \subset R$ massimale. $MM^{-1} \subseteq R$. Sicuramente $M^{-1} \supseteq R$. Ma allora $R \supseteq MM^{-1} \supseteq MR = M$, dunque per massimalitá $MM^{-1} = R \vee MM^{-1} = M$.
Se per assurdo $MM^{-1} = M$, dico che $M^{-1} = R$.
Un'inclusione é giá stata vista, dunque vediamo che $M^{-1} \subseteq R$; per fare questo ci basta mostrare che ogni $x \in M^{-1}$ é intero su R, poiché R é integralmente chiuso.
$x \in M^{-1} \Rightarrow xM \in MM^{-1} = M, \ldots, x^nM \in M \ \forall n \in \mathbb{N}$; inoltre se $0 \neq d \in M$, $dx^n \in MM^{-1} = M \ \forall n$, quindi $R[x] \subseteq d^{-1}R$ (poiché $x^n \in d^{-1}M \subseteq d^{-1}R \ \forall n$ e $R \subseteq d^{-1}R$). Allora $R[x]$ é un R-modulo finitamente generato in quanto sottomodulo di un R-modulo noetheriano $d^{-1}R$, cioé x é intero su R.

Ci resta da vedere che $M^{-1} = R$ é un assurdo.
Se $0 \neq a \in M$, per il lemma, $0 \neq aR \supseteq P_1 \cdot \ldots \cdot P_r$ ideali primi; scelgo r minimo possibile.
$M \supseteq aR \supseteq P_1 \cdot \ldots \cdot P_r$, ma M é primo, quindi (per un risultato classico di algebra commutativa) contiene un P_i, diciamo P_1; ma i primi sono massimali in R, quindi $M = P_1$.
Se $I = P_2 \cdot \ldots \cdot P_r$, $aR \supseteq MI$, ma $aR \not\supseteq I$ per minimalitá di r, dunque $\exists \alpha \in I$ tale che $\alpha \notin aR$.
$a^{-1}\alpha \notin R$, ma $a^{-1} \underbrace{\alpha M}_{\subseteq aR} \subseteq a^{-1}aR = R$, cioé $a^{-1}\alpha \in M^{-1} = R$, assurdo. □

Definizione 3.1.7. *R dominio di Dedekind. Definiamo $\mathcal{F}(R) = \{I \neq (0)$ ideali frazionari di $R\}$.*

Osservazione. $(\mathcal{F}(R), \cdot)$ é un monoide.

Proposizione 3.1.10. *$P_1, \ldots, P_r$ ideali primi di R dominio di Dedekind, $e_1, \ldots, e_r \in \mathbb{Z}$.
Allora $I = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ é un ideale frazionario di R ed é invertibile con $I^{-1} = P_1^{-e_1} \cdot \ldots \cdot P_r^{-e_r}$.*

Dimostrazione. P_i frazionario $\Rightarrow P_i^{-1}$ frazionario, ma $\mathcal{F}$ é un monoide, dunque I é un ideale frazionario. Per giungere alla tesi basta osservare che:

$$II^{-1} = \prod_{i=1}^{r} P_i^{e_i} P_i^{-e_i} = \prod_{i=1}^{r} (P_i P_i^{-1})^{e_i} = R.$$

□

Teorema 3.1.11. *R dominio di Dedekind. Ogni ideale frazionario $(0) \neq I$ di R si scrive in modo unico come prodotto di ideali primi (cioé $I = P_1^{e_i} \cdot \ldots \cdot P_r^{e_r}$, $e_i \in \mathbb{Z}$).
Inoltre $I \subseteq R \iff e_i \geq 0 \ \forall i = 1, \ldots r$.*

Dimostrazione. Vediamo l'esistenza. Mi basta mostrare che la tesi vale per gli ideali interi; infatti se I é un ideale frazionario, $\exists d$ per cui $dI \subseteq R$, dunque $I = (d)^{-1}dI$, e sia (d) che dI sono ideali interi per cui vale la fattorizzazione. Considero $\mathcal{F} = \{(0) \neq I \subsetneq R | I$ non si fattorizza$\}$.
Se per assurdo $\mathcal{F} \neq \emptyset$, per noetherianitá avrei $J \in \mathcal{F}$ elemento massimale.
Sicuramente J non é massimale, altrimenti si fattorizzerebbe come se stesso. Allora $J \subsetneq P$ primo (cioé massimale).
$P^{-1} \supseteq R \Rightarrow J \subseteq P^{-1}J \subseteq PP^{-1} = R$; dico che $J \subsetneq JP^{-1}$.
Se si avesse $J = JP^{-1}$, $x \in P^{-1} \Rightarrow xJ \in J, \ldots, x^nJ \in J$; se $0 \neq d \in J$, $dx^n \in J \ \forall n$ e dunque come nella dimostrazione del teorema precedente, $R[x] \subseteq d^{-1}R$, cioé x é intero su R.
Quindi come prima si avrebbe $P^{-1} \subseteq R$, cioé $P^{-1} = R$, che come prima é un assurdo.
Dunque $P^{-1}J$ é un ideale intero piú grande di $J \Rightarrow P^{-1}J \notin \mathcal{F} \Rightarrow P^{-1}J = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$, con $e_i > 0 \Rightarrow J = PP_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ con esponenti positivi, assurdo.
Ci resta da far vedere che la fattorizzazione é unica; supponiamo:

$$\prod_{P \in \mathscr{P}} P^{e_P} = \prod_{P \in \mathscr{P}} P^{a_P},$$

dove $\mathscr{P}$ é l'insieme degli ideali primi, ed e_P, a_P sono nulli tranne un numero finito. Semplificando gli ideali in comune e spostando quelli con esponenti negativi, si arriva ad una scrittura:

$$P_1^{b_1} \cdot \ldots \cdot P_r^{b_r} = Q_1^{c_1} \cdot \ldots \cdot Q_t^{c_t}, \qquad c_i > 0, b_i > 0, \qquad P_i \neq Q_j \quad \forall i, j.$$

$P_1 \supseteq P_1^{b_1} \cdot \ldots \cdot P_r^{b_r} \Rightarrow P_1 \supseteq Q_1^{c_1} \cdot \ldots \cdot Q_t^{c_t} \Rightarrow P_1 \supseteq Q_j$, ma Q_j é primo (cioé massimale) e dunque $P_1 = Q_j$, assurdo (e l'assurdo é stato supporre $r \neq 0, t \neq 0$). □

Corollario 3.1.12. *$\mathcal{F}(R)$ é un gruppo abeliano generato dagli ideali primi; inoltre é un modulo libero.*

Dimostrazione. La prima parte segue dal teorema; é un modulo libero perché vale la fattorizzazione unica (e dunque un prodotto di primi non sará mai 0). □

Definizione 3.1.8. $K \supseteq \mathbb{Q}$. Definiamo **gruppo delle classi di ideali** il quoziente

$$\mathrm{Cl}(K) = \frac{\mathcal{F}(K)}{\mathcal{P}(K)},$$

dove $\mathcal{P}(K)$ é il sottogruppo degli ideali principali.

Osservazione. $\mathrm{Cl}(K)$ é un gruppo abeliano in quanto quoziente di un gruppo abeliano.

Osservazione. Sia $I \in \mathcal{F}(K)$ un ideale, che si fattorizza come $I = P_1^{e_1} \cdot \ldots \cdot P_t^{e_t}$, $P_i \subseteq \mathscr{O}_K$ primi. Denotiamo con $e_{P_i}(I) := e_i$ il massimo esponente di P_i contenuto in I; allora l'applicazione:

$$\begin{array}{rccc} e_P: & \mathcal{F}(K) & \longrightarrow & \mathbb{Z} \\ & I & \longrightarrow & e_P(I) \end{array}$$

é una valutazione.

Proposizione 3.1.13. *1.* $e_P(IJ) = e_P(I) + e_P(J)$

2. I *é intero (cioé* $I \subseteq \mathscr{O}_K$*)* $\iff$ $e_P(I) \geq 0$ $\forall P$ *primo*

3. $I \subseteq J \iff e_P(I) \geq e_P(J)$ $\forall P$ *primo*

4. $I, J \in \mathscr{O}_K$*.* $I|J$ *(cioé* $\exists L \in \mathscr{O}_K$ *tale che* $J = IL$*)* $\iff$ $J \subseteq I$*.*

Dimostrazione. I punti 1) e 2) sono del tutto ovvi.
Il punto 3) segue dal 2) osservando che $I \subseteq J \iff IJ^{-1} \subseteq \mathscr{O}_K$.
Per il punto 4) basta notare che $I^{-1}J \subseteq \mathscr{O}_K$ e $I(I^{-1}J) = J$. □

Definizione 3.1.9. Poiché vale la fattorizzazione unica, si possono definire **massimo comune divisore** e **minimo comune multiplo** fra ideali: $\gcd(I, J)$ é il piú grande ideale che divide sia I che J; $\mathrm{lcm}(I, J)$ é il piú piccolo ideale che é diviso da I e da L (grande e piccolo nel senso degli esponenti).

Osservazione. Si puó verificare che il massimo comune multiplo e il massimo comune divisore si calcolano nel modo usuale a partire dalla fattorizzazione: se $m_i = \min(a_i, b_i)$ e $M_i = \max(a_i, b_i)$, allora

$$\gcd(P_1^{a_1} \cdot \ldots \cdot P_s^{a_s}, P_1^{b_1} \cdot \ldots \cdot P_s^{b_s}) = P_1^{m_1} \cdot \ldots \cdot P_s^{m_s};$$
$$\mathrm{lcm}(P_1^{a_1} \cdot \ldots \cdot P_s^{a_s}, P_1^{b_1} \cdot \ldots \cdot P_s^{b_s}) = P_1^{M_1} \cdot \ldots \cdot P_s^{M_s}.$$

Inoltre é ovvio che $\gcd(I, J) = (I, J) = I + J$.

Proposizione 3.1.14. I *ideale frazionario di* $\mathscr{O}_K$*.* $\forall \alpha \in I$*,* $\exists \beta \in I$ *tale che* $I = (\alpha, \beta)$*.*

Dimostrazione. Per l'osservazione precedente, $I = (\alpha, \beta) \iff I = \gcd((\alpha), (\beta))$.
Posso supporre I intero, altrimenti basta moltiplicare per $d \in \mathscr{O}_K$ per renderlo tale.
So che $I = Q_1^{e_1} \cdot \ldots \cdot Q_t^{e_t}$, Q_i primo, $e_i \geq 0$.
$\alpha \in I \Rightarrow I \supseteq (\alpha) \Rightarrow (\alpha) = Q_1^{a_1} \cdot \ldots \cdot Q_t^{a_t} \cdot P_1^{b_1} \cdot \ldots \cdot P_s^{b_s}$, con $a_i \geq e_i$, $b_i \geq 0$.
Ma $\gcd((\alpha), (\beta)) = I \iff (\beta) = Q_1^{e_1} \cdot \ldots \cdot Q_t^{e_t} J$, con $P_i \nmid J$ $\forall i$, $Q_h \nmid J$ $\forall h$.
Scegliamo $\forall i$ un $\beta_i \in Q_i^{e_i} \backslash Q_i^{e_i+1}$, che esiste perché $Q_i^{e_i} \neq Q_i^{e_i+1}$ (in quanto hanno fattorizzazioni diverse); ma allora il sistema:

$$\begin{cases} \beta \equiv \beta_i & (Q_i^{e_i+1}) \quad \forall i \\ \beta \equiv 1 & (P_h) \quad \forall h \end{cases}$$

ha soluzione per il teorema cinese, poiché gli ideali sono coprimi. Un tale β dá la tesi. □

Proposizione 3.1.15. *$\mathscr{O}_K$ PID $\iff$ $\mathscr{O}_K$ UFD.*

Dimostrazione. L'implicazione $\Rightarrow$ é banale; per vedere l'altra dimostriamo la contronominale. Sia $P \subseteq \mathscr{O}_K$ primo non principale, che esiste perché se tutti gli ideali primi fossero principali, l'anello sarebbe PID.
Sia $\mathcal{F} = \{I \subseteq \mathscr{O}_K | PI \text{ é principale}\}$; $\mathcal{F} \neq \emptyset$, poiché se $P^{-1} \subseteq \frac{1}{d}\mathscr{O}_K$, $dP^{-1} \subseteq \mathscr{O}_K$ e $P(dP^{-1}) = (d)$, cioé $dP^{-1} \in \mathcal{F}$.
Per noetherianitá, sia $M \in \mathcal{F}$ un elemento massimale; $PM = (\alpha)$.
Dico che α é irriducibile ma non primo (e avrei la tesi).
Se $\alpha = \beta\gamma$, $(\alpha) = (\beta)(\gamma) = PM$, ma P é primo, quindi per fattorizzazione unica $P|(\beta) \vee P|(\gamma)$; diciamo $(\beta) = PL$.
Ma allora $L|M$, cioé $M \subseteq L$, ma M é massimale in $\mathcal{F}$ e $PL = (\beta)$ é principale $\Rightarrow L = M \Rightarrow \alpha \sim \beta$.
Vediamo infine che α non é primo; cerchiamo dunque $\beta, \gamma \notin (\alpha)$ tali che $\beta\gamma \in \alpha = PM$.
Se $\beta \in P\backslash(\alpha)$, $\gamma \in M\backslash(\alpha)$ (che esistono in quanto altrimenti avrei rispettivamente che $M = (1)$, cioé P principale, e $P = (1)$, entrambi assurdi) giungo alla tesi, in quanto $\beta\gamma \in PM = (\alpha)$. □

3.2 Ramificazione di ideali primi

In questa sezione ci occuperemo della fattorizzazione di ideali primi in estensioni successive di campi; piú precisamente, date le estensioni:

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

ci proponiamo di studiare la fattorizzazione di $P\mathscr{O}_F \subseteq \mathscr{O}_F$, al variare di P fra gli ideali primi di $\mathscr{O}_K$.

<u>*Osservazione*</u>. Sia $Q \subseteq \mathscr{O}_F$ primo. $P = Q^c = Q \cap \mathscr{O}_K$ é primo e non é zero, poiché $0 \neq x \in Q \Rightarrow 0 \neq \mathrm{N}_{F/K}(x) \in Q \cap \mathscr{O}_K$.

Definizione 3.2.1. Nelle notazioni dell'osservazione precedente, si dice che P **sta sotto** Q oppure che Q **sta sopra** P, e si scrive $Q|P$.

<u>*Osservazioni*</u>. 1. $Q \subseteq \mathscr{O}_F$; $\exists! P$ primo che sta sotto Q (ed é Q^c).

2. $\forall P \subseteq \mathscr{O}_K$ primo, i primi che stanno sopra P sono esattamente quelli che compaiono nella fattorizzazione di $P\mathscr{O}_F \neq \mathscr{O}_F$.

   Dimostrazione. $P^{-1} \supsetneq \mathscr{O}_K$, in quanto hanno fattorizzazioni diverse, quindi $\exists x \in P^{-1}\backslash\mathscr{O}_K$; ma allora $(xP)\mathscr{O}_F \subseteq \mathscr{O}_K\mathscr{O}_F \subseteq \mathscr{O}_F$.
   Se per assurdo $P\mathscr{O}_F = \mathscr{O}_F$, $1 \in P\mathscr{O}_F$, quindi $x = x \cdot 1 \in \mathscr{O}_F$, cioé $x \in K \cap \mathscr{O}_F = \mathscr{O}_K$, assurdo.
   Passiamo alla parte principale dell'osservazione; sia $P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$.
   Sicuramente $P\mathscr{O}_F \subseteq Q_i$ $\forall i$, cioé $Q_i \cap \mathscr{O}_K \supseteq P$, ma per la massimalitá di P, $P = Q_i \cap \mathscr{O}_K = Q_i^c$.
   Viceversa, se $Q \cap \mathscr{O}_K = P$, $P\mathscr{O}_F \subseteq Q$, cioé $Q|P\mathscr{O}_F$, cioé $Q = Q_i$ per un certo i. □

Definizione 3.2.2. Se $P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$, denoto $e_i = e(Q_i|P) = e_{Q_i}(P)$ l'**indice di ramificazione** di Q_i in P.

Osservazione. $\frac{\mathscr{O}_F}{Q_i}$ é un campo finito, detto **campo residuo**; del resto, la composizione

$$\mathscr{O}_K \xhookrightarrow{i} \mathscr{O}_F \xrightarrow{\pi} \frac{\mathscr{O}_F}{Q_i}$$

$\varphi = \pi \circ i$ ha nucleo $\mathrm{Ker}(\varphi) = Q_i^c = Q_i \cap \mathscr{O}_K = P$, cioé $\frac{\mathscr{O}_K}{P} \subseteq \frac{\mathscr{O}_F}{Q_i}$ é un sottocampo.

Definizione 3.2.3. Nelle notazioni precedenti, definiamo $f_i = f(Q_i|P) = \left[\frac{\mathscr{O}_F}{Q_i} : \frac{\mathscr{O}_K}{P}\right]$ **grado d'inerzia** di Q_i su P.

Proposizione 3.2.1. $[K : \mathbb{Q}] = n$, $0 \neq x \in K$. *Allora* $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = \left|\frac{\mathscr{O}_K}{x\mathscr{O}_K}\right|$.

Dimostrazione. $x\mathscr{O}_K$ é uno $\mathbb{Z}$-modulo libero di rango n, perció vale la formula:

$$\mathrm{disc}(x\mathscr{O}_K) = \left|\frac{\mathscr{O}_K}{x\mathscr{O}_K}\right|^2 \mathrm{disc}(\mathscr{O}_K).$$

$\exists\{e_1, \ldots, e_n\}$ base di $\mathscr{O}_K$ tale che $\{xe_1, \ldots, xe_n\}$ é base di $x\mathscr{O}_K$, dunque:

$$\mathrm{disc}(x\mathscr{O}_K) = \mathrm{disc}(xe_1, \ldots, xe_n) = \det(\varphi_x)^2 \,\mathrm{disc}(e_1, \ldots, e_n) = \det(\varphi_x)^2 \,\mathrm{disc}(\mathscr{O}_K),$$

dove $\varphi_x : \begin{array}{ccc} \mathscr{O}_K & \to & x\mathscr{O}_K \\ \alpha & \to & x\alpha \end{array}$ é un isomorfismo di $\mathbb{Z}$-moduli.
Si arriva alla tesi osservando che $\det(\varphi_x) = \mathrm{N}_{K/\mathbb{Q}}(x)$. □

Definizione 3.2.4. $(0) \neq I \subseteq \mathscr{O}_K$ ideale. Definiamo $\mathrm{N}(I) = \left|\frac{\mathscr{O}_K}{I}\right| < +\infty$ **norma** di I.

Osservazione. Per quanto appena visto, $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = \mathrm{N}(x\mathscr{O}_K)\ \forall x \in \mathscr{O}_K\backslash\{0\}$.

Proposizione 3.2.2. $I, J \subseteq \mathscr{O}_K$ *ideali. Allora* $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

Dimostrazione. Ci basta mostrare che $\forall P \subseteq \mathscr{O}_K$ primo, $\forall m$, $\mathrm{N}(P^m) = \mathrm{N}(P)^m$, poiché posso fattorizzare I e J in primi e per il teorema cinese $\left|\frac{\mathscr{O}_K}{PQ}\right| = \left|\frac{\mathscr{O}_K}{P}\right| \cdot \left|\frac{\mathscr{O}_K}{Q}\right|$, in quanto P, Q sono (co)massimali.
$P^m \subsetneqq P^{m-1} \subsetneqq \cdots \subsetneqq P \subsetneqq \mathscr{O}_K$, dunque $\left|\frac{\mathscr{O}_K}{P^m}\right| = \prod_{i=0}^{m-1} \left|\frac{P^i}{P^{i+1}}\right|$.
Dico che $\left|\frac{P^i}{P^{i+1}}\right| = \left|\frac{\mathscr{O}_K}{P}\right| \quad \forall i$ (e avrei la tesi).
Fissato $x \in P^i\backslash P^{i+1}$, consideriamo la composizione:

$$\varphi : \begin{array}{ccccc} \mathscr{O}_K & \xrightarrow{\varphi_x} & P^i & \xrightarrow{\pi} & \frac{P^i}{P^{i+1}} \\ \alpha & \longrightarrow & x\alpha & \longrightarrow & [x\alpha]_{P^{i+1}} \end{array}.$$

φ é un omomorfismo di $\mathbb{Z}$-moduli e $\mathrm{Ker}(\varphi) = \{\alpha | x\alpha \in P^{i+1}\} = \{\alpha | \alpha \in P\} = P$, in quanto $x \in P^i$.
Inoltre φ é surgettiva, infatti $\varphi(\mathscr{O}_K) = \frac{x\mathscr{O}_K + P^{i+1}}{P^{i+1}}$ e $x\mathscr{O}_K + P^{i+1} = \gcd((x), P^{i+1}) = P^i$, poiché deve essere una potenza di P e P^i é la massima potenza di P che divide (x).
Quindi $\overline{\varphi} : \frac{\mathscr{O}_K}{P} \to \frac{P^i}{P^{i+1}}$ é un isomorfismo, da cui la tesi. □

Teorema 3.2.3. $\mathbb{Q} \subseteq K \subseteq F$ *estensioni di campi di numeri,* $[F : K] = n$, $P \subseteq \mathscr{O}_K$ *primo. Se* $P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$, *allora vale la relazione:*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Dimostrazione. $\mathrm{N}(P\mathscr{O}_F) = \mathrm{N}(Q_1)^{e_1} \cdot \ldots \cdot \mathrm{N}(Q_r)^{e_r}$; inoltre per definizione di grado d'inerzia si ha che $\mathrm{N}(Q_i) = \left|\frac{\mathscr{O}_F}{Q_i}\right| = \left|\frac{\mathscr{O}_K}{P}\right|^{f_i} = \mathrm{N}(P)^{f_i}$, dunque:

$$\mathrm{N}(P\mathscr{O}_F) = \mathrm{N}(P)^{\sum_{i=1}^{r} e_i f_i}.$$

Per avere la tesi ci basta mostrare che $\mathrm{N}(P\mathscr{O}_F) = \mathrm{N}(P)^n$.
Se $K = \mathbb{Q}$ é particolarmente semplice, poiché se $P = (p)$, $p \in \mathbb{Z}$, $\mathrm{N}(p\mathscr{O}_F) = \left|\mathrm{N}_{F/\mathbb{Q}}(p)\right|$ per l'ultima osservazione, e $\mathrm{N}_{F/\mathbb{Q}}(p) = p^n$.
Nel caso generale, abbiamo che la mappa

$$\mathscr{O}_K \xhookrightarrow{i} \mathscr{O}_F \xrightarrow{\pi} \frac{\mathscr{O}_F}{P\mathscr{O}_F}$$

si quozienta a un'immersione $\frac{\mathscr{O}_K}{P} \hookrightarrow \frac{\mathscr{O}_F}{P\mathscr{O}_F}$ (poiché $\mathrm{Ker}(\pi \circ i) = P$); quindi $\frac{\mathscr{O}_F}{P\mathscr{O}_F}$ é un $\frac{\mathscr{O}_K}{P}$-spazio vettoriale.
La tesi equivale a dimostrare che $\dim_{\frac{\mathscr{O}_K}{P}} \frac{\mathscr{O}_F}{P\mathscr{O}_F} = n$; vediamo che valgono entrambe le disuguaglianze.

- $\leq$) Devo vedere che, dati comunque $n+1$ elementi, essi sono linearmente dipendenti.
  Siano $\alpha_1, \ldots, \alpha_{n+1} \in \mathscr{O}_F$; essi sono elementi dipendenti su K (e dunque su $\mathscr{O}_K$) perché $[F : K] = n$, dunque $\exists b_1, \ldots, b_{n+1} \in \mathscr{O}_K$ non tutti nulli tali che $\sum_{i=1}^{n+1} b_i \alpha_i = 0$. Voglio vedere che si possono scegliere i b_i in modo che ce ne sia almeno uno tale che $\overline{b_j} \neq 0 \quad (P)$, cioé $b_j \notin P$.
  $B = (b_1, \ldots, b_{n+1}) \subseteq \mathscr{O}_K$; B é invertibile, cioé $B^{-1}B = \mathscr{O}_K \Rightarrow \exists b \in B^{-1}$ tale che $bB \subseteq \mathscr{O}_K$ e $bB \not\subseteq P\mathscr{O}_K$ (poiché altrimenti $B^{-1}B = P\mathscr{O}_K$), cioé $\exists i$ tale che $bb_i \notin P$.
  A meno di cambiare $b_1, \ldots, b_{n+1}$ con $bb_1, \ldots, bb_{n+1}$, posso supporre che $\exists j$ tale che $b_j \not\equiv 0 \quad (P)$.

- $\geq$) Sia $p = P^c = P \cap \mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{Q} & & p = P \cap \mathbb{Z} \\ & & \uparrow \\ m \Big| & & \\ & & \\ K & & P \\ & & \Big\downarrow \\ n \Big| & & \\ & & \\ F & & P\mathscr{O}_F \end{array}$$

  Sia $p\mathscr{O}_K = P_1^{\varepsilon_1} \cdot \ldots \cdot P_s^{\varepsilon_s}$; per quanto visto nel primo caso si ha che $\sum_{i=1}^{s} \varepsilon_i f(P_i|p) = m$.
  Inoltre $p\mathscr{O}_F = (P_1\mathscr{O}_F)^{\varepsilon_1} \cdot \ldots \cdot (P_s\mathscr{O}_F)^{\varepsilon_s}$.
  Sappiamo che $\mathrm{N}(p\mathscr{O}_F) = p^{nm}$ e $\mathrm{N}(P_i\mathscr{O}_F) = \mathrm{N}(P_i)^{n_i}$ con $n_i \leq n$ per la prima disuguaglianza; inoltre $\mathrm{N}(P_i) = p^{f(P_i|p)}$.

  Dunque:

$$p^{nm} = \mathrm{N}(P_1\mathscr{O}_F)^{\varepsilon_1} \cdot \ldots \cdot \mathrm{N}(P_s\mathscr{O}_F)^{\varepsilon_s} = \left(\mathrm{N}(P_1)^{n_1}\right)^{\varepsilon_1} \cdot \ldots \cdot \left(\mathrm{N}(P_s)^{n_s}\right)^{\varepsilon_s} = p^{\sum_{i=1}^{s} f(P_i|p) n_i \varepsilon_i} \leq$$
$$\leq p^{n \sum_{i=1}^{s} f(P_i|p)\varepsilon_i} = p^{nm},$$

  da cui la disuguaglianza é un'uguaglianza e $n_i = n \ \forall i$ (e in particolare per $P = P_i$).

□

Proposizione 3.2.4. *L'indice di ramificazione e il grado d'inerzia sono moltiplicativi nelle torri, cioé date le estensioni successive*

$$\begin{array}{ll} \mathbb{Q} & p \\ | & \uparrow \\ K & P \\ | & \downarrow \\ F & P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r} \\ | & \downarrow \\ L & P\mathscr{O}_L = U_1^{\varepsilon_1} \cdot \ldots \cdot U_t^{\varepsilon_t} \end{array}$$

con i rispettivi primi, si ha che, se $U|Q|P$:

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

Dimostrazione. Per i gradi d'inerzia é semplice, poiché $\left[\frac{\mathscr{O}_L}{U} : \frac{\mathscr{O}_K}{P}\right] = \left[\frac{\mathscr{O}_L}{U} : \frac{\mathscr{O}_F}{Q}\right] \cdot \left[\frac{\mathscr{O}_F}{Q} : \frac{\mathscr{O}_K}{P}\right]$ come spazi vettoriali.
Invece per gli indici di ramificazione:

$$P\mathscr{O}_L = (P\mathscr{O}_F)\mathscr{O}_L = (Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r})\mathscr{O}_L = (Q_1\mathscr{O}_L)^{e_1} \cdot \ldots \cdot (Q_r\mathscr{O}_L)^{e_r} = \left(U_1^{e(U_1|Q_1)}\right)^{e(Q_1|P)} \cdot \ldots \cdot \left(U_t^{e(U_t|Q_r)}\right)^{e(Q_r|P)},$$

da cui $e(U_i|P) = e(U_i|Q_j) \cdot e(Q_1|P) \quad U_i|Q_j$. □

Concentriamoci ora su un caso particolare delle estensioni di campi, le estensioni di Galois. Vedremo infatti che in queste speciali estensioni, le condizioni per r, e_i, f_i sono ancora piú restrittive.
Nel seguito sia L/K un'estensione di Galois, $[L : K] = n$, $G = \mathrm{Gal}(L/K)$.

Proposizione 3.2.5. *$P \subseteq \mathscr{O}_K$ primo. G agisce transitivamente sull'insieme dei primi di $\mathscr{O}_L$ sopra P.*

Dimostrazione. $P\mathscr{O}_L = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$; $\{Q_1, \ldots, Q_r\}$ é dunque l'insieme dei primi sopra P.
Gli elementi del gruppo di Galois mandano elementi interi in elementi interi (poiché non cambiano il polinomio minimo), quindi se $\sigma \in G$,

$$P\mathscr{O}_L = \sigma(P)\mathscr{O}_L = \sigma(Q_1)^{e_1} \cdot \ldots \cdot \sigma(Q_r)^{e_r}$$

(in quanto $P \subseteq K$), da cui $\{Q_1, \ldots, Q_r\} = \{\sigma(Q_1), \ldots, \sigma(Q_r)\}$ per fattorizzazione unica.
Supponiamo per assurdo che esistano $Q, Q'|P$ tali che $\sigma(Q) \neq Q' \quad \forall \sigma \in G$; allora $\exists \alpha \in Q'$, $\alpha \notin \sigma(Q) \quad \forall \sigma \in G$ (infatti per il teorema cinese il sistema

$$\begin{cases} \alpha \equiv 0 \pmod{Q'} \\ \alpha \equiv 1 \pmod{\sigma(Q)} \quad \forall \sigma \in G \end{cases}$$

ha soluzione, in quanto essendo $\sigma(Q)$ primo, $(\sigma_1(Q), \sigma_2(Q)) \neq 1 \iff \sigma_1(Q) = \sigma_2(Q)$, dunque togliendo le condizioni ridondanti gli ideali sono a due a due coprimi).
$\alpha \in Q' \Rightarrow \mathrm{N}_{L/K}(\alpha) \in Q' \cap \mathscr{O}_K = P$; inoltre $\alpha \notin \sigma(Q) \quad \forall \sigma \in G \iff \sigma(\alpha) \notin Q \quad \forall \sigma \in G$ (in quanto G é un gruppo).
Ma $\mathrm{N}_{L/K}(\alpha) \in P \subseteq Q$ e $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in Q$, che é primo, assurdo. □

Corollario 3.2.6. *$P \subseteq \mathscr{O}_K$ primo. Allora $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e$ (cioé $e_i = e_j \quad \forall i, j$) e $f(Q_i|P) = f \quad \forall i$.*
Inoltre $f \cdot e \cdot r = n$.

Dimostrazione. Presi Q_i e Q_j, per la proposizione precedente $\exists \sigma \in G$ tale che $\sigma(Q_i) = Q_j$, dunque $P\mathscr{O}_L = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r} = \sigma(Q_1)^{e_1} \cdot \ldots \cdot \sigma(Q_r)^{e_r}$, da cui $e_i = e_j$ (in quanto $\sigma((Q_1, Q_2)) = (\sigma(Q_1), \sigma(Q_2)) \Rightarrow \sigma(Q_1), \ldots, \sigma(Q_r)$ sono a due a due coprimi).
Vediamo ora che anche i gradi d'inerzia sono tutti uguali; restringiamo σ a $\sigma : \mathscr{O}_L \to \mathscr{O}_L$, e abbiamo:

$$\begin{array}{ccc} \mathscr{O}_L & \xrightarrow{\sigma} & \mathscr{O}_L \\ \downarrow{\scriptstyle \pi_i} & \searrow^{\pi_j \circ \sigma} & \downarrow{\scriptstyle \pi_j} \\ \dfrac{\mathscr{O}_L}{Q_i} & \xrightarrow[\overline{\sigma}]{\sim} & \dfrac{\mathscr{O}_L}{Q_j} \end{array}$$

in quanto $Q_i = \sigma^{-1}(Q_j) \Rightarrow \mathrm{Ker}(\pi_j \circ \sigma) = Q_i$.
Ma allora $\left[\frac{\mathscr{O}_L}{Q_i} : \frac{\mathscr{O}_K}{P}\right] = \left[\frac{\mathscr{O}_L}{Q_j} : \frac{\mathscr{O}_K}{P}\right]$, cioé $f_i = f_j$. □

Esempio. In generale non tutte le possibili fattorizzazioni si realizzano in pratica; ad esempio in un'estensione generica di grado 3 posso avere spezzamenti del tipo:

$$P\mathscr{O}_L = \begin{cases} Q_1Q_2Q_3 & f_i = 1 \quad \forall i \\ Q_1Q_2 & f_1 = 2, f_2 = 1 \\ Q & f = 3 \\ Q_1^2Q_2 & f_i = 1 \quad \forall i \\ Q^3 & f = 1 \end{cases},$$

mentre se l'estensione é di Galois posso avere solo fattorizzazioni del tipo:

$$P\mathscr{O}_L = \begin{cases} Q_1Q_2Q_3 & f_i = 1 \quad \forall i \\ Q & f = 3 \\ Q^3 & f = 1 \end{cases}.$$

Vedremo a breve che in un'estensione c'é solo un numero finito di primi ramificati; per quelli non ramificati invece vale il seguente importantissimo risultato, che ovviamente non dimostriamo:

Teorema 3.2.7 (di densitá di Chebotarev)**.** *$K/\mathbb{Q}$ estensione, $\widetilde{K}$ chiusura normale di K in $\mathbb{Q}$, $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. Allora:*

$$d(\{p \in \mathbb{Z} | p\mathscr{O}_K \text{ ha la fattorizzazione di tipo } F\}) = \frac{|\{\sigma \in G < \mathcal{S}_n | \sigma \text{ é di tipo } F\}|}{|G|},$$

dove $F = (f_1, \ldots, f_r)$ con $f_1 \leq \ldots \leq f_r$ e $d(X)$ é la densitá naturale definita da:

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

dove $\mathscr{P}(n)$ é l'insieme dei numeri primi $\leq n$.

Esempio. Sia $[L : \mathbb{Q}] = 3$ e $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \cong \mathcal{S}_3$. Allora:

$$d(\{p \in \mathbb{Z} | p\mathscr{O}_L = P_1P_2P_3\}) = \frac{|\{\sigma \in \mathcal{S}_3 | \sigma = 1+1+1\}|}{|\mathcal{S}_3|} = \frac{1}{6}$$
$$d(\{p \in \mathbb{Z} | p\mathscr{O}_L = P_1P_2\}) = \frac{|\{\sigma \in \mathcal{S}_3 | \sigma = 1+2\}|}{|\mathcal{S}_3|} = \frac{1}{2}$$
$$d(\{p \in \mathbb{Z} | p\mathscr{O}_L = P\}) = \frac{|\{\sigma \in \mathcal{S}_3 | \sigma = 3\}|}{|\mathcal{S}_3|} = \frac{1}{3}$$

Definizione 3.2.5. L/K estensione. Si dice che un primo $P \subseteq \mathscr{O}_K$ **ramifica** in L se $\exists Q | P$ tale che $e(Q|P) > 1$.
$P\mathscr{O}_L$ si dice **ramificato** se $P\mathscr{O}_L = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$ e $\exists i$ tale che $e_i > 1$.

