Algebraische Zahlentheorie

Prof. J. Sander
Universität Hannover
SS 2002

LaTeX 2_ε-Umsetzung von Miriam Westerfrölke und Marco Pries

Inhaltsverzeichnis

1 Algebraische Zahlen

1.1. Grundlagen

Die algebraische Zahlentheorie verallgemeinert das Konzept der gewöhnlichen ganzrationalen Zahlen

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

auf andere Zahlenbereiche. Eine wesentliche Triebfeder für die Entwicklung der Theorie im 19. Jahrhundert war das Fermat'sche Problem, die Unlösbarkeit der Gleichung

$$x^n + y^n = z^n$$

für $n \in \mathbb{N}_{\geq 3}$ in ganzen Zahlen $x, y, z \in \mathbb{Z} \setminus \{0\}$ zu zeigen.
Die Elemente von $\mathbb{Z}$ lassen sich charakterisieren als die Nullstellen linearer Polynome $f(x) = x - a \in \mathbb{Z}[x]$. Wir verallgemeinern dies zu

Definition 1.1

Sei $\alpha \in \mathbb{C}$ Nullstelle des Polynoms

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \quad \in \mathbb{Z}[x]$$

für ein $d \in \mathbb{N}$. Ist α nicht Nullstelle eines solchen Polynoms von geringerem Grad, so heißt α *ganzalgebraisch vom Grad d*.

Beispiel:
Die Zahlen $a + b\sqrt{-1} = a + bi$ mit $a, b \in \mathbb{Z}, b \neq 0$, sind ganzalgebraisch vom Grad 2, denn sie sind Nullstellen von $f(x) = x^2 - 2ax + a^2 + b^2$, aber wegen $b \neq 0$ nicht Nullstellen eines linearen Polynoms. Zu Ehren von Gauß, der diese Zahlen untersuchte, heißt

$$\mathbb{Z}[i] := \{a + bi : \quad a, b \in \mathbb{Z}\}$$

Menge der *ganzen Gauß'schen Zahlen*.

Wir beobachten, daß die Primzahl $5 \in \mathbb{Z}$ in $\mathbb{Z}[i]$ nicht mehr prim ist, denn wir haben die Faktorisierung

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

Da allgemeiner jede Primzahl $p \equiv 1 \bmod 4$ sich als Summe von zwei Quadraten darstellen lässt, d.h. $p = a^2 + b^2$ für gewisse $a, b \in \mathbb{Z}$, folgt die Zerlegung

$$p = (a+bi)(a-bi).$$

Das Verständnis der Faktorisierung ganzalgebraischer Zahlen ist das Kernanliegen der algebraischen Zahlentheorie.

Definition 1.2

Sei R ein kommutativer Ring mit Einselement $1 = 1_R$.

(i) $\alpha \in R$ heißt *Einheit in* R, falls es ein $\beta \in R$ gibt derart, dass $\alpha\beta = 1_R$.

(ii) Ein $\gamma \in R, \quad \gamma \neq 0$, heißt *irreduzibel*, sofern γ keine Einheit ist und nur Faktorisierungen der Gestalt $\gamma = \sigma \cdot u$ mit $\sigma \in R$ und einer Einheit $u \in R$ zuläßt. Derartige Zerlegungen heißen trivial.

(iii) Falls $\alpha = u \cdot \beta$ mit $\alpha, \beta \in R$ und einer Einheit $u \in R$ gilt, so heißen α und β *assoziiert* (zueinander).

(iv) Eine ganzalgebraische Zahl $\alpha \in R$ heißt *eindeutig zerlegbar in* R, wenn zwei Zerlegungen von α in irreduzible Elemente sich nur in der Reihenfolge der Faktoren oder um Einheitsfaktoren unterscheiden. D.h. Faktorisierung ist eindeutig bis auf Reihenfolge und Assoziierte.

Beispiele:

Es lässt sich leicht nachrechnen, dass die Zerlegung $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$ eindeutig ist. Demgegenüber haben wir in $\mathbb{Z}[\sqrt{10}]$

$$6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10}),$$

wobei alle Faktoren irreduzibel sind und $2, 3$ nicht assoziiert zu $4 + \sqrt{10}$, $4 - \sqrt{10}$ sind. Also ist 6 in $\mathbb{Z}[\sqrt{10}]$ nicht eindeutig zerlegbar.
Vorsicht: In $\mathbb{Z}[\sqrt{3}]$ ist

$$6 = 2 \cdot 3 = (3 + \sqrt{3})(3 - \sqrt{3}).$$

Trotzdem ist 6 eindeutig zerlegbar, denn die vier Faktoren sind nicht irreduzibel:

$$2 = (-1+\sqrt{3})(1+\sqrt{3}), \quad 3 = \sqrt{3}\cdot\sqrt{3}, \quad 3+\sqrt{3} = \sqrt{3}(1+\sqrt{3}), \quad 3-\sqrt{3} = \sqrt{3}(-1+\sqrt{3}).$$

Die Nichteindeutigkeit der Zerlegung ganzalgebraischer Zahlen in gewissen Ganzzahlbereichen erfordert Untersuchungen, die in $\mathbb{Z}$ nicht nötig sind.

Definition 1.3

Sei $\alpha \in R, \alpha \neq 0$, eine ganzalgebraische Zahl.

(i) Wir sagen: α *teilt* $\beta \in R$, geschrieben $\alpha \mid \beta$, falls es ein $\gamma \in R$ gibt mit $\beta = \alpha\gamma$.

(ii) Ist α keine Einheit in R, so nennen wir α *prim*, falls für alle $\beta, \gamma \in R$ gilt:

$$\alpha \mid \beta\gamma \Longrightarrow \alpha \mid \beta \text{ oder } \alpha \mid \gamma.$$

Die Unterscheidung zwischen irreduziblen und primen Elementen bei ganzalgebraischen Zahlen, die in $\mathbb{Z}$ bedeutungslos ist, spielt dort eine wesentliche Rolle, wo keine eindeutige Faktorisierung vorliegt. Wäre jedes irreduzible Element prim, so würde ein simples Induktionsargument über die Anzahl der irreduziblen (primen) Faktoren zeigen, dass die Faktorisierung eindeutig ist (so wird die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ bewiesen).

Beispiel:
Es lässt sich zeigen, dass die irreduziblen Zahlen $2, 3, 4 \pm \sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ nicht prim sind. Wir sagen: $\mathbb{Z}[\sqrt{10}]$ besitzt keine eindeutige Faktorisierung.

Eine besonders intensiv studierte Klasse von ganzalgebraischen Zahlen bilden die sogenannten Einheitswurzeln.

Definition 1.4

Sei $n \in \mathbb{N}$. Eine Nullstelle $\zeta_n \in \mathbb{C}$ des Polynoms $x^n - 1$ heißt *primitive n-te Einheitswurzel*, sofern $\zeta_n^d - 1 \neq 0$ für alle $d < n$.

Die Fermat-Gleichung $x^n + y^n = z^n$ lässt sich mit Hilfe primitiver n-ter Einheitswurzeln faktorisieren. Ist ζ_n eine primitive n-te Einheitswurzel, so gilt

$$z^n = x^n + y^n = (x + y)(x + \zeta_n\, y)(x + \zeta_n^2\, y) \cdot \ldots \cdot (x + \zeta_n^{n-1}\, y).$$

Hat die Gleichung eine Lösung $x, y, z \in \mathbb{Z}$, so haben wir also $x^n + y^n$ in $\mathbb{Z}[\zeta_n]$ faktorisiert.

Der kleinste Körper, in dem $\mathbb{Z}$ liegt, ist $\mathbb{Q}$. Entsprechend gibt es zu jedem Ganzzahlbereich in $\mathbb{C}$ einen eindeutigen kleinsten Körper, der ein Teilkörper von $\mathbb{C}$ ist und den Ganzzahlbereich enthält.

Definition 1.5

Sei $\alpha \in \mathbb{C}$ Nullstelle des Polynoms

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 \quad \in \mathbb{Z}[x]$$

für ein $d \in \mathbb{N}$. Ist α nicht Nullstelle eines solchen Polynoms von geringerem Grad, so heißt α *algebraisch vom Grad d*.
Ist α eine algebraische Zahl vom Grad d, so nennen wir den Erweiterungskörper $\mathbb{Q}(\alpha)$ von $\mathbb{Q}$ einen *algebraischen Zahlkörper vom Grad d über $\mathbb{Q}$ erzeugt von α*.

Bemerkungen:

(i) Betrachten wir $\mathbb{Q}(\alpha)$ als Vektorraum über $\mathbb{Q}$, so ist der Grad d die Dimension von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$. Eine Basis ist $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$.

(ii) Der kleinste algebraische Zahlkörper ist $\mathbb{Q}$ selbst, wobei selbstverständlich $d = 1$ ist. Eine einfache Körpererweiterung $\mathbb{Q}(\alpha)$ ist der kleinste Körper, der $\mathbb{Q}$ und α enthält.

(iii) Cantor bewies, dass die Menge aller algebraischen Zahlen (beliebigen Grades) abzählbar ist. Da $\mathbb{R}$ und somit $\mathbb{C}$ überabzählbare Mengen sind, existieren überabzählbar viele nichtalgebraische Zahlen, genannt transzendente Zahlen. Beispiele sind e und π.

Im Jahre 1847 stellte Lamé eine Grundidee von Liouville vor, um die Fermat-Vermutung zu beweisen: Sind in der Zerlegung

$$z^n = (x+y)(x+\zeta_n\, y)(x+\zeta_n^2\, y)\cdot\ldots\cdot(x+\zeta_n^{n-1}\, y)$$

die Faktoren auf der rechten Seite paarweise teilerfremd, so gilt für $0 \le j \le n-1$

$$x + \zeta_n^j\, y = z_j^n$$

mit gewissen z_j. Liouville bemerkte, dass dieser Schluss die eindeutige Faktorisierung in $\mathbb{Z}[\zeta_n]$ voraussetzt. Es stellte sich jedoch heraus, dass dies im Allgemeinen nicht gilt. Kummer überwand die Schwierigkeit durch Einführung sogenannter „idealer Zahlen“, für die sich die Eindeutigkeit der Faktorisierung zeigen lässt.

Definition 1.6

Sei R ein kommutativer Ring. Eine Menge $I \subseteq R$, $I \neq \emptyset$, heißt *Ideal in* R, falls gilt:

(i) $\alpha, \beta \in I \Longrightarrow \alpha - \beta \in I$;

(ii) $\alpha \in I, r \in R \Longrightarrow \alpha r \in I$.

Beispiel:

Die Mengen

$$(2) := \{2a + 2b\sqrt{10} : a, b \in \mathbb{Z}\} \quad , \quad (3) := \{3a + 3b\sqrt{10} : a, b \in \mathbb{Z}\}$$

sind Ideale in $\mathbb{Z}[\sqrt{10}]$. Da sie jeweils von einem einzigen Element erzeugt werden (d.h. $(2) = 2 \cdot R$), sprechen wir von Hauptidealen. Das Produkt der beiden Ideale,

d.h. die Menge aller endlichen Summen von Produkten der Elemente der beiden Ideale, ergibt sich zu

$$(6) = \{6a + 6b\sqrt{10} : a, b \in \mathbb{Z}\} = (2) \cdot (3).$$

Zwecks eindeutiger Faktorisierung von Idealen müssen wir das Konzept der Primzahl in $\mathbb{Z}$ auf Ideale übertragen.

Definition 1.7

Seien $I \neq \{0\}$ und J Ideale in einem kommutativen Ring R mit Identität 1_R.
Wir sagen: I *teilt* J, geschrieben $I \mid J$, falls es ein Ideal H in R gibt mit $J = H \cdot I$.
Ein Ideal P in einem Ring R ganzalgebraischer Zahlen heißt *Primideal*, falls für alle Ideale $I, J \subseteq R$ gilt

$$P \mid I \cdot J \Longrightarrow P \mid I \text{ oder } P \mid J \ .$$

Beispiel:
In Fortsetzung des obigen Beispiels haben wir (2) | (6) und (3) | (6) in $\mathbb{Z}[\sqrt{10}]$. Wir verwenden folgende Kurzschreibweise für Ideale:

$$[2, \sqrt{10}] := 2\mathbb{Z} + \sqrt{10}\mathbb{Z} \quad , \quad [3, \pm 1 + \sqrt{10}] := 3\mathbb{Z} + (\pm 1 + \sqrt{10})\mathbb{Z} \ .$$

Dabei stellen sich alle drei Ideale als Primideale in $\mathbb{Z}[\sqrt{10}]$ heraus. Wir haben

$$(2) = [2, \sqrt{10}]^2 \quad \text{und} \quad (3) = [3, 1 + \sqrt{10}] \cdot [3, -1 + \sqrt{10}]$$

und somit – wie sich zeigen lässt – eine eindeutige Primidealzerlegung von (6) in $\mathbb{Z}[\sqrt{10}]$.

1.2. Algebraische Zahlen und Zahlkörper

Definition 1.8

Sei E ein Erweiterungskörper eines Grundkörpers F. Ein $\alpha \in E$ heißt *algebraisch über F*, falls für ein Polynom $f(x) \in F[x] \setminus \{0\}$ gilt $f(\alpha) = 0$. Ist α nicht algebraisch über F , so heißt α *transzendent über F*. Sind alle Elemente von E algebraisch über F, so nennen wir E *algebraische Erweiterung von F*, andernfalls *transzendente Erweiterung von F*.

Satz 1.9

Sei F ein algebraischer Zahlkörper (d.h. eine algebraische Erweiterung von $\mathbb{Q}$). Zu algebraischen $\alpha \in \mathbb{C}$ über F existiert eindeutig das sogenannte *Minimalpolynom* $m_{\alpha,F}(x) \in F[x] \setminus \{0\}$ von α über F, d.h. $m_{\alpha,F}(x)$ hat führenden Koeffizienten 1 und minimalen Grad derart, dass $m_{\alpha,F}(\alpha) = 0$. Ist umgekehrt α Nullstelle eines irreduziblen Polynoms $f(x) \in F[x] \setminus \{0\}$ mit führendem Koeffizienten 1, so ist $f(x) = m_{\alpha,F}(x)$. Außerdem gilt für jedes Polynom $f(x) \in F[x]$ mit $f(\alpha) = 0$, dass $m_{\alpha,F}(x) \mid f(x)$.

Beweis:
Es existiert ein $f(x) \in F[x] \setminus \{0\}$ mit $f(\alpha) = 0$. Durch Abspalten von Faktoren und Division durch den höchsten Koeffizienten erhalten wir „ein“ Minimalpolynom $g(x) \in F[x] \setminus \{0\}$ von α über F. Sei $h(x) \in F[x]$ irgendein Polynom mit $h(\alpha) = 0$. Bekanntlich ist $F[x]$ ein euklidischer Ring (für jeden Körper F), d.h. es gibt $q(x), r(x) \in F[x]$ derart, dass

$$h(x) = q(x) \cdot g(x) + r(x),$$

wobei $0 \leq \deg r < \deg g$ oder $r(x) = 0$. Wegen $h(\alpha) = g(\alpha) = 0$ folgt $r(\alpha) = 0$ im Widerspruch zum minimalen Grad von g, es sei denn $r(x) = 0$. Also haben

wir $g(x) \mid h(x)$. Wäre $f(x)$ ein anderes Minimalpolynom von α über F, so folgte $g(x) \mid f(x)$ und $f(x) \mid g(x)$, d.h. $f(x) = c \cdot g(x)$ für ein $c \in F$. Wegen führender Koeffizienten 1 in f und g bleibt nur $c = 1$, also $f(x) = g(x) =: m_{\alpha,F}(x)$.

□

Korollar 1.10

Ein irreduzibles Polynom über einem algebraischen Zahlkörper F hat nur einfache Nullstellen in $\mathbb{C}$.

Beweis:

Sei $f(x) \in F[x]$ irreduzibel mit einer doppelten Nullstelle α, d.h.

$$f(x) = (x - \alpha)^2 \cdot g(x)$$

für ein Polynom $g(x)$ über $\mathbb{C}$. Wegen $f(\alpha) = 0$ folgt aus Satz 1.9, dass $m_{\alpha,F}(x) \mid f(x)$. Da f irreduzibel ist, bleibt nur $f(x) = b \cdot m_{\alpha,F}(x)$ für ein $b \in F$. Wir haben

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$$

also $f'(\alpha) = 0$, wobei selbstverständlich $f'(x) \in F[x]$. Erneute Anwendung von Satz 1.9 liefert $m_{\alpha,F}(x) \mid f'(x)$. Es ergibt sich der Widerspruch

$$\deg m_{\alpha,F}(x) \leq \deg f'(x) = \deg f(x) - 1 = \deg m_{\alpha,f}(x) - 1.$$

□

Beispiel:

Sei $F = \mathbb{Q}(i)$ und sei $\alpha = \zeta_8 = (1+i)/\sqrt{2}$ eine primitive 8. Einheitswurzel. Offenbar gilt $\zeta_8^2 = i$, also ist $m_{\zeta_8,F}(x) = x^2 - i \in F[x]$. Dagegen ist

$$m_{\zeta_8,\mathbb{Q}}(x) = x^4 + 1 \ .$$

Korollar 1.11

Sei α algebraisch über einen Zahlkörper F mit Minimalpolynom $m_{\alpha,F}(x)$. Dann besitzt die einfache algebraische Erweiterung $F(\alpha)$ (d.h. der kleinste Körper, der F und α umfasst) die Eigenschaft, dass jedes $\beta \in F(\alpha)$ eine eindeutige Darstellung der Gestalt

$$\beta = \sum_{j=0}^{d-1} a_j \alpha^j \quad \in F[\alpha]$$

hat, wobei $d = \deg m_{\alpha,F}$.

Beweis:

Jedes $\beta \in F(\alpha)$ besitzt eine Darstellung $\beta = f(\alpha)/g(\alpha)$ mit Polynomen $f(x), g(x) \in F[x]$ und $g(\alpha) \neq 0$. Nach Satz 1.9 folgt $m_{\alpha,F}(x) \nmid g(x)$, also sind $g(x)$ und $m_{\alpha,F}(x)$ teilerfremd. Dabei gibt es im euklidischen Ring $F[x]$ Polynome $s(x)$ und $t(x)$ derart, dass

$$s(x)g(x) + t(x)m_{\alpha,F}(x) = 1.$$

Wegen $m_{\alpha,F}(\alpha) = 0$ ist $s(\alpha) = 1/g(\alpha)$, also $\beta = f(\alpha)/g(\alpha) = f(\alpha) \cdot s(\alpha)$. Wir setzen $h(x) := f(x) \cdot s(x) \in F[x]$. Dazu existieren Polynome $q(x), r(x) \in F[x]$ mit

$$h(x) = q(x) \cdot m_{\alpha,F}(x) + r(x),$$

wobei $0 \leq \deg r < \deg m_{\alpha,F}$ oder $r(x) = 0$. Wegen $m_{\alpha,F}(\alpha) = 0$ folgt $\beta = h(\alpha) = r(\alpha)$, d.h. β besitzt eine Darstellung in gewünschter Form.

Zum Beweis der Eindeutigkeit von $r(x)$ sei $v(x) \in F[x]$ mit $\deg v(x) \leq d-1$ und $v(\alpha) = \beta$. Damit ist $r(\alpha) - v(\alpha) = 0$, d.h. $r(x) - v(x) \in F[x]$ mit $\deg(r-v) \leq d-1$ besitzt die Nullstelle α. Dies widerspricht $\deg m_{\alpha,F}(x) = d$ außer für $r(x) - v(x) = 0$, also $r(x) = v(x)$.

□

Korollar 1.12

Sei $F \subseteq E \subseteq \mathbb{C}$ mit einem Erweiterungskörper E eines algebraischen Zahlkörpers F. Für $\alpha \in E$ ist $F(\alpha)$ eine endliche Erweiterung von F (d.h. $F(\alpha)$ hat als Vektorraum über F endliche Dimension d, geschrieben $[F(\alpha) : F] = d$) genau dann, wenn α algebraisch über F ist. In diesem Fall gilt

$$[F(\alpha) : F] = \deg m_{\alpha,F}.$$

Beweis:

„$\Longrightarrow$“

Sei $[F(\alpha) : F] = d \in \mathbb{N}$. Dann sind $1, \alpha, \alpha^2, \ldots, \alpha^d$ linear abhängig über F (in jedem Vektorraum der Dimension d sind $d+1$ Elemente linear abhängig), d.h. α erfüllt eine Polynomgleichung vom Grad d.

„$\Longleftarrow$“

Ist α algebraisch über F, so lässt sich nach Korollar 1.11 jedes Element von $F(\alpha)$ als Linearkombination von $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ mit $d = \deg m_{\alpha,F}$ eindeutig darstellen. Es folgt $[F(\alpha) : F] = d < \infty$.

□

Satz 1.13

Sei E ein Erweiterungskörper eines Körpers F und K die Menge aller algebraischen Elemente von E über F. Dann ist K eine algebraische Körpererweiterung von F. Ist dabei $K = F(X)$ für eine endliche Menge $X \subseteq K$, so ist K eine endliche Erweiterung von F.

Beweis:

Um zu zeigen, dass K ein Körper ist, genügt der Nachweis der Abgeschlossenheit bezüglich Addition, Multiplikation und Inversenbildung. Dafür wiederum ist hinreichend, für $\alpha, \beta \in K$ zu folgern, dass $\alpha+\beta \in K$ und $\alpha/\beta \in K$ $(\beta \neq 0)$ (dies impliziert

auch $\alpha - \beta \in K$ und $\alpha \cdot \beta \in K$). Seien

$$m_{\alpha,F}(x) = \prod_{i=1}^{d_\alpha}(x - \alpha_i) \quad \text{bzw.} \quad m_{\beta,F}(x) = \prod_{j=1}^{d_\beta}(x - \beta_j)$$

mit $d_\alpha = \deg m_{\alpha,F}$ und $d_\beta = \deg m_{\beta,F}$ die Minimalpolynome von α bzw. β. Wir bilden die Polynome

$$f_{\alpha+\beta}(x) := \prod_{i=1}^{d_\alpha}\prod_{j=1}^{d_\beta}(x - (\alpha_i + \beta_j))$$

und

$$f_{\alpha\beta}(x) := \prod_{i=1}^{d_\alpha}\prod_{j=1}^{d_\beta}(x - \alpha_i\beta_j) \ .$$

Nach dem Satz über elementarsymmetrische Funktionen sind $f_{\alpha+\beta}(x)$ und $f_{\alpha\beta}(x) \in F[x]$. Damit sind $\alpha + \beta$ und $\alpha\beta$ algebraisch über F, d.h. sie liegen in K. Das Polynom $x^{d_\beta} m_{\beta,F}\,(1/x) \in F[x]$ hat die Nullstelle $1/\beta$, also liegt $1/\beta$ in K. Das obige Argument impliziert somit, dass auch $\alpha/\beta = \alpha \cdot 1/\beta \in K$.

□

Korollar 1.14

Die Menge $\overline{\mathbb{Q}}$ aller algebraischen Zahlen in $\mathbb{C}$ ist ein Teilkörper von $\mathbb{C}$ ($\overline{\mathbb{Q}}$ ist der algebraische Abschluß von $\mathbb{Q}$).

Satz 1.15 (vom primitiven Element)

Ist F endliche Erweiterung von $\mathbb{Q}$ und E endliche Erweiterung von F, so ist $E = F(\alpha)$ für ein $\alpha \in \overline{\mathbb{Q}}$. Insbesondere sind alle endlichen Erweiterungen von $\mathbb{Q}$ von der Form $\mathbb{Q}(\alpha)$ für ein geeignetes $\alpha \in \overline{\mathbb{Q}}$.

Beweis:

Sei $[E : F] = d \ \in \mathbb{N}$. Für jedes $\gamma \in E$ sind $1, \gamma, \gamma^2, \ldots, \gamma^d$ linear abhängig über F, d.h. $\sum_{j=0}^{d} q_j \gamma^j = 0$ für gewisse $q_j \in F$, nicht alle 0. Damit ist E eine algebraische Erweiterung von F, d.h. $E = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ für gewisse algebraische $\alpha_1, \ldots, \alpha_m \in E$.

Zum Beweis der Existenz eines primitiven Elements α genügt es aufgrund eines Induktionsarguments zu zeigen:

$$E = F(\alpha_1, \alpha_2),\ \alpha_1, \alpha_2 \text{ algebraisch } \Longrightarrow E = F(\alpha) \text{ für ein algebraisches } \alpha.$$

Seien $m_j(x) := m_{\alpha_j, F}(x)$ für $j = 1, 2$. Faktorisierung über $\mathbb{C}$ liefert

$$m_j(x) = \prod_{i=1}^{d_j} (x - \alpha_{j,i})$$

für $d_j := \deg m_j$ und geeignete $\alpha_{j,i} \in \mathbb{C}$, wobei o.B.d.A. gelte $\alpha_{j,1} = \alpha_j$ $(j = 1, 2)$. Nach Korollar 1.10 sind die Zahlen $\alpha_{1,i}$ $(1 \leq i \leq d_1)$ wie auch die Zahlen $\alpha_{2,k}$ $(1 \leq k \leq d_2)$ jeweils paarweise verschieden. Daher hat für $1 \leq i \leq d_1$ und $1 < k \leq d_2$ jede der Gleichungen

$$\alpha_{1,i} + x \cdot \alpha_{2,k} = \alpha_{1,1} + x \cdot \alpha_{2,1}$$

höchstens eine Lösung $x \in F$ (nämlich $x = (\alpha_{1,i} - \alpha_{1,1})/(\alpha_{2,1} - \alpha_{2,k})$). Also können wir ein $c \in F \setminus \{0\}$ finden derart, dass

$$(*) \quad \alpha_{1,i} + c \cdot \alpha_{2,k} \neq \alpha_{1,1} + c \cdot \alpha_{2,1} \quad (1 \leq i \leq d_1\ ,\ 1 < k \leq d_2)\ .$$

Wir setzen $\alpha := \alpha_{1,1} + c \cdot \alpha_{2,1}$. Es bleibt zu zeigen, dass $E = F(\alpha)$.
Wegen $E = F(\alpha_{1,1}, \alpha_{2,1})$ gilt sicherlich $F(\alpha) \subseteq F(\alpha_{1,1}, \alpha_{2,1})$. Wir müssen nur noch nachweisen, dass $\alpha_{1,1}, \alpha_{2,1} \in F(\alpha)$. Wegen $\alpha_{1,1} = \alpha - c \cdot \alpha_{2,1}$ genügt $\alpha_{2,1} \in F(\alpha)$.
Dafür setzen wir $f(x) := m_1(\alpha - cx) \in F(\alpha)[x]$. Es gilt

$$f(\alpha_{2,1} = m_1(\alpha - c \cdot \alpha_{2,1}) = m_1(\alpha_{1,1}) = 0 = m_2(\alpha_{2,1})\ .$$

Es zeigt sich, dass $\alpha_{2,1}$ die einzige gemeinsame Nullstelle von $f(x)$ und $m_2(x)$ ist, denn:
Sei $f(\sigma) = m_2(\sigma) = 0$. Dann ist $\sigma = \alpha_{2,k}$ für ein k und $\alpha - c \cdot \sigma = \alpha_{1,i}$ für ein i. Daher ist

$$\alpha_{1,i} = \alpha - c \cdot \sigma = \alpha - c \cdot \alpha_{2,k} = \alpha_{1,1} + c \cdot \alpha_{2,1} - c \cdot \alpha_{2,k}\ .$$

Wegen $(*)$ bleibt nur $k = 1$, d.h. $\sigma = \alpha_{2,1}$. Es sei $m_3(x) := m_{\alpha_{2,1}, F(\alpha)}(x)$. Nach Satz 1.9 haben wir $m_3(x) \mid f(x)$ und $m_3(x) \mid m_2(x)$. Da $f(x)$ und $m_2(x)$ nur eine gemeinsame Nullstelle, nämlich $\alpha_{2,1}$, haben, folgt $\deg m_3 = 1$. Damit ist $\alpha_{2,1}$ algebraisch

vom Grad 1 über $F(\alpha)$, d.h. $\alpha_{2,1} \in F(\alpha)$.

□

Bemerkung:

Wir haben zu Beginn des Beweises gezeigt, dass jede endliche Erweiterung algebraisch ist. Die Umkehrung ist im Allgemeinen falsch: $\overline{\mathbb{Q}}$ ist algebraisch über $\mathbb{Q}$, aber keine endliche Erweiterung von $\mathbb{Q}$.

Definition 1.16

Sei F ein Zahlkörper. Eine Abbildung $\Theta : F \to \mathbb{C}$ heißt *Einbettung von F in $\mathbb{C}$*, falls Θ ein injektiver Ring-Homomorphismus ist.
Ist F die Erweiterung eines Zahlkörpers L, geschrieben F/L, und ist Θ Einbettung von F in $\mathbb{C}$, die L punktweise festlässt (d.h. $\Theta(l) = l$ für alle $l \in L$), so heißt Θ *L-Isomorphismus von F*. Ist Θ ein L-Isomorphismus und $F = L(\alpha)$ für ein algebraisches α, so heißt $\Theta(\alpha)$ *Konjugierte von α über L*. Im Falle einer quadratischen Erweiterung $F = \mathbb{Q}(\sqrt{D})$ nennen wir die Konjugierte $a - b\sqrt{D}$ von $a + b\sqrt{D} \in F$ die *algebraische Konjugierte von $a + b\sqrt{D}$*.

Bemerkung:

Jede Einbettung eines Zahlkörpers K in $\mathbb{C}$ ist automatisch ein $\mathbb{Q}$-Isomorphismus von K.
$\big(\Theta(a) = \Theta(1 + 1 + \cdots + 1) = a \cdot \Theta(1) = a \quad \text{für } a \in \mathbb{Z}$
$b \cdot \Theta\,(a/b) = \Theta(b) \cdot \Theta\,(a/b) = \Theta(a) = a \Longrightarrow \Theta\,(a/b) = a/b\big)$.

Satz 1.17

Sei $F = \mathbb{Q}(\alpha)$ algebraischer Zahlkörper mit $[F : \mathbb{Q}] = d$. Dann gibt es genau d Einbettungen Θ_j $(1 \leq j \leq d)$ von F in $\mathbb{C}$. Die Konjugierten $\alpha_j := \Theta_j(\alpha)$ von α über $\mathbb{Q}$ mit $\alpha_1 := \alpha$ sind genau die Nullstellen von $m_{\alpha,\mathbb{Q}}(x)$.

Beweis:

Sei Θ eine Einbettung von F in $\mathbb{C}$ mit $\beta := \Theta(\alpha)$. Für gewisse $q_j \in \mathbb{Q}$ gilt

$$0 = m_{\alpha,\mathbb{Q}}(\alpha) = \sum_{j=0}^{d} q_j \ \alpha^j \ ,$$

also

$$0 = \Theta(0) = \Theta\left(\sum_{j=0}^{d} q_j \ \alpha^j\right) = \sum_{j=0}^{d} q_j \ \Theta(\alpha)^j = \sum_{j=0}^{d} q_j \ \beta^j = m_{\alpha,\mathbb{Q}}(\beta) \ .$$

Somit ist $\beta = \alpha_j$ für eine der Nullstellen $\alpha_1, \ldots, \alpha_d$ von $m_{\alpha,\mathbb{Q}}(x)$. Da die Einbettung Θ nur von $\Theta(\alpha)$ abhängt, gibt es deshalb höchstens d verschiedene Einbettungen von F in $\mathbb{C}$.

Es bleibt zu zeigen, dass tatsächlich d verschiedene Einbettungen $\Theta_1, \ldots, \Theta_d$ von F nach $\mathbb{C}$ existieren. Nach Korollar 1.11 besitzt jedes Element $\gamma \in F$ eine Darstellung

$$\gamma = \sum_{j=0}^{d} r_j \ \alpha^j \quad \in \mathbb{Q}[\alpha] \ .$$

Wir definieren damit für jedes j die Einbettung $\Theta_j : F \to \mathbb{C}$ durch $\Theta_j(f(\alpha)) := f(\alpha_j)$ für beliebiges $f(x) \in \mathbb{Q}[x]$. Wegen der Eindeutigkeit der Darstellung der $\gamma \in F$ in obiger Gestalt (Korollar 1.11) sind die Θ_j injektiv. Es bleibt lediglich die Wohldefiniertheit zu zeigen. Dazu sei $f(\alpha) = g(\alpha)$ für $f(x), g(x) \in \mathbb{Q}[x]$. Es folgt mit Satz 1.9, dass

$$f(x) - g(x) = h(x) \cdot m_{\alpha,\mathbb{Q}}(x)$$

für ein $h(x) \in \mathbb{Q}[x]$. Also haben wir

$$f(\alpha_j) - g(\alpha_j) = h(\alpha_j) \cdot m_{\alpha,\mathbb{Q}}(\alpha_j) = 0$$

und somit

$$\Theta_j(f(\alpha)) = f(\alpha_j) = g(\alpha_j) = \Theta_j(g(\alpha)) \ .$$

Damit sind die Θ_j wohldefiniert und $\Theta_j(\alpha) = \alpha_j$.

□

Definition 1.18

Seien $\Theta_j \quad (1 \leq j \leq d := [F : \mathbb{Q}])$ die Einbettungen von F in $\mathbb{C}$. Ein Θ_j mit $\Theta_j(F) \subseteq \mathbb{R}$ heißt *reelle Einbettung*, und wir setzen $r_1 := \sharp\{1 \leq j \leq d : \ \Theta_j(F) \subseteq \mathbb{R}\} \geq 0$. Für $r_1 = d$ heißt F *total-reeller Zahlkörper*.
Ein Θ_j mit $\Theta_j(F) \nsubseteq \mathbb{R}$ heißt *(eigentlich) komplexe Einbettung*, und es gibt $2r_2$ solche Einbettungen, da zu jeder komplexen Einbettung Θ_j die konjugierte komplexe Einbettung $\overline{\Theta_j}$ existiert. Für $2r_2 = d$ heißt F *total-komplexer Zahlkörper*.
In jedem Fall gilt $d = r_1 + 2r_2$, und wir nennen $\{r_1, r_2\}$ die *Signatur von F*.

Beispiel:
Es ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ mit den Einbettungen

$$\Theta_1 : \sqrt[3]{2} \longmapsto \sqrt[3]{2}, \quad \Theta_2 : \sqrt[3]{2} \longmapsto \zeta_3\sqrt[3]{2}, \quad \Theta_3 : \sqrt[3]{2} \longmapsto \zeta_3^2\sqrt[3]{2} \ ,$$

wobei ζ_3 eine der beiden primitiven 3. Einheitswurzeln bezeichne. Damit ist Θ_1 eine reelle Einbettung, und Θ_2, Θ_3 sind zueinander konjugierte komlexe Einbettungen; also haben wir $r_1 = r_2 = 1$.

Satz 1.19

Sei $E \subseteq \mathbb{C}$ eine endliche Erweiterung eines Zahlkörpers F. Jede Einbettung von F in $\mathbb{C}$ lässt sich zu genau $[E : F]$ Einbettungen von E in $\mathbb{C}$ fortsetzen. Insbesondere gibt es $[E : F]$ F-Isomorphismen von E.

Beweis:
Nach Satz 1.15 existiert ein $\alpha \in E$ mit $E = F(\alpha)$, wobei α vom Grad $d := [E : F]$ über F ist.
Sei Θ eine Einbettung von F in $\mathbb{C}$, und sei $\widetilde{\Theta}$ eine Einbettung von E in $\mathbb{C}$ mit $\widetilde{\Theta}\big|_F = \Theta$. Dann ist $\widetilde{\Theta}$ eindeutig bestimmt durch den Wert $\widetilde{\Theta}(\alpha) =: \beta$.
Sei $m_{\alpha,F}(x) := \sum_{j=0}^{d} q_j \ x^j$. Dann ist auch

$$m_{\alpha,F}^{\Theta}(x) := \sum_{j=0}^{d} \Theta(q_j)x^j$$

irreduzibel über $\Theta(F)$. Seien $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ die paarweise verschiedenen Nullstellen von $m^{\Theta}_{\alpha,F}(x)$. Wir haben dann

$$0 = \widetilde{\Theta}(0) = \widetilde{\Theta}\left(\sum_{j=0}^{d} q_j \cdot \alpha^j\right) = \sum_{j=0}^{d} \widetilde{\Theta}(q_j) \cdot \widetilde{\Theta}(\alpha)^j = \sum_{j=0}^{d} \Theta(q_j) \cdot \beta^j \ ,$$

d.h. $\beta = \alpha_j$ für ein $j \in \{1, \ldots, d\}$. Damit sind die d Körper-Isomorphismen $\Theta_j : F(\alpha) \longrightarrow F(\alpha_j)$ mit $\Theta_j\big|_F = \Theta$ und $\Theta_j(\alpha) = \alpha_j \quad (1 \leq j \leq d)$ gerade die gesuchten Fortsetzungen von Θ.

□

Die letzte Aussage des Satzes besagt nur, dass die Identität auf F als spezielle Einbettung von F in $\mathbb{C}$ ebenfalls d Fortsetzungen besitzt.

