Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

BASI INTEGRALI IN CAMPI DI NUMERI

Tesi di Laurea in Teoria Algebrica dei Numeri

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Mirco Carnaroli

Sessione Unica
Anno Accademico 2021-2022

a mio padre

Introduzione

I campi di numeri, cioè le estensioni finite del campo dei numeri razionali, sono uno degli oggetti più studiati in teoria algebrica dei numeri. L'anello R degli interi algebrici di un campo di numeri K riveste un particolare interesse, sia per la sua struttura di $\mathbb{Z}$-modulo libero, sia perché è possibile determinare una base di K costituita da elementi di R, detta base integrale.

In questo elaborato, che si articola in tre capitoli, descriviamo le principali caratteristiche dell'anello R e delle basi integrali.

Nel primo capitolo dimostriamo le principali proprietà dei moduli liberi su domini a ideali principali, in particolare il fatto che ogni tale modulo ha una base, la cui cardinalità, detta rango, è un invariante del modulo stesso. Dimostriamo inoltre che ogni sottomodulo di un modulo libero di rango n è libero di rango $k \leq n$. Trattiamo poi alcuni prerequisiti riguardanti le immersioni di campi e il composto di due campi.

Nel secondo capitolo introduciamo i concetti fondamentali di intero algebrico, traccia, norma, e discriminante. Quindi passiamo a studiare la struttura dell'anello R degli interi algebrici contenuti in un campo di numeri K. Esso risulta essere uno $\mathbb{Z}$-modulo libero di rango n, ove n è il grado di K sui razionali. Quindi studiamo le basi integrali, dando diversi criteri che utilizzano il discriminante per determinarle, e dimostrando che esiste sempre una base integrale di una forma particolare (si veda il Teorema 2.4.16). Infine, studiamo la struttura di R nel caso del composto di due campi, e anche in questo caso il discriminante sarà uno strumento fondamentale.

Nel terzo capitolo applichiamo le nozioni viste nel capitolo precedente

a due classi molto importanti di campi di numeri, i campi quadratici e i campi ciclotomici, caratterizzando l'anello R in entrambi i casi. In particolare mostriamo il celebre risultato che l'anello degli interi algebrici in un campo ciclotomico $\mathbb{Q}[\omega]$, ove ω è una radice primitiva m-esima dell'unità, è $\mathbb{Z}[\omega]$.

Indice

Capitolo 1

Alcune nozioni preliminari

In questo capitolo vedremo alcune nozioni preliminari che saranno utili più avanti nel corso della tesi.

1.1 Moduli su anelli commutativi

In questo paragrafo tratteremo le nozioni più elementari sui moduli unitari su anelli commutativi; in particolare vedremo che ogni sottomodulo di un modulo libero di rango n è libero di rango $k \leq n$.

Definizione 1.1.1. Sia A un anello. Un A-modulo è un insieme V dotato di due operazioni:

- una somma $+ \colon V \times V \to V, (u, v) \mapsto u + v$, e
- un prodotto per scalari $A \times V \to V, (a, v) \mapsto av$,

tali che $(V, +)$ sia un gruppo commutativo, e

1. $a(u + v) = au + av$ per ogni $a \in A$, $u, v \in V$
2. $(a + b)u = au + bu$ per ogni $a, b \in A$, $u \in V$
3. $(ab)u = a(bu)$ per ogni $a, b \in A$, $u \in V$

Se l'anello A è dotato di elemento unitario 1_A, e vale anche

4. $1_A u = u$ per ogni $u \in V$ ove 1_A è l'unita di A

si dice che il modulo V è unitario.

Nel seguito supporremo che l'anello A sia commutativo con unità e che gli A-moduli siano unitari.

Osservazione 1.1.2. 1. Ogni gruppo abeliano G, scritto in notazione additiva, è uno $\mathbb{Z}$-modulo ponendo

$$\begin{aligned} 0g &:= \mathbf{0} && \text{per ogni } g \in G \\ ng &:= \underbrace{a + \cdots + a}_{n \text{ volte}} && \text{per ogni } g \in G, \text{ per } n \in \mathbb{Z}^+ \\ mg &:= -|m|g && \text{per ogni } g \in G, \text{ per } m \in \mathbb{Z}^- \end{aligned}$$

2. Se K è un campo, ogni K-spazio vettoriale è un K-modulo.

Definizione 1.1.3. Siano U e V A-moduli. Una funzione $f\colon U \to V$ si dice *A-omomorfismo* o *omomorfismo di A-moduli* se è un omomorfismo di gruppi additivi e vale $f(au) = af(u)$ per ogni $a \in A$, per ogni $u \in U$.

Definizione 1.1.4. Sia U un A-modulo. Un sottoinsieme $S \subseteq U$ si dice sottomodulo di U se S è sottogruppo additivo di U e vale $au \in S$ per ogni $a \in A$, per ogni $u \in S$.

Osservazione 1.1.5. Ogni anello A è un A-modulo, e i suoi sottomoduli sono gli ideali.

Definizione 1.1.6. Dato V un A-modulo, e preso $X \subseteq V$ definiamo il sottomodulo generato da X su A come l'intersezione di tutti i sottomoduli di V contenenti X e lo denotiamo $\mathrm{Span}_A(X)$; in simboli

$$\mathrm{Span}_A(X) := \bigcap_{\substack{X \subseteq S \subseteq V \\ S \text{ sottomodulo di } V}} S.$$

Proposizione 1.1.7. *Nelle notazioni della definizione precedente vale*

$$\mathrm{Span}_A(X) = \left\{ \sum_{i=1}^{k} \lambda_i x_i \;\middle|\; k \in \mathbb{N}, \lambda_i \in A, x_i \in X \right\}.$$

Dimostrazione. Poniamo

$$D := \left\{ \sum_{i=1}^{k} \lambda_i x_i \;\middle|\; k \in \mathbb{N}, \lambda_i \in A, x_i \in X \right\}.$$

Poiché un sottomodulo è chiuso rispetto a somma e prodotto per scalari, ogni elemento di D è chiaramente contenuto in ogni sottomodulo di V che contiene X, e quindi anche nella loro intersezione. D'altra parte D è chiaramente un tale sottomodulo. □

Proposizione 1.1.8. *1. Siano U, V A-moduli, $f\colon U \to V$ un A-omomorfismo; allora* $\operatorname{Ker} f$ *e* $\operatorname{Im} f$ *sono sottomoduli rispettivamentedi U e V.*

2. Siano U, V A-moduli, con $U \subseteq V$. Allora V/U è un A-modulo con l'operazione di prodotto scalare definita da $a(v + U) := av + U$ per $a \in A$ e $v + U \in V/U$. Inoltre la funzione proiezione $\pi\colon V \to V/U$ è un omomorfismo di A-moduli.

3. Siano U, V A-moduli, $f\colon U \to V$ un A-omomorfismo; allora

$$\operatorname{Im} f \cong U/\operatorname{Ker} f$$

come A-moduli.

Definizione 1.1.9. Sia V un A-modulo e siano $V_1, \ldots, V_s$ sottomoduli di V. Si dice che V è somma diretta di $V_1, \ldots, V_s$ e si scrive

$$V = V_1 \oplus \cdots \oplus V_s = \bigoplus_{i=1}^{s} V_i$$

se

1. $V = \operatorname{Span}_A(V_1 \cup \cdots \cup V_s)$ e
2. $V_i \cap \operatorname{Span}_A(V_1 \cup \cdots \cup V_{i-1} \cup V_{i+1} \cup \cdots \cup V_s) = \mathbf{0}$ per ogni $i = 1, \ldots, s$.

Proposizione 1.1.10. *Sia V un A-modulo. Se $V = V_1 \oplus \cdots \oplus V_s$ allora ogni $v \in V$ si scrive in modo unico come*

$$v = v_1 + \cdots + v_s$$

con $v_i \in V_i$ per ogni $i = 1, \ldots, s$.

Dimostrazione. Sia $v \in V$. Poiché i V_i sono sottomoduli, per ogni $i = 1, \ldots, s$ esitono $v_i \in V_i$ tali che $v = v_1 + \cdots + v_s$. Se $v = \mathbf{0}$ l'unico modo di scrivere v in questo modo è se $v_i = \mathbf{0}$ per ogni $i = 1, \ldots, s$, perchè altrimenti avremmo che un elemento non nullo di V_i si esprimerebbe come somma di elementi di $V_1 \cup \cdots \cup V_{i-1} \cup V_{i+1} \cup \cdots \cup V_s$, in contraddizione con la definizione di somma diretta. Supponiamo ora $v \neq \mathbf{0}$. Se $v_i' \in V_i$ sono tali che $v = v_1' + \cdots + v_s'$, segue che

$$\sum_{i=1}^{s} v_i - v_i' = \mathbf{0}$$

e quindi $v_i = v_i'$ per ogni $i = 1, \ldots, s$. □

Definizione 1.1.11. Un A-modulo V si dice *finitamente generato* se esiste un sottoinsieme finito $X \subseteq V$ tale che $V = \mathrm{Span}_A(X)$.

Introduciamo le seguenti notazioni: se V è un A-modulo e $v \in V$ indichiamo con Av il sottomodulo generato da v, ossia

$$Av = \{av | a \in A\}$$

Inoltre indichiamo con $\{e_1, \ldots, e_n\}$ la base canonica di A^n, cioè e_i è l'n-pla di elementi di A il cui unico elemento non nullo è quello di posto i uguale a 1.

Definizione 1.1.12. Un A-modulo V finitamente generato si dice libero se $V \cong Ae_1 \oplus \cdots \oplus Ae_n = A^n$ per qualche $n \in \mathbb{Z}^+$

Definizione 1.1.13. Sia V un A-modulo. Un sottoinsieme $B \subseteq V$, $B = \{ v_\lambda \mid \lambda \in \Lambda \}$ si dice base di V se $V = \mathrm{Span}_A(B)$ e gli elementi di B sono linearmente indipendenti, il che vuol dire che per ogni scelta di un numero finito di indici $\lambda_1, \ldots, \lambda_k \in \Lambda$ e presi comunque $a_{\lambda_1}, \ldots, a_{\lambda_k} \in A$ da $\sum_{i=1}^{k} a_{\lambda_i} v_{\lambda_i} = \mathbf{0}$ segue che $a_{\lambda_i} = 0$ per ogni $i = 1, \ldots, k$.

Proposizione 1.1.14. *Un A-modulo V finitamente generato è libero se e solo se ha una base.*

Dimostrazione. Se V è libero esiste un isomorfismo $\phi\colon V \to A^n$. Mostriamo che allora $B := \phi^{-1}(\{e_1, \dots, e_n\})$ è una base di V. Preso $v \in V$ esistono $a_1, \dots, a_n \in A$ tali che $\phi(v) = \sum_{i=1}^n a_i e_i$ per cui applicando ϕ^{-1} otteniamo $v = \sum_{i=1}^n a_i \phi^{-1}(e_i)$ per cui B genera V. Inoltre presi $a_1, \dots, a_n \in A$ tali che $\sum_{i=1}^n a_i \phi^{-1}(e_i) = \mathbf{0}$ applicando ϕ segue che $\sum_{i=1}^n a_i e_i = \mathbf{0}$ da cui ovviamente $a_1 = \cdots = a_n = 0$, per cui B è anche un insieme di vettori linearmente indipendenti.

Viceversa, sia $B = \{\, v_\lambda \mid \lambda \in \Lambda \,\}$ una base di V. Per ipotesi esiste un sottoinsieme finito $X \subseteq V, X = \{x_1, \dots, x_n\}$ tale che $V = \mathrm{Span}_A(X)$; dunque per ogni $x_i \in X$ esistono $\lambda_1^{(i)}, \dots, \lambda_{k_i}^{(i)} \in \Lambda$ e $a_1^{(i)}, \dots, a_{k_i}^{(i)} \in A$ tali che

$$x_i = \sum_{j=1}^{k_i} a_j^{(i)} v_{\lambda_j^{(i)}}$$

e dunque deve essere $B = \left\{ v_{\lambda_j^{(i)}} \;\middle|\; j \in \{1, \dots, k_i\}, i \in \{1, \dots, n\} \right\}$ poiché questo è un insieme di generatori che sono linearmente indipendenti. Abbiamo quindi mostrato che B è necessariamente un insieme finito; denotiamo i suoi elementi $B = \{v_1, \dots, v_n\}$. Mostriamo allora che la funzione

$$\begin{aligned} \psi\colon A^n &\to V \\ a &\mapsto \sum_{i=1}^n a_i v_i \end{aligned}$$

è un isomorfismo di A-moduli. Indichiamo $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n)$ $a, b \in A^n$. Abbiamo che $\psi(0, \dots, 0) = \mathbf{0}$, inoltre

$$\psi(a + b) = \sum_{i=1}^n (a_i + b_i) v_i = \sum_{i=1}^n a_i v_i + \sum_{i=1}^n b_i v_i = \psi(a) + \psi(b),$$

e, per $\lambda \in A$

$$\psi(\lambda a) = \sum_{i=1}^n \lambda a_i v_i = \lambda \sum_{i=1}^n a_i v_i = \lambda \psi(a).$$

Questo mostra che ψ è un A-omomorfismo. Inoltre è iniettivo, perché da $\psi(a) = \psi(b)$ segue che

$$\sum_{i=1}^n (a_i - b_i) v_i = \mathbf{0}$$

da cui, per la lineare indipendenza, $a_i = b_i$ per ogni $i = 1, \dots, n$ cioè $a = b$. Infine ψ è suriettivo, poiché, preso $v \in V$ esistono $a_1, \dots, a_n \in A$ tali che $v = \sum_{i=1}^{n} a_i v_i$ il che vuol dire che $v = \psi(a)$. □

Proposizione 1.1.15. *Sia A un dominio a ideali principali, V un A-modulo libero finitamente generato, e $(a) \subseteq A$ un ideale massimale. Poniamo*

$$V_a := \mathrm{Span}_A(\{bv \mid b \in (a), v \in V\}).$$

Allora V_a è sottomodulo di V e ${}^{V}\!/_{V_a}$ è un ${}^{A}\!/_{(a)}$-modulo ponendo

$$\big(\lambda + (a)\big)\big(v + V_a\big) = \lambda v + V_a.$$

Inoltre, se $B = \{v_1, \dots, v_n\}$ è una base di V allora $B' = \{v_1 + V_a, \dots, v_n + V_a\}$ è una base di ${}^{V}\!/_{V_a}$ come ${}^{A}\!/_{(a)}$-modulo.