Enunciamo ora un teorema di cui dimostriamo una sola implicazione, mentre l'altra sará vista piú in lá:

Teorema 3.2.8. *$[K : \mathbb{Q}] = n$. $p \in \mathbb{Z}$ é ramificato in $K \Rightarrow p | \mathrm{disc}(K)$.*

Dimostrazione. $p \in \mathbb{Z}$, $p\mathscr{O}_K$ ramificato, $p\mathscr{O}_K = PI$, con $e(P|p) \geq 2$.
$\forall P' | p$, $P' | I$, ma $p\mathscr{O}_K \subsetneq I$, quindi $\exists \alpha \in I \backslash p\mathscr{O}_K$.
Sia $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Z}$-base di $\mathscr{O}_K$; $\mathrm{disc}(K) = \mathrm{disc}(\alpha, \ldots, \alpha_n)$.
$\alpha = \sum_i m_i\alpha_i$, con $m_i \in \mathbb{Z}$, ma $\alpha \notin p\mathscr{O}_K = \langle p\alpha_1, \ldots, p\alpha_n \rangle_{\mathbb{Z}}$, dunque $\exists i$ per cui $p \nmid m_i$.

Supponiamo per semplicitá $i = 1$.
Allora $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det(M)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)$, dove:

$$M = \left(\begin{array}{c|ccc} m_1 & 0 & \dots & 0 \\ \hline m_2 & & & \\ \vdots & & I_{n-1} & \\ m_n & & & \end{array}\right),$$

perció $\det(M)^2 = m_1^2$, ma $p \nmid m_1$, quindi $p | \operatorname{disc}(K) \iff p | \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$.
Siano $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ le immersioni di $K/\mathbb{Q}$ e sia $L = \widetilde{K}$ la chiusura normale di $K/\mathbb{Q}$.
$\forall Q \subseteq \mathscr{O}_L$ sopra p, $\alpha \in Q$, poiché $\forall Q | p$, abbiamo visto che $\alpha \in Q^c$ e dunque in Q.
Fisso $Q \subseteq \mathscr{O}_L$, $Q|p$; $\alpha \in \sigma(Q) \quad \forall \sigma \in G = \operatorname{Gal}(L/\mathbb{Q})$ (poiché i $\sigma(Q)$ sono tutti e soli i primi sopra p per transitivitá dell'azione di G), cioé $\sigma(\alpha) \in Q \quad \forall \sigma \in G$, quindi $\sigma_i(\alpha) \in Q \quad \forall i = 1, \dots, n$ (in quanto ogni σ_i si estende a L).

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

ma la prima colonna sta tutta in Q, quindi $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in Q$.
Ma $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in \mathbb{Z} \Rightarrow \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in Q \cap \mathbb{Z} = (p)$. □

Corollario 3.2.9. *$K = \mathbb{Q}(\alpha)$, α intero. $p \nmid \mathrm{N}(\mu'(\alpha)) \Rightarrow p$ non é ramificato.*

Corollario 3.2.10. *L/K estensione. Solo un numero finito di primi di $\mathscr{O}_K$ ramifica in $\mathscr{O}_L$.*

Dimostrazione. Se $K = \mathbb{Q}$ la tesi segue immediatamente dal teorema precedente.
Se $P \subseteq \mathscr{O}_K$ primo é tale che $P\mathscr{O}_L$ é ramificato, allora, se $p = P \cap \mathbb{Z}$, $p\mathscr{O}_L$ é ramificato, in quanto gli indici di ramificazione sono moltiplicativi nelle torri.
Ma allora $p | \operatorname{disc}(L)$, quindi i primi di $\mathscr{O}_L$ ramificati su p sono in numero finito, e di conseguenza anche i primi di $\mathscr{O}_L$ ramificati sopra P sono in numero finito. □

Definizione 3.2.6. $[F : K] = n$ campi di numeri. $P \subseteq \mathscr{O}_K$ ideale primo, $P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$.
P si dice:

- **totalmente ramificato** se $r = 1$, $f_1 = 1$, $e_1 = n$;
- **inerte** se $r = 1$, $e_1 = 1$, $f_1 = n$;
- che si **spezza completamente** se $r = n$, $e_i = f_i = 1$.

3.3 Il teorema di Kummer

$F = K(\alpha)$, α intero, $T = \mu_\alpha \in \mathscr{O}_K[x]$, $\deg(T) = n$.
Sia $P \subseteq \mathscr{O}_K$, e sia $\frac{\mathscr{O}_K}{P}[x] \ni \overline{T} = \overline{T_1}^{e_1} \cdot \ldots \cdot \overline{T_r}^{e_r}$ (P) la fattorizzazione di T in $\frac{\mathscr{O}_K}{P}[x]$.
Allora vale il seguente:

Teorema 3.3.1 (di Kummer)**.** *Sia $p = P \cap \mathbb{Z}$ e $p \nmid \left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha]}\right| = \operatorname{ind}(\alpha)$.*
Allora $P\mathscr{O}_F = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$, dove r e gli e_i sono quelli della fattorizzazione di $\overline{T}$, $f_i = \left[\frac{\mathscr{O}_F}{Q_i} : \frac{\mathscr{O}_K}{P}\right] = \deg(\overline{T_i})$, e $Q_i = (P, T_i(\alpha))$, dove T_i é un qualsiasi sollevamento monico di $\overline{T_i}$ a $\mathscr{O}_F[x]$.

Dimostrazione. Mostriamo innanzitutto i seguenti fatti:

1. $\forall i$, $Q_i = \mathscr{O}_F \vee \frac{\mathscr{O}_F}{Q_i}$ é un campo e $\left[\frac{\mathscr{O}_F}{Q_i} : \frac{\mathscr{O}_K}{P}\right] = \deg(\overline{T_i})$;
2. $\forall i, j$, $Q_i + Q_j = \mathscr{O}_F$;
3. $P\mathscr{O}_F | Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$.

1. Sia $F_i = \frac{\frac{\mathscr{O}_K}{P}[x]}{(\overline{T_i})}$; é un campo perché quoziente di un anello di polinomi in una indeterminata per un ideale principale generato da un elemento irriducibile (per Bezout), e $\left[F_i : \frac{\mathscr{O}_K}{P}\right] = \deg(\overline{T_i}) = f_i$.
   Consideriamo la composizione:
   $$\mathscr{O}_K[x] \xrightarrow{\pi_P} \frac{\mathscr{O}_K}{P}[x] \xrightarrow{\overline{\pi_i}} \frac{\frac{\mathscr{O}_K}{P}[x]}{(\overline{T_i})};$$
   ovviamente $\varphi = \overline{\pi_i} \circ \pi_P$ é surgettiva (in quanto composizione di proiezioni), e $\mathrm{Ker}(\varphi) = \{a(x) \in \mathscr{O}_K[x] | \overline{a}(x) \in (\overline{T_i}(x))\} = (P, T_i(x))$ (infatti l'inclusione $\supseteq$ é evidente, mentre $a \in \mathrm{Ker}(\varphi) \Rightarrow \overline{T_i}(x) | \overline{a}(x)$ in $P \Rightarrow a(x) = q(x)T_i(x) + r(x)$ con $r(x) \in P\mathscr{O}_K[x]$).
   Dunque per il teorema di omomorfismo:
   $$\frac{\mathscr{O}_K[x]}{(P, T_i(x))} \cong \frac{\frac{\mathscr{O}_K}{P}[x]}{(\overline{T_i}(x))},$$
   quindi $\left[\frac{\mathscr{O}_K[x]}{(P,T_i(x))} : \frac{\mathscr{O}_K}{P}\right] = \deg(\overline{T_i})$.
   Consideriamo inoltre la composizione:
   $$\begin{array}{rccccc} \psi : & \mathscr{O}_K[x] & \longrightarrow & \mathscr{O}_K[\alpha] & \longrightarrow & \frac{\mathscr{O}_F}{Q_i} \\ & x & \longrightarrow & \alpha & \longrightarrow & \alpha + Q_i = \overline{\alpha} \end{array};$$
   $\mathrm{Ker}(\psi) = \{a(x) \in \mathscr{O}_K[x] | a(\alpha) \in Q_i\} \supseteq (P, T_i(x))$, che é massimale (in quanto il quoziente é un campo), quindi $\mathrm{Ker}(\psi) = \mathscr{O}_K[x] \vee \mathrm{Ker}(\psi) = (P, T_i(x))$.
   ψ é surgettiva, cioé $Im(\psi) = \mathscr{O}_K[\alpha] + Q_i = \mathscr{O}_F$:
   $\subseteq$) ovvia.
   $\supseteq$) $\mathscr{O}_K[\alpha] \subseteq \mathscr{O}_K[\alpha] + p\mathscr{O}_F \subseteq \mathscr{O}_F$; inoltre $p\mathscr{O}_F \subseteq \mathscr{O}_K[\alpha] + p\mathscr{O}_F \subseteq \mathscr{O}_F$, dunque:
   $$\left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha] + p\mathscr{O}_F}\right| \Bigg| \left(\left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha]}\right|, \left|\frac{\mathscr{O}_F}{p\mathscr{O}_F}\right|\right)$$
   (li divide entrambi per la formula delle torri).
   Ma il massimo comune divisore é 1, in quanto il secondo termine vale $p^{[F:\mathbb{Q}]}$, mentre il primo é coprimo con p, dunque $\left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha]+p\mathscr{O}_F}\right| = 1$, cioé $\mathscr{O}_F = \mathscr{O}_K[\alpha] + p\mathscr{O}_F$, ma:
   $$\mathscr{O}_F \supseteq \mathscr{O}_K[\alpha] + Q_i \supseteq \mathscr{O}_K[\alpha] + p\mathscr{O}_F,$$
   da cui $\mathscr{O}_F = \mathscr{O}_K[\alpha] + Q_i$.
   Ma allora:
   $$Q_i = \mathscr{O}_F \quad \vee \quad \frac{\mathscr{O}_F}{Q_i} \cong \frac{\mathscr{O}_K[x]}{(P, T_i(x))} \cong F_i,$$
   cioé Q_i é primo e $\left[\frac{\mathscr{O}_F}{Q_i} : \frac{\mathscr{O}_K}{P}\right] = f_i$.

2. $Q_i = (P, T_i(\alpha))$, $Q_j = (P, T_j(\alpha))$; in $\frac{\mathscr{O}_K}{P}[x]$, $\overline{T_i}$ e $\overline{T_j}$ sono coprimi, quindi $\exists \overline{a}, \overline{b} \in \frac{\mathscr{O}_K}{P}[x]$ tali che $\overline{a}(x)\overline{T_i}(x) + \overline{b}(x)\overline{T_j}(x) = \overline{1}$, cioé $a(x)T_i(x) + b(x)T_j(x) \equiv 1 \quad (P)$, dunque:
   $$a(x)T_i(x) + b(x)T_j(x) \in 1 + P\mathscr{O}_K[x].$$

Valutando in α:

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

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

3. Vediamo che $Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r} \subseteq P\mathscr{O}_F$.

$$Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r} = \prod_{i=1}^{r} (P, T_i(\alpha))^{e_i} \subseteq (P, T_1^{e_1}(\alpha) \cdot \ldots \cdot T_r^{e_r}(\alpha));$$

ma $T(x) \equiv T_1^{e_1}(x) \cdot \ldots \cdot T_r^{e_r}(x) \quad (P)$, quindi $\underbrace{T(\alpha)}_{=0} - T_1^{e_1}(\alpha) \cdot \ldots \cdot T_r^{e_r}(\alpha) \in P\mathscr{O}_F$, cioé $(P, T_1^{e_1}(\alpha) \cdot \ldots \cdot T_r^{e_r}(\alpha)) \subseteq P\mathscr{O}_F$.

A questo punto ci resta da mostrare la tesi con questi tre punti.
Siano $Q_1, \ldots, Q_s$ primi e $Q_{s+1}, \ldots, Q_r = \mathscr{O}_F$.
$P\mathscr{O}_F | Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r} = Q_1^{e_1} \cdot \ldots \cdot Q_s^{e_s}$, dunque $P\mathscr{O}_F = Q_1^{d_1} \cdot \ldots \cdot Q_s^{d_s}$, con $0 \leq d_i \leq e_i \quad \forall i$.
Passando alle norme, si ha:

$$n = \sum_{i=1}^{s} d_i \cdot \underbrace{\deg(\overline{T_i})}_{=f_i} = \sum_{i=1}^{r} e_i f_i,$$

ma $s \leq r$ e $d_i \leq e_i \quad \forall i$, quindi valgono le uguaglianze, cioé $s = r$ e $d_i = e_i \quad \forall i$. □

Esempi. Applichiamo il teorema di Kummer alle estensioni piú facili da trattare: le estensioni quadratiche e le estensioni ciclotomiche.

1. Le estensioni quadratiche $K = \mathbb{Q}(\sqrt{m})$, m libero da quadrati.
   Dico che, se $p \neq 2$ é primo:

$$p\mathscr{O}_K = \begin{cases} (p, \sqrt{m})^2 & \text{se } p|m \\ (p, n - \sqrt{m})(p, n + \sqrt{m}) & \text{se } p \nmid m \wedge m \equiv n^2 \quad (p) \\ (p) & \text{se } p \nmid m \wedge m \not\equiv \square \quad (p) \end{cases},$$

   mentre se $p = 2$:

$$2\mathscr{O}_K = \begin{cases} (2, \sqrt{m})^2 & \text{se } 2|m \\ (2, 1 + \sqrt{m})^2 & \text{se } m \equiv 3 \quad (4) \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & \text{se } m \equiv 1 \quad (8) \\ (2) & \text{se } m \equiv 5 \quad (8) \end{cases}.$$

   Dimostrazione. Sia $p \neq 2$. $T(x) = x^2 - m$; poiché $p > 2$, si ha che:

$$p \nmid \left| \frac{\mathscr{O}_K}{\mathbb{Z}[\sqrt{m}]} \right| = \begin{cases} 1 & \text{se } m \equiv 2, 3 \quad (4) \\ 2 & \text{se } m \equiv 1 \quad (4) \end{cases}.$$

   Quindi si puó usare $T(x)$ per applicare Kummer $\forall p > 2$.
   Se $p|m$, $T(x) \equiv x^2 \quad (p) \Rightarrow p\mathscr{O}_K = (p, \sqrt{m})^2$.
   Se $p \nmid m$ e $m \equiv n^2 \quad (p)$, $T(x) \equiv (x - n)(x + n) \quad (p) \Rightarrow p\mathscr{O}_K = (p, n - \sqrt{m})(p, n + \sqrt{m})$.
   Se $p \nmid m$ e $m \not\equiv \square \quad (p) \Rightarrow T$ é irriducibile, cioé $p\mathscr{O}_K$ é inerte.
   Sia ora $p = 2$. Se $m \equiv 2, 3 \quad (4)$, posso usare ancora $T(x)$ per applicare Kummer.
   Se $2|m$, $T(x) \equiv x^2 \quad (2) \Rightarrow 2\mathscr{O}_K = (2, \sqrt{m})^2$.

Se $m \equiv 3 \pmod 4$, $T(x) \equiv x^2 + 1 = (x+1)^2 \pmod 2 \Rightarrow 2\mathscr{O}_K = (2, 1+\sqrt{m})^2$.
Infine, se $m \equiv 1 \pmod 4$, devo cambiare polinomio. Sia $H(x) = x^2 - x + \frac{1-m}{4}$ polinomio minimo di $\frac{1+\sqrt{m}}{2}$.
Se $m \equiv 1 \pmod 8$, $H(x) \equiv x^2 + x = x(x+1) \pmod 2 \Rightarrow 2\mathscr{O}_K = \big(2, \frac{1+\sqrt{m}}{2}\big)\big(2, \frac{3+\sqrt{m}}{2}\big)$.
Se $m \equiv 5 \pmod 8$, $H(x) \equiv x^2 + x + 1 \pmod 2$, che é irriducibile, dunque $2\mathscr{O}_K$ é inerte. □

2. Le estensioni ciclotomiche $K = \mathbb{Q}(\zeta_m)$, p un certo primo, $m = p^k n$ con $(n,p) = 1$.
Dico che:

$$p\mathscr{O}_K = (Q_1 \cdot \ldots \cdot Q_r)^e, \quad e = \phi(p^k), \quad f = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^*} p, \quad r \text{ tale che } fer = \phi(m).$$

Dimostrazione. Notiamo che per applicare Kummer si puó usare il polinomio ciclotomico $\forall p$ primo, in quanto $\mathscr{O}_K = \mathbb{Z}[\zeta_m]$.

$m = p^k$) Sappiamo che $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(p^k)$; inoltre $\mu(x) | x^{p^k} - 1 \equiv (x-1)^{p^k} \pmod p$, dunque $\mu(x) \equiv (x-1)^{\phi(p^k)} \pmod p$, da cui $p\mathscr{O}_K = P^{\phi(p^k)}$ (e dunque $f = r = 1$).

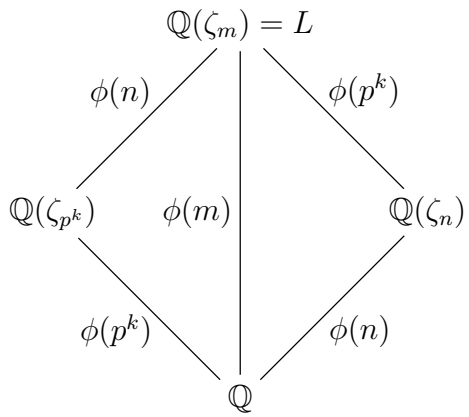
$m = n$) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$; inoltre $\mu | x^n - 1$ ha radici semplici in quanto divisore di $x^n - 1$ che ha radici semplici per il criterio della derivata (e $(p,n) = 1$).
Quindi $p\mathscr{O}_K$ non é ramificato (potevamo arrivare anche prima a questa conclusione, in quanto $p \nmid \operatorname{disc}(K) =$ potenza di n).
Notiamo che, se $\overline{\mu} = \overline{\mu_1} \cdot \ldots \cdot \overline{\mu_k}$, $\overline{\mu}(\overline{\zeta_n}) = 0$, dunque $\exists i$ tale che $\overline{\mu_i}(\overline{\zeta_n}) = 0$; ma allora $\mu_{\overline{\zeta_n}} | \overline{\mu_i}$ irriducibile, da cui $\mu_{\overline{\zeta_n}} = \overline{\mu_i}$ e:

$$\frac{\mathscr{O}_K}{Q_i} = \frac{\mathbb{Z}[\zeta_n]}{(p, \mu_{\overline{\zeta_n}}(\zeta_n)} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[\zeta_n]}{(\mu_{\overline{\zeta_n}}(\zeta_n))} \cong (\mathbb{Z}/p\mathbb{Z})[\overline{\zeta_n}],$$

dunque $\big[\frac{\mathscr{O}_K}{Q_i} : \mathbb{Z}/p\mathbb{Z}\big] = \deg(\mu_{\overline{\zeta_n}})$ polinomio minimo di $\overline{\zeta_n}$ su $\mathbb{Z}/p\mathbb{Z}$. Ma $\overline{\zeta_n}$ é una radice n-esima di 1, ed é anche primitiva in $\mathbb{F}_p$, in quanto $\overline{G} = \{\alpha \in \mathbb{F}_p | \alpha^n = 1\} \cong \mathbb{Z}/n\mathbb{Z}$ é ciclico ed ha $\phi(n)$ elementi di ordine n, che in particolare sono gli $\overline{\zeta}$ tali che ζ é una radice primitiva in $\mathbb{Q}$.
Ma allora, per un noto teorema sui campi finiti:

$$(\mathbb{Z}/p\mathbb{Z})[\overline{\zeta_n}] \cong \mathbb{F}_{p^k}, \qquad k = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^*} p.$$

$m = p^k n$) $(n,p) = 1$. Abbiamo il diagramma:



Sappiamo che $p\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e$, con $fer = \phi(m) = \phi(p^k)\phi(n)$.
Per il primo punto $\phi(p^k) | e$ per moltiplicativitá nelle torri, mentre per il secondo punto $\phi(n) \leq rf$, poiché se in $\mathbb{Q}(\zeta_n)$ ci sono a primi con grado d'inerzia b, allora

$ab = \phi(n)$, ma $r \geq a$ e $b|f$.
Ma $\phi(m) = \phi(p^k)\phi(n) \leq fer = \phi(m)$, dunque ci sono uguaglianze: in particolare $e = \phi(p^k)$ e $\mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^*} n | f \Rightarrow \mathrm{ord}_{(\mathbb{Z}/p\mathbb{Z})^*} n = f$.

(Detto in parole povere, i primi si spezzano in $\mathbb{Q}(\zeta_n)$ e poi ramificano in L; viceversa ramificano in $\mathbb{Q}(\zeta_{p^k})$ e poi si spezzano in L.) □

Proposizione 3.3.2. *$K = \mathbb{Q}(\alpha)$, α intero. Se μ_α é p-Eisenstein $\Rightarrow p\mathscr{O}_K = Q^n$, cioé p é totalmente ramificato in K.*

Dimostrazione. $p \nmid \mathrm{ind}_K(\alpha)$ perché μ_α é p-Eisenstein, dunque si puó applicare Kummer al polinomio $\mu_\alpha(x) \equiv x^n \quad (p)$. □

<u>Osservazione</u>. Nel caso delle estensioni ciclotomiche, abbiamo visto che si poteva applicare Kummer con lo stesso polinomio $\forall$ primo; questo é peró un caso molto fortunato, perché non sempre é possibile.
Infatti, nel caso delle estensioni quadratiche, abbiamo dovuto cambiare polinomio per trattare il primo $p = 2$; peró riuscivamo a trovare, $\forall$ primo, un polinomio μ_α tale che $p \nmid \mathrm{ind}_K(\alpha)$.
Purtroppo in generale questo non é possibile: esistono delle estensioni in cui alcuni primi (ovviamente in numero finito) non possono essere fattorizzati con Kummer. Vediamo alcuni esempi.

Definizione 3.3.1. $K/\mathbb{Q}$ di grado n. $\mathrm{ind}(K) := \gcd\{\mathrm{ind}_K(\alpha) | \alpha \in \mathscr{O}_K \text{ di grado } n\}$.

<u>Osservazione</u>. Se $\mathrm{ind}(K) = 1$, riesco a fattorizzare tutti i primi con Kummer (eventualmente cambiando elemento e polinomio).
Inoltre $\mathscr{O}_K$ monogenico $\Rightarrow \mathrm{ind}(K) = 1$.

<u>Esempi.</u> 1. $\mathrm{ind}(K) = 1 \not\Rightarrow \mathscr{O}_K$ monogenico.
Sia $K = \mathbb{Q}(\sqrt[3]{m})$, $m = ab^2$, $(a, b) = 1$, $\alpha = \sqrt[3]{m}$, $m \not\equiv \pm 1 \quad (9)$.
Abbiamo visto che $\mathrm{disc}(K) = -27a^2b^2$ e $\left\{1, \alpha, \frac{\alpha^2}{b} = \beta\right\}$ é una base intera.
Inoltre:

$$\mathrm{ind}(\alpha) = \sqrt{\frac{\mathrm{disc}(\alpha)}{\mathrm{disc}(K)}} = \sqrt{\frac{-27a^2b^4}{-27a^2b^2}} = b$$

$$\mathrm{ind}(\beta) = \sqrt{\frac{\mathrm{disc}(\beta)}{\mathrm{disc}(K)}} = \sqrt{\frac{-27a^4b^2}{-27a^2b^2}} = a.$$

$\mathrm{ind}(K) | (\mathrm{ind}(\alpha), \mathrm{ind}(\beta)) = (a, b) = 1$, da cui $\mathrm{ind}(K) = 1$.
Vediamo ora che $\mathrm{ind}(\omega) \neq 1$ $\forall \omega$ (cioé non é monogenico).
Sia $\omega \in \mathscr{O}_K$; $\omega = x + y\alpha + z\beta$, $x, y, z \in \mathbb{Z}$.
$\mathrm{ind}(\omega) = \mathrm{ind}(\omega - x)$, poiché $\mathbb{Z}[\omega] = \mathbb{Z}[\omega - x]$; consideriamo dunque $\omega = y\alpha + z\beta$.
$\omega^2 = y^2\alpha^2 + 2yz\alpha\beta + z^2\beta^2$, ma $\alpha\beta = ab$ e $\beta^2 = \alpha a$, quindi, sapendo che $\mathrm{ind}(\omega)$ é pari al valore assoluto del determinante della matrice del cambiamento di base da $\{1, \omega, \omega^2\}$ a $\{1, \alpha, \beta\}$:

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

Dico che $\exists a, b$ tali che $ab^2 \not\equiv \pm 1 \quad (9)$ e $y^3b - z^3a \neq \pm 1 \quad \forall y, z$.
Se $a = 7, b = 5$, $ab^2 \equiv 4 \neq 1 \quad (9)$, e $5y^3 - 7z^3 = \pm 1$ non ha soluzioni intere perché non le ha modulo 7 (poiché $5y^3 \not\equiv \pm 1 \quad (7)$ $\forall z$, in quanto i cubi modulo 7 sono ± 1).
Dunque $K = \mathbb{Q}(\sqrt[3]{7 \cdot 5^2})$ ha indice 1 ma $\mathscr{O}_K$ non é monogenico.

2. $\exists K$ tale che $[K:\mathbb{Q}]=3$ e $\mathrm{ind}(K)=2$.
Sia $\mu_\alpha(x)=x^3-x^2-2x-8$; é irriducibile su $\mathbb{Q}$, in quanto non ha radici razionali, dunque, se $K=\mathbb{Q}(\alpha)$, α radice di μ_α, $[K:\mathbb{Q}]=3$.
Si calcola che:

$$\mathrm{disc}(\alpha)=\mathrm{disc}(\mu_\alpha)=\mathrm{Ris}(\mu_\alpha,\mu'_\alpha)=\det\begin{pmatrix}1&-1&-2&-8&0&0\\0&1&-1&-2&-8&0\\0&0&1&-1&-2&-8\\3&-2&-2&0&0&0\\0&3&-2&-2&0&0\\0&0&3&-2&-2&0\\0&0&0&3&-2&-2\end{pmatrix}=-4\cdot 503.$$

Inoltre $\mathrm{disc}(K)=-503$: sia $\beta=\frac{\alpha^2+\alpha}{2}$; vediamo che é intero.
Con facili calcoli si giunge a: $\alpha^2=2\beta-\alpha$ e $\alpha\beta=2\beta+4$, da cui $\beta^2=\frac{\alpha^4+2\alpha^3+\alpha^2}{4}=6+2\alpha+3\beta$, cioé $\beta^2-3\beta$ é intero, cioé $\beta\in\mathscr{O}_K$.
Osserviamo che $\mathrm{disc}(1,\alpha,\beta)=\left(\frac{1}{2}\right)^2\mathrm{disc}(1,\alpha,\alpha^2)=-503$, da cui $\mathrm{disc}(K)=-503$ (poiché 503 é squarefree) e $\{1,\alpha,\beta\}$ é una base intera.
Sia $\xi=a+b\alpha+c\beta$, $a,b,c\in\mathbb{Z}$; come prima si pone $\xi=b\alpha+c\beta$.
$\xi^2=(6c^2+8bc)+(2c^2-b)\alpha+(2b+3c^2+4bc)\beta$, quindi:

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

poiché se sono entrambi dispari, la somma é pari.
Dunque $\mathrm{ind}(\alpha)=2$, e $\forall\xi\in\mathscr{O}_K$, $\mathrm{ind}(\xi)\equiv 0\quad(2)$, cioé $\mathrm{ind}(K)=2$.
In particolare $\mathscr{O}_K$ non é monogenico.

<u>*Osservazione*</u>. Nell'ultimo esempio, c'é una ragione per cui il primo 2 non si puó fattorizzare tramite Kummer; infatti si puó calcolare che $2\mathscr{O}_K$ si spezza completamente, cioé $2\mathscr{O}_K=P_1P_2P_3$, dunque dovrebbero esistere 3 fattori lineari distinti in $\mathbb{F}_2[x]$, il che é falso perché esistono solo x e $x+1$.

Esercizio (Marcus, n° 30, pag. 91)**.** *$K\subseteq L$ campi di numeri. $\exists$ infiniti primi di K che si spezzano completamente in L.*

Dimostrazione. Dimostriamo innanzitutto un utile lemma:

Lemma. *Sia $f\in\mathbb{Z}[x]$, $\deg(f)\geq 1$. $\exists$ infiniti primi p tali che f ha una radice modulo p.*

Dimostrazione. Notiamo che non é restrittivo supporre $f(0)=1$. Infatti, se $f(0)=0$, divido f per x^k in modo che il termine noto non sia 0; inoltre, se $f(0)=c\neq 0$, considero $g(x)=\frac{f(xf(0))}{f(0)}$, con $g(x)\in\mathbb{Z}[x]$, $g(0)=1$ e $g(x)=0\Rightarrow f(x)=0$, poiché se g ha una radice modulo p e $p|c$, allora $f(0)=0$ modulo p, mentre se $p\nmid c$, allora $g(\alpha)=0$ modulo p e $f(f(0)\alpha)=0$ modulo p.
Supponiamo per assurdo che $\{p|f$ ha una radice modulo $p\}=\{p_1,\dots,p_s\}$.
Sia $n>p_i\ \forall i$ e consideriamo $f(n!)\neq 0$ (altrimenti $f(n!)\equiv 0\quad(p)\ \forall p$ primo). Inoltre $f(n!)\neq\pm 1$ (altrimenti cambio n, e se $\forall n$ si avesse che $f(n!)=\pm 1$ allora $f=\pm 1$, assurdo).
Ma allora $\exists p$ primo che divide $f(n!)$, cioé $f(n!)\equiv 0\quad(p)$; peró $p\notin\{p_1,\dots,p_s\}$, in quanto $p_i|n!\wedge p_i\nmid 1\Rightarrow p_i\nmid f(n!)$, assurdo. □

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

Sia $M = \widetilde{L}$ la chiusura normale di $L/\mathbb{Q}$; $M = \mathbb{Q}(\alpha)$, α intero, μ_α polinomio minimo di α.
Per Kummer, tutti i primi tranne al piú un numero finito si fattorizzano come $\overline{\mu_\alpha}$ modulo p; ma allora, se $\mathscr{P}_M = \{p \in \mathbb{Z} | \exists U \subseteq \mathscr{O}_M, U|p, f(U|p) = 1\}$, $|\mathscr{P}_M| = +\infty$ per il lemma.
Notiamo che $p \in \mathscr{P}_M \Rightarrow p\mathscr{O}_M = (U_1 \cdot \ldots \cdot U_s)^e$ con $f(U_i|p) = 1\ \forall i$, poiché M é di Galois.
Dunque $e \cdot s = [M : \mathbb{Q}]$, ma i primi ramificati sono in numero finito $\Rightarrow e = 1$ per un numero finito di primi, cioé un numero infinito di primi si spezza completamente.
In altre parole, ponendo $\mathscr{P}'_M = \mathscr{P}_M \backslash \{\text{primi ramificati}\} = \{\text{primi che si spezzano completamente}\}$, $|\mathscr{P}'_M| = +\infty$.
Visto che $\forall p$ c'é almeno un primo $P \subseteq \mathscr{O}_K$, $P|p$, anche i primi di $\mathscr{O}_K$ che si spezzano completamente sono in numero infinito.
A questo punto basta osservare che $P\mathscr{O}_M$ si spezza completamente $\Rightarrow P\mathscr{O}_L$ si spezza completamente, poiché indice di ramificazione e grado d'inerzia sono moltiplicativi nelle torri. □

Corollario 3.3.3. *Esistono infiniti primi nella progressione aritmetica* $1 + km\ \forall m \in \mathbb{Z}$.
In altre parole, esistono infiniti primi $p \equiv 1 \quad (m)\ \forall m \in \mathbb{Z}$.

Dimostrazione. Consideriamo $K = \mathbb{Q}(\zeta_m)$. Esistono infiniti primi di $\mathbb{Q}$ che si spezzano completamente in K.
Questi primi hanno $e = f = 1$; $e = 1 \Rightarrow p \nmid \operatorname{disc}(K) = m$, mentre $f = 1 \Rightarrow \operatorname{ord}_m^\times(p) = f = 1$, cioé $p \equiv 1 \quad (m)$. □

4 Fattorizzazione di ideali primi in estensioni di Galois

In questa sezione spostiamo il nostro interesse sulle estensioni di Galois; abbiamo infatti giá intravisto che in tali estensioni valgono proprietá speciali, ed alcune di esse possono essere utilizzate per lavorare su estensioni generiche, passando alla chiusura normale.

4.1 Gruppo di decomposizione e gruppo d'inerzia

Nel seguito sia L/K un'estensione normale, $G = \mathrm{Gal}(L/K)$.

Osservazione. Sia $\sigma \in G$; σ puó essere ristretta a $\sigma : \mathscr{O}_L \to \mathscr{O}_L$.
Sia $Q \subseteq \mathscr{O}_L$ primo. Abbiamo il diagramma:

$$\begin{array}{ccc} \mathscr{O}_L & \xrightarrow{\sigma} & \mathscr{O}_L \\ \downarrow{\scriptstyle \pi} & \searrow^{\varphi} & \downarrow{\scriptstyle \pi_Q} \\ \dfrac{\mathscr{O}_L}{\mathrm{Ker}(\varphi)} & \xrightarrow[\overline{\sigma}]{\sim} & \dfrac{\mathscr{O}_L}{Q} \end{array}$$

Notiamo che $\mathrm{Ker}(\varphi) = \sigma^{-1}(Q)$; $\sigma^{-1}(Q)$ é primo e $Q|P \Rightarrow \sigma^{-1}(Q)|P$; per quanto visto prima $\frac{\mathscr{O}_L}{\sigma^{-1}(Q)} \cong \frac{\mathscr{O}_L}{Q}$.

Definizione 4.1.1. Sia $P \subseteq \mathscr{O}_K$ primo, $Q|P$. Definiamo **gruppo di decomposizione** di Q su P lo stabilizzatore di Q in G, cioé:

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

Osservazione. Sia $\sigma \in D(Q|P)$; il diagramma precedente diventa:

$$\begin{array}{ccc} \mathscr{O}_L & \xrightarrow{\sigma} & \mathscr{O}_L \\ \downarrow & & \downarrow \\ \dfrac{\mathscr{O}_L}{Q} & \xrightarrow[\overline{\sigma}]{\sim} & \dfrac{\mathscr{O}_L}{Q} \end{array}$$

cioé $\overline{\sigma}$ é un automorfismo di $\frac{\mathscr{O}_L}{Q}$, cioé:

$$\overline{\sigma} \in \mathrm{Gal}\Big(\frac{\mathscr{O}_L}{Q}\Big|\frac{\mathscr{O}_K}{P}\Big) =: \overline{G}.$$

Inoltre l'applicazione:

$$\begin{array}{rccc} \psi: & D(Q|P) & \longrightarrow & \overline{G} \\ & \sigma & \longrightarrow & \overline{\sigma} \end{array}$$

é un omomorfismo di gruppi, con $\mathrm{Ker}(\psi) = \big\{\sigma \in D(Q|P)\big|\overline{\sigma}(\overline{\alpha}) = \overline{\alpha}\ \forall \overline{\alpha} \in \frac{\mathscr{O}_L}{Q}\big\} = \{\sigma \in G | \sigma(\alpha) \equiv \alpha \pmod{Q}\ \forall \alpha \in \mathscr{O}_L\}$.

Definizione 4.1.2. Nelle notazioni dell'osservazione precedente, $\mathrm{Ker}(\psi)$ si definisce **gruppo d'inerzia** di Q su P e si denota $E(Q|P)$.

Osservazione. Abbiamo che $E(Q|P) \triangleleft D(Q|P)$ e:

$$\frac{D(Q|P)}{E(Q|P)} \hookrightarrow \overline{G}.$$

In particolare, $\left|\frac{D(Q|P)}{E(Q|P)}\right| \Big| f(Q|P) = |\overline{G}|$.

