Masterstudium Mathematik
Universität Wien

– **Vorlesungsskript** –

Algebraische Zahlentheorie

Dietrich Burde

2013

Inhaltsverzeichnis

1 Einleitung

Die Zahlentheorie ist ein Teilgebiet der Mathematik, die sich im weitesten Sinne mit den Eigenschaften von ganzen Zahlen beschäftigt. Sie ist eine der ältesten Wissenschaften überhaupt. Traditionell unterscheidet man in der Zahlentheorie noch verschiedene Richtungen, wie beispielsweise die elementare Zahlentheorie, die analytische Zahlentheorie, die algebraische Zahlentheorie und arithmetische Geometrie, und in letzter Zeit auch die algorithmische Zahlentheorie. Auf der anderen Seite ist diese Trennung in verschiedene Teilgebiete nicht immer sinnvoll. So sind zum Beispiel analytische Methoden in der algebraischen Zahlentheorie durchaus wichtig. Bei dem gerne verwendeten Begriff der *modernen* Zahlentheorie kommen zahlreiche verschiedene Methoden zum Einsatz. Der Beweis des großen Satzes von Fermat etwa zeigt sehr eindrucksvoll, wie viele verschiedene Gebiete und Methoden angewendet worden sind. Zudem kann man sagen, daß dieses Fermatsche Problem, nämlich die Frage nach der ganzzahligen Lösbarkeit der Diophantischen Gleichung der Form $x^n + y^n = z^n$ für $n \geq 2$, die algebraische Zahlentheorie wesentlich mitgeprägt hat. In Analogie zu den ganzen Zahlen in den rationalen Zahlen, also des Ringes $\mathbb{Z}$ in seinem Quotientenkörper $\mathbb{Q}$, studiert man in der algebraischen Zahlentheorie die Ganzzahlringe in Zahlkörpern, also in endlichen Erweiterungen von $\mathbb{Q}$. Warum das interessant ist, sehen wir im Prinzip schon an der Fermatschen Gleichung zum Exponenten $n = 3$. Eine ganzzahlige Lösung (x, y, z) der Fermatschen Gleichung heißt *trivial*, wenn $xyz = 0$ ist. Das Beispiel $(0, y, y)$ zeigt, daß es unendlich viele triviale Lösungen gibt.

Satz 1.0.1 (Euler 1770)**.** *Die Gleichung $x^3+y^3 = z^3$ hat keine nicht-triviale ganzzahlige Lösung.*

Beweis. Für einen detailierten Beweis siehe etwa [6]. Wir skizzieren hier nur die wichtigsten Argumente und wollen vor allen Dingen ja den Zusammenhang mit Ganzzahlringen aufzeigen. Sei ζ eine primitive dritte Einheitswurzel, also etwa $\zeta = e^{\frac{2\pi i}{3}}$. Das Minimalpolynom von ζ über $\mathbb{Q}$ ist x^2+x+1. Damit ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine quadratische Körpererweiterung, und $\mathbb{Q}(\zeta)$ ist ein Vektorraum über $\mathbb{Q}$ mit Basis $\{1, \zeta\}$. Das Polynom $t^3 - 1$ zerfällt über $\mathbb{Q}(\zeta)$ als

$$t^3 - 1 = (t - 1)(t - \zeta)(t - \zeta^2).$$

Einsetzen von $t = -x/y$ und hochmultiplizieren ergibt

$$z^3 = x^3 + y^3 = (x + y)(x + \zeta y)(x + \zeta^2 y). \tag{1.1}$$

Damit haben wir unsere Fermatgleichung nun als Produktzerlegung einer dritten Potenz geschrieben, und zwar über dem Ring

$$\mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}.$$

Dieser Ring, auch manchmal der Ring der *Eisensteinschen ganzen Zahlen* genannt, hat nun glücklicherweise sehr gute Eigenschaften. Er ist ein Euklidischer Ring, und daher auch ein Hauptidealring und ein faktorieller Ring. Seine Einheiten sind durch $\pm 1, \pm\zeta, \pm\zeta^{-1}$ gegeben. Er ist der Ganzzahlring von $\mathbb{Q}(\zeta)$.
Nehmen wir jetzt also an, (x, y, z) ist eine nicht-triviale Lösung der Fermatgleichung, und alle Zahlen sind paarweise teilerfremd. Dann muß $3 \mid xyz$ gelten, denn ansonsten wäre $x^3 + y^3 \equiv -2, 0, 2 \mod 9$ und $z^3 \equiv 1, -1$; also sicherlich nicht $x^3 + y^3 = z^3$. Das bedeutet, zumindest eine der Zahlen ist durch 3 teilbar. Wir dürfen $3 \mid z$ annehmen, und $3 \nmid xy$. Nun formulieren wir unser Problem neu. Wir müssen zeigen, daß die Gleichung

$$x^3 + y^3 = (3^m z)^3 \tag{1.2}$$

keine nicht-trivialen Lösungen hat, mit ganzen Zahlen x, y, z paarweise teilerfremd, $3 \nmid xyz$, und m eine nicht-negative ganze Zahl. Für $m = 0$ haben wir gerade gezeigt, daß es keine Lösungen geben kann. Wir erhalten aus (1.2), wie in (1.1),

$$(3^m z)^3 = (x + y)(x + \zeta y)(x + \zeta^2 y)$$

in $\mathbb{Z}[\zeta]$. Die drei Faktoren sind nicht paarweise teilerfremd. Es ist aber leicht zu sehen, daß ihr größter gemeinsamer Teiler jeweils das Primelement $1 - \zeta$ ist. Zum Beispiel gilt wegen $3 = (1-\zeta)(1-\zeta^2)$ etwa $1-\zeta \mid 3 \mid x+y$ und somit $1-\zeta \mid x+y$. Nun wird wesentlich benutzt, daß der Ring $\mathbb{Z}[\zeta]$ faktoriell ist. Die drei Faktoren in unserer Gleichung sind also auch dritte Potenzen, bis auf Einheiten und Potenzen von $1 - \zeta$. Teilbarkeitsargumente in $\mathbb{Z}[\zeta]$ zeigen, daß man sogar

$$\begin{aligned} x + y &= 3^{3m-1} c^3, \\ x + \zeta y &= (1 - \zeta)\rho^3 \end{aligned}$$

schreiben kann, mit $\rho \in \mathbb{Z}[\zeta]$, $c \in \mathbb{Z}$; c und ρ teilerfremd, und nicht durch $1 - \zeta$ teilbar. Also hat man auch $3 \nmid c$. Setzt man $\rho = a + \zeta b$ mit $a, b \in \mathbb{Z}$ in die zweite Gleichung ein, so erhält man mit $\zeta^2 = -1 - \zeta$,

$$\begin{aligned} x + \zeta y &= (1 - \zeta)(a + b\zeta)^3 \\ &= (1 - \zeta)(a^3 - 3ab^2 + b^3 + 3a^2 b\zeta - 3ab^2\zeta) \\ &= (a^3 + b^3 + 3a^2 b - 6ab^2) + \zeta(-a^3 - b^3 + 6a^2 b - 3ab^2). \end{aligned}$$

Koeffizientenvergleich ergibt $x = a^3 + b^3 + 3a^2 b - 6ab^2$ und $y = -a^3 - b^3 + 6a^2 b - 3ab^2$, so daß $9ab(a - b) = x + y = 9(3^{m-1}c)^3$, d.h.

$$ab(a - b) = (3^{m-1}c)^3.$$

Wegen $xyz \neq 0$ sind auch $a, b, a - b$ nicht Null. Zudem sind sie paarweise teilerfremd. Da der Ring $\mathbb{Z}$ faktoriell ist, sind $a, b, a - b$ selbst dritte Potenzen in $\mathbb{Z}$, und zwar gilt

$$\{a, b, a - b\} = \{x_1^3, y_1^3, (3^{m-1} z_1)^3\}$$

mit x_1, y_1, z_1 paarweise teilerfremd und $3 \nmid z_1$. Wegen $a + (-b) = a - b$, $a + (b - a) = b$ und $b + (a - b) = a$ ergibt dies jedenfalls eine Gleichung der Form (1.2) mit $x_0^3 + y_0^3 = (3^{m-1} z_0)^3$, wobei x_0, y_0, z_0 paarweise teilerfremde ganze Zahlen sind mit $3 \nmid x_0 y_0 z_0$, aber mit Exponenten $m - 1$ anstatt m. So können wir iterativ zu $m = 0$ *absteigen* (eine Methode, die schon Fermat für $x^4 + y^4 = z^4$ angewandt hat), was unmöglich ist. □

Leider funktionieren diese Ideen so nicht für $x^p + y^p = z^p$, wenn p eine beliebige Primzahl ist. Denn der Ring $\mathbb{Z}[\zeta]$ ist dann, für eine primitive p-te Einheitswurzel ζ, nur noch sehr selten faktoriell - tatsächlich nur für $p \leq 19$. Zudem sind die Einheiten von $\mathbb{Z}[\zeta]$ nicht mehr nur von der Form $\pm\zeta^j$ mit $j \geq 0$. Immerhin ist $\mathbb{Z}[\zeta]$ aber immer der Ganzzahlring von $\mathbb{Q}(\zeta)$, und es lohnt sich, diese Ganzzahlringe zu studieren. Kummer machte große Fortschritte bezüglich der Fermatschen Gleichung, indem er die verlorene Eindeutigkeit der Faktorisierung in irreduzible Elemente von $\mathbb{Z}[\zeta]$ durch eine eindeutige Faktorisierung von *Idealen* in $\mathbb{Z}[\zeta]$ in Primideale ersetzen konnte. Das war gleichzeitig auch in gewisser Weise die Geburtsstunde für die algebraische Zahlentheorie.

2 Ganze Ringerweiterungen

Alle Ringe werden als kommutativ mit Eins vorausgesetzt, wenn nichts anderes gesagt wird.

2.1 Globale Körper und Ganzheit

Es bezeiche $\mathbb{F}_p$ den endlichen Körper $\mathbb{Z}/p$ für eine Primzahl p, und $\mathbb{F}_p[t]$ den Polynomring in einer Variablen mit Koeffizienten in $\mathbb{F}_p$. Der Quotientenkörper von $\mathbb{F}_p[t]$ wird mit $\mathbb{F}_p(t)$ bezeichnet. Der Quotientenkörper von $\mathbb{Z}$ wird wie gewohnt mit $\mathbb{Q}$ bezeichnet.

Definition 2.1. Ein *Zahlkörper* K ist eine endliche Körpererweiterung von $\mathbb{Q}$. Ein *Funktionenkörper* K ist eine endliche Körpererweiterung von $\mathbb{F}_p(t)$.

Zahlkörper und Funktionenkörper werden oft zusammen betrachtet und als *globale Körper* bezeichnet. Ein Unterschied ist, daß Zahlkörper Charakteristik Null haben, während Funktionenkörper Charakteristik p haben.

Beispiel 2.1.1. *Sei K eine Körpererweiterung vom Grad 2 über $\mathbb{Q}$. Dann gibt es ein quadratfreies $d \in \mathbb{Z}$ mit $K = \mathbb{Q}(\sqrt{d})$.*

Man nennt $\mathbb{Q}(\sqrt{d})$ dann einen quadratischen Zahlkörper.

Beispiel 2.1.2. *Sei K eine Körpererweiterung vom Grad 2 über $\mathbb{F}_p(t)$. Dann gibt es ein quadratfreies Polynom $D \in \mathbb{F}_p[t]$ mit $K = \mathbb{F}_p(t, \sqrt{D}) = \{A + B\sqrt{D} \mid A, B \in \mathbb{F}_p(t)\}$.*

Man nennt $\mathbb{F}_p(t, \sqrt{D})$ einen quadratischen Funktionenkörper.

Definition 2.2. Sei $A \subset B$ eine Ringerweiterung. Ein Element $x \in B$ heißt *ganz über* A, falls es ein normiertes Polynom $f \in A[t]$ gibt mit $f(x) = 0$. Mit anderen Worten, x erfüllt eine polynomiale Gleichung

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

mit Koeffizienten a_i in A.

Beispiel 2.1.3. *Sei $A = \mathbb{Z}$ und $B = \mathbb{R}$. Dann ist $\sqrt{2}$ ganz über $\mathbb{Z}$, während $\frac{1}{2}$ nicht ganz über $\mathbb{Z}$ ist.*

Das sieht man wie folgt: $\sqrt{2}$ ist Nullstelle des normierten Polynoms $t^2 - 2$ aus $\mathbb{Z}[t]$. Angenommen $\frac{1}{2}$ würde eine Polynomgleichung wie oben erfüllen. Dann erhielte man nach Multiplikation mit 2^n eine Gleichung

$$1 + 2a_1 + \cdots + 2^n a_n = 0,$$

mit ganzzahligen Koeffizienten. Eine Betrachtung modulo 2 zeigt, daß das unmöglich ist.

Definition 2.3. Eine Ringerweiterung $A \subset B$ heißt *ganz*, wenn jedes Element $b \in B$ ganz über A ist.

Satz 2.1.4. *Sei $A \subset B$ eine Ringerweiterung. Die Elemente $b \in B$, die ganz über A sind, bilden einen Unterring von B.*

Beweis. Wir werden zwei Beweise geben. Der erste verwendet Newtons Theorie von symmetrischen Funktionen und benötigt sonst keine weiteren Vorbereitungen. Allerdings müssen wir voraussetzen, daß A ein Integritätsring ist. Der zweite Beweis ist der Standardbeweis von Dedekind, der mit endlich erzeugten A-Moduln argumentiert. Wir werden ihn später ausführen.
Ein Polynom $P(x_1, \ldots, x_r)$ im Polynomring $A[x_1, \ldots, x_r]$ heißt *symmetrisch*, falls

$$P(x_{\sigma(1)}, \ldots, x_{\sigma(r)}) = P(x_1, \ldots, x_r)$$

für alle Permutationen $\sigma \in \mathcal{S}_n$ gilt. Insbesondere sind die Polynome

$$S_1 = \sum_i x_i, \quad S_2 = \sum_{i<j} x_i x_j, \ \ldots \ , S_r = x_1 x_2 \cdots x_r$$

alle symmetrisch. Sie heißen die *elementarsymmetrischen Polynome*. Jedes symmetrische Polynom $P(x_1, \ldots, x_r)$ ist ein Polynom in den elementarsymmetrischen Polynomen, also in $A[S_1, \ldots, S_r]$. Das ist eine wohlbekannte Tatsache, die wir hier voraussetzen wollen.

Behauptung: Sei Ω ein algebraisch abgeschlossener Körper, der A enthält. Sind $\alpha_1, \ldots, \alpha_n$ die Wurzeln in Ω eines normierten Polynoms im Polynomring $A[x]$, dann ist jedes Polynom $g(\alpha_1, \ldots, \alpha_n)$ mit Koeffizienten in A Wurzel eines normierten Polynoms in $A[x]$.

In der Tat,

$$h(x) := \prod_{\sigma \in \mathcal{S}_n} ((x - g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$$

ist ein normiertes Polynom, dessen Koeffizienten symmetrische Polynome in den α_i sind, und deshalb in A liegen. Offensichtlich ist $g(\alpha_1, \ldots, \alpha_n)$ aber eine der Wurzeln von $h(x)$. Nun können wir den ersten Beweis vollenden. Seien dazu α_1 und α_2 zwei Elemente von B, die ganz über A sind. Es gibt also ein normiertes Polynom in $A[x]$, daß α_1 und α_2 beide als Wurzeln hat.Wir können nun obige Behauptung anwenden, indem wir g als $\alpha_1 + \alpha_2$ oder $\alpha_1 \alpha_2$ wählen. Dann folgt, daß diese Elemente auch ganz über A sind. □

Bevor wir Dedekinds Beweis vorbereiten, hier noch einige Bezeichnungen.

Definition 2.4. Sei $A \subset B$ eine Ringerweiterung. Der Ring der über A ganzen Elemente $b \in B$ wird mit $\overline{A}^B$ bezeichnet. Ist $\overline{A}^B = A$, so heißt A *ganz abgeschlossen* in B. Ist ein Integritätsbereich A ganz abgeschlossen in seinem Quotientenkörper K, so heißt A *ganz abgeschlossen*.

Für $\overline{A}^K$ schreiben wir meistens nur $\overline{A}$.

Beispiel 2.1.5. *Der Integritätsring $\mathbb{Z}$ ist ganz abgeschlossen, d.h., $\overline{\mathbb{Z}} = \mathbb{Z}$.*

Der Beweis geht wie folgt. Für $A = \mathbb{Z}$ ist $K = \mathbb{Q}$ der Quotientenkörper. Sei $x \in \mathbb{Q}$ ganz über $\mathbb{Z}$. Dann ist x Nullstelle eines normierten Polynoms

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

mit ganzzahligen Koeffizienten. Nach dem Lemma von Gauß gilt $x \in \mathbb{Z}$.

Satz 2.1.6. *Sei $A \subset B$ eine Ringerweiterung und $b \in B$. Dann sind folgende Aussagen äquivalent.*

(1) Das Element b ist ganz über A.

(2) Der Ring $A[b] = \{\sum_{i=0}^{n} a_i b^i \mid n \in \mathbb{N},\ a_i \in A\}$ ist ein endlich-erzeugter A-Modul.

(3) Der Ring $A[b]$ ist in einem Unterring C von B enthalten, der ein endlich-erzeugter A-Modul ist.

Beweis. (1) $\Rightarrow$ (2): nach Voraussetzung erfüllt b eine Gleichung $b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_n = 0$ mit $a_i \in A$. Es gilt also für alle $j \geq 0$,

$$b^{n+j} = -(a_1 b^{n+j-1} + a_2 b^{n+j-2} + \cdots + a_{n-1} b^{j+1} + a_n b^j).$$

Induktiv folgt daraus $b^k \in A[1, b, b^2, \ldots, b^{n-1}]$ für alle $k \geq 0$. Also ist der Ring $A[b]$ als A-Modul von den endlich vielen Elementen $1, b, b^2, \ldots, b^{n-1}$ erzeugt.

(2) $\Rightarrow$ (3): setze $C = A[b] \subset B$.

(3) $\Rightarrow$ (1): sei C als A-Modul von endlich vielen Elementen $c_1, c_2, \ldots, c_n$ erzeugt. Es gilt $A \subseteq A[b] \subseteq C \subseteq B$. Also sind alle bc_i in C, so daß es $a_{ij} \in A$ gibt mit

$$bc_i = \sum_{j=1}^{n} a_{ij} c_j.$$

Sei $M = (m_{ij}) \in M_n(A[b])$ die Matrix mit $m_{ij} = \delta_{ij} b - a_{ij}$. Es bezeichne M' die adjungierte Matrix von M. Es gilt $M'M = \det(M) I_n$. Mit $u = (c_1, \ldots, c_n)^t$ gilt $M'Mu = 0$ und $\det(M) c_i = 0$ für alle $i = 1, \ldots, n$. Also gilt $\det(M) c = 0$ für alle $c \in C = \sum_{i=1}^{n} A c_i$. Da C als Unterring von B das Einselement enthält, folgt auch $\det(M) = 0$. Das liefert aber das Polynom für b, nach dem wir suchen: $f(x) = \det(\delta_{ij} x - a_{ij})$ ist ein normiertes Polynom mit Koeffizienten in A mit $f(b) = \det(M) = 0$. □

Oft finden wir auch folgende Variante des obigen Satzes: sei L ein Körper, der A enthält und $b \in L$. Dann ist b genau dann ganz über A, wenn es einen von Null verschiedenen endlich-erzeugten A-Untermodul C von L gibt mit $bC \subseteq C$ (zum Beispiel $C = A[b]$).

Korollar 2.1.7. *Sei C zudem ein endlich-erzeugter A-Modul. Dann ist $A \subset C$ eine ganze Ringerweiterung.*

Korollar 2.1.8 (Transitivität)**.** *Seien $A \subset B$ und $B \subset C$ ganze Ringerweiterungen. Dann ist auch $A \subset C$ eine ganze Ringerweiterung.*

Beweis. Sei $c \in C$. Es erfüllt eine Gleichung

$$c^n + b_1 c^{n-1} + \cdots + b_n = 0$$

mit $b_i \in B$. Wegen Satz 2.1.6 ist $A[b_i]$ ein endlich-erzeugter A-Modul für jedes i, weil B ganz über A ist. Analog zum Beweis von (1) $\Rightarrow$ (2) oben folgt induktiv, daß auch $A[b_1, \ldots, b_n]$ ein endlich-erzeugter A-Modul ist. Somit sind alle seine Elemente ganz über A, insbesondere auch $c \in A[b_1, \ldots, b_n]$. □

Wir kommen zu dem versprochenem zweiten Beweis von Satz 2.1.4.

Korollar 2.1.9 (Dedekind)**.** *Sei $A \subset B$ eine Ringerweiterung. Dann ist $\overline{A}^B$ ein Ring.*

Beweis. Es seien $x, y \in \overline{A}^B$. Dann sind die A-Moduln $A[x]$ und $A[y]$ endlich erzeugt nach Satz 2.1.6. Es folgt wiederum, daß der A-Modul $A[x, y]$ endlich-erzeugt ist. Denn wenn $\{e_1, \ldots, e_n\}$ den A-Modul $A[x]$ erzeugen, und $\{f_1, \ldots, f_m\}$ den A-Modul $A[y]$, so erzeugen $\{e_1 f_1, \ldots, e_i f_j, \ldots, e_n f_m\}$ den A-Modul $A[x, y]$. Da die Elemente $x \pm y$ und xy in $A[x, y]$ liegen, sind sie ganz über A, und liegen somit in $\overline{A}^B$. □

Beispiel 2.1.10. *Der $\mathbb{Z}$-Modul $M = \mathbb{Z}[\frac{1}{2}]$ ist nicht endlich erzeugt.*

In der Tat, M ist eine unendliche abelsche Gruppe mit $M/2M = 0$. Also kann sie nicht endlich-erzeugt sein. Somit besagt Satz 2.1.6, daß $\frac{1}{2}$ nicht ganz sein kann über $\mathbb{Z}$. Das hatten wir schon in Beispiel 2.1.3 gesehen. Allgemeiner wissen wir ja schon aus Beispiel 2.1.5, daß $\mathbb{Z}$ ganz abgeschlossen ist. Diese Tatsache läßt sich wie folgt verallgemeinern.

Satz 2.1.11. *Sei A ein faktorieller Ring. Dann ist A ganz abgeschlossen.*

Beweis. Sei K der Quotientenkörper von A. Sei $a/s \in K$ ganz über A, mit $a, s \in A$, $s \neq 0$ und a und s teilerfremd. Wir wollen $a/s \in A$ zeigen. Es gibt ein $n \geq 1$ und $a_0, \ldots, a_{n-1} \in A$ mit

$$(a/s)^n + a_{n-1}(a/s)^{n-1} + \cdots + a_1(a/s) + a_0 = 0.$$

Multipliziert man diese Gleichung mit s^n, so erhält man

$$a^n + s a_{n-1} a^{n-1} + \cdots + s^{n-1} a_1 a + s^n a_0 = 0.$$

Da s jeden Summanden teilt, bis auf den ersten, folgt $s \mid a^n$. Das ist ein Widerspruch zur Teilerfremdheit, da A faktoriell ist. Somit ist s eine Einheit in A und deshalb $a/s \in A$. □

Zum Beispiel sind $\mathbb{Z}$ und $\mathbb{Z}[i]$ Hauptidealringe und deshalb faktoriell, und somit auch ganz abgeschlossen. Dieser Satz ermöglicht auch, interessante Beispiele von Ringen zu finden, die nicht faktoriell sind.

Beispiel 2.1.12. *Der Ring $\mathbb{Z}[\sqrt{5}]$ ist nicht faktoriell.*

Angenommen, $\mathbb{Z}[\sqrt{5}]$ wäre faktoriell und somit ganz abgeschlossen. Das Element $\frac{1+\sqrt{5}}{2}$ ist ganz über $\mathbb{Z}[\sqrt{5}]$, da es Nullstelle des normierten Polynoms $x^2 - x - 1$ ist. Allerdings ist es nicht in $\mathbb{Z}[\sqrt{5}]$ enthalten. Also ist $\mathbb{Z}[\sqrt{5}]$ nicht ganz abgeschlossen.
Diese Schlussfolgerung funktioniert allerdings nicht immer so gut, da die Umkehrung von Satz 2.1.11 im allgemeinen nicht gilt. So ist etwa der Ring $\mathbb{Z}[\sqrt{-5}]$ ganz abgeschlossen, wie wir in 2.2.4 sehen werden. Dennoch ist er nicht faktoriell.

Beispiel 2.1.13. *Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell.*

Um das zu zeigen, müssen wir also mehr tun als im Beispiel $\mathbb{Z}[\sqrt{5}]$. Wir können aber direkt zeigen, daß nicht jedes Element eine eindeutige Faktorisierung besitzt. Zum Beispiel haben wir

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

Man kann relativ leicht zeigen, daß alle Faktoren irreduzibel sind und keine zwei assoziiert. Dazu benutzt man die Normabbildung $N(z) = z\overline{z}$ für $z = a + b\sqrt{-5}$, also $a+b\sqrt{-5} \mapsto a^2+5b^2$. Sie ist multiplikativ, und $\alpha \in \mathbb{Z}[\sqrt{-5}]$ erfüllt genau dann $N(\alpha) = 1$ wenn α eine Einheit ist. Angenommen, wir könnten $1+\sqrt{-5} = \alpha\beta$ schreiben. Dann wäre $N(\alpha)N(\beta) = N(\alpha\beta) = N(1+\sqrt{-5}) = 6$, also $N(\alpha) = 1, 2, 3$ oder 6. Im ersten Fall wäre α eine Einheit, und im letzten Fall wäre β eine Einheit. Die anderen Fälle können gar nicht auftreten, weil $a^2 + 5b^2 = 2, 3$ in $\mathbb{Z}$ nicht lösbar ist. Also ist $1 + \sqrt{-5}$ irreduzibel. Ebenso zeigt man, daß die anderen Faktoren irreduzibel sind. Sind irgendwelche zwei Faktoren assoziiert ? Dann hätten sie die gleiche Norm. Wir müssen also nur prüfen, ob $1 + \sqrt{-5}$ und $1 + \sqrt{-5}$ assoziiert sind. Dann hätten wir

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(1 - \sqrt{-5})$$

mit ganzen Zahlen a, b. Doch das ist unmöglich.

Beispiel 2.1.14. *Der Ring $\mathbb{Z}[\sqrt{-2}]$ ist faktoriell.*

Dieser Ring ist sogar Euklidisch, was man leicht zeigen kann. Wir wollen dieses Beispiel aber mit dem vorherigen vergleichen, denn zunächst scheint es, als könnten wir die eindeutige Faktorisierung wiederum am Beispiel

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

widerlegen. Der Unterschied hier ist aber, daß die Faktoren in $\mathbb{Z}[\sqrt{-2}]$ *nicht* irreduzibel sind. Es gilt nämlich

$$\begin{aligned} 2 &= -(\sqrt{-2})^2, \\ 3 &= (1 + \sqrt{-2})(1 - \sqrt{-2}), \\ 2 + \sqrt{-2} &= (\sqrt{-2})(1 - \sqrt{-2}), \\ 2 - \sqrt{-2} &= -(\sqrt{-2})(1 + \sqrt{-2}). \end{aligned}$$

Damit werden die zwei scheinbar verschiedenen Faktorisierungen von 6 gleich:

$$6 = 2 \cdot 3 = -(\sqrt{-2})^2(1+\sqrt{-2})(1-\sqrt{-2}) = (2+\sqrt{-2})(2-\sqrt{-2}).$$

2.2 Ganzheitsringe

Definition 2.5. Sei K ein Zahlkörper. Der ganze Abschluss von $\mathbb{Z}$ in K heißt der *Ganzheitsring* $\mathcal{O}_K$ von K.

Wegen Satz 2.1.6 sind Ganzheitsringe tatsächlich Ringe.

Satz 2.2.1. *Ganzheitsringe sind ganz abgeschlossen.*

Beweis. Es sei $\mathcal{O}$ der ganze Abschluss von $B = \mathcal{O}_K$ in $C = K$. Die Ringerweiterungen $B \subset C$ und $A = \mathbb{Z} \subset B$ sind also ganz. Wegen der Transitivität, Korollar 2.1.8, ist also auch $\mathcal{O}$ ganz über $\mathbb{Z}$, und somit $\mathcal{O} \subset \mathcal{O}_K$. □

Beispiel 2.2.2. *Der Ganzheitsring von $\mathbb{Q}$ ist $\mathbb{Z}$, d.h., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

Wie sehen die Ganzheitsringe für quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ aus ? Üblicherweise wird hier die kürzere Notation $\mathcal{O}_d$ verwendet, anstatt $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Wir erinnern daran, daß d quadratfrei ist.

Satz 2.2.3. *Der Ganzheitsring eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ ist durch $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\omega_d = \{a + b\omega_d \mid a, b \in \mathbb{Z}\}$ gegeben, mit*

$$\omega_d = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2, 3(4), \\ \frac{1}{2}(1+\sqrt{d}), & \text{falls } d \equiv 1(4). \end{cases}$$

Beweis. Es ist $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $\alpha = a + b\sqrt{d} \in \mathcal{O}_d$ mit $a, b \in \mathbb{Q}$. Dann ist $P(\alpha) = 0$ für ein Polynom

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

mit ganzzahligen Koeffizienten. Betrachte das Polynom

$$\begin{aligned} Q(x) &= (x-\alpha)(x-\sigma(\alpha)) \\ &= x^2 - (\alpha + \sigma(\alpha))x + \alpha\sigma(\alpha) \\ &= x^2 - (a + b\sqrt{d} + a - b\sqrt{d})x + (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= x^2 - 2ax + (a^2 - b^2 d) \end{aligned}$$

Wegen $Q(\alpha) = 0$ gilt $Q(x) \mid P(x)$. Nach dem Lemma von Gauß hat $Q(x)$ also ganze Koeffizienten. Das bedeutet $2a \in \mathbb{Z}$ und $a^2 - b^2 d \in \mathbb{Z}$. Daraus folgt $4a^2 \in \mathbb{Z}$ und deshalb $4b^2 d \in \mathbb{Z}$. Nun folgt $2b \in \mathbb{Z}$, da d quadratfrei war. Insgesamt haben wir dann entweder $a, b \in \mathbb{Z}$, oder $a, b \in \frac{1}{2} + \mathbb{Z}$. Wenn wir $a = \frac{u}{2}$ und $b = \frac{v}{2}$ mit $u, v \in \mathbb{Z}$ schreiben, so bedeutet $a^2 - b^2 d \in \mathbb{Z}$ genau $\frac{u^2 - v^2 d}{4} \in \mathbb{Z}$, also $u^2 - v^2 d \equiv 0(4)$. Für $d \equiv 2, 3(4)$ kommt nur $u^2 \equiv v^2 \equiv 0(4)$ in Frage, also u und v gerade und $a, b \in \mathbb{Z}$. Für $d \equiv 1(4)$ kommt auch noch $u^2 \equiv v^2 \equiv 1(4)$ in Frage, also auch noch $a, b \in \frac{1}{2} + \mathbb{Z}$. □

Beispiel 2.2.4. *Der Ganzheitsring von* $\mathbb{Q}(\sqrt{-5})$ *ist* $\mathbb{Z}[\sqrt{-5}]$. *Somit ist* $\mathbb{Z}[\sqrt{-5}]$ *nach Satz* 2.2.1 *ganz abgeschlossen.*

Der Ganzheitsring von $\mathbb{Q}(\sqrt{-3})$ ist nicht $\mathbb{Z}[\sqrt{-3}]$, sondern $\mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$. Das gilt entsprechend für jedes $d \equiv 1(4)$. In diesem Fall ist $\mathbb{Z}[\sqrt{d}]$ niemals ganz abgeschlossen, weil das Element $\frac{1+\sqrt{d}}{2}$ zwar ganz über $\mathbb{Z}[\sqrt{d}]$ ist, mit normiertem Polynom $x^2 - x + \frac{1-d}{4}$, aber nicht in $\mathbb{Z}[\sqrt{d}]$ enthalten ist.

Bemerkung 2.2.5. Eine interessante Frage für Ganzheitsringe $\mathcal{O}_d$ quadratischer Zahlkörper ist, wie gesagt, welche faktorielle Ringe sind, und welche nicht. Wir haben schon einige Beispiele studiert. Ganzzahlringe sind Dedekindringe, und diese wiederum sind genau dann faktoriell wenn sie Hauptidealringe sind. Für $d < 0$ ist die Antwort auf unsere Frage genau bekannt [11], siehe Baker-Heegner-Stark Theorem. Dann ist $\mathcal{O}_d$ genau dann faktoriell bzw. ein Hauptidealring, wenn

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Für $d > 0$ ist die Antwort im allgemeinen nicht bekannt. Man stellt allerdings fest, daß dann die Ringe $\mathcal{O}_d$ relativ oft faktoriell sind. Die ersten solchen Zahlen sind $d = 1, 2, 3, 5, 6, 7, 11, 13, 14$. Eine Vermutung von Gauß besagt, daß $\mathcal{O}_d$ für unendlich viele positive ganze Zahlen d faktoriell ist.

Bemerkung 2.2.6. Sei K ein Funktionenkörper. Der ganze Abschluss von $\mathbb{F}_p[t]$ in K heißt der Ganzheitsring von K. Der Ganzheitsring von $\mathbb{F}_p(t)$ ist $\mathbb{F}_p[t]$. Die Rolle von $\mathbb{Z}$ im Zahlkörperfall wird also hier von $\mathbb{F}_p[t]$ übernommen. Entscheidend ist, daß beide Ringe Hauptidealringe sind. Damit haben wir den Begriff des Ganzheitsrings für globale Körper.