Wir wissen bereits, dass für algebraisches α vom Grad n und die Einbettungen Θ_j $(1 \leq j \leq n)$ von $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ gilt

$$\prod_{j=1}^{n}(x - \Theta_j(\alpha)) = m_{\alpha,\mathbb{Q}}(x) \ .$$

Wir untersuchen dies nun für beliebiges $\beta \in \mathbb{Q}(\alpha)$ anstelle von α.

Satz 1.20

Sei $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ mit den Einbettungen $\Theta_1, \ldots, \Theta_n$ in $\mathbb{C}$. Für beliebiges $\beta \in \mathbb{Q}(\alpha)$ vom Grad d über $\mathbb{Q}$ gilt $d \mid n$ und

$$f(x) := \prod_{j=1}^{n}(x - \Theta_j(\beta)) = (m_{\beta,\mathbb{Q}}(x))^{n/d} \ ;$$

d.h. in der Faktorisierung des Polynoms $f(x) \in \mathbb{Q}[x]$ sind die $\Theta_j(\beta)$ die Nullstellen von $m_{\beta,\mathbb{Q}}(x)$ jeweils mit Vielfachheit n/d. Außerdem ist $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ genau dann, wenn $d = n$.

Beweis:

Klar ist: $\mathbb{Q}(\beta)$ ist Teilkörper von $\mathbb{Q}(\alpha)$, also Untervektorraum von $\mathbb{Q}(\alpha)$. Es gilt

$$n = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot d \ ,$$

und es folgt $d \mid n$ und $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ nur für $n = d$.
Die Einschränkung $\Theta_j\big|_{\mathbb{Q}(\beta)}$ ist offenbar eine Einbettung von $\mathbb{Q}(\beta)$. Wir ordnen die Θ_j so an, dass $\Theta_1 \mid \mathbb{Q}(\beta), \ldots, \Theta_\alpha \mid \mathbb{Q}(\beta)$ die d verschiedenen Einbettungen von $\mathbb{Q}(\beta)$ in $\mathbb{C}$ sind (vgl. Sätze 1.17 und 1.19). Also gilt

$$m_{\beta,\mathbb{Q}}(x) = \prod_{j=1}^{d} (x - \Theta_j(\beta)) \ .$$

Wegen $f(\beta) = f(\Theta_1(\beta)) = 0$ (o.B.d.A. $\Theta_1 = \mathrm{id}$) folgt nach Satz 1.9, dass $m_{\beta,\mathbb{Q}}(x) \mid f(x)$. Damit haben wir

$$f(x) = (m_{\beta,\mathbb{Q}}(x))^k \cdot g(x)$$

für ein $k \in \mathbb{N}$ und ein $g(x) \in \mathbb{Q}(\alpha)[x]$ mit führendem Koeffizienten 1, wobei $m_{\beta,\mathbb{Q}}(x)$ und $g(x)$ teilerfremd sind. Wäre $\deg g \geq 1$ (d.h. $g(x) \neq 1$), so hätten wir $g(\gamma) = 0$ für eine algebraische Zahl γ. Damit $f(\gamma) = 0$, d.h. $\gamma = \Theta_j(\beta)$ für ein $j \in \{1, \ldots, d\}$. Dies implizierte $m_{\beta,\mathbb{Q}}(x) \mid g(x)$ im Widerspruch zur Definition von $f(x)$. Also haben wir $f(x) = (m_{\beta,\mathbb{Q}}(x))^k \in \mathbb{Q}[x]$ und somit

$$n = \deg f = \deg(m_{\beta,\mathbb{Q}})^k = kd \ ,$$

d.h. $k = n/d$.

□

Beispiel:

Sei $F = \mathbb{Q}(\zeta_8)$ mit der primitiven 8. Einheitswurzel $\zeta_8 = \frac{1}{\sqrt{2}}(i+1)$. Für $\beta = i = \zeta_8^2$ haben wir $m_{i,\mathbb{Q}}(x) = x^2 + 1$. Die $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$ Einbettungen von F in $\mathbb{C}$ sind gegeben durch $\Theta_j : \zeta_8 \longmapsto \zeta_8^{2j-1}$ $(1 \leq j \leq 4)$. Damit erhalten wir

$$\begin{aligned} f(x): &= \prod_{j=1}^{4}(x - \Theta_j(i)) = \prod_{j=1}^{4}(x - \Theta_j(\zeta_8^2)) \\ &= \prod_{j=1}^{4}(x - \zeta_8^{2(2j-1)}) = (x-\zeta_8^2)(x-\zeta_8^6)(x-\zeta_8^{10})(x-\zeta_8^{14}) \\ &= (x-i)(x+i)(x-i)(x+i) = (x^2+1)^2 = (m_{i,\mathbb{Q}}(x))^2 \ . \end{aligned}$$

1.3. Norm, Spur und Diskriminante

Definition 1.21

Sei F Zahlkörper mit $[F:\mathbb{Q}] = d$, und seien $\Theta_1, \ldots, \Theta_d$ die Einbettungen von F in $\mathbb{C}$. Für $\alpha \in F$ heißt

$$T_F(\alpha) := \sum_{j=1}^{d} \Theta_j(\alpha)$$

Spur von α in F und

$$N_F(\alpha) := \prod_{j=1}^{d} \Theta_j(\alpha)$$

Norm von α in F.

Da die Einbettungen Θ_j Ring-Homomorphismen sind, ist offensichtlich T_F additiv (d.h. $T_F(\alpha+\beta) = T_F(\alpha) + T_F(\beta)$ für $\alpha, \beta \in F$) bzw. N_F multiplikativ (d.h. $N_F(\alpha\beta) = N_F(\alpha) \cdot N_F(\beta)$ für $\alpha, \beta \in F$).

Satz 1.22

Sei $[F:\mathbb{Q}] = n$ und $\alpha \in F$ mit $[\mathbb{Q}(\alpha):\mathbb{Q}] = d$. Sind $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ die Konjugierten von α über $\mathbb{Q}$ (d.h. die Nullstellen von $m_{\alpha,\mathbb{Q}}(x)$), so gilt:

(i) $T_F(\alpha) = \dfrac{n}{d} \displaystyle\sum_{j=1}^{d} \alpha_j = \frac{n}{d} T_{\mathbb{Q}(\alpha)}(\alpha)$;

(ii) $N_F(\alpha) = \left(\displaystyle\prod_{j=1}^{d} \alpha_j \right)^{n/d} = (N_{\mathbb{Q}(\alpha)}(\alpha))^{n/d}$;

(iii) $m_{\alpha,\mathbb{Q}}(x) = x^d - T_{\mathbb{Q}(\alpha)}(\alpha) \cdot x^{d-1} + \cdots \pm N_{\mathbb{Q}(\alpha)}(\alpha)$.

Beweis:

Seien die Einbettungen $\Theta_1, \ldots, \Theta_d$ von $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ gegeben durch $\Theta_j(\alpha) = \alpha_j$ (und $\Theta_j(q) = q$ für $q \in \mathbb{Q}$). Nach Definition gilt

$$T_{\mathbb{Q}(\alpha)}(\alpha) = \sum_{j=1}^{d} \alpha_j \quad \text{und} \quad N_{\mathbb{Q}(\alpha)}(\alpha) = \prod_{j=1}^{d} \alpha_j \ .$$

Nach Satz 1.19 besitzt jedes Θ_i $(1 \leq i \leq d)$ genau n/d Fortsetzungen zu Einbettungen $\Theta_i^{(j)}$ $(1 \leq j \leq n/d)$ von F in $\mathbb{C}$. Damit folgt

$$T_F(\alpha) = \sum_{i=1}^{d} \sum_{j=1}^{n/d} \Theta_i^{(j)}(\alpha) = \sum_{i=1}^{d} \sum_{j=1}^{n/d} \alpha_i = \frac{n}{d} \sum_{i=1}^{d} \alpha_i = \frac{n}{d} T_{\mathbb{Q}(\alpha)}(\alpha)$$

und

$$N_F(\alpha) = \prod_{i=1}^{d} \prod_{j=1}^{n/d} \Theta_i^{(j)}(\alpha) = \prod_{i=1}^{d} \left(\prod_{j=1}^{n/d} \alpha_i \right) = \left(\prod_{i=1}^{d} \alpha_i \right)^{n/d} = (N_{\mathbb{Q}(\alpha)})^{n/d} \ .$$

Koeffizientenvergleich bei den Potenzen x^{d-1} bzw. x^0 in

$$m_{\alpha,\mathbb{Q}}(x) = \prod_{j=1}^{d} (x - \alpha_j)$$

liefert (iii).

□

Korollar 1.23

Liegt α in einem Zahlkörper F, so sind $T_F(\alpha)$ und $N_F(\alpha)$ rationale Zahlen.

Beweis:

Nach Satz 1.22 (iii) sind $T_F(\alpha)$ und $N_F(\alpha)$ Koeffizienten des Minimalpolynoms $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$, also Elemente von $\mathbb{Q}$.

□

Beispiele:

(i) Sei

$$f(x) = ax^2 + bx + c \quad \in \mathbb{Q}[x]$$

mit $a \neq 0$. Üblicherweise heißt $\Delta := b^2 - 4ac$ die Diskriminante von $f(x)$ und auch Diskriminante des quadratischen Körpers $F = \mathbb{Q}(\sqrt{\Delta})$. Nach p-q-Formel sind die Nullstellen α, α' von $f(x)$ gegeben durch

$$\alpha = \frac{-b + \sqrt{\Delta}}{2a} \quad , \quad \alpha' = \frac{-b - \sqrt{\Delta}}{2a} \ .$$

Es lässt sich leicht zeigen, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$. Also haben wir

$$T_F(\alpha) = T_{\mathbb{Q}(\alpha)}(\alpha) = \alpha + \alpha' = -\frac{b}{a}$$

und

$$N_F(\alpha) = N_{\mathbb{Q}(\alpha)}(\alpha) = \alpha \cdot \alpha' = \frac{b^2 - \Delta}{4a^2} = \frac{c}{a} \ .$$

Damit folgt nach Satz 1.22 (iii)

$$m_{\alpha,\mathbb{Q}}(x) = x^2 - T_F(\alpha) \cdot x + N_F(\alpha) = x^2 + \frac{b}{a}x + \frac{c}{a}$$

(ii) Sei $F = \mathbb{Q}(\zeta_p)$ mit einer primitiven p-ten Einheitswurzel, wobei $p \in \mathbb{P}_{>2}$. Mit Hilfe des Eisenstein-Kriteriums lässt sich leicht nachweisen, dass

$$m_{\zeta_p,\mathbb{Q}}(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

ist ($x^p - 1 = (x-1) \cdot (x^{p-1} + \cdots + x + 1)$ mit irreduziblen Faktoren). Da $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ allesamt primitive p-te Einheitswurzeln sind, haben wir

$$(*) \quad \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{j=1}^{p-1}(x - \zeta_p^j) \ .$$

Wir differenzieren und setzen $x = \zeta_p^i$. Wegen $\zeta_p^p = 1$ erhalten wir

$$(**) \quad \frac{p \cdot \zeta_p^{p-i}}{\zeta_p^i - 1} = \prod_{\substack{j=1 \\ j \neq i}}^{p-1}(\zeta_p^i - \zeta_p^j) \ .$$

Aus $(*)$ mit $x = 0$ bzw. $x = 1$ kommt

$$\prod_{j=1}^{p-1} \zeta_p^j = (-1)^{p-1} \quad \text{bzw.} \quad \prod_{j=1}^{p-1}(1 - \zeta_p^j) = p \ .$$

Durch Produktbildung $\prod_{i=1}^{p-1}(\ldots)$ in $(**)$ bekommen wir nach paarweiser Bündelung

$$\begin{aligned} p^{p-2} &= \prod_{i=1}^{p-1} \prod_{\substack{j=1 \\ j \neq i}}^{p-1}(\zeta_p^i - \zeta_p^j) \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{1 \leq i < j \leq p-1} (\zeta^i - \zeta^j)^2 \ . \end{aligned}$$

Wegen $2 \nmid p$ folgt

$$\prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = (-1)^{\frac{p-1}{2}} p^{p-2} \ .$$

Definition 1.24

Sei $f(x) \in F[x]$ für einen Körper $F \subseteq \mathbb{C}$, wobei $d := \deg f \ge 2$ und

$$f(x) = a \cdot \prod_{j=1}^{d} (x - \alpha_j)$$

für $a \in F$ und gewisse $\alpha_j \in \mathbb{C}$. Dann heißt

$$\operatorname{discr}(f) := a^{2d-2} \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2$$

Diskriminante von f.

Satz 1.25

Sei $F = \mathbb{Q}(\alpha)$ mit $[F : \mathbb{Q}] = d$, und seien $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ die Konjugierten von α über $\mathbb{Q}$. Dann gilt

$$\operatorname{discr}(m_{\alpha,\mathbb{Q}}(x)) = (-1)^{d(d-1)/2} \prod_{j=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_j) = (-1)^{d(d-1)/2} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)) \ ,$$

wobei $m'_{\alpha,\mathbb{Q}}(x)$ die Ableitung von $m_{\alpha,\mathbb{Q}}(x)$ bezeichnet.

Beweis:

Nach Definition ist

$$\operatorname{discr}(m_{\alpha,\mathbb{Q}}) = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2 \ .$$

Wegen

$$m'_{\alpha,\mathbb{Q}}(x) = \sum_{j=1}^{d} \prod_{\substack{i=1 \\ i \ne j}}^{d} (x - \alpha_i)$$

haben wir

$$m'_{\alpha,\mathbb{Q}}(\alpha_j) = \prod_{\substack{i=1 \\ i \ne j}}^{d} (\alpha_j - \alpha_i) \ .$$

Also folgt

$$\begin{aligned} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)) &= \prod_{j=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_j) = \prod_{j=1}^{d} \prod_{\substack{i=1 \\ i\neq j}}^{d} (\alpha_j - \alpha_i) \\ &= (-1)^{\frac{d(d-1)}{2}} \prod_{1\leq i<j\leq d} (\alpha_j - \alpha_i)^2 = (-1)^{\frac{d(d-1)}{2}} \operatorname{discr}(m_{\alpha,\mathbb{Q}}) \ . \end{aligned}$$

□

1.4. Ganzalgebraische Zahlen und Ganzheitsbasen

Wir bezeichnen mit $\mathbb{A} \subseteq \overline{\mathbb{Q}}$ die Menge der ganzalgebraischen Zahlen in $\mathbb{C}$.

Satz 1.26

Sei $\alpha \in \overline{\mathbb{Q}}$. Dann ist $\alpha \in \mathbb{A} \iff m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Außerdem gilt für $\alpha \in \mathbb{A}$, dass $T_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Z}$ und $N_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Z}$.

Beweis:

Sei zunächst $\alpha \in \mathbb{A}$. Nach Definition 1.1 existiert ein Polynom $f(x) \in \mathbb{Z}[x]$ mit führendem Koeffizienten 1 und $f(\alpha) = 0$. Wir können o.B.d.A. annehmen, dass f minimalen Grad besitzt. Nach Satz 1.9 gilt $m_{\alpha,\mathbb{Q}}(x) \mid f(x)$ über $\mathbb{Q}$, d.h.

$$f(x) = m_{\alpha,\mathbb{Q}}(x) \cdot h(x) \quad \text{für } m_{\alpha,\mathbb{Q}}\ ,\ h(x) \in \mathbb{Q}[x]\ .$$

Nach Gauß' Lemma existieren $M(x), H(x) \in \mathbb{Z}[x]$ mit $\deg M = \deg m_{\alpha,\mathbb{Q}}$ und $\deg H = \deg h$ derart, dass $f(x) = M(x) \cdot H(x)$. Wegen der führenden Koeffizienten 1 in $f(x)$ und $m_{\alpha,\mathbb{Q}}(x)$ folgt $M(x) = m_{\alpha,\mathbb{Q}}(x)$, also $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Ist umgekehrt $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, so ist $\alpha \in \mathbb{A}$ nach Definition.
Nach Satz 1.22 (iii) sind $T_{\mathbb{Q}(\alpha)}$ und $N_{\mathbb{Q}(\alpha)}$ Koeffizienten von $m_{\alpha,\mathbb{Q}}(x)$. Da $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ für $\alpha \in \mathbb{A}$, folgt das Gewünschte.

□

Bemerkung:

Wir haben im vorstehenden Beweis auch gezeigt:
Ist $\alpha \in \mathbb{A}$ Nullstelle eines Polynoms $f(x) \in \mathbb{Z}[x]$ mit minimalem Grad und führendem Koeffizienten 1, so ist $f(x)$ irreduzibel über $\mathbb{Q}$.

Wir haben in Korollar 1.11 gesehen, dass $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine $\mathbb{Q}$-Basis des Vektorraums $\mathbb{Q}(\alpha)$ für algebraisches α vom Grad d ist. Entsprechend ist $\alpha \in \mathbb{A}$ gdw. der $\mathbb{Z}$-Modul $\mathbb{Z}[\alpha]$ endlich erzeugt ist.

Satz 1.27

Für $\alpha \in \mathbb{C}$ sind die folgenden Aussagen äquivalent:

(i) $\alpha \in \mathbb{A}$;

(ii) $\mathbb{Z}[\alpha]$ ist als $\mathbb{Z}$-Modul endlich erzeugt ;

(iii) $\alpha \in R$ für einen Ring $R \subseteq \mathbb{C}$, der als $\mathbb{Z}$-Modul endlich erzeugt ist ;

(iv) $\alpha M \subseteq M$ für einen endlich erzeugten $\mathbb{Z}$-Modul $M \subseteq \mathbb{C}$.

Beweis:

(i) $\Longrightarrow$ (ii): Nach Korollar 1.11 ist $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ erzeugt von $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, sofern α algebraisch vom Grad d ist. Also wird insbesondere $\mathbb{Z}[\alpha]$ über $\mathbb{Z}$ von $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ erzeugt.

(ii) $\Longrightarrow$ (iii): Wähle $R := \mathbb{Z}[\alpha]$.

(iii) $\Longrightarrow$ (iv): Wähle $M := R$.

(iv) $\Longrightarrow$ (i): Sei $M = \mathbb{Z}m_1 + \cdots + \mathbb{Z}m_d$. Dann gibt es für $j = 1, \ldots, d$ Koeffizienten $a_{j,i} \in \mathbb{Z}$ mit

$$\alpha m_j = \sum_{i=1}^{d} a_{j,i} m_i \ .$$

Also hat das homogene lineare Gleichungssystem

$$\begin{aligned}
(a_{1,1} - \alpha)x_1 + a_{1,2}x_2 + \cdots + a_{1,d}x_d &= 0 \\
a_{2,1}x_1 + (a_{2,2} - \alpha)x_2 + \cdots + a_{2,d}x_d &= 0 \\
\vdots \qquad\qquad\qquad\qquad\qquad &\ \ \vdots \\
a_{d,1}x_1 + a_{d,2}x_2 + \cdots + (a_{d,d} - \alpha)x_d &= 0
\end{aligned}$$

eine nichttriviale Lösung (nämlich $x_j = m_j$ für $1 \leq j \leq d$). Also gilt für die $(d \times d)$-Matrix

$$A := \begin{pmatrix}
a_{1,1} - \alpha & a_{1,2} & \ldots & a_{1,d} \\
a_{2,1} & a_{2,2} - \alpha & \ldots & a_{2,d} \\
\vdots & \vdots & & \vdots \\
a_{d,1} & a_{d,2} & \ldots & a_{d,d} - \alpha
\end{pmatrix} ,$$

dass $\det A = 0$. Entwickeln wir $\det A$, so entsteht ein Poylnom aus $\mathbb{Z}[\alpha]$ mit höchstem Term $\pm\alpha^d$, und somit ist α ganzalgebraisch.

□

Korollar 1.28

$\mathbb{A}$ ist ein Unterring von $\overline{\mathbb{Q}}$.

Beweis:

Es genügt, die Abgeschlossenheit von $\mathbb{A}$ bezüglich Addition und Multiplikation zu zeigen. Seien also $\alpha, \beta \in \mathbb{A}$. Nach Satz 1.27 (ii) sind $\mathbb{Z}[\alpha]$ und $\mathbb{Z}[\beta]$ beide endlich erzeugte $\mathbb{Z}$-Moduln; genauer: Sind

$$\mathbb{Z}[\alpha] = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_k \quad , \quad \mathbb{Z}[\beta] = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_l \ ,$$

so ist

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=1}^{k} \sum_{j=1}^{l} \mathbb{Z}\alpha_i\beta_j \ .$$

Wegen $\alpha + \beta,\ \alpha \cdot \beta \in \mathbb{Z}[\alpha, \beta]$ sind nach Satz 1.27 (iii) $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch. Es lässt sich mühelos zeigen, dass für einen algebraischen Zahlkörper F der Durchschnitt $F \cap \mathbb{A}$ ein (Unter-)Ring in F ist.

□

Definition 1.29

Sei $F \subseteq \mathbb{C}$ ein algebraischer Zahlkörper. Dann heißt $\mathcal{O}_F := F \cap \mathbb{A}$ *Ring der ganz(algebraisch)en Zahlen in F.*

Nach Satz 1.26 besteht $\mathcal{O}_F$ aus allen algebraischen Zahlen $\alpha \in \overline{\mathbb{Q}} \cap F$ derart, dass $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Im Spezialfall $F = \mathbb{Q}$ haben wir

Korollar 1.30

Der Ring der ganzen Zahlen in $\mathbb{Q}$ ist $\mathcal{O}_{\mathbb{Q}} := \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Beweis:

Für $\alpha \in \mathbb{A} \cap \mathbb{Q}$ ist $m_{\alpha,\mathbb{Q}}(x) = x - \alpha$, wobei nach Satz 1.26 gilt $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$. Also folgt $\alpha \in \mathbb{Z}$. Offensichtlich ist $\mathbb{Z} \subseteq \mathbb{A} \cap \mathbb{Q}$.

□

Wir sprechen von $\mathbb{Q}$ als dem (speziellen) rationalen Zahlkörper und von $\mathbb{Z}$ als dem Ring der ganzrationalen Zahlen – im Gegensatz zu ganzen Zahlen in beliebigen Zahlkörpern.
Als Verfeinerung des Satzes vom primitiven Element gilt

Satz 1.31

Zu einem algebraischen Zahlkörper F existiert ein $\alpha \in \mathbb{A}$ mit $F = \mathbb{Q}(\alpha)$.

Beweis:

Nach Satz 1.15 gibt es ein $\beta \in \overline{\mathbb{Q}}$ mit $F = \mathbb{Q}(\beta)$. Sei

$$m_{\beta,\mathbb{Q}}(x) = x^d + \sum_{j=0}^{d-1} q_j x^j \ \in \ \mathbb{Q}[x] \ .$$

Sei b der Hauptnenner der Zahlen q_j, also $b \cdot q_j \in \mathbb{Z}$ für $0 \leq j < d$. Dann ist

$$b^d \cdot m_{\beta,\mathbb{Q}}(x) = (bx)^d + \sum_{j=0}^{d-1} b^{d-j} q_j (bx)^j \ \in \ \mathbb{Z}[x]$$

und

$$f(x) := x^d + \sum_{j=0}^{d-1} b^{d-j} q_j \cdot x^j \ \in \ \mathbb{Z}[x]$$

besitzt die Nullstellen $b\beta$. Also ist $\alpha := b\beta \in \mathbb{A}$, und offenbar gilt $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = F$.

□

Nach dem Satz vom primitiven Element (bzw. nach Satz 1.31) besitzt jeder Zahlkörper die Darstellung $F = \mathbb{Q}(\alpha)$ für ein $\alpha \in \overline{\mathbb{Q}}$ (bzw. $\alpha \in \mathbb{A}$) vom Grad $d \in \mathbb{N}$. Nach Korollar 1.11 ist dann $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine $\mathbb{Q}$-Basis des Vektorraums F über $\mathbb{Q}$. Da $\mathcal{O}_F$ ein $\mathbb{Z}$-Modul ist, liegt die Frage nach einer $\mathbb{Z}$-Basis auf der Hand.

Definition 1.32

Eine $\mathbb{Z}$-Basis des Ganzzahlrings $\mathcal{O}_F$ (über $\mathbb{Z}$) in einem Zahlkörper F heißt *Ganzheitsbasis von F*.

Es ist leicht zu zeigen, dass jede Ganzheitsbasis eines Zahlkörpers F auch eine $\mathbb{Q}$-Basis von F ist. Das folgende Beispiel belegt, dass die Umkehrung im Allgemeinen falsch ist: Nicht jede $\mathbb{Q}$-Basis von F, die aus ganzalgebraischen Zahlen besteht, ist notwendig eine Ganzheitsbasis von F.

Beispiel:
Sei $F = \mathbb{Q}(\sqrt{13}) = \{a + b\sqrt{13} : \ a, b \in \mathbb{Q}\}$. Die Zahl $\alpha := \frac{1}{2}(1 + \sqrt{13})$ hat das Minimalpolynom

$$m_{\alpha,\mathbb{Q}}(x) = x^2 - x - 3 \ \in \mathbb{Z}[x] \ ,$$

also ist $\alpha \in \mathcal{O}_F = F \cap \mathbb{A}$. Selbstverständlich ist $1, \sqrt{13}$ eine $\mathbb{Q}$-Basis von F, wobei 1 und $\sqrt{13}$ ganzalgebraisch sind ($x^2 - 13 \ \in \mathbb{Z}[x]$). Trotzdem ist $1, \sqrt{13}$ keine Ganzheitsbasis von F, denn $\alpha \notin \mathbb{Z} + \mathbb{Z}\sqrt{13}$. Es lässt sich nachrechnen, dass $\mathcal{O}_F = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{13})]$.

Definition 1.33

Sei $F = \mathbb{Q}(\alpha)$ algebraischer Zahlkörper mit $[F : \mathbb{Q}] = d$. Ist $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ eine $\mathbb{Q}$-Basis von F und sind $\Theta_1, \ldots, \Theta_d$ die Einbettungen von F in $\mathbb{C}$, so heißt

$$\operatorname{discr}(\mathcal{B}) := \det(\Theta_j(\alpha_i))^2_{\substack{1\le i\le d\\ 1\le j\le d}}$$

Diskriminante der Basis $\mathcal{B}$. Für eine spezielle Basis $\mathcal{B}$ der Form

$$\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$$

heißt $\det(\Theta_j(\alpha^{j-1}))_{\substack{1\le i\le d\\ 1\le j\le d}}$ Vandermonde-Determinante. Mittels Induktion lässt sich leicht zeigen

Lemma 1.34

Die Vandermondsche-Determinante hat den Wert

$$\det(\Theta_j(\alpha^{j-1}))_{\substack{1\le i\le d\\ 1\le j\le d}} = \prod_{1\le i<j\le d} (\alpha_i - \alpha_j) \ ,$$

wobei $\alpha_i := \Theta_i(\alpha)$ die i-te Konjugierte von α ist.

Satz 1.35

Seien $\mathcal{B}_1 := \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ und $\mathcal{B}_2 := \{\beta_1, \beta_2, \ldots, \beta_d\}$ zwei $\mathbb{Q}$-Basen eines algebraischen Zahlkörpers F. Dann gilt

$$\operatorname{discr}(\mathcal{B}_2) = D^2 \cdot \operatorname{discr}(\mathcal{B}_1) \ ,$$

wobei $D = \det(q_{i,k})_{\substack{1\le i\le d\\ 1\le k\le d}}$ für die Darstellungen

$$\beta_k = \sum_{i=1}^{d} q_{i,k}\alpha_i \quad (k = 1, \ldots, d;\ q_{i,k} \in \mathbb{Q}) \ .$$

Beweis:

Seien $\Theta_1, \ldots, \Theta_d$ die Einbettungen von F in $\mathbb{C}$. Damit gilt

$$\Theta_j(\beta_k) = \sum_{i=1}^{d} q_{i,k}\Theta_j(\alpha_i) \quad (j = 1, \ldots, d;\ k = 1, \ldots, d) \ .$$

$$\begin{pmatrix} \Theta_1(\beta_1) & \cdots & \Theta_d(\beta_1) \\ \vdots & & \vdots \\ \Theta_1(\beta_d) & \cdots & \Theta_d(\beta_d) \end{pmatrix} = \begin{pmatrix} q_{1,1} & \cdots & q_{1,d} \\ \vdots & & \vdots \\ q_{d,1} & \cdots & q_{d,d} \end{pmatrix} \cdot \begin{pmatrix} \Theta_1(\alpha_1) & \cdots & \Theta_d(\alpha_1) \\ \vdots & & \vdots \\ \Theta_1(\alpha_d) & \cdots & \Theta_d(\alpha_d) \end{pmatrix} ,$$

also durch quadrieren der Determinanten

$$\operatorname{discr}(\mathcal{B}_2) = D^2 \cdot \operatorname{discr}(\mathcal{B}_1) \ .$$

□

Beispiel:

Sei $F = \mathbb{Q}(\sqrt{13})$, und seien $\alpha = \frac{1}{2}(1 + \sqrt{13})$, $\beta = \sqrt{13}$. Dann sind $\mathcal{B}_1 = \{1, \alpha\}$ und $\mathcal{B}_2 = \{1, \beta\}$ $\mathbb{Q}$-Basen von F (aber $\mathcal{B}_2$ ist keine Ganzheitsbasis von F). Die Einbettungen vo F in $\mathbb{C}$ sind

$$\Theta_1 : \sqrt{13} \longmapsto \sqrt{13} \quad \text{und} \quad \Theta_2 : \sqrt{13} \longmapsto -\sqrt{13} \ .$$

Wir haben

$$\operatorname{discr}(\mathcal{B}_2) = \det \begin{pmatrix} \Theta_1(1) & \Theta_2(1) \\ \Theta_1(\sqrt{13}) & \Theta_2(\sqrt{13}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 \\ \sqrt{13} & -\sqrt{13} \end{pmatrix}^2 = 52$$

und

$$\begin{aligned} \operatorname{discr}(\mathcal{B}_1) &= \det \begin{pmatrix} \Theta_1(1) & \Theta_2(1) \\ \Theta_1(\frac{1}{2}(1+\sqrt{13})) & \Theta_2(\frac{1}{2}(1+\sqrt{13})) \end{pmatrix}^2 \\ &= \det \begin{pmatrix} 1 & 1 \\ \frac{1}{2}(1+\sqrt{13}) & \frac{1}{2}(1-\sqrt{13}) \end{pmatrix}^2 = 13. \end{aligned}$$

Also $\operatorname{discr}(\mathcal{B}_2) = 2^2 \cdot \operatorname{discr}(\mathcal{B}_1)$. Wegen

$$\beta_1 = 1 = 1 \cdot 1 + 0 \cdot \alpha \quad , \quad \beta_2 = \sqrt{13} = -1 \cdot 1 + 2 \cdot \frac{1}{2}(1 + \sqrt{13})$$

haben wir

$$D = 2 = \det \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} .$$

Satz 1.36

Ist $\mathcal{B} = \{\alpha_1, \ldots, \alpha_d\}$ eine $\mathbb{Q}$-Basis eines algebraischen Zahlkörpers F, so gilt

$$\Delta := \operatorname{discr}(\mathcal{B}) = \det(T_F(\alpha_i\alpha_j))_{\substack{1\le i\le d \\ 1\le j\le d}} \in \mathbb{Q}$$

und $\Delta \neq 0$. Ist F total-reell, so ist $\Delta > 0$.

Beweis:

Die Rechenregeln für Determinanten ergeben

$$\begin{aligned} \Delta &= \det(\Theta_j(\alpha_i))^2 = \det(\Theta_j(\alpha_i)) \cdot \det\left((\Theta_j(\alpha_i))^t\right) \\ &= \det(\Theta_j(\alpha_i)) \cdot \det(\Theta_i(\alpha_j)) = \det((\Theta_j(\alpha_i)) \cdot (\Theta_i(\alpha))) \\ &= \det\left(\sum_{k=1}^{d} \Theta_k(\alpha_i\alpha_j)\right) = \det(T_F(\alpha_i\alpha_j)) . \end{aligned}$$

Nach Korollar 1.23 sind alle $T_F(\alpha_i\alpha_j)$ mit $1 \le i, j \le d$ rational, also $\Delta \in \mathbb{Q}$.
Nach dem Satz vom primitiven Element existiert ein $\alpha \in F$ mit $F = \mathbb{Q}(\alpha)$. Damit ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\} =: \mathcal{B}'$ $\mathbb{Q}$-Basis von F. Nach Lemma 1.34 folgt

$$\operatorname{discr}(\mathcal{B}') = \prod_{1\le i<j\le d} (\Theta_i(\alpha) - \Theta_j(\alpha))^2$$

für die Einbettungen $\Theta_1, \ldots, \Theta_d$ von F in $\mathbb{C}$. Dies impliziert

(i) $\operatorname{discr}(\mathcal{B}') \neq 0$;

(ii) $\operatorname{discr}(\mathcal{B}') > 0$ für F total-reell.

Da für $D = \det(q_{i,k})$ in Satz 1.35 gilt $D \neq 0$ (Basistransformationen sind invertierbar), folgt wegen $D \in \mathbb{Q}$, dass $D^2 > 0$. Wenden wir nun Satz 1.35 mit $\mathcal{B}_1 := \mathcal{B}'$ und $\mathcal{B}_2 := \mathcal{B}$ an, so haben wir sofort $\Delta \neq 0$ wegen (i) und $\Delta > 0$ für total-reelles F wegen (ii).

□

Korollar 1.37

Ist $\mathcal{B}$ eine $\mathbb{Q}$-Basis von F mit $\mathcal{B} \subseteq \mathcal{O}_F$, so ist $\operatorname{discr}(\mathcal{B}) \in \mathbb{Z}$.

Beweis:

Die Behauptung folgt aus Satz 1.36 sofort mit Hilfe von Satz 1.26.

□

Korollar 1.38

Sei $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ eine $\mathbb{Q}$-Basis von F. Ist $\mathcal{B}_2 = \{\beta_1, \beta_2, \ldots, \beta_d\} \subseteq F$ mit

$$\beta_k = \sum_{i=1}^{d} q_{i,k}\alpha_i \quad (k = 1, \ldots, d;\ q_{i,k} \in \mathbb{Q}) \ ,$$

so gilt: $\mathcal{B}_2$ ist $\mathbb{Q}$-Basis von $F \iff \det(q_{i,k}) \neq 0$.

Beweis:

„$\Longrightarrow$“

Sei $\mathcal{B}_2$ $\mathbb{Q}$-Basis von F. Nach Satz 1.35 ist

$$\operatorname{discr}(\mathcal{B}_2) = D^2 \cdot \operatorname{discr}(\mathcal{B}_1)$$

mit $D = \det(q_{i,k})$. Nach Satz 1.36 ist $\operatorname{discr}(\mathcal{B}_2) \neq 0$, also auch $D \neq 0$.

„$\Longleftarrow$“

Sei $\det(q_{i,k}) \neq 0$. Wir haben zu zeigen, dass $\beta_1, \beta_2, \ldots, \beta_d$ linear unabhängig über $\mathbb{Q}$ sind. Die Annahme $\gamma_1\beta_1 + \cdots + \gamma_d\beta_d = 0$ für gewisse $\gamma_i \in \mathbb{Q}$ impliziert

$$0 = \sum_{k=1}^{d} \gamma_k\beta_k = \sum_{k=1}^{d} \gamma_k \sum_{i=1}^{d} q_{i,k}\alpha_i = \sum_{i=1}^{d} \alpha_i \sum_{k=1}^{d} \gamma_k \cdot q_{i,k} \ .$$

Wegen der linearen Unabhängigkeit der α_i folgt

$$\sum_{k=1}^{d} \gamma_k \cdot q_{i,k} = 0 \quad (1 \leq i \leq d) \ .$$

Wegen $\det(q_{i,k}) \neq 0$ hat dieses homogene lineare GLeichungssystem nur die triviale Lösung $\gamma_1 = \ldots = \gamma_d = 0$.

□

Satz 1.39

Jeder algebraische Zahlkörper F mit $[F : \mathbb{Q}] = d$ besitzt eine Ganzheitsbasis und $\mathcal{O}_F$ ist eine freie abelsche Gruppe vom Rang d (d.h. $\mathcal{O}_F = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_d$ für geeignete $\beta_j \in \mathcal{O}_F$).

Beweis:

Nach Satz 1.31 existiert ein $\alpha \in \mathcal{O}_F = F \cap \mathbb{A}$ mit $F = \mathbb{Q}(\alpha)$. Insbesondere ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\} \subseteq \mathcal{O}_F$ eine $\mathbb{Q}$-Basis von F. Es ist zu zeigen, dass in der nichtleeren Menge aller solcher $\mathbb{Q}$-Basen von F mindestens eine ist, die gleichzeitig eine $\mathbb{Z}$-Basis von $\mathcal{O}_F$ bildet. Nach Korollar 1.37 und Satz 1.36 wissen wir, dass deren Diskriminante in $\mathbb{Z} \setminus \{0\}$ liegt.

Sei also $\mathcal{B}_1 = \{\beta_1, \beta_2, \ldots, \beta_d\} \subseteq \mathcal{O}_F$ eine $\mathbb{Q}$-Basis von F, wobei $|\mathrm{discr}\,(\mathcal{B}_1)|$ minimal sei unter allen derartigen Basen.

Annahme: $\mathcal{B}_1$ ist keine $\mathbb{Z}$-Basis von $\mathcal{O}_F$.