Teorema 4.1.1. *Sia $P \subseteq \mathscr{O}_K$, $Q|P$. $E = E(Q|P)$, $D = D(Q|P)$. Allora, se $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e$ con indice d'inerzia f:*

			indice ramificazione	*grado inerzia*
$\mathscr{O}_L$	L	Q		
	$\vert_e$	$\vert$	e	1
$\mathscr{O}_{L^E}$	L^E	$Q_E = Q \cap \mathscr{O}_{L^E}$		
	$\vert_f$	$\vert$	1	f
$\mathscr{O}_{L^D}$	L^D	$Q_D = Q \cap \mathscr{O}_{L^D}$		
	$\vert_r$	$\vert$	1	1
$\mathscr{O}_K$	K	$P = Q \cap \mathscr{O}_K$		

Dimostrazione.

- $[L^D : K] = r$.
  Infatti $[L^D : K] = [G : D] = [G : \mathrm{Stab}_G(Q)] = |\operatorname{orb}_G(Q)| = r$ perché l'azione é transitiva.

- $f(Q|Q^E) = 1$.
  Per definizione $f(Q|Q_E) = \left[\frac{\mathscr{O}_L}{Q} : \frac{\mathscr{O}_{L^E}}{Q_E}\right]$; inoltre $\exists\overline{\alpha}$ tale che $\frac{\mathscr{O}_L}{Q} = \frac{\mathscr{O}_{L^E}}{Q_E}(\overline{\alpha})$, in quanto ogni estensione finita di campi finiti é separabile (e quindi semplice).
  Sia $\alpha \in \mathscr{O}_L$ tale che $\pi_Q(\alpha) = \overline{\alpha}$; il polinomio:

  $$g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha)) \in \mathscr{O}_{L^E}[x]$$

  é un multiplo del polinomio minimo, ma, se $\overline{g}(x) = \pi_{Q_E}(g(x))$:

  $$\overline{g}(x) = \prod_{\sigma \in E} (x - \underbrace{\overline{\sigma(\alpha)}}_{=\overline{\sigma}(\overline{\alpha})}) = (x - \overline{\alpha})^{|E|}.$$

  $\mu_{\overline{\alpha}} | \overline{g}(x) \Rightarrow \mu_{\overline{\alpha}} = x - \overline{\alpha}$, cioé $\left[\frac{\mathscr{O}_L}{Q} : \frac{\mathscr{O}_{L^E}}{Q_E}\right] = 1$.

- Q é l'unico primo di $\mathscr{O}_L$ sopra Q_D.
  Infatti $\mathrm{Gal}(L/L^D) = D$ e il gruppo di Galois agisce transitivamente sui primi sopra Q_D, ma per definizione di D, $\sigma(Q) = Q\ \forall\sigma \in D$.

A questo punto abbiamo che $[L : L^D] = ef$ e $e(Q|Q_D)f(Q|Q_D) = [L : L^D]$; peró per moltiplicativitá nelle torri, $e(Q|Q_D)|e \wedge f(Q|Q_D)|f$, dunque ci sono uguaglianze.
Quindi $f(Q_D|P) = e(Q_D|P) = 1$.
Ma abbiamo visto che $f(Q|Q_E) = 1 \Rightarrow f(Q_E|Q_D) = f$, da cui $[D : E]|f \Rightarrow [D : E] = [L^E : L^D] = f$, da cui $e(Q_E|Q_D) = 1$.
Di conseguenza $[L : L^E] = e$ e $e(Q|Q_E) = e$. □

Corollario 4.1.2. $\frac{D(Q|P)}{E(Q|P)} \cong \overline{G}$.
In particolare é ciclico di ordine f.

Dimostrazione. $[D : E] = f$ e il gruppo di Galois di estensioni di campi finiti é sempre ciclico. □

Osservazioni. 1. $Q_D\mathscr{O}_L = Q^e$. In particolare Q é l'unico primo di $\mathscr{O}_L$ sopra Q_D.

2. Q_D é non ramificato e ha grado d'inerzia 1 su P (ma in generale L^D/K non é di Galois e quindi in generale $P\mathscr{O}_{L^D} = Q_D Q_1'^{e_1} \cdot \ldots \cdot Q_s'^{e_s}$).

3. Q_E é totalmente ramificato in $\mathscr{O}_L$.
   $Q_E\mathscr{O}_L = Q^e$, e non ci sono altri primi perché e é il grado dell'estensione.

4. Q_E non é ramificato su P, ma sugli altri primi della fattorizzazione non si puó dire niente; in particolare non é detto che P si spezzi completamente in L^D.
   Infatti, se $Q'|P$, $Q \neq Q'$, in generale $D(Q|P) \neq D(Q'|P)$; peró $|D(Q|P)| = |D(Q'|P)|$, in quanto r, e, f non dipendono dal primo sopra P.
   Inoltre, se $Q' = \sigma(Q)$:
   $$D(\sigma(Q)|P) = \sigma D(Q|P)\sigma^{-1}.$$
   Infatti hanno la stessa cardinalitá e $\tau \in D(Q|P) \Rightarrow \tau(Q) = Q \Rightarrow \sigma\tau\sigma^{-1}(\sigma(Q)) = \sigma(Q) \Rightarrow \sigma\tau\sigma^{-1} \in D(\sigma(Q)|P)$.
   Analogamente:
   $$E(\sigma(Q)|P) = \sigma E(Q|P)\sigma^{-1}.$$
   Infine per la teoria di Galois $L^{\sigma D\sigma^{-1}} = \sigma(L^D)$; se $D \triangleleft G$, L^D é campo di decomposizione di tutti i primi di $\mathscr{O}_L$ sopra P, dunque ogni primo ha $e = f = 1$, cioé P si spezza completamente in $\mathscr{O}_{L^D}$.

Esercizio (Marcus, n° 20, pag. 87)**.** *$K \subseteq L$ campi di numeri, $[L : K] = n$, $P \subseteq \mathscr{O}_K$ primo. Sappiamo che $\frac{\mathscr{O}_L}{P\mathscr{O}_L}$ é un $\frac{\mathscr{O}_K}{P}$-spazio vettoriale di dimensione n. Poniamo $P\mathscr{O}_L = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$. Sia $\mathscr{B}_i$ una $\frac{\mathscr{O}_K}{P}$-base di $\frac{\mathscr{O}_L}{Q_i}$, $|\mathscr{B}_i| = f_i$, $\mathscr{B}_i = \left\{\beta_\lambda^{(i)}\right\}$.*
$\forall i = 1, \ldots, r$, $\forall j = 1, \ldots, e_i = e(Q_i|P)$, prendiamo $\alpha_{ij} \in (Q_i^{j-1} \backslash Q_i^j) \cap \bigcap_{h\neq i} Q_h^{e_h}$ (che esiste perché $Q_i^{j-1} \cap \bigcap_{h\neq i} Q_h^{e_h} \neq \emptyset$ per il teorema cinese, ed almeno uno di questi elementi non sta in Q_i^j, altrimenti si avrebbe $Q_i^{j-1} \cap \bigcap_{h\neq i} Q_h^{e_h} \subseteq Q_i^j$, assurdo perché hanno primi distinti nella fattorizzazione).
Sia $\mathscr{B} = \left\{\alpha_{ij}\beta_\lambda^{(i)}\right\}$, $\lambda = 1, \ldots, f_i, j = 1, \ldots, e_i, i = 1, \ldots, r$.
Allora le proiezioni modulo $P\mathscr{O}_L$ di $\mathscr{B}$ sono indipendenti su $\frac{\mathscr{O}_K}{P}$, cioé sono una base di $\frac{\mathscr{O}_L}{P\mathscr{O}_L}$ su $\frac{\mathscr{O}_K}{P}$.

Dimostrazione. Supponiamo che valga la relazione di dipendenza:

$$\sum_{i,j,\lambda} a_{ij\lambda}\alpha_{ij}\beta_\lambda^{(i)} \equiv 0 \quad (P\mathscr{O}_L),\ a_{ij\lambda} \in \mathscr{O}_K.$$

La tesi é che $a_{ij\lambda} \equiv 0 \quad (P)\ \forall i, j, \lambda$.
Abbiamo che, $\forall t$:

$$\sum_{i,j,\lambda} a_{ij\lambda}\alpha_{ij}\beta_\lambda^{(i)} \equiv 0 \quad (Q_t);$$

ma se $i \neq t$, $\alpha_{ij} \in Q_t^{e_t}$, dunque:

$$\sum_{j,\lambda} a_{tj\lambda}\alpha_{tj}\beta_\lambda^{(t)} \equiv 0 \quad (Q_t).$$

Inoltre $\alpha_{tj} \in Q_t^{j-1}$, dunque, se $j \geq 2$, $\alpha_{tj} \in Q_t$, da cui:

$$\underbrace{\overline{\alpha_{t1}}}_{\notin Q_t} \sum_\lambda a_{t1\lambda}\beta_\lambda^{(t)} \equiv 0 \quad (Q_t),$$

cioé $a_{t1\lambda} \equiv 0 \quad (Q_t)$, in quanto $\left\{\beta_\lambda^{(t)}\right\}_t$ era una base.
Ripetendo lo stesso ragionamento per $Q_t^2, \dots, Q_t^{e_t} | P\mathscr{O}_L$, considerando la congruenza modulo $Q_t^2, \dots, Q_t^{e_t}$, si ottiene $a_{t2\lambda} \equiv 0 \quad (Q_t^2), \dots, a_{te_t\lambda} \equiv 0 \quad (Q_t^{e_t})$, da cui $a_{tj\lambda} \equiv 0 \quad (P)$ ripetendo il ragionamento $\forall t$. □

Esercizio (Marcus, n° 21, pag. 88)**.** *Riprendendo la notazione dell'esercizio precedente, sia $K = \mathbb{Q}$ e $P = p\mathbb{Z}$. Allora:*

1. *$\alpha_1, \dots, \alpha_n \in \mathscr{O}_L$ sono indipendenti modulo $p \Rightarrow p \nmid \left|\frac{\mathscr{O}_L}{G}\right|$, dove $G = \langle \alpha_1, \dots, \alpha_n \rangle_\mathbb{Z}$.*
   (Dunque $p^k | \operatorname{disc}(\alpha_1, \dots, \alpha_n) \iff p^k | \operatorname{disc}(\mathscr{O}_L)$).
2. *$p^k | \operatorname{disc}(L)$ per $k = n - \sum_{i=1}^r f_i$.*

Dimostrazione. 1. Se per assurdo $p \left| \frac{\mathscr{O}_L}{G} \right| \Rightarrow \exists \beta \in \mathscr{O}_L \backslash G$ tale che $p\beta \in G \Rightarrow p\beta = \sum_{i=1}^n \lambda_i \alpha_i$, con $\lambda_i \in \mathbb{Z}$, ma $\exists i$ per cui $p \nmid \lambda_i$ (altrimenti $\beta \in G$).
Allora $\sum_{i=1}^n \lambda_i \alpha_i \equiv 0 \quad (p\mathscr{O}_L) \Rightarrow \lambda_i \equiv 0 \quad (p)$ (in quanto $\alpha_1, \dots, \alpha_n$ erano indipendenti modulo p), assurdo.

2. Mi basta vedere che $p^k | \operatorname{disc}(\gamma_1, \dots, \gamma_n)$, con $\gamma_1, \dots, \gamma_n$ indipendenti modulo p.
   Scegliamo una n-upla costruita come nell'esercizio precedente; sappiamo che:

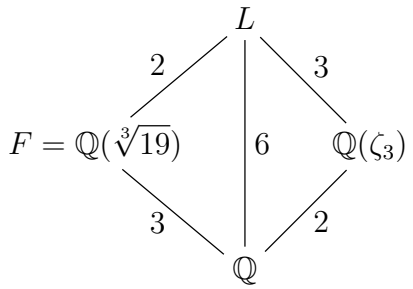
$$\operatorname{disc}(\{\alpha_{ij}\beta_\lambda^{(i)}\}_{i,j,\lambda}) = \det\left(\operatorname{Tr}(\alpha_{ij}\beta_\lambda^{(i)}\alpha_{i'j'}\beta_{\lambda'}^{(i')})\right).$$

   Sia $\widetilde{L}$ la chiusura di Galois di $L/\mathbb{Q}$; se mostrassi che per $n - \sum_{i=1}^r f_i$ colonne della matrice $\operatorname{Tr}(\alpha_{ij}\beta_\lambda^{(i)}\alpha_{i'j'}\beta_{\lambda'}^{(i')})$, ogni elemento della colonna sta in un primo $Q \subseteq \mathscr{O}_{\widetilde{L}}$ sopra p, avrei la tesi (poiché il determinante é multilineare e posso portare fuori questi k fattori p).
   Osserviamo peró che basta ancora meno per giungere alla tesi: infatti se mostriamo che k elementi del tipo $\alpha_{ij}\beta_\lambda^{(i)}\alpha_{i'j'}\beta_{\lambda'}^{(i')}$ stanno in tutti i primi di $\mathscr{O}_{\widetilde{L}}$ sopra p, anche i loro coniugati ci staranno (poiché $\widetilde{L}/\mathbb{Q}$ é di Galois), e dunque ci staranno anche le tracce (che sono somme).
   Notiamo che, se $j \geq 2$, $\alpha_{ij}\beta_\lambda^{(i)} \in Q \ \forall Q | p$ per costruzione; inoltre $\alpha_{i1}\beta_\lambda^{(i)}$ sta in tutti i $Q|p$ tranne quelli sopra Q_i.
   Dunque $\alpha_{ij}\beta_\lambda^{(i)}\alpha_{i'j'}\beta_{\lambda'}^{(i')}$ non sta in tutti i $Q|p$ solo nel caso in cui $i = i'$ e $j = j' = 1$; $\forall i$, ho f_i scelte di λ, dunque in totale le colonne non divisibili per p sono esattamente $\sum_{i=1}^r f_i$, da cui la tesi.

   □

Esempio. $L = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$, $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathcal{S}_3$.
Allora $3\mathscr{O}_L = (Q_1Q_2Q_3)^2$, $f = 1$.

Dimostrazione. Abbiamo il diagramma:



Per la teoria svolta, $3 | \operatorname{disc}(\mathbb{Q}(\zeta_3)) \Rightarrow 3\mathscr{O}_{\mathbb{Z}[\zeta_3]} = P^2$ (poiché ramifica); inoltre $\operatorname{disc}(F) = -3 \cdot 19^2$, dunque $3\mathscr{O}_F = Q^3 \vee 3\mathscr{O}_F = Q^2Q'$.
Ma la prima possibilitá é da escludere per la proposizione precedente, altrimenti $3^{3-1} | \operatorname{disc}(F)$,

assurdo.
Dunque $2|e(Q_1|3)$, ma $r \geq 2$, dunque $r = 3$, $e(Q_1|3) = 2$ e $f = 1$, cioé $3\mathscr{O}_L = (Q_1Q_2Q_3)^2$.
Inoltre, per la teoria di Galois, le sottoestensioni di L di grado 3 su $\mathbb{Q}$ sono $F = \mathbb{Q}(\sqrt[3]{19})$, $F' = \mathbb{Q}(\zeta_3\sqrt[3]{19})$, $F'' = \mathbb{Q}(\zeta_3^2\sqrt[3]{19})$; questi tre campi sono i campi di decomposizione dei primi Q_1, Q_2, Q_3. □

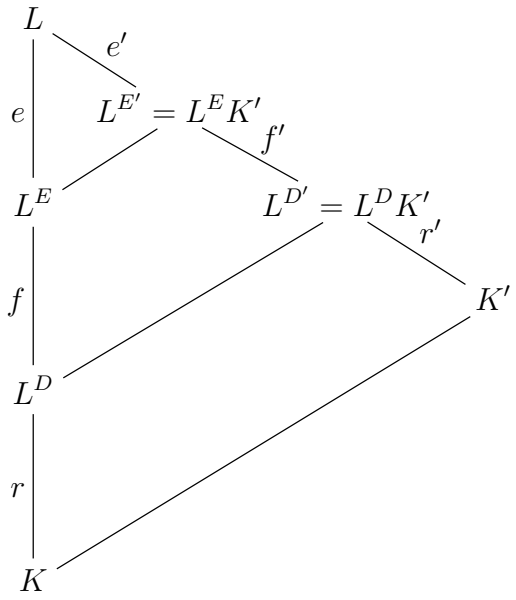
Siano date le estensioni $K \subseteq K' \subseteq L$; diciamo che $K' = L^H$ per un certo $H < G$. Sia $Q \subseteq \mathscr{O}_L$, e siano $P' = Q^c = Q \cap K'$ e $P = P'^c = P' \cap K$; allora $\mathrm{Gal}(L/K') = H$ e:

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

Da questo segue che, se $E' = E(Q|P')$, $D' = D(Q|P')$:

$$L^{E'} = L^{E \cap H} = L^E L^H = L^E K' \qquad L^{D'} = L^{D \cap H} = L^D K'.$$

Abbiamo dunque il diagramma di estensioni:



Teorema 4.1.3. *Secondo le notazioni precedenti, valgono i seguenti fatti:*

1. *L^D é il piú grande campo intermedio K' tale che $f(P'|P) = e(P'|P) = 1$.*
2. *L^D é il piú piccolo campo intermedio K' tale che $\exists$ un unico primo di $\mathscr{O}_L$ sopra P'.*
3. *L^E é il piú grande campo intermedio K' tale che P' non é ramificato su P.*
4. *L^E é il piú piccolo campo intermedio K' tale che Q é totalmente ramificato su P'.*

Dimostrazione. Sicuramente L^D e L^E soddisfano tali condizioni; vediamo che valgono anche le condizioni di minimalitá/massimalitá:

1. Se K' é tale che $f(P'|P) = e(P'|P) = 1 \Rightarrow e' = e(Q|P') = e$, $f' = f(Q|P') = f$, ma $L \supseteq L^{D'} \supseteq L^D$ con $[L : L^D] = ef$, $[L : L^{D'}] = e'f'$, dunque $L^D = L^{D'} = L^D K'$, da cui $K' \subseteq L^D$.
2. Se K' é tale che in $\mathscr{O}_L$ c'é un solo primo sopra P', allora $r' = 1$, e dal diagramma precedente si ha $K' = L^D K'$, da cui $L^D \subseteq K'$.

3. Se K' é tale che $e(P'|P) = 1 \Rightarrow e = e'$, ma $L \supseteq L^{E'} \supseteq L^E$, da cui $L^E = L^E K'$, cioé $K' \subseteq L^E$.

4. Se K' é tale che Q é totalmente ramificato su P', allora $f' = r' = 1$, da cui $L^E K' = K'$, cioé $L^E \subseteq K'$.

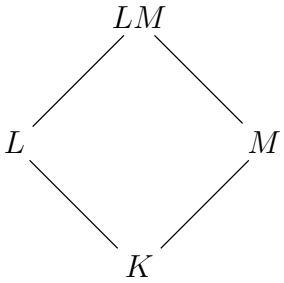
□

Corollario 4.1.4. *$D \triangleleft G \iff P$ si spezza completamente in L^D.*

Dimostrazione. L'implicazione $\Rightarrow$ é giá stata vista come osservazione; vediamo l'altra.
P si spezza completamente in $L^D \Rightarrow$ per 1) del teorema precedente L^D contiene il campo di decomposizione di tutti i primi $Q'|P$, $Q' = \sigma(Q)$.
Dunque $\forall Q'|P$, $L^{D'} \subseteq L^D$, ma hanno lo stesso grado, dunque $L^D = L^{D'} \Rightarrow D' = D$, cioé $\sigma D \sigma^{-1} = D \ \forall \sigma \in G$. □

Corollario 4.1.5. *$D \triangleleft G$. P si spezza completamente in $K' \iff K' \subseteq L^D$.*

Teorema 4.1.6. *Dato il diagramma di estensioni:*



sia $P \subseteq \mathscr{O}_K$. Allora:

1. *P non ramificato in L e $M \Rightarrow P$ é non ramificato in LM.*

2. *P si spezza completamente in L e $M \Rightarrow P$ si spezza completamente in LM.*

Dimostrazione. Sia F la chiusura normale di LM/K.

1. Sia $Q \subseteq \mathscr{O}_F$, $Q|P$; denotiamo $P' = Q \cap LM$.
   Se F^E é il campo d'inerzia di $Q|P$, per il punto 3) del teorema precedente $L, M \subseteq F^E$, quindi $LM \subseteq F^E$, ma allora $e(P'|P)|e(Q^E|P) = 1$.

2. $\mathscr{O}_F \supseteq Q|P$, $P' = Q \cap LM$, $P_L = P' \cap L$, $P_M = P' \cap M$.
   $e(P_L|P) = f(P_L|P) = 1 \Rightarrow L, M \subseteq F^D \Rightarrow LM \subseteq F^D$.
   Ma allora $e(P'|P)|e(Q_D|P) = 1$ e analogamente $f(P'|P) = 1$, cioé la tesi.

□

<u>*Osservazione*</u>. $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_p)$. Se $q \neq p \Rightarrow e = 1$, cioé $q\mathscr{O}_L = P_1 \cdot \ldots \cdot P_r$; inoltre $f = \mathrm{ord}_p^{\times}(q)$, da cui $r = \frac{p-1}{f}$.
$G = \mathrm{Gal}(L/K)$ é abeliano, quindi $D \triangleleft G$, dunque L^D é campo di decomposizione di tutti i primi sopra q.
Inoltre $\forall d|p-1$, $\exists! F_d$ tale che $[F_d : \mathbb{Q}] = d$ (e dunque $[L : F_d] = \frac{p-1}{d}$); F_r sará il campo di decomposizione.

Teorema 4.1.7. *p primo, $d|p-1$, $q \neq p$ primo.*
q si spezza completamente in $F_d \iff q$ é una potenza d-esima in $\mathbb{Z}/p\mathbb{Z}$.

Dimostrazione. q si spezza completamente in $F_d \iff F_d \subseteq F_r \iff d|r$.
Ora, q é potenza d-esima modulo $p \iff q^{\frac{p-1}{d}} \equiv 1 \quad (p)$. Infatti l'implicazione $\Rightarrow$ é ovvia, mentre per l'altra basta notare che, se $\mathbb{F}_p = \langle \xi \rangle$, $\mathrm{ord}(\xi) = p-1$, e $q = \xi^a$, allora $\mathrm{ord}(q) = \frac{p-1}{(a,p-1)}$; sapendo che $\mathrm{ord}(q) \Big| \frac{p-1}{d}$, si ha $d|(a, p-1)$, cioé $d|a$.
Ma $\mathrm{ord}_p^{\times}(q) = f \Rightarrow f \Big| \frac{p-1}{d}$; visto che $f = \frac{p-1}{r}$, si conclude $d|r$. □

Definizione 4.1.3. p primo, $n \in \mathbb{Z}$, $p \nmid n$. Definiamo **simbolo di Legendre**:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{se } n \equiv \square \quad (p) \\ -1 & \text{se } n \not\equiv \square \quad (p) \end{cases}.$$

Teorema 4.1.8 (Legge di reciprocitá quadratica)**.** *$p \neq q$ primi. Se $p, q > 2$, si ha:*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{se } p \equiv 1 \quad (4) \vee q \equiv 1 \quad (4) \\ -\left(\frac{p}{q}\right) & \text{altrimenti} \end{cases}$$

mentre se $q = 2$:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \quad (8) \\ -1 & \text{se } p \equiv \pm 3 \quad (8) \end{cases}.$$

Dimostrazione. $\left(\frac{q}{p}\right) = 1 \iff q$ é un quadrato modulo $p \iff q$ si spezza completamente in F_2.
Ma $F_2 = \mathbb{Q}(\sqrt{\pm p})$, $+$ se $p \equiv 1 \quad (4)$, $-$ altrimenti, dunque distinguiamo i casi.

$p \equiv 1$ (4): Sia $q \neq 2$. $\mathbb{Z}[\sqrt{p}] \overset{2}{\subseteq} \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]$.
Possiamo utilizzare $x^2 - p$ per applicare Kummer, in quanto $q \nmid 2$; ma $x^2 - p$ si spezza modulo $q \iff p$ é un quadrato modulo q.
Se $q = 2$, uso il polinomio $x^2 + x + \frac{p-1}{4}$; questo si spezza completamente in $F_2 \iff p - 1 \equiv 0 \quad (8)$.

$p \equiv 3$ (4): $F_2 = \mathbb{Q}(\sqrt{-p})$ e $-p \equiv 1 \quad (4) \Rightarrow \mathbb{Z}[\sqrt{-p}] \overset{2}{\subseteq} \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$.
Se $q \neq 2$, come prima $x^2 + p$ si spezza $\iff -p$ é un quadrato modulo q.
Se $q \equiv 1 \quad (4) \Rightarrow -1$ é un quadrato, dunque $-p$ é un quadrato modulo $q \iff p$ é un quadrato modulo q.
Altrimenti, se $q \equiv 3 \quad (4)$, $-p$ é un quadrato modulo $q \iff p$ non é un quadrato modulo q.
Se $q = 2$, 2 é un quadrato modulo $p \iff 2$ si spezza in $F_2 = \mathbb{Q}(\sqrt{-p}) \iff x^2 + x + \frac{1+p}{4}$ si spezza $\iff p \equiv -1 \quad (8)$.

□

Concludiamo ora la dimostrazione di un teorema giá enunciato, ma di cui é stata mostrata una sola implicazione:

Teorema 4.1.9. *K campo di numeri, p primo. $p|\operatorname{disc}(K) \iff p$ é ramificato.*

Dimostrazione. L'implicazione $\Leftarrow$ é giá stata vista; vediamo l'altra.
$\{\alpha_1, \ldots, \alpha_n\}$ base intera di K. Sappiamo che:

$$\operatorname{disc}(K) = \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right),$$

dunque $p|\operatorname{disc}(K) \iff \det(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)) \equiv 0 \quad (p) \iff \det(\overline{\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)}) = 0$.
Dunque $\exists m_1, \dots, m_n$ non tutti nulli modulo p tali che:

$$\sum_{i=1}^{n} m_i \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) \equiv 0 \quad (p)\ \forall j.$$

Se poniamo $\alpha = \sum_{i=1}^{n} m_i\alpha_i$, la condizione precedente si riscrive come:

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha\alpha_j) \equiv 0 \quad (p)\ \forall j, \qquad \text{cioé} \qquad \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathscr{O}_K) \subseteq p\mathbb{Z}.$$

Ma $\alpha \notin p\mathscr{O}_K$, poiché una base di $p\mathscr{O}_K$ si ottiene moltiplicando per p una base di $\mathscr{O}_K$, dunque se stesse in $p\mathscr{O}_K$ sarebbe somma di multipli di $p\alpha_i$, che non é vero perché gli m_i non sono tutti nulli modulo p.
Sia per assurdo p non ramificato. $p\mathscr{O}_K = P_1 \cdot \ldots \cdot P_r$.
$\alpha \notin p\mathscr{O}_K \Rightarrow \exists P = P_i$ tale che $\alpha \notin P$.
Sia L la chiusura normale di $K/\mathbb{Q}$; p non ramificato in $K \Rightarrow p$ non ramificato in L, in quanto non é ramificato in tutti i coniugati di K e dunque neanche nel composto.
P non é ramificato in $\mathscr{O}_L$ per moltiplicativitá dell'indice di ramificazione nelle torri; inoltre $\exists Q|p$, $Q \subseteq \mathscr{O}_L$, tale che $\alpha \notin Q$ (ad esempio se $Q|P$).
Si ha:

$$\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathscr{O}_L) = \operatorname{Tr}_{K/\mathbb{Q}}(\operatorname{Tr}_{L/K}(\alpha\mathscr{O}_L)) = \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \operatorname{Tr}_{L/K}(\mathscr{O}_L)) \subseteq \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathscr{O}_K) \subseteq p\mathbb{Z}.$$

Sia $\beta \in \mathscr{O}_L$ tale che $\beta \notin Q$ ma $\beta \in Q'\ \forall Q \neq Q'|p$ (é possibile per il teorema cinese).
Sia $\gamma \in \mathscr{O}_L$. $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\gamma) \in p\mathbb{Z} \subseteq Q$.
$\forall \sigma \in \operatorname{Gal}(L/\mathbb{Q})\backslash D(Q|p)$, $\alpha\beta\gamma \in \sigma^{-1}(Q)$, in quanto $\sigma^{-1}(Q) \neq Q$ e $\beta \in Q'\ \forall Q' \neq Q$; dunque $\sigma(\alpha\beta\gamma) \in Q$.
Dunque $\sum_{\sigma\in D} \sigma(\alpha\beta\gamma) = \sum_{\sigma\in G} \sigma(\alpha\beta\gamma) - \sum_{\sigma\in G\backslash D} \sigma(\alpha\beta\gamma) \in Q$, cioé $\sum_{\overline{\sigma}\in\overline{D}} \overline{\sigma}(\overline{\alpha\beta\gamma}) = 0$.
Notiamo che $\overline{D} = \overline{G} = \operatorname{Gal}\big(\frac{\mathscr{O}_L}{Q}\big|(\mathbb{Z}/p\mathbb{Z})\big)$, in quanto p é non ramificato, quindi, $\forall \gamma \in \mathscr{O}_L$:

$$\sum_{\overline{\sigma}\in\overline{G}} \overline{\sigma}(\overline{\alpha\beta\gamma}) = 0.$$

Ma $\overline{\alpha\beta} \neq 0$, cioé $\alpha\beta \notin Q$, in quanto Q é primo e $\alpha, \beta \notin Q$, dunque, $\forall \overline{x} \in \frac{\mathscr{O}_L}{Q}$:

$$\sum_{\overline{\sigma}\in\overline{G}} \overline{\sigma}(\overline{x}) = 0,$$

in quanto $\frac{\mathscr{O}_L}{Q}$ é un campo.
Ma questo é assurdo per il teorema di indipendenza dei caratteri. □

Esercizio (Marcus, n° 5, pag. 115)**.** *L/K di Galois, $G = \operatorname{Gal}(L/K)$, $P \subseteq \mathscr{O}_K$ primo.*

1. *Se P é inerte in $L \Rightarrow G$ é ciclico.*
2. *P totalmente ramificato in ogni estensione intermedia, ma non in $L \Rightarrow$ non ci sono estensioni intermedie (cioé G é ciclico di ordine p primo).*
3. *Se ogni estensione intermedia ha un unico primo sopra P, ma per L questo non vale $\Rightarrow$ non ci sono estensioni intermedie.*
4. *P non é ramificato in ogni estensione intermedia, ma é ramificato in $L \Rightarrow \exists\{e\} \neq H \triangleleft G$ minimale, cioé che é contenuto in ogni sottogruppo non banale di G (e dunque $|G| = p^n$ e $H \subseteq Z(G)$).*

5. *P si spezza completamente in ogni estensione intermedia, ma non si spezza in $L \Rightarrow \exists H \triangleleft G$ minimale. Dare un esempio.*

6. *P inerte in ogni estensione intermedia ma non in $L \Rightarrow G$ é ciclico di ordine p^n.*

Dimostrazione. 1. $D = G$, in quanto $r = 1$. Ma $e = 1 \Rightarrow D \cong \overline{G}$, che é ciclico perché gruppo di Galois di campi finiti.

2. $f \cdot r > 1 \Rightarrow E \lneqq G$.
In $L^E \supsetneqq K$, $e(P_E|P) = 1$, cioé P_E non é ramificato in L^E, dunque $L^E = L$.
Ma L^E é il piú piccolo campo in cui P é totalmente ramificato, dunque non ci sono estensioni intermedie.

3. Analogo al precedente usando L^D.

4. P ramificato in $L \Rightarrow L \supsetneqq L^E$, cioé $\{e\} \subsetneqq E$.
P non ramificato in $K' \Rightarrow e(P'|P) = 1$, ma L^E é il piú grande campo tale che $e(P'|P) = 1$, dunque $K' \subseteq L^E$.
Ma quindi $\forall H < G$, $K' = L^H \subseteq L^E \Rightarrow E < H$.
A questo punto E é normale in quanto minimo, G ha ordine potenza di p (altrimenti non potrebbe esistere un sottogruppo minimo) e E sta nel centro perché $Z(G)$ é un sottogruppo non banale (in quanto $|G| = p^n$).

5. La dimostrazione é analoga alla precedente usando L^D. Un esempio puó essere:
Sia $L = \mathbb{Q}(\zeta_5)$, $G = \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. L'unica sottoestensione é $\mathbb{Q}(\sqrt{5})$.
Cerco un primo p tale che $p\mathbb{Q}(\sqrt{5}) = P_1P_2$ e:
$$p\mathbb{Q}(\zeta_5) = \begin{cases} Q_1Q_2 & f = 2 \\ (Q_1Q_2)^2 & f = 1 \end{cases}$$
La seconda possibilitá peró é impossibile, in quanto c'é un solo primo ramificato (5), dunque cerco $q \neq 5$ con $f = 2$, cioé $q^2 \equiv 1 \quad (5)$. 19 va bene.

6. P inerte in $K' \Rightarrow P$ non ramificato in K'.
In L, $e > 1 \vee r > 1$, in quanto non é inerte; se $r > 1$, per 3) G é ciclico di ordine p, cioé la tesi.
Se $e > 1$, per 4) $|G| = p^n$ ed $\exists H \triangleleft G$ minimo, ma per 1) $\frac{G}{Z(G)}$ é ciclico, quindi G é abeliano con un sottogruppo minimo, dunque G é ciclico di ordine p^n.

□

4.2 L'automorfismo di Frobenius

Sia L/K estensione di Galois, $G = \mathrm{Gal}(L/K)$.
Osservazione. $P \subseteq \mathscr{O}_K$ non ramificato in L. $Q \subseteq \mathscr{O}_L$, $Q|P$.
$D(Q|P) \cong \overline{G} = \mathrm{Gal}\big(\frac{\mathscr{O}_L}{Q}\big|\frac{\mathscr{O}_K}{P}\big)$.
$\frac{\mathscr{O}_K}{P} = \mathbb{F}_q$, con q potenza di $p = P \cap \mathbb{Z}$; inoltre $\big[\frac{\mathscr{O}_L}{Q} : \frac{\mathscr{O}_K}{P}\big] = f \Rightarrow \frac{\mathscr{O}_L}{Q} = \mathbb{F}_{q^f}$. $\mathrm{N}(P) = \big|\frac{\mathscr{O}_K}{P}\big| = q$.
Dunque, per la teoria di Galois, $\overline{G} = \langle\varphi\rangle$, dove $\varphi(x) = x^{\mathrm{N}(P)}$; in altre parole, $\overline{G}$ é il sottogruppo di $\mathrm{Gal}\big(\frac{\mathscr{O}_L}{Q} : \mathbb{F}_p\big)$ che fissa $\frac{\mathscr{O}_K}{P}$.

Definizione 4.2.1. L'automorfismo φ della precedente osservazione si definisce **automorfismo di Frobenius**. Inoltre l'isomorfismo:
$$\begin{array}{ccc} \overline{G} & \xleftrightarrow{\sim} & D(Q|P) \\ \varphi & \longrightarrow & \phi(Q|P) \end{array}$$
identifica φ con l'elemento $\phi(Q|P)$, che prende il nome di **Frobenius di** $Q|P$.

Osservazione. $\phi(Q|P)(x) \equiv x^{\mathrm{N}(P)} \quad (Q)$; inoltre tale proprietá identifica un unico elemento di G (in quanto un tale automorfismo deve stare in $D(Q|P)$ perché mappa Q in Q).

