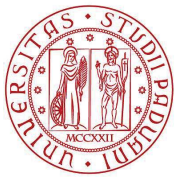


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Il Teorema di Kronecker - Weber

Relatore:
Prof. Riccardo Colpi

Laureando: Francesco Feltrin
Matricola: 2000425

Anno Accademico 2022/2023

22/09/2023

Indice

Introduzione

Il Teorema di Kronecker - Weber afferma che ogni estensione abeliana finita del campo $\mathbb{Q}$ dei numeri razionali è contenuta in un'estensione ciclotomica: ossia, se $L/\mathbb{Q}$ è un'estensione finita, normale e separabile tale che il gruppo di Galois $Gal(L/\mathbb{Q})$ a essa associato sia abeliano, allora esiste un numero naturale n tale che $L \subset \mathbb{Q}(\zeta_n)$, con ζ_n una radice primitiva n-esima di 1. Questo teorema fu enunciato per la prima volta da Kronecker nel 1853, e le prime dimostrazioni complete furono date da Weber (1886) e da Hilbert (1896); in seguito ne vennero formulate diverse altre. In questa tesi presentiamo alcuni risultati della *class field theory*, il ramo della teoria algebrica dei numeri che studia le estensioni di campi abeliane, e dedurremo da essi il Teorema di Kronecker - Weber; premetteremo le necessarie nozioni di teoria algebrica dei numeri.

L'oggetto principale di studio della teoria algebrica dei numeri sono i *campi di numeri algebrici*, cioè le estensioni finite (dunque algebriche) $K/\mathbb{Q}$, con le loro proprietà: i numeri interi algebrici (radici di polinomi monici a coefficienti interi), che formano un anello, indicato spesso con O_K; gli ideali di tale anello, il quale spesso non è un dominio a ideali principali; la fattorizzazione unica degli elementi e degli ideali. Nel Capitolo 1 introduciamo le nozioni di base ed enunciamo alcuni importanti risultati, quali il teorema di fattorizzazione unica degli ideali nei *domini di Dedekind*, una particolare classe di anelli di cui fanno parte anche gli anelli degli interi algebrici. Successivamente definiamo gli *ideali frazionari* di un campo K, che rivestiranno un ruolo importante nel seguito, e il gruppo I_K (l'insieme costituito da essi). Parleremo poi della fattorizzazione degli ideali primi di un anello di interi algebrici in una sua estensione, ad esempio di cosa succede a un ideale di $\mathbb{Z}$ se pensato in un anello più grande. Infine definiremo le valutazioni su un campo di numeri algebrici, introducendo così il concetto di *posto di un campo di numeri* K, cioè una classe di equivalenza di valutazioni su K.

Il Capitolo 2 presenta i concetti fondamentali della *class field theory*: le norme degli ideali frazionari, l'automorfismo di Frobenius e la mappa di Artin associati a un'estensione abeliana L/K, con K campo di numeri. Alla fine di questo capitolo enunciamo brevemente dei risultati della teoria analitica dei numeri, il settore della matematica che utilizza metodi analitici, principalmente le serie numeriche, per risolvere problemi riguardanti i numeri interi, e in particolare la distribuzione dei numeri primi. Vedremo che i risultati di questa sezione mostreranno non solo delle caratteristiche di alcuni sottogruppi di I_K, ma anche un legame importante tra certi ideali primi di O_K, quelli che *spezzano completamente* in una estensione, e l'estensione stessa (teorema 2.4.2).

La *class field theory* per i campi di numeri algebrici ha come obiettivo quello di studiare le estensioni abeliane di un campo di numeri K, ed eventualmente classificarle, in termini di proprietà di I_K e di certi suoi sottogruppi e quozienti: il Teorema di Kronecker - Weber esaurisce la rischiesta nel caso $K = \mathbb{Q}$. Nel Capitolo 3 dimostriamo, attraverso una serie di risultati, un importante teorema, detto *della reciprocità di Artin*; grazie a questo e un altro fatto (teorema 3.3.1), dimostreremo il Teorema di Kronecker - Weber. Gli enunciati e le dimostrazioni di questo capitolo sono tratti da [4, cap. V.5]. Concludiamo con una breve discussione sul caso $K \neq \mathbb{Q}$.

Capitolo 1

Anelli di interi algebrici e ideali frazionari

1.1 Domini di Dedekind

Cominciamo presentando alcune nozioni base dell'Algebra commutativa.

Osservazione 1.1.1. Ogni anello che considereremo sarà commutativo e con identità; un *dominio* è un anello privo di divisori dello zero.

Definizione 1.1.1. Sia A un anello. Un sottoinsieme $I \subset A$ si dice *ideale* di A, e si indica $I \lhd A$, se I è un sottogruppo additivo di $(A, +, 0)$ tale che

$$ax \in I \quad \forall\, x \in I\,, \forall\, a \in A.$$

La nozione di ideale, e in particolare quella di ideale *primo*, riveste un'importanza fondamentale nell'Algebra commutativa.

Definizione 1.1.2. Sia I un ideale proprio (ossia, $I \neq A$) dell'anello A. I si dice *ideale massimale* se non è strettamente contenuto in alcun altro ideale proprio di A.
I si dice *ideale primo* se

$$xy \in I \implies (x \in I \vee y \in I).$$

Indicheremo gli ideali primi di un anello con $\mathfrak{p}, \mathfrak{q}, \mathfrak{P}, \mathfrak{Q} \ldots$.

L'insieme di tutti gli ideali primi di A viene chiamato *spettro di A* e si indica con $Spec(A)$.

Osservazione 1.1.2. Ricordiamo che, dato $I \lhd A$, l'insieme quoziente $\frac{A}{I}$ è un anello, e valgono le seguenti equivalenze:

$$I \text{ è un ideale massimale} \iff \text{l'anello } \frac{A}{I} \text{ è un campo;}$$

$$I \text{ è un ideale primo} \iff \text{l'anello } \frac{A}{I} \text{ è un dominio.}$$

Poichè ogni campo è un dominio, ogni ideale massimale è primo.

Definizione 1.1.3. Un anello A con un solo ideale massimale M è detto *anello locale*; il campo $\frac{A}{M}$ è detto *campo residuo di A*.

Cominciamo a isolare delle categorie particolari di anelli: la prima categoria di interesse è quella degli anelli *noetheriani*.

Definizione 1.1.4. Un dominio A è detto *dominio noetheriano*, o *dominio di Noether*, se ogni suo ideale è finitamente generato.

Esempio 1.1.1. Ogni PID è un anello noetheriano, in quanto ogni suo ideale è generato da addirittura un solo elemento.

Il Teorema della base di Hilbert afferma che, se A è noetheriano, allora anche $A[x]$ lo e.

L'anello dei polinomi a coefficienti reali in infinite variabili, $\mathbb{R}[x_0, x_1, x_2, \dots]$, non è noetheriano: l'ideale $(\{x_i \,|\, i \in \mathbb{N}\})$ non è finitamente generato.

È possibile definire delle operazioni sugli ideali di un anello: infatti, dati $I, J \triangleleft A$, si ha che l'intersezione $I \cap J$ è un ideale di A; sono inoltre definite nel modo seguente la somma e il prodotto degli ideali I, J.

Definizione 1.1.5. Sia A un anello, $I, J \triangleleft A$ ideali.

L'*ideale somma* $I + J$ è il più piccolo ideale di A che contiene $I \cup J$; esso è dato dall'insieme

$$I + J \equiv \{i + j \,|\, i \in I, j \in J\}.$$

L'*ideale prodotto* IJ è l'ideale di A generato dall'insieme

$$\{ij \,|\, i \in I, j \in J\}.$$

Si osservi che vale sempre l'inclusione $IJ \subset I \cap J$.

Esempio 1.1.2. Siano $A = \mathbb{Z}, I = (4) = 4\mathbb{Z} = \{\cdots -8, -4, 0, 4, 8 \dots\}, J = (6) = 6\mathbb{Z}$.

$I \cap J = (12) = 12\mathbb{Z}$.

$I + J = \{i + j \,|\, i \in (4), j \in (6)\} = \{4a + 6b \,|\, a, b \in \mathbb{Z}\} = (MCD(4, 6)) = (2) = 2\mathbb{Z}$, per il teorema di Bézout.

$IJ = (\{ij \,|\, i \in (4), j \in (6)\}) = (6 \cdot 4) = 24\mathbb{Z}$.

In generale in $A = \mathbb{Z}$, dati $(m), (n) \triangleleft \mathbb{Z}$, si ha:

$$(m) \cap (n) = (mcm(m, n)); \quad (m) + (n) = (MCD(m, n)); \quad (m)(n) = (mn).$$

Di queste operazioni, l'operazione "prodotto di ideali" è la più importante, per il seguente motivo: come negli UFD ogni elemento si fattorizza (in modo unico a meno di elementi invertibili) in un prodotto di elementi irriducibili, così in una certa classe di anelli, i *domini di Dedekind*, ogni ideale si fattorizza nel prodotto di ideali primi.

Ci avviciniamo alla definizione di questa particolare classe di anelli.

Definizione 1.1.6. Siano $A \subset A'$ anelli. Un elemento $b \in A'$ si dice *intero su A* se $\exists\, f \in A[x]$ polinomio monico t.c. $f(b) = 0$.

Esempio 1.1.3. Consideriamo $\mathbb{Z} \subset \mathbb{Z}[i]$. L'elemento i è intero su $\mathbb{Z}$, in quanto radice del polinomio monico $x^2 + 1 \in \mathbb{Z}[x]$. In generale, se $z = a + ib \in \mathbb{Z}[i]$, con $b \neq 0$, z è radice del polinomio $(x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{Z}[x]$. Dunque, ogni elemento di $\mathbb{Z}[i]$ è intero su $\mathbb{Z}$.

Definizione 1.1.7. Siano A un dominio e K un campo. La *chiusura integrale di A in K* è l'insieme

$$\{b \in K \mid b \text{ è intero su } A\}.$$

Si dimostra che esso è un sottoanello di K.
La *chiusura integrale di A* è la chiusura integrale di A in $K = Q(A)$, campo dei quozienti di A; un dominio A si dice *integralmente chiuso* se coincide con la sua chiusura integrale in $Q(A)$.

Esempio 1.1.4. Consideriamo l'anello $A = \mathbb{Z}[\sqrt{5}]$. L'elemento $\phi \equiv \frac{1+\sqrt{5}}{2}$ è intero su A, in quanto radice del polinomio $x^2 - x - 1 \in \mathbb{Z}[x] \subset \mathbb{Z}[\sqrt{5}][x]$; tuttavia, $\phi \in Q(A) \setminus A$. Dunque A non è integralmente chiuso.

Esempio 1.1.5. $\mathbb{Z}$ è un dominio integralmente chiuso: se $q \in \mathbb{Q}$ è radice di un polinomio monico a coefficienti interi, allora $q \in \mathbb{Z}$ (dai lemmi di Gauss sui polinomi). In realtà vale il seguente risultato, assai più generale.

Proposizione 1.1.1. *Ogni UFD è integralmente chiuso.*

Dimostrazione. Consideriamo A un UFD, K il suo campo dei quozienti e $\frac{x}{y} \in K, (x, y) = 1$, $\frac{x}{y}$ intero su A:

$$\left(\frac{x}{y}\right)^n + a_{n-1}\left(\frac{x}{y}\right)^{n-1} + \cdots + a_0 = 0, \quad a_i \in A.$$

Segue che

$$x^n + (a_{n-1}x^{n-1}y + \cdots + a_1 x y^{n-1} + a_0 y^n) = 0,$$

dunque $y | x^n$. Se $y \notin U(A)$, allora, detta $y = {p_1}^{b_1} \dots {p_r}^{b_r}$ la sua fattorizzazione in irriducibili, si ha che $p_j | x^n \; \forall \, j = 1 \dots r$. Poiché p_j è primo $\forall \, j$ (A è UFD, dunque gli elementi irriducibili sono primi), allora $p_j | x$, contro il fatto che $(x, y) = 1$. Dunque $y \in U(A)$ e $\frac{x}{y} \in A$. □

Esempio 1.1.6. Consideriamo $A = \mathbb{Z}[i]$ l'anello degli interi di Gauss e $K = \mathbb{Q}(i)$ il suo campo dei quozienti. La proposizione precedente implica che $\mathbb{Z}[i]$ è integralmente chiuso, in quanto PID e dunque UFD; d'altra parte, ritroviamo lo stesso risultato anche alla luce dell'esempio 1.1.3: $\forall \, z = a + bi \in \mathbb{Q}(i)$, il suo polinomio minimo su $\mathbb{Q}$ è $f_z \equiv x^2 - 2ax + (a^2 + b^2)$; $f_z \in \mathbb{Z}[x] \iff a, b \in \mathbb{Z} \iff z \in \mathbb{Z}[i]$. Cioè, $z \in \mathbb{Q}(i)$ è intero su $\mathbb{Z}[i]$ (se e) solo se $z \in \mathbb{Z}[i]$; abbiamo mostrato che la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(i)$ è l'anello $\mathbb{Z}[i]$.

Esempio 1.1.7. Dall'esempio 1.1.4 e dalla proposizione precedente segue che il dominio $\mathbb{Z}[\sqrt{5}]$ non è a fattorizzazione unica, perché non è integralmente chiuso. In effetti, in questo anello il numero 4 ha due distinte fattorizzazioni:

$$2 \cdot 2 = 4 = (3 + \sqrt{5}) \cdot (3 - \sqrt{5});$$

si verifica, usando la proprietà moltiplicativa della funzione "norma", $N(a + b\sqrt{5}) \equiv (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$, che $2, (3 + \sqrt{5})$ e $(3 - \sqrt{5})$ sono elementi irriducibili e non associati, dunque le fattorizzazioni sono effettivamente diverse.

Definizione 1.1.8. Un dominio A è detto *dominio di Dedekind* se ha le seguenti proprietà:

1. è un anello noetheriano;

2. è integralmente chiuso;

3. $\forall\, \mathfrak{p} \lhd A$ ideale primo, $\mathfrak{p} \neq (0)$, $\mathfrak{p}$ è massimale.

Enunciamo la principale proprietà dei domini di Dedekind, che abbiamo anticipato poco sopra.

Teorema 1.1.1. *Sia A un dominio di Dedekind e $\mathfrak{A} \lhd A$ un suo ideale non nullo. Allora*

$$\mathfrak{A} = {\mathfrak{P}_1}^{a_1} \dots {\mathfrak{P}_n}^{a_n},$$

ossia $\mathfrak{A}$ si fattorizza nel prodotto di un numero finito di ideali primi di A; gli ideali $\mathfrak{P}_i$ primi sono tutti e soli gli ideali primi di A che contengono $\mathfrak{A}$; gli esponenti a_i sono univocamente determinati da $\mathfrak{A}$.

Nella prossima sezione vedremo un esempio di applicazione di questo teorema.

1.2 Campi di numeri

Lo studio delle estensioni algebriche finite del campo $\mathbb{Q}$ dei numeri razionali è uno degli ambiti principali di studio della Teoria algebrica dei numeri. In questa sezione applicheremo la teoria generale dei domini di Dedekind agli anelli degli interi algebrici.

Definizione 1.2.1. Un *campo di numeri algebrici*, o *campo di numeri* (*algebraic number field*) K è un'estensione $K/\mathbb{Q}$ algebrica finita: $[K : \mathbb{Q}] < \infty$.

Esempio 1.2.1. Sono esempi di campi di numeri:

- $\mathbb{Q}$ stesso;
- $\mathbb{Q}(\sqrt{d})$, con d un intero non divisibile da quadrati perfetti; queste estensioni sono dette *estensioni quadratiche*;
- $\mathbb{Q}(\zeta_m)$, con ζ_m una radice primitiva m-esima di $1 \in \mathbb{C}$; questa estensione si chiama *estensione ciclotomica m-esima.*
- $\mathbb{Q}(\alpha)$, con $\alpha \in \mathbb{C}$ numero algebrico su $\mathbb{Q}$.

Non sono campi di numeri le estensioni trascendenti: $\mathbb{Q}(\pi)$, $\mathbb{Q}(e)$, $\mathbb{R}$, $\mathbb{C}$, etc.