Dimostrazione. Per come l'abbiamo definito, V_a è un sottomodulo. Mostriamo ora che il prodotto scalare

$$\begin{aligned} {}^{A}\!/_{(a)} \times {}^{V}\!/_{V_a} &\to {}^{V}\!/_{V_a} \\ (\lambda + (a), v + V_a) &\mapsto \lambda v + V_a \end{aligned}$$

è ben definito. Supponiamo di avere $\lambda_1, \lambda_2 \in A$ tali che $\lambda_1 + (a) = \lambda_2 + (a)$ e $v_1, v_2 \in V$ tali che $v_1 + V_a = v_2 + V_a$. Dalla prima uguaglianza segue che $\lambda_1 - \lambda_2 \in (a)$, da cui $\lambda_1 v_1 - \lambda_2 v_2 \in V_a$ e quindi $\lambda_1 v_1 + V_a = \lambda_2 v_2 + V_a$. Dalla seconda uguaglianza segue che $v_1 - v_2 \in V_a \subseteq V$, da cui $\lambda_2 v_1 - \lambda_2 v_2 \in V_a$ e quindi $\lambda_2 v_1 + V_a = \lambda_2 v_2 + V_a$. Abbiamo quindi che $\lambda_1 v_1 + V_a = \lambda_2 v_2 + V_a$, ossia che il prodotto scalare non dipende dai rappresentanti delle classi di equivalenza scelti ed è quindi ben definito. In conseguenza di ciò esso eredita tutte le proprietà della definizione 1.1.1 del prodotto scalare di V e quindi abbiamo anche mostrato che ${}^{V}\!/_{V_a}$ è un ${}^{A}\!/_{(a)}$-modulo. Mostriamo ora che B' è una base di ${}^{V}\!/_{V_a}$.

Essa è un insieme di generatori, poiché, preso $v + V_a \in {}^{V}\!/_{V_a}$, esisteranno $\lambda_1, \dots, \lambda_n \in A$ tali che $v = \sum_{i=1}^{n} \lambda_i v_i$ e quindi abbiamo che

$$v + V_a = \sum_{i=1}^{n} \lambda_i v_i + V_a = \sum_{i=1}^{n} \big(\lambda_i + (a)\big)\big(v_i + V_a\big).$$

Per mostrare che gli elementi di B' sono linearmente indipendenti, supponiamo di avere $\lambda_1+(a),\dots,\lambda_n+(a) \in {}^{A}\!/_{(a)}$ tali che $\sum_{i=1}^{n}\big(\lambda_i+(a)\big)\big(v_i+V_a\big) = \mathbf{0}$, ossia $\sum_{i=1}^{n}\lambda_i v_i \in V_a$, per cui esistono $b_j \in (a)$, $w_j \in V$ per $j = 1,\dots,k$ tali che

$$\sum_{i=1}^{n}\lambda_i v_i = \sum_{j=1}^{k} b_j w_j.$$

Ora, per ogni j esistono $r_{1j},\dots,r_{nj} \in A$ tali che $w_j = \sum_{i=1}^{n} r_{ij}v_i$, dunque abbiamo che

$$\sum_{i=1}^{n}\lambda_i v_i = \sum_{j=1}^{k} b_j w_j = \sum_{j=1}^{k} b_j \sum_{i=1}^{n} r_{ij}v_i = \sum_{i=1}^{n}\Big(\sum_{j=1}^{k} b_j r_{ij}\Big)v_i$$

da cui $\sum_{i=1}^{n}\big(\lambda_i - \sum_{j=1}^{k} b_j r_{ij}\big)v_i = 0$, e quindi, per la lineare indipendenza dei v_i segue che

$$\lambda_i = \sum_{j=1}^{k} b_j r_{ij} \in (a)$$

per ogni $i = 1,\dots,n$, che è esattamente quello che volevamo. □

Corollario 1.1.16. *Siano A un dominio a ideali principali e V un A-modulo libero finitamente generato non nullo. Allora due basi di V hanno la stessa cardinalità.*

Dimostrazione. Osserviamo che, se (a) è un ideale massimale, ossia se a è un elemento irriducibile di A, ${}^{A}\!/_{(a)}$ è un campo, e dunque ${}^{V}\!/_{V_a}$ è un ${}^{A}\!/_{(a)}$-spazio vettoriale. Dunque, se B e C sono due basi di V e B',C' le corrispondenti basi di ${}^{V}\!/_{V_a}$, allora $|B'| = |C'|$ per la definizione di dimensione di uno spazio vettoriale finitamente generato. Dunque $|B| = |B'| = |C'| = |C|$. □

Da qui fino alla fine del paragrafo supporremo che A sia un dominio a ideali principali.

Definizione 1.1.17. Si dice che un A-modulo libero finitamente generato ha rango n se n è la cardinalità di una sua qualsiasi base.

Osservazione 1.1.18. Il sottomodulo generato da n elementi linearmente indipendenti di un modulo è un modulo libero di rango n.

Teorema 1.1.19. *Se V è un A-modulo libero finitamente generato di rango n allora ogni suo sottomodulo è libero di rango $m \leq n$.*

Dimostrazione. Sia M un sottomodulo di V. La dimostrazione è per induzione su n. Supponiamo che $n = 1$; se $M = \{\mathbf{0}\}$ non c'è nulla da dimostrare. Se invece $M \neq \{\mathbf{0}\}$, siccome in questo caso $V \cong A$ e i sottomoduli di A sono gli ideali, dev'essere $M \cong (a)$ per qualche $a \in A, a \neq 0$. Infine (a) è un modulo libero di rango 1, poiché è isomorfo ad A mediante l'isomorfismo

$$\begin{aligned} \phi\colon A &\to (a) \\ \lambda &\mapsto \lambda a. \end{aligned}$$

Supponiamo ora che il teorema sia vero per $n-1$ e mostriamolo per n. Se $\{v_1, \ldots, v_n\}$ è una base di V, poniamo

$$\begin{aligned} \pi\colon V &\to A \\ \lambda_1 v_1 + \ldots + \lambda_n v_n &\mapsto \lambda_n \end{aligned}$$

e osserviamo che $\operatorname{Ker}\pi$ è un sottomodulo di V di rango $n-1$. Infatti $\operatorname{Ker}\pi = \operatorname{Span}_A(\{v_1, \ldots, v_{n-1}\})$. Dunque per ipotesi induttiva ogni sottomodulo di $\operatorname{Ker}\pi$ è un modulo libero di rango $\leq n-1$. Consideriamo ora $\pi|_M$ e distinguiamo due casi: se $\operatorname{Im}\pi|_M = \{\mathbf{0}\}$ allora $M \subseteq \operatorname{Ker}\pi$ e quindi per ipotesi induttiva è un modulo libero di rango $\leq n-1 < n$. Se invece $\operatorname{Im}\pi|_M \neq \{\mathbf{0}\}$ abbiamo che $\operatorname{Im}\pi|_M$ è un sottomodulo di A, ossia un ideale, per cui esiste $a \in A, a \neq 0$ tale che $\operatorname{Im}\pi|_M = (a)$ e quindi esiste $v \in M, v \neq \mathbf{0}$ tale che $\pi(v) = a$. Poniamo $N := (\operatorname{Ker}\pi) \cap M = \operatorname{Ker}\pi|_M$ e mostriamo che

$$M = N \oplus Av. \tag{1.1}$$

Sia $u \in M$; allora $\pi(u) \in (a)$ e quindi esiste $\lambda \in A$ tale che

$$\pi(u) = \lambda a = \lambda\pi(v) = \pi(\lambda v)$$

per cui $x := u - \lambda v \in (\operatorname{Ker}\pi) \cap M = N$. Quindi $u = x + \lambda v$ e abbiamo mostrato che $M = \operatorname{Span}_A(N \cup Av)$. Supponiamo ora che $u \in Av \cap N$. Allora esiste $b \in A$ tale che $u = bv$ per cui $\pi(u) = b\pi(v) = ba$. Ma dev'essere anche $\pi(u) = 0$, da cui $ba = 0$. Poiché $a \neq 0$ da questo segue $b = 0$ e quindi $u = 0$. Abbiamo quindi mostrato (1.1). A questo punto osserviamo che N è sottomodulo di $\operatorname{Ker}\pi$, per cui per ipotesi induttiva è un modulo libero di rango $k \leq n-1$, ossia $N \cong A^k$. Abbiamo però che $Av \cong A$, per cui da (1.1) segue che

$$M = N \oplus Av \cong A^{k+1}$$

ossia M è un modulo libero di rango $k+1 \leq n$. □

Corollario 1.1.20. *Siano $U \subseteq V \subseteq W$ A-moduli, con U, W moduli liberi di rango n. Allora anche V è un modulo libero di rango n.*

Dimostrazione. Per il teorema precedente V, essendo sottomodulo di W, deve essere un modulo libero di rango $\leq n$. Tuttavia non può avere rango minore di n poiché in tal caso anche il rango di U dovrebbe essere minore di n e questo è in contraddizione con l'ipotesi che U ha rango n. □

1.2 Immersioni di campi

In questa sezione richiamiamo alcuni fatti e dimostriamo alcuni teoremi sulle estensioni algebriche di $\mathbb{Q}$ e sugli omomorfismi tra di esse.

Definizione 1.2.1. Siano K, L due campi, e sia $\sigma\colon K \to L$ un omomorfismo di anelli. Si dice che σ è un'*immersione di campi* se è iniettivo.

Osservazione 1.2.2. Ricordiamo che, poiché il nucleo di un omomorfismo di anelli è un ideale del dominio, e gli unici ideali di un campo K sono $\{0\}$ e K stesso, in realtà affinché un omomorfismo di campi sia iniettivo è sufficiente chiedere che sia non nullo. Inoltre, essendo ogni omomorfismo suriettivo sulla sua immagine, restringendo opportunamente il codominio ogni immersione diventa isomorfismo di campi.

Se $\sigma\colon K \to L$ è un'immersione di campi denotiamo con σK la sua immagine.

Lemma 1.2.3. *Sia $\sigma\colon K \to K'$ un isomorfismo di campi, e sia L un'estensione semplice di K, $L = K(\alpha)$, con f polinomio minimo di α su K. Sia poi L' un'estensione di K'. Allora σ si estende a un omomorfismo iniettivo $L \to L'$ se e solo se L' contiene una radice del polinomio $\sigma(f)$. Inoltre, se β è una radice di $\sigma(f)$ in L', c'è un unico omomorfismo iniettivo $\phi\colon L \to L'$ che estende σ e tale che $\phi(\alpha) = \beta$.*

Dimostrazione. Si veda [2, Teorema 5.3.3] □

Definizione 1.2.4. Un *campo di numeri* è un'estensione di grado finito di $\mathbb{Q}$.

Osservazione 1.2.5. Ogni campo di numeri è quindi anche un'estensione algebrica, e, per il teorema dell'elemento primitivo (si veda [1, Capitolo 5, Paragrafo 4][Cox]), un'estensione semplice.

I campi che considereremo nel resto di questo paragrafo saranno tutti campi di numeri.

Osservazione 1.2.6. Siccome $\mathbb{C}$ è algebricamente chiuso e contiene $\mathbb{Q}$, possiamo pensare ogni campo di numeri come sottocampo di $\mathbb{C}$. Inoltre, se $\sigma\colon K \to L$ è un'immersione di campi, essa fissa $\mathbb{Q}$, per cui anche σK è un campo di numeri, essendo $[K : \mathbb{Q}] = [\sigma K : \mathbb{Q}]$. Dunque possiamo pensare che il codominio di ogni immersione il cui dominio è un campo di numeri sia $\mathbb{C}$.

Teorema 1.2.7. *Siano $K \subseteq L$ campi di numeri. Allora ogni immersione di K in $\mathbb{C}$ si estende esattamente a $[L : K]$ immersioni di L in $\mathbb{C}$.*

Dimostrazione. La dimostrazione è per induzione su $[L : K]$. Se $[L : K] = 1$, allora $L = K$ e non c'è nulla da dimostrare. Supponiamo ora che $[L : K] > 1$ e che la tesi sia vera per ogni estensione di grado minore di $[L : K]$. Sia

dunque σ immersione di K in $\mathbb{C}$, sia $\alpha \in L \setminus K$ e sia f il polinomio minimo di α su K, $f(x) = a_0 + \cdots + a_n x^n$. Sia

$$g(x) := \sum_{i=0}^{n} \sigma(a_i) x^i.$$

Abbiamo che g è irriducibile su σK, poiché $K[x]$ e $\sigma K[x]$ sono isomorfi mediante l'ovvia estensione di σ. Dunque, per il lemma precedente, per ogni radice $\beta \in \mathbb{C}$ di g esiste un isomorfismo

$$K[\alpha] \to \sigma K[\beta]$$

che estende σ e manda α in β. Dunque σ si estende a un'immersione di $K[\alpha]$ in $\mathbb{C}$ che manda K in σK e α in β. Poiché possiamo scegliere β in n modi diversi, possiamo estendere σ a $K[\alpha]$ in n modi diversi. Inoltre non ci sono altri modi per estendere σ a $K[\alpha]$, perché ogni estensione di questo tipo deve mandare α in una radice di g, sempre per il lemma. Per ipotesi induttiva ciascuna di queste n immersioni di $K[\alpha]$ si estende a esattamente $\big[L : K[\alpha]\big]$ immersioni di L in $\mathbb{C}$. Dunque abbiamo che ci sono esattamente

$$\big[L : K[\alpha]\big] n = \big[L : K[\alpha]\big] \big[K[\alpha] : K\big] = [L : K]$$

immersioni di L in $\mathbb{C}$ che estendono σ. □

Corollario 1.2.8. *Siano $K \subseteq L$ campi di numeri. Allora ci sono esattamente $[L : K]$ immersioni di L in $\mathbb{C}$ che fissano K.*

Dimostrazione. Basta applicare il teorema precedente alla funzione identità su K, che è un'immersione di K in $\mathbb{C}$. □

Definizione 1.2.9. Siano $K \subseteq L$ campi di numeri, sia $\alpha \in L \setminus K$ e sia $f \in K[x]$ il polinomio minimo di α su K. Le radici di f in $\mathbb{C}$ sono dette coniugati di α.

Osservazione 1.2.10. Osserviamo che, nelle notazioni della definizione precedente, se σ è un'immersione di L che fissa K, $\sigma(\alpha)$ è un coniugato di α. Infatti, se $f(x) = a_0 + \cdots + a_n x^n$ è il polinomio minimo di α su K, applicando σ all'equazione $f(\alpha) = a_0 + \cdots + a_n \alpha^n = 0$ otteniamo $f(\sigma(\alpha)) = a_0 + \cdots + a_n \sigma(\alpha)^n = 0$

Osservazione 1.2.11. Osserviamo che un'estensione $K \subseteq N$ è normale se e solo se N contiene tutti i coniugati di ogni suo elemento su K.