Osservazione. Se $\sigma \in G$, $\phi(\sigma(Q)|P) = \sigma\phi(Q|P)\sigma^{-1}$; dunque ogni primo $P \subseteq \mathscr{O}_K$ non ramificato individua un'unica classe di coniugio in G:

$$\begin{array}{ccc} \{P \subseteq \mathscr{O}_K | P\mathscr{O}_L \text{ non é ramificato}\} & \longrightarrow & \{\text{classi di coniugio di } G\} \\ P & \longrightarrow & [\phi(Q|P)] \end{array}$$

Se G é abeliano:

$$\begin{array}{ccc} \{P \subseteq \mathscr{O}_K | P\mathscr{O}_L \text{ non é ramificato}\} & \longrightarrow & G \\ P & \longrightarrow & \phi(P) := \phi(Q|P) \end{array}$$

in quanto $\phi(Q|P)$ non dipende da Q.
Inoltre, nel caso abeliano, si ha che $\phi(P)(\alpha) = \alpha^{\mathrm{N}(P)} \quad (Q)\ \forall Q$, dunque $\phi(P)(\alpha) \equiv \alpha^{\mathrm{N}(P)} \quad (P\mathscr{O}_L)$.

Osservazione. Se $\mathrm{ord}(\phi(Q|P)) = f \Rightarrow \left[\frac{\mathscr{O}_L}{Q} : \frac{\mathscr{O}_K}{P}\right] = f$, dunque basta per individuare il tipo di fattorizzazione di $P\mathscr{O}_L$ (in quanto $e = 1$).

Esempi. • Le estensioni quadratiche $K = \mathbb{Q}(\sqrt{m})$, m libero da quadrati.
$\mathrm{Gal}(K/\mathbb{Q}) = \{\pm id\} \cong \mathbb{Z}/2\mathbb{Z}$; per la corrispondenza precedente:

$$p\mathscr{O}_K = \begin{cases} PQ & f = 1 \quad \longrightarrow \quad id \\ P & f = 2 \quad \longrightarrow \quad -id \end{cases}$$

Equivalentemente, potevamo ragionare in questo modo: sappiamo che $\phi(\sqrt{m}) = \pm\sqrt{m}$.
Per ϕ fissato, quali elementi soddisfano l'equazione $\phi(x) \equiv x^p \quad (p)$?
Se $\phi = id$, l'equazione $x \equiv x^p \quad (p)$ ha soluzione in $\overline{\mathbb{F}_p} \iff x \in \mathbb{Z}/p\mathbb{Z}$; dunque $\sqrt{m} = (\sqrt{m})^p \quad (p) \iff \sqrt{m} \in \mathbb{Z}/p\mathbb{Z}$, cioé m é un quadrato modulo p (e dunque per Kummer $r = 2$, che é lo stesso risultato uscito con l'altro ragionamento).

- $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$, $\mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_i | 1 \le i \le m, (i,m) = 1\} \cong (\mathbb{Z}/m\mathbb{Z})^*$, dove $\sigma_i(\zeta_m) = \zeta_m^i$.
Sia $p \nmid m$. $\phi(p) = \sigma_i$ per un certo $(i,m) = 1$, dunque $\zeta_m^i = \phi(\zeta_m) = \zeta_m^p \quad (p\mathscr{O}_L)$, da cui $\zeta_m^{p-i} = 1 \quad (p\mathscr{O}_L)$.
$\mathrm{ord}(\zeta_m) = m$ in $\mathbb{C}^*$.
Visto che $p \nmid m$, $x^m - 1$ é separabile per il criterio della derivata; se $C_m = \{\alpha \in \overline{\mathbb{F}_p} | \alpha^m = 1\} < \overline{\mathbb{F}_p}^*$, $|C_m| = m$.
Dunque $\zeta_m^{p-i} \equiv 1 \quad (p\mathscr{O}_L) \Rightarrow i \equiv p \quad (m)$.

Enunciamo il seguente teorema senza dimostrazione, osservando che, se applicato all'esempio precedente delle estensioni ciclotomiche, dá il teorema di Dirichlet (secondo cui esistono infiniti primi $p \equiv i \quad (m)\ \forall i, m$):

Teorema 4.2.1 (di Artin)**.** *$\forall\sigma$, σ é Frobenius di infiniti primi.*

Osservazione. Sia $K \subseteq L$ un'estensione di grado n; sia $M = \widetilde{L}$ la chiusura normale di L/K (ma un discorso analogo si puó fare $\forall M \supseteq \widetilde{L}$).
Sia $P \subseteq \mathscr{O}_K$ tale che $P\mathscr{O}_M$ non sia ramificato; sia $\mathscr{O}_L \supseteq Q|P$, $\mathscr{O}_M \supseteq U|Q$.
Se $G = \mathrm{Gal}(M/K)$, denotiamo $\phi = \phi(U|P)$; inoltre sia H il sottogruppo di G per cui $L = M^H$.
Posto $X = \{H\sigma | \sigma \in G\}$, consideriamo l'azione:

$$\begin{array}{ccc} D(U|P) = \langle\phi\rangle & \longrightarrow & S(X) \cong S_n \\ \phi & \longrightarrow & \{H\sigma \to H\sigma\phi\} \end{array}$$

in quanto $n = [L : K] = [G : H] = |X|$.
$\mathrm{orb}(H\sigma) = \{H\sigma, H\sigma\phi, \ldots, H\sigma\phi^{m-1}\}$ per un certo $m = |\mathrm{orb}(H\sigma)|$.

Teorema 4.2.2. *Nelle notazioni dell'osservazione precedente, siano $m_1, \dots, m_r$ le lunghezze delle r orbite degli elementi di X sotto l'azione di $\langle\phi\rangle$, con $n = m_1 + \dots + m_r$.*
Allora $P\mathcal{O}_L = Q_1 \cdot \dots \cdot Q_r$ con $f(Q_i|P) = m_i$ e $Q_i = \sigma_i(U) \cap \mathcal{O}_L$, dove $H\sigma_i$ é un rappresentante della i-esima orbita.

Dimostrazione. I $\sigma_i(U)$, con $1 \leq i \leq n$ sono i primi di $\mathcal{O}_M$ sopra P; dunque i $\sigma_i(U) \cap \mathcal{O}_L$, con $1 \leq i \leq n$, sono i primi di $\mathcal{O}_L$ sopra P; dico che $Q_i \neq Q_j \ \forall 1 \leq i \neq j \leq r$ (e mi basterebbe per dedurre il tipo di fattorizzazione di P).
Se $Q_i = Q_j$, $\sigma_i(U)$ e $\sigma_j(U)$ stanno sopra lo stesso primo di L, dunque $\exists \tau \in \mathrm{Gal}(M/L) = H$ tale che $\tau\sigma_i(U) = \sigma_j(U)$.
Ma allora $\sigma_j^{-1}\tau\sigma_i(U) = U$, cioé $\sigma_j^{-1}\tau\sigma_i \in D(U|P) = \langle\phi\rangle$, da cui $\sigma_j^{-1}\tau\sigma_i = \phi^l$. Dunque $\tau\sigma_i = \sigma_j\phi^l$, ma $\tau \in H \Rightarrow H\sigma_i = H\sigma_j\phi^l$, cioé stanno nella stessa orbita, assurdo.
Ci rimane da vedere che $f_i = f(Q_i|P) = m_i$; notiamo che basta la disuguaglianza $m_i \leq f_i$, in quanto:

$$\sum_i m_i = \sum_i f_i = n.$$

Se vedo che $H\sigma_i\phi^{f_i} = H\sigma_i$, cioé $\sigma_i\phi^{f_i}\sigma_i^{-1} \in H$, avrei la tesi (in quanto si avrebbe che $m_i | f_i$).
Considero $\phi(\sigma_i(U)|Q_i) \in H$: $\phi(\sigma_i(U)|Q_i) \in D(\sigma_i(U)|P) = \langle\phi(\sigma_i(U)|P)\rangle$; inoltre $\phi(\sigma_i(U)|P) = \sigma_i\phi\sigma_i^{-1}$.
Dico che $\phi(\sigma_i(U)|Q_i) = \phi(\sigma_i(U)|P)^{f_i}$; infatti:

$$\phi(\sigma_i(U)|Q_i)(x) = x^{\mathrm{N}(Q_i)} \quad (\sigma_i(U)) \qquad \text{e} \qquad \phi(\sigma_i(U)|P)(x) = x^{\mathrm{N}(P)} \quad (\sigma_i(U))$$

e $\mathrm{N}(Q_i) = \mathrm{N}(P)^{f_i}$.
Ma allora $\forall \sigma_i \in G$, $H \ni \phi(\sigma_i(U)|Q_i) = \sigma_i\phi^{f_i}\sigma_i^{-1}$, da cui la tesi. □

Esercizio (Marcus, n° 13, pag. 119)**.** *$m \in \mathbb{Z}$ non quadrato, $K = \mathbb{Q}(\sqrt[4]{m})$, $[K : \mathbb{Q}] = 4$.*
$L = \widetilde{K} = K(\sqrt[4]{m}, i)$ chiusura normale di $K/\mathbb{Q}$, $[L : \mathbb{Q}] = 8$, $\alpha = \sqrt[4]{m}$.
Le radici di $x^4 - m$ sono $\alpha, i\alpha, -\alpha, -i\alpha$; numeriamole in questo ordine con i numeri $1, 2, 3, 4$. Allora:

1. *$G = \langle(2\ 4), (1\ 2\ 3\ 4)\rangle \cong D_4$.*
2. *Se $p > 2$ primo tale che $p \nmid m$, p non é ramificato in L.*
3. *Se $\mathcal{O}_L \supseteq Q|p$ tale che $\phi(Q|p) = \tau$, allora $p\mathcal{O}_K = P_1P_2P_3$.*
4. *Determinare lo spezzamento di $p\mathcal{O}_K$ al variare di $\phi(Q|p)$.*

Dimostrazione.
1. Se $\sigma \in G = \mathrm{Gal}(L/\mathbb{Q})$ é tale che $\sigma(\alpha) = i\alpha$ e $\sigma(i) = i$, mentre $\tau \in G$ é tale che $\tau(\alpha) = \alpha$ e $\tau(i) = -i$, per la teoria di Galois $G = \langle\sigma, \tau\rangle$.
   A questo punto basta notare che $\sigma \leftrightarrow (1\ 2\ 3\ 4)$ e $\tau \leftrightarrow (2\ 4)$ tramite l'inclusione $G \hookrightarrow S_4$.
2. Mi basta far vedere che non é ramificato in K, ma basta anche che $p \nmid \mathrm{disc}(\alpha) = \pm\,\mathrm{N}_{K/\mathbb{Q}}(\mu'(\alpha))$, in quanto questo é un multiplo del discriminante del campo.
   $\mu'(x) = 4x^3$, dunque $\mu(\alpha) = 4\sqrt[4]{m^3}$, da cui $\mathrm{N}_{K/\mathbb{Q}}(\mu'(\alpha)) = 4^4\,\mathrm{N}(\alpha)^3 = 4^4m^3$.
   Ma per ipotesi $p \nmid 2m$, da cui $p \nmid 4^4m^3$.
3. $H = \langle\tau\rangle$, $K = L^H$.
   Se $X = \{H\rho | \rho \in G\} = \{H, H\sigma, H\sigma^2, H\sigma^3\}$, si ha l'azione:

$$\begin{array}{ccc} \langle\tau\rangle & \longrightarrow & S(X) \cong S_4 \\ \tau & \longrightarrow & \varphi_\tau \end{array}$$

dove $\varphi_\tau(H) = H\tau = H$. Dunque:
$\varphi_\tau(H) = H$, da cui $|\operatorname{orb}(H)| = 1$;
$\varphi_\tau(H\sigma) = H\sigma\tau$, da cui $|\operatorname{orb}(H\sigma) = 2$;
$\varphi_\tau(H\sigma^2) = H\sigma^2\tau = H\tau\sigma^2 = H\sigma^2$, da cui $|\operatorname{orb}(H\sigma^2)| = 1$.
Per il teorema precedente, $p\mathscr{O}_K = P_1P_2P_3$, con $f_1 = f_2 = 1$, $f_3 = 2$.

4. Se $\phi(Q|P) = \sigma$ e p é non ramificato, $X = \{H, H\sigma, H\sigma^2, H\sigma^3\}$ é un'unica orbita e dunque $p\mathscr{O}_K$ é inerte. Gli altri casi sono del tutto analoghi.

□

Esercizio (Marcus, n° 6, pag. 116)**.** *Siano $m \neq n \in \mathbb{Z}$, $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$,* $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Denotiamo con $K_1 = \mathbb{Q}(\sqrt{m})$, $K_2 = \mathbb{Q}(\sqrt{n})$, $K_3 = \mathbb{Q}(\sqrt{mn})$ le tre sottoestensioni quadratiche di L. Sia $p \in \mathbb{Z}$ primo.

1. *Se p é ramificato in K_i $\forall i$, cosa succede in L? Trovare un esempio.*
2. *Se p si spezza completamente in K_i $\forall i$, cosa succede in L? Trovare un esempio.*
3. *Se p é inerte in K_i $\forall i$, cosa succede in L? Puó succedere?*
4. *Trovare esempi in cui:*

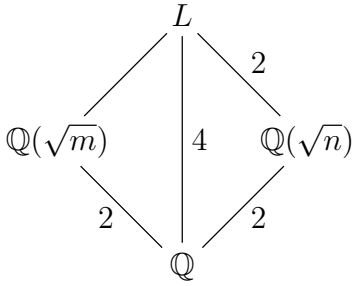
$$p\mathscr{O}_L = \begin{cases} PQ \\ P^2Q^2 \\ P^2 \end{cases}$$

Dimostrazione. 1. p ramificato in un'estensione di grado $2 \Rightarrow p$ totalmente ramificato, quindi p é totalmente ramificato in L (per un esercizio giá visto).
$p = 2$; sappiamo che se $m \equiv 2, 3 \pmod 4$, 2 é ramificato in $\mathbb{Q}(\sqrt{m})$, dunque un esempio puó essere con $m = 2$, $n = 3$ (e dunque $mn = 6 \equiv 2 \pmod 4$).

2. Per il solito esercizio, p si spezza completamente in L.
Se scelgo $p = 2$, devo scegliere $m, n \equiv 1 \pmod 4$ in modo che il polinomio $x^2 + x + \frac{1-m}{4}$ si spezzi completamente, cioé $m, n \equiv 1 \pmod 8$.
Ad esempio 17 e 33 funzionano.

3. Per il solito esercizio, il gruppo di Galois di $L/\mathbb{Q}$ deve essere ciclico, assurdo.

4. Abbiamo il diagramma:



Per avere $2\mathscr{O}_L = PQ$, 2 si deve spezzare completamente in $\mathbb{Q}(\sqrt{m})$ e deve essere inerte nell'altra; per quanto abbiamo visto si ha $n \equiv 1 \pmod 8$ e $m \equiv 1 \pmod 4$, $m \not\equiv 1 \pmod 8$ (cioé $m \equiv 5 \pmod 8$). $m = 17$ e $n = 5$ vanno bene.
Per avere $2\mathscr{O}_L = P^2Q^2$, 2 si deve spezzare completamente in $\mathbb{Q}(\sqrt{m})$ e deve ramificare nell'altra; dunque $m = 17$ e $n = 2$ vanno bene.
Per avere $2\mathscr{O}_L = P^2$, 2 deve essere inerte in $\mathbb{Q}(\sqrt{m})$ e deve ramificare nell'altra; $m = 5$ e $n = 2$ vanno bene.

□

4.3 Differente

$K \subseteq L$ estensione finita e separabile; non é necessario che siano campi di numeri, ma ci poniamo nella situazione piú generale in cui R é un dominio di Dedekind, $K = K(R)$ il suo campo delle frazioni, L é un'estensione finita e separabile e S é la chiusura integrale di S in L.

Osservazione. Sappiamo che gli ideali frazionari $\mathcal{F}(L)$ formano un gruppo, generato dagli ideali interi $\mathcal{I}(L) = \mathcal{I}(S)$ (e analogamente in K); si puó considerare l'immersione:

$$\begin{array}{rccc} i_{L/K}: & \mathcal{F}(K) & \longrightarrow & \mathcal{F}(L) \\ & I & \longrightarrow & I^e = IS \end{array}$$

che é é iniettiva in quanto:

$$\mathrm{Ker}(i_{L/K}) = \{I \in \mathcal{F}(K) | IS = S\} = \{I \in \mathcal{F}(K) | I \subseteq S \wedge IS = S\} = \{I \subseteq R | IS = S\},$$

ma l'estensione di un primo é sempre un ideale proprio, e I si fattorizza in ideali primi.
Notiamo che $i_{L/K}(\mathcal{I}(K)) \subseteq \mathcal{I}(L)$.
Inoltre abbiamo giá visto un omomorfismo:

$$\begin{array}{rccc} \mathrm{N}_{L/K}: & \mathcal{F}(L) & \longrightarrow & \mathcal{F}(K) \\ & I & \longrightarrow & \mathrm{N}_{L/K}(I) \end{array}$$

dove $\mathrm{N}_{L/K}(Q) = P^{f(Q|P)}$ e $P = Q^c$ per gli ideali primi, e $\mathrm{N}_{L/K}$ si estende in modo naturale a tutti i prodotti di primi.

Definizione 4.3.1. $I \in \mathcal{F}(L)$. Definiamo **duale** o **codifferente** di I:

$$I^* = \left\{x \in L | \, \mathrm{Tr}_{L/K}(xI) \subseteq R\right\}.$$

Teorema 4.3.1. *1. $I \in \mathcal{F}(L) \Rightarrow I^* \in \mathcal{F}(L)$ e $II^* = S^*$.*

2. $I \in \mathcal{I}(S) \Rightarrow (I^*)^{-1} \in \mathcal{I}(S)$.

Dimostrazione. 1. I^* é un S-modulo, in quanto, se $x_1, x_2 \in I^*$, $\lambda \in S$, $\mathrm{Tr}_{L/K}((x_1+x_2)I) \subseteq R$ per linearitá della traccia e $\mathrm{Tr}_{L/K}(\lambda xI) = \mathrm{Tr}_{L/K}(x\lambda I) \subseteq \mathrm{Tr}_{L/K}(xI) \subseteq R$ in quanto $\lambda I \subseteq I$.
Inoltre I^* é non banale, poiché $\exists a \in S$ tale che $aI \subseteq S$, dunque $\mathrm{Tr}_{L/K}(aI) \subseteq \mathrm{Tr}_{L/K}(S) \subseteq R$, da cui $a \in I^*$.
Cerco $d \in S$ tale che $dI^* \subseteq S$. Dico che $d = b \cdot \det\left(\mathrm{Tr}_{L/K}(w_i w_j)\right)$ funziona, dove $w_1, \ldots, w_n \in S$ é una K-base di L e $b \in I \cap R$ (che esiste perché sicuramente $\exists c \in aI \subseteq I \cap S$ e $\mathrm{N}_{L/K}(c) \in I \cap R$).
Sia $x \in I^* \subseteq L$; $x = c_1 w_1 + \ldots + c_n w_n$ con $c_i \in K$.
$bw_i \in I \ \forall i$, in quanto $b \in I$, dunque, per definizione di I^*:

$$\mathrm{Tr}_{L/K}(bxw_i) \in R \ \forall i = 1, \ldots, n.$$

Ma:

$$\mathrm{Tr}_{L/K}(bxw_i) = b \sum_{j=1}^{n} c_j \, \mathrm{Tr}_{L/K}(w_j w_i) \ \forall i = 1, \ldots, n,$$

dunque ho n equazioni con n incognite (i bc_i).
Risolvendo con Cramer:

$$bc_i = \frac{\det(M_i)}{\det\left(\mathrm{Tr}_{L/K}(w_i w_j)\right)},$$

dove M_i é a entrate intere, dunque $dc_i = \det(M_i) \in R$.
Ma allora $dx = \sum_{i=1}^{n} dc_i w_i \in S \ \forall x \in I^*$, cioé $dI^* \subseteq S$.
Per vedere che $II^* = S^*$, osserviamo che:

$$a \in I^* \iff \mathrm{Tr}_{L/K}(aI) \subseteq R \iff \mathrm{Tr}_{L/K}(aIS) \subseteq R \iff aI \subseteq S^* \iff a \in I^{-1}S^*,$$

da cui $I^* = I^{-1}S^*$.

2. $I \subseteq S \Rightarrow \mathrm{Tr}_{L/K}(IS) \subseteq R \iff S \subseteq I^* \Rightarrow (I^*)^{-1} \subseteq S^{-1} = S$.

□

Definizione 4.3.2. Sia $I \subseteq \mathcal{F}(L)$. Definiamo **differente** L/K di I:

$$\mathfrak{D}_{L/K}(I) = (I^*)^{-1}.$$

Inoltre definiamo **differente** di L/K:

$$\mathfrak{D}_{L/K} = \mathfrak{D}_{L/K}(S).$$

Osservazione. Per il teorema precedente, $I \subseteq S \Rightarrow \mathfrak{D}_{L/K}(I) \subseteq S$.

Teorema 4.3.2. *1.* $I \in \mathcal{F}(L) \Rightarrow \mathfrak{D}_{L/K}(I) = I\mathfrak{D}_{L/K}$.

2. (Proprietá delle torri) $K \subseteq L \subseteq M$. *Allora* $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}$.

3. L/K *di Galois* $\Rightarrow \mathfrak{D}_{L/K}$ *é invariante per l'azione di* $\mathrm{Gal}(L/K)$ *(cioé* $\sigma(\mathfrak{D}_{L/K}) = \mathfrak{D}_{L/K}$*).*

4. $I \in \mathcal{F}(K) \Rightarrow \forall J \in \mathcal{F}(L)$, $\mathrm{Tr}_{L/K}(J) \subseteq I \iff J \subseteq I\mathfrak{D}_{L/K}^{-1}$.

Dimostrazione. 1. Basta notare che:

$$\big(\mathfrak{D}_{L/K}(I)\big)^{-1} I\mathfrak{D}_{L/K} = I^* I\mathfrak{D}_{L/K} = S^*(S^*)^{-1} = S.$$

2. Sia W la chiusura normale di S in M.
$\subseteq$) Notiamo che:

$$\begin{aligned}&\mathrm{Tr}_{M/K}\big((\mathfrak{D}_{M/L}^{-1}\mathfrak{D}_{L/K}^{-1})W\big) = \mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}\big(\mathfrak{D}_{L/K}^{-1}(\mathfrak{D}_{M/L}^{-1}W)\big)\big) = \\ &= \mathrm{Tr}_{L/K}\big(\mathfrak{D}_{L/K}^{-1}\big(\mathrm{Tr}_{M/L}(W^*W)\big)\big) \subseteq \mathrm{Tr}_{L/K}(S^*S) \subseteq R,\end{aligned}$$

dunque $\mathfrak{D}_{M/L}^{-1}\mathfrak{D}_{L/K}^{-1} \subseteq \mathfrak{D}_{M/K}^{-1}$.
$\supseteq$) Si ha che:

$$\mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}\big(\mathfrak{D}_{M/K}^{-1}W\big)S\big) = \mathrm{Tr}_{M/K}\big(\mathfrak{D}_{M/K}^{-1}W\big) \subseteq R,$$

dunque $\mathrm{Tr}_{M/L}\big(\mathfrak{D}_{M/K}^{-1}W\big) \subseteq S^* = \mathfrak{D}_{L/K}^{-1}$.
Quindi:

$$\mathfrak{D}_{L/K}\,\mathrm{Tr}_{M/L}\big(\mathfrak{D}_{M/K}^{-1}W\big) \subseteq S \Rightarrow \mathrm{Tr}_{M/L}\big(\mathfrak{D}_{L/K}\mathfrak{D}_{M/K}^{-1}W\big) \subseteq S,$$

da cui $\mathfrak{D}_{L/K}\mathfrak{D}_{M/K}^{-1} \subseteq \mathfrak{D}_{M/L}^{-1}$.

3. Ovvia.

4. $\mathrm{Tr}_{L/K}(J) \subseteq I \iff \mathrm{Tr}_{L/K}(I^{-1}J) \subseteq R \iff I^{-1}J \subseteq S^*$.

□

Corollario 4.3.3. $\mathfrak{D}_{L/K}^{-1}$ *é il piú grande fra gli ideali frazionari di* S *che hanno tutti gli elementi con traccia in* R.

Dimostrazione. Basta applicare 4) del precedente teorema con $I = R$. □

Osservazione. Sappiamo che, essendo L/K separabile, la traccia é un omomorfismo surgettivo. In generale peró la sua restrizione a S $\mathrm{Tr}_{L/K} : S \to R$ non é surgettiva.
Esempio. Sia $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, quindi $R = \mathbb{Z}$, $S = \mathbb{Z}[i]$.
$\mathrm{Tr}_{L/K}(a + ib) = 2a \Rightarrow \mathrm{Tr}_{L/K}(\mathbb{Z}[i]) = 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Corollario 4.3.4. $\mathrm{Tr}_{L/K}(S) = \mathrm{lcm}\{I \subseteq R \text{ tale che } IS | \mathfrak{D}_{L/K}\}$.

Dimostrazione. Applicando il punto 4) del teorema precedente al caso $J = S$, si ha:

$$\mathrm{Tr}_{L/K}(S) \subseteq I \iff S \subseteq I\mathfrak{D}_{L/K}^{-1} \iff \mathfrak{D}_{L/K} \subseteq IS \iff IS | \mathfrak{D}_{L/K}.$$

□

Osservazione. Nel caso dell'esempio precedente, si aveva che $\mathfrak{D}_{L/K} = 2\mathbb{Z}[i]$, infatti:

$$\mathfrak{D}_{L/K}^{-1} = S^* = \big\{a + ib \in \mathbb{Q}(i) | \, \mathrm{Tr}_{L/K}\big((a + ib)\mathbb{Z}[i]\big) \subseteq \mathbb{Z}\big\},$$

ma $\mathrm{Tr}_{L/K}(a + ib) = 2a$ e $\mathrm{Tr}_{L/K}((a + ib)i) = -2b$, dunque $\mathfrak{D}_{L/K}^{-1} = \frac{1}{2}\mathbb{Z}[i]$, cioé $\mathfrak{D}_{L/K} = 2\mathbb{Z}[i]$.

Corollario 4.3.5. $\mathrm{Tr}_{L/K} : S \to R$ *é surgettiva* $\iff$ $\mathfrak{D}_{L/K}$ *non ha divisori propri in* $i_{L/K}\big(\mathcal{I}(R)\big)$.

Nel caso in cui L sia un'estensione dei razionali, abbiamo il seguente:

Teorema 4.3.6. L *campo di numeri,* $I \in \mathcal{F}(L)$, $\{a_1, \dots, a_n\}$ $\mathbb{Z}$*-base di* I. *Se* $b_1, \dots, b_n$ *é la base duale, allora* $I^* = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}}$.
Inoltre $\mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}(I)\big) = \mathrm{N}(I) |\operatorname{disc}(L)|$.
In particolare per $I = S$ *si ha:*

$$\mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}\big) = |\operatorname{disc}(L)|.$$

Dimostrazione. Sia $x \in I^*$. $\{a_1, \dots, a_n\}$ é una $\mathbb{Q}$-base di $L \Rightarrow \{b_1, \dots, b_n\}$ é una $\mathbb{Q}$-base di L, dunque $x = \sum_{i=1}^n \lambda_i b_i$, $\lambda_i \in \mathbb{Q}$.
Vogliamo vedere che $\lambda_i \in \mathbb{Z}$. Si ha:

$$x \in I^* \iff \mathrm{Tr}_{L/\mathbb{Q}}(xI) \subseteq \mathbb{Z} \iff \mathrm{Tr}_{L/\mathbb{Q}}(xa_i) \in \mathbb{Z} \ \forall i \iff \sum_{i=1}^n \lambda_i \, \mathrm{Tr}_{L/\mathbb{Q}}(b_i a_j) = \lambda_j \in \mathbb{Z},$$

cioé $x \in I^* \iff x \in \langle b_1, \dots, b_n \rangle_{\mathbb{Z}}$.
Poiché $\mathfrak{D}_{L/\mathbb{Q}}(I) = I\mathfrak{D}_{L/\mathbb{Q}}$, allora $\mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}(I)\big) = \mathrm{N}(I)\,\mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}\big)$.
Sia $w_1, \dots, w_n$ una base intera; $\mathscr{O}_L = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$, $\mathscr{O}_L^* = \mathfrak{D}_{L/\mathbb{Q}}^{-1} = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}}$.
Sia $m \in \mathbb{Z}$ tale che $c_i = mb_i \in \mathscr{O}_L$ $\forall i$ (e tale m esiste perché $\mathscr{O}_L^*$ é un ideale frazionario e dunque esiste un tale $m \in L$; prendendo la sua norma $L/\mathbb{Q}$ si ha l'elemento voluto); $I = m\mathfrak{D}_{L/\mathbb{Q}}^{-1} \subseteq \mathscr{O}_L$, $I = \langle c_1, \dots, c_n \rangle_{\mathbb{Z}}$.
Sappiamo che $\operatorname{disc}(c_1, \dots, c_n) = \mathrm{N}(I)^2 \operatorname{disc}(L)$, e $\mathrm{N}(I) = \mathrm{N}(m)N\big(\mathfrak{D}_{L/\mathbb{Q}}\big)^{-1} = m^n N\big(\mathfrak{D}_{L/\mathbb{Q}}\big)^{-1}$, ma vale anche la relazione $\operatorname{disc}(c_1, \dots, c_n) = m^{2n} \operatorname{disc}(b_1, \dots, b_n)$, dunque:

$$m^{2n} \operatorname{disc}(b_1, \dots, b_n) = m^{2n} \, \mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}\big)^{-2} \operatorname{disc}(L),$$

da cui:

$$\mathrm{N}_{L/\mathbb{Q}}\big(\mathfrak{D}_{L/\mathbb{Q}}\big)^2 = \frac{\operatorname{disc}(L)}{\operatorname{disc}(b_1, \dots, b_n)}.$$

A questo punto basta notare che $(\sigma_i(w_j))_{i,j}{}^t(\sigma_i(b_j))_{i,j} = \big(\mathrm{Tr}(w_i b_j)\big)_{i,j} = I_n \Rightarrow \operatorname{disc}(b_1, \dots, b_n) = (\operatorname{disc}(L))^{-1}$. □

Grazie a questo teorema, possiamo estendere il concetto di discriminante anche a estensioni L/K con $K \neq \mathbb{Q}$:

Definizione 4.3.3. L/K estensione. Definiamo il **discriminante** di L/K come $\mathrm{disc}(L) = \mathrm{N}_{L/K}\big(\mathfrak{D}_{L/K}\big)$.

Proposizione 4.3.7. $M \supseteq L \supseteq K$. $\mathrm{disc}(M/K) = \mathrm{N}_{L/K}(\mathrm{disc}(M/L))(\mathrm{disc}(L/K))^{[M:L]}$.

Dimostrazione. Abbiamo visto che $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}$. Applicando la norma M/K, si ha:

$$\mathrm{disc}(M/K) = \mathrm{N}_{L/K}\,\mathrm{N}_{M/L}\big(\mathfrak{D}_{M/L}\mathfrak{D}_{L/K}\big) = \mathrm{N}_{L/K}\Big(\big(\underbrace{\mathrm{N}_{M/L}\big(\mathfrak{D}_{M/L}\big)}_{=\mathrm{disc}(M/L)}\big)\big(\underbrace{\mathrm{N}_{M/L}\big(\mathfrak{D}_{L/K}\big)}_{=\mathfrak{D}_{L/K}^{[M:L]}}\big)\Big) =$$

$$= \mathrm{N}_{L/K}(\mathrm{disc}(M/L))(\mathrm{disc}(L/K))^{[M:L]}.$$

□

<u>*Osservazione*</u>. Se $K = \mathbb{Q}$, dalla fattorizzazione di $\mathrm{disc}(M)$ posso dedurre i gradi di possibili estensioni intermedie in quanto, se $M \supsetneq L \supsetneq \mathbb{Q}$, $|\mathrm{disc}(L)| > 1$ (lo vedremo) e $|\mathrm{disc}(L)|^{[M:L]}$ deve dividere $\mathrm{disc}(M)$.

Enunciamo il seguente teorema senza dimostrazione, che é particolarmente faticosa (puó essere dimostrato come conseguenza della formula di Hilbert, mostrata nel paragrafo 6.4):

Teorema 4.3.8. *$L \supseteq K$ estensione finita e separabile, P primo di R, $PS = Q^e I$, con $(I, Q) = 1$ (cioé e é l'indice di ramificazione). Allora $Q^{e-1} | \mathfrak{D}_{L/K}$.*
Se vale anche che $(e, \mathrm{N}(Q)) = 1 \Rightarrow Q^e \nmid \mathfrak{D}_{L/K}$.

Corollario 4.3.9. *1. $Q \subseteq S$ é ramificato su $P \iff Q | \mathfrak{D}_{L/K}$.*

2. $P \subseteq R$ si ramifica in $S \iff P | \mathrm{disc}(L/K)$.

Proposizione 4.3.10. *K_1/K, K_2/K estensioni finite e separabili, $L = K_1K_2$, $P \subseteq R$ primo. Allora:*

$$P | \mathrm{disc}(L/K) \iff P | \mathrm{disc}(K_1/K)\,\mathrm{disc}(K_2/K).$$

Dimostrazione. $\Rightarrow$) $P | \mathrm{disc}(L/K) \Rightarrow P$ é ramificato in L/K.
Se per assurdo $P \nmid \mathrm{disc}(K_1/K)$, $P \nmid \mathrm{disc}(K_2/K)$, P non é ramificato né in K_1 né in K_2, dunque non é ramificato nel composto.
$\Leftarrow$) Se ad esempio $P | \mathrm{disc}(K_1/K)$, P é ramificato in $K_1 \Rightarrow P$ ramificato in L. □

Corollario 4.3.11. *L/K estensione, M chiusura normale di L/K. Allora* $\mathrm{disc}(M/K)$ *e* $\mathrm{disc}(L/K)$ *hanno gli stessi primi.*

Dimostrazione. Segue dalla proposizione precedente e dal fatto che P ramificato in $L \iff P$ ramificato in M. □

<u>*Osservazione*</u>. $\mathbb{Q} \subseteq K \subseteq L$ campi di numeri, $p \in \mathbb{Z}$, $\mathscr{O}_K \supseteq P | p$, $\mathscr{O}_L \supseteq Q | P$.
Abbiamo visto che, se $(e, \mathrm{N}(Q)) = 1$, conosciamo l'esatta potenza di Q che divide $\mathfrak{D}_{L/K}$; inoltre osserviamo che $(e, \mathrm{N}(Q)) = 1 \iff (e, p) = 1$, in quanto $\mathrm{N}(Q)$ é una potenza di p.

Definizione 4.3.4. Q ha ramificazione **tame** su P se $p = Q \cap \mathbb{Z}$ é tale che $p \nmid e(Q|P)$. P ha ramificazione **tame** in S se $PS = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$, con $p \nmid e_i \forall i$.
In caso contrario, si dice che Q ha ramificazione **wild** su P.

Corollario 4.3.12. *Se Q ha ramificazione tame su P,* $\mathrm{Tr}_{L/K}(S) \not\subseteq P$.
Dunque, se $\forall P \subseteq R\ \exists Q | P$ con ramificazione tame, $\mathrm{Tr}_{L/K}(S) = R$, *cioé é surgettiva.*

Dimostrazione. $\mathrm{Tr}_{L/K}(S) \subseteq P \iff PS | \mathfrak{D}_{L/K}$.
$PS = Q^e I$ con $(I, Q) = 1$ e $Q^e \nmid \mathfrak{D}_{L/K}$, dunque $PS \nmid \mathfrak{D}_{L/K}$. □

Esempio. Riprendiamo l'esempio $L = \mathbb{Q}(i)$. Abbiamo visto che $\mathrm{Tr}_{L/\mathbb{Q}}(\mathbb{Z}[i]) = 2\mathbb{Z}$ e $\mathfrak{D}_{L/\mathbb{Q}} = (2)$.
$\overline{2\mathbb{Z}[i] = (1-i)^2}$, dunque ha ramificazione wild, in quanto $2|e = 2$.