Satz 2.2.7. *Sei* A *ein Integritätsring mit Quotientenkörper* K, *und* $L \supset K$ *eine Körpererweiterung. Ist* $\alpha \in L$ *algebraisch über* K, *dann existiert ein* $d \in A$, *so daß* $d\alpha$ *ganz über* A *ist.*

Beweis. Nach Voraussetzung erfüllt α eine Gleichung

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

mit $a_i \in K$. Sei d der Hauptnenner der a_i, d.h., mit $da_i \in A$ für alle i. Nach Multiplikation mit d^m erhält man

$$d^m\alpha^m + a_1d^m\alpha^{m-1} + \cdots + d^ma_m = 0,$$

oder auch

$$(d\alpha)^m + a_1d(d\alpha)^{m-1} + \cdots + a_md^m = 0.$$

Die Koeffizienten $1, a_1d, \ldots, a_md^m$ liegen alle in A, weshalb $d\alpha$ ganz über A ist. □

Korollar 2.2.8. *Seien* A, K *und* L *wie im Satz gegeben und* B *der ganze Abschluß von* A *in* L. *Ist die Körpererweiterung* $L \supset K$ *algebraisch, so ist* L *der Quotientenkörper von* B.

Beweis. Sei $\alpha \in L$. Nach dem Satz kann dann $\alpha = \beta/d$ geschrieben werden mit $\beta \in B$ und $d \in A$. □

Korollar 2.2.9. *Der Quotientenkörper eines Ganzzahlringes $\mathcal{O}_K$ ist K.*

Satz 2.2.10. *Sei $A \subset B$ eine ganze Ringerweiterung und B ein Integritätsring. Dann ist A genau dann ein Körper wenn B es ist.*

Beweis. Angenommen B ist ein Körper. Sei $a \in A$ von Null verschieden. Es gilt $a^{-1} \in B$. Da a^{-1} ganz über A ist, gibt es eine Gleichung der Form

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

mit $c_i \in A$. nach Multiplikation mit a^{n-1} erhalten wir

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in A.$$

Also ist A ein Körper.
Sei nun A ein Körper und $b \in B^\times$. Da b ganz über A ist, ist $A[b]$ ein endlich-erzeugter A-Modul nach Satz 2.1.6, also ein endlich-dimensionaler A-Vektorraum. Sei $f \in \mathrm{End}(A)$ gegeben durch die Linksmultiplikation mit b, also durch $f(z) = bz$ für $z \in A[b]$. Nun ist $A[b]$ als Unterring von B ein Integritätsring. Also ist f injektiv: aus $bz = 0$ und $b \neq 0$ folgt $z = 0$. Da $A[b]$ endlich-dimensional ist, ist f auch surjektiv. Also gibt es zu unserem $b \neq 0$ ein $c \in A[b] \subseteq B$ mit $bc = 1$. Also ist B ein Körper. □

2.3 Krulldimension

Definition 2.6. Sei A ein nicht-trivialer Ring. Eine Kette von $n+1$ verschiedenen Primidealen

$$P_0 \subset P_1 \subset \ldots \subset P_n$$

hat die *Länge* n. Die *Krulldimension* $\dim(A)$ von A ist die maximale Länge n einer solchen Kette von Primidealen.

Existiert keine Kette endlicher Länge, so setzen wir $\dim(A) = \infty$. Das kann durchaus vorkommen, sogar bei Noetherschen Ringen. Nach Definition ist ein Primideal P auch eine Kette von Primidealen der Länge 0. Ein Körper K hat nur ein Primideal, nämlich $P = 0$. Also hat K die Krulldimension 0.

Beispiel 2.3.1. *Der Ring $\mathbb{Z}$ hat Krulldimension* 1.

Es gibt keine Kette von Primidealen $P_0 = 0 \subset P_1 \subset P_2$ der Länge 2 in $\mathbb{Z}$, weil P_1 und P_2 maximale Ideale wären, und somit gleich. Andererseits ist $0\mathbb{Z} \subset p\mathbb{Z}$ für jede Primzahl p eine Kette der Länge 1. Also folgt $\dim(\mathbb{Z}) = 1$. Allgemeiner gilt folgender Satz.

Satz 2.3.2. *Sei A ein Hauptidealring. Dann gilt* $\dim(A) = 1$ *genau dann, wenn A kein Körper ist.*

Beweis. Es sei A kein Körper. Für ein Primideal P in A ist die maximale Kettenlänge genau dann gleich 1, wenn $P = (p)$ für ein irreduzibles Element p von A gilt. □

Für die Krulldimension von ganzen Ringerweiterungen gilt folgendes Resultat. Wir haben es in der kommutativen Algebra bewiesen, siehe [1].

Satz 2.3.3. *Sei $A \subset B$ eine ganze Ringerweiterung. Dann gilt*

$$\dim(A) = \dim(B).$$

Dieses Resultat ist sehr stark. Für die Ringerweiterung $\mathbb{Z} \subset \mathbb{Q}$ gilt

$$\dim(\mathbb{Z}) = 1 \neq \dim(\mathbb{Q}) = 0.$$

Also ist diese Ringerweiterung nicht ganz. Das wissen wir allerdings schon, weil $\mathbb{Z}$ ganz abgeschlossen ist. Es folgt auch aus Satz 2.2.10, weil $\mathbb{Z}$ kein Körper ist. Wir notieren noch eine wichtige Folgerung für Ganzzahlringe.

Korollar 2.3.4. *Sei K ein globaler Körper mit Ganzheitsring $\mathcal{O}_K$. Dann gilt* $\dim(\mathcal{O}_K) = 1$.

Beweis. Im Zahlkörperfall gilt $\dim(\mathcal{O}_K) = \dim(\mathbb{Z}) = 1$ nach obigem Satz. Im Funktionenkörperfall gilt $\dim(\mathcal{O}_K) = \dim(\mathbb{F}_p[t]) = 1$, da auch $\mathbb{F}_p[t]$ ein Haupidealring ist. □

Wir erwähnen noch den folgenden Satz. Einen relativ kurzen Beweis findet man in [4].

Satz 2.3.5. *Die Krulldimension eines Polynomrings $K[x_1, \ldots, x_n]$ in n Variablen über einem Körper K ist gleich n.*

Es gilt allgemeiner $\dim(A[x_1, \ldots, x_n]) = \dim(A) + n$ für Noethersche Ringe A. Zum Beispiel ist $\dim(\mathbb{Z}[x]) = 2$.

2.4 Norm und Spur

Um weitere Eigenschaften von Ganzzahlringen $\mathcal{O}_K$ zu studieren, befassen wir uns mit Normen und Spuren von Körpererweiterungen, und mit Diskriminanten. Wir wollen zeigen, daß Ganzzahlringe als $\mathbb{Z}$-Moduln endlich erzeugt sind, und daraus folgern, daß sie Noethersche Ringe sind. Ein Ring A heißt *Noethersch*, wenn jedes Ideal in A endlich erzeugt ist. Für die Grundlagen aus der kommutativen Algebra siehe, zum Beispiel, [1].

Sei also $L \supset K$ eine algebraische Körpererweiterung und $\alpha \in L$. Es bezeichne $m(\alpha)$ das Minimalpolynom von α, also das normierte Polynom kleinsten Grades mit Koeffizienten in K und Nullstelle α. Die Linksmultiplikation mit α definiert eine K-lineare Abbildung

$$\ell_\alpha \colon K(\alpha) \to K(\alpha),\ x \mapsto \alpha x.$$

Lemma 2.4.1. *Sei $L \supset K$ eine algebraische Körpererweiterung und $\alpha \in L$. Dann ist das Minimalpolynom $m(\alpha)$ genau das charakteristische Polynom $p_\alpha(x) = \det(x\,\mathrm{id} - \ell_\alpha)$ der Linksmultiplikation ℓ_α auf $K(\alpha)$.*

Beweis. Es gilt $\deg(p_\alpha) = [K(\alpha) : K] = \deg(m(\alpha))$, und p_α ist normiert. Nach dem Satz von Cayley-Hamilton gilt $p_\alpha(\ell_\alpha) = 0$ als Abbildung $K(\alpha) \to K(\alpha)$. Auswertung in 1 ergibt $p_\alpha(\alpha) = p_\alpha(\ell_\alpha(1)) = 0$. Also erfüllt p_α alle Eigenschaften von $m(\alpha)$. □

Sei nun $\ell_\alpha \colon L \to L$ die Linksmultiplikation mit α auf *ganz* L, und

$$P_\alpha(x) = \det(x \,\mathrm{id} - \ell_\alpha)$$

das charakteristische Polynom von α.

Definition 2.7. Sei $L \supset K$ eine endliche Körpererweiterung und $\alpha \in L$. Die *Norm* von α ist definiert als $N_{L/K}(\alpha) = \det(\ell_\alpha)$. Die *Spur* von α ist definiert durch $\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}(\ell_\alpha)$.

Für das charakteristische Polynom gilt übrigens

$$P_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

mit $n = [L : K]$, $a_{n-1} = -\mathrm{tr}_{L/K}(\alpha)$ und $a_0 = (-1)^n N_{L/K}(\alpha)$. Weiterhin ist

$$\begin{aligned} N_{L/K}(\alpha\beta) &= N_{L/K}(\alpha)N_{L/K}(\beta), \\ \mathrm{tr}_{L/K}(\alpha + \beta) &= \mathrm{tr}_{L/K}(\alpha) + \mathrm{tr}_{L/K}(\beta) \end{aligned}$$

für alle $\alpha, \beta \in L$, so daß $N \colon L^\times \to K^\times$ und $\mathrm{tr} \colon L \to K$ Homomorphismen sind. Ist $\beta \in L$ sogar in K, so gilt $\mathrm{tr}_{L/K}(\beta) = n\beta$ und $N_{L/K}(\beta) = \beta^n$.

Beispiel 2.4.2. *Sei $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$ und $\alpha = a + b\sqrt{d}$ in L. Dann ist $\{1, \sqrt{d}\}$ eine Basis für L/K, bezüglich derer die Linksmultiplikation die Matrix*

$$\ell_\alpha = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

hat. Daher ist $\mathrm{tr}_{L/K}(\alpha) = 2a$ und $N_{L/K}(\alpha) = a^2 - b^2 d$.

Man vergleiche das mit der Rechnung im Beweis von Satz 2.2.3.

Satz 2.4.3. *Sei $L \supset K$ eine endliche und separable Körpererweiterung, $\alpha \in L$ und $r = [L : K(\alpha)]$. Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von P_α in einem algebraischen Abschluß $\overline{K}$ von K, sowie $\sigma_i \colon L \to \overline{K}$ die Einbettungen mit $\sigma_i|_K = \mathrm{id}$ für $i = 1, \ldots, n$. Dann gilt*

$$\begin{aligned} P_\alpha(x) = m(\alpha)(x)^r &= \prod_{i=1}^{n}(x - \alpha_i) \\ &= \prod_{i=1}^{n}(x - \sigma_i(\alpha)), \\ \mathrm{tr}_{L/K}(\alpha) &= \sum_{i=1}^{n}\alpha_i = \sum_{i=1}^{n}\sigma_i(\alpha), \\ N_{L/K}(\alpha) &= \prod_{i=1}^{n}\alpha_i = \prod_{i=1}^{n}\sigma_i(\alpha). \end{aligned}$$

Beweis. Es gilt $p_\alpha(x) = m(\alpha)(x)$ wegen Lemma 2.4.1. Wir haben $\deg(p_\alpha) = d = [K(\alpha) : K]$ und $rd = [L : K(\alpha)][K(\alpha) : K] = [L : K] = n$. Wir behaupten, daß für die charakteristischen Polynome P_α und p_α der Linksmultiplikation auf L bzw. $K(\alpha)$ gilt

$$P_\alpha(x) = p_\alpha(x)^r.$$

Daraus folgt dann natürlich $P_\alpha(x) = m(\alpha)(x)^r$. Dazu sei $\{y_1, \ldots, y_r\}$ eine Basis von $L/K(\alpha)$ und $\{z_1, \ldots, z_d\}$ eine Basis von $K(\alpha)/K$. Dann ist

$$\{y_i z_j \mid i = 1, \ldots, r,\ j = 1, \ldots, d\}$$

eine Basis von L/K. In dieser Basis hat die Matrix zu ℓ_α auf L aber eine Blockdiagonalform mit r Blockmatrizen A, so daß A gerade die Matrix von ℓ_α auf $K(\alpha)$ bezüglich der Basis $z_1, \ldots, z_d$ ist. Nimmt man von dieser blockdiagonalen Matrix das charakteristische Polynom, so folgt die Behauptung.
Sind $\alpha_1, \ldots, \alpha_d$ die verschiedenen Nullstellen von $m(\alpha)$, so gilt $m(\alpha)(x) = \prod_{i=1}^{d}(x - \sigma_i(\alpha))$ und deshalb

$$P_\alpha(x) = m(\alpha)(x)^r = \prod_{i=1}^{d}(x - \sigma_i(\alpha))^r = \prod_{i=1}^{n}(x - \sigma_i(\alpha)).$$

Weiterhin gilt

$$\{\alpha_1, \ldots, \alpha_n\} = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$$

als Mengen mit Vielfachheit, denn jede der d Einbettungen $K(\alpha) \to \overline{K}$ lässt sich auf genau r viele Weisen nach L fortsetzen. □

Beispiel 2.4.4. *Für $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$ ist L/K galoissch mit Galoisgruppe $\{\mathrm{id}, \sigma\}$, $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Für $\alpha = a + b\sqrt{d} \in L$ gilt also*

$$\begin{aligned}
\mathrm{tr}_{L/K}(\alpha) &= \mathrm{id}(\alpha) + \sigma(\alpha) = a + b\sqrt{d} + a - b\sqrt{d} \\
&= 2a, \\
N_{L/K}(\alpha) &= \mathrm{id}(\alpha)\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) \\
&= a^2 + b^2 d, \\
P_\alpha(x) &= (x - \alpha)(x - \sigma(\alpha)) = x^2 - 2ax + (a^2 - b^2 d) \\
&= x^2 - \mathrm{tr}(\alpha)x + N(\alpha).
\end{aligned}$$

Korollar 2.4.5. *Sei $L \supset K$ eine separable Erweiterung von globalen Körpern und $\alpha \in \mathcal{O}_L$. Dann gilt $P_\alpha \in \mathcal{O}_K[x]$. Insbesondere sind die Spur $\mathrm{tr}_{L/K}(\alpha)$ und die Norm $N_{L/K}(\alpha)$ in $\mathcal{O}_K$.*

Beweis. Da α ganz über $\mathcal{O}_K$ ist, erfüllt es eine Gleichung

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

mit Koeffizienten in $\mathcal{O}_K$. Dann erfüllen aber auch alle $\sigma_i(\alpha)$ diese Gleichung, weil die Operation der Galoisgruppe des Zerfällungskörpers, welche die $\sigma_i(\alpha)$ vertauscht ein Homomorphismus ist, und daher die Koeffizienten der obigen Gleichung invariant lässt. Deshalb sind alle $\sigma_i(\alpha)$ ganz über $\mathcal{O}_K$. Wegen $P_\alpha(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$ sind alle Koeffizienten von P_α ganz über $\mathcal{O}_K$ und liegen in K. Da $\mathcal{O}_K$ ganz abgeschlossen ist, liegen die Koeffizienten in $\mathcal{O}_K$. □

Für $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$ und $\alpha = a + b\sqrt{d} \in L$ ist also $P_\alpha(x) = x^2 - 2ax + (a^2 - b^2 d)$ in $\mathbb{Z}[x]$.

Wir kommen nun zum Begriff der Diskriminante für Körpererweiterungen L/K, und noch allgemeiner für Ringerweiterungen B/A, wobei B ein freier A-Modul vom Rang n ist, mit Basis $\{x_1, \ldots, x_n\}$. Das könnte zum Beispiel eine Ringerweiterung $\mathcal{O}_K/\mathbb{Z}$ sein. Auch im allgemeineren Fall B/A definiert die Linksmultiplikation mit einem $\beta \in B$ eine A-lineare Abbildung auf L, und die Spur $\mathrm{tr}_{B/A}(\beta)$ und die Norm $N_{B/A}(\beta)$ sind wohldefiniert.

Definition 2.8. Sei $B \supset A$ eine Ringerweiterung und B ein freier A-Modul mit Basis $\{x_1, \ldots, x_n\}$. Sei $(\mathrm{tr}_{B/A}(x_i x_j))_{i,j}$ die Fundamentalmatrix der symmetrischen Bilinearform $B \times B \to A$, $(x, y) \mapsto \mathrm{tr}_{B/A}(xy)$ bezüglich dieser Basis. Dann heißt

$$D(x_1, \ldots, x_n) = \det((\mathrm{tr}_{B/A}(x_i x_j))_{i,j}) \in A$$

die *Diskriminante* der Basis $\{x_1, \ldots, x_n\}$.

Im Fall von Beispiel 2.4.2 für $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ haben wir also

$$D(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{d}) \\ \mathrm{tr}(\sqrt{d}) & \mathrm{tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d,$$

da ja $\mathrm{tr}(a + b\sqrt{d}) = 2a$ ist.
Die Definition wirft die Frage auf, ob wir sie basisunabhängig machen können. Dazu rechnen wir aus, wie sich $D(x_1, \ldots, x_n)$ und $D(y_1, \ldots, y_n)$ für zwei Basen des freien A-Moduls B zueinander verhalten.

Lemma 2.4.6. *Gilt $y_j = \sum_{i=1}^n a_{ji} x_i$ mit $a_{ij} \in A$ und $M = (a_{ij})_{i,j}$, so folgt*

$$D(y_1, \ldots, y_n) = \det(M)^2 D(x_1, \ldots, x_n).$$

Beweis. Sei $\psi\colon B \times B \to A$ eine symmetrische Bilinearform. Dann gilt

$$\psi(y_k, y_l) = \sum_{i,j} \psi(a_{ki} x_i, a_{lj} x_j) = \sum_{i,j} a_{ki} \psi(x_i, x_j) a_{lj},$$

und somit die Matrixgleichung

$$(\psi(y_k, y_l))_{k,l} = M \cdot (\psi(x_i, x_j)) \cdot M^t$$

Nimmt man die Determinante auf beiden Seiten und beachtet $\det(MM^t) = \det(M)^2$, so folgt die Behauptung mit $\psi(x, y) = \mathrm{tr}_{B/A}(xy)$. □

Sind die x_i und die y_j Basen von B über A, so ist $\det(M)$ eine Einheit in A. Diskriminanten von je zwei Basen unterscheiden sich also nur bis auf das Quadrat einer Einheit in A. Das Ideal in A, das von der Diskriminante einer Basis erzeugt wird, ist also basisunabhängig. Für $A = \mathbb{Z}$ ist nur 1 ein Quadrat einer Einheit. Also sind dort alle Diskriminanten sogar gleich.

Definition 2.9. Die Diskriminante $\mathcal{D}_{B/A}$ einer Ringerweiterung B/A mit einem freien A-Modul B ist das von der Diskriminante einer Basis von B erzeugte Ideal in A.

Oft wird auch das Element $D(x_1, \ldots, x_n)$ in $A/(A^\times)^2$ selbst als Diskriminante von B/A bezeichnet.

Lemma 2.4.7. *Sei L/K eine endliche, separable Körpererweiterung vom Grad n und $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Einbettungen $L \hookrightarrow \overline{K}$, sowie $\{x_1, \ldots, x_n\}$ eine Basis von L/K. Dann gilt*

$$D(x_1, \ldots, x_n) = \det((\sigma_i(x_j))_{i,j})^2 \neq 0.$$

Insbesondere ist $\mathcal{D}_{L/K} \neq 0$.

Beweis. Es gilt $\mathrm{tr}_{L/K}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i)\sigma_k(x_j)$, siehe Satz 2.4.3. Dann folgt

$$\begin{aligned} D(x_1, \ldots, x_n) &= \det((\mathrm{tr}_{L/K}(x_i x_j))_{i,j}) \\ &= \det\left(\left(\sum_{k=1}^n \sigma_k(x_i)\sigma_k(x_j)\right)_{i,j}\right) \\ &= \det((\sigma_k(x_i))_{k,i}) \cdot \det((\sigma_k(x_j))_{k,j}) \\ &= \det((\sigma_k(x_j))_{k,j})^2. \end{aligned}$$

Angenommen, diese Determinante verschwindet. Dann gibt es $c_1, \ldots, c_n \in \overline{K}$ mit

$$\sum_{i=1}^n c_i \sigma_i(x_j) = 0$$

für alle j. Da die x_j eine Basis sind, folgt $\sum_{i=1}^n c_i \sigma_i = 0$ als Abbildungen von $L^\times \to \overline{K}$. Als Gruppenhomomorphismen $L^\times \to (\overline{K})^\times$ sind die σ_i jedoch linear unabhängig nach Dedekind's Satz über die Unabhängigkeit von Charakteren. Das ist ein Widerspruch. □

Korollar 2.4.8. *Sei K der Quotientenkörper von A und L eine endliche, separable Körpererweiterung von K vom Grad n, so daß B, der ganze Abschluss von A in L, ein freier A-Modul vom Rang n ist. Dann gilt $\mathcal{D}_{B/A} \neq 0$.*

Beweis. Jede Basis von B/A ist auch eine Basis von L/K wegen Satz 2.2.7. Also wird $\mathcal{D}_{B/A}$ durch $\mathcal{D}_{L/K}$ repräsentiert, und ist deshalb nach Lemma 2.4.7 nicht Null. □

Bemerkung 2.4.9. Die Voraussetzung in Satz 2.4.7 über die Separabilität ist wesentlich. Die Spurpaarung $L \times L \to K$, $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ ist genau dann nicht-ausgeartet, wenn L/K separabel ist. Tatsächlich ist $\mathcal{D}_{L/K} = 0$, wenn L/K nicht separabel ist.

Wir können nun zeigen, daß Ganzzahlringe $\mathcal{O}_K$ endlich-erzeugte $\mathbb{Z}$-Moduln sind.

Satz 2.4.10. *Sei A ein ganz abgeschlossener Integritätsring mit Quotientenkörper K und L/K eine separable Körpererweiterung vom Grad n. Sei B der ganze Abschluß von A in L. Ist A Noethersch, so ist B ein endlich-erzeugter A-Modul und ebenfalls Noethersch. Ist A ein Hauptidealring, so ist B ein freier A-Modul vom Rang n.*

Beweis. Wir zeigen, daß es endlich-erzeugte, freie A-Moduln N und M vom Rang n gibt mit $N \subset B \subset M$. Daraus folgen dann die Behauptungen: ist A Noethersch, dann ist jeder endlich-erzeugte A-Modul ebenfalls Noethersch, siehe Satz 3.4.9 in [1]. Das bedeutet, jeder A-Untermodul von M ist endlich-erzeugt. Insbesondere ist auch $B \subset M$ endlich erzeugt. Sei nun $I \subset B$ ein Ideal von B. Dann ist I ein A-Modul, also endlich-erzeugt, wie gerade bemerkt. Dann ist I aber erst recht als B-Modul endlich erzeugt, d.h., als Ideal. Somit ist jedes Ideal von B endlich-erzeugt, und B also ein Noetherscher Ring.
Ist A ein Hauptidealring, dann ist B frei vom Rang $r \leq n$, da B in einem freien A-Modul M vom Rang n enthalten ist. Das folgt sofort aus dem Elementarteilersatz für Moduln über Hauptidealringen. Denn jeder A-Untermodul B eines freien A-Moduls ist selbst wieder frei, und hat höchstens den gleichen Rang. Ebenso gilt $r \geq n$, da B einen freien A-Modul N vom Rang n enthält.
Es bleibt, unsere obige Behauptung zu zeigen. Sei $\{x_1, \ldots, x_n\}$ eine Basis von L/K. Wegen Satz 2.2.7 existiert ein $d \in A$ mit $dx_i \in B$ für alle i. Nun ist $\{dx_1, \ldots, dx_n\}$ immer noch eine Basis von L/K. Wir können also von vornherein annehmen, daß alle x_i in B liegen. Da die Spurpaarung nicht-ausgeartet ist, gibt es eine duale Basis $\{x'_1, \ldots, x'_n\}$ von L/K mit $\mathrm{tr}_{L/K}(x_i x'_j) = \delta_{ij}$. Es seien

$$N := Ax_1 + \cdots + Ax_n, \quad M := Ax'_1 + \cdots + Ax'_n.$$

Natürlich gilt $N \subset B$. Wir zeigen noch $B \subset M$. Sei dazu $x \in B$. Es gibt eine eindeutige Darstellung $x = \sum_{j=1}^n b_j x'_j$ mit $b_j \in K$. Da x und alle x_i in B sind, gilt $xx_i \in B$, und damit $b_i = \mathrm{tr}_{L/K}(xx_i) \in A$, also $x \in M$. Es gilt nämlich

$$\begin{aligned} \mathrm{tr}_{L/K}(xx_i) &= \mathrm{tr}\left(\sum_{j=1}^n b_j x'_j x_i\right) \\ &= \sum_{j=1}^n b_j \cdot \mathrm{tr}_{L/K}(x'_j x_i) = \sum_{j=1}^n b_j \delta_{ij} \\ &= b_i. \end{aligned}$$

□

Korollar 2.4.11. *Ganzzahlringe von Zahlkörpern sind ganz abgeschlossene Noethersche Ringe der Krulldimension* 1.

Beweis. Sei L ein Zahlkörper. Wähle $A = \mathbb{Z}$ und $B = \mathcal{O}_L$ im Satz. Dann ist $K = \mathbb{Q}$ und $\mathcal{O}_K = \mathbb{Z}$, und $\mathcal{O}_L$ ein endlich-erzeugter $\mathcal{O}_K$-Modul und ein Noetherscher Ring. Das folgt aus dem Satz, weil $\mathbb{Z}$ Noethersch ist. Ganzzahlringe sind ganz abgeschlossen, siehe Satz 2.2.1. Wegen Korollar 2.4.3 haben sie die Krulldimension 1. □

Korollar 2.4.12. *Ganzzahlringe von Zahlkörpern sind freie $\mathbb{Z}$-Moduln von endlichem Rang, dem Grad des Zahlkörpers.*

Beweis. Sei L ein Zahlkörper vom Grad n über $\mathbb{Q}$. Dann ist der Ganzzahlring $\mathcal{O}_L$ ein freier $\mathbb{Z}$-Modul vom Rang n. Das folgt aus dem Satz, weil $\mathbb{Z}$ ein Hauptidealring ist. □

Bemerkung 2.4.13. Für Zahlkörpererweiterungen L/K ist also $\mathcal{O}_L$ ein endlich-erzeugter $\mathcal{O}_K$-Modul. Allerdings muß $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul sein, wenn $\mathcal{O}_K$ kein Haupidealring ist. Zum Beispiel ist für $K = \mathbb{Q}(\sqrt{-14})$ der Ganzzahlring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ kein Haupidealring, und für die Zahlkörpererweiterung L/K mit $L = \mathbb{Q}(\sqrt{-14}, \sqrt{-7})$ kann man zeigen, daß $\mathcal{O}_L$ nicht frei ist als $\mathcal{O}_K$-Modul.

Bemerkung 2.4.14. Man kann die Ergebnisse für $\mathcal{O}_K$ auch für globale Körper zeigen. Allerdings muß man dann den inseparablen Fall, der bei Funktionenkörpern ja auftreten kann, noch separat behandeln. Auch für eine endliche Erweiterung L/K von globalen Körpern gilt, daß $\mathcal{O}_L$ ein endlich-erzeugter $\mathcal{O}_K$-Modul ist.

Definition 2.10. Sei K ein Zahlkörper vom Grad n. Eine Basis $\omega_1, \ldots, \omega_n$ des freien $\mathbb{Z}$-Moduls $\mathcal{O}_K$ heißt *Ganzheitsbasis* von $\mathcal{O}_K$ über $\mathbb{Z}$, oder auch von K. Die *Diskriminante von K* $d = d_K$ ist definiert als $D(\omega_1, \ldots, \omega_n)$.

Diese Diskriminante von K ist die Diskriminante einer Ganzheitsbasis von $\mathcal{O}_K/\mathbb{Z}$ im Sinne der Definition 2.8.

Beispiel 2.4.15. *Für quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit $d \equiv 2, 3 \mod 4$ ist $\{1, \sqrt{d}\}$ eine Ganzheitsbasis, d.h., $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Es gilt $D(1, \sqrt{d}) = 4d$, wie wir im Beispiel nach Definition 2.8 ausgerechnet haben. Für $d \equiv 1 \mod 4$ ist $\{1, \frac{1+\sqrt{d}}{2}\}$ eine Ganzheitsbasis, d.h., $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\,\frac{1+\sqrt{d}}{2}$. Dann ist*

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\frac{1+\sqrt{d}}{2}) \\ \mathrm{tr}(\frac{1+\sqrt{d}}{2}) & \mathrm{tr}(\frac{1+2\sqrt{d}+d}{4}) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Also ist $\mathcal{D}_{\mathcal{O}_d/\mathbb{Z}} = 4d$ für $d \equiv 2, 3 \mod 4$, und $\mathcal{D}_{\mathcal{O}_d/\mathbb{Z}} = d$ für $d \equiv 1 \mod 4$. Insbesondere ist der Ganzzahlring eines quadratischen Zahlkörpers eindeutig durch seine Diskriminante bestimmt. Das ist im allgemeinen nicht richtig. Man findet schon Gegenbeispiele für kubische Zahlkörper.

Beispiel 2.4.16. *Die kubischen Zahlkörper $K = \mathbb{Q}(\sqrt[3]{6})$ und $K = \mathbb{Q}(\sqrt[3]{12})$ haben beide die Diskriminante $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = -2^2 3^5 = -972$, sind aber verschieden.*

Sei $\alpha = \sqrt[3]{6}$. Das Minimalpolynom $m(\alpha)(x) = x^3 - 6$ hat Grad drei, und $\{1, \alpha, \alpha^2\}$ ist eine Basis für $K = \mathbb{Q}(\sqrt[3]{6})$ über $\mathbb{Q}$. Natürlich ist α ganz über $\mathbb{Z}$, so daß $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ gilt. Tatsächlich kann man Gleichheit zeigen, und $\{1, \alpha, \alpha^2\}$ ist eine Ganzheitsbasis von K mit Diskriminante

$$D(1,\alpha,\alpha^2) = \det\begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\alpha) & \mathrm{tr}(\alpha^2) \\ \mathrm{tr}(\alpha) & \mathrm{tr}(\alpha^2) & \mathrm{tr}(\alpha^3) \\ \mathrm{tr}(\alpha^2) & \mathrm{tr}(\alpha^3) & \mathrm{tr}(\alpha^4) \end{pmatrix}$$
$$= \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 18 \\ 0 & 18 & 0 \end{pmatrix} = -3 \cdot 18^2 = -972.$$

Dabei haben wir $\mathrm{tr}(\alpha) = \mathrm{tr}(\alpha^2) = 0$ und $\mathrm{tr}(a) = 3a$ für $a \in \mathbb{Q}$ benutzt. Für $K = \mathbb{Q}(\sqrt[3]{12})$ kann man zeigen, daß $\{1, \sqrt[3]{12}, \frac{1}{2}(\sqrt[3]{12})^2\}$ eine Ganzheitsbasis von K ist, siehe Theorem 6.4.13 in Cohens Buch [3]. Wiederum zeigt man leicht, daß $D(1, \sqrt[3]{12}, \frac{1}{2}(\sqrt[3]{12})^2) = -972$ ist.
Die Berechnung solcher Ganzheitsbasen für kubische Zahlkörper der Form $\mathbb{Q}(\sqrt[3]{d})$ geht auf Dedekind zurück.

Bemerkung 2.4.17. Der Satz vom primitiven Element besagt, daß jeder Zahlkörper K vom Grad n von der Form $K = \mathbb{Q}(\alpha)$ ist für ein $\alpha \in \mathcal{O}_K$. Damit ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis für $K/\mathbb{Q}$. Nun wäre es sehr schön, wenn diese Basis auch eine Ganzheitsbasis für $\mathcal{O}_K$ über $\mathbb{Z}$ wäre, also

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z}1 \oplus \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$$

gälte. Das ist allerdings nicht immer der Fall, wie wir schon gesehen haben: für $\mathbb{Q}(\sqrt{5})$ ist $\{1, \sqrt{5}\}$ zum Beispiel keine Ganzheitsbasis. Das Element $\frac{1+\sqrt{5}}{2}$ ist ganz über $\mathbb{Z}$, aber nicht in $\mathbb{Z} \oplus \mathbb{Z}\sqrt{5}$ enthalten. Aber es gibt ein anderes Element $\beta \in K$ mit $\mathcal{O}_K = \mathbb{Z}[\beta]$, nämlich $\beta = \frac{1+\sqrt{5}}{2}$. Ein Zahlkörper K heißt *monogenisch*, falls sein Ganzzahlring eine Potenzganzheitsbasis zulässt, d.h., falls $\mathcal{O}_K = \mathbb{Z}[\alpha]$ für ein $\alpha \in \mathcal{O}_K$ gilt. Quadratische Zahlkörper und Kreisteilungszahlkörper $\mathbb{Q}(\zeta)$ sind monogenisch, weshalb man vielleicht denken könnte, das sei immer der Fall. Aber schon die kubischen Zahlkörper zeigen, daß dem nicht so ist. Ist $p \equiv 1 \mod 9$ etwa eine Primzahl, die man durch $7x^2 + 3xy + 9y^2$ mit ganzzahligen x, y darstellen kann, so ist $\mathbb{Q}(\sqrt[3]{p})$ nicht monogenisch. Für $x = y = 1$ erhält man das Beispiel $\mathbb{Q}(\sqrt[3]{19})$. Dagegen sind die Zahlkörper aus Beispiel 2.4.16 beide monogenisch. Das Kriterium ist wie folgt: sei $K = \mathbb{Q}(\sqrt[3]{d})$ und $d = ab^2$ kubikfrei mit teilerfremden, quadratfreien ganzen Zahlen a und b. Dann werden zwei Fälle unterschieden. Ist $a^2 \not\equiv b^2 \mod 9$, so ist K monogenisch genau dann, wenn $ax^3 + by^3 = 1$ ganzzahlige Lösungen hat. Ist $a^2 \equiv b^2 \mod 9$, so ist K monogenisch genau dann, wenn $ax^3 + by^3 = 9$ ganzzahlige Lösungen hat.