Proposizione 1.2.12. *L'estensione $K \subseteq N$ è normale se e solo se ogni immersione di N in $\mathbb{C}$ che fissa K è un automorfismo di N.*

Dimostrazione. Se $K \subset N$ è normale, allora, preso $\alpha \in N$ e σ immersione di N in $\mathbb{C}$ che fissa K, in effetti $\sigma(\alpha) \in N$, per cui $\sigma\colon N \to N$. In effetti σ è anche suriettivo, poiché la sua immagine ha grado $[N : K]$ su K.

Viceversa, sia $\alpha \in N$, e sia β un coniugato di α. Allora, per il lemma 1.2.3, esiste un'immersione σ di N in $\mathbb{C}$ che fissa K e manda α in β. Per ipotesi σ è un automorfismo, per cui $\beta \in N$. □

1.3 Composto di due campi

In questo paragrafo definiamo il composto di due campi, lo caratterizziamo nel caso dei campi di numeri e dimostriamo un lemma che verrà impiegato più avanti.

Definizione 1.3.1. Siano $F \subseteq K \subseteq M$ e $F \subseteq L \subseteq M$ estensioni di campi. Definiamo il composto dei due campi K e L, e lo denotiamo con KL, come l'intersezione di tutti i campi contenuti in M che contengono sia K che L. In simboli

$$KL := \bigcap_{\substack{K,L \subseteq E \subseteq M \\ E \text{ campo}}} E.$$

Osservazione 1.3.2. Per come lo abbiamo definito, KL è il minimo campo che contiene sia K che L. Dunque vale $KL = K(L)$ poiché $K(L)$ è la minima estensione di K che contiene L, e analogamente $KL = L(K)$. Vale anche $KL = F(K \cup L)$ per lo stesso motivo.

Passiamo ora al caso dei campi di numeri. Se K e L sono campi di numeri abbiamo che $\mathbb{Q}$ è sottocampo di entrambi, e entrambi sono sottocampi di $\mathbb{C}$. Quindi ha senso parlare del loro composto. Abbiamo inoltre che

$K(L) = K[L]$ perché ogni elemento di L è algebrico su $\mathbb{Q}$ e quindi su K, e analogamente $L(K) = L[K]$. L'insieme $K[L]$ è caratterizzato come segue:

$$K[L] = \left\{ f(l_1, \ldots, l_s) \mid f \in K[x_1, \ldots, x_s], l_1, \ldots, l_s \in L, s \in \mathbb{Z}^+ \right\}.$$

Poiché però le potenze di $l \in L$ sono ancora elementi di L abbiamo in effetti che

$$KL = K[L] = \left\{ k_1 l_1 + \cdots + k_s l_s \mid k_1, \ldots, k_s \in K, l_1, \ldots, l_s \in L, s \in \mathbb{Z}^+ \right\}.$$

Per concludere dimostriamo il

Lemma 1.3.3. *Siano K e L campi di numeri con $[K : \mathbb{Q}] = m$ e $[L : \mathbb{Q}] = n$, tali che $[KL : \mathbb{Q}] = mn$. Siano σ un'immersione di K in $\mathbb{C}$ e τ un'immersione di L in $\mathbb{C}$. Allora esiste un'immersione di KL in $\mathbb{C}$ che ristretta a K coincide con σ e ristretta a L coincide con τ.*

Dimostrazione. Per il corollario 1.2.8 σ si estende a $n = [KL : K]$ immersioni di KL in $\mathbb{C}$, siano esse $\sigma_1, \ldots, \sigma_n$. Queste n immersioni sono tutte distinte quando ristrette a L. Infatti, prese $\sigma_i \neq \sigma_j$ esiste $\alpha \in KL$ tale che $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. Ma allora per quanto osservato sopra esistono $k_1, \ldots, k_s \in K, l_1, \ldots, l_s \in L$ tali che

$$\alpha = \sum_{t=1}^{s} k_t l_t$$

e quindi abbiamo che

$$\sigma_i(\alpha) = \sum_{t=1}^{s} \sigma(k_t)\sigma_i(l_t)$$
$$\sigma_j(\alpha) = \sum_{t=1}^{s} \sigma(k_t)\sigma_j(l_t)$$

da cui segue che, per qualche $l_t \in L$, $\sigma_i(l_t) \neq \sigma_j(l_t)$. Ora, poiché L ha esattamente $n = [L : \mathbb{Q}]$ immersioni in $\mathbb{C}$, queste devono essere le $\sigma_1, \ldots, \sigma_n$ e quindi fra queste ci deve essere τ. □

Capitolo 2

Interi algebrici

2.1 Definizione e prime proprietà

Definizione 2.1.1. Un elemento $\alpha \in \mathbb{C}$ si dice *intero algebrico* se esiste un polinomio monico $f \in \mathbb{Z}[x]$ tale che $f(\alpha) = 0$.

Notiamo che non abbiamo richiesto che il polinomio f sia irriducibile su $\mathbb{Q}$, quindi ad esempio tutte le radici e le radici dell'unità sono interi algebrici. In effetti però possiamo provare che ogni intero algebrico è radice di un polinomio monico irriducibile a coefficienti in $\mathbb{Z}$.

Lemma 2.1.2. *Sia $f \in \mathbb{Z}[x]$ polinomio monico, e supponiamo che $f = gh$, con $g, h \in \mathbb{Q}[x]$ monici. Allora $g, h \in \mathbb{Z}[x]$.*

Dimostrazione. Siano $m, n \in \mathbb{Z}^+$ rispettivamente i minimi interi positivi tali che mg, nh abbiano coefficienti interi. Mostriamo che allora i coefficienti di mg non hanno alcun fattore in comune. Supponiamo che

$$g(x) = a_0 + a_1 x + \cdots + x^k,$$

con $a_i \in \mathbb{Q}$ per ogni $i = 0, \ldots, k-1$, e supponiamo anche che esista $l \in \mathbb{Z}^+, l > 1$ tale che $l \mid ma_i$ per ogni $i = 0, \ldots, k-1$ e $l \mid m$. Allora $\frac{m}{l} g$ è ancora a coefficienti in $\mathbb{Z}$, contro la minimalità nella scelta di m. Analogamente anche i coefficienti di nh non hanno alcun fattore in comune.

Vogliamo ora mostrare che $m = n = 1$. Supponiamo per assurdo che $mn > 1$, e sia p un numero primo che divide mn. Consideriamo l'equazione

$$mnf = (mg)(nh)$$

e applichiamo l'omomorfismo di anelli $\mathbb{Z}[x] \to \mathbb{Z}_p[x], f \mapsto \overline{f}$, ottenendo così $0 = \overline{mg}\,\overline{nh}$. Tuttavia $\mathbb{Z}_p[x]$ è un dominio di integrità, per cui $\overline{mg} = 0$ oppure $\overline{nh} = 0$. Ma questo vuol dire che p divide tutti i coefficienti di mg oppure di nh. Per quanto mostrato sopra questo è assurdo. Dunque $m = n = 1$ e $g, h \in \mathbb{Z}[x]$. □

Teorema 2.1.3. *Sia α un intero algebrico, e sia $f \in \mathbb{Z}[x]$ il polinomio monico di grado minimo tale che $f(\alpha) = 0$. Allora f è irriducibile su $\mathbb{Q}$. Equivalentemente, il polinomio minimo di α su $\mathbb{Q}$ è a coefficienti in $\mathbb{Z}$.*

Dimostrazione. Supponiamo per assurdo che f non sia irriducibile; allora $f = gh$ con $g, h \in \mathbb{Q}[x]$ non costanti. Possiamo supporre g, h monici. Allora per il lemma precedente $g, h \in \mathbb{Z}[x]$. Ma α deve essere una radice di g o di h, ed entrambi hanno grado minore di f, che è in contraddizione con le ipotesi del teorema. □

Corollario 2.1.4. *Gli unici interi algebrici in $\mathbb{Q}$ sono gli elementi di $\mathbb{Z}$.*

Dimostrazione. Se $\alpha \in \mathbb{Q}$, il suo polinomio minimo su $\mathbb{Q}$ è di grado 1, e se α è un intero algebrico questo polinomio deve essere a coefficienti interi, quindi è della forma $x + a$ con $a \in \mathbb{Z}$. Allora $\alpha = -a$. □

Diamo alcune caratterizzazioni alternative della nozione di intero algebrico.

Teorema 2.1.5. *Sia $\alpha \in \mathbb{C}$. Sono allora equivalenti:*

1. *α è un intero algebrico;*
2. *lo $\mathbb{Z}$-modulo $\mathbb{Z}[\alpha]$ è finitamente generato;*
3. *α appartiene a un qualche sottoanello di $\mathbb{C}$ che è uno $\mathbb{Z}$-modulo finitamente generato;*

4. $\alpha A \subseteq A$ per un qualche $\mathbb{Z}$-modulo A finitamente generato.

Dimostrazione. [1 $\Rightarrow$ 2] Se α è radice di un polinomio monico a coefficienti in $\mathbb{Z}$ di grado n allora $1, \alpha, \ldots, \alpha^{n-1}$ è un insieme di generatori di $\mathbb{Z}[\alpha]$ come $\mathbb{Z}$-modulo.

[2 $\Rightarrow$ 3] L'elemento α appartiene a $\mathbb{Z}[\alpha]$ che è uno $\mathbb{Z}$-modulo finitamente generato.

[3 $\Rightarrow$ 4] Sia A il sottoanello di $\mathbb{C}$ che è anche $\mathbb{Z}$-modulo finitamente generato a cui appartiene α. Allora $\alpha A \subseteq A$, cioè $\alpha\beta \in A$ per ogni $\beta \in A$.

[4 $\Rightarrow$ 1] Sia $\{a_1, \ldots, a_n\}$ un insieme di generatori per A. Per ipotesi possiamo esprimere ogni αa_i come combinazione a coefficienti in $\mathbb{Z}$ degli $a_1, \ldots, a_n$. Abbiamo quindi che

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

ove M è una marice $n \times n$ a coefficienti in $\mathbb{Z}$. Equivalentemente vale

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

ove I è la matrice identità. Siccome gli a_i non sono tutti nulli, da questo segue che $\det(\alpha I - M) = 0$. Sviluppando l'espressione del determinante in termini dei coefficienti della matrice $(\alpha I - M)$ otteniamo che α è radice di un polinomio monico a coefficienti interi di grado n. □

Corollario 2.1.6. *Se $\alpha, \beta \in \mathbb{C}$ sono interi algebrici, allora anche $\alpha + \beta$ e $\alpha\beta$ sono interi algebrici.*

Dimostrazione. Per la caratterizzazione 2, sappiamo che gli $\mathbb{Z}$-moduli $\mathbb{Z}[\alpha]$ e $\mathbb{Z}[\beta]$ sono finitamente generati. Se $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_n\}$ sono insiemi di generatori, rispettivamente, per $\mathbb{Z}[\alpha]$ e $\mathbb{Z}[\beta]$, allora $\mathbb{Z}[\alpha, \beta]$ è generato da $\{\, \alpha_i\beta_j \mid i = 1, \ldots, m, j = 1, \ldots, n \,\}$, che è un insieme finito. Siccome $\alpha + \beta$ e $\alpha\beta$ appartengono a $\mathbb{Z}[\alpha, \beta]$, per la caratterizzazione 3, sono interi algebrici. □

Il risultato precedente mostra che l'insieme degli interi algebrici è un anello, che denoteremo $\mathbb{A}$. In particolare, se K è un campo di numeri, $\mathbb{A} \cap K$ è un sottoanello di K, che chiameremo anello degli interi algebrici di K. Abbiamo già visto che $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$, e nel capitolo successivo vedremo la forma che assume questo anello per alcuni casi particolari di K.

2.2 La norma e la traccia

In questo paragrafo supporremo che $K \subseteq L$ siano campi di numeri, e che $n = [L : K]$.

Definizione 2.2.1. Siano $\sigma_1, \dots, \sigma_n$ le n immersioni di L in $\mathbb{C}$ che fissano K. Preso $\alpha \in L$ definiamo la *traccia relativa* e la *norma relativa* di α come segue:

$$\mathrm{T}_K^L(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$
$$\mathrm{N}_K^L(\alpha) := \sigma_1(\alpha) \dots \sigma_n(\alpha)$$

Se $K = \mathbb{Q}$ scriveremo T^L e N^L al posto di $\mathrm{T}_{\mathbb{Q}}^L$ e $\mathrm{N}_{\mathbb{Q}}^L$, e in tal caso parleremo semplicemente di norma e traccia.

Proposizione 2.2.2. *Nelle notazioni della definizione precedente per ogni $\alpha, \beta \in L, \delta \in K$ valgono*

$$\mathrm{T}_K^L(\alpha+\beta) = T_K^L(\alpha) + T_K^L(\beta), \quad \mathrm{T}_K^L(\delta) = n\delta, \quad \mathrm{T}_K^L(\delta\alpha) = \delta T_K^L(\alpha);$$
$$\mathrm{N}_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta), \quad \mathrm{N}_K^L(\delta) = \delta^n, \quad \mathrm{N}_K^L(\delta\alpha) = \delta^n N_K^L(\alpha).$$

La dimostrazione della proposizione precedente è una facile verifica.