Come abbiamo detto, vedremo che se $K \supsetneq \mathbb{Q}$, allora $|\operatorname{disc}(K)| > 1$; da questo segue un importante corollario:

Corollario 4.3.13. *Se $K \supsetneq \mathbb{Q}$, c'é almeno un primo ramificato.*

Osservazione. Se considero la torre $L \supsetneq K \supsetneq \mathbb{Q}$, non é vero che in L/K ci debbano essere primi ramificati, dunque é possibile che differente e discriminante valgano 1.

Esempio. Denotiamo $K_x = \mathbb{Q}(\sqrt{x})$. Siano $a \equiv b \equiv 1 \pmod 4$ tali che $(a, b) = 1$.
Poniamo $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$; sappiamo che le sottoestensioni quadratiche sono K_a, K_b e K_{ab}.
p ramifica in $L \iff p$ ramifica in almeno una delle estensioni intermedie (altrimenti esisterebbe un'estensione propria massima).
Dunque p ramifica in $L \iff p|a \vee p|b$; supponiamo ad esempio $p|a$ ($\Rightarrow p \nmid b$).
Se $\mathscr{O}_a = \mathscr{O}_{K_a}$ (e analogo per gli altri), si ha che $p\mathscr{O}_a = P^2$, mentre:

$$p\mathscr{O}_b = \begin{cases} Q & f = 2 \\ Q_1 Q_2 & f = 1 \end{cases}$$

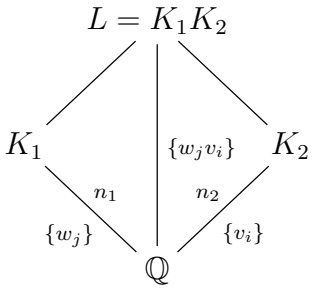
da cui:

$$p\mathscr{O}_L = \begin{cases} U^2 & f = 2 \\ U_1^2 U_2^2 & f = 1 \end{cases}$$

Dico che L/K_{ab} non ha primi ramificati.
U primo di L. U ramificato su $K_{ab} \Rightarrow U$ ramificato su $\mathbb{Q}$, dunque $Q \cap \mathbb{Z} = p|a$ (oppure $p|b$, ma sarebbe un caso analogo), ma allora $p\mathscr{O}_{ab} = Q^2$, assurdo (non é possibile che in L un primo abbia indice di ramificazione 4, in quanto $(a, b) = 1$).
(Osserviamo che l'esempio poteva essere risolto calcolando $\operatorname{disc}(L/\mathbb{Q})$ e $\operatorname{disc}(K_{ab}/\mathbb{Q})$ e deducendo $\operatorname{disc}(L/K_{ab})$.)

Riprendiamo una situazione giá vista: un diagramma di estensioni in cui i discriminanti delle estensioni intermedie sono coprimi; vediamo in particolare che, in un caso, un'ipotesi posta in precedenza é in realtá superflua.

Teorema 4.3.14. *Consideriamo il diagramma di estensioni:*



dove $\{w_j\}$ é una base intera di K_1 e $\{v_i\}$ é una base intera di K_2.
Supponiamo $(\operatorname{disc}(K_1), \operatorname{disc}(K_2)) = 1$. *Allora:*

1. $[L : \mathbb{Q}] = n_1 n_2$.
2. $\{w_j v_i\}$ *é una base intera di* L.

3. $\operatorname{disc}(L) = \operatorname{disc}(K_1)^{n_2} \cdot \operatorname{disc}(K_2)^{n_1}$.

Dimostrazione. 1. $K_1 = \mathbb{Q}(a)$, $\mu = \mu_a$ polinomio minimo di a su $\mathbb{Q}$.
Sia K la chiusura normale di $K_1/\mathbb{Q}$, cioé il campo di spezzamento di μ; $\operatorname{disc}(K)$ ha gli stessi primi di $\operatorname{disc}(K_1)$, dunque $(\operatorname{disc}(K), \operatorname{disc}(K_2)) = 1$.
$L = K_2(a)$, dunque $[L : \mathbb{Q}] = [K_2(a) : K_2] \cdot [K_2 : \mathbb{Q}] = \deg(g) \cdot n_2$, dove g é il polinomio minimo di a su K_2.
Sicuramente $g|\mu$; la tesi é equivalente a $g = \mu$.
Sia $F = K \cap K_2$; $g \in F[x]$, in quanto $g \in K_2[x]$ e $a \in K \Rightarrow g \in K[x]$.
$F \subseteq K \Rightarrow \operatorname{disc}(F)|\operatorname{disc}(K)$, mentre $F \subseteq K_2 \Rightarrow \operatorname{disc}(F)|\operatorname{disc}(K_2)$, ma $(\operatorname{disc}(K), \operatorname{disc}(K_2)) = 1$, dunque $|\operatorname{disc}(F)| = 1$, cioé $F = \mathbb{Q}$. Ma allora $g = \mu$.

2. Grazie a 1), segue da un teorema giá visto.

3. $\operatorname{disc}(L) = \operatorname{disc}(\{w_j v_i\})$. Denotiamo con $\sigma_1, \dots, \sigma_{n_1} : K_1 \to \overline{\mathbb{Q}}$ le immersioni di $K_1/\mathbb{Q}$ e con $\tau_1, \dots, \tau_{n_2} : K_2 \to \overline{\mathbb{Q}}$ le immersioni di $K_2/\mathbb{Q}$.
Siano $\widetilde{\sigma_1}, \dots, \widetilde{\sigma_{n_1}}$ le immersioni di L/K_2; allora le $\widetilde{\sigma}_{k|K_1}$ sono distinte (e dunque sono le immersioni di $K_1/\mathbb{Q}$).
Con un ragionamento del tutto analogo per le $\widetilde{\tau_l}$ deduciamo che le $\{\widetilde{\sigma_k}\widetilde{\tau_l}\}$ sono le immersioni di $L/\mathbb{Q}$.
Dunque:
$$\operatorname{disc}(L) = \det\left(\widetilde{\sigma_k}\widetilde{\tau_l}(w_j v_i)\right)^2 = \det\left(\sigma_k(w_j)\tau_l(v_i)\right)^2.$$
Visto che $\operatorname{disc}(K_1) = \det\left(\sigma_k(w_j)\right)^2$ e $\operatorname{disc}(K_2) = \det\left(\tau_l(v_i)\right)^2$, basta notare che:
$$\det(A \otimes B) = \det(A)^{\dim(B)} \det(B)^{\dim(A)},$$
dove $A \otimes B$ indica il prodotto di Kronecker di A e B.

□

5 Il gruppo delle classi di ideali e il gruppo delle unitá

5.1 Finitezza del gruppo delle classi di ideali

Sia $K \supseteq \mathbb{Q}$. Abbiamo giá definito $\mathcal{F}(K)$ come il gruppo degli ideali frazionari, $\mathcal{P}(K)$ come il sottogruppo degli ideali frazionari principali e:

$$\mathrm{Cl}(K) = \frac{\mathcal{F}(K)}{\mathcal{P}(K)}$$

come il **gruppo delle classi di ideali**. Iniziamo con qualche osservazione.

Osservazioni. 1. $\mathrm{Cl}(K) = \{e\} \iff \mathscr{O}_K$ é PID.

2. $\mathrm{Cl}(K)$ "misura" quanto $\mathscr{O}_K$ non é PID.

3. $\forall C \in \mathrm{Cl}(K)\ \exists I \subseteq \mathscr{O}_K$ tale che $I \in C$.
   Infatti, $\forall J \in \mathrm{Cl}(K)\ \exists d$ tale che $dJ \subseteq \mathscr{O}_K$, ma allora $I = (d)J \in C$ e I é intero.

Proposizione 5.1.1. *$\exists \lambda = \lambda(K) \in \mathbb{R}$ tale che $\forall I \subseteq \mathscr{O}_K\ \exists \alpha \in I$ tale che:*

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| \leq \lambda\, \mathrm{N}(I).$$

Dimostrazione. Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base intera di K; siano inoltre $\sigma_1, \ldots, \sigma_n$ le immersioni di $K/\mathbb{Q}$.
Poniamo:

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|;$$

vediamo che un tale λ funziona.
$\mathrm{N}(I) \in \mathbb{N} \Rightarrow \exists m \in \mathbb{N}$ tale che $m^n \leq \mathrm{N}(I) \leq (m+1)^n$.
Considero gli $(m+1)^n$ elementi $\sum_{j=1}^{n} m_j \alpha_j \in \mathscr{O}_K$, con $0 \leq m_j \leq m\ \forall j$.
$(m+1)^n \geq \mathrm{N}(I) \Rightarrow \exists$ due elementi come sopra che coincidono in $\frac{\mathscr{O}_K}{I}$; dunque $\exists 0 \neq \alpha \in I$, $\alpha = \sum_{j=1}^{n} \overline{m_j}\alpha_j$, dove $\overline{m_j}$ é la differenza fra i coefficienti j-esimi dei due elementi sopra indicati, e dunque $|\overline{m_j}| \leq m$.
Si ha la catena di disuguaglianze:

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| = \left|\mathrm{N}_{K/\mathbb{Q}}\left(\sum_{j=1}^{n} \overline{m_j}\alpha_j\right)\right| = \prod_{i=1}^{n} \left|\sigma_i\left(\sum_{j=1}^{n} \overline{m_j}\alpha_j\right)\right| = \prod_{i=1}^{n} \left|\sum_{j=1}^{n} \overline{m_j}\sigma_i(\alpha_j)\right| \leq$$

$$\leq \prod_{i=1}^{n} \sum_{j=1}^{n} |\overline{m_j}||\sigma_i(\alpha_j)| \leq m^n \cdot \underbrace{\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|}_{=\lambda} \leq \lambda\, \mathrm{N}(I).$$

□

Corollario 5.1.2. *$\forall C \in \mathrm{Cl}(K)\ \exists J \in C$, $J \subseteq \mathscr{O}_K$, tale che $\mathrm{N}(J) \leq \lambda$ (dove λ é la costante della proposizione precedente).*

Dimostrazione. $C \in \mathrm{Cl}(K)$; $C^{-1} \in \mathrm{Cl}(K)$, dunque sia $I \in C^{-1}$.
Per la proposizione precedente $\exists \alpha \in I$ tale che $\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| \leq \lambda\, \mathrm{N}(I)$; $\alpha \in I \Rightarrow I|(\alpha) \Rightarrow \alpha = IJ$ (e dunque $[IJ] = [e]$ in $\mathrm{Cl}(K)$).
Ma allora $J \in (C^{-1})^{-1} = C$, e inoltre:

$$\mathrm{N}(I)\,\mathrm{N}(J) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| \leq \lambda\, \mathrm{N}(I),$$

da cui $\mathrm{N}(J) \leq \lambda$. □

Teorema 5.1.3. $\forall K \supseteq \mathbb{Q}$, $\mathrm{Cl}(K)$ *é un gruppo finito.*

Dimostrazione. Notiamo che per avere la tesi, basta vedere che c'é solo un numero finito di ideali interi che verificano $\mathrm{N}(J) \leq \lambda$, in quanto ogni classe contiene un tale ideale.
$J \subseteq \mathscr{O}_K$. $J = P_1^{n_1} \cdot \ldots \cdot P_s^{n_s}$.
Passando alle norme:

$$\mathrm{N}(J) = \prod_{i=1}^{s} \mathrm{N}(P_i)^{n_i} = \prod_{i=1}^{s} (p_i^{f_i})^{n_i},$$

dove $p_i = P_i \cap \mathbb{Z}$ e $f_i = f(P_i|p_i)$.
Ma:

$$\mathrm{N}(J) \leq \lambda \iff \prod_{i=1}^{s} p_i^{f_i n_i} \leq \lambda,$$

dunque sicuramente $p_i \leq \lambda \ \forall i$, cioé i P_i possono essere scelti da un insieme finito.
Ma un discorso analogo si puó fare per gli esponenti $\Rightarrow$ primi e esponenti possono essere scelti in un insieme limitato, quindi gli ideali con norma $\leq \lambda$ sono in numero finito. □

Esempio. Sia $K = \mathbb{Q}(\sqrt{-5})$. Determinare $\mathrm{Cl}(K)$.

Dimostrazione. Sappiamo che $\mathscr{O}_K = \mathbb{Z}[\sqrt{-5}]$ e $\mathrm{disc}(K) = -20$.
Seguendo la dimostrazione della prima proposizione, visto che $\{1, \sqrt{-5}\}$ é una base intera e $\sigma_{1,2} : \sqrt{-5} \to \pm\sqrt{-5}$ sono le immersioni di $K/\mathbb{Q}$, si ha:

$$\lambda = (1 + |\sqrt{-5}|)(1 + |-\sqrt{-5}|) = (1 + \sqrt{5})^2 = 6 + 2\sqrt{5} < 11,$$

dunque possiamo scegliere $\lambda = 10$ (in quanto la norma degli ideali é un intero).
Per il corollario, $\forall C \in \mathrm{Cl}(K)\ \exists J \in C$ tale che $\mathrm{N}(J) \leq 10$.
Se $J = P_1^{n_1} \cdot \ldots \cdot P_s^{n_s} \Rightarrow p_i = P_i \cap \mathbb{Z} \leq 10$, cioé $p_i \in \{2, 3, 5, 7\}$.
Per Kummer sappiamo che:
$2\mathscr{O}_K = P^2 = (2, 1 + \sqrt{-5})^2$, in quanto 2 é ramificato;
$3\mathscr{O}_K = P_1 P_2$, $f = 1$, in quanto $x^2 + 5 \equiv x^2 - 1 \equiv (x - 1)(x + 1) \pmod 3$;
$5\mathscr{O}_K = Q^2 = (\sqrt{-5})^2$ é principale (e dunque banale in $\mathrm{Cl}(K)$);
$7\mathscr{O}_K = Q_1 Q_2$, $f = 1$, in quanto $x^2 + 5 \equiv x^2 - 9 \equiv (x + 3)(x - 3) \pmod 7$.
Osserviamo che, se P fosse principale, sarebbe generato da un elemento di norma 2, ma l'equazione:

$$\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$$

non ha soluzioni intere, dunque P non é principale.
Inoltre P^2 é principale, cioé $[P^2] = [P]^2 = [e]$ in $\mathrm{Cl}(K)$, quindi in $\mathrm{Cl}(K)$ ha un elemento di ordine 2 e $2|\,\mathrm{Cl}(K)$.
Con un ragionamento analogo si vede che P_1 e P_2 non sono principali, ma $[P_1 P_2] = [e] \Rightarrow [P_1] = [P_2]^{-1}$.
Osservo che $\mathrm{N}(1 + \sqrt{-5}) = 6$, dunque $(1 + \sqrt{-5})$ si fattorizza con un primo di norma 2 e uno di norma 3; ma l'unico primo sopra 2 é P e gli unici primi sopra 3 sono P_1 e P_2, quindi $(1 + \sqrt{-5}) = PP_1$ (il caso con P_2 é analogo), cioé $[P]^{-1} = [P] = [P_1]^{-1}$, da cui $[P] = [P_1] = [P_2]$.
Con il solito ragionamento, $a^2 + 5b^2 = 7$ non ha soluzione, quindi gli ideali Q_1 e Q_2 non sono principali; notiamo che in $\mathrm{Cl}(K)$ non ci possono essere prodotti di Q_1, Q_2 con altri elementi, in quanto $\mathrm{N}(Q_1) = \mathrm{N}(Q_2) = 7$ non lascia spazio a primi W tali che $\mathrm{N}(Q_1 W) \leq 10 \vee \mathrm{N}(Q_2 W) \leq 10$.
Peró come prima si nota che $\mathrm{N}(3 + \sqrt{-5}) = 14$, dunque $(3 + \sqrt{-5}) = Q_1 P$, cioé $[Q_1][P] = [e]$, da cui $[Q_1] = [Q_2] = [P]$.
Riassumendo, l'unico elemento non banale in $\mathrm{Cl}(K)$ é P, dunque $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. □

Osservazione. Dal punto di vista teorico, la sezione puó concludersi qua, in quanto é stato dimostrato quello che volevamo; dal punto di vista pratico, peró, la dimostrazione costruttiva della proposizione iniziale dá sí una costante λ facilmente calcolabile, ma, come abbiamo visto nell'esempio, non abbastanza piccola da rendere agevole i calcoli in situazioni anche molto semplici.
Nasce quindi il bisogno di cercare una costante migliore, problema che ci porremo nei prossimi paragrafi.

5.2 Un approccio geometrico: il teorema di Minkowski

Definizione 5.2.1. $H \subseteq \mathbb{R}^n$ sottogruppo additivo. H si dice **discreto** se $\forall K \subseteq \mathbb{R}^n$ compatto, $H \cap K$ é finito.

Esempi.
- $\mathbb{Z}^n \subseteq \mathbb{R}^n$ é un sottogruppo discreto.
- $\mathbb{Z}^r \times \{0\}^{n-r}$ é un sottogruppo discreto $\forall r$.
- Se $v_1, \dots, v_r \in \mathbb{R}^n$ sono linearmente indipendenti su $\mathbb{R}$, $H = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$ é un sottogruppo discreto.
  Infatti, dopo aver esteso i vettori a una base $\{v_i\}$ di $\mathbb{R}^n$, ogni compatto di $\mathbb{R}^n$ é contenuto in $\sum_{i=1}^n \lambda_i v_i$ con $0 \leq \lambda_i \leq c$ per un certo $c < +\infty$, e in questo politopo c'é solo un numero finito di elementi a coordinate intere.

Teorema 5.2.1. *H sottogruppo discreto di $\mathbb{R}^n$. Allora $\exists v_1, \dots, v_r \in \mathbb{R}^n$ linearmente indipendenti su $\mathbb{R}$ tali che $H = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$.*

Dimostrazione. Siano $e_1, \dots, e_r \in H$ linearmente indipendenti su $\mathbb{R}$, r massimo possibile.
$\forall x \in H$, x é dipendente su $\mathbb{R}$ da $e_1, \dots, e_r$, cioé $\exists \lambda_1, \dots, \lambda_r \in \mathbb{R}$ tali che:

$$x = \sum_i \lambda_i e_i.$$

Osserviamo che $P = \left\{ \sum_{i=1}^r \alpha_i e_i \middle| 0 \leq \alpha_i \leq 1 \right\} \subseteq \mathbb{R}^n$ é compatto, quindi $P \cap H$ é finito.
$\forall j \in \mathbb{Z}$, poniamo:

$$x_j = jx - \sum_{i=1}^r [j\lambda_i] e_i = \sum_{i=1}^r (j\lambda_i - [j\lambda_i]) e_i \in H,$$

ma $x_j \in P \Rightarrow x_j \in P \cap H \ \forall j$.
Se $x \in H$, x si scrive come:

$$x = \underbrace{x_1}_{\in P \cap H} + \sum_i [\lambda_i] e_i,$$

quindi H é generato su $\mathbb{Z}$ da $\{P \cap H, e_1, \dots, e_r\}$ (e finitamente generato).
$P \cap H$ é finito, dunque $\exists j, h$ tali che $x_j = x_h$, quindi:

$$(j-h)\lambda_i = [j\lambda_i] - [h\lambda_i] \ \forall i.$$

Ma allora $(j-h)\lambda_i \in \mathbb{Z}$, quindi $\lambda_i \in \mathbb{Q} \ \forall i$; ne segue che H é generato su $\mathbb{Z}$ da $e_1, \dots, e_r$ e da altri elementi che sono combinazioni razionali degli e_i, cioé $H \subseteq \frac{1}{d}\langle e_1, \dots, e_r \rangle_{\mathbb{Z}}$ (con d denominatore comune dei coefficienti di quegli elementi).

$$dH \subseteq \langle e_1, \dots, e_r \rangle_{\mathbb{Z}} \subseteq H,$$

ma $\langle e_1, \dots, e_r \rangle_{\mathbb{Z}}$ é uno $\mathbb{Z}$-modulo libero di rango r, quindi anche dH é libero e $\mathrm{rk}(dH) \leq r$, mentre $\mathrm{rk}(H) \geq r$.

$\mathrm{rk}(dH) = \mathrm{rk}(H) \Rightarrow \mathrm{rk}(dH) = \mathrm{rk}(H) = r$, dunque esiste $\{f_1, \dots, f_r\}$ $\mathbb{Z}$-base di $\langle e_1, \dots, e_r \rangle_{\mathbb{Z}}$, e $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$ tali che $\{\alpha_1 f_1, \dots, \alpha_r f_r\}$ é una $\mathbb{Z}$-base di dH, $\alpha_i \neq 0$ $\forall i$ perché hanno lo stesso rango.
$f_1, \dots, f_r$ sono linearmente indipendenti su $\mathbb{R}$ perché lo sono $e_1, \dots, e_r$, quindi anche $\frac{\alpha_1 f_1}{d}, \dots, \frac{\alpha_r f_r}{d}$ lo sono e sono la base cercata di H. □

Definizione 5.2.2. Un sottogruppo discreto di $\mathbb{R}^n$ di rango n si dice **reticolo** di $\mathbb{R}^n$.

Osservazione. Λ é un reticolo di $\mathbb{R}^n \iff \Lambda = \langle e_1, \dots, e_n \rangle_{\mathbb{Z}}$ e $\{e_1, \dots, e_n\}$ é una base di $\mathbb{R}^n$.

Definizione 5.2.3. Sia $\Lambda = \langle e_1, \dots, e_n \rangle_{\mathbb{Z}}$, $e = (e_1, \dots, e_r)$. Definiamo **dominio fondamentale** di Λ:

$$P_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \middle| 0 \leq \alpha_i \leq 1 \right\}.$$

Osservazione. Il dominio fondamentale dipende dalla base. Peró la prossima proposizione ci assicura che il volume di P_e dipende solo da Λ e non da e.

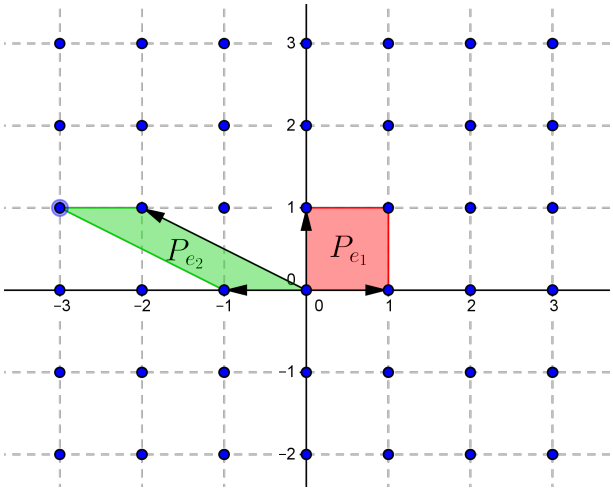


Figura 1: Domini fondamentali diversi hanno lo stesso volume

Proposizione 5.2.2. *Se μ indica la misura di Lebesgue, $\mu(P_e)$ dipende solo da Λ.*

Dimostrazione. $\mu(P_e) = |\det(e_1, \dots, e_n)|$. Se $v = \{v_1, \dots, v_n\}$ é un'altra base di Λ, $\mu(P_v) = |\det(v_1, \dots, v_n)|$.
I v_i sono combinazioni degli e_i e viceversa, dunque esiste una matrice del cambiamento di base M invertibile, cioé $\det(M) \in \mathbb{Z}^* = \{\pm 1\}$.
La tesi segue notando che:

$$\mu(P_v) = |\det(M(e_1, \dots, e_n))| = |\det(M)| \cdot \mu(P_e).$$

□

Definizione 5.2.4. $\mu(P_e)$ si definisce **volume** del reticolo, e si indica con $\mathrm{vol}(\Lambda)$.

Teorema 5.2.3 (di Minkowski)**.** *Λ reticolo di $\mathbb{R}^n$, $S \subseteq \mathbb{R}^n$ integrabile in senso di Lebesgue e $\mu(S) > \mathrm{vol}(\Lambda) \Rightarrow \exists x \neq y \in S$ tali che $x - y \in \Lambda$.*

Dimostrazione. Sia come al solito $\{e_1, \dots, e_n\}$ base di Λ, P_e il suo dominio fondamentale.
Per definizione di dominio fondamentale:

$$S = \bigcup_{\lambda \in \Lambda} (S \cap (\lambda + P_e)) \Rightarrow \mu(S) = \sum_{\lambda \in \Lambda} \mu(S \cap (\lambda + P_e))$$

(in quanto si puó coprire $\mathbb{R}^n$ con "pezzi" uguali a P_e).
Ma la misura di Lebesgue é invariante per traslazioni, dunque "sposto" tutte le intersezioni di S con i $\lambda + P_e$ su P_e:

$$\mu(S \cap (\lambda + P_e)) = \mu((-\lambda + S) \cap P_e).$$

Osserviamo a questo punto che le intersezioni $(-\lambda + S) \cap P_e$ al variare di $\lambda \in \Lambda$ non possono essere tutte disgiunte, altrimenti, essendo tutte contenute in P_e, la loro unione avrebbe misura $< \mathrm{vol}(P_e)$; siano quindi $\lambda_1 \neq \lambda_2 \in \Lambda$ tali che:

$$(-\lambda_1 + S) \cap (-\lambda \cap S) \cap P_e \neq \emptyset.$$

Quindi esistono $x, y \in S$ tali che $-\lambda_1 + x = -\lambda_2 + y$, cioé $0 \neq \lambda_1 - \lambda_2 = x - y \in \Lambda$. □

Corollario 5.2.4 (Teorema del corpo convesso di Minkowski)**.** *$\Lambda \subseteq \mathbb{R}^n$ reticolo, S misurabile, convesso e simmetrico rispetto* 0*. Supponiamo inoltre che valga una delle due condizioni:*

1. *$\mu(S) > 2^n \,\mathrm{vol}(\Lambda)$;*
2. *$\mu(S) \geq 2^n \,\mathrm{vol}(\Lambda)$ e S compatto.*

Allora S contiene un punto $0 \neq u \in \Lambda$.

Dimostrazione. Vediamo che con entrambe le ipotesi si giunge alla tesi.

1. Poniamo $S' = \frac{1}{2}S$ (con l'ovvio significato che S' é generato dai generatori di S divisi per 2); $\mu(S') = \frac{1}{2^n}\mu(S) > \mathrm{vol}(\Lambda)$, quindi posso applicare il teorema di Minkowski, che mi assicura che $\exists x \neq y \in S'$ tali che $x - y \in \Lambda$.
   Dico che $x - y \in S$. Sicuramente $2x, 2y \in S$, ma S é simmetrico rispetto a 0, quindi anche $-2x, -2y \in S$; ma S é convesso, dunque $x - y = \frac{1}{2}(2x - 2y) \in S$.

2. Se $S_m = \left(1 + \frac{1}{m}\right)S$, S_m é nelle ipotesi del caso 1), quindi $\forall m \in \mathbb{N}$, $S_m \cap (\Lambda \backslash \{0\}) \neq \emptyset$.
   Ma S_m é compatto, quindi $S_m \cap (\Lambda \backslash \{0\})$ é finito $\forall m$.
   Dico che:

   $$S \cap (\Lambda \backslash \{0\}) = \bigcap_{m>0} S_m \cap (\Lambda \backslash \{0\}) \neq \emptyset,$$

   poiché se fosse vuota, esisterebbe una sottointersezione $\bigcap_{j=1}^{s} S_{i_j} \cap (\Lambda \backslash \{0\}) = \emptyset$, assurdo, poiché l'intersezione finita di elementi concatenati non é altro che l'elemento piú piccolo (secondo l'inclusione).

□

<u>*Osservazione*</u>. Sia K un campo di numeri, $[K : \mathbb{Q}] = n$, $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ le immersioni di $K/\mathbb{Q}$. Se:

$$\begin{array}{rccc} \varepsilon : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longrightarrow & \overline{z} \end{array}$$

é il coniugio, $\varepsilon \circ \sigma_i$ é una delle immersioni, cioé $\forall i \ \exists j$ tale che $\varepsilon \circ \sigma_i = \sigma_j$.
Inoltre $\varepsilon \circ \sigma_i = \sigma_i \iff \sigma_i(K) \subseteq \mathbb{R}$.

Se $\varepsilon \circ \sigma_i \neq \sigma_i$, denotiamo con $\overline{\sigma_i}$ l'immersione $\varepsilon \circ \sigma_i$; numeriamo dunque le immersioni in questo modo:

$$\sigma_1, \dots, \sigma_r : K \to \mathbb{R}, \qquad \sigma_{r+1}, \dots, \sigma_{r+s} : K \to \mathbb{C} \text{ tali che } \overline{\sigma_{r+t}} = \sigma_{r+s+t} \ \forall t;$$

con $r + 2s = n$.
Quindi l'omomorfismo:

$$\begin{array}{rccc} \overline{\sigma} : & K & \longrightarrow & \mathbb{R}^r \times \mathbb{C}^s \\ & x & \longrightarrow & (\sigma_1(x), \dots, \sigma_r(x), \sigma_{r+1}(x), \dots, \sigma_{r+s}(x)) \end{array}$$

contiene tutte le informazioni delle immersioni $\sigma_1, \dots, \sigma_n$.
Possiamo anche immergere $\mathbb{R}^r \times \mathbb{C}^s$ in $\mathbb{R}^n$ in modo canonico:

$$\begin{array}{rccccc} \sigma : & K & \xrightarrow{\overline{\sigma}} & \mathbb{R}^r \times \mathbb{C}^s & \xrightarrow{i} & \mathbb{R}^n \\ & & & (x_1, \dots, x_r, z_1, \dots, z_s) & \longrightarrow & (x_1, \dots, x_r, \mathfrak{Re}(z_1), \dots, \mathfrak{Im}(z_1), \dots, \mathfrak{Re}(z_s), \dots, \mathfrak{Im}(z_s)) \end{array}$$

ottenendo un'immersione $\sigma : K \hookrightarrow \mathbb{R}^n$.

<u>*Osservazione*</u>. Se $K/\mathbb{Q}$ é di Galois, $\sigma_i(K) = K \ \forall i$. Dunque:

- se $K \subseteq \mathbb{R}$, $n = r$;
- se $K \not\subseteq \mathbb{R}$, $n = 2s$, cioé n é pari.

(Questo stesso fatto poteva essere visto notando che nella torre di estensioni $K \supseteq K \cap \mathbb{R} \supseteq \mathbb{Q}$, il grado $[K : K \cap \mathbb{R}]$ puó essere 1 o 2, in quanto gli unici polinomi irriducibili di $\mathbb{R}$ hanno grado 1 o 2.)

Proposizione 5.2.5. *$M = \langle x_1, \dots, x_n \rangle_{\mathbb{Z}} \subseteq K$ $\mathbb{Z}$-modulo libero di rango n.*
Allora $\sigma(M)$ é un reticolo di $\mathbb{R}^n$ e:

$$\operatorname{vol}(\sigma(M)) = 2^{-s}\sqrt{|\operatorname{disc}(M)|}.$$

Dimostrazione. Sicuramente $\sigma(M) = \langle \sigma(x_1), \dots, \sigma(x_n) \rangle_{\mathbb{Z}} \subseteq \mathbb{R}^n$. Per vedere che é un reticolo, devo mostrare che gli elementi sono indipendenti su $\mathbb{R}$, cioé che $\operatorname{vol}(M) \neq 0$ (in quanto se fossero dipendenti, genererebbero un politopo di dimensione $< n$, che ha misura di Lebesgue 0 in $\mathbb{R}^n$).
Sia $x = (x_1, \dots, x_n)$.

$$\begin{aligned} \operatorname{vol}(\sigma(M)) = \mu\big(P_{\sigma(x)}\big) = |\det(\sigma(x_1), \dots, \sigma(x_n))| = \\ = \left| \det \begin{pmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \dots & \sigma_1(x_n) \\ \vdots & \vdots & & \vdots \\ \sigma_r(x_1) & \sigma_r(x_2) & \dots & \sigma_r(x_n) \\ \mathfrak{Re}(\sigma_{r+1}(x_1)) & \mathfrak{Re}(\sigma_{r+1}(x_2)) & \dots & \mathfrak{Re}(\sigma_{r+1}(x_n)) \\ \mathfrak{Im}(\sigma_{r+1}(x_1)) & \mathfrak{Im}(\sigma_{r+1}(x_2)) & \dots & \mathfrak{Im}(\sigma_{r+1}(x_n)) \\ \vdots & \vdots & & \vdots \\ \mathfrak{Re}(\sigma_{r+s}(x_1)) & \mathfrak{Re}(\sigma_{r+s}(x_2)) & \dots & \mathfrak{Re}(\sigma_{r+s}(x_n)) \\ \mathfrak{Im}(\sigma_{r+s}(x_1)) & \mathfrak{Im}(\sigma_{r+s}(x_2)) & \dots & \mathfrak{Im}(\sigma_{r+s}(x_n)) \end{pmatrix} \right|. \end{aligned}$$

Sostituendo la coppia di righe:

$$\begin{pmatrix} \mathfrak{Re}(\sigma_{r+t}(x_1)) & \dots & \mathfrak{Re}(\sigma_{r+t}(x_n)) \\ \mathfrak{Im}(\sigma_{r+t}(x_1)) & \dots & \mathfrak{Im}(\sigma_{r+t}(x_n)) \end{pmatrix}$$

con la coppia:

$$\begin{pmatrix} \mathfrak{Re}(\sigma_{r+t}(x_1)) + i\mathfrak{Im}(\sigma_{r+t}(x_1)) & \dots & \mathfrak{Re}(\sigma_{r+t}(x_n)) + i\mathfrak{Im}(\sigma_{r+t}(x_n)) \\ \mathfrak{Re}(\sigma_{r+t}(x_1)) - i\mathfrak{Im}(\sigma_{r+t}(x_1)) & \dots & \mathfrak{Re}(\sigma_{r+t}(x_n)) - i\mathfrak{Im}(\sigma_{r+t}(x_n)) \end{pmatrix} = \begin{pmatrix} \sigma_{r+t}(x_1) & \dots & \sigma_{r+t}(x_n) \\ \overline{\sigma_{r+t}}(x_1) & \dots & \overline{\sigma_{r+t}}(x_n) \end{pmatrix}$$

raddoppio il valore assoluto del determinante; visto che ripeto questa operazione s volte, e visto che con tale procedimento ottengo la matrice $(\sigma_i(x_j))_{i,j}$, ho che:

$$\operatorname{vol}(\sigma(M)) = 2^{-s} |\det(\sigma_i(x_j))| = 2^{-s}\sqrt{|\operatorname{disc}(M)|}.$$

□

Corollario 5.2.6. *$0 \neq I \subseteq \mathscr{O}_K$. Allora:*

$$\operatorname{vol}(\sigma(I)) = 2^{-s}\,\mathrm{N}(I)\sqrt{|\operatorname{disc}(K)|}.$$

In particolare:

$$\operatorname{vol}(\sigma(\mathscr{O}_K)) = 2^{-s}\sqrt{|\operatorname{disc}(K)|}.$$

Teorema 5.2.7. *K campo di numeri, $[K:\mathbb{Q}] = r + 2s = n$, $0 \neq I \subseteq \mathscr{O}_K$ ideale.*
Allora $\exists 0 \neq x \in I$ tale che:

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \leq \lambda\,\mathrm{N}(I),$$

dove

$$\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

*é la **costante di Minkowski**.*

Dimostrazione. $\forall t \in \mathbb{R}^+$, definisco:

$$B_t = \left\{ (y,z) \in \mathbb{R}^r \times \mathbb{C}^s \,\middle|\, \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t \right\}.$$

B_t é convesso, compatto e simmetrico rispetto a 0.
Senza svolgere il (faticoso) calcolo, dico che:

$$\mu(B_t) = 2^r\left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}.$$

Scelgo t in modo che $\mu(B_t) = 2^n \operatorname{vol}(\sigma(I)) = 2^n 2^{-s}\sqrt{|\operatorname{disc}(K)|}\,\mathrm{N}(I)$, cioé
$t^n = 2^{n-r}\pi^{-s}n!\sqrt{|\operatorname{disc}(K)|}\,\mathrm{N}(I)$. Per il teorema del corpo convesso, $\exists 0 \neq x \in I$ tale che $\sigma(x) \in B_t$; prendendo la norma:

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \cdot \left(\prod_{j=1}^{s} |\sigma_{r+j}(x)|\right)^2,$$

in quanto i coniugati hanno la stessa norma. Per la disuguaglianza fra media aritmetica e media geometrica, otteniamo:

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \leq \left(\frac{1}{n}\left(\sum_{i=1}^{r} |\sigma_i(x)| + 2\sum_{j=1}^{s} |\sigma_{r+j}(x)|\right)\right)^n,$$

ma $\sigma(x) \in B_t$, dunque:

$$\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \leq \frac{1}{n^n}t^n = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}\,\mathrm{N}(I).$$

□

Osservazione. Per calcolare la costante di Minkowski, é necessario calcolare il discriminante del campo, cosa non agevole nella maggior parte dei casi.
Notiamo peró che, sostituendo $\operatorname{disc}(K)$ con $\operatorname{disc}(\alpha)$, $\alpha \in \mathscr{O}_K$, si ottiene una costante piú grande, ma molto piú veloce da determinare, che puó agevolare i calcoli.