Definizione 1.2.2. Un'estensione $K/\mathbb{Q}$ finita, normale e separabile si dice *abeliana* se il gruppo di Galois $Gal(K/\mathbb{Q})$ è abeliano. Le estensioni quadratiche sono abeliane, con gruppo di Galois ciclico di ordine 2; l'estensione ciclotomica m-esima è abeliana, con gruppo di Galois isomorfo a $U(\mathbb{Z}/m\mathbb{Z})$.

Definizione 1.2.3. Dato K un campo di numeri, l'*anello degli interi algebrici di K* è la chiusura integrale di $\mathbb{Z}$ in K.
Esso è l'insieme

$$O_K \equiv \{\alpha \in K \mid f_\alpha \in \mathbb{Z}[x], f_\alpha \text{ polinomio minimo di } \alpha \text{ su } \mathbb{Q}\}.$$

Esempio 1.2.2. Data una qualsiasi estensione $K/\mathbb{Q}$ algebrica finita, non è immediato determinarne l'anello degli interi O_K. Abbiamo visto in 1.1.6 che l'anello degli interi in $\mathbb{Q}(i)$ è effettivamente $\mathbb{Z}[i]$, tuttavia non è in generale vero che l'anello degli interi di $\mathbb{Q}(\alpha)$ sia $\mathbb{Z}[\alpha]$: questo è falso anche nel caso di alcune estensioni quadratiche, che è il più semplice possibile. Infatti, da quanto visto nell'esempio 1.1.4 segue che l'anello degli interi di $\mathbb{Q}(\sqrt{5})$ non è $\mathbb{Z}[\sqrt{5}]$. Il problema di trovare l'anello degli interi O_K può essere computazionalmente molto complesso; ci limitiamo a enunciare i seguenti risultati, per le estensioni quadratiche e ciclotomiche:

Teorema 1.2.1. *Sia $d \in \mathbb{Z}$ un intero non divisibile da alcun quadrato perfetto, e $K = \mathbb{Q}(\sqrt{d})$. Allora l'anello degli interi algebrici di K è*

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], \text{ se } d \equiv 1 \text{(mod 4)};$$

$$\mathbb{Z}[\sqrt{d}], \text{ se } d \equiv 2, 3 \text{(mod 4)}.$$

Teorema 1.2.2. *Sia $K = \mathbb{Q}(\zeta_m)$ il campo ciclotomico m-esimo. Allora l'anello degli interi algebrici di $\mathbb{Q}(\zeta_m)$ è*

$$O_K = \mathbb{Z}[\zeta_m].$$

Enunciamo ora un teorema fondamentale.

Teorema 1.2.3. *Sia A un dominio di Dedekind, K il suo campo dei quozienti, L/K un'estensione finita di K. Allora la chiusura integrale di A in L è un dominio di Dedekind.*

Applicando questo teorema con $A = \mathbb{Z}$, $K = \mathbb{Q}$, e $L/\mathbb{Q}$ estensione algebrica finita, si trova che O_L, l'anello degli interi algebrici di L, è un dominio di Dedekind: questo spiega l'importanza di questi anelli.

Esempio 1.2.3. Vediamo un esempio di applicazione di questi risultati, e di fattorizzazione degli ideali nei domini di Dedekind.

Consideriamo il campo $K = \mathbb{Q}(\sqrt{-5})$. Il Teorema 1.2.1 implica che $O_K = \mathbb{Z}[\sqrt{-5}]$, perché $-5 \equiv -1 \equiv 3 \pmod 4$. Dunque, per il Teorema 1.2.3, $\mathbb{Z}[\sqrt{-5}]$ è un dominio di Dedekind. Osserviamo che questo anello non è un UFD: il numero 6, ad esempio, ha due distinte fattorizzazioni:

$$2 \cdot 3 = 6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5});$$

Analogamente all'esempio 1.1.7, definendo la norma $N(a+b\sqrt{-5}) \equiv (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$, si trova che $2, 3, (1+\sqrt{-5})$ e $(1-\sqrt{-5})$ sono elementi irriducibili e non associati, quindi le fattorizzazioni sono diverse. Il Teorema 1.1.1 ci dice però che in $\mathbb{Z}[\sqrt{-5}]$ (benché fallisca la fattorizzazione unica degli elementi) vale la fattorizzazione unica degli ideali: si ha infatti che

$$(6) = (2, 1+\sqrt{-5})^2 (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \equiv \mathfrak{p}_1{}^2 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

Questo è conseguenza delle seguenti uguaglianze:

$$(2, 1+\sqrt{-5})^2 = (2)$$
$$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$$
$$(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (1+\sqrt{-5})$$
$$(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1-\sqrt{-5}).$$

Queste quattro uguaglianze si dimostrano con le doppie inclusioni; la primalità degli ideali $\mathfrak{p}_i$ si prova costruendo opportuni omomorfismi tra $\mathbb{Z}$ e $\frac{\mathbb{Z}[\sqrt{-5}]}{\mathfrak{p}_i}$, per mostrare che questi quozienti sono domini di integrità.

1.3 Ideali frazionari

Per definire gli *ideali frazionari* di un campo è necessario ricordare la definizione di *modulo*.

Definizione 1.3.1. Sia A un anello. Un *modulo su* A, o A*-modulo*, è un gruppo abeliano $(M, +, 0)$ dotato di una mappa

$$\mu\colon A \times M \to M, \quad (a, x) \mapsto \mu(a, x) \equiv ax$$

t.c.:

(a) $a(x+y) = ax + ay \quad \forall\, a \in A$ e $\forall\, x, y \in M$;

(b) $(a+b)x = ax + bx \quad \forall\, a, b \in A$ e $\forall\, x \in M$;

(c) $(ab)x = a(bx) \quad \forall\, a, b \in A$ e $\forall\, x \in M$;

(d) $1x = x \quad \forall\, x \in M$.

Esempio 1.3.1. Se A è un anello e $I \triangleleft A$ un ideale, I è un A-modulo: è un gruppo abeliano e la moltiplicazione per gli scalari μ è ben definita grazie alla proprietà di assorbimento di I. In particolare, A stesso è un A-modulo.

Se $A = K$ è un campo, la nozione di A-modulo equivale a quella di K-spazio vettoriale.

Se $A = \mathbb{Z}$, uno $\mathbb{Z}$-modulo M è un gruppo abeliano: $nx \equiv x + \cdots + x \quad \forall\, x \in M, \forall\, n \in \mathbb{Z}$.

La nozione di *insieme di generatori* per un modulo si definisce in modo analogo a quella per gli spazi vettoriali:

Definizione 1.3.2. Sia M un A-modulo; un insieme $\{x_i \mid i \in I\} \subset M$ di elementi di M è un *insieme di generatori* per M se ogni elemento di M può essere scritto (non in modo unico, in generale) come combinazione lineare finita a coefficienti in A degli x_i:

$$\forall\, x \in M\ \exists\, a_1, \ldots, a_n \in A \text{ t.c. } x = \sum_{i=1}^{n} a_i x_i.$$

Se M ammette un insieme finito di generatori, M si dice A-modulo *finitamente generato*.

La seguente proposizione è una caratterizzazione dell'integralità degli elementi su un anello tramite la nozione di "modulo finitamente generato".

Proposizione 1.3.1. *Siano $A \subset A'$ anelli, e $b \in A'$. Sono equivalenti le seguenti affermazioni:*

1. *b è intero su A;*
2. *$A[b]$ è un A-modulo finitamente generato;*
3. *$\exists\, B \subset A'$ sottoanello che è un A-modulo finitamente generato e t.c. $A[b] \subset B$.*

Definizione 1.3.3. Siano A un dominio e K il suo campo dei quozienti. Un sottoinsieme $\mathfrak{M} \subset K$ è detto *ideale frazionario di A* (oppure *di K*) se è un A-sottomodulo di K con la proprietà che $\exists\, y \in A$, $y \neq 0$, t.c. $y\mathfrak{M} \subset A$.
Ogni ideale di A è un ideale frazionario: basta prendere $y = 1$. Gli ideali di A sono anche detti *ideali interi di K*.

Osservazione 1.3.1. Gli ideali frazionari di A sono della forma $y^{-1}I$, con $y \in A$ e $I \lhd A$.
Infatti, dalla definizione di ideale frazionario segue che $y\mathfrak{M} \lhd A$; dunque $\mathfrak{M} = y^{-1}(y\mathfrak{M})$, come affermato.

Esempio 1.3.2. Ogni elemento $y \in K^*$ genera un ideale frazionario, così definito: $yA = \{ya \,|\, a \in A\}$. Questi ideali frazionari sono detti *principali*.

Consideriamo ora $A = \mathbb{Z}$ e $K = \mathbb{Q}$; un ideale frazionario di $\mathbb{Z}$ è necessariamente della forma $\mathfrak{M} = \frac{1}{n}I$ con $n \in \mathbb{Z}$, $n \neq 0$ e $I \lhd \mathbb{Z}$; dunque $I = m\mathbb{Z}$, $m \in \mathbb{Z}$, $m \neq 0$ e allora $\mathfrak{M} = \frac{1}{n}(m\mathbb{Z}) = \frac{m}{n}\mathbb{Z}$, cioè è l'ideale frazionario principale generato da $\frac{m}{n}$. Quindi

$$\{\text{ideali frazionari di } \mathbb{Z}\} = \{q\mathbb{Z} \,|\, q \in \mathbb{Q}^*\} :$$

gli ideali frazionari di $\mathbb{Z}$ sono tutti principali.

Vediamo una caratterizzazione equivalente degli ideali frazionari per i domini di Dedekind.

Proposizione 1.3.2. *Siano A un dominio di Dedekind e K il suo campo dei quozienti; $\mathfrak{M} \subset K$ un A-sottomodulo di K.*
$\mathfrak{M}$ è un ideale frazionario $\iff$ è un A-sottomodulo di K finitamente generato.

Dimostrazione. ($\Rightarrow$) Sia $\mathfrak{M} \subset K$ un ideale frazionario: $\exists\, y \in A$, $y \neq 0$, t.c. $y\mathfrak{M} \lhd A$, e $\mathfrak{M} = y^{-1}I$, $I \lhd A$. Poichè A è un dominio di Dedekind, l'ideale I è finitamente generato: $I = (x_1, \ldots, x_n)$, $x_i \in A$. Allora $\mathfrak{M} = y^{-1}I = (y^{-1}x_1, \ldots, y^{-1}x_n)$, cioè è finitamente generato come A-sottomodulo di K.

($\Leftarrow$) Viceversa, sia $\mathfrak{M} \subset K$ un sottomodulo generato da $\{w_1, \ldots, w_n\} \subset \mathfrak{M}$; cioè,

$$x \in \mathfrak{M} \iff x = \sum_{i=1}^{n} x_i w_i, \quad x_i \in A.$$

Poiché i w_i sono in numero finito, possiamo trovare un comune denominatore per essi, e scrivere $w_i = \frac{y_i}{w}$, con $y_i, w \in A$. Allora

$$x \in \mathfrak{M} \iff x = \sum_{i=1}^{n} x_i \frac{y_i}{w}, \quad x_i \in A.$$

Dall'ultima espressione segue che $w\mathfrak{M} \subset A$, cioè $\mathfrak{M}$ è un ideale frazionario. □

Vediamo ora che, nei domini di Dedekind, l'insieme di tutti gli ideali frazionari può essere munito di una struttura di gruppo.

Definiamo infatti la moltiplicazione tra ideali frazionari in modo analogo a quella tra ideali interi: dati $\mathfrak{M}, \mathfrak{N}$ ideali frazionari di un dominio A, l'ideale frazionario prodotto è definito da

$$\mathfrak{MN} \equiv \left\{ \sum_{i=1}^{k} m_i n_i \,|\, k \in \mathbb{N}, m_i \in \mathfrak{M}, n_i \in \mathfrak{N} \right\}.$$

$\mathfrak{MN}$ è effettivamente un ideale frazionario: è un sottomodulo di K e se $\mathfrak{M}$ è generato da $\{x_1, \ldots, x_m\}$ e $\mathfrak{N}$ da $\{y_1, \ldots, y_n\}$, allora $\mathfrak{MN}$ è generato da $\{x_i y_j \,|\, i = 1, \ldots, m, j = 1, \ldots, n\}$.

Si verifica che questa operazione è associativa, ossia che $\mathfrak{M}(\mathfrak{NO}) = (\mathfrak{MN})\mathfrak{O}$, e commutativa: $\mathfrak{MN} = \mathfrak{NM}$.

Osserviamo inoltre che A ha il ruolo dell'elemento neutro:

$$A\mathfrak{M} = \left\{ \sum_{i=1}^{k} a_i m_i \,|\, k \in \mathbb{N}, a_i \in A, m_i \in \mathfrak{M} \right\} = \mathfrak{M}.$$

Dobbiamo ora mostrare che, se A è un dominio di Dedekind, ogni ideale frazionario è invertibile.

Definizione 1.3.4. Siano A un dominio di Dedekind e $\mathfrak{M}$ un ideale frazionario. Definiamo

$$\mathfrak{M}^{-1} \equiv \{x \in K \,|\, x\mathfrak{M} \subset A\}.$$

Anche $\mathfrak{M}^{-1}$ è un ideale frazionario: presi $x, y \in \mathfrak{M}^{-1}$ e $a \in A$, allora $x-y, ax \in \mathfrak{M}^{-1}$, perché $(x-y)m$, $axm \in A \;\forall\, m \in \mathfrak{M}$; infine, $z\mathfrak{M}^{-1} \subset A \;\forall z \in \mathfrak{M}$.

Un ideale frazionario $\mathfrak{M}$ si dice *invertibile* se

$$\mathfrak{MM}^{-1} = A,$$

e in questo caso $\mathfrak{M}^{-1}$ è detto *ideale frazionario inverso di* $\mathfrak{M}$.

Esempio 1.3.3. Ogni ideale frazionario principale yA è invertibile, con inverso $(yA)^{-1} = y^{-1}A$.

Infatti, $(yA)(y^{-1}A) = (yy^{-1}A) = A$.

Lemma 1.3.1. *Per ogni $\mathfrak{p} \lhd A$ ideale primo di un dominio di Dedekind A $\exists\, x \in K \setminus A$ t.c. $x \in \mathfrak{p}^{-1}$.*

Dimostrazione. Sia $a \in \mathfrak{p}$; se $(a) = \mathfrak{p}$ allora $\mathfrak{p}$ è principale, quindi invertibile, con $\mathfrak{p}^{-1} = (a^{-1})$. Allora la tesi è verificata con $x = a^{-1}$: se $a^{-1} \in A$, allora $\mathfrak{p}$ conterrebbe 1, assurdo.

Scriviamo la fattorizzazione di (a):

$$\mathfrak{p}_1{}^{a_1} \dots \mathfrak{p}_n{}^{a_n} \mathfrak{p}^m = (a) \subset \mathfrak{p}, \quad \text{con } n \geq 0, m > 1;$$

$\mathfrak{p}$ compare nella fattorizzazione perché contiene (a) (Teorema 1.1.1). Chiamiamo $\mathfrak{b}$ l'ideale $\mathfrak{p}_1{}^{a_1} \dots \mathfrak{p}_n{}^{a_n} \mathfrak{p}^{m-1}$, sicché $(a) = \mathfrak{b}\mathfrak{p}$.

Poiché $\mathfrak{b}\mathfrak{p} \subset \mathfrak{b}$ e l'inclusione è propria (per via della fattorizzazione unica di (a)), allora $\exists\, b \in \mathfrak{b} \setminus (a)$; tale b non è diviso da a, dunque $x \equiv b/a = a^{-1}b \notin A$.

Mostriamo infine che $x \in \mathfrak{p}^{-1}$:

$$x\mathfrak{p} = a^{-1}b\mathfrak{p} \subset a^{-1}\mathfrak{b}\mathfrak{p} = a^{-1}(a) = A.$$

□

Teorema 1.3.1. *Se A è un dominio di Dedekind, ogni ideale primo non nullo di A è invertibile.*

Dimostrazione. Consideriamo $\mathfrak{p} \triangleleft A$ ideale primo, e l'ideale frazionario $\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subset A\}$; mostriamo che $\mathfrak{p}\mathfrak{p}^{-1} = A$. Proviamo le due seguenti affermazioni:

$$\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \triangleleft A, \tag{1.1}$$

$$\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}; \tag{1.2}$$

poiché $\mathfrak{p}$ è un ideale massimale di A, da (1.1) e (1.2) segue la tesi.