Lemma 2.4.18. *Sei L/K eine Erweiterung von Zahlkörpern vom Grad n und $L = K(\alpha)$ mit $\alpha \in L$. Dann gilt für die Diskriminante der Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$*

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

wobei $\alpha_1, \ldots, \alpha_n$ die Konjugierten von α in $\overline{K}$ sind.

Beweis. Sind $\sigma_i \colon K(\alpha) \to \overline{K}$ die K-Einbettungen, so sind die Konjugierten von α genau die $\sigma_i(\alpha)$. Also gilt nach Lemma 2.4.7

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \det((\sigma_i(\alpha^{j-1}))_{i,j})^2 \\ &= \det((\alpha_i^{j-1})_{i,j})^2 \\ &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \end{aligned}$$

nach der Determinantenformel von Vandermonde. □

Satz 2.4.19. *Sei $K(\alpha)/K$ eine Erweiterung von Zahlkörpern vom Grad n. Dann ist $D(1, \alpha, \ldots, \alpha^{n-1})$ die Diskriminante des Minimalpolynoms $p = m(\alpha)$ von α über K. Bezeichnet p' die formale Ableitung, so gilt*

$$D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{K(\alpha)/K}(p'(\alpha)).$$

Beweis.

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \prod_i \Big(\prod_{j \ne i} (\alpha_i - \alpha_j) \Big) \\ &= (-1)^{n(n-1)/2} \prod_j p'(\alpha_j) \\ &= (-1)^{n(n-1)/2} N_{K(\alpha)/K}(p'(\alpha)). \end{aligned}$$

□

Satz 2.4.20. *Sei A ein ganz abgeschlossener Integritätsring mit Quotientenkörper K, L/K eine endliche separable Erweiterung, und B der ganze Abschluß von A in L. Sei $\{x_1, \ldots, x_n\}$ ein Basis von L/K, die in B liegt. Für die Diskriminante $d = D(x_1, \ldots, x_n)$ gilt dann*

$$dB \subseteq Ax_1 + \cdots + Ax_n.$$

Beweis. Sei $\alpha = \sum_{i=1}^n a_i x_i \in B$ mit $a_i \in K$. Dann gilt

$$\mathrm{tr}_{L/K}(x_i \alpha) = \sum_{j=1}^n \mathrm{tr}_{L/K}(x_i x_j) \cdot a_j$$

für $i = 1, \ldots, n$. Das ist ein lineares Gleichungssystem für $a_1, \ldots, a_n$, mit Matrix $M = (\mathrm{tr}_{L/K}(x_i x_j))_{i,j}$. Die Koeffizienten liegen in A. Es gilt $d = \det(M)$ nach Definition. Aus der Cramerschen Regel folgt $a_j = a_j'/d$ für $a_j' \in A$, also $d\alpha \in Ax_1 + \ldots Ax_n$. □

3 Ideale von Dedekindringen

3.1 Gebrochene Ideale

Es gibt mehrere Möglichkeiten, wie man Dedekindringe definieren kann, siehe [1]. Wir beginnen hier mit folgender Definition.

Definition 3.1. Ein *Dedekindring* ist ein Noetherscher, ganz abgeschlossener Ring der Krulldimension 1.

Man beachte, daß ein ganz abgeschlossener Ring ein Integritätsring ist. Die Eigenschaft Krulldimension 1 bedeutet, daß der Ring kein Körper ist, und daß alle von Null verschiedenen Primideale maximal sind. Wir erhalten also folgende Umformulierung.

Satz 3.1.1. *Ein Dedekindring ist ein Integritätsring, der kein Körper ist, und folgende Eigenschaften hat: er ist Noethersch, ganz abgeschlossen, und jedes von Null verschiedene Primideal ist maximal.*

Beispiel 3.1.2. *Jeder Hauptidealring, der kein Körper ist, ist ein Dedekindring.*

Das sieht man wie folgt. Sei A ein Hauptidealring, der kein Körper ist. Wegen Satz 2.1.11 ist A ganz abgeschlossen. Es gilt $\dim(A) = 1$, siehe Satz 2.3.2. Ferner ist natürlich jeder Hauptidealring Noethersch. Insbesondere ist $\mathbb{Z}$ ein Dedekindring. Nicht jeder Dedekindring ist ein Hauptidealring.

Beispiel 3.1.3. *Keiner der Ringe $\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[x]$, $\mathbb{C}[x, y]$ ist ein Dedekindring.*

Alle vier angegebenen Ringe sind zwar Noethersch, aber $\mathbb{Z} \oplus \mathbb{Z}$ ist kein Integritätsring, $\mathbb{Z}[\sqrt{5}]$ ist nicht ganz abgeschlossen, und $\mathbb{Z}[x]$ und $\mathbb{C}[x, y]$ haben Krulldimension 2. Andererseits ist $\mathbb{Z}[\sqrt{-5}]$ ein Dedekindring, denn er ist der Ganzheitsring des Zahlkörpers $\mathbb{Q}(\sqrt{-5})$, siehe Beispiel 2.2.4. Es gilt nämlich folgender Satz.

Satz 3.1.4. *Jeder Ganzzahlring $\mathcal{O}_K$ eines Zahlkörpers K ist ein Dedekindring.*

Beweis. Das folgt sofort aus Korollar 2.4.11. □

Definition 3.2. Sei A ein Integritätsring mit Quotientenkörper K. Ein *gebrochenes Ideal* von A ist ein A-Untermodul $I \subset K$ mit gemeinsamem Hauptnenner, d.h., so daß ein $d \neq 0$ in A existiert mit $dI \subseteq A$.

Jedes gewöhnliche Ideal I von A ist auch ein gebrochenes Ideal, mit $d = 1$. Manchmal nennen wir sie auch *ganze* Ideale zur Unterscheidung.

Lemma 3.1.5. *Jeder endlich-erzeugte A-Untermodul $I \subset K$ ist ein gebrochenes Ideal. Ist A Noethersch, so ist umgekehrt jedes gebrochene Ideal ein endlich-erzeugter A-Untermodul von K.*

Beweis. Ist I von $x_1, \ldots, x_n$ erzeugt, und d der Hauptnenner der x_i, so gilt $dI \subseteq A$. Ist umgekehrt $dI \subseteq A$, so ist dI ein endlich-erzeugtes Ideal, weil A Noethersch ist. Daher ist auch I endlich-erzeugt. □

Seien I und J zwei gebrochene Ideale von A. Bezeichne IJ das von allen Produkten ab mit $a \in I$, $b \in J$ erzeugte Ideal, und

$$I^{-1} := \{\alpha \in K \mid \alpha I \subseteq A\}.$$

Beachte hier, daß $0 \in I^{-1}$ gilt. Dann sind IJ und I^{-1} wieder gebrochene Ideale. Es gilt $II^{-1} \subseteq A$, aber Gleichheit muß nicht gelten.

Definition 3.3. Ein gebrochenes Ideal von A heißt *invertierbar*, wenn $II^{-1} = A$ gilt.

Man beachte, daß die Schreibweise I^{-1} nicht bedeutet, daß I notwendig invertierbar ist. Einige Autoren schreiben deshalb I' anstelle von I^{-1}.

Beispiel 3.1.6. *Sei $A = \mathbb{Z}$. Dann ist $I = \frac{1}{2}\mathbb{Z}$ ein gebrochenes Ideal mit $I^{-1} = 2\mathbb{Z}$. Daher ist $II^{-1} = A$ und I ist invertierbar.*

Ist A ein Hauptidealring, so sind alle gebrochenen Ideale von der Form $I = Ab$, mit $b \in K$, und $I^{-1} = Ab^{-1}$. Die Multiplikation von gebrochenen Idealen nimmt dann eine spezielle Form an: $Ab \cdot Ac = A(bc)$.

3.2 Eindeutige Faktorisierung von Idealen

Wir wollen in diesem Abschnitt zeigen, daß jedes echte Ideal in einem Dedekindring eine eindeutige Faktorisierung in endlich viele Primideale hat. Wir benötigen einige Lemmata.

Lemma 3.2.1. *Sei A ein Noetherscher Ring, und I ein von Null verschiedenes ganzes Ideal. Dann gibt es von Null verschiedene Primideale $P_1, \ldots, P_n$ mit $P_1 \cdots P_n \subseteq I$.*

Beweis. Sei Φ die Menge der Ideale I ungleich Null von A, für die die Aussage nicht gilt. Angenommen, $\Phi \neq \emptyset$. Da A Noethersch ist, besitzt Φ ein maximales Element M. Nach Voraussetzung ist M nicht prim, also gibt es $x, y \in A \setminus M$ mit $xy \in M$. Also ist $M \subsetneq M + (x)$ und $M \subsetneq M + (y)$. Also sind die Ideale $M + (x)$ und $M + (y)$ nicht in Φ, da M maximal war. Daher enthalten sie ein Produkt von Primidealen ungleich Null:

$$P_1 \cdots P_n \subseteq M + (x),$$
$$Q_1 \cdots Q_m \subseteq M + (y).$$

Damit folgt aber $P_1 \cdots P_n \cdot Q_1 \cdots Q_m \subseteq (M + (x))(M + (y)) = M$ wegen $xy \in M$. Wir erhalten $M \notin \Phi$, was ein Widerspruch ist. □

Lemma 3.2.2. *Sei A ein Noetherscher Integritätsbereich der Dimension 1 und M ein maximales Ideal in A. Dann ist $A \subsetneq M^{-1}$ eine echte Inklusion.*

Beweis. Wegen $1 \in M^{-1}$ ist $A \subseteq M^{-1}$. Sei $a \neq 0$ in M. Da jedes von Null verschiedene Primideal maximal ist, gibt es nach Lemma 3.2.1 maximale Ideale $P_1, \ldots, P_n$ mit $P_1 \cdots P_n \subseteq Aa = (a)$. Wir wählen solche Ideale mit minimalem $n \geq 1$. Aus $P_1 \cdots P_n \subseteq M$ folgt $P_i = M$ für ein i, sagen wir $P_1 = M$. Da n minimal war, folgt $P_2 \cdots P_n \subsetneq (a)$. Also gibt es ein $b \in P_2 \cdots P_n$ mit $b \notin (a)$. Es ist $Mb = P_1 b \subseteq (a)$, also $Mba^{-1} \subseteq A$. Mit anderen Worten, $ba^{-1} \in M^{-1}$. Wegen $b \notin (a)$ gilt aber $ba^{-1} \notin A$. Somit ist ba^{-1} zwar in M^{-1}, aber nicht in A, und die Inklusion ist echt. □

Lemma 3.2.3. *Sei A ein Dedekindring, I ein Ideal in A, P ein Primideal in A, und beide von Null verschieden. Dann ist $I \subsetneq IP^{-1}$ eine echte Inklusion.*

Beweis. Wegen $1 \in P^{-1}$ ist $I \subseteq IP^{-1}$. Angenommen, es gilt $I = IP^{-1}$. Sei $\alpha \in P^{-1}$. Dann gilt $I\alpha \subseteq I$. Nun ist aber α genau dann ganz über A, wenn es einen endlicherzeugten A-Untermodul $N \neq 0$ gibt mit $N\alpha \subseteq N$, z.B. $N = A[\alpha]$, siehe Beweis zu Satz 2.1.6, Aussage (3). Mit I haben wir aber einen solchen A-Untermodul. Daher ist α ganz über A, und deshalb $\alpha \in A$, da A ganz abgeschlossen ist. Daraus folgt $P^{-1} \subseteq A$. Wegen Lemma 3.2.2 gilt aber $A \subsetneq P^{-1}$. Das ist ein Widerspruch. □

Nun können wir folgendes Resultat zeigen.

Satz 3.2.4. *Sei A ein Dedekindring. Dann ist jedes maximale Ideal invertierbar bezüglich der Multiplikation von gebrochenen Idealen.*

Beweis. Sei M ein maximales Ideal von A. Dann gilt $M \subsetneq MM^{-1} \subseteq A$ nach Lemma 3.2.3. Die Maximalität von M impliziert $MM^{-1} = A$. □

Korollar 3.2.5 (Zerlegung in Primideale)**.** *Sei A ein Dedekindring. Dann ist jedes von Null verschiedene Ideal ein endliches Produkt maximaler Ideale, und ist invertierbar.*

Beweis. Sei Φ die Menge der echten Ideale von A, die kein (endliches) Produkt von maximalen Idealen sind. Angenommen, $\Phi \neq \emptyset$. Dann besitzt Φ wieder ein maximales Element I, und es gibt ein maximales Ideal M von A mit $I \subseteq M$. Nach Definition gilt $M \notin \Phi$. Nach Lemma 3.2.3 gilt $I \subsetneq IM^{-1}$. Außerdem ist $IM^{-1} \neq A$, sonst wäre $I = M$ im Widerspruch zu $I \in \Phi$ und $M \notin \Phi$. Da I maximales Element in Φ war, folgt also $IM^{-1} \notin \Phi$, und wir können $IM^{-1} = P_1 \cdots P_n$ mit maximalen Idealen $P_1, \ldots, P_n$ schreiben. Daraus folgt aber $I = IM^{-1}M = P_1 \cdots P_n M$, ein Widerspruch zu $I \in \Phi$. Also ist doch $\Phi = \emptyset$ und wir können jedes Ideal $I \neq 0$ als $I = P_1 \cdots P_n$ schreiben mit maximalen Idealen $P_1, \ldots, P_n$. Mit Satz 3.2.4 folgt

$$IP_1^{-1} \cdots P_n^{-1} = P_1 \cdots P_n \cdot P_1^{-1} \cdots P_n^{-1} = A,$$

und I ist daher invertierbar. □

Satz 3.2.6. *Sei A ein Dedekindring. Dann besitzt jedes echte Ideal I eine bis auf Reihenfolge eindeutige Zerlegung $I = P_1 \ldots P_n$ in Primideale.*

Beweis. Die Existenz der Zerlegung folgt aus Korollar 3.2.5. Angenommen, wir hätten zwei Primidealzerlegungen für ein echtes Ideal I,

$$I = P_1 \cdots P_n = Q_1 \cdots Q_m.$$

Algemein gilt für Primideale P, daß $IJ \subseteq P$ entweder $I \subseteq P$ oder $J \subseteq P$ impliziert. Wegen $I \subseteq P_1 \cdots P_n \subseteq P_1$ enthält P_1 also irgendein Q_j, sagen wir $Q_1 \subseteq P_1$. Da $Q_1 \neq 0$ auch ein maximales Ideal ist, folgt $Q_1 = P_1$. Nun können wir die zwei Primidealzerlegungen für I mit $P^{-1} = Q^{-1}$ multiplizieren, und erhalten wegen $P^{-1}P = Q^{-1}Q = A$ dann $I = P_2 \cdots P_n = Q_2 \cdots Q_m$. Nun fahren wir induktiv fort und erhalten $n = m$ und $P_i = Q_i \; \forall \; i$. □

Es bezeichne $\mathrm{Spm}(A)$ die Menge aller maximalen Ideale eines kommutativen Ringes A. Es wird auch das *Maximalspektrum* von A genannt. Dagegen bezeichnet $\mathrm{Spec}(A)$ die Menge aller Primideale von A, das sogenannte *Spektrum* von A. Für Dedekindringe ist $\mathrm{Spec}(A) = \mathrm{Spm}(A) \cup \{(0)\}$.
Satz 3.2.6 lässt sich nun leicht auf gebrochene Ideale von A übertragen.

Satz 3.2.7. *Sei A ein Dedekindring. Dann besitzt jedes gebrochene Ideal I in A eine eindeutige Produktdarstellung*

$$I = \prod_{P \in \mathrm{Spm}(A)} P^{\nu_P(I)}$$

mit ganzzahligen $\nu_P(I)$, fast alle Null. Es gilt $\nu_P(I) \geq 0$ für alle P genau dann, wenn I ein ganzes Ideal ist.

Beweis. Jedes gebrochene Ideal I ist Quotient $I = J(J')^{-1}$ von zwei ganzen Idealen J, J' von A. Daher impliziert die Zerlegung für ganze Ideale auch die Zerlegung für gebrochene Ideale. Die Eindeutigkeit folgt ebenso. □

Satz 3.2.8. *Sei A ein Dedekindring. Die Menge der gebrochenen Ideale* $\mathrm{Id}(A)$ *von A bildet eine abelsche Gruppe bezüglich Idealmultiplikation.*

Beweis. Offensichtlich gilt $IJ = JI$ für gebrochene Ideale I und J von A, und $(1) = A$ ist das neutrale Element. Die Assoziativität ist auch klar. Es bleibt zu zeigen, daß jedes gebrochene Ideal I ein Inverses hat. Wähle ein $d \in K$ mit $dI \subseteq A$. Dann gilt $(dI)^{-1} = d^{-1}I^{-1}$, und das ganze Ideal dI ist invertierbar. Es folgt $A = dI \cdot d^{-1}I^{-1} = II^{-1}$. Also ist auch I invertierbar mit Inversem I^{-1}. □

Bemerkung 3.2.9. Emmy Noether hat umgekehrt gezeigt, daß ein Integritätsbereich mit der Eigenschaft, daß seine gebrochenen Ideale bezüglich Idealmultiplikation eine abelsche Gruppe bilden, ein Dedekindring ist.

Es bezeiche $P(A)$ die Menge der gebrochenen Hauptideale von A, also die Mengen $(a) = Aa \subseteq K$ für ein $a \in K^\times$. Dann bildet $P(A)$ eine Untergruppe von $\mathrm{Id}(A)$.

Definition 3.4. Der Quotient $Cl(A) := \mathrm{Id}(A)/P(A)$ heißt die *Idealklassengruppe* von A. Ihre Ordnung heißt *Klassenzahl* von A.

Bemerkung 3.2.10. Es gibt Dedekindringe mit unendlicher Klassenzahl, wie etwa

$$\mathbb{C}[x,y]/(y^2 - x^3 - x - 1).$$

Die Idealklassengruppe ist hier in natürlicher Weise isomorph zu $\mathbb{C}/\Lambda$, wobei Λ ein Gitter in $\mathbb{C}$ ist. Es kann sogar jede abelsche Gruppe als Idealklassengruppe eines Dedekindringes realisiert werden [2]. Für Ganzzahlringe $A = \mathcal{O}_K$ von Zahlkörpern allerdings ist die Klassenzahl immer *endlich*. Das ist ein wichtiges Resultat unserer Vorlesung, das wir in Kapitel 4 zeigen werden.

Für den Fall eines Zahlkörpers K und seines Ganzzahlringes $\mathcal{O}_K$ schreibt man oft $Cl(K)$ für die Idealklassengruppe $Cl(\mathcal{O}_K)$ von K. Mit

$$h_K = \#Cl(\mathcal{O}_K)$$

wird die Klassenzahl von K bezeichnet. Beides sind wichtige Invarianten des Zahlkörpers K. Es ist bisher nicht bekannt, ob jede endliche abelsche Gruppe als Idealklassengruppe eines Zahlkörpers realisiert werden kann. Für imaginär-quadratische Zahlkörper ist aber bekannt, dass die kleinste Gruppe, die nicht als Klassengruppe realisiert werden kann, die Gruppe $(\mathbb{Z}/3\mathbb{Z})^3$ der Ordnung 27 ist. Für reell-quadratische Zahlkörper allerdings gilt zum Beispiel

$$CL(K) \cong (\mathbb{Z}/3\mathbb{Z})^3 \text{ for } K = \mathbb{Q}(\sqrt{188184253}).$$

Satz 3.2.11. *Sei A ein Dedekindring. Dann ist A genau dann faktoriell, wenn A ein Hauptidealring ist. Das ist genau dann der Fall, wenn A Klassenzahl 1 hat.*

Beweis. Jeder Hauptidealring ist faktoriell. Die Umkehrung ist allerdings im allgemeinen nicht richtig. Für einen Dedekindring gilt sie allerdings schon. Sei A also faktoriell, und P ein Primideal ungleich Null von A mit $a \in P$. Dann enthält P auch einen irreduziblen Faktor $t \mid a$, also $(t) \subseteq P$. Da A Dimension 1 hat, gilt $P = (t)$. Also ist jedes Primideal ein Hauptideal. Nach Satz 3.2.6 gilt für jedes Ideal $I \neq 0$ aber $I = P_1 \cdots P_n = (t_1) \cdots (t_n) = (t_1 \cdots t_n)$. Deshalb ist A ein Hauptidealring. Das bedeutet genau, dass die Idealklassengruppe von A trivial ist. □

Beispiel 3.2.12. *Die Klassenzahl von $\mathbb{Z}[\sqrt{-5}]$ ist nicht 1, sondern 2.*

Wir hatten in Beispiel 2.1.12 schon gesehen, daß der Ganzzahlring $\mathbb{Z}[\sqrt{-5}]$ des Zahlkörpers $\mathbb{Q}(\sqrt{-5})$ nicht faktoriell, also kein Hauptidealring ist. Mit Hilfe der Norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$ können wir aber auch direkt zeigen, daß etwa das Ideal $P = (2, 1 + \sqrt{-5})$ kein Hauptideal ist. Angenommen, es gälte $P = (\alpha)$. Dann gäbe es $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ mit $\beta\alpha = 2$ und $\gamma\alpha = 1 + \sqrt{-5}$. Das hieße $N(\beta)N(\alpha) = N(2) = 4$ und $N(\gamma)N(\alpha) = N(1 + \sqrt{-5}) = 6$. Also wäre $N(\alpha)$ ein Teiler von nicht-trivialer 4 und 6, d.h., $N(\alpha) = 2$. Mit $\alpha = x + y\sqrt{-5}$ für $x, y \in \mathbb{Z}$ hieße das $x^2 + 5y^2 = 2$. Doch diese quadratische Gleichung ist nicht lösbar in $\mathbb{Z}$. Man kann zeigen, daß $h_{\mathbb{Q}(\sqrt{-5})} = 2$ gilt.

Wir können jetzt am Beispiel $\mathbb{Z}[\sqrt{-5}]$ demonstrieren, wie man die fehlende Eindeutigkeit der Primfaktorzerlegung für Elemente für Ideale zurückgewinnt.

Beispiel 3.2.13. *Die zwei Faktorisierungen in irreduzible Elemente*

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

im Ganzzahlring $\mathbb{Z}[\sqrt{-5}]$ *sind wesentlich verschieden. Die entsprechenden Primidealzerlegungen des Ideals* (21) *sind hingegen bis auf Reihenfolge gleich.*

In der Tat, wie in Beispiel 2.1.12 zeigt man, daß alle Elemente $3, 7, 1 \pm 2\sqrt{-5}$ irreduzibel sind und paarweise nicht assoziiert. Deshalb sind die beiden obigen Faktorisierungen in irreduzible Elemente wesentlich verschieden. Man benutzt wieder die Norm. Einheiten in $\mathbb{Z}[\sqrt{-5}]$ sind nur ± 1. Wir haben $N(3) = 9$, $N(7) = 49$ und $N(1 \pm 2\sqrt{-5}) = 21$. Sei $K = \mathbb{Q}(\sqrt{-5})$ und $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Definiere folgende Ideale:

$$\begin{aligned} P_1 &= (3, 1 + 2\sqrt{-5}), \\ P_2 &= (3, 1 - 2\sqrt{-5}), \\ P_3 &= (7, 1 + 2\sqrt{-5}), \\ P_4 &= (7, 1 - 2\sqrt{-5}). \end{aligned}$$

Man prüft leicht nach, daß

$$\begin{aligned} P_1 P_2 &= (3), \\ P_3 P_4 &= (7), \\ P_1 P_3 &= (1 + 2\sqrt{-5}), \\ P_2 P_4 &= (1 - 2\sqrt{-5}). \end{aligned}$$

Nun stellt sich heraus, daß $P_1, \ldots, P_4$ maximale Ideale sind. Wir zeigen das für P_1, die anderen Fälle gehen analog. Betrachte die Abbildung $\varphi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/3$ gegeben durch $a + b\sqrt{-5} \mapsto \overline{a + b}$. Das ist ein Ringhomomorphismus. Die Additivität ist klar. Es gilt $\varphi(1) = 1$ und

$$\begin{aligned} \varphi((a + b\sqrt{-5})(c + d\sqrt{-5})) &= \varphi((ac - 5bd) + (ad + bc)\sqrt{-5}) \\ &= \overline{ac - 5bd + ad + bc} \\ &= \overline{ac + bd + ad + bc} \\ &= \overline{(a + b)(c + d)} \\ &= \varphi((a + b\sqrt{-5})\varphi(c + d\sqrt{-5})), \end{aligned}$$

also ist φ auch multiplikativ. Weiterhin ist

$$(3) \subsetneq P_1 \subseteq \ker(\varphi) \subsetneq \mathcal{O}_K.$$

Nun ist

$$\begin{aligned} \mathcal{O}_K/(3) &= \mathbb{Z}[x]/(x^2 + 5, 3) \\ &= \mathbb{F}_3[x]/(x^2 - 1) \\ &= \mathbb{F}_3[x]/(x - 1) \times \mathbb{F}_3[x]/(x + 1). \end{aligned}$$

Dieser Quotientenring hat 9 Elemente. Wegen der echten Inklusionen folgt $\#\mathcal{O}_K/\ker(\varphi)$ $= \#\mathcal{O}_K/P_1 = 3$, also $P_1 = \ker(\varphi)$. Damit ist $\mathcal{O}_K/P_1 = \mathcal{O}_K/\ker(\varphi) = \mathbb{Z}/3$ ein Körper, und P_1 maximal. Die zwei Idealzerlegungen $(21) = (3)(7)$ und $(21) = (1+2\sqrt{-5})(1-2\sqrt{-5})$ werden nun gleich, wenn man alle Ideale als Primidealprodukte schreibt:

$$\begin{aligned}(3)(7) &= (P_1P_2)(P_3P_4)\\ &= (P_1P_3)(P_2P_4)\\ &= (1+2\sqrt{-5})(1-2\sqrt{-5}),\end{aligned}$$

und die Zerlegung $(21) = P_1P_2P_3P_4$ ist eindeutig.

Satz 3.2.14. *Sei A ein Dedekindring und $I = \prod_P P^{\nu_P(I)}$, $J = \prod_P P^{\nu_P(J)}$ ganze Ideale von A. Dann gilt*

$$I \cap J = \prod_P P^{\max\{\nu_P(I),\nu_P(J)\}},$$
$$I + J = \prod_P P^{\min\{\nu_P(I),\nu_P(J)\}}.$$

Beweis. Aus Satz 3.2.7 folgt, daß sich die Inklusionsrelationen von Idealen in $\geq$-Relationen ihrer Exponenten ν_P übersetzen. Mit anderen Worten, $J \supseteq I$ genau dann wenn $\nu_P(J) \leq \nu_P(I)$. Man sagt dann auch, J teilt I. Wegen $I \cap J \subseteq I$ gilt also $\nu_P(I \cap J) \geq \nu_P(I)$. Ebenso gilt $\nu_P(I \cap J) \geq \nu_P(J)$ wegen $I \cap J \subseteq J$. Also ist $\nu_P(I \cap J) \geq \max\{\nu_P(I), \nu_P(J)\}$ und deshalb $I \cap J \subseteq \prod_P P^{\max\{\nu_P(I),\nu_P(J)\}}$. Andererseits ist die rechte Seite in I und J enthalten, also auch in $I \cap J$. Die zweite Behauptung folgt analog. □

Korollar 3.2.15. *Sei A ein Dedekindring und $I = \prod_P P^{\nu_P(I)}$ ein ganzes Ideal von A. Dann gilt*

$$A/I \simeq \prod_P A/P^{\nu_P(I)}.$$

Beweis. Wir bemerken zunächst, daß das Produkt endlich ist, da fast alle Faktoren $A/P^{\nu_P(I)}$ Null sind. Die Ideale $P^{\nu_P(I)}$ sind für verschiedene maximale Ideale paarweise teilerfremd, also $P^{\nu_P(I)} + Q^{\nu_Q(I)} = A$ wegen Satz 3.2.14. Ihr Schnitt ist I nach Satz 3.2.14, da $P \cap Q = PQ$ für teilerfremde Ideale gilt. Nun liefert der chinesische Restsatz genau die Aussage. □

Lemma 3.2.16. *Sei A ein Dedekindring und P ein maximales Ideal von A. Sei $\mathbb{F} = A/P$ der Restklassenkörper und $n \geq 0$ eine ganze Zahl. Dann ist $P^n/P^{n+1} \simeq \mathbb{F}$ ein 1-dimensionaler $\mathbb{F}$-Vektorraum.*

Beweis. Sei $b \in P^n \setminus P^{n+1}$. Die Abbildung $\varphi\colon A \to P^n/P^{n+1}$ mit $\varphi(a) = ab$ ist ein A-Modul-Homomorphismus mit $\ker(\varphi) = P$. Also induziert φ einen injektiven A-Modul-Homomorphismus $A/P \hookrightarrow P^n/P^{n+1}$. Somit hat P^n/P^{n+1} mindestens Dimension 1 über $\mathbb{F}$. Wir zeigen, daß es ein $y \in P^n$ gibt, das P^n/P^{n+1} erzeugt. Sei $x \in P \setminus P^2$. Das bedeutet $\nu_P(x) = 1$ und daher $\nu_p(x^n) = n$. Nach Satz 3.2.14 ist $(x^n) + P^{n+1} = P^n$. Also ist $y = x^n$ der gesuchte Erzeuger. □

3.3 Idealnorm

Die Idealnorm in einem Ganzzahlring ist wie folgt definiert.

Definition 3.5. Sei $\mathcal{O}_K$ der Ganzzahlring eines Zahlkörpers K und I ein von Null verschiedenes ganzes Ideal in $\mathcal{O}_K$. Dann heißt

$$N(I) := \#(\mathcal{O}_K/I) = [\mathcal{O}_K : I]$$

die *Idealnorm* von I.

Für $K = \mathbb{Q}$ bedeutet das $\mathcal{O}_K = \mathbb{Z}$ und $I = (a)$ für ein $a \neq 0$ in $\mathbb{Z}$. Dann ist $N(I) = \#(\mathbb{Z}/a) = |a|$. Insbesondere ist die Idealnorm in diesem Fall endlich. Das gilt auch allgemein.

Lemma 3.3.1. *Die Idealnorm in einem Ganzzahlring ist endlich.*

Beweis. Nach dem Elementarteilersatz gibt es eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und ganze Zahlen $a_1, \ldots, a_n$, so daß $a_1x_1, \ldots, a_nx_n$ eine $\mathbb{Z}$-Basis von I ist. Damit erhalten wir einen Gruppenisomorphismus

$$\mathcal{O}_K/I \simeq \mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_n.$$

Insbesondere folgt $N(I) = |a_1 \cdots a_n|$. □

Ist $p \in \mathbb{Z}$ eine Primzahl, und $(p) = \mathcal{O}_K p = P_1^{\nu_1} \cdots P_r^{\nu_r}$ die Zerlegung in Primideale, mit $\nu_i \geq 1$ und P_i paarweise verschieden, so sind die P_i genau die Primideale, die *über p liegen*, d.h., $P_i \cap \mathbb{Z} = (p)$ erfüllen. Dann ist $\mathbb{F}_p \subseteq \mathcal{O}_K/P_i$ eine Erweiterung von endlichen Körpern mit Körpergrad

$$f_{P_i} := [\mathcal{O}_K/P_i : \mathbb{F}_p].$$

Dieser Körpergrad heißt auch der *Restklassengrad* von P_i. Jedes Primideal $P \neq 0$ liegt über genau einer Primzahl $p \in \mathbb{Z}$. Für die Idealnorm von P gilt dann

$$N(P) = \#(\mathcal{O}_K/P) = p^{[\mathcal{O}_K/P:\mathbb{F}_p]}.$$

Lemma 3.3.2. *Sei A ein Dedekindring und $I = \prod_P P^{\nu_P(I)}$ ein ganzes Ideal von A. Dann gilt*

$$N(I) = \prod_P N(P)^{\nu_P(I)}.$$

Es gilt also $N(IJ) = N(I)N(J)$, d.h., die Idealnorm ist multiplikativ.

Beweis. Nach dem chinesischem Restsatz genügt es, Ideale $I = P^n$ zu betrachten. Für $n = 1$ gilt die Aussage. Angenommen sie gilt schon für n. Wir zeigen sie für $n + 1$. Die Abbildung

$$\mathcal{O}_K/P^{n+1} \to \mathcal{O}_K/P^n$$

ist surjektiv mit Kern P^n/P^{n+1}. Nach Lemma 3.2.16 ist P^n/P^{n+1} ein 1-dimensionaler $\mathcal{O}_K/P$-Vektorraum, der also $N(P) = \#(\mathcal{O}_K/P)$ viele Elemente hat. Es folgt $N(P^{n+1}) = N(P^n)N(P) = N(P)^{n+1}$. □

Die Idealnorm verallgemeinert die Norm der Körpererweiterung $K/\mathbb{Q}$ aus Definition 2.7.

