Appunti del corso:
Teoria algebrica dei numeri
Prof. Ilaria Del Corso

Stefano Maggiolo
http://poisson.phc.unipi.it/~maggiolo/
maggiolo@mail.dm.unipi.it

2006–2007

Indice

1 Introduzione e prerequisiti

3.10.2006

Definizione 1.1. Un campo K è un *campo di numeri* se è un'estensione finita di $\mathbb{Q}$ (in particolare, $K = \mathbb{Q}(\alpha)$).

Le estensioni su cui si costruiranno gli esempi saranno le estensioni quadratiche $\mathbb{Q}(\sqrt{m})$ e le estensioni ciclotomiche $\mathbb{Q}(\zeta_m)$, con ζ_m radice m-esima dell'unità. Per le quadratiche $\mathbb{Q}(\sqrt{a/b}) = \mathbb{Q}(\sqrt{ab})$ e, se m e n sono liberi da quadrati, $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ se e solo se $m = n$. Per le ciclotomiche $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ e, se m è dispari, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$; tra gli m pari, si dimostra che $\mathbb{Q}(\zeta_m)$ sono tutte estensioni distinte. Inoltre $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ è un'estensione normale con $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \mathbb{Z}_m^\star$.

Definizione 1.2. Un numero $\alpha \in \mathbb{C}$ si dice *intero algebrico* se esiste $f \in \mathbb{Z}[X]$ tale che $f(\alpha) = 0$.

Proposizione 1.3. *Siano $\alpha \in \mathbb{C}$ di polinomio minimo μ_α, allora α è un intero algebrico se e solo se $\mu_\alpha \in \mathbb{Z}[X]$.*

Dimostrazione. $\Rightarrow$ Se α è intero algebrico, l'insieme dei polinomi di $\mathbb{Z}[X]$ che si annullano su α non è vuoto e quindi esiste f tra questi di grado minimo; per assurdo, se f fosse riducibile su $\mathbb{Q}$, lo sarebbe anche su $\mathbb{Z}$ per il lemma di Gauss, quindi $f = gh$ in $\mathbb{Z}[X]$. Allora $g(\alpha) = 0$ o $h(\alpha) = 0$ e si ha l'assurdo.

$\Leftarrow$ Il polinomio minimo è monico. □

Definizione 1.4. L'insieme degli interi algebrici si denota con $\mathbb{A} := \{\, \alpha \in \mathbb{C} \mid \alpha \text{ intero algebrico} \,\}$.

Se K è un campo di numeri, gli interi di K si denotano con $\mathscr{O}_K := K \cap \mathbb{A}$; in particolare, $\mathscr{O}_\mathbb{Q} = \mathbb{Z}$. Per $K = \mathbb{Q}(\sqrt{m})$, un elemento generico è $a + b\sqrt{m}$, di polinomio minimo $\mu = X^2 - 2aX + a^2 - b^2 m$; per appartenere a $\mathbb{Z}[X]$ deve essere $a = r/s$ con $s \mid 2$. Se $s = 1$, si deve anche avere $b^2 m \in \mathbb{Z}$, cioè $b \in \mathbb{Z}$ (perché m è libero da quadrati); altrimenti. Se $s = 2$, posto $b = t/q$, deve risultare $r^2/4 - (t/q)^2 m \in \mathbb{Z}$, da cui si ricava che se $m \equiv 1\ (4)$, allora $q \in \{1, 2\}$, altrimenti se $m \equiv 2, 3\ (4)$, $q = 1$. In definitiva, se $m \equiv 2, 3\ (4)$, $\mathscr{O}_K = \mathbb{Z}[\sqrt{m}]$, altrimenti se $m \equiv 1\ (4)$, $\mathscr{O}_K = \mathbb{Z}[1/2(a + b\sqrt{m})]$. In particolare, se $K = \mathbb{Q}(\alpha)$, non è vero che $\mathscr{O}_K$ è sempre $\mathbb{Z}[\alpha]$; però, è vero che esiste $d \in \mathbb{Z}$ tale che $d\alpha \in \mathbb{A}$ e $\mathbb{Q}\alpha = \mathbb{Q}(d\alpha)$: si può supporre che l'elemento primitivo α sia un intero algebrico. In particolare si ha che se $\mu_\alpha = X^n + a_1/s_1 X^{n-1} \ldots + a_n/s_n$, allora si può prendere $d = [s_1, \ldots, s_n]$.

Si mostra che l'inclusione $\mathbb{Z}[\alpha] \subseteq \mathbb{Q}(\alpha) \cap \mathbb{A}$ è sempre verificata; il viceversa non è vero, anzi, è possibile che $\mathbb{Q}(\alpha) \cap \mathbb{A}$ non sia nemmeno generato da un solo elemento.

4.10.2006

Alcuni prerequisiti.

- Teorema cinese del resto: se $I, J \leq A$ sono tali che $I + J = (1)$, allora $A/IJ = A/I \times A/J$.
- Teorema fondamentale della teoria di Galois: se L/K è un'estensione di Galois finita, allora la mappa

$$\begin{array}{ccc} \{\, F \mid L \supseteq F \supseteq K \,\} & \to & \{\, H \mid H \leq \mathrm{Gal}(L/K) \,\} \\ F & \mapsto & \mathrm{Gal}(L/F) \\ L^H & \leftarrow\!\shortmid & H \end{array}$$

è una corrispondenza biunivoca.

- Se $[L:K] = n$ e L/K è un'estensione separabile, allora esistono $\sigma_1, \dots, \sigma_n \colon L \to \bar{K}$ tali che $\sigma_{i|K} = \tau$ fissata.
- Se F/K è di Galois, $[FL:L] \mid [F:K]$ e $\mathrm{Gal}(FL/L) \cong \mathrm{Gal}(F/F \cap L)$.
- Il campo $\mathbb{F}_{p^n}$ è $\left\{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0 \right\}$ e $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi \rangle$, con $\varphi(x) = x^p$. Ancora, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$.
- Sono equivalenti:
  - $x \in B$ è intero su A;
  - $A[x]$ è un A-modulo finitamente generato;
  - esiste un A-modulo finitamente generato contenente $A[x]$ che sia un sottoanello di B;
  - esiste un $A[x]$-modulo fedele, finitamente generato come A-modulo.
- Se $A \subseteq B$ sono anelli, B è un A-modulo finitamente generato se e solo se $B \cong A[x_1, \dots, x_n]$ con $x_i \in B$ interi su A.
- La chiusura integrale di A è un sottoanello di B; se $A \subseteq B \subseteq C$ sono estensioni intere, anche $A \subseteq C$ è intera; la chiusura integrale di A in B è integralmente chiusa in B.
- Se A è un UFD, è integralmente chiuso.
- $\mathscr{O}_K = \mathbb{A} \cap K$ è la chiusura integrale di $\mathbb{Z}$ in K e quindi è integralmente chiuso.
- Non è vero che A integralmente chiuso implica A UFD: ad esempio, $\mathbb{Z}[\sqrt{-5}]$ è integralmente chiuso perché è $\mathscr{O}_{\mathbb{Q}(\sqrt{-5})}$, ma non è un UFD.
- Se A è un dominio integralmente chiuso e $K \coloneqq \mathbb{Q}(A)$, $\alpha \in \bar{K}$ è intero su A se e solo se $\mu_\alpha \in A[X]$.

Definizione 1.5. Sia $K \subseteq F$ con $[F:K] = n$, allora chiamando $\sigma_1, \dots, \sigma_n$ le estensioni, si definiscono *traccia* e *norma* dell'estensione come $\mathrm{Tr}_{F/K}, \mathrm{N}_{F/K} \colon F \to K$, $\mathrm{Tr}_{F/K}(x) = \sum_{i=1}^n \sigma_i(x)$ e $\mathrm{N}_{F/K}(x) = \prod_{i=1}^n \sigma_i(x)$.

Proposizione 1.6. *Traccia e norma sono ben definite (l'immagine è in K) e, se $\alpha \in \mathscr{O}_F$, $\mathrm{Tr}_{F/K}(\alpha), \mathrm{N}_{F/K}(\alpha) \in \mathscr{O}_K$.*

Dimostrazione. Siano $L \coloneqq K(\alpha)$, $\tau_1, \dots, \tau_d$ le estensioni di L/K con $d \mid n$, $t(\alpha) \coloneqq \tau_1(\alpha) + \cdots + \tau_d(\alpha)$, $n(\alpha) \coloneqq \tau_1(\alpha) \cdots \tau_d(\alpha)$; $t(\alpha), n(\alpha) \in K$ perché coefficienti di μ_α e se $\alpha \in \mathscr{O}_F$, $t(\alpha), n(\alpha) \in \mathscr{O}_K$ perché la chiusura integrale è un anello e $\tau_i(\alpha) \in \mathscr{O}_F$ perché radice dello stesso μ_α; infine, ogni τ_i si estende in n/d modi a F, in modo da ottenere le σ_i, da cui

$$\mathrm{Tr}_{F/K}(\alpha) = \frac{n}{d} \sum_{i=1}^{d} \tau_i(\alpha) \in \mathscr{O}_K$$

$$\mathrm{N}_{F/K}(\alpha) = \left(\prod_{i=1}^{d} \tau_i(\alpha) \right)^{\frac{n}{d}} \in \mathscr{O}_K. \qquad \square$$

10.10.2006

Proposizione 1.7. *La traccia è un'applicazione K-lineare, mentre la norma è K-moltiplicativa ($\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ e $\mathrm{N}(\lambda) = \lambda^{[F:K]}$).*

Proposizione 1.8. *Se M/F e F/K sono estensioni allora $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{M/F}$ e $\mathrm{N}_{M/K} = \mathrm{N}_{F/K} \circ \mathrm{N}_{M/F}$.*

Proposizione 1.9. *Sia $\alpha \in \mathscr{O}_K$, allora $\alpha \in \mathscr{O}_K^\star \Leftrightarrow \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Dimostrazione. $\Rightarrow$ Per ipotesi, esiste $\beta \in \mathscr{O}_K^\star$ tale che $\alpha\beta = 1$, allora $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = 1$, quindi $\mathrm{N}(\alpha) = \pm 1$, dato che $\mathrm{N}(\alpha) \in \mathbb{Z}$.

$\Leftarrow$ Si ha che $\mathrm{N}(\alpha) = \alpha \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha) = \pm 1$, quindi $\alpha^{-1} = \pm \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha) \in \mathscr{O}_K$. □

Esempio 1.10. Si vogliono calcolare le unità dei campi quadratici immaginari. Sia quindi $m > 0$ un intero libero da quadrati e si ponga $K \coloneqq \mathbb{Q}(\sqrt{-m})$; allora se $m \equiv 1, 2 \pmod 4$, $\mathscr{O}_K = \mathbb{Z}[i\sqrt{m}]$, altrimenti se $m \equiv 3 \pmod 4$, $\mathscr{O}_K = \mathbb{Z}[1/2(1 + i\sqrt{m})]$. Nel primo caso, sia $x = a + ib\sqrt{m}$; $\mathrm{N}(x) = a^2 + mb^2$, che è ± 1 se e solo se $x = \pm 1$ (nel caso che $m > 1$) oppure $x = \pm 1, \pm i$ (nel caso che $m = 1$). Nel secondo caso, sia $x = 1/2(a + ib\sqrt{m})$; allora $\mathrm{N}(x) = 1/4(a^2 + mb^2)$, che è ± 1 se e solo se $x = \pm 1$ (nel caso che $m > 3$), oppure $x = \pm 1, 1/2(\pm 1 \pm i\sqrt{3})$.

Osservazione 1.11. In un campo quadratico immaginario K, le unità di $\mathscr{O}_K$ sono le radici di 1 contenute in K.

Teorema 1.12 (Dirichlet)**.** *Sia K un campo di numeri. Allora $\mathscr{O}_K^\star$ è un gruppo abeliano finitamente generato e $\mathscr{O}_K^\star \cong R \times \mathbb{Z}^{r+s-1}$, dove R è l'insieme delle radici di 1 contenute in K, r è il numero di σ_i reali e s è il numero di coppie complesse coniugate di σ_i.*

Esempio 1.13. Sia $K \coloneqq \mathbb{Q}(\sqrt{2})$. Si ha che $\mathscr{O}_K = \mathbb{Z}[\sqrt{2}]$; se $x = a + b\sqrt{2}$, allora $\mathrm{N}(x) = \pm 1$ se e solo se $a^2 - 2b^2 = \pm 1$. Alcune soluzioni sono $x \in \{\pm 1, 1 + \sqrt{2}\}$, ma anche $\pm(1 + \sqrt{2})^k$ sono soluzioni: $\mathrm{N}(\pm(1 + \sqrt{2})^k) = \mathrm{N}(\pm 1)\mathrm{N}(1 + \sqrt{2})^k = (-1)^k(-1)^k = 1$. Si mostra che queste sono le uniche soluzioni: per assurdo, sia $1 < \varepsilon < 1 + \sqrt{2}$ una unità; si può supporre $\varepsilon + x + \sqrt{2}y$, con $x, y \in \mathbb{N} \setminus \{0\}$: $x \neq 0$ perché $-2y^2 \neq \pm 1$ per ogni y, e $y \neq 0$ perché $\varepsilon > 1$. Allora $x^2 - 2y^2 = \pm 1 = \varepsilon\bar{\varepsilon}$; da questo deriverebbe $|\bar{\varepsilon}| < 1$, cioè $-1 < x - \sqrt{2}y < 1$. Sommando, $0 < \varepsilon + \bar{\varepsilon} = 2x < 2 + \sqrt{2}$, da cui $x = 1$. D'altra parte, si ottiene anche $1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$, assurdo. Se ora ω fosse un'unità tale che $(1 + \sqrt{2})^k < \omega < (1 + \sqrt{2})^{k+1}$, allora $\varepsilon = \omega(1 + \sqrt{2})^{-k}$ soddisferebbe $1 < \varepsilon < 1 + \sqrt{2}$, assurdo.

11.10.2006

Definizione 1.14. Dati un gruppo abeliano G e un campo K, un *carattere* è un morfismo $\chi \colon G \to K^n$.

Teorema 1.15 (indipendenza dei caratteri di Artin)**.** *Dati G e K, i caratteri distinti di G in K sono linearmente indipendenti.*

Dimostrazione. Per assurdo, sia n il minimo numero di caratteri linearmente dipendenti, allora $n \geq 2$, in quanto un carattere non è mai dipendente e $\sum_{i=1}^n a_i\chi_i = 0$ con $a_i \neq 0$ per ogni i. Per ipotesi, esiste h tale che $\chi_1(h) \neq \chi_2(h)$, allora per ogni $g \in G$, applicando la combinazione lineare a gh si ha $\sum_{i=1}^n a_i\chi_i(g)\chi_i(h) = 0$, mentre moltiplicando per

$\chi_1(h)$ si ha $\sum_{i=1}^n a_i\chi_i(g)\chi_1(h) = 0$. Sottraendo le due espressioni si ottiene $0 = \sum_{i=1}^n a_i\chi_i(g)\left(\chi_i(h) - \chi_1(h)\right) = \sum_{i=2}^n a_i\chi_i(g)\left(\chi_i(h) - \chi_1(h)\right)$, cioè $\sum_{i=2}^n a_i\left(\chi_i(h) - \chi_1(h)\right)\chi_i = 0$ con il coefficiente di χ_2 diverso da zero, ma questo è impossibile perché si era supposto che n fosse il minimo numero di caratteri dipendenti. □

Osservazione 1.16. Dal teorema segue che se L/K è separabile, $\mathrm{Tr}_{L/K}\colon L \to K$ è non nulla (e quindi suriettiva in quanto applicazione lineare verso uno spazio di dimensione unitaria) perché $\mathrm{Tr}_{L/K} = \sum_{i=1}^n \sigma_i$ e σ_i si può vedere come un carattere da $L^\star$ a K.

Definizione 1.17. Sia $\varphi\colon L^2 \to K$, $\varphi(x,y) = \mathrm{Tr}_{L/K}(xy)$; φ è un'applicazione bilineare non degenere, quindi T tale che $T(x) = \mathrm{Tr}_{L/K}(x_\bullet)$ è un isomorfismo di L con il suo duale. Siano $(\alpha_1,\dots,\alpha_n)$ una base di L/K e $(f_1,\dots,f_n)$ la corrispondente base duale, $\beta_i = T^{-1}(f_i)$; $(\beta_1,\dots,\beta_n)$ è detta la *base duale* di $(\alpha_1,\dots,\alpha_n)$ rispetto alla traccia. In particolare si ha $\mathrm{Tr}_{L/K}(\beta_i\alpha_j) = \delta_{i,j}$.

Se F è un A-modulo libero finitamente generato, allora $F \cong \bigoplus_{i\in I} A$ e il rango di F è $|I| = \mathrm{rk}_A F = \dim_{A/\mathfrak{m}} F/\mathfrak{m}F$ per qualsiasi ideale massimale $\mathfrak{m}$. In generale non è vero che un sottomodulo di un A-modulo libero sia libero, ad esempio se I è un ideale non principale di A, I è sottomodulo del modulo libero A ma non è libero.

Teorema 1.18. *Siano A un anello a ideali principali e F un A-modulo libero, allora ogni sottomodulo M di F è libero e $\mathrm{rk}_A M \le \mathrm{rk}_A F$.*

Dimostrazione. Si dimostrerà solo il caso in cui F è finitamente generato. Per induzione su $n = \mathrm{rk}_A F$: se $n = 0$ non c'è niente da dimostrare; si suppone ora che ogni sottomodulo di un A-modulo libero di rango minore di n sia libero e $F = \langle x_1,\dots,x_n\rangle$; sia $F' = \langle x_2,\dots,x_n\rangle$, allora se $M \subseteq F'$ si ha finito; se $M \nsubseteq F'$, sia $\pi\colon F \to A$ con $\pi\left(\sum_{i=1}^n a_i x_i\right) = a_1$, allora $\pi(M) \neq \varnothing$ e per ipotesi $\pi(M) = (\bar a)$ con $\bar a = \pi(m)$ per qualche $m \in M$. Allora $m = \bar a x_1 + m'$ con $m' \in F'$. Si vuole dimostrare che $M = Am \oplus M'$ con $M' = M \cap F'$: se $z \in M$, $\pi(z) = \alpha_z\bar a$, quindi $z = \alpha_z m + (z - \alpha_z m)$ e $z - \alpha_z m \in M'$ perché $\pi(z - \alpha_z m) = 0$. Questo significa che $M = Am \oplus M'$, inoltre $\mathrm{rk}_A M = 1 + \mathrm{rk}_A M' \le 1 + \mathrm{rk}_A F' = n$. □

Teorema 1.19. *Siano A un PID, F un A-modulo libero, $M \subseteq F$ finitamente generato di rango n, allora esiste una base di F contenente degli elementi $b_1,\dots,b_n$ ed esistono degli elementi $a_1,\dots,a_n \in A$ tali che $(a_1b_1,\dots,a_nb_n)$ è una base di M e inoltre $a_i \mid a_{i+1}$ e gli a_i sono univocamente determinati a meno di moltiplicazioni per unità.*

Teorema 1.20. *Il gruppo $\mathscr{O}_K$ è abeliano libero di grado $n = [K:\mathbb{Q}]$.*

Dimostrazione. Si vogliono trovare due $\mathbb{Z}$-moduli A e B, di rango n tali che $A \subseteq \mathscr{O}_K \subseteq B$. Sia $(\alpha_1,\dots,\alpha_n)$ una $\mathbb{Q}$-base di K; senza perdità di generalità si può supporre che ogni α_i sia intero, cioè $\alpha_i \in \mathscr{O}_K$. Allora $A = \langle\alpha_1,\dots,\alpha_n\rangle_{\mathbb{Z}} \subseteq \mathscr{O}_K$ e A è libero di rango n. Sia ora $(\beta_1,\dots,\beta_n)$ la base duale corrispondente; sia $B = \langle\beta_1,\dots,\beta_n\rangle_{\mathbb{Z}}$, allora per ogni $x \in \mathscr{O}_k \subseteq K$, $x = \sum_{i=1}^n x_i\beta_i$ con $x_i \in \mathbb{Q}$; si deve dimostrare che ogni x_i è intero. Per ogni j, $x\alpha_j$ è intero, ma $x\alpha_j = \sum_{i=1}^n x_i\beta_i\alpha_j$, quindi $\mathbb{Z} \ni \mathrm{Tr}_{K/\mathbb{Q}}(x\alpha_j) = \sum_{i=1}^n x_i\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\alpha_j) = x_j$. □

Definizione 1.21. Una *base intera* è una $\mathbb{Z}$-base di $\mathscr{O}_K$.

Osservazione 1.22. Una base intera è in particolare una base di interi, ma non è vero il viceversa: se $m \equiv 1 \pmod 4$, $\mathscr{O}_K = \mathbb{Z}[1/2(1+\sqrt{m})]$ e $(1, \sqrt{m})$ è una base di interi ma non una base intera, in quanto $1/2 \notin \langle 1, \sqrt{m} \rangle_{\mathbb{Z}}$.

Definizione 1.23. Siano F/K un'estensione separabile di grado n, $\sigma_1, \dots, \sigma_n$ le immersioni di F in K, $\alpha_1, \dots, \alpha_n \in F$, allora il *discriminante* dell'estensione è $\operatorname{disc}_{F/K}(\alpha_1, \dots, \alpha_n) \coloneqq \det^2\left((\sigma_i(\alpha_j))_{i,j}\right)$. Il discriminante è ben definito poiché se varia l'ordine delle σ_i, varia solo il segno del determinante.

Proposizione 1.24. *Dati* $\alpha_1, \dots, \alpha_n \in F$, $\operatorname{disc}_{F/K}(\alpha_i, \dots, \alpha_n) = \det\left(\left(\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)\right)_{i,j}\right) \in K$, *inoltre se* $\alpha_1, \dots, \alpha_n \in \mathscr{O}_F$, *il discriminante è in* $\mathscr{O}_K$.