Teorema 2.2.3. *Siano $\alpha \in L$ e d il grado di α su K. Siano $t(\alpha)$ e $n(\alpha)$ rispettivamente la somma e il prodotto dei d coniugati di α su K. Allora*

$$\mathrm{T}_K^L(\alpha) = \frac{n}{d} t(\alpha),$$
$$\mathrm{N}_K^L(\alpha) = \big(n(\alpha)\big)^{\frac{n}{d}}.$$

Dimostrazione. Vale $t(\alpha) = \mathrm{T}_K^{K[\alpha]}(\alpha)$ e $n(\alpha) = \mathrm{N}_K^{K[\alpha]}(\alpha)$. Inoltre, poiché

$$\frac{n}{d} = \big[L : K[\alpha]\big]$$

ogni immersione di $K[\alpha]$ in $\mathbb{C}$ si estende a $\frac{n}{d}$ immersioni di L. Le due formule nell'enunciato seguono da questi due fatti. □

Corollario 2.2.4. *Sia $\alpha \in L$. Vale che $\mathrm{T}_K^L(\alpha), \mathrm{N}_K^L(\alpha) \in K$ e, se $\alpha \in \mathbb{A} \cap L$, $\mathrm{T}_K^L(\alpha), \mathrm{N}_K^L(\alpha) \in \mathbb{A} \cap K$. In particolare, se $K = \mathbb{Q}$, allora $\mathrm{T}^L(\alpha), \mathrm{N}^L(\alpha) \in \mathbb{Z}$.*

Dimostrazione. Per il teorema precedente, è sufficiente mostrare che

$$t(\alpha), n(\alpha) \in K.$$

Ma, se $f(x) = a_0 + \cdots + a_{d-1}x^{d-1} + x^d$ è il polinomio minimo di α su K, abbiamo che $a_{d-1} = -t(\alpha)$ e $a_0 = (-1)^d n(\alpha)$. □

Proposizione 2.2.5. *Sia $\alpha \in L$, e sia $\phi_\alpha \colon L \to L$ l'applicazione K-lineare che a $\beta \in L$ associa $\alpha\beta$. Se A è la sua matrice rispetto a una base di L come K-spazio vettoriale, allora $\mathrm{T}_K^L(\alpha) = \mathrm{tr}(A)$ e $\mathrm{N}_K^L(\alpha) = \det(A)$.*

Dimostrazione. La traccia e il determinante della matrice A non cambiano a seconda della base scelta per L. Supponiamo che il polinomio minimo di α su K sia $f(x) = a_0 + \cdots + a_{d-1}x^{d-1} + x^d$. Allora $\big[K[\alpha] : K\big] = d$ e $\{1, \alpha, \ldots, \alpha^{d-1}\}$ è una base di $K[\alpha]$ su K. Sia poi $\{\beta_1, \ldots, \beta_{\frac{n}{d}}\}$ una base di L su $K[\alpha]$. Allora

$$\{\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{d-1}, \beta_2, \beta_2\alpha, \ldots, \beta_2\alpha^{d-1}, \ldots, \beta_{\frac{n}{d}}, \beta_{\frac{n}{d}}\alpha, \ldots, \beta_{\frac{n}{d}}\alpha^{d-1}, \}$$

è una base di L su K e rispetto a questa base ϕ_α ha matrice

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

che è diagonale a blocchi, con $\frac{n}{d}$ blocchi $d \times d$ ciascuno dei quali uguale a

$$J = \begin{pmatrix} 0 & \dots\dots\dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Siccome $\mathrm{tr}(J) = -a_{d-1}$ e $\det(J) = (-1)^d a_0$ abbiamo che

$$\mathrm{tr}(A) = \frac{n}{d}\,\mathrm{tr}(J) = \frac{n}{d} t(\alpha) = \mathrm{T}_K^L(\alpha),$$
$$\det(A) = \big(\det(J)\big)^{\frac{n}{d}} = \big(n(\alpha)\big)^{\frac{n}{d}} = \mathrm{N}_K^L(\alpha).$$

□

2.3 Il discriminante

La nozione di discriminante sarà centrale nello studio dell'anello degli interi algebrici in un campo.

Anche in questo paragrafo supporremo che $K \subseteq L$ siano campi di numeri, e che $[L : K] = n$.

Definizione 2.3.1. Siano $\sigma_1, \dots, \sigma_n$ le immersioni di L in $\mathbb{C}$ che fissano K, e siano $\alpha_1, \dots, \alpha_n \in L$. Sia $D := \big(\sigma_i(\alpha_j)\big)_{i,j=1,\dots,n}$ matrice $n \times n$. Definiamo il *discriminante relativo* della n-pla $(\alpha_1, \dots, \alpha_n)$ come

$$\mathrm{disc}_K^L(\alpha_1, \dots, \alpha_n) := \big(\det(D)\big)^2.$$

Anche in questo caso, se $K = \mathbb{Q}$ indicheremo disc_K^L semplicemente con disc, e parleremo di discriminante.

Teorema 2.3.2. *Nelle notazioni della definizione precedente, se*

$$T := \big(\mathrm{T}_N^K(\alpha_i \alpha_j)\big)_{i,j=1,\dots,n}$$

allora

$$\mathrm{disc}_K^L(\alpha_1, \dots, \alpha_n) = \det(T).$$

Dimostrazione. Osserviamo che, poiché i σ_k sono omomorfismi di campi, il coefficiente di posto i, j della matrice $D^T D$ è

$$\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)$$

che è proprio il coefficiente di posto i, j della matrice T. A questo punto la tesi segue dal teorema di Binet e dal fatto che $\det(D^T) = \det(D)$. □

Corollario 2.3.3. *Nelle notazioni precedenti abbiamo che*

$$\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in K,$$

e, se $\alpha_1 \ldots, \alpha_n \in \mathbb{A} \cap L$*,*

$$\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in \mathbb{A} \cap K.$$

Dimostrazione. Questi due fatti seguono dalle proprietà della traccia dimostrate nel Corollario 2.2.4. □

Teorema 2.3.4. *Nelle notazioni precedenti,* $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = 0$ *se e solo se* $\alpha_1, \ldots, \alpha_n$ *sono linearmente dipendenti su* K*.*

Dimostrazione. Se $\alpha_1, \ldots, \alpha_n$ sono linearmente dipendenti, allora esistono $a_1, \ldots, a_n \in K$, non tutti nulli, tali che $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$, da cui, per ogni $i = 1, \ldots, n$

$$a_1\sigma_i(\alpha_1) + \cdots + a_n\sigma_i(\alpha_n) = 0.$$

Ma allora

$$a_1 \begin{pmatrix} \sigma_1(\alpha_1) \\ \vdots \\ \sigma_n(\alpha_1) \end{pmatrix} + \cdots + a_n \begin{pmatrix} \sigma_1(\alpha_n) \\ \vdots \\ \sigma_n(\alpha_n) \end{pmatrix} = \mathbf{0}$$

ossia le colonne della matrice D sono linearmente dipendenti, per cui

$$\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = 0.$$

Viceversa, se $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = 0$, allora le righe della matrice T sono linearmente dipendenti; denotiamole, per ogni $i = 1, \ldots, n$

$$R_i = \begin{pmatrix} \mathrm{T}_N^K(\alpha_i\alpha_1) \\ \vdots \\ \mathrm{T}_N^K(\alpha_i\alpha_n) \end{pmatrix}.$$

Allora esistono $a_1, \ldots, a_n \in K$, non tutti nulli, tali che $a_1R_1 + \cdots + a_nR_n = \mathbf{0}$, ossia, per ogni $j = 1, \ldots, n$

$$a_1 \mathrm{T}_N^K(\alpha_1\alpha_j) + \cdots + a_n \mathrm{T}_N^K(\alpha_n\alpha_j) = 0. \tag{2.1}$$

Supponiamo ora per assurdo che $\alpha_1, \ldots, \alpha_n$ siano linearmente indipendenti su K e consideriamo $\alpha := a_1\alpha_1 + \cdots + a_n\alpha_n$. Allora $\alpha \neq 0$, poiché gli $a_1, \ldots, a_n$ non sono tutti nulli. Da (2.1) segue che $\mathrm{T}_N^K(\alpha\alpha_j) = 0$ per ogni $j = 1, \ldots, n$. Ora, avendo supposto che $\alpha_1, \ldots, \alpha_n$ sono linearmente indipendenti, essi formano una base, e poiché $\alpha \neq 0$, anche $\{\alpha\alpha_1, \ldots, \alpha\alpha_n\}$ è una base. Quindi, preso $\beta \in L$ esistono $b_1, \ldots, b_n \in K$ tali che $\beta = b_1\alpha\alpha_1 + \cdots + b_n\alpha\alpha_n$ e quindi

$$\mathrm{T}_N^K(\beta) = b_1 \mathrm{T}_N^K(\alpha\alpha_1) + \cdots + b_n \mathrm{T}_N^K(\alpha\alpha_n) = 0$$

ma questo è assurdo, perché ad esempio $\mathrm{T}_N^K(1) = n$. □

Dimostreremo ora un risultato che caratterizza il discriminante nel caso di un'estensione semplice. A questo premettiamo due lemmi.

Lemma 2.3.5. *Sia A un anello commutativo con unità e siano $a_1, \ldots, a_n \in A$. Se $V = \left(a_i^{j-1}\right)_{i,j=1,\ldots,n}$ allora*

$$\det(V) = \prod_{1 \leq r < s \leq n} (a_s - a_r).$$

Dimostrazione. La prova è per induzione su n. Se $n = 2$ abbiamo che

$$V = \begin{pmatrix} 1 & a_1 \\ 1 & a_2 \end{pmatrix}$$

e $\det(V) = (a_2 - a_1)$.

Supponiamo ora che la tesi sia vera per n e mostriamola per $n+1$. Consideriamo quindi

$$V = \begin{pmatrix} 1 & \dots & a_1^n \\ \dots & \dots & \dots \\ 1 & \dots & a_{n+1}^n \end{pmatrix}.$$

Poiché sommando a una colonna combinazioni lineari delle altre colonne il determinante non cambia, abbiamo che, per qualunque polinomio monico $f \in A[x]$ di grado n

$$\det(V) = \det \begin{pmatrix} 1 & \dots & a_1^{n-1} & f(a_1) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 1 & \dots & a_{n+1}^{n-1} & f(a_{n+1}) \end{pmatrix}.$$

Scegliamo allora $f(x) = \prod_{i=1}^{n}(x - a_i)$ per cui abbiamo

$$\det(V) = \det \begin{pmatrix} 1 & \dots & a_1^{n-1} & 0 \\ \dots & \dots & \dots & \dots \\ 1 & \dots & a_n^{n-1} & 0 \\ 1 & \dots & a_{n+1}^{n-1} & f(a_{n+1}) \end{pmatrix} = \prod_{i=1}^{n}(a_{n+1} - a_i) \det \begin{pmatrix} 1 & \dots & a_1^{n-1} \\ \dots & \dots & \dots \\ 1 & \dots & a_n^{n-1} \end{pmatrix}$$

e quindi, per ipotesi induttiva,

$$\det(V) = \prod_{i=1}^{n}(a_{n+1} - a_i) \prod_{1 \le r < s \le n} (a_s - a_r) = \prod_{1 \le r < s \le n+1} (a_s - a_r). \qquad \square$$

Lemma 2.3.6. *Sia $f \in K[x]$ un polinomio monico irriducibile, e sia $\alpha \in \mathbb{C}$ una sua radice. Allora*

$$f'(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta)$$

ove il prodotto è esteso a tutte le radici di f diverse da α.

Dimostrazione. Abbiamo che

$$f(x) = (x - \alpha)g(x), \tag{2.2}$$

con g un polinomio monico a coefficienti nel campo di spezzamento di f, $g(x) = \prod_{\beta \neq \alpha}(x - \beta)$. Derivando (2.2) otteniamo

$$f'(x) = g(x) + (x - \alpha)g'(x)$$

da cui, calcolando in α, si ottiene la tesi. □

Teorema 2.3.7. *Sia $\alpha \in L$ e supponiamo che $L = K[\alpha]$. Siano poi $\alpha_1, \ldots, \alpha_n$ i coniugati di α su K e sia f il polinomio minimo di α su K. Abbiamo allora che*

$$\operatorname{disc}_L^K(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_s - \alpha_r)^2 = (-1)^{\frac{n(n-1)}{2}} \operatorname{N}_K^{K[\alpha]}\big(f'(\alpha)\big).$$

Dimostrazione. Ordiniamo i σ_i in modo che $\sigma_i(\alpha) = \alpha_i$. La prima uguaglianza segue dal fatto che in questo caso il coefficiente di posto i, j della matrice D è

$$\sigma_i(\alpha^{j-1}) = \big(\sigma_i(\alpha)\big)^{j-1} = \alpha_i^{j-1}.$$

Allora, per il Lemma 2.3.5, abbiamo che

$$\det(D) = \prod_{1 \leq r < s \leq n} (\alpha_s - \alpha_r).$$

Per quanto riguarda la seconda uguaglianza, osserviamo anzitutto che la produttoria ha $\frac{n^2-n}{2}$ fattori e che per ciascuno di essi vale $(\alpha_s - \alpha_r)^2 = -(\alpha_r - \alpha_s)(\alpha_s - \alpha_r)$, per cui abbiamo

$$\prod_{1 \leq r < s \leq n} (\alpha_s - \alpha_r)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{\substack{1 \leq r,s \leq n \\ r \neq s}} (\alpha_r - \alpha_s).$$

Ora, poiché f ha coefficienti in K abbiamo che

$$\operatorname{N}_K^{K[\alpha]}\big(f'(\alpha)\big) = \prod_{r=1}^{n} \sigma_r\big(f'(\alpha)\big) = \prod_{r=1}^{n} f'\big(\sigma_r(\alpha)\big) = \prod_{r=1}^{n} f'(\alpha_r).$$

Per il Lemma 2.3.6 abbiamo che, per ogni $r = 1, \ldots, n$,

$$f'(\alpha_r) = \prod_{\substack{1 \leq s \leq n \\ s \neq r}} (\alpha_r - \alpha_s).$$

Mettendo assieme tutti questi fatti otteniamo la seconda uguaglianza. □

Alla luce del teorema precedente, indicheremo con $\mathrm{disc}(\alpha)$ il discriminante $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$ ogni volta che $\alpha \in \mathbb{C}$ è algebrico di grado n su $\mathbb{Q}$.

2.4 L'anello degli interi algebrici di un campo di numeri come $\mathbb{Z}$-modulo

Iniziamo ora a trattare in maniera più particolare dell'anello degli interi algebrici di un campo di numeri. In questo paragrafo, se non altrimenti specificato, denoteremo con K un campo di numeri di grado n su $\mathbb{Q}$ e con $R = \mathbb{A} \cap K$ l'anello degli interi algebrici in esso contenuti. Il risultato principale di questo paragrafo è che R è uno $\mathbb{Z}$-modulo libero di rango n.