Riprendiamo l'esempio visto nel primo paragrafo; vediamo in particolare che la costante di Minkowski aiuta ad abbassare notevolmente il volume di calcoli necessario per determinare $\mathrm{Cl}(K)$.

Esempio. Sia $K = \mathbb{Q}(\sqrt{-5})$, $\operatorname{disc}(K) = -20$. La costante di Minkowski é:

$$\lambda = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{20} = \frac{4}{\pi}\sqrt{5} < 3,$$

dunque l'esempio si risolveva subito notando che $2\mathscr{O}_K = P^2$ con P non principale.

Corollario 5.2.8. $[K : \mathbb{Q}] = n \geq 2$. *Allora:*

$$|\operatorname{disc}(K)| \geq \frac{\pi}{3}\Big(\frac{3\pi}{4}\Big)^{n-1}.$$

Equivalentemente, esiste una costante universale θ, indipendente dal campo K, tale che:

$$\frac{n}{\log|\operatorname{disc}(K)|} \leq \theta.$$

Dimostrazione. Per quanto visto:

$$1 \leq \mathrm{N}(I) \leq \Big(\frac{4}{\pi}\Big)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|} \Rightarrow |\operatorname{disc}(K)| \geq \Big(\frac{\pi}{4}\Big)^{2s}\frac{n^{2n}}{(n!)^2} \geq \Big(\frac{\pi}{4}\Big)^{n}\frac{n^{2n}}{(n!)^2} = a_n.$$

Dico che $a_n \geq \frac{\pi}{3}\big(\frac{3\pi}{4}\big)^{n-1}\ \forall n \geq 2$; procediamo per induzione su n, essendo il caso $n = 2$ una banale verifica:

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\frac{(n+1)^{2(n+1)}}{(n+1)^2(n!)^2}\cdot\frac{(n!)^2}{n^{2n}} = \frac{\pi}{4}\Big(1+\frac{1}{n}\Big)^{2n} \geq \frac{3\pi}{4},$$

dove l'ultimo passaggio é consentito (ad esempio) dalla disuguaglianza di Bernoulli. □

Corollario 5.2.9. $K \supsetneq \mathbb{Q} \Rightarrow |\operatorname{disc}(K)| > 1$.

Teorema 5.2.10 (di Hermite)**.** *Esiste solo un numero finito di campi di numeri di discriminante assegnato.*

Dimostrazione. Fissato $d > 0$, vediamo che esiste un numero finito di $K/\mathbb{Q}$ con $|\operatorname{disc}(K)| = d$.
Sappiamo peró che $|\operatorname{disc}(K)| = d \Rightarrow [K : \mathbb{Q}] \leq \theta\log(d)$, dunque basta mostrare che esiste un numero finito di campi K con $|\operatorname{disc}(K)| = d$ e $[K : \mathbb{Q}] = n$.
Equivalentemente, basta che $\forall r, s$ tali che $n = r + 2s$, esista solo un numero finito di campi con le stesse proprietá. Fissiamo $r, s \in \mathbb{N}$.
Definiamo:

$$B = \begin{cases} \Big\{(y,z) \in \mathbb{R}^r \times \mathbb{C}^s \Big| |y_1| \leq A, |y_i| \leq \frac{1}{2}\ \forall i = 2,\dots,r, |z_j| \leq \frac{1}{2}\ \forall j\Big\} \subseteq \mathbb{R}^r \times \mathbb{C}^s & \text{se } r > 0 \\ \Big\{z \in \mathbb{C}^s \Big| |z_1 - \overline{z_1}| \leq C, |z_1 + \overline{z_1}| \leq \frac{1}{2}, |z_j| \leq \frac{1}{2}\ \forall j \geq 2\Big\} \subseteq \mathbb{C}^s & \text{se } r = 0 \end{cases}$$

Scegliamo A e C in modo che $\mu(B) = 2^n \operatorname{vol}(\sigma(\mathscr{O}_K)) = 2^{n-s}\sqrt{d}$:

$$\mu(B) = 2A\Big(\frac{\pi}{4}\Big)^s \Rightarrow A = \frac{2^n 2^{2s}}{2^s 2\pi^s}\sqrt{d} = \frac{2^{n+s-1}}{\pi^s}\sqrt{d};$$

$$\mu(B) = \left(\frac{\pi}{4}\right)^{s-1}\frac{C}{2} \Rightarrow C = \frac{2\cdot 2^n 2^{2s-2}}{2^s\pi^{s-1}} = \frac{2^{n+s-1}}{\pi^{s-1}}\sqrt{d}.$$

B é compatto, convesso e simmetrico rispetto a 0, quindi $\exists 0 \neq x \in \mathscr{O}_K$ tale che $\sigma(x) \in B$.
Dico che $K = \mathbb{Q}(x)$.
Sicuramente $K \supseteq \mathbb{Q}(x)$; diciamo $[K : \mathbb{Q}(x)] = m$. Allora le immersioni $\sigma_1, \dots, \sigma_n$ di $K/\mathbb{Q}$ coincidono m a m su $\mathbb{Q}(x)$, dunque per vedere che $m = 1$, basta mostrare che $\sigma_1(x) \neq \sigma_i(x)$ $\forall i \geq 2$.
$x \in \mathscr{O}_K \Rightarrow \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| \geq 1$; ma $\sigma(x) \in B \Rightarrow$ se $r > 0$, $|\sigma_i(x)| \leq \frac{1}{2}$ e dunque $|\sigma_1(x)| > 1$ (altrimenti la norma non puó essere almeno 1); se invece $r = 0$, con un discorso analogo si vede che $|\sigma_i(x)| \leq \frac{1}{2}$ $\forall i \geq 2$, mentre $|\sigma_1(x)| > 1$.
Quindi abbiamo visto che un campo K con r, s, d assegnati é generato da un elemento $x \in \mathscr{O}_K$ tale che $\sigma(x) \in B$. Se vediamo che gli $x \in \mathscr{O}_K$ con questa proprietá sono in numero finito, avremmo la tesi.
Ma se $\sigma(x) \in B$, x ha tutti i coniugati di modulo limitato, e quindi i coefficienti del suo polinomio minimo (che sono interi) sono limitati, cioé ho un numero finito di possibili polinomi minimi e dunque di elementi. □

5.3 Il gruppo delle unitá

Teorema 5.3.1. *$\mathscr{O}_K^* \cong \mathbb{Z}^{r+s-1} \oplus T$, dove $T = \{\alpha \in K | \exists d$ tale che $x^d = 1\}$ é ciclico finito. Detto in altre parole, $\frac{\mathscr{O}_K^*}{T} \cong \langle \varepsilon_1, \dots, \varepsilon_{r+s-1}\rangle$, dove le ε_i sono dette **unitá fondamentali**.*

Dimostrazione. Definiamo **immersione logaritmica**:

$$\begin{array}{rccccc} L: & K^* & \xrightarrow{\overline{\sigma}} & \mathbb{R}^r \times \mathbb{C}^s & \longrightarrow & \mathbb{R}^{r+s} \\ & x & \longrightarrow & \overline{\sigma}(x) & \longrightarrow & (\log|\sigma_1(x)|, \dots, \log|\sigma_{r+s}(x)|) \end{array}$$

Sicuramente é un omomorfismo, in quanto $L(xy) = L(x) + L(y)$.
Sia $B \subseteq \mathbb{R}^{r+s}$ compatto; dico che $B' = \{x \in \mathscr{O}_K | L(x) \in B\}$ é finito.
Infatti B compatto $\Rightarrow \exists \alpha \in \mathbb{R}$ tale che $|\log|\sigma_i(x)|| < \alpha$ $\forall i$, $\forall x \in K^*$, cioé $\frac{1}{e^\alpha} < |\sigma_i(x)| < e^\alpha$.
Ma allora i coniugati di x sono limitati, dunque le possibilitá per il polinomio minimo di $x \in \mathscr{O}_K$ sono in numero finito, in quanto i coefficienti devono essere interi.
Osserviamo che $\mathrm{Ker}(L_{|\mathscr{O}_K^*}) = \{x \in \mathscr{O}_K^* | L(x) = 0\}$ é finito, in quanto é B' con $B = 0$. Dico che $\mathrm{Ker}(L_{|\mathscr{O}_K^*}) = T$.
$\mathrm{Ker}(L_{|\mathscr{O}_K^*}) < K^*$ é finito e dunque ciclico, e gli unici elementi di ordine finito in K^* sono le radici di 1; perció $\mathrm{Ker}(L_{|\mathscr{O}_K^*}) \subseteq T$.
Viceversa, $x \in K^*$ tale che $x^d = 1 \Rightarrow |\sigma_i(x)| = 1$ $\forall i \Rightarrow L(x) = 0$.
$L(\mathscr{O}_K^*)$ é un sottogruppo discreto di $\mathbb{R}^{r+s}$, in quanto se $B \subseteq \mathbb{R}^{r+s}$ é compatto, $L(\mathscr{O}_K^*) \cap B = L(B')$, che é finito; ma allora $L(\mathscr{O}_K^*)$ é uno $\mathbb{Z}$-modulo libero finitamente generato di rango $d \leq r + s$.
Consideriamo la successione esatta:

$$0 \longrightarrow T \hookrightarrow \mathscr{O}_K^* \longrightarrow L(\mathscr{O}_K^*) \longrightarrow 0$$

$L(\mathscr{O}_K^*)$ é libero e dunque proiettivo, quindi la successione spezza e $\mathscr{O}_K^* \cong L(\mathscr{O}_K^*) \oplus T$.
Resta solo da vedere che $d = r + s - 1$. Vediamo le due disuguaglianze.

$\leq$) Consideriamo l'iperpiano:

$$W = \left\{(x, y) \in \mathbb{R}^r \times \mathbb{R}^s \,\middle|\, \sum_{i=1}^{r} x_i + 2\sum_{j=1}^{s} y_j = 0\right\};$$

dico che $L(\mathscr{O}_K^*) \subseteq W$.
Se $x \in \mathscr{O}_K^*$, $\left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = 1$, ma:

$$1 = \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = \prod_{i=1}^{r} |\sigma_i(x)| \cdot \prod_{j=1}^{s} |\sigma_{r+j}(x)| \cdot \prod_{j=1}^{s} |\overline{\sigma_{r+j}}(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \cdot \prod_{j=1}^{s} |\sigma_{r+j}(x)|^2,$$

dunque, tramite L, si ha che:

$$\sum_{i=1}^{r} |\sigma_i(x)| + 2\sum_{j=1}^{s} |\sigma_{r+j}(x)| = \log(1) = 0,$$

cioé $L(x) \in W$.

$\geq$) Cerco $u_1, \ldots, u_{r+s-1} \in \mathscr{O}_K^*$ tali che $L(u_1), \ldots, L(u_{r+s-1})$ sono linearmente indipendenti su $\mathbb{R}$.

Lemma. *Fissiamo $1 \leq k \leq r+s$. $\forall \alpha \in \mathscr{O}_K \backslash \{0\}$, $\exists \beta \in \mathscr{O}_K \backslash \{0\}$ tale che $\left|\mathrm{N}_{K/\mathbb{Q}}(\beta)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$ e, se $L(\alpha) = (a_1, \ldots, a_{r+s})$ e $L(\beta) = (b_1, \ldots, b_{r+s})$, si ha $b_i < a_i$ $\forall i \neq k$.*

Dimostrazione. Sia $B = \left\{(y, z) \in \mathbb{R}^r \times \mathbb{C}^s \middle| |y_i| \leq c_i,\ \|z_j\| \leq c_{r+j}\right\}$, con $0 < c_i < e^{a_i}$ $\forall i = 1, \ldots, r+s$, $i \neq k$.
c_k lo determino imponendo che $\mu(B) = 2^r c_1 \cdot \ldots \cdot c_r \cdot \pi^s \cdot c_{r+1}^2 \cdot \ldots \cdot c_{r+s}^2$ sia tale che $c_1 \cdot \ldots \cdot c_r \cdot c_{r+1}^2 \cdot \ldots \cdot c_{r+s}^2 = \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$, cioé $\mu(B) = 2^n \operatorname{vol}(\sigma(\mathscr{O}_K))$.
Per il teorema di Minkowski, $\exists \beta \in \mathscr{O}_K \backslash \{0\}$ tale che $\sigma(\beta) \in B$, cioé $|\sigma_i(\beta)| \leq c_i < e^{a_i}$ $\forall i \neq k$ (cioé $|\log|\sigma_i(\beta)|| < a_i$ $\forall i \neq k$) e $\left|\mathrm{N}_{K/\mathbb{Q}}(\beta)\right| \leq \prod c_i \cdot \prod c_{r+j}^2 = \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$. □

Lemma. *Fissiamo $1 \leq k \leq r+s$. $\exists u_k \in \mathscr{O}_K^*$ tale che, posto $L(u_k) = (x_1, \ldots, x_{r+s})$, si ha $x_i < 0$ $\forall i \neq k$ (e dunque $x_k > 0$, poiché $\left|\mathrm{N}_{K/\mathbb{Q}}(u_k)\right| = 1$, e perció $x_k = -\sum_{i \neq k} x_i > 0$).*

Dimostrazione. Sia $\alpha \in \mathscr{O}_K \backslash \{0\}$. Applicando ricorsivamente il lemma precedente ad α, si ottiene una successione $\alpha_1, \alpha_2, \ldots \in \mathscr{O}_K \backslash \{0\}$ tale che $\mathrm{N}((\alpha_j)) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_j)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$ $\forall j \in \mathbb{N}$.
Ma gli ideali di norma limitata sono in numero finito, dunque $\exists l > \lambda$ tale che $(\alpha_l) = (\alpha_\lambda)$ e $|\log|\sigma_i(\alpha_l)|| < |\log|\sigma_i(\alpha_\lambda)||$ $\forall i \neq k$.
Ma allora $\exists u_k \in \mathscr{O}_K^*$ tale che $\alpha_l = u_k \cdot \alpha_\lambda$, dunque $|\log|\sigma_i(u_k)|| < 0$ $\forall i \neq k$. □

Lemma. *Sia $A = (a_{ij}) \in \mathcal{M}(m)$ tale che $a_{ij} < 0$ $\forall i \neq j$, $a_{ii} > 0$ $\forall i$ e $\sum_{i=1}^m a_{ij} = 0$ $\forall j$; allora $\operatorname{rk}(A) = m - 1$.*

Dimostrazione. Sicuramente $\operatorname{rk}(A) \leq m-1$; vediamo che le prime $m-1$ colonne sono indipendenti.
Supponiamo per assurdo che $t_1 v_1 + \ldots + t_{m-1} v_{m-1} = 0$, dove i v_j sono i vettori colonna e i t_j sono numeri reali non tutti 0; a meno di dividere per $\pm \max(|t_1|, \ldots, |t_{m-1}|) > 0$, si puó supporre $t_k = 1$ per un certo k e $t_j \leq 1$ $\forall j \neq k$.
Ma allora, guardando alla k-esima riga, si ha:

$$0 = \sum_{j=1}^{m-1} t_j a_{kj} \geq \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^{m} a_{kj} = 0,$$

da cui l'assurdo voluto. □

Ma allora, degli $r+s$ vettori trovati nel secondo lemma, $r+s-1$ hanno immagini secondo L indipendenti grazie al terzo lemma; segue dunque la tesi.

□

Osservazione. Il teorema di Dirichlet conferma il risultato di un vecchio esercizio in cui si calcolava $\mathscr{O}_K^*$ con $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$: infatti $\phi(n) = 2 \iff n \in \{3, 4, 6\}$, dunque gli unici K per cui $\mathscr{O}_K^*$ contiene strettamente $\{\pm 1\}$ sono $K = \mathbb{Q}(\sqrt{-1})$ e $K = \mathbb{Q}(\sqrt{-3})$.

Esempio (Campi quadratici reali). Sia $K = \mathbb{Q}(\sqrt{d})$, con $d > 0$ libero da quadrati. $\mathscr{O}_K^* \cong \{\pm 1\} \oplus \mathbb{Z}$ per il teorema di Dirichlet, in quanto le radici reali dell'unitá sono ± 1 e $r = 2$, $s = 0$. In particolare $\mathscr{O}_K^* \cong \{\pm 1\} \oplus \langle \varepsilon \rangle_{\mathbb{Z}}$, dove ε é l'unitá fondamentale; visto che se α é un'unitá fondamentale, anche $\pm\alpha$, $\pm\alpha^{-1}$ lo sono, imponiamo che ε sia l'(unica) unitá fondamentale > 1. Cerchiamo un modo per determinare ε.
$\mathscr{O}_K = \mathbb{Z}[\omega]$, con $\omega = \sqrt{d}$ se $d \equiv 2, 3 \pmod 4$, altrimenti $\omega = \frac{1+\sqrt{d}}{2}$.
Sia $\alpha = a + b\omega$; $\alpha \in \mathscr{O}_K^* \iff a, b \in \mathbb{Z}$ e $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$. Poniamo $a \geq 0$, $b > 0$..
Se $\omega = \sqrt{d}$, si ha che $\{\pm\alpha, \pm\alpha^{-1}\} = \{\pm(a+b\sqrt{d}), \pm(a-b\sqrt{d})\}$ (in quanto $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d = \pm 1$), ma visto che ce n'é solo una > 1, deve essere quella con segni positivi, cioé $a+b\sqrt{d}$; dunque $a + b\sqrt{d} \geq \pm a \pm b\sqrt{d}$ e $a > 0$, $b > 0$.
Se $\omega = \frac{1+\sqrt{d}}{2}$, si ha:

$$\left(a + b\left(\frac{1+\sqrt{d}}{2}\right)\right) \cdot \left(a + b\left(\frac{1-\sqrt{d}}{2}\right)\right) = \pm 1,$$

che con facili calcoli diventa:

$$(2a + b)^2 - b^2 d = \pm 4.$$

Se $d = 5$, si vede che l'unitá fondamentale corrisponde a $a = 0$, $b = 1$, cioé $\varepsilon = \omega$; se invece $d > 5$, si ha necessariamente $a > 0$, $b > 0$.
Dunque, escludendo il (banale) caso $d = 5$, l'unitá fondamentale ha i coefficienti a, b strettamente positivi.
Per quanto visto, abbiamo che, detta ε l'unitá fondamentale, $\forall \alpha \in \mathscr{O}_K^*$, $\alpha > 1$, $\exists n > 0$ tale che $\alpha = \varepsilon^n$, dunque é la piú piccola possibile; inoltre, per come abbiamo definito l'unica unitá fondamentale, si ha che, se $\varepsilon^n = a_n + b_n\omega$, le successioni $\{a_n\}$ e $\{b_n\}$ sono strettamente crescenti.
Esplicitamente, se $d \equiv 2, 3 \pmod 4$, si ha che $a_{n+1} = a_n a_1 + b_n b_1 d$ e $b_{n+1} = a_n b_1 + b_n a_1$; un conto simile puó essere fatto per $d \equiv 1 \pmod 4$.
Dunque, per $d \equiv 2, 3 \pmod 4$ (altrimenti il ragionamento é analogo), un algoritmo banale (e piuttosto inefficiente) puó essere il seguente: consideriamo la successione $\{b^2 d \pm 1\}_{b>1}$; non appena uno di questi numeri é un quadrato, si ricava b e a dell'unitá fondamentale.
Ad esempio, se $d = 7$:

$$\{7b^2 \pm 1\}_{b>1} = \{6, 8, 27, 29, 62, 64, \ldots\}.$$

64 é un quadrato, dunque si ricava $b = 3$ e $a = \sqrt{64} = 8$, cioé $\varepsilon = 8 + 3\sqrt{7}$.

Un algoritmo piú raffinato sfrutta il seguente classico risultato; ricordiamo prima una definizione:

Definizione 5.3.1. Sia $\xi = [c_0, c_1, c_2, c_3, \ldots]$, cioé:

$$\xi = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$$

Allora i numeri $[c_0, \ldots, c_k]$, con $k \geq 1$, sono detti i **convergenti** della frazione continua di ξ.

Teorema 5.3.2. *Sia $\xi \in \mathbb{R}^+$, e siano $x, y \in \mathbb{N}$ coprimi tali che $\left|\xi - \frac{x}{y}\right| < \frac{1}{2y^2}$.*
Allora $\frac{x}{y}$ é uno dei convergenti della frazione continua di ξ.

Osservazione. Sia $\varepsilon = a + b\omega$, $\sigma(\varepsilon) = a + b\sigma(\omega)$; $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \pm 1$, dunque $|\sigma(\varepsilon)| = \frac{1}{|\varepsilon|} = \frac{1}{\varepsilon} = \frac{1}{a+b\omega}$, in quanto $\varepsilon > 1$.
Stimiamo $\left|\frac{\sigma(\varepsilon)}{b}\right| = \left|\frac{a}{b} + \sigma(\omega)\right| = \frac{1}{b(a+b\omega)}$.

- $d \equiv 1 \quad (4)$, $d > 5$. Si ha:

$$\left|\frac{a}{b} + \frac{1-\sqrt{d}}{2}\right| = \frac{1}{b^2\Big(\underbrace{\frac{a}{b}}_{>0} + \underbrace{\frac{1+\sqrt{d}}{2}}_{>2}\Big)} < \frac{1}{2b^2}.$$

- $d \equiv 2, 3 \quad (4)$. Si ha $a^2 = \pm 1 + b^2 d \geq b^2 d - 1 \geq b^2(d-1)$, dunque:

$$\left|\frac{a}{b} - \sqrt{d}\right| = \frac{1}{b(a+b\sqrt{d})} = \frac{1}{b^2\left(\frac{a}{b} + \sqrt{d}\right)} < \frac{1}{b^2(\sqrt{d-1} + \sqrt{d})} < \frac{1}{2b^2}.$$

In ogni caso, si deve cercare a, b in modo che $\frac{a}{b}$ sia uno dei convergenti della frazione continua di $-\sigma(\omega)$.

Segue immediatamente il seguente:

Algoritmo. *Per trovare a, b tali che $\varepsilon = a + b\omega$ é l'unitá fondamentale, calcolo i convergenti $\frac{p_k}{q_k}$ di $-\sigma(\omega)$ e poi testo se $\mathrm{N}_{K/\mathbb{Q}}(p_k + q_k\omega) = \pm 1$. Il primo che trovo é il convergente voluto.*

Esempio. Consideriamo $K = \mathbb{Q}(\sqrt{41})$. $\omega = \frac{1+\sqrt{41}}{2}$, dunque $-\sigma(\omega) = \frac{\sqrt{41}-1}{2}$.
Si calcola che:

$$\frac{\sqrt{41}-1}{2} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cdots}}}}$$

Dunque $p_0 = 2$, $q_0 = 1$, $\frac{p_1}{q_1} = c_0 + \frac{1}{c_1} = \frac{c_0 c_1 + 1}{c_1}$, e usando le relazioni $p_k = c_k p_{k-1} + p_{k-1}$, $q_k = c_k q_{k-1} + q_{k-2}$, si ottiene la tabella:

k	0	1	2	3	4
c_k	2	1	2	2	1
p_k	2	3	8	19	27
q_k	1	1	3	7	10
$\mathrm{N}_{K/\mathbb{Q}}(p_k + q_k\omega)$	-4	2	-2	4	-1

Da questo segue che $\varepsilon = 27 + 10\omega$ é l'unitá fondamentale cercata.

6 Appendice

6.1 Un'introduzione alla Class Field

Esempio. Determinare $\mathrm{Cl}(K)$, dove $K = \mathbb{Q}(\sqrt{-21})$.

Dimostrazione. $-21 \equiv 3 \pmod 4$, dunque $\mathscr{O}_K = \mathbb{Z}[\sqrt{-21}]$ e $\mathrm{disc}(K) = -4 \cdot 21 = -2^2 \cdot 3 \cdot 7$. Inoltre $r = 0$, $s = 1$.
Sappiamo che, se $(e(P|p), \mathrm{N}(P)) = 1$, allora $P^{e-1} \parallel \mathfrak{D}_{K/\mathbb{Q}}$.
Dunque, se $p \neq 2$, si puó applicare la precedente relazione, ottenendo che, se $P|p$, $\mathfrak{D}_{K/\mathbb{Q}} = P^{e-1}I$, con $(I, P) = 1$.
$\mathrm{disc}(K) = \mathrm{N}(P)^{e-1}\,\mathrm{N}(I) = p^{f(e-1)}m$, dunque se $p = 3, 7$, m deve essere coprimo con p (altrimenti l'esponente sarebbe > 1), perció 3 e 7 hanno ramificazione tame.
La costante di Minkowski é:

$$\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\,\mathrm{disc}(K)|} = \frac{2}{2^2}\frac{2^2}{\pi}\sqrt{2^2 \cdot 3 \cdot 7} = \frac{4}{\pi}\sqrt{21} < 6.$$

Quindi ogni classe di ideali contiene un'ideale intero I con $\mathrm{N}(I) \leq 5$. Se $P|I$, allora $p = P \cap \mathbb{Z} \leq 5$.
Vediamo come si fattorizzano $2, 3, 5$.
$p = 2$ é ramificato, dunque $2\mathscr{O}_K = P^2$.
$p = 3$ é ramificato, dunque $3\mathscr{O}_K = Q^2$.
$p = 5$ non é ramificato, e per Kummer $5\mathscr{O}_K = Q_1Q_2$, in quanto $x^2 + 21 \equiv x^2 - 4 \pmod 5$.
$\mathrm{N}(P) = 2$, ma non esiste un elemento di norma 2, perché l'equazione $a^2 + 21b^2 = 2$ non ha soluzione, dunque P non é principale, da cui $ord([P]) = 2$.
Un ragionamento del tutto analogo si puó ripetere anche per Q, ottenendo $ord([Q]) = 2$.
Inoltre $[P] = [Q] \iff [PQ] = e \iff PQ$ é principale, ma $\mathrm{N}(PQ) = \mathrm{N}(P)\,\mathrm{N}(Q) = 6$ e non esistono elementi di norma 6. Dunque $P \neq Q$.
Abbiamo che $[Q_1] = [Q_2]^{-1}$. Se Q_1^2 fosse principale, sarebbe generato da un elemento di ordine 25.
Osserviamo che $\mathrm{N}_{K/\mathbb{Q}}(2 + \sqrt{-21}) = 25$; dunque l'ideale $(2 + \sqrt{-21})$ si fattorizza come prodotto di due ideali di norma 5: $(2 + \sqrt{-21}) = Q_1Q_2$ oppure $(2 + \sqrt{-21}) = Q_1^2$, ma la prima possibilitá é impossibile perché $Q_1Q_2 = (5)$.
Dunque $ord([Q_1]) = ord([Q_2]) = 2$.
Nel gruppo ci deve essere $[PQ]$, e non puó essere e né P né Q, dunque $[PQ] = [Q_1]$ (e non ci sono altri elementi perché altri possibili ideali avrebbero norma > 5), da cui segue che $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (ha ordine 4 e tutti gli elementi hanno ordine 2). □

Esercizio (Marcus, n° 28, pag. 151)**.** *Sia K un campo di numeri, $I \subseteq \mathscr{O}_K$ un ideale.*

1. *Mostrare che esiste un'estensione L/K finita tale che $I\mathscr{O}_L$ é principale.*
2. *Mostrare che esiste un'estensione L/K finita tale che $\forall J \subseteq \mathscr{O}_K$, $J\mathscr{O}_L$ é principale.*
3. *Trovare un'estensione di grado 4 di $\mathbb{Q}(\sqrt{21})$ in cui ogni ideale diventa primo.*

Dimostrazione. 1. $\exists m$ tale che $I^m = (\alpha)$. Poniamo $L = K(\sqrt[m]{\alpha})$; mostriamo che $I\mathscr{O}_L = (\sqrt[m]{\alpha})$.
$(I\mathscr{O}_L)^m = I^m\mathscr{O}_L = (\alpha)\mathscr{O}_L$ e $(\sqrt[m]{\alpha})^m = (\alpha)\mathscr{O}_L$, dunque per il teorema di fattorizzazione unica, le fattorizzazioni di $(I\mathscr{O}_L)^m$ e $(\sqrt[m]{\alpha})^m$ coincidono, ma essendo l'elevamento a potenza una semplice moltiplicazione negli esponenti della fattorizzazione, si ha che anche le fattorizzazioni di $(\sqrt[m]{\alpha})$ e $I\mathscr{O}_L$ devono coincidere, da cui $I\mathscr{O}_L = (\sqrt[m]{\alpha})$.

2. Sia $\mathrm{Cl}(K) = \{[I_1], \dots, [I_d]\}$. $\forall 1 \leq i \leq d$, $\exists m_i$ tale che $I_i^{m_i} = (\alpha_i)$, dunque se $L_i = K(\sqrt[m]{\alpha_i})$, per il punto precedente $I_i\mathscr{O}_{L_i} = (\sqrt[m_i]{\alpha_i})$.
Se $L = \prod L_i$, é un'estensione finita (perché composto di estensioni finite) e ogni ideale di $\mathscr{O}_K$ diventa principale in L: infatti sia $J \subseteq \mathscr{O}_K$. Esiste i tale che $J \sim I_i$, dunque $\exists \beta \in \mathscr{O}_K^*$ tale che $J = \beta I$, da cui $J\mathscr{O}_L = (\beta)I_i\mathscr{O}_L = (\beta \sqrt[m_i]{\alpha_i})$ é principale.

3. Per l'esercizio precedente, $\mathrm{Cl}(K) = \langle [P] \rangle \times \langle [Q] \rangle$, e $P^2 = (2)$, $Q^2 = (3)$. Per quanto visto, $L = K(\sqrt{2}, \sqrt{3})$ é l'estensione voluta.

□

Osservazione. $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Cl}(K)$.

Definizione 6.1.1. Il fenomeno descritto nell'esercizio precedente é chiamato **capitolazione degli ideali**.

Definizione 6.1.2. Sia K un campo di numeri. Si definisce l'**Hilbert Class Field** H di K la piú grande estensione abeliana non ramificata di K (dunque $\forall P \subseteq \mathscr{O}_K$, P non ramifica in H e non ramificano neanche i primi infiniti, cioé, dette $\sigma_1, \dots, \sigma_r$ le immersioni reali di K, si deve avere che $\forall \tau : H \hookrightarrow \mathbb{C}$ tale che $\tau_{|K} = \sigma_i$ con $1 \leq i \leq r$, $\tau(H) \subseteq \mathbb{R}$).

Osservazione. L'Hilbert Class Field di K é il composto di tutte le estensioni con tali proprietá (che formano un insieme non vuoto in quanto contenente $\{K\}$), dunque esiste sempre.

Enunciamo ora un risultato fondamentale della Class Field globale, che motiva l'osservazione subito dopo l'ultimo esercizio, ma ne presentiamo solo un accenno di dimostrazione:

Teorema 6.1.1 (della Class Field globale)**.** *Sia H l'Hilbert Class Field di K. Allora* $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$.

Idea della dimostrazione. Consideriamo la mappa di Artin:

$$\begin{array}{ccc} \mathcal{I}(K) & \longrightarrow & \mathrm{Gal}(H/K) \\ P & \longrightarrow & \phi(P) \end{array}$$

dove $\phi(P)$ é il Frobenius di P, che si estende moltiplicativamente:

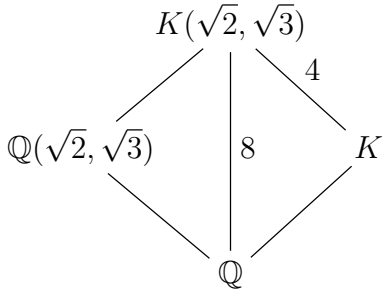
$$\prod_i P_i^{e_i} \longrightarrow \prod_i \phi(P_i)^{e_i}.$$

L'obiettivo della dimostrazione é di mostrare che tale mappa é surgettiva e che il nucleo non é altro che il sottogruppo degli ideali principali. □

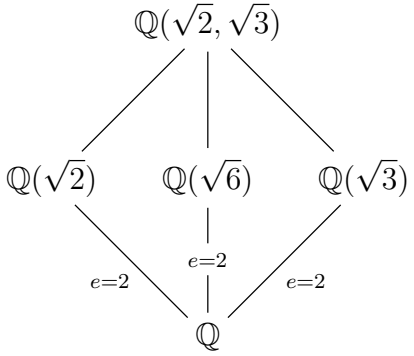
Enunciamo un altro importantissimo teorema, senza dimostrazione:

Teorema 6.1.2 (dell'ideale principale)**.** *Nell'Hilbert Class Field H, tutti gli ideali di K capitolano (cioé diventano principali).*

Osservazione. Nell'ultimo esercizio abbiamo visto che, posto $K = \mathbb{Q}(\sqrt{-21})$ e $L = K(\sqrt{2}, \sqrt{3})$, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$ e in L tutti gli ideali di K capitolano: é dunque L l'Hilbert Class Field di K?
La risposta é negativa, in quanto il primo 2 ramifica; per vederlo consideriamo il diagramma:



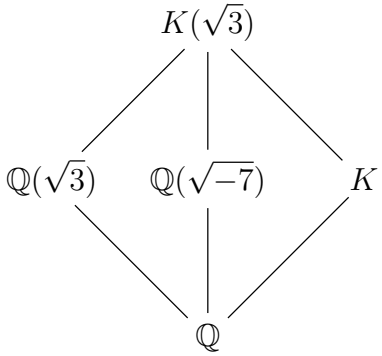
Nell'estensione $K/\mathbb{Q}$, il primo $p = 2$ ha indice di ramificazione $e = 2$; invece, grazie al diagramma:



mostra che il primo 2 é totalmente ramificato nell'estensione $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, in quanto se non lo fosse, non esisterebbero estensioni intermedie; dunque segue che $e = 4$ in tale estensione.
Dunque, ritornando al primo diagramma, vediamo che l'indice di ramificazione nell'estensione $K(\sqrt{2},\sqrt{3})/K$ deve essere almeno $e = 2 > 1$, che dimostra che L non é l'Hilbert Class Field di K.