Lemma 3.3.3. *Sei $\mathcal{O}_K$ der Ganzzahlring eines Zahlkörpers K und $I = (\alpha)$ ein von Null verschiedenes ganzes Hauptideal in $\mathcal{O}_K$. Dann gilt*

$$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Beweis. Es gibt, wie gesagt, eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und ganze Zahlen $a_1, \ldots, a_n$, so daß $a_1x_1, \ldots, a_nx_n$ eine $\mathbb{Z}$-Basis für I ist. Es gilt $N(I) = |a_1 \cdots a_n|$, siehe Lemma 3.3.1. Jetzt berechnen wir $N_{K/\mathbb{Q}}(\alpha)$ auf eine geschickte Weise, die zeigt, daß sich bis auf Vorzeichen ebenfalls der Wert $N(I)$ ergibt. Der Zahlkörper K hat drei $\mathbb{Q}$-Basen: $\{x_i\}$, $\{a_ix_i\}$ und $\{\alpha x_i\}$. Wir erhalten ein kommutatives Diagramm von $\mathbb{Q}$-linearen Abbildungen

$$\begin{array}{ccc} K & \xrightarrow{\ell_\alpha} & K \\ {\scriptstyle \mathrm{id}}\downarrow & & \uparrow{\scriptstyle v} \\ K & \xrightarrow[u]{} & K \end{array}$$

wobei u und v durch $u(x_i) = a_ix_i$ und $v(a_ix_i) = \alpha x_i$ definiert sind. Es gilt $v(u(\mathrm{id}(x_i))) = \alpha x_i = \ell_\alpha(x_i)$, weshalb das Diagramm kommutiert. Nun untersuchen wir die Determinanten der vier linearen Abbildungen. Nach Definition ist $\det(\ell_\alpha) = N_{K/\mathbb{Q}}(\alpha)$. Natürlich ist $\det(u) = a_1 \cdots a_n$ und $\det(\mathrm{id}) = 1$. Wir behaupten, daß $\det(v) = \pm 1$ gilt. Dazu bemerken wir, daß $\{a_ix_i\}$ und $\{\alpha x_i\}$ nicht nur $\mathbb{Q}$-Basen von K sind, sondern auch $\mathbb{Z}$-Basen des freien $\mathbb{Z}$-Moduls I. Die Basiswechselmatrix eines freien $\mathbb{Z}$-Moduls hat aber bekanntlich eine in $\mathbb{Z}$ invertierbare Determinante, also ± 1. Es folgt also

$$N_{K/\mathbb{Q}}(\alpha) = \det(\ell_\alpha) = \det(u)\det(v) = \pm a_1 \cdots a_n.$$

□

Bemerkung 3.3.4. Die Definition der Idealnorm macht für jeden globalen Körper Sinn. Ist K ein Funktionenkörper, und I ein Ideal in $\mathcal{O}_K$, so erhält man

$$\mathcal{O}_K/I \simeq \mathbb{F}_p[t]/(\lambda_1) \times \cdots \times \mathbb{F}_p[t]/(\lambda_n)$$

mit Polynomen $\lambda_i \in \mathbb{F}_p[t]$. Deshalb gilt auch $N(I) = \prod_{i=1}^n |\mathbb{F}_p[t]/(\lambda_i)| < \infty$. Ebenso gilt Lemma 3.3.3 auch im Funktionenkörperfall. Man hat

$$N((\lambda)) = N(N_{K/\mathbb{F}_p(t)}(\lambda)).$$

Das ist die analoge Formel, da ja $N((y)) = |y|$ für $y \in \mathbb{Z}$ gilt.

4 Endlichkeit der Klassenzahl

Wir wollen in diesem Kapitel zeigen, daß die Idealklassengruppe eines Zahlkörpers K endlich ist. Dazu zeigen wir ein stärkeres Resultat von Minkowski, das zusätzlich eine effektive Schranke für die Norm von Idealen in jeder Idealklasse liefert. Diese Schranke ist hinreichend effektiv, um die Idealklassengruppe für einige Beispiele explizit berechnen zu können.
Die Idealklassengruppe ist auch ein Maß dafür, wie weit entfernt der Ganzzahlring $\mathcal{O}_K$ von einem Hauptidealring ist. Zudem liefern die Idealklassengruppe und ihre Verallgemeinerungen tiefe Einsichten darüber, welche Zahlkörpererweiterungen von K galoissch mit abelscher Galoisgruppe sind. Das wird in der sogenannten Klassenkörpertheorie studiert.

4.1 Minkowski-Theorie

Sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$.

Definition 4.1. Ein *Gitter* Λ in V ist eine Untergruppe der Form

$$\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r,$$

wobei $v_1, \ldots, v_r$ linear unabhängige Vektoren in V sind. Ist $r = n$, so heißt Λ ein *vollständiges Gitter*.

Ein Gitter ist also eine freie abelsche Untergruppe vom Rang r von V, die durch linear unabgängige Elemente über $\mathbb{R}$ von V erzeugt wird.

Definition 4.2. Sei $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$ ein Gitter in V, und $\alpha \in \Lambda$. Dann heißt

$$F = \left\{ \alpha + \sum_{i=1}^{r} \xi_i v_i \mid 0 \leq \xi_i < 1 \right\}$$

eine *Grundmasche*, oder *fundamentales Parallelepiped* von Λ.

Ein Gitter Λ in V ist genau dann vollständig, wenn die sämtlichen Translate $\alpha + F$ mit $\alpha \in \Lambda$ den ganzen Raum V überdecken.

Beispiel 4.1.1. *$\mathbb{Z}^n \subseteq \mathbb{R}^n$ ist ein vollständiges Gitter. Die Untergruppe $\mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ von $\mathbb{R}$ ist eine freie abelsche Gruppe vom Rang 2, aber kein Gitter in $\mathbb{R}$. Weiterhin ist $\mathbb{Z} \oplus \mathbb{Z}i$ ein vollständiges Gitter in $\mathbb{C}$.*

Definition 4.3. Eine Untergruppe L von V heißt *diskret*, falls jeder Punkt $\alpha \in L$ eine offene Umgebung U in V hat mit $U \cap L = \{\alpha\}$.

Mit anderen Worten, L ist genau dann diskret, wenn L diskret ist bezüglich der Relativtopologie von V.

Lemma 4.1.2. *Sei L eine Untergruppe von V. Dann sind äquivalent:*

(a) L ist diskret.

(b) Es gibt eine offene Umgebung U in V mit $U \cap L = \{0\}$.

(c) Jede kompakte Teilmenge von V schneidet L in einer endlichen Menge.

(d) Jede beschränkte Teilmenge von V schneidet L in einer endlichen Menge.

Beweis. $(a) \Rightarrow (b)$: klar.
$(b) \Rightarrow (a)$: Die Translationsabbildung $t_v \colon V \to V$ mit $x \mapsto x + v$ ist ein Homeomorphismus. Erfüllt U die Annahme in (b), so ist also $\alpha + U$ eine offene Umgebung von α mit $(\alpha + U) \cap L = \{\alpha\}$.
$(a) \Rightarrow (c)$: L ist ein diskreter topologischer Raum bezüglich der induzierten Topologie. Für eine kompakte Menge K in V ist $K \cap L$ sowohl diskret als auch kompakt, und daher endlich.
$(c) \Rightarrow (d)$: Der Abschluß einer beschränkten Menge in V ist kompakt, da das im $\mathbb{R}^n$ gilt, und V sich nur durch Basiswahl von $\mathbb{R}^n$ unterscheidet, die Topologie aber unabhängig von der Basis ist. Die Behauptung folgt also durch Abschlußbildung.
$(d) \Rightarrow (b)$: Sei U eine beschränkte offene Umgebung von 0. Dann ist $S = (U \cap L) \setminus \{0\}$ endlich und daher abgeschlossen. Folglich ist $U \setminus S$ eine offene Umgebung von 0 mit $(U \setminus S) \cap L = \{0\}$. □

Satz 4.1.3. *Eine Untergruppe Λ von V ist genau dann ein Gitter, wenn Λ diskret ist.*

Beweis. Ein Gitter ist diskret. Dazu sei $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$, $\alpha = \sum_{i=1}^{r} a_i v_i$ in Λ und $\{v_1, \ldots, v_n\}$ eine Basis von V. Dann ist

$$U = \left\{ \sum_{i=1}^{n} \xi_i v_i \mid \xi_i \in \mathbb{R},\ |\xi_i - a_i| < 1 \quad \forall\, i \right\}$$

eine offene Umgebung von α in V mit $U \cap \Lambda = \{\alpha\}$.
Sei umgekehrt Λ eine diskrete Untergruppe von V. Sei U der Untervektorraum von V, der durch die Menge Λ aufgespannt wird. Wähle eine Basis $\{v_1, \ldots, v_n\}$ von V, so daß $\{v_1, \ldots, v_r\}$ eine Basis von U ist. Dann ist

$$\Lambda' := \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r \subseteq \Lambda$$

ein vollständiges Gitter in U. Wir behaupten, daß der Index $(\Lambda : \Lambda')$ endlich ist. Es seien λ_i mit $i \in \mathcal{I}$ die Repräsentanten für die Nebenlassen in Λ/Λ'. Da Λ' vollständig ist gilt

$$U = \bigcup_{\lambda \in \Lambda'} (\lambda + F)$$

mit einer Grundmasche $F = \{\sum_{i=1}^{r} \xi_i v_i \mid \xi_i \in [0,1)\}$. Daher ist $\lambda_i = \lambda_i' + m_i$ für jedes $i \in \mathcal{I}$, mit $\lambda_i' \in \Lambda'$ und $m_i \in F$. Da die Menge $\{m_i = \lambda_i - \lambda_i' \mid i \in \mathcal{I}\}$ diskret ist und in der beschränkten Menge F liegt, ist sie endlich. Also ist Λ/Λ' endlich. Mit $(\Lambda : \Lambda') = k$ gilt also $k\Lambda \subseteq \Lambda'$, und

$$\Lambda \subseteq \frac{1}{k}\Lambda' = \frac{1}{k}\mathbb{Z}v_1 \oplus \cdots \oplus \frac{1}{k}\mathbb{Z}v_r.$$

Mit dem Elementarteilersatz folgt $\Lambda = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r$, wobei $\{w_1, \ldots, w_s\}$ eine $\mathbb{Z}$-Basis ist mit $w_i \in U$. Da die w_i ebenfalls U aufspannen, gilt $r = s$, und $\{w_1, \ldots, w_r\}$ sind linear unabhängig über $\mathbb{R}$. Somit ist Λ ein Gitter in V. □

Sei V ein Euklidischer Vektorraum, also ein n-dimensionaler $\mathbb{R}$-Vektorraum mit symmetrischer, positiv definiter Bilinearform $<,>: V \times V \to \mathbb{R}$. Sei $M \subset \mathbb{R}^n$ eine messbare Menge bezüglich des Lebesque-Maßes μ. Dann definiert man das Volumen von M durch $\mathrm{vol}(M) = \mu(M)$.
Ist $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ ein vollständiges Gitter in $\mathbb{R}^n$, so gilt

$$\mathrm{vol}(F) = |\det(v_1, \ldots, v_n)|$$

für eine Grundmasche F von Λ.
Für einen beliebigen Euklidischen Vektorraum V sei $\mathcal{B} = \{v_i\}$ eine Orthonormalbasis von V und $\{e_i\}$ die Standardbasis $\{e_i\}$ des $\mathbb{R}^n$. Dann ist $\varphi = \varphi_{\mathcal{B}}: \mathbb{R}^n \to V$, $e_i \mapsto v_i$ eine Isometrie von V, und wir nennen eine Menge $M \subseteq V$ messbar, wenn $\varphi^{-1}(M) \subseteq \mathbb{R}^n$ Lebesgue-messbar im $\mathbb{R}^n$ ist. Wir definieren das Volumen von M in V durch

$$\mathrm{vol}(M) := \mathrm{vol}_{\mathcal{B}}(M) = \mu(\varphi^{-1}(M)).$$

Lemma 4.1.4. *Sei A ein Automorphismus von V. Dann gilt*

$$\mathrm{vol}(A(M)) = |\det(A)| \cdot \mathrm{vol}(M).$$

Insbesondere ist das Volumen $\mathrm{vol}(M)$ *unabhängig von der Wahl einer Orthonormalbasis von V.*

Beweis. Es sei $\mathcal{B}_1 = \{v_i\}$ eine Orthonormalbasis von V und $A = (a_{ij}) \in GL(n, \mathbb{R})$. Die zugehörige lineare Abbildung $A: v_j \mapsto \sum_{i=1}^{n} a_{ij} v_i := w_j$ liefert eine neue Basis $\mathcal{B}_2 = \{w_j\}$ von V und Isometrien $\varphi_{\mathcal{B}_1}: \mathbb{R}^n \to V$, $\varphi_{\mathcal{B}_2}: \mathbb{R}^n \to V$ mit $A \circ \varphi_{\mathcal{B}_1} = \varphi_{\mathcal{B}_2} = \varphi_{\mathcal{B}_1} \circ A$. Dabei muß $\mathcal{B}_2$ nicht notwendig eine Orthonormalbasis sein. Wir haben

$$\begin{aligned}
\mathrm{vol}_{\mathcal{B}_2}(M) &= \mu(\varphi_{\mathcal{B}_2}^{-1}(M)) \\
&= \mu(A^{-1}\varphi_{\mathcal{B}_1}^{-1}(M)) \\
&= |\det(A^{-1})| \cdot \mu(\varphi_{\mathcal{B}_1}^{-1}(M)) \\
&= |\det(A)|^{-1} \cdot \mathrm{vol}_{\mathcal{B}_1}(M).
\end{aligned}$$

Ist $\mathcal{B}_2$ auch eine Orthonormalbasis, so gilt $\det(A) = \pm 1$ und $\mathrm{vol}_{\mathcal{B}_1}(M) = \mathrm{vol}_{\mathcal{B}_2}(M)$. □

Das Parallelepiped $F_{\mathcal{B}_1} = \{\sum_{i=1}^n \xi_i v_i \mid 0 \leq \xi_i < 1\}$ bezüglich der Orthonormalbasis $\{v_i\}$ hat Volumen 1. Für das Parallelepiped $F_{\mathcal{B}_2} = \{\sum_{i=1}^n \xi_i w_i \mid 0 \leq \xi_i < 1\}$ bezüglich der neuen Basis $\mathcal{B}_2$ gilt $F_{\mathcal{B}_2} = A \cdot F_{\mathcal{B}_1}$, also

$$\begin{aligned}\mathrm{vol}(F_{\mathcal{B}_2}) &= |\det(A)| \cdot \mathrm{vol}(F_{\mathcal{B}_1}) \\ &= |\det(A)| \cdot 1 \\ &= |\det((< w_i, w_j >)_{i,j})|^{\frac{1}{2}}.\end{aligned}$$

Der letzte Schritt folgt aus folgender Rechnung, mit $< v_k, v_l >= \delta_{kl}$,

$$\begin{aligned}(< w_i, w_j >)_{i,j} &= \sum_{k,l} a_{ik} a_{jl} < v_k, v_l > \\ &= \left(\sum_k a_{ik} a_{jk} \right) \\ &= AA^t,\end{aligned}$$

also wegen $\det((< w_i, w_j >)_{i,j}) = \det(AA^t) = \det(A)^2$.

Definition 4.4. Sei $\Lambda = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r$ ein Gitter in V bezüglich einer Basis $\mathcal{B} = \{w_i\}$ eines Unterraums von V. Definiere das Volumen von Λ durch

$$\mathrm{vol}(\Lambda) = \mathrm{vol}(F_{\mathcal{B}}) = |\det((< w_i, w_j >)_{i,j})|^{\frac{1}{2}}.$$

Da für eine andere $\mathbb{Z}$-Basis des Gitters die Basiswechselmatrix in $GL(r, \mathbb{Z})$ liegt, also Determinante ± 1 hat, ist das Volumen von Λ unabhängig von der gewählten Basis.

Bemerkung 4.1.5. Sei Λ ein Gitter in V, und Λ' ein Untergitter von endlichem Index. Dann gilt

$$\mathrm{vol}(\Lambda') = (\Lambda : \Lambda') \cdot \mathrm{vol}(\Lambda).$$

Satz 4.1.6. *Sei Λ ein vollständiges Gitter in V und S eine messbare Menge in V. Gilt* $\mathrm{vol}(S) > \mathrm{vol}(\Lambda)$*, so gibt es zwei verschiedene Elemente x, y in S mit $y - x \in \Lambda$.*

Beweis. Sei D eine Grundmasche von Λ und $\mathcal{F}$ die Menge aller Translate von D unter Λ. Dann ist $S \cap F$ messbar für alle $F \in \mathcal{F}$, und

$$\mathrm{vol}(S) = \sum_{F \in \mathcal{F}} \mathrm{vol}(S \cap F).$$

Für jedes F gibt es ein *eindeutiges* Translat von $S \cap F$ durch ein Element von Λ, das eine Teilmenge von D ist. Wegen $\mathrm{vol}(S) > \mathrm{vol}(D) = \mathrm{vol}(\Lambda)$ müssen sich mindestens zwei dieser Translate überlappen. Also gibt es zwei verschiedene Elemente x, y in S mit $x - \lambda = y - \lambda'$ für Elemente $\lambda, \lambda' \in \Lambda$. Dann gilt $y - x \in \Lambda$. □

Nun kommen wir zum Gitterpunktsatz von Minkowski. Dazu brauchen wir noch folgende Definitionen.

Definition 4.5. Eine Teilmenge S in V heißt *konvex*, wenn für je zwei $x, y \in S$ auch ihre Verbindungsstrecke $\{(1-t)x + ty \mid 0 \leq t \leq 1\}$ in S liegt. Sie heißt *zentralsymmetrisch*, wenn für alle $x \in S$ auch $-x \in S$ gilt.

Theorem 4.1.7 (Minkowski 1896)**.** *Sei Λ ein vollständiges Gitter in einem n-dimensionalen Euklidischen Vektorraum, und S eine konvexe, zentralsymmetrische Menge in V. Gilt eine der zwei folgenden Bedingungen*

(1) $\mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Lambda)$,

(2) $\mathrm{vol}(S) \geq 2^n \cdot \mathrm{vol}(\Lambda)$, *und S ist kompakt,*

so enthält S einen von Null verschiedenen Gitterpunkt.

Beweis. Fall (1): Für $T = \frac{1}{2}S$ gilt

$$\mathrm{vol}(T) = \frac{1}{2^n}\mathrm{vol}(S) > \mathrm{vol}(\Lambda).$$

Nach Satz 4.1.6 gibt es $x, y \in T$ mit $y - x \in \Lambda$ und $y - x \neq 0$. Dann sind $2x$ und $2y$ in S, also auch $-2x$ in S. Die Darstellung

$$y - x = \frac{1}{2}(2y + (-2x))$$

zeigt, daß $y - x$ auch in S liegt, da S konvex ist. Daher ist $y - x \in S \cap \Lambda$, und auch $x - y$, ein von Null verschiedener Gitterpunkt in S.
Fall (2): Wir können den ersten Fall auf $(1+\varepsilon)S$ anwenden, mit $\varepsilon > 0$. Wegen $\mathrm{vol}((1+\varepsilon)S) = (1+\varepsilon)^n \mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Lambda)$ folgt

$$S_\varepsilon := (\Lambda \setminus 0) \cap (1+\varepsilon)S \neq \emptyset.$$

Jede Menge S_ε ist endlich, da S kompakt ist, und Λ diskret. Deshalb ist auch die Menge $\cap_{\varepsilon>0} S_\varepsilon$ nicht leer. Sei $z \in \cap_{\varepsilon>0} S_\varepsilon$. Dann gilt $z \in \Lambda \setminus 0$ und

$$z \in \bigcap_{\varepsilon>0} (1+\varepsilon)S = S,$$

da S abgeschlossen ist. Also ist $z \in S \cap \Lambda$ ein von Null verschiedener Gitterpunkt in S. □

Bemerkung 4.1.8. Obwohl das Theorem nicht so schwer zu beweisen ist, hat es viele nicht-triviale Konsequenzen. Man kann daraus zum Beispiel relativ leicht den Satz von Lagrange (1770) folgern, daß jede natürliche Zahl die Summe von vier Quadratzahlen ist.

4.2 Ganzzahlringe als Gitter

Sei K ein Zahlkörper vom Grad $n = [K : \mathbb{Q}]$. Dann ist $K = \mathbb{Q}(\alpha)$ für ein α und daher $K \simeq \mathbb{Q}[x]/(f(x))$, wobei $f(x) \in \mathbb{Q}[x]$ das Minimalpolynom von α ist. Es hat genau n komplexe Nullstellen. Jede komplexe Nullstelle z induziert einen Homomorphismus $\mathbb{Q}[x] \to \mathbb{C}$ mit Kern $(f(x))$. Auf diese Weise erhalten wir n verschiedene Einbettungen $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$. Eine Einbettung $\sigma \colon K \hookrightarrow \mathbb{C}$ heißt *reell*, falls $\sigma(K) \subseteq \mathbb{R}$ gilt, und *komplex* anderenfalls. Sei r die Anzahl der verschiedenen reellen Einbettungen von K. Jede komplexe Einbettung σ definiert durch $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ eine weitere komplexe Einbettung, die wegen $\sigma(K) \not\subseteq \mathbb{R}$ von σ verschieden ist. Daher können wir die verschiedenen komplexen Einbettungen in Paaren $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}$ gruppieren. Insgesamt haben wir also

$$n = r + 2s$$

verschiedene Einbettungen von K. Wir wollen sie so anordnen, daß die ersten r davon die reellen Einbettungen sind.

Beispiel 4.2.1. *Der Zahlkörper $K = \mathbb{Q}(\sqrt[3]{5})$ hat eine reelle und zwei komplexe Einbettungen. Es ist also $r = s = 1$.*

Das Minimalpolynom von $\alpha = \sqrt[3]{5}$ ist $x^3 - 5$. Die Einbettungen in $\mathbb{C}$ entstehen daraus, indem man α auf die Nullstellen $\alpha, \zeta\alpha, \zeta^2\alpha$ von $x^3 - 5$ in $\mathbb{C}$ abbildet. Hierbei ist ζ eine primitive dritte Einheitswurzel.

Definition 4.6. Die *kanonische Einbettung* eines Zahlkörpers K in den Euklidischen Vektorraum $V_K := \mathbb{R}^r \times \mathbb{C}^s$ ist durch

$$\sigma \colon K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$$

gegeben.

Wir können V_K mit dem $\mathbb{R}^n$ identifizieren, indem wir die Basis $\{1, i\}$ für $\mathbb{C}$ benutzen. Das identifiziert $z = a + bi$ mit $(a, b) = (\Re(z), \Im(z))$. Mit diesen Bezeichnungen gilt nun folgendes Lemma.

Lemma 4.2.2. *Sei M ein freier $\mathbb{Z}$-Untermodul von K und $\{x_1, \ldots, x_n\}$ eine Basis von M. Dann ist $\sigma(M)$ ein vollständiges Gitter in $\mathbb{R}^n$ mit Volumen*

$$\operatorname{vol}(\sigma(M)) = 2^{-s} \cdot |\det((\sigma_i(x_j)_{i,j}))|.$$

Beweis. Sei A die Matrix mit den Zeilenvektoren $\sigma(x_i)$. Es gilt

$$\begin{aligned}\sigma(x_i) = (&\sigma_1(x_i), \ldots, \sigma_r(x_i), \Re(\sigma_{r+1}(x_i)), \Im(\sigma_{r+1}(x_i)), \ldots, \\ &\Re(\sigma_{r+s}(x_i)), \Im(\sigma_{r+s}(x_i))),\end{aligned}$$

und $\operatorname{vol}(\sigma(M)) = |\det(A)|$. Sei B die Matrix, deren i-te Zeile durch

$$(\sigma_1(x_i), \ldots, \sigma_r(x_i), \sigma_{r+1}(x_i), \overline{\sigma_{r+1}(x_i)}, \ldots, \sigma_{r+s}(x_i), \overline{\sigma_{r+s}(x_i)})$$

gegeben ist. Wir haben in Lemma 2.4.7 gesehen, daß gilt

$$\begin{aligned}\det(B)^2 &= D(x_1,\ldots,x_n)\\ &= \det((\sigma_i(x_j)_{i,j}))^2 \neq 0\end{aligned}$$

gilt. Wir behaupten nun, daß

$$\det(B) = (-2i)^s \det(A)$$

gilt. Dann folgt $\det(A) \neq 0$. Deshalb sind die Vektoren $\sigma(x_1),\ldots,\sigma(x_n)$ linear unabhängig über $\mathbb{R}$, und $\sigma(M)$ ist ein vollständiges Gitter in $\mathbb{R}^n$. Wegen $|i^s| = 1$ folgt auch

$$\begin{aligned}|\det((\sigma_i(x_j)_{i,j}))| &= |\det(B)|\\ &= 2^s|\det(A)|\\ &= 2^s\mathrm{vol}(\sigma(M)).\end{aligned}$$

Die behauptete Relation zwischen beiden Determinanten sieht man wie folgt. Für eine komplexe Zahl z kann man $\Re(z)$ und $\Im(z)$ als

$$\Re(z) = \frac{1}{2}(z+\overline{z}),\ \Im(z) = \frac{1}{2i}(z-\overline{z})$$

ausdrücken. Das tun wir für $z = \sigma(x_j)$ für $j = r+1,\ldots,n$. Wegen

$$\det(\ldots,\frac{1}{2}(z+\overline{z}),\frac{1}{2i}(z-\overline{z}),\ldots) = -\frac{1}{2i}\det(\ldots,z,\overline{z},\ldots)$$

folgt die Behauptung, nach s-facher Anwendung. □

Korollar 4.2.3. *Sei K ein Zahlkörper mit Ganzzahlring $\mathcal{O}_K$ und Diskriminante d_K. Dann ist $\sigma(\mathcal{O}_K)$ ein vollständiges Gitter in $\mathbb{R}^n$ mit Volumen*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-s}\sqrt{|d_K|}.$$

Beweis. Sei $\{x_1,\ldots,x_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$. Dann ist

$$d_K = D(x_1,\ldots,x_n) = \det((\sigma_i(x_j)_{i,j}))^2$$

und

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-s}\cdot|\det((\sigma_i(x_j)_{i,j}))| = 2^{-s}\sqrt{|d_K|}.$$

□

Korollar 4.2.4. *Sei K ein Zahlkörper mit Diskriminante d_K, und I ein von Null verschiedenes Ideal in $\mathcal{O}_K$. Dann ist $\sigma(I)$ ein vollständiges Gitter in $\mathbb{R}^n$ mit Volumen*

$$\mathrm{vol}(\sigma(I)) = 2^{-s}N(I)\sqrt{|d_K|}.$$

Beweis. Das Ideal I ist ebenfalls ein freier $\mathbb{Z}$-Modul vom Rang n. Daher ist $\sigma(I)$ ein vollständiges Gitter. Nach dem Elementarteilersatz können wir eine $\mathbb{Z}$-Basis $\{x_1, \ldots, x_n\}$ von $\mathcal{O}_K$ wählen, und $a_i \in \mathbb{Z}$, so daß gleichzeitig $\{a_1 x_1, \ldots, a_n x_n\}$ eine $\mathbb{Z}$-Basis von I ist. Dann gilt $N(I) = |a_1 \cdots a_n|$, siehe Lemma 3.3.1. Es folgt also

$$\begin{aligned}\mathrm{vol}(\sigma(I)) &= 2^{-s}|\det((\sigma_i(a_j x_j)_{i,j}))| \\ &= 2^{-s}|a_1 \cdots a_n| \cdot |\det((\sigma_i(x_j)_{i,j}))| \\ &= 2^{-s} N(I)\sqrt{|d_K|}.\end{aligned}$$

□

Jetzt können wir folgendes Theorem beweisen, aus dem die Endlichkeit der Klassenzahl folgt.

Theorem 4.2.5. *Sei K ein Zahlkörper vom Grad n mit Diskriminante d_K, und I ein von Null verschiedenes Ideal in $\mathcal{O}_K$. Dann gibt es ein $x \neq 0$ in I mit*

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

Beweis. Wir benutzen im folgenden manchmal auch die Abkürzungen

$$\begin{aligned}C_K &= \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s, \\ B_K &= C_K\sqrt{|d_K|} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.\end{aligned}$$

Die Konstante B_K heißt *Minkowski-Schranke*, und C_K heißt *Minkowski-Konstante*. Wir betrachten die kanonische Einbettung $\sigma\colon K \hookrightarrow V_K$ in den Euklidischen Vektorraum $V_K = \mathbb{R}^r \times \mathbb{C}^s$, mit der Norm

$$\|x\| = \sum_{i=1}^{r}|y_i| + 2\sum_{j=1}^{s}|z_j|$$

für $x = (y_1, \ldots, y_r, z_1, \ldots, z_s) \in V_K$. Sei $t > 0$ eine reelle Zahl, und

$$B_t = \{x \in V_K \mid \|x\| \leq t\}.$$

Wir werden zeigen, daß

$$\mu(B_t) = 2^r\left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \tag{4.1}$$

gilt. Dann folgt die Behauptung aus dem Gitterpunktsatz von Minkowski mit der richtigen Wahl von $t > 0$. Die Menge B_t ist nämlich kompakt, konvex und zentralsymmetrisch. Man muß $\mu(B_t) \geq 2^n\mathrm{vol}(\sigma(I))$ wählen. Das bedeutet wegen Korollar 4.2.4 aber

$$\begin{aligned}2^r\left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} &= \mu(B_t) \\ &\geq 2^n\mathrm{vol}(\sigma(I)) \\ &= 2^{n-s}\sqrt{|d_K|}N(I),\end{aligned}$$

also genau

$$t^n \geq n!\, 4^s\, \pi^{-s} \sqrt{|d_K|} N(I),$$

wegen $n = r + 2s$. Wenn wir t^n so wählen, daß Gleichheit besteht, dann gibt es nach (2) in Theorem 4.1.7 ein $x \in I$ mit $\sigma(x) \in B_t$ und $\sigma(x) \neq 0$, also mit $x \neq 0$. Die Norm von x können wir nun mit Hilfe der Ungleichung

$$a_1 \cdots a_n \leq n^{-n}(a_1 + \cdots + a_n)^n$$

für $a_i > 0$ mit obiger Formel für t^n abschätzen. Wir erhalten

$$\begin{aligned}
|N_{K/\mathbb{Q}}(x)| &= |\sigma_1(x)| \cdots |\sigma_r(x)| \cdot |\sigma_{r+1}(x)|^2 \cdots |\sigma_{r+s}(x)|^2 \\
&\leq n^{-n}(|\sigma_1(x)| + \cdots + |\sigma_r(x)| + 2|\sigma_{r+1}(x)| + \cdots + 2|\sigma_{r+s}(x)|)^n \\
&= n^{-n}\|x\|^n \\
&\leq n^{-n} t^n \\
&= n^{-n}\, n!\, 4^s\, \pi^{-s} \sqrt{|d_K|} N(I).
\end{aligned}$$

Das ist offenbar die Behauptung. Wir müssen jetzt nur noch die Formel 4.1 für $\mu(B_t)$ beweisen. Das geschieht mit Induktion über r und s. Wir schreiben deshalb $V(r, s, t) = \mu(B_t)$. Für den Induktionsanfang überprüfen wir die Fälle $(r, s) = (1, 0)$ und $(r, s) = (0, 1)$:

$$\begin{aligned}
V(1, 0, t) &= \mu(\{y_1 \in \mathbb{R} \mid |y_1| \leq t\}) = 2t, \\
V(0, 1, t) &= \mu(\{z_1 \in \mathbb{C} \mid 2|z_1| \leq t\}) = \pi \left(\frac{t}{2}\right)^2,
\end{aligned}$$

wobei $V(0, 1, t)$ die Fläche des Kreises mit Radius $t/2$ ist. Die Ergebnisse entsprechen der Formel 4.1. Der erste Induktionsschritt $r \mapsto r+1$ geht so, mit $(y_0, \ldots, y_r, z_1, \ldots, z_s) \in B_t$:

$$\begin{aligned}
V(r+1, s, t) &= \int_{\mathbb{R}} V(r, s, t - |y_0|) dy_0 \\
&= \int_{-t}^{t} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t - |y_0|)^n}{n!} dy_0 \\
&= 2^r \left(\frac{\pi}{2}\right)^s \frac{2}{n!} \int_0^t (t - y_0)^n dy_0 \\
&= 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!},
\end{aligned}$$

denn

$$\int_0^t (t - y_0)^n dy_0 = \frac{-(t - y_0)^{n+1}}{n+1}\Big|_0^t = \frac{t^{n+1}}{n+1}.$$

Für den zweiten Induktionsschritt $s \mapsto s + 1$ schreiben wir die neue Koordinate $z_0 \in \mathbb{C}$

in Polarkoordinaten $z_0 = \rho e^{i\theta}$, mit $d\mu(z_0) = \rho\, d\rho\, d\theta$ und erhalten

$$\begin{aligned} V(r, s+1, t) &= \int_{\mathbb{C}} V(r, s, t - 2|z_0|) d\mu(z_0) \\ &= \int_{|z_0| \le t/2} V(r, s, t - 2|z_0|) d\mu(z_0) \\ &= \int_0^{t/2} \int_0^{2\pi} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-2\rho)^n}{n!} \rho\, d\rho\, d\theta \\ &= 2^r \left(\frac{\pi}{2}\right)^s \frac{2\pi}{n!} \cdot \int_0^{t/2} (t-2\rho)^n \rho\, d\rho \\ &= 2^r \left(\frac{\pi}{2}\right)^{s+1} \frac{t^{n+2}}{(n+2)!}, \end{aligned}$$

denn mit der Substitution $2\rho = x$ und partieller Integration erhalten wir

$$\begin{aligned} \int_0^{t/2} (t-2\rho)^n \rho\, d\rho &= \frac{1}{4} \int_0^x (t-x)^n x\, dx \\ &= \frac{1}{4} \left(\frac{-(t-x)^{n+1}}{n+1} x \Big|_0^t - \int_0^x \frac{-(t-x)^{n+1}}{n+1} dx \right) \\ &= \frac{1}{4} \frac{t^{n+2}}{(n+1)(n+2)}. \end{aligned}$$

□

Korollar 4.2.6. *Jede Idealklasse in $Cl(K)$ enthält ein ganzes Ideal J von $\mathcal{O}_K$ mit*

$$N(J) \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

Beweis. Sei J' ein gebrochenes Ideal in K. Dann gibt es ein $d \in K^\times$, so daß $I = d(J')^{-1}$ ein ganzes Ideal von $\mathcal{O}_K$ ist, also $I = (d)(J')^{-1}$ und $I \sim (J')^{-1}$. Nach Theorem 4.2.5 gibt es ein $y \in I$, $y \neq 0$ mit $|N_{K/\mathbb{Q}}(y)| \le B_K N(I)$. Wegen $y\mathcal{O}_K \subseteq I$ gilt $(y) = JI$ für ein ganzes Ideal J mit $J \sim I^{-1} \sim J'$. Die Lemmata 3.3.2 und 3.3.3 implizieren $N(J)N(I) = N(JI) = N((y)) = |N_{K/\mathbb{Q}}(y)| \le B_K N(I)$. Kürzen mit $N(I)$ ergibt $N(J) \le B_K$. □

Korollar 4.2.7 (Dirichlet)**.** *Die Idealklassengruppe $Cl(K)$ eines Zahlkörpers K ist endlich.*

Beweis. Jede Idealklasse von K enthält ein ganzes Ideal J mit $N(J) \le B_K$ nach Korollar 4.2.6. Es gibt aber nur endlich viele solche Ideale mit beschränkter Norm: ist $N(J) = \#\mathcal{O}_K/J = q$ für ein festes q, so folgt $q \in J$. Die Ideale J von $\mathcal{O}_K$ mit $q \in J$ entrpechen aber den Idealen des endlichen Ringes $\mathcal{O}_K/(q)$, der natürlich nur endlich viele Ideale hat. □

Beispiel 4.2.8. *Die Idealklassengruppe von $K = \mathbb{Q}(i)$ ist trivial.*

Wir haben $(r,s) = (0,1)$, also $n = 2$. Es gilt $d_K = -4$, siehe Beispiel 2.4.15. Daher ist die Minkowski-Schranke $B_K = 4/\pi < 2$, $N(J) \leq B_K < 2$, also $N(J) = 1$. Also ist jedes gebrochene Ideal I äquivalent zu einem ganzen Ideal J der Norm 1, also zu $J = \mathbb{Z}[i]$, dem trivialen Element von $Cl(K)$. Denn nur $\mathbb{Z}[i]$ kann Norm 1 haben. Somit ist die Gruppe $Cl(K)$ trivial.
Natürlich hätten wir das auch anders sehen können, indem wir elementar nachrechnen, daß $\mathbb{Z}[i]$ mit der Norm $N(z) = z\overline{z}$ ein Euklidischer Ring ist, und daher auch ein Hauptidealring.