(1.1) $1 \in \mathfrak{p}^{-1}$ perché $\mathfrak{p}$ è un ideale intero, quindi $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$; dalla definizione di $\mathfrak{p}^{-1}$ segue che un prodotto xy con $x \in \mathfrak{p}, y \in \mathfrak{p}^{-1}$ appartiene ad A, e allora vale l'inclusione $\mathfrak{p}\mathfrak{p}^{-1} \subset A$. Poiché $\mathfrak{p}\mathfrak{p}^{-1}$ è un A-modulo e un sottoinsieme di A, è un ideale di A.

(1.2) Sia per assurdo $\mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}$. Questo implica che $\mathfrak{p}^{-1}$ è moltiplicativamente chiuso: siano infatti $a, b \in \mathfrak{p}^{-1}$, e mostriamo che $ab \in \mathfrak{p}^{-1}$ verificando che soddisfa la proprietà di definizione di $\mathfrak{p}^{-1}$. Preso $x \in \mathfrak{p}$, si ha che

$$bx \in \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p},$$

dunque $(ab)x = a(bx) \in A$.

Quindi $\mathfrak{p}^{-1}$, che è un A-modulo finitamente generato, è anche un anello; si ha $A \subset \mathfrak{p}^{-1}$, e l'inclusione (di anelli) è propria, per il lemma 1.3.1. Sia $b \in \mathfrak{p}^{-1} \setminus A$: abbiamo che

$$A \subset A[b] \subset \mathfrak{p}^{-1}.$$

La proposizione 1.3.1 implica che b è un elemento intero di A che non vi appartiene: questo è assurdo perché A è integralmente chiuso. □

Teorema 1.3.2. *Siano A un dominio di Dedekind e K il suo campo dei quozienti. Ogni ideale frazionario $\mathfrak{M}$ di A si può scrivere in modo unico come prodotto*

$$\mathfrak{M} = \mathfrak{P}_1{}^{a_1} \dots \mathfrak{P}_n{}^{a_n} \mathfrak{Q}_1{}^{-b_1} \dots \mathfrak{Q}_m{}^{-b_m},$$

con $\mathfrak{P}_i, \mathfrak{Q}_j$ ideali primi di A e $a_i, b_j \in \mathbb{N}$; con $\mathfrak{Q}^{-n}, n > 0$, si intende $(\mathfrak{Q}^{-1})^n$.

Dimostrazione. Sia $\mathfrak{M}$ un ideale frazionario, e $s \in A$ t.c. $s\mathfrak{M} \triangleleft A$. Il Teorema 1.1.1 implica che gli ideali $s\mathfrak{M}$ e $(s) = sA$ si fattorizzano come

$$s\mathfrak{M} = {\mathfrak{P}_1}^{a_1} \dots {\mathfrak{P}_n}^{a_n},$$
$$sA = {\mathfrak{Q}_1}^{b_1} \dots {\mathfrak{Q}_m}^{b_m},$$

con $\mathfrak{P}_i, \mathfrak{Q}_j$ ideali primi di A e $a_i, b_j \in \mathbb{N}$.

Allora, poiché $s\mathfrak{M} = (s)\mathfrak{M}$ e gli ideali $\mathfrak{P}_i, \mathfrak{Q}_j$ sono invertibili per il Teorema 1.3.1, segue che

$$\mathfrak{M} = {\mathfrak{P}_1}^{a_1} \dots {\mathfrak{P}_n}^{a_n} {\mathfrak{Q}_1}^{-b_1} \dots {\mathfrak{Q}_m}^{-b_m}.$$

La fattorizzazione è unica, sempre per il Teorema 1.3.1.

□

Possiamo quindi dare la seguente definizione.

Definizione 1.3.5. Dati A un dominio di Dedekind e K il suo campo dei quozienti, l'insieme

$$I_K = I(A) \equiv \{\text{ideali frazionari di } A\}$$

è detto *gruppo degli ideali di A*.

Dalla discussione precedente segue che $I(A)$ è il gruppo abeliano libero generato da tutti gli ideali primi di A, ossia da $Spec(A)$.

1.4 Fattorizzazione degli ideali primi nelle estensioni

Consideriamo un dominio di Dedekind A, con K campo dei quozienti (in seguito ci interesserà il caso in cui K è un campo di numeri algebrici e $A = O_K$), e L una estensione algebrica finita di K; la chiusura integrale B di A in L è anch'essa un dominio di Dedekind per il Teorema 1.2.3; in questa sezione esamineremo le relazioni sussistenti tra gli ideali di A e quelli di B. Cominciamo osservando che un ideale $I \triangleleft A \subset B$ di A non è in generale un ideale di B: non avrà la proprietà di assorbimento. Si pensi ad esempio a $A = \mathbb{Z}, B = \mathbb{Z}[i], I = (2) = 2\mathbb{Z} \subset \mathbb{Z}[i]$.

Dato un ideale primo $\mathfrak{p} \triangleleft A$, possiamo considerare l'ideale $\mathfrak{p}B \triangleleft B$, ossia il più piccolo ideale di B che contiene $\mathfrak{p}$; non sarà primo in generale. Per il Teorema 1.1.1, esso avrà una fattorizzazione in ideali primi di B:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Vediamo ora che tra gli ideali $\mathfrak{P}_i$ e $\mathfrak{p}$ ci sono dei legami particolari. Detto $\mathfrak{P}$ un ideale che compare nella fattorizzazione, l'insieme $\mathfrak{P} \cap A$ è un ideale di A; mostriamo che è esattamente $\mathfrak{p}$.

$\mathfrak{P} \cap A$ è propriamente contenuto in A, perché $1 \notin \mathfrak{P}$. Poiché la mappa

$$\phi\colon \frac{A}{\mathfrak{P} \cap A} \to \frac{B}{\mathfrak{P}},$$
$$x + \mathfrak{P} \cap A \mapsto x + \mathfrak{P}$$

è un ben definito omomorfismo iniettivo di anelli, vediamo che il *campo* (perché $\mathfrak{P}$ è massimale, dal momento che B è dominio di Dedekind) $\frac{B}{\mathfrak{P}}$ contiene una copia isomorfa dell'anello $\frac{A}{\mathfrak{P}\cap A}$; quest'ultimo è dunque un dominio. Quindi $\mathfrak{P}\cap A$ è un ideale primo di A; e allora il dominio $\frac{A}{\mathfrak{P}\cap A}$ è anch'esso un campo, perché l'ideale $\mathfrak{P}\cap A$ è massimale in A.

Inoltre questo ideale contiene $\mathfrak{p}$, perché $A \supset \mathfrak{p}$ e $\mathfrak{P} \supset \mathfrak{p}B \supset \mathfrak{p}$.
Ma allora le inclusioni

$$\mathfrak{p} \subset \mathfrak{P} \cap A \subset A$$

e il fatto che $\mathfrak{p}$ e $\mathfrak{P}\cap A$ sono ideali primi di A implicano che

$$\mathfrak{P} \cap A = \mathfrak{p},$$

perché gli ideali primi di A sono massimali.

Introduciamo la terminologia della *ramificazione*.

Definizione 1.4.1. Nel contesto di cui sopra, diciamo che i primi $\mathfrak{P}_i$ che compaiono nella fattorizzazione di $\mathfrak{p}B$ *dividono* $\mathfrak{p}$.

Se $\exists\, i$ t.c. $e_i > 1$, si dice che $\mathfrak{p}$ (e dunque anche $\mathfrak{P}_i$) *ramifica* (o *è ramificato*) *in* B (o *in* L), e il numero

$$e(\mathfrak{P}_i/\mathfrak{p}) \equiv e_i$$

è detto *indice di ramificazione* (*di* $\mathfrak{P}_i$).

Il numero

$$f(\mathfrak{P}_i/\mathfrak{p}) \equiv \left[\frac{B}{\mathfrak{P}_i} : \frac{A}{\mathfrak{p}}\right],$$

grado dell'estensione di campi $\frac{B}{\mathfrak{P}_i}/\frac{A}{\mathfrak{P}_i\cap A}$, è detto *grado di inerzia* (*residue class degree*) di $\mathfrak{P}_i$ su $\mathfrak{p}$.

Un primo $\mathfrak{p}\triangleleft A$ *spezza completamente* (*splits completely*) in L se $e_i = f_i = 1\,\forall\, i$; è detto *inerte* se $\mathfrak{p}B$ è un ideale primo di B, cioè se $g = 1$ ed $e_1 = 1$.

Osservazione 1.4.1. Abbiamo visto che, se $\mathfrak{P}_i \triangleleft B$ primo divide $\mathfrak{p} \triangleleft A$, allora $\mathfrak{P}_i \cap A = \mathfrak{p}$. Si vede così che l'indice di ramificazione e_i è completamente determinato dal solo $\mathfrak{P}_i$. Si può cioè definire, per ogni ideale primo $\mathfrak{P} \triangleleft B$, l'*indice di ramificazione di* $\mathfrak{P}$ *rispetto ad* A come il numero

$$e(\mathfrak{P}/A) \equiv e(\mathfrak{P}/\mathfrak{P}\cap A),$$

ossia l'esponente con cui compare $\mathfrak{P}$ nella fattorizzazione di $(\mathfrak{P}\cap A)B$.

Vediamo alcuni esempi di questi concetti.

Esempio 1.4.1. Siano $A = \mathbb{Z}$, $K = \mathbb{Q}$, $B = \mathbb{Z}[\sqrt{-5}]$, $L = \mathbb{Q}(\sqrt{-5})$. Consideriamo gli ideali $\mathfrak{p} = (2), \mathfrak{q} = (3) \triangleleft \mathbb{Z}$, primi. In $\mathbb{Z}[\sqrt{-5}]$ abbiamo le seguenti fattorizzazioni, come visto nell'esempio 1.2.3:

$$(2) = (2, 1 + \sqrt{-5})^2,$$

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Dunque, in $\mathbb{Z}[\sqrt{-5}]$, (2) ramifica con $e = 2$, mentre (3) spezza completamente (si verifica che $f_1 = f_2 = 1$), e in particolare non è ramificato.

Esempio 1.4.2. Siano ora $A = \mathbb{Z}$, $K = \mathbb{Q}$, $B = \mathbb{Z}[i]$, $L = \mathbb{Q}(i)$. Consideriamo gli ideali $(2), (3), (5) \triangleleft \mathbb{Z}$, primi. In $\mathbb{Z}[i]$ abbiamo le seguenti fattorizzazioni:

$$(2) = (1 + i)(1 - i) = (1 + i)^2,$$

$$(3) = 3\mathbb{Z}[i] = (3),$$

$$(5) = (2 + i)(2 - i).$$

Ossia (2) ramifica; (3) è inerte, con $f = 2$ (resta un ideale primo); (5) spezza completamente nel prodotto di due ideali primi. Notiamo che, poiché $\mathbb{Z}[i]$ è un PID, la fattorizzazione degli ideali corrisponde alla fattorizzazione in elementi irriducibili dei generatori.

Osserviamo che, in questo esempio e nel precedente, per ogni $\mathfrak{p} \triangleleft \mathbb{Z}$ si ha $efg = 2 = [L : \mathbb{Q}]$: si veda il Teorema 1.4.2.

Proposizione 1.4.1. *Siano $K < L$ campi di numeri; per ogni ideale $\mathfrak{p} \triangleleft O_K$ e per ogni $\mathfrak{P} \triangleleft O_L$ che lo divide, i campi $\frac{O_L}{\mathfrak{P}}$ e $\frac{O_K}{\mathfrak{p}}$ sono finiti. Inoltre, se $E > L$ e $\mathfrak{Q} \triangleleft O_E$ divide $\mathfrak{P}$, allora*

$$f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}).$$

Enunciamo ora due importanti risultati.

Teorema 1.4.1. *Sia K un campo di numeri algebrici, L/K un'estensione finita, O_K e O_L i rispettivi anelli degli interi algebrici. Solo un numero finito di ideali primi di O_K ramifica in L.*

Nel caso particolare di $K = \mathbb{Q}$ e $L = \mathbb{Q}(\zeta_m)$ (estensione ciclotomica m-esima), gli unici $(p) \triangleleft \mathbb{Z}$ che ramificano in $\mathbb{Q}(\zeta_m)$ sono gli ideali generati dai divisori primi di m.

Teorema 1.4.2. *Siano A un dominio di Dedekind, K il suo campo dei quozienti, L un'estensione finita e separabile di K, B la chiusura integrale di A in L. Sia $\mathfrak{p}$ un ideale primo di A con fattorizzazione in B data da*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g};$$

Allora si ha che

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Se poi L/K è normale, allora il gruppo di Galois $G \equiv Gal(L/K)$ agisce transitivamente sull'insieme $\{\mathfrak{P}_1, \dots \mathfrak{P}_g\}$ (l'azione è: $\forall \sigma \in G, \sigma\mathfrak{P} \equiv \sigma(\mathfrak{P})$); inoltre

$$e_1 = \dots = e_g \equiv e,$$

$$f_1 = \dots = f_g \equiv f,$$

e dunque

$$\mathfrak{p}B = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e,$$
$$efg = [L : K].$$

1.5 Valutazioni

Definizione 1.5.1. Sia K un campo. Una *valutazione discreta su* K, o *valutazione esponenziale su* K, è un omomorfismo di gruppi non banale

$$v \colon K^* \to \mathbb{Z}$$

tale che

$$v(x+y) \geq min\{v(x), v(y)\} \quad \forall\, x, y \in K^*.$$

A volte si pone, per convenzione, $v(0) = \infty$.

Esempio 1.5.1. Siano A un dominio di Dedekind, K il suo campo dei quozienti e $\mathfrak{P} \triangleleft A$ un ideale primo di A. Per ogni $x \in K^*$ definiamo $v_{\mathfrak{P}}(x)$ come l'esponente di $\mathfrak{P}$ nella fattorizzazione dell'ideale frazionario (x); si ha cioè

$$(x) = xA = \prod \mathfrak{P}^{v_{\mathfrak{P}}(x)},$$

dove il prodotto è preso su tutti gli ideali primi di A (e $v_{\mathfrak{P}}(x) \neq 0$ solo per un numero finito di ideali).

Consideriamo il caso $A = \mathbb{Z}$, $K = \mathbb{Q}$, $\mathfrak{P} = p\mathbb{Z}$. Ogni numero razionale non nullo $q = \frac{c}{d}$ si può scrivere come $q = p^m \frac{a}{b}$, con $m \in \mathbb{Z}$ e $(a, p) = (b, p) = 1$. Allora si ha che $v_p(q) \equiv v_{p\mathbb{Z}}(q) = m$, perché la fattorizzazione dell'ideale frazionario (q) in ideali primi di $\mathbb{Z}$ corrisponde alle fattorizzazioni di c e d.

Dimostriamo che in questo caso v_p è effettivamente una valutazione discreta.

1. $v_p(qr) = v_p\left(p^m \frac{a}{b} p^n \frac{c}{d}\right) = v_p\left(p^{m+n} \frac{ac}{bd}\right) = m + n = v_p(q) + v_p(r)$;
2. supponiamo $m \geq n$: allora

$$v_p(q+r) = v_p\left(p^m \frac{a}{b} + p^n \frac{c}{d}\right) = v_p\left(p^n \left(p^{m-n} \frac{a}{b} + \frac{c}{d}\right)\right) =$$

$$v_p\left(p^n\right) + v_p\left(p^{m-n} \frac{a}{b} + \frac{c}{d}\right) = n + v_p\left(\frac{p^{m-n}ad + bc}{bd}\right) =$$

$$= n + v_p\left(\frac{1}{bd}\right) + v_p\left(p^{m-n}ad + bc\right) \geq n,$$

perché

$$v_p\left(\frac{1}{bd}\right) = 0$$

e

$$p^{m-n}ad + bc \in \mathbb{Z} \Rightarrow v_p\left(p^{m-n}ad + bc\right) \geq 0.$$

Definizione 1.5.2. Sia K un campo. Una funzione

$$|\cdot|\colon K \to \mathbb{R}, \quad x \mapsto |x|$$

si dice *valutazione su* K, o *valore assoluto*, se

1. $|x| \geq 0$, e $|x| = 0 \iff x = 0$;
2. $|xy| = |x||y|$, cioè $|\cdot|$ è un omomorfismo di gruppi moltiplicativi di K^* in $\mathbb{R}^+$;
3. $|x + y| \leq |x| + |y|$ (disuguaglianza triangolare).