Dimostrazione. Si ha:

$$\begin{aligned}\operatorname{disc}_{F/K}(\alpha_1, \dots, \alpha_j) &= \det{}^2\left((\sigma_i(\alpha_j))_{i,j}\right) = \\ &= \det\left((\sigma_i(\alpha_j))_{i,j}\right)\det\left((\sigma_j(\alpha_i))_{i,j}\right) = \\ &= \det\left((\sigma_i(\alpha_j))_{i,j}(\sigma_j(\alpha_i))_{i,j}\right) = \\ &= \det\left(\left(\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)\right)_{i,j}\right). \qquad \square\end{aligned}$$

Proposizione 1.25. *Gli elementi* $\alpha_1, \dots, \alpha_n$ *sono* K*-linearmente dipendenti se e solo se* $\operatorname{disc}_{F/K}(\alpha_1, \dots, \alpha_n) = 0$.

Dimostrazione. $\Rightarrow$ Se $\alpha_1, \dots, \alpha_n$ sono linearmente dipendenti, le colonne di $(\sigma_i(\alpha_j))_{i,j}$ sono linearmente dipendenti e il discriminante è nullo.

$\Leftarrow$ Se $\alpha_1, \dots, \alpha_n$ fossero linearmente indipendenti, sarebbero una base e per il teorema di indipendenza dei caratteri la matrice $(\sigma_i(\alpha_j))_{i,j}$ avrebbe determinante non nullo. $\square$

17.10.2006

Teorema 1.26. *Sia* $K \coloneqq \mathbb{Q}(\alpha)$, *allora*

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

Dimostrazione. Per definizione,

$$\begin{aligned}\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) &= \det\begin{pmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 = \\ &= \left(\prod_{i \le j} (\sigma_i(\alpha) - \sigma_j(\alpha))\right)^2 = \\ &= \prod_{i \ne j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \cdot (-1)^{\frac{n(n-1)}{2}}.\end{aligned}$$

Da $\mu_\alpha = \prod_{i=1}^n (X - \sigma_i(x))$, si ottiene $\mu'_\alpha = \sum_{i=1}^n \prod_{j\neq i}(x - \sigma_i(\alpha))$. Di conseguenza

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(\mu'_\alpha(\alpha)) &= \prod_{i=1}^n \sigma_i(\mu'_\alpha(\alpha)) = \prod_{i=1}^n \mu'_\alpha(\sigma_i(\alpha)) = \\ &= \prod_{i=1}^n \prod_{j\neq i} (\sigma_i(\alpha) - \sigma_j(\alpha)) = \prod_{i\neq j} (\sigma_i(\alpha) - \sigma_j(\alpha))\,. \qquad \square\end{aligned}$$

Esempio 1.27. Siano $\zeta := \zeta_m = e^{2\pi i/m}$, $K := \mathbb{Q}(\zeta)$, $\mathrm{disc}(\zeta) := \mathrm{disc}(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) = (-1)^{\varphi(m)/2(\varphi(m)-1)}\,\mathrm{N}_{K/\mathbb{Q}}(\mu'_\zeta(\zeta))$. Si sa che $\mu_\zeta g = X^m - 1$ e $\mu_\zeta = \prod_{(k,m)=1}(X - \zeta^k)$; perciò $mX^{m-1} = \mu'_\zeta g + \mu_\zeta g'$ e $m\zeta^{m-1} = \mu'_\zeta(\zeta)g(\zeta) + \cancel{\mu_\zeta(\zeta)g'(\zeta)}$ e poiché il termine noto del polinomio minimo è 1, si ha

$$\mathrm{N}_{K/\mathbb{Q}}(\mu'_\zeta(\zeta)) = \frac{\mathrm{N}(m)\mathrm{N}(\zeta)^{m-1}}{\mathrm{N}(g(\zeta))} = \frac{m^{\varphi(m)} \cdot 1^{m-1}}{\mathrm{N}(g(\zeta))};$$

questo significa che $\mathrm{disc}(\zeta) \mid m^{\varphi(m)}$, dato che $\mathrm{N}(g(\zeta))$ è intero. Se si prende m primo, $X^m - 1 = \mu_\zeta(X - 1)$, cioè $g = X - 1$ e

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

perché $\mathrm{N}(\zeta - 1) = p$ (è il termine noto del polinomio minimo di $\zeta - 1$). Si può anche dimostrare che $\mathrm{disc}\,\zeta_{p^n} = (-1)^k\, p^{p^{n-1}(pn-n-1)}$ con $k = 1/2\varphi(p^n)(\varphi(p^n) - 1)$.

Osservazione 1.28. Siano $(\alpha_1, \ldots, \alpha_n)$ e $(\beta_1, \ldots, \beta_n)$ due $\mathbb{Q}$-basi di K con $\beta_j = \sum_{i=1}^n m_{j,i}\alpha_i$ e $m_{j,i} \in \mathbb{Q}$ e sia M la matrice del cambiamento di base. Si ha che $M\sigma_\lambda(\alpha) = \sigma_\lambda(\beta)$. Quindi $\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = (\det M)^2\, \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$.

Proposizione 1.29. *Siano $(\alpha_1, \ldots, \alpha_n)$ e $(\beta_1, \ldots, \beta_n)$ basi intere di K, allora* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\beta_1, \ldots, \beta_n)$.

Dimostrazione. Per l'osservazione e perché M è una matrice a coefficienti interi e invertibile in $\mathbb{Z}$, quindi $\det M \in \{\pm 1\}$. $\square$

Definizione 1.30. Se $(\alpha_1, \ldots, \alpha_n)$ è una base intera di K, il *discriminante* di K è $\mathrm{disc}\, K = \mathrm{disc}\, \mathscr{O}_K := \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$.

Esempio 1.31. Si considerano le estensioni quadratiche $K := \mathbb{Q}(\sqrt{m})$; se $m \equiv 2, 3\ (4)$, $\mathscr{O}_K = \mathbb{Z}[\sqrt{m}]$ e $(1, \sqrt{m})$ è una base intera, quindi

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

Se invece $m \equiv 1\ (4)$, $\mathscr{O}_K = \mathbb{Z}[1/2(1 + \sqrt{m})]$, quindi una base intera è $(1, 1/2(1 + \sqrt{m}))$ e

$$\mathrm{disc}\, K = \mathrm{disc}\left(1, \frac{1 + \sqrt{m}}{2}\right) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = \left(-\sqrt{m}\right)^2 = m.$$

Definizione 1.32. Sia $X \subseteq K$ uno $\mathbb{Z}$-modulo libero di base $(\alpha_1, \dots, \alpha_n)$, con $\operatorname{rk} X = n \coloneqq [K : \mathbb{Q}]$; il *discriminante* di X è $\operatorname{disc} X \coloneqq \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

Si dimostra che il discriminante di X non dipende dalla base scelta, come per il discriminante di K.

Proposizione 1.33. *Siano X e Y due $\mathbb{Z}$-moduli liberi, $X \subseteq Y \subseteq K$ con $\operatorname{rk} X = \operatorname{rk} Y = n \coloneqq [K : \mathbb{Q}]$, allora $\operatorname{disc} X = [Y : X]^2 \operatorname{disc} Y$ e $X = Y$ se e solo se $\operatorname{disc} X = \operatorname{disc} Y$.*

Dimostrazione. Per il teorema di struttura, esistono una $\mathbb{Z}$-base di Y $(y_1, \dots, y_n)$ e $a_1, \dots, a_n$ tali che $(a_1 y_1, \dots, a_n y_n)$ è una base di X. Quindi $\operatorname{disc} X = \operatorname{disc}(a_1 y_1, \dots, a_n y_n) = (\det M)^2 \operatorname{disc}(y_1, \dots, y_n)$, dove $M = \operatorname{diag}(a_1, \dots, a_n)$ e $\det M = a_1 \cdots a_n = [Y : X]$. Infatti

$$Y/X = \frac{y_1\mathbb{Z} \oplus \cdots \oplus y_n\mathbb{Z}}{a y_1\mathbb{Z} \oplus \cdots a y_n\mathbb{Z}} = \bigoplus_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z} \qquad \square$$

Osservazione 1.34. Sia $(\alpha_1, \dots, \alpha_n)$ una base di interi; per sapere se è una base intera, si calcola il discriminante $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = k^2 \operatorname{disc} K$; se $k = \pm 1$, la base è intera. In particolare, se $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ è libero da quadrati, la base è intera.

Se si indica con $\operatorname{disc}(\alpha) \coloneqq \operatorname{disc}(1, \alpha, \dots, \alpha^{n-1})$, si chiama l'*indice* di α il numero $\operatorname{ind}(\alpha) \coloneqq [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ e si ha $\operatorname{disc}(\alpha) = \operatorname{ind}(\alpha)^2 \operatorname{disc} K$.

18.10.2006

Teorema 1.35. *Siano K e L dei campi di numeri tali che $[KL : \mathbb{Q}] = [K : \mathbb{Q}]\,[L : \mathbb{Q}]$ (cioè $[KL : L] = [K : \mathbb{Q}]$); sia $d = (\operatorname{disc} L, \operatorname{disc} K)$. Allora $\mathcal{O}_{KL} \subseteq 1/d\,\mathcal{O}_K \mathcal{O}_L$. In particolare, se i discriminanti sono coprimi, $d = 1$ e $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$.*

Dimostrazione. Siano $(\alpha_1, \dots, \alpha_n)$ e $(\beta_1, \dots, \beta_m)$ basi intere di $\mathcal{O}_K$ e $\mathcal{O}_L$, $x \in \mathcal{O}_{KL}$, allora $x = \sum_{i,j} m_{i,j}/r \alpha_i \beta_j$, in quanto $(\alpha_i \beta_j)_{i,j}$ è una $\mathbb{Q}$-base di KL e si prende r il denominatore comune dei coefficienti. Si deve dimostrare che $r \mid d$ o analogamente $r \mid \operatorname{disc} K$ e $r \mid \operatorname{disc} L$.

Sia $x_i \coloneqq \sum_{j=1}^{m} m_{i,j}/r \beta_j$; $x_i \in L$ e $x = \sum_{i=1}^{n} x_i \alpha_i$. Ora, $r \mid \operatorname{disc} K$ se e solo se $x_i \operatorname{disc} K \in \mathcal{O}_L$: la prima implicazione è ovvia, per la seconda, se $x_i \operatorname{disc} K \in \mathcal{O}_L$, allora $x_i \operatorname{disc} K = \sum_{j=1}^{m} a_j \beta_j$ con $a_j = m_{i,j}/r \operatorname{disc} K \in \mathbb{Z}$, cioè $r \mid \operatorname{disc} K$. È necessario ora dimostrare che $x_i \operatorname{disc} K \in \mathcal{O}_L$.

Siano $\sigma_1, \dots, \sigma_n$ le immersioni di $K/\mathbb{Q}$; per ogni λ, esiste un'immersione $\tilde{\sigma}_\lambda$ di KL/L tale che $\tilde{\sigma}_\lambda(k) = \sigma_\lambda(k)$ per ogni $k \in K$ e $\tilde{\sigma}_\lambda(l) = l$ per ogni $l \in L$. Si ha $\tilde{\sigma}_\lambda(x) = \sum_i x_i \tilde{\sigma}_\lambda(\alpha_i) = \sum_i x_i \sigma_\lambda(\alpha_i)$. Questo si può vedere come un sistema a n equazioni e n incognite in $x_1, \dots, x_n$, che risolto con Cramer dà $x_i = \gamma_i/\delta_i$, dove $\delta_i = \det(\sigma_\lambda(\alpha_i))_{i,\lambda} = \sqrt{\operatorname{disc} K}$ e γ_i è il determinante di una matrice con coefficienti interi algebrici, quindi è un intero algebrico e $x_i \operatorname{disc} K = \delta_i \gamma_i \in \mathbb{A}$. D'altra parte, $x_i \in L$ e $\operatorname{disc} K$ è intero, quindi $x_i \operatorname{disc} K \in \mathcal{O}_L$, cioè $r \mid \operatorname{disc} L$. Allo stesso modo si dimostra che $r \mid \operatorname{disc} K$. $\square$

Lemma 1.36.

$$p = \prod_{\substack{k=1 \\ (k,p)=1}}^{p^l} (1 - \zeta^k).$$

Dimostrazione. Si ha che

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

dove la somma ha esattamente p termini, perciò $\mu_\zeta(1) = p$. □

Teorema 1.37. *Sia $K \coloneqq \mathbb{Q}(\zeta)$ con ζ radice m-esima primitiva dell'unità, allora $\mathscr{O}_K = \mathbb{Z}[\zeta]$.*

Dimostrazione. Si suppone innanzitutto che $m = p^l$ con p primo. Allora preso $\alpha \in \mathscr{O}_K$ si deve dimostrare $\alpha \in \mathbb{Z}[\zeta]$, poiché l'altra inclusione vale in generale. Per comodità si considera $\mathbb{Z}[1-\zeta] = \mathbb{Z}[\zeta]$; sia $d \coloneqq \operatorname{disc}\zeta = \operatorname{disc}(1-\zeta)$ (uguali perché gli $\mathbb{Z}$-moduli che generano sono uguali) e sia $n \coloneqq \varphi(p^l)$.

Poiché $d = \operatorname{disc}(1-\zeta)$, posto $\Delta \coloneqq [\mathscr{O}_K : \mathbb{Z}[1-\zeta]]$, è anche vero che $d = \Delta^2 \operatorname{disc}\mathscr{O}_K = \Delta^2 \operatorname{disc} K$. Chiaramente, $\Delta\mathscr{O}_K \subseteq \mathbb{Z}[1-\zeta]$, inoltre $\Delta \mid d$, quindi anche $d\mathscr{O}_K \subseteq \mathbb{Z}[1-\zeta]$. Questo comporta l'esistenza di $m_1, \ldots, m_n \in \mathbb{Z}$ tali che $\alpha = {}^1\!/_d \left(m_1 + \cdots + m_n (1-\zeta)^{n-1}\right)$; inoltre $d = p^t$ perché il discriminante divide $m^{\varphi(m)}$, e si vuole dimostrare che il denominatore si può semplificare. Se ciò non fosse possibile, allora esisterebbe i tale che $p \nmid m_i$; sia allora $\beta \coloneqq {}^1\!/_p \left(m_i (1-\zeta)^{i-1} + \cdots + m_n (1-\zeta)^{n-1}\right)$ con $p \nmid m_i$, cosa possibile a meno di moltiplicare per una potenza di p. Ora, in $\mathbb{Z}[1-\zeta]$ si ha che $(1-\zeta) \mid (1-\zeta^k)$, quindi per il lemma $p(1-\zeta)^{-i} \in \mathbb{Z}[1-\zeta]$. In particolare, $\beta \in \mathscr{O}_K$, perciò $\beta p (1-\zeta)^{-i} = m_i (1-\zeta)^{-1} + \cdots \in \mathscr{O}_K$ e di conseguenza anche $m_i (1-\zeta)^{-1} \in \mathscr{O}_K$. Allora $\mathrm{N}(m_i (1-\zeta)^{-1}) = \mathrm{N}(m_i)\,\mathrm{N}(1-\zeta)^{-1} = m_i^n p^{-1} \in \mathbb{Z}$, assurdo.

Si considera ora il caso generale e si dimostra per induzione su m: il passo base è $m = 2$ che è una potenza di un primo; se invece m è qualsiasi e la tesi è vera per ogni $m' < m$, si può inoltre supporre che m non sia una potenza di un primo, caso già dimostrato, perciò si può scrivere $m = m_1 m_2$ con $(m_1, m_2) = 1$ e $2 \leq m_1, m_2 < m$. In questo caso, posto $K_i \coloneqq \mathbb{Q}(\zeta_{m_i})$, si ha $\mathbb{Q}(\zeta_m) = K_1 K_2$: infatti $m_i \mid m$, quindi ζ_{m_i} è radice m-esima dell'unità, viceversa m_1 e m_2 sono coprimi, quindi $\zeta_{m_1} = \zeta_m^{m_2}$ e $\zeta_{m_2} = \zeta_m^{m_1}$ ed esistono $a_1, a_2 \in \mathbb{Z}$ tali che $a_1 m_1 + a_2 m_2 = 1$.

Inoltre, $\operatorname{disc} K_i \mid m_i^{\varphi(m_i)}$, perciò $(\operatorname{disc} K_1, \operatorname{disc} K_2) = 1$ e per il teorema $\mathscr{O}_K = \mathscr{O}_{K_1}\mathscr{O}_{K_2} = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}]$; infine si mostra che questo anello è $\mathbb{Z}[\zeta_m]$ come fatto prima per $K = K_1 K_2$. □

Teorema 1.38 (Kronecker - Weber)**.** *Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in un'estensione ciclotomica. In particolare, $\mathbb{Q}(\sqrt{m})$ è contenuta in $\mathbb{Q}(\zeta_d)$, dove $d \coloneqq \operatorname{disc}\mathbb{Q}(\sqrt{m})$.*

Dimostrazione. Si dimostra solo il caso particolare. Si sa che $\operatorname{disc}\zeta_p \in \left\{\pm p^{p-2}\right\}$, col segno positivo se $p \equiv 1\ (4)$, negativo altrimenti. Se il segno è positivo, da $\sqrt{\operatorname{disc} K} \in K$ risulta $\sqrt{p} \in \mathbb{Q}(\zeta_p)$; se invece $q \equiv 3\ (4)$, per lo stesso motivo si ha $\sqrt{-q} \in \mathbb{Q}(\zeta_p)$. Inoltre $\sqrt{-1} \in \mathbb{Q}(\zeta_4)$ e $\sqrt{2}, \sqrt{-2} \in \mathbb{Q}(\zeta_8)$, mentre $\sqrt{q} \notin \mathbb{Q}(\zeta_q)$ perché il suo gruppo di Galois è ciclico di ordine pari, quindi contiene un unico sottogruppo di ordine 2.

Sia ora m libero da quadrati, $K \coloneqq \mathbb{Q}(\sqrt{m})$, allora $\operatorname{disc} K = m$ se $m \equiv 1\ (4)$, mentre $\operatorname{disc} K = 4m$ se $m \equiv 2, 3\ (4)$. Si scrive $m = \pm p_1 \cdots p_r q_1 \cdots q_s 2^\varepsilon$, con $p_i \equiv 1\ (4)$, $q_i \equiv 3\ (4)$ e $\varepsilon \in \{0, 1\}$. Si sa che $\sqrt{p_i} \in \mathbb{Q}(\zeta_{p_i}) \subseteq \mathbb{Q}(\zeta_d)$ e $\sqrt{-q_i} \in \mathbb{Q}(\zeta_{q_i}) \subseteq$

$\mathbb{Q}(\zeta_d)$. Se $m \equiv 1 \ (4)$, $\varepsilon = 0$ e s è pari, quindi $m = p_1 \cdots p_r(-q_1) \cdots (-q_s)$ e $\sqrt{m} \in \mathbb{Q}(\zeta_d)$ e $d = m$. Se $m \equiv 3 \ (4)$, $d = 4m$ e $\sqrt{-1} \in \mathbb{Q}(\zeta_d)$, quindi $\sqrt{m} \in \mathbb{Q}(\zeta_d)$. Se $m \equiv 2 \ (4)$, $m = 2t$ e $d = 4m = 8t$, quindi $\sqrt{-1}, \sqrt{2}, \sqrt{-2} \in \mathbb{Q}(\zeta_d)$ e $\sqrt{m} \in \mathbb{Q}(\zeta_d)$. Si ottiene anche che d è il minimo intero per cui si ha l'inclusione. □

Si vuole ora dimostrare che $K := \mathbb{Q}(\zeta_m + \overline{\zeta_m}) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ è uguale a $\mathbb{Q}(\zeta_m) \cap \mathbb{R}$. Sicuramente si ha $K \subseteq \mathbb{Q}(\zeta_m) \cap \mathbb{R} \subseteq \mathbb{Q}(\zeta_m)$ e $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{R}] \geq 2$. Per mostrare l'uguaglianza è sufficiente dimostrare che $[\mathbb{Q}(\zeta_m) : K] \leq 2$, ma $(X - \zeta_m)(X - \zeta_m^{-1}) = X^2 - (\zeta_m + \zeta_m^{-1}) + 1$, polinomio di grado 2 di K che ha come radice ζ_m.

Ora si mostra che $\mathscr{O}_K = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$. Infatti, $[K : \mathbb{Q}] = {}^{\varphi(m)}/_2$, perciò $(1, (\zeta_m + \zeta_m^{-1}), \ldots, (\zeta_m + \zeta_m^{-1})^{{}^{\varphi(m)}/_2 - 1})$ è una $\mathbb{Q}$-base di K. Preso $\alpha \in \mathscr{O}_K$, $\alpha = \alpha_0 + \alpha_1(\zeta_m + \zeta_m^{-1}) + \cdots + \alpha_N(\zeta_m + \zeta_m^{-1})^N$ con $N < {}^{\varphi(m)}/_2$ e $\alpha_i \in \mathbb{Q}$. Per assurdo, se $\alpha \notin \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$, a meno di sottrarre elementi di $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$, si può supporre $\alpha_N \notin \mathbb{Z}$; moltiplicando per ζ_m^N, si ottiene $\mathbb{Z}[\zeta_m] \ni \zeta_m^N \alpha = \alpha_N + \zeta_m(\ldots) + \alpha_N \zeta_m^{2N}$, rispetto alla base canonica di $\mathbb{Z}[\zeta_m]$. Poiché $2N \leq \varphi(m) - 2 < \varphi(m) - 1$, allora ζ_m^N si scrive come combinazione lineare della base $1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ e per l'unicità della scrittura tutti i coefficienti devono essere interi e in particolare lo deve essere α_N, assurdo.

2 Domini di Dedekind

24.10.2006

Definizione 2.1. Un A-modulo M si dice *noetheriano* se vale una delle seguenti condizioni equivalenti:

- ogni famiglia non vuota di sottomoduli di M ammette un elemento massimale;
- ogni successione crescente di sottomoduli di M è stazionaria;
- ogni sottomodulo di M è finitamente generato.

Definizione 2.2. Un anello A si dice *noetheriano* se è noetheriano come A-modulo (in quanto i sottomoduli di A come A-modulo sono esattamente gli ideali).

Definizione 2.3. Un *dominio di Dedekind* è un dominio di integrità R se valgono:

- R è noetheriano;
- ogni suo ideale primo non nullo è massimale;
- R è integralmente chiuso.