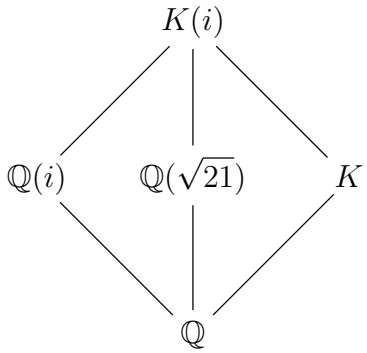
Proviamo quindi a trovare l'effettivo Hilbert Class Field di K.

Esempio. Determiniamo l'Hilbert Class Field H di $K = \mathbb{Q}(\sqrt{-21})$. Notiamo innanzitutto che ci dobbiamo occupare solamente dei primi finiti, in quanto le immersioni di K sono puramente immaginarie.
Dico che l'estensione $K(\sqrt{3})/K$ é abeliana (ovviamente) e non ramificata; per vederlo mostriamo che $\mathrm{disc}(K(\sqrt{3})/K) = 1$.
Consideriamo il diagramma:



Nell'estensione $K/\mathbb{Q}$, gli unici primi ramificati sono $p = 2, 3, 7$, mentre nell'estensione $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ gli unici primi ramificati sono $p = 2, 3$: concludiamo che, se $p \neq 2, 3, 7$, p non ramifica in $K(\sqrt{3})/\mathbb{Q}$ e dunque, per moltiplicativitá nelle torri, neanche in $K(\sqrt{3})/K$.
Sia $p = 7$. In $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, $rf = 2$, dunque $rf = 2$ anche in $K(\sqrt{3})/K$ e perció 7 non é ramificato in $K(\sqrt{3})/K$ (alternativamente si poteva arrivare allo stesso risultato notando che se 7 fosse totalmente ramificato in $K(\sqrt{3})/K$, sarebbe totalmente ramificato in $K(\sqrt{3})/\mathbb{Q}$ e dunque anche in ogni estensione intermedia, assurdo).
Inoltre $\mathrm{disc}(\mathbb{Q}(\sqrt{-7})) = -7$, dunque per moltiplicativitá nelle torri $2, 3$ non possono essere ramificati in $K(\sqrt{3})/K$.
Concludiamo che $\mathrm{disc}(K(\sqrt{3})/K) = 1$.
Potevamo giungere allo stesso risultato nel modo seguente: $K(\sqrt{3}) = \mathbb{Q}(\sqrt{3},\sqrt{-7})$ e, posti $K_1 = \mathbb{Q}(\sqrt{3})$, $K_2 = \mathbb{Q}(\sqrt{-7})$, si ha $\mathrm{disc}(K_1) = 12$, $\mathrm{disc}(K_2) = 7$, che sono coprimi, dunque $\mathrm{disc}(K(\sqrt{3})/\mathbb{Q}) = (\mathrm{disc}(K_1))^2(\mathrm{disc}(K_2))^2 = 2^4 \cdot 3^2 \cdot 7^2$.
Ma $\mathrm{disc}(K(\sqrt{3})/\mathbb{Q}) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{disc}(K(\sqrt{3})/K)) \cdot \mathrm{disc}(K/\mathbb{Q})^2 = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{disc}(K(\sqrt{3})/K)) \cdot 2^4 \cdot 3^2 \cdot 7^2$, da cui $\mathrm{N}_{K/\mathbb{Q}}(\mathrm{disc}(K(\sqrt{3})/K)) = 1$ e quindi $\mathrm{disc}(K(\sqrt{3})/K) = 1$.
Vogliamo ora mostrare che anche $K(i)/K$ é abeliana e non ramificata; per farlo procediamo

come prima.
Abbiamo il diagramma:



Si ha che $\text{disc}(\mathbb{Q}(i)) = -4$ e $\text{disc}(\mathbb{Q}(\sqrt{21})) = 21$, dunque come prima $\text{disc}(K(i)/\mathbb{Q}) = 2^4 \cdot 3^2 \cdot 7^2$ e quindi $\text{disc}(K(i)/K) = 1$.
Siamo giunti quindi alla conclusione che l'Hilbert Class Field di K é $H = K(\sqrt{3}, i)$ (é infatti evidente che ha grado 4).

Esercizio. *Mostra che effettivamente nell'esempio precedente gli ideali di K capitolano in H. (Suggerimento: basta vedere che 2 e 3 capitolano).*

6.2 Un'introduzione ai campi ciclotomici

Nel seguito sia $K = \mathbb{Q}(\zeta_n)$ e $\zeta = \zeta_n$.

Osservazione. 1. Se $n = p^m$, allora $p\mathscr{O}_K$ é totalmente ramificato, in particolare $p\mathscr{O}_K = P^{\phi(p^n)}$, dove $P = (1-\zeta)$.

2. Se $n = p_1^{m_1} \cdot \ldots \cdot p_t^{m_t}$, con $t > 1$, $1 - \zeta$ é un'unitá.

Dimostrazione. 1. Per dimostrare che $P = (1-\zeta)$, basta vedere che $\text{N}_{K/\mathbb{Q}}(1-\zeta) = p$ (in quanto sappiamo che $p\mathscr{O}_K$ é totalmente ramificato).
Il polinomio minimo di ζ é:

$$\mu_\zeta(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = \prod_{(i,p)=1} (x - \zeta^i) = \left(x^{p^{m-1}}\right)^{p-1} + \ldots + x^{p^{m-1}} + 1$$

dunque:

$$p = \mu_\zeta(1) = \prod_{(i,p)=1} (1 - \zeta^i) = \text{N}_{K/\mathbb{Q}}(1-\zeta).$$

2. Abbiamo la relazione $\forall n$:

$$x^{n-1} + \ldots + x + 1 = \prod_{i=1}^{n-1} (x - \zeta^i) \Rightarrow n = \prod_{i=1}^{n-1} (1 - \zeta^i).$$

In particolare, $\forall 1 \leq k \leq t$, abbiamo che $p_k^{m_k} = \prod_{i=1}^{p_k^{m_k}-1} (1 - \zeta_{p_k^{m_k}}^i)$, ma osservando che $\zeta_{p_k^{m_k}}^i = \zeta_n^{\frac{n}{p_k^{m_k}} i}$, dividendo entrambi i membri della prima relazione si ha:

$$1 = \prod_{(i,n)=1} (1 - \zeta^i).$$

□

Denotiamo $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$.

Osservazione. Abbiamo che $E = \mathscr{O}_K^* \cong \underbrace{W}_{=\langle \pm\zeta \rangle} \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1}$, mentre $E^+ = \mathscr{O}_{K^+}^* \cong \langle \pm 1 \rangle \oplus \mathbb{Z}^{\frac{\phi(n)}{2}-1}$
(in quanto K é totalmente immaginari e K^+ é totalmente reale).
Segue dunque che $\frac{E}{E^+}$ é finito.

Lemma 6.2.1. *α intero algebrico tale che ogni suo coniugato (e α stesso) hanno valore assoluto 1. Allora α é una radice dell'unitá.*

Dimostrazione. L'insieme $\{\alpha^h\}_{h \geq 1}$ é composto da interi algebrici e $\left|\sigma(\alpha^h)\right| = \left|\sigma(\alpha)^h\right| = 1 \ \forall \sigma$ immersione di $K = \mathbb{Q}(\alpha)/\mathbb{Q}$.
Ma in K ci sono solo un numero finito di elementi con la proprietá dell'enunciato (in quanto il loro polinomio minimo ha grado limitato e i coefficienti sono interi e limitati perché combinazioni dei coniugati), dunque $h > k$ tale che $\alpha^h = \alpha^k$, cioé $\alpha^{h-k} = 1$. □

Osservazione. Il precedente lemma diventa falso se si toglie l'ipotesi che α sia intero; ad esempio $\alpha = \frac{3}{5} + i\frac{4}{5}$ sarebbe un controesempio.

Teorema 6.2.2. *$Q = [E : E^+W] \in \{1, 2\}$; in particolare $Q = 1 \iff$ n é potenza di un primo.*

Dimostrazione. Consideriamo la mappa:

$$\begin{array}{rccc} \phi: & E & \longrightarrow & W \\ & \varepsilon & \longrightarrow & \frac{\varepsilon}{\overline{\varepsilon}} \end{array}$$

L'elemento $\frac{\varepsilon}{\overline{\varepsilon}}$ é un intero algebrico in $\mathscr{O}_K^*$, dunque se mostro che tutti i suoi coniugati hanno valore assoluto 1, per il lemma ho che é una radice dell'unitá e dunque necessariamente dovrebbe stare in W. In effetti:

$$\left|\sigma\left(\frac{\varepsilon}{\overline{\varepsilon}}\right)\right| = \left|\frac{\sigma(\varepsilon)}{\sigma(\overline{\varepsilon})}\right| = \left|\frac{\sigma(\varepsilon)}{\overline{\sigma(\varepsilon)}}\right| = 1,$$

in quanto, essendo $\mathrm{Gal}(K/\mathbb{Q})$ abeliano, σ e coniugio commutano.
Consideriamo la composizione:

$$\psi : E \xrightarrow{\phi} W \xrightarrow{\pi} \frac{W}{W^2},$$

dove π é la proiezione; dico che $\mathrm{Ker}(\psi) = E^+W$ (e quindi $\frac{E}{E^+W}$ si immergerebbe in un gruppo di ordine $[W : W^2] = 2$).

$\supseteq$) Se $\zeta \in W$ e $\varepsilon_1 \in E^+ \subseteq \mathbb{R}$, si ha$\phi(\zeta\varepsilon_1) = \frac{\zeta\varepsilon_1}{\overline{\zeta\varepsilon_1}} = \frac{\zeta}{\overline{\zeta}} = \frac{\zeta}{\zeta^{-1}} = \zeta^2 \in W^2$.

$\subseteq$) Se $\varepsilon \in \mathrm{Ker}(\psi)$, allora $\phi(\varepsilon) = \frac{\varepsilon}{\overline{\varepsilon}} = \zeta^2$, con $\zeta \in W$.
Ma allora $\varepsilon_1 = \zeta^{-1}\varepsilon \in E^+$, poiché $\overline{\varepsilon_1} = \overline{\zeta^{-1}}\overline{\varepsilon} = \zeta\frac{\varepsilon}{\zeta^2} = \zeta^{-1}\varepsilon = \varepsilon_1$.

Sia ora $n = p^\alpha$, con $p \neq 2$; vediamo che ogni elemento $\frac{\varepsilon}{\overline{\varepsilon}} \in W$, in realtá $\in W^2$.
Sicuramente $\frac{\varepsilon}{\overline{\varepsilon}} = \pm\zeta^a$; se mostriamo che $-$ non é possibile, avremmo la tesi (in quanto se $2 \nmid a$, $2|a+n$ e $\zeta^a = \zeta^{a+n}$).
Se per assurdo $\varepsilon = -\zeta^a\overline{\varepsilon} = a_0 + a_1\zeta + \ldots + a_{\phi(n)-1}\zeta^{\phi(n)-1}$, si avrebbe $\varepsilon \equiv a_0 + a_1 + \ldots + a_{\phi(n)-1} \quad (1-\zeta)$, mentre $\overline{\varepsilon} = a_0 + a_1\overline{\zeta} + \ldots + a_{\phi(n)-1}\overline{\zeta}^{\phi(n)-1} \equiv a_0 + a_1 + \ldots + a_{\phi(n)-1} \quad (1-\overline{\zeta})$, ma $(1-\zeta) = (1-\overline{\zeta})$ (in quanto differiscono per moltiplicazione di ζ), dunque $\varepsilon \equiv \overline{\varepsilon} \quad (1-\zeta)$.
Avendo peró che $\varepsilon = -\zeta^a\overline{\varepsilon}$, si avrebbe anche $\varepsilon \equiv \overline{\varepsilon} \quad (1-\zeta)$, cioé $2\varepsilon \equiv 0 \quad (1-\zeta)$, e quindi $\varepsilon \in (1-\zeta)$ (in quanto $(1-\zeta)$ é primo e $(1-\zeta) \nmid 2$), assurdo perché ε é invertibile.
Sia invece $n = 2^m$; se per assurdo $\exists \varepsilon \in E$ tale che $\frac{\varepsilon}{\overline{\varepsilon}} \notin W^2$, si avrebbe che $\frac{\varepsilon}{\overline{\varepsilon}} = \zeta$, con ζ radice 2^m-esima primitiva dell'unitá.

$\mathrm{N}_{K/\mathbb{Q}(i)}(\zeta) = \zeta^a$, con $a = \sum_{\substack{0<b<2^m \\ b\equiv 1 \ (4)}} b$, in quanto $i = \zeta^{2^{m-2}}$ e affinché $i \to i$, si deve avere che $\zeta^{2^{m-2}} = \zeta^{2^{m-2}b}$, cioé $b \equiv 1 \pmod 4$; inoltre $a \equiv 2^{m-2} \pmod{2^{m-1}}$, in quanto:

$$a = \sum_{k=0}^{2^{m-2}-1} (1+4k) = 2^{m-2} + 4\frac{(2^{m-2}-1)2^{m-2})}{2} = 2^{m-2} + 2^{m-1}(2^{m-2}-1).$$

Ma allora ζ^a ha ordine 4, cioé é una radice quarta dell'unitá, cioé:

$$\pm i = \mathrm{N}_{K/\mathbb{Q}(i)}(\zeta) = \frac{\mathrm{N}_{K/\mathbb{Q}(i)}(\varepsilon)}{\mathrm{N}_{K/\mathbb{Q}(i)}(\overline{\varepsilon})} = \frac{\mathrm{N}_{K/\mathbb{Q}(i)}(\varepsilon)}{\overline{\mathrm{N}_{K/\mathbb{Q}(i)}(\varepsilon)}},$$

assurdo, poiché essendo ε invertibile, $\mathrm{N}_{K/\mathbb{Q}(i)}(\varepsilon)$ deve essere invertibile in $\mathbb{Q}(i)$, cioé $\mathrm{N}_{K/\mathbb{Q}(i)}(\varepsilon) = \pm 1, \pm i$.
Sia infine n non una potenza di un primo; abbiamo visto che $1-\zeta$ é un'unitá.
$\frac{1-\zeta}{1-\zeta} = -\zeta \notin W^2$, in quanto, se $-\zeta \in W^2$, $-\zeta = \zeta^{2r}$, cioé $-1 = \zeta^{2r-1}$ (e dunque $2|n$).
Se $4|n$, $-1 = \zeta^{\frac{n}{2}}$ e perció $\frac{n}{2} \equiv 2r-1 \pmod n$, cioé $\frac{n}{2} \equiv -1 \pmod 2$, assurdo; se $n \equiv 2 \pmod 4$, si ha $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\frac{n}{2}})$ e qua si avrebbe l'assurdo. □

Teorema 6.2.3. *Sia $C = \mathrm{Cl}(K)$, $C^+ = \mathrm{Cl}(K^+)$. Allora si ha un'immersione $C^+ \hookrightarrow C$.*

Dimostrazione. Consideriamo la composizione:

$$\begin{array}{ccccc} \mathcal{I}(K^+) & \longrightarrow & \mathcal{I}(K) & \longrightarrow & C \\ I & \longrightarrow & I\mathscr{O}_K & \longrightarrow & [I\mathscr{O}_K] \end{array}$$

Sicuramente la mappa passa al quoziente per $\mathcal{P}(K^+)$; per vedere che é iniettiva, dobbiamo vedere che, se $I\mathscr{O}_K = (\alpha)$, I era giá principale in $\mathcal{I}(K^+)$.
$I \subseteq \mathscr{O}_{K^+}$, dunque $I = \overline{I}$, perció $(1) = \frac{I\mathscr{O}_K}{\overline{I}\mathscr{O}_K} = \left(\frac{\alpha}{\overline{\alpha}}\right)$ e $\frac{\alpha}{\overline{\alpha}}$ é un'unitá tale che $\left|\frac{\alpha}{\overline{\alpha}}\right| = 1$.
Visto che questo stesso ragionamento puó essere ripetuto per i coniugati di $\frac{\alpha}{\overline{\alpha}}$ (in quanto il gruppo di Galois é abeliano e il coniugio commuta con le immersioni), abbiamo che $\frac{\alpha}{\overline{\alpha}}$ é una radice dell'unitá.
Se n non é una potenza dell'unitá, sappiamo che $\phi(E) = W$, dunque $\exists \varepsilon \in E$ tale che $\frac{\varepsilon}{\overline{\varepsilon}} = \frac{\alpha}{\overline{\alpha}}$, cioé $\varepsilon\alpha = \overline{\varepsilon\alpha} \in E^+$.
Per l'invertibilitá di ε, $I\mathscr{O}_K = (\alpha) = (\varepsilon\alpha)$, ma allora per fattorizzazione unica $I = (\varepsilon\alpha)$ in $\mathscr{O}_{K^+}$.
Sia invece $n = p^a$, e denotiamo $\pi = \zeta_{p^a} - 1$.
$\frac{\pi}{\overline{\pi}} = -\zeta_{p^a}$, e inoltre si vede che $W = \langle -\zeta_{p^a} \rangle$ (se $p > 2$ basta elevare alla p^a per ottenere -1, se p é pari basta elevare alla p^{a-1} per ottenere -1).
Sia $\frac{\alpha}{\overline{\alpha}} \in W = \langle \frac{\pi}{\overline{\pi}} \rangle$; allora $\frac{\alpha}{\overline{\alpha}} = \frac{\pi^d}{\overline{\pi}^d}$. Mostriamo che d é pari (e avremmo la tesi, perché avremmo che $\phi(E) = W^2 = W$ e potremmo concludere come prima).
Detto $K = \mathbb{Q}(\zeta_{p^a})$, abbiamo le estensioni:

$$\begin{array}{cc} K & Q \\ | & \\ K^+ & P \\ | & \\ \mathbb{Q} & p \end{array}$$

dove $Q = (\pi)$ e $P\mathscr{O}_K = Q^2$ (in quanto $p\mathscr{O}_K = Q^{\phi(p^a)}$).
Denotiamo con $v_\pi(\alpha)$ l'esponente di (π) in (α); allora $v_\pi(\alpha) = v_\pi(I)$ é pari, in quanto, se $I = P^x J$, con $(P, J) = 1$, si ha che $I\mathscr{O}_K = Q^{2x}(J\mathscr{O}_K)$.
Per lo stesso ragionamento, essendo $\pi^d\alpha \in \mathbb{R}$ in quanto $\pi^d\alpha = \overline{\pi^d\alpha}$, si ha $v_\pi(\pi^d\alpha)$ pari, e perció $d = v_\pi(\pi^d) = v_\pi(\pi^d\alpha) - v_\pi(\alpha)$ é pari. □

Definizione 6.2.1. Un campo K di dice **CM** se é totalmente immaginario (cioé $\forall \sigma : K \hookrightarrow \mathbb{C}$, $\sigma(K) \not\subseteq \mathbb{R}$) e K é un'estensione quadratica di K^+ che é totalmente reale (cioé $\sigma(K^+) \subseteq \mathbb{R}\ \forall \sigma$).

Osservazioni.
- I campi ciclotomici sono CM.
- Se K^+ é un campo totalmente reale e $\alpha \in K^+$ é tale che $\sigma(\alpha) < 0\ \forall \sigma$, allora $K = K^+(\sqrt{\alpha})$ é CM.
- Se K é non reale e $K/\mathbb{Q}$ é abeliana, allora K é CM, in quanto K^+ é il campo fissato dal coniugio e K é totalmente immaginario perché elementi in $\mathrm{Gal}(K/\mathbb{Q})$ e coniugio commutano.
- $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ non é CM, perché l'unica sottoestensione di grado 2 é $\mathbb{Q}(\sqrt[3]{2})$ e non é totalmente reale.

Visto che i campi CM sono una estensione dei campi ciclotomici, é naturale chiedersi quali dei precedenti risultati continuano a valere in questa situazione piú generale; in effetti il primo rimane vero, mentre il secondo ha una tesi piú debole.

Teorema 6.2.4. *K campo CM. Allora $[E : E^+W] \in \{1, 2\}$.*

Teorema 6.2.5. *K campo CM, $h = |\mathrm{Cl}(K)|$, $h^+ = |\mathrm{Cl}(K^+)|$. Allora $h^+|h$.*

Esempio. Un esempio in cui, se K é CM, non é vero che $\mathrm{Cl}(K^+)$ si immerge in $\mathrm{Cl}(K)$, puó essere $K = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$. Ovviamente $K^+ = \mathbb{Q}(\sqrt{10})$.
Infatti sia $I = (2, \sqrt{10}) \subseteq \mathscr{O}_{K^+}$; I non é principale, poiché per Kummer $2\mathscr{O}_K = (2, \sqrt{10})^2$, ma in $\mathscr{O}_{K^+}$ non ci sono elementi di norma 2, peró $I\mathscr{O}_K = (2, \sqrt{10})\mathscr{O}_K = (\sqrt{-2})$.

6.3 Anelli di gruppo e basi normali intere

Definizione 6.3.1. Sia A un anello e G un gruppo finito. Definiamo **anello di gruppo** l'insieme $A[G] = \left\{ \sum_{g \in G} a_g g \middle| a_g \in A \right\}$ con le operazioni:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{h \in G} b_h h \right) = \sum_{g,h \in G} (a_g b_h)(gh)$$

Esempi. 1. Sia K un campo e L/K un'estensione finita e di Galois; sia $G = \mathrm{Gal}(L/K)$. Allora L é un $K[G]$-modulo con l'azione:

$$\left(\sum_{g \in G} \lambda_g g \right)(\alpha) = \sum_{g \in G} \lambda_g g(\alpha).$$

2. L, K campi di numeri, L/K di Galois, $G = \mathrm{Gal}(L/K)$. Allora $\mathscr{O}_L$ é un $\mathscr{O}_K[G]$-modulo per restrizione dell'azione precedente.

Enunciamo il seguente risultato di teoria di Galois senza dimostrazione:

Teorema 6.3.1 (della base normale)**.** *L/K estensione finita di Galois, $G = \mathrm{Gal}(L/K)$. Allora esiste $\alpha \in L$ tale che $\{\sigma(\alpha)\}_{\sigma \in G}$ é una base di L/K.*
Una tale base si dice ***base normale****.*

Corollario 6.3.2. *L é un $K[G]$-modulo di rango 1. In particolare:*

$$L = K[G]\alpha = \left\{ \sum_{\sigma\in G} \lambda_\sigma \sigma(\alpha) \middle| \lambda_\sigma \in K \right\} = \langle \{\sigma(\alpha)_{\sigma\in G}\rangle_K$$

Ci poniamo ora il problema della struttura di $\mathscr{O}_L$ come $\mathscr{O}_K[G]$-modulo. Come prima cosa, $\mathscr{O}_L$ é $\mathscr{O}_K[G]$-libero? (in caso affermativo, avremmo che il rango sarebbe 1 in quanto sono due K-spazi di dimensione n).
In generale peró non é vero, in quanto se si avesse sempre che $\mathscr{O}_L = \mathscr{O}_K[G]\alpha$ per un certo $\alpha \in \mathscr{O}_L$, allora $\{\sigma(\alpha)\}_{\sigma\in G}$ sarebbe una base intera di $\mathscr{O}_L$ su $\mathscr{O}_K$, che in generale non esiste.

Consideriamo peró il caso di $K/\mathbb{Q}$ estensione finita di Galois con gruppo di Galois G; é vero in questo caso che $\mathscr{O}_K = \mathbb{Z}[G]\alpha$?
Anche in questo caso la risposta é negativa, anche se l'inclusione (ovvia) $\supseteq$ é sempre vera.

Esempio. Vediamo un caso in cui $\mathscr{O}_K \supsetneq \mathbb{Z}[G]\alpha$: sia $K = \mathbb{Q}(i)$ e dunque $\mathscr{O}_K = \mathbb{Z}[i]$.
Sia $\alpha \in \mathbb{Z}[i]$. Allora $\alpha = a + bi$, con $a, b \in \mathbb{Z}$.
Gli elementi in $\mathbb{Z}[G]\alpha$ sono del tipo $c\alpha + d\overline{\alpha} = c(a+ib) + d(a-ib) = a(c+d) + ib(c-d)$, con $c, d \in \mathbb{Z}$.
Con una tale combinazione lineare riesco ad ottenere $1 \iff$:

$$\begin{cases} b(c-d) = 0 \\ a(c+d) = 1 \end{cases} \iff \begin{cases} b = 0 \\ a = 1 \\ c+d = 1 \end{cases} \vee \begin{cases} c = d \\ 2ac = 1 \end{cases} \iff b = 0,$$

in quanto il secondo sistema é impossibile ($2 \nmid 1$).
Analogamente si ottiene $i \iff a = 0$, dunque si conclude che un tale α non puó esistere.

Definizione 6.3.2. Siano L, K campi di numeri. Se esiste $\alpha \in \mathscr{O}_L$ tale che $\mathscr{O}_L = \mathscr{O}_K[G]\alpha$, si dice che $\mathscr{O}_L$ (oppure L) ha una **base normale intera** (**NIB**) su K. In tal caso $\{\sigma(\alpha)\}$ é una K-base di L e α si dice **generatore** della base intera.

Definizione 6.3.3. L/K estensione di campi di numeri, $P \subseteq \mathscr{O}_K$ primo. $Q|P$ si dice **tame** su P se, detto $p = P \cap \mathbb{Z}$, $p \nmid e(Q|P)$; P si dice **tame** in L se $p \nmid e(Q|P)\ \forall Q|P$; L/K si dice **tame** se $\forall P \subseteq \mathscr{O}_K$ primo, P é tame in L.

Teorema 6.3.3 (Noether)**.** *Sia L/K di Galois con gruppo di Galois G. Allora sono equivalenti:*

1. *L/K ha solo ramificazione tame.*
2. *$\mathrm{Tr}_{L/K}(\mathscr{O}_L) = \mathscr{O}_K$.*
3. *$\mathscr{O}_L$ é $\mathscr{O}_K[G]$-proiettivo.*

Dimostrazione. Vedremo solo l'equivalenza (1) $\iff$ (2); ricordiamo inoltre che $\mathrm{Tr}_{L/K}(\mathscr{O}_L) = \mathrm{lcm}\left\{ I \subseteq \mathscr{O}_K \middle| I\mathscr{O}_L | \mathfrak{D}_{L/K} \right\}$ e, se L/K é di Galois, $\mathfrak{D}_{L/K}$ é invariante per azione di elementi del gruppo di Galois $(\sigma(\mathfrak{D}_{L/K})) = \mathfrak{D}_{L/K}\ \forall \sigma \in \mathrm{Gal}(L/K)$.

$\Rightarrow$) Basta vedere che $\forall P \subseteq \mathscr{O}_K$, $\mathrm{Tr}_{L/K}(\mathscr{O}_L) \not\subseteq P$.
Se per assurdo si avesse che $\mathrm{Tr}_{L/K}(\mathscr{O}_L) \subseteq P$, allora $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e | \mathfrak{D}_{L/K}$ e dunque $Q_i^e | \mathfrak{D}_{L/K}$, assurdo, in quanto la ramificazione é tame.

$\Leftarrow$) Sia per assurdo $P \subseteq \mathscr{O}_K$ tale che $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e$ e $\exists i$ per cui $Q_i^e | \mathfrak{D}_{L/K}$ (cioé la ramificazione é wild).
Visto che $\sigma(\mathfrak{D}_{L/K}) = \mathfrak{D}_{L/K}$ e G agisce transitivamente sull'insieme $\{Q_i\}_i$, si ha che $Q_j^e | \mathfrak{D}_{L/K}\ \forall j$, cioé $P\mathscr{O}_L | \mathfrak{D}_{L/K}$, e dunque $\mathrm{Tr}_{L/K}(\mathscr{O}_L) \subseteq P$.

□

Proposizione 6.3.4. *Se L/K ha una NIB, allora L/K é tame.*

Dimostrazione. Voglio vedere che la traccia é surgettiva (e avrei la tesi per il teorema precedente).
Sia α tale che $\mathscr{O}_L = \mathscr{O}_K[G]\alpha$; l'elemento (intero) $x = \sum_{g\in G} a_g g(\alpha)$ sta in K (e dunque in $\mathscr{O}_K$) $\iff \tau(x) = x\ \forall \tau \in G$. Ora:

$$\tau(x) = \sum_{g\in G} a_h(\tau\circ g)(\alpha) = \sum_{g\in G} a_{\tau^{-1}g} g(\alpha) = x \iff a_{\tau^{-1}g} = a_g\ \forall g,$$

in quanto $\{g(\alpha)\}_{g\in G}$ é base di L.
Dunque $x \in \mathscr{O}_K \iff a_{\tau^{-1}g} = a_g = a\ \forall g \in G \iff x = a\sum_{g\in G} g(\alpha) \iff x \in \mathrm{Tr}_{L/K}(\mathscr{O}_L)$. □

<u>*Osservazione*</u>. Il viceversa della precedente proposizione é falso, in quanto si puó trovare un'estensione $K/\mathbb{Q}$ con $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$ tale che $\mathscr{O}_K$ é uno $\mathbb{Z}[Q_8]$-modulo proiettivo ma non libero.

Proposizione 6.3.5. *$L/\mathbb{Q}$ estensione di Galois con una NIB generata da $\alpha \in L$. Allora $\forall K$ estensione intermedia tale che $K/\mathbb{Q}$ é di Galois, $K/\mathbb{Q}$ ha una NIB generata da $\beta = \mathrm{Tr}_{L/K}(\alpha)$.*

Dimostrazione. Sia $G = \mathrm{Gal}(L/\mathbb{Q})$ e $H \triangleleft G$ tale che $K = L^H$. Per ipotesi $\mathscr{O}_L = \mathbb{Z}[G]\alpha$.
Sia $x = \sum_{g\in G} a_g g(\alpha) \in \mathscr{O}_L$; ragionando come prima, si ha che $x \in \mathscr{O}_K \iff a_{h^{-1}g} = a_g\ \forall h \in H$, cioé $\iff$ gli a_g sono costanti sulle classi laterali sinistre di H (cioé $\{H, Hg_1, \ldots, Hg_d\}$).
Si ha dunque:

$$x = \sum_{g\in G} a_g g(\alpha) = \sum_{i=1}^{d}\sum_{h\in H} a_{hg_i}(h\circ g_i)(\alpha) = \sum_{i=1}^{d} a_{g_i}\sum_{h\in H}(h\circ g_i)(\alpha) = \sum_i a_{g_i}\sum_h g_i(g_i^{-1}hg_i)(\alpha) =$$
$$= \sum_{i=1}^{d} a_{g_i}\sum_{h\in H} g_i\circ h(\alpha) = \sum_{i=1}^{d} a_{g_i} g_i\big(\mathrm{Tr}_{L/K}(\alpha)\big) = \sum_{\sigma\in G/H} a_\sigma\sigma(\beta),$$

cioé la tesi. □

Proposizione 6.3.6. *Siano $K_i/\mathbb{Q}$ estensioni finite di Galois con NIB generate da $\alpha_i\ \forall i = 1,\ldots,m$ tali che $\big(\mathrm{disc}(K_i), \mathrm{disc}(K_j)\big) = 1\ \forall i \neq j$.*
Allora $L = K_1\cdot\ldots\cdot K_m$ ha una NIB generata da $\prod \alpha_i$.

Dimostrazione. Sia $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$; $\big\{\sigma^{(i)}(\alpha_1)\big\}_{\sigma^{(i)}\in G_i}$ é una base intera di $K_i/\mathbb{Q}$, dunque $\big\{\sigma^{(1)}(\alpha_1)\cdot\sigma^{(2)}(\alpha_2)\cdot\ldots\cdot\sigma^{(m)}(\alpha_m)\big\}_{\sigma^{(1)}\in G_1,\ldots,\sigma^{(m)}\in G_m}$ é una base intera di $L/\mathbb{Q}$.
Visto che $G = \mathrm{Gal}(L/\mathbb{Q}) \cong G_1\times\ldots\times G_m$, si ha che $\{\sigma(\alpha_1\cdot\ldots\cdot\alpha_m)\}_{\sigma\in G}$ non é altro che la base di prima e questa é una NIB. □

Corollario 6.3.7. *$\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ha una NIB (generata da ζ_m) $\iff$ m é squarefree $\iff$ é tame.*

Dimostrazione. L'implicazione $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ha una NIB $\Rightarrow$ é tame é giá stata vista; inoltre, se m non é squarefree e $p^2|m$, allora p ha ramificazione wild in $\mathbb{Q}(\zeta_{p^2}) \subseteq \mathbb{Q}(\zeta_m)$, in quanto $p\mathbb{Z}[\zeta_{p^2}] = P^{\phi(p^2)}$ e $p|\phi(p^2)$. Ci rimane dunque da mostrare che m squarefree $\Rightarrow$ ζ_m genera una NIB per $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.
Sia $m = p_1\cdot\ldots\cdot p_r$; se p é primo, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ha una NIB data da $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^p\} = \{\sigma(\zeta_p)\}_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}$.
Inoltre $\mathrm{disc}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ é potenza di p e $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p_1})\cdot\ldots\cdot\mathbb{Q}(\zeta_{p_r})$, dunque siamo nelle ipotesi della proposizione precedente e quindi $\prod\zeta_{p_i}$ (che é una radice m-esima primitiva dell'unitá) genera una NIB per $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. □

Concludiamo con un importantissimo risultato, che migliora in un certo senso il teorema di Kronecker-Weber:

Teorema 6.3.8 (Hilbert-Speiser)**.** *$K/\mathbb{Q}$ estensione finita, abeliana e tame $\Rightarrow \exists m$ squarefree tale che $K \subseteq \mathbb{Q}(\zeta_m)$ (e tale m si dice **conduttore**).*

Corollario 6.3.9. *$K/\mathbb{Q}$ estensione finita e abeliana ha una NIB $\iff$ é tame.*

Dimostrazione. La freccia $\Rightarrow$ é giá stata vista; l'altra segue dal precedente teorema, in quanto se $K \subseteq \mathbb{Q}(\zeta_m)$ con m squarefree, K ha una NIB perché é una sottoestensione normale di un'estensione $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ di Galois con una NIB. □

Vale infine il seguente risultato, che é una specie di viceversa del teorema di Hilbert-Speiser:

Teorema 6.3.10 (Greither, Replogle, Rubin)**.** *Ogni estensione finita, abeliana e tame L di un fissato campo di numeri K ha una NIB $\iff$ $K = \mathbb{Q}$.*

6.4 Un'introduzione ai gruppi di ramificazione

In questa piccola sezione ci occuperemo dei cosiddetti gruppi di ramificazione; ci serviranno per mostrare alcuni fatti sui gruppi di decomposizione e di inerzia, necessari per la prossima sezione. Questa non é altro che la risoluzione degli esercizi 19-28, pag. 121-125 del libro di Marcus.

Nel seguito sia L/K un'estensione di Galois con gruppo di Galois G, P un primo di K e Q un primo di L sopra P; denotiamo inoltre $E = E(Q|P)$ e $D = D(Q|P)$.