Dann existiert ein $\gamma \in \mathcal{O}_F$ derart, dass

$$\gamma = \sum_{j=1}^{d} q_j \beta_j \quad (q_j \in \mathbb{Q})$$

mit mindestens einem $q_j \notin \mathbb{Z}$. O.B.d.A. sei $q_1 \notin \mathbb{Z}$, d.h. $q_1 = [q_1] + r$ für ein $0 < r < 1$.

Sei

$$\delta := \gamma - [q_1]\beta_1 = \sum_{j=1}^{d} q_j \beta_j - [q_1]\beta_1 = r\beta_1 + \sum_{j=2}^{d} q_j \beta_j \ \in \mathcal{O}_F \ .$$

Die Matrix

$$A = \begin{pmatrix} r & q_2 & q_3 & \cdots & q_d \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 \end{pmatrix}$$

hat die Determinante $\det A = r \neq 0$. Nach Korollar 1.38 ist auch

$$\mathcal{B}_2 = \{\delta, \beta_2, \beta_3, \ldots, \beta_d\} \subseteq \mathcal{O}_F$$

eine $\mathbb{Q}$-Basis von F. Nach Satz 1.35 haben wir $\operatorname{discr}(\mathcal{B}_2) = r^2 \cdot \operatorname{discr}(\mathcal{B}_1)$, also

$$|\operatorname{discr}(\mathcal{B}_2)| < |\operatorname{discr}(\mathcal{B}_1)| \ .$$

Dieser Widerspruch zur Minimalität von $|\operatorname{discr}(\mathcal{B}_2)|$ beweist, dass $\mathcal{B}_1$ $\mathbb{Z}$-Basis von $\mathcal{O}_F$ ist, d.h. als $\mathbb{Z}$-Modul haben wir

$$\mathcal{O}_F = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_d \ .$$

□

Korollar 1.40

Ist $\mathcal{B} \subseteq \mathcal{O}_F$ eine Basis von F über $\mathbb{Q}$ und ist $\operatorname{discr}(\mathcal{B})$ quadratfrei, so ist $\mathcal{B}$ eine Ganzheitsbasis von F.

Beweis:

Sei $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_d\} \subseteq \mathcal{O}_F$. Nach Satz 1.39 besitzt F eine Ganzheitsbasis $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$. Nach Satz 1.35 gilt

$$\operatorname{discr}(\mathcal{B}) = D^2 \cdot \operatorname{discr}(\mathcal{B}_1) \ ,$$

wobei $D = \det(q_{i,k})$ mit $q_{i,k} \in \mathbb{Z}$ definiert durch

$$(*) \quad \beta_k = \sum_{i=1}^{d} q_{i,k}\alpha_i \quad (k = 1, \ldots, d) \ .$$

Nach Korollar 1.37 sind $\mathrm{discr}\,(\mathcal{B}) \in \mathbb{Z}$ und $\mathrm{discr}\,(\mathcal{B}_1) \in \mathbb{Z}$. Da $\mathrm{discr}\,(\mathcal{B})$ quadratfrei nach Voraussetzung ist, folgt mit $D \in \mathbb{Z}$, dass $D = \pm 1$. Matrizen $(q_{i,k})$ mit Determinante ± 1 heißen unimodular und besitzen bekanntlich eine Inverse über $\mathbb{Z}$ ($(q_{i,k}) \in GL_n(\mathbb{Z})$). Also folgt aus $(*)$ für geeignete $q'_{i,k} \in \mathbb{Z}$

$$\alpha_k = \sum_{i=1}^{d} q'_{i,k}\beta_i \quad (k = 1, \ldots, d) \ .$$

Damit ist auch $\mathcal{B}$ Ganzheitsbasis von F.

□

Bemerkung:

Die Umkehrung des Korollars gilt im Allgemeinen nicht:

$\mathcal{B} = \{1, \sqrt{2}\}$ ist Ganzheitsbasis von $\mathbb{Q}(\sqrt{2})$, aber $\mathrm{discr}\,(\mathcal{B}) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}^2$ $= (-2\sqrt{2})^2 = 8$ ist nicht quadratfrei.

Korollar 1.41

Für zwei Ganzheitsbasen $\mathcal{B}_1$ und $\mathcal{B}_2$ eines algebraischen Zahlkörpers F gilt

$$\mathrm{discr}\,(\mathcal{B}_1) = \mathrm{discr}\,(\mathcal{B}_2) \ .$$

Beweis:

Nach Satz 1.35 haben wir

$$(*) \quad \mathrm{discr}\,(\mathcal{B}_2) = D^2 \cdot \mathrm{discr}\,(\mathcal{B}_1)$$

für das dort ausgegebene D, in unserer Situation $D \in \mathbb{Z}$. Da nach Korollar 1.37 auch die beiden Diskriminanten ganzrational sind, folgt $\mathrm{discr}\,(\mathcal{B}_1) \mid \mathrm{discr}\,(\mathcal{B}_2)$. Durch Vertauschen der Rollen ergibt sich auf die gleiche Weise $\mathrm{discr}\,(\mathcal{B}_2) \mid \mathrm{discr}\,(\mathcal{B}_1)$. Also

$$\mathrm{discr}\,(\mathcal{B}_1) = \pm \mathrm{discr}\,(\mathcal{B}_2) \ ,$$

wobei das Minuszeichen wegen $(*)$ nicht möglich ist.

□

Das vorstehende Korollar besagt im Wesentlichen, dass die Diskriminante einer Ganzheitsbasis eines Zahlkörpers F eine Invariante von F ist.

Definition 1.42

Sei $\mathcal{B}$ irgendeine Ganzheitsbasis eines algebraischen Zahlkörpers F. Dann heißt $\Delta_F := \operatorname{discr}(\mathcal{B})$ *Diskriminante von* F (und hängt nach Korollar 1.41 nicht von der gewählten Ganzheitsbasis $\mathcal{B}$ ab).

Satz 1.43

Sei $D \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei, und sei $F := \mathbb{Q}(\sqrt{D})$; dabei heißt D Radikand von F. Dann gilt

$$\Delta_F = \begin{cases} D & \text{für} \quad D \equiv 1 \bmod 4, \\ 4D & \text{für} \quad D \equiv 2,3 \bmod 4, \end{cases}$$

und

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{D})\right] & \text{für} \quad \Delta_F \equiv D \equiv 1 \bmod 4, \\ \mathbb{Z}[\sqrt{D}] & \text{für} \quad \Delta_F \equiv 0 \bmod 4 \ \ (\Longleftrightarrow D \equiv 2,3 \bmod 4). \end{cases}$$

Beweis:

Wegen $[F:\mathbb{Q}] = 2$ hat $\mathcal{O}_F$ eine Ganzheitsbasis der Gestalt $\{1, \alpha\}$ für ein

$$\alpha = \frac{a + b\sqrt{D}}{c} \ \in F$$

mit $\operatorname{ggT}(a,b,c) = 1$ und $a,b,c \in \mathbb{Z},\ c > 0$. Ist $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ eine Basis, so haben wir nach Definition und Lemma 1.34 (mit $\alpha_j := \Theta_j(\alpha)$)

$$\begin{aligned} \operatorname{discr}(\mathcal{B}) &= \det(\Theta_j(\alpha^{i-1}))^2 = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2 \\ &= \operatorname{discr}(m_{\alpha,\mathbb{Q}}) \ . \end{aligned}$$

In unserem Fall folgt mit Satz 1.25

$$\Delta_F = \operatorname{discr}(m_{\alpha,\mathbb{Q}}) = -m'_{\alpha,\mathbb{Q}}(\alpha) \cdot m'_{\alpha,\mathbb{Q}}(\overline{\alpha}) \ ,$$

wobei $\overline{\alpha} := \dfrac{a - b\sqrt{D}}{c}$. Wegen $m'_{\alpha,\mathbb{Q}}(x) = 2x - T_F(\alpha)$ erhalten wir

$$\begin{aligned}\Delta_F &= -(2\alpha - T_F(\alpha))(2\overline{\alpha} - T_F(\alpha)) \\ &= -4\alpha\overline{\alpha} + 2(\alpha + \overline{\alpha})T_F(\alpha) - T_F(\alpha)^2 \\ &= 4\left(\frac{-a^2 + b^2 D}{c^2}\right) + 2\left(\frac{2a}{c}\right)^2 - \left(\frac{2a}{c}\right)^2 = \frac{4b^2 D}{c^2} \in \mathbb{Z} ,\end{aligned}$$

wobei $\Delta_F \in \mathbb{Z}$ nach Korollar 1.37 gilt. Nach Satz 1.26 wisssen wir außerdem, dass

$$T_F(\alpha) = \frac{2a}{c} \in \mathbb{Z} \quad \text{und} \quad N_F(\alpha) = \frac{a^2 - b^2 D}{c^2} \in \mathbb{Z} .$$

Behauptung: $c \in \{1, 2\}$.

Hätte c einen Primteiler $p \geq 3$, so folgte wegen $T_F(\alpha) \in \mathbb{Z}$, dass $p \mid a$. Wegen D quadratfrei und $N_F(\alpha) \in \mathbb{Z}$ hätten wir auch $p \mid b$, also $p \mid (a, b, c)$ im Widerspruch zur Voraussetzung $(a, b, c) = 1$. Also bleibt nur $c = 2^j$ für ein $j \in \mathbb{N}_0$. Für $j \geq 2$ bekämen wir mit der vorstehenden Argumentation $2 \mid (a, b, c)$. Also gilt die Behauptung.

1. Fall: $D \not\equiv 1 \bmod 4$ (d.h. $D \equiv 2, 3 \bmod 4$).

Für $c = 2$ hätten wir $\Delta_F = b^2 D$. Wegen $(a, b, c) = 1$ implizierte $N_F(\alpha) \in \mathbb{Z}$ dann $2 \nmid ab$ (D quadratfrei!). Somit

$$1 \equiv a^2 \equiv b^2 D \equiv D \bmod 4 \quad \text{Widerspruch! } (D \not\equiv 1 \bmod 4) .$$

Es bleibt nur $c = 1$. Wie im ersten Teil des Beweises folgt mit Satz 1.25

$$4b^2 D = \Delta_F = \operatorname{discr}(m_{\sqrt{D},\mathbb{Q}}) = -(2\sqrt{D}) \cdot (-2\sqrt{D}) = 4D .$$

Es ergibt sich $b = \pm 1$, o.B.d.A. $b = 1$. Damit haben wir

$$\mathcal{O}_F = \mathbb{Z}[a + \sqrt{D}] = \mathbb{Z}[\sqrt{D}] .$$

2. Fall: $D \equiv 1 \bmod 4$.

Die Situation $c = 1$ kann nicht auftreten, denn $\beta := \frac{1}{2}(1 + \sqrt{D}) \in F$ hat das Minimalpolynom

$$m_{\beta,\mathbb{Q}}(x) = x^2 - x + \frac{1 - D}{4} \in \mathbb{Z}[x] ,$$

also $\beta \in \mathcal{O}_F = \mathbb{Z}[\alpha] = \mathbb{Z}[a + b\sqrt{D}]$. Widerspruch!

Es bleibt $c = 2$ und wegen

$$\frac{a + b\sqrt{D}}{2} = \frac{a - b}{2} + b\left(\frac{1}{2}(1 + \sqrt{D})\right)$$

(mit $(a - b)/2 \in \mathbb{Z}$ wegen $2 \nmid ab$ (s.o.)) erhalten wir

$$\mathcal{O}_F = \mathbb{Z}[\alpha] = \mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{D})\right] .$$

Schließlich kommt analog zum 1. Fall

$$\Delta_F = \operatorname{discr}(m_{\beta,\mathbb{Q}}) = -(\sqrt{D})(-\sqrt{D}) = D .$$

□

Bemerkungen:

(i) Aufgrund von Satz 1.43 haben wir

$$F := \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{\Delta_F}) .$$

(ii) Bei quadratischen Zahlkörpern F haben wir stets $\mathcal{O}_F = \mathbb{Z}[\alpha]$ für ein geeignetes α. Für Zahlkörper höheren Grades ist dies im Allgemeinen falsch. Man kann z.B. zeigen, dass für $F = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$ gilt: $\mathcal{O}_F \neq \mathbb{Z}[\beta]$ für alle $\beta \in \mathcal{O}_F$. Während also nach dem Satz vom primitiven Element stets eine $\mathbb{Q}$-Basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ zu einem Zahlkörper F vom Grad d existiert, gibt es im Allgemeinen keine derartigen Ganzheitsbasen.

Aus Satz 1.43 folgt, dass für quadratische Zahlkörper F stets $\Delta_F \equiv 0, 1 \bmod 4$ ist. Dies gilt allgemein.

Satz 1.44 (Kriterium von Stickelberger)

Für jeden algebraischen Zahlkörper F haben wir

$$\Delta_F \equiv 0, 1 \bmod 4 .$$

Beweis: (I. Schur)

Sei $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ eine Ganzheitsbasis von F mit $[F : \mathbb{Q}] = n$.Wir bezeichnen mit $\alpha_k^{(j)} \quad (j = 1, \ldots, n)$ die Konjugierten von $\alpha_k^{(1)} := \alpha_k \quad (k = 1, \ldots, n)$. Nach Definition haben wir $\sqrt{\Delta_F} = \det\left(\alpha_k^{(j)}\right)_{\substack{k=1,\ldots,n \\ j=1,\ldots,n}}$. Aus der Linearen Algebra ist bekannt

$$\begin{aligned} \det\left(\alpha_k^{(j)}\right) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \alpha_1^{(\sigma(1))} \cdot \alpha_2^{(\sigma(2))} \cdot \ldots \cdot \alpha_n^{(\sigma(n))} \\ &= \sum_{\sigma \in A_n} \alpha_1^{(\sigma(1))} \cdot \ldots \cdot \alpha_n^{(\sigma(n))} - \sum_{\sigma \notin A_n} \alpha_1^{(\sigma(1))} \cdot \ldots \cdot \alpha_n^{(\sigma(n))} \\ &=: \mathcal{G} - \mathcal{U} \ , \end{aligned}$$

wobei S_n die symmetrische Gruppe der Ordnung $n!$ (S_n = Menge aller Permutationen von $\{1, 2, \ldots, n\}$) und A_n die alternierende Gruppe der Ordnung $\frac{1}{2}n!$ (A_n = Menge aller geraden Permutationen von $\{1, 2, \ldots, n\}$) bezeichnen. Offenbar sind $\mathcal{G}, \mathcal{U} \in \mathbb{A}$. Außerdem sind $\mathcal{G} + \mathcal{U}$ und $\mathcal{G} \cdot \mathcal{U}$ symmetrische Ausdrücke in den $\alpha_1, \alpha_2, \ldots, \alpha_n$ (das Vertauschen von $\alpha_i \longleftrightarrow \alpha_j$ führt nur zu einer Änderung der Reihenfolge der Summanden von $\mathcal{G}$ bzw. $\mathcal{U}$ oder zu einem Tausch der Rollen von $\mathcal{G}$ und $\mathcal{U}$). Nach dem Satz über elementarsymmetrische Funktionen sind somit $\mathcal{G} + \mathcal{U}$ und $\mathcal{G} \cdot \mathcal{U}$ aus dem Grundkörper von F, d.h. $\mathcal{G} + \mathcal{U}$, $\mathcal{G} \cdot \mathcal{U} \ \in \mathbb{Q}$. Nach Korollar 1.30 folgt $\mathcal{G} + \mathcal{U}$, $\mathcal{G} \cdot \mathcal{U} \ \in \mathbb{Z}$. Es ergibt sich

$$\begin{aligned} \Delta_F &= (\mathcal{G} - \mathcal{U})^2 = (\mathcal{G} + \mathcal{U})^2 - 4\mathcal{G} \cdot \mathcal{U} \\ &\equiv (\mathcal{G} + \mathcal{U})^2 \equiv 0, 1 \bmod 4 \ . \end{aligned}$$

□

Nach Satz 1.36 ist $\Delta_f > 0$ für total-reelles F. Allgemeiner gilt

Satz 1.45 (von Kronecker)

Ist F ein algebraischer Zahlkörper mit Signatur $\{r_1, r_2\}$, so ist das Vorzeichen von Δ_F gleich $(-1)^{r_2}$.

Beweis:

Sei $[F : \mathbb{Q}] = n$ und $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ eine Ganzheitsbasis von F. Mit den Bezeichnungen aus dem vorangehenden Beweis ist $\Delta_F = \det\left(\alpha_k^{(j)}\right)^2$, wobei

$$\det\left(\alpha_k^{(j)}\right) = a + bi \quad \in \mathbb{C}$$

mit gewissen $a, b \in \mathbb{R}$ und $i = \sqrt{-1}$. Vertauschen wir in $\det\left(\alpha_k^{(j)}\right)$ die r_2 Paare von Zeilen mit komplexen Einbettungen und den jeweiligen konjugierten Einbettungen, so wird in der Entwicklung der Determinante offenbar jeder Imaginärteil durch sein Negatives ersetzt. Es entsteht also der Wert $a - bi$. Andererseits liefert das Vertauschen von r_2 Paaren von Zeilen in $\det\left(\alpha_k^{(j)}\right)$ den Wert $(-1)^{r_2} \cdot \det\left(\alpha_k^{(j)}\right)$. Es folgt

$$a - bi = (-1)^{r_2} \det\left(\alpha_k^{(j)}\right) = (-1)^{r_2}(a + bi) \ .$$

Für $2 \mid r_2$ ergibt sich $b = 0$, also $\Delta_F = a^2 > 0$. Für $2 \nmid r_2$ kommt $a = 0$, also $\Delta_F = (bi)^2 = -b^2 < 0$.

□

1.5. Faktorisierung und Teilbarkeit

Es lässt sich leicht zeigen, dass in einem kommutativen Ring R mit Einselement die Einheiten (d.h. die multiplikativ invertierbaren Elemente) eine multiplikative (Unter-)Gruppe $\mathcal{U}_R$ bilden. Wir bezeichnen mit $\langle g \rangle$ die von einem Element g einer Gruppe erzeugte zyklische (Unter-)Gruppe.

Satz 1.46

Ist $\Delta_F < 0$ für den komplexen quadratischen Zahlkörper $F = \mathbb{Q}(\sqrt{\Delta_F})$, so gilt für die Einheitengruppe

$$\mathcal{U}_F := \mathcal{U}_{\mathcal{O}_F} = \begin{cases} \langle \zeta_6 \rangle := \left\langle \frac{1}{2}(1 - i\sqrt{3}) \right\rangle & \text{für } \Delta_F = -3 \ , \\ \langle \zeta_4 \rangle := \langle i \rangle & \text{für } \Delta_F = -4 \ , \\ \langle \zeta_2 \rangle := \langle -1 \rangle & \text{sonst .} \end{cases}$$

Beweis:

Sei $u = a + b\sqrt{D} \ \in \mathcal{U}_F$, wobei $2a, 2b \in \mathbb{Z}$ und D ist der Radikand von F (d.h. $D \in \{\Delta_F, \Delta_F/4\}$) gemäß Satz 1.43. Wegen

$$1 = N_F(1) = N_F(u \cdot u^{-1}) = N_F(u) \cdot N_F(u^{-1})$$

und $N_F(u),\ N_F(u^{-1}) \in \mathbb{Z}$ nach Satz 1.26 folgt $N_F(u) = \pm 1$. Mit $N_F(u) = a^2 - b^2 D \ > 0$ ergibt sich $N_F(u) = 1$.

1. Fall: $D \equiv 2, 3 \bmod 4$ und $D < -1$.

Nach Satz 1.43 ist $\Delta_F = 4D$ und $a^2 - b^2 D = 1$ für gewisse $a, b \in \mathbb{Z}$. Wegen $D < -1$ folgt $b = 0$ und $a = \pm 1$, also $\mathcal{U}_F = \langle -1 \rangle$.

2. Fall: $D \equiv 1 \bmod 4$ und $D < -4$.

Nach Satz 1.43 ist $a^2 - b^2 D = 1$ für gewisse $a, b \in \frac{1}{2}\mathbb{Z}$, d.h. $a'^2 - b'^2 D = 4$ für $a', b' \in \mathbb{Z}$. Wegen $D < -4$ folgt $b' = 0$, also $a' = \pm 2$, d.h. $a = \pm 1$ und wieder $\mathcal{U}_F = \langle -1 \rangle$.

Es bleiben die Fälle $D = -1, -2, -3$. Für $D = -1$ haben wir $a^2 + b^2 = 1$, also

$a = \pm 1,\ b = 0$ oder $a = 0,\ b = \pm 1$. Das bedeutet $u = \pm 1$ oder $u = \pm i$, und somit $\mathcal{U}_F = \langle i \rangle$ für $\Delta_F = -4$. Im Falle $D = -2$ gilt $a^2 + 2b^2 = 1$, also $a = \pm 1,\ b = 0$ und daher $\mathcal{U}_F = \langle -1 \rangle$. Schließlich für $D = 3$ haben wir $a^2 + 3b^2 = 4$ mit $a, b \in \mathbb{Z}$, d.h. $a = \pm b = \pm 1$ oder $a = \pm 2,\ b = 0$. Wir erhalten die Einheiten

$$u = \pm 1 \quad , \quad u = \frac{1}{2}(1 \pm \sqrt{-3}) \quad , \quad u = \frac{1}{2}(-1 \pm \sqrt{-3}) \ ,$$

d.h. die Potenzen der 6. Einheitswurzel $\zeta_6 := \frac{1}{2}(1 - i\sqrt{3})$.

□

Nach Definition 1.2 heißt ein Element aus $\mathcal{O}_F$ eindeutig zerlegbar, wenn es bis auf Reihenfolge der Faktoren und Assoziierte eindeutig in irreduzible Elemente faktorisiert. Wir haben schon Beispiele für irreduzible Elemente gesehen, die nicht prim sind. Der folgende Satz zeigt, dass eindeutige Faktorisierung genau dann vorliegt, wenn die irreduziblen Elemente prim sind.

Satz 1.47

Sei F ein Zahlkörper. Dann gilt:

(i) Jedes $\alpha \in \mathcal{O}_F,\ \alpha \neq 0$, lässt sich in ein Produkt irreduzibler Faktoren zerlegen.

(ii) Jedes $\alpha \in \mathcal{O}_F,\ \alpha \neq 0$, besitzt eine bis auf Reihenfolge der Faktoren und Assoziierte eindeutige solche Zerlegung genau dann, wennn jedes irreduzible Element von $\mathcal{O}_F$ prim ist.

Beweis:

(i) Ist α nicht selbst irreduzibel, so gilt $\alpha = \beta \cdot \gamma$ für gewisse $\beta, \gamma \in \mathcal{O}_F \setminus \mathcal{U}_F$. Iteration dieses Zerlegungsprozesses liefert die gewünschte Faktorisierung. Der Prozess ist endlich, denn: Ist $N(\delta) = \pm 1$ für ein $\delta \in \mathcal{O}_F$, so gilt

$$1 = \pm N(\delta) = \delta \cdot ((\pm 1) \cdot \delta_2 \cdot \delta_3 \cdot \delta_4 \cdot \ldots \cdot \delta_d)$$

mit den Konjugierten $\delta_2, \ldots, \delta_d \in \mathcal{O}_F$ von δ, also $\delta \in \mathcal{U}_F$. Für eine Zerlegung $\alpha = \alpha_! \cdot \alpha_2 \cdot \ldots \cdot \alpha_m$ in irreduzible Elemente haben wir also $|N(\alpha_j)| \geq 2$ $(j = 1, \ldots, m)$ und somit

$$m \leq 2^m \leq \prod_{j=1}^{m} |N(\alpha_j)| = |N(\alpha)| \ .$$

(ii) „$\Longrightarrow$“

Seien alle Zerlegungen eindeutig. Für $\alpha \in \mathcal{O}_F$ irreduzibel ist zu zeigen: α ist prim. Sei also $\alpha \mid \beta\gamma$, d.h. es gibt $\sigma \in \mathcal{O}_F$ mit $\beta\gamma = \alpha\sigma$. Nach Voraussetzung haben $\beta, \gamma\sigma$ eindeutige Zerlegungen

$$\beta = u \cdot \prod_{j=1}^{r} \beta_j \quad , \quad \gamma = v \cdot \prod_{j=1}^{s} \gamma_j \quad , \quad \sigma = w \cdot \prod_{j=1}^{t} \sigma_j$$

mit $u, v, w \in \mathcal{U}_F$ und $\beta_j, \gamma_j, \sigma_j$ alle irreduzibel. Also

$$\alpha \cdot w \cdot \prod_{j=1}^{t} \sigma_j = \alpha\sigma = \beta\gamma = uv \prod_{j=1}^{r} \beta_j \cdot \prod_{j=1}^{s} \gamma_j \ .$$

Da α irreduzibel ist, folgt aus der eindeutigen Faktorisierung, dass $\alpha \in \{\beta_j : \ 1 \leq j \leq r\} \cap \{\gamma_j : \ 1 \leq j \leq s\}$. Also $\alpha \mid \beta$ oder $\alpha \mid \gamma$, d.h. α ist prim.

„$\Longleftarrow$“

Sei jedes irreduzible Element von $\mathcal{O}_F$ prim. Sei für irreduzible α_j, β_j und $u, v \in \mathcal{U}_F$ mit $1 \leq s \leq r$

$$(*) \quad u\alpha_1 \cdot \ldots \cdot \alpha_r = v\beta_1 \cdot \ldots \cdot \beta_s \ .$$

Zu zeigen: $r = s$ und jedes α_j ist assoziiert zu einem β_k. Wir machen Induktion über r. Für $r = 1$ ist $s = 1$, und alles ist klar. Wir nehmen nun eindeutige Faktorisierung bis zur Länge $r - 1 \geq 1$ an. Da β_s nach Voraussetzung prim (also keine Einheit) ist, impliziert $\beta_s \mid u\alpha_1 \cdot \ldots \cdot \alpha_r$, dass $\beta_s \mid \alpha_j$ für geeignetes j, o.B.d.A. $\beta_s \mid \alpha_r$. Damit sind β_s und α_r assoziiert. Da $\mathcal{O}_F$ Integritätsring ist ($\mathcal{O}_F$ besitzt keine Nullteiler, denn $\mathbb{C}$ besitzt keine Nullteiler), können wir $\beta_s = w\alpha_r$, $w \in \mathcal{U}_F$, in $(*)$ kürzen und erhalten

$$u'\alpha_1 \cdot \ldots \cdot \alpha_{r-1} = v\beta_1 \cdot \ldots \cdot \beta_{s-1}$$

Induktion liefert die Behauptung.

□

Definition 1.48

Sei D ein Integritätsbereich, in dem jedes Element $\neq 0$ eindeutig in irreduzible Elemente zerfällt. Dann heißt D ein *ZPE-Ring* (Zerlegung in Primelemente eindeutig).

Bemerkung:

Nach Satz 1.47 ist der Name ZPE-Ring anstelle von ZIE-Ring (Zerlegung in irreduzible Elemente eindeutig) gerechtfertigt.

Definition 1.49

Sei D ein ZPE-Ring. Für $\alpha, \beta, \gamma, \delta \in D$, heißt γ *größter gemeinsamer Teiler von* α *und* β, $\gamma = \mathrm{ggT}(\alpha, \beta)$, falls

(i) $\gamma \mid \alpha$ und $\gamma \mid \beta$;

(ii) falls $\sigma \mid \alpha$ und $\sigma \mid \beta$ für ein $\sigma \in D$, so gilt $\sigma \mid \gamma$;

und δ *kleinstes gemeinsames Vielfaches von* α *und* β, $\delta = \mathrm{kgV}(\alpha, \beta)$, falls

(iii) $\alpha \mid \delta$ und $\beta \mid \delta$;

(iv) falls $\alpha \mid \Theta$ und $\beta \mid \Theta$ für ein $\Theta \in D$, so gilt $\delta \mid \Theta$.

(Beachte, dass ggT$(\alpha, \beta$ und kgV(α, β) eindeutig bis auf Assoziierte sind).
Ist ggT$(\alpha, \beta) = 1$ (d.h. ggT(α, β) ist Einheit), so heißen α und β *teilerfremd*.

Definition 1.50

Ein Integritätsbereich D heißt *euklidischer Ring*, falls es eine *euklidische Funktion* $f : D \longrightarrow \mathbb{N}_0$ gibt, d.h. f erfüllt die Bedingungen

(i) Für $\alpha\beta \in D \setminus \{0\}$ ist $f(\alpha) \leq f(\alpha\beta)$.

(ii) Für $\alpha, \beta \in D,\ \beta \neq 0$, existieren $\gamma, \rho \in D$ mit

$$\alpha = \gamma\beta + \rho \text{ und } f(\rho) < f(\beta) \text{ oder } \rho = 0 \ .$$

Beispiel:
In $F := \mathbb{Q}(\sqrt{-2})$ ist $\mathcal{O}_F = \mathbb{Z}[\sqrt{-2}]$ nach Satz 1.43. Wir wollen zeigen, dass $\mathbb{Z}[\sqrt{-2}]$ euklidischer Ring ist. Klar ist, dass $\mathbb{Z}[\sqrt{-2}]$ Integritätsbereich ist, denn $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$ besitzt keine Nullteiler.
Behauptung: $N_F : \mathbb{Z}[\sqrt{-2}] \longrightarrow \mathbb{N}_0$ ist euklidische Funktion.
Zunächst ist $N_F(\alpha) \in \mathbb{N}_0$ für alle $\alpha = a+b\sqrt{-2}\ \in \mathbb{Z}[\sqrt{-2}]$, denn $N_F(\alpha) = a^2+2b^2\ \in \mathbb{N}$ für $\alpha \neq 0$ und $N_F(0) = 0$. Damit ist auch Eigenschaft (i) klar, denn

$$N_F(\alpha\beta) = N_F(\alpha) \cdot N_F(\beta) \geq N_F(\alpha)$$

für $\alpha\beta \neq 0$.
Zum Beweis von (ii) seien $\alpha = a + b\sqrt{-2}\ ,\ \beta = c + d\sqrt{-2}\ \in \mathbb{Z}[\sqrt{-2}]$. Dann haben wir

$$\frac{\alpha}{\beta} = \frac{(a + b\sqrt{-2})(c - d\sqrt{-2})}{c^2 + 2d^2} = \frac{ac + 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{-2} =: u + v\sqrt{-2}$$

mit $u, v \in \mathbb{Q}$. Wir wählen $\gamma := x + y\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ mit $|u - x| \leq 1/2$ und $|v - y| \leq 1/2$.

Damit folgt für $\rho := \alpha - \gamma\beta \in \mathbb{Z}[\sqrt{-2}]$, dass $\rho = 0$ oder

$$\begin{aligned} N_F\rho) &= N_F\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N_F(\beta) \cdot N_F\left(\frac{\alpha}{\beta} - \gamma\right) \\ &= N_F(\beta) \cdot N_F((u - x) + (v - y)\sqrt{-2}) \\ &= N_F(\beta) \cdot ((u - x)^2 + 2 \cdot (v - y)^2) \\ &\leq N_F(\beta) \cdot \left(\frac{1}{4} + 2 \cdot \frac{1}{4}\right) < N_F(\beta) \ . \end{aligned}$$

Satz 1.51

Jeder euklidische Ring ist ein ZPE-Ring.

Beweis:

Sei D euklidischer Ring und sei $\alpha \in D \setminus \{0\}$. Wir zeigen zunächst, dass α in irreduzible Elemente faktorisiert. Dazu bezeichne f die euklidische Funktion auf D. Wir haben $f(\alpha) = f(1)$ gdw. $\alpha \in \mathcal{U}_D$, denn:

Für alle $\alpha \neq 0$ gilt $f(1) \leq f(1 \cdot \alpha) = f(\alpha)$. Ist $f(\alpha) = f(1)$, so gilt für jedes $\beta \in D \setminus \{0\}$, dass $\beta = \gamma\alpha + \rho$ mit $\rho = 0$ oder $f(\rho) < f(\alpha) = f(1) \leq f(\rho)$ Widerspruch, d.h. $\rho = 0$ und somit $\alpha \mid \beta$ für jedes $\beta \neq 0$, insbesondere $\alpha \mid 1_D$, d.h. $\alpha \in \mathcal{U}_D$. Sei umgekehrt $\alpha \in \mathcal{U}_D$, so folgt

$$f(1) \leq f(\alpha) \leq f(\alpha \cdot \alpha^{-1}) = f(1) \ ,$$

also $f(\alpha) = f(1)$.

Nach den vorangehenden Überlegungen können wir Induktion über $f(\alpha)$ machen. Ist $f(\alpha) = f(1)$, so ist $\alpha \in \mathcal{U}_D$ und es ist nichts zu zeigen. Sei nun $\alpha \notin \mathcal{U}_D$ und Faktorisierung gewährleistet für alle $\beta \in D \setminus \{0\}$ mit $f(\beta) < f(\alpha)$. Ist α selbst irreduzibel, so sind wir fertig. Sei also $\alpha = \beta\gamma$ mit $\beta, \gamma \in D \setminus \mathcal{U}_D$. Dann haben wir

$$f(\beta) \leq f(\beta\gamma) = f(\alpha) \quad \text{und} \quad f(\gamma) \leq f(\gamma\beta) = f(\alpha) \ .$$

Dabei gilt $f(\beta) \neq f(\alpha)$ (und analog $f(\gamma) \neq f(\alpha)$), denn:

Wäre $f(\beta) = f(\alpha)$, so hätten wir $\beta = \eta \cdot \alpha + \rho$ mit $\rho = 0$ oder $f(\rho) < f(\alpha)$. Wegen

$\beta \mid \alpha$ folgte im zweiten Fall, dass $\beta \mid \rho$, also $f(\beta) \leq f(\rho) < f(\alpha)$. Es bleibt nur $\rho = 0$, d.h. $\alpha \mid \beta$. Damit wären α und β assoziiert, d.h. $\gamma \in \mathcal{U}_D$. Widerspruch!
Wir haben also $f(\beta) < f(\alpha)$ und $f(\gamma) < f(\alpha)$ und somit nach Induktionsannahme Faktorisierungen von β und γ in irreduzible Elemente. Daher ist auch $\alpha = \beta \cdot \gamma$ faktorisiert.

Es bleibt noch die Eindeutigkeit der Zerlegung zu zeigen. Wir beweisen zuerst, dass jedes irreduzible Element prim ist. Sei dazu α irreduzibel mit $\alpha \mid \beta\gamma$. Gilt $\alpha \nmid \beta$, so ist $\mathrm{ggT}(\alpha, \beta) = 1$. Mit Hilfe des euklidischen Algorithmus (d.h. wiederholter Anwendung von (ii) aus Definition 1.50) ergibt sich die Existenz von $\sigma, \tau \in D$ derart, dass

$$\sigma\alpha + \tau\beta = 1 \ .$$

Also $\sigma\alpha\gamma + \tau\beta\gamma = \gamma$ und wegen $\alpha \mid \beta\gamma$ somit $\alpha \mid \gamma$, d.h. α ist prim. Mit demselben Argument wie im zweiten Teil des Beweises von Satz 1.47(ii) folgt die Eindeutigkeit der Zerlegung, wobei wie oben Induktion über $f(\alpha)$ benutzt wird.

□

Als Anwendungsbeispiel für Faktorisierung in Zahlkörpern betrachten wir eine sogenannte Bachet-Gleichung

$$y^2 = x^3 + k$$

mit festem $k \in \mathbb{Z}$.

Satz 1.52

Die diophantische Gleichung (d.h. Lösungen über $\mathbb{Z}$)

$$y^2 = x^3 - 2$$

hat nur die beiden Lösungen $x = 3,\ y = \pm 5$.

Beweis:

Zunächst ist x ungerade, denn für gerades x hätten wir $y^2 \equiv -2 \bmod 4$ Widerspruch. Aufgrund des Beispiels im Anschluss an Definition 1.50 wissen wir, dass $\mathcal{O}_F = \mathbb{Z}[\sqrt{-2}]$ mit $F = \mathbb{Q}(\sqrt{-2})$ ein euklidischer Ring und somit nach Satz 1.51 ein ZPE-Ring ist. Die gegebene Bachet-Gleichung liefert in $\mathbb{Z}[\sqrt{-2}]$ die Faktorisierung

$$(y + \sqrt{-2}) \cdot (y - \sqrt{-2}) = x^3 \ .$$

Behauptung: $\quad \mathrm{ggT}(y + \sqrt{-2}, y - \sqrt{-2}) = 1.$

Sei dazu für $a, b \in \mathbb{Z}$

$$\alpha := (a + b\sqrt{-2}) \mid \mathrm{ggT}(y + \sqrt{-2}, y - \sqrt{-2}) \ .$$

Es folgt

$$N_F(\alpha) \mid N_F((y + \sqrt{-2}) - (y - \sqrt{-2})) = N_F(2\sqrt{-2}) = 8$$

und

$$N_F(\alpha) \mid N_F(x^3) = x^6 \ .$$

Wegen $2 \nmid x$ folgt $N_F(\alpha) = \pm 1$, d.h. $\alpha \in \mathcal{U}_F$, also gilt die Zwischenbehauptung. Aufgrund der eindeutigen Faktorisierung in $\mathbb{Z}(\sqrt{-2}]$ erhalten wir damit

$$y + \sqrt{-2} = u \cdot \gamma^3 = \pm(c + d\sqrt{-2})^3$$

für eine Einheit $u \in \mathcal{U}_F$ und eine $\gamma := c + d\sqrt{-2} \ \in \mathcal{O}_F$, wobei gemäß Satz 1.46 gilt $u = \pm 1$. Nach Ausmultiplizieren der rechten Seite ergibt Koeffizientenvergleich

$$y = \pm c(c^2 - 6d^2) \quad \text{und} \quad 1 = \pm d(3c^2 - 2d^2) \ .$$

Die zweite Gleichung liefert $d = \pm 1$, also $1 = \pm(3c^2 - 2)$ und somit $c = \pm 1$. Einsetzen in die erste Gleichung ergibt $y = \pm(1 - 6) = \pm 5$, also $x = 3$.