Beispiel 4.2.9. *Die Idealklassengruppe von $K = \mathbb{Q}(\sqrt{-5})$ ist isomorph zu $\mathbb{Z}/2$.*

Wir haben $(r,s) = (0,1)$, also $n = 2$. Es gilt $d_K = -20$, siehe Beispiel 2.4.15. Daher ist jedes gebrochene Ideal I äquivalent zu einem ganzen Ideal J mit $N(J) \leq \frac{4}{\pi}\sqrt{5} < 3$, also mit $N(J) = 1$ oder $N(J) = 2$. Im ersten Fall ist $J = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, welches das triviale Element in $Cl(K)$ repräsentiert. Ideale der Norm 2 entsprechen den Idealen von $\mathcal{O}_K/(2)$ mit $(2) = P^2$, wobei $P = (2, 1+\sqrt{-5})$ das eindeutige Primideal der Norm 2 ist: $N(P)N(P) = N(P^2) = N(2) = 4$, also $N(P) = 2$. Also gilt $Cl(K) =< P >$ und P hat höchstens Ordnung 2, da $P^2 \sim \mathcal{O}_K$. P kann nicht Ordnung 1 haben, weil $\mathcal{O}_K$ kein Hauptidealring ist, bzw. weil P kein Hauptideal ist.

Korollar 4.2.10. *Sei K ein Zahlkörper vom Grad $n \geq 2$ mit Diskriminante d_K. Dann gilt*

$$|d_K| \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2s} \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Insbesondere gilt

$$\frac{n}{\log(|d_K|)} < 1.17.$$

Beweis. Für das Ideal $J = \mathcal{O}_K$ gilt nach Korollar 4.2.6

$$1 = N(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

Das bedeutet genau

$$\sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

Durch Quadrieren erhält man die erste Abschätzung. Wegen $2s \leq n$ und $\pi/4 < 1$ kann man $\left(\frac{\pi}{4}\right)^{2s} \geq \left(\frac{\pi}{4}\right)^n$ folgern, wodurch die Abschätzung nur noch von n abhängt. Wir erhalten also $|d_K| \geq a_n$ mit

$$a_n := \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

Die Folge beginnt mit $a_2 = \frac{\pi^2}{4}$, $a_3 = \frac{81\pi^3}{256}$, und erfüllt

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \cdot \frac{(n+1)^2(n+1)^{2n}(n!)^2}{((n+1)!)^2 n^{2n}} \\ &= \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \\ &\geq \frac{3\pi}{4},\end{aligned}$$

da ja $(1+1/n)^{2n} = 1 + 2+$ positive Terme nach der binomischen Formel ist. Nun folgt $a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ leicht mit Induktion über $n \geq 2$. Damit ist $|d_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ gezeigt. Logarithmieren ergibt

$$1.166796 \sim \frac{1}{\log(3\pi/4)} \geq \frac{n}{\log(|d_K|)}.$$

□

Beispiel 4.2.11. *Für imaginär-quadratische Zahlkörper K gilt $|d_K| \geq 3$, und die Schranke wird angenommen für $K = \mathbb{Q}(\sqrt{-3})$.*

In der Tat, beide Abschätzungen in Korollar 4.2.10 ergeben $|d_K| \geq \frac{\pi^2}{4} > 2$, da ja $s = 1$ und $n = 2$ ist.

Beispiel 4.2.12. *Für reell-quadratische Zahlkörper K gilt $|d_K| \geq 4$, und der kleinste Wert ist $|d_K| = 5$, für $K = \mathbb{Q}(\sqrt{5})$.*

Diesmal ist die erste Abschätzung in Korollar 4.2.10 besser, wegen $s = 0$. Man erhält $|d_K| \geq 4$. Die Gleichheit ist natürlich unmöglich, wie wir aus den Formeln von Beispiel 2.4.15 ersehen können.

Satz 4.2.13 (Hermite-Minkowski)**.** *Sei K ein Zahlkörper ungleich $\mathbb{Q}$. Dann gilt $|d_K| > 1$.*

Beweis. Es gilt $|d_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$ für $n \geq 2$ nach Korollar 4.2.10. □

Satz 4.2.14 (Hermite)**.** *Für jedes $d \in \mathbb{Z}$ gibt es nur endlich viele Zahlkörper K mit $d_K = d$.*

Beweis. Nach Korollar 4.2.10 gilt $[K : \mathbb{Q}] = n \leq C \cdot \log(d)$ für eine Konstante $C > 0$. Somit ist der Grad solcher Zahlkörper beschränkt. Es genügt also zu zeigen, daß es nur endlich viele Zahlkörper zu fest gegebenen Zahlen d, r, s gibt. Für $r > 0$ sei B die Menge der Vektoren $(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$ mit

$$\begin{aligned}|y_1| &\leq 2^n \left(\frac{\pi}{2}\right)^{-s} \sqrt{|d|}, \\ |y_i| &\leq \frac{1}{2},\ i = 2, \ldots, r, \\ |z_j| &\leq \frac{1}{2},\ j = 1, \ldots, s.\end{aligned}$$

Für $r = 0$ sei B die Menge der Vektoren $(z_1, \ldots, z_s) \in \mathbb{C}^s$ mit

$$|z_1 - \overline{z_1}| \leq 2^n \left(\frac{\pi}{2}\right)^{1-s} \sqrt{|d|}, \quad |z_1 + \overline{z_1}| \leq \frac{1}{2},$$
$$|z_j| \leq \frac{1}{2},\ j = 2, \ldots, s.$$

Dann ist B konvex, kompakt, zentralsymmetrisch und hat Volumen

$$\mathrm{vol}(B) = 2^{n-s}\sqrt{|d|} = 2^n \mathrm{vol}(\sigma(\mathcal{O}_K))$$

nach Korollar 4.2.3. Deshalb können wir den Gitterpunktsatz von Minkowski anwenden und erhalten ein Element $0 \neq x \in \mathcal{O}_K$ mit $\sigma(x) \in B$. Wir behaupten nun, daß $K = \mathbb{Q}(x)$ gilt, und daß es nur endlich viele solche x geben kann. Damit gibt es dann auch nur endlich viele solche Zahlkörper $K = \mathbb{Q}(x)$. Für $r > 0$ ist nach Voraussetzung $|\sigma_i(x)| \leq 1/2$ für $i \neq 1$. Wegen

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} |\sigma_i(x)| \geq 1$$

folgt $|\sigma_1(x)| \geq 1$, und somit $\sigma_1(x) \neq \sigma_i(x)$ für $i \neq 1$. Angenommen K wäre nicht in $\mathbb{Q}(x)$ enthalten. Dann besitzt $\sigma_1 \mid_{\mathbb{Q}(x)} \mathbb{Q}(x) \to \mathbb{C}$ eine von σ_1 verschiedene Fortsetzung σ auf K, die wieder eine der Einbettungen $\sigma_1, \ldots, \sigma_n$ sein muß. Das ist aber unmöglich. Also gilt $K = \mathbb{Q}(x)$.
Für $r = 0$ sieht man analog $|\sigma_1(x)| = \overline{|\sigma_1(x)|} \geq 1$ und daher $\sigma_1(x) \neq \sigma_j(x)$, außer für $\sigma_j = \sigma_1$ oder $\sigma_j = \overline{\sigma_1}$. Aus der Definition von B folgt aber $\Re(\sigma_1(x)) \leq 1/4$. Damit kann σ_1 nicht reell sein, d.h., es gilt $\sigma_1(x) \neq \overline{\sigma_1(x)}$. Wie vorher folgt $K = \mathbb{Q}(x)$.
In beiden Fällen sind die Konjugierten $|\sigma_i(x)|$ von x beschränkt. Daher hat auch das Minimalpoynom $m(x)(t) \in \mathbb{Z}[t]$ vom Grad n beschränkte Koeffizienten. Da es überhaupt nur endlich viele Polynome $f \in \mathbb{Z}[t]$ vom Grad n mit beschränkten Koeffizienten gibt, hat man auch nur endlich viele mögliche x, bzw. Zahlkörper $K = \mathbb{Q}(x)$. □

4.3 Klassenzahl 1

Die Zahlkörper K mit Klassenzahl $h_K = 1$ sind genau diejenigen, für die der Ganzzahlring $\mathcal{O}_K$ ein Hauptidealring ist. Es ist naheliegend zu fragen, ob man die Zahlkörper mit Klassenzahl 1 bestimmen oder beschreiben kann. Leider ist das bisher nicht möglich. Es ist noch nicht einmal bekannt, ob es nur endlich viele, oder unendlich viele Zahlkörper mit Klassenzahl 1 gibt. Für quadratische Zahlkörper gibt es immerhin einige Antworten, allerdings vornehmlich im imaginär-quadratischen Fall. Wir wollen hier einige Resultate vorstellen.

Beispiel 4.3.1. *Jeder Zahlkörper K mit Minkowski-Schranke $B_K < 2$ hat Klassenzahl 1.*

In der Tat, das folgt wie in Beispiel 4.2.8. Wir können das für quadratische Zahlkörper näher anschauen. Ist $K = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$, so bedeutet $B_K < 2$ für

$d < 0$ gerade $|d_K| < \pi^2$, also $d = -1, -2, -3, -7$. Für $d > 0$ bedeutet es $|d_K| < 16$, also $d = 2, 3, 5, 13$. Also haben folgende Zahlkörper schon mal Klassenzahl 1:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{13}).$$

Allerdings gibt es auch andere quadratische Zahlkörper mit Klassenzahl 1, die nicht $B_K < 2$ erfüllen. Dann muß man noch mehr tun.

Für *imaginär-quadratische* Zahlkörper ist die Frage nach der Bestimmung der Klassenzahl 1 Fälle gelöst, siehe 2.2.5:

Satz 4.3.2 (Baker, Stark 1967)**.** *Es gibt genau* 9 *imaginär-quadratische Zahlkörper* $K = \mathbb{Q}(\sqrt{d})$ *mit Klassenzahl* 1 *für quadratfreies* $d < 0$*, nämlich für*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Man beachte, daß es relativ leicht ist zu überprüfen, daß die Klassenzahl der genannten Zahlkörper tatsächlich 1 ist. Die Schwierigkeit besteht darin zu zeigen, daß es keine weiteren Fälle geben kann. In den ersten fünf Fällen ist der Ganzzahlring $\mathcal{O}_K$ sogar Euklidisch, in den letzten vier Fällen dagegen nicht.

Auch für Klassenzahlen $h > 1$ gibt es solche Resultate. Die Klassifikation im Fall $h = 2$ ist wie folgt:

Satz 4.3.3 (Baker 1971)**.** *Es gibt genau* 18 *imaginär-quadratische Zahlkörper* $K = \mathbb{Q}(\sqrt{d})$ *mit Klassenzahl* 2 *für quadratfreies* $d < 0$*, nämlich für*

$$\begin{aligned} d = &-5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, \\ &-123, -187, -235, -267, -403, -427. \end{aligned}$$

Die Liste ist für jede Klassenzahl immer endlich:

Satz 4.3.4 (Heilbronn 1934)**.** *Zu jeder natürlichen Zahl* $h \geq 1$ *gibt es nur endlich viele imaginär-quadratische Zahlkörper* $K = \mathbb{Q}(\sqrt{d})$ *mit Klassenzahl* h*.*

Entsprechende Klassifikationsresultate gibt es mindestens für $1 \leq h \leq 100$. Die Anzahl der imaginär-quadratischen Zahlkörper mit $1 \leq h \leq 100$ ist, nach Mark Watkins, wie folgt:

h	#	h	#	h	#	h	#	h	#	h	#	h	#
1	9	16	322	31	73	46	268	61	132	76	1075	91	214
2	18	17	45	32	708	47	107	62	323	77	216	92	1248
3	16	18	150	33	101	48	1365	63	216	78	561	93	262
4	54	19	47	34	219	49	132	64	1672	79	175	94	509
5	25	20	350	35	103	50	345	65	164	80	2277	95	241
6	51	21	85	36	668	51	159	66	530	81	228	96	3283
7	31	22	139	37	85	52	770	67	120	82	402	97	185
8	131	23	68	38	237	53	114	68	976	83	150	98	580
9	34	24	511	39	115	54	427	69	209	84	1715	99	289
10	87	25	95	40	912	55	163	70	560	85	221	100	1736
11	41	26	190	41	109	56	1205	71	150	86	472		
12	206	27	93	42	339	57	179	72	1930	87	222		
13	37	28	457	43	106	58	291	73	119	88	1905		
14	95	29	83	44	691	59	128	74	407	89	192		
15	68	30	255	45	154	60	1302	75	237	90	801		

Mit der sogenannten *analytischen Klassenzahlformel* von Dirichlet kann man die Klassenzahl quadratischer Zahlkörper berechnen. Es gibt in diesem Fall auch Algorithmen, mit denen man ein Repräsentantensystem der Idealklassengruppe bestimmen kann. Im imaginär-quadratischen Fall haben wir folgendes Resultat.

Satz 4.3.5. *Sei K ein imaginär-quadratischer Zahlkörper mit Diskriminante d_K. Ein vollständiges Repräsentantensystem der Idealklassengruppe ist gegeben durch die Ideale*

$$I = a\mathbb{Z} + \frac{b+\sqrt{d_K}}{2}\mathbb{Z}$$

für $a, b \in \mathbb{Z}$ mit

$$\begin{aligned} a &\geq 1, \\ 4a &\mid d_k - b^2, \\ |b| &\leq a, \\ 4a^2 &\leq b^2 - d_K, \end{aligned}$$

wobei im Fall der Gleichheit $|b| = a$ oder $4a^2 = b^2 - d_K$ zusätzlich $b \geq 0$ gelten muß.

Aus diesem Satz folgt erneut, daß die Klassenzahl von $\mathbb{Q}(\sqrt{-d})$ endlich ist. Denn aus $|b| \leq a$ und $4a^2 \leq b^2 - d_K$ folgt $3a^2 \leq -d_K = |d_K|$, weswegen nur endlich viele Werte für a möglich sind. Wegen $|b| \leq a$ gibt es also nur endlich viele Paare (a, b), die den Bedingungen des Satzes genügen.

Beispiel 4.3.6. *Die Klassenzahl von $K = \mathbb{Q}(\sqrt{-67})$ ist gleich* 1.

Es ist $d_K = -67$. Aus $3a^2 \leq -d_K = 67$ folgt $a \leq 4$. Wegen $|b| \leq a \leq 4$ und $4 \mid d_k - b^2$ gilt $|b| = 1$ oder 3. Für $|b| = 1$ hat man $4a \mid d_k - 1^2 = -68$, also $a \mid 17$. Wegen $a \leq 4$

folgt $a = 1$. Für $|b| = 3$ erhält man $4a \mid d_k - 3^2 = -76$, also $a \mid 19$, also $a = 1$ und $3 = |b| \leq a = 1$, ein Widerspruch. Da nun $a = |b| = 1$ ist, also Gleichheit gilt, folgt $a = b = 1$. Damit gibt es nur eine Klasse in $Cl(K)$, nämlich

$$\mathbb{Z} + \frac{1+\sqrt{-67}}{2}\mathbb{Z} = \mathcal{O}_K.$$

Im *reell-quadratischen* Fall ergibt eine Berechnung, die man mit zahlentheoretischen Computeralgebrasystemen machen kann, folgende Tabelle von quadratfreien Zahlen $0 < d < 1000$ mit Klassenzahl $h_{\mathbb{Q}(\sqrt{d})} = 1$:

```
1,2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,
43,46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,
97,101,103,107,109,113,118,127,129,131,133,134,137,139,
141,149,151,157,158,161,163,166,167,173,177,179,181,191,
193,197,199,201,206,209,211,213,214,217,227,233,237,239,
241,249,251,253,262,263,269,271,277,278,281,283,293,301,
302,307,309,311,313,317,329,331,334,337,341,347,349,353,
358,367,373,379,381,382,383,389,393,397,398,409,413,417,
419,421,422,431,433,437,446,449,453,454,457,461,463,467,
478,479,487,489,491,497,501,502,503,509,517,521,523,526,
537,541,542,547,553,557,563,566,569,571,573,581,587,589,
593,597,599,601,607,613,614,617,619,622,631,633,641,643,
647,649,653,661,662,669,673,677,681,683,691,694,701,709,
713,717,718,719,721,734,737,739,743,749,751,753,757,758,
766,769,773,781,787,789,797,809,811,813,821,823,827,829,
838,849,853,857,859,862,863,869,877,878,881,883,886,887,
889,893,907,911,913,917,919,921,926,929,933,937,941,947,
953,958,967,971,973,974,977,983,989,991,997,998.
```

Wir vermuten, wie vor uns schon Gauß, daß es wohl unendlich viele reell-quadratische Zahlkörper mit Klassenzahl 1 gibt. Doch das ist bis heute nicht bewiesen.

Zuletzt wollen wir noch auf das Klassenzahl-Problem für zyklotomische Zahlkörper $K = \mathbb{Q}(\zeta_n)$ eingehen. Mit Teilbarkeitsargumenten kann man zeigen, daß $x^n + y^n = z^n$ für $n > 2$ keine nicht-trivialen ganzzahligen Lösungen hat, wenn die Klassenzahl von $\mathbb{Q}(\zeta_n)$ gleich 1 ist. Leider trifft letzteres nur sehr selten zu, wie folgendes Resultat zeigt, siehe [9]

Satz 4.3.7 (Montgomery, Masley 1976)**.** *Sei* $n \not\equiv 2 \mod 4$. *Die Klassenzahl von* $\mathbb{Q}(\zeta_n)$ *ist gleich* 1 *genau für*

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28,$$
$$32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

Für $n \equiv 2 \mod 4$ *ist die Klassenzahl von* $\mathbb{Q}(\zeta_n)$ *ist gleich* 1 *genau für*

$$n = 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 50, 54, 66, 70, 90.$$

Im zweiten Fall ist n gerade, und daher gilt $\mathbb{Q}(\zeta_{n/2}) = \mathbb{Q}(\zeta_n)$. Für $n = p$ Primzahl die Klassenzahl von $\mathbb{Q}(\zeta_p)$ gleich 1 nach dem Satz genau dann, wenn $p \leq 19$.

Bemerkung 4.3.8. Eine Primzahl p heißt *regulär*, wenn sie nicht die Klassenzahl von $Q(\zeta_p)$ teilt. Diese Primzahlen sind sehr wichtig, weil man für sie auch Fermats letzten Satz leicht mit Teilbarkeitsargumenten zeigen kann. Leider sind nicht alle Primzahlen regulär. Es gibt unendlich viele irreguläre Primzahlen. Das wurde 1915 von K.L. Jensen bewiesen. Er zeigte sogar, daß es unendlich viele irreguläre Primzahlen der Form $4n+3$ gibt. Die irregulären Primzahlen bis 2017 (2013 is keine Primzahl) sind

```
37,59,67,101,103,131,149,157,233,257,263,271,283,293,
307,311,347,353,379,389,401,409,421,433,461,463,467,
491,523, 541,547,557,577,587,593,607,613,617,619,631,
647,653,659,673,677,683,691,727,751,757,761,773,797,
809,811,821,827,839,877,881,887,929,953,971,1061,1091,
1117,1129,1151,1153,1193,1201,1217,1229,1237,1279,
1283,1291,1297,1301,1307,1319,1327,1367,1381,1409,
1429,1439,1483,1499,1523,1559,1597,1609,1613,1619,
1621,1637,1663,1669,1721,1733,1753,1759,1777,1787,
1789,1811,1831,1847,1871,1877,1879,1889,1901,1933,
1951,1979,1987,1993,1997,2003,2017
```

Man vermutet, daß es auch unendlich viele reguläre Primzahlen gibt. Carl Ludwig Siegel vermutete 1964, daß $e^{-1/2}$, oder etwa 60.65% aller Primzahlen regulär sind, asymptotisch gesehen bezüglich der natürlichen Dichte. Allerdings sind diese Vermutungen noch beide offen.
Kummers Kriterium besagt, daß eine Primzahl p genau dann irregulär ist, wenn sie den Nenner einer Bernoulli-Zahl B_k teilt, für $k = 2, 4, 6, \ldots, p-3$. Hierbei ist $B_k = -k\zeta(1-k)$ für $k = 2, 4, 6, \ldots$, und $B_{2k+1} = 0$. Man hat

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Die folgende Tabelle zeigt, daß $p = 37, 59, 67, 101, 103, 131$ irregulär sind:

p	$h_{\mathbb{Q}(\zeta_p)}$
37	37
59	$41241 = 3 \cdot 59 \cdot 233$
67	$853513 = 67 \cdot 12739$
101	$3547404378125 = 5 \cdot 101 \cdot 601 \cdot 18701$
103	$9069094643165 = 5 \cdot 103 \cdot 1021 \cdot 17247691$
131	$28496379729272136525 = 3^3 \cdot 5^2 \cdot 53 \cdot 131 \cdot 1301 \cdot 4673706701$

Für $p \leq 19$ gilt, wie gesagt, $h_{\mathbb{Q}(\zeta_p)} = 1$. Überhaupt gilt $h_{\mathbb{Q}(\zeta_n)} = 1$ für alle $n \leq 22$. Hier sind die Klassenzahlen $h_{\mathbb{Q}(\zeta_p)}$ für alle Primzahlen $p < 150$. Offensichtlich wachsen die Klassenzahlen von $\mathbb{Q}(\zeta_p)$ mit p rapide an.

p	$h_{\mathbb{Q}(\zeta_p)}$
2	1
3	1
5	1
7	1
11	1
13	1
17	1
19	1
23	3
29	8
31	9
37	37
41	121
43	211
47	695
53	4889
59	41241
61	76301
67	853513
71	3882809
73	11957417
79	100146415
83	838216959
89	13379363737
97	411322824001
101	3547404378125
103	9069094643165
107	63434933542623
109	161784800122409
113	1612072001362952
127	2604529186263992195
131	28496379729272136525
137	646901570175200968153
139	1753848916484925681747
149	687887859687174720123201

5 Dirichlets Einheitensatz

In diesem Kapitel werden wir Dirichlets Einheitensatz beweisen, der ein Strukturtheorem für die Einheitengruppe des Ganzzahlrings $\mathcal{O}_K$ eines Zahlkörpers K ist. Das Ergebnis ist bemerkenswert einfach. Hat K r reelle Einbettungen und s Paare komplexer Einbettungen, so gilt

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times T,$$

wobei T eine endliche zyklische Gruppe ist. Für den Beweis können wir wieder Minkowski-Theorie anwenden.
Jede endlich-erzeugte abelsche Gruppe A ist ja von der Form $A \simeq \mathbb{Z}^t \times A_{\text{tors}}$, wobei $t \geq 0$ der *Rang* von A heißt, und A_{tors} die endliche Untergruppe der Torsionselemente ist.
Viele Fragen der Zahlentheorie können auf die Struktur der Einheitengruppe zurückgeführt werden - wie etwa die Frage nach ganzzahligen Lösungen der Pellschen Gleichung $x^2 - dy^2 = 1$.

5.1 Die Einheitengruppe

Die Einheitengruppe $A^\times$ eines Ringes A besteht aus den invertierbaren Elementen von A. Mit anderen Worten, a ist eine Einheit, falls es ein b gibt mit $ab = 1$.

Definition 5.1. Die Einheitengruppe eines *Zahlkörpers* K ist $\mathcal{O}_K^\times$, die Einheitengruppe seines Ganzzahlringes.

Beispiel 5.1.1. *Für $K = \mathbb{Q}(\sqrt{3})$ ist $x = 2 + \sqrt{3}$ eine Einheit in $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ mit Inversem $2 - \sqrt{3}$. Dagegen ist $y = 1 + \sqrt{3}$ keine Einheit. Es gilt $\mathcal{O}_K^\times = \{\pm(2+\sqrt{3})^k \mid k \in \mathbb{Z}\}$ nach dem Einheitensatz von Dirichlet.*

Wegen $(2+\sqrt{3})(2-\sqrt{3}) = 1$ ist $2+\sqrt{3}$ eine Einheit, während $(1+\sqrt{3})(a+b\sqrt{3}) = 1$ keine ganzzahlige Lösung hat. Wegen $N(1+\sqrt{3}) = -2$ folgt das auch aus dem nächsten Lemma.

Lemma 5.1.2. *Ein $x \in K$ ist genau dann eine Einheit, wenn x ganz ist, und $N(x) = \pm 1$ gilt.*

Beweis. Ist x eine Einheit, so ist

$$1 = N(1) = N(xx^{-1}) = N(x)N(x)^{-1}.$$

Wegen $N(x) \in \mathbb{Z}$ folgt $N(x) = \pm 1$. Sei umgekehrt $x \in \mathcal{O}_K$ mit $N(x) = \pm 1$ gegeben. Für das charakteristische Polynom von x gilt

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

mit $n = [K : \mathbb{Q}]$, $a_{n-1} = -\mathrm{tr}_{K/\mathbb{Q}}(x)$ und $a_0 = (-1)^n N_{K/\mathbb{Q}}(x) = \pm 1$, siehe die Bemerkung nach Definition 2.7. Also gilt

$$\pm x(x^{n-1} + \cdots + a_1) = 1.$$

Damit ist x eine Einheit. □

Die Torsionsuntergruppe von $\mathcal{O}_K^\times$ ist genau die Gruppe der in K enthaltenen Einheitswurzeln. Wir bezeichnen sie mit μ_K. Für imaginär-quadratische Zahlkörper können wir Dirichlets Einheitensatz sofort beweisen.

Lemma 5.1.3. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein imaginär-quadratischer Zahlkörper mit quadratfreiem $d < 0$. Dann gilt $\mathcal{O}_K^\times = \mu_K$, und diese endliche zyklische Gruppe ist wie folgt gegeben:*

$$\mu_K = \begin{cases} \mathbb{Z}/4 = \{\pm 1, \pm i\} & \text{falls } d = -1, \\ \mathbb{Z}/6 = \{\pm 1, \pm \zeta, \pm \zeta^2\} & \text{falls } d = -3, \\ \mathbb{Z}/2 = \{\pm 1\} & \text{sonst.} \end{cases}$$

Insbesondere gilt immer $\mathcal{O}_K^\times = \{\pm 1\}$, außer für $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{-3})$.

Beweis. Ein $x = a + b\sqrt{d}$ ist genau dann eine Einheit in $\mathcal{O}_K$, wenn $N(x) = \pm 1$ ist. Für $d \not\equiv 1 \mod 4$ ist $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ und deshalb die Normbedingung äquivalent zu der Diophantischen Gleichung

$$a^2 - b^2 d = \pm 1.$$

Für $d \equiv 1 \mod 4$ ist $\mathcal{O}_K = \{a + b(1 + \sqrt{d})/2 \mid a, b \in \mathbb{Z}\}$ und deshalb x genau dann eine Einheit wenn

$$(2a + b)^2 - b^2 d = \pm 4.$$

Für $d < 0$ haben diese Gleichungen in beiden Fällen nur endlich viele ganzzahlige Lösungen. Deshalb folgt schon $\mathcal{O}_K^\times = \mu_K$. Eine primitive m-te Einheitswurzel liegt genau dann in K, wenn $\mathbb{Q}(\zeta_m) \subseteq K$ gilt. Dann hat man $\varphi(m) \mid [K : \mathbb{Q}] = 2$, also $m \mid 4$ oder $m \mid 6$. Daraus folgt das Resultat. Wir können natürlich auch direkt nachrechnen, welche Lösungen die Gleichungen haben. Für $d \leq -2$ folgt aus $a^2 - b^2 d = \pm 1$ etwa sofort $b = 0$ und $a = \pm 1$. Für $d = -1$ erhält man zusätzlich noch $a = 0$ und $b = \pm 1$. Die Lösungen der zweiten Gleichung bestimmt man ebenso. Für $d \leq -7$ folgt $b = 0$ und $a = \pm 1$. Beachte, daß $d = -5$ nicht kongruent $1 \mod 4$ ist. Für $d = -3$ hat man zusätzlich noch die Lösungen $b = \pm 1$ und $(2a \pm 1)^2 = 1$, also insgesamt 6 Lösungen

$$(a, b) = (\pm 1, 0),\ (0, \pm 1),\ (1, -1),\ (-1, 1).$$

□

Bemerkung 5.1.4. Im reell-quadratischen Fall haben die beiden Normgleichungen nicht nur endlich viele Lösungen. Wir können die Lösungen also nicht so einfach bestimmen. Die Einheitengruppe μ_K dagegen ist immer $\{\pm 1\}$, da die Einheitswurzeln dann ja reell sein müssen. Die Struktur der Einheitengruppe ist in diesem Fall nach dem Satz von Dirichlet wie folgt:

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times \mu_K \simeq \mathbb{Z} \times \{\pm 1\}.$$

Theorem 5.1.5 (Dirichlet). *Die Gruppe der Einheiten $\mathcal{O}_K^\times$ eines Zahlkörpers K ist isomorph zu*

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times \mu_K,$$

wobei μ_K eine endliche zyklische Gruppe ist.