Esempio 2.4. Tutti gli anelli a ideali principali sono domini di Dedekind: ogni ideale è finitamente generato, ogni ideale primo non nullo è massimale, e sono integralmente chiusi perché UFD.

Si vorrà dimostrare che gli anelli di numeri sono domini di Dedekind. Paragonarli agli anelli a ideali principali serve perché gli anelli di numeri in generale non sono a fattorizzazione unica, ma si vuole comunque avere qualche idea simile a quelle che si trovano negli UFD.

In generale, se R è un dominio di Dedekind, K il suo campo quoziente, ${}^{F}/_{K}$ estensione finita e separabile, allora la chiusura integrale di R in F è ancora un dominio di Dedekind. Si dimostrerà un teorema più debole (gli anelli di numeri sono chiusure integrali di $\mathbb{Z}$ in estensioni finite e separabili di $\mathbb{Q}$).

Lemma 2.5. *Sia $I \leq \mathscr{O}_K$ un ideale, allora ${}^{\mathscr{O}_K}/_I$ è finito. In particolare* $\operatorname{rk} I = n$.

Dimostrazione. Sia $\alpha \in I$, $\alpha \neq 0$, allora $N_{K/\mathbb{Q}}(\alpha) = \alpha\beta = m \in \mathbb{Z}$ con $\beta \in \mathbb{A}$; viceversa $\beta = {}^{m}/_{\alpha} \in K$, quindi $\beta \in K \cap \mathbb{A} = \mathscr{O}_K$. Quindi $\alpha\beta = m \in I$, cioè se $\alpha \in I$, $N_{K/\mathbb{Q}}(\alpha) \in I$. Si ha $(m) \subseteq I$ e si ha un'applicazione iniettiva ${}^{\mathscr{O}_K}/_I \to {}^{\mathscr{O}_K}/_{(m)} \cong \left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^n$, cioè ${}^{\mathscr{O}_K}/_I$ è finito. □

Teorema 2.6. *Ogni anello di numeri è un dominio di Dedekind.*

Dimostrazione. Si dimostrano le tre richieste.

- Sia $I \leq \mathscr{O}_K$ un ideale; $\mathscr{O}_K$ è abeliano libero di rango n quindi I è abeliano libero di rango minore o uguale a n, quindi i suoi generatori come ideale sono gli stessi che come $\mathbb{Z}$-modulo cioè I è finitamente generato.
- Sia $\mathfrak{p}$ ideale primo non nullo; ${}^{\mathscr{O}_K}/_{\mathfrak{p}}$ è un dominio e si deve dimostrare che è un campo: ma per il lemma è finito (ogni dominio d'integrità finito è un campo).
- Per definizione, un anello di numeri è integralmente chiuso. □

Esempio 2.7. Per $K = \mathbb{Q}\left(\sqrt{-5}\right)$, $\mathscr{O}_K = \mathbb{Z}[\sqrt{-5}]$, quindi $\mathscr{O}_K$ è un dominio di Dedekind ma non è un UFD.

Lemma 2.8. *Siano $A \subseteq B$ anelli, $\mathfrak{q}$ ideale primo di B, allora $\mathfrak{q} \cap A$ è primo in A (equivalentemente, la contrazione di un ideale primo è primo). Al contrario, se $\mathfrak{p}$ è ideale primo di A, in generale l'estensione di $\mathfrak{p}$ in B, $(\mathfrak{p})$ non è un ideale primo.*

Lemma 2.9. *Sia $\mathfrak{p} \leq A$ ideale primo, $\mathfrak{p} \supseteq I_1 \dots I_n$ con I_j ideali di A, allora esiste j_0 tale che $\mathfrak{p} \supseteq I_{j_0}$.*

Lemma 2.10. *Sia A un dominio noetheriano, allora ogni ideale non nullo di A contiene un prodotto di ideali primi.*

Dimostrazione. Per assurdo, sia

$$\mathscr{F} = \{\, I \leq A \mid I \text{ non contiene un prodotto di ideali primi non nulli} \,\}$$

diverso dal vuoto, allora per la noetherianità, esiste un $J \in \mathscr{F}$ massimale rispetto a $\subseteq$; J è un ideale proprio perché $A \notin \mathscr{F}$. Sicuramente J non è primo, perché gli ideali primi non appartengono a $\mathscr{F}$.Se $xy \in J$, ma $x, y \notin J$, $J \subsetneq J + x \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$, $J \subsetneq J + y \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_s$ quindi $J \supseteq (J + x)(J + y) \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s$, assurdo. □

Definizione 2.11. Sia A un dominio, K il suo campo dei quozienti; un *ideale frazionario* di A è un A-sottomodulo I di K tale che esiste un elemento $d \in A \setminus \{0\}$ tale che $I \subseteq {}^{1}/_{d}A$.

Proposizione 2.12. *Sia $I \subseteq K$ un A-modulo finitamente generato, allora I è un ideale frazionario. Se A è un dominio noetheriano, e I è un ideale frazionario, allora I è finitamente generato.*

Dimostrazione. Se $I = \langle x_1, \dots x_s \rangle$ $x_i = {}^{\alpha_i}/_{d_i} \in K$, allora posto $d = d_1 \cdots d_s$, $I \subseteq {}^1/_d A$. Se A è noetheriano e $I \subseteq {}^1/_d A$, ${}^1/_d A$ un A-modulo noetheriano perché isomorfo a A, quindi un suo sottomodulo è finitamente generato. □

25.10.2006

Definizione 2.13. Sua A un dominio e I un ideale frazionario di A; si definisce $I^{-1} \coloneqq \{ x \in K \mid xI \subseteq A \}$.

Osservazione 2.14. Se I è un ideale frazionario di A, anche I^{-1} è un ideale frazionario di A e $II^{-1} \subseteq A$. Infatti il secondo fatto è evidente e se $d \in I \setminus \{0\}$, $I^{-1}d \subseteq A$, quindi $I^{-1} \subseteq {}^1/_d A$.

Definizione 2.15. Sia A un dominio, I un suo ideale frazionario; I si dice *invertibile* se $II^{-1} = A$.

Proposizione 2.16. *Siano I e J ideali frazionari di A tali che $IJ = A$; allora I è invertibile, $J = I^{-1}$ e $I = J^{-1}$.*

Dimostrazione. Chiaramente, $J \subseteq I^{-1}$, e $II^{-1} \subseteq A$, allora $JII^{-1} \subseteq JA = J$, quindi $I^{-1} \subseteq J$, cioè $J = I^{-1}$, quindi I è invertibile e si può ripetere le stesso argomento per J. □

Teorema 2.17. *Gli ideali massimali di un dominio di Dedekind sono invertibili.*

Dimostrazione. Sia R un dominio di Dedekind e $\mathfrak{m}$ un suo ideale massimale; $\mathfrak{m}^{-1}$ è un ideale frazionario e $\mathfrak{m}\mathfrak{m}^{-1} \subseteq R$; si deve dimostrare che vale l'uguaglianza. Si sa inoltre che $R \subseteq \mathfrak{m}^{-1}$ quindi $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$, ma $\mathfrak{m}$ è massimale, perciò vale esattamente una uguaglianza. Si suppone per assurdo $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$, per ogni $x \in \mathfrak{m}^{-1}$, $x\mathfrak{m} \subseteq \mathfrak{m}$, da cui $x^2\mathfrak{m} \subseteq x\mathfrak{m} \subseteq \mathfrak{m}$, cioè $x^n\mathfrak{m} \subseteq \mathfrak{m}$ per ogni n e se $d \in \mathfrak{m} \setminus \{0\}$, vale $x^n d \in \mathfrak{m}$ per ogni n, cioè $dR[x] \subseteq R$, e $R[x] \subseteq {}^1/_d R$. Allora $R[x]$ è finitamente generato come R-modulo, cioè x è intero. Allora poiché R è un dominio di Dedekind, $x \in R$, cioè $\mathfrak{m}^{-1} = R$. Sia $a \in \mathfrak{m} \setminus \{0\}$, allora $aR \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$ con r il minimo che abbia questa proprietà. Allora $\mathfrak{m} \supseteq aR \subseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$ e si può supporre che $\mathfrak{m} \supseteq \mathfrak{p}_1$, e $\mathfrak{p}_1$ è ideale primo non nullo in un dominio di Dedekind, quindi è massimale e $\mathfrak{p}_1 = \mathfrak{m}$, allora $\mathfrak{m} \supseteq aR \supseteq \mathfrak{m}I$ con $I = \mathfrak{p}_2 \dots \mathfrak{p}_r$; per la minimalità di r, $aR \not\supseteq I$, allora esiste $\alpha \in I$ tale che $\alpha \notin aR$, cioè ${}^\alpha/_a \notin R$. Ma ${}^\alpha/_a \in K$ e $\alpha\mathfrak{m} \subseteq I\mathfrak{m} \subseteq aR$ implica ${}^\alpha/_a\mathfrak{m} \subseteq R$ e ${}^\alpha/_a \in \mathfrak{m}^{-1}$, assurdo. □

Teorema 2.18 (di fattorizzazione unica per gli ideali)**.** *Igni ideale frazionario non nullo di R si scrive in modo unico come prodotto di ideali primi: $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ con $e_i = e_{\mathfrak{p}_i}(I) \in \mathbb{Z}$.*

Dimostrazione. Si osserva che è sufficiente dimostrare il teorema per gli ideali interi, infatti se I è ideale frazionario, $I \subseteq {}^1/_d R$ con $d \in R \setminus \{0\}$, allora $I = (dR)^{-1}(dI)$; sia dR che dI sono ideali interi e si suppone che si scrivano come prodotto di primi, si verifica che $(dR)^{-1}$ è prodotto degli stessi primi con esponenti opposti, quindi si è ottenuta la fattorizzazione di un ideale frazionario a partire da quella degli ideali interi.

Sia $\mathscr{F} = \{ I \leq R \mid I \text{ non si fattorizza} \}$; se per assurdo, $\mathscr{F} \neq \varnothing$, per la noetherianità, esiste un elemento massimale $J \in \mathscr{F}$; chiaramente J non può essere

massimale, allora $J \subsetneq \mathfrak{m}$ con $\mathfrak{m}$ ideale massimale. Si ha $J\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. Ma $\mathfrak{m}^{-1} \supseteq R$, allora $J \subseteq J\mathfrak{m}^{-1} \subseteq R$ e per la massimalità di J, $J\mathfrak{m}^{-1} \notin \mathscr{F}$. Si può scrivere $J\mathfrak{m}^{-1} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, allora $J = \mathfrak{m} \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, assurdo perché $J \in \mathscr{F}$.

Per l'unicità della fattorizzazione, si suppone $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{s} \mathfrak{q}_i^{f_i}$ e senza perdità di generalità si fissano $e_i \geq 0$ e $f_i \geq 0$, inoltre $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\mathfrak{q}_i \neq \mathfrak{q}_j$ per $i \neq j$ e $\mathfrak{p}_i \neq \mathfrak{q}_j$ per ogni i e j. Se dopo queste semplificazioni rimane almeno un ideale primo a sinistra, si ha $\mathfrak{p}_1 \supseteq \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$, allora $\mathfrak{p}_1$ contiene almeno un $\mathfrak{q}_j$ interamente, ma questo non è possibile. □

Corollario 2.19. *Se R è un dominio di Dedekind e I è un suo ideale frazionario non nullo, allora I è invertibile, cioè l'insieme degli ideali frazionari di R rispetto al prodotto è un gruppo abeliano con R come elemento neutro.*

Dimostrazione. Sia $I = \prod \mathfrak{p}_i^{e_i}$; $J = \prod_{i=1}^{r} \mathfrak{p}_i^{-e_i}$ è ancora un ideale frazionario e $IJ = \prod_{i=1}^{r} \left(\mathfrak{p}_i \mathfrak{p}_i^{-1}\right)^{e_i} = R$. □

Osservazione 2.20. Con la notazione $e_{\mathfrak{p}}(I)$ per l'esponente di $\mathfrak{p}$ nella fattorizzazione di I, si ha:

- $e_{\mathfrak{p}}(IJ) = e_{\mathfrak{p}}(I) + e_{\mathfrak{p}}(J)$;
- I è un ideale intero se e solo se $e_{\mathfrak{p}}(I) \geq 0$ per ogni $\mathfrak{p}$ primo (un verso è ovvio, l'altro deriva dalla dimostrazione del teorema di fattorizzazione unica);
- se $I \subseteq J$, $e_{\mathfrak{p}}(I) \geq e_{\mathfrak{p}}(J)$ (perché $I \subseteq J$ implica $IJ^{-1} \subseteq A$).

Definizione 2.21. Il *gruppo delle classi di ideali di R* con R dominio di Dedekind è, posto $I(R) = \{ I \mid I \text{ ideali frazionario non nulli} \}$ e $P(R) = \{ I \mid I \text{ ideale principale} \}$, $C_K = {}^{I(R)}/_{P(R)}$, con

$$[I] = \{ J \in I(R) \mid (\exists \alpha \in K) \alpha \neq 0, \alpha I = J \}.$$

31.10.2006

Definizione 2.22. Dati $I, J \leq R$ ideali, si scrive $I \mid J$ se esiste $L \leq R$ tale che $J = IL$.

Proposizione 2.23. *Sono equivalenti $I \mid J$ e $I \supseteq J$.*

Dimostrazione. Se $J = IL$, $J = IL \subseteq I$; se $J \subseteq I$ e $I = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$, J deve contenere gli stessi fattori primi con esponenti maggiori o uguali ed eventualmente altri fattori; definendo L come i fattori mancanti, si ha $J = IL$. □

Definizione 2.24. Dati $I, J \leq R$ ideali, si definisce il *massimo comune divisore* di I e J come $\gcd(I, J)$, il più piccolo ideale che contiene I e J, perciò si ha evidentemente $\gcd(I, J) = I + J$. Si definisce il *minimo comune multiplo* di I e J come $\operatorname{lcm}(I, J)$, il più grande ideale che è contenuto in I e in J; chiaramente $\operatorname{lcm}(I, J) = I \cap J$.

Teorema 2.25. *Sia R un dominio di Dedekind, allora R è UFD se e solo se è PID.*

Dimostrazione. Un PID è sempre un UFD; anche non si sapesse, si può dimostrare facilmente con la scomposizione degli ideali in ideali primi: se $\alpha \in R$, $(\alpha) = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ e $\alpha = u \prod_{i=1}^{s} p_i^{e_i}$ con $\mathfrak{p}_i = (p_i)$.

Viceversa, per assurdo si hanno ideali non principali; da questo, si può dimostrare che esiste un ideale primo non principale (ad esempio, un ideale massimale tra gli ideali non principali deve essere primo; in particolare nei domini di Dedekind, se tutti i primi fossero principali, lo sarebbero tutti perché prodotto di ideali primi). Sia quindi $\mathfrak{p}$ un ideale primo non principale e sia $\mathscr{F} = \{ I \leq R \mid \mathfrak{p}I \text{ è principale} \}$; $\mathscr{F} \neq \varnothing$, in quanto si sa esistere $\mathfrak{p}^{-1} \subseteq {}^1\!/_d R$, quindi $d\mathfrak{p}^{-1} \subseteq R$ e $\mathfrak{p}\left(d\mathfrak{p}^{-1}\right) = (d)$ e $d\mathfrak{p}^{-1} \in \mathscr{F}$. Sia $\mathfrak{m}$ un ideale massimale in $\mathscr{F}$, per cui vale $\mathfrak{p}\mathfrak{m} = (\alpha)$ con $\alpha \in R$. Si dirà che α è irriducibile ma non primo, assurdo poiché R è un UFD per ipotesi.

Si dimostra che α è irriducibile: se $\alpha = \beta\gamma$, $(\alpha) = (\beta)(\gamma) = \mathfrak{p}\mathfrak{m}$, allora $(\beta) = \mathfrak{p}J$ con $J \mid \mathfrak{m}$ (cioè esiste un I tale che $IJ = \mathfrak{m}$, equivalentemente $J \supseteq \mathfrak{m}$). Per la massimalità di $\mathfrak{m}$, $J = \mathfrak{m}$ e $(\beta) = \mathfrak{p}\mathfrak{m} = (\alpha)$, quindi $(\gamma) = R$ e γ è invertibile. Però α non è primo perché $(\alpha) = \mathfrak{p}\mathfrak{m}$, assurdo. □

Teorema 2.26. *Dati un ideale $I \leq R$ e $\alpha \in I$ non nullo, esiste $\beta \in I$ tale che $I = (\alpha, \beta)$.*

Dimostrazione. Si suppone $I = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$; poiché $\alpha \in I$, $I \mid (\alpha)$ e $\alpha = I = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i} \prod_{j=1}^{t} \mathfrak{q}_j^{b_j}$ con $a_i \geq e_i$. Si vuole trovare un β tale che $I = (\alpha, \beta) = (\alpha) + (\beta) = \gcd((\alpha), (\beta))$, quindi si deve scegliere β in modo che $\beta \in \mathfrak{p}_i^{e_i}$ ma $\beta \notin \mathfrak{p}_i^{e_i+1}$ per ogni i e $\beta \notin \mathfrak{q}_j$ per ogni j. Sicuramente, per ogni i esiste $\beta_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_1+1}$: la differenza non è vuota perché per il teorema di fattorizzazione unica, avendo fattorizzazioni diverse, sono diversi. Si deve quindi trovare β in modo che $\beta \equiv \beta_i \ (\mathfrak{p}_i^{e_i+1})$ e $\beta \equiv 1 \ (\mathfrak{q}_j)$ per ogni i e j; questo β si può trovare per il teorema cinese del resto, in quanto gli ideali sono coprimi. □

Teorema 2.27. *Siano $F \supseteq K$ anelli di numeri, $\mathfrak{p} \leq \mathscr{O}_K$ e $\mathfrak{q} \leq \mathscr{O}_F$ ideali primi; sono equivalenti $\mathfrak{q} \mid \mathfrak{p}\mathscr{O}_F$; $\mathfrak{q} \supseteq \mathfrak{p}\mathscr{O}_F$; $\mathfrak{q} \supseteq \mathfrak{p}$; $\mathfrak{q} \cap \mathscr{O}_K = \mathfrak{p}$; $\mathfrak{q} \cap K = \mathfrak{p}$.*

Dimostrazione. Ovvio da alcune considerazioni: $\mathfrak{p}$ è massimale; $\mathscr{O}_K \supsetneq \mathfrak{q} \cap \mathscr{O}_K \supseteq \mathfrak{p} \cap \mathscr{O}_K = \mathfrak{p}$; $\mathfrak{q} \cap K = \mathfrak{q} \cap \mathscr{O}_F \cap K = \mathfrak{q} \cap \mathscr{O}_K$. □

Definizione 2.28. Se $\mathfrak{q}$ e $\mathfrak{p}$ soddisfano una delle condizioni del teorema (quindi tutte), si dice che $\mathfrak{q}$ *sta sopra* $\mathfrak{p}$.

Proposizione 2.29. *Ogni ideale primo $\mathfrak{q}$ di $\mathscr{O}_F$ sta sopra ad un unico primo di $\mathscr{O}_K$, $\mathfrak{q} \cap \mathscr{O}_K$; ogni ideale primo $\mathfrak{p}$ di $\mathscr{O}_K$ sta sotto ad almeno un primo di $\mathscr{O}_F$ e precisamente ai primi che compaiono nella fattorizzazione dell'estensione di $\mathfrak{p}$ a $\mathscr{O}_F$, $\mathfrak{p}\mathscr{O}_F$.*

7.11.2006

Dimostrazione. La prima proposizione è evidente. Per la seconda, è sufficiente dimostrare che $\mathfrak{p}\mathscr{O}_F \subsetneq \mathscr{O}_F$. Da $\mathfrak{p}^{-1}(\mathfrak{p}\mathscr{O}_F) \subseteq \mathscr{O}_F$ si deduce che $\left(\mathfrak{p}^{-1}\mathscr{O}_F\right)(\mathfrak{p}\mathscr{O}_F) \subseteq \mathscr{O}_F$ e $\mathfrak{p}^{-1}\mathscr{O}_F \subseteq (\mathfrak{p}\mathscr{O}_F)^{-1}$. Preso $\alpha \in \mathfrak{p}^{-1} \setminus \mathscr{O}_K$, $\alpha \notin \mathscr{O}_F$ e $\alpha(\mathfrak{p}\mathscr{O}_F) \subseteq \mathscr{O}_F$ e quindi $(\mathfrak{p}\mathscr{O}_F)^{-1} \neq \mathscr{O}_F$ perché α ci appartiene. □

Definizione 2.30. Scrivendo $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$ con $\mathfrak{q}_i \subseteq \mathscr{O}_L$ primi, si definisce e_i come l'*indice di ramificazione* si $\mathfrak{q}_i$ in $\mathfrak{p}$.

Si ha per ogni $\mathfrak{q}_i$ che divide $\mathfrak{p}$ l'inclusione ${}^{\mathscr{O}_K}\!/_{\mathfrak{p}} \subseteq {}^{\mathscr{O}_L}\!/_{\mathfrak{q}_i}$ *TODO*

Definizione 2.31. Il *grado d'inerzia* la funzione $f(\mathfrak{q}_i \mid \mathfrak{p}) \coloneqq [{}^{\mathscr{O}_L}\!/_{\mathfrak{q}_i} : {}^{\mathscr{O}_K}\!/_{\mathfrak{p}}]$. Questo grado è finito perché $\mathscr{O}_K$ e $\mathscr{O}_L$ sono campi di numeri, quindi i campi residui

sono campi finiti[1]. Un primo $\mathfrak{p}$ si dice ramificato in L se nella fattorizzazione di $\mathfrak{p}\mathscr{O}_L$ c'è un indice di ramificazione maggiore di 1.

Teorema 2.32. *Sia* $[L:K] = n$, $\mathfrak{p} \subseteq \mathscr{O}_K$ *primo e* $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$. *Allora* $\sum_{i=1}^{s} e_i f_i = n$.