□

2 Arithmetik in Zahlkörpern

2.1. Quadratische Zahlkörper

Folgendes wissen wir bereits über quadratische Zahlkörper F:

- Explizite Formel für die Diskriminante Δ_F (Satz 1.43).
- Explizite Darstellung des Ganzzahlrings $\mathcal{O}_F = \mathbb{Z}[\alpha]$ mit explizitem α (Satz 1.43).
- Explizite Darstellung der Einheitengruppe $\mathcal{U}_F$ für den Fall $\Delta_F < 0$ (Satz 1.46).
- $F = \mathbb{Q}(\sqrt{-2})$ hat den euklidischen Ganzzahlring $\mathcal{O}_F = \mathbb{Z}[\sqrt{-2}]$ (Beispiel nach Definition 1.50).

Satz 2.1

Ist F komplexer quadratischer Zahlkörper mit Diskriminante $\Delta_F < -12$, so ist $\mathcal{O}_F$ kein euklidischer Ring.

Beweis:
Wir nehmen an, dass $\mathcal{O}_F$ ein euklidischer Ring mit euklidischer Funktion f sei. Sei $\alpha \in \mathcal{O}_F \setminus \mathcal{U}_F,\ \alpha \neq 0$, derart gewählt, dass f minimal ist. Da $\mathcal{O}_F$ euklidischer Ring ist, existieren zu jedem $\beta \in \mathcal{O}_F$ Elemente $\gamma, \rho \in \mathcal{O}_F$ mit $\beta = \gamma\alpha + \rho$, wobei $\rho = 0$ oder $f(\rho) < f(\alpha)$. Wegen der Minimalität von $f(\alpha)$ bleiben nur $\rho = 0$ oder $\rho \in \mathcal{U}_F$ (d.h. $\rho = \pm 1$ nach Satz 1.46 wegen $\Delta_F < -12$). Insgesamt haben wir bei Division eines beliebigen $\beta \in \mathcal{O}_F$ durch α nur drei mögliche Reste, also

$$|\mathcal{O}_F / \langle\alpha\rangle| \leq 3 \ .$$

Für algebraische Zahlkörper F und $\alpha \in \mathcal{O}_F,\ \alpha \neq 0$, gilt allgemein

$$|\mathcal{O}_F / \langle\alpha\rangle| = |N_F(\alpha)|$$

(man zeigt: $\mathcal{O}_F$ und $\langle\alpha\rangle$ haben als freie Gruppen über $\mathbb{Z}$ denselben Rang, also $|\mathcal{O}_F/\langle\alpha\rangle|$ endlich). Wir erhalten $N_F(\alpha) \leq 3$.

1. Fall: $\Delta_F \equiv 0 \bmod 4$.

Nach Satz 1.43 haben wir $\alpha = a+b\sqrt{D}$ mit $a, b \in \mathbb{Z}$, wobei $D = \Delta_F/4$ der Radikand von F ist. Es folgt

$$3 \geq N_F(\alpha) = a^2 - b^2 D$$

mit $-D > 3$ wegen $\Delta_F < -12$. Dies liefert für $\alpha \neq 0, \pm 1$ einen Widerspruch.

2. Fall: $\Delta_F \equiv 1 \bmod 4$.

Wieder nach Satz 1.43 haben wir $\alpha = (a + b\sqrt{D})/2$ mit $a, b \in \mathbb{Z},\ a \equiv \bmod 2$. Für $a \equiv b \equiv 0 \bmod 2$ und $\alpha \neq 0, \pm 1$ kommt

$$3 \geq N_F(\alpha) = \frac{1}{4}(a^2 - b^2 D)\ . \quad \text{Widerspruch! } (D = \Delta_F < -12)$$

Als bleibt nur $a \equiv b \equiv 1 \bmod 2$, und wir erhalten

$$\begin{aligned} 3 &\geq N_F(\alpha) = \frac{1}{4}(a^2 - b^2 D) = \frac{1}{4}(a^2 - b^2 \Delta_F) \\ &> \frac{1}{4}(a^2 + 12b^2) \geq \frac{1}{4}(1 + 12 \cdot 1) > 3 \end{aligned}$$

Widerspruch!

□

Bemerkungen:

(i) Wir haben als Beispiel gezeigt, dass $\mathcal{O}_F$ für $F = \mathbb{Q}(\sqrt{-2})$ euklidischer Ring ist. In ähnlicher Weise stellen sich $F = \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11})$ als Zahlkörper mit euklidischem $\mathcal{O}_F$ heraus. Dies sind genau die fünf euklidischen Ringe $\mathcal{O}_F$ mit $\Delta_F < 0$.

(ii) Es lässt sich leicht zeigen, dass die fünf euklidischen komplexen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$ mit $D = -1, -2, -3, -7, -11$ norm-euklidisch sind, d.h. die euklidische Funktion ist jeweils die Norm (bzw. allgemeiner der Betrag der Norm).

Wir wollen nun reelle quadratische Zahlkörper untersuchen.

Satz 2.2

Für $D = 2, 3, 5, 6, 7, 13, 17, 21, 29$ ist $F = \mathbb{Q}(\sqrt{D})$ norm-euklidisch (d.h. $\mathcal{O}_F$ ist norm-euklidisch).

Beweis:

Wir setzen

$$\varepsilon := \begin{cases} 2 & \text{für} \quad D \equiv 1 \bmod 4, \\ 1 & \text{für} \quad D \equiv 2, 3 \bmod 4. \end{cases}$$

Offenbar lässt sich jedes $\sigma \in F$ schreiben als

$$\sigma = r_1 + \left(\frac{r_2}{\varepsilon}\right)\sqrt{D} \quad r_1, r_2 \in \mathbb{Q} \ .$$

Bedingung (ii) in Definition 1.50 für norm-euklidische Ringe ist äquivalent zu: Für alle $\sigma \in \mathbb{Q}(\sqrt{D})$ existiert ein $\beta \in \mathcal{O}_F$ mit

$$|N_F(\sigma - \beta)| < 1 \ .$$

Gemäß Satz 1.43 haben wir also ein

$$\beta = \frac{1}{\varepsilon}(x + y\sqrt{D}) \ \in \mathcal{O}_F \quad (x, y \in \mathbb{Z})$$

zu finden derart, dass

$$(*) \quad |N_F(\sigma - \beta)| = \left| \left(r_1 - \frac{x}{\varepsilon}\right)^2 - \frac{1}{\varepsilon^2}(r_2 - y)^2 D \right| < 1 \ .$$

Wir nehmen an, dass $(*)$ bei gegebenem $r_1, r_2 \in \mathbb{Q}$ für alle $x, y \in \mathbb{Z}$ verletzt ist. O.B.d.A. können wir in $(*)$ voraussetzen, dass $0 \leq r_i \leq 1/2$ für $i = 1, 2$ (ansonsten ersetzen wir x, y durch geeignete x', y'). Damit liefert $(*)$ mindestens eine der beiden folgenden Ungleichungen für alle $x, y \in \mathbb{Z}$:

$$(**) \quad \left(r_1 - \frac{x}{\varepsilon}\right)^2 \geq 1 + \frac{1}{\varepsilon^2}(r_2 - y)^2 D$$

oder

$$(***) \quad \frac{1}{\varepsilon^2}(r_2 - y)^2 D \geq 1 + \left(r_1 - \frac{x}{\varepsilon}\right)^2 \ .$$

Für $r_1 = r_2 = 0$ wären beide Ungleichungen verletzt mit $x = y = 0$. Also wissen wir $r_1 > 0$ oder $r_2 > 0$. Für $x = y = 0$ oder $x = 1,\ y = 0$ ist $(**)$ wegen $r_1 \leq 1/2$ verletzt:

$$\left(r_1 - \frac{x}{\varepsilon}\right)^2 < 1 + \frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \ .$$

Also muß für diese beiden Situationen jeweils $(***)$ erfüllt sein, d.h.

$$(***) \quad \frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \geq 1 + r_1^2 \quad \text{und} \quad \frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \geq 1 + \left(r_1 - \frac{1}{\varepsilon}\right)^2 \ .$$

Wir unterschieden nun zwei Fälle:

1. Fall: $(**)$ gilt für $x = -\varepsilon,\ = 0$, also mit $(***)$

$$(r_1 + 1)^2 \geq 1 + \frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \geq 2 + \left(r_1 - \frac{1}{\varepsilon}\right)^2 \geq 2 + (r_1 - 1)^2 \ .$$

Daraus folgt $r_1 \geq 1/2$, d.h. $r_1 = 1/2$. Einsetzen liefert

$$\frac{9}{4} = \left(\frac{1}{2} + 1\right)^2 \geq 1 + \frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \geq 2 + \left(\frac{1}{2} - 1\right)^2 = \frac{9}{4}$$

und somit $r_2^2 \cdot D/\varepsilon^2 = 5/4$. Sei nun $r_2 = a/b$ mit $(a, b) = 1$. Für $\varepsilon = 1$ haben wir $4a^2D = 5b^2$, also $a^2 \mid 5$, d.h. $a = 1$. Da D quadratfrei nach Voraussetzung ist, bleibt nur $b = 2$, d.h. $r_2 = 1/2$ und $D = 5$ (s. Liste im Satz). Für $\varepsilon = 2$ folgt $a^2D = 5b^2$ und damit $a = b = 1$ Widerspruch! $(r_2 \leq 1/2)$.

2. Fall: $(***)$ gilt für $x = -\varepsilon,\ y = 0$, also

$$\frac{1}{\varepsilon^2} \cdot r_2^2 \cdot D \geq 1 + (r_1 - 1)^2 \geq 2 \ .$$

Wegen $r_2^2 \leq 1/4$ folgt $D \geq 8 \cdot \varepsilon^2$, d.h. für $D < 8 \cdot \varepsilon^2$ ist F norm-euklidisch. Für $D \equiv 1 \bmod 4$ heißt dies $D < 32$, also $D = 5, 13, 17, 21, 29$. Für $D \equiv 2, 3 \bmod 4$ haben wir $D < 8$, also $D = 2, 3, 6, 7$.

□

Bemerkungen:

(i) Zu den in Satz 2.2 angegebenen norm-euklidischen reell-quadratischen Zahlkörpern kommen noch die $\mathbb{Q}(\sqrt{D})$ mit $D = 11, 19, 33, 37, 41, 57, 73$ hinzu. 1938 bewies Heilbronn, dass es nur endlich viele derartige Zahlkörper gibt, und 1950 zeigten Chatland & Davenport sowie unabhängig davon Inheri, dass die oben angegebene Liste vollständig ist (Methode: Geometrie der Zahlen).

(ii) Während die fünf euklidischen komplex-quadratischen Zahlkörper automatisch norm-euklidisch sind, zeigte Clark 1994, dass dies im reellen Fall anders ist: In $\mathbb{Q}(\sqrt{69})$ gibt es eine euklidische Funktion, die nicht die Norm ist.

Mit unseren Mitteln können wir zeigen

Satz 2.3

Es gibt nur endlich viele norm-euklidische reell-quadratische Zahlkörper $F = \mathbb{Q}(\sqrt{D})$ mit $D > 0$ und $\Delta_F \equiv 0 \bmod 4$ (d.h. $D \not\equiv 1 \bmod 4$).

Beweis:

Sei $F = \mathbb{Q}(\sqrt{D})$ norm-euklidisch mit $D > 0$ und $\Delta_F \equiv 0 \bmod 4$. Zu jedem $\sigma = t \cdot \sqrt{D}/D \ \in F,\ t \in \mathbb{Z}$, existiert ein $x, y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ (vgl. Satz 1.43) derart, dass

$$\left|N_F(\sigma - (x + y\sqrt{D}))\right| = \left|x^2 - \left(y - \frac{t}{D}\right)^2 \cdot D\right| < 1 \ ,$$

also

$$\left|Dx^2 - (Dy - t)^2\right| < D \ .$$

Mit $z := Dy - t \ \in \mathbb{Z}$ haben wir

$$(*) \quad z^2 - Dx^2 \equiv t^2 \bmod D \quad \text{und} \quad \left|z^2 - Dx^2\right| < D \ .$$

1. Fall: $D \equiv 3 \bmod 4$.

Wir setzen $t := 2 \cdot [1/2(\sqrt{6D} - 1)] + 1$. Eine kleine Rechnung zeigt, dass für $D \geq 88$ gilt (jedenfalls für D hinreichend groß)

$$5D < t^2 < 6D \ .$$

Mit $(*)$ folgt

$$z^2 - Dx^2 = t^2 - a \cdot D \ ,$$

wobei $a = 5$ oder $a = 6$. Also

$$(**) \quad D(a - x^2) = t^2 - z^2 \ .$$

Für $a = 5$ haben wir wegen $2 \nmid t$

$$3(1 - x^2) \equiv 1 - z^2 \bmod 4 \ ,$$

also $2 \nmid x$ und $2 \nmid z$. Wir setzen $t = 2k + 1,\ z = 2l + 1$ und $x = 2m + 1$ und erhalten aus $(**)$

$$D \cdot (4 - 4m - 4m^2) = (4k^2 + 4k + 1) - (4l^2 + 4l + 1) \ ,$$

also

$$D \cdot (1 - m(m + 1)) = k(k + 1) - l(l + 1) \ .$$

Dies ist unlösbar, denn links steht eine ungerade Zahl und rechts eine gerade Zahl; d.h. $(**)$ ist für $a = 5$ nicht lösbar.
Für $a = 6$ liefert $(**)$ wegen $2 \nmid t$

$$3(2 - x^2) \equiv 1 - z^2 \bmod 4 \ ,$$

auch dies unlösbar. Also ist für $D \equiv 3 \bmod 4$ und $D \geq 88$ der Körper $\mathbb{Q}(\sqrt{D})$ nicht norm-euklidisch.
2. Fall: $D \equiv 2 \bmod 4$.
Wir setzen $t := 2[(\sqrt{3} - 1)/2] + 1$, womit für $D \geq 40$ gilt

$$2D < t^2 < 3D \ ,$$

also mit $(*)$ für $a \in \{2, 3\}$

$$D(a - x^2) = t^2 - z^2 \ .$$

Die gleichen Argumente wie im 1. Fall liefern auch hier die Unlösbarkeit, womit Satz 2.3 vollständig bewiesen ist.

□

Bemerkung:

Nach Satz 1.51 umfasst die Menge der quadratischen „ZPE-Zahlkörper“ die Menge der euklidischen quadratischen Zahlkörper. 1966 bewiesen Baker und Stark unabhängig voneinander, dass die komplexen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$ mit ZPE-Eigenschaft genau für $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$ gegeben sind. Es kann bislang nur vermutet werden, dass es unendlich viele reelle quadratische ZPE-Zahlkörper gibt.
Aus der Theorie der Kettenbrüche ist bekannt:

- Jede reelle Zahl α besitzt eine (nahezu) eindeutige Darstellung als endlicher oder unendlicher Kettenbruch, d.h. es gibt Zahlen $a_0 \in \mathbb{Z}$ und $a_j \in \mathbb{N}$ $(j \geq 1)$ mit
$$\alpha = \langle a_0; a_1, a_2, \ldots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$
- Jede quadratische Irrationalzahl α besitzt einen eindeutigen unendlichen periodischen Kettenbruch
$$\alpha = \langle a_0; a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k}} \rangle \ .$$
- Die Lösungen der Pell'schen Gleichung $x^2 - y^2 D \equiv \pm 1$ werden bestimmt durch die Näherungsbrüche des Kettenbruchs von $\sqrt{D}$.

Mit derlei Hilfsmitteln bestimmen wir nun die Einheitengruppe der reell-quadratischen Zahlkörper.

Satz 2.4

Sei $F = \mathbb{Q}(\sqrt{D})$ mit $D > 1$ quadratfrei. Dann existiert eine minimale Einheit $\varepsilon_1 = \varepsilon_1(F) > 1$ in $\mathcal{U}_F$ derart, dass

$$\mathcal{U}_F = \{\pm\, \varepsilon_1^n :\ n \in \mathbb{Z}\}\ .$$

Ist l die Periodenlänge des Kettenbruchs von $\sqrt{D}$ und bezeichnet A_j/B_j den j-ten Näherungsbruch von $\sqrt{D}$, so gilt

$$A_{l-1} + B_{l-1}\sqrt{D} = \begin{cases} \varepsilon_1 & \text{für} \quad D \not\equiv 5 \bmod 8, \\ \varepsilon_1 \text{ oder } \varepsilon_1^3 & \text{für} \quad D \equiv 5 \bmod 8. \end{cases}$$

Außerdem ist $N_F(\varepsilon_1) = (-1)^l$.

Beweis:

Nach Satz 1.43 können wir jedes Element von $\mathcal{O}_F$ in der Form $(x + y\sqrt{D})/2$ mit $x \equiv y \bmod 2$ schreiben, wobei für $D \not\equiv 1 \bmod 4$ sogar $x \equiv y \equiv 0 \bmod 2$ gilt. Ist speziell $u \in \mathcal{U}_F$, so haben wir für x, y mit diesen Eigenschaften

$$u = \frac{1}{2}(x + y\sqrt{D})$$

und

$$(*) \quad x^2 - Dy^2 = \pm 4$$

wegen $N_F(u) = \pm 1$. Wir wählen

$$\varepsilon_1 = \varepsilon_1(F) = \frac{1}{2}(x_1 + y_1\sqrt{D}) \ \in \mathcal{U}_F$$

als die kleinste Lösung von $(*)$ mit $y_1 > 0$. Dann ist $x_1 \neq 0$, und mit $x_1 > 0$ (o.B.d.A.) wird ε_1 eindeutig. Bekanntlich sind die positiven Lösungen der Pell'schen Gleichung

$$(**) \quad x^2 - y^2 D = \pm 1$$

genau gegeben durch $x = A_{kl-1}$, $y = B_{kl-1}$ $(k = 1, 2, \ldots)$; hinzu kommen die entsprechenden Lösungen durch Änderung von Vorzeichen und die triviale Lösung

$x = 1,\ y = 0$. Die kleinste positive Lösung ist demnach $x = A - l - 1,\ y = B_{l-1}$. Für $D \not\equiv 1 \bmod 4$ haben wir in $(*)$ $x \equiv y \equiv 0 \bmod 2$, d.h. $(*) \iff (**)$. Für $D \equiv 1 \bmod 8$ in $(*)$ ergibt sich

$$x^2 - y^2 \equiv x^2 - Dy^2 = \pm 4 \equiv 4 \bmod 8 \ ,$$

was nur für $x \equiv y \equiv 0 \bmod 2$ möglich ist. Also folgt auch in diesem Fall $(**)$ aus $(*)$, und wir haben in den bisherigen Situationen

$$\varepsilon_1 = A_{l-1} + B_{l-1}\sqrt{D} \ .$$

Es bleibt der Fall $D \equiv 5 \bmod 8$ und $\varepsilon_1 \neq A_{l-1} + B_{l-1}\sqrt{D}$. Dann gilt $x \equiv y \equiv 1 \bmod 2$ in $(*)$, und

$$\varepsilon_1^2 = \frac{1}{4}\left(x + y\sqrt{D}\right)^2 = \frac{1}{4}\left((x^2 + y^2 D) + 2xy\sqrt{D}\right) \ \notin \mathbb{Z}[\sqrt{D}] \ ,$$

aber

$$\varepsilon_1^3 = \frac{1}{8}\left(x + y\sqrt{D}\right)^3 = \frac{1}{8}\left(x\left(x^2 + 3y^2 D\right) + y\left(3x^2 + y^2 D\right)\sqrt{D}\right) \ \in \mathbb{Z}[\sqrt{D}]$$

wegen $x^2 + 3y^2 D \equiv 1 + 3 \cdot 1 \cdot 5 \equiv 0 \bmod 8$ und auch $3x^2 + y^2 D \equiv 3 \cdot 1 + 1 \cdot 5 \equiv 0 \bmod 8$. Selbstverständlich ist

$$N_F(\varepsilon_1^3) = N_F(\varepsilon_1)^3 = N_F(\varepsilon_1) \ ,$$

also ist ε_1^3 die kleinste positive Lösung von $(**)$, d.h.

$$\varepsilon_1^3 = A_{l-1} + B_{l-1}\sqrt{D} \ .$$

Die Tatsache, dass

$$A_{kl-1}^2 - B_{kl-1}^2 D = (-1)^{kl}$$

und dies alle Lösungen von $x^2 - y^2 D = \pm 1$ sind, impliziert nun, dass $\mathcal{U}_F$ genau die angegebene Menge ist. Außerdem folgt auch, dass

$$N_F(\varepsilon_1) = N_F(\varepsilon_1^3) = (-1)^{1 \cdot l} \ .$$

□

Beispiele:

(i) Sei $D = 226 \equiv 2 \bmod 4$, also $\Delta_F = 904$ für $F = \mathbb{Q}(\sqrt{226})$. Wir haben $\sqrt{226} = \langle 15; \overline{30} \rangle$, denn für $\alpha := \langle \overline{30} \rangle = 30 + 1/\alpha$ gilt

$$\alpha^2 - 30\alpha - 1 = 0 \quad \Longrightarrow \quad \alpha_{1,2} = 15 \pm \sqrt{226} \quad \overset{\alpha>0}{\Longrightarrow} \quad \alpha = 15 + \sqrt{226}\ ,$$

also

$$\sqrt{226} = 15 + (\sqrt{226} - 15) = 15 + \frac{1}{\sqrt{226} + 15} = 15 + \frac{1}{\alpha} = \langle 15; \overline{30} \rangle\ .$$

Somit ist in Satz 2.4 $l = 1$ und wegen $A_0/B_0 = 15/1$

$$\varepsilon_1 = A_0 + B_0\sqrt{226} = 15 + \sqrt{226}$$

die minimale positive Einheit in $\mathcal{U}_F$.

(ii) Sei $D = 293 = \Delta_F \equiv 5 \bmod 8$ mit $F = \mathbb{Q}(\sqrt{293})$. Wir finden $\sqrt{293} = \langle 17; \overline{8, 1, 1, 8, 34} \rangle$, also $l = 5$. Man berechnet

$$\frac{A_4}{B_4} = \langle 17; 8, 1, 1, 8 \rangle = \frac{2482}{145} = \varepsilon_1 \text{ oder } \varepsilon_1^3\ .$$

Es zeigt sich

$$\varepsilon_1 := \frac{1}{2}(A_0 + B_0\sqrt{293}) = \frac{1}{2}(17 + \sqrt{293})$$

erfüllt $\varepsilon_1^3 = A_4/B_4$, also ist ε_1 die minimale positive Einheit in $\mathcal{U}_F$.

2.2. Kreisteilungskörper

Ist ζ_n eine primitive n-te Einheitswurzel, so heißt $\mathbb{Q}(\zeta_n)$ n-ter Kreisteilungskörper (aus offensichtlichen Gründen; vgl. Defnition 1.4). Wir wollen im Folgenden den Ring der ganzen Zahlen in $\mathbb{Q}(\zeta_n)$ bestimmen.

Definition 2.5

Für $n \in \mathbb{N}$ heißt

$$\Phi_n(x) := \sum_{\substack{1 \le j \le n \\ (j,n)=1}} (x - \zeta_n^j)$$

n-tes Kreisteilungspolynom. Der Grad von $\Phi_n(x)$ ist offenbar gleich Eulers $\varphi(n)$.

Satz 2.6

Für $n \in \mathbb{N}$ gilt mit einer primitven n-ten Einheitswurzel ζ_n

$$\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x) \ .$$

Insbesondere ist $\Phi_n(x) \in \mathbb{Z}[x]$ irreduzibel in $\mathbb{Z}[x]$.

Beweis:

Wir zeigen zunächst, dass $\Phi_n(x) \in \mathbb{Z}[x]$. Für $j = 1, \ldots, n$ ist ζ_n^j eine n/d-te primitive Einheitswurzel, sofern $d = \mathrm{ggT}(j, n)$. Damit folgt

$$\begin{aligned} x^n - 1 &= \prod_{j=1}^{n} (x - \zeta_n^j) = \prod_{d|n} \prod_{\substack{j=1 \\ (j,n)=d}}^{n} (x - \zeta_n^j) \\ &= \prod_{d|n} \prod_{\substack{k=1 \\ (k,n/d)=1}}^{n/d} (x - (\zeta_n^d)^k) \qquad \left[j = d \cdot k,\ k = \frac{j}{d};\ \left(\frac{j}{d}, \frac{n}{d}\right) = 1 \right] \\ &= \prod_{d|n} \Phi_{n/d}(x) = \prod_{d|n} \Phi_d(x) \ . \end{aligned}$$

Wir haben $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Unter Verwendung von Induktion sei $\Phi_k(x) \in \mathbb{Z}[x]$ für alle $k < n$. Nach obiger Identität ist

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(x)} \ ,$$

wobei in Zähler und Nenner Polynome aus $\mathbb{Z}[x]$ mit führenden Koeffizienten 1 stehen. Nach dem Gauß-Lemma muß dann auch $\Phi_n(x) \in \mathbb{Z}[x]$ gelten.
Behauptung: Ist ζ eine primitive n-te Einheitswurzel, so gilt $M_{\zeta_x,\mathbb{Q}}(\zeta^p) = 0$ für jedes $p \in \mathbb{P},\ p \nmid n$. Wir kürzen ab $m_1(x) := m_{\zeta_n,\mathbb{Q}}(x)$ und $m_2(x) := m_{\zeta^p,\mathbb{Q}}(x)$.
Da ζ n-te Einheitswurzel ist, gilt $m_1(x) \mid (x^n - 1)$. Da auch ζ^p n-te Einheitswurzel ist, folgt $m_2(x) \mid (x^n - 1)$. Mit $m_1(\zeta^p) = 0$ wäre unsere Behauptung bewiesen. Sei also $m_1(\zeta^p) \neq 0$. Wegen der Irreduzibilität von $m_1(x)$ und $m_2(x)$ hätten wir dann $m_1(x) \cdot m_2(x) \mid (x^n - 1)$, d.h.

$$(*) \quad x^n - 1 = m_1(x) \cdot m_2(x) \cdot g(x)$$

für ein $g(x) \in \mathbb{Z}[x]$. Das Polynom $m_2(x^p)$ hat die Nullstelle ζ, also $m_1(x) \mid m_2(x^p)$, d.h. es gibt $h(x) \in \mathbb{Z}[x]$ mit

$$m_2(x^p) = m_1(x) \cdot h(x)\ .$$

Wir betrachten die Polynomidentitäten über $\mathbb{Z}$ nun modulo p. Man zeigt leicht mit dem Binomischen Lehrsatz, dass für beliebige Polynome $f(x)$ gilt $f(x^p) \equiv f(x)^p \bmod p$. Also haben wir

$$m_2(x)^p \equiv m_1(x) \cdot h(x) \bmod p\ .$$

Ist nun $k(x)$ ein beliebiger irreduzibler Faktor von $m_1(x) \bmod p$, so ist $k(x)$ auch ein solcher Teiler von $m_2(x)^p$ und damit von $m_2(x) \bmod p$. Mit $(*)$ folgt, dass $x^n - 1 \bmod p$ durch $k(x)^2$ teilbar ist, d.h. $k(x) \mid (x^n - 1) \bmod p$ und $k(x) \mid (x^n - 1)' = nx^{n-1} \bmod p$. Wegen $p \nmid n$ hat $n \cdot x^{n-1}$ nur irreduzible Faktoren x, die jedoch nicht $x^n - 1$ teilen. Dieser Widerspruch beweist unsere Zwischenbehauptung.
Wir zeigen nun, dass jede primitive n-te Eineitswurzel eine Nullstelle von $m_{\zeta_n,\mathbb{Q}}(x)$ ist. Jede solche Einheitswurzel ist von der Form ζ_n^j für ein $(j, n) = 1$, d.h. $j = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ für gewisse $p_i \in \mathbb{P},\ p_i \nmid n$. Trivialerweise gilt $m_{\zeta_n,\mathbb{Q}}(\zeta_n) = 0$. Durch iterative Anwendung der Zwischenbehauptung erhalten wir

$$m_{\zeta_n,\mathbb{Q}}(\zeta_n^{p_1}) = m_{\zeta_n,\mathbb{Q}}(\zeta_n^{p_1 \cdot p_2}) = \cdots = m_{\zeta_n,\mathbb{Q}}(\zeta_n^{p_1 \cdot \ldots \cdot p_r}) = 0\ .$$

Damit folgt $\Phi_n(x) \mid m_{\zeta_n,\mathbb{Q}}(x)$. Da schon gezeigt wurde, dass $\Phi_n(x) \in \mathbb{Z}[x]$, und offenbar $\Phi_n(x)$ führenden Koeffizienten 1 besitzt, bleibt wegen der Irreduzibilität von $m_{\zeta_n,\mathbb{Q}}(x)$ nur $\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x)$.

□

Korollar 2.7

Für $n \in \mathbb{N}$ und eine primitive n-te Einheitswurzel ζ_n gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beweis:

Nach Korollar 1.12 und Satz 2.6 gilt

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}} = \deg \Phi_n = \varphi(n) \ .$$

□

Satz 2.8

Für $F = \mathbb{Q}(\zeta_n)$ mit einer primitven n-ten Einheitswurzel ζ_n gilt $\Delta_F \mid n^{\varphi(n)}$.

Beweis:

Klar ist

$$(*) \quad x^n - 1 = \prod_{j=1}^{n} (x - \zeta_n^j) = \Phi_n(x) \cdot g(x)$$

für ein $g(x) \in \mathbb{Z}[x]$. Differenzieren liefert

$$n \cdot x^{n-1} = \Phi_n'(x) \cdot g(x) + \Phi_n(x) \cdot g'(x)$$

also für $x := \zeta_n$

$$n \cdot \zeta_n^{n-1} = \Phi_n'(\zeta_n) \cdot g(\zeta_n) \ .$$

Aus $(*)$ folgt, dass die Konstante in $\Phi_n(x)$, d.h. bis aufs Vorzeichen das Produkt der Konjugierten von ζ_n (nach Satz 2.6), gleich ± 1 ist; mit anderen Worten: $N_F(\zeta_n) = \pm 1$. Also erhalten wir

$$\begin{aligned} \pm n^{\varphi(n)} &= N_F(\zeta_n)^{n-1} \cdot N_F(n) = N_F(n \cdot \zeta_n^{n-1}) \\ &= N_F(\Phi_n'(\zeta_n)) \cdot N_F(g(\zeta_n)) \ . \end{aligned}$$

Nach Satz 1.25 gilt

$$N_F(\Phi_n'(\zeta_n)) = \pm \mathrm{discr}(m_{\zeta_n,\mathbb{Q}}) = \pm \mathrm{discr}(B)$$

(als Vandermonde-Determinante, vgl. Lemma 1.34) für
$\mathcal{B} = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}\} \subseteq \mathcal{O}_F$. Sei $\mathcal{B}_1$ eine Ganzheitsbasis von F, also $\mathrm{discr}(\mathcal{B}_1) = \Delta_F$. Nach Satz 1.35 gilt $\mathrm{discr}(\mathcal{B}) = D^2 \cdot \mathrm{discr}(\mathcal{B}_1)$ mit einem $D \in \mathbb{Z}$. Wegen $\mathrm{discr}(\mathcal{B}) \in \mathbb{Z}$ haben wir also zusammen

$$\Delta_F = \mathrm{discr}(\mathcal{B}_1) \mid \mathrm{discr}(\mathcal{B}) = \pm N_F(\Phi_n'(\zeta_n)) \ ,$$

und es folgt die Behauptung.

□

Satz 2.9

Für $F = \mathbb{Q}(\zeta_n)$ mit einer primitiven n-ten Einheitswurzel ζ_n gilt $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$.

Beweis:

Für $n = 1, 2$ haben wir $\zeta_n = 1$ bzw. $\zeta_n = -1$, und die Behauptung ist trivial. Sei also o.B.d.A. $n \geq 3$.

Wir zeigen den Satz zunächst für Primzahlpotenzen $n = p^a$.

Wir setzen $\zeta := \zeta_{p^a}$. Nach Korollar 2.7 ist $\mathcal{B}_1 = \{1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(p^a)-1}\}$ eine $\mathbb{Q}$-Basis von F.

Behauptung: $|\mathrm{discr}(\mathcal{B}_1)| = p^s$ für ein $s \in \mathbb{N}$.

Mit Hilfe des Beweises von Satz 2.6 haben wir

$$x^{p^a} - 1 = \prod_{d|p^a} \Phi_d(x) = \Phi_{p^a}(x) \cdot \prod_{d|p^{a-1}} \Phi_d(x) = \Phi_{p^a}(x) \cdot (x^{p^{a-1}} - 1) \ .$$

Wir differenzieren und setzen $x = \zeta$, also

$$p^a \cdot \zeta^{p^a-1} = \Phi'_{p^a}(\zeta) \cdot (\zeta^{p^{a-1}} - 1) \ ,$$

und somit wegen $\zeta^{p^a} = 1$

$$(*) \quad \Phi'_{p^a}(\zeta) \cdot (\zeta^{p^{a-1}} - 1) \cdot \zeta = p^a \ .$$

Es ist $\xi := \zeta^{p^{a-1}}$ eine primitive p-te Einheitswurzel, also

$$N_{\mathbb{Q}(\xi)}(1 - \xi) = \prod_{j=1}^{p-1}(1 - \xi^j) = \Phi_p(1) = p$$

wegen $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Mit Satz 1.22 (ii) kommt wegen $N_{\mathbb{Q}(\zeta)}(-1) = \pm 1$

$$N_{\mathbb{Q}(\zeta)}(\xi - 1) = \pm(N_{\mathbb{Q}(\xi)}(\xi - 1))^{p^{a-1}} = \pm p^{p^{a-1}} \ .$$

Da auch $N_{\mathbb{Q}(\zeta)}(\zeta^{-1}) = \pm 1$, erhalten wir aus $(*)$

$$N_{\mathbb{Q}(\zeta)}(\Phi'_{p^a}(\zeta)) \cdot (\pm p^{p^{a-1}}) = N_{\mathbb{Q}(\zeta)}(p^a) = (p^a)^{\varphi(p^a)} = p^{a(p^a - p^{a-1})} \ .$$

Wie im Beweis zu Satz 1.43 erhalten wir $\mathrm{discr}(\mathcal{B}_1) = \mathrm{discr}(m_{\zeta,\mathbb{Q}})$, also mit Satz 1.25 und Satz 2.6

$$\begin{aligned} \mathrm{discr}(\mathcal{B}_1) &= \pm N_{\mathbb{Q}(\zeta)}(m'_{\zeta,\mathbb{Q}}(\zeta)) = \pm N_{\mathbb{Q}(\zeta)}(\Phi'_{p^a}(\zeta)) \\ &= \pm p^{p^{a-1}}(ap - a - 1) \ . \end{aligned}$$

Dies beweist die Zwischenbehauptung, da $n \geq 3$.

Wir setzen $\eta := 1 - \zeta$. Dann ist $\mathcal{B}_2 := \{1, \eta, \eta^2, \ldots, \eta^{\varphi(p^a)-1}\}$ auch eine $\mathbb{Q}$-Basis

von F, wobei nach Satz 1.35 $\mathrm{discr}(\mathcal{B}_2) = \mathrm{discr}(\mathcal{B}_1) = \pm p^s$ für ein $s \in \mathbb{N}$ (die Transformationsmatrix ist obere Dreiecksmatrix mit Diagonalelement ± 1). Wegen $\zeta = 1 - (1 - \zeta)$ ist $\mathbb{Z}[\zeta] = \mathbb{Z}[1 - \zeta]$, d.h. es genügt $\mathcal{O}_F = \mathbb{Z}[\eta]$ zu zeigen.

Behauptung: Jedes $\beta \in \mathcal{O}_F$ besitzt eine Darstellung

$$(**) \quad \beta = \sum_{j=1}^{\varphi(p^a)} \frac{z_j}{\mathrm{discr}(\mathcal{B}_2)} \cdot \eta^{j-1}$$

mit $z_j \in \mathbb{Z}$.

Ist $\mathcal{B}_3 := \{\alpha_1, \alpha_2, \ldots, \alpha_{\varphi(p^a)}\}$ eine Ganzheitsbasis von F, so existieren für $j = 1, \ldots, \varphi(p^a)$ Zahlen $a_{j,k} \in \mathbb{Z}$ $(1 \le k \le \varphi(p^a))$ mit

$$\eta^{j-1} = \sum_{k=1}^{\varphi(p^a)} a_{j,k} \cdot \alpha_j \ .$$

Nach der Cramer'schen Regel existieren dann Zahlen $a'_{j,k} \in \mathbb{Z}$ derart, dass

$$\alpha_j = \sum_{k=1}^{\varphi(p^a)} \frac{a'_{j,k}}{\det(a_{j,k})} \cdot \eta^{k-1} \quad (1 \le j \le \varphi(p^a)) \ ,$$

wobei wegen Satz 1.35 in ganzen Zahlen gilt

$$\mathrm{discr}(\mathcal{B}_2) = (\det(a_{j,k}))^2 \cdot \mathrm{discr}(\mathcal{B}_3) \ ,$$

also $\det(a_{j,k}) \mid \mathrm{discr}(\mathcal{B}_2)$. Da β als Linearkombination der α_j geschrieben werden kann, folgt die Zwischenbehauptung.