Beweis. Wir betrachten die logarithmische Einbettung

$$L\colon K^\times \to \mathbb{R}^{r+s},\ x \mapsto (\log(|\sigma_1(x)|), \ldots, \log(|\sigma_{r+s}(x)|)),$$

die die Zusammensetzung der kanonischen Einbettung $\sigma\colon K^\times \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ mit der multiplikativen Betragsfunktion und dem Logarithmus ist. Offensichtlich ist L ein Gruppenhomomorphismus, erfüllt also $L(xy) = L(x) + L(y)$. Bei der Betragsfunktion geht die Injektivität verloren. Daher ist der Kern von L nicht-trivial. Es gilt $\ker(L_{|\mathcal{O}_K^\times}) \simeq \mu_K$. Um das einzusehen, sei $B \subseteq \mathbb{R}^{r+s}$ eine kompakte Teilmenge und $B_L = L^{-1}(B) \cap \mathcal{O}_K^\times$. Da B beschränkt ist, müssen auch die Beträge $|\sigma_i(x)|$ für $x \in B_L$ beschränkt sein. Damit sind die Koeffizienten des charakteristischen Polynoms von x beschränkt. Da sie ganzzahlig sind, gibt es nur endlich viele solche x, und B_L ist eine endliche Menge. Also ist $\ker(L_{|\mathcal{O}_K^\times})$ eine endliche Untergruppe von $\mathcal{O}_K^\times$, und daher eine zyklische Gruppe von Einheitswurzeln, also mit $\ker(L_{|\mathcal{O}_K^\times}) \subseteq \mu_K$. Da für Einheitswurzeln ζ_m aber $|\sigma_i(\zeta_m)|^m = |\sigma_i(\zeta_m^m)| = 1$ gilt, folgt $\log(\sigma_i(\zeta_m)) = 0$ und $\ker(L_{|\mathcal{O}_K^\times}) = \mu_K$.
Da B_L endlich ist, muß das Bild $L(\mathcal{O}_K^\times)$ eine diskrete Untergruppe von $\mathbb{R}^{r+s}$ sein. Insbesondere ist $L(\mathcal{O}_K^\times)$ eine freier $\mathbb{Z}$-Modul vom Rang $t \leq r+s$ und

$$\mathcal{O}_K^\times \simeq L(\mathcal{O}_K^\times) \times \mu_K.$$

Es bleibt noch zu zeigen, daß $t = r+s-1$ gilt. Die Ungleichung $t \leq r+s-1$ ist leicht zu zeigen. In der Tat, $L(\mathcal{O}_K^\times)$ liegt in der Hyperebene

$$H := \left\{ (y_1, \ldots, y_{r+s}) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r} y_i + 2 \sum_{j=r+1}^{r+s} y_j = 0 \right\}$$

der Kodimension 1: für $x \in \mathcal{O}_K^\times$ gilt immer

$$\pm 1 = N(x) = \left(\prod_{i=1}^{r} \sigma_i(x) \right) \cdot \left(\prod_{j=r+1}^{r+s} \sigma_j(x)\overline{\sigma_j(x)} \right).$$

Betrag nehmen und Logarithmieren ergibt die Behauptung.
Die zweite Ungleichung $t \geq r+s-1$ ist etwas schwieriger zu zeigen. Wir müssen $L(\mathcal{O}_K^\times) = H$ beweisen. Mit anderen Worten, jede Linearform, die auf $L(\mathcal{O}_K^\times)$ verschwindet, muß auch auf H verschwinden. Das bedeutet wiederum, daß wir für jede von Null verschiedene $\mathbb{R}$-lineare Abbildung $f\colon H \to \mathbb{R}$ eine Einheit $u \in \mathcal{O}_K^\times$ finden müssen mit $f(L(u)) \neq 0$. Wir identifizieren ein $(y_1, \ldots, y_{r+s}) \in H$ mit $(y_1, \ldots, y_{r+s-1}) \in \mathbb{R}^{r+s-1}$. Damit schreiben wir

$$f(y_1, \ldots, y_{r+s-1}) = c_1 y_1 + \cdots + c_{r+s-1} y_{r+s-1}$$

mit $c_i \in \mathbb{R}$. Für ein gegebenes Tupel positiver reeller Zahlen

$$\lambda = (\lambda_1, \ldots, \lambda_{r+s})$$

mit

$$\alpha := \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 \geq 2^n (2\pi)^{-s} \sqrt{|d_K|}$$

definieren wir eine kompakte, konvexe und zentralsymmetrische Menge

$$B_\lambda = \{y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \leq \lambda_i,\ |z_j| \leq \lambda_{j+r}\}.$$

Sie hat das Volumen

$$\begin{aligned} \mathrm{vol}(B_\lambda) &= \left(\prod_{i=1}^{r} 2\lambda_i \right) \cdot \left(\prod_{j=r+1}^{r+s} \pi \lambda_j^2 \right) \\ &= 2^r \pi^s \alpha \\ &\geq 2^{n-s} \sqrt{|d_K|}. \end{aligned}$$

Aus dem Gitterpunktsatz von Minkowski und Korollar 4.2.3 folgt, daß es ein $x_\lambda \in \mathcal{O}_K$ gibt mit $\sigma(x_\lambda) \in B_\lambda$. Es gilt $|\sigma_i(x_\lambda)| \leq \lambda_i$ für die reellen Einbettungen, aber auch für die Paare komplexer Einbettungen wegen $|\sigma_j(x_\lambda)\sigma_{j+1}(x_\lambda)| = |\sigma_j(x_\lambda)\overline{\sigma_j(x_\lambda)}| = |\sigma_j(x_\lambda)|^2 \leq \lambda_j^2$. Wir erhalten

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 = \alpha$$

und deshalb

$$|\sigma_i(x_\lambda)| = |N_{K/\mathbb{Q}}(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \frac{\lambda_i}{\alpha}.$$

Zusammen haben wir

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i,$$

und Logarithmieren ergibt

$$0 \leq \log(\lambda_i) - \log(|\sigma_i(x_\lambda)|) \leq \log(\alpha).$$

Für unser $f \in \mathrm{Hom}(H, \mathbb{R})$ folgt nun

$$\begin{aligned} \left| f(L(x_\lambda)) - \sum_{i=1}^{r+s-1} c_i \log(\lambda_i) \right| &\leq \left| \sum_{i=1}^{r+s-1} c_i \big(\log(|\sigma_i(x_\lambda)|) - \log(\lambda_i) \big) \right| \\ &\leq \left(\sum_{i=1}^{r+s-1} |c_i| \right) \log(\alpha). \end{aligned}$$

Sei nun $\beta \geq \left(\sum_{i=1}^{r+s-1}|c_i|\right)\log(\alpha)$. Für $h \in \mathbb{N}$ seien positive Zahlen $\lambda_{i,h}$ für i=1,...,$r+s-1$ so gewählt, daß

$$\sum_{i=1}^{r+s-1} c_i \log(\lambda_{i,h}) = 2\beta h$$

gilt, und $\lambda_{r+s,h} > 0$ so gewählt, daß

$$\prod_{i=1}^{r} \lambda_{i,h} \prod_{j=r+1}^{r+s} \lambda_{j,h}^2 = \alpha.$$

Mit $\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r+s,h})$ und $x_h := x_{\lambda(h)}$ gilt nach obiger Abschätzung für f also

$$|f(L(x_h)) - 2\beta h| < \beta,$$

und deshalb

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta.$$

Dann ist $\beta < f(L(x_1)) < 3\beta < f(L(x_2)) < 5\beta < f(L(x_3)) < \cdots$, also alle Werte $f(L(x_h))$ paarweise verschieden für $h \in \mathbb{N}$. Betrachten wir nun die Hauptideale $(x_h) \subseteq \mathcal{O}_K$. Wegen $|N((x_h))| \leq \alpha$ gibt es nur endlich viele verschiedene Ideale der Form (x_h), siehe Beweis von Korollar 4.2.7. Also gibt es verschiedene natürliche Zahlen h_1 und h_2 mit $(x_{h_1}) = (x_{h_2})$. Damit ist $(x_{h_1}^{-1}x_{h_2}) = \mathcal{O}_K$, und somit $u = x_{h_1}^{-1}x_{h_2}$ eine Einheit. Es folgt $f(L(u)) = f(L(x_{h_2})) - f(L(x_{h_1})) \neq 0$, was zu zeigen war. □

Bemerkung 5.1.6. Wir haben eine exakte Sequenz von abelschen Gruppen

$$0 \to \mu_K \to \mathcal{O}_K^\times \to L(\mathcal{O}_K^\times) \to 0$$

mit $L(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{r+s-1}$. Wählen wir eine $\mathbb{Z}$-Basis $\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_{r+s-1}}$ von $L(\mathcal{O}_K^\times)$, dann nennt man die Urbilder $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ ein *System von Grundeinheiten*. Jede Einheit $\varepsilon \in \mathcal{O}_K$ hat dann eine eindeutige Darstellung

$$\varepsilon = \zeta \cdot \varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$$

mit einer Einheitswurzel ζ in K und $n_i \in \mathbb{Z}$.

Beispiel 5.1.7. *Für reell-quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ ist $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}$, und jede Einheit hat die Form $\pm\varepsilon^k$ für eine Einheit ε und $k \in \mathbb{Z}$.*

Mit ε sind auch $\pm\varepsilon^{\pm 1}$ Grundeinheiten. Fixiert man eine Einbettung

$$\sigma\colon K \hookrightarrow \mathbb{R},$$

so gibt es genau eine Grundeinheit ε mit $\sigma(\varepsilon) > 0$. Dieses ε nennt man dann die *fundamentale* Einheit von K. Sei $d \not\equiv 1 \mod 4$. Dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ und die Einheiten in $\mathcal{O}_K^\times$ sind die Zahlen $a + b\sqrt{d}$, wobei (a, b) die ganzzahligen Lösungen der Pellschen

Gleichung $a^2 - db^2 = \pm 1$ durchläuft. Diese Lösungen sind aber wegen $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}$ alle durch die fundamentale Einheit $\varepsilon = a_1 + b_1\sqrt{d}$ gegeben, und zwar durch die Paare (a_n, b_n) mit

$$a_n + b_n\sqrt{d} = \varepsilon^n = (a_1 + b_1\sqrt{d})^n.$$

Analoges gilt für den Fall $d \equiv 1 \mod 4$ und einer leicht modifizierten Pellschen Gleichung. Die fundamentale Einheit für $\mathbb{Q}(\sqrt{d})$ kann man mit Hilfe der Kettenbruchentwicklung für $\sqrt{d}$ bestimmen. Die folgende Tabelle zeigt, daß die fundamentale Einheit auch für kleines d schon recht groß ausfallen kann:

d	ε
2	$1 + \sqrt{2}$
3	$2 + \sqrt{3}$
7	$8 + 3\sqrt{7}$
31	$1520 + 273\sqrt{31}$
46	$24335 + 3588\sqrt{46}$
94	$2143295 + 221064\sqrt{94}$
151	$1728148040 + 140634693\sqrt{151}$
331	$2785589801443970 + 153109862634573\sqrt{331}$
571	$181124355061630786130 + 7579818350628982587\sqrt{571}$

In dem Skript von James S. Milne wird die Fundamentaleinheit von $\mathbb{Q}(\sqrt{9199})$ erwähnt, allerdings ohne explizite Angabe. Das können wir selbst leicht mit PARI GP ausrechnen: Die Diskriminante ist $4 \cdot 9199$, da $9199 \equiv 3 \mod 4$.

```
? quadunit(4*9199)

%1 = 10533449278161191071963751576949295194172 66
955491964582169476720418214485349747839063034640 +
109824769111439370223410310039186819141537351326
52023268221576527593244593149235240351449*sqrt(9199).
```

5.2 Analytische Klassenzahlformel

Ist $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ ein System von Grundeinheiten für den Zahlkörper K, so wird der Regulator von K als das Volumen des vollständigen Gitters $L(\mathcal{O}_K^\times)$ in $\mathbb{R}^{r+s-1}$ definiert.

Definition 5.2. Sei $\mathcal{O}_K^\times$ die Einheitengruppe eines Zahlkörpers K und $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ ein System von Grundeinheiten. Dann heißt

$$R = |\det((\log|\sigma_i(\varepsilon_j)|)_{i,j=1}^{r+s-1})|$$

der *Regulator* von K.

Die letzte Einbettung σ_{r+s} bleibt also unberücksichtigt. Für die nächste Definition brauchen wir s als komplexe Variable, und benennen (r, s) der Körpereinbettungen in (r_1, r_2) um, mit $[K : \mathbb{Q}] = r_1 + 2r_2$.

Definition 5.3. Sei K ein Zahlkörper und $s \in \mathbb{C}$ mit $\Re(s) > 1$. Sei

$$\zeta_K(s) := \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s}$$

die *Dedekindsche Zetafunktion.*

Für $K = \mathbb{Q}$ ist

$$\zeta_{\mathbb{Q}}(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}$$

gerade die *Riemannsche Zetafunktion*, denn I durchläuft dann die Menge der Ideale (n) für $n \in \mathbb{N}$. Wie schon $\zeta(s)$ konvergiert auch $\zeta_K(s)$ absolut und lokal gleichmässig für $\Re(s) > 1$, und hat eine holomorphe Fortsetzung auf $\mathbb{C} \setminus \{1\}$. Man hat auch ein Eulerprodukt, nämlich

$$\zeta_K(s) = \prod_{P \in \mathrm{Spec}(\mathcal{O}_K)} \frac{1}{1 - \frac{1}{N(P)^s}}.$$

Zudem erfüllt $\zeta_K(s)$ auch wieder eine Funktionalgleichung:

$$\zeta_K(1-s)\Gamma\left(\frac{1-s}{2}\right)^{r_1}\Gamma(1-s)^{r_2} = \zeta_K(s)\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}(4^{-r_2}\pi^{-n}|d_K|)^{s-1}$$

Das kann man benutzen, um die holomorphe Fortsetzung auf $\mathbb{C} \setminus \{1\}$ zu zeigen, und daß $\zeta_K(s)$ bei 1 einen einfach Pol hat. Das Residuum $\mathrm{res}_{s=1}\zeta_K(s)$ kann man ausrechnen. Erstaunlicherweise hängt es mit der Klassenzahl h von K zusammen.

Theorem 5.2.1 (Analytische Klassenzahlformel)**.** *Sei K ein Zahlkörper mit Klassenzahl h und mit r_1 reellen und r_2 komplexen Einbettungen. Es bezeichne $w = w_K$ die Anzahl der Einheitswurzeln in K, und R den Regulator von K. Dann gilt*

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}R \cdot h}{w\sqrt{|d_K|}}.$$

Diese Formel wird, sowohl theoretisch wie auch praktisch, für die Berechnung der Klassenzahl genutzt. Alle anderen Terme in der Formel sind nämlich einfacher zu berechnen als die Klassenzahl.

Für quadratische Zahlkörper und Kreisteilungskörper kann man die Formel noch spezialisieren. Wir wollen das Ergebnis für quadratische Zahlkörper noch angeben. Sei $\chi(n) = (d_K/n)$ der quadratische Dirichlet-Charakter, gegeben durch das Legendre-Symbol. Dann bezeichnet

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

die L-Reihe zu χ. Sie hat eine holomorphe Fortsetzung auf ganz $\mathbb{C}$. Wir erhalten $\zeta_K(s) = \zeta(s)L(s, \chi)$ und folgende Klassenzahlformel.

Korollar 5.2.2. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein imaginär-quadratischer Zahlkörper mit Diskriminante d_K und Klassenzahl h, und w die Anzahl der Einheitswurzeln in K, d.h. $w = 2, 4, 6$. Dann gilt*

$$h = \frac{w\sqrt{|d_K|}}{2\pi} L(1, \chi).$$

Beispiel 5.2.3. *Für $K = \mathbb{Q}(i)$ gilt $h = 1$.*

Dann ist nämlich $w = 4$, $|d_K| = 4$, und $L(1, \chi)$ ist die Leibniz-Reihe

$$L(1, \chi) = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \cdots = \frac{\pi}{4}.$$

Die Formel aus Korollar 5.2.2 ergibt also

$$h = \frac{4 \cdot 2}{2\pi} L(1, \chi) = 1.$$

Hier ist ein etwas interessanteres Beispiel: der Zahlkörper $K = \mathbb{Q}(\sqrt{-15})$ ist derjenige kleinster Diskriminante mit Klassenzahl $h > 1$.

Beispiel 5.2.4. *Für $K = \mathbb{Q}(\sqrt{-15})$ gilt $h = 2$.*

Dann ist $w = 2$, $d_K = -15$, also $h = \frac{\sqrt{15}}{\pi} L(1, \chi)$. Es gilt

$$L(1, \chi) \sim 1.62231147038944475878118430 8 \sim \frac{2\pi}{\sqrt{15}},$$

also $h = 2$.

Im reell-quadratischen Fall erhalten wir folgende Formel.

Korollar 5.2.5. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein reell-quadratischer Zahlkörper mit Diskriminante d_K, Klassenzahl h und Grundeinheit ε. Dann gilt*

$$h = \frac{\sqrt{d_K}}{2\log(|\varepsilon|)} L(1, \chi).$$

Beispiel 5.2.6. *Für $K = \mathbb{Q}(\sqrt{5})$ gilt $h = 1$.*

Wir haben $d_K = 5$, $\varepsilon = (1 + \sqrt{5})/2$, und

$$\begin{aligned} L(1, \chi) &= \sum_{n=1}^{\infty} \left(\frac{1}{5n+1} - \frac{1}{5n+2} - \frac{1}{5n+3} + \frac{1}{5n+4} \right) \\ &\int_0^1 \frac{1 - x - x^2 + x^3}{1 - x^5} dx \\ &\sim 0.4304089410. \end{aligned}$$

Damit ist

$$h = \frac{\sqrt{5}}{2\log(\frac{1+\sqrt{5}}{2})} \cdot L(1, \chi) = 1.$$

6 Zerlegung und Verzweigung

Wir haben schon gesehen, daß das Studium von Primidealen in Ganzzahlringen und allgemeiner in Dedekindringen interessant ist. In solchen Ringen haben wir ja eine eindeutige Faktorisierung von Idealen in Primideale. Hat man ein Primideal $\mathfrak{p}$ in einem Ganzzahlring $\mathcal{O}_K$ eines Zahlkörpers gegeben, und eine Erweiterung L/K von Zahlkörpern, so betrachtet man das Ideal $\mathfrak{p}$ als $\mathfrak{p}\mathcal{O}_L$ im Ganzzahlring $\mathcal{O}_L$ von L. Die Frage ist dann, wie sich das Ideal als Produkt von Primidealen in $\mathcal{O}_L$ zerlegt. Wir können jedenfalls

$$\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$$

mit verschiedenen Primidealen P_i in $\mathcal{O}_L$ mit Exponenten $e_i \geq 1$ schreiben. Tritt dort nur ein Primideal auf, mit Exponenten 1, so ist $\mathfrak{p}\mathcal{O}_L$ wieder ein Primideal in $\mathcal{O}_L$. Dann wird $\mathfrak{p}$ als *träge* bezeichnet. Im allgemeinen kann sich $\mathfrak{p}\mathcal{O}_L$ aber in mehrere Primideale zerlegen, und es kommt auf die Art der Zerlegung an. Dafür wird es verschiedene Bezeichnungen geben. Man sagt zum Beispiel, daß $\mathfrak{p}$ *verzweigt* ist, wenn einer der Exponenten mindestens quadratisch auftritt.
Wir werden also die Zerlegungsgesetze für Zahlkörpererweiterungen L/K studieren. Falls die Erweiterung Galoissch ist, vereinfacht sich die Situation erheblich. Auch der Fall $K = \mathbb{Q}$ ist einfacher, insbesondere wenn L ein quadratischer Zahlkörper ist. Ein Primideal $\mathfrak{p}$ ist dann von der Form (p) für eine rationale Primzahl p, und es gilt $\sum_{i=1}^{r} e_r \leq [L : K] = 2$ für die Exponenten in der Zerlegung von $(p) = p\mathcal{O}_L$ in $\mathcal{O}_L$. Damit können höchstens zwei Exponenten auftreten, und es gibt bis auf Umnummerierung nur drei Fälle:

$$\begin{aligned} &e_1 = 2, && \text{falls } p\mathcal{O}_L = P^2 \text{ verzweigt} \\ &e_1 = 1, e_2 = 1, && \text{falls } p\mathcal{O}_L = P_1P_2 \text{ zerlegt} \\ &e_1 = 1, && \text{falls } p\mathcal{O}_L = P \text{ träge} \end{aligned}$$

Wir werden in Satz 6.2.5 sehen, daß das Zerlegungsverhalten von Idealen (p) in quadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d})$ durch das Legendre-Symbol (d/p) beschrieben werden kann. So ist etwa eine Primzahl $p > 2$ genau dann träge, wenn $(d/p) = -1$ gilt, also d und p teilerfremd sind, und d kein Quadrat modulo p ist.

Beispiel 6.0.1. *Sei $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ und $L = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$.*

(a) Für $\mathfrak{p} = (2)$ ist $\mathfrak{p}\mathcal{O}_L = P^2$ verzweigt.

(b) Für $\mathfrak{p} = (3)$ ist $\mathfrak{p}\mathcal{O}_L = P_1P_2$ zerlegt.

(c) Für $\mathfrak{p} = (11)$ ist $\mathfrak{p}\mathcal{O}_L$ träge.

Es gilt $(2) = P^2$ mit dem Primideal $P = (2, 1 + \sqrt{-5})$, siehe Beispiel 4.2.9. Mit den Primidealen $P_1 = (3, 1 + 2\sqrt{-5})$ und $P_2 = (3, 1 - 2\sqrt{-5})$ in $\mathcal{O}_L$ gilt $(3) = P_1 P_2$, siehe Beispiel 3.2.13. Da das Legendre-Symbol

$$\left(\frac{-5}{11}\right) = -1$$

erfüllt, also -5 kein Quadrat modulo 11 ist, bleibt (11) ein Primideal in $\mathbb{Z}[\sqrt{-5}]$, siehe Satz 6.2.5.

6.1 Lokalisierung

Wir wiederholen kurz Lokalisierungen von Ringen, soweit wir sie hier brauchen. Eine Teilmenge $S \subset R$ eines Ringes R heißt *multiplikativ abgeschlossen*, falls $1 \in S$ und aus $a, b \in S$ auch $ab \in S$ folgt. In der Sprache von Primidealen bedeutet das folgendes. Ein Ideal P in R ist prim, wenn $R \setminus P$ multiplikativ abgeschlossen ist. Mit S kann man den Ring $S^{-1}R$ der Brüche bilden, der auch als *Lokalisierung* von R bezeichnet wird, siehe Definition 1.2.11 in [1].

Beispiel 6.1.1. *Sei R ein Integriätsbereich. Dann ist $S = R \setminus 0$ eine multiplikativ abgeschlossene Teilmenge und $S^{-1}R = \mathrm{Quot}(R)$ genau der Quotientenkörper von R.*

Beispiel 6.1.2. *Sei R ein Integriätsbereich und $\mathfrak{p}$ ein Primideal in R. Dann ist $S = R \setminus \mathfrak{p}$ eine multiplikativ abgeschlossene Teilmenge und $R_\mathfrak{p} := S^{-1}R$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$.*

Dazu siehe Beispiel 1.2.13 in [1]. Wir brauchen folgende Sätze über Lokalisierungen.

Satz 6.1.3. *Die Primideale P der Lokalisierung $S^{-1}R$ stehen in bijektiver Korrespondenz zu den Primidealen $\mathfrak{p}$ in R, die S nicht schneiden, also mit $\mathfrak{p} \cap S = \emptyset$.*

Zum Beweis siehe Satz 1.2.22, (4) in [1].

Satz 6.1.4. *Sei R ein Noetherscher Ring und S eine multiplikativ abgeschlossene Teilmenge von R. Dann ist die Lokalisierung $S^{-1}R$ ebenfalls ein Noetherscher Ring.*

Zum Beweis siehe Satz 1.3.5 in [1].

Satz 6.1.5. *Sei R ein Integritätsbereich, $A \subseteq R$ ein Unterring, $S \subseteq A$ eine multiplikativ abgeschlossene Teilmenge, und B der ganze Abschluß von A in R. Dann ist $S^{-1}B$ der ganze Abschluß von $S^{-1}A$ in $S^{-1}R$.*

Zum Beweis siehe Lemma 4.2.8 in [1].

Korollar 6.1.6. *Die Lokalisierung eines Dedekindringes ist wieder ein Dedekindring.*

Beweis. Sei A ein Dedekindring. Dann ist $S^{-1}A$ wieder ein Noetherscher Ring nach Satz 6.1.4 und hat Krull-Dimension 1 wegen Satz 6.1.3. Nach Satz 6.1.5 ist $S^{-1}A$ auch ganz abgeschlossen. □

Satz 6.1.7. *Sei R ein Integritätsbereich, $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge, und $\mathfrak{m} \subseteq R$ ein maximales Ideal in R mit $\mathfrak{m} \cap S = \emptyset$. Dann gilt*

$$S^{-1}R/\mathfrak{m}S^{-1}R \simeq R/\mathfrak{m}$$

6.2 Gradformel

Bei der Frage, wie Primideale $\mathfrak{p}$ von $\mathcal{O}_K$ sich für eine Zahlkörpererweiterung L/K in $\mathcal{O}_L$ zerlegen, können wir eine etwas allgemeinere Situation betrachten. Wir nehmen ein Primideal $\mathfrak{p}$ in einem Dedekindring A mit $\mathrm{Quot}(A) = K$ und betrachten eine endliche Körpererweiterung L/K. Dann untersuchen wir die Zerlegung von $\mathfrak{p}$ als Ideal in B, dem ganzen Abschluß von A. Der Fall $A = \mathcal{O}_K$ und $B = \mathcal{O}_L$ ist dann ein Spezialfall. Man kann zeigen, daß B im allgemeinen Fall ein Dedekindring ist mit $\mathrm{Quot}(B) = L$. Wir brauchen diese Tatsache hier aber nur für separable Erweiterungen.

Satz 6.2.1. *Sei A ein Dedekindring mit Quotientenkörper K und L eine endliche, separable Erweiterung von K. Dann ist der ganze Abschluß B von A in L ein Dedekindring mit Quotientenkörper L.*

Beweis. Da A Noethersch ist, gilt das auch für B wegen Satz 2.4.10. Weiter ist der ganze Abschluß in einer algebraischen Körpererweiterung seines Quotientenkörpers immer ganz abgeschlossen: ist nämlich C der ganze Abschluss von B in L, dann ist C ganz über B, und B ganz über A, also C ganz über A wegen der Transitivität aus Korollar 2.1.8. Also gilt $C \subseteq B$, und B ist ganz abgeschlossen. Wegen Satz 2.3.3 gilt $\dim(B) = \dim(A) = 1$. Schliesslich gilt $\mathrm{Quot}(B) = L$ wegen Korollar 2.2.8. □

Sei also A ein Dedekindring mit $\mathrm{Quot}(A) = K$, und L/K eine separable, endliche Körpererweiterung. Sei B der ganze Abschluß von A in L. Dann besitzt jedes Primideal $\mathfrak{p}$ von A eine Faktorisierung in B

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$$

mit verschiedenen Primidealen P_i in B. Es gilt $\mathfrak{p} \subseteq \mathfrak{p}B \subseteq P_i$, also $P_i \mid \mathfrak{p}$ im Sinne der Teilbarkeit von Idealen in Dedekindringen.

Lemma 6.2.2. *Für Primideale $\mathfrak{p}$ von A und P von B, beide ungleich Null, sind äquivalent.*

(a) P liegt über $\mathfrak{p}$, also $P \cap A = \mathfrak{p}$.

(b) $\mathfrak{p}B \subseteq P$.

(c) $P \mid \mathfrak{p}B$.

Beweis. $(a) \Rightarrow (b)$: nach Voraussetzung ist $\mathfrak{p} \subseteq P$, also $\mathfrak{p}B \subseteq PB \subseteq P$.
$(b) \Leftrightarrow (c)$: $I \mid J$ bedeutet nach Definition $I \supseteq J$. Es gibt dann ein Ideal I' mit $J = II'$.
$(b) \Rightarrow (a)$: nach Voraussetzung gilt $\mathfrak{p} \subseteq P \cap A$. Da $\mathfrak{p}$ auch ein maximales Ideal ist, siehe Satz 3.1.1, und $1 \notin P$, so folgt $P \cap A \neq A$ und $P \cap A = \mathfrak{p}$. □

Wir wollen hier immer annehmen, daß Primideale ungleich Null sind.

Lemma 6.2.3. *Sei $\mathfrak{p}$ ein Primideal von A, und P ein Primideal von B, das über $\mathfrak{p}$ liegt. Dann ist die kanonische Abbildung $A/\mathfrak{p} \hookrightarrow B/P$ eine Einbettung von Körpern und B/P ein endlich-dimensionaler $A/\mathfrak{p}$-Vektorraum.*

Beweis. Die Einbettung $A \hookrightarrow B$ induziert wegen $\mathfrak{p} = P \cap A$ eine Abbildung $A/\mathfrak{p} \to B/P$, $a+\mathfrak{p} \mapsto a+P$, die ein wohldefinierter, injektiver Homomorphismus von Körpern ist. Da B nach Satz 2.4.10 ein endlich-erzeugter A-Modul ist, muß B/P ein endlich-erzeugter $A/\mathfrak{p}$-Modul sein. Da sowohl P als auch $\mathfrak{p}$ maximal sind, sind beide Quotienten aber Körper. Ein endlich-erzeugter K-Modul ist gerade ein endlich-dimensionaler K-Vektorraum. □

Definition 6.1. Sei $\mathfrak{p}$ ein Primideal in A und

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$$

die Primfaktorzerlegung von $\mathfrak{p}B$ in B.

(1) Die Zahl $e_i = e(P_i/\mathfrak{p})$ heißt *Verzweigungsindex* von P_i über $\mathfrak{p}$.

(2) Die Zahl $f_i = f(P_i/\mathfrak{p}) = [B/P_i : A/\mathfrak{p}]$ heißt *Restklassengrad* von P_i über $\mathfrak{p}$.

(3) $\mathfrak{p}$ heißt *verzweigt*, wenn $e_i \geq 2$ für ein $i = 1, \ldots, r$ gilt, oder ein B/P_i eine inseparable Erweiterung von $A/\mathfrak{p}$ ist.

(4) $\mathfrak{p}$ heißt *rein verzweigt*, wenn $\mathfrak{p}$ verzweigt ist und $f_i = 1$ gilt für alle $i = 1, \ldots, r$.

(5) $\mathfrak{p}$ heißt *unzerlegt*, wenn $r = 1$ gilt, also wenn es nur ein Primideal P über $\mathfrak{p}$ gibt.

(6) $\mathfrak{p}$ heißt *träge*, wenn $r = 1$ und $e_1 = 1$ gilt, d.h., wenn $\mathfrak{p}B$ ein Primideal in B ist.

(7) $\mathfrak{p}$ heißt *vollständig zerlegt*, wenn $e_i = f_i = 1$ gilt für alle $i = 1, \ldots, r$. Das bedeutet, für jedes Primideal P_i über $\mathfrak{p}$ ist $B/P_i = A/\mathfrak{p}$.

Diese Namensgebungen erfordern ein wenig Konzentration, besonders in Hinblick auf ihre Verneinungen. So ist $\mathfrak{p}$ eben *unverzweigt*, wenn $e_i = 1$ für alle i gilt, *und* alle Körpererweiterungen B/P_i über $A/\mathfrak{p}$ separabel sind. Im Fall von Ganzheitsringen $B = \mathcal{O}_L$ und $A = \mathcal{O}_K$ sind diese Restklassenkörper ja endlich, und deshalb die Körpererweiterungen niemals inseparabel. Dann kann diese Bedingung in der Definition fallengelassen werden. Man überprüfe, ob die Namen in Beispiel 6.0.1 konform mit obiger Definition sind. Nun kommen wir zu dem Gradsatz, der die Zahlen e_i, f_i, r und $[L : K] = n$ in Beziehung setzt.

Theorem 6.2.4 (Gradsatz)**.** *Sei A ein Dedekindring mit Quotientenkörper K und L eine endliche, separable Erweiterung von K. Sei B der ganze Abschluß von A in L, $\mathfrak{p}$ ein Primideal in A mit Faktorisierung $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Dann gilt*

$$\sum_{i=1}^{r} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Beweis. Um die erste Gleichheit zu zeigen, wenden wir zuerst den chinesischen Restsatz an:

$$B/\mathfrak{p}B \simeq B/(P_1^{e_1} \cdots P_r^{e_r}) \simeq (B/P_1^{e_1}) \times \cdots \times (B/P_r^{e_r}).$$

Damit genügt es also, $[B/P_i^{e_i} : A/\mathfrak{p}] = e_i f_i$ zu zeigen. Für jedes r_i ist $P_i^{r_i}/P_i^{r_i+1}$ ein B/P_i-Modul. Da zwischen $P_i^{r_i}$ und $P_i^{r_i+1}$ kein Ideal mehr liegt, ist $\dim_{B/P_i}(P_i^{r_i}/P_i^{r_i+1}) = 1$ als Vektorraum über B/P_i. Es folgt

$$\dim_{A/\mathfrak{p}}(P_i^{r_i}/P_i^{r_i+1}) = f_i$$

wegen $f_i = \dim_{A/\mathfrak{p}}(B/P_i)$. Wir erhalten eine Kette von Idealen

$$B \supseteq P_i \supseteq P_i^2 \supseteq \cdots \supseteq P_i^{e_i}$$

wo jeder Quotient $P_i^{r_i}/P_i^{r_i+1}$ die Dimension f_i über $A/\mathfrak{p}$ hat. Also hat $B/P_i^{e_i}$ die Dimension $e_i f_i$ über $A/\mathfrak{p}$.
Um $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K] = n$ zu zeigen, nehmen wir zuerst an, daß A ein Hauptidealring ist. Dann ist B ein freier A-Modul vom Rang n wegen Satz 2.4.10. Dann haben wir einen Isomorphismus $A^n \to B$, der einen Isomorphismus $K^n \to L$ induziert, durch Tensorieren mit K. Tensoriert man weiter mit $A/\mathfrak{p}$, so induziert das einen Isomorphismus $(A/\mathfrak{p})^n \to B/\mathfrak{p}B$, weswegen $n = [B/\mathfrak{p}B : A/\mathfrak{p}]$ gilt. Den allgemeinen Fall führen wir durch Lokalisierung auf diesen Fall zurück. Dazu sei $S = A \setminus \mathfrak{p}$. Das ist eine multiplikativ abgeschlossene Teilmenge von A mit lokalen Ringen $A_\mathfrak{p} = S^{-1}A$ und $B_\mathfrak{p} = S^{-1}B$. Wegen Satz 6.1.3 ist die Krulldimension von $A_\mathfrak{p}$ gleich 1, also ist $A_\mathfrak{p}$ ein Hauptidealring mit maximalem Ideal $\mathfrak{p}A_\mathfrak{p}$. Wegen Satz 6.1.5 ist $B_\mathfrak{p}$ der ganze Abschluß von $A_\mathfrak{p}$ in L. Deswegen ist $B_\mathfrak{p}$ ein freier $A_\mathfrak{p}$-Modul vom Rang n, also $[B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = n$ wie oben. Aus der Faktorisierung $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ folgt mit Satz 6.1.3 und $P_i \cap S = \emptyset$ die Faktorisierung $\mathfrak{p}B_\mathfrak{p} = (P_1 B_\mathfrak{p})^{e_1} \cdots (P_r B_\mathfrak{p})^{e_r}$. Wegen Satz 6.1.7 gilt $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq A/\mathfrak{p}$ und $B_\mathfrak{p}/(P_i B_\mathfrak{p}) \simeq B/P_i$. Das ergibt zusammen

$$\begin{aligned} n &= [B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] \\ &= \sum_{i=1}^{r} e_i \cdot [B_\mathfrak{p}/(P_i B_\mathfrak{p}) : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] \\ &= \sum_{i=1}^{r} e_i \cdot [B/P_i : A/\mathfrak{p}] \\ &= \sum_{i=1}^{r} e_i f_i. \end{aligned}$$

□

Für $A = \mathbb{Z}$, $K = \mathbb{Q}$ und $B = \mathcal{O}_L$ mit $L = \mathbb{Q}(\sqrt{d})$ impliziert der Gradsatz, daß es nur drei verschiedene Möglichkeiten für die Indizes gibt. Ein Primideal (p) in $\mathbb{Z}$ hat also nur folgende Möglichkeiten der Faktorisierung als Ideal in $\mathcal{O}_L$:

$$\begin{aligned} p\mathcal{O}_L &= P^2, && r = 1, e_1 = 2, f_1 = 1, \\ p\mathcal{O}_L &= P_1 P_2, && r = 2, e_1 = e_2 = f_1 = f_2 = 1 \\ p\mathcal{O}_L &= P, && r = 1, e_1 = 1, f_1 = 2. \end{aligned}$$

Man kann genau sagen, welcher der drei Fälle für gegebenes Primideal (p) eintritt.