Se la valutazione soddisfa anche la condizione

$$|x + y| \leq max\{|x|, |y|\}$$

allora è detta *valutazione non archimedea*; altrimenti è detta *archimedea*.

Esempio 1.5.2. Sia $K \subset \mathbb{R}$ un sottocampo dei numeri reali. L'usuale valore assoluto è una valutazione archimedea; non vale in generale che $|x + y| \leq max\{|x|, |y|\}$: $2 = |1 + 1| > max\{|1|, |1|\} = 1$.

Esempio 1.5.3. Siano A un dominio di Dedekind e K il suo campo dei quozienti; $\mathfrak{P} \triangleleft A$ un ideale primo di A. La mappa $v_{\mathfrak{P}}$ è una valutazione esponenziale (valutazione discreta su K). A partire da $v_{\mathfrak{P}}$ e da un qualsiasi $a \in (0, 1) \subset \mathbb{R}$ si ottiene una valutazione non archimedea su K definendo

$$|x|_{\mathfrak{P}} \equiv a^{v_{\mathfrak{P}}(x)}.$$

Infatti:

1. se $x \neq 0$ allora $|x|_{\mathfrak{P}} = a^{v_{\mathfrak{P}}(x)} > 0$, perché è un'esponenziale; $|0|_{\mathfrak{P}} = 0$, per convenzione;
2. $|xy|_{\mathfrak{P}} = a^{v_{\mathfrak{P}}(xy)} = a^{v_{\mathfrak{P}}(x)+v_{\mathfrak{P}}(y)} = a^{v_{\mathfrak{P}}(x)} a^{v_{\mathfrak{P}}(y)} = |x|_{\mathfrak{P}}|y|_{\mathfrak{P}}$;
3. $|x + y|_{\mathfrak{P}} = a^{v_{\mathfrak{P}}(x+y)} \leq a^{min\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\}} = max\{a^{v_{\mathfrak{P}}(x)}, a^{v_{\mathfrak{P}}(y)}\}$. La disuguaglianza segue da

   $$v_{\mathfrak{P}}(x + y) \geq min\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\}$$

   e da $a < 1$.

La valutazione non archimedea ottenuta dalla valutazione discreta $v_{\mathfrak{P}}$ si chiama *valutazione* $\mathfrak{P}$*-adica su* K.

Nel caso $A = \mathbb{Z}$, $K = \mathbb{Q}$ abbiamo quindi, per ogni primo $p \in \mathbb{Z}$, la *valutazione p-adica* su $\mathbb{Q}$:

$$|q|_p \equiv a^{v_p(q)}.$$

Definizione 1.5.3. Diciamo che due valutazioni $|\cdot|_1$, $|\cdot|_2$ su K sono *equivalenti* se

$$|x|_1 < 1 \iff |x|_2 < 1.$$

Con questa relazione di equivalenza si trova che, nella costruzione della valutazione $\mathfrak{P}$-adica, scelte diverse di $a \in (0, 1)$ producono valutazioni equivalenti.

Per la valutazione p-adica su $\mathbb{Q}$ si effettua solitamente la scelta $a = \frac{1}{p}$, cosicché $|p|_p = \frac{1}{p}^{v_p(p)} = \frac{1}{p}^1 = \frac{1}{p}$.

Il seguente risultato fornisce una descrizione di tutte le classi di equivalenza di valutazioni su $\mathbb{Q}$.

Proposizione 1.5.1. *Ogni valutazione non archimedea su $\mathbb{Q}$ è equivalente a una valutazione p-adica per un certo primo p, e sarà indicata con $|\cdot|_p$; ogni valutazione archimedea su $\mathbb{Q}$ è equivalente all'usuale valore assoluto, e sarà indicata con $|\cdot|$ o con $|\cdot|_\infty$.*

Definizione 1.5.4. Sia K un campo. Una classe di equivalenza di valutazioni su K è detta un *posto* di K, o un *primo* di K. Denoteremo i posti di un campo con $\mathfrak{p}, \mathfrak{q}, \mathfrak{P}, \mathfrak{Q}$.

Una classe di equivalenza di valutazioni non archimedee è detta *primo finito di K*; una classe di equivalenza di valutazioni archimedee è detta *primo infinito di K*. Questa notazione riflette il fatto che, per $K = \mathbb{Q}$,

$$\{\text{primi finiti di } \mathbb{Q}\} \longleftrightarrow \{p \in \mathbb{Z} \,|\, p \text{ è primo}\},$$

$$\{\text{primi infiniti di } \mathbb{Q}\} \longleftrightarrow \{|\cdot|_\infty\}.$$

Una valutazione $|\cdot|$ su un campo K permette di generalizzare il procedimento di costruzione di $\mathbb{R}$ come l'insieme delle classi di equivalenza di successioni di Cauchy di numeri razionali: una successione $\{a_n\} \subset K$ si dice *di Cauchy* se $\lim_{m,n\to\infty} |a_n - a_m| = 0$, e tale successione *converge* ad a se $\lim_{n\to\infty} |a - a_n| = 0$; diciamo che K è *completo* se ogni successione di Cauchy converge a un elemento di K.

Si definisce poi la seguente relazione, che si verifica essere di equivalenza: due successioni di Cauchy $\{a_n\}, \{b_n\}$ sono equivalenti se $\lim_{n\to\infty} |a_n - b_n| = 0$; $\{a_n\}^*$ denota la classe di equivalenza della successione $\{a_n\}$. Si verifica poi che l'insieme

$$\hat{K} \equiv \{\{a_n\}^* \,|\, \{a_n\} \text{ è una successione di Cauchy in } K\},$$

dotato delle operazioni di addizione e moltiplicazione effettuate componente per componente, è un campo che contiene K attraverso l'identificazione di $a \in K$ con la successione costante $\{a\}$.

Infine si estende la valutazione $|\cdot|$ a $\hat{K}$ definendo

$$|\{a_n\}^*| \equiv \lim_{n\to\infty} |a_n|,$$

e si verifica che il campo $\hat{K}$ è completo rispetto a $|\cdot|$, ed è unico a meno di isomorfismo.

Nel caso $K = \mathbb{Q}$ abbiamo quindi un completamento per $|\cdot|$, che è $\mathbb{R}$, e un completamento per ogni primo p, che si denota con $\mathbb{Q}_p$ e si chiama *campo dei numeri p-adici*.

Il seguente teorema classifica i posti di un campo di numeri K. Ricordiamo che un'*immersione (embedding)* di K in $\mathbb{C}$ è un omomorfismo di campi (dunque iniettivo) $j\colon K \to \mathbb{C}$.

Teorema 1.5.1. *Sia K un campo di numeri algebrici. I posti di K sono esattamente:*

- *uno (finito) per ogni ideale primo $\mathfrak{p} \triangleleft O_K$, corrispondente alla valutazione $\mathfrak{p}$-adica;*
- *uno (infinito, detto* reale*) per ogni immersione reale $\rho\colon K \to \mathbb{R}$, con una valutazione rappresentante data da*

$$\alpha \mapsto |\rho(\alpha)|;$$

- *uno (infinito, detto* complesso*) per ogni coppia di immersioni complesse coniugate $\sigma, \bar{\sigma}\colon K \to \mathbb{C}$, con una valutazione data da*

$$\alpha \mapsto |\sigma(\alpha)|^2 = |\sigma(\alpha)||\bar{\sigma}(\alpha)|.$$

Si ha inoltre che, se v è una valutazione archimedea appartenente a un posto reale (rispettivamente: complesso), il completamento di K rispetto a v è $\mathbb{R}$ (rispettivamente: $\mathbb{C}$).

Osservazione 1.5.1. Siano $K = \mathbb{Q}(\alpha)$, $f_\alpha \in \mathbb{Q}[x]$ il polinomio minimo di α su $\mathbb{Q}$ e $[K : \mathbb{Q}] = deg(f_\alpha) = n$; le immersioni σ di K in $\mathbb{C}$ sono univocamente determinate da $\sigma(\alpha)$, che deve essere necessariamente uno zero di f_α; quindi sono esattamente n, perché f_α è separabile (e sono tutti $\mathbb{Q}$-automorfismi di K se e solo se $K/\mathbb{Q}$ è un'estensione normale). Se indichiamo con r il numero di immersioni reali e con $2s$ il numero di immersioni complesse (sono a coppie coniugate), allora il numero di posti infiniti di K è $r + s$.

Capitolo 2

Automorfismo di Frobenius e mappa di Artin

In questo capitolo introduciamo i primi concetti fondamentali della "Class field theory": l'automorfismo di Frobenius e la mappa di Artin per estensioni L/K abeliane. Prima di tutto definiamo la nozione di *norma* degli ideali frazionari.

2.1 Norme di ideali

Ricordiamo che, dato un campo di numeri K, l'insieme I_K degli ideali frazionari di K è il gruppo abeliano libero generato da $Spec(O_K)$, l'insieme di tutti gli ideali primi di O_K.

Definizione 2.1.1. Consideriamo due campi di numeri $K \leq L$. Definiamo la seguente funzione:

$$N_{L|K} \colon Spec(O_L) \to I_K,$$
$$\mathfrak{P} \mapsto N_{L|K}(\mathfrak{P}) \equiv \mathfrak{p}^f,$$

con

$$\mathfrak{p} \equiv \mathfrak{P} \cap O_K \lhd O_K \text{ e } f = f(\mathfrak{P}/\mathfrak{p}) = \left[\frac{O_L}{\mathfrak{P}} : \frac{O_K}{\mathfrak{p}}\right].$$

Essa si estende poi per moltiplicatività a un omomorfismo di I_L in I_K: se

$$\mathfrak{A} = \prod_{\mathfrak{P}_i} {\mathfrak{P}_i}^{a_i},$$

allora

$$N_{L|K}(\mathfrak{A}) = \prod_{\mathfrak{P}_i} (\mathfrak{P}_i \cap O_K)^{a_i f(\mathfrak{P}_i/\mathfrak{P}_i \cap O_K)}.$$

L'ideale frazionario $N_{L|K}(\mathfrak{A})$ di K è detto *norma* dell'ideale frazionario $\mathfrak{A}$ di L.

Osservazione 2.1.1. Siano $K \leq L \leq M$. Abbiamo le mappe

$$N_{M|L} \colon I_M \to I_L; \quad N_{L|K} \colon I_L \to I_K; \quad N_{M|K} \colon I_M \to I_K.$$

Tali mappe si compongono nel seguente modo:

$$N_{L|K}(N_{M|L}(\mathfrak{A})) = N_{M|K}(\mathfrak{A}) \quad \forall\, \mathfrak{A} \in I_M;$$

segue dalla proprietà 1.4.1.

2.2 Gruppi di decomposizione e inerzia

D'ora in avanti K denoterà un campo di numeri, L una sua estensione algebrica finita, normale e separabile; $G = Gal(L/K)$, $n = [L : K] = |G|$; O_K e O_L i rispettivi anelli degli interi algebrici.

Sappiamo che, se $\mathfrak{p} \triangleleft O_K$, si ha la fattorizzazione

$$\mathfrak{p}O_L = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e,$$

dove i $\mathfrak{P}_i$ sono gli ideali primi di O_L che dividono $\mathfrak{p}$; inoltre G agisce transitivamente sull'insieme $\{\mathfrak{P}_1 \dots \mathfrak{P}_g\}$.

Definizione 2.2.1. Nelle notazioni precedenti, definiamo il *gruppo di decomposizione di* $\mathfrak{P}$ come lo stabilizzatore di $\mathfrak{P}$ in G:

$$G(\mathfrak{P}) \equiv \{\sigma \in G \,|\, \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

L'ordine di $G(\mathfrak{P})$ è pari a ef, perché $|G : G(\mathfrak{P})| = g$, la cardinalità dell'orbita di $\mathfrak{P}$ (che è appunto uguale a g per la transitività dell'azione); dunque $|G(\mathfrak{P})| = |G|/|G : G(\mathfrak{P})| = n/g = efg/g = ef$.

Consideriamo l'estensione di campi $\frac{O_L}{\mathfrak{P}}/\frac{O_K}{\mathfrak{p}}$: la proposizione 1.4.1 ci dice che il campo $\frac{O_K}{\mathfrak{p}}$ è finito, con q elementi (q potenza di primo); l'estensione è di grado f, dunque $\left|\frac{O_L}{\mathfrak{P}}\right| = q^f$. Sappiamo che allora l'estensione è di Galois con gruppo

$$Gal\left(\frac{O_L}{\mathfrak{P}}/\frac{O_K}{\mathfrak{p}}\right) \cong C_f$$

ciclico di ordine f, generato dall'automorfismo di Frobenius:

$$F\colon \frac{O_L}{\mathfrak{P}} \to \frac{O_L}{\mathfrak{P}},$$

$$(\alpha + \mathfrak{P}) \mapsto (\alpha + \mathfrak{P})^q = \alpha^q + \mathfrak{P}, \quad \forall\, \alpha \in O_L.$$

Consideriamo ora la seguente mappa:

$$\Phi\colon G(\mathfrak{P}) \to Gal\left(\frac{O_L}{\mathfrak{P}}/\frac{O_K}{\mathfrak{p}}\right),$$

$$\sigma \mapsto \bar{\sigma},$$

con $\bar{\sigma}$ così definito:

$$\bar{\sigma}\colon \frac{O_L}{\mathfrak{P}} \to \frac{O_L}{\mathfrak{P}},$$

$$(\alpha + \mathfrak{P}) \mapsto \bar{\sigma}(\alpha + \mathfrak{P}) \equiv \sigma(\alpha) + \mathfrak{P}.$$

Si verifica che Φ è un omomorfismo di gruppi, con nucleo

$$Ker\Phi = \{\sigma \in G(\mathfrak{P}) \,|\, \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \; \forall\, \alpha \in O_L\};$$

$Ker\Phi$ è detto *gruppo di inerzia di* $\mathfrak{P}$ e viene indicato con $I(\mathfrak{P})$.

Teorema 2.2.1. *La mappa* Φ *sopra definita è suriettiva. Pertanto*

$$\frac{G(\mathfrak{P})}{I(\mathfrak{P})} \cong Gal\left(\frac{O_L}{\mathfrak{P}}/\frac{O_K}{\mathfrak{p}}\right) \cong C_f,$$

e dunque $|I(\mathfrak{P})| = e$.

Consideriamo ora il caso in cui $\mathfrak{p} \lhd O_K$ non sia ramificato, ossia $e = 1$:

$$\mathfrak{p}O_L = \mathfrak{P}_1 \dots \mathfrak{P}_g.$$

In questa situazione particolare, l'omomorfismo Φ appena definito è un isomorfismo, perché $|Ker\Phi| = |I(\mathfrak{P})| = e = 1$. Dunque, per ogni primo $\mathfrak{P} \lhd O_L$ che divide $\mathfrak{p}$, il suo gruppo di decomposizione è ciclico di ordine f:

$$G(\mathfrak{P}) \cong Gal\left(\frac{O_L}{\mathfrak{P}}/\frac{O_K}{\mathfrak{p}}\right) \cong C_f.$$

Questo isomorfismo motiva la seguente definizione.

Definizione 2.2.2. Nel contesto di cui sopra, si definisce *automorfismo di Frobenius* l'unico elemento $\sigma \in G(\mathfrak{P})$ tale che

$$\sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}} \quad \forall\, \alpha \in O_L.$$

Ricordiamo che $q = \left|\frac{O_K}{\mathfrak{p}}\right|$.