Questo teorema dà una limitazione sulla fattorizzazione. Se $n = 2$, ci sono poche possibilità: $\mathfrak{p}\mathscr{O}_L = \mathfrak{q}$ con $f(\mathfrak{q} \mid \mathfrak{p}) = 2$, $\mathfrak{p}\mathscr{O}_L = \mathfrak{q}^2$ con $f(\mathfrak{q} \mid \mathfrak{p}) = 1$, $\mathfrak{p}\mathscr{O}_L = \mathfrak{q}_1\mathfrak{q}_2$ con $f(\mathfrak{q}_i \mid \mathfrak{p}) = 1$. Allo stesso modo, la casistica per $n = 3$ comprende cinque casi. In genere ovviamente i tipi di fattorizzazioni sono in numero finito per ogni n.

Si può dimostrare che i primi ramificati sono in numero finito e si può studiare in generale la distribuzione dei primi nelle varie tipologie di fattorizzazione.

Teorema 2.33 (Chebotarev)**.** *Sia* $K/\mathbb{Q}$ *un'estensione di grado* n, $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$*; allora la densità dei primi con un certo tipo di fattorizzazione (escludendo quelli ramificati) è* $|G|^{-1} |\{\sigma \in G \mid \sigma \text{ di tipo fissato}\}|$.

Esempio 2.34. Per $n = 2$, $G = S_2$ e $d\{\mathfrak{p} \in \mathbb{Z} \mid \mathfrak{p}\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2\} = 1/2$ e $d\{\mathfrak{p} \in \mathbb{Z} \mid \mathfrak{p}\mathscr{O}_K = \mathfrak{q}\} = 1/2$. Per $n = 3$, si suppone che $G = S_3$; la densità dei primi che si fattorizzano come $\mathfrak{q}$ è pari al numero dei 3-cicli di S_3 diviso la cardinalità di S_3, $1/3$; quelli che si fattorizzano come $\mathfrak{q}_1\mathfrak{q}_2$ è $1/2$; quelli che si fattorizzano come $\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ è $1/6$.

8.11.2006

Proposizione 2.35. *Sia* $[K:\mathbb{Q}] = n$ *e* $x \in \mathscr{O}_K \setminus \{0\}$*, allora* $\left|N_{K/\mathbb{Q}}(x)\right| = |\mathscr{O}_K/x\mathscr{O}_K|$.

Dimostrazione. Si sa che $\mathscr{O}_K$ è uno $\mathbb{Z}$-modulo libero di rango n, ma anche $x\mathscr{O}_K$ lo è; si può considerare l'applicazione $\mu_x \colon \mathscr{O}_K \to x\mathscr{O}_K$, $\mu_x(q) = xq$: questa è un'applicazione iniettiva di $\mathbb{Z}$-moduli, quindi se $(e_1, \dots, e_n)$ è una $\mathbb{Z}$-base di $\mathscr{O}_K$, le loro immagini lo sono per $x\mathscr{O}_K$. Allora $\operatorname{disc} x\mathscr{O}_K = \operatorname{disc}(xe_1, \dots, xe_n) = (\det \mu_x)^2 \operatorname{disc}(e_1, \dots, e_n) = (\det \mu_x)^2 \operatorname{disc} \mathscr{O}_K$, ma $\det \mu_x = N_{K/\mathbb{Q}}(x)$, quindi $\operatorname{disc} x\mathscr{O}_K = \left|N_{K/\mathbb{Q}}(x)\right|^2 \operatorname{disc} \mathscr{O}_K$. Il rapporto tra questi discriminanti si può calcolare anche come l'indice di sottogruppo al quadrato, in quanto $x\mathscr{O}_K \subseteq \mathscr{O}_K$ sono $\mathbb{Z}$-moduli di rango n, quindi $\left|N_{K/\mathbb{Q}}(x)\right|^2 = [\mathscr{O}_K : x\mathscr{O}_K]^2$. □

Osservazione 2.36. Per ogni $I \subseteq \mathscr{O}_K$, $I \neq (0)$, si ha $|\mathscr{O}_K/I| < \infty$, perché se $I \neq (0)$, esiste $x \neq 0$ in I tale che $x\mathscr{O}_K \subseteq I \subseteq \mathscr{O}_K$, quindi I è uno $\mathbb{Z}$-modulo di rango n.

Definizione 2.37. Si definisce la *norma* di I come $N(I) \coloneqq |\mathscr{O}_K/I|$. Per la proposizione si ha $N(x\mathscr{O}_K) = \left|N_{K/\mathbb{Q}}(x)\right|$.

Proposizione 2.38. *Siano* $I, J \subseteq \mathscr{O}_K$ *ideali non nulli, allora* $N(IJ) = N(I)N(J)$.

Dimostrazione. Si deve dimostrare $|\mathscr{O}_K/IJ| = |\mathscr{O}_K/I|\,|\mathscr{O}_K/J|$. Se I e J sono coprimi, si conclude facilmente per il teorema cinese: $\mathscr{O}_K/IJ \cong \mathscr{O}_K/I \times \mathscr{O}_K/J$. Basta quindi dimostrare che $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$, grazie alla fattorizzazione unica degli ideali: se $I = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i}$, $J = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i}$, $N(IJ) = \prod N\left(\mathfrak{p}_i^{a_i+b_i}\right) = \prod N(\mathfrak{p}_i)^{a_i+b_i} = N(I)N(J)$.

[1] Questa ipotesi è fondamentale ed è richiesta in qualsiasi estensione della teoria.

Per definizione, $N(\mathfrak{p}^m) = |\mathscr{O}_K/\mathfrak{p}^m|$. Considerando la filtrazione $\mathscr{O}_K \supseteq \mathfrak{p} \supseteq \ldots \supseteq \mathfrak{p}^m$, $N(\mathfrak{p}^m) = \prod_{i=0}^{m-1} \left|\frac{\mathfrak{p}^i}{\mathfrak{p}^{i+1}}\right|$; per avere l'uguaglianza con $N(\mathfrak{p})^m$, è sufficiente mostrare che $\left|\frac{\mathfrak{p}^i}{\mathfrak{p}^{i+1}}\right| = |\mathscr{O}_K/\mathfrak{p}|$.

Sia $\mu_\alpha \colon \mathscr{O}_K \to \frac{\mathfrak{p}^i}{\mathfrak{p}^{i+1}}$ con $\mu_\alpha(x) = \alpha x + \mathfrak{p}^{i+1}$ con $\alpha \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ (che esiste sempre perché vale la fattorizzazione unica degli ideali). Si ha $(\alpha) \subseteq \mathfrak{p}^i$, quindi nella fattorizzazione di (α) c'è $\mathfrak{p}^i$, ma non c'è $\mathfrak{p}^{i+1}$: $(\alpha) = \mathfrak{p}^i I$ con $(I, \mathfrak{p}) = \mathscr{O}_K$. Ora, $\ker \mu_\alpha = \left\{ x \in \mathscr{O}_K \mid \alpha x \in \mathfrak{p}^{i+1} \right\} = \mathfrak{p}$. L'immagine di μ_α è $\left\{ \alpha x + \mathfrak{p}^{i+1} \mid x \in \mathscr{O}_K \right\} = \alpha\mathscr{O}_K + \mathfrak{p}^{i+1} = \mathfrak{p}^i I + \mathfrak{p}^{i+1} = \mathfrak{p}^i (I + \mathfrak{p}) = \mathfrak{p}^i \mathscr{O}_K = \mathfrak{p}^i$. Per il primo teorema d'isomorfismo, si ha $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathscr{O}_K/\mathfrak{p}$ e in particolare le cardinalità sono uguali. □

Osservazione 2.39. Se si prende un ideale primo $\mathfrak{p} \subseteq \mathscr{O}_K$, la norma di $\mathfrak{p}$ è $|\mathscr{O}_K/\mathfrak{p}|$ è $p^{f(\mathfrak{p}|p)}$ dove $p = \mathfrak{p} \cap \mathbb{Z}$. Questo perché $f(\mathfrak{p} \mid p) = [\mathscr{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Se $\mathfrak{p} \subseteq \mathscr{O}_K$ sta sotto $\mathfrak{q} \subseteq \mathscr{O}_L$, si ha $N(\mathfrak{q}) = |\mathscr{O}_L/\mathfrak{q}| = |\mathscr{O}_K/\mathfrak{p}|^{f(\mathfrak{q}|\mathfrak{p})}$.

Teorema 2.40. *Sia* $[L : K] = n$, $\mathfrak{p} \subseteq \mathscr{O}_K$, $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$, $f_i = f(\mathfrak{q}_i \mid \mathfrak{p})$, *allora* $n = \sum_{i=1}^r f_i e_i$.

Dimostrazione. Sia prima $K = \mathbb{Q}$. Allora

$$N(p\mathscr{O}_L) = \prod_{i=1}^r N(\mathfrak{q}_i)^{e_i} = \prod_{i=1}^r p^{f_i e_i} = p^{\sum_{i=1}^r f_i e_i}.$$

Nel caso generale, $N(\mathfrak{p}\mathscr{O}_L) = \prod_{i=1}^r N(\mathfrak{q}_i)^{e_i} = \prod_{i=1}^r |\mathscr{O}_K/\mathfrak{p}|^{f_i e_i} = |\mathscr{O}_K/\mathfrak{p}|^{\sum f_i e_i}$; per concludere allo stesso modo si deve mostrare che $N(\mathfrak{p}\mathscr{O}_L) = |\mathscr{O}_K/\mathfrak{p}|^n$, ma questo è dato dalla proposizione seguente. □

Proposizione 2.41. *Sia* $I \subseteq \mathscr{O}_K$, *allora* $N(I\mathscr{O}_L) = N(I)^{[L:K]}$.

Dimostrazione. È sufficiente dimostrarlo per $I = \mathfrak{p}$ primo e usare la moltiplicatività. Si vuole dimostrare che $|\mathscr{O}_L/\mathfrak{p}\mathscr{O}_L| = |\mathscr{O}_K/\mathfrak{p}|^n$. Si ha che $\mathscr{O}_L/\mathfrak{p}\mathscr{O}_L$ è un $\mathscr{O}_K/\mathfrak{p}$-spazio vettoriale, sia d la sua dimensione.

Si dimostra che $d \leq n$: se $\alpha_1, \ldots, \alpha_{n+1} \in \mathscr{O}_L$, allora le loro classi sono linearmente dipendenti su $\mathscr{O}_K/\mathfrak{p}$: infatti, gli α_i sono dipendenti su $\mathscr{O}_K$, quindi esistono $b_1, \ldots, b_{n+1} \in \mathscr{O}_K$ tali che $\sum_{i=1}^{n+1} b_i \alpha_i = 0$ con i b_i non tutti nulli. Mandando al quoziente, $\sum_{i=1}^{n+1} \bar{b}_i \bar{\alpha}_i = 0$ ed è una relazione di dipendenza lineare se e solo se i b_i non sono tutti nulli, cioè se esiste i tale che $b_i \notin \mathfrak{p}$. Se questo non fosse vero, $B = (b_1, \ldots, b_{n+1}) \subseteq \mathfrak{p}$, B è un ideale proprio in $\mathscr{O}_K$ quindi è invertibile e $B^{-1} \supseteq \mathscr{O}_K$, $BB^{-1} = \mathscr{O}_K$ ed esisterebbe $\beta \in B^{-1} \setminus \mathscr{O}_K$ tale che $\beta B \subseteq \mathscr{O}_K$ e $\beta B \nsubseteq \mathfrak{p}$. Ma $\beta B = (\beta b_1, \ldots, \beta b_{n+1}) \nsubseteq \mathfrak{p}$ quindi i βb_i sono dei coefficienti per una relazione di dipendenza lineare che passa al quoziente.

Si dimostra che $d \geq n$: si ha $[L : K] = n$, $[K : \mathbb{Q}] = m$, l'ideale $\mathfrak{p}$ in $\mathscr{O}_K$ passa a $\mathbb{Q}$ come $p = \mathfrak{p} \cap \mathbb{Z}$ con $p\mathscr{O}_K = \prod_{i=1}^s \mathfrak{p}_i^{\varepsilon_i}$ (quindi $m = \sum_{i=1}^s f(\mathfrak{p}_i \mid p)\varepsilon_i$); inoltre $p\mathscr{O}_L = \prod_{i=1}^s (\mathfrak{p}_i \mathscr{O}_L)^{\varepsilon_i}$. Allora $p^{nm} = N_{L/\mathbb{Q}}(p) = N(p\mathscr{O}_L) = \prod_{i=1}^s N(\mathfrak{p}_i\mathscr{O}_L)^{\varepsilon_i}$ e $N(\mathfrak{p}_i\mathscr{O}_L) = N(\mathfrak{p}_i)^{n_i}$ con $n_i \leq n$. Quindi $p^{nm} = \prod_{i=1}^s N(\mathfrak{p}_i)^{n_i\varepsilon_i} = \prod_{i=1}^s p^{f(\mathfrak{p}_i|p)n_i\varepsilon_i} = p^{\sum_{i=1}^s f(\mathfrak{p}_i|p)\varepsilon_i n_i}$. D'altra parte, $p^{nm} = p^{n\sum_{i=1}^s f(\mathfrak{p}_i|p)\varepsilon_i}$, quindi gli esponenti devono essere uguali e per la condizione $n_i \leq n$ deve essere $n_i = n$ per ogni i. □

Osservazione 2.42. Sia $K \subseteq L \subseteq M$, $\mathfrak{p} \subseteq K$, $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$, $\mathfrak{q}_i\mathscr{O}_M = \beta_{i,1}^{\varepsilon_{i,1}} \dots \beta_{i,s}^{\varepsilon_{i,s}}$. Allora se $\beta \mid \mathfrak{q}$ e $\mathfrak{q} \mid \mathfrak{p}$, $f(\beta \mid p) = f(\beta \mid \mathfrak{q}) f(\mathfrak{q} \mid \mathfrak{p})$ e $e(\beta \mid p) = e(\beta \mid \mathfrak{q}) e(\mathfrak{q} \mid \mathfrak{p})$. La prima osservazione segue dal teorema della torre su $\mathscr{O}_K/\mathfrak{p}$, $\mathscr{O}_L/\mathfrak{q}$ e $\mathscr{O}_M/\beta$; per la seconda basta sostituire una fattorizzazione dentro l'altra.

3 Teorema di Kummer

In questo contesto di separabilità, un'estensione è normale se e solo se è di Galois, il modello è un'estensione L/K con $G = \mathrm{Gal}(L/K)$ e $\mathfrak{p} \subseteq \mathscr{O}_K$.

Proposizione 3.1. *Il gruppo di Galois G agisce transitivamente sull'insieme dei primi di L sopra $\mathfrak{p}$.*

Dimostrazione. Si può scrivere $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$; si deve dimostrare che G agisce su $\mathfrak{q}_1, \dots, \mathfrak{q}_r$: questo è semplice perché se $\mathfrak{q} \mid \mathfrak{p}$, allora $\sigma\mathfrak{q} \mid \sigma\mathfrak{p}$, ma $\sigma\mathfrak{p} = \mathfrak{p}$ perché $\mathfrak{p} \subseteq \mathscr{O}_K$, quindi $\sigma\mathfrak{q}$ deve essere ancora sopra $\mathfrak{p}$.

Inoltre l'azione è transitiva: siano $\mathfrak{q}_1, \mathfrak{q}_2$ sopra $\mathfrak{p}$, si pone per assurdo $\sigma\mathfrak{q}_1 \neq \mathfrak{q}_2$ per ogni $\sigma \in G$. Allora si può trovare $\alpha \in \mathscr{O}_L$ tale che $\alpha \equiv 0 \ (\mathfrak{q}_2)$ e $\alpha \equiv 1 \ (\sigma\mathfrak{q}_1)$ per ogni σ, per il teorema cinese del resto. Allora $\alpha \in \mathfrak{q}_2$ e $N(\alpha) = \prod \sigma(\alpha) \notin \mathfrak{q}_1$ perché $\sigma(\alpha) \notin \mathfrak{q}_1$. Ma la norma di α sta in $\mathfrak{q}_2 \cap \mathscr{O}_K = \mathfrak{p} \subseteq \mathfrak{q}_1$, assurdo. □

Corollario 3.2. *Se L/K è di Galois, $\mathfrak{p} \subseteq \mathscr{O}_K$ ideale primo, allora $\mathfrak{p}\mathscr{O}_L = \left(\prod_{i=1}^{r} \mathfrak{q}_i\right)^e$ con $f(\mathfrak{q}_i \mid \mathfrak{p}) = f$ e $ref = [L : K]$.*

Dimostrazione. Si ha $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$, ma $\mathfrak{p}\mathscr{O}_L = \sigma\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{s} (\sigma\mathfrak{q}_i)^{e_i}$; poiché l'azione di G è transitiva, gli esponenti devono essere tutti uguali. L'azione del gruppo di Galois si restringe all'anello degli interi: si può restringere σ a $\sigma\colon \mathscr{O}_L \to \mathscr{O}_L$ e si può scrivere:

$$\begin{array}{ccc} \mathscr{O}_L & \xrightarrow{\sigma} & \mathscr{O}_L \\ \pi \downarrow & & \downarrow \pi \\ \frac{\mathscr{O}_L}{\mathfrak{q}_i} & \xrightarrow{\bar{\sigma}} & \frac{\mathscr{O}_L}{\mathfrak{q}_i}. \end{array}$$

□

Definizione 3.3. Sia L/K estenzione, $\mathfrak{p} \subseteq \mathscr{O}_K$, $\mathfrak{q} \subseteq \mathscr{O}_L$; si dice che:

- $\mathfrak{p}$ è *ramificato* in L se esiste $\mathfrak{q} \subseteq \mathscr{O}_L$ tale che $\mathfrak{q}^2 \mid \mathfrak{p}$ (oppure che $\mathfrak{q}$ è ramificato sopra $\mathfrak{p}$);
- $\mathfrak{p}$ è *inerte* in L se $\mathfrak{p}\mathscr{O}_L$ è primo;
- $\mathfrak{p}$ si *spezza completamente* in L se $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{n} \mathfrak{q}_i$ con $n = [L : K]$ (in particolare, $f(\mathfrak{q}_i \mid \mathfrak{p}) = 1$).

Teorema 3.4. *Sia $p \in \mathbb{Z}$ un numero intero primo, K un campo di numeri, allora p è ramificato in K se e solo se $p \mid \mathrm{disc}\, K$.*

Dimostrazione. Si dimostrerà solo la prima inclusione: sia p ramificato in K cioè tale che esiste $\mathfrak{p} \subseteq \mathscr{O}_K$ con $e(\mathfrak{p} \mid p) > 1$, allora $p\mathscr{O}_K = \mathfrak{p}I$ con $\mathfrak{p}' \mid I$ per ogni $\mathfrak{p}'$ tale che $\mathfrak{p}' \mid \mathfrak{p}$. Siano $\sigma_1, \dots, \sigma_n$ le immersioni di K in $\bar{\mathbb{Q}}$ e $\alpha_1, \dots, \alpha_n$ una $\mathbb{Z}$-base di $\mathscr{O}_K$, allora $\mathrm{disc}(\alpha_1, \dots, \alpha_n) = \mathrm{disc}\, K$.

Sia $\alpha \in I \setminus p\mathscr{O}_K$ (esiste per la fattorizzazione unica); allora per ogni $\mathfrak{p}' \mid p\mathscr{O}_K$, $\alpha \in \mathfrak{p}'$, ma $\alpha \notin p\mathscr{O}_K$; sulla base, $\alpha = \sum_{i=1}^{n} m_i\alpha_i \notin p\mathscr{O}_K$, cioè non tutti gli m_i sono multipli di p. Si suppone che $p \nmid m_1$, allora $\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) = (\det A)^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ dove A è la matrice del cambio di coordinate, che si mostra essere m_1^2, che non è multiplo di p, cioè p divide $\operatorname{disc} K$ se e solo se p divide $\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$.

Sia L la chiusura normale di K su $\mathbb{Q}$ e sia $\mathfrak{q} \subseteq \mathscr{O}_L$ un primo sopra p. Per definizione di α, $\alpha \in \mathfrak{q}$. Inoltre, per ogni $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$, $\sigma(\alpha) \in \mathfrak{q}$, perché $\alpha \in \sigma^{-1}(\mathfrak{q})$ che è vero perché G agisce sui primi sopra $\mathfrak{p}$; questo è quindi vero in particolare per ogni σ_i e $\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{q}$, ma sta anche in $\mathbb{Z}$, quindi $\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) \in (p)$. □

14.11.2006

Corollario 3.5. *Se $K = \mathbb{Q}(\alpha)$, α intero, allora se $p \nmid \operatorname{disc}(\alpha)$, p non è ramificato, se $p \mid \operatorname{disc}(\alpha)$ ma $p^2 \nmid \operatorname{disc}(\alpha)$, si ha che $p \mid \operatorname{disc}(K)$ e p è ramificato.*

I primi di $\mathbb{Z}$ ramificati in K sono in numero finito.

Teorema 3.6 (Kummer)**.** *Siano $K \subseteq F$ campi di numeri, $F = K(\alpha)$ con α intero, $\mathscr{O}_F(\alpha) \subseteq \mathscr{O}_F$, $\mu_\alpha(x) \in \mathscr{O}_K[x]$ il polinomio minimo di α. Preso un ideale primo $\mathfrak{p} \subseteq \mathscr{O}_K$, sia $p = \mathfrak{p} \cap \mathbb{Z}$ il primo che sta sotto $\mathfrak{p}$; se si suppone che $p \nmid \left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha]}\right|$, sia $\bar{\mu_\alpha}(x) = \prod_{i=1}^{r} \bar{\mu_i}^{e_i} \in \mathscr{O}_K/\mathfrak{p}[x]$, allora $\mathfrak{p}\mathscr{O}_F = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ e $f(\mathfrak{q}_i \mid \mathfrak{p}) = \deg \bar{\mu_i}$ e $\mathfrak{q}_i = (\mathfrak{p}, \mu_i(\alpha))$, dove μ_i è un qualsiasi sollevamento monico in $\mathscr{O}_K[x]$ di $\bar{\mu_i}$.*

In particolare, usando μ_α si possono fattorizzare tutti i $\mathfrak{p}\mathscr{O}_F$ eccetto un numero finito.