Wir nehmen nun an, es gäbe ein $\beta \in \mathcal{O}_F$ mit $\beta \notin \mathbb{Z}[\eta]$. Wegen $(**)$ und $\mathrm{discr}(\mathcal{B}_2) = \pm p^s$ können wir durch Multiplikation von $(**)$ mit einer geeigneten Potenz von p o.B.d.A. annehmen, dass

$$\beta = \sum_{j=d}^{\varphi(p^a)} \frac{z_j}{p} \eta^{j-1}$$

für ein d in $1 \le d \le \varphi(p^a)$, wobei $p \nmid z_d$. Mit einem Argument wie weiter oben im Beweis folgt

$$N_F(1 - \zeta) = p \ .$$

Wegen $(1 - \zeta^j)/(1 - \zeta) = 1 + \zeta + \cdots + \zeta^{j-1} \in \mathbb{Z}[\zeta]$ erhalten wir

$$\frac{p}{\eta^{\varphi(p^a)}} = \frac{N_F(1 - \zeta)}{(1 - \zeta)^{\varphi(p^a)}} = \prod_{\substack{j=1 \\ (j,p^a)=1}}^{p^a} \frac{1 - \zeta^j}{1 - \zeta} \ \in \mathbb{Z}[\zeta] \ ;$$

also insbesondere

$$\frac{p}{\eta^d} = \frac{p}{\eta^{\varphi(p^a)}} \cdot \eta^{\varphi(p^a)-d} \in \mathbb{Z}[\zeta] \ .$$

Dies impliziert, dass

$$\frac{p^\beta}{\eta^d} = \frac{1}{\eta^d} \sum_{j=d}^{\varphi(p^a)} z_j \cdot \eta^{j-1} = \frac{z_d}{\eta} + \sum_{j=d+1}^{\varphi(p^a)} z_j \cdot \eta^{j-d-1}$$

in $\mathcal{O}_F$ liegt, d.h. $z_d/\eta \in \mathcal{O}_F$. Es folgt

$$N_F(\eta) = N_F(1-\zeta) = p \mid N_F(z_d) = z_d^{\varphi(p^a)} \quad \text{Widerspruch! } (p \nmid z_d) \ .$$

Dieser Widerspruch widerlegt unsere Annahme $\beta \in \mathbb{Z}[\eta]$, d.h. der Satz gilt für alle $n = p^a$.

Sei nun $n \in \mathbb{N}$ beliebig mit Primfaktorisierung

$$n = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r} \ .$$

Für $F_j := \mathbb{Q}(\zeta_{p_j^{a_j}})$ haben wir $\mathrm{ggT}(\Delta_{F_k}, \Delta_{F_l}) = 1$ für $k \neq l$ wegen Satz 2.8 und $p_k \neq p_l$. Für zwei Zahlkörper F und G bezeichnet FG den kleinsten Körper in $\mathbb{C}$, der F und G umfaßt (d.h. FG besteht aus allen endlichen Summen $\sum \alpha_i \beta_j$ mit $\alpha_i \in F$ und $\beta_j \in G$). Falls $\mathrm{ggT}(\Delta_F, \Delta_G) = 1$, so folgt nach einem Ergebnis von Hilbert, dass $\mathcal{O}_{FG} = \mathcal{O}_F \mathcal{O}_G$. Bei uns ergibt sich

$$\begin{aligned} \mathcal{O}_{F_1F_2} &= \mathcal{O}_{F_1} \cdot \mathcal{O}_{F_2} = \mathbb{Z}[\zeta_{p_1^{a_1}}] \cdot \mathbb{Z}[\zeta_{p_2^{a_2}}] \\ &= \mathbb{Z}[\zeta_{p_1^{a_1}}, \zeta_{p_2^{a_2}}] = \mathbb{Z}[\zeta_{p_1^{a_1} \cdot p_2^{a_2}}] \end{aligned}$$

und damit induktiv

$$\mathcal{O}_F = \mathcal{O}_{F_1} \cdot \ldots \cdot \mathcal{O}_{F_r} = \mathbb{Z}[\zeta_{p_1^{a_1} \cdot \ldots \cdot p_2^{a_2}}] = \mathbb{Z}[\zeta_n] \ .$$

□

Korollar 2.10

Für $F = \mathbb{Q}(\zeta_{p^a})$ gilt $\Delta_F = (-1)^{\varphi(p^a)/2} \cdot p^{p^{a-1}}(a \cdot (p-1) - 1)$.

Beweis:

Im Beweis von Satz 2.9 haben wir nach Satz 2.9 $\Delta_F = \mathrm{discr}(\mathcal{B}_1)$. Eine etwas genauere Analyse des Vorzeichens in der ersten Zwischenbehauptung dort liefert die gewünschte Aussage.

□

2.3. Einheiten in Ganzzahlringen

Wir listen einige Ergebnisse über Einheiten auf, die uns im Wesentlichen schon bekannt sind.

Satz 2.11

Für $\alpha \in \mathbb{A}$ sind die folgenden Aussagen äquivalent:

(i) α ist eine Einheit.

(ii) $\alpha \mid 1$ in $\mathbb{A}$.

(iii) Für jeden Zahlkörper F mit $\alpha \in F$ gilt $|N_F(\alpha)| = 1$.

(iv) Für $F = \mathbb{Q}(\alpha)$ gilt $|m_{\alpha,\mathbb{Q}}(0)| = 1$.

Beweis:
Die Äquivalenz (i) $\Longleftrightarrow$ (ii) folgt direkt aus der Definition der Einheit. Die Gleichwertigkeit von (i) und (ii) wurde schon im Beweis von Satz 1.46 gezeigt:
$1 = N_F(1) = N_F(\alpha) \cdot N_F(\alpha^{-1})$ mit $N_F(\alpha),\ N_F(\alpha^{-1}) \in \mathbb{Z}$, also $|N_F(\alpha)| = 1$; umgekehrt ist $\pm 1 = N_F(\alpha) = \alpha \cdot \prod_j \alpha^{(j)}$ für die Konjugierten $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(d)}$ vo α, also ist α invertierbar. Zur Äquivalenz von (i) und (iv):
Nach Satz 1.22 (iii) gilt wegen (i) $\Longleftrightarrow$ (iii)

$$|m_{\alpha,\mathbb{Q}}(0)| = 1 \quad \Longleftrightarrow \quad |N_F(\alpha)| = 1 \quad \Longleftrightarrow \quad \alpha \text{ ist Einheit .}$$

□

In den Sätzen 1.46 bzw. 2.4 enthielt die Einheitengruppe jeweils die Komponente bestehend aus Einheitswurzeln. Wir bezeichnen mit $\mathcal{R}_F$ die Menge der Einheitswurzeln in einem gegebenen Zahlkörper F (offenbar ist $\mathcal{R}_F \subseteq \mathcal{U}_F$).

Satz 2.12

Sei F ein Zahlkörper. Dann gilt

(i) $\mathcal{R}_F$ ist eine endliche zyklische Gruppe (bzgl. Multiplikation).

(ii) $|\mathcal{R}_F|$ ist gerade und $\frac{|\mathcal{R}_F|}{2} \mid \Delta_F$.

Beweis:

(i) Offenbar ist $\mathcal{R}_F$ eine kommutative Gruppe mit Einselement 1 und Inversem ζ_n^{n-1} zu gegebenem $\zeta_n \in \mathcal{R}_F$. Ist $[F : \mathbb{Q}] = d$, so existieren nur endlich viele $n \in \mathbb{N}$ mit $\varphi(n) \leq d$ und zu jedem solchen n genau $\varphi(n)$ primitive n-te Einheitswurzeln. Nach Korollar 2.7 ist somit $\mathcal{R}_F$ endlich. Ist $|\mathcal{R}_F| = n$, so gilt nach dem Satz von Lagrange $\zeta^n = 1$ für alle $\zeta_\in \mathcal{R}_F$, d.h. in $\mathcal{R}_F$ liegen nur n-te Einheitswurzeln. Da es aber nur n n-te Einheitswurzeln gibt, folgt mit $|\mathcal{R}_F| = n$, dass $\mathcal{R}_F$ genau aus den n-ten Einheitswurzeln besteht. Jede primitive n-te Einheitswurzel erzeugt also $\mathcal{R}_F$.
(ii) Wegen $\{1, -1\} \subseteq \mathbb{Q} \subseteq F$, also $\{1, -1\} \subseteq \mathcal{R}_F$, haben wir für jedes $\alpha \in \mathcal{R}_F$, dass auch $-\alpha \in \mathcal{R}_F$. Damit ist $|\mathcal{R}_F|$ gerade.
Sei nun $|\mathcal{R}_F| = n$ mit der Primfaktorisierung

$$n = p_1^{a_1} \cdot \ldots \cdot_r^{a_r} \ .$$

Nach (i) besteht $\mathcal{R}_F$ genau aus den n-ten Einheitswurzeln, also insbesondere $\zeta_{p_j^{a_j}} \in \mathcal{R}_F$ für alle $1 \leq j \leq r$. Demnach ist $F_j := \mathbb{Q}(\zeta_{p_j^{a_j}}) \subseteq F$ für alle j, und nach Korollar 2.10 gilt

$$(*) \quad \Delta_{F_j} = \pm p_j^{p_j^{a_j-1}(a_j(p_j-1)-1)} \ .$$

Behauptung: $\Delta_{F_j} \mid \Delta_F$ für $1 \leq j \leq r$.
Seien dazu ganz allgemein $\mathbb{Q} \subseteq K \subseteq L$ Zahlkörper. Dann gilt $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$, also

$$d_1 := [K : \mathbb{Q}] \mid d_2 := [L : \mathbb{Q}] \ .$$

Wir wissen nach Satz 1.39, dass für geeignete Ganzheitsbasen $\{\alpha_1, \ldots, \alpha_{d_1}\}$ bzw. $\{\beta_1, \ldots, \beta_{d_2}\}$

$$\mathcal{O}_K = \bigoplus_{j=1}^{d_1} \mathbb{Z}\alpha_j \quad , \quad \mathcal{O}_L = \bigoplus_{j=1}^{d_2} \mathbb{Z}\beta_j$$

als freie abelsche Gruppen. Wegen $\mathcal{O}_K \subseteq \mathcal{O}_L$ ist $\mathcal{O}_K$ freier Untermodul von $\mathcal{O}_K$, also können wir $\{\alpha_1, \ldots, \alpha_{d_1}\}$ zu einer Ganzheitsbasis $\{\alpha_1, \ldots, \alpha_{d_2}\}$ von L ergänzen. Analog zu Satz 1.35 folgt

$$\begin{aligned} \Delta_L &= \operatorname{discr}(\alpha_1, \ldots, \alpha_{d_2}) = D^2 \cdot \operatorname{discr}(\alpha_1, \ldots, \alpha_{d_1}) \\ &= D^2 \cdot \Delta_K \ , \end{aligned}$$

also $\Delta_K \mid \Delta_L$, und die Zwischenbehauptung ist bewiesen. Mit $(*)$ ergibt sich

$$\prod_{j=1}^{r} p_j^{p_j^{a_j-1}} (a_j(p_j-1)-1) \mid \Delta_F \ .$$

Für $p_j > 2$ ist

$$p_j^{a_j-1}(a_j(p_j-1)-1) \geq a_j \ ,$$

und für $p_j = 2$ gilt

$$p_j^{a_j-1}(a_j(p_j-1)-1) = 2^{a_j-1}(a_j-1) \geq a_j - 1 \ ,$$

also

$$\frac{|\mathcal{R}_F|}{2} = \frac{1}{2} \prod_{j=1}^{r} p_j^{a_j} \left| \prod_{j=1}^{r} p_j^{p_j^{a_j-1}} (a_j(p_j-1)-1) \right| \Delta_F \ .$$

□

Satz 2.13

Sei F ein Zahlkörper mit $[F : \mathbb{Q}] = d$, seien $\Theta_1, \ldots, \Theta_d$ die Einbettungen von F. Zu jedem $r \in \mathbb{R}_{>0}$ existieren nur endlich viele $\alpha \in \mathcal{O}_F$ derart, dass $|\Theta_j(\alpha)| \leq r$ für alle $j = 1, \ldots, d$.

Beweis:

Wir setzen:

$$M := \max\left\{ \binom{d}{j} \cdot r^j \ : \ j = 1, \ldots, d \right\}$$

und

$$\mathcal{F} := \left\{ x^d + \sum_{j=0}^{d} z_j x^j \ \in \mathbb{Z}[x] : \ |z_j| \, M \ (0 \leq j < d) \right\} \ .$$

Offenbar ist $\mathcal{F}$ eine endliche Menge von Polynomen, und damit ist auch

$$\mathcal{S} := \{\alpha \in F : \ f(\alpha) = 0 \text{ für ein } f(x) \in \mathcal{F}\}$$

endlich. Sei nun $\alpha \in F$ mit $|\Theta_j(\alpha)| \leq r$ für alle $j = 1, \ldots, d$. Bezeichnen $s_1, s_2, \ldots, s_d$ die elementarsymmetrischen Funktionen von $x_1, \ldots, x_d$, so folgt

$$\begin{aligned} |s_j(\Theta_1(\alpha), \ldots, \Theta_d(\alpha))| &\leq s_j(r, r, \ldots, r) \\ &= \binom{d}{j} \cdot r^j \leq M \end{aligned}$$

für $j = 1, \ldots, d$. Wegen $\alpha \in \mathcal{O}_F$ wissen wir außerdem, dass alle $s_j(\Theta_1(\alpha), \ldots, \Theta_d(\alpha)) \in \mathbb{Z}$ sind. Also gilt

$$\prod_{j=1}^{d} (x - \Theta_j(\alpha)) = x^d + \sum_{j=1}^{d} (-1)^j s_j(\Theta_1(\alpha), \ldots, \Theta_d(\alpha)) x^{d-j} \ \in \mathcal{F} \ ,$$

und somit $\alpha \in \mathcal{S}$.

□

Korollar 2.14

Es gibt ein $\alpha \in \mathcal{R}_F$ gdw. $|\Theta_j(\alpha)| = 1$ für $j = 1, 2, \ldots, d = [F : \mathbb{Q}]$.

Beweis:

„$\Longrightarrow$“

Ist $\alpha \in \mathcal{R}_F$, so folgt für alle $j = 1, \ldots, d$

$$(\Theta_j(\alpha))^n = \Theta_j(\alpha^n) = \Theta_J(1) = 1$$

mit einem geeigneten $n \in \mathbb{N}$. Also ist $|\Theta_j(\alpha)|^n = 1$, d.h. $|\Theta_j(\alpha)| = 1$.

„$\Longleftarrow$“

Sei $|\Theta_j(\alpha)| = 1$ für $j = 1, \ldots, d$. Nach Satz 2.13 gibt es nur endlich viele $\alpha \in \mathcal{O}_F$ mit dieser Eigenschaft. Für alle $k \in \mathbb{N}$ ist $\alpha^k \in \mathcal{O}_F$ und

$$\left|\Theta_j(\alpha^k)\right| = \left|(\Theta_j(\alpha))^k\right| = |\Theta_j(\alpha)|^k = 1$$

für $j = 1, \ldots, d$. Also gibt es $1 \leq k < l$ mit $\alpha^k = \alpha^l$, d.h. $\alpha^{l-l} = 1$. Das bedeutet $\alpha \in \mathcal{R}_F$.

□

Satz 2.15

Sei $p \neq 2$ Primzahl und ζ_p eine primitve p-te Einheitswurzel. Dann ist

$$\mathcal{R}_F = \langle -1 \rangle \times \langle \zeta_p \rangle$$

als multiplikative Gruppe.

Beweis:

Nach Satz 2.9 ist $\mathcal{O}_F = \mathbb{Z}[\zeta_p]$. Selbsverständlich gilt $\langle -1 \rangle \times \langle \zeta_p \rangle \subseteq \mathcal{R}_F$. Wäre $\langle -1 \rangle \times \langle \zeta_p \rangle \neq \mathcal{R}_F$, so gäbe es ein $\zeta_n \in \mathcal{R}_F$ mit $n \nmid 2p$. Nach Satz 2.12 und Korollar 2.10 haben wir

$$|\mathcal{R}_F| \mid 2\Delta_F = \pm 2 \cdot p^{p-2} \ ,$$

d.h. die Ordnung der Gruppe $\mathcal{R}_F$ ist $2 \cdot p^t$ für ein $t \in \mathbb{N}$. Nach dem Satz von Lagrange hat dann auch jedes Element von $\mathcal{R}_F$ eine Ordnung p^s oder $2p^s$ für ein $s \leq t$.

Nach obiger Annahme existiert also ein $\zeta_{p^2} \in \mathcal{R}_F$. Aber

$$[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}] = \varphi(p^2) = p^2 - p > [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \text{ . Widerspruch!}$$

Damit folgt $\langle -1 \rangle \times \langle \zeta_p \rangle = \mathcal{R}_F$.

□

Bemerkung:

Man kann zeigen, dass für $F = \mathbb{Q}(\zeta_p)$, $p > 2$, jede Einheit $u \in \mathcal{U}_F$ eine Darstellung $u = w \cdot \zeta_p^k$ mit $w \in \mathcal{U}_F \cap \mathbb{R}$ und $k \in \mathbb{N}$ besitzt. Selbstverständlich sind $\pm 1 \in \mathcal{U}_F \cap \mathbb{R}$, aber es gibt noch weitere Elemente in $\mathcal{U}_F \cap \mathbb{R}$:
Sei $u := (1 - \zeta_p^j)/(1 - \zeta_p)$ für ein $j \in \{1, \ldots, p-1\}$. Im Beweis zu Satz 2.9 hatten wir gesehen, dass

$$N_F(1 - \zeta_p^j) = N_F(1 - \zeta_p) = p \text{ ,}$$

also $N_F(u) = 1$, d.h. $u \in \mathcal{U}_F$ nach Satz 2.11. Die komplex Konjugierte von u ist

$$\overline{u} = \frac{1 - \zeta_p^{-j}}{1 - \zeta_p^{-1}} = \frac{\zeta_p^{-j}(\zeta_p^j - 1)}{\zeta_p^{-1}(\zeta_p - 1)} = \zeta_p^{1-j} \cdot u \text{ .}$$

Also ist auch $\overline{u} \in \mathcal{U}_F$. Damit ist

$$u \cdot \overline{u} = \frac{1 - \zeta_p^j}{1 - \zeta_p} \cdot \frac{1 - \zeta_p^{-j}}{1 - \zeta_p^{-1}} = \zeta_p^{1-j} \cdot u^2 \ \in \mathcal{U}_F \cap \mathbb{R} \text{ ,}$$

und für $2 \nmid j$ ist auch

$$v = \sqrt{u\overline{u}} = \zeta_p^{\frac{1-j}{2}} \cdot u \ \in \mathcal{U}_F \cap \mathbb{R} \text{ .}$$

2.4. Geometrie der Zahlen

Die Grundlagen der im Folgenden dargestellten Theorie mit dem Namen „Geometrie der Zahlen“ wurden von Minkowski im 19. Jahrhundert gelegt.

Definition 2.16

Seien $\vec{v}_1, \ldots, \vec{v}_m \in \mathbb{R}^n$ mit $m, n \in \mathbb{N},\ m \leq n$, linear unabhängige Vektoren über $\mathbb{R}$. Dann heißt

$$\Gamma = \left\{ \vec{v} \in \mathbb{R}^n : \vec{v} = \sum_{j=1}^{m} z_j \vec{v}_j,\ z_j \in \mathbb{Z} \right\} = \mathbb{Z}\left[\vec{v}_1, \ldots, \vec{v}_m\right]$$

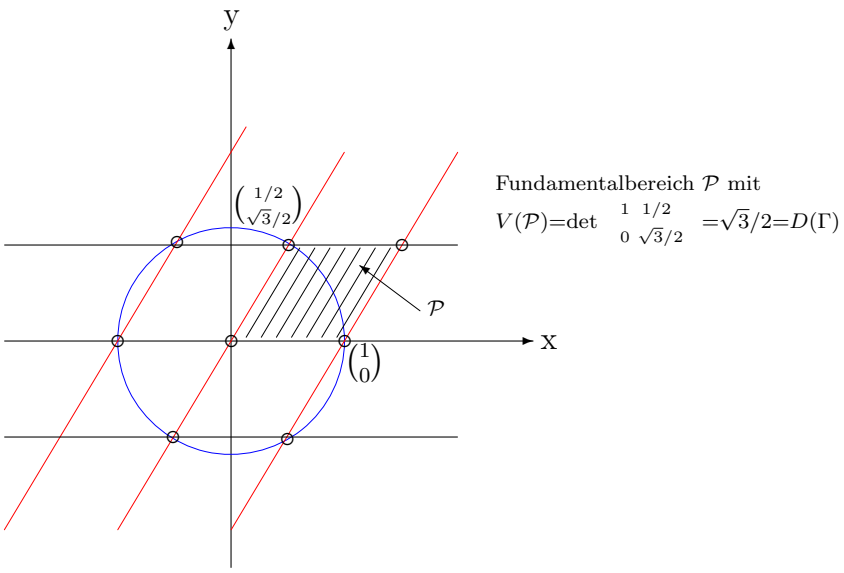
ein *Gitter der Dimension m in $\mathbb{R}^n$*. Für $m = n$ heißt Γ *volles Gitter*, d.h. ein volles Gitter ist eine freie abelsche Gruppe vom Rang n mit einer $\mathbb{Z}$-Basis, die gleichzeitig eine $\mathbb{R}$-Basis des $\mathbb{R}^n$ bildet.
Desweiteren nennen wir für $m = n$

$$\mathcal{P} = \left\{ \sum_{j=1}^{n} r_j \vec{v}_j :\ 0 \leq r_j < 1\ (j = 1, \ldots, n) \right\}$$

den *Fundamentalbereich* (Fundamentalparallelepiped) von Γ. Das Volumen $V(\mathcal{P}) = |\det(\vec{v}_j)|$ des Fundamentalbereichs heißt auch *Diskriminante von* Γ, bezeichnet mit $D(\Gamma)$.

Beispiel:
Sei $F = \mathbb{Q}(\sqrt{3})$. Nach Satz 1.43 haben wir

$$\mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z} + \mathbb{Z} \cdot \frac{1+\sqrt{-3}}{2} \cong \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \end{pmatrix} = \Gamma$$



Eine Menge $S \subseteq \mathbb{R}^n$ heißt diskret, wenn in jeder beschränkten Teilmenge von $\mathbb{R}^n$ höchstens endlich viele Punkte von S liegen.

Satz 2.17

Sei $L \subseteq \mathbb{R}^n, L \neq \emptyset$. Dann ist L ein Gitter, gdw. L eine diskrete, additive Untergruppe von $\mathbb{R}^n$ ist.

Bemerkung:

Häufig wird die in Satz 2.17 genannte Eigenschaft von Gittern als definierende Eigenschaft verwendet.

Üblicherweise heißt eine Menge $S \subseteq \mathbb{R}^n$ konvex, wenn für alle $s, t \in S$ auch die Punkte

$$\lambda s + (1-\lambda)t \quad (0 \leq \lambda \leq 1)$$

in S liegen, d.h. mit s und t liegt auch die Verbindungsstrecke in S. Nach einem Satz von Blaschke besitzen konvexe Mengen in $\mathbb{R}^n$ ein Volumen, nämlich

$$V(S) = \int_S \dots \int dx_1 \dots dx_n \ .$$

Eine Menge $S \subseteq \mathbb{R}^n$ heißt symmetrisch, falls für jedes $s \in S$ auch $-s \in S$ gilt. Beispiele für konvexe Mengen im $\mathbb{R}^2$ sind Ellipsen und Quadrate; Beispiele für beschränkte, symmetrische, konvexe Mengen im $\mathbb{R}^n$ sind n-dimensionale Würfel

$$\{\vec{s} = (s_1, \ldots, s_n) \in \mathbb{R}^n : \ |s_j| \leq 1 \ (j = 1, \ldots, n)\}$$

und die n-dimensionale Einheitskugel

$$\{\vec{s} \in \mathbb{R}^n : \ |\vec{s}| \leq 1\} \ .$$

Lemma 2.18

Sei $S \subseteq \mathbb{R}^n$ beschränkt, und sei $\Gamma \subseteq \mathbb{R}^n$ ein volles Gitter. Sind die verschobenen Mengen

$$S_{\vec{z}} := S + \vec{z} := \{\vec{s} + \vec{z} : \ \vec{s} \in S\} \quad (\vec{z} \in \Gamma)$$

paarweise disjunkt, d.h. $S_{\vec{z}_1} \cap S_{\vec{z}_2} = \emptyset$ für $\vec{z}_1, \vec{z}_2 \in \Gamma, \ \vec{z}_1 \neq \vec{z}_2$, so gilt für das Volumen des Fundamentalbereichs $\mathcal{P}$

$$V(\mathcal{P}) \geq V(S) \ .$$

Beweis:

Wegen $\mathcal{P}_{\vec{z}_1} \cap \mathcal{P}_{\vec{z}_2} = \emptyset$ für $\vec{z}_1, \vec{z}_2 \in \Gamma, \ \vec{z}_1 \neq \vec{z}_2$, und $\bigcup_{\vec{z} \in \Gamma} \mathcal{P}_{\vec{z}} = \mathbb{R}^n$ haben wir die disjunkte Zerlegung

$$S = \bigcupdot_{\vec{z} \in \Gamma} (S \cap \mathcal{P}_{-\vec{z}}) \ ,$$

also

$$V(S) = \sum_{\vec{z} \in \Gamma} V\left(S \cap \mathcal{P}_{-\vec{z}}\right) \ .$$

Mit $(S \cap \mathcal{P}_{-\vec{z}}) + \vec{z} = S_{\vec{z}} \cap \mathcal{P}$ folgt $V\left(S \cap \mathcal{P}_{-\vec{z}}\right) = V\left(S_{\vec{z}} \cap \mathcal{P}\right)$ und damit

$$V(S) = \sum_{\vec{z} \in \Gamma} V\left(S_{\vec{z}} \cap \mathcal{P}\right) \ .$$

Da die $S_{\vec{z}}$ paarweise disjunkt sind, so gilt dies erst recht für die $(S_{\vec{z}} \cap \mathcal{P})$. Mit $S_{\vec{z}} \cap \mathcal{P} \subseteq \mathcal{P}$ ergibt sich

$$V(S) = \sum_{\vec{z} \in \Gamma} V\left(S_{\vec{z}} \cap \mathcal{P}\right) \leq V(\mathcal{P}) \ ,$$

also insgesamt die Behauptung.

□

Satz 2.19 (Minkowskis Gitterpunktsatz)

Sei $\Gamma \in \mathbb{R}^n$ ein volles Gitter mit Fundamentalbereich $\mathcal{P}$. Ist $S \subseteq \mathbb{R}^n$ symmetrisch und konvex derart, dass

$$V(S) > 2^n \cdot V(\mathcal{P}) \ ,$$

so gibt es einen Punkt $\vec{x} \in S \cap \Gamma$ mit $\vec{x} \neq \vec{0}$.
(Für unbeschränktes S setzen wir $V(S) := \infty$).

Beweis:

Sei o.B.d.A. S beschränkt; andernfalls wählen wir eine beschränkte Teilmenge von S mit hinreichend großem Volumen (z.B. $S \cap \{\vec{s} \in \mathbb{R}^n : \ |\vec{s}| \leq r\}$, $r \in \mathbb{R}$ groß). Sei $T := 1/2 \cdot S := \{1/2 \cdot \vec{s} : \ \vec{s} \in S\}$. Dann gilt

$$V(T) = \frac{1}{2^n} V(S) > V(\mathcal{P}) \ .$$

Wären alle $T_{\vec{z}} = 1/2 \cdot S + \vec{z}$ paarweise disjunkt, so wäre nach Lemma 2.18 $V(\mathcal{P}) \geq V(T)$. Widerspruch! Also gibt es $\vec{s} \neq \vec{t} \in \Gamma$ mit

$$T_{-\vec{s}} \cap T_{\vec{t}} = \left(\frac{1}{2}S - \vec{s}\right) \cap \left(\frac{1}{2}S - \vec{t}\right) \neq \emptyset \ .$$

Seien $\vec{x}, \vec{y} \in S$ so, dass $1/2 \cdot \vec{x} - \vec{s} = 1/2 \cdot \vec{y} - \vec{t}$, d.h. $\vec{t} - \vec{s} = 1/2 \cdot \vec{y} - 1/2 \cdot \vec{x}$. Da S symmetrisch und konvex ist, haben wir $-\vec{x} \in S$ und $1/2 \cdot \vec{y} + 1/2 \cdot (-\vec{x}) \in S$, also $\vec{t} - \vec{s} \in S$. Außerdem ist $\vec{t} - \vec{s} \in \Gamma$, zusammen also $\vec{t} - \vec{s} \in S \cap \Gamma \setminus \{\vec{0}\}$.

□

Korollar 2.20 (Minkowskis Linearformensatz)

Für $j = 1, \ldots, n$ seien die Linearformen

$$L_j(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{i,j} x_i$$

mit $a_{i,j} \in \mathbb{C}$ gegeben, wobei zu L_j ein $L_{j'}$ existiert, mit $L_{j'}(\vec{x}) = \overline{L_j(\vec{x})} := \sum_{i=1}^{n} \overline{a_{i,j}} x_i$ (diese Bedingung ist leer, sofern die $a_{i,j} \in \mathbb{R}$ sind). Sei $\Gamma \subseteq \mathbb{R}^n$ ein volles Gitter mit Diskriminante $D(\Gamma)$. Sind $c_1, \ldots, c_n \in \mathbb{R}_{>0}$ mit $c_j = c_{j'}$ und

$$\prod_{j=1}^{n} c_j \geq |\det(a_{i,j})| \cdot D(\Gamma) \ ,$$

so existiert ein $\vec{x} \in \Gamma,\ \vec{x} \neq \vec{0}$ derart, dass

$$|L_1(\vec{x})| \leq c_1 \quad \text{und} \quad |L_j(\vec{x})| < c_j \ (j = 2, \ldots, n) \ .$$

Beweis: (nur für den reellen Fall $a_{i,j} \in \mathbb{R}$)
Zu festem ε mit $0 < \varepsilon < 1$ sei $S_\varepsilon \subseteq \mathbb{R}^n$ definiert durch

$$S_\varepsilon := \{\vec{x} \in \mathbb{R}^n : \ |L_1(\vec{x})| < c_1 + \varepsilon, \ |L_j(\vec{x})| < c_j \ (j = 2, \ldots, n)\} \ .$$

Offenbar ist S_ε eine von Hyperebenen begrenzte beschränkte, konvexe und symmetrische Menge. Es folgt

$$V(S_\varepsilon) > \frac{1}{|\det(a_{i,j})|} \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_n}^{c_n} dx_n = \frac{2^n \cdot c_1 \cdot \ldots \cdot c_n}{|\det(a_{i,j})|} \geq 2^n \cdot D(\Gamma)$$

für jedes $\varepsilon > 0$. Also gibt es nach Satz 2.19 zu jedem $\varepsilon > 0$ ein $\vec{x}_\varepsilon \in \Gamma \setminus \{\vec{0}\}$ mit

$$|L_1(\vec{x}_\varepsilon)| < c_1 + \varepsilon \quad \text{und} \quad |L_j(\vec{x}_\varepsilon)| < c_j \quad (j = 2, \ldots, n) \ .$$

Da $\vec{x}_\varepsilon \in \Gamma \cap\ S_\varepsilon$, also $\vec{x}_\varepsilon$ aus einer endlichen Menge stammt, gibt es ein $\vec{x} \in \Gamma \setminus \{\vec{0}\}$, so dass

$$|L_1(\vec{x})| < c_1 + \varepsilon \quad \text{und} \quad |L_j(\vec{x})| < c_j \quad (j = 2, \ldots, n)$$

für alle $\varepsilon > 0$, und dieses $\vec{x}$ erfüllt die Behauptung des Korollars.

□

Satz 2.21

Für einen Zahlkörper $F \neq \mathbb{Q}$ gilt $|\Delta_F| \geq 2$.

Beweis:

Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine Ganzheitsbasis von F mit den Konjugierten $\alpha_i^{(1)}, \ldots, \alpha_i^{(n)}$ von $\alpha_i = \alpha_i^{(1)}$ für $i = 1, \ldots, n$. Seien

$$L_j(x_1, \ldots, x_n) := \sum_{i=1}^{n} \alpha_i^{(j)} x_j \quad (j = 1, \ldots, n) \ ,$$

und sei $\Gamma := \mathbb{Z}^n$, also $D(\Gamma) = 1$. Wir wählen
$c_1 = c_2 = \cdots = c_n = |\Delta_F|^{1/2n} = \sqrt[n]{|\det(\alpha_i^{(j)}|}$. Damit sind alle Bedingungen aus Korollar 2.20 erfüllt, insbesondere

$$\prod_{j=1}^{n} c_j = \left|\det(\alpha_i^{(j)})\right| \cdot D(\Gamma) \ .$$

Somit existieren $x_1, \ldots, x_n \in \mathbb{Z}$, nicht alle 0 derart, dass

$$|N_F(x_1\alpha_1 + \cdots + x_n\alpha_n)| = \prod_{j=1}^{n} |L_j(x_1, \ldots, x_n)| < \prod_{j=1}^{n} c_j = \sqrt{|\Delta_F|} \ .$$

Mit $x_1\alpha_1 + \cdots + x_n\alpha_n \in \mathcal{O}_F$ folgt $|N_F(x_1\alpha_1 + \cdots + x_n\alpha_n)| \geq 1$ und damit die Behauptung.

□

Definition 2.22

Sei $\{r_1, r_2\}$ die Signatur eines Zahlkörpers F, seien $\Theta_j(F) \subseteq \mathbb{R}$ für $j = 1, \ldots, r_1$ und $\Theta_j(F) \nsubseteq \mathbb{R}$ für $j = r_1+1, \ldots, r_1+r_2$ und $\Theta_j = \overline{\Theta}_{j-r_2}$ für $j = r_1+r_2+1, \ldots, r_1+2r_2$. Wir definieren die Abbildung

$$\Theta_F := \begin{cases} F & \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} \\ \alpha & \longmapsto (\Theta_1(\alpha), \ldots, \Theta_{r_1}(\alpha), \Theta_{r_1+1}(\alpha), \ldots, \Theta_{r_1+r_2}(\alpha)) \\ & \cong (\Theta_1(\alpha), \ldots, \Theta_{r_1}(\alpha), \mathrm{Re}\ \Theta_{r_1+1}(\alpha), \mathrm{Im}\ \Theta_{r_1+1}(\alpha), \ldots) \ . \end{cases}$$

Bemerkungen:

(i) Sowohl F wie auch $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ sind $\mathbb{Q}$-Algebren (d.h. kommutative Ringe mit Einselement und gleichzeitig $\mathbb{Q}$-Moduln, wobei $r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta)$ für $r \in \mathbb{Q}$ und α, β aus der Algebra), und Θ_F ist ein injektiver $\mathbb{Q}$-Algebra-Homomorphismus (d.h. Ring-Homomorphismus und $\mathbb{Q}$-Modul-Monomorphismus). Dabei ist die Multiplikation auf $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ komponentenweise erklärt.