Proposizione 2.4.1. *Esistono basi di K i cui elementi sono tutti interi algebrici.*

Dimostrazione. Sia $\alpha \in K$, sia f il polinomio minimo di α su $\mathbb{Q}$, sia m il minimo intero tale che mf sia a coefficienti interi e sia $g = mf$; scriviamo

$$g(x) = a_d x^d + \sum_{i=1}^{d} a_{d-i} x^{d-i}.$$

Consideriamo ora il polinomio

$$h(x) = x^d + \sum_{i=1}^{d} a_{d-i} a_d^{i-1} x^{d-i}$$

e osserviamo che

$$h(a_d \alpha) = a_d^d \alpha^d + \sum_{i=1}^{d} a_{d-i} a_d^{d-1} x^{d-i} = a_d^{d-1} f(\alpha) = 0.$$

Dunque $a_d\alpha$ è un intero algebrico. Abbiamo quindi mostrato che possiamo ottenere un intero algebrico da ogni elemento di K moltiplicandolo per un intero opportuno. Sia dunque $\{\alpha_1, \ldots, \alpha_n\}$ una base di K, e siano $c_1, \ldots, c_n \in \mathbb{Z}$ con la proprietà che $c_i\alpha_i$ è un intero algebrico per ogni $i = 1 \ldots, n$. Allora, poiché il prodotto di un intero per un intero algebrico è ancora un intero

algebrico, se c è il minimo comune multiplo dei c_i, $\{c\alpha_1, \ldots, c\alpha_n\}$ è una base di K costituita da interi algebrici. □

Proposizione 2.4.2. *L'anello R contiene uno $\mathbb{Z}$-modulo libero di rango n.*

Dimostrazione. Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di interi algebrici per K, e sia

$$A = \mathrm{Span}_{\mathbb{Z}}(\{\alpha_1, \ldots, \alpha_n\}) = \{\, m_1\alpha_1 + \cdots + m_n\alpha_n \mid m_1, \ldots, m_n \in \mathbb{Z} \,\}$$

lo $\mathbb{Z}$-modulo generato da $\{\alpha_1, \ldots, \alpha_n\}$. Poiché gli α_i sono linearmente indipendenti su $\mathbb{Q}$ lo sono anche su $\mathbb{Z}$. Allora A è uno $\mathbb{Z}$-modulo libero di rango n e in particolare $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. □

Teorema 2.4.3. *Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di K su $\mathbb{Q}$ i cui elementi sono tutti interi algebrici, e sia $d = \mathrm{disc}(\alpha_1 \ldots, \alpha_n)$. Allora ogni elemento $\alpha \in R$ è della forma*

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

con $m_j \in \mathbb{Z}$ e $d \mid m_j^2$ per ogni $j = 1, \ldots, n$.

Dimostrazione. Notiamo che, poiché gli α_j sono linearmente indipendenti, $d \neq 0$, e poiché sono interi algebrici, $d \in \mathbb{Z}$. Sia $\alpha \in R$ e siano $x_1, \ldots, x_n \in \mathbb{Q}$ tali che

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n. \tag{2.3}$$

Siano poi $\sigma_1, \ldots, \sigma_n$ le immersioni di K in $\mathbb{C}$. Applicando ogni σ_i all'equazione (2.3) otteniamo il sistema

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n) \quad \text{per } i = 1, \ldots, n.$$

Se $D = \big(\sigma_i(\alpha_j)\big)_{i,j=1,\ldots,n}$ e G_j è ottenuta da D sostituendo

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} \qquad \text{alla } j\text{-esima colonna di } D \qquad \begin{pmatrix} \sigma_1(\alpha_j) \\ \vdots \\ \sigma_n(\alpha_j) \end{pmatrix}$$

e $\delta = \det(D), \gamma_j = \det(G_j)$ abbiamo, per la regola di Cramer, che $x_j = \frac{\gamma_j}{\delta}$ per ogni $j = 1, \ldots, n$. Siccome i coniugati di interi algebrici sono ancora

interi algebrici, e δ e γ_j sono quindi ottenuti mediante somme e prodotti da interi algebrici, segue che sono anche essi interi algebrici. In effetti abbiamo che $\delta^2 = d$ e quindi $dx_j = \delta\gamma_j$. Dunque $dx_j \in \mathbb{Q}$ è un intero algebrico, per cui $dx_j \in \mathbb{Z}$, e poniamo $m_j := dx_j$. Resta da mostrare che $\frac{m_j^2}{d} \in \mathbb{Z}$; essendo questo razionale è sufficiente mostrare che è un intero algebrico. In effetti

$$\frac{m_j^2}{d} = \frac{(dx_j)^2}{d} = \frac{(\delta\gamma_j)^2}{d} = \frac{\delta^2\gamma_j^2}{d} = \gamma_j^2$$

che è un intero algebrico. □

Osservazione 2.4.4. Il teorema precedente mostra che R è contenuto nello $\mathbb{Z}$-modulo libero di rango n

$$\mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}.$$

Abbiamo quindi il seguente

Corollario 2.4.5. *L'anello R è uno $\mathbb{Z}$-modulo libero di rango n.*

Dimostrazione. Questo risultato segue immediatamente dal Corollario 1.1.20, tenuto conto della Proposizione 2.4.2 e dell'osservazione precedente. □

Poiché R è uno $\mathbb{Z}$-modulo libero di rango n esso ha una base su $\mathbb{Z}$.

Definizione 2.4.6. Una base di R su $\mathbb{Z}$ è detta *base integrale*.

Proposizione 2.4.7. *Una base integrale di R su $\mathbb{Z}$ è anche una base di K su $\mathbb{Q}$.*

Dimostrazione. Sia $B = \{\beta_1, \ldots, \beta_n\}$ una base integrale per R. Essa ha n elementi poiché R è uno $\mathbb{Z}$-modulo libero di rango n. Inoltre essa genera R su $\mathbb{Z}$, e quindi anche su $\mathbb{Q}$. Poiché sappiamo che esistono sottoinsiemi di R che generano K su $\mathbb{Q}$, abbiamo che B genera K su $\mathbb{Q}$. Questo mostra che B è una base di K su $\mathbb{Q}$ poiché K è un $\mathbb{Q}$-spazio vettoriale di dimensione n. □

Teorema 2.4.8. *Siano $\{\beta_1, \ldots, \beta_n\}$ e $\{\gamma_1, \ldots, \gamma_n\}$ due basi integrali per R. Allora* $\mathrm{disc}(\beta_1, \ldots, \beta_n) = \mathrm{disc}(\gamma_1, \ldots, \gamma_n)$.

Dimostrazione. Poniamo nel seguito

$$d_1 = \operatorname{disc}(\beta_1, \dots, \beta_n) \quad \text{e} \quad d_2 = \operatorname{disc}(\gamma_1, \dots, \gamma_n).$$

Poiché $\{\gamma_1, \dots, \gamma_n\}$ è una base integrale di R, possiamo esprimere i β_i come combinazioni a coefficienti interi dei γ_i, per cui abbiamo che

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \tag{2.4}$$

con M matrice $n \times n$ a coefficienti in $\mathbb{Z}$. Se $\sigma_1, \dots, \sigma_n$ sono le immersioni di K in $\mathbb{C}$, applicando ogni σ_j alle n equazioni del sistema (2.4) otteniamo l'equazione matriciale

$$D_1 = MD_2$$

con $D_1 = \big(\sigma_j(\beta_i)\big)_{i,j=1,\dots,n}$ e $D_2 = \big(\sigma_j(\gamma_i)\big)_{i,j=1,\dots,n}$. Calcolando il determinante ed elevando al quadrato otteniamo

$$d_1 = \big(\det(M)\big)^2 d_2.$$

A questo punto osserviamo che sia d_1 che d_2 sono interi, e che anche $\det(M)$ è intero, per cui abbiamo mostrato che $d_1 \mid d_2$, e hanno entrambi lo stesso segno. Analogamente si mostra che $d_2 \mid d_1$ e questo prova la tesi. □

Dunque abbiamo appena mostrato che il discriminante di una base integrale è un invariante dell'anello R, che denoteremo con $\operatorname{disc}(R)$. Vediamo ora alcune applicazioni del discriminante.

Proposizione 2.4.9. *Siano $\alpha_1, \dots, \alpha_n \in R$. Essi costituiscono una base integrale se e solo se* $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(R)$.

Dimostrazione. Sia $\{\gamma_1, \dots, \gamma_n\}$ una base integrale per R, e siano $b_{ij} \in \mathbb{Z}$ per ogni $i, j = 1, \dots, n$ tali che $\alpha_i = \sum_{j=i}^{n} b_{ij}\gamma_j$ per ogni $i = 1, \dots, n$, ossia, se $B = \big(b_{ij}\big)_{i,j=1,\dots,n}$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = B \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}. \tag{2.5}$$

Mostriamo anzitutto che $\{\alpha_1, \ldots, \alpha_n\}$ è una base integrale se e solo se B è invertibile su $\mathbb{Z}$ (cioè B è invertibile su $\mathbb{Q}$ e l'inversa B^{-1} è ancora a coefficienti in $\mathbb{Z}$).

Se $\{\alpha_1, \ldots, \alpha_n\}$ è una base integrale allora esiste una matrice C $n \times n$ a coefficienti interi tale che

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

e deve essere necessariamente $C = B^{-1}$. Viceversa, se B è invertibile su $\mathbb{Z}$, allora B^{-1} è tale che

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = B^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

e quindi abbiamo che gli α_i generano R su $\mathbb{Z}$. Mostriamo ora che sono anche linearmente indipendenti su $\mathbb{Z}$. Siano $a_1, \ldots, a_n \in \mathbb{Z}$ tali che $\sum_{i=1}^n a_i \alpha_i = 0$. Allora

$$0 = \sum_{i=1}^{n} a_i \sum_{j=i}^{n} b_{ij} \gamma_j = \sum_{j=i}^{n} \Big(\sum_{i=1}^{n} a_i b_{ij} \Big) \gamma_j$$

e poiché i γ_j sono linearmente indipendenti su $\mathbb{Z}$ da questo segue che

$$\sum_{i=1}^{n} a_i b_{ij} = 0 \quad \text{per ogni } j = 1, \ldots, n.$$

Ma questo è un sistema lineare omogeneo negli a_i, e poiché $\det(B) \neq 0$ avendo supposto B invertibile, segue che $a_1 = \cdots = a_n = 0$.

A questo punto, a partrire dall'equazione (2.5), analogamente alla dimostrazione precedente, possiamo dedurre che

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \big(\det(B)\big)^2 \operatorname{disc}(\gamma_1, \ldots, \gamma_n) = \big(\det(B)\big)^2 \operatorname{disc}(R). \quad (2.6)$$

Ricordiamo ora che una matrice a coefficienti interi è invertibile su $\mathbb{Z}$ se e solo se ha determinante ± 1. Dunque, se B è invertibile su $\mathbb{Z}$, $\big(\det(B)\big)^2 = 1$ e da 2.6 segue che $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(R)$. Viceversa, se $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(R)$, da 2.6 segue che $\big(\det(B)\big)^2 = 1$ e quindi $\det(B) = \pm 1$. □

Proposizione 2.4.10. *Siano* $\alpha_1, \ldots, \alpha_n \in R$. *Se* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ *è privo di quadrati, cioè non è divisibile per nessun quadrato perfetto tranne* 1, *allora* $\{\alpha_1, \ldots, \alpha_n\}$ *è una base integrale.*

Dimostrazione. Abbiamo che, siccome 0 non è privo di quadrati, gli α_i sono linearmente indipendenti su $\mathbb{Q}$ per il Teorema 2.3.4. Osserviamo che, poiché $\mathbb{Z} \subseteq \mathbb{Q}$, questo implica anche che sono linearmente indipendenti su $\mathbb{Z}$. Abbiamo allora che $\{\alpha_1, \ldots, \alpha_n\}$ è una base per K su $\mathbb{Q}$ i cui elementi sono tutti interi algebrici. Dunque possiamo applicare il Teorema 2.4.3 e abbiamo quindi che

$$R \subseteq M := \left\{ \frac{\sum_{i=1}^n m_i \alpha_i}{d} \;\middle|\; m_i \in \mathbb{Z}, d \mid m_i^2 \right\}$$

ove $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Ora, siccome per ipotesi d è privo di quadrati, da $d \mid m_i^2$ segue che $d \mid m_i$, per cui abbiamo che in realtà

$$M = \left\{ \sum_{i=1}^n a_i \alpha_i \;\middle|\; a_i \in \mathbb{Z} \right\}$$

e quindi abbiamo che $\{\alpha_1, \ldots, \alpha_n\}$ genera R su $\mathbb{Z}$. Questo, unitamente all'osservazione fatta all'inizio, mostra che $\{\alpha_1, \ldots, \alpha_n\}$ è una base integrale per R. □

Proposizione 2.4.11. *Siano* $\alpha_1, \ldots, \alpha_n \in R$ *e sia* $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. *Allora* $d \equiv 0$ *oppure* $d \equiv 1 \pmod 4$. *In particolare* $\operatorname{disc}(R) \equiv 0$ *oppure* $\operatorname{disc}(R) \equiv 1 \pmod 4$

Dimostrazione. Osserviamo che, poiché gli α_i sono interi algebrici, effettivamente $d \in \mathbb{Z}$. Siano ora $\sigma_1, \ldots, \sigma_n$ le immersioni di K in $\mathbb{C}$, e sia $D = \big(\sigma_i(\alpha_j)\big)_{i,j=1,\ldots,n}$, per cui $d = \big(\det(D)\big)^2$. Se denotiamo con S_n il gruppo delle permutazioni su $\{1, \ldots, n\}$ e con A_n il sottogruppo delle permutazioni pari, e poniamo

$$P := \sum_{\tau \in A_n} \prod_{i=1}^n \sigma_{\tau i}(\alpha_i) \qquad N := \sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^n \sigma_{\tau i}(\alpha_i)$$

abbiamo che $d = (P-N)^2 = (P+N)^2 - 4PN$, per cui è sufficiente mostrare che $P+N$ e PN sono interi, essendo 0 e 1 gli unici residui quadratici modulo

4. Essi sono interi algebrici in quanto ottenuti mediante somme e prodotti da interi algebrici. Resta da mostrare che $P+N, PN \in \mathbb{Q}$. Consideriamo quindi un'estensione normale $\mathbb{Q} \subseteq L$; estendiamo ogni σ_i a un automorfismo, che denoteremo ancora σ_i, di L. Sia poi ϕ un automorfismo di L. Allora $\phi \circ \sigma_i$ è ancora un automorfismo di L, che ristretto a K coincide con uno dei σ_j. In altre parole, per ogni $i = 1, \dots, n$ esiste $j \in \{1, \dots, n\}$ tale che

$$(\phi \circ \sigma_i)|_K = \sigma_j.$$

Inoltre, se $\phi \circ \sigma_i = \phi \circ \sigma_j$, applicando ϕ^{-1} segue che $\sigma_i = \sigma_j$. Dunque ϕ agisce sull'insieme $\{\sigma_1, \dots, \sigma_n\}$ permutando gli indici; sia τ_ϕ tale permutazione. Abbiamo allora che

$$\phi(P+N) = \phi\Big(\sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma_{\tau i}(\alpha_i)\Big) = \sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma_{\tau_\phi \tau i}(\alpha_i) = \sum_{\tau \in S_n} \prod_{i=1}^{n} \sigma_{\tau i}(\alpha_i) = P+N.$$

Il fatto che $\phi(PN) = PN$ segue da un calcolo analogo. Bisogna però osservare che, se τ_ϕ è pari la sua composizione con permutazioni pari è ancora pari, mentre la sua composizione con permutazioni dispari è dispari; invece, se τ_ϕ è dispari, la sua composizione con permutazioni pari è dispari, mentre la sua composizione con permutazioni dispari è pari.