Satz 6.2.5. *Sei $p > 2$ eine Primzahl in $\mathbb{Z}$ und $L = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit Diskriminante D.*

(a) Falls $(D/p) = 0$ gilt, so ist $p\mathcal{O}_L = (p, \sqrt{d})^2$, und (p) verzweigt.

(b) Falls $(D/p) = 1$ gilt, so ist $p\mathcal{O}_L = P_1P_2$, mit zwei verschiedenen Primidealen P_1 und P_2, und (p) zerfällt.

(c) Falls $(D/p) = -1$ gilt, so ist $p\mathcal{O}_L = P$, und (p) ist träge.

Beweis. Im ersten Fall gilt $p \mid D$, und wegen $p > 2$ deshalb auch $p \mid d$. Dann ist

$$(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, d/p) = (p),$$

weil p und $\frac{d}{p}$ teilerfremd sind, also $(p, \sqrt{d}, \frac{d}{p}) = (1) = \mathcal{O}_L$ gilt.
Im zweiten Fall ist $D \equiv x^2 \mod p$ für ein $x \in \mathbb{Z}$. Mit $P_1 = (p, x + \sqrt{d})$, $P_2 = (p, x - \sqrt{d})$ gilt

$$\begin{aligned} P_1P_2 &= (p^2, p(x \pm \sqrt{d}), x^2 - d) \\ &= (p)(p, x \pm \sqrt{d}, (x^2 - d)/p) \end{aligned}$$

Wegen $2\sqrt{d} = (x + \sqrt{d}) - (x - \sqrt{d})$ ist $4d = (2\sqrt{d})^2$ in dem zweiten Ideal enthalten. Da p und $4d$ aber hier teilerfremd sind, ist das zweite Ideal gleich (1) und $P_1P_2 = p\mathcal{O}_L$.
Im dritten Fall nehmen wir an, $p\mathcal{O}_L$ wäre kein Primideal in $\mathcal{O}_L$. Dann könnte man aber $p\mathcal{O}_L = Q_1Q_2$ mit zwei Primidealen schreiben, und $p^2 = N(p\mathcal{O}_L) = N(Q_1)N(Q_2)$ hieße, daß $N(Q_1) = N(Q_2) = p$ ist. Wir zeigen aber, daß es im Fall $(D/p) = -1$ kein Ideal der Norm p in $\mathcal{O}_L$ geben kann. Sei also Q ein Primideal mit $N(Q) = p$. Es ist nicht schwer zu zeigen, daß $Q = (p, a + \omega)$ geschrieben werden kann, mit mit $a \in \mathbb{Z}$ und $\omega = \sqrt{d}$ oder $\omega = (1 + \sqrt{d})/2$, so daß $p \mid N(a + \omega)$. Dabei ist $\{1, \omega\}$ die Standard-Ganzheitsbasis von $\mathcal{O}_L = \mathbb{Z}[\omega]$. Für $\omega = \sqrt{d}$ bedeutet das $a^2 - d \equiv 0 \mod p$, also $(D/p) = (4d/p) = (d/p) = 1$, im Widerspruch zur Annahme. Für $\omega = (1+\sqrt{d})/2$ haben wir $(2a + 1)^2 \equiv 0 \mod p$, was ebenfalls ein Widerspruch ist. □

Bemerkung 6.2.6. Für den Sonderfall $p = 2$ lässt sich ebenfalls ein Kriterium wie in Satz 6.2.5 formulieren. Für $d \equiv 2 \mod 4$ ist $2\mathcal{O}_L = (2, \sqrt{d})^2$, für $d \equiv 3 \mod 4$ ist $2\mathcal{O}_L = (2, 1 + \sqrt{d})^2$, für $d \equiv 1 \mod 8$ ist $2\mathcal{O}_L = (2, (1 + \sqrt{d})/2) \cdot (2, (1 - \sqrt{d})/2)$, und für $d \equiv 5 \mod 8$ ist $2\mathcal{O}_L$ prim.

Wir können damit nun erneut Besipiel 6.0.1 anschauen. Das bedeutet $d = D = -5$.

(*a*) Wegen $-5 \equiv 3 \mod 4$ ist $\mathfrak{p} = (2)$ also verzweigt, nämlich $2\mathcal{O}_L = P^2 = (2, 1+\sqrt{-5})^2$. Dann ist $e_1 = e(P \mid \mathfrak{p}) = 2$ und $f_1 = [\mathbb{Z}[\sqrt{-5}]/(2, 1 + \sqrt{-5}) : \mathbb{Z}/2] = 1$.

(*b*) Wegen $\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$ zerfällt $\mathfrak{p} = (3)$, mit $3\mathcal{O}_L = P_1P_2$ und $e_1 = e_2 = 1$ und $f_1 = [\mathcal{O}_L/P_1 : \mathbb{Z}/3] = 1$, $f_2 = [\mathcal{O}_L/P_2 : \mathbb{Z}/3] = 1$, siehe auch Beispiel 3.2.13.

(*c*) Wegen $\left(\frac{-5}{11}\right) = -1$ bleibt $\mathfrak{p} = (11)$ prim in $\mathcal{O}_L$.

6.3 Zerlegung in Galoiserweiterungen

Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Erweiterung und B der ganze Abschluß von A in B. Eine besondere Situation tritt ein, wenn die Erweiterung L/K sogar galoissch ist, mit Galoisgruppe G. Dann operiert G auf B, weil für jedes Element $b \in B$ und jedes $\sigma \in G$ auch $\sigma(b)$ wieder ganz über A ist, also zu $B = \overline{A}^L$ gehört. Die Galoisgruppe operiert sogar auf der Menge der Primideale P in B, die über einem Primideal $\mathfrak{p}$ von A liegen: erstens ist $\sigma(P)$ wieder ein Primideal in B, wenn P es ist, da σ einen Isomorphismus $B/P \simeq B/\sigma(P)$ induziert und deshalb $B/\sigma(P)$ ebenfalls Integritätsring ist. Zweitens gilt

$$\sigma(P) \cap A = \sigma(P \cap A) = \sigma(\mathfrak{p}),$$

und $\sigma(P)$ liegt auch wieder über $\mathfrak{p}$.

Definition 6.2. Sei P in B ein Primideal und $\sigma \in G = Gal(L/K)$. Dann heißt $\sigma(P)$ ein zu P *konjugiertes* Primideal.

Satz 6.3.1. *Für jedes Primideal $\mathfrak{p}$ von A operiert die Galoisgruppe G transitiv auf der Menge der über $\mathfrak{p}$ gelegenen Primideale P von B. Je zwei Primideale P und P' über $\mathfrak{p}$ von B sind also konjugiert.*

Beweis. Wir haben schon gezeigt, daß G auf der Menge der über $\mathfrak{p}$ gelegenen Primideale von B operiert. Die Transitivität bedeutet, daß wir für je zwei solche Primideale P und P' über $\mathfrak{p}$ ein $\sigma \in G$ finden müssen mit $P' = \sigma(P)$. Angenommen, $P' \neq \sigma(P)$ für alle $\sigma \in G$. Dann gäbe es nach dem chinesischen Restsatz ein $x \in B$ mit $x \equiv 0 \mod P'$ und $x \equiv 1 \mod \sigma(P)$ für alle $\sigma \in G$. Damit wäre

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in P' \cap A = \mathfrak{p} = P \cap A.$$

Nach Annahme wäre aber $x \notin \sigma(P)$ für alle σ, also $\sigma(x) \notin P$ für alle σ, und daher $\prod_{\sigma \in G} \sigma(x)$ auch nicht in $P \cap A = \mathfrak{p}$. Denn da P ein Primideal ist, folgte aus $\prod_{\sigma \in G} \sigma(x) \in P$ doch $\sigma(x) \in P$ für zumindest ein σ. Das ist ein Widerspruch. □

Jetzt können wir den Gradsatz vereinfachen.

Theorem 6.3.2. *Sei A ein Dedekindring mit Quotientenkörper K und L eine endliche Galoiserweiterung von K. Sei B der ganze Abschluß von A in L, $\mathfrak{p}$ ein Primideal in A mit Faktorisierung $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Dann sind alle Verzweigungsindizes und Restklassengrade gleich, d.h., es gilt $e_i = e$ und $f_i = f$ für alle $i = 1, \ldots, r$ und*

$$ref = [B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Beweis. Ist P ein Primideal in der Faktorisierung, also $P^k \mid \mathfrak{p}B$, so bedeutet das $\sigma(P)^k \mid \sigma(\mathfrak{p}B) = \mathfrak{p}B$, also wieder ein Faktor von $\mathfrak{p}B$. Nach Satz 6.3.1 gibt es für jedes P_i ein $\sigma \in G$ mit $\sigma(P_i) = P_1$. Also sind alle e_i gleich e_1. Dieses σ induziert dann einen Isomorphismus $B/P_1 \simeq B/P_i$, so daß alle f_i gleich f_1 sind. □

Bemerkung 6.3.3. Wir hatten die Gleichheit der Indizes bei quadratischen Zahlkörpern $L/\mathbb{Q}$ schon festgestellt. Quadratische Erweiterungen sind automatisch Galoiserweiterungen. Also könnten wir das nun auch aus obigem Satz folgern.

Definition 6.3. Sei P ein Primideal von B und $G = Gal(L/K)$. Dann heißt

$$D_P := \{\sigma \in G \mid \sigma(P) = P\}$$

die *Zerlegungsgruppe* von P über K, und

$$Z_P := \{x \in L \mid \sigma(x) = x \ \ \forall\, \sigma \in D_P\}$$

der zugehörige *Zerlegungskörper* von P in L/K.

Satz 6.3.4. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Galoiserweiterung und B der ganze Abschluß von A in L. Sei $\mathfrak{p}$ ein Primideal in A mit Zerlegung $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Dann ist $r = (G : D_P)$, und für ein Primideal P über $\mathfrak{p}$ gilt:*

(a) $D_P = 1$ genau dann wenn $Z_P = L$ gilt, also $\mathfrak{p}$ vollständig zerlegt ist.

(b) $D_P = G$ genau dann wenn $Z_P = K$ gilt, also $\mathfrak{p}$ unzerlegt ist.

(c) Es gilt $D_{\sigma(P)} \simeq \sigma D_P \sigma^{-1}$ für alle $\sigma \in G$.

Beweis. G operiert transitiv auf der Menge $\mathcal{M}$ der Primideale P von B über $\mathfrak{p}$. Also ist die Abbildung $G/D_P \to \mathcal{M}$, $\overline{\sigma} \mapsto \sigma P$ eine Bijektion. Die Menge $\mathcal{M}$ hat genau r Elemente, und die Behauptungen sind offensichtlich. □

Definition 6.4. Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Galoiserweiterung und B der ganze Abschluß von A in L. Sei $\mathfrak{p}$ ein Primideal in A und P ein Primideal in B, das über $\mathfrak{p}$ liegt.

(a) Es bezeichne $k(P) = B/P$ und $k(\mathfrak{p}) = A/\mathfrak{p}$ die Restklassenkörper.

(b) Es bezeichne I_P die Untergruppe von D_P, die durch

$$I_P = \{\sigma \in D_P \mid \sigma_{|k(P)} = \mathrm{id}\}$$

gegeben ist. Sie heißt die *Trägheitsgruppe* von P in L/K.

(c) Der Fixkörper $T_P = \{x \in L \mid \sigma(x) = x \ \ \forall\, \sigma \in I_P\}$ heißt der zugehörige *Trägheitskörper* von P in L/K.

Jedes $\sigma \in D_P$ induziert wegen $\sigma(P) \subseteq P$ und $\sigma(B) \subseteq B$ einen Automorphismus

$$\overline{\sigma}\colon k(P) = B/P \to B/P, \quad x \mod P \mapsto \sigma(x) \mod P,$$

der $k(\mathfrak{p}) \subseteq k(P)$ elementweise festhält. Mit anderen Worten, wir erhalten ein Element $\overline{\sigma} \in Gal(k(P)/k(\mathfrak{p}))$, sofern die Körpererweiterung $k(P)/k(\mathfrak{p})$ galoissch ist. Das ist allerdings nicht immer der Fall. Zwar ist die Erweiterung stets normal, aber nicht immer

separabel. Ist $k(\mathfrak{p})$ *endlich*, so ist sie aber separabel. Jedenfalls, im Fall einer Galoiserweiterung erhalten eine Abbildung

$$\varphi\colon D_P \to Gal(k(P)/k(\mathfrak{p})),\ \sigma \mapsto \overline{\sigma}$$

mit $\ker(\varphi) = I_P$.

Satz 6.3.5. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Galoiserweiterung und B der ganze Abschluß von A in L. Sei $\mathfrak{p}$ ein Primideal in A und P ein Primideal in B, das über $\mathfrak{p}$ liegt. Dann ist die Körpererweiterung $k(P)/k(\mathfrak{p})$ normal.*

Beweis. Für $y \in k(P)$ wähle man ein $x \in B$ mit $y \equiv x \mod P$. Sei $p(t)$ das Minimalpolynom von x über K und $q(t)$ das Minimalpolynom von y über $k(\mathfrak{p})$. Für

$$\overline{p}(t) = p(t) \mod \mathfrak{p}$$

gilt dann $\overline{p}(x) = 0$, also $q(t) \mid p(t)$. Da L/K normal ist, zerfällt $p(t)$ über L in Linearfaktoren. Deshalb zerfällt auch $\overline{p}(t)$ in Linearfaktoren über $k(P)$, und somit auch $q(t)$. Also ist die Erweiterung $k(P)/k(\mathfrak{p})$ normal. □

Satz 6.3.6. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Galoiserweiterung und B der ganze Abschluß von A in L. Sei $\mathfrak{p}$ ein Primideal in A und P ein Primideal in B, das über $\mathfrak{p}$ liegt. Angenommen, die Erweiterung $k(P)/k(\mathfrak{p})$ ist separabel. Dann ist die Abbildung $\varphi\colon D_P \to Gal(k(P)/k(\mathfrak{p}))$ ein Gruppenhomomorphismus, und wir erhalten folgende exakte Sequenz von Gruppen:*

$$1 \to I_P \to D_P \xrightarrow{\varphi} Gal(k(P)/k(\mathfrak{p})) \to 1.$$

Es gilt $\#I_P = e(P \mid \mathfrak{p})$, $\#D_P = e(P \mid \mathfrak{p})f(P \mid \mathfrak{p})$ und

$$Gal(k(P)/k(\mathfrak{p})) \simeq D_P/I_P.$$

Beweis. Wir skizzieren den Beweis. Sei $e = e(P \mid \mathfrak{p})$ und $f = f(P \mid \mathfrak{p})$, und r die Anzahl der Konjugierten von P. Dann gilt, wegen Theorem 6.3.2

$$r = \frac{n}{\#D_P} = \frac{ref}{\#D_P},$$

also $\#D_P = ef$. Sei $E = T_P$ der Fixkörper von D_P. Nach dem Haupsatz der Galoistheorie ist $Gal(L/E) \simeq D_P$. Setze $\mathfrak{p}_E = P \cap (B \cap E)$. Nach Definition liegt $\mathfrak{p}_E$ über $\mathfrak{p}$. Das Primideal P wird von allen Elementen aus D_P festgelassen, also ist die Zerlegungsgruppe von P in L/E ganz D_P. Damit folgt

$$ef = \#D_P = [L : E] = e(P \mid \mathfrak{p}_E)f(P \mid \mathfrak{p}_E) = e'f'.$$

Wir haben die Erweiterungen $L/E/K$, und der Verzeigungsgrad sowie der Restklassengrad in Körpertürmen ist multiplikativ:

$$\begin{aligned} e(P \mid \mathfrak{p}) &= e(P \mid \mathfrak{p}_E) \cdot e(\mathfrak{p}_E \mid \mathfrak{p}) \\ f(P \mid \mathfrak{p}) &= f(P \mid \mathfrak{p}_E) \cdot f(\mathfrak{p}_E \mid \mathfrak{p}) \end{aligned}$$

Nun ist aber $ef = e'f'$ gleichwertig mit $e = e'$ und $f = f'$, da ja $e' \mid e$ und $f' \mid f$ gilt. Das wiederum ist gleichwertig mit $e(\mathfrak{p}_E \mid \mathfrak{p}) = e/e' = 1$ und $f(\mathfrak{p}_E \mid \mathfrak{p}) = f/f' = 1$. Insbesondere sind die Restklassenkörper $k(\mathfrak{p}_E)$ und $k(\mathfrak{p})$ gleich. Nun zeigen wir, daß φ surjektiv ist. Nach dem Satz vom primitiven Element ist $k(P) = k(\mathfrak{p})(\overline{\alpha})$ für ein $\alpha \in B$. Sei $m \in (B \cap E)[t]$ das normierte Minimalpolynom von α. Es stimmt mit dem charakteristischen Polynom von α überein. Deshalb ist $\overline{m} \in k(\mathfrak{p}_E)[t]$ eine Potenz des Minimalpolynoms von $\overline{\alpha}$. Sei $\overline{\sigma} \in Gal(k(P)/k(\mathfrak{p}_E))$, also $\overline{\sigma}(\overline{\alpha})$ eine Nullstelle von $\overline{m}$. Dann gibt es also ein $\sigma \in Gal(L/E) \simeq D_P$ mit $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. Dann gilt $\overline{\sigma} = \varphi(\sigma)$, d.h., φ ist surjektiv. Es folgt

$$f = f(P \mid \mathfrak{p}_E) = \#\operatorname{im}(\varphi) = \frac{\#D_P}{\#I_P} = \frac{ef}{\#I_P},$$

also $\#I_P = e$. □

Korollar 6.3.7. *Ein Primideal $\mathfrak{p}$ von A ist genau dann unverzweigt in L/K, wenn $\#I_P = 1$ ist für ein Primideal P von B über $\mathfrak{p}$.*

Wir können die Situation spezialisieren, indem wir verlangen, daß für alle Primideale $\mathfrak{p} \neq 0$ in A, der Restklassenkörper $k(\mathfrak{p}) = A/\mathfrak{p}$ *endlich* ist. Dann ist, wie gesagt, die Erweiterung $k(P)/k(\mathfrak{p})$ galoissch, da endliche Körper perfekt sind. Die Galoisgruppen von Erweiterungen von endlichen Körpern sind sogar zyklisch, erzeugt vom Frobenius-Automorphismus. Als Beispiel betrachte man einen Zahlkörper L mit $B = \mathcal{O}_L$, und $K = \mathbb{Q}$, $A = \mathbb{Z}$. Ist P ein Primideal über $\mathfrak{p} = (p)$ mit einer rationalen Primzahl p, so ist $k(\mathfrak{p}) = \mathbb{F}_p$, $k(P) = \mathcal{O}_L/P$ und

$$Gal(k(P)/\mathbb{F}_p) \simeq \langle Frob_p \rangle,$$

mit $Frob_p(x) = x^p$.

6.4 Verzweigung und Diskriminante

Sei A ein Hauptidealring und B/A eine Ringerweiterung, so daß B ein freier A-Modul ist mit Basis $\{x_1, \ldots x_n\}$. Dann hatten wir die Diskriminante von B/A definiert als das Hauptideal

$$\mathcal{D}_{B/A} = (D(x_1, \ldots, x_n)),$$

siehe Definition 2.9. Im Spezialfall $A = \mathbb{Z}$ und $B = \mathcal{O}_K$ mit einem Zahlkörper K nennen wir den positiven Erzeuger dieses Ideals die *absolute Diskriminante d von K*. Es gilt $d \in \mathbb{N}$. Es gilt folgendes Resultat über die absolute Diskriminante und Verzweigung in Zahlkörpern.

Satz 6.4.1. *Sei K ein Zahlkörper mit absoluter Diskriminante d, und p eine rationale Primzahl. Dann ist das Ideal $\mathfrak{p} = (p)$ genau dann unverzweigt in $K/\mathbb{Q}$, wenn $p \nmid d$ gilt.*

Beweis. Es gilt $p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$ mit verschiedenen Primidealen P_i von $\mathcal{O}_K$. Nach dem chinesischen Restsatz ist

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_r^{e_r}.$$

Das Ideal $\mathfrak{p}$ ist genau dann unverzweigt in $K/\mathbb{Q}$, wenn alle $e_i = 1$ sind, also $\mathcal{O}_K/p\mathcal{O}_K$ ein Produkt von Körpern ist. Sei $A = \mathbb{Z}$ und $B = \mathcal{O}_K$. Sei $\{x_1, \dots x_n\}$ eine Basis des freien A-Moduls B. Für jedes Ideal I von A ist dann $\{\overline{x_1}, \dots \overline{x_n}\}$ eine Basis des freien A/I-Moduls B/IB, und

$$D(\overline{x_1}, \dots \overline{x_n}) \equiv D(x_1, \dots, x_n) \mod I.$$

Mit $I = \mathfrak{p}$ folgt, daß die Bedingung $p \mid d$ genau

$$\mathcal{D}_{B/A} \mod \mathfrak{p} = \mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0$$

bedeutet. Wir müssen also zeigen, daß $B/\mathfrak{p}B$ genau dann ein Produkt von Körpern ist, wenn $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} \neq 0$ ist. In unserem Fall ist $A/\mathfrak{p} = \mathbb{F}_p$ und $B/\mathfrak{p}B = \mathcal{O}_K/(p)$. Sei zunächst $B/\mathfrak{p}B = \prod_i k_i$, wobei k_i endliche Körpererweiterungen von $\mathbb{F}_p$ sind. Es gilt $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = \prod_i \mathcal{D}_{k_i/\mathbb{F}_p}$. Da die Erweiterungen $k_i/\mathbb{F}_p$ separabel sind, ist kein Erzeuger in den Faktoren Null wegen Lemma 2.4.7. Also ist auch $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} \neq 0$. Sei umgekehrt $B/\mathfrak{p}B = \prod_i B/P_i^{e_i}$ kein Produkt von Körpern. Dann enthält $B/\mathfrak{p}B$ ein nilpotentes Element $x \neq 0$. Ergänze $x = x_1$ zu einer Basis $\{x_1, \dots x_n\}$ von $B/\mathfrak{p}B$. Da dann auch die Produkte x_1x_i nilpotent sind, ist die Multiplikation mit x_1x_i eine nilpotenter Endomorphismus. Somit sind seine Eigenwerte alle gleich Null, und deshalb $\mathrm{tr}(x_1x_j) = 0$. Nach Definition der Diskriminante ist dann $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0$. □

Offensichtlich folgt aus dem Satz, daß nur *endliche viele* Primideale $\mathfrak{p}$ von $\mathbb{Z}$ in einer Zahlkörpererweiterung verzweigt sein können, da d nur endlich viele Primteiler in $\mathbb{Z}$ hat. Es ist auch möglich, den Satz allgemeiner zu formulieren. Wir verzichten auf den Beweis, obwohl er eigentlich nicht wesentlich schwieriger ist, und wir auch schon Teilargumente allgemeiner gezeigt haben, siehe Korollar 2.4.8.

Satz 6.4.2. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Körpererweiterung, und B der ganze Abschluß von A in L. Sei B ein freier A-Modul (das ist etwa der Fall, wenn A ein Hauptidealring ist). Dann ist das Primideal $\mathfrak{p} = (p)$ von A genau dann verzweigt in L/K, wenn $\mathfrak{p} \supseteq \mathcal{D}_{B/A}$ gilt, also $\mathfrak{p} \mid \mathcal{D}_{B/A}$ im Sinne der Teilbarkeit von Idealen. Insbesondere verzweigen nur endlich viele Primideale von A.*

Definition 6.5. Die Körpererweiterung L/K in der Situation des obigen Satzes heißt *unverzweigt*, wenn alle Primideale ungleich Null von K, also von $\mathcal{O}_K$, in L unverzweigt sind.

Satz 6.4.3. *Sei K ein Zahlkörper. Ist die Erweiterung $K/\mathbb{Q}$ unverzweigt, so gilt $K = \mathbb{Q}$.*

Beweis. Nach Satz 4.2.13 gilt $|d_K| > 1$ für alle Zahlkörper $K \neq Q$, also $d > 1$ für die absolute Diskriminante. Also hat d immer einen Primteiler $p \mid d$. Das zugehörige Ideal $\mathfrak{p} = (p)$ ist also verzweigt nach Satz 6.4.1. Ist $K \neq \mathbb{Q}$, so ist die Erweiterung $K/\mathbb{Q}$ also immer verzweigt. □

7 Kreisteilungskörper

Ein Kreisteilungskörper ist ein Zahlkörper $K = \mathbb{Q}(\zeta)$, wobei ζ eine primitive n-te Einheitswurzel ist. Solche Körper sind interessante Beispiele für die Theorie, und haben auch wichtige Anwendungen, wie zum Beispiel für einen Fall der Fermatschen Gleichung. Die Galoisgruppe $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ ist hier isomorph zu $(\mathbb{Z}/n)^\times$, also insbesondere abelsch. Zudem sind Kreisteilungskörper im Zentrum der Klassenköpertheorie. Ein Beispiel dafür ist der sogenannte *Satz von Kronecker-Weber*, den wir in Kapitel 9 behandeln werden. Er besagt, daß jeder algebraische Zahlkörper mit abelscher Galoisgruppe in einem Kreisteilungskörper enthalten ist.

7.1 Einheitswurzeln

Sei K ein Körper und $n \in \mathbb{N}$. dann heißt ζ eine *n-te Einheitswurzel in K*, wenn $\zeta^n = 1$ gilt.

Definition 7.1. Eine n-te Einheitswurzel ζ in K heißt *primitiv*, wenn sie die Ordnung n in der Gruppe $K^\times$ hat, also $\zeta^d \neq 1$ für $d < n$ gilt. Die Gruppe

$$\mu_n(K) = \{\zeta \in K^\times \mid \zeta^n = 1\}$$

heißt *Gruppe der Einheitswurzeln in K*.

Da jede endliche Untergruppe von $K^\times$ zyklisch ist, handelt es sich bei $\mu_n(K)$ um eine endliche zyklische Gruppe.

Beispiel 7.1.1. *Für $K = \mathbb{C}$ ist $\mu_n(\mathbb{C}) = \{e^{\frac{2\pi i m}{n}} \mid 0 \leq m \leq n-1\}$.*

Lemma 7.1.2. *Sei ζ eine primitive n-te Einheitswurzel in K. Dann ist ζ^m genau dann eine primitive Einheitswurzel in K, wenn $ggt(n, m) = 1$ ist.*

Beweis. Es gilt folgende Tatsache aus der Gruppentheorie, siehe z.B. Satz 1.12 in [7]. Sei G eine Gruppe, und $\alpha \in G$ ein Element der Ordnung n. Dann hat α^m genau dann Ordnung n, wenn $ggt(n, m) = 1$ ist. Das wenden wir hier für die Gruppe $G = \mu_n(K)$ an, und sind fertig. □

Wir wollen nun Einheitswurzeln ζ in $K = \overline{\mathbb{Q}}$ betrachten, also komplexe Einheitswurzeln.

Definition 7.2. Das Minimalpolynom $\Phi_n(t) \in \mathbb{Q}[t]$ über $\mathbb{Q}$ einer primitiven n-ten Einheitswurzel ζ heißt das *n-te Kreisteilungspolynom*.

Folgendes Resultat ist wohlbekannt, und wir verweisen auf Kapitel VI, 2 in [7].

Satz 7.1.3. *Sei ζ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine Galoiserweiterung vom Grad $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$ mit Galoisgruppe*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n)^\times.$$

Es gilt $\Phi_n(t) = \prod_{(n,m)=1}(t-\zeta^m)$ und

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

Für $n = 12$ hat man die Teiler $d = 1, 2, 3, 4, 6, 12$, und

$$\begin{aligned}
\Phi_1(t) &= t - 1,\\
\Phi_2(t) &= t + 1,\\
\Phi_3(t) &= t^2 + t + 1,\\
\Phi_4(t) &= t^2 + 1,\\
\Phi_6(t) &= t^2 - t + 1,\\
\Phi_{12}(t) &= t^4 - t^2 + 1.
\end{aligned}$$

Deshalb zerlegt sich $t^{12} - 1 \in \mathbb{Q}[t]$ in folgende irreduzible Faktoren

$$t^{12} - 1 = (t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)(t^4-t^2+1).$$

Beispiel 7.1.4. *Für $n = p$ Primzahl gilt $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$.*

In der Tat, der Grad von Φ_p ist $\varphi(p) = p - 1$, und $t^p - 1 = \prod_{d|p} \Phi_d(t) = \Phi_1(t)\Phi_p(t) = (t-1)\Phi_p(t)$. Das bedeutet

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Für Primzahlpotenzen $n = p^r$ folgt wegen $\Phi_{p^r}(t) = \Phi_p(t^{p^{r-1}})$ dann

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

Insbesondere gilt $\Phi_{p^r}(1) = p$.

7.2 Der Ganzzahlring

Sei ζ eine primitive n-te Einheitswurzel. Dann ist ζ natürlich ganz über $\mathbb{Z}$, so daß

$$\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$$

gilt. Wir wollen die Gleichheit zeigen.

Lemma 7.2.1. *Sei $n = p^r$ eine Primzahlpotenz, ζ eine primitive n-te Einheitswurzel, und $K = \mathbb{Q}(\zeta)$. Setze $\pi := 1 - \zeta$ und $P = (\pi)$, $\mathfrak{p} = (p)$. Dann ist P ein Primideal in $\mathcal{O}_K$ und $p\mathcal{O}_K = P^e$ mit*

$$e = e(P \mid \mathfrak{p}) = \varphi(p^r) = p^{r-1}(p-1)$$

und $f(P \mid \mathfrak{p}) = 1$. Also ist $\mathfrak{p}$ rein verzweigt in $K/\mathbb{Q}$.

Beweis. Ist ζ' eine weitere primitive p^r-te Einheitswurzel, so ist $\zeta' = \zeta^s$ mit $p \nmid s$ nach Lemma 7.1.2. Ebenso ist $\zeta = (\zeta')^t$ mit $p \nmid t$. Daraus folgt $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta')$ und $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$. Es gilt

$$\frac{1-\zeta'}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$$

und auch

$$\frac{1-\zeta}{1-\zeta'} = 1 + \zeta' + \cdots + (\zeta')^{t-1} \in \mathbb{Z}[\zeta]$$

Damit sind diese Elemente invertierbar, also Einheiten in $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$. Es folgt

$$\begin{aligned} p = \Phi_{p^r}(1) &= \prod_{\mathrm{ord}\zeta' = p^r} (1 - \zeta') \\ &= \prod_{\mathrm{ord}\zeta' = p^r} (1 - \zeta') \frac{1-\zeta}{1-\zeta'} \\ &= u \cdot (1-\zeta)^e \end{aligned}$$

für eine Einheit u in $\mathbb{Z}[\zeta]$. Das bedeutet $p\mathcal{O}_K = (1-\zeta)^e = P^e$ für die Ideale. Es sei $p\mathcal{O}_K$ das Produkt von g verschiedenen Primidealen in $\mathcal{O}_K$. Dann gilt nach dem Gradsatz für Galoiserweiterungen

$$e = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^r) = gef.$$

Daraus folgt aber sofort $g = f = 1$. Damit ist P ein Primideal mit Restklassengrad $f(P \mid \mathfrak{p}) = [\mathcal{O}_K/(p) : \mathbb{Z}/p] = 1$ und Verzweigungsindex $e(P \mid \mathfrak{p}) = \varphi(p^r)$. □

Lemma 7.2.2. *Sei $n = p^r$ eine Primzahlpotenz, ζ eine primitive n-te Einheitswurzel, und $K = \mathbb{Q}(\zeta)$. Dann gilt $N_{K/\mathbb{Q}}(1-\zeta) = p$.*

Beweis. Wegen $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^r)^\times$ sind die Galoiskonjugierten genau die ζ^j, wobei j ein Repräsentantensystem von $(\mathbb{Z}/p^r)^\times$ durchläuft. Also gilt nach Satz 2.4.3

$$N_{K/\mathbb{Q}}(1-\zeta) = \prod_{(j,p^r)=1} (1 - \zeta^j) = \Phi_{p^r}(1) = p.$$

□

Lemma 7.2.3. *Sei $n = p^r$ eine Primzahlpotenz, ζ eine primitive n-te Einheitswurzel, und $K = \mathbb{Q}(\zeta)$. Dann hat die $\mathbb{Q}$-Basis $\{1, \zeta, \ldots, \zeta^{e-1}\}$ mit $e = \varphi(p^r)$ die Diskriminante*

$$D(1, \zeta, \zeta^2, \ldots, \zeta^{e-1}) = \pm p^m,$$

mit $m = p^{r-1}(pr - r - 1)$. Von allen Primidealen (ℓ) in $\mathbb{Z}$ ist also nur (p) verzweigt, die anderen sind unverzweigt.