(ii) Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine Ganzheitsbasis von F, so sind die Vektoren $\Theta_F(\alpha_1), \ldots \Theta_F(\alpha_n) \in \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$, denn sonst wäre $\det(\Theta_F(\alpha_i)) = 0$ und somit $\Delta_F = 0$ (siehe unten). Also ist

$$\Theta_F(\mathcal{O}_F) = \Theta_F\left(\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n\right)$$

ein volles Gitter in $\mathbb{R}^n$. Für den zugehörigen Fundamentalbereich $\mathcal{P}_{\mathcal{O}_F}$ haben wir wegen $\mathrm{Re}\ z = (z + \overline{z})/2$ und $\mathrm{Im}\ z = (z - \overline{z})/(2\sqrt{-1})$ $(z \in \mathbb{C})$

$$
\begin{aligned}
V(\mathcal{P}_{\mathcal{O}_F}) &= \left|\det\big((\Theta_1(\alpha_i),\dots,\Theta_{r_1}(\alpha_i),\operatorname{Re}\Theta_{r_1+1}(\alpha_i),\operatorname{Im}\Theta_{r_1+1}(\alpha_i),\dots,\operatorname{Re}\Theta_{r_1+r_2}(\alpha_i),\operatorname{Im}\Theta_{r_1+r_2}(\alpha_i))\big)\right| \\
&= \left|\det\left(\left(\dots,\frac{z+\overline{z}}{2},\frac{z-\overline{z}}{2\sqrt{-1}},\dots\right)\right)\right| \qquad \text{mit } z := \Theta_{r_1+1}(\alpha_i) \\
&= \left|\left(\sqrt{-1}\right)^{-r_2}\cdot\det\left(\left(\dots,\frac{z+\overline{z}}{2},\frac{z-\overline{z}}{2},\dots\right)\right)\right| \\
&= \left|\det\left(\left(\dots,z,\frac{z-\overline{z}}{2},\dots\right)\right)\right| \\
&= \left|\det\left(\left(\dots,z,\frac{-\overline{z}}{z},\dots\right)\right)\right| \\
&= \left|\left(-\frac{1}{2}\right)^{r_2}\cdot\det\left((\dots,z,\overline{z},\dots)\right)\right| \\
&= \left|\left(-\frac{1}{2}\right)^{r_2}\cdot\det\left(\left(\Theta_1(\alpha_i),\dots,\Theta_{r_1}(\alpha_i),\Theta_{r_1+1}(\alpha_i),\overline{\Theta_{r_1+1}(\alpha_i)},\dots\right)\right)\right| \\
&= \left(\frac{1}{2}\right)^{r_2}\cdot\sqrt{|\Delta_F|}\ .
\end{aligned}
$$

(iii) Sei $M \subseteq F$ ein freier $\mathbb{Z}$-Modul vom Rang $n = [F:\mathbb{Q}]$. Ist der Index $[\mathcal{O}_F : M] = m \in \mathbb{N}$, so ist das volle Gitter $\Theta(M) \subseteq \mathbb{R}^n$ ein Teilgitter von $\Theta(\mathcal{O}_F)$, und für den Fundamentalbereich $\mathcal{P}_M$ gilt $V(\mathcal{P}_M) = m \cdot V(\mathcal{O}_F)$.

Satz 2.23

Sei $\{r_1, r_2\}$ die Signatur eines Zahlkörpers F mit $[F:\mathbb{Q}] = n = r_1 + 2r_2$. Sei $M \subseteq \mathcal{O}_F$ ein $\mathbb{Z}$-Modul von endlichem Index in $\mathcal{O}_F$, d.h. $m := [\mathcal{O}_F : M] \in \mathbb{N}$ (also ist insbesondere der Rang von M gleich dem Rang des $\mathbb{Z}$-Moduls $\mathcal{O}_F$). Dann gibt es ein $\alpha \in M \setminus \{0\}$ mit

$$|N_F(\alpha)| \le \left(\frac{4}{\pi}\right)^{r_2}\cdot\frac{n!}{n^n}\cdot m\cdot\sqrt{|\Delta_f|}\ .$$

Beweis:

Für $B \in \mathbb{R}_{>0}$ setzen wir

$$S_B(r_1,r_2) := \left\{(\alpha_1,\dots,\alpha_{r_1},\beta_1,\dots,\beta_{r_2}) \in \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} :\ \sum_{j=1}^{r_1}|\alpha_j| + 2\cdot\sum_{j=1}^{r_2}|\beta_j| \le B\right\}\ ,$$

wobei wir $S_B(r_1, r_2)$ auch als Teilmenge des $\mathbb{R}^{r_1+2r_2}$ auffassen können. Offenbar ist $S_B(r_1, r_2)$ beschränkt und symmetrisch. Außerdem ist $S_B(r_1, r_2)$ konvex, denn: Seien $(\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2})$, $(\gamma_1, \ldots, \gamma_{r_1}, \delta_1, \ldots, \delta_{r_2}) \in S_B(r_1, r_2)$. Dann gilt für $\mu \geq 0,\ \lambda \geq 0,\ \mu + \lambda = 1$

$$\begin{aligned}
\sum_{j=1}^{r_1} |\mu\alpha_j + \lambda\gamma_j| + 2 \cdot \sum_{j=1}^{r_2} |\mu\beta_j + \lambda\delta_j| &\leq \sum_{j=1}^{r_1} \mu|\alpha_j| + \sum_{j=1}^{r_1} \lambda|\gamma_j| + 2 \cdot \sum_{j=1}^{r_2} \mu|\beta_j| + 2 \cdot \sum_{j=1}^{r_2} \lambda|\delta_j| \\
&\leq \mu \left(\sum_{j=1}^{r_1} |\alpha_j| + 2 \cdot \sum_{j=1}^{r_2} |\beta_j| \right) + \lambda \left(\sum_{j=1}^{r_1} |\gamma_j| + 2 \cdot \sum_{j=1}^{r_2} |\delta_j| \right) \\
&\leq \mu B + \lambda B = (\mu + \lambda) \cdot B = B \ ,
\end{aligned}$$

d.h. $\mu(\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}) + \lambda(\gamma_1, \ldots, \gamma_{r_1}, \delta_1, \ldots, \delta_{r_2}) \in S_B(r_1, r_2)$.

Behauptung: $V(S_B(r_1, r_2)) = 2^{r_1} \cdot (\pi/2)^{r_2} \cdot B^n/n!$.
Wir benutzen Doppelinduktion über r_1 und r_2. Der Induktionsanfang besteht aus den Fällen $r_1 = 1,\ r_2 = 0$ und $r_1 = 0,\ r_2 = 1$: Es ist $S_B(1, 0)$ das Intervall $[-B, B] \subseteq \mathbb{R}$, also $n = 1$, und mit $V(S_B(1, 0)) = 2B$ gilt die Behauptung. Des Weiteren ist $S_B(0, 1)$ die Kreisscheibe mit Radius $B/2$ um $\vec{0}$ in $\mathbb{R}^2 \cong \mathbb{C}$, also $n = 2$ und

$$V(S_B(0, 1)) = \pi \cdot \frac{B^2}{4}$$

wie behauptet. Als Induktionshypothese dürfen wir nun annehmen, dass

$$(*) \qquad V(S_B(m, k)) = 2^m \cdot \left(\frac{\pi}{2}\right)^k \cdot \frac{B^n}{n!} \qquad (m \leq r_1,\ k \leq r_2) \ .$$

Wir untersuchen zuerst $S_B(r_1 + 1, r_2)$, definiert durch die Ungleichung

$$|\alpha| + \sum_{j=1}^{r_1} |\alpha_j| + 2 \cdot \sum_{j=1}^{r_2} |B_j| \leq B \ ,$$

wobei $\alpha \in \mathbb{R}$ mit $|\alpha| \leq B$ und $n = r_1 + 2r_2 + 1$. Mit $(*)$ folgt

$$\begin{aligned}
V(S_B(r_1 + 1, r_2)) &= \int_{-B}^{B} V\left(S_{B-|\alpha|}(r_1, r_2)\right) d\alpha \\
&= \frac{2^{r_1}}{(r_1 + 2r_2)!} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \int_{-B}^{B} (B - |\alpha|)^{r_1+2r_2} d\alpha
\end{aligned}$$

$$
\begin{aligned}
&= \frac{2^{r_1}}{(r_1+2r_2)!}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\int_0^B (B-\alpha)^{r_1+2r_2}d\alpha \\
&= \frac{2^{r_1}}{(r_1+2r_2)!}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{B^{r_1+2r_2+1}}{r_1+2r_2+1} = 2^{r_1+1}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{B^n}{n!}\ .
\end{aligned}
$$

Es bleibt $S_B(r_1, r_2+1)$ mit der Ungleichung

$$\sum_{j=1}^{r_1}|\alpha_j| + 2\cdot\sum_{j=1}^{r_2}|\beta_j| + 2|\beta| \le B\ ,$$

wobei $\beta = x+yi \in \mathbb{C}$ mit $|\beta|^2 = x^2+y^2 \le (B/2)^2$ und $n = r_1+2(r_2+1)$. Mit $(*)$ kommt

$$
\begin{aligned}
V\left(S_B\left(r_1, r_2+1\right)\right) &= \iint\limits_{x^2+y^2\le B^2/4} V\left(S_{B-2\sqrt{x^2+y^2}}(r_1,r_2)\right)dx\,dy \\
&= \frac{2^{r_1}}{(r_1+2r_2)!}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\iint\limits_{x^2+y^2\le B^2/4}\left(B-2\sqrt{x^2+y^2}\right)^{r_1+2r_2}dx\,dy \\
&= \frac{2^{r_1}}{(n-2)!}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\int_0^{B/2}\int_0^{2\pi}(B-2\omega)^{n-2}\omega\ dn\,d\omega \quad \text{(Polarkoordinaten)} \\
&= 2^{r_1}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{2\pi}{(n-2)!}\cdot\int_0^{B/2}(B-2\omega)^{n-2}\omega\,d\omega \\
&= 2^{r_1}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{2\pi}{(n-2)!}\cdot\frac{B^n}{4(n-1)\cdot n} \quad \text{(partielle Integration)} \\
&= 2^{r_1}\cdot\left(\frac{\pi}{2}\right)^{r_2+1}\cdot\frac{B^n}{n!}\ .
\end{aligned}
$$

Damit ist die Zwischenbehauptung gezeigt.

Sei $0<\varepsilon<1$. Wir setzen

$$B_\varepsilon := \left(\left(\frac{4}{\pi}\right)^{r_2}\cdot n!\cdot m\cdot\sqrt{|\Delta_F|}+\varepsilon\right)^{1/n}\ .$$

Nach Zwischenbehauptung und Bemerkung (ii) und (iii) nach Definition 2.22 erhalten wir

$$
\begin{aligned}
V\left(S_{B_\varepsilon}(r_1,r_2)\right) &= 2^{r_1}\cdot\frac{\pi}{2}^{r_2}\cdot\frac{1}{n!}\cdot\left(\left(\frac{4}{\pi}\right)^{r_2}\cdot n!\cdot m\cdot\sqrt{|\Delta_F|}+\varepsilon\right) \\
&= 2^{r_1+r_2}\cdot\sqrt{|\Delta_F|}+\frac{1}{n!}\cdot 2^{r_1-r_2}\cdot\pi^{r_2}\cdot\varepsilon \\
&> m\cdot\left(2^{-r_2}\cdot\sqrt{|\Delta_F|}\right)\cdot 2^n = m\cdot V(\mathcal{O}_F)\cdot 2^n = V(\mathcal{P}_M)\cdot 2^n\ .
\end{aligned}
$$

Wir können nun Minkowskis Gitterpunktsatz 2.19 für das volle Gitter $\Theta(M) \subseteq \mathbb{R}^n$ und die symmetrische, konvexe Menge $S_{B_\varepsilon}(r_1, r_2) \subseteq \mathbb{R}^n$ anwenden und erhalten ein $\alpha_\varepsilon \in M \setminus \{0\}$ mit $\Theta(\alpha_\varepsilon) \in S_{B_\varepsilon}(r_1, r_2)$. Wegen $\sqrt[n]{x_1 \cdot \ldots \cdot x_n} \leq 1/n \cdot (x_1 + \cdots + x_n)$ für $x_i \in \mathbb{R}_{\geq 0}$ folgt

$$\begin{aligned} |N_F(\alpha_\varepsilon)| &= \prod_{j=1}^{r_1} |\Theta_j(\alpha_\varepsilon)| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\Theta_j(\alpha_\varepsilon)|^2 \\ &\leq \left(\frac{1}{n} \cdot \prod_{j=1}^{r_1} |\Theta_j(\alpha_\varepsilon)| + \frac{2}{n} \cdot \prod_{j=r_1+1}^{r_1+r_2} |\Theta_j(\alpha_\varepsilon)| \right)^n \leq \left(\frac{b_\varepsilon}{n} \right)^n , \end{aligned}$$

wobei die letzte Ungleichung genau die Bedingung $\Theta(\alpha_\varepsilon) \in S_{B_\varepsilon}(r_1, r_2)$ widerspiegelt. Nach Definition von B_ε erhalten wir

$$(**) \qquad |N_F(\alpha_\varepsilon)| \leq \left(\frac{4}{\pi} \right)^{r_2} \cdot \frac{n!}{n^n} \cdot m \cdot \sqrt{|\Delta_F|} + \varepsilon \ .$$

Wegen $0 < \varepsilon < 1$ gibt es für α_ε nur endlich viele Möglichkeiten in $M \setminus \{0\}$. Also existiert ein $\alpha \in M \setminus \{0\}$ derart, dass $(**)$ für alle $\varepsilon > 0$ gilt. Somit folgt der Satz.

□

Als Anwendung geben wir zunächst eine untere Abschätzung für Diskriminanten.

Satz 2.24

Ist F ein Zahlkörper mit Signatur $\{r_1, r_2\}$ und $n = [F : \mathbb{Q}] = r_1 + 2r_2$, so gilt

$$|\Delta_F| \geq \left(\frac{\pi}{4} \right)^{2r_2} \cdot \left(\frac{n^n}{n!} \right)^2 .$$

Beweis:

Sei $M := \mathcal{O}_F$. Nach Satz 2.23 mit $m = [\mathcal{O}_F : M] = 1$ folgt

$$|\Delta_F| \geq \left(\frac{\pi}{4} \right)^{2r_2} \cdot \left(\frac{n^n}{n!} \right)^2 \cdot N_F(\alpha)^2$$

für ein $\alpha \in \mathcal{O}_F \setminus \{0\}$. Mit $N_F(\alpha) \geq 1$ ergibt sich das Gewünschte.

□

Korollar 2.25

Für einen Zahlkörper F mit $[F:\mathbb{Q}] = n$ gilt

$$|\Delta_F| > \left(\frac{11}{12}\right)^2 \cdot \left(\frac{\pi e^2}{4}\right)^n \cdot \frac{1}{2\pi n} \ .$$

Beweis:

Nach der Formel von Stirling für $n!$ ist für ein c, $0 < c < 1$,

$$\frac{n^n}{n!} = \frac{1}{\sqrt{2\pi n}} \cdot e^{n - c/12n} \ .$$

Wegen $e^{c/12n} < e^{1/12} < \sum_{j=0}^{\infty} 1/12^j = 12/11$ und Satz 2.24 erhalten wir

$$|\Delta_F| > \left(\frac{\pi}{4}\right)^{2r_2} \cdot \left(\frac{n^n}{n!}\right)^2 > \left(\frac{\pi}{4}\right)^{2r_2} \cdot \left(\frac{11e^n}{12}\right)^2 \cdot \frac{1}{2\pi n} \geq \left(\frac{11}{12}\right)^2 \cdot \left(\frac{\pi e^2}{4}\right)^n \cdot \frac{1}{2\pi n} \ .$$

□

Satz 2.26 (von Hermite)

Sei $d \in \mathbb{N}$ gegeben. Dann existieren höchstens endlich viele Zahlkörper F mit $|\Delta_F| = d$.

Beweis:

Zu gegebenem $d \in \mathbb{N}$ ist $|\Delta_F| > d$ für alle Zahlkörper F mit $[F:\mathbb{Q}] \geq n_0$ für ein hinreichend großes n_0 gemäß Korollar 2.25. Also ist nur zu zeigen, dass zu festem $d \in \mathbb{N}$ und $n \in \mathbb{N}$ höchstens endlich viele Zahlkörper$F$ mit $|\Delta_F| \leq D$ und $[F:\mathbb{Q}] = n$ existieren.

Nach Satz 2.21 haben wir für $d = 1$ nur den Zahlkörper $F = \mathbb{Q}$, d.h. $r_1 = 1, r_2 = 0$. Sei also $d \geq 2$. Für $r_1 = 0$ und $r_2 = 1$ ist $n = r_1 + 2r_2 = 2$, also ist $F = \mathbb{Q}(\sqrt{D})$ für ein quadratfreies $D < 0$. Nach Satz 1.43 ist $\Delta_F = 4D$ oder $\Delta_f = D$, es gibt jedenfalls höchstens einen quadratischen Zahlkörper mit $\Delta_f = d$.

Wir dürfen im Folgenden $r := r_1 + r_2 \geq 2$ voraussetzen und werden zeigen, dass ein $\delta \in F$ mit $F = \mathbb{Q}(\delta)$ existiert, wobei δ aus einer endlichen Menge stammt, die nur von d abhängt.

1. Fall: $r_1 \neq 0$.

Wir definieren

$$\begin{aligned} S_1 \;=\; & \{(\alpha_1, \ldots, \alpha_{r_1}, \beta_{r_1+1}, \gamma_{r_1+1}, \ldots, \beta_r, \gamma_r) \in \mathbb{R}^n : \\ & |\alpha_1| < \sqrt{d+1}, |\alpha_i| < 1 \;\; (2 \leq i \leq r_1),\; \beta_j^2 + \gamma_j^2 < 1 \;\; (r_1 + 1 \leq j \leq r)\Big\} \; . \end{aligned}$$

Selbstverständlich ist $S_1 \subseteq \mathbb{R}^n$ beschränkt und symmetrisch. Wir zeigen, dass S_1 auch konvex ist. Dazu seien $\lambda, \mu \geq 0$ mit $\lambda + \mu = 1$. Wir nehmen an, dass $(\alpha_1, \ldots, \alpha_{r_1}, \beta_{r_1+1}, \gamma_{r_1+1}, \ldots, \beta_r, \gamma_r),\; (\delta_1, \ldots, \delta_{r_1}, \rho_{r_1+1}, \sigma_{r_1+1}, \ldots, \rho_r, \sigma_r) \in S_1$. Dann gilt für $j = 2, \ldots, r_1$

$$|\lambda\alpha_j + \mu\delta_j| \leq \lambda|\alpha_j| + \mu|\delta_j| < \lambda + \mu = 1 \; ,$$

und

$$|\lambda\alpha_1 + \mu\delta_1| \leq \lambda|\alpha_1| + \mu|\delta_1| < \lambda\sqrt{d+1} + \mu\sqrt{d+1} = \sqrt{d+1} \; .$$

Für $j = r_1 + 1, \ldots, r$ haben wir

$$\lambda\left(\beta_j^2 + \gamma_j^2\right) + \mu\left(\rho_j^2 + \sigma_j^2\right) < \lambda + \mu = 1 \; .$$

Insgesamt hat sich S_1 als konvex herausgestellt.

2. Fall: $r_1 = 0$.

Wir definieren

$$S_2 = \Big\{(\beta_1, \gamma_1, \ldots, \beta_r, \gamma_r) \in \mathbb{R}^n :\; |\beta_1| < 1,\; |\gamma_1| < \sqrt{d+1},\; \beta_j^2 + \gamma_j^2 < 1 \;\; (2 \leq j \leq r)\Big\} \; .$$

Wie im ersten Fall lässt sich zeigen, dass $S_2 \subseteq \mathbb{R}^n$ beschränkt, symmetrisch und konvex ist. Durch Integration über Produkte von Intervallen und Kreisen erhalten wir (analog zum Beweis von Satz 2.23)

$$V(S_1) = 2^{r_1} \cdot \pi^{r_2} \cdot \sqrt{d+1} \quad \text{und} \quad V(S_2) = 2 \cdot \pi^{r_2 - 1} \cdot \sqrt{d+1} \; ,$$

und mit Bemerkung (ii) nach Definition 2.22 erhalten wir

$$V(S_1) > 2^{r_1 + r_2} \cdot \sqrt{|\Delta_F|} = 2^{r_1 + 2r_2} \cdot V(\mathcal{P}_{\mathcal{O}_F}) = 2^n \cdot V(\mathcal{P}_{\mathcal{O}_F})$$

bzw. (wegen $r_2 \geq 1$ für $r_1 = 0$)

$$V(S_2) > 2^{r_2} \cdot \sqrt{|\Delta_F|} = 2^{2r_2} \cdot V(\mathcal{P}_{\mathcal{O}_F}) = 2^n \cdot V(\mathcal{P}_{\mathcal{O}_F}) \ .$$

Nach Minkowskis Gitterpunktsatz 2.19 gibt es $\delta_1, \delta_2 \in \mathcal{O}_F \setminus \{0\}$ mit $\Theta(\delta_j) \in \Theta(\mathcal{O}_F) \cap S_j$ für $j = 1, 2$. Wegen $\Theta(\delta_j) \in S_j$ können wir folgendes feststellen:
Für die Konjugierten $\delta_j = \delta_j^{(1)}, \delta_j^{(2)}, \ldots, \delta_j^{(n)}$ (unter Umständen mit Wiederholung) von δ_j ist

(i) $|\delta_1^{(1)}| < \sqrt{d+1}$ und $|\delta_1^{(l)}| < 1$ für $l = 2, \ldots, n$;

(ii) $|\delta_2^{(1)}| = |\overline{\delta_2^{(1)}}| = |\delta_2^{(2)}| < \sqrt{1^2 + \sqrt{d+1}^2} = \sqrt{d+2}$ und $|\delta_2^{(l)}| < 1$ für $l = 3, \ldots, n$.

Es folgt mit $\delta_j \in \mathcal{O}_F \setminus \{0\}$, dass

$$1 \leq |N_F(\delta_j)| = |\delta_j^{(1)}, \delta_j^{(2)}, \ldots, \delta_j^{(n)}| \ ,$$

also $|\delta_j^{(1)}| > 1$. Damit tritt $\delta_j^{(1)}$ unter den anderen Konjugierten $\delta_j^{(2)}, \ldots, \delta_j^{(n)}$, nicht mehr auf, d.h. es gibt darunter keine Wiederholungen. Also sind die Konjugierten $\delta_j^{(1)}, \ldots, \delta_j^{(n)}$ paarweise verschieden, und das bedeutet $[\mathbb{Q}(\delta_j) : \mathbb{Q}] = n$, mit anderen Worten $F = \mathbb{Q}(\delta_j)$.
Es bleibt nur noch zu zeigen, dass δ_j aus einer endlichen Menge stammt, die nur von d abhängt. Nach den obigen Überlegungen haben wir für gewisse $z_j \in \mathbb{Z}$ mit $z_n = 1$

$$m_{\delta_j, \mathbb{Q}}(x) = \sum_{j=0}^{n} z_j x^j = \prod_{l=1}^{n} (x - \delta_j^{(l)}) \ ,$$

wobei die $\delta_j^{(l)}$ und damit die z_j durch eine Konstante, die nur von d abhängt, beschränkt sind. Damit ist δ_j Nullstelle eines von endlich vielen Polynomen.

□

2.5. Dirichlets Einheitensatz

Wir wollen die Einheitengruppe $\mathcal{U}_F \subseteq \mathcal{O}_F$ für beliebige Zahlkörper F beschreiben. Da $\mathcal{U}_F$ eine multiplikative Gruppe, ein Gitter Γ jedoch eine additive Gruppe ist, „logarithmieren“ wir die Funktion Θ_F aus Definition 2.22.

Definition 2.27

Sei F ein Zahlkörper mit Signatur $\{r_1, r_2\}$ und $[F : \mathbb{Q}] = n = r_1 + 2r_2$. Es bezeichne $(\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$ die multiplikative Gruppe in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ bestehend aus allen Vektoren, deren Koordinaten alle ungleich 0 sind. Wir definieren die Abbildung

$$\Psi : \begin{cases} (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} & \longrightarrow \mathbb{R}^{r_1+r_2} \\ (\alpha_1, \ldots, \alpha_{r_1}, \alpha_{r_1+1}, \ldots, \alpha_{r_1+r_2}) & \longmapsto (l_1(\alpha_1), \ldots, l_{r_1+r_2}(\alpha_{r_1+r_2})) \ , \end{cases}$$

wobei

$$l_j(\alpha) := \begin{cases} \log(|\alpha|) & \text{für } \ j = 1, \ldots, r_1 \ , \\ \log(|\alpha|^2) & \text{für } \ j = r_1 + 1, \ldots, r_1 + r_2 \ . \end{cases}$$

Die Abbildung $\mathcal{L}_F : F \longrightarrow \mathbb{R}^{r_1+r_2}$ definiert durch $\mathcal{L}_F = \Psi \circ \Theta_F$ mit

$$\mathcal{L}_F(\alpha) = \big(\log|\Theta_1(\alpha)|, \ldots, \log|\Theta_{r_1}(\alpha)|, \log|\Theta_{r_1+1}(\alpha)|^2, \ldots, \log|\Theta_{r_1+r_2}(\alpha)|^2\big)$$

heißt *logarithmische Darstellung von* F, und $\mathbb{R}^{r_1+r_2}$ heißt der *logarithmische Raum von* F.

Bemerkung:

Die logarithmische Darstellung $\mathcal{L}_F$ ist ein Homomorphismus von der multiplikativen Gruppe $F^* := F \setminus \{0\}$ in die additive Gruppe des logarithmischen Raumes $\mathbb{R}^{r_1+r_2}$.

Satz 2.28

Sei F ein Zahlkörper mit Signatur $\{r_1, r_2\}$. Dann gilt

(i) $\ker(\mathcal{L}_F) = \mathcal{R}_F$;

(ii) $\mathcal{L}_F(\mathcal{U}_F) \subseteq \mathbb{R}^{r_1+r_2}$ ist ein Gitter der Dimension $r_1 + r_2 - 1$.

Beweis:

(i) Es ist

$$\begin{aligned} \ker(\mathcal{L}_F) &= \left\{\alpha \in F^* : \ \mathcal{L}_F(\alpha) = \vec{0}\right\} \\ &= \{\alpha \in F^* : \ |\Theta(\alpha)| = 1 \text{ für alle Einbettungen } \Theta\} \\ &= \{\alpha \in F^* : \ \alpha \in \mathcal{R}_F\} = \mathcal{R}_F \end{aligned}$$

nach Korollar 2.14.

(ii) Wir setzen $r := r_1 + r_2$ und haben für $\alpha \in \mathcal{U}_F$

$$\begin{aligned} \pm 1 = N_F(\alpha) &= \prod_{j=1}^{n} \Theta_j(\alpha) = \prod_{j=1}^{r_1} \Theta_j(\alpha) \cdot \prod_{j=r_1+1}^{r} \Theta_j(\alpha) \cdot \overline{\Theta_j(\alpha)} \\ &= \prod_{j=1}^{r_1} \Theta_j(\alpha) \cdot \prod_{j=r_1+1}^{r} |\Theta_j(\alpha)|^2 \ . \end{aligned}$$

Logarithmieren liefert

$$\sum_{j=1}^{r} l_j(\Theta_j(\alpha)) = \log \left| \prod_{j=1}^{r_1} \Theta_j(\alpha) \cdot \prod_{j=r_1+1}^{r_1+r_2} \Theta_j(\alpha)^2 \right| = 0 \ ,$$

d.h.

$$\mathcal{L}_F(\mathcal{U}_F) \subseteq \left\{ (x_1, \ldots, x_r) \in \mathbb{R}^r : \ \sum_{j=1}^{r_1} x_j + 2 \cdot \sum_{j=r_1+1}^{r_1+r_2} x_j = 0 \right\} \ .$$

Demnach liegt $\mathcal{L}_F(\mathcal{U}_F)$ in einer Hyperebene des $\mathbb{R}^r$, hat also Dimension $\leq r-1$. $\mathcal{U}_F$ ist eine multiplikative Untergruppe von $\mathcal{O}_F$, also ist $\mathcal{L}_F(\mathcal{U}_F)$ eine additive (Unter-)Gruppe ($\mathcal{L}_F$ ist Homomorphismus). Um zu zeigen, dass $\mathcal{L}_F(\mathcal{U}_F)$ ein Gitter ist, müssen wir nach Satz 2.17 nur noch nachweisen, dass $\mathcal{L}_F(\mathcal{U}_F)$ in $\mathbb{R}^r$ diskret liegt. Im Kreis um $\vec{0}$ mit Radius $N > 1$ haben wir

$$\begin{aligned} |\{\alpha \in \mathcal{U}_F : \ |\mathcal{L}_F(\alpha)| \leq N\}| &\leq |\{\alpha \in \mathcal{U}_F : \ \log|\Theta_j(\alpha)| \leq N \quad (j = 1, \ldots, r)\}| \\ &\leq \left|\{\alpha \in \mathcal{O}_F : \ |\Theta_j(\alpha)| \leq e^N \quad (j = 1, \ldots, r)\}\right| < \infty \end{aligned}$$

nach Satz 2.13.

Zur Vollständigkeit des Beweises von Aussage (ii) des Satzes fehlt nur noch, dass

$$\dim \mathcal{L}_F(\mathcal{U}_F) \geq r_1 + r_2 - 1 \ .$$

Dies gelingt mit Hilfe des Minkowskischen Gitterpunktsatzes durch Konstruktion von Einheiten $u_1, \ldots, u_{r_1+r_2} \in \mathcal{U}_F$ derart, dass die $\mathcal{L}_F(u_j)$ linear unabhängig über $\mathbb{R}$ sind. Wir geben hierfür ein Konstruktionsverfahren an.

Für $\vec{\nu} = (\nu_1, \ldots, \nu_{r_1+r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ sei

$$\lambda_{\vec{\nu}} : \begin{cases} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} & \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \vec{x} & \longmapsto \vec{\nu}\vec{x} \ \text{ (komponentenweise Multiplikation)} \end{cases}$$

eine lineare Abbildung mit

$$\det(\lambda_{\vec{\nu}}) = \prod_{j=1}^{r_1} \nu_j \cdot \prod_{j=r_1+1}^{r_1+r_2} |\nu_j|^2 \ .$$

Ist $|\det(\lambda_{\vec{\nu}})| = 1$, so haben die beiden Gitter $\Theta_F(\mathcal{O}_F)$ und $\lambda_{\vec{\nu}}(\Theta_F(\mathcal{O}_F))$ dieselbe Diskriminante

$$V\left(\lambda_{\vec{\nu}}(\Theta_F(\mathcal{O}_F)\right) = V(\Theta_F(\mathcal{O}_F)) = 2^{-r_2} \cdot \sqrt{|\Delta_F|} \ .$$

Setzen wir für geeignete $c_j \in \mathbb{R}_{>0}$

$$S = \left\{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \ |x_j| < c_j \ (1 \leq j \leq r_1), \ |x_j|^2 < c_j \ (r_1 + 1 \leq j \leq r_1 + r_2)\right\}$$

mit

$$V(S) = 2^{r_1} \cdot \pi^{r_2} \cdot \prod_{j=1}^{r_1+r_2} c_j > 2^n \cdot 2^{-r_2} \cdot \sqrt{|\Delta_F|} = V\left(\lambda_{\vec{\nu}}(\Theta(\mathcal{O}_F)\right) \cdot 2^n \ ,$$

so existiert nach Minkowski ein $\alpha \in \mathcal{O}_F \setminus \{0\}$ mit $\lambda_{\vec{\nu}}(\Theta_F(\alpha)) \in S$, d.h.

$$(*) \qquad |\Theta_j(\alpha) \cdot \nu_j| < c_j \ \ (1 \leq j \leq r_1) \ \text{ und } \ |\Theta_j(\alpha) \cdot \nu_j|^2 < c_j \ \ (r_1 + 1 \leq j \leq r_1 + r_2) \ .$$

Insbesondere haben wir wegen $|\det(\lambda_{\vec{\nu}})| = 1$

$$\begin{aligned} |N_F(\alpha)| &= \prod_{j=1}^{r_1} |\Theta_j(\alpha)| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\Theta_j(\alpha)|^2 \\ &= \prod_{j=1}^{r_1} |\Theta_j(\alpha) \cdot \nu_j| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\Theta_j(\alpha) \cdot \nu_j|^2 < \prod_{j=1}^{r_1+r_2} c_j \ . \end{aligned}$$

Da für $\beta \in \mathcal{O}_F$ stets $N_F(\beta) \in \mathbb{Z}$ ist, nimmt $|N_F(\beta)| < \prod_{j=1}^{r_1+r_2} c_j$ nur endlich viele Werte an, d.h. es gibt $\{\beta_1, \ldots, \beta_k\} \subseteq \mathcal{O}_F$ so, dass alle diese Normwerte angenommen werden. Also gilt für ein t, $1 \leq t \leq k$, dass $|N_F(\alpha)| = |N_F(\beta_t)|$, d.h. $\alpha = u_1\beta_t$ für eine Einheit $u_1 \in \mathcal{U}_F$. Mit $b_j := \min_{1\leq t\leq k} |\Theta_j(\beta_t)|$ und $(*)$ erhalten wir

$$|\Theta_j(u_1)| \cdot |\nu_j| < \frac{c_j}{b_j} \quad (1 \leq j \leq r_1), \quad |\Theta_j(u_1)| \cdot |\nu_j| < \frac{\sqrt{c_j}}{b_j} \quad (r_1 + 1 \leq j \leq r_1 + r_2) \ .$$

Wir setzen nun über die Bedingung $|\det(\lambda_{\vec{\nu}})| = 1$ hinaus voraus, dass

$$|\nu_1| = B^{-(r_1+2r_2-1)} \text{ und } |\nu_j| = B \quad (2 \leq j \leq r_1 + r_2) \ ,$$

wobei B eine hinreichend große Konstante sei. Wir erhalten

$$|\Theta_1(u_1)| < \frac{B^{r_1+r_2-1} \cdot c_1}{b_1}, \quad |\Theta_j(u_1)| < \frac{c_j}{b_j B} \quad (2 \leq j \leq r_1), \quad |\Theta_j(u_1)| < \frac{\sqrt{c_j}}{b_j B} \quad (r_1{+}1 \leq j \leq r_1{+}r_2) \ .$$

Wir setzen noch voraus, dass B so groß gewählt wurde, dass $|\Theta_j(u_1)| < 1$ für $j \geq 2$. Damit gilt mit der Bezeichnung $l_j(\alpha)$ aus Definition 2.27, dass $l_j(\Theta_j(u_1)) < 0$ für alle $j = 2, \ldots, r_1 + r_2$. Wegen $|N_F(u_1)| = 1$ folgt

$$l_1(\Theta_1(u_1)) = -\sum_{j=2}^{r_1+r_2} l_j(\Theta_j(u_1)) > 0 \ .$$

Durch Verwendung der vorstehenden Methode mit anderen $\vec{\nu}$ $(|\vec{\nu_i}| := B^{-(r_1+2r_2-1)})$ erhalten wir $u_2, \ldots, u_{r_1+r_2-1} \in \mathcal{U}_F$ derart, dass

$$(**) \qquad l_j(\Theta_j(u_i)) < 0 \ \ (i \neq j) \quad \text{und} \quad \sum_{j=1}^{r_1+r_2-1} l_j(\Theta_j(u_i)) > 0 \ \ (i = 1, \ldots, r_1{+}r_2{-}1)$$

wegen $\sum_{j=1}^{r_1+r_2} l_j(\Theta_j(u_i)) = 0$ und $l_{r_1+r_2}(\Theta_{r_1+r_2}(u_i)) < 0$. Es bezeichne $P : \mathbb{R}^{r_1+r_2} \longrightarrow \mathbb{R}^{r_1+r_2-1}$ die Projektion $(w_1, \ldots, w_{r_1+r_2}) \longmapsto (w_1, \ldots, w_{r_1+r_2-1})$.

Behauptung: Die Vektoren $P(\mathcal{L}_F(u_1)), \ldots, P(\mathcal{L}_F(u_{r_1+r_2-1})) \in \mathbb{R}$ sind linear unabhängig über $\mathbb{R}$. Es genügt zu zeigen, dass die $(n \times n)$-Matrix (mit $n := r_1 + r_2 - 1$) über $\mathbb{R}$

$$(m_{i,j}) := (P(\mathcal{L}_F(u_i)))_{n\times n}$$

eine Determinante $\det(m_{i,j}) \neq 0$ besitzt. Nach $(**)$ haben wir

$$m_{i,j} < 0 \quad (i \neq j) \quad \text{und} \quad \sum_{j=1}^{n} m_{i,j} > 0 \quad (i = 1, \ldots, n) \ .$$

Wir nehmen an, dass $\det(m_{i,j}) = 0$. Dann gibt es ein $r_j \in \mathbb{R}$ $(1 \leq j \leq n$, nicht alle 0) derart, dass

$$\sum_{j=1}^{n} m_{i,j} r_j = 0 \quad (i = 1, \ldots, n) \ .$$

Sei $1 \leq n_0 \leq n$ derjenige Index mit $|r_{n_0}| \geq |r_j|$ für alle $1 \leq j \leq n$. O.B.d.A. ist $r_{n_0} > 0$ (sonst ersetzen wir alle r_j durch $-r_j$). Wir erhalten aus $(**)$

$$0 = r_{n_0} m_{n_0} + \sum_{j \neq n_0} m_{n_0,j} \cdot r_j > r_{n_0} m_{n_0} + \sum_{j \neq n_0} m_{n_0,j} \cdot r_{n_0} > 0 \ .$$

Dieser Widerspruch beweist die Zwischenbehauptung, und somit sind $r_1 + r_2 - 1$ linear unabhängige Vektoren in $\mathcal{L}_F(\mathcal{U}_F)$ gefunden.