Avendo mostrato che ogni automorfismo di L fissa $P+N$ e PN, segue che essi appartengno a $\mathbb{Q}$. □

Passiamo ora ad esaminare il caso del composto di due campi.

Proposizione 2.4.12. *Siano K ed L due campi di numeri, KL il loro composto, e R, S, T gli anelli di interi algebrici contenuti, rispettivamente, in K, L, KL. Allora T contiene l'anello*

$$RS := \left\{ \alpha_1\beta_1 + \cdots + \alpha_s\beta_s \;\middle|\; \alpha_1, \dots, \alpha_s \in R, \beta_1, \dots, \beta_s \in S, s \in \mathbb{Z}^+ \right\}.$$

Dimostrazione. Abbiamo visto, nel paragrafo 3 del capitolo 1, che vale

$$KL = \left\{ k_1l_1 + \cdots + k_sl_s \mid k_1, \dots, k_s \in K, l_1, \dots, l_s \in L, s \in \mathbb{Z}^+ \right\}.$$

Dunque la tesi segue dal fatto che ogni intero algebrico di K e di L è anche un intero algebrico di KL, e che T è chiuso rispetto a somme e prodotti. □

Teorema 2.4.13. *Nelle notazioni precedenti, supponiamo che* $[K:\mathbb{Q}] = m$, $[L:\mathbb{Q}] = n$, *e* $[KL:\mathbb{Q}] = mn$; *denotiamo con* d *il massimo comun divisore di* $\mathrm{disc}(R)$ *e* $\mathrm{disc}(S)$. *Allora* T *è contenuto in*

$$\frac{1}{d}RS := \left\{ \frac{\sum_{i=1}^{s} \alpha_i\beta_i}{d} \;\middle|\; \alpha_1,\dots,\alpha_s \in R, \beta_1,\dots,\beta_s \in S, s \in \mathbb{Z}^+ \right\}.$$

Dimostrazione. Siano $\{\alpha_1 \dots, \alpha_m\}$ una base integrale per R e $\{\beta_1,\dots,\beta_n\}$ una base integrale per S. Allora $B := \{\, \alpha_i\beta_j \mid i = 1,\dots,m, j = 1,\dots,n \,\}$ è una base per RS su $\mathbb{Z}$. Infatti, se $\gamma \in RS$, esistono $r_1,\dots,r_t \in R$ e $s_1,\dots,s_t \in S$ tali che

$$\gamma = \sum_{k=1}^{t} r_k s_k.$$

Ma allora, per ogni $k = 1,\dots,t$ esistono $a_{1k},\dots,a_{mk}, b_{1k},\dots,b_{nk} \in \mathbb{Z}$ tali che

$$r_k = \sum_{i=1}^{m} a_{ik}\alpha_i \qquad \text{e} \qquad s_k = \sum_{j=1}^{n} b_{jk}\beta_j$$

per cui

$$\gamma = \sum_k r_k s_k = \sum_k \Big(\sum_i a_{ik}\alpha_i\Big)\Big(\sum_j b_{jk}\beta_j\Big) = \sum_{i,j}\Big(\sum_k a_{ik}b_{jk}\Big)\alpha_i\beta_j.$$

Dunque B genera RS su $\mathbb{Z}$. Mostriamo ora che che gli $\alpha_i\beta_j$ sono linearmente indipendenti su $\mathbb{Q}$. Da questo segue che sono anche linearmente indipendenti su $\mathbb{Z}$, e quindi che B è una base su $\mathbb{Z}$ di RS e, poiché B ha mn elementi, anche che B è una base di KL su $\mathbb{Q}$.

Siano quindi $c_{ij} \in \mathbb{Q}$ tali che

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\alpha_i\beta_j = 0. \tag{2.7}$$

Poiché $\{\beta_1,\dots,\beta_n\}$ è una base di L su $\mathbb{Q}$, e

$$[KL:K] = \frac{[KL:\mathbb{Q}]}{[K:\mathbb{Q}]} = n,$$

essa è anche una base di KL su K, per cui, dall'equazione (2.7), segue che, per ogni $j = 1,\dots,n$

$$\sum_{i=1}^{m} c_{ij}\alpha_i = 0.$$

Essendo poi $\{\alpha_1 \dots, \alpha_m\}$ una base di K su $\mathbb{Q}$, abbiamo che $c_{ij} = 0$ per ogni $i = 1, \dots, m$, per ogni $j = 1, \dots, n$.

Dunque, riducendo a denominatore comune tutti i coefficienti razionali, abbiamo che ogni $\alpha \in T \subseteq KL$ si può scrivere come

$$\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{m_{ij}}{r} \alpha_i \beta_j$$

ove $r \in \mathbb{Z}$ e $m_{ij} \in \mathbb{Z}$ per ogni $i = 1, \dots, m$ e per ogni $j = 1, \dots, n$, sono $mn + 1$ interi a due a due coprimi. Alla luce di ciò è sufficiente mostrare che $r \mid d$. Mostriamo che $r \mid \mathrm{disc}(R)$.

Siano $\sigma_1, \dots, \sigma_m$ le immersioni di K in $\mathbb{C}$. Per il Lemma 1.3.3, per ogni $h = 1, \dots, m$, σ_h si estende a un'immersione (che denoteremo ancora σ_h) di KL in $\mathbb{C}$ che ristretta a L coincide con l'identità. Dunque, per ogni $h = 1, \dots, m$ abbiamo

$$\sigma_h(\alpha) = \sum_{i,j} \frac{m_{ij}}{r} \sigma_h(\alpha_i) \beta_j.$$

Ponendo $x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r} \beta_j$ per ogni $i = 1, \dots, m$, otteniamo il sistema

$$\sum_{i=1}^{m} \sigma_h(\alpha_i) x_i = \sigma_h(\alpha) \quad \text{per } h = 1, \dots, m.$$

Se $D = \big(\sigma_h(\alpha_i)\big)_{h,i=1,\dots,m}$ e G_i è ottenuta da D sostituendo

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_m(\alpha) \end{pmatrix} \qquad \text{alla } i\text{-esima colonna di } D \qquad \begin{pmatrix} \sigma_1(\alpha_j) \\ \vdots \\ \sigma_m(\alpha_j) \end{pmatrix}$$

e $\delta = \det(D), \gamma_i = \det(G_i)$ abbiamo, per la regola di Cramer, che $x_i = \frac{\gamma_i}{\delta}$ per ogni $i = 1, \dots, m$. Inoltre δ e i γ_i sono interi algebrici, in quanto ottenuti mediante somme e prodotti da interi algebrici. In effetti $\delta^2 = \mathrm{disc}(R)$. Ponendo $e := \delta^2 = \mathrm{disc}(R)$ abbiamo che $ex_i = \delta\gamma_i$ è un intero algebrico, e

$$ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r} \beta_j \in L.$$

Dunque $ex_i \in S$, e, ricordando che $\{\beta_1, \ldots, \beta_n\}$ è una base integrale per S, deve essere che, per ogni $i = 1, \ldots, m$ e per ogni $j = 1, \ldots, n$, $\frac{em_{ij}}{r} \in \mathbb{Z}$; quindi $r \mid em_{ij}$, da cui, ricordando come sono stati scelti r e gli m_{ij} segue che $r \mid e = \mathrm{disc}(R)$.

Analogamente si prova che $r \mid \mathrm{disc}(S)$ e quindi abbiamo che $r \mid d$, da cui la tesi. □

Corollario 2.4.14. *Nelle notazioni precedenti, se $[K : \mathbb{Q}] = m$, $[L : \mathbb{Q}] = n$, e $[KL : \mathbb{Q}] = mn$, e inoltre $d = 1$, allora $T = RS$.*

Dimostrazione. Questo risultato segue immediatamente dal fatto che il teorema precedente per $d = 1$ ci dice che $T \subseteq RS$, unitamente alla Proposizione 2.4.12. □

Per concludere dimostriamo un teorema, che mostra l'esistenza di una particolare base integrale per l'anello degli interi algebrici contenuti in un campo di numeri. Ad esso premettiamo un lemma.

Lemma 2.4.15. *Sia $\alpha \in \mathbb{C}$ algebrico di grado n su $\mathbb{Q}$ e siano $f, g \in \mathbb{Q}[x]$ di grado minore di n tali che $f(\alpha) = g(\alpha)$. Allora $f = g$.*

Dimostrazione. Per ipotesi $(f - g)(\alpha) = 0$, per cui $f - g$ divide il polinomio minimo di α su $\mathbb{Q}$, che però ha grado n, mentre $f - g$ ha grado minore di n. Dunque deve essere che $f - g = 0$. □

Teorema 2.4.16. *Sia K un campo di numeri di grado n su $\mathbb{Q}$, sia $R = \mathbb{A} \cap K$ l'anello degli interi algebrici in esso contenuti, e sia $\alpha \in R$ di grado n su $\mathbb{Q}$. Allora esiste una base integrale della forma*

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

ove, per ogni $i = 1, \ldots, n-1$, $d_i \in \mathbb{Z}$, $f_i \in \mathbb{Z}[x]$ sono polinomi monici di grado i. Inoltre $d_1 \mid d_2 \mid \cdots \mid d_{n-1}$ e $d_1, d_2, \ldots, d_{n-1}$ sono univocamente determinati.

Dimostrazione. Sia $d = \mathrm{disc}(\alpha)$. Per ogni $k \in \{1, \dots, n\}$, indichiamo con F_k lo $\mathbb{Z}$-modulo libero di rango k generato da $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{k-1}}{d}$, e poniamo $R_k := R \cap F_k$. Abbiamo allora che $R_1 = \mathbb{Z}$. Infatti, $F_1 = \mathbb{Z}\frac{1}{d} \subseteq \mathbb{Q}$, per cui gli unici interi algebrici in F_1 sono gli interi. Inoltre $R_n = R$. Infatti, $1, \alpha, \dots, \alpha^{n-1}$ è una base di K su $\mathbb{Q}$ costituita interamente da interi algebrici, e poiché $d = \mathrm{disc}(\alpha) = \mathrm{disc}(1, \alpha, \dots, \alpha^{n-1})$ per il Teorema 2.4.3 R è contenuto in

$$\mathbb{Z}\frac{1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^{n-1}}{d} =: F_n.$$

Osserviamo che $\alpha R_k \subseteq R_{k+1}$ per ogni $k \leq n-1$, poiché α è per ipotesi un intero algebrico.

La dimostrazione procede ora per induzione su k. Definiremo i d_i e gli f_i e per ogni $k \in \{1, \dots, n\}$ mostreremo che

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

è una base di R_k su $\mathbb{Z}$.

Se $k = 1$ non c'è nulla da dimostrare. Sia ora $k < n$ e supponiamo che $B_k := \{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\}$ sia una base per R_k su $\mathbb{Z}$, con gli f_i e i d_i come nell'enunciato del teorema.

Sia

$$\begin{aligned} \pi \colon \mathbb{Z}\frac{1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^k}{d} &\to \mathbb{Z}\frac{\alpha^k}{d} \\ \frac{m_1}{d} + \cdots + \frac{m_k\alpha^k}{d} &\mapsto \frac{m_k\alpha^k}{d}. \end{aligned}$$

Allora $\pi(R_{k+1})$ è sottomodulo di $\mathbb{Z}\frac{\alpha^k}{d}$, che è un modulo libero di rango 1. Osserviamo che R_{k+1} contiene elementi del tipo $m\frac{\alpha^k}{d}$ con $m \in \mathbb{Z}$, e quindi, essendo $\pi(R_{k+1}) \neq 0$, $\pi(R_{k+1})$ è un modulo libero di rango 1 e pertanto esiste $\beta \in R_{k+1}$ tale che $\pi(\beta) \neq 0$ è una base di $\pi(R_{k+1})$ su $\mathbb{Z}$. In particolare il coefficiente di α^k in β è diverso da 0. Abbiamo allora che $B := \{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}, \beta\}$ è un insieme di elementi di K linearmente indipendenti su $\mathbb{Q}$, altrimenti avremmo che α avrebbe grado $k < n$ su $\mathbb{Q}$ contro l'ipotesi su α. Pertanto B è anche un insieme di elementi di R_{k+1} linearmente

indipendenti su $\mathbb{Z}$. Sia ora $\gamma \in R_{k+1}$; allora $\pi(\gamma) \in \pi(R_{k+1})$ e quindi esiste $m_k \in \mathbb{Z}$ tale che $\pi(\gamma) = m_k\pi(\beta) = \pi(m_k\beta)$. Allora $\gamma - m_k\beta \in R_k$ e pertanto si può esprimere come combinazione a coefficienti in $\mathbb{Z}$ di $1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{k-1}(\alpha)}{d_{k-1}}$. Questo mostra che B è anche un insieme di generatori per R_{k+1}; è dunque una base per R_{k+1} su $\mathbb{Z}$.

Resta da mostrare che β è della forma $\frac{f_k(\alpha)}{d_k}$. Abbiamo che

$$\frac{\alpha^k}{d_{k-1}} = \pi\big(\frac{\alpha f_{k-1}(\alpha)}{d_{k-1}}\big) \in \pi(R_{k+1})$$

poiché $\alpha f_{k-1}(\alpha)$ è un polinomio monico di grado k in α, e $\alpha R_k \subseteq R_{k+1}$. Dunque esiste $m \in \mathbb{Z}$ tale che $\frac{\alpha^k}{d_{k-1}} = m\pi(\beta)$. Ponendo $d_k := md_{k-1}$, abbiamo che $\pi(\beta) = \frac{\alpha^k}{d_k}$, per cui esiste un polinomio monico $f_k \in \mathbb{Q}[x]$ di grado k tale che $\beta = \frac{f_k(\alpha)}{d_k}$. Vogliamo mostrare che f_k è in effetti a coefficienti in $\mathbb{Z}$. Poiché $\frac{f_k(\alpha)}{d_{k-1}} = m\beta \in R_{k+1} \subseteq R$ abbiamo che

$$\frac{f_k(\alpha) - \alpha f_{k-1}(\alpha)}{d_{k-1}} =: \delta \in R$$

e in effetti $\delta \in R_k$ poiché il polinomio in α al numeratore ha grado al più $k-1$. Dunque, poiché B_k è base di R_k su $\mathbb{Z}$, possiamo scrivere $\delta = \frac{g(\alpha)}{d_{k-1}}$ per qualche polinomio $g \in \mathbb{Z}[x]$ di grado al più $k-1$. Dunque abbiamo che $f_k(\alpha) - \alpha f_{k-1}(\alpha) = g(\alpha)$. Per il Lemma 2.4.15 segue che $f_k(x) - xf_{k-1}(x) = g(x)$, e quindi che $f_k \in \mathbb{Z}[x]$.