Dimostrazione. Per brevità, si pone $f_i = \deg \bar{\mu_i}$ e dati $\mathfrak{q}_i = (\mathfrak{p}, \mu_i(\alpha))$ si dimostra che:

- per ogni i, $\mathfrak{q}_i = \mathscr{O}_F$ oppure $\mathscr{O}_F/\mathfrak{q}_i$ è un campo con $[\mathscr{O}_F/\mathfrak{q}_i : \mathscr{O}_K/\mathfrak{p}] = f_i$;
- per ogni i, j, $\mathfrak{q}_i + \mathfrak{q}_j = \mathscr{O}_F$;
- $\mathfrak{p}\mathscr{O}_F \mid \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$.

Da questi tre fatti segue la tesi: si può supporre senza perdità di generalità che $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ siano ideali primi e che $\mathfrak{q}_{s+1}, \ldots, \mathfrak{q}_r = \mathscr{O}_F$; inoltre gli ideali primi sono distinti perché $\mathfrak{q}_i + \mathfrak{q}_j = \mathscr{O}_F$. Per il terzo punto, $\mathfrak{p}\mathscr{O}_F \mid \prod_{i=1}^{r} \mathfrak{q}_i^{e_i} = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}$, cioè $\mathfrak{p}\mathscr{O}_F = \prod_{i=1}^{s} \mathfrak{q}_i^{d_i}$ con $0 \le d_i \le e_i$; allora $n = \sum_{i=1}^{s} f_i d_i$, dove n è il grado dell'estensione. Ma allora n è anche il grado del polinomio minimo μ_α, allora $n = \sum_{i=1}^{r} f_i e_i$ e questo è possibile se e solo se $s = r$ e $d_i = e_i$ per ogni $i \in \{1, \ldots, r\}$.

Si dimostrano i tre fatti.

- Si osserva che $\frac{\mathscr{O}_K[x]}{(\mathfrak{p}, \mu_i(x))} \cong \frac{\mathscr{O}_K/\mathfrak{p}[x]}{(\bar{\mu_i}(x))} =: F_i$, per il primo teorema d'isomorfismo a partire dall'applicazione $\varphi(f) = \bar{f} + (\bar{\mu_i}(x))$ che ha kernel uguale a $(\mathfrak{p}, \mu_i(x))$. Chiaramente, $[F_i : \mathscr{O}_K/\mathfrak{p}] = f_i$ (si sta quozientando l'anello dei polinomi per un polinomio di grado f_i), allora si considera l'applicazione $\psi\colon \mathscr{O}_K[x] \to \mathscr{O}_F \to \mathscr{O}_F/\mathfrak{q}_i$ che manda x in α e poi in $\alpha + \mathfrak{q}_i$. Si ha $\ker\psi \supseteq (\mathfrak{p}, \mu_i(x))$, ma questo è un ideale massimale perché F_i è un campo, quindi $\ker\psi = (\mathfrak{p}, \mu_i(x))$ o $\ker\psi = \mathscr{O}_K[x]$: se $\ker\psi = \mathscr{O}_K[x]$, $\mathfrak{q}_i = \mathscr{O}_F$, altrimenti se $\ker\psi = (\mathfrak{p}, \mu_i(x))$, $\mathfrak{q}_i$ è primo e $\mathscr{O}_F/\mathfrak{q}_i \cong F_i$. Rimane da dimostrare che ψ è suriettivo: la proiezione è suriettiva ma il primo passaggio no (si ha

solo $\mathscr{O}_K[\alpha] \subseteq \mathscr{O}_F$): ψ è suriettivo se e solo ogni elemento di $\mathscr{O}_F/\mathfrak{q}_i$ ha un rappresentante in $\mathscr{O}_K[\alpha]$ cioè se e solo se $\mathscr{O}_K[\alpha] + \mathfrak{q}_i = \mathscr{O}_F$; si dimostrerà una cosa più forte: che $\mathscr{O}_F = \mathscr{O}_K[\alpha] + p\mathscr{O}_F$: infatti, $p\mathscr{O}_F \subseteq \mathscr{O}_K[\alpha] + p\mathscr{O}_F \subseteq \mathscr{O}_F$, quindi $p^{[F:\mathbb{Q}]} = |\mathscr{O}_F/p\mathscr{O}_F|$, ma $p \nmid |\mathscr{O}_F/\mathscr{O}_K[\alpha]|$, perciò

$$\left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha] + p\mathscr{O}_F}\right| \mid \gcd\left(\left|\frac{\mathscr{O}_F}{p\mathscr{O}_F}\right|, \left|\frac{\mathscr{O}_F}{\mathscr{O}_K[\alpha]}\right|\right) = 1.$$

- Si osserva che $\bar{\mu_i}$ e $\bar{\mu_j}$ sono coprimi in $\mathscr{O}_K/\mathfrak{p}[x]$ perché sono fattori irriducibili distinti di una fattorizzazione, allora esistono $\bar{a}(x), \bar{b}(x) \in \mathscr{O}_K/\mathfrak{p}[x]$ tali che $\bar{a}(x)\bar{\mu_i}(x) + \bar{b}(x)\bar{\mu_j}(x) = 1$, cioè che $1 - (a(x)\mu_i(x) + b(x)\mu_j(x)) \in \mathfrak{p}\mathscr{O}_K[x]$. Valutato in α, si ottiene che $a(\alpha)\mu_i(\alpha) + b(\alpha)\mu_j(\alpha) \in 1 + \mathfrak{p}\mathscr{O}_K[\alpha] \subseteq 1 + \mathfrak{p}\mathscr{O}_F$. Da questo segue che $\mathfrak{q}_i + \mathfrak{q}_j = (\mathfrak{p}, \mu_i(\alpha), \mu_j(\alpha)) = (1)$.

- Si sa che $(\mathfrak{p}, \prod_{i=1}^r \mu_i^{e_i}(\alpha)) \mid \prod_{i=1}^r \mathfrak{q}_i^{e_i}$, cioè $\prod_{i=1}^r \mathfrak{q}_i^{e_i} = \prod_{i=1}^r (\mathfrak{p}, \mu_i(\alpha))^{e_i} \subseteq (\mathfrak{p}, \prod_{i=1}^r \mu_i^{e_i}(\alpha))$. È sufficiente dimostrare che questo ideale è uguale a $\mathfrak{p}\mathscr{O}_F$: un contenimento è banale ($\mathfrak{p}\mathscr{O}_F \subseteq (\mathfrak{p}, \prod_{i=1}^r \mu_i^{e_i}(\alpha))$), per l'altra si considera $\mu(x) - \prod_{i=1}^r \mu_i^{e_i}(x) \in \mathfrak{p}\mathscr{O}_K[x]$ che valutato in α dà $0 - \prod_{i=1}^r \mu_i^{e_i}(\alpha) \in \mathfrak{p}\mathscr{O}_K[\alpha] \subseteq \mathfrak{p}\mathscr{O}_F$. □

15.11.2006

Esempio 3.7. Nel caso delle estensioni quadratiche $K = \mathbb{Q}(\sqrt{m})$, $\mathscr{O}_K$ è monogenico (generato da un solo elemento): $\mathscr{O}_K = \mathbb{Z}[\sqrt{m}]$ se $m \equiv 2, 3 \ (4)$ e in questo caso $\operatorname{disc} \mathscr{O}_K = 4m$, oppure $\mathscr{O}_K = \mathbb{Z}[1/2(1 + \sqrt{m})]$ se $m \equiv 1 \ (4)$ e $\operatorname{disc} \mathscr{O}_K = m$. Posto $\alpha = \sqrt{m}$, si ha $\mathbb{Z}[\sqrt{m}] \subseteq \mathscr{O}_K$ con indice 2, quindi α serve per fattorizzare tutti i primi tranne 2.

Se $p \mid m$ (anche 2), $p\mathscr{O}_K = (p, \sqrt{m})^2$ per il teorema di Kummer. In effetti, $\sqrt{m} = \sqrt{p}\sqrt{n}$ con $\gcd(n, p) = 1$ e $p \mid N(\sqrt{m}) = m$; quindi $(\sqrt{m}) = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ e poiché la norma è moltiplicativa, deve esistere qualche primo tra i $\mathfrak{p}_i$ deve stare sopra p, ad esempio $\mathfrak{p}_1$; inoltre poiché m è libero da quadrati, $p^2 \nmid m$ e quindi $\varepsilon_1 e_1 = 1$ dove ε_1 è il grado d'inerzia. Quindi facendo $(p, \sqrt{m})$ si stanno prendendo i fattori comuni che sono esattamente $\mathfrak{p}_1$.

Se invece $p \nmid m$ e $p \neq 2$, si può ancora usare $\alpha = \sqrt{m}$ e il polinomio $x^2 - m = (x - n)(x + n)$ se $m \equiv n^2 \ (p)$, altrimenti se $m \not\equiv n^2 \ (p)$, $x^2 - m$ è irriducibile. Nel primo caso, $p\mathscr{O}_K = (p, \sqrt{m} - n)(p, \sqrt{m} + n)$, altrimenti $p\mathscr{O}_K$ è già primo (è inerte).

L'ultimo caso è $p = 2$ e m dispari: $x^2 - m = x^2 - 1 = (x - 1)^2 \ (2)$ e si hanno ancora due casi: se $m \equiv 3 \ (4)$ si può usare Kummer e $2\mathscr{O}_K = (2, \sqrt{m} - 1)^2$; se $m \equiv 1 \ (4)$, si usa $\beta = \frac{1}{2}(1 + \sqrt{m})$ con $\mu_\beta = x^2 - x + \frac{1}{4}(1 - m)$; se $m \equiv 1 \ (8)$, il termine noto è pari e $\mu_\beta(x) = x(x - 1) \ (2)$ e $2\mathscr{O}_K = \left(2, \frac{1}{2}(1 + \sqrt{m})\right)\left(2, \frac{1}{2}(\sqrt{m} - 1)\right)$; se $m \equiv 5 \ (8)$, $\mu_\beta(x) = x^2 + x + 1$ che è irriducibile e quindi $2\mathscr{O}_K$ non si scompone.

Esempio 3.8. Sia $K_m = \mathbb{Q}(\zeta_m)$, $m = p^k n$ con $\gcd(p, n) = 1$. Poiché $\operatorname{disc} K_m \mid m^t$, p è ramificato se e solo se $p \mid m$. Inoltre si sa che $\mathscr{O}_{K_m} = \mathbb{Z}[\zeta_m]$, quindi si può sempre usare μ_m, il polinomio minimo di ζ_m, per fattorizzare $p\mathscr{O}_{K_m}$.

Se $m = p^k$, allora $\mu_{p^k} \mid x^{p^k} - 1$ cioè $x^{p^j} = Q(x)\mu_{p^k}(x) = (x - 1)^{p^k} \ (p)$, perciò $\mu_{p^k}(x) = (x - 1)^{\varphi(p^k)} \ (p)$. Quindi $p\mathscr{O}_{K_{p^k}} = (p, \zeta_{p^k} - 1)^{\varphi(p^k)} = (\zeta_{p^k} - 1)^{\varphi(p^k)}$.

Se $m = n$, $\gcd(p, n) = 1$; allora $\mu_n(x) = \prod_{\gcd(i,n)=1}(x - \zeta_i)$ che modulo p si fattorizza come $\prod_{i=1}^r \bar{\mu_i}$ con grado $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p]$ (le estensioni dei vari ζ_i sono tutte uguali quindi i gradi sono uguali, inoltre non ci sono fattori comuni

perché il polinomio minimo divide $x^n - 1$ che non ha radici distinte). Allora $p\mathscr{O}_{K_n} = \prod_{i=1}^{r} \mathfrak{p}_i$ con $rf = \varphi(n)$, dove $f = \operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}^\star}[p]$.

Nel caso generale, $m = p^k n$, si ha $x^m - 1 = (x^n - 1)^{p^k}\ (p)$. Allora $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$; se si parte da $p \in \mathbb{Q}$, si ha $p\mathscr{O}_{K_{p^k}} = \mathfrak{p}^{\varphi(p^k)}$ e $p\mathscr{O}_{K_n} = \prod_{i=1}^{r} \mathfrak{q}_i$ con $f(\mathfrak{q}_i \mid p) = f$ e $rf = \varphi(n)$. Ora, se $p\mathscr{O}_{K_m}$ *TODO*

In conclusione, $p\mathscr{O}_{K_m} = (\prod_{i=1}^{r})^{\varphi(p^k)}$ con $f(\mathfrak{p}_i \mid p) = \operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}^\star}[p]$ e $rf = \varphi(m)$.

Esempio 3.9 (di Dedekind). Sia $K = \mathbb{Q}(\alpha)$ con $\mu_\alpha = x^3 - x^2 - 2x - 8$ (non ha radici, quindi è irriducibile). Si osserva che $\mathbb{Z}[\alpha] \subsetneq \mathscr{O}_K$, perché $\operatorname{disc}\alpha = N(\mu'_\alpha(\alpha)) = -4 \cdot 503$, quindi l'indice o è 1 o è 2; ma posto $\beta = \frac{1}{2}(\alpha^2 + \alpha)$, $1, \alpha, \beta$ sono interi, sono una base di ${}^{K}/_{\mathbb{Q}}$ come $1, \alpha, \alpha^2$ e si osserva che

$$\operatorname{disc}(1, \alpha, \beta) = \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}^2 \operatorname{disc}\alpha = -503.$$

Perciò $1, \alpha, \beta$ è una base intera di $\mathscr{O}_K$ e $\xi = a + b\alpha + c\beta$ descrive tutti gli elementi di $\mathscr{O}_K$ al variare di $a, b, c \in \mathbb{Z}$.

Si vuole dimostrare che 2 divide l'indice di ξ per ogni $\xi = a + b\alpha + c\beta$; si ha

$$\det \begin{pmatrix} 1 & a & a^2 + 6c^2 + 8bc \\ 0 & b & 2c^2 - b^2 + 2ab \\ 0 & c & 2b^2 + 3c^2 + 2ac + 4bc \end{pmatrix} = bc^2 + cb^2 - cb(c + b) = 0 \quad (2).$$

Quindi $2\mathscr{O}_K$ non si può fattorizzare tramite Kummer.

Questo avviene quando si hanno troppi primi che stanno sopra un certo primo; ad esempio si può dimostrare che $2\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

4 Gruppo di decomposizione e gruppo d'inerzia

Sia ${}^{L}/_{K}$ estensione di Galois, $G = \operatorname{Gal}({}^{L}/_{K})$, $\mathfrak{p}$ primo in $\mathscr{O}_K$ e $\mathfrak{q}$ primo di $\mathscr{O}_L$ sopra $\mathfrak{p}$. Si definisce il *gruppo di decomposizione* di $\mathfrak{q}$ su $\mathfrak{p}$ il sottogruppo $D(\mathfrak{q} \mid \mathfrak{p}) \coloneqq \{\, \sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q} \,\}$: non è altro che lo stabilizzatore di $\mathfrak{q}$ rispetto all'azione di G sui primi sopra $\mathfrak{p}$; si definisce anche il *gruppo d'inerzia* di $\mathfrak{q}$ su $\mathfrak{p}$ come il sottogruppo $E(\mathfrak{q} \mid \mathfrak{p}) = \{\, \sigma \in G \mid (\forall \alpha \in \mathscr{O}_L)\sigma(\alpha) = \alpha\ (\mathfrak{q}) \,\}$. In particolare, $\{e\} \leq E \leq D \leq G$.

Gli elementi del gruppo di Galois mandano elementi interi in elementi interi, quindi da $\sigma\colon L \to L$ si ricava $\sigma\colon \mathscr{O}_L \to \mathscr{O}_L$:

$$\begin{array}{ccc} \mathscr{O}_L & \xrightarrow{\sigma} & \mathscr{O}_L \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \frac{\mathscr{O}_L}{\mathfrak{q}} & \xrightarrow{\bar{\sigma}} & \frac{\mathscr{O}_L}{\mathfrak{q}}, \end{array}$$

il diagramma commuta, quindi per ogni $\sigma \in D(\mathfrak{q} \mid \mathfrak{p})$, $\bar{\sigma} \in \bar{G} = \operatorname{Gal}({}^{\mathscr{O}_L}/_{\mathfrak{q}}, {}^{\mathscr{O}_K}/_{\mathfrak{p}})$, cioè esiste un'applicazione $\varphi\colon D \to G$ il cui nucleo è $\ker\varphi = \{\, \sigma \in D \mid \bar{\sigma} = \mathrm{Id} \,\} = \{\, \sigma \in D \mid \bar{\sigma}\,(\bar{\alpha}) = \bar{\alpha} \,\} = E(\mathfrak{q} \mid \mathfrak{p})$ e si ha un isomorfismo ${}^{D}/_{E} \to \bar{G}$.

Si considerano il *campo di decomposizione* L_D e il *campo d'inerzia* L_E; si ha $K = L_G \leq L_D \leq L_E \leq L$ con anelli degli interi rispettivamente $\mathscr{O}_K \subseteq \mathscr{O}_D \subseteq$

$\mathscr{O}_E \subseteq \mathscr{O}_L$. Contraendo $\mathfrak{q}$ a $\mathscr{O}_E$ e $\mathscr{O}_D$ si ottendono altri due primi $\mathfrak{q}_E$ e $\mathfrak{q}_D$ che stanno sopra $\mathfrak{p}$.

Teorema 4.1. *Sia $[L:K] = efr$; allora si ha $[L:L_E] = e$, $[L_E:L_D] = f$, $[L_D:K] = r$; queste estensioni non sono necessariamente normali perché in generale D e E non sono in generale sottogruppi normali. Si hanno inoltre i gradi d'inerzia rispettivamente* 1, f, 1 *e gli indici di ramificazione* e, 1, 1.

Dimostrazione. Si dimostra per prima cosa $[L_D:K] = r$: il grado dell'estensione è uguale a $[G:D]$ e G agisce transitivamente sui primi sopra $\mathfrak{p}$, quindi ogni orbita ha r elementi (r è il numero dei primi sopra $\mathfrak{p}$); inoltre $D = \operatorname{Stab}\mathfrak{q}$, quindi $[G:D] = r$.

Si dimostra che $e(\mathfrak{q}_D \mid \mathfrak{p}) = f(\mathfrak{q}_D \mid \mathfrak{p}) = 1$, dimostrando che $e(\mathfrak{q} \mid \mathfrak{q}_D) = e$ e $f(\mathfrak{q} \mid \mathfrak{q}_D) = f$. Si sa che $\mathrm{Gal}(L/L_D) = D$ e il numero dei primi sopra $\mathfrak{q}_D$ è pari a $|\{\sigma\mathfrak{q} \mid \sigma \in D\}| = 1$: $\mathfrak{q}$ è l'unico primo di $\mathscr{O}_L$ sopra $\mathfrak{q}_D$. Allora $ef = [L:L_D] = f(\mathfrak{q} \mid \mathfrak{q}_D)\, e(\mathfrak{q} \mid \mathfrak{q}_D)$, quindi $e = e(\mathfrak{q} \mid \mathfrak{q}_D)$ e $f = f(\mathfrak{q} \mid \mathfrak{q}_D)$.

Si dimostra che $f(\mathfrak{q} \mid \mathfrak{q}_E) = 1$: per definizione, è $[\mathscr{O}_L/\mathfrak{q} : \mathscr{O}_E/\mathfrak{q}_E]$: sia $\alpha \in \mathscr{O}_L$, $\bar{\alpha} \in \mathscr{O}_L/\mathfrak{q}$ e sia $g(x) = \prod_{\sigma\in E}(x - \sigma(\alpha))$ il suo polinomio minimo, che appartiene a $\mathscr{O}_E[x]$ perché α è intero. Allora $\bar{g}(x) = \prod_{\sigma\in E}(x - \bar{\sigma}(\bar{\alpha})) = (x-\bar{\alpha})^{|E|}$ e il polinomio minimo di $\bar{\alpha}$ su $\mathscr{O}_E/\mathfrak{q}_E$ è $x - \bar{\alpha}$, $\bar{\alpha} \in \mathscr{O}_E/\mathfrak{q}_E$ e l'estensione ha dimensione 1. Poiché il grado d'inerzia è moltiplicativo, si ottiene anche $f(\mathfrak{q}_E \mid \mathfrak{q}_D) = f$.

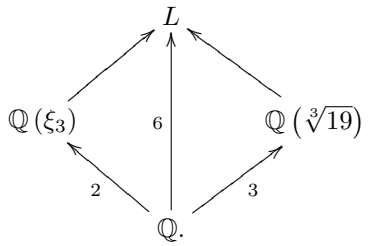
Si è dimostrato anche che $[L_E:L_D] = |D/E| \leq f = \left|\bar{G}\right|$, d'altra parte $f(\mathfrak{q}_E \mid \mathfrak{q}_D) = f$ si ha $[L_E:L_D] = f$, cioè $D/E \cong \bar{G}$, il che implica $e(\mathfrak{q}_E \mid \mathfrak{q}_D) = 1$ (ancora si trova che c'è un unico primo sopra $\mathfrak{q}_D$). Con queste si completa la dimostrazione perché l'indice e i gradi sono moltiplicativi. □

21.11.2006

Grazie al teorema si ha quindi che $\mathfrak{q}$ è l'unico primo di $\mathscr{O}_L$ sopra $\mathfrak{q}_D$; che $\mathfrak{q}_D$ è non ramificato su $\mathfrak{p}$ e $f(\mathfrak{q}_D \mid \mathfrak{p}) = 1$; che $\mathfrak{q}_E$ è totalmente ramificato in $\mathscr{O}_L$ (cioè $\mathfrak{q}_E\mathscr{O}_L = \mathfrak{q}^e$) e non ramificato su $\mathfrak{p}$.

In generale, L_D/K non è normale, quindi non è detto che ogni primo che sta sopra $\mathfrak{p}$ sia non ramificato su $\mathfrak{p}$ con grado d'inerzia 1.