□

Satz 2.29 (Dirichlets Einheitensatz)

Sei F ein Zahlkörper mit Signatur, und sei $m := |\mathcal{R}_F|$. Dann gilt

$$\mathcal{U}_F \cong \overbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}^{r_1+r_2-1 \text{ Stück}} \times \langle \zeta_m \rangle \cong \langle u_1 \rangle \times \cdots \times \langle u_{r_1+r_2-1} \rangle \times \langle \zeta_m \rangle$$

mit einer primitiven m-ten Einheitswurzel ζ_m und einem System $u_1, \ldots, u_{r_1+r_2-1} \in \mathcal{U}_F$. Jedes solche System heißt *Fundamentalsystem von Einheiten* bzw. *System von Fundamentaleinheiten.*

Beweis:

Nach Satz 2.28 (ii) existieren $u_1, \ldots, u_{r-1} \in \mathcal{U}_F$ mit $r := r_1 + r_2$ derart, dass $\mathcal{L}_F(u_1), \ldots, \mathcal{L}_F(u_{r-1})$ eine $\mathbb{Z}$-Basis von $\mathcal{L}_F(\mathcal{U}_F)$ ist, d.h. zu jedem $u \in \mathcal{U}_F$ existieren eindeutige $z_j \in \mathbb{Z}$ mit

$$\mathcal{L}_F(u) = \sum_{j=1}^{r-1} z_j \cdot \mathcal{L}_F(u_j) \ .$$

Es folgt für den Gruppenhomomorphismus $\mathcal{L}_F$

$$\mathcal{L}_F\left(u \cdot \prod_{j=1}^{r-1} u_j^{-z_j}\right) = \mathcal{L}_F(u) + \sum_{j=1}^{r-1}(-z_j) \cdot \mathcal{L}_F(u_j) = 0 \ .$$

Ist $\nu \in \mathcal{U}_F$ beliebig mit $\mathcal{L}_F(\nu) = 0$, so gilt nach Satz 2.28 (i), dass $\nu \in \mathcal{R}_F$. Aus Satz 2.12 (i) ergibt sich , dass $\nu = \zeta_m^s$ für eine primitive m-te Einheitswurzel ζ_n und ein $s \in \mathbb{Z}$. Für $\nu := u \cdot \prod_{j=1}^{r-1} u_j^{-z_j}$ folgt

$$u \cdot \prod_{j=1}^{r-1} u_j^{-z_j} = \zeta_m^s$$

und somit die Behauptung.

□

Beispiel:

Für reell-quadratische Zahlkörper F, d.h. $r_1 = 2, r_2 = 0$, erhalten wir gemäß Satz 2.29 $\mathcal{U}_F \cong \langle u_1 \rangle \times \langle -1 \rangle$, da $\mathcal{R}_F = \{\pm 1\}$ (vgl. Satz 2.4). Für komplex-quadratische Zahlkörper F, d.h. $r_1 = 0, r_2 = 1$, kommt mit Satz 2.29 $\mathcal{U}_F = \mathcal{R}_F$ (vgl. Satz 1.46).

Bemerkung:

Sei F ein Zahlkörper mit Signatur $\{r_1, r_2\}$ und seien $u_1, \ldots, u_{r_1+r_2-1}$ und $\nu_1, \ldots, \nu_{r_1+r_2-1}$ zwei Systeme von Fundamentaleinheiten. Mit Hilfe von Dirichlets Einheitensatz lässt sich leicht zeigen, dass

$$|\det(\mathcal{L}_F(u_i))| = |\det(\mathcal{L}_F(\nu_i))| \ .$$

Diese charakteristische Größe von F, die nur vom Zahlkörper selbst abhängt, heißt der *Regulator von* F, geschrieben r_F. Im Allgemeinen ist die Berechnung des Regulators eines Zahlkörpers schwierig, da ein System von Fundamentaleinheiten bekannt sein muss. Für reell-quadratische Zahlkörper jedoch, d.h. $r_1 = 2, r_2 = 0$ und $\mathcal{U}_F = \langle u_1 \rangle \times \langle -1 \rangle$, ist die Fundamentaleinheit u_1 die „kleinste“ Lösung einer bestimmten Pell'schen Gleichung (vgl. Satz 2.4). Für $F = \mathbb{Q}(\sqrt{5})$ haben wir zum Beispiel $u_1 = \varepsilon_5 = (1 + \sqrt{5})/2$, also $r_{\mathbb{Q}(\sqrt{5})} = \log\big((1 + \sqrt{5})/2\big)$.

3 Idealtheorie

3.1. Eigenschaften von Idealen

Wir hatten bereits zu Beginn der Vorlesung Beispiele dafür gesehen, dass die Faktorisierung von Zahlen in $\mathcal{O}_F$ (für einen Zahlkörper F) in Primelemente im Allgemeinen nicht eindeutig ist. Wir wollen zeigen, dass jedoch eindeutige Zerlegung bezüglich Idealen vorliegt. Ideale in einem kommutativen Ring R mit Eins wurden bereits in Definition 1.6 erklärt und heißen auch kurz *R-Ideale*.

Satz 3.1

Sei F ein Zahlkörper mit $[F : \mathbb{Q}] = d$ und sei $I \neq (0)$ ein $\mathcal{O}_F$-Ideal. Dann ist I eine freie abelsche Gruppe vom Rang d, d.h. es gibt *Erzeugende* $\alpha_1, \ldots, \alpha_d \in I$ derart, dass

$$I = [\alpha_1, \ldots, \alpha_d] := \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_d.$$

Beweis:

Nach Satz 1.39 ist $\mathcal{O}_F$ eine freie abelsche vom Rang d. Nach Definition des Ideals ist I eine Untergruppe von $\mathcal{O}_F$ und somit selbst freie abelsche Gruppe, wobei der Rang $r \leq d$ ist. Also besitzt I eine $\mathbb{Z}$-Basis $\{\alpha_1, \ldots, \alpha_r\} \subseteq \mathcal{O}_F$. Sei $\{\beta_1, \ldots, \beta_d\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_F$. Sei $\alpha \in I \setminus \{0\}$. Dann sind $\alpha\beta_1, \ldots, \alpha\beta_d \in I$ linear unabhängig und bilden eine $\mathbb{Q}$-Basis von F. Außerdem gibt es $z_{i,j} \in \mathbb{Z}$ mit

$$\alpha\beta_j = \sum_{i=1}^{r} z_{i,j}\alpha_i \qquad (j = 1, \ldots, d).$$

Wäre $r < d$, so hätte das lineare Gleichungssystem

$$\sum_{j=1}^{d} z_{i,j}r_j = 0 \qquad (i = 1, \ldots r)$$

eine nichttriviale Lösung $r_j \in \mathbb{Q}, j = 1, \ldots d$, nicht alle gleich 0.

Es folgte

$$\sum_{j=1}^{d} r_j(\alpha\beta_j) = \sum_{j=1}^{d} r_j \sum_{i=1}^{r} z_{i,j}\alpha_i = \sum_{i=1}^{r} \alpha_i \sum_{j=1}^{d} z_{i,j} r_j = 0$$

im Widerspruch zur linearen Unabhängigkeit der $\alpha\beta_j$.

□

Wir bezeichnen mit $(\alpha_1, \ldots, \alpha_d)$ das kleinste Ideal, welches $\alpha_1, \ldots, \alpha_d$ enthält. Man beachte, dass $(\alpha_1, \ldots, \alpha_d)$ per definitionem stets ein Ideal ist, hingegen $[\alpha_1, \ldots, \alpha_d]$ nicht unbedingt.

Beispiel:

$\left[2, 1+\sqrt{10}\right]$ ist kein Ideal in $\mathcal{O}_F$ mit $F = \mathbb{Q}\left(\sqrt{10}\right)$, denn

$\left(1+\sqrt{10}\right) \cdot \left(1-\sqrt{10}\right) \notin \left[2, 1+\sqrt{10}\right] = \left\{(2a+b) + b\sqrt{10} : a, b \in \mathbb{Z}\right\}$.

Jedes R-Ideal I, das eine endliche Menge von Erzeugenden besitzt, heißt *endlich erzeugt*. Ist $I = (\alpha)$, so heißt I *Hauptideal*. Sind $I = (\alpha)$ und $J = (\beta)$ Hauptideale, so gilt $I = J$ gdw. $\alpha \mid \beta$ und $\beta \mid \alpha$ gdw. $(\beta) \subseteq (\alpha)$ und $(\alpha) \subseteq (\beta)$. Unter dem Produkt zweier endlich erzeugter R-Ideale

$$I = (\alpha_1, \ldots, \alpha_r) \quad \text{und} \quad J = (\beta_1, \ldots, \beta_s)$$

verstehen wir das R-Ideal

$$I \cdot J := (\alpha_1\beta_1, \ldots, \alpha_1\beta_s, \alpha_2\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_s)$$

erzeugt von allen Produkten $\alpha_i\beta_j \quad (1 \leq i \leq r, 1 \leq j \leq s)$. Dabei hängt $I \cdot J$ nicht von den speziellen Erzeugendensystemen der α_i bzw. der β_j ab.

Lemma 3.2

Seien I und J R-Ideale in einem kommutativen Ring R mit Eins. Aus $I \mid J$ folgt $J \subseteq I$.

Beweis:

Gemäß Definition 1.7 bedeutet $I \mid J$, dass $J = I \cdot H$ für ein R-Ideal H. Aus $IH \subseteq I$ ergibt sich die Behauptung.

□

Von großer Bedeutung für uns wird sein, dass im Falle $R = \mathcal{O}_F$ für einen Zahlkörper F auch die Umkehrung von Lemma 3.2 gilt, nämlich $J \subseteq I \Longrightarrow I \mid J$. In geringer Abänderung von Definition 1.7 haben wir

Definition 3.3

Sei F ein Zahlkörper. Ein $\mathcal{O}_F$-*Primideal* (kurz: Primideal) ist ein $\mathcal{O}_F$-Ideal $P \neq \mathcal{O}_F$ mit der Eigenschaft, dass aus $P \mid IJ$ für zwei $\mathcal{O}_F$-Ideale I, J folgt, dass $P \mid I$ oder $P \mid J$. Das spezielle Primideal (0) heißt das *triviale Ideal*.

Beispiel:

Für $F = \mathbb{Q}$ ist $\mathcal{O}_F = \mathbb{Z}$ nach Korollar 1.30. Die Menge der Primideale ist dann

$$\{(p) : p \in \mathbb{P}\} \cup \{(0)\} \cong \mathbb{P} \cup \{0\}.$$

Es erweist sich in diesem Zusammenhang als sinnvoll, 0 als Primzahl zu betrachten.

Definition 3.4

Sei R ein kommutativer Ring mit Eins. Ein R-Ideal $I \neq R$ heißt *maximal*, falls $I \subseteq J$ für ein R-Ideal J impliziert, dass $J = R$. Ein R-Ideal $I \neq (0)$ heißt *minimal*, falls $J \subseteq I$ für ein R-Ideal J impliziert, dass $J = (0)$.

Beispiele:

(i) In $R = \mathbb{Z}$ sind die Ideale von der Form $n \cdot \mathbb{Z}$, $n \in \mathbb{N}_0$. Die Primideale $\neq (0)$ sind genau die $p \cdot \mathbb{Z}$ mit $p \in \mathbb{P}$, und dies sind wiederum genau die maximalen Ideale.

(ii) Sei F ein Körper und $R := F[x]$. Ist $r \in F$, so ist $\{f(x) \in F[x] : f(r) = 0\}$ ein maximales Ideal in $F[x]$.

Es ist nicht schwer zu beweisen, dass jedes maximale R-Ideal $I \neq R$ ein Primideal ist. Außerdem gilt, dass jedes Ideal $I \neq R$ in einem maximalen Ideal enthalten ist.

Definition 3.5

Ein Integritätsring R heißt *Dedekind-Ring*, sofern die folgenden Bedingungen gelten:

(i) Jedes Ideal in R ist endlich erzeugt.

(ii) Jedes Primideal $\neq 0$ in R ist maximal.

(iii) R ist ganzabgeschlossen in seinem Quotientenkörper

$$F := \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R, \beta \neq 0 \right\},$$

d.h. ist $f(\alpha/\beta) = 0$ für ein $\alpha/\beta \in F$ und $f(x) \in R[x]$ mit führendem Koeffizienten 1, so ist $\alpha/\beta \in R$.

Bemerkung:

Bedingung (i) in Definition 3.5 charakterisiert sogenannte *Noethersche Ringe* und ist äquivalent zu jeder der beiden folgenden Bedingungen:

(i') Jede nichtleere Menge von R-Idealen besitzt ein (nicht notwendigerweise eindeutiges) maximales Element.

(i") Sind $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq \cdots$ R-Ideale, so existiert ein $j_0 \in \mathbb{N}$ mit $I_j = I_{j_0}$ für alle $j \geq j_0$ (Teilerkettenbedingung).

Nachdem das Produkt von Idealen bereits erklärt ist, definieren wir auch die Summe zweier R-Ideale I und J als

$$I + J := \{\alpha + \beta : \alpha \in I, \beta \in J\}.$$

Selbstverständlich ist $I + J$ auch ein R-Ideal, denn für $r \in R, \alpha \in I, \beta \in J$ gilt $r(\alpha + \beta) = r\alpha + r\beta \in I + J$, da $r\alpha \in I$ und $r\beta \in J$.

Wir nennen I und J *teilerfremd*, falls es kein R-Ideal $H \neq R$ gibt mit $H \mid I$ und $H \mid J$. Es ist leicht zu sehen, dass dies äquivalent ist zu $I + J = R$.

Satz 3.6

Ist F ein Zahlkörper, so ist $\mathcal{O}_F$ ein Dedekind-Ring.

Beweis:

Wir zeigen die drei definierenden Eigenschaften eines Dedekind-Rings für $R = \mathcal{O}_F$:

(i) Klar nach Satz 1.39.

(ii) Aus der Algebra ist bekannt, dass ein R-Ideal I genau dann maximal ist, wenn der Quotientenring $R/I := \{\alpha + I : \alpha \in R\}$ ein Körper ist. Wir zeigen zunächst, dass $\mathcal{O}_F/P$ für ein Primideal $\neq (0)$ eine endliche Menge ist. Sei dazu $\alpha \in P \setminus \{0\}$. Schon im Beweis zu Satz 2.1 hatten wir benutzt, dass für jedes $\alpha \in \mathcal{O}_F \setminus \{0\}$ gilt

$$|\mathcal{O}_F/(\alpha)| = |N_F(\alpha)|\,,$$

also insbesondere $\mathcal{O}_F/(\alpha)$ endlich. Selbstverständlich ist der Ring $\mathcal{O}_F/P$ (wie $\mathcal{O}_F$ selbst) ein Integritätsbereich. Jeder endliche Integritätsbereich wiederum ist ein Körper, denn zu jedem Element $g \neq 0$ existiert $n > m$ mit $g^m = g^n$, also
$g^m(g^{n-m} - 1) = 0$, also $g^{n-m} - 1 = 0$, d.h. jedes $g \neq 0$ besitzt ein multiplikatives Inverses.

(iii) Sei $f(x) \in \mathcal{O}_F[x]$ mit führendem Koeffizienten 1, und sei $f(\alpha/\beta) = 0$, also

$$f(x) = x^m + \sum_{j=0}^{m-1} \alpha_j x^j \quad (\alpha_j \in \mathcal{O}_F).$$

Sei $\tilde{f}(x)$ das Polynom, welches durch Multiplikation aller Polynome, die aus $f(x)$ durch Übergang zu konjugierten Koeffizienten hervorgehen, entsteht. Dann hat $\tilde{f}(x)$ ganzalgebraische Koeffizienten und ist symmetrisch in diesen. Nach dem Satz über

elementarsymmetrische Funktionen folgt $\tilde{f} \in \mathbb{Z}[x]$, offenbar mit führenden Koeffizienten 1 und Nullstelle α/β. Also ist $\alpha/\beta \in \mathbb{A}$ und somit $\alpha/\beta \in F \cap \mathbb{A} = \mathcal{O}_F$.

□

Lemma 3.7

Sei R ein Dedekind-Ring. Jedes R-Ideal $I \neq (0)$ enthält ein Produkt von Primidealen.

Beweis:

Sei S die Menge aller R-Ideale $\neq 0$, die kein Produkt von Primidealen enthalten. Wäre $S \neq \emptyset$, so gäbe es in S wegen (i') in der Bemerkung zu Definition 3.5 ein maximales Element M. Dabei kann M kein Primideal sein (sonst folgte $M \notin S$). Also existieren $r, s \in \mathbb{R}$ mit $rs \in M$, aber $r \notin M$, $s \notin M$. Wegen $M \subsetneq M + (r)$ und $M \subsetneq M + (s)$ enthalten $M + (r)$ und $M + (s)$ beide Produkte von Primidealen. Damit gilt dies auch für

$$(M + (r)) \cdot (M + (s)) = M + (rs) = M \ .$$

Dieser Widerspruch beweist das Lemma.

□

Lemma 3.8

Sei R ein Dedekind-Ring mit Quotientenkörper F. Ist $I \neq R$ ein R-Ideal, so existiert ein $\gamma \in F \setminus R$ mit $\gamma I \subseteq R$.

Beweis:

Für $I = (0)$ ist das Lemma trivial. Sei also $\alpha \in I \setminus \{0\}$ beliebig. Nach Lemma 3.7 enthält das Hauptideal (α) ein Produkt $\mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_r$ von Primidealen, wobei wir annehmen, dass r minimal ist. Da $I \neq R$, ist I in einem maximalen Ideal und somit

in einem Primideal $\mathcal{P}$ enthalten, also zusammen

$$\mathcal{P} \mid I \mid \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_r \ .$$

Es folgt $\mathcal{P} \mid \mathcal{P}_j$ für ein j, o.B.d.A. $\mathcal{P} \mid \mathcal{P}_1$, d.h. $\mathcal{P}_1 \subseteq \mathcal{P}$. Nach Bedingung (ii) aus Definition 3.5 folgt $\mathcal{P}_1 = \mathcal{P}$. Wegen der Minimalität von r ist $\mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \setminus (\alpha) \neq \emptyset$. Sei $\beta \in \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \setminus (\alpha)$ beliebig. Dann gilt

$$\frac{\beta}{\alpha} \in \frac{1}{\alpha} \cdot \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \setminus \frac{(\alpha)}{\alpha} = \frac{1}{\alpha} \cdot \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \setminus (1) = \frac{1}{\alpha} \cdot \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \setminus \mathcal{P} \ .$$

Außerdem ist

$$\beta \cdot \mathcal{P} \subseteq \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \cdot \mathcal{P} = \mathcal{P}_1 \cdot \mathcal{P}_2 \cdot \ldots \cdot \mathcal{P}_r \subseteq (\alpha) \ ,$$

also gilt für jedes $\delta \in \mathcal{P}$, dass $\beta\delta \in (\alpha)$ und damit $\dfrac{\beta}{\alpha} \cdot \delta \in \dfrac{(\alpha)}{\alpha} = (1) = R$. Mit $\gamma := \beta/\alpha$ folgt die Behauptung.

□

Satz 3.9

Sei R ein Dedekind-Ring und sei $I \neq (0)$ ein R-Ideal. Dann gibt es ein R-Ideal $J \neq (0)$ derart, dass $I \cdot J$ ein Hauptideal ist.

Beweis:

Für $\alpha \in I \setminus \{0\}$ setzen wir $J := \{\beta \in R : \beta I \subseteq (\alpha)\}$. Damit ist $\alpha \in J$, also $J \neq (0)$. Offenbar ist J ein R-Ideal, und es gilt $I \cdot J \subseteq (\alpha)$. Wir zeigen, dass $I \cdot J = (\alpha)$ gilt. Wir setzen $L := {}^{1}\!/_{\alpha} \cdot I \cdot J \subseteq {}^{(\alpha)}\!/_{\alpha} = R$. Mit I und J ist auch L ein Ideal, also ein R-Ideal. Mit $L = R$ wäre der Satz bewiesen. Wir nehmen also an, dass $L \neq R$. Nach Lemma 3.8 existiert ein $\gamma \in F \setminus R$ (F ist Quotientenkörper von R) mit $\gamma L \subseteq R$. Wir werden nachweisen, dass γ Nullstelle eines Polynoms $f(x) \in R[x]$ mit führendem Koeffizienten 1 ist, und dies stände im Widerspruch zu Bedingung (iii) von Definition 3.5, da $\gamma \notin R$.

Wegen $\alpha \in I$ ist I/α ein R-Ideal und somit $L := {}^1\!/_\alpha \cdot I \cdot J \supseteq J$. Es folgt $\gamma J \subseteq \gamma L \subseteq R$, also

$$(\gamma J) \cdot I = \gamma \cdot (I \cdot J) = \gamma \cdot (\alpha L) = (\alpha) \cdot (\gamma L) \subseteq (\alpha) \cdot R \subseteq (\alpha) \ ,$$

und deshalb $\gamma J \subseteq J$ nach Definition von J. Sei

$$J = R \cdot \beta_1 \oplus \cdots \oplus R \cdot \beta_r \ .$$

Wegen $\gamma J \subseteq J$ gibt es $z_{i,j} \in R$ mit

$$\gamma \beta_i = \sum_{j=1}^{r} z_{i,j} \beta_j \qquad (1 \leq i \leq r) \ .$$

Damit hat das homogene lineare Gleichungssystem

$$\begin{array}{rcl} (z_{1,1} - \gamma) \cdot x_1 + z_{1,2} \cdot x_2 + \cdots + z_{1,r} \cdot x_r & = & 0 \\ z_{2,1} \cdot x_1 + (z_{2,2} - \gamma) \cdot x_2 + \cdots + z_{2,r} \cdot x_r & = & 0 \\ \vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots & = & \vdots \\ z_{r,1} \cdot x_1 + z_{r,2} \cdot x_2 + \cdots + (z_{r,r} - \gamma) \cdot x_r & = & 0 \end{array}$$

die nichttriviale Lösung $x_j = \beta_j$ $(1 \leq j \leq r)$. Also verschwindet die Determinante der Koeffizientenmatrix, und dies ist ein Polynom in γ über R mit führendem Koeffizienten 1.

□

Korollar 3.10

Sind $I \neq (0)$, J und L Ideale in einem Dedekind-Ring R, so folgt aus $I \cdot J = I \cdot L$, dass $J = L$.

Beweis:

Nach Satz 3.9 existiert ein Ideal $H \neq (0)$ und ein $\alpha \in R \setminus \{0\}$ mit $I \cdot H = (\alpha)$, also

$$J \cdot (\alpha) = IJ \cdot H = IL \cdot H = L \cdot (\alpha) \ .$$

Es folgt

$$J = J \cdot R = J \cdot \frac{(\alpha)}{\alpha} = L \cdot \frac{(\alpha)}{\alpha} = LR = L \ .$$

□

Korollar 3.11

Sind I und J Ideale in einem Dedekind-Ring, dann gilt

$$I \mid J \Longleftrightarrow J \subseteq I \ .$$

Beweis:

Nach Lemma 3.2 ist nur zu zeigen: $J \subseteq I \Longrightarrow I \mid J$. Sei $J \subseteq I$ und sei L ein Ideal gemäß Satz 3.9 derart, dass $LI = (\alpha)$ für ein $\alpha \neq 0$. Es folgt, dass

$$H := \frac{1}{\alpha} \cdot LJ \subseteq \frac{1}{\alpha} \cdot LI = \frac{(\alpha)}{\alpha} = R \ ,$$

also H ein R-Ideal ist. Dabei haben wir

$$I \cdot H = \frac{1}{\alpha} \cdot LI \cdot J = \frac{(\alpha)}{\alpha} \cdot J = R \cdot J = J \ ,$$

also $I \mid J$.

□

Satz 3.12

In einem Dedekind-Ring R besitzt jedes R-Ideal I mit $I \neq (0)$ und $I \neq R$ eine eindeutige Darstellung als Produkt von Primidealen, d.h. bis auf die Reihenfolge der Faktoren gibt es einen eindeutigen Ausdruck

$$I = P_1^{a_1} \cdot P_2^{a_2} \cdot \ldots \cdot P_n^{a_n}$$

mit verschiedenen R-Primidealen $P_j \supseteq I$ und $a_j \in \mathbb{N}$ $(1 \leq j \leq n)$.

Beweis:

Existenz: Sei S die Menge aller R-Ideale $I \neq (0)$, $I \neq R$, die keine gewünschte Darstellung besitzen. Ist $S \neq \emptyset$, so enthält S nach (i') der Bemerkung zu Definition 3.5 ein maximales Element M. Da $M \neq R$, ist M in einem maximalen Ideal, also in einem Primideal P enthalten. Nach Korollar 3.11 folgt $P \mid M$, d.h. $M = I \cdot P$ für ein R-Ideal I. Wir haben demnach $I \mid M$, d.h. $M \subseteq I$. Für den Fall $M = I$ ergäbe sich $I \cdot R = I = I \cdot P$, also aus Korollar 3.10 $P = R$. Widerspruch! Es bleibt nur $M \subsetneq I$. Da M maximal in S ist, ist I ein Produkt von Primidealen. Dann ist aber auch $M = I \cdot P$ ein Produkt von Primidealen im Widerspruch zu $M \in S$.
Eindeutigkeit: Seien P_j $(1 \leq j \leq r)$ und Q_k $(1 \leq k \leq s)$ Primideale mit

$$P_1 \cdot \ldots \cdot P_r = Q_1 \cdot \ldots \cdot Q_s \ .$$

Also gilt $P_1 \mid Q_k$ für ein k, o.B.d.A. $P_1 \mid Q_1$, d.h. nach Korollar 3.11, dass $Q_1 \subseteq P_1$. Wegen (ii) in Definition 3.5 sind Q_1 und P_1 maximale Ideale, also $Q_1 = P_1$. Aus Korollar 3.10 folgt

$$P_2 \cdot \ldots \cdot P_r = Q_2 \cdot \ldots \cdot Q_s \ .$$

Induktiv ergibt sich $r = s$ und $P_j = Q_j$ $(1 \leq j \leq r)$.

□

Mit Hilfe von Satz 3.6 liefert Satz 3.12 sofort

Korollar 3.13

Sei F ein Zahlkörper. Jedes $\mathcal{O}_F$-Ideal $\neq (0)$ und $\neq \mathcal{O}_F$ ist eindeutiges Produkt von Primidealen.

Bemerkung:

Die Tatsache, dass in $\mathcal{O}_F$ im Allgemeinen keine eindeutige Faktorisierung in Primelemente vorliegt (vgl. Beispiele aus Abschnitt 1.1.), erwies sich in Satz 1.47 (ii) gleichwertig damit, dass nicht alle irreduziblen Elemente prim sind. Nennen wir ein

R-Ideal, welches außer sich selbst und R keine Teiler besitzt, irreduzibel, so lässt sich zeigen, dass irreduzibel äquivalent zu prim und damit zu maximal ist, sofern R ein Dedekind-Ring ist.

Definition 3.14

Seien I und J R-Ideale in einem Dedekind-Ring R. Wir definieren den *größten gemeinsamen Teiler*

$$\text{ggT } (I, J) := I + J$$

und das *kleinste gemeinsame Vielfache*

$$\text{kgV } (I, J) := I \cap J \ .$$

Offenbar ist ggT (I, J) das kleinste Ideal, das I und J umfasst. Nach Korollar 3.11 ist kgV (I, J) das größte Ideal, welches in I und in J enthalten ist. Ist $I = (\alpha)$ ein Hauptideal, so verwenden wir auch die abkürzende Schreibweise

$$\text{ggT } (\alpha, J) := \text{ggT } (I, J) \text{ bzw. kgV } (\alpha, J) := \text{kgV } (I, J) \ .$$

Der Chinesiche Restsatz in $\mathbb{Z}$ besagt, dass für paarweise teilerfremde Moduln $m_1, \ldots, m_r \in \mathbb{Z}$ und beliebige Zahlen $a_1, \ldots, a_r \in \mathbb{Z}$ ein eindeutiges a mod $m_1, \ldots, m_r$ existiert mit $a \equiv a_i \bmod m_i$ $(1 \leq i \leq r)$, d.h. $a - a_i \in (m_i)$.

Satz 3.15 (Chinesischer Restsatz für Ideale)

Sei R ein Dedekind-Ring und seien $I_1, \ldots I_r$ paarweise teilerfremde R-Ideale. Dann ist die Abbildung

$$\Psi : \begin{cases} R \Big/ \bigcap\limits_{j=1}^{r} I_j & \longrightarrow \quad R/I_1 \times \cdots \times R/I_r \\ \alpha + \bigcap\limits_{i=1}^{r} I_i & \longmapsto \quad (\alpha + I_1, \ldots, \alpha + I_r) \end{cases}$$

ein additiver Gruppen-Isomorphismus, d.h. zu beliebigen $\alpha_1, \ldots, \alpha_r \in R$ existiert ein („modulo $\bigcap\limits_{j=1}^{r} I_j$“ eindeutiges) $\alpha \in R$ mit $\alpha - \alpha_j \in I_j$ für $1 \leq j \leq r$.

Beweis:

Der Nachweis der Isomorphismus-Eigenschaften von Ψ ist offensichtlich bis auf die Surjektivität von Ψ:

Sei zunächst $r = 2$. Wegen ggT $(I_1, I_2) = R$ existieren $x_1 \in I_1$, $x_2 \in I_2$ mit $x_1 + x_2 = 1$. Sind $\alpha_1, \alpha_2 \in R$ beliebig, so gilt für $\alpha := x_2\alpha_1 + x_1\alpha_2$, dass

$$\alpha - \alpha_1 = (x_2 - 1)\alpha_1 + x_1\alpha_2 = (\alpha_2 - \alpha_1)x_1 \in I_1$$

und analog $\alpha - \alpha_2 \in I_2$, d.h. $\alpha_j \in \alpha + I_j$ $(j = 1, 2)$. Für $r > 2$ finden wir analog zu jedem i, $1 \leq i \leq r$, ein $y_i \in R$ derart, dass $y_i - 1 \in I_1$ und $y_i \in \bigcap_{j \neq i} I_j$. Zu beliebigen $\alpha_1, \ldots, \alpha_r \in R$ erhalten wir damit für $\alpha := y_1\alpha_1 + \cdots + y_r\alpha_r$, dass

$$\alpha - \alpha_1 = (y_1 - 1)\alpha_1 + y_2\alpha_2 + \cdots + y_r\alpha_r \in I_1$$

und analog $\alpha - \alpha_j \in I_j$ für $j \geq 2$.

□

Lemma 3.16

Seien $I \neq (0)$ und $J \neq (0)$ R-Ideale in einem Dedekind-Ring R.

(i) Es existiert ein $\alpha \in I$ derart, dass ggT $(\alpha, IJ) = I$.

(ii) Es gibt ein R-Ideal H teilerfremd zu J derart, dass $H \cdot I$ ein Hauptideal ist.

Beweis:

(i) Nach Satz 3.12 gibt es paarweise verschiedene Primideale P_j mit

$$I = \prod_{j=1}^{r} P_j^{a_j} \quad \text{und} \quad J = \prod_{j=1}^{r} P_j^{b_j}$$

für gewisse $a_j, b_j \in \mathbb{N}_0$. Sei $\alpha_j \in P_j^{a_j} \setminus P_j^{a_j+1}$ $(1 \leq j \leq r)$. Nach dem Chinesischen Restsatz 3.15 existiert ein $\alpha \in R$ mit $\alpha - \alpha_j \in P_j^{a_j+1}$ $(1 \leq j \leq r)$, d.h.

$$\alpha \in a_j + P_j^{a_j+1} \subseteq P_j^{a_j} \setminus P_j^{a_j+1} \quad (1 \leq j \leq r)\ ,$$

denn sonst wäre $\alpha_j + P_j^{a_j+1} \subseteq P_j^{a_j+1}$, also $\alpha_j \in P_j^{a_j+1}$. Widerspruch!
Insbesondere ist $\alpha \in P_j^{a_j}$ für alle j, also $\alpha \in I$. Außerdem haben wir für gewisse Primideale $Q_j = P_i$ und $c_j \in \mathbb{N}$

$$(\alpha) = \prod j = 1^r P_j^{a_j} \cdot \prod j = 1^s Q_j^{c_j} \ .$$

Es folgt

$$\begin{aligned} \text{ggT } (\alpha, IJ) &= \text{ggT } \left(\prod_{j=1}^{r} P_j^{a_j} \cdot \prod_{j=1}^{s} Q_j^{c_j} \ , \ \prod_{j=1}^{r} P_j^{a_j+b_j} \right) \\ &= \prod_{j=1}^{r} P_j^{a_j} = I \ . \end{aligned}$$

(ii) Sei $\alpha \in I$ gemäß (i), also $\alpha \neq 0$. Nach dem Beweis zu Satz 3.9 existiert ein R-Ideal H mit $H \cdot I = (\alpha)$, also $H \cdot I$ Hauptideal. Dabei haben wir nach (i)

$$I \cdot \text{ggT } (H, J) = \text{ggT } (HI, IJ) = \text{ggT } (\alpha, IJ) = I \ ,$$

also nach Korollar 3.10 ggT $(H, J) = R$.

□

Satz 3.17

Sei I ein R-Ideal in einem Dedekind-Ring R. Zu jedem $\alpha \in I \setminus \{0\}$ existiert ein $\beta \in I$ mit $I = (\alpha, \beta)$, d.h. jedes Ideal in einem Dedekind-Ring ist Hauptideal oder wird von zwei Elementen erzeugt.

Beweis:

Mit $J := (\alpha)$ liefert Lemma 3.16 (ii) ein R-Ideal H derart, dass $H + (\alpha) = R$ und $H \cdot I = (\beta)$ für ein $\beta \in R$. Es folgt

$$(\alpha) + (\beta) = (\alpha) + H \cdot I \subseteq I \ ,$$

und die umgekehrte Inklusion bleibt zu zeigen. Wegen $H + (\alpha) = R$ existieren $h \in H$ und $r \in R$ mit $h + \alpha r = 1$.

Also ist für jedes $\delta \in I$

$$\delta = h\delta + \alpha r\delta \in H \cdot I + (\alpha) = (\beta) + (\alpha) \ ,$$

d.h. $I \subseteq (\alpha) + (\beta)$.

□

Satz 3.18

Sei R ein Dedekind-Ring mit verschiedenen Primidealen $P_1, \ldots, P_r$. Zu $a_1, \ldots, a_r \in \mathbb{N}_0$ existiert ein $\alpha \in R$ und ein R-Ideal I mit ggT $(I, P_j) = R$ für $1 \leq j \leq r$, derart, dass

$$(\alpha) = I \cdot \prod_{j=1}^{r} P_j^{a_j} \ .$$

Beweis:

Folgt sofort aus Lemma 3.16 (ii).

□

Korollar 3.19

Sind $I \neq (0)$, $J \neq (0)$ R-Ideale in einem Dedekind-Ring R, so haben wir als additive Gruppen $R/I \cong J/IJ$.

Beweis:

Nach Lemma 3.16 (ii) existiert ein R-Ideal H, teilerfremd zu I, mit $H \cdot J = (\alpha)$ für ein $\alpha \in R$. Wir definieren den Gruppen-Homomorphismus

$$\Psi : \begin{cases} R & \longrightarrow & J/IJ \\ r & \longmapsto & r\alpha + IJ \ . \end{cases}$$

Dabei ist Ψ surjektiv, denn

$$(\alpha) + I \cdot J = H \cdot J + I \cdot J = (H + I) \cdot J = R \cdot J = J \ .$$

Nach dem Isomorphiesatz für Gruppen erhalten wir

$$R/\ker\Psi \cong \text{img } \Psi = J/IJ \ .$$

Es bleibt zu zeigen, dass $\ker\Psi = I$. Sei $\alpha\beta \in I \cdot J$, d.h. $\beta \in \ker\Psi$. Dann gilt

$$\alpha\beta H \subseteq IJH \subseteq I(\alpha) \ ,$$

also nach Korollar 3.10 $\beta \cdot H \subseteq I$. Wegen $H + I = R$ existieren $h \in H$ und $\gamma \in I$ mit $h + \gamma = 1$, also

$$\beta = \beta h + \beta\gamma \in I + R \cdot I = I \ .$$

Sei umgekehrt $\beta \in I$, also

$$\Psi(\beta) = \alpha\beta + I \cdot J = I \cdot J \ ,$$

denn $\alpha \in H \cdot J \subseteq J$. Somit haben wir $I \subseteq \ker\Psi$ und insgesamt $\ker\Psi = I$.

□

3.2. Hauptidealringe

Definition 3.20

Ein Integritätsbereich R, in dem alle R-Ideale Hauptideale sind, heißt *Hauptidealring.*

Aus der Algebra verwenden wir

Satz 3.21

Jeder Hauptidealring ist ZPE-Ring (vgl. Definition 1.48).

Korollar 3.22

In einem Hauptidealring R ist ein R-Ideal P prim genau dann, wenn $P \neq (0)$ maximal ist.

Beweis:

„$\Longrightarrow$“

Sei P ein Primideal. Wir haben $P = (\alpha)$ für ein $\alpha \in R$. Ist $(\alpha \subseteq I = (\beta)$, so folgt $\beta \mid \alpha$. Ist dabei $(\alpha) \neq (\beta)$, so folgt $\alpha \nmid \beta$. Dann muss β eine Einheit sein, d.h. $I = R$. Also ist $P = (\alpha)$ maximal.

„$\Longleftarrow$“

Jedes maximale Ideal $\neq (0)$ ist prim.

□

Satz 3.23

Ist R ein Dedekind-Ring, so gilt:
R ist ein ZPE-Ring genau dann, wenn R ein Hauptidealring ist.