Per concludere osserviamo che d_k è il minimo intero positivo m tale che $mR_{k+1} \subseteq \mathbb{Z}[\alpha]$, e quindi i d_i sono determinati in maniera univoca. □

Proposizione 2.4.17. *Siano K, R, α e $d_1, \ldots, d_{n-1}$ come nel teorema precedente. Se, per ogni $i = 1, \ldots, n-1$, $g_i \in \mathbb{Z}[x]$ è un polinomio monico di grado i tale che $\frac{g_i(\alpha)}{d_i}$ è un intero algebrico, allora*

$$1, \frac{g_1(\alpha)}{d_1}, \ldots, \frac{g_{n-1}(\alpha)}{d_{n-1}}$$

è una base integrale.

Dimostrazione. Siano f_i come nell'enunciato del teorema precedente, e poniamo $f_0 := 1$, $g_0 := 1$ e $d_0 := 1$. Vogliamo mostrare per induzione che esistono $a_{jk} \in \mathbb{Z}$ tali che

$$\frac{g_k(\alpha)}{d_k} = \frac{f_k(\alpha)}{d_k} + \sum_{j=0}^{k-1} a_{jk} \frac{g_j(\alpha)}{d_j}$$

per ogni $k < n$. Per $k = 1$ la tesi si riduce al fatto che $1 = 1$. Supponiamo ora che la tesi sia vera per $k-1$ e dimostriamola per k. Poiché f_k e g_k sono monici abbiamo che $\frac{g_k(\alpha)}{d_k} - \frac{f_k(\alpha)}{d_k} \in R_k$ per cui, in virtù della dimostrazione del teorema precedente, esistono $a_{jk} \in \mathbb{Z}$ tali che

$$\frac{g_k(\alpha)}{d_k} - \frac{f_k(\alpha)}{d_k} = \sum_{j=0}^{k-1} a_{jk} \frac{g_j(\alpha)}{d_j}.$$

Dunque abbiamo che la matrice M, $n \times n$ a coefficienti interi tale che

$$\begin{pmatrix} 1 \\ \frac{g_1(\alpha)}{d_1} \\ \vdots \\ \frac{g_{n-1}(\alpha)}{d_{n-1}} \end{pmatrix} = M \begin{pmatrix} 1 \\ \frac{f_1(\alpha)}{d_1} \\ \vdots \\ \frac{f_{n-1}(\alpha)}{d_{n-1}} \end{pmatrix}$$

è triangolare inferiore con 1 sulla diagonale, e dunque $\det(M) = 1$. Allora, dalla dimostrazione della Proposizione 2.4.9 segue che anche

$$1, \frac{g_1(\alpha)}{d_1}, \ldots, \frac{g_{n-1}(\alpha)}{d_{n-1}}$$

è una base integrale. □

Capitolo 3

Esempi e Applicazioni

In questo capitolo vedremo alcune applicazioni dei risultati visti finora.

3.1 I campi quadratici

I campi quadratici sono i campi della forma $\mathbb{Q}[\sqrt{m}]$ con $m \in \mathbb{Z}$ privo di quadrati. Questo non è restrittivo, poiché $a\sqrt{m} = \sqrt{a^2 m}$ e $\mathbb{Q}[a\sqrt{m}] = \mathbb{Q}[\sqrt{m}]$ per ogni $a \in \mathbb{Z}$.

Proposizione 3.1.1. *Ogni campo di numeri K di grado 2 su $\mathbb{Q}$ è un campo quadratico.*

Dimostrazione. Per il teorema dell'elemento primitivo, esiste $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$, e poiché $[K : \mathbb{Q}] = 2$, il polinomio minimo di α è della forma $f(x) = x^2 + ax + b$. Allora

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{oppure} \quad \alpha = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

In ogni caso, siccome $a^2 - 4b \in \mathbb{Q}$ esiste $k \in \mathbb{Z}$ tale che $m := k(a^2 - 4b) \in \mathbb{Z}$, e abbiamo che $\alpha \in \mathbb{Q}[\sqrt{m}]$ e $\sqrt{m} \in \mathbb{Q}[\alpha]$ da cui $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$. Notiamo che non è detto che m sia privo di quadrati, ma questo non è restrittivo. □

Proposizione 3.1.2. *Siano $m, n \in \mathbb{Z}$ due interi distinti e privi di quadrati. Allora $\mathbb{Q}[\sqrt{m}] \neq \mathbb{Q}[\sqrt{n}]$.*

Dimostrazione. Supponiamo per assurdo che esista un isomorfismo

$$\phi\colon \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$$
$$\sqrt{m} \mapsto a + b\sqrt{n}$$

per qualche $a, b \in \mathbb{Q}$. Allora avremmo che

$$m = \phi(m) = \left(\phi(\sqrt{m})\right)^2 = (a + b\sqrt{n})^2 = a^2 + 2ab\sqrt{n} + b^2 n$$

da cui $a = 0$ oppure $b = 0$. Ma nel primo caso avremmo che $\sqrt{\frac{m}{n}} = b \in \mathbb{Q}$, il che è assurdo, perché m e n sono privi di quadrati, mentre nel secondo caso avremmo $\sqrt{m} = a \in \mathbb{Q}$, che è assurdo perché m è privo di quadrati. □

Teorema 3.1.3. *Sia $m \in \mathbb{Z}$ privo di quadrati. Allora*

$$\mathbb{A} \cap \mathbb{Q}[\sqrt{m}] = \begin{cases} \{\, a + b\sqrt{m} \mid a, b \in \mathbb{Z} \,\} & \text{se } m \equiv 2, 3 \pmod 4 \\ \left\{ \frac{a+b\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} & \text{se } m \equiv 1 \pmod 4 \end{cases}$$

Dimostrazione. Osserviamo che il caso $m \equiv 0 \pmod 4$ è escluso in quanto m è privo di quadrati. Sia quindi $\alpha = r + s\sqrt{m}$ con $r, s \in \mathbb{Q}$. Se $s \neq 0$ allora il polinomio minimo di α è

$$x^2 - 2rx + r^2 - ms^2.$$

Pertanto α è un intero algebrico se e solo se $2r \in \mathbb{Z}$ e $r^2 - ms^2 \in \mathbb{Z}$.

Se $2r$ è dispari, sia $2r = 2k + 1$ con $k \in \mathbb{Z}$, allora

$$r^2 - ms^2 = \frac{4k^2 + 4k + 1 - 4ms^2}{4}$$

ma questo non è intero a meno che $1 - m(2s)^2 \in \mathbb{Z}$ e $1 - m(2s)^2 \equiv 0 \pmod 4$. Siccome m è privo di quadrati, $2s$ deve essere intero; inoltre non può essere pari, per cui $2s = 2l + 1$ con $l \in \mathbb{Z}$ e abbiamo

$$1 - m(2s)^2 = 1 - m(4l^2 + 4l + 1) \equiv 1 - m \equiv 0 \pmod 4$$

ossia $m \equiv 1 \pmod 4$.

Se invece $2r$ è pari, allora $r \in \mathbb{Z}$, per cui $ms^2 \in \mathbb{Z}$ e, siccome m è privo di quadrati, $s^2 \in \mathbb{Z}$ da cui $s \in \mathbb{Z}$. Questo conclude la dimostrazione, poiché quanto mostrato sopra ci dice anche che, se $m \equiv 2, 3 \pmod 4$, allora $2r$ è pari. □

Il teorema precedente ci permette anche di individuare una base integrale per $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ nei due casi: se $m \equiv 2, 3 \pmod 4$ una base integrale è $\{1, \sqrt{m}\}$, mentre se $m \equiv 1 \pmod 4$ una base integrale è $\{1, \frac{1+\sqrt{m}}{2}\}$.

Il primo caso essendo banale, mostriamo che nel secondo caso $\{1, \frac{1+\sqrt{m}}{2}\}$ è effettivamente una base integrale. Osserviamo anzitutto che $\frac{1+\sqrt{m}}{2}$ è un intero algebrico, poiché è radice del polinomio

$$x^2 - x + \frac{1-m}{4}$$

che è a coefficienti interi perchè siamo nel caso $m \equiv 1 \pmod 4$. Essendo 1 e $\frac{1+\sqrt{m}}{2}$ linearmente indipendenti, basta mostrare che generano

$$\left\{ \frac{a+b\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}.$$

Poiché $a \equiv b \pmod 2$, allora esiste $c \in \mathbb{Z}$ tale che $a = b + 2c$. Ma allora

$$\frac{a+b\sqrt{m}}{2} = \frac{2c+b+b\sqrt{m}}{2} = c \cdot 1 + b \cdot \frac{1+\sqrt{m}}{2}.$$

Osserviamo che in entrambi i casi, la base integrale di $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ è del tipo descritto dal Teorema 2.4.16. In particolare nel secondo caso 2 è il minimo intero n tale che $n(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]) \subseteq \mathbb{Z}[\alpha]$.

A questo punto possiamo anche calcolare $\operatorname{disc} \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$.

Proposizione 3.1.4. *Sia $m \in \mathbb{Z}$ privo di quadrati. Allora*

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

Dimostrazione. Vogliamo applicare il Teorema 2.3.2. Indichiamo $\mathrm{T}^{\mathbb{Q}[\sqrt{m}]}$ con T. Osserviamo che le uniche immersioni di $\mathbb{Q}[\sqrt{m}]$ in $\mathbb{C}$ sono l'identità e l'applicazione $\sqrt{m} \mapsto -\sqrt{m}$. Dunque $\mathrm{T}(r + s\sqrt{m}) = 2r$ per $r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$. Quindi, se $m \equiv 2, 3 \pmod 4$, abbiamo che

$$\operatorname{disc}(\sqrt{m}) = \operatorname{disc}(1, \sqrt{m}) = \det \begin{pmatrix} \mathrm{T}(1) & \mathrm{T}(\sqrt{m}) \\ \mathrm{T}(\sqrt{m}) & \mathrm{T}(m) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} = 4m,$$

mentre, se $m \equiv 1 \pmod 4$, abbiamo che

$$\begin{aligned}\operatorname{disc}(\tfrac{1+\sqrt{m}}{2}) = \operatorname{disc}(1, \tfrac{1+\sqrt{m}}{2}) &= \det \begin{pmatrix} \mathrm{T}(1) & \mathrm{T}(\frac{1+\sqrt{m}}{2}) \\ \mathrm{T}(\frac{1+\sqrt{m}}{2}) & \mathrm{T}(\frac{1+m+2\sqrt{m}}{4}) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+m}{2} \end{pmatrix} = 1 + m - 1 = m. \end{aligned}$$

□

3.2 I campi ciclotomici

Sia $m \in \mathbb{Z}^+$. Una radice m-esima dell'unità è una radice complessa del polinomio $x^m - 1$. In questo paragrafo porremo $\omega := e^{\frac{2\pi i}{m}} \in \mathbb{C}$ per $m \in \mathbb{Z}^+$, e specificheremo all'occorrenza m. Un tale ω è in effetti una radice m-esima dell'unità, e come tale anche un intero algebrico. Il campo $\mathbb{Q}[\omega]$ è detto m-esimo campo ciclotomico. Ricordiamo per completezza i principali fatti sui campi ciclotomici. Per quanto non viene dimostrato qui si rimanda a [1, Capitolo 9, Paragrafo 1].

Denotiamo nel seguito con φ la funzione phi di Eulero.

Proposizione 3.2.1. *I coniugati di ω sono gli ω^k per $1 \leq k \leq m$, k coprimo con m. Quindi ω ha $\varphi(m)$ coniugati. In altre parole, il polinomio minimo di ω su $\mathbb{Q}$ ha grado $\varphi(m)$.*

In effetti il polinomio minimo di ω è a coefficienti in $\mathbb{Z}$, ed è detto m-esimo polinomio ciclotomico.

Segue immediatamente dalla proposizione precedente la seguente

Proposizione 3.2.2. *Il campo $\mathbb{Q}[\omega]$ ha grado $\varphi(m)$ su $\mathbb{Q}$.*

Si può dire di più: ricordando che il gruppo moltiplicativo degli interi modulo m, $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ ha ordine $\varphi(m)$, abbiamo

Teorema 3.2.3. *Il gruppo di Galois dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}[\omega]$ è isomorfo a*

$$\left(\mathbb{Z}/m\mathbb{Z}\right)^\times.$$

Per ogni $k \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ il corrispondente automorfismo del gruppo di Galois manda ω in ω^k.

Il teorema precedente ci permette di affermare che, per $m = p$ primo dispari, il p-esimo campo ciclotomico contiene un unico campo quadratico, che corrisponde all'unico sottogruppo di indice 2 in $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$. Vedremo fra poco come si caratterizza questo campo.

Mostriamo ora alcune proprietà di $\mathrm{disc}(\omega)$ che saranno utili per gli ultimi risultati.

Lemma 3.2.4. *Per $m = p^r$, p un numero primo, vale*

$$\prod_{k \in I}(1 - \omega^k) = p$$

ove I è l'insieme di tutti i k, $1 \leq k \leq m$ tali che $p \nmid k$.