Esempio 4.2. Siano $f = x^3 - 19$, $L = \mathbb{Q}\left(\sqrt[3]{19}, \xi_3\right)$, $G = S_3$, $K = \mathbb{Q}\left(\sqrt[3]{19}\right)$ e $\mathfrak{p} = 3$. Si sa che $3\mathbb{Z}[\xi_3] = \mathfrak{p}^2$, inoltre $3\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$:



Quindi $3\mathscr{O}_L = (\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)^2$. Dalla teoria di Galois si sa che $|D/E| = 1$ e $|E| = 2$, quindi $L_D = L_E$; i sottocampi di grado 3 sono $\mathbb{Q}\left(\sqrt[3]{19}\right)$, $\mathbb{Q}\left(\xi_3\sqrt[3]{19}\right)$ e $\mathbb{Q}\left(\xi_3^2\sqrt[3]{19}\right)$ e in tutti questi campi 3 si spezza come $\mathfrak{p}_1\mathfrak{p}_2^2$.

Corollario 4.3. *Se D è sottogruppo normale di G, $\mathfrak{p}$ si spezza in r primi distinti in L_D e se inoltre E è sottogruppo normale di G, allora ogni primo di $\mathscr{O}_D$ sopra $\mathfrak{p}$ rimane inerte in $\mathscr{O}_E$; inoltre, ogni primo di L_E diventa una potenza e-esima (è totalmente ramificato) in L.*

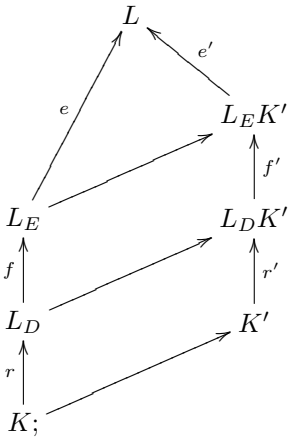
In più: siano $\mathfrak{q} \subseteq \mathscr{O}_L$, $\mathfrak{p} \subseteq \mathscr{O}_K$ con $\mathfrak{q} \mid \mathfrak{p}$, $\sigma \in G$, allora $D(\sigma\mathfrak{q} \mid \mathfrak{p}) = \sigma D(\mathfrak{q} \mid \mathfrak{p})\sigma^{-1}$ (se D è normale, il coniugio non lo cambia). Questo in particolare avviene se e solo se L_D è campo di decomposizione per ogni primo che sta sopra $\mathfrak{p}$ e se e solo se tutti hanno $e = f = 1$ (se L_D è campo di decomposizione di tutti i primi sopra $\mathfrak{p}$, devono avere per forza $e = f = 1$ per il teorema, l'altra freccia si dimostrerà nel prossimo teorema) se e solo se $\mathfrak{p}\mathscr{O}_D$ è prodotto di r primi distinti (perché vale la formula dimensionale).

Se $K \subseteq K' \subseteq L$, allora $K' = L_H$ con $H \subseteq G$; se $\mathfrak{p} \subseteq \mathscr{O}_K$ e $\mathfrak{q} \subseteq \mathscr{O}_L$, allora la contrazione di $\mathfrak{q}$ in $\mathscr{O}_{L_H}$ si indica con $\mathfrak{p}'$ e si ha $D(\mathfrak{q} \mid \mathfrak{p}) \cap H = D(\mathfrak{q} \mid \mathfrak{p}')$ e lo stesso per E. Inoltre $L_{D(\mathfrak{q}|\mathfrak{p}')} = L_{D\cap H} = L_D L_H = L_D K'$.

Teorema 4.4. *Con le notazioni precedenti:*

- *L_D è il più grande K' tale che $K \subseteq K' \subseteq L$ e $e(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{p}' \mid \mathfrak{p}) = 1$;*
- *L_D è il più piccolo K' tale che $K \subseteq K' \subseteq L$ e $\mathfrak{q}$ è l'unico primo di L sopra $\mathfrak{p}'$;*
- *L_E è il più grande K' tale che $K \subseteq K' \subseteq L$ e $e(\mathfrak{p}' \mid \mathfrak{p}) = 1$;*
- *L_E è il più piccolo K' tale che $K \subseteq K' \subseteq L$ e $\mathfrak{q}$ è totalmente ramificato su $\mathfrak{p}'$.*

Dimostrazione. Si ha:



Se K' verifica la seconda, $r' = 1$ perché r' conta i primi che tanno sopra $\mathfrak{p}'$, quindi $K' = L_D K'$ e $L_D \subseteq K'$.

Se K' verifica la prima (rispettivamente, la terza), $e = e'$ e $f = f'$, quindi $L_D = L_D K'$ ($L_E = L_E K'$) e $K' \subseteq L_D$ ($K' \subseteq L_E$).

Se K' soddisfa la quarta, allora $f' = r' = 1$ quindi $L_E K' = K'$ e $L_E \subseteq K'$. □

Corollario 4.5. *Se D è normale, allora $\mathfrak{p}$ si spezza completamente in K' se e solo se $K' \subseteq L_D$; $\mathfrak{p}$ è non ramificato in K' se e solo se $K' \subseteq L_E$.*

Teorema 4.6. *Siano L/K e M/K estensioni qualsiasi; se $\mathfrak{p} \subseteq \mathscr{O}_K$ è non ramificato (rispettivamente si spezza completamente) sia in L che in M allora $\mathfrak{p}$ è non ramificato (si spezza completamente) in LM.*

Dimostrazione. Sia F/K estensione di Galois che contiene LM; siano $\mathfrak{p}' \subseteq \mathscr{O}_{LM}$ con $\mathfrak{p}' \mid \mathfrak{p}$ e $\mathfrak{q} \subseteq \mathscr{O}_F$ con $\mathfrak{q} \mid \mathfrak{p}$ e $E = E(\mathfrak{q} \mid \mathfrak{p})$. Allora F_E deve contenere sia L che M inoltre $F_E \supseteq LM$. □

Corollario 4.7. *Sia L/K estensione qualsiasi e $\mathfrak{p} \subseteq \mathscr{O}_K$ non ramificato (si spezza completamente) in L, allora $\mathfrak{p}$ è non ramificato (si spezza completamente) in $\tilde{L}$ con $\tilde{L}$ chiusura di Galois di L/K.*

22.11.2006

Si considera ξ_p e $\mathrm{Gal}\left(\mathbb{Q}(\xi_p)/\mathbb{Q}\right) \cong \mathbb{Z}_p^\star \cong \mathbb{Z}_{p-1}$. Si sa che per ogni $d \mid p-1$, esiste un unico sottocampo $\mathbb{F}_d$ di grado d su $\mathbb{Q}$ e si ha:

$$\begin{array}{c} \mathbb{Q}(\xi_p) \\ \Big\uparrow {\scriptstyle \frac{p-1}{d}} \\ \mathbb{F}_d \\ \Big\uparrow {\scriptstyle d} \\ \mathbb{Q}. \end{array}$$

Se si prende $q \neq p$, q è non ramificato e $q\mathbb{Z}[\xi_p] = \mathfrak{p}_1 \dots \mathfrak{p}_r$ con $fr = p-1$.

Teorema 4.8. *Siano $p \neq 2$, $q \neq p$ primi e $d \mid p-1$; si ha che q è una potenza d-esima modulo p se e solo se q si spezza completamente in $\mathbb{F}_d$.*

Dimostrazione. Si osserva che $\mathbb{Z}_p^\star$ è ciclico generato da x e al suo interno c'è un unico sottogruppo di indice d: se $H_d = \langle x^d \rangle$, $|H_d| = {}^{p-1}/_d$, ma allora $H_d = \left\{ a \in \mathbb{Z}_p^\star \mid \mathrm{ord}\, a \mid {}^{p-1}/_d \right\}$. Si ha che q è una potenza d-esima se e solo se $q \in H_d$ se e solo se $\mathrm{ord}\, \bar{q} \mid {}^{p-1}/_d$, ma l'ordine moltiplicativo di q è il grado d'inerzia f, che a sua volta è ${}^{p-1}/_r$. Quindi q è potenza d-esima se e solo se $d \mid r$ se e solo se $\mathbb{F}_d \subseteq \mathbb{F}_r$ se e solo se q si spezza completamente nel suo campo di decomposizione $\mathbb{F}_d$ (in quanto il gruppo di Galois è abeliano). □

Definizione 4.9. Siano $p \neq 2$ primo, n intero tale che $p \nmid n$. Il *simbolo di Legendre* si definisce come $\left(\frac{n}{p}\right) = 1$ se n è un quadrato modulo p, $\left(\frac{n}{p}\right) = -1$ se n non è un quadrato modulo p.

Teorema 4.10 (legge di reciprocità quadratica)**.** *Si ha $\left(\frac{2}{p}\right) = 1$ se $p \equiv \pm 1$ (8), $\left(\frac{2}{p}\right) = -1$ se $p \equiv \pm 3$ (8); $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ se $p \equiv 1$ (4) o $q \equiv 1$ (4), $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ se $p \equiv q \equiv 3$ (4).*

Dimostrazione. Si ha $\left(\frac{q}{p}\right) = 1$ se e solo se q si spezza completamente in $\mathbb{F}_2$. Il primo caso è $q = 2$: se $p \equiv 1$ (4), $\mathbb{F}_2 = \mathbb{Q}\left(\sqrt{p}\right)$ e bisogna vedere come si spezza 2 in $\mathbb{Q}\left(\sqrt{p}\right) = K$; può essere $2\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ (se $p \equiv 1$ (8)) o $2\mathscr{O}_K = \mathfrak{p}$ (se $p \equiv 5$ (8)). Se $p \equiv 3$ (4), $K = \mathbb{Q}(\sqrt{-p})$ e può essere $2\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ (se $p \equiv 3$ (8)), $2\mathscr{O}_K = \mathfrak{p}$ (se $p \equiv 7$ (8)).

Nel caso $q \neq 2$ e $p \equiv 1$ (4), $K = \mathbb{Q}\left(\sqrt{p}\right)$ allora $q\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, cioè si spezza completamente, se e solo se p è un quadrato modulo q se e solo se $\left(\frac{p}{q}\right) = 1$. Se $p \equiv 3$ (4), $K = \mathbb{Q}(\sqrt{-p})$ allora $q\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ se e solo se $-p$ è un quadrato modulo q, quindi se $q \equiv 1$ (4) questo avviene se e solo se p è un quadrato e

$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, invece se $q \equiv 3$ (4) avviene se esolo se p non è un quadrato modulo q e $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. □

5 Automorfismo di Frobenius

Sia $^L/_K$ un'estensione normale e $\mathfrak{p} \leq \mathscr{O}_K$ non ramificato in L (questo toglie un numero finito di primi, in quanto sono in particolare primi di L che stanno sopra $\mathfrak{q}$); siano $E(\mathfrak{q} \mid \mathfrak{p}) = \{e\}$ per ogni $\mathfrak{q} \mid \mathfrak{p}$ e $D(\mathfrak{q} \mid \mathfrak{p}) \cong G = \mathrm{Gal}\left(\frac{\mathscr{O}_L/\mathfrak{q}}{\mathscr{O}_K/\mathfrak{p}}\right) = \left\langle x \to x^{\|\mathfrak{p}\|} \right\rangle$. Quindi in D c'è un unico elemento che va a finire nel morfismo di Frobenius che genera il gruppo di Galois; questo viene chiamato l'automorfismo di Frobenius e si indica con $\varphi(\mathfrak{q} \mid \mathfrak{p}) \in D$ (è tale che $\varphi(\alpha) \equiv \alpha^{\|\mathfrak{p}\|}$ $(\mathfrak{q})$ per ogni $\alpha \in \mathscr{O}_L$). In realtà, $\varphi(\mathfrak{q} \mid \mathfrak{p})$ è unico in G, perché un oggetto di questo tipo deve necessariamente stare nel gruppo di decomposizione. Si verifica facilmente che se $\sigma\mathfrak{q}$ è un altro primo sopra $\mathfrak{p}$, allora $\varphi(\sigma\mathfrak{q} \mid \mathfrak{p}) = \sigma\varphi(\mathfrak{q} \mid \mathfrak{p})\sigma^{-1}$: il primo sopra determina l'automorfismo di Frobenius all'interno della classe di coniugio fissata dal primo sotto. In particolare, se G è abeliano, $\varphi(\alpha) = \alpha^{\|\mathfrak{p}\|}$ $(\sigma\mathfrak{q})$ per ogni $\sigma \in G$, allora $\varphi(\alpha) = \alpha^{\|\mathfrak{p}\|}$ $(\mathfrak{p}\mathscr{O}_L)$.

Esempio 5.1. Nel caso delle estensioni quadratiche $K = \mathbb{Q}(\sqrt{m})$, $G = \mathbb{Z}_2$. Poiché G è abeliano si può parlare del Frobenius di p: se $p\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, il Frobenius è 1, se $p\mathscr{O}_L = \mathfrak{p}$, allora il Frobenius è -1. Nel primo caso m è un quadrato modulo p, altrimenti no.

Nel caso dei campi ciclotomici, $K = \mathbb{Q}(\xi_m)$ e sia p un primo non ramificato (cioè che non divide m). Di nuovo il gruppo di Galois è abeliano ($G = \mathbb{Z}_m^\star = \left\{ \sigma_i \mid \sigma_i(\xi) = \xi^i \right\}$) e ci si può chiedere chi è il Frobenius di $\mathfrak{q} \mid p$: si trova $\varphi(\mathfrak{q} \mid p) = \sigma_p$; basta verificare che soddisfa l'equazione, in quanto ne esiste uno solo. Si deve dimostrare che $\varphi(\alpha) \equiv \alpha^p$ $(p\mathscr{O}_K)$ per ogni $\alpha \in \mathscr{O}_K$ (cioè $\alpha = \sum_{\substack{i=0 \\ (i,m)=1}}^{m-1} x_i\xi_i$): infatti, $\varphi(\alpha) \equiv \sum x_i\varphi(\xi)^i \equiv \sum x_i\xi^{ip} \equiv \left(\sum x_i\xi^i\right)^p$ (p).

La domanda interessante è capire per un certo elemento del gruppo di Galois, quali sono i primi che lo hanno come Frobenius. Se G è abeliano, si definisce l'applicazione di Artin $\mathscr{P} = \{ p \leq \mathscr{O}_K \mid p \text{ primo non ramificato} \} \to G$ e si dimostra che la preimmagine di ogni elemento di G è infinita. Nel caso particolare delle estensioni ciclotomiche, la cardinalità dell'insieme $\{ p \mid \sigma_p = \sigma \}$ è infinita, cioè è infinito l'insieme $\{ p \mid p \equiv i \ (m) \}$ è infinito (si è ottenuta un'estensione del teorema di Dirichlet sui primi nelle progressioni aritmetiche).

Siano ora $^L/_K$ un'estensione qualsiasi, non necessariamente normale, $^M/_L$ un'estensione con $^M/_K$ di Galois (ad esempio, la chiusura di Galois) e sia $\mathfrak{p} \leq \mathscr{O}_K$ un primo non ramificato in M (se M è la chiusura di Galois, basta che $\mathfrak{p}$ non sia ramificato in L). Siano $G = \mathrm{Gal}(^M/_K)$, $H \leq G$ con $M_H = L$ sia $\mathfrak{q} \leq \mathscr{O}_L$ sopra $\mathfrak{p}$ e $\mathfrak{u} \leq \mathscr{O}_M$ sopra $\mathfrak{p}$ e $\mathfrak{q}$, $\varphi = \varphi(\mathfrak{u} \mid \mathfrak{p})$ e $D(\mathfrak{u} \mid \mathfrak{p}) = \langle\varphi\rangle$. L'insieme delle classi laterali $\{ H_\sigma \mid \sigma \in G \}$ ha cardinalità $[G : H] = [L : K] = n$; si considera l'azione di D sulle classi laterali (quindi $D \to S_n$) definita da $\varphi H_\sigma \coloneqq H_{\sigma\varphi}$: l'orbita di H_σ sarà $\left\{H_\sigma, \dots H_{\sigma\varphi^{m-1}}\right\}$.

Teorema 5.2. *Sia $m_1 + \cdots + m_r = n$ il tipo della permutazione determinata dall'azione di φ su S_n, allora $\mathfrak{p}\mathscr{O}_L = \mathfrak{q}_1 \dots \mathfrak{q}_r$ con $f(\mathfrak{q}_i \mid \mathfrak{p}) = m_i$; inoltre, se le orbite sono $\left\{H_{\sigma_i}, \dots, H_{\sigma_i\varphi^{m_i-1}}\right\}$, allora $\sigma_i\mathfrak{u} \cap \mathscr{O}_L = \mathfrak{q}_i$.*

Dimostrazione. Intanto, $\sigma_i U$ è ben definito in quanto φ^k è contenuto nello stabilizzatore di $\mathfrak{u}$, quindi $\sigma_i \varphi^k \mathfrak{u} = \sigma_i \mathfrak{u}$. Si pongono $\mathfrak{q}_i = \sigma_i \mathfrak{u} \cap \mathscr{O}_L$: sono primi perché contrazioni di ideali primi e stanno sopra $\mathfrak{p}$; inoltre $\mathfrak{q}_i \neq \mathfrak{q}_j$ per ogni $i \neq j$: se fossero uguali, $\sigma_i \mathfrak{u}$ e $\sigma_j \mathfrak{u}$ starebbero entrambi sopra $\mathfrak{q}_i$, allora possono essere mandati l'uno nell'altro mediante un elemento di H: esiste $\tau \in H$ tale che $\tau \sigma_i \mathfrak{u} = \sigma_j \mathfrak{u}$, cioè $\sigma_j^{-1} \tau \sigma_i \in D(\mathfrak{u} \mid \mathfrak{q}_i) \subseteq D(\mathfrak{u} \mid \mathfrak{p}) = \langle \varphi \rangle$, allora $\tau \sigma_i = \sigma_j \varphi^k$ e $H_{\sigma_i} = H_{\sigma_j \varphi^k}$, ma questo non è possibile perché i due elementi stanno in orbite diverse.

Si sono individuati r primi distinti sopra $\mathfrak{p}$; grazie alla formula dimensionale, se si dimostra che $f(\mathfrak{q}_i \mid \mathfrak{p}) \geq m_i$ si conclude. Sia quindi $\mathfrak{q} = \mathfrak{q}_i$ e si vuole dimostrare che $m = m_i \mid f(\mathfrak{q} \mid \mathfrak{p})$ o equivalentemente che $H_{\sigma \varphi^f} = H_\sigma$, cioè che $\sigma \varphi^f \sigma^{-1} \in H$. Si osserva che $H \ni \varphi(\sigma \mathfrak{u} \mid \mathfrak{q}) = \varphi(\sigma \mathfrak{u} \mid \mathfrak{p})^f$, perché $\|\mathfrak{p}\|^f = \|\mathfrak{q}\|$. D'altra parte, $\varphi(\sigma \mathfrak{u} \mid \mathfrak{p})^f = \left(\sigma \varphi(\mathfrak{u} \mid \mathfrak{p}) \sigma^{-1}\right)^f = \sigma \varphi^f \sigma^{-1}$ che quindi appartiene ad H, per ogni $\sigma \in H$. □

Esercizio 5.3. Siano L/K un'estensione di Galois di gruppo G e $\mathfrak{p} \leq \mathscr{O}_K$.

- Se $\mathfrak{p}$ è inerte in L, allora G è ciclico: questo perché se $\mathfrak{p}$ è inerte, $L = L_E$ e $L_D = K$, in quanto $r = e = 1$; inoltre $\mathrm{Gal}(L_E/L_D)$ è ciclico, quindi anche G è ciclico.

- Se $\mathfrak{p}$ è totalmente ramificato in ogni estensione intermedia ma non in L, allora $G \cong \mathbb{Z}_p$: infatti, $\mathfrak{p}$ non può essere totalemente ramificato in L_E, che quindi deve essere L o K. Se $L_E = L$, non ci possono essere estensioni intermedie quindi il Galois non può avere sottogruppi.

TODO
28.11.2006

Teorema 5.4. *Sia K un campo di numeri, $p \in \mathbb{Z}$ primo, allora $p \mid \operatorname{disc} K$ se e solo se p è ramificato in K.*

Dimostrazione. Si è già mostrata la seconda implicazione. Per l'altra, si ha $\operatorname{disc} K = \left|\mathrm{Tr}(\alpha_i \alpha_j)_{i,j}\right|$ con $(\alpha_1, \ldots, \alpha_n)$ una base intera. Il fatto che $p \mid \operatorname{disc} K$ implica che esistono $m_1, \ldots, m_n \in \mathbb{Z}$ non tutti divisibili per p tali che $p \mid \sum_{i=1}^n m_i \mathrm{Tr}(\alpha_i \alpha_j)$ per ogni j. Sia $\alpha = \sum_{i=1}^n m_i \alpha_i$; $\alpha \in \mathscr{O}_K$ perché è combinazione a coefficienti interi di elementi interi, ma $\alpha \notin p\mathscr{O}_K$ perché la scrittura sulla base è unica e gli elementi di $p\mathscr{O}_K$ hanno coefficienti tutti multipli di p. Per la linearità della traccia si ha che $p \mid \mathrm{Tr}(\alpha \alpha_j)$ per ogni j, da cui si ha che $\mathrm{Tr}(\alpha \mathscr{O}_K) \subseteq p\mathbb{Z}$.

Per assurdo, si suppone che p non sia ramificato in $\mathscr{O}_K$, quindi $p\mathscr{O}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ e esiste $\mathfrak{p} \mid p$ tale che $\alpha \notin \mathfrak{p}$ (se fosse stato ramificato non si sarebbe potuto fare questa ipotesi). Sia $L = \tilde{K}$, quindi p è non ramificato in $\mathscr{O}_L$ e per ogni $\mathfrak{q} \leq \mathscr{O}_L$ con $\mathfrak{q} \mid \mathfrak{p}$, si ha $\alpha \notin \mathfrak{q}$, perché $\alpha \in \mathscr{O}_K \setminus \mathfrak{p}$ e $\mathfrak{q} \cap \mathscr{O}_K = \mathfrak{p}$. Ora, $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha \mathscr{O}_L) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{Tr}_{L/K}(\alpha \mathscr{O}_L)\right) \subseteq \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \mathscr{O}_K) \subseteq p\mathbb{Z}$. Sia $\beta \in \mathscr{O}_L \setminus \mathfrak{q}$ con $\beta \in \mathfrak{q}'$ per ogni $\mathfrak{q}' \mid p$. Per ogni $\gamma \in \mathscr{O}_L$, vale che $\mathrm{Tr}_{L/\mathbb{Q}} \alpha\beta\gamma \in \mathbb{Q}$ perché $\beta\gamma \in \mathscr{O}_L$ quindi la traccia appartiene a $p\mathbb{Z} \subseteq \mathbb{Q}$; inoltre $\sigma(\alpha\beta\gamma) \in \mathfrak{q}$ per ogni $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus D(\mathfrak{q} \mid p)$, perché per questi σ si ha $\sigma^{-1}\mathfrak{q} \neq \mathfrak{q}$ e $\alpha\beta\gamma \in \sigma^{-1}\mathfrak{q} \neq \mathfrak{q}$.