Beweis:

„$\Longrightarrow$“

Sei R ein ZPE-Ring. Wir nehmen an, dass ein R-Ideal existiert, welches kein Hauptideal ist. Nach Satz 3.12 gibt es dann auch ein Primideal P, das kein Hauptideal ist. Sei

$$S := \{I : \ I \text{ ist } R\text{-Ideal und } P \cdot I \text{ ist Hauptideal}\} \ .$$

Nach Satz 3.9 ist $S \neq \emptyset$ und enthält somit wegen (i') zu Definition 3.5 ein maximales Element M. Wir setzen $P \cdot M = (\alpha)$ für ein geeignetes $\alpha \in R$. Also ist $\alpha = \beta\gamma$ für ein $\beta \in P$ und ein $\gamma \in R$. Da R ein ZPE-Ring ist, zerfällt β (eindeutig) in irreduzible Elemente $\beta_1, \ldots, \beta_r$, also

$$\beta = \beta_1 \cdot \ldots \cdot \beta_r \ .$$

Es folgt $(\beta_1) \cdot \ldots \cdot (\beta_r) = (\beta) \subseteq P$, d.h. $P \mid (\beta_1) \cdot \ldots \cdot (\beta_r)$. Da P ein Primideal ist, haben wir $P \mid (\beta_j)$ für ein j, also $(\beta_j) \subseteq P$, also $\beta_j \in P$. Damit ist $\alpha = \beta_j \cdot \gamma'$ für ein irreduzibles $\beta_j \in P$; wir schreiben wieder $\alpha = \beta\gamma$ mit $\beta \in P$ irreduzibel. Also ist $(\beta) \subseteq P$, d.h. $P \mid (\beta)$, also $(\beta) = P \cdot J$ für ein R-Ideal J, wobei wegen

$$P \cdot M = (\alpha) = (\beta)(\gamma) = P \cdot J \cdot (\gamma)$$

nach Korollar 3.10 folgt $J \mid M$, also $M \subseteq J$. Aus der Maximalität von M in S erhalten wir andererseits $J \subseteq M$, also $J = M$. Somit gilt $(\alpha) = P \cdot M = (\beta)$, d.h. α und β sind assoziiert, und daher ist auch α irreduzibel. Nach Voraussetzung ist P kein Hauptideal, also existiert ein $\delta \in P \setminus (\alpha)$. Außerdem ist $(\alpha) \subsetneq M$ (sonst wäre $P = R$), also gibt es ein $\sigma \in M \setminus (\alpha)$. Es folgt

$$\delta \cdot \sigma \in P \cdot M = (\alpha) \ ,$$

d.h. $\alpha \mid \delta\sigma$, aber $\alpha \nmid \delta$ und $\alpha \nmid \sigma$. Es gibt also in R ein irreduzibles Element α, das nicht prim ist. Dies widerspricht der ZPE-Eigenschaft von R (Satz 1.47 (ii) gilt in beliebigen Integritätsbereichen mit demselben Beweis).

„$\Longleftarrow$“

Folgt direkt aus Satz 3.21.

□

Satz 3.24

Ein Integritätsbereich R ist ein Hauptidealring genau dann, wenn eine Funktion $f : R \longrightarrow \mathbb{N}_0$ existiert mit folgenden Eigenschaften:

(i) Aus $\alpha \mid \beta$ folgt $f(\alpha) \leq f(\beta)$, wobei $f(\alpha) = f(\beta)$ genau für Assoziierte α, β gilt.

(ii) Sind $\alpha, \beta \in R \setminus \{0\}$ mit $\alpha \nmid \beta$ und $\beta \nmid \alpha$, so gibt es Elemente $p, q, r \in R$ derart, dass

$$r = p\alpha + q\beta$$

und $f(r) < \min\{f(\alpha),\, f(\beta)\}$.

Beweis:

„$\Longrightarrow$“

Ein Hauptidealring R ist nach Satz 3.21 ein ZPE-Ring. Wir definieren $f(\alpha)$ als die Anzahl der irreduziblen Faktoren von α. Damit ist (i) sofort klar. Bedingung (ii) ergibt sich mit $r := \text{ggT}\ (\alpha, \beta)$ (vgl. Beweis zu Satz 1.51).

„$\Longleftarrow$“

Sei f mit (i) und (ii) gegeben, und sei $I \neq (0)$, $I \neq R$ ein R-Ideal. Sei $\alpha \in I \setminus \{0\}$ derart gewählt, dass $f(\alpha)$ minimal ist. Wir zeigen, dass $I = (\alpha)$ gilt. Wäre $\beta \in I$ mit $\alpha \nmid \beta$, so folgte wegen $f(\alpha) \leq f(\beta)$ aus (i), dass $\beta \nmid \alpha$ (sonst wären α und β assoziiert, also $\alpha \mid \beta$). Dann hätten wir mit (ii), dass für ein $r \in R$

$$f(r) < \min\{f(\alpha),\, f(\beta)\} \leq f(\alpha)\ .$$

Widerspruch! Also gilt $\alpha \mid \beta$ für alle $\beta \in I$, d.h. $I = (\alpha)$.

□

Korollar 3.25

Ist R ein euklidischer Ring, so ist R Hauptidealring und damit ZPE-Ring.

Beweis:

Eine euklidische Funktion (vgl. Definition 1.50) erfüllt die Bedingungen (i) und (ii) aus Satz 3.24, also ist R ein Hauptidealring und damit nach Satz 3.21 ein ZPE-Ring.

□

Korollar 3.26

Sei F ein Zahlkörper. Dann ist $\mathcal{O}_F$ ein Hauptidealring gdw. für alle $\alpha, \beta \in \mathcal{O}_F \setminus \{0\}$ mit $\alpha \nmid \beta$ und $\beta \nmid \alpha$ existieren $\gamma, \delta \in \mathcal{O}_F$ derart, dass

$$0 < \left| N_F\left(\frac{\alpha}{\beta} \cdot \gamma - \delta\right)\right| < 1\ .$$

Beweis:

Wir wählen $f(\alpha) = |N_F(\alpha)|$ in Satz 3.24. Dann ist (i) klar, und für $|N_F(\alpha)| \geq |N_F(\beta)|$ haben wir

$$\left| N_F\left(\frac{\alpha}{\beta} \cdot \gamma - \delta\right)\right| < 1 = \min\left\{\frac{|N_F(\alpha)|}{|N_F(\beta)|},\, 1\right\}\ ,$$

also

$$|N_F(\alpha\gamma - \beta\delta)| < \min\{|N_F(\alpha)| \ , \ |N_F(\beta)|\} \ ,$$

und damit ist (ii) erfüllt.

□

Bemerkung:

Korollar 3.26 kann verwendet werden, um explizit zu untersuchen, ob ein gegebenes $\mathcal{O}_F$ Hauptidealring ist oder nicht.

3.3. Normen von Idealen

Nach Satz 3.12 haben wir in einem Dedekind-Ring R für jedes R-Ideal $I \neq (0)$, $I \neq R$, eine eindeutige Zerlegung in Primideale

$$I = P_1^{\alpha_1} \cdot \ldots \cdot P_r^{\alpha_r} = \text{kgV } (P_1^{\alpha_1}, \ldots, P_r^{\alpha_r}) = \bigcap_{j=1}^{r} P_j^{\alpha_j} \ .$$

Aus dem Chinesischen Restsatz 3.15 ergibt sich damit

$$R/I = R/\bigcap_{j=1}^{r} p_j^{\alpha_j} \cong \prod_{j=1}^{r} R/P_j^{\alpha_j} \ .$$

In $R = \mathcal{O}_F$ mit einem Zahlkörper F haben wir für ein Primideal P gemäß Beweis zu Satz 3.6, dass $\mathcal{O}_F/P$ endlich ist. Darüber hinaus zeigt man leicht, dass

$$\left|\mathcal{O}_F/P^a\right| = \left|\mathcal{O}_F/P\right|^a \ .$$

Also erhalten wir insgesamt für ein $\mathcal{O}_F$-Ideal I

$$\left|\mathcal{O}_F/I\right| = \prod_{j=1}^{r} \left|\mathcal{O}_F/P_j\right|^{a_j} \ .$$

Definition 3.27

Sei F ein Zahlkörper, und sei I ein beliebiges $\mathcal{O}_F$-Ideal. Wir definieren die *Norm von I* durch

$$N(I) = \left|\mathcal{O}_F/I\right| \ .$$

Satz 3.28

Sei F ein Zahlkörper, seien $I \neq (0)$ und $J \neq (0)$ $\mathcal{O}_F$-Ideale, sei $P \neq (0)$ ein $\mathcal{O}_F$-Primideal. Dann gilt:

(i) $N(I) \in \mathbb{P} \Longrightarrow I$ ist Primideal;

(ii) $I \mid (N(I))$;

(iii) $N(P) = p^m$, wobei $P \cap \mathbb{Z} = (p)$ mit einem $p \in \mathbb{P}$ und $m \in \mathbb{N}$;

(iv) $N(I \cdot J) = N(I) \cdot N(J)$;

(v) $\alpha \in \mathcal{O}_F$ prim $\Longrightarrow (\alpha)$ ist Primideal.

Beweis:

(i) Mit $I = \prod_{j=1}^{r} P_j^{a_j}$ gemäß Satz 3.12 folgt nach Definition der Norm

$$N(I) = \prod_{j=1}^{r} N\left(P_j\right)^{a_j} \ .$$

Wegen $N(P_j) = \left|\mathcal{O}_F/P_j\right| > 1$, da $P_j \neq \mathcal{O}_F$, ist $N(I) \in \mathbb{P}$ nur möglich für $r = 1$ und $a_1 = 1$, d.h. $I = P_1$.

(ii) Sei $\mathcal{O}_F/I = \{\alpha_1 + I, \ldots, \alpha_n + I\}$ mit $n := \left|\mathcal{O}_F/I\right|$. Dann gilt auch

$$\mathcal{O}_F/I = \{\alpha_1 + 1 + I, \ldots, \alpha_n + 1 + I\} \ ,$$

denn aus $\alpha_i + 1 + I = \alpha_j + 1 + I$ folgte sofort $\alpha_i - \alpha_j = (\alpha_i + 1) - (\alpha_j + 1) \in I$, d.h. $\alpha_i + I = \alpha_j + I$. Widerspruch!

Das bedeutet

$$\sum_{j=1}^{n} (\alpha_j + I) = \sum_{j=1}^{n} (\alpha_j + 1 + I) \ ,$$

also

$$N(I) = \left|\mathcal{O}_F/I\right| = n = \sum_{j=1}^{n} (\alpha_j + 1) - \sum_{j=1}^{n} \alpha_j \in I \ .$$

Es ergibt sich $(N(I)) \subseteq I$, d.h. $I \mid (N(I))$.

(iii) Sei $N(P) = \prod_{j=1}^{r} p_j^{m_j}$ mit $p_j \in \mathbb{P}$, $m_j \in \mathbb{N}$. Es folgt mit (ii), dass $P \mid N(P) = \prod_{j=1}^{r} (p_j)^{m_j}$, also $P \mid (p_j)$ für ein j. Wäre auch $P \mid (p_k)$ für ein $k \neq j$, so hätten wir wegen $up_j + vp_k = 1$ für gewisse $u, v \in \mathbb{Z}$ und wegen $up_j \in P$ und $vp_k \in P$, dass $1 = up_j + vp_k \in P$, also $P = \mathcal{O}_F$. Widerspruch!

Also haben wir insgesamt , dass $N(P) = p^m$ für ein $p \in \mathbb{P}$ mit $P \mid (p)$, also $p \in P$ und $q \notin P$ für alle $q \in \mathbb{P} \setminus \{p\}$.

(iv) Seien $I = \prod_{j=1}^{r} P_j^{a_j}$ und $J = \prod_{j=1}^{r} P_j^{b_j}$ mit $a_j, b_j \in \mathbb{N}_0$ gemäß Satz 3.12. Dann haben wir

$$\begin{aligned} N(I \cdot J) &= N\left(\prod_{j=1}^{r} P_j^{a_j+b_j}\right) = \prod_{j=1}^{r} N(P_j)^{a_j+b_j} \\ &= \prod_{j=1}^{r} N(P_j)^{a_j} \cdot \prod_{j=1}^{r} N(P_j)^{b_j} = N(I) \cdot N(J) \ . \end{aligned}$$

(v) (α) ist ein Primideal in $\mathcal{O}_F$ gdw. $\mathcal{O}_F/(\alpha)$ ein Integritätsring ist, d.h. es genügt zu zeigen, dass $\mathcal{O}_F/(\alpha)$ keine Nullteiler besitzt. Sei also

$$(\beta + (\alpha)) \cdot (\gamma + (\alpha)) = \beta\gamma + (\alpha) = 0 \in \mathcal{O}_F/(\alpha) \ ,$$

d.h. $\beta\gamma \in (\alpha)$. Demnach gilt $\alpha \mid \beta\gamma$, also $\alpha \mid \beta$ oder $\alpha \mid \gamma$, da α prim ist. Es folgt $\beta \in (\alpha)$ oder $\gamma \in (\alpha)$, d.h. $\beta + (\alpha) = 0$ oder $\gamma + (\alpha) = 0$.

□

Beispiel:

Sei $F = \mathbb{Q}(\sqrt{10})$, also $\mathcal{O}_F = \mathbb{Z}[\sqrt{10}]$ nach Satz 1.43. Wir betrachten die $\mathcal{O}_F$-Ideale

$$P = (2, \sqrt{10}) \ , \ Q = (3, 1 + \sqrt{10}) \ , \ Q' = (3, 1 - \sqrt{10}) \ .$$

Dann gilt

$$Q \cdot Q' = \Big(9,\, 3(1 - \sqrt{10}),\, 3(1 + \sqrt{10})\Big) \subseteq (3)$$

und auch $3 = 9 - 3(1 - \sqrt{10}) - 3(1 + \sqrt{10}) \in Q \cdot Q'$, also $(3) \subseteq Q \cdot Q'$, d.h. $Q \cdot Q' = (3)$.

Analog erhalten wir

$$P^2 = (4,\, 2\sqrt{10},\, 10) \subseteq (2)$$

und $2 = 10 - 2 \cdot 4 \in P^2$, also $(2) \subseteq P^2$ und daher $P^2 = (2)$. Zusammen erhalten wir

$$(6) = (2) \cdot (3) = P^2 \cdot Q \cdot Q' \ .$$

Wir wollen zeigen, dass dies die Primidealzerlegung von (6) ist (vgl. letztes Beispiel in Abschnitt 1.1.). Wir haben $\mathcal{O}_F = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$ und somit

$$\begin{aligned} \mathcal{O}_F \setminus P &= \{a + b\sqrt{10} : a, b \in \mathbb{Z}\} \setminus \{2a + b\sqrt{10} : a, b \in \mathbb{Z}\} \\ &= \{a + b\sqrt{10} : a, b \in \mathbb{Z},\ 2 \nmid a\} \ . \end{aligned}$$

Daher gilt für ein beliebiges $u + v\sqrt{10} \in \mathcal{O}_F \setminus P$, dass

$$(P,\ u + v\sqrt{10}) = \mathbb{Z}[\sqrt{10}] = \mathcal{O}_F \ ,$$

denn mit $(u + 1) + v\sqrt{10} \in P$ haben wir

$$1 = \Big((u + 1) + v\sqrt{10}\Big) - \Big(u + v\sqrt{10}\Big) \in \Big(P,\ u + v\sqrt{10}\Big) \ .$$

Also ist P ein maximales Ideal und somit ein Primideal. Außerdem ist jedes Element in $\mathbb{Z}[\sqrt{10}]$ von der Form $\alpha \in P$ oder von der Form $\alpha + 1$ mit $\alpha \in P$, also

$$N(P) = \big|\mathcal{O}_F / P\big| = \Big|\mathbb{Z}[\sqrt{10}]/P\Big| = 2 \ .$$

Analog lässt sich zeigen, dass jedes Element in $\mathbb{Z}[\sqrt{10}]$ von der Form $\alpha := 3a + b + b\sqrt{10} \in Q$ oder von der Form $\alpha + 1$ oder $\alpha + 2$ mit $\alpha \in Q$ ist, also

$$N(Q) = \Big|\mathbb{Z}[\sqrt{10}]/Q\Big| = 3 \ .$$

Entsprechend gilt $N(Q') = 3$. Nach Satz 3.28 (i) folgt, dass Q und Q' Primideale sind. Damit haben wir die gewünschte Primidealzerlegung von (6) und darüber hinaus

$$N((6)) = N(P)^2 \cdot N(Q) \cdot N(Q') = 2^2 \cdot 3^2 = 36 \ ,$$

wobei wir feststellen, dass $N((6)) = N_F(6)$ (vgl. Beweis zu Satz 2.1).

Satz 3.29

Sei F ein Zahlkörper und sei $I \neq (0)$ ein $\mathcal{O}_F$-Ideal. Für jede $\mathbb{Z}$-Basis $\mathcal{B}$ von I gilt

$$N(I) = \sqrt{\frac{\text{discr } (\mathcal{B})}{\Delta_F}} \ .$$

Beweis:

Nach Bemerkung (ii) und (iii) zu Definition 2.22 sind für $[F : \mathbb{Q}] =: n = r_1 + 2r_2$ die Gitter $\Theta(\mathcal{O}_F) \subseteq \mathbb{R}^n$ und $\Theta(I) \subseteq \Theta(\mathcal{O}_F)$ volle Gitter in $\mathbb{R}^n$, wobei für die Fundamentalbereiche gilt

$$V\left(P_{\Theta(\mathcal{O}_F)}\right) = \left(\frac{1}{2}\right)^{r_2} \cdot \sqrt{|\Delta_F|} \quad , \quad V\left(P_{\Theta(I)}\right) = \left(\frac{1}{2}\right)^{r_2} \cdot \sqrt{|\text{discr } \mathcal{B}|} \ ,$$

und

$$V\left(P_{\Theta(I)}\right) = \left|\mathcal{O}_F/I\right| \cdot V\left(P_{\Theta(\mathcal{O}_F)}\right) \ .$$

Also folgt

$$N(I) = \left|\mathcal{O}_F/I\right| = \frac{\left(\frac{1}{2}\right) \cdot \sqrt{|\text{discr } (\mathcal{B})|}}{\left(\frac{1}{2}\right) \cdot \sqrt{|\Delta_F|}} = \sqrt{\left|\frac{\text{discr } (\mathcal{B})}{\Delta_F}\right|} \ .$$

Nach Satz 1.35 haben discr $(\mathcal{B})$ und Δ_F dasselbe Vorzeichen, und damit folgt die Behauptung.

□

Korollar 3.30

Ist (α) ein Hauptideal in $\mathcal{O}_F$, so gilt $N((\alpha)) = |N_F(\alpha)|$.

Beweis:

Sei $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ mit $n = [F : \mathbb{Q}]$ eine Ganzheitsbasis von F, also discr $\mathcal{B} = \Delta_F$. Dann ist

$$\alpha\mathcal{B} = \{\alpha\beta_1, \ldots, \alpha\beta_n\}$$

eine $\mathbb{Z}$-Basis von (α). Dabei haben wir

$$\begin{aligned} \text{discr } (\alpha\mathcal{B}) &= \det\left(\Theta_i(\alpha\beta_j)\right)^2 = \det\left(\Theta_i(\alpha)\cdot\Theta_i(\beta_j)\right)^2 \\ &= \prod_{i=1}^{n}\Theta_i(\alpha)^2\cdot\det\left(\Theta_i(\beta_j)\right)^2 \\ &= N_F(\alpha)^2\cdot\text{discr }(\mathcal{B}) = N_F(\alpha)^2\cdot\Delta_F\ . \end{aligned}$$

Mit Satz 3.29 folgt

$$N((\alpha)) = \sqrt{\frac{\text{discr }(\alpha\mathcal{B})}{\Delta_F}} = \sqrt{N_F(\alpha)^2} = |N_F(\alpha)|\ .$$

□

Satz 3.31

Sei F ein Zahlkörper mit $[F:\mathbb{Q}] = n = r_1 + 2r_2$, wobei $\{r_1, r_2\}$ die Signatur von F bezeichne. In jedem $\mathcal{O}_F$-Ideal I gibt es ein $\alpha \in I \setminus \{o\}$ derart, dass

$$|N_F(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2}\cdot\frac{n!}{n^n}\cdot\sqrt{|\Delta_F|}\cdot N(I)\ .$$

Beweis:

Dies ist nur eine Neuformulierung von Satz 2.23 mit $M := I$.

□

3.4. Idealformen und die Klassengruppe

Aus $\mathbb{Z}$ entsteht durch Bildung von Brüchen der Körper $\mathbb{Q}$ der rationalen Zahlen. Die bislang untersuchten Ideale lassen sich als „ganze“ Ideale auffassen.

Definition 3.32

Sei R ein Integritätsbereich mit Quotientenkörper F. Ein R-Modul $M \neq \{0\}$ in F heißt *gebrochenes R-Ideal*, falls es ein $\alpha \in R \setminus \{0\}$ gibt so, dass $\alpha M \subseteq R$. Ist M ein gebrochenes Ideal mit $M \subseteq R$, so nennen wir M ein *ganzes Ideal*.

Bemerkungen:

(i) Ganze Ideale sind genau die R-Ideale im früheren Sinne.

(ii) Ist M ein gebrochenes Ideal mit $\alpha M \subseteq R$ für ein $\alpha \in R \setminus \{0\}$, so ist αM ein ganzes Ideal I, d.h. jedes gebrochene Ideal M besitzt eine Darstellung

$$M = \frac{1}{\alpha} \cdot I$$

für ein $\alpha \in R \setminus \{0\}$ und ein ganzes Ideal I.

Wir wollen zeigen, dass die Menge der gebrochenen Ideale eine Gruppe bildet. Wie bei ganzen Idealen erklären wir das Produkt $M_1 \cdot M_2$ zweier gebrochener R-Ideale M_1 und M_2 als den kleinsten R-Modul M, der alle Produkte $m_1 \cdot m_2$ mit $m_i \in M_i$ enthält, d.h. M besteht aus allen endlichen Summen solcher Produkte.

Ist M ein gebrochenes R-Ideal in einem Integritätsring R mit Quotientenkörper F, so setzen wir

$$M^{-1} := \{\alpha \in F : \alpha M \subseteq R\} \ .$$

M^{-1} ist ein gebrochenes Ideal, denn:
M^{-1} ist offensichtlich ein R-Modul. Sei $\beta \in R \setminus \{0\}$ mit $\beta M \subseteq R$ (M ist ein

gebrochenes Ideal), und sei $\gamma \in M^{-1}$ beliebig, d.h. $\gamma m \in R$ für alle $m \in M$. Mit einem beliebigen $m_0 \in M \setminus \{0\}$ erhalten wir

$$(\beta m_0) \cdot \gamma = \beta \cdot (\gamma m_0) \in R \cdot R = R \ ,$$

d.h. $(\beta m_0) \cdot M^{-1} \subseteq R$.

Ein gebrochenes R-Ideal M heißt *invertierbar*, falls $M \cdot M^{-1} = R$ (also wird R das Einselement in unserer Gruppe von Idealen sein).

Lemma 3.33

Sei R ein Dedekindring. Jedes ganze R-Primideal $P \neq (0)$ ist invertierbar.

Beweis:

Nach Satz 3.12 existieren zu einem beliebigen $\alpha \in P \setminus \{0\}$ Primideale $P_1, \ldots, P_r$ mit

$$(\alpha) = P_1 \cdot \ldots \cdot P_r \ .$$

Wegen $\alpha \in P$ ist $(\alpha) \subseteq P$, also $P \mid (\alpha)$ und somit $P = P_j$ für ein j. Sei o.B.d.A. $P = P_1$. Selbstverständlich ist $(\alpha) \nmid P_2 \cdot \ldots \cdot P_r$, also $P_2 \cdot \ldots \cdot P_r \nsubseteq (\alpha)$. Wir wählen ein $\beta \in P_2 \cdot \ldots \cdot P_r \setminus (\alpha)$. Es folgt

$$\beta P \subseteq P \cdot P_2 \cdot \ldots \cdot P_r = (\alpha) \ ,$$

also $\beta/\alpha \cdot P \subseteq R$ und daher $\beta/\alpha \in P^{-1}$. Wegen $\beta \notin (\alpha)$ ist $\beta/\alpha \notin R$, und wegen P ganz (also $P \subseteq R$) ist $R \subseteq P^{-1}$. Also haben wir

$$\frac{\beta}{\alpha} \cdot P \subseteq \left(P^{-1} \setminus R\right) \cdot P = P \cdot P^{-1} \setminus P \ ,$$

und damit

$$P = P \cdot R \subsetneq P \cdot P^{-1} \subseteq R \ ,$$

wobei die letzte Inklusion direkt aus der Definition P^{-1} folgt. Damit gilt für die ganzen Ideale P und $P \cdot P^{-1}$

$$P \subsetneq P \cdot P^{-1} \subseteq R \ .$$

Da P ein Primideal ist, folgt aus Eigenschaft (ii) für Dedekind-Ringe (Definition 3.5), dass P maximal ist. Also bleibt nur $P \cdot P^{-1} = R$, d.h. P ist invertierbar.

□

Satz 3.34

Sei R ein Dedekind-Ring. Die Menge $\mathcal{F}(R)$ der gebrochenen Ideale in R bildet eine multiplikative Gruppe mit neutralem Element R und Inversem M^{-1} von M für alle $M \in \mathcal{F}(R)$. Die Menge $\mathcal{P}(R)$ der gebrochenen Hauptideale ist eine Untergruppe von $\mathcal{F}(R)$.

Beweis:

Es sind alle Aussagen klar bis auf die Inversenbildung:
Sei zunächst $M \in \mathcal{F}(R)$ ganz. Dann existieren nach Satz 3.12 eindeutig Primideale $P_1, \ldots, P_r$ mit

$$M = P_1 \cdot \ldots \cdot P_r \ .$$

Nach Lemma 3.33 besitzt jedes P_j das Inverse P_j^{-1}. Also ist $M' := P_1^{-1} \cdot \ldots \cdot P_r^{-1}$ ein Inverses von M , d.h. $M \cdot M' = R$. Es folgt sofort

$$M' \subseteq M^{-1} := \{\alpha \in F : \alpha M \subseteq R\} \ ,$$

wobei F den Quotientenkörper von R bezeichnet. Ist umgekehrt $\alpha \in M^{-1}$, d.h. $\alpha M \subseteq R$, so haben wir

$$\alpha \in \alpha R = \alpha M \cdot M' \subseteq R \cdot M' = M' \ ,$$

also insgesamt $M' = M^{-1}$.
Sei nun M ein gebrochenes Ideal. Dann gibt es ein $\alpha \in R \setminus \{0\}$ mit $\alpha M \subseteq R$, d.h. αM ist ein ganzes Ideal. Nach obigen Überlegungen ist $(\alpha M)^{-1}$ das Inverse von αM, wobei

$$\begin{aligned}(\alpha M)^{-1} &= \{\beta \in F : \beta \cdot (\alpha M) \subseteq R\} \\ &\overset{\alpha\beta=:\gamma}{=} \left\{\frac{\gamma}{\alpha} \in F : \gamma M \subseteq R\right\} \\ &= \frac{1}{\alpha} \cdot \{\gamma \in F : \gamma M \subseteq R\} \\ &= \alpha^{-1} \cdot M^{-1} \ .\end{aligned}$$

Es folgt

$$M \cdot M^{-1} = (\alpha M) \cdot (\alpha M)^{-1} = R \ .$$

Definition 3.35

Sei R ein Dedekind-Ring. Die Faktorgruppe

$$\mathcal{C}_R := \mathcal{F}(R)/\mathcal{P}(R)$$

heißt *Klassengruppe von* R. Für $R = \mathcal{O}_F$ schreiben wir $\mathcal{C}_R = \mathcal{C}_F$.

Zwei gebrochene Ideale heißen *äquivalent*, falls sie in dieselbe Nebenklasse von $\mathcal{P}(R)$ in $\mathcal{F}(R)$ gehören; mit anderen Worten:
Zwei gebrochene Ideale I, J sind äquivalent, geschrieben $I \sim J$, sofern $\Psi(I) = \Psi(J)$ unter der kanonischen Abbildung

$$\Psi : \begin{cases} \mathcal{F}(R) & \longrightarrow & \mathcal{F}(R)/\mathcal{P}(R) \\ I & \longmapsto & I \cdot \mathcal{P}(R) =: \overline{I} \ . \end{cases}$$

Bemerkung:

Nach Definition von $\sim$ ist klar, dass $I \sim J \iff I = (\gamma) \cdot J$ für ein $\gamma \in F$. Nach Bemerkung (ii) zu Definition 3.32 ist jedes gebrochene Ideal I darstellbar als $I = \frac{1}{\alpha}J$ mit einem $\alpha \in F$ und einem ganzen Ideal J, also $(\alpha) \cdot I = J$, d.h. $I \sim J$ ($\iff \overline{I} = \overline{J}$). Damit ist gezeigt, dass jede Idealklasse ganze Ideale enthält.

Satz 3.36

Sei R ein Dedekind-Ring. Dann ist R ein ZPE-Ring gdw. $|\mathcal{C}| = 1$.

Beweis:

Nach Satz 3.23 ist R ein ZPE-Ring genau dann, wenn R ein Hauptidealring ist, d.h. alle ganzen Ideale sind Hauptideale. Nach vorangegangener Bemerkung sind demnach alle Ideale Hauptideale, d.h. $\mathcal{F}(R) = \mathcal{P}(R)$, d.h. $|\mathcal{C}_R| = 1$.

□

Satz 3.37

Für jeden Zahlkörper F besitzt $\mathcal{C}_F$ nur endlich viele Elemente.

Beweis:

Behauptung: Zu jeder Konstanten $C \in \mathbb{R}_{>0}$ gibt es nur endlich viele ganze $\mathcal{O}_F$-Ideale I mit $N(I) \leq C$.

Dann sei zunächst $P \neq (0)$ ein ganzes Primideal. Nach Satz 3.28 (iii) ist $N(P) = p^m$ für ein $p \in P \cap \mathbb{Z}$ und ein $m \in \mathbb{N}$, wobei $p \in \mathbb{P}$. Zu jedem festen $p \in \mathbb{P}$ gibt es nur endlich viele ganze Primideale P mit $N(P) = p^m$ für irgendein $m \in \mathbb{N}$, denn $(p) \subseteq P$, d.h. $P \mid (p)$, und (p) zerfällt eindeutig in endlich viele Primideale nach Satz 3.12. Da es nur endlich viele Primzahlpotenzen $p^m \leq C$ gibt, haben wir die obige behauptung für Primideale bereits gezeigt.

ist nun I beliebig, so haben wir nach Satz 3.12

$$I = P_1^{a_1} \cdot \ldots \cdot P_r^{a_r}$$

für gewisse ganze Primideale P_j und $a_j \in \mathbb{N}$ $(1 \leq j \leq r)$. Aus $N(I) \leq C$ folgt wegen $N(I) = N(P_1)^{a_1} \cdot \ldots \cdot N(P_r)^{a_r}$ (nach Satz 3.28 (iv)), dass

$$N(P_j)^{a_j} \leq C \qquad (1 \leq j \leq r) \ ,$$

denn $N(P_j) \geq 2$ (da $N(P_j) = |\mathcal{O}_F/P_j|$ und $\mathcal{O}_F \neq P_j$). Daher und aufgrund der bereits bewiesenen Behauptung für Primideale folgt die Richtigkeit der eingangs gemachten Aussage.
Sei nun H ein beliebiges gebrochenes $\mathcal{O}_F$-Ideal. Nach der Bemerkung hinter Definition 3.35 gibt es ein ganzes $\mathcal{O}_F$-Ideal $J \in \overline{H}$. Wir können ein $\beta \in \mathcal{O}_F \setminus \{0\}$ wählen derart, dass $I = \beta \cdot J^{-1} \subseteq \mathcal{O}_F$. Nach Satz 3.31 existiert dann ein $\alpha \in I \setminus \{0\}$ mit

$$|N_F(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|\Delta_F|} \cdot N(I) \ .$$

Wegen $\alpha \in I$ ist $\alpha \cdot I^{-1} \subseteq I \cdot I^{-1} = \mathcal{O}_F$, d.h. $H_0 := \alpha I^{-1}$ ist ein ganzes $\mathcal{O}_F$-Ideal. Außerdem folgt

$$\begin{aligned} N(H_0) &= N((\alpha) \cdot I^{-1}) = N((\alpha)) \cdot N(I^{-1}) = |N_F(\alpha)| \cdot N(I)^{-1} \\ &\leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|\Delta_F|} =: C \end{aligned}$$

nach Satz 3.28 (iv), Korollar 3.30 und wegen $1 = N(\mathcal{O}_F) = N(I \cdot I^{-1}) = N(I) \cdot N(I^{-1})$. Wir haben also wegen

$$H_0 = \alpha I^{-1} = \alpha \cdot \beta^{-1} \cdot J \sim J \sim H$$

jedem gebrochenen Ideal H ein ganzes Ideal H_0 mit $\overline{H_0} = \overline{H}$ und $N(H_0) \leq C$ zugeordnet. Nach der zu Beginn des Beweises gezeigten Aussage gibt es nur endlich viele ganze Ideale H_0 mit $N(H_0) \leq C$ und somit nur endlich viele Idealklassen $\overline{H}$, d.h. $\mathcal{C}_F$ ist endlich.

□

Definition 3.38

Sei F ein Zahlkörper mit Signatur $\{r_1, r_2\}$ und $[F : \mathbb{Q}] = n = r_1 + 2r_2$. Dann heißt $|\mathcal{C}_F|$ die *Klassenzahl von* $\mathcal{O}_F$; Standardbezeichnung: $h_F := |\mathcal{C}_F|$. Außerdem heißt

$$M_F := \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|\Delta_F|}$$

die *Minkowski-Schranke von F.*

Bemerkung:

Der Ausdruck „Minkowski-Schranke“ findet seine Berechtigung in der von Minkowski bewiesenen Ungleichung

$$h_F \leq |\{I \subseteq \mathcal{O}_F : N(I) \leq M_F\}| \ .$$

Beispiel:

Sei F ein quadratischer Zahlkörper mit $-8 \leq \Delta_F \leq 13$. Dann gilt $N(I) \leq M_F$ nur für $N(I) = |\mathcal{O}_F/I| = 1$, d.h. $I = \mathcal{O}_F$ $(M_F = \frac{2}{\pi} \cdot \sqrt{|\Delta_F|} < 2$ für $-8 \leq \Delta_F \leq 0$ bzw. $M_F = \frac{1}{2} \cdot \sqrt{|\Delta_F|} < 2$ für $0 \leq \Delta_F \leq 13)$. Nach Satz 3.36 folgt, dass $\mathcal{O}_F$ ein ZPE-Ring ist für $\Delta_F \in \{-3, -4, -7, -8, 5, 8, 12, 13\}$.

Bemerkung:

Satz 3.37 von der Endlichkeit der Klassenzahl h_F zeigt, dass der Übergang von den Zahlen zu den Idealen nicht ins Uferlose führt. Der günstigste Fall ist natürlich $h_F = 1$, d.h. $\mathcal{O}_F$ ist Hauptidealring, was wiederum gleichbedeutend ist damit, dass der Satz von der eindeutigen Primfaktorzerlegung wie in $\mathbb{Z}$ gilt. Bei den quadrqtischen Zahlkörpern ist der Stand der Dinge wie folgt: Es gibt genau neun komplexquadratische Zahlkörper $\mathbb{Q}(\sqrt{D})$ mit Klassenzahl 1, nämlich für $D = -1, -2, -3, -7$, $-11, -19, -43, -67, -163$ und vermutlich unendlich viele reell-quadratische Zahlkörper (vgl. Bemerkung nach Satz 2.3). Dabei ist bis heute nicht einmal bewiesen, dass es unter allen Zahlkörpern unendlich viele mit Klassenzahl 1 gibt.

In vielen Untersuchungen hat sich ergeben, dass die Klassengruppe $\mathcal{C}_F$ zu verschiedenen Zahlkörpern F nach Größe und Struktur anscheinend ganz regellos ausfallen. Eine Ausnahme hiervon bilden die Kreisteilungskörper $\mathbb{Q}(\zeta_{p^a})$ mit primitiven p^a-ten Einheitswurzeln ζ_{p^a}. Die von Iwasawa entdeckte Gesetzmäßigkeit ist eng verknüpft mit der in Abschnitt 1.1. erwähnten Fermat-Vermutung:

Aus $x^p + y^p = z^p$ folgt

$$(x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdot \ldots \cdot (x + \zeta_p^{p-1} y) = z \cdot z \cdot \ldots \cdot z \ ,$$

d.h. wir haben zwei multiplikative Zerlegungen einer einzigen Zahl in $\mathbb{Z}[\zeta_p]$. Das widerspräche der eindeutigen Primfaktorzerlegung, vorausgesetzt, dass sie in $\mathbb{Z}[\zeta_p]$ gilt, d.h. dass $h_{\mathbb{Q}(\zeta_p)} = 1$ gilt. Leider ist dies im Allgemeinen falsch. Kummer bewies jedoch, dass sie genannte Schlussweise zu retten ist, sofern (anstelle von $h_{\mathbb{Q}(\zeta_p)} = 1$) wenigstens $p \nmid h_{\mathbb{Q}(\zeta_p)}$ gilt Primzahlen mit dieser Eigenschaft nannte Kummer *regulär*. Von den ersten 25 Primzahlen p (d.h. $p < 100$) sind nur drei irregulär (nämlich $p = 37, 59, 67$). Damit ist also zum Beispiel die Fermat-Vermutung für alle anderen Exponenten $p < 100$ bewiesen.

Index