Dimostriamo esplicitamente l'esistenza di σ: sappiamo che $\exists!\, \sigma \in G(\mathfrak{P})$ tale che $F = \Phi(\sigma) = \bar{\sigma}$; ciò significa che

$$\bar{\sigma}(\alpha + \mathfrak{P}) = F(\alpha + \mathfrak{P}) = \alpha^q + \mathfrak{P} \quad \forall\, \alpha \in O_L,$$

ossia che

$$\sigma(\alpha) + \mathfrak{P} = \alpha^q + \mathfrak{P} \quad \forall\, \alpha \in O_L,$$

cioè

$$\sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}} \quad \forall\, \alpha \in O_L.$$

L'automorfismo σ è cioè l'elemento $\Phi^{-1}(F)$, da cui la denominazione. Viene usata la seguente notazione:

$$\sigma = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Esempio 2.2.1. Siano $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $O_K = \mathbb{Z}$ e $O_L = \mathbb{Z}[i]$;

$$G = Gal(\mathbb{Q}(i)/\mathbb{Q})) = \langle \tau \rangle \cong C_2, \quad \text{con } \tau(i) = -i \text{ (coniugio)}.$$

Consideriamo l'ideale $\mathfrak{p} = (p) = 3\mathbb{Z} \lhd \mathbb{Z}$. La fattorizzazione in $\mathbb{Z}[i]$ è $3\mathbb{Z}[i] = (3) = \mathfrak{P}$: $3\mathbb{Z}$ è inerte, e

$$f(3\mathbb{Z}[i]/3\mathbb{Z}) = [\mathbb{Z}[i]/3\mathbb{Z}[i] : \mathbb{Z}/3\mathbb{Z}] = [\mathbb{F}_9 : \mathbb{F}_3] = 2;$$

Infine, $q = |O_K/\mathfrak{p}| = |\mathbb{Z}/3\mathbb{Z}| = 3$.
Allora $G(\mathfrak{P}) = G$. In effetti $\tau(\mathfrak{P}) = \mathfrak{P}$:

$$\tau(3a + 3ib) = 3a - 3ib = 3(a - ib) \in \mathfrak{P}.$$

Verifichiamo infine che l'automorfismo di Frobenius è proprio τ:

$$\tau(\alpha) - (\alpha)^3 = \tau(a + ib) - (a + ib)^3 = (a - ib) - (a^3 + 3ia^2b - 3ab^2 - ib^3) =$$
$$= (a - a^3 + 3ab^2) + i(-b - 3a^2b + b^3) \in \mathfrak{P} = 3\mathbb{Z}[i],$$

perché

$$3| - 3a^2b; \quad 3|(b^3 - b) = b(b - 1)(b + 1) \quad (b \in \mathbb{Z}),$$

e similmente per la parte reale.

Osserviamo che $\tau(i) = -i = i^3$, e $3 = p$. In 2.3.1 generalizzeremo questo esempio.

Vediamo ora alcune proprietà dell'automorfismo di Frobenius.

Proposizione 2.2.1. *Siano $\mathfrak{p} \lhd O_K$ non ramificato, $\mathfrak{P}$ un ideale primo di O_L che divide $\mathfrak{p}$, e $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$; $q = \left|\frac{O_K}{\mathfrak{p}}\right|$. Valgono le seguenti proprietà:*

1. *$\sigma = id_L \iff \mathfrak{p}$ spezza completamente in L;*
2. *I gruppi $G(\mathfrak{P}_i)$ al variare di $\mathfrak{P}_i$ tra i divisori di $\mathfrak{p}$ sono coniugati in $G = Gal(L/K)$;*
3. *Se $\tau \in G$ è tale che $\tau(\mathfrak{P}) = \mathfrak{Q}$, allora*
$$\left[\frac{L/K}{\mathfrak{Q}}\right] = \tau \left[\frac{L/K}{\mathfrak{P}}\right] \tau^{-1}.$$
4. *Siano $K < E < L$, con anche E/K di Galois; $\mathfrak{P} \lhd O_L$, $\mathfrak{P}_E = \mathfrak{P} \cap E$, $\mathfrak{p} = \mathfrak{P} \cap K$. Allora*
$$\left[\frac{E/K}{\mathfrak{P}_E}\right] = \left[\frac{L/K}{\mathfrak{P}}\right]\Bigg|_E \quad \textit{(restrizione a E).}$$
5. *Siano E_1, E_2 estensioni di Galois di K; $\mathfrak{P} \lhd O_{E_1E_2}$, e $\mathfrak{p}_i = \mathfrak{P} \cap E_i$. Sia*
$$\Psi \colon Gal(E_1E_2/K) \to Gal(E_1/K) \times Gal(E_2/K),$$
$$\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$$
l'omomorfismo iniettivo dato dalla restrizione a E_1 ed E_2. Allora si ha che
$$\Psi\left(\left[\frac{E_1E_2/K}{\mathfrak{P}}\right]\right) = \left(\left[\frac{E_1/K}{\mathfrak{p}_1}\right], \left[\frac{E_2/K}{\mathfrak{p}_2}\right]\right).$$

Dimostrazione. 1. $\sigma = id_L \iff 1 = |\sigma| = |G(\mathfrak{P})| = ef \iff 1 = e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$, il che accade se e solo se $\mathfrak{p}$ spezza completamente in L, perché $e_i = e \; \forall\, i = 1, \ldots, g$, $f_i = f \; \forall\, i = 1, \ldots, g$.

2. Sia $\mathfrak{P}_i$ un altro primo di L che divide $\mathfrak{p}$; esiste $\tau \in G$ tale che $\tau(\mathfrak{P}) = \mathfrak{P}_i$. Allora si ha che

$$\rho \in G(\mathfrak{P}_i) = G(\tau(\mathfrak{P})) \iff \rho(\tau(\mathfrak{P})) = \tau(\mathfrak{P}) \iff$$

$$\iff \tau^{-1}\rho(\tau(\mathfrak{P})) = \mathfrak{P} \iff \tau^{-1}\rho\tau \in G(\mathfrak{P}),$$

dunque $G(\mathfrak{P}_i) = \tau G(\mathfrak{P})\tau^{-1}$.

3. Sia $\tau \in G$ tale che $\tau(\mathfrak{P}) = \mathfrak{Q}$. Preso $x \in O_L$, $\tau^{-1}(x) \in O_L$; allora

$$\sigma(\tau^{-1}(x)) - (\tau^{-1}(x))^q \in \mathfrak{P}.$$

Applicando τ si trova

$$\tau\big((\sigma(\tau^{-1}(x)) - \tau^{-1}(x^q))\big) = \tau(\sigma(\tau^{-1}(x)) - x^q \in \tau(\mathfrak{P}) = \mathfrak{Q},$$

cioè

$$\tau\sigma\tau^{-1}(x) \equiv x^q \; mod(\mathfrak{Q}).$$

Dall'unicità dell'automorfismo di Frobenius segue la tesi: $\tau\sigma\tau^{-1} = \left[\frac{L/K}{\mathfrak{Q}}\right]$.

4. Osserviamo innanzitutto che $\left[\frac{E/K}{\mathfrak{P}_E}\right]$ è ben definito: poiché $\mathfrak{p}$ non ramifica in L, non ramifica nemmeno in E (se ramificasse in E lo farebbe anche in L). Sia $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right] \in G = Gal(L/K)$; poichè E/K è normale, $\sigma|_E(E) = E$, cioè $\sigma \in Gal(E/K)$. Dobbiamo mostrare che

$$\sigma(x) - x^q \in \mathfrak{P}_E = P \cap E,$$

con $q = \left|\frac{O_K}{\mathfrak{p}}\right|$, $\forall\, x \in O_E$.

Preso $x \in O_E \subset E$, $\sigma(x) \in E$, e $x^q \in E$; allora $\sigma(x) - x^q \in E$; d'altra parte $\sigma(x) - x^q \in \mathfrak{P}$, perché $x \in O_L$ e $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$. Dunque $\sigma(x) - x^q \in \mathfrak{P} \cap E = \mathfrak{P}_E$. Questo prova che

$$\sigma|_E = \left[\frac{E/K}{\mathfrak{P}_E}\right].$$

5. Segue dalla proprietà precedente, perché

$$\left[\frac{E_1E_2/K}{\mathfrak{P}}\right]\Bigg|_{E_i} = \left[\frac{E_i/K}{\mathfrak{p}_i}\right].$$

□

Concludiamo questa sezione enunciando il seguente risultato.

Proposizione 2.2.2. *Siano K un campo di numeri, L/K un'estensione di Galois con gruppo $G = Gal(L/K)$, $\mathfrak{P} \triangleleft O_L$ e $\mathfrak{p} = \mathfrak{P} \cap O_K$; supponiamo inoltre $G(\mathfrak{P}) \triangleleft G$.*

Allora $\mathfrak{p}$ spezza completamente in $K^{G(\mathfrak{P})}$ (detto decomposition field *di $\mathfrak{P}$ su K).*

2.3 Mappa di Artin per estensioni abeliane

Da ora in avanti ci concentreremo al caso di un'estensione L/K abeliana (ossia $G = Gal(L/K)$ è un gruppo abeliano). Come sempre sia $\mathfrak{p}O_L = \mathfrak{P}_1 \dots \mathfrak{P}_g$, con $\mathfrak{p}$ non ramificato.

La proprietà 3 della Proposizione 2.2.1 implica che, per ogni $\mathfrak{P}, \mathfrak{Q}$ che dividono $\mathfrak{p}$, i rispettivi automorfismi di Frobenius sono uguali, perché le coniugazioni in G sono banali. Allora è possibile definire l'automorfismo di Frobenius relativo a $\mathfrak{p}$, indicato con

$$\left[\frac{L/K}{\mathfrak{p}}\right],$$

come l'automorfismo di Frobenius di ogni $\mathfrak{P}$ che divide $\mathfrak{p}$.

Definiremo ora la mappa di Artin per un'estensione abeliana. Consideriamo $S \subset Spec(O_K)$ un sottoinsieme finito di ideali primi di O_K contenente tutti i primi $\mathfrak{p}$ che ramificano in L. Indicheremo con

$$I_K^S = I^S \equiv \langle Spec(O_K) \setminus S \rangle$$

l'insieme di tutti gli ideali frazionari di K la cui fattorizzazione in ideali primi contiene solo ideali che non ramificano; è il sottogruppo di I_K generato da tutti i primi di $Spec(O_K) \setminus S$:

$$\mathfrak{A} \in I_K^S \iff \mathfrak{A} = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{a(\mathfrak{p})}.$$

Definizione 2.3.1. Con queste notazioni, la *mappa di Artin* associata all'estensione abeliana L/K è la funzione

$$\phi_{L/K} \colon I_K^S \to G = Gal(L/K),$$

$$\mathfrak{A} \mapsto \phi_{L/K}(\mathfrak{A}) \equiv \prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{a(\mathfrak{p})}.$$

Osservazione 2.3.1. Poiché $Gal(L/K)$ è abeliano, la mappa è ben definita: non dipende dall'ordine dei primi $\mathfrak{p}$ nella scrittura della fattorizzazione di $\mathfrak{A}$.

$\phi_{L/K}$ è un omomorfismo di gruppi per costruzione: per gli ideali $\mathfrak{p} \in Spec(O_K) \setminus S$ (ossia per i generatori del gruppo I_K^S), $\phi_{L/K}(\mathfrak{p}) = \left[\frac{L/K}{\mathfrak{p}}\right]$, l'automorfismo di Frobenius di $\mathfrak{p}$; la mappa è poi estesa per moltiplicatività.

L'automorfismo di Frobenius è definito solamente per i primi $\mathfrak{p}$ che non ramificano: questo chiarisce le ipotesi sull'insieme S.

Esempio 2.3.1. Dato $m \in \mathbb{N}^*$, sia $\zeta \equiv \zeta_m$ una radice primitiva m-esima di $1 \in \mathbb{C}$ e consideriamo l'estensione ciclotomica $\mathbb{Q}(\zeta)/\mathbb{Q}$ (quindi $K = \mathbb{Q}, L = \mathbb{Q}(\zeta)$). Sappiamo che

$$G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}/m\mathbb{Z}),$$

gruppo moltiplicativo di ordine $\phi(m)$ dei numeri interi coprimi con m (ϕ è la funzione di Eulero); l'estensione è dunque abeliana. In particolare,

$$G = \{\sigma_r \,|\, r \in U(\mathbb{Z}/m\mathbb{Z})\}, \text{ con } \sigma_r(\zeta) = \zeta^r.$$

Troviamo l'automorfismo di Frobenius di un primo $\mathfrak{p} \triangleleft O_K$ che non ramifichi in L; poiché $K = \mathbb{Q}$, allora $O_K = \mathbb{Z}$, dunque $\mathfrak{p} = (p) \triangleleft \mathbb{Z}$, con $p \in \mathbb{Z}$ numero primo. Segue che $\frac{O_K}{\mathfrak{p}} = \frac{\mathbb{Z}}{p\mathbb{Z}}$, il campo con p elementi; dunque $\left|\frac{O_K}{\mathfrak{p}}\right| = p$.

Quindi l'automorfismo di Frobenius è l'elemento $\sigma \in G$ che soddisfa

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}} \quad \forall\, \alpha \in O_L,$$

con $\mathfrak{P} \triangleleft O_L$ che divide (p). Mostriamo che $\sigma = \sigma_p$ (il fatto che $\sigma_p \in G$ è dovuto al Teorema 1.4.1: se p non ramifica allora p non divide m, dunque $(p, m) = 1$). Poiché $O_L = \mathbb{Z}[\zeta]$, possiamo scrivere

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta^i, \text{ con } a_i \in \mathbb{Z}.$$

Dobbiamo mostrare che $\sigma_p(\alpha) - \alpha^p \in \mathfrak{P}$; poiché $p \in \mathfrak{P}$, e $\mathfrak{P}$ è un ideale, basta mostrare che p divide $\sigma_p(\alpha) - \alpha^p$. Si può cioè lavorare modulo p, e allora

$$\sigma_p(\alpha) - \alpha^p = \sigma_p\left(\sum_i a_i\zeta^i\right) - \left(\sum_i a_i\zeta^i\right)^p = \sum_i \sigma_p(a_i)\sigma_p(\zeta)^i - \left(\sum_i a_i\zeta^i\right)^p =$$

$$= \sum_i a_i\zeta^{pi} - \left(\sum_i a_i\zeta^i\right)^p \equiv \sum_i a_i\zeta^{pi} - \sum_i {a_i}^p\zeta^{pi} = \sum_i \zeta^{pi}(a_i - {a_i}^p).$$

Nel quarto passaggio abbiamo usato il fatto che tutti gli addendi non scritti nella seconda sommatoria sono multipli di p; possiamo concludere perché, in virtù del piccolo teorema di Fermat, $(a_i - {a_i}^p)$ è divisibile per p, quindi l'ultima sommatoria scritta rappresenta un elemento di $\mathfrak{P}$.

Consideriamo ora un'estensione E/K finita. Sappiamo dalla teoria di Galois che EL/E è un'estensione di Galois, con

$$\Psi \colon Gal(EL/E) \to Gal(L/K),$$

$$\sigma \mapsto \sigma|_L,$$

l'omomorfismo di restrizione, iniettivo: quindi $Gal(EL/E)$ è isomorfo a un sottogruppo di $Gal(L/K)$, e perciò è anch'esso abeliano. Allora è possibile definire la mappa di Artin per EL/E. Con S definito come sopra, definiamo

$$I_E^S \equiv \langle \{\mathfrak{P} \triangleleft O_E \,|\, \mathfrak{P} \text{ non divide alcun primo di } S\}\rangle \leq I_E$$

come il sottogruppo di I_E (ideali frazionari di E) generato dai primi che non dividono nessun primo di S; in altri termini,

$$N_{E|K}(\mathfrak{A}) \in I_K^S \quad \forall\, \mathfrak{A} \in I_E^S.$$

Il lemma seguente lega la mappa di Artin di L/K e quella di EL/E.

Lemma 2.3.1. *Per ogni ideale $\mathfrak{A} \in I_E^S$ vale*

$$\phi_{EL/E}(\mathfrak{A}) = \phi_{L/K}(N_{E|K}(\mathfrak{A})).$$

Corollario 2.3.1. $N_{L|K}(I_L^S) \leq ker\phi_{L/K}$.

Dimostrazione. Applichiamo il Lemma 2.3.1 con $E = L$, e troviamo

$$\phi_{L/L}(\mathfrak{A}) = \phi_{L/K}(N_{L|K}(\mathfrak{A})) \quad \forall\, \mathfrak{A} \in I_L^S.$$

Poiché

$$\phi_{L/L} \colon I_L^S \to Gal(L/L) \leq Gal(L/K)$$

è l'omomorfismo banale, allora abbiamo che

$$id_{Gal(L/K)} = \phi_{L/K}(N_{L|K}(\mathfrak{A})) \quad \forall\, \mathfrak{A} \in I_L^S,$$

cioè

$$N_{L|K}(I_L^S) \leq ker\phi_{L/K}.$$

□

Esempio 2.3.2. Sia $m \in \mathbb{N}^*$ un numero intero e $\zeta = \zeta_m$ una radice primitiva m-esima di $1 \in \mathbb{C}$; $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$ il campo ciclotomico m-esimo. Nell'esempio 2.3.1 abbiamo trovato $\phi_{L/\mathbb{Q}}(p)$ (l'automorfismo di Frobenius di p) per ogni primo p che non ramifica in L; descriviamo ora nel dettaglio la mappa di Artin

$$\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}} \colon I_{\mathbb{Q}}^S \to G = \{\sigma_r \,|\, r \in U(\mathbb{Z}/m\mathbb{Z})\},$$

con $S = \{p \in \mathbb{Z} \,|\, p \text{ divide } m\}$.