Si ha $\mathfrak{q} \ni \mathrm{Tr}(\alpha\beta\gamma) = \sum_{\sigma \in G} \sigma(\alpha\beta\gamma) = \sum_{\sigma \in D} \sigma(\alpha\beta\gamma) + \sum_{\sigma \in G \setminus D} \sigma(\alpha\beta\gamma)$ e quest'ultimo addendo appartiene a $\mathfrak{q}$, quindi anche $\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) \in \mathfrak{q}$. Si ha inoltre che

$$D \cong \bar{G} = \mathrm{Gal}\left(\frac{\mathscr{O}_L/\mathfrak{q}}{\mathbb{Z}/p\mathbb{Z}}\right)$$

e per ogni $\gamma \in \mathscr{O}_L$, $\sum_{\bar{\sigma}\in\bar{G}} \bar{\sigma}(\alpha\beta\gamma) = 0$; inoltre $\alpha, \beta \notin \mathfrak{q}$, cioè non sono nulli in $\mathscr{O}_L/\mathfrak{q}$. Allora $\sum_{\bar{\sigma}\in\bar{G}} \bar{\sigma}$ è il morfismo nullo, ma questo è assurdo per l'indipendenza dei caratteri. □

6 Gruppo delle classi di ideali

Le cose che si diranno valgono per i campi di numeri e non per domini di Dedekind in generale. Si ha quindi K un campo di numeri con $[K:\mathbb{Q}] = n$; si considera $\mathscr{F}(K)$ il gruppo degli ideali frazionari non nulli (il gruppo libero generato dagli ideali primi), $\mathscr{P}(K)$ il gruppo degli ideali principali di K e $[(K)] = \mathscr{F}(K)/\mathscr{P}(K)$ il gruppo delle classi di ideali. Si dimostrerà che questo è un gruppo finito.

Teorema 6.1. *Se K è un campo di numeri, allora esiste una costante $\lambda = \lambda(K) \in \mathbb{R}$ tale che per ogni $I \leq \mathscr{O}_K$ esiste $\alpha \in I$, $\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq \lambda N(I)$.*

Dimostrazione. Siano $(\alpha_1, \dots, \alpha_n)$ una base intera di $\mathscr{O}_K$ e $\sigma_1, \dots, \sigma_n \colon K \to \bar{\mathbb{Q}}$ le immersioni; si definisce λ come $\prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)|$. Ora, si fissa m in modo che $m^n \leq N(I) \leq (m+1)^n$ e si considerano gli elementi $\sum_{j=1}^n m_j\alpha_j$ con $0 \leq m_j \leq m$: questi non possono essere distinti in $\mathscr{O}_K/I$ perché questo ha $N(I)$ elementi, quindi esiste $\alpha \in I$ non nullo tale che $\alpha = \sum_{j=1}^n m_j\alpha_j$ con $|m_j| \leq m$. Allora

$$|N(\alpha)| = \prod_{i=1}^n |\sigma_i(\alpha)| = \prod_{i=1}^n \left|\sum_{j=1}^n m_j\sigma_i(\alpha_j)\right| \leq$$
$$\leq \prod_{i=1}^n \sum_{j=1}^n |m_j|\,|\sigma_i(\alpha_j)| \leq m^k \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)| \leq \lambda N(I). \qquad \square$$

Corollario 6.2. *Ogni classe di ideali contiene un ideale intero J con $N(J) \leq \lambda$.*

Dimostrazione. Innanzitutto, poiché le classi sono definite a meno di moltiplicazioni per ideali principali, ogni classe contiene almeno un ideale intero. Sia C una classe di ideali e sia $I \in C^{-1}$ un ideale intero. Per il teorema, esiste $\alpha \in I$ tale che $|N(\alpha)| \leq \lambda N(I)$. Inoltre $(\alpha) \subseteq I$ implica $J = (\alpha)I^{-1} \subseteq \mathscr{O}_K$; $J \in C$ perché se I è un rappresentante di C^{-1}, I^{-1} è un rappresentante di C ed è intero. Ora, $(\alpha) = JI$ quindi $|N(\alpha)| = N(J)\,N(I) \leq \lambda N(I)$, perciò $N(J) \leq \lambda$. □

Teorema 6.3. *Se K è un campo di numeri, il gruppo delle classi di ideali è finito.*

Dimostrazione. Basta dimostrare che gli ideali interi J come nel corollario sono finiti. Se un ideale J deve avere norma limitata e $J = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$, allora $N(J) = \prod_{i=1}^r N(\mathfrak{p}_i)^{a_i}$, ma $N(\mathfrak{p}_i)$ è il primo che sta sotto elevato al grado d'inerzia e in particolare se $p_i = \mathfrak{p}_i \cap \mathbb{Z}$ deve essere $p_i \leq \lambda$, quindi i primi p_i (perciò anche i $\mathfrak{p}_i$) sono in numero finito, e gli esponenti sono limitati. □

29.11.2006

Definizione 6.4. Un sottogruppo $H \leq \mathbb{R}^n$ si dice *discreto*[2] se per ogni $K \leq \mathbb{R}^n$ compatto, $|H \cap K| < \infty$.

[2] Samuel, "Theorie algebrique des nombres".

Esempio 6.5. Sottoinsiemi discreti di $\mathbb{R}^n$ sono $\mathbb{Z}^k$ con $k \leq n$, o più in generale $\langle v_1, \dots, v_k \rangle_{\mathbb{Z}}$ con $v_1, \dots, v_k$ linearmente indipendenti.

Teorema 6.6. *Un sottoinsieme discreto H di $\mathbb{R}^n$ è generato come $\mathbb{Z}$-modulo da $r \leq n$ vettori linearmente indipendenti su $\mathbb{R}$.*

Dimostrazione. Siano $e_1, \dots, e_r$ un insieme di elementi linearmente indipendenti di H con r massimale rispetto a questa proprietà; l'insieme $P = \{ \sum_{i=1}^r a_i e_i \mid 0 \leq a_i \leq 1 \}$ è compatto, quindi $|P \cap H| < \infty$. Se $x \in H$, $x = \sum_{i=1}^r \lambda_i e_i$ con $\lambda_i \in \mathbb{R}$. Per ogni $j \in \mathbb{Z}$, sia $x_j = jx - \sum_{i=1}^r [j\lambda_i]\, e_i = \sum_{i=1}^r (j\lambda_i - [j\lambda_i])\, e_i \in H \cap P$. Ora, per ogni $x \in H$, $x = x_1 + \sum_{i=1}^r [\lambda_i]\, e_i \in P \cap H$, quindi H è generato su $\mathbb{Z}$ da $P \cap H$, perciò è uno $\mathbb{Z}$-modulo finitamente generato da e_i e x_j.

D'altra parte, poiché $x_j \in P \cap H$, esistono j e k tali che $x_j = x_k$ che avviene se e solo se $(j-k)\,\lambda_i = [j\lambda_i] - [k\lambda_i]$ per ogni i: in particolare si ottiene che $\lambda_i \in \mathbb{Q}$, perché il secondo membro è intero. Sia d un denominatore comune di tutti i coefficienti di x_i rispetto a e_i: $H \subseteq {}^1\!/_d \bigoplus_{i=1}^r \mathbb{Z}$ e si ha $dH \subseteq \bigoplus_{i=1}^r e_i\mathbb{Z} \subseteq H$; ma $\bigoplus_{i=1}^r e_i\mathbb{Z}$ è libero di rango r, allora dH è libero di rango minore o uguale a r; ma allora anche H è uno $\mathbb{Z}$-modulo libero di rango maggiore o uguale a r. In definitiva, H è libero e ha rango r. □

Definizione 6.7. Un *reticolo* Λ di $\mathbb{R}^n$ è un sottogruppo discreto di rango n. Se $\langle e_1, \dots, e_n \rangle_{\mathbb{Z}} = \Lambda$ è un reticolo (quindi $e_1, \dots, e_n$ sono linearmente indipendenti); il *dominio fondamentale* di Λ è $P_{\underline{e}} = \{ \sum_{i=1}^n a_i e_i \mid 0 \leq a_i < 1 \}$.

Lemma 6.8. *Sia μ la misura di Lebesgue su $\mathbb{R}^n$; $\mu\left(P_{\underline{e}}\right)$ non dipende dalla base scelta, ma solo da Λ; in particolare, $\mu\left(P_{\underline{e}}\right) =: V(\Lambda)$, il* volume *di Λ.*

Dimostrazione. Se $v_1, \dots, v_n$ è un'altra $\mathbb{Z}$-base di Λ, la matrice del cambiamento di variabile può avere determinante ± 1, quindi $\mu\left(P_{\underline{e}}\right) = |\det A|\, \mu\left(P_{\underline{v}}\right)$. □

Teorema 6.9 (Minkowski)**.** *Sia Λ un reticolo di $\mathbb{R}^n$, $S \subseteq \mathbb{R}^n$ un sottoinsieme integrabile e tale che $\mu(S) > V(\Lambda)$. Allora, esistono $x, y \in S$ distinti tali che $x - y \in \Lambda$*

Dimostrazione. Sia $e_1, \dots, e_n$ una base di Λ, allora $S = \bigcup_{\lambda \in \Lambda} S \cap \left(\lambda + P_{\underline{e}}\right)$ sarà un'unione disgiunta, quindi $\mu(S) = \sum_{\lambda \in \Lambda} \mu\left(S \cap \left(\lambda + P_{\underline{e}}\right)\right) = \sum_{\lambda \in \Lambda} \mu\left((-\lambda + S) \cap P_{\underline{e}}\right)$ perché la misura di Lebesgue è invariante per traslazione. Ma $V(\Lambda) < \mu(S)$, quindi esistono $\lambda_1, \lambda_2 \in \Lambda$ tali che $(-\lambda_1 + S) \cap (-\lambda_2 + S) \cap P_{\underline{e}} \neq \varnothing$ e $x + \lambda_1, x + \lambda_2 \in S$, perciò $(x + \lambda_1) - (x + \lambda_2) \in \Lambda$. □

Corollario 6.10. *Sia Λ un reticolo di $\mathbb{R}^n$ e S un sottoinsieme misurabile, convesso e simmetrico rispetto all'origine; se $\mu(S) > 2^n V(\Lambda)$ o S è compatto e $\mu(S) \geq 2^n V(\Lambda)$, allora $S \cap \Lambda$ contiene un elemento diverso da 0.*

Dimostrazione. Per la prima condizione si applica il teorema a $S' = {}^1\!/_2 S$: esistono $x, y \in S$ tali che $x - y \in \Lambda \setminus \{0\}$. Allora $x - y = {}^1\!/_2\,(2x - 2y)$, ma $2x, 2y \in S = 2S'$ e per la convessità e la simmetria $x - y \in S$. Nel secondo caso, si definisce $S'_m = (1 + {}^1\!/_m)\, S$ e si trova una successione di punti per il primo caso che converge ad un punto che deve stare in S per la compattezza. □

Siano K un campo di numeri, $n = [K : \mathbb{Q}]$ e $\sigma_1, \dots, \sigma_n \colon K \to \mathbb{C}$ le estensioni. Siano $\sigma_1, \dots, \sigma_r$ le eventuali estensioni reali, cioè $\sigma_1, \dots, \sigma_r \colon K \to \mathbb{R}$; le altre si raggruppano in s coppie coniugate: $r + 2s = n$. Sia $\varepsilon \colon \mathbb{C} \to \mathbb{C}$ il coniugio e si suppone che $(\sigma_1, \dots, \sigma_n) = (\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_{r+s}, \varepsilon\sigma_{r+1}, \dots, \varepsilon\sigma_{r+s})$. Si definisce

$$\begin{array}{rccc} \boldsymbol{\sigma}\colon & K & \to & \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n \\ & \alpha & \mapsto & (\sigma_1\alpha, \dots, \sigma_r\alpha, \Re(\sigma_{r+1}\alpha), \Im(\sigma_{r+1}\alpha), \dots, \Re(\sigma_{r+s}\alpha), \Im(\sigma_{r+s}\alpha)). \end{array}$$

Proposizione 6.11. *Se $M = \langle x_1, \dots, x_n \rangle_{\mathbb{Z}} \subseteq K$ è uno $\mathbb{Z}$-modulo libero di rango n, allora $\boldsymbol{\sigma}(M)$ è un reticolo di $\mathbb{R}^n$ di volume $2^{-s} \left| \det \left(\sigma_i(x_j) \right)_{i,j} \right|$.*

Dimostrazione. Si ha $V(\boldsymbol{\sigma}M) = |(\boldsymbol{\sigma}(x_1), \dots, \boldsymbol{\sigma}(x_n))|$; per far comparire le $\sigma_{r+1}, \dots, \sigma_n$ si usa la formula $\Im(z) = {}^1\!/_2 \, (z - \bar{z})$, che introduce il fattore 2^{-s}. □

Corollario 6.12. *Siano $d = \operatorname{disc} K$, $I \subseteq \mathscr{O}_K$, allora $\boldsymbol{\sigma}(\mathscr{O}_K)$ e $\boldsymbol{\sigma}(I)$ sono reticoli di $\mathbb{R}^n$ tali che $V(\boldsymbol{\sigma}\mathscr{O}_K) = 2^{-s} d^{1/2}$ e $V(\boldsymbol{\sigma}I) = 2^{-s} \sqrt{\operatorname{disc}(\alpha_1, \dots, \alpha_t)} = 2^{-s} N(I) d^{1/2}$, con $\alpha_1, \dots, \alpha_t$ una base intera di I.*

Teorema 6.13. *Siano K un campo di numeri, $n = r+2s = [K : \mathbb{Q}]$, $d = \operatorname{disc} K$, $I \subseteq \mathscr{O}_K$, $I \neq 0$, allora esiste $x \in I$ tale che*

$$\left| N_{K/\mathbb{Q}}(x) \right| \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s d^{1/2} N(I).$$

In particolare, il gruppo delle classi di ideali di K è finito e ogni classe di ideali contiene un ideale intero tale che $N(I) \leq {}^{n!}\!/_{n^n} \, ({}^4\!/_\pi)^s \, d^{1/2}$.

Dimostrazione. Per ogni $t \in \mathbb{R}^+$ sia

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

Si osserva che B_t è compatto, convesso e simmetrico rispetto all'origine, e $\mu(B_t) = 2^r \, ({}^\pi\!/_2)^s \, {}^{t^n}\!/_{n!}$. Sia t tale che $\mu(B_t) = 2^n V(\boldsymbol{\sigma}I)$; allora $2^n 2^{-s} N(I) d^{1/2} = 2^r \, ({}^\pi\!/_2)^s \, {}^{t^n}\!/_{n!}$, da cui $t^n = d^{1/2} \, ({}^4\!/_\pi)^{-s} \, n! N(I)$; per il corollario, esiste $x \neq 0$, $x \in I$ tale che $\boldsymbol{\sigma}x \in B_t \cap \boldsymbol{\sigma}(I)$.

Si ha

$$\begin{aligned} \left| N_{K/\mathbb{Q}}(x) \right| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)|^2 \leq \\ \leq \left(\frac{1}{n} \sum_{i=1}^{r} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r+1}^{r+s} |\sigma_j(x)| \right)^n \end{aligned}$$

per la disuguaglianza tra media geometrica e media aritmetica. Questa quantità si maggiora ancora con ${}^{t^n}\!/_{n^n}$ che, una volta sostituito il valore di t^n, dà la tesi.

Rimane da dimostrare la formula $\mu(B_t) = 2^r \, ({}^\pi\!/_2)^s \, {}^{t^n}\!/_{n!} =: V(r, s, t)$, tramite un'induzione doppia su r e s. Si inizia $V(1, 0, t) = 2t$ e $V(0, 1, t) = {}^{t^2}\!/_{4\pi}$. Per passare da r a $r + 1$,

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

e

$$V(r+1,s,t) = \int_{-t}^{t} V(r,s,t-|y|)\,\mathrm{d}y =$$
$$= 2\int_{0}^{t} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-|y|)^n}{n!}\mathrm{d}y = 2^{r+1}\left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!}.$$

Allo stesso modo si fa il calcolo per passare da s a $s+1$, solo passando attraverso le coordinate polari. □

Esempio 6.14. Si vuole calcolare il gruppo delle classi di ideali di $\mathbb{Q}\left(\sqrt{-5}\right) = K$; si ha $\mathscr{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$, $\operatorname{disc} K = 20$, $r = 0$, $s = 1$. Ogni classe di ideali contiene un ideale intero I tale che $N(I) \leq {}^2\!/_4 4/\pi\sqrt{20} < 3$, quindi ogni ideale contiene un ideale intero di norma 2. Se tutti gli ideali di norma 2 fossero principali, il gruppo delle classi di ideali sarebbe banale; altrimenti se ci fosse qualche ideale non principale questo avrà un rappresentante di norma 2. Se la limitazione fosse stata più lasca, si sarebbero comunque studiati gli ideali di norma un primo. Nel caso in questione, se la norma di un primo $\mathfrak{p}$ è 2, allora $\mathfrak{p} \mid 2$, e 2 non può essere non ramificato altrimenti $\mathfrak{p}$ avrebbe norma 4, quindi $2 = \mathfrak{p}^2$. In particolare, $\mathbb{Z}\left[\sqrt{-5}\right]$ non è UFD quindi non è PID perciò esiste un $\mathfrak{p}$ non principale e il gruppo delle classi è $\mathbb{Z}_2$.

5.12.2006

Corollario 6.15. *Sia* $[K:\mathbb{Q}] = n = r + 2s \geq 2$, $d = \operatorname{disc} K$, *allora* $|d| \geq {}^\pi\!/_3 \left({}^{3\pi}\!/_4\right)^{n-1}$, *quindi in particolare* ${}^n\!/_{\log d}$ *è maggiorato da una costante indipendente dal campo* K.

Dimostrazione. Si ha la maggiorazione su un ideale contenuto in una classe, $\mathrm{N}(I) \leq \left({}^4\!/_\pi\right)^s {}^{n!}\!/_{n^n} |d|^{1/2}$; poiché $\mathrm{N}(I) \geq 1$, in particolare $d^{1/2} \geq \left({}^\pi\!/_4\right)^s {}^{n^n}\!/_{n!}$, cioè $d \geq \left({}^\pi\!/_4\right)^{2s} \left({}^{n^{2n}}\!/_{(n!)^2}\right) =: a_n$. La tesi è che $a_n \geq {}^\pi\!/_3 \left({}^{3\pi}\!/_4\right)^{n-1}$ per ogni $n \geq 2$.

Per induzione: $a_2 = \left({}^\pi\!/_4\right)^2 \left({}^{2^4}\!/_{2^2}\right) = \left({}^\pi\!/_4\right)^2 2^2 = {}^{\pi^2}\!/_4$; se vale per ogni $k \leq n$,

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\frac{(n+1)^{2(n+1)}}{((n+1)!)^2}\frac{\cancel{(n!)^2}}{n^{2n}} =$$
$$= \frac{\pi}{4}\left(\frac{n+1}{n}\right)^{2n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} =$$
$$= \frac{\pi}{4}(1+2+\cdots) \geq \frac{\pi}{4}3.$$

Quindi

$$a_{n+1} \leq \frac{3\pi}{4}a_n \leq \frac{3\pi}{4}\left(\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}\right) = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^n. \qquad \square$$

Teorema 6.16 (Hermite)**.** *Esistono solo un numero finito di campi di numeri di discriminante assegnato.*

Dimostrazione. Sia $d \in \mathbb{Z}$ fissato; per il corollario, se K è tale che $\operatorname{disc} K = d$, allora $[K:\mathbb{Q}] = n$ soddisfa $n \leq k \log d$ con k costante fissata. Basta perciò dimostrare che fissati d e n esistono un numero finito di campi di numeri di

discriminante d e grado n e si può anche fissare la partizione $n = r + 2s$ (il numero di queste partizioni è ancora finito, fissato n).

Sia $B \subseteq \mathbb{R}^r \times \mathbb{C}^s$; se $r > 0$,

$$B \coloneqq \left\{ (y,z) \mid |y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-s} |d|^{\frac{1}{2}}, |y_i| \leq \frac{1}{2}, |z_j| \leq \frac{1}{2} \right\},$$

altrimenti se $r = 0$,

$$B \coloneqq \left\{ z \mid |z_1 - \bar{z_1}| \leq 2^n \frac{8}{\pi} \left(\frac{\pi}{2}\right)^{-s} |d|^{\frac{1}{2}}, |z_1 + \bar{z_1}| \leq \frac{1}{2}, |z_j| \leq \frac{1}{2} \right\}.$$

In ogni caso, B è un compatto convesso e simmetrico rispetto a 0; se $\mu(B) \geq 2^n V(\boldsymbol{\sigma}(\mathscr{O}_K))$, B contiene un punto di $\boldsymbol{\sigma}(\mathscr{O}_K)$ non nullo. Ma $V(\boldsymbol{\sigma}(\mathscr{O}_K)) = 2^{-s} |d|^{1/2}$, quindi si deve verificare $\mu(B) \geq 2^{n-s} |d|^{1/2}$; ma la definizione di B è stata fatta in modo da far risultare questo.