Definizione 6.4.1. Sia $m \geq 0$ un intero. Definiamo **m-esimo gruppo di ramificazione** il gruppo:

$$V_m = \{\sigma \in G | \sigma(\alpha) \equiv \alpha \quad (Q^{m+1}) \ \forall \alpha \in \mathscr{O}_L\}.$$

<u>*Osservazioni.*</u>

- $E = V_0 \supseteq V_1 \supseteq \ldots$.
- $V_m \triangleleft D \ \forall m$, poiché, se $\tau \in D$ e $\sigma \in V_m$:

$$\tau\sigma(\tau^{-1}(\alpha)) \equiv \tau(\tau^{-1}(\alpha)) = \alpha \quad (Q^{m+1}).$$

- Per tutti gli m abbastanza grandi, diciamo per $m > \overline{m}$ con $\overline{m}$ sufficientemente grande, si ha che $V_m = \{1\}$; infatti, se $(\sigma(\alpha) - \alpha) = Q^{m_0} I$, $(I, Q) = 1$, $\alpha \notin V_m$ se $m > m_0$, e ripetendo il discorso per gli altri elementi di G (che sono in numero finito), si ha la tesi.

Lemma 6.4.1. *Sia $\pi \in Q \backslash Q^2$ e $\sigma \in V_{m-1}$. Allora:*

$$\sigma \in V_m \iff \sigma(\pi) \equiv \pi \quad (Q^{m+1}).$$

Dimostrazione. La freccia $\Rightarrow$ é del tutto ovvia; vediamo l'altra.
Se $\alpha \in (\pi)$, si ha che $\sigma(\alpha) \equiv \alpha \quad (Q^{m+1})$, in quanto, posto $\alpha = \pi\beta$:

$$\sigma(\alpha) - \alpha = \sigma(\beta)\sigma(\pi) - \beta\pi \equiv \underbrace{\pi}_{\in Q}(\underbrace{\sigma(\beta) - \beta}_{\in Q^m}) \equiv 0 \quad (Q^{m+1}).$$

Ma allora sia $\alpha \in Q$; se $(\pi) = QI$, $(Q, I) = 1$, scelgo $\beta \in (I \backslash Q) \cap \mathscr{O}_K$ e dunque, visto che $\alpha\beta \in (\pi)$:

$$\beta\alpha \equiv \sigma(\alpha\beta) = \beta\sigma(\alpha) \quad (Q^{m+1}) \Rightarrow \sigma(\alpha) \equiv \alpha \quad (Q^{m+1}),$$

in quanto $\beta \notin Q$ é invertibile in $\frac{\mathscr{O}_L}{Q}$.
Infine, osservando che $\mathscr{O}_L = \mathscr{O}_{L^E} + Q$, in quanto, se $\gamma \in Q \cap \mathscr{O}_{L^E}$, $1 = 1 + \gamma - \gamma$ e $\sigma(1 - \gamma) = 1 - \gamma$ $\forall \sigma \in E$, si giunge alla tesi scomponendo un qualsiasi $\alpha \in \mathscr{O}_L$ in $\alpha = \alpha_1 + \alpha_2$ con $\alpha_1 \in \mathscr{O}_{L^E}$ e $\alpha_2 \in Q$. □

Proposizione 6.4.2. *Sia $\pi \in Q \backslash Q^2$ e $\sigma \in E$. Allora:*

$$\sigma \in V_m \iff \sigma(\pi) \equiv \pi \quad (Q^{m+1}).$$

Dimostrazione. Come prima osservazione, vediamo che, preso $\sigma \in V_i \backslash V_{i+1}$, la congruenza $\sigma(\pi) \equiv \pi \quad (Q^{m+1})$ vale $\iff$ $m \leq i$. Infatti, se per assurdo $\sigma(\pi) - \pi \in Q^{i+2}$, essendo $\sigma \in V_i$, per il lemma si avrebbe $\sigma \in V_{i+1}$, assurdo.
Sia dunque $\sigma \in E = V_0$. Se per assurdo $\sigma \in V_i \backslash V_{i+1}$ con $i < m$, allora per l'ipotesi $\sigma(\pi) \equiv \pi \quad (Q^{m+1})$ e per quanto visto, si avrebbe $m \leq i$, assurdo. □

Lemma 6.4.3. *Sia $\pi \in Q \backslash Q^2$ e $\sigma \in E$. Allora esiste $\alpha \in \mathscr{O}_L$ tale che $\sigma(\pi) \equiv \alpha\pi \quad (Q^2)$ e tale α é unico modulo Q.*

Dimostrazione. Scriviamo $(\pi) = QI$ con $(I, Q) = 1$; allora per il teorema cinese del resto il sistema

$$\begin{cases} x \equiv \sigma(\pi) & (Q^2) \\ x \equiv 0 & (I) \end{cases}$$

ha soluzione, e $x \equiv \sigma(\pi) \equiv \pi \equiv 0 \quad (Q)$, cioé $x \in Q$.
$x \in I = (\pi)Q^{-1}$, dunque $\exists \alpha \in Q^{-1}$ tale che $x = \pi\alpha$; ma se $\alpha \notin \mathscr{O}_L$, allora $x \notin Q$, assurdo, dunque $x = \pi\alpha \equiv \sigma(\pi) \quad (Q^2)$.
Inoltre, se $\alpha_1\pi \equiv \alpha_2\pi \quad (Q^2)$, allora $\pi(\alpha_1 - \alpha_2) \in Q^2$, cioé $\alpha_1 \equiv \alpha_2 \quad (Q)$. □

Teorema 6.4.4. *Il gruppo quoziente $\frac{E}{V_1}$ si immerge nel gruppo moltiplicativo $\frac{\mathscr{O}_L}{Q}^*$; dunque $\frac{E}{V_1}$ é ciclico di ordine divisore di $\left|\frac{\mathscr{O}_L}{Q}\right| - 1$.*

Dimostrazione. Sia:

$$\begin{array}{rccc} \psi: & E & \longrightarrow & \frac{\mathscr{O}_L}{Q}^* \\ & \sigma & \longrightarrow & \alpha_\sigma \end{array}$$

dove α_σ é l'α trovato nel lemma.
ψ é un omomorfismo, in quanto:

$$\sigma(\tau(\pi)) \equiv \sigma(\alpha_\tau\pi) \equiv \sigma(\alpha_\tau)\sigma(\pi) \equiv \alpha_\sigma\alpha_\tau\pi \quad (Q^2),$$

(poiché $\sigma(\alpha_\tau)\sigma(\pi) - \alpha_\tau\sigma(\pi) = \underbrace{\sigma(\pi)}_{\in Q}\underbrace{(\sigma(\alpha_\tau) - \alpha_\tau)}_{\in Q} \in Q^2$) e dunque per l'unicitá, $\alpha_{\sigma\tau} \equiv \alpha_\sigma\alpha_\tau \quad (Q)$.
Inoltre ψ é ben definito, poiché $\alpha_\sigma \notin Q$, in quanto se ci stesse si avrebbe $\sigma(\pi) \in Q^2$; infine $\mathrm{Ker}\,(\psi) = V_1$ per la proposizione precedente, dunque la mappa si quozienta all'immersione voluta. □

Lemma 6.4.5. *Sia $\pi \in Q\backslash Q^2$ e $\sigma \in V_{m-1}$, $m \geq 2$. Allora $\exists \alpha \in \mathscr{O}_L$ tale che $\sigma(\pi) \equiv \pi + \alpha\pi^m \quad (Q^{m+1})$ e tale α é unico modulo Q.*

Dimostrazione. La dimostrazione ricalca quella del precedente lemma. □

Teorema 6.4.6. *Sia $m \geq 2$. Allora il quoziente $\frac{V_{m-1}}{V_m}$ si immerge nel gruppo additivo $\frac{\mathscr{O}_L}{Q}$; dunque $\frac{V_{m-1}}{V_m}$ é somma diretta di gruppi ciclici di ordine p (in quanto il campo $\frac{\mathscr{O}_L}{Q}$ ha caratteristica p).*

Dimostrazione. Sia:

$$\begin{array}{rccc} \psi: & V_{m-1} & \longrightarrow & \frac{\mathscr{O}_L}{Q} \\ & \sigma & \longrightarrow & \alpha_\sigma \end{array}$$

dove α_σ é l'α trovato nel lemma.
In modo analogo a prima si vede che $\alpha_{\sigma\tau} \equiv \alpha_\sigma + \alpha_\tau \quad (Q)$, e $\mathrm{Ker}\,(\psi) = V_m$; segue dunque la tesi. □

<u>*Osservazione*</u>. Abbiamo visto che $\left|\frac{E}{V_1}\right|\left|\frac{\mathscr{O}_L}{Q}\right| - 1$, dunque $\left|\frac{E}{V_1}\right|$ é coprimo con $p = P \cap \mathbb{Z}$ (infatti $\left|\frac{\mathscr{O}_L}{Q}\right| = p^f$); segue dunque che V_1 é il p-Sylow di E.
Da questa osservazione segue:

Corollario 6.4.7. *$V_1 \neq \{1\} \iff p|e(Q|P) = |E| \iff Q$ é wild su P.*

Teorema 6.4.8. *D ed E sono gruppi risolubili.*

Dimostrazione. La catena discendente:

$$E \triangleright V_1 \triangleright V_2 \triangleright \ldots \triangleright \{1\}$$

é tale che $\frac{V_{m-1}}{v_m}$ é somma diretta di gruppi ciclici e cioé abeliano, dunque E é risolubile.
Ricordando che $E \triangleleft D$ e $\frac{D}{E}$ é ciclico di ordine f, si ha la tesi. □

Lemma 6.4.9. *Sia $\pi \in Q\backslash Q^2$, $\sigma \in V_{m-1}$ tale che $\sigma(\pi) \equiv \alpha\pi \quad (Q^{m+1})$ per un certo α. Allora $\sigma(\beta) \equiv \alpha\beta \quad (Q^{m+1})\ \forall \beta \in Q$.*

Dimostrazione. Si procede come nel primo lemma, mostrando prima la tesi per $\beta \in (\pi)$. □

Teorema 6.4.10. *Supponiamo $\frac{D}{V_1}$ abeliano. Allora l'immersione di $\frac{E}{V_1}$ in ${\frac{\mathscr{O}_L}{Q}}^*$ in realtá ha immagine contenuta in ${\frac{\mathscr{O}_K}{P}}^*$; dunque $\frac{E}{V_1}$ é ciclico di ordine divisore di $\mathrm{N}(P) - 1$.*

Dimostrazione. Sia $\sigma \in E$ e α tale che $\sigma(\pi) \equiv \alpha\pi \quad (Q^2)$; allora, posto $\phi = \phi(Q|P)$ il Frobenius di $Q|P$, per il lemma si ha:

$$\phi\sigma\phi^{-1}(\pi) = \phi\sigma(\phi^{-1}(\pi)) \equiv \phi(\alpha\phi^{-1}(\pi)) \equiv \alpha^{\mathrm{N}(P)}\pi \quad (Q^2).$$

Visto che $\frac{D}{V_1}$ é abeliano, allora $\phi\sigma\phi^{-1}\sigma^{-1} \in V_1$, dunque:

$$\phi\sigma\phi^{-1}(\pi) = \phi\sigma\phi^{-1}\sigma^{-1}(\sigma(\pi)) \equiv \sigma(\pi) \equiv \alpha\pi \quad (Q^2),$$

ma allora per unicitá di α, $\alpha^{\mathrm{N}(P)} \equiv \alpha \quad (Q)$.
Ma allora α é fissato dal Frobenius di $Q|P$, cioé é fissato da $\mathrm{Gal}\big(\frac{\mathscr{O}_L}{Q}/\frac{\mathscr{O}_K}{P}\big)$, cioé $\alpha \in {\frac{\mathscr{O}_K}{P}}^*$. □

Lemma 6.4.11. *Sia L/K un'estensione finita e separabile e sia $\alpha \in \mathscr{O}_L$ tale che $L = K(\alpha)$ e sia f il polinomio minimo di α su K; scriviamo $f(x) = (x-\alpha)g(x)$, con $g(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{n-1}x^{n-1}$ per certi $\gamma_0, \ldots, \gamma_{n-1} \in L$. Allora:*

$$\left\{ \frac{\gamma_0}{f'(\alpha)}, \ldots, \frac{\gamma_{n-1}}{f'(\alpha)} \right\}$$

é la base duale di $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Dimostrazione. Detti $\sigma_1, \ldots, \sigma_n$ le immersioni di L/K, osserviamo che $\sigma_i(f) = f$ e dunque, posto $\alpha_i = \sigma_i(\alpha)$ e $g_i = \sigma_i(g)$, si ha che $f(x) = (x-\alpha_i)g_i(x)\ \forall i$.
Notiamo inoltre che $g_i(\alpha_j) = f'(\alpha_j)\delta_{ij}$, in quanto, se $i \neq j$, $0 = f(\alpha_j) = (\alpha_j - \alpha_i)g_i(\alpha_j)$, mentre $f'(\alpha_i) = g(\alpha_i) + (\alpha_i - \alpha_i)(g_i'(\alpha_i))$.
Poniamo dunque:

$$M = \begin{pmatrix} 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix} \qquad N = \begin{pmatrix} \sigma_1\left(\frac{\gamma_0}{f'(\alpha)}\right) & \ldots & \sigma_1\left(\frac{\gamma_{n-1}}{f'(\alpha)}\right) \\ \vdots & \ddots & \vdots \\ \sigma_n\left(\frac{\gamma_0}{f'(\alpha)}\right) & \ldots & \sigma_n\left(\frac{\gamma_{n-1}}{f'(\alpha)}\right) \end{pmatrix}$$

Con un calcolo diretto si vede che $NM = \left(\frac{g_i(\alpha_j)}{f'(\alpha_i)}\right) = (\delta_{ij}) = I$, ma M é invertibile, dunque $M = N^{-1}$. Segue quindi che $\left\{\frac{\gamma_0}{f'(\alpha)}, \ldots, \frac{\gamma_{n-1}}{f'(\alpha)}\right\}$ é effettivamente la base duale di $\{1, \alpha, \ldots, \alpha^{n-1}\}$. □

Proposizione 6.4.12. *Mettiamoci nelle condizioni del lemma. Allora $\mathfrak{D}_{L/K}(\mathscr{O}_K[\alpha]) = f'(\alpha)\mathscr{O}_L$.*

Dimostrazione. Come prima cosa vediamo che $\mathscr{O}_K[\alpha] = \langle \gamma_0, \ldots, \gamma_{n-1} \rangle_{\mathscr{O}_K}$:

$\subseteq$): $\gamma_{n-1} = 1$ perché f é monico, dunque $\mathscr{O}_K \subseteq \langle \gamma_0, \ldots, \gamma_{n-1} \rangle_{\mathscr{O}_K}$; svolgendo il calcolo si ha che:

$$f(x) = -\alpha\gamma_0 + (\gamma_0 - \alpha\gamma_1)x + \ldots + (\gamma_{n-2} - \alpha\gamma_{n-1})x^{n-1} + \gamma_{n-1}x^n.$$

Abbiamo dunque che $f(\gamma_0) = -\alpha\gamma_0 + (\gamma_0 - \alpha\gamma_1)\gamma_0 + \ldots + (\gamma_{n-2} - \alpha\gamma_{n-1})\gamma_0^{n-1} + \gamma_{n-1}\gamma_0^n$, dunque $\alpha \in \langle \gamma_0, \ldots, \gamma_{n-1} \rangle_{\mathscr{O}_K}$, poiché $\frac{f(\gamma_0)}{\gamma_0}$ e i monomi divisi per γ_0 stanno in $\langle \gamma_0, \ldots, \gamma_{n-1} \rangle_{\mathscr{O}_K}$.

$\supseteq$): $0 = f(\alpha) = -\alpha\gamma_0 + (\gamma_0 - \alpha\gamma_1)\alpha + \ldots + (\gamma_{n-2} - \alpha\gamma_{n-1})\alpha^{n-1} + \gamma_{n-1}\alpha^n$, dunque per lo stesso ragionamento precedente $\gamma_0 \in \mathscr{O}_K[\alpha]$; eliminando i termini $-\alpha\gamma_0 + \alpha\gamma_0$ e ragionando analogamente si ha che $\gamma_1 \in \mathscr{O}_K[\alpha]$ e cosí via.

A questo punto, essendo $\left\{\frac{\gamma_0}{f'(\alpha)}, \ldots, \frac{\gamma_{n-1}}{f'(\alpha)}\right\}$ una base di $(\mathscr{O}_K[\alpha])^*$, si ha che $(\mathscr{O}_K[\alpha])^* = (f'(\alpha))^{-1}\mathscr{O}_K[\alpha]$, da cui:

$$\mathfrak{D}_{L/K}(\mathscr{O}_K[\alpha]) = f'(\alpha)(\mathscr{O}_K[\alpha])^{-1} = f'(\alpha)\mathscr{O}_L,$$

in quanto $1 \in \mathscr{O}_K[\alpha]$. □

Lemma 6.4.13. *Sia P un primo di K e sia $Q \subseteq \mathscr{O}_L$ sopra P. Detto $n = [L : K]$, siano $\alpha_1, \ldots, \alpha_n \in \mathscr{O}_L$ indipendenti modulo P (e dunque sono una K-base di L); posto $A = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathscr{O}_K}$, allora la potenza esatta di Q che divide $\mathfrak{D}_{L/K}$ é la stessa che divide $\mathfrak{D}_{L/K}(A)$.*

Dimostrazione. Osserviamo che $P\mathscr{O}_L \cap A = PA$; infatti l'inclusione $\supseteq$ é banale, mentre se $x_1\alpha_1 + \ldots + x_n\alpha_n \in P\mathscr{O}_L$, allora $\overline{x_1\alpha_1} + \ldots + \overline{x_n\alpha_n} = 0 \quad (P)$ e dunque $\overline{x_1} = \ldots = \overline{x_n} = 0 \quad (P)$ per l'indipendenza modulo P di $\alpha_1, \ldots, \alpha_n$.
Poniamo $I = \mathrm{Ann}_{\mathscr{O}_K}\left(\frac{\mathscr{O}_L}{A}\right) = \{r \in \mathscr{O}_K | r\mathscr{O}_L \subseteq A\}$; allora $I \not\subseteq P$, poiché se $I \subseteq P$, allora si avrebbe $I\mathscr{O}_L \subseteq P\mathscr{O}_L$, ma $I\mathscr{O}_L \subseteq A$, dunque $I\mathscr{O}_L \subseteq PA$ e di conseguenza $P^{-1}I \subseteq A \cap \mathscr{O}_K \subseteq I$, cioé $P^{-1} \subseteq \mathscr{O}_K$, assurdo.
Notando che $\mathfrak{D}_{L/K} | \mathfrak{D}_{L/K}(A) | I\mathscr{O}_L\mathfrak{D}_{L/K}$ (in quanto $A | I\mathscr{O}_L$) e che $Q \nmid I\mathscr{O}_L$ (poiché $P \nmid I$), si ottiene che $Q^k | \mathfrak{D}_{L/K} \iff Q^k | \mathfrak{D}_{L/K}(A)$. □

Proposizione 6.4.14. *Nelle condizioni del lemma, supponiamo che $e(Q|P) = n$. Allora, preso $\pi \in Q \backslash Q^2$, la potenza esatta di Q che divide $\mathfrak{D}_{L/K}$ é la stessa che divide $f'(\pi)\mathscr{O}_L$, dove f é il polinomio minimo di π su K.*

Dimostrazione. Abbiamo che $1, \pi, \ldots, \pi^{n-1}$ sono indipendenti modulo P, poiché $\pi \notin Q^2 \subseteq P$ e $\pi^i \in P \iff \pi^i \in Q^n \iff i \geq n$.
Ma allora per il lemma si ha che la potenza esatta di Q che divide $\mathfrak{D}_{L/K}$ é la stessa che divide $\mathfrak{D}_{L/K}(\mathscr{O}_K[\pi])$.
A questo punto basta ricordare che $\mathfrak{D}_{L/K}(\mathscr{O}_K[\pi]) = f'(\pi)\mathscr{O}_L$. □

Ritorniamo adesso a considerare un'estensione L/K di Galois con le stesse notazioni usate precedentemente; vale allora la **formula di Hilbert**:

Teorema 6.4.15. *Sia Q^k l'esatta potenza di Q che divide $\mathfrak{D}_{L/K}$; allora:*

$$k = \sum_{m \geq 0} (|V_m| - 1).$$

Dimostrazione. Notiamo innanzitutto che possiamo supporre Q totalmente ramificato su P; in caso contrario infatti possiamo considerare il campo d'inerzia L^E e usare la relazione $\mathfrak{D}_{L/K} = \mathfrak{D}_{L/L^E}\mathfrak{D}_{L^E/K}$, in quanto P non é ramificato in L^E e dunque $Q \nmid \mathfrak{D}_{L^E/K}\mathscr{O}_L$.
Per quanto visto nelle proposizioni precedenti, Q^k é la potenza esatta di Q che divide $f'(\pi)$, dove $\pi \in Q\backslash Q^2$ e f é il suo polinomio minimo su K; sia $\sigma \in V_{m-1}\backslash V_m$.
Sappiamo che $Q^m \| (\sigma(\pi) - \pi)$, poiché se $Q^{m+1} | (\sigma(\pi) - \pi)$, si avrebbe che $\sigma \in V_m$; ma:

$$f = \prod_{\sigma \in E} (x - \sigma(\pi)) \quad \Rightarrow \quad f'(\pi) = \sum_{i=1}^{n} \prod_{\sigma \neq \sigma_i} (\pi - \sigma(\pi)) = \prod_{\sigma \in E \backslash \{1\}} (\pi - \sigma(\pi)),$$

dunque la potenza esatta di Q che divide $f'(\pi)$ é:

$$k = \sum_{m \geq 1} m|V_{m-1}\backslash V_m|.$$

A questo punto, detto r il minimo m per cui $V_m = \{1\}$, si ha:

$$k = \sum_{m\geq 1} m|V_{m-1}\backslash V_m| = \sum_{m=0}^{r-1} |V_m| - r|V_r| = \sum_{m=0}^{r-1} (|V_m| - 1).$$

□

Osservazione. Riotteniamo dunque che $Q^{e-1}|\mathfrak{D}_{L/K}$ e $Q^e|\mathfrak{D}_{L/K} \iff V_1 \neq \{1\} \iff p|e$.

6.5 Una dimostrazione del teorema di Kronecker-Weber

Quest'ultima sezione raccoglie gli esercizi $29 - 36$ di pag. $125 - 129$ del libro di Marcus per dimostrare il famoso:

Teorema 6.5.1 (Kronecker-Weber)**.** *Ogni estensione abeliana di $\mathbb{Q}$ é contenuta in un'estensione ciclotomica.*

Cominciamo con alcuni semplici richiami.

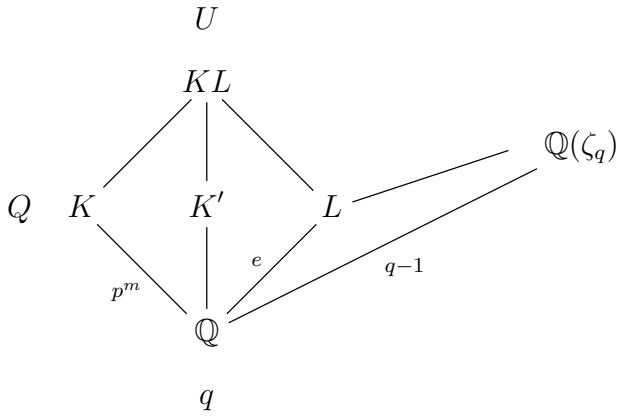
Osservazione. Siano K, L estensioni abeliane di $\mathbb{Q}$; allora anche KL é abeliana e si ha un'immersione:

$$\begin{array}{ccc} \mathrm{Gal}(KL/\mathbb{Q}) & \hookrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \\ \sigma & \longrightarrow & (\sigma_{|K}, \sigma_{|L}) \end{array}$$

Dunque ogni estensione abeliana é il composto di estensioni abeliane di grado potenza di un primo.

Proposizione 6.5.2. *Sia $K/\mathbb{Q}$ un'estensione abeliana di grado p^m. Allora esiste un'estensione $K'/\mathbb{Q}$ di grado potenza di p in cui p é l'unico primo ramificato e, se K' é contenuta in un'estensione ciclotomica, allora lo é anche K.*

Dimostrazione. Sia $q \neq p$ un primo di $\mathbb{Z}$ ramificato in K e sia $Q|q$ primo di K; poniamo $e = e(Q|q)$.
Allora $V_1(Q|q) = \{1\}$, in quanto $q \nmid e$ che é potenza di p.
Per una proposizione nella precedente sezione, si ha che $e|\,\mathrm{N}(q) - 1 = q - 1$; dunque esiste un'unica sottoestensione L di $\mathbb{Q}(\zeta_q)$ di grado e su $\mathbb{Q}$. Evidentemente q ramifica totalmente in L, in quanto lo fa in $\mathbb{Q}(\zeta_q)$.
Sia U un primo di KL sopra Q, e sia $K' = (KL)^{E(U|q)}$; abbiamo il diagramma:



Sicuramente q non é ramificato in K'; ma se $p' \neq q$ non é ramificato in K, allora non é ramificato in KL in quanto non é ramificato in L e a maggior ragione non é ramificato in K'; segue che p é l'unico primo ramificato in K'.
Consideriamo l'immersione $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ e osserviamo che la sua restrizione a $E(U|q)$ dá un'immersione

$$E(U|q) \hookrightarrow E(Q|q) \times \mathrm{Gal}(L/\mathbb{Q})$$

in quanto se $\sigma(\alpha) \equiv \alpha \pmod{U}\ \forall \alpha \in \mathscr{O}_{KL}$, allora $\sigma_{|K}(\alpha) \equiv \alpha \pmod{U \cap K}\ \forall \alpha \in \mathscr{O}_K$.
Ma allora $e|e(U|q)|e^2$, da cui $V_1(U|q) = \{1\}$ perché $e(U|q)$ é potenza di p; di conseguenza $E(U|q)$ é ciclico (poiché $\frac{E}{V_1}$ é ciclico) e quindi $E(U|q) \cong \mathbb{Z}/e\mathbb{Z}$ in quanto si immerge in $E(Q|q) \times \mathrm{Gal}(L/\mathbb{Q})$.
Visto che gli indici di ramificazione sono moltiplicativi nelle torri, si ha che U non é ramificato

su L, ma é totalmente ramificato sul campo d'inerzia K'; segue quindi che $KL = K'L$, poiché se $K'L \subsetneq KL$, U sarebbe contemporaneamente totalmente ramificato e non ramificato su $K'L$, assurdo.
Notiamo infine che $[K' : \mathbb{Q}] | ep^m$ é potenza di p e se $K' \subseteq \mathbb{Q}(\zeta_m)$, allora $K \subseteq KL = K'L \subseteq \mathbb{Q}(\zeta_{[m,q]})$. □

La precedente proposizione ci assicura che dobbiamo mostrare il teorema di Kronecker-Weber solo per le estensioni abeliane K di $\mathbb{Q}$ di grado p^m in cui p é l'unico primo ramificato.
Concentriamoci come primo caso su $p = 2$.

Osservazione. Se $[K : \mathbb{Q}] = 2$, allora K é una fra $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{-2})$ (tutte contenute ad esempio in $\mathbb{Q}(\zeta_8)$).
Infatti essendo 2 l'unico primo ramificato, $\mathrm{disc}(K)$ deve essere una potenza di 2; posto $K = \mathbb{Q}(\sqrt{m})$, $m \not\equiv 1 \quad (4)$ perché $\mathrm{disc}(K)$ sarebbe dispari, se $m \equiv 3 \quad (4)$ allora $\mathrm{disc}(K) = 4m$ deve essere potenza di 2 e quindi $m = -1$, se $m \equiv 2 \quad (4)$ allora $\mathrm{disc}(K) = 4m$ deve essere potenza di 2 e quindi $m = \pm 2$.

Proposizione 6.5.3. *Fissato $p = 2$ e $m > 1$, allora $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$.*

Dimostrazione. Sicuramente $\mathbb{Q}(\sqrt{2}) \subseteq K$, in quanto $K \cap \mathbb{R}$ ha un'estensione quadratica di $\mathbb{Q}$ reale che per quanto visto nell'osservazione deve essere $\mathbb{Q}(\sqrt{2})$.
Sia $L = \mathbb{Q}(\zeta_{2^{m+2}}) \cap \mathbb{R}$; $\mathrm{Gal}(L/\mathbb{Q}) \cong \frac{(\mathbb{Z}/2^{m+2}\mathbb{Z})^*}{\{\pm 1\}} \cong \mathbb{Z}/2^m\mathbb{Z}$ é ciclico; dunque sia $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ un generatore del gruppo.
σ si estende a $\tau \in \mathrm{Aut}(KL)$; poniamo $F = (KL)^{\langle \tau \rangle}$.
Evidentemente $F \cap L = \mathbb{Q}$, in quanto $F \cap L$ é il sottocampo di L fissato da $\tau_{|L} = \sigma$ che ha ordine $2^m = [L : \mathbb{Q}]$; di conseguenza $F \not\subseteq \mathbb{R}$, altrimenti conterrebbe $\mathbb{Q}(\sqrt{2})$ e $L \supseteq \mathbb{Q}(\sqrt{2})$.
Inoltre $[F : \mathbb{Q}] \leq 2$, poiché altrimenti allo stesso modo $F \cap \mathbb{R} \supsetneq \mathbb{Q}$ avrebbe intersezione non banale con L, dunque per l'osservazione precedente F é uno fra $\mathbb{Q}$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-2})$.
Si vede anche che $\mathrm{ord}(\tau) = 2^m$, in quanto $2^m = \mathrm{ord}(\sigma) | \mathrm{ord}(\tau)$, mentre l'immersione $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ mostra che $\mathrm{ord}(\tau) | 2^m$; da questo segue che $[KL : \mathbb{Q}] = 2^m$ oppure $[KL : \mathbb{Q}] = 2 \cdot 2^m = 2^{m+1}$.
Nel primo caso si ha che $KL = K = L \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$, mentre se $F = \mathbb{Q}(i)$ (se $F = \mathbb{Q}(\sqrt{-2})$ é analogo), si ha che $L(i) = KL$ e $L(i) = \mathbb{Q}(\zeta_{2^{m+2}})$, in quanto $[L(i) : L] = 2$ e $i \in \mathbb{Q}(\zeta_{2^{m+2}})$ e $i \in F \subseteq KL$, da cui $K \subseteq KL = \mathbb{Q}(\zeta_{2^{m+2}})$. □

Supponiamo ora $p > 2$ e $m = 1$. Sia P un primo di K sopra p. Allora P é ramificato su p, altrimenti non ci sarebbero primi ramificati nell'estensione, e dunque $e(P|p) = p$.
Allora:

Proposizione 6.5.4. $\mathfrak{D}_{K/\mathbb{Q}} = P^{2(p-1)}$.

Dimostrazione. Sia $\pi \in P \backslash P^2$ (e dunque $\pi \notin Q = P^p$); allora π ha grado p su $\mathbb{Q}$ e dunque sia $f(x) = x^p + a_1 x^{p-1} + \ldots + a_p$ il suo polinomio minimo.
Visto che $1, \pi, \ldots, \pi^{n-1}$ sono indipendenti modulo p, allora la combinazione lineare $\pi^p + a_1\pi^{p-1} + \ldots + a_p = 0$ mostra che $p | a_i \ \forall i$.
Sia P^k la potenza esatta di P che divide $f'(\pi)$; allora $p-1 | k$ per la formula di Hilbert, in quanto essendo $|E| = p - 1$, $|V_m| = 0$ o $p - 1 \ \forall m \geq 0$. Scriviamo inoltre $f'(\pi) = p\pi^{p-1} + \ldots + a_{p-1}$; la potenza esatta di P che divide $j a_{p-j} \pi^{j-1}$ é $P^{\delta(j)}$ con $\delta(j) \equiv j \quad (p)$, dunque gli esponenti delle potenze esatte di P che dividono i monomi di $f'(\pi)$ sono tutti diversi (perché diversi modulo p), da cui $k = \min_j \delta(j)$.
Ora $\delta(p) = 2p - 1$, dunque $k \leq 2p - 1$, ma $p - 1 | k$, dunque $k = 2(p - 1)$.
Osservando che P é l'unico primo ramificato su $\mathbb{Q}$, per quanto visto $\mathfrak{D}_{K/\mathbb{Q}} = P^{2(p-1)}$. □

Proposizione 6.5.5. *Supponiamo $p > 2$ e $m = 2$. Allora $G = \mathrm{Gal}(K/\mathbb{Q})$ é ciclico.*

Dimostrazione. Sia P un primo di K sopra p. Allora P é totalmente ramificato sopra p, poiché in caso contrario non ci sarebbe nessun primo ramificato nel campo d'inerzia K^E; ma allora $|E(P|p)| = p^2$ e $|V_1(P|p)| = p^2$, in quanto V_1 é il p-Sylow di E.
Inoltre, detto V_r il primo gruppo di ramificazione per cui $|V_r| < p^2$, si ha che $|V_r| = p$, in quanto $\frac{V_{r-1}}{V_r}$ é somma diretta di gruppi ciclici di ordine p.
Sia ora H un qualsiasi sottogruppo (normale) di G di ordine p, e sia K^H il campo fissato da H; si ha per la proposizione precedente:

$$\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{K/K^H}(\mathfrak{D}_{K^H/\mathbb{Q}}\mathscr{O}_K) = \mathfrak{D}_{K/K^H}(P_H^{2(p-1)}\mathscr{O}_K) = \mathfrak{D}_{K/K^H}P^{2(p-1)p},$$

con $P_H = P \cap K^H$, in quanto P é totalmente ramificato su p (e dunque su P_H).
Perció $\mathfrak{D}_{K/K^H}$ é indipendente da H, ma d'altra parte, la potenza massima di P che divide $\mathfrak{D}_{K/K^H}$ é $\sum_{m\geq 0}(|V_m(P|P_H) - 1) = \sum_{m\geq 0}(|V_m(P|p) \cap H| - 1)$, che é strettamente massimizzato se $H = V_r$ (altrimenti $|V_m(P|p) \cap H| < |V_m(P|p)|$).
Segue quindi che ci puó essere solo un sottogruppo di G di ordine p, cioé G é ciclico. □

Corollario 6.5.6. *Esiste un unico campo con $p > 2$ e $m = 1$; in particolare per l'unicitá é l'unico sottocampo di grado p su $\mathbb{Q}$ di $\mathbb{Q}(\zeta_{p^2})$.*

Dimostrazione. Supponiamo per assurdo che ne esistano due, diciamo K_1 e K_2. Allora $K_1 \cap K_2 = \mathbb{Q}$ (il grado dell'intersezione deve dividere p), dunque K_1K_2 ha grado p^2 su $\mathbb{Q}$ (se fosse p allora $K_1K_2 = K_1 = K_2$) e $\mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, assurdo per la proposizione precedente. □

Teorema 6.5.7. *Sia $p > 2$ e $m > 1$. Allora K é l'unica sottoestensione di grado p^m su $\mathbb{Q}$ di $L = \mathbb{Q}(\zeta_{p^{m+1}})$ (l'unicitá segue dal fatto che $\mathbb{Z}/p^{m+1}\mathbb{Z}$ é ciclico).*

Dimostrazione. Sia $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ un generatore del gruppo di Galois di $L/\mathbb{Q}$ e si estenda a $\tau \in \mathrm{Aut}(KL)$; sia inoltre $F = (KL)^{\langle\tau\rangle}$.
Con un ragionamento analogo a quello del teorema con $p = 2$, si vede che $\mathrm{ord}(\tau) = p^m$ e $F \cap L = \mathbb{Q}$; ma allora $F = \mathbb{Q}$, poiché altrimenti F e L conterrebbero un campo di grado p su $\mathbb{Q}$, che é unico, e quindi si avrebbe $F \cap L \supsetneq \mathbb{Q}$.
Abbiamo in conclusione che $[KL : \mathbb{Q}] = p^m$, cioé $KL = K = L$. □