Ricordiamo che un elemento di $I_{\mathbb{Q}}$, cioè un ideale frazionario di $\mathbb{Q}$, è principale, ossia è della forma $(q) = (a/b)$, con $a, b \in \mathbb{Z}, b \neq 0$. $I_{\mathbb{Q}}^S$ contiene quindi ideali frazionari del tipo (a/b) con $(a, m) = 1 = (b, m)$. Con lo scopo di determinare nucleo e immagine di $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, individuiamo l'immagine di un generico elemento di $I_{\mathbb{Q}}^S$. Scriveremo $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}(q)$ intendendo $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}((q))$.

Se $p \in \mathbb{Z}$ è primo, $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}(p) = \sigma_p$.

Se $a \in \mathbb{Z}$ è un intero coprimo con m, con fattorizzazione $a = {p_1}^{a_1} \dots {p_n}^{a_n}$, allora $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a) = \sigma_a$. Infatti:

$$\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a) = \phi\left(\prod_i {p_i}^{a_i}\right) = \prod_i \phi({p_i}^{a_i}) = \prod_i {\sigma_{p_i}}^{a_i} = \sigma_a;$$

L'ultima uguaglianza è giustificata dal fatto che

$$\prod_i {\sigma_{p_i}}^{a_i}(\zeta) = \zeta^{\prod_i {p_i}^{a_i}} = \zeta^a = \sigma_a(\zeta).$$

Se $b \in \mathbb{Z}$ è coprimo con m (vorremmo calcolare $\phi(1/b)$), denotiamo con b^* il suo inverso moltiplicativo in $U(\mathbb{Z}/m\mathbb{Z})$: cioè $bb^* \equiv 1 \pmod m$. Allora

$$\phi(bb^*) = \sigma_{bb^*} = id_G \Rightarrow \phi(b)\phi(b^*) = id \Rightarrow \phi(b)^{-1} = \phi(b^*),$$

cioè

$$\phi(1/b) = \phi(b^{-1}) = \phi(b^*).$$

Possiamo ora calcolare $\phi(a/b)$ per qualsiasi $(a/b) \in I_{\mathbb{Q}}^S$:

$$\phi(a/b) = \phi(a)\phi(1/b) = \sigma_a \sigma_{b^*} = \sigma_{ab^*}.$$

Infine determiniamo il nucleo e l'immagine della mappa di Artin. Mostriamo che:

1. La mappa di Artin $\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ è suriettiva;
2. $Ker(\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}) = \{(a/b) \in I_{\mathbb{Q}}^S \mid a \equiv b \pmod{m}\}$.

Dimostrazione. 1. Sia $\sigma_r \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, ossia $(r, m) = 1$. Allora

$$\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}(r) = \sigma_r,$$

da quanto appena visto.

2. $\phi(a/b) = id_G \iff \sigma_{ab^*} = id \iff ab^* \equiv 1 \pmod{m} \iff ab^*b \equiv 1 \iff a \equiv b$.

□

Definizione 2.3.2. Sia K un campo di numeri. Un *modulus* di K è una scrittura formale del tipo

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

tale che:

- $\mathfrak{p}$ sono primi di K, finiti o infiniti;
- $n(\mathfrak{p}) \in \mathbb{N}$, ed è > 0 solo per un numero finito di $\mathfrak{p}$;
- se $\mathfrak{p}$ è un primo infinito reale, $n(\mathfrak{p}) = 0$ o $n(\mathfrak{p}) = 1$;
- se $\mathfrak{p}$ è un primo infinito complesso, $n(\mathfrak{p}) = 0$.

Si può quindi anche scrivere

$$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty,$$

con $\mathfrak{m}_0 \triangleleft O_K$, perché prodotto di ideali primi con esponente positivo, e $\mathfrak{m}_\infty$ un prodotto formale di primi infiniti reali di K con esponente 1.

Introduciamo la seguente notazione (naturale): diciamo che un ideale $\mathfrak{a} \triangleleft O_K$ è *coprimo* con $\mathfrak{m}$ se nessun ideale primo di $\mathfrak{m}_0$ compare nella fattorizzazione di $\mathfrak{a}$; analogamente se $\mathfrak{A}$ è un ideale frazionario di K. In modo simile definiamo la divisibilità e la coprimalità tra moduli $\mathfrak{m}, \mathfrak{n}$.

Ricordiamo che, se $S \subset Spec(O_K)$, $I_K^S = \langle Spec(O_K) \setminus S \rangle$. Dato un modulus $\mathfrak{m}$, con $\mathfrak{m}_0 = {\mathfrak{p}_1}^{n_1} \dots {\mathfrak{p}_r}^{n_r}$, definiamo

$$I_K^{\mathfrak{m}} \equiv I_K^S,$$

con $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$; in altri termini, $I_K^{\mathfrak{m}}$ contiene ideali frazionari coprimi con $\mathfrak{m}$. Osserviamo che la definizione non dipende né da $n_1, \dots, n_r$ né da $\mathfrak{m}_\infty$.

Definiamo ora una relazione di equivalenza $mod(\mathfrak{m})$ su K^*. Siano $\alpha, \beta \in K^*$.

Se $\mathfrak{p}$ è un primo infinito reale di K, con valutazione rappresentante data dall'immersione reale ρ, diciamo che $\alpha \equiv \beta \ mod(\mathfrak{p})$ se $\rho(\alpha)/\rho(\beta) \in \mathbb{R}^+$, ossia se $\rho(\alpha)$ e $\rho(\beta)$ hanno lo stesso segno in $\rho(K) \subset \mathbb{R}$.

Se $\mathfrak{p}$ è un primo finito di K, ossia $\mathfrak{p} \triangleleft O_K$ è un ideale primo, diciamo che $\alpha \equiv \beta \ mod(\mathfrak{p}^n)$ se $v_{\mathfrak{p}}(\alpha/\beta - 1) \geq n$.

Definizione 2.3.3. Sia $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty = {\mathfrak{p}_1}^{n_1} \dots {\mathfrak{p}_r}^{n_r}\mathfrak{m}_\infty$; $\alpha, \beta \in K^*$. Diciamo che

$$\alpha \equiv \beta \ mod(\mathfrak{m})$$

se

$$\alpha \equiv \beta \quad mod\left(\mathfrak{p}^{n(\mathfrak{p})}\right)$$

$\forall\, i = 1, \dots, r$ e per ogni primo reale che compare in $\mathfrak{m}_\infty$.

Definizione 2.3.4. Sia $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. Definiamo due sottogruppi di K^*:

$$K_{\mathfrak{m}} \equiv \{\alpha = \frac{a}{b} \in K^* \,|\, \text{gli ideali } (a), (b) \triangleleft O_K \text{ sono coprimi con } \mathfrak{m}_0\};$$

$$K_{\mathfrak{m},1} \equiv \{\alpha \in K_{\mathfrak{m}} \,|\, \alpha \equiv 1 \quad mod(\mathfrak{m})\}.$$

Osserviamo che l'omomorfismo

$$i \colon K^* \to I_K,$$

$$\alpha \mapsto (\alpha), \text{ l'ideale frazionario principale generato da } \alpha,$$

soddisfa $i(K_{\mathfrak{m}}) \leq I_K^{\mathfrak{m}}$: se $\alpha = a/b$ è tale che (a) e (b) sono coprimi con $\mathfrak{m}$, allora $i(\alpha) = \frac{(a)}{(b)}$ è un ideale frazionario di K coprimo con $\mathfrak{m}$, cioè è in $I_K^{\mathfrak{m}}$.

Esempio 2.3.3. Le definizioni appena introdotte generalizzano il concetto di congruenza $mod(m)$, con $m \in \mathbb{Z}$. Vediamo il caso $K = \mathbb{Q}$.

Sia $\mathfrak{m} = (2)^3(3)^2(5)p_\infty$, cioè $\mathfrak{m}_0 = (360) \triangleleft \mathbb{Z}$, e p_∞ rappresenta l'unico primo infinito di $\mathbb{Q}$, ossia quello associato all'usuale valore assoluto (l'immersione reale corrispondente è l'identità). Allora abbiamo che

$$\mathbb{Q}_m = \left\{ \frac{a}{b} \;\middle|\; (a, 360) = (b, 360) = 1 \right\}.$$

Sia $\alpha = \frac{a}{b} \in \mathbb{Q}_m$. Si ha che

$$\alpha \equiv 1 \ mod(\mathfrak{m}) \iff \begin{cases} \alpha \equiv 1 \ mod((2)^3) \\ \alpha \equiv 1 \ mod((3)^2) \\ \alpha \equiv 1 \ mod((5)) \\ \alpha \equiv 1 \ mod(p_\infty) \end{cases} \iff \begin{cases} v_2(\frac{a}{b} - 1) \geq 3 \\ v_3(\frac{a}{b} - 1) \geq 2 \\ v_5(\frac{a}{b} - 1) \geq 1 \\ \alpha/1 > 0 \end{cases}$$

Esaminiamo la prima condizione:

$$v_2\left(\frac{a-b}{b}\right) \geq 3 \iff v_2(a-b) \geq 3,$$

perché $(b,2)=1$. Allora la condizione equivale a

$$2^3 = 8|(a-b),$$

cioè

$$a \equiv b \mod(8).$$

Similmente per $(3)^2$ e (5), e così

$$\mathbb{Q}_{\mathfrak{m},1} = \left\{ \frac{a}{b} > 0 \;\middle|\; (a,360) = (b,360) = 1 \text{ e } a \equiv b \; mod(360) \right\}.$$

Osservazione 2.3.2. Se $\mathfrak{m}$ divide $\mathfrak{n}$, allora $K_{\mathfrak{n},1} \subset K_{\mathfrak{m},1}$. Siano infatti $\mathfrak{m} = {\mathfrak{p}_1}^{m_1} \dots {\mathfrak{p}_r}^{m_r}$, e $\mathfrak{n} = {\mathfrak{p}_1}^{n_1} \dots {\mathfrak{p}_r}^{n_r}$, con $m_i \leq n_i$. Preso $\alpha \in K_{\mathfrak{n},1}$, allora (α) è coprimo con $\mathfrak{n}_0$, dunque con $\mathfrak{m}_0$; $\alpha \equiv 1 \bmod({\mathfrak{p}_i}^{n_i})$ implica $\alpha \equiv 1 \bmod({\mathfrak{p}_i}^{m_i})$:

$$v_{\mathfrak{p}_i}(\alpha - 1) \geq n_i \geq m_i.$$

2.4 Risultati analitici

In questa sezione enunciamo alcuni importanti risultati della teoria analitica dei numeri.

Teorema 2.4.1. *Siano K un campo di numeri e L/K un'estensione abeliana. Se $\mathfrak{m}$ contiene tutti i primi di K che ramificano in L, allora la mappa di Artin*

$$\phi_{L/K} \colon I_K^{\mathfrak{m}} \to Gal(L/K)$$

è suriettiva.

D'ora in avanti $\mathfrak{m}$ sarà sempre divisibile da tutti i primi di O_K che ramificano in L: così la mappa di Artin sarà ben definita e suriettiva.

Una conseguenza di questo teorema è che, sotto queste ipotesi su $\mathfrak{m}$, l'indice del nucleo della mappa di Artin in $I_K^{\mathfrak{m}}$ è

$$|I_K^{\mathfrak{m}} : Ker(\phi_{L/K})| = [L:K].$$

Teorema 2.4.2. *Siano K un campo di numeri e L_1, L_2 due estensioni di Galois di K. Definiamo*

$$S_i = \{\mathfrak{p} \lhd O_K \text{ primo} \,|\, \mathfrak{p} \text{ spezza completamente in } L_i\}, \quad i = 1,2.$$

Se $S_1 \subset S_2$ a meno di un insieme finito di ideali primi, allora $L_2 \leq L_1$.

Questo teorema chiarisce l'importanza dello studio dei primi che spezzano completamente: c'è questa relazione tra le inclusioni tra gli insiemi S_i e le inclusioni tra le estensioni; sarà fondamentale nel provare il Teorema di Kronecker - Weber.

Osserviamo inoltre che i primi di O_K che spezzano completamente in L sono, a meno eventualmente di un numero finito di essi che divida $\mathfrak{m}$, contenuti nel nucleo della mappa di Artin $\phi_{L/K}$ (segue da 2.2.1, 1).

Teorema 2.4.3. *Siano K un campo di numeri, L/K un'estensione di Galois, $\mathfrak{m}$ modulus di K. Sia $I_L^{\mathfrak{m}}$ il sottogruppo di I_L generato dai primi con norma in $I_K^{\mathfrak{m}}$. Allora vale la seguente disuguaglianza*

$$|I_K^{\mathfrak{m}} : N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})| \leq [L : K],$$

detta prima disuguaglianza fondamentale della class field theory.

Questo teorema e il seguente rendono possibile, in precise circostanze, determinare il nucleo della mappa di Artin, come vedremo nel prossimo capitolo.

Teorema 2.4.4 (uguaglianza fondamentale)**.** *Siano K un campo di numeri, L/K un'estensione di Galois con gruppo $Gal(L/K)$ ciclico, $\mathfrak{m}$ modulus di K che sia divisibile da potenze sufficientemente alte di ogni primo $\mathfrak{p} \triangleleft O_K$ che ramifica in L. Allora*

$$|I_K^{\mathfrak{m}} : N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})| = [L : K].$$

Capitolo 3

Class field theory

L'obiettivo di questo capitolo è quello di determinare il nucleo della mappa di Artin per un'estensione abeliana L/K; in particolare, mostreremo che

$$Ker(\phi_{L/K}) = N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}) \leq I_K^{\mathfrak{m}}$$

per un opportuno $\mathfrak{m}$.

3.1 Legge di reciprocità

Sia K un campo di numeri, e L/K un'estensione abeliana; $G = Gal(L/K)$.

Definizione 3.1.1. Diciamo che la *legge di reciprocità* vale per $(L, K, \mathfrak{m})$ se G è abeliano e

$$i(K_{\mathfrak{m},1}) \leq Ker(\phi_{L/K}).$$

Questa proprietà è importante a motivo del lemma seguente.

Lemma 3.1.1. *Se $\mathfrak{m}$ è un modulus di K che contiene tutti i primi $\mathfrak{p} \triangleleft O_K$ che ramificano in L e la legge di reciprocità vale per $(L, K, \mathfrak{m})$, allora*

$$Ker(\phi_{L/K}) = N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}).$$

Dimostrazione. Sappiamo che (corollario 2.3.1)

$$N_{L|K}(I_L^{\mathfrak{m}}) \leq Ker(\phi_{L/K});$$

La legge di reciprocità e questa inclusione implicano che

$$N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}) \leq Ker(\phi_{L/K}).$$

Poiché l'indice $|I_K^{\mathfrak{m}} : N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})|$ è $\leq [L : K]$ (Teorema 2.4.3), e l'indice $|I_K^{\mathfrak{m}} : Ker(\phi_{L/K})|$ è esattamente $[L : K]$ (Teorema 2.4.1), l'inclusione è un'uguaglianza.

□

Esempio 3.1.1. Siano $K = \mathbb{Q}$, $\zeta = \zeta_m$, $L = \mathbb{Q}(\zeta)$ l'estensione ciclotomica m-esima; $\mathfrak{m} \equiv (m)p_\infty$. Nell'esempio 2.3.2 abbiamo visto che

$$Ker(\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}) = \left\{ \frac{(a)}{(b)} \in I_{\mathbb{Q}}^{\mathfrak{m}} \;\middle|\; a \equiv b \pmod{m} \right\};$$

d'altra parte, l'esempio 2.3.3 ci dice che

$$\mathbb{Q}_{\mathfrak{m},1} = \left\{ \frac{a}{b} > 0 \;\middle|\; (a,m) = (b,m) = 1 \text{ e } a \equiv b \; mod(m) \right\}.$$

Poiché

$$(a/b) \in I_{\mathbb{Q}}^{\mathfrak{m}} \iff (a,m) = (b,m) = 1,$$

si ha che

$$i(\mathbb{Q}_{\mathfrak{m},1}) = Ker(\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}).$$

Dunque per $(\mathbb{Q}(\zeta), \mathbb{Q}, (m)p_\infty)$ vale la legge di reciprocità.