Allora, esiste $x \in \mathscr{O}_K$ non nullo tale che $\boldsymbol{\sigma}(x) \in B$. Si vuole dimostrare che $K = \mathbb{Q}(x)$, cioè che x ha grado n e per dire questo si può mostrare che non è fissato da nessuna immersione. Se $r > 0$, $|\sigma_i(x)| \leq 1/2$ per ogni $i \in \{2, \dots, n\}$. Allora per avere $\mathrm{N}_{K/\mathbb{Q}} \in \mathbb{Z}$ deve essere $|\sigma_1(x)| \geq 1$, da cui $\sigma_1(x) \neq \sigma_i(x)$ per ogni $i \in \{2, \dots, n\}$. Si sa che $\mathbb{Q} \subseteq \mathbb{Q}(x) \subseteq K$; se $[K : \mathbb{Q}(x)] = m$, si ha che ogni σ su $\mathbb{Q}(x)$ si estende in m modi ad una σ su K, ma $\sigma_1(x)_{|\mathbb{Q}(x)} \neq \sigma_i(x)_{|\mathbb{Q}(x)}$ per ogni $i \in \{2, \dots, n\}$, da cui si ha necessariamente $m = 1$. Se $r = 0$, $\Re(\sigma_i(x)) \leq 1/4$ e con argomentazioni simili si mostra che σ_1 è diverso da ogni altra σ_i; inoltre non è reale e quindi non può essere uguale nemmeno alla sua coniugata.

Rimane da dimostrare che gli x possibili sono in numero finito. Infatti, $\boldsymbol{\sigma}(x) \in B$ per la forma di B dà che tutti i coniugati di x (quindi anche le funzioni simmetriche di grado assegnato) sono limitate, perciò anche i coefficienti del polinomio minimo di x; questo significa che si hanno solo un numero finito di polinomi minimi e di conseguenza un numero finito di elementi x. □

Esempio 6.17. Sia $K = \mathbb{Q}\left(\sqrt{-26}\right)$; si vogliono calcolare le classi di ideali; si ha $-26 \equiv 2\ (4)$, quindi $\mathscr{O}_K = \mathbb{Z}\left[\sqrt{-26}\right]$ e $\operatorname{disc} K = -104$. Per la limitazione $\mathrm{N}(I) \leq (4/\pi)^s\, n!/n^n\, |d|^{1/2} = 4/\pi^2/4\sqrt{104} < 13/2$, quindi $\mathrm{N}(I) \leq 6$. Questo significa che se p sta sotto I, $\mathrm{N}(p) = p^f \leq 6$. I candidati per p sono 2, 3, 5 e bisogna verificare come si spezzano.

Per 2: $2 \mid d$, quindi è ramificato e può essere solo $2\mathscr{O}_K = \mathfrak{p}^2$. Si ha $\mathrm{N}(\mathfrak{p}) = 2$ perché è la norma del primo che sta sotto elevato al grado d'inerzia. In questo caso, $\mathfrak{p}$ è principale se e solo se esiste $\alpha \in \mathscr{O}_K$ tale che $\left|N_{K/\mathbb{Q}}(\alpha)\right| = 2$; ma $\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{-26}) = a^2 + 26b^2$ che non può mai essere ± 2. Quindi $\mathfrak{p}$ non è principale e $\operatorname{ord} \bar{\mathfrak{p}} = 2$.

Per 3: $3\mathscr{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ con $\mathfrak{q}_1 = (3, 1 + \sqrt{-26})$ e $\mathfrak{q}_2 = (3, 1 - \sqrt{-26})$ e non sono principali perché non esistono ideali di norma 3. Si ha $\bar{\mathfrak{q}_1}\bar{\mathfrak{q}_2} = \mathscr{O}_K$, quindi $\bar{\mathfrak{q}_1} = \bar{\mathfrak{q}_2}^{-1}$. Se $\mathfrak{q}_1$ avesse ordine 2, significherebbe che $\mathfrak{q}_1^2$ è principale, cioè $\mathfrak{q}_1^2 = (\beta)$, ma non esistono elementi β di norma 9. Si verifica che $\operatorname{ord} \mathfrak{q}_1 = 3$, cioè $\mathfrak{q}_1^3 = (\gamma)$: infatti $\mathrm{N}(1 \pm \sqrt{-26}) = 27$ e $\gamma = 1 + \sqrt{-26} \in \mathfrak{q}_1$. Poiché la norma di γ è 27, (γ) si fattorizza tramite primi che stanno sopra 3, cioè $\mathfrak{q}_1$ e $\mathfrak{q}_2$; ma $\gamma \notin \mathfrak{q}_2$, quindi $(\gamma) = \mathfrak{q}_1^3$. Si sono trovati un elemento di ordine 2 e due di ordine 3 quindi almeno il gruppo delle classi di ideali è $\mathbb{Z}_6$.

Si conclude con le classi date dai primi che stanno sopra 5.

6.11.2006

Osservazione 6.18. Un elemento $x \in \mathscr{O}_K$ è un'unità se e solo se $\mathrm{N}_{[K:\mathbb{Q}]}(x) = 1$. Dire che $x \in \mathscr{O}_K$ è necessario perché non è vero che gli elementi di K di norma 1 siano interi.

Teorema 6.19 (Dirichlet)**.** *Sia $[K : \mathbb{Q}] = n = r + 2s$, allora $\mathscr{O}_K^\star \cong G \times \mathbb{Z}^{r+s-1}$, dove G è il gruppo G delle radici dell'unità in K. In particolare, essendo G un sottogruppo finito di un campo, è ciclico. I generatori della parte libera si dicono un* sistema di unità fondamentali[3]*.*

Dimostrazione. Innanzitutto, si mostra che $\mathscr{O}_K^\star$ è uno $\mathbb{Z}$-modulo finitamente generato, quindi costituito da una parte di torsione T e una parte libera $\mathbb{Z}^d$; poi rimarrà da dimostrare che $T = G$ e $d = r + s - 1$. A partire da $\boldsymbol{\sigma} \colon K \to \mathbb{R}^r \times \mathbb{C}^s$ di definisce l'immersione logaritmica $L \colon K \to \mathbb{R}^{r+s} \colon x \mapsto (\log|\sigma_1(x)|, \dots, \log|\sigma_{r+s}(x)|)$. Si ha che $L(xy) = L(x) + L(y)$ in quanto $\boldsymbol{\sigma}$ è un morfismo. Siano $B \subseteq \mathbb{R}^{r+s}$ un compatto e $B' = \{\, x \in \mathscr{O}_K^\star \mid L(x) \in B \,\}$; B' è finito: poiché B è limitato, per ogni $x \in B'$, esiste $\alpha \in \mathbb{R}$ tale che $\log|\sigma_i(x)| \leq \alpha$, da cui esiste β tale che $1/\beta \leq |\sigma_i(x)| \leq \beta$; questo dà che tutti i coniugati di x sono limitati e anche le loro funzioni simmetriche. Ma queste sono intere, quindi in numero finito, di conseguenza i polinomi caratteristici dei possibili x sono in numero finito e anche i possibili x.

Si dimostra che $G = \ker L_{|\mathscr{O}_K^\star}$: il nucleo è finito prendendo $B = \{0\}$, quindi come sottogruppo finito di un campo è ciclico e di conseguenza è costituito da radici dell'unità. Per l'altro contenimento, se $x \in G$, $x^m = 1$ quindi $1 = \boldsymbol{\sigma}(x^m) = \boldsymbol{\sigma}(x)^m$ e $|\boldsymbol{\sigma}(x)| = 1$. Prendendo il logaritmo si ha che $L(x) = 0$.

D'altra parte, $L(\mathscr{O}_K^\star) \subseteq \mathbb{R}^{r+s}$ interseca ogni compatto in un insieme finito, che è la definizione di insieme discreto di $\mathbb{R}^{r+s}$, ma è anche uno $\mathbb{Z}$-modulo libero di rango $d \leq r + s$; si ha la successione esatta

$$0 \longrightarrow G \longrightarrow \mathscr{O}_K^\star \longrightarrow L(\mathscr{O}_K^\star) \longrightarrow 0.$$

Se la successione si spezza si ha che $\mathscr{O}_K^\star \cong G \times \mathbb{Z}^d$ (l'immagine è un modulo libero). Inoltre $d \leq r + s - 1$, infatti $L(\mathscr{O}_K^\star) \subseteq W = \left\{ y \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r} y_i + 2\sum_{i=r+1}^{r+s} y_i = 0 \right\}$ perché il prodotto delle norme dei coniugati di $\boldsymbol{\sigma}$ fa 1. L'altra disuguaglianza è più macchinosa: si mostra che esistono $u_1, \dots, u_{r+s-1} \in \mathscr{O}_K^\star$ tali che le loro immagini tramite L sono linearmente indipendenti.

Lemma 6.20. *Per ogni k fissato, $1 \leq k \leq r + s$, per ogni $\alpha \in \mathscr{O}_K \setminus \{0\}$, esiste $\beta \in \mathscr{O}_K \setminus \{0\}$ tale che $L(\beta) = (b_1, \dots, b_{r+s})$, $|\mathrm{N}(\beta)| \leq (2/\pi)^s \sqrt{|\operatorname{disc} K|}$ e $L(\alpha) = (a_1, \dots, a_{r+s})$ con $a_i > b_i$ per ogni $i \neq k$.*

Dimostrazione. Sia $B = \{\, (y, z) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \leq c_i, |z_i| \leq c_{i+r} \,\}$ con $0 < c_i < e^{a_i}$ per ogni $i \neq k$ e $c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2 = (2/\pi)^s \sqrt{|\operatorname{disc} K|}$; in questo modo $\mu(B) = 2^r c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2 \pi^s = 2^{n-s}\sqrt{|\operatorname{disc} K|} = 2^n V(\boldsymbol{\sigma}(\mathscr{O}_K))$, che è l'ipotesi necessaria per usare il teorema del corpo convesso. Perciò esiste $\beta \in \mathscr{O}_K \setminus \{0\}$ tale che $\boldsymbol{\sigma}(\beta) \in B$ e β ha le proprietà cercate. □

[3] Conoscere la parte di torsione non è difficile, ma trovare le unità fondamentali in generale lo è; spesso si lavora con dei generatori di un sottogruppo della parte libera.

Lemma 6.21. *Per ogni k fissato, $1 \leq k \leq r+s$, esiste $u_k \in \mathscr{O}_K^\star$ tale che $L(u_k) = (x_1, \dots, x_{r+s})$ e $x_i < 0$ per ogni $i \neq k$.*

Dimostrazione. Sia $\alpha_1 \in \mathscr{O}_K \setminus \{0\}$; applicando il lemma varie volte si ottiene una successione $(\alpha_i)_i$ tale che per ogni $j < h$ e $i \neq k$, $L(\alpha_h)_i < L(\alpha_j)_i$. Quindi $\left|\mathrm{N}_{\kappa/\mathbb{Q}}(\alpha_j)\right| \leq (2/\pi)^s \sqrt{\operatorname{disc} K}$, cioè tutte le norme sono minori di una costante. Ma $\left|\mathrm{N}_{\kappa/\mathbb{Q}}(\alpha_j)\right| = \mathrm{N}((\alpha_j))$ e tutti questi ideali si fattorizzano con primi di norma limitata (che sono in numero finito) ed esponenti limitati, di conseguenza non possono essere tutti distinti: esistono $j < h$ tali che $(\alpha_j) = (\alpha_h)$, allora esiste $u_k \in \mathscr{O}_K^\star$ tale che $\alpha_h = u_k \alpha_j$, perciò $L(\alpha_h) = L(u_k) + L(\alpha_j)$ e $L(u_k)_i < 0$ per ogni $i \neq k$. □

Ora, $\operatorname{rk} \langle L(u_1), \dots, L(u_{r+s}) \rangle \geq r+s-1$; per un lemma di algebra lineare, se M è una matrice quadrata di dimensione m con elementi positivi sulla diagonale e negativi altrove tale che per ogni riga la somma degli elementi sulla riga è nulla, allora $\operatorname{rk} M = m-1$. Questo lemma si può applicare alla matrice con le prime righe date da $L(u_i)$ e le ultime da $2L(u_j)$.

Per dimostrare il lemma si considerano V_i, le colonne di M; se le prime $m-1$ colonne fossero dipendenti, $\sum_{i=1}^{m-1} t_i V_i = 0$ con i t_i non tutti nulli, quindi si può normalizzare e pensare che il più grande sia $t_k = 1$; allora $0 = \sum_{i=1}^{m-1} t_i a_{k,i} = a_{k,k} + \sum_{i \neq k} t_i a_{k,i} \geq \sum_{i=1}^{m-1} a_{k,i} > \sum_{i=1}^{m} a_{k,i} = 0$, assurdo. □

7 Esercizi

13.12.2006

Esercizio 7.1. Siano K un campo di numeri, $\alpha \in \mathscr{O}_K$ un intero algebrico tale che $|\sigma(\alpha)| = 1$ per ogni immersione σ, allora α è una radice dell'unità.

Soluzione. Sicuramente è un'unità perché ha norma 1; il trucco è mostrare che non tutte le potenze di α sono distinte. Ma dall'ipotesi, per ogni σ e per ogni n, $|\sigma(\alpha^n)| = 1$; se d è il grado dell'estensione, i coefficienti del polinomio minimo di α^n sono limitati con una costante che dipende solo da d (ad esempio, la traccia è limitata da d). Quindi i polinomi minimi di tutti gli α^n sono in numero finito, perciò esistono $n \neq m$ tali che $\alpha^n = \alpha^m$ e α è radice dell'unità. □

Esercizio 7.2. Siano p primo, $\zeta := \zeta_p$; si considerano $K := \mathbb{Q}(\zeta)$ e $L := \mathbb{Q}(\zeta + \zeta^{-1})$; si è già dimostrato che $\mathscr{O}_K = \mathbb{Z}[\zeta]$ e $\mathscr{O}_L = \mathbb{Z}[\zeta + \zeta^{-1}]$. Per il teorema di Dirichlet, $\mathbb{Z}[\zeta]^\star \cong \langle \pm 1, \zeta \rangle \times \mathbb{Z}^{1/2(p-1)-1}$ perché le immersioni sono tutte complesse; invece, per $\mathbb{Z}[\zeta + \zeta^{-1}]$ le immersioni sono tutte reali e quindi $\mathbb{Z}[\zeta + \zeta^{-1}]^\star \cong \langle \pm 1 \rangle \times \mathbb{Z}^{1/2(p-1)-1}$. Se ε è un'unità di $\mathbb{Z}[\zeta]^\star$, allora esiste un'unità $\varepsilon_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^\star$ tale che $\varepsilon = \zeta^r \varepsilon_1$, cioè le due unità differiscono per due radici dell'unità.

Soluzione. Se $\varepsilon \in \mathbb{Z}[\zeta]^\star$, allora $\varepsilon/\bar{\varepsilon}$ e tutti i suoi coniugati hanno norma 1 (il coniugio commuta con le altre immersioni), quindi ε è una radice dell'unità, cioè $\varepsilon/\bar{\varepsilon} = \pm\zeta^a$.

- Se vale il segno positivo, $a = 2i$ (p); si pone $\varepsilon_1 = \zeta^{-i}\varepsilon$; rimane da verificare che $\varepsilon_1 \in \mathbb{R}$, ma $\bar{\varepsilon_1} = \zeta^i \bar{\varepsilon} = \zeta^i \zeta^{-a} \varepsilon = \zeta^{-i}\varepsilon = \varepsilon_1$. Inoltre è invertibile perché è prodotto di invertibili e il suo inverso è reale perché è reale.

- Se vale il segno negativo, si scrive $\varepsilon = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, che modulo $(1-\zeta)$ (il generatore dell'ideale primo sopra p) è $a_0 + \cdots + a_{p-2}$; vale ancora $\varepsilon = -\zeta^a\bar{\varepsilon}$, perciò $\bar{\varepsilon} = a_0 + a_1\zeta^{-1} + \cdots + a_{p-2}\zeta^{-(p-2)}$ e si ha $\varepsilon \equiv \bar{\varepsilon}\ (1-\zeta)$, ma dalla relazione $\varepsilon = -\zeta^a\bar{\varepsilon}$ si ha $\varepsilon \equiv -\bar{\varepsilon}\ (1-\zeta)$. Da questo si ottiene che $2\varepsilon \equiv 0\ (1-\zeta)$. Poiché $1-\zeta$ ha norma p non contiene 2, quindi $\varepsilon \equiv 0\ (1-\zeta)$, ma questo è impossibile perché ε è un'unità e non può stare in un ideale primo. □

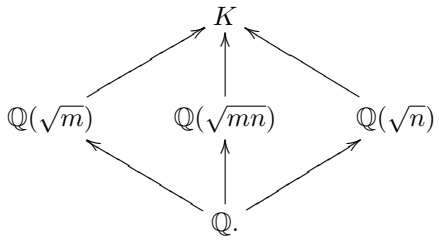
Esercizio 7.3. Sia L/K un'estensione di campi di numeri, allora esistono infiniti primi di K che si spezzano completamente in L. Come corollario si ha che con $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, si hanno infiniti primi che si spezzano completamente modulo m, cioè tali che $p \equiv 1\ (m)$.

Soluzione. Innanzitutto si dimostra che se $f \in \mathbb{Z}[x]$, $\deg f \geq 1$, allora f ha una radice modulo p per infiniti primi p. Se $f(0) = 1$ e per assurdo siano $p_1, \ldots, p_m$ i primi tali che f ha una radice modulo p. Non può essere che $f(n) = 1$ per ogni n, quindi sia $n > p_i$ per ogni i un numero tale che esiste un primo p con $p \mid f(n!)$. Allora $f(n!) \equiv 0\ (p)$ ma $p > p_i$ per ogni i, perché se $p \leq n$ implica $p \mid n!$ e $p \mid f(0) = 1$, assurdo. Se invece f è un polinomio generico, sia $g(x) = f(xf(0))/f(0)$; g soddisfa $g(0) = 1$ e si può usare quanto dimostrato in precedenza.

Ora, sia K un campo di numeri, allora esistono infiniti primi $\mathfrak{p}$ di $\mathscr{O}_K$ tali che $f(\mathfrak{p} \mid p) = 1$.

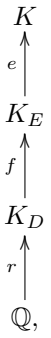
Sia $\tilde{L}$ la chiusura normale di $L/\mathbb{Q}$, allora per quanto detto, esistono infiniti primi $\tilde{\mathfrak{q}}$ di $\tilde{L}$ con $f(\tilde{\mathfrak{q}} \mid p) = 1$, quindi esistono infiniti primi di $\mathbb{Z}$ che si spezzano completamente in $\tilde{L}$ (togliendo quelli ramificati che sono un numero finito). Se $d = \left[\tilde{L} : \mathbb{Q}\right]$, e p è un primo, allora $p\mathscr{O}_{\tilde{L}} = \tilde{\mathfrak{q}_1} \ldots \tilde{\mathfrak{q}_d}$. Se un primo si spezza completamente in $\tilde{L}$, a maggior ragione si spezza completamente in L. Ma allora tutti i primi di $\mathscr{O}_K$ che stanno sopra p si spezzano completamente in $\mathscr{O}_L$ e questi sono infiniti. □

Esercizio 7.4. Sia $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ con mn libero da quadrati, allora



Si prende un p tale che p si spezza in un unico fattore di grado 2 in tutte le estensioni parziali; allora $p\mathscr{O}_K$ può essere $\mathfrak{p}^4$, $\mathfrak{p}^2\mathfrak{q}^2$ (con $r = 2$) o $\mathfrak{p}^2$ (con $f = 2$).

Ma



quindi le ultime due possibilità non possono accadere perché non esistono dei sottocampi con $r = 2$ o con $f = 2$; perciò $p\mathscr{O}_K = \mathfrak{p}^4$. Ora, $p\mathscr{O}_{\mathbb{Q}(\sqrt{m})}$ (con $p \neq 2$) può fattorizzarsi come $\mathfrak{p}^2$ se $p \mid m$, come $\mathfrak{pq}$ se m è un quadrato modulo p o come $\mathfrak{p}$ se m non è un quadrato modulo p. Nella situazione precedente, si avrebbe $p \mid n$ e $p \mid m$, quindi $p^2 \mid mn$ che non è possibile per le ipotesi. Quindi si deve cercare con $p = 2$: ad esempio se $m \equiv 2 \pmod 4$ e $n \equiv 3 \pmod 4$, $mn \equiv 2 \pmod 4$.

Esercizio 7.5. Siano $K \coloneqq \mathbb{Q}(\sqrt{m})$ e $L \coloneqq \mathbb{Q}(\sqrt{n})$; trovare degli esempi per cui $p\mathscr{O}_K = \mathfrak{p}^2$ e $p\mathscr{O}_L = \mathfrak{q}^2$, ma $p\mathscr{O}_{KL} \neq \mathfrak{p}^4$.

Soluzione. Ad esempio, con $p \neq 2$, $m = pa$, $n = pb$, allora $mn = p^2ab$ e l'estensione è $\sqrt{ab}$; scegliendo opportunamente a e b si ottiene la richiesta. Oppure con $p = 2$, $m = 2$ e $n = 10$. □

Esercizio 7.6. Trovare un punto a coordinate intere nella curva $y^2 = x^3 - 2$.

Soluzione. Se $K = \mathbb{Q}(\sqrt{-2})$, $\mathscr{O}_K$ è un PID per il teorema di Minkowsky (la costante è strettamente minore di 2). Si scrive $x^3 = y^2 + 2$ e si ragiona in modo simile a quanto fatto per le terne pitagoriche: $x^3 = (y-\sqrt{-2})(y+\sqrt{-2})$; si mostra che i due fattori sono coprimi: $I = (y-\sqrt{-2}, y+\sqrt{-2}) = (1)$ perché $I \supseteq (\sqrt{-2})^3$, quindi le possibilità sono $I = (\sqrt{-2})$ o $I = (1)$. Se $y + \sqrt{-2} \subseteq (\sqrt{-2})$ si avrebbe $y \in (\sqrt{-2})$, cioè $\sqrt{-2} \mid y$ e $2 \mid y$. Questo non è possibile perché se y fosse pari, anche x sarebbe pari e non potrebbe essere 0 modulo 8. Poiché si è in un anello a ideali principali, se un prodotto è un cubo anche i fattori lo sono e $y + \sqrt{-2} = (a + \sqrt{-2}b)^3 = a^3 - 6ab^2 + \sqrt{-2}(3a^2b - 2b^3)$, da cui si ha che $b = \pm 1$ e $a = \pm 1$, quindi $y = \pm 5$ e $x = 3$. □