Dimostrazione. Sia

$$f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}.$$

Allora tutte le ω^k con $k \in I$, sono radici di f in quanto radici di $x^{p^r} - 1$ ma non di $x^{p^{r-1}} - 1$. In effetti

$$f(x) = \prod_{k \in I}(x - \omega^k)$$

poiché ci sono esattamente $\varphi(p^r) = p^{r-1}(p-1)$ valori di k. La tesi segue da quest'ultima equazione, ponendo $x = 1$. □

Proposizione 3.2.5. *Per $m = p$ primo dispari, abbiamo che*

$$\mathrm{disc}(\omega) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

Dimostrazione. Vogliamo applicare il Teorema 2.3.7. Il polinomio minimo di ω è $f(x) = 1 + x + \cdots + x^{p-1}$. Dall'uguaglianza $x^p - 1 = (x-1)f(x)$, derivando, segue

$$px^{p-1} = f(x) + (x-1)f'(x)$$

da cui

$$f'(\omega) = \frac{p}{\omega(\omega - 1)}.$$

Calcolando la norma abbiamo, per $\mathrm{N} = \mathrm{N}^{\mathbb{Q}[\omega]}$,

$$\mathrm{N}\big(f'(\omega)\big) = \frac{\mathrm{N}(p)}{\mathrm{N}(\omega)\,\mathrm{N}(\omega-1)}.$$

Si vede facilmente che $\mathrm{N}(p) = p^{p-1}$, poiché ci sono $p-1$ immersioni di $\mathbb{Q}[\omega]$ in $\mathbb{C}$. Inoltre $\mathrm{N}(\omega) = 1$, poiché i coniugati di ω si dividono in coppie, ciascuna delle quali ha come prodotto $\omega^p = 1$. Infine il Lemma 3.2.4, per $r = 1$, mostra che $\mathrm{N}(\omega - 1) = p$, e $\mathrm{N}(\omega - 1) = \mathrm{N}(1 - \omega)$ poiché $p - 1$, il numero delle immersioni, è pari. A questo punto la tesi segue applicando il Teorema 2.3.7. □

Più in generale possiamo mostrare la seguente

Proposizione 3.2.6. *Per m qualsiasi,* $\mathrm{disc}(\omega) \mid m^{\varphi(m)}$.

Dimostrazione. Sia f il polinomio minimo di ω su $\mathbb{Q}$, abbiamo che $x^m - 1 = f(x)g(x)$ per qualche $g \in \mathbb{Z}[x]$. Derivando e calcolando in ω otteniamo $m\omega^{m-1} = f'(\omega)g(\omega)$ cioè $m = \omega f'(\omega)g(\omega)$. Per il Teorema 2.3.7, calcolando la norma abbiamo, per $\mathrm{N} = \mathrm{N}^{\mathbb{Q}[\omega]}$,

$$m^{\varphi(m)} = (-1)^{\frac{\varphi(m)(\varphi(m)-1)}{2}}\,\mathrm{disc}(\omega)\,\mathrm{N}\big(\omega g(\omega)\big).$$

A questo punto per concludere osserviamo che $g(\omega) = \prod_i(\omega - \omega_i)$ ove le ω_i sono le radici m-esime dell'unità che non sono primitive, per cui $g(\omega)$ è un intero algebrico, e quindi $\mathrm{N}\big(\omega g(\omega)\big) \in \mathbb{Z}$. □

Proposizione 3.2.7. *Sia $m = p$ un numero primo dispari. Allora*

$$\sqrt{p} \in \mathbb{Q}[\omega] \quad \textit{se } p \equiv 1 \pmod 4$$
$$\sqrt{-p} \in \mathbb{Q}[\omega] \quad \textit{se } p \equiv -1 \pmod 4$$

Dimostrazione. Dalla Proposizione 3.2.5 sappiamo che $\mathrm{disc}(\omega) = \pm p^{p-2}$, e vale il segno + solo se $p \equiv 1 \pmod 4$. A questo punto ricordiamo che $\mathrm{disc}(\omega) = \mathrm{disc}(1, \omega, \ldots, \omega^{p-2})$, e che per definizione

$$\mathrm{disc}(1, \omega, \ldots, \omega^{p-2}) = \big(\det(D)\big)^2$$

ove $D = \big(\sigma_j(\omega^{i-1})\big)_{i,j=1,\dots,p-1}$ e $\sigma_1, \dots, \sigma_{p-1}$ sono gli automorfismi di $\mathbb{Q}[\omega]$. Abbiamo allora che $\mathbb{Q}[\omega]$ contiene $\det(D) = \pm\big(\mathrm{disc}(\omega)\big)^{\frac{1}{2}}$ e quindi abbiamo che , posto $p-2 = 2k+1$ per $k \in \mathbb{Z}$, $\mathbb{Q}[\omega]$ contiene $p^k\sqrt{p}$ se $p \equiv 1 \pmod 4$, e $p^k\sqrt{-p}$ se $p \equiv -1 \pmod 4$, da cui la tesi. □

Osserviamo anche che, se $m = 8$, $\mathbb{Q}[\omega]$ contiene $\sqrt{2}$ poiché vale $\sqrt{2} = 2\omega + 2\omega^7$. Abbiamo quindi il seguente

Teorema 3.2.8. *Sia n un intero privo di quadrati. Allora il campo $\mathbb{Q}[\sqrt{n}]$ è contenuto nel d-esimo campo ciclotomico, ove $d = \mathrm{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{n}])$.*

Dimostrazione. Osserviamo che, in generale, l'r-esimo campo ciclotomico contiene tutti gli s-esimi campi ciclotomici, con $s \mid r$. Sia p un numero primo che divide n. Dalla proposizione precedente, se $p \equiv 1 \pmod 4$, $\sqrt{p}$ è contenuta nel p-esimo campo ciclotomico. Analogamente, se $p \equiv 3 \pmod 4$, $\sqrt{-p}$ è contenuta nel p-esimo campo ciclotomico. Infine, se $p = 2$, $\sqrt{2}$ è contenuta nell'ottavo campo ciclotomico. Distinguiamo ora i tre casi $n \equiv 1$, $n \equiv 3$, e $n \equiv 2 \pmod 4$.

Se $n \equiv 1 \pmod 4$ i primi p che dividono n e tali che $p \equiv 3 \pmod 4$ sono in numero pari, pertanto, se p_1, p_2 sono due di essi, l'n-esimo campo ciclotomico contiene $\sqrt{-p_1}\sqrt{-p_2} = -\sqrt{p_1p_2}$ e quindi l'n-esimo campo ciclotomico contiene $\sqrt{n}$. Ricordando la Proposizione 3.1.4, essendo $d = n$, il teorema è in questo caso dimostrato.

Se $n \equiv 3 \pmod 4$ i primi p che dividono n e tali che $p \equiv 3 \pmod 4$ sono in numero dispari. Allora l'n-esimo campo ciclotomico contiene $\sqrt{-n}$ per cui, se consideriamo il $4n$-esimo campo ciclotomico, che contiene anche l'unità immaginaria $i = \sqrt{-1}$, esso contiene $\sqrt{n}$. Essendo $d = 4n$, il teorema è in questo caso dimostrato.

Infine, se $n \equiv 2 \pmod 4$ in particolare n è pari. Per i primi p che dividono n e che sono dispari si può ragionare in maniera analoga ai casi precedenti. In questo caso dobbiamo considerare anche $p = 2$, ma abbiamo che, siccome n è pari, il $4n$-esimo campo ciclotomico contiene $\sqrt{2}$. Dunque anche in que-

sto caso il $4n$-esimo campo ciclotomico contiene $\sqrt{n}$, ed essendo $d = 4n$, il teorema è in questo caso dimostrato. □

Passiamo ora a descrivere la forma dell'anello degli interi algebrici contenuti in un campo ciclotomico, dapprima nel caso $m = p^r$ e poi in generale. Premettiamo un lemma.

Lemma 3.2.9. *Per $m \geq 3$ vale $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$ e*

$$\operatorname{disc}(1-\omega) = \operatorname{disc}(\omega).$$

Dimostrazione. L'inclusione $\mathbb{Z}[1-\omega] \subseteq \mathbb{Z}[\omega]$ è ovvia, mentre l'altra segue dal fatto che $\omega = 1-(1-\omega)$. Per mostrare l'uguaglianza dei discriminanti, osserviamo che, poiché $\mathbb{Q}[\omega] = \mathbb{Q}[1-\omega]$, essi hanno le stesse immersioni in $\mathbb{C}$. Allora, al variare di α_i fra i coniugati di ω, $1-\alpha_i$ descrive i coniugati di $1-\omega$. Dunque, per il Teorema 2.3.7, abbiamo che

$$\operatorname{disc}(\omega) = \prod_{1\leq r<s\leq n} (\alpha_s - \alpha_r)^2 = \prod_{1\leq r<s\leq n} \big((1-\alpha_s)-(1-\alpha_r)\big)^2 = \operatorname{disc}(1-\omega). \ \square$$

Teorema 3.2.10. *Per $m = p^r$, p un numero primo, $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$.*

Dimostrazione. Osserviamo che $\{1, (1-\omega), \ldots, (1-\omega)^{n-1}\}$ è una base di interi algebrici per $\mathbb{Q}[\omega]$ su $\mathbb{Q}$. Dunque, per il Teorema 2.4.3, abbiamo che ogni $\alpha \in R = \mathbb{A} \cap \mathbb{Q}[\omega]$ si può esprimere nella forma

$$\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{d}$$

ove $n = \varphi(p^r)$, $m_1, \ldots, m_n \in \mathbb{Z}$ e $d = \operatorname{disc}(1-\omega) = \operatorname{disc}(\omega)$. Dalla Proposizione 3.2.6 sappiamo che $\operatorname{disc}(\omega)$ divide $m^{\varphi(m)}$, quindi in questo caso d è una potenza di p, sia $d = p^l$. Vogliamo mostrare che $R = \mathbb{Z}[1-\omega]$.

Supponiamo per assurdo che $R \neq \mathbb{Z}[1-\omega]$; poichè $\mathbb{Z}[1-\omega] \subseteq R$ questo vuol dire che esiste $\alpha \in R$ per cui non tutti gli m_i sono divisibili per $d = p^l$. Sia quindi $s \leq l-1$ il massimo intero positivo tale che $p^s \mid m_i$ per ogni $i = 1, \ldots, n$, e sia j il minimo indice tale che $p^l \nmid m_j$. A questo punto poniamo, per ogni i,

$$b_i := \frac{m_i}{p^s}.$$

Sottraendo da α i termini relativi agli $i < j$, che sono il prodotto di un intero per una potenza di $(1-\omega)$, otteniamo che

$$\sum_{i=j}^{n} \frac{b_i p^s}{p^l}(1-\omega)^{i-1} \in R$$

e moltiplicando per $p^{l-s-1} \in \mathbb{Z}$ otteniamo

$$\frac{\sum_{i=j}^{n} b_i(1-\omega)^{i-1}}{p} =: \beta \in R$$

con b_j non divisibile per p.

Ora, dal Lemma 3.2.4 sappiamo che

$$\prod_{k \in I}(1-\omega^k) = p$$

con I come nell'enunciato del Lemma. Poiché $(1-\omega^k)$ è divisibile per $(1-\omega)$ in $\mathbb{Z}[\omega]$, e $|I| = n$, da questo segue che $\frac{p}{(1-\omega)^n} \in \mathbb{Z}[\omega]$. Pertanto anche $\frac{p}{(1-\omega)^j} \in \mathbb{Z}[\omega]$ e quindi abbiamo

$$\beta\frac{p}{(1-\omega)^j} = \frac{b_j}{1-\omega} + \sum_{i=j+1}^{n} \frac{b_i}{(1-\omega)^{i-j-1}} \in R.$$

Sottraendo i termini relativi a $i > j$, che sono ovviamente in R, otteniamo che $\frac{b_j}{1-\omega} \in R$. Da questo segue che $\mathrm{N}(1-\omega) \mid \mathrm{N}(b_i)$, per $\mathrm{N} = \mathrm{N}^{\mathbb{Q}[\omega]}$. Ma questo è assurdo, perché $\mathrm{N}(b_i) = b_i^n$, mentre il Lemma 3.2.4 mostra che $\mathrm{N}(1-\omega) = p$. Abbiamo quindi provato che $R = \mathbb{Z}[1-\omega]$. A questo punto la tesi segue dal Lemma 3.2.9. □

Corollario 3.2.11. *Per m qualsiasi, $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$.*

Dimostrazione. La dimostrazione è per induzione su m. Se $m = p^r$ è la potenza di un numero primo la tesi è vera per il teorema precedente. Supponiamo ora che la tesi sia vera per ogni $n < m$ e mostriamola per m. Siccome m non è la potenza di un numero primo, possiamo scrivere $m = m_1 m_2$ con $m_1, m_2 > 1$ e primi tra loro. Poniamo per $i = 1, 2$

$$\omega_i = e^{\frac{2\pi i}{m_i}}, \quad K_i = \mathbb{Q}[\omega_i], \quad R_i = \mathbb{A} \cap K_i.$$

Allora, per ipotesi induttiva, abbiamo che $R_1 = \mathbb{Z}[\omega_1]$ e $R_2 = \mathbb{Z}[\omega_2]$. Vogliamo applicare il Corollario 2.4.14.

Abbiamo che $\omega^{m_1} = \omega_2$ e $\omega^{m_2} = \omega_1$, per cui, siccome $(m_1, m_2) = 1$, per il teorema di Bézout, esistono $r, s \in \mathbb{Z}$ tali che $rm_1 + sm_2 = 1$, da cui segue $\omega = \omega_2^r \omega_1^s$, e quindi $K = K_1 K_2$. Questo mostra anche che $\mathbb{Z}[\omega] = \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2]$. Inoltre $\varphi(m) = \varphi(m_1)\varphi(m_2)$, poiché m_1 e m_2 sono primi tra loro. Infine abbiamo che, per la Proposizione 3.2.6, $\mathrm{disc}(\omega_1) = \mathrm{disc}(R_1)$ divide una potenza di m_1 e $\mathrm{disc}(\omega_2) = \mathrm{disc}(R_2)$ divide una potenza di m_2, per cui $\big(\mathrm{disc}(R_1), \mathrm{disc}(R_2)\big) = 1$. Dunque, applicando il Corollario 2.4.14 concludiamo che

$$R = R_1 R_2 = \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2] = \mathbb{Z}[\omega]. \qquad \square$$

Osservazione 3.2.12. Osserviamo che questo corollario implica in particolare che $\{1, \omega, \ldots, \omega^{\varphi(m)-1}\}$ è una base integrale per $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$, e questa è una base del tipo descritto dal Teorema 2.4.16.

Bibliografia

[1] David A. Cox, *Galois Theory*, Second Edition, John Wiley and Sons, Hoboken, New Jersey, 2012.

[2] I. N. Herstein, *Algebra*, Editori Riuniti, Roma 1982, traduzione dell'originale inglese *Topics in Algebra*, John Wiley and Sons, Hoboken, New Jersey, 1975.

[3] Thomas W. Hungerford, *Algebra*, Springer-Verlag, New York, 1980.

[4] Daniel A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.