Esempio 3.1.2. Se $\mathfrak{m}$ divide $\mathfrak{n}$ e la legge di reciprocità vale per $(L, K, \mathfrak{m})$, allora essa vale anche per $(L, K, \mathfrak{n})$. Infatti

$$i(K_{\mathfrak{n},1}) \leq i(K_{\mathfrak{m},1}) \leq Ker(\phi_{L/K}),$$

perché $K_{\mathfrak{n},1} \leq K_{\mathfrak{m},1}$ (osservazione 2.3.2).

Definizione 3.1.2. Sia G un gruppo abeliano e $\sigma, \tau \in G$; σ e τ si dicono *indipendenti* se $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$.

Due interi a, b coprimi con $m \in \mathbb{Z}$ si dicono *indipendenti mod* m se sono elementi indipendenti nel gruppo moltiplicativo $U(\mathbb{Z}/m\mathbb{Z})$.

Indicheremo con $|a|_m$ l'ordine di a in $U(\mathbb{Z}/m\mathbb{Z})$, ossia il minor $t \in \mathbb{N}$ tale che $a^t \equiv 1 \bmod m$.

Il nostro obiettivo è dimostrare che per un'estensione abeliana L/K esiste un opportuno $\mathfrak{m}$ tale che la legge di reciprocità valga per $(L, K, \mathfrak{m})$. Vedremo con la proposizione 3.1.1 e con il lemma 3.1.3 che dovremo costruire delle estensioni ciclotomiche con delle proprietà particolari. Cominciamo con un lemma numerico, che non dimostriamo.

Lemma 3.1.2. *Sia $n \in \mathbb{N}$ e $n = q_1^{r_1} \dots q_s^{r_s}$ la sua fattorizzazione; $a \in \mathbb{N}_{\geq 1}$. Allora:*

1. *Esistono infiniti numeri $m \in \mathbb{N}$ della forma $m = p_1 \dots p_{2s}$ tali che n divide $|a|_m$;*
2. *Esiste $b \in \mathbb{N}$ tale che n divide $|b|_m$ e a, b sono indipendenti mod m;*
3. *$min\{p_1, \dots, p_{2s}\}$ può essere scelto arbitrariamente grande.*

La prossima proposizione traduce questo risultato in termini di estensioni ciclotomiche di un campo di numeri K.

Proposizione 3.1.1. *Siano K un campo di numeri, L/K un'estensione abeliana, $[L : K] = n$, e $s \in \mathbb{N}_{\geq 1}$; sia $\mathfrak{p} \triangleleft O_K$ un primo che non ramifichi in L. Allora esiste un numero naturale m coprimo con s e con $\mathfrak{p}$ (ossia, detto $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, si ha $(m, p) = 1$) tale che:*

1. *se $\zeta = \zeta_m$ è una radice primitiva m-esima di 1, ed $E = K(\zeta)$, allora n divide l'ordine di $\phi_{E/K}(\mathfrak{p})$ in $Gal(E/K)$;*

2. $L \cap E = K$*;*

3. esiste $\tau \in Gal(E/K)$ *indipendente da* $\phi_{E/K}(\mathfrak{p})$ *e di ordine multiplo di* n*.*

Dimostrazione. Sia $(p) \lhd \mathbb{Z}$, $(p) = \mathfrak{p} \cap \mathbb{Z}$; applicheremo il lemma precedente con $n = [L : K]$ e $a = p^f$, con $f = f(\mathfrak{p}/(p)) = [O_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Facciamo la seguente costruzione: poiché L/K è un'estensione di Galois, il reticolo dei campi intermedi è finito: quindi è finito anche l'insieme

$$S \equiv \{\ F \text{ campo} \mid K \leq F \leq L \text{ ed esiste } r \in \mathbb{N} \text{ tale che } F \leq \mathbb{Q}(\zeta_r)\ \}$$

di tutti i campi intermedi tra K ed L che sono contenuti in un campo ciclotomico. Allora esiste $M \in \mathbb{N}$ tale che $\mathbb{Q}(\zeta_M) \geq F$ per ogni $F \in S$.

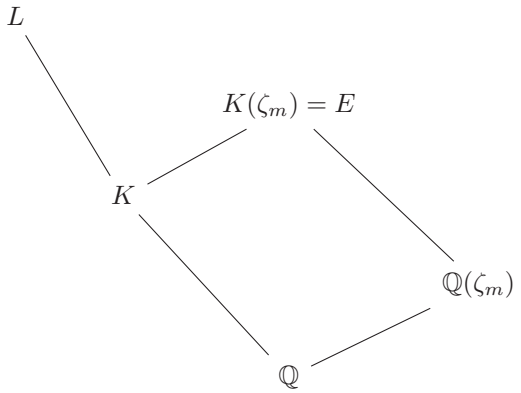
Per il lemma precedente possiamo trovare $m \in \mathbb{N}$ tale che:

(a) $n = [L : K]$ divide $|a|_m$;

(b) esiste $b \in \mathbb{N}$ tale che n divide $|b|_m$ e a, b sono indipendenti mod m;

(c) il più piccolo divisore primo di m è maggiore di Msp, cosicché $(m, p) = (m, M) = (m, s) = 1$.

Poiché $(m, M) = 1$, $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q}$: quindi, per com'è stato costruito $\mathbb{Q}(\zeta_M)$, abbiamo che $L \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$; da quest'ultima relazione segue anche che $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.



Sia $E = K(\zeta_m)$: abbiamo che

$$Gal(K(\zeta_m)/K) \cong Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong U(\mathbb{Z}/m\mathbb{Z});$$

inoltre $L \cap E = L \cap K(\zeta_m) = K$, perché i reticoli delle estensioni E/K e $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ sono isomorfi, e $L \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. Dunque il punto 2 è dimostrato.

Sia ora $\sigma = \phi_{K(\zeta_m)/K}(\mathfrak{p}) \in Gal(E/K)$. Si verifica che $\sigma(\zeta_m) = {\zeta_m}^a$, dunque $ord(\sigma) = |a|_m$, che è multiplo di n per (a), e quindi anche 1 è provato.

Infine, preso $b \in \mathbb{N}$ come in (b), sia $\tau \in Gal(K(\zeta_m)/K)$ l'elemento tale che $\tau(\zeta_m) = {\zeta_m}^b$: allora $ord(\tau) = |b|_m$, che è multiplo di n, e il punto 3 segue dal fatto che a e b sono indipendenti in $U(\mathbb{Z}/m\mathbb{Z}) \cong Gal(E/K)$.

□

Prima di arrivare al teorema di reciprocità di Artin, dimostreremo il risultato desiderato (trovare $\mathfrak{m}$ tale che $(L, K, \mathfrak{m})$ soddisfino la legge di reciprocità) per una estensione ciclica L/K. Il seguente lemma va in questa direzione.

Lemma 3.1.3 (Artin)**.** *Sia L/K un'estensione ciclica, ossia con $Gal(L/K)$ ciclico di ordine n; siano $s \in \mathbb{Z}$ un intero e $\mathfrak{p} \triangleleft O_K$ un primo che non ramifichi in L. Allora esistono un intero $m \in \mathbb{Z}$, coprimo con s e con $\mathfrak{p}$, e un'estensione F/K tali che:*

1. *$L \cap F = K$;*
2. *$L \cap K(\zeta_m) = K$ (ζ_m radice primitiva m-esima di 1);*
3. *$L(\zeta_m) = F(\zeta_m)$;*
4. *$\mathfrak{p}$ spezza completamente in F.*

Dimostrazione. Prendiamo $m \in \mathbb{Z}$, $\zeta = \zeta_m$ radice primitiva m-esima come nella proposizione precedente, ed $E = K(\zeta)$; dunque:

(a) $n | ord(\phi_{E/K}(\mathfrak{p}))$ in $Gal(E/K)$;

(b) $E \cap L = K$ (così il punto 2 è provato);

(c) esiste $\tau \in Gal(E/K)$ indipendente da $\phi_{E/K}(\mathfrak{p})$ e di ordine multiplo di n.

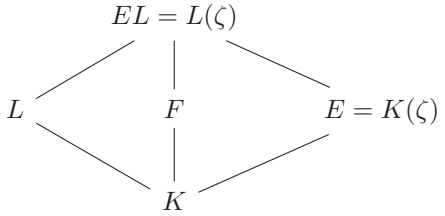
$L(\zeta) = EL$ e $L \cap E = K$, quindi

$$G = Gal(L(\zeta)/K) = Gal(EL/K) \cong Gal(L/K) \times Gal(E/K);$$

Inoltre $Gal(EL/E) \cong Gal(L/K)$. Dobbiamo trovare il campo F. Siano $G = \langle \sigma \rangle$ e $\tau \in Gal(E/K)$ l'elemento la cui esistenza è data da (c), e consideriamo il seguente sottogruppo di G:

$$H = \langle (\sigma, \tau), (\phi_{L/K}(\mathfrak{p}), \phi_{E/K}(\mathfrak{p})) \rangle;$$

sia $F \leq L(\zeta)$ il campo tenuto fisso da H.



Per la proprietà 5 della proposizione 2.2.1 abbiamo che

$$(\phi_{L/K}(\mathfrak{p}), \phi_{E/K}(\mathfrak{p})) = \phi_{EL/K}(\mathfrak{p}),$$

che è il generatore del gruppo di decomposizione $G(\mathfrak{P}) \leq Gal(EL/K)$ (con $\mathfrak{P}$ un qualsiasi primo di EL che divide $\mathfrak{p}$); denotiamo questo elemento con ψ. Allora $G(\mathfrak{P}) = \langle \psi \rangle \leq H$, dunque $F \leq K^{G(\mathfrak{P})}$: $\mathfrak{p}$ spezza completamente in $K^{G(\mathfrak{P})}$(per 2.2.2 e perché $Gal(EL/K)$ è abeliano, dunque $G(\mathfrak{P})$ ne è un sottogruppo normale), e pertanto anche in F.

Consideriamo ora il campo $F(\zeta) = EF \leq L(\zeta)$; è il campo tenuto fisso da $Gal(EL/E) \cap Gal(EL/F) = (Gal(L/K) \times \{1\}) \cap H$. Mostriamo che questo gruppo è banale: supponiamo

$$(\sigma, \tau)^u (\phi_{L/K}(\mathfrak{p}), \phi_{E/K}(\mathfrak{p}))^v \in (Gal(L/K) \times \{1\}),$$

e dimostriamo che questo elemento $(\sigma,\tau)^u\psi^v$ è l'identità. Abbiamo che

$$\begin{cases}\sigma^u\cdot(\phi_{L/K}(\mathfrak{p}))^v\in G=\langle\sigma\rangle\\ \tau^u\cdot(\phi_{E/K}(\mathfrak{p}))^v=1\end{cases}$$

La seconda condizione implica che $\tau^u\in\langle\phi_{E/K}(\mathfrak{p})\rangle$, e la proprietà (c) forza $\tau^u=1$; segue che $ord(\tau)$ divide u. Allora, sempre per (c), $n|u$. Quindi $\sigma^u=1$, perché $n=|\sigma|$. Infine, poiché anche $(\phi_{E/K}(\mathfrak{p}))^v=1$ (perché $\tau^u=1$), $ord(\phi_{E/K}(\mathfrak{p}))$ divide v, e dunque $n|v$, per (a): quindi $ord(\phi_{L/K}(\mathfrak{p}))$ (dividendo n, essendo $\phi_{L/K}(\mathfrak{p})\in G$) divide v; allora anche $(\phi_{L/K}(\mathfrak{p}))^v=1$.

Riassumendo, EF è tenuto fisso da $\{1\}\leq Gal(EL/K)$: quindi $F(\zeta)=EF=EL=L(\zeta)$, e così anche 3 è provato.

Resta da dimostrare 1, ossia che $L\cap F=K$. Poiché $(\sigma,\tau)\in H$, questo elemento tiene fisso il campo F, e dunque anche $L\cap F\leq F$; d'altra parte

$$(\sigma,\tau)|_L=\sigma.$$

Quindi $L\cap F$ è il sottocampo di L tenuto fisso da σ, che è K.

□

3.2 Teorema di reciprocità di Artin

Come anticipato, prima di dimostrare il risultato per L/K estensione abeliana ci restringiamo al caso di un'estensione ciclica.

Teorema 3.2.1. *Sia L/K un'estensione ciclica, con $\mathfrak{m}$ divisibile da tutti i primi di K che ramificano in L. Si supponga che valga l'uguaglianza*

$$|I_K^{\mathfrak{m}}:N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})|=[L:K].$$

Allora vale la legge di reciprocità per $(L,K,\mathfrak{m})$.

Dimostrazione (cenni). Mostreremo l'inclusione

$$Ker(\phi_{L/K})\leq N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1});$$

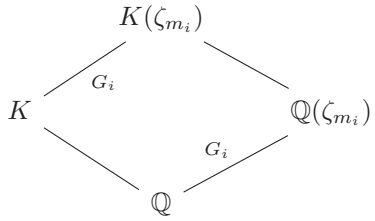
dall'uguaglianza degli indici seguirà l'uguaglianza di sottogruppi.
Sia

$$\mathfrak{A}=\prod_{i=1}^{r}\mathfrak{p}_i^{a_i}\in Ker(\phi_{L/K})\leq I_K^{\mathfrak{m}};$$

poiché $\mathfrak{m}$ è divisibile da tutti i primi di K che ramificano in L, i vari $\mathfrak{p}_i$ non ramificano. Dunque si può applicare il lemma 3.1.3 a ciascuno di essi: per ogni i esiste ζ_{m_i}, radice primitiva m_i-esima di 1, che soddisfi le proprietà 1-4 del lemma. Inoltre si può fare in modo che $(m_i,m_j)=1$ se $i\neq j$ (si vede qui il ruolo di $s\in\mathbb{Z}$ nella proposizione e nel lemma precedenti: m può essere scelto coprimo con un qualsiasi numero intero fissato all'inizio): per m_1 si prenda $s_1=1$; per m_2, $s_2=m_1$; per m_k, $s_k=m_1m_2\dots m_{k-1}$.

Inoltre $K\cap\mathbb{Q}(\zeta_{m_i})=\mathbb{Q}$ (sempre grazie alla proposizione 3.1.1): allora

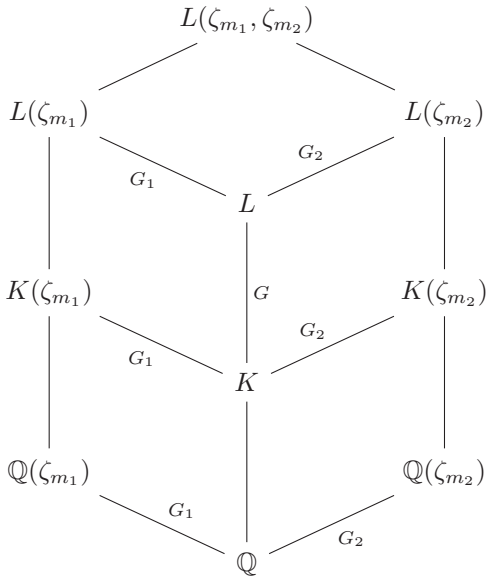
$$G_i\equiv Gal(K(\zeta_{m_i})/K)\cong Gal(\mathbb{Q}(\zeta_{m_i})/\mathbb{Q})\cong U(\mathbb{Z}/m_i\mathbb{Z}).$$



Consideriamo l'estensione $L(\zeta_{m_1}, \ldots, \zeta_{m_r})/K$. Abbiamo che

$$Gal(L(\zeta_{m_1}, \ldots, \zeta_{m_r})/K) \cong G \times G_1 \times \cdots \times G_r.$$

Il seguente reticolo rappresenta il caso $r = 2$.



Siano $G = \langle \sigma \rangle$ e, per ogni i, $\tau_i \in G_i$ come nella dimostrazione del lemma di Artin; in $G \times G_i$ consideriamo il sottogruppo

$$H_i = \langle (\sigma, \tau_i), (\phi_{L/K}(\mathfrak{p}_i), \phi_{K(\zeta_{m_i})/K}(\mathfrak{p}_i)) \rangle;$$

sia F_i il sottocampo di $L(\zeta_{m_1}, \ldots, \zeta_{m_r})$ tenuto fisso da $H_i \times \prod_{j \neq i} G_j$; $F \equiv F_1 \ldots F_r$.

Osserviamo che $F_i \leq L(\zeta_{m_i})$ (stiamo cioè facendo la stessa costruzione del lemma di Artin, per ogni $i = 1, \ldots, r$): nel caso $r = 2$, F_1 è fissato da $H_1 \times G_2 \geq 1 \times 1 \times G_2 = Gal(L(\zeta_{m_1}, \zeta_{m_2})/L(\zeta_{m_1}))$, quindi $F_1 \leq L(\zeta_{m_1})$.

Si dimostra che $F \cap L = K$, così $Gal(LF/F) \cong Gal(L/K)$.

Si trova che:

$$\mathfrak{A} = \mathfrak{B} \left(\prod_{i=1}^{r} \alpha_i \right) \left(\prod_{i=1}^{r} N_{LF_i|K}(\mathfrak{D}_i) \right),$$

con $\mathfrak{B} \in N_{L|K}(I_L^{\mathfrak{m}})$, $\alpha_i \in K_{m,1}$ e $\mathfrak{D}_i \in I_{LF_i}^{\mathfrak{m}}$. Definiamo $\mathfrak{D}'_i = N_{LF_i|L}(\mathfrak{D}_i) \in I_L^{\mathfrak{m}}$. Poiché (per 2.1.1)

$$N_{L|K}(\mathfrak{D}'_i) = N_{L|K}(N_{LF_i|L}(\mathfrak{D}_i)) = N_{LF_i|K}(\mathfrak{D}_i),$$

segue che

$$N_{LF_i|K}(\mathfrak{D}_i) = N_{L|K}(\mathfrak{D'}_i) \in N_{L|K}(I_L^{\mathfrak{m}}),$$

e dunque

$$\mathfrak{A} = \left(\prod_{i=1}^{r} \alpha_i\right) \mathfrak{B} \left(\prod_{i=1}^{r} N_{L|K}(\mathfrak{D'}_i)\right) = \left(\prod_{i=1}^{r} \alpha_i\right) \mathfrak{B} N_{L|K} \left(\prod_{i=1}^{r} \mathfrak{D'}_i\right).$$

In conclusione

$$\mathfrak{A} \in i(K_{\mathfrak{m},1}) N_{L|K}(I_L^{\mathfrak{m}}),$$

da cui la tesi.

Omettiamo i dettagli.

□

Con il risultato valido per un'estensione ciclica possiamo ora provarlo per un'estensione abeliana.

Teorema 3.2.2 (Teorema di reciprocità di Artin)**.** *Sia L/K un'estensione abeliana, con $\mathfrak{m}$ divisibile da tutti i primi di K che ramificano in L; si supponga che gli esponenti dei divisori primi di $\mathfrak{m}$ siano sufficientemente grandi. Allora*

$$Ker(\phi_{L/K}) = N_{L|K}(I_L^{\mathfrak{m}}) i(K_{\mathfrak{m},1}).$$

Dimostrazione. Sia $G = Gal(L/K)$; essendo un gruppo abeliano finito, si ha la decomposizione in prodotto diretto di gruppi ciclici:

$$G = C_1 \times \cdots \times C_s.$$

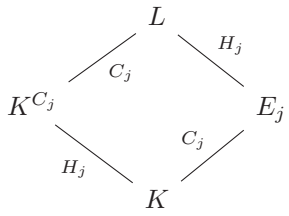
Definiamo

$$H_j = \prod_{i \neq j} C_i,$$

cosicché $G = C_j \times H_j$, $\forall\, j = 1, \ldots, s$; infine sia

$$E_j = \{\, x \in L \mid \rho(x) = x \ \forall \rho \in H_j \,\}$$

il sottocampo di L tenuto fisso da H_j.



Le estensioni E_j/K sono normali perché G è abeliano, e

$$Gal(E_j/K) \cong \frac{Gal(L/K)}{Gal(L/E_j)} = \frac{G}{H_j} \cong C_j,$$

cioè tali estensioni sono cicliche. Il Teorema 3.2.1 ci dice allora che, per ogni j, esiste un modulus $\mathfrak{m}_j$ di K tale che $(E_j, K, \mathfrak{m}_j)$ soddisfano la legge di reciprocità, quindi

$$i(K_{\mathfrak{m}_j,1}) \leq Ker(\phi_{E_j/K}) \quad \forall\, j = 1, \ldots, s.$$

Possiamo supporre $\mathfrak{m}$ divisibile da tutti gli $\mathfrak{m}_j$: allora (esempio 3.1.2) la legge di reciprocità vale anche per $(E_j, K, \mathfrak{m})$, per tutti i j: quindi

$$i(K_{\mathfrak{m},1}) \leq Ker(\phi_{E_j/K}) \quad \forall\, j = 1, \ldots, s,$$

cioè

$$i(K_{\mathfrak{m},1}) \leq \bigcap_{j=1}^{s} Ker(\phi_{E_j/K}).$$

Ora dimostriamo che per $(L, K, \mathfrak{m})$ vale la legge di reciprocità, ossia che

$$i(K_{\mathfrak{m},1}) \leq Ker(\phi_{L/K}).$$

Sia $\mathfrak{A} \in I_K^{\mathfrak{m}}$ un ideale frazionario di K. La proprietà 4 della proposizione 2.2.1 implica che

$$\phi_{L/K}(\mathfrak{A})|_{E_j} = \phi_{E_j/K}(\mathfrak{A}).$$

Infatti, detto $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, allora:

$$\phi_{L/K} \colon I_K^{\mathfrak{m}} \to Gal(L/K), \quad \mathfrak{A} \mapsto \prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{n(\mathfrak{p})},$$

$$\phi_{E_j/K} \colon I_K^{\mathfrak{m}} \to Gal(E_j/K), \quad \mathfrak{A} \mapsto \prod_{\mathfrak{p}} \left[\frac{E_j/K}{\mathfrak{p}}\right]^{n(\mathfrak{p})},$$

e si ha che

$$\phi_{L/K}(\mathfrak{A})|_{E_j} = \phi_{L/K}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}\right)\Big|_{E_j} = \left(\prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{n(\mathfrak{p})}\right)\Big|_{E_j} =$$

$$= \prod_{\mathfrak{p}} \left(\left[\frac{L/K}{\mathfrak{p}}\right]\Big|_{E_j}\right)^{n(\mathfrak{p})} = \prod_{\mathfrak{p}} \left[\frac{E_j/K}{\mathfrak{p}}\right]^{n(\mathfrak{p})} = \phi_{E_j/K}(\mathfrak{A}).$$

Consideriamo ora $\mathfrak{A} \in i(K_{\mathfrak{m},1})$ e dimostriamo che $\mathfrak{A} \in Ker(\phi_{L/K})$.

$$\mathfrak{A} \in i(K_{\mathfrak{m},1}) \leq \bigcap_{j=1}^{s} Ker(\phi_{E_j/K}) \Rightarrow id_{E_j} = \phi_{E_j/K}(\mathfrak{A}) = \phi_{L/K}(\mathfrak{A})|_{E_j},$$

per ogni j. Sia $E = E_1 \ldots E_s \leq L$. Poiché $\phi_{L/K}(\mathfrak{A}) \in Gal(L/K)$, $\phi_{L/K}(\mathfrak{A})|_{E_j} = id_{E_j}$ $\forall j$, allora $\phi_{L/K}(\mathfrak{A})|_E = id_E$, cioè $\phi_{L/K}(\mathfrak{A})$ tiene fisso E. Ma E è il campo tenuto fisso dall'intersezione degli H_j, che è banale: dunque $E = L$. Abbiamo così mostrato che $\phi_{L/K}(\mathfrak{A}) = id_L$, e dunque

$$i(K_{\mathfrak{m},1}) \leq Ker(\phi_{L/K}).$$

Il lemma 3.1.1 permette allora di concludere che

$$Ker(\phi_{L/K}) = N_{L|K}(I_L^{\mathfrak{m}}) i(K_{\mathfrak{m},1}).$$

□

3.3 Teorema di Kronecker - Weber

Il seguente teorema permette, grazie al teorema 2.4.2, di dimostrare l'inclusione tra estensioni di K sotto alcune ipotesi su certi sottogruppi di $I_K^{\mathfrak{m}}$.

Teorema 3.3.1. *Sia L/K un'estensione abeliana, con $\mathfrak{m}$ tale che valga la legge di reciprocità per $(L, K, \mathfrak{m})$. Sia E/K un'estensione di Galois tale che*

$$N_{E|K}(I_E^{\mathfrak{m}}) \leq N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}).$$

Allora $L \leq E$.

Dimostrazione. Siano S_E, S_L gli insiemi degli ideali primi $\mathfrak{p} \triangleleft O_K$ che spezzano completamente rispettivamente in E e in L: mostriamo che $S_E \subset S_L$ eccetto che per un numero finito di primi, e concludiamo grazie al Teorema 2.4.2. Sia $\mathfrak{p} \in S_E$; se $\mathfrak{p}$ non è un divisore di $\mathfrak{m}_0$ (i quali sono in un numero finito), allora $\mathfrak{p} \in N_{E|K}(I_E^{\mathfrak{m}})$. Infatti

$$\mathfrak{p}O_E = \mathfrak{P}_1 \dots \mathfrak{P}_g \quad (g = [E : K]);$$

$$N_{E|K}(\mathfrak{P}_1) = \mathfrak{P}_1 \cap K = \mathfrak{p} \in N_{E|K}(I_E^{\mathfrak{m}}),$$

perché $\mathfrak{P}_1 \in I_E^{\mathfrak{m}}$ (proprio perché $\mathfrak{p}$ non divide $\mathfrak{m}_0$). Allora

$$\mathfrak{p} \in N_{E|K}(I_E^{\mathfrak{m}}) \leq N_{L|K}(I_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}) = Ker(\phi_{L/K});$$

la disuguaglianza è l'ipotesi, e l'uguaglianza segue dal fatto che $(L, K, \mathfrak{m})$ soddisfano la legge di reciprocità. Quindi $\mathfrak{p} \in Ker(\phi_{L/K})$, cioè spezza completamente in L (Proposizione 2.2.1, proprietà 1). Dunque, a meno di un numero finito di primi, $S_E \subset S_L$: per il Teorema 2.4.2, $L \leq E$.

□

Siamo ora pronti per dimostrare il Teorema di Kronecker - Weber.

Teorema 3.3.2 (Kronecker - Weber)**.** *Sia $L/\mathbb{Q}$ un'estensione abeliana. Esiste un campo ciclotomico $\mathbb{Q}(\zeta_m)$ che contiene L.*

Dimostrazione. Per il Teorema 3.2.2 esiste $\mathfrak{m}$ modulus di K tale che $(L, \mathbb{Q}, \mathfrak{m})$ soddisfano la legge di reciprocità, dunque

$$N_{L|\mathbb{Q}}(I_L^{\mathfrak{m}})i(\mathbb{Q}_{\mathfrak{m},1}) = Ker(\phi_{L/\mathbb{Q}}).$$

Poiché $K = \mathbb{Q}$, possiamo supporre $\mathfrak{m} = (m)p_\infty$, con $m \in \mathbb{N}$; siano allora $\zeta = \zeta_m$ una radice primitiva m-esima di 1, ed $E = \mathbb{Q}(\zeta)$. Dall'esempio 3.1.1 sappiamo che

$$i(\mathbb{Q}_{\mathfrak{m},1}) = Ker(\phi_{\mathbb{Q}(\zeta)/\mathbb{Q}}) = Ker(\phi_{E/\mathbb{Q}}).$$

Allora

$$N_{E|\mathbb{Q}}(I_E^{\mathfrak{m}}) \subset N_{E|\mathbb{Q}}(I_E^{\mathfrak{m}})i(\mathbb{Q}_{\mathfrak{m},1}) = Ker(\phi_{E/\mathbb{Q}}) =$$

$$= i(\mathbb{Q}_{\mathfrak{m},1}) \subset N_{L|\mathbb{Q}}(I_L^{\mathfrak{m}})i(\mathbb{Q}_{\mathfrak{m},1}) = Ker(\phi_{L/\mathbb{Q}}).$$

Per il Teorema 3.3.1, $L \leq E = \mathbb{Q}(\zeta_m)$.

□

Osservazione 3.3.1. Conseguenza immediata del teorema 3.3.2 è la seguente: sia $\alpha \in \mathbb{C}$ un intero algebrico, $f = f_\alpha \in \mathbb{Z}[x]$ il suo polinomio minimo, $\Omega/\mathbb{Q}$ il campo di spezzamento di f. Se $Gal(\Omega/\mathbb{Q})$ è abeliano, allora esiste ζ_m radice primitiva m-esima di 1 tale che $\Omega \subset \mathbb{Q}(\zeta_m)$. Dunque $\alpha \in O_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$, cioè

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i {\zeta_m}^i,$$

con $a_i \in \mathbb{Z}$.

Esempio 3.3.1. Sia $K = \mathbb{Q}(\sqrt{2})$; mostriamo che il Teorema 3.3.2 non vale per K, ossia che esistono estensioni abeliane L/K che non sono contenute in alcuna estensione ciclotomica $K(\zeta)/K$.

Prendiamo $L = \mathbb{Q}(\sqrt[4]{2})$; l'estensione $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ è normale, con gruppo di Galois ciclico di ordine 2, così L/K è abeliana; $L/\mathbb{Q}$, invece, non è normale. Sia ζ_m una qualsiasi radice primitiva m-esima di 1, e $\phi_m(x) \in \mathbb{Q}[x]$ il polinomio ciclotomico m-esimo: l'estensione $K(\zeta_m)/\mathbb{Q} = \mathbb{Q}(\sqrt{2}, \zeta_m)/\mathbb{Q}$ è di Galois, perché campo di spezzamento del polinomio $(x^2 - 2)\phi_m(x)$, con gruppo

$$Gal(\mathbb{Q}(\sqrt{2}, \zeta_m)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong C_2 \times U(\mathbb{Z}/m\mathbb{Z}),$$

che è abeliano. Allora tutti i sottocampi di $K(\zeta_m)$ sono estensioni normali di $\mathbb{Q}$, quindi $L = \mathbb{Q}(\sqrt[4]{2})$ non è contenuto in $K(\zeta_m)$.

Osservazione 3.3.2. Successivamente alla dimostrazione del Teorema di Kronecker - Weber si è cominciato ad affrontare il caso $K \neq \mathbb{Q}$, con l'obiettivo di trovare risultati analoghi per le estensioni abeliane di un generico campo di numeri K. Abbiamo visto con l'esempio 3.3.1 che le estensioni ciclotomiche non sono più sufficienti allo scopo. Tale questione costituisce il *dodicesimo problema di Hilbert*, che è stato risolto solamente per $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, e in altri casi molto particolari.

Bibliografia

[1] Michael F. Atiyah, Ian G. Macdonald, *Introduction to Commutative Algebra*, Addison - Wesley Publishing Company, Reading (Massachusetts) - Menlo Park (California) - London - Don Mills (Ontario), 1969.

[2] Dennis Garbanati, *Class Field Theory summarized*, Rocky Mountain Journal of Mathematics, Volume 11, Number 2, 1981.

[3] Eknath Ghate, *The Kronecker - Weber Theorem*, in *Cyclotomic fields and related topics (Proceedings of the Summer school on Cyclotomic Fields, Pune, June 7-30, 1999)*, Bhaskaracharya Pratishthana, Pune, 1999.

[4] Gerald J. Janusz, *Algebraic number fields*, Academic Press, New York - London, 1973.

[5] Daniel A. Marcus, *Number Fields*, second edition, Springer International Publishing, Cham (Switzerland), 2018.

[6] James S. Milne, *Algebraic Number Theory*, Course notes, Version 3.08, 2020.

[7] James S. Milne, *Class Field Theory*, Course notes, Version 4.03, 2020.

[8] Richard A. Mollin, *Algebraic Number Theory*, second edition, Chapman & Hall/CRC, Boca Raton (Florida) - London - New York, 2011.

[9] William Stein, *Algebraic Number Theory, a Computational Approach*, Course notes, 2012.

[10] Lorenzo Vecchi, *Ideali nell'anello degli interi algebrici*, Tesi di Laurea in Matematica, 2017/2018, Università di Bologna.