Beweis. Wegen Satz 2.4.19 gilt

$$D(1, \zeta, \zeta^2, \ldots, \zeta^{e-1}) = \pm N_{K/\mathbb{Q}}(\Phi_n'(\zeta)).$$

Wir müssen also die Norm von $\Phi_n'(\zeta)$ ausrechnen. Dazu differenziert man die Gleichung

$$\Phi_{p^r}(t) = \frac{t^{p^r} - 1}{t^{p^{r-1}} - 1}$$

und setzt dann $t = \zeta$ ein. Man erhält wegen $\zeta^{p^r-1} = \zeta^{-1}$

$$\zeta(\zeta^{p^{r-1}} - 1)\Phi_n'(\zeta) = p^r.$$

Nun nimmt man die Norm auf beiden Seiten. Auf der rechten Seite ist $N_{K/\mathbb{Q}}(p^r) = (p^r)^e$, und links gilt $N_{K/\mathbb{Q}}(\zeta) = \pm 1$ wegen

$$1 = a_0 = (-1)^e N_{K/\mathbb{Q}}(\zeta).$$

Hier ist a_0 der konstante Term des Minimalpolynoms von ζ, also 1. Es bleibt noch,

$$N_{K/\mathbb{Q}}(\zeta^{p^{r-1}} - 1) = \pm p^{p^{r-1}}$$

zu zeigen. Dann folgt nämlich

$$\begin{aligned} p^{re} &= N_{K/\mathbb{Q}}(p^r) = N_{K/\mathbb{Q}}(\zeta) \cdot N_{K/\mathbb{Q}}(\zeta^{p^{r-1}} - 1) \cdot N_{K/\mathbb{Q}}(\Phi_n'(\zeta)) \\ &= \pm 1 \cdot p^{p^{r-1}} \cdot N_{K/\mathbb{Q}}(\Phi_n'(\zeta)), \end{aligned}$$

also

$$N_{K/\mathbb{Q}}(\Phi_n'(\zeta)) = \pm \frac{p^{re}}{p^{p^{r-1}}} = \pm p^{rp^r - rp^{r-1} - p^{r-1}}.$$

Sei nun p^s eine p-Potenz mit $0 \leq s < r$. Wir zeigen

$$N_{K/\mathbb{Q}}(1 - \zeta^{p^s}) = p^{p^s}.$$

Für $s = 0$ folgt das aus Lemma 7.2.2, also $N_{K/\mathbb{Q}}(1 - \zeta) = p$. Da ζ^{p^s} eine primitive p^{r-s}-te Einheitswurzel ist, kann man das Lemma wiederum für p^{r-s} anwenden. Das ergibt $N_{\mathbb{Q}(\zeta^{p^s})/\mathbb{Q}}(1 - \zeta^{p^s}) = p$. Die Norm ist transitiv für Körpererweiterungen $K/M/\mathbb{Q}$, d.h., es gilt $N_{K/\mathbb{Q}}(\alpha) = N_{K/M}(N_{M/\mathbb{Q}}(\alpha))$ für $\alpha \in K$. Für $\alpha \in M$ gilt $N_{K/M}(\alpha) = \alpha^{[K:M]}$. Wir setzen $M = \mathbb{Q}(\zeta^{p^s})$. Dann ist nach dem Gradsatz für Körpererweiterungen

$$[K : M] = \frac{\varphi(p^r)}{\varphi(p^{r-s})} = p^s.$$

Es folgt also

$$\begin{aligned} N_{K/\mathbb{Q}}(1 - \zeta^{p^s}) &= N_{K/M}(N_{M/\mathbb{Q}}(1 - \zeta^{p^s})) \\ &= N_{K/M}(p) \\ &= p^{[K:M]} \\ &= p^{p^s}. \end{aligned}$$

Also ist die Diskriminante eine echte p-Potenz, und die Aussage über die Verzweigung folgt direkt aus Satz 6.4.1. □

Theorem 7.2.4. *Sei ζ eine primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$. Dann gilt $\mathcal{O}_K = \mathbb{Z}[\zeta]$ und $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ ist eine Ganzheitsbasis für $\mathcal{O}_K$ über $\mathbb{Z}$.*

Beweis. Im ersten Schritt beweisen wir das Resultat für Primzahlpotenzen $n = p^r$. Nach Satz 2.4.20 gilt $d\mathcal{O}_K \subseteq Z[\zeta]$ für die Diskriminante $d = D(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) = \pm p^m$ aus Lemma 7.2.3. Deshalb gilt

$$p^m \mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K.$$

In Lemma 7.2.1 hatten wir gesehen, daß $[\mathcal{O}_K/(\pi) : \mathbb{Z}/(p)] = 1$ gilt, also die Inklusion $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ einen Isomorphismus $\mathbb{Z}/(p) \simeq \mathcal{O}_K/(\pi)$ induziert. Deswegen gilt $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$, also auch

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi\mathcal{O}_K.$$

Multipliziert man mit π, so folgt $\pi\mathcal{O}_K = \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K$, also

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\zeta] + \pi\mathcal{O}_K \\ &= \mathbb{Z}[\zeta] + \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K \\ &= \mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K. \end{aligned}$$

Daraus erhält man iterativ

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^k\mathcal{O}_K$$

für alle $k \geq 1$. Wegen $(\pi^{\varphi(p^r)}) = (p)$ folgt

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + p^m\mathcal{O}_K \subseteq \mathbb{Z}[\zeta].$$

Für den allgemeinen Fall sei $n = p_1^{r_1} \cdots p_g^{r_g}$ und ζ eine primitive n-te Einheitswurzel. Dann kann man zeigen, daß

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{r_1}}) \cdots \mathbb{Q}(\zeta_{p_g^{r_g}})$$

und

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_g^{r_g}}] = \mathbb{Z}[\zeta]$$

gilt. Dazu braucht man folgendes Argument. Sind K und L zwei endliche Erweiterungen von $\mathbb{Q}$ mit $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$ und d der größte gemeinsame Teiler der Erzeuger von $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$ und $\mathcal{D}_{\mathcal{O}_L/\mathbb{Z}}$, so gilt

$$\mathcal{O}_{KL} \subseteq d^{-1}\mathcal{O}_K\mathcal{O}_L.$$

Für einen ausführlichen Beweis verweisen wir auf [12]. □

7.3 Fermatsche Gleichung

Kummer bewies den großen Satz von Fermat für reguläre Primzahlen. Wir wollen diesen Beweis hier vorstellen, wobei wir aus Zeitgründen nur den sogenannten *ersten Fall* behandeln, also mit $p \nmid xyz$ für die Gleichung

$$x^p + y^p = z^p.$$

Der zweite Fall ist $p \mid xyz$. Den Beweis beider Fälle haben wir immerhin schon für $p = 3$ in Satz 1.0.1 skizziert. Der erste Fall wurde dort erledigt, indem die Gleichung modulo 9 betrachtet wurde. Ebenso kann man auch noch den ersten Fall für $p = 5$ abhandeln, indem man die Gleichung modulo 25 studiert.

Wir wollen also ab jetz $p > 5$ und $p \nmid xyz$ annehmen. Weiterhin dürfen wir annehmen, daß x, y, z paarweise teilerfremd sind.

Sei ζ eine primitive p-te Einheitswurzel. Aus

$$t^p - 1 = \prod_{i=0}^{p-1} (t - \zeta^i)$$

erhält man durch Einsetzen von $t = -x/y$ und hochmultiplizieren

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y).$$

Lemma 7.3.1. *Die Elemente $x + \zeta^i y$ von $\mathbb{Z}[\zeta]$ sind paarweise teilerfremd.*

Beweis. Wir zeigen, daß die Ideale $(x + \zeta^i y)$ in $\mathbb{Z}[\zeta]$ paarweise teilerfremd sind für $i = 0, 1 \ldots, p-1$. Sei $P = (\pi) = (1 - \zeta)$ das eindeutige Primideal in $\mathbb{Z}[\zeta]$ über (p), siehe Lemma 7.2.1. Wegen $1 - \zeta^i = \left(\frac{1-\zeta^i}{1-\zeta}\right)(1 - \zeta) = u \cdot (1 - \zeta)$ mit einer Einheit u, ist $P = (1 - \zeta^k)$ für $1 \leq k \leq p - 1$. Angenommen, Q ist ein Primideal in $\mathbb{Z}[\zeta]$, das zwei verschiedene Ideale $(x + \zeta^i y)$ und $(x + \zeta^j y)$ teilt. Dann folgt

$$Q \mid (x + \zeta^j y) - (x + \zeta^i y) = ((\zeta^i - \zeta^j)y) = (\varepsilon \cdot (1 - \zeta)y) = Py$$

für eine Einheit ε. Da Q Primideal ist, folgt $Q = (1 - \zeta)$ oder $Q \mid y$. Ebenso gilt

$$Q \mid \zeta^i(x + \zeta^j y) - \zeta^j(x + \zeta^i y) = ((\zeta^i - \zeta^j)x) = Px,$$

also $Q = (1 - \zeta)$ oder $Q \mid x$. Da x und y teilerfremd sind, kann Q nicht beide teilen. Deshalb muß $Q = P$ gelten. Es folgt

$$x + y \equiv x + \zeta^i y \equiv 0 \mod P,$$

und daher $x + y \equiv 0 \mod p$ wegen $x + y \in P \cap \mathbb{Z} = (p)$. Das ergibt

$$z^p = x^p + y^p \equiv x + y \equiv 0 \mod p$$

und daher $p \mid z$, im Widerspruch zur Annahme $p \nmid xyz$. □

Lemma 7.3.2. *Für jedes $\alpha \in \mathbb{Z}[\zeta]$ gilt $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta]$. Es gibt also ein $b \in \mathbb{Z}$ mit $\alpha^p \equiv b \mod p$.*

Beweis. Sei $\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$ mit $b_i \in \mathbb{Z}$. Dann gilt

$$\begin{aligned}\alpha^p &\equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-2}\zeta^{p-2})^p \mod p \\ &= b_0^p + b_1^p + \cdots + b_{p-2}^p \mod p \\ &= b \mod p.\end{aligned}$$

□

Lemma 7.3.3. *Sei $\alpha = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}$ mit ganzen Koeffizienten, wovon wenigstens einer gleich Null ist. Gilt $n \mid \alpha$, also $\alpha \in n\mathbb{Z}[\zeta]$ für ein $n \in \mathbb{Z}$, so folgt $n \mid b_j$ für alle j.*

Beweis. Wegen $1 + \zeta + \cdots + \zeta^{p-1} = 0$ ist jede $(p-1)$-elementige Teilmenge von $\{1, \zeta, \ldots, \zeta^{p-1}\}$ eine $\mathbb{Z}$-Basis. Es gelte $b_i = 0$. Dann schreiben wir α in der $\mathbb{Z}$-Basis, die ζ^i auslässt. Dann folgt die Behauptung aus der Eindeutigkeit der Basisdarstellung. □

Definition 7.3. Sei ζ eine primitive n-te Einheitswurzel und $n \geq 3$. Dann heißt

$$\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$$

der *maximal reelle* Unterkörper von $\mathbb{Q}(\zeta)$.

In der Tat, unter jeder Einbettung von $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$ wird ζ^{-1} auf das komplex Konjugierte von ζ abgebildet, also auf $\overline{\zeta}$. Also ist das Bild von $\mathbb{Q}(\zeta)^+$ unter jeder Einbettung invariant unter komplexer Konjugation, und liegt daher in $\mathbb{R}$. Ein Zahlkörper K heißt übrigens *total reell*, wenn alle seine Einbettungen nach $\mathbb{C}$ schon in $\mathbb{R}$ liegen. Er heißt *total imaginär*, wenn keine davon in $\mathbb{R}$ liegt. Ein *CM-Körper* ist ein total imaginärer Zahlkörper, der eine quadratische Erweiterung eines total reellen Zahlkörper ist.
$\mathbb{Q}(\zeta)$ ist ein typisches Beispiel eines CM-Körpers, mit maximalem total reellen Unterkörper $\mathbb{Q}(\zeta)^+$.

Lemma 7.3.4. *Sei $n = p > 2$ eine Primzahl und ζ eine primitive p-te Einheitswurzel. Dann kann man jede Einheit u in $\mathbb{Z}[\zeta]$ schreiben als $u = \zeta^r v$, mit $r \in \mathbb{Z}$ und einer reellen Einheit v in $\mathbb{Q}(\zeta)^+$.*

Beweis. Sei $\alpha = u/\overline{u}$. Das ist eine Einheit in $\mathbb{Z}[\zeta]$, da u eine ist. Zudem haben alle Galois-Konjugierten von α den Absolutbetrag 1. Damit liegt α im Kern der logarithmischen Einbettung, der ja aus Einheitswurzeln besteht, siehe den Beweis in Theorem 5.1.5. In der Tat, jede ganze algebraische Zahl $\alpha \in C$, deren Konjugierte alle den Absolutbetrag 1 haben ist eine Einheitswurzel. Das Minimalpolynom von jeder Potenz von α hat dann nämlich beschränkte Koeffizienten in $\mathbb{Z}[x]$, also gibt es nur endlich viele solche Polynome, also nur endlich viele Potenzen von α. Die Einheitswurzeln sind alle von der Form $\pm\zeta^a$ mit $a \in \mathbb{Z}$. Wir können also

$$\alpha = u/\overline{u} = \pm\zeta^a$$

schreiben. Wir behaupten, daß das negative Vorzeichen nicht auftreten kann. Sei $u = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$ mit $b_i \in \mathbb{Z}$. Dann ist

$$\begin{aligned} u &\equiv b_0 + \cdots + b_{p-2} \mod (1-\zeta), \\ &\equiv b_0 + b_1\zeta^{-1} + \cdots + b_{p-2}\zeta^{-p+2} \mod (1-\zeta) \\ &\equiv \overline{u} \mod (1-\zeta). \end{aligned}$$

Gälte jetzt $u = -\zeta^a\overline{u}$, so wäre

$$\overline{u} \equiv u \equiv -\zeta^a\overline{u} \equiv -\overline{u} \mod (1-\zeta),$$

also $1-\zeta \mid 2\overline{u}$ in $\mathbb{Z}[\zeta]$. Da $\overline{u}$ eine Einheit ist, folgt $1-\zeta \mid 2$. Somit würde $(1-\zeta)$ über (2) liegen. Aber $(1-\zeta) \cap \mathbb{Z} = (p)$, mit $p > 2$. Das ist ein Widerspruch. Also gilt das positive Vorzeichen. Da p ungerade ist, gibt es $r \in \mathbb{Z}$ mit $2r \equiv a \mod p$. So können wir $\alpha = u/\overline{u} = +\zeta^{2r}$, also $u = \zeta^{2r}\overline{u}$ schreiben. Damit ist

$$\zeta^{-r}u = \zeta^r\overline{u} = \overline{\zeta^{-r}u}.$$

Setzt man $v := \zeta^{-r}u$, so gilt $u = \zeta^r v$ und $v = \overline{v}$. Also ist v eine reelle Einheit in $\mathbb{Q}(\zeta)^+$. □

Nun können wir Kummers Resultat für den ersten Fall beweisen.

Theorem 7.3.5 (Kummer)**.** *Sei $p > 5$ eine Primzahl, die nicht die Klassenzahl h von $\mathbb{Q}(\zeta)$ teilt, für eine primitive p-te Einheitswurzel. Dann hat die Fermatsche Gleichung*

$$x^p + y^p = z^p$$

keine ganzzahligen Lösungen mit $p \nmid xyz$.

Beweis. Zunächst können wir x, y, z teilerfremd wählen mit $p \nmid x-y$. Denn wäre $x \equiv y \equiv -z \mod p$, so wäre $-2z \equiv z \mod p$ und deshalb $p \mid 3z$. Wegen $p > 3$ und $p \nmid z$ ist das unmöglich. Also kann einer der obigen drei Kongruenzen nicht gelten. Nach möglicher Umordnung $x^p + (-z)^p = (-y)^p$ dürfen wir also immer annehmen, daß $p \nmid x - y$ gilt. Nun betrachten wir die Fermatsche Gleichung als Gleichung von Idealen in $\mathbb{Z}[\zeta]$, indem wir die Identität vor Lemma 7.3.1 benutzen:

$$(z)^p = (x^p + y^p) = (x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y).$$

Da $\mathbb{Z}[\zeta]$ ein Dedekindring ist, und die Ideale $(x+\zeta^i y)$ paarweise teilerfremd sind nach Lemma 7.3.1, kann man wegen der eindeutigen Idealfaktorisierung jedes Ideal auf der rechten Seite als p-te Potenz eines Ideals in $\mathbb{Z}[\zeta]$ schreiben, also etwa

$$(x+\zeta^i y) = \mathfrak{a}_i^p.$$

In der Klassengruppe von $\mathbb{Q}(\zeta)$ gilt $p[\mathfrak{a}_i] = [\mathfrak{a}_i^p] = [(x+\zeta^i y)] = [0]$, weil $(x+\zeta^i y)$ ein Hauptideal ist. Da die Klassengruppe eine endliche Gruppe ist, deren Ordnung nach

Voraussetzung nicht durch p geteilt wird, ist die Multiplikation mit p ein Gruppenisomorphismus. Es gibt also keine p-Torsion. Somit ist $[\mathfrak{a}_i] = [0]$, also jedes $\mathfrak{a}_i$ ein Hauptideal. Wir schreiben $\mathfrak{a}_i = (\alpha_i)$ mit einem $\alpha_i \in \mathbb{Z}[\zeta]$. Wir betrachten nur $i = 1$ und setzen $\alpha = \alpha_1$. Es ist also

$$x + \zeta y = u\alpha^p$$

für eine Einheit u in $\mathbb{Z}[\zeta]$. Nun wenden wir Lemma 7.3.4 an, um $u = \zeta^r v$ zu schreiben für eine Einheit v mit $\overline{v} = v$. Wegen Lemma 7.3.2 gibt es ein $b \in \mathbb{Z}$ mit $\alpha^p \equiv b \mod p$. Also ist

$$\begin{aligned} x + \zeta y &= u\alpha^p = \zeta^r v\alpha^p \equiv \zeta^r vb \mod p, \\ x + \overline{\zeta} y &= \overline{x + \zeta y} = \zeta^{-r} v(\overline{\alpha})^p \equiv \zeta^{-r} vb \mod p. \end{aligned}$$

Zusammen folgt

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1} y) \mod p,$$

oder

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \mod p. \tag{7.1}$$

Jetzt wollen wir Lemma 7.3.3 anwenden, mit $n = p$. Offensichtlich teilt p ja den Ausdruck links. Wären alle Potenzen von ζ in diesem Ausdruck verschieden, so wäre wegen $p > 5$ mindestens ein Koeffizient bezüglich der Darstellung in der $\mathbb{Z}$-Basis Null. Also besagte das Lemma, daß alle Koeffizienten durch p teilbar wären, also insbesondere $p \mid x$ und $p \mid y$ gälte. Das wäre ein Widerspruch zur Annahme, und wir wären fertig.
Wir müssen aber noch zeigen, daß die Zahlen $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ wirklich paarweise verschieden sind. Wegen $\zeta \neq 1$ und $\zeta^{2r} \neq \zeta^{2r-1}$ bleiben noch 3 Fälle.

1. Fall: Sei $\zeta^{2r} = 1$. Dann heißt (7.1) $\zeta y - \zeta^{-1} y \equiv 0 \mod p$, und Lemma 7.3.3 ergibt erneut einen Widerspruch, nämlich $p \mid y$.

2. Fall: Sei $\zeta^{2r-1} = 1$. Dann ist $\zeta^{2r} = \zeta$ und (7.1) heißt $(x - y) - (x - y)\zeta \equiv 0 \mod p$. das hieße $p \mid x - y$, was wir aber ausgeschlossen hatten.

3. Fall: Sei $\zeta^{2r-1} = \zeta$. Dann heißt (7.1) $x - \zeta^2 x \equiv 0 \mod p$, und Lemma 7.3.3 liefert $p \mid x$, also wiederum einen Widerspruch. □

Bemerkung 7.3.6. Auch den zweiten Fall, den Kummer bewiesen hat, kann man mit ähnlichen Argumenten führen. Er ist aber komplizierter als der erste Fall. Man schaue in [12] nach. Moderne Beweise verwenden hier eher Methoden der Iwasawa-Theorie. Insgesamt hat man damit Fermat's Theorem auch nur für **reguläre** Primzahlexponenten bewiesen. Leider gibt es ja unendlich viele irreguläre Primzahlen, siehe Bemerkung 4.3.8, für die man erheblich mehr tun muß. Kummers Beweis liefert trotzdem einen großen Beitrag zur Lösung der Fermatschen Gleichung, und hat viele weitere Entwicklungen ermöglicht.

8 Bewertungen und lokale Körper

8.1 Bewertungen

Definition 8.1. Eine *Bewertung* - oder auch *Absolut-Bewertung* - auf einem Körper K ist eine Funktion $K \to \mathbb{R}$, $x \mapsto |x|$ mit folgenden Eigenschaften.

(a) Es gilt $|x| > 0$, mit Ausnahme von $|0| = 0$.

(b) $|xy| = |x||y|$.

(c) $|x + y| \leq |x| + |y|$.

Der übliche Absolutbetrag $\mathbb{C} \to \mathbb{R}$, $z \mapsto |z| = \sqrt{z\overline{z}}$ ist eine Bewertung auf $\mathbb{C}$, ebenso seine Einschränkung auf $\mathbb{R}$.
Die Bedingungen (a) und (b) besagen auch, daß eine Bewertung ein Gruppenhomomorphismus $K^\times \to \mathbb{R}_+$ ist. Da die Gruppe $\mathbb{R}_+$ torsionsfrei ist, gilt $|\zeta| = 1$ für alle Einheitswurzeln ζ in $K^\times$, insbesondere also $|-1| = 1$ und $|-x| = |x|$ für alle $x \in K$.

Beispiel 8.1.1. *Sei K ein Zahlkörper, und $\sigma\colon K \hookrightarrow \mathbb{C}$ eine Einbettung von K nach $\mathbb{C}$. Dann definiert $|a|_\sigma = |\sigma(a)|$ eine Bewertung auf K.*

Definition 8.2. Durch $|a| = 1$ für alle $a \neq 0$ in K wird eine Bewertung definiert, die sogenannte *triviale Bewertung* auf K.

Lemma 8.1.2. *Sei K ein endlicher Körper. Dann ist jede Bewertung auf K trivial.*

Beweis. In einem endlichen Körper sind alle Elemente $a \neq 0$ Einheitswurzeln. Da $|\ |\colon K^\times \to \mathbb{R}_+$ ein Gruppenhomomorphismus ist, gilt $1 = |1| = |a^n| = |a|^n$ in $\mathbb{R}_+$, also $|a| = 1$. □

Definition 8.3. Eine Bewertung auf einem Körper K heißt *nicht-archimedisch*, falls (a), (b) und (c') gilt, mit

$$(c') \quad |x + y| \leq \max\{|x|, |y|\}.$$

Gilt nur (c) und nicht (c'), so heißt die Bewertung *archimedisch*.

Die Ungleichung (c') heißt auch ultra-metrische Dreiecksungleichung. Sie ist offenbar stärker als die gewöhnliche Dreiecksungleichung (c). Es gilt sogar immer die Gleichheit in (c'), außer wenn $|x| = |y|$ ist. Denn angenommen, es wäre $|x| < |y|$ und $|x + y| < \max\{|x|, |y|\} = |y|$. Dann wäre

$$|y| = |y + x - x| \leq \max\{|y + x|, |x|\} < |y|,$$

ein Widerspruch.

Beispiel 8.1.3. *Sei p eine Primzahl. Dann definiert $|a|_p := (1/p)^{\mathrm{ord}_p(a)}$ eine nicht-archimedische Norm auf $\mathbb{Q}$, die sogenannte p-adische Bewertung.*

Ist $a = a_0 p^r$ mit $\mathrm{ord}_p(a_0) = 0$, also $a_0 = \frac{m}{n}$ mit $(m,p) = (n,p) = 1$, so gilt $|a|_p = p^{-r}$. Offenbar definiert $a \mapsto |a|_p$ eine Bewertung auf $\mathbb{Q}$. Die Werte $|n|_p$ sind für alle $n \in \mathbb{Z}$ beschränkt, denn es gilt $|n|_p \leq 1$ für alle $n \in \mathbb{Z}$. Daher folgt aus dem nächsten Satz, daß die Bewertung nicht-archimedisch ist.

Satz 8.1.4. *Eine Bewertung $|\ |$ auf K ist genau dann nicht-archimedisch, wenn sie beschränkte Werte auf $\{m1 \mid m \in \mathbb{Z}\}$ annimmt.*

Beweis. Sei $|\ |$ nicht-archimedisch, und $m \in \mathbb{N}$. Dann gilt

$$|m1| = |1 + 1 + \cdots + 1| \leq |1| = 1,$$

und $|-1| = 1$, $|-m1| = |m1| \leq 1$. Es gelte umgekehrt $|m1| \leq N$ für alle $m \in \mathbb{Z}$ und ein $N \in \mathbb{N}$. Dann gilt, wegen $|\binom{n}{r}| \leq N$,

$$\begin{aligned} |x+y|^n = \left|\sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}\right| &\leq \sum_{r=0}^{n} \left|\binom{n}{r}\right| |x|^r |y|^{n-r} \\ &\leq (n+1)N \cdot \max\{|x|^n, |y|^n\} \\ &\leq (n+1)N \cdot \max\{|x|, |y|\}^n. \end{aligned}$$

Zieht man daraus die n-te Wurzel, so erhält man

$$|x+y| \leq \sqrt[n]{N(n+1)} \cdot \max\{|x|, |y|\}.$$

Das ergibt für $n \to \infty$ genau die ultra-metrische Dreiecksungleichung. □

Korollar 8.1.5. *Sei K ein Körper mit positiver Charakteristik. Dann besitzt K nur nicht-archimedische Bewertungen.*

Beweis. Wegen Charakteristik ungleich Null ist die Menge $\{m1 \mid m \in \mathbb{Z}\}$ endlich. Daher folgt die Behauptung aus dem Satz. □

Beispiel 8.1.6. *Sei K ein Zahlkörper und $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. Dann definiert*

$$|a|_{\mathfrak{p}} = (1/N(\mathfrak{p}))^{\mathrm{ord}_{\mathfrak{p}}(a)}$$

eine nicht-archimedische Bewertung auf K, die sogenannte $\mathfrak{p}$-adische Bewertung.

Offenbar ist Beispiel 8.1.3 ein Spezialfall hiervon mit $K = \mathbb{Q}$, und $\mathfrak{p} = (p)$.

Definition 8.4. Eine *Exponentialbewertung* auf K ist eine Abbildung $\nu\colon K \to \mathbb{R} \cup \{\infty\}$ mit folgenden Eigenschaften.

(a) Es gilt $\nu(x) < \infty$, mit Ausnahme von $\nu(0) = \infty$.

(b) $\nu(xy) = \nu(x) + \nu(y)$.

(c) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

Eine Exponentialbewertung ist die additive Version einer nicht-archimedischen multiplikativen Bewertung.

Satz 8.1.7. *Ist $|\ |$ eine nicht-archimedische Bewertung auf K, so definiert $\nu(x) = -\log(|x|)$ für $x \neq 0$ und $\nu(0) = \infty$ eine Exponentialbewertung auf K. Diese Zuordnung induziert eine Bijektion zwischen nicht-archimedischen Absolut-Bewertungen und Exponentialbewertungen.*

Definition 8.5. Zwei Exponentialbewertungen ν und μ auf K heißen *äquivalent*, falls es ein $t > 0$ gibt mit $\nu(x) = t\mu(x)$ für alle $x \in K$.
Zwei Absolut-Bewertungen $|\ |_1$ und $|\ |_2$ heißen *äquivalent*, falls es ein $t > 0$ gibt mit $|x|_1 = |x|_2^t$ für alle $x \in K$.

Für eine Bewertung $|\ |$ auf K definiert $d(x,y) = |x-y|$ eine Metrik, und damit eine Topologie auf K: für $a \in K$ bilden die offenen Mengen

$$U(a,\varepsilon) = \{x \in K \mid |x-a| < \varepsilon\}$$

für $\varepsilon > 0$ eine Basis für die Topologie.

Satz 8.1.8. *Es seien $|\ |_1$ und $|\ |_2$ zwei Bewertungen auf K, und $|\ |_1$ nicht-trivial. Dann sind folgende Aussagen gleichwertig.*

(a) $|\ |_1$ und $|\ |_2$ definieren die gleiche Topologie auf K.

(b) $|x|_1 < 1 \Rightarrow |x|_2 < 1$.

(c) $|\ |_1$ und $|\ |_2$ sind äquivalent.

Beweis. $(a) \Rightarrow (b)$: Wegen $|x^n| = |x|^n$ gilt $|x| < 1$ genau dann, wenn $x^n \to 0$ für $n \to \infty$. Aus (a) folgt also $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.

$(b) \Rightarrow (c)$: Da $|\ |_1$ nicht-trivial ist, gibt es ein $y \in K$ mit $|y|_1 > 1$. Dann ist $a := \log(|y|_2)/\log(|y|_1)$ wohldefiniert und es gilt $\log(|y|_2) = a\log(|y|_1)$, also

$$|y|_2 = |y|_1^a.$$

Sei $x \neq 0$ aus K. Dann gibt es eine reelle Zahl b mit $|x|_1 = |y|_1^b$. Um (c) zu zeigen, genügt es, $|x|_2 = |y|_2^b$ zu zeigen, wegen

$$|x|_2 = |y|_2^b = |y|_1^{ab} = |x|_1^a.$$

Dazu sei $\frac{m}{n} > b$ eine rationale Zahl mit $n > 0$. Dann gilt

$$|x|_1 = |y|_1^b < |y|_1^{\frac{m}{n}},$$

also

$$|x^n/y^m|_1 < 1.$$

Aus (b) folgt $|x^n/y^m|_2 < 1$. Da das für alle rationalen Zahlen $\frac{m}{n} > b$ gilt, bedeutet das

$$|x|_2 \leq |y|_2^b.$$

Die andere Ungleichung $|x|_2 \geq |y|_2^b$ folgt ganz analog, mit rationalen Zahlen $\frac{m}{n} < b$. Also gilt die Gleichheit.

$(c) \Rightarrow (a)$: Nach Voraussetzung ist eine ε-Umgebung bezüglich $|\ |_2$ eine ε^t-Umgebung bezüglich $|\ |_1$. Demnach stimmen die Topologien überein. □

8.2 Der Satz von Ostrowski

Alexander Markowich Ostrowski war ein ukrainischer Mathematiker, der von 1893−1986 lebte. Sein Resultat über Bewertungen beschreibt alle möglichen Bewertungen auf den rationalen Zahlen bis auf Äquivalenz. Wir schreiben $|\ |_p$ für die p-adischen Bewertungen auf $\mathbb{Q}$, und $|\ |_\infty$ für den Absolutbetrag auf $\mathbb{R}$.

Theorem 8.2.1 (Ostrowski)**.** *Sei $|\ |$ eine nicht-triviale Bewertung auf $\mathbb{Q}$.*

(a) Ist $|\ |$ archimedisch, so ist $|\ |$ äquivalent zu $|\ |_\infty$.

(b) Ist $|\ |$ nicht-archimedisch, so ist $|\ |$ äquivalent zu $|\ |_p$ für genau eine Primzahl p.

Beweis. Es seien $n, m > 1$ ganze Zahlen. Dann kann man

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

mit ganzen Zahlen $0 \leq a_i < n$ und $n^r \leq m$ schreiben. Sei $N = \max\{1, |n|\}$. Die Dreiecksungleichung ergibt

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq (r+1)N^r \sum_{i=0}^{r} |a_i|.$$

Ebenso gilt

$$|a_i| = |1 + \cdots + 1| \leq a_i|1| = a_i \leq n.$$

Zusammen hat man, wegen $r \leq \log(m)/\log(n)$,

$$|m| \leq (1+r)nN^r \leq \left(1 + \frac{\log(m)}{\log(n)}\right) n N^{\frac{\log(m)}{\log(n)}}.$$

Nun ersetzt man m in dieser Ungleichung durch m^k, mit $k \in \mathbb{N}$ und zieht die k-te Wurzel:

$$|m| \leq \left(1 + \frac{k\log(m)}{\log(n)}\right)^{\frac{1}{k}} n^{\frac{1}{k}} N^{\frac{\log(m)}{\log(n)}}.$$

Für $k \to \infty$ folgt

$$|m| \leq N^{\frac{\log(m)}{\log(n)}}. \tag{8.1}$$

Fall 1: Für alle $n > 1$ gilt $|n| > 1$. Dann ist $N = |n|$, und (8.1) liefert

$$|m|^{\frac{1}{\log(m)}} \leq |n|^{\frac{1}{\log(n)}}.$$

Aus Symmetriegräunden gilt sogar Gleichheit, und es gibt ein $c > 1$ mit

$$c = |m|^{\frac{1}{\log(m)}} = |n|^{\frac{1}{\log(n)}}$$

für alle natürlichen Zahlen $n, m > 1$. Also ist

$$|n| = c^{\log(n)} = e^{\log(c)\cdot\log(n)} = n^{\log(c)} = n^a$$

für alle $n > 1$. Es gilt also $|n| = |n|_\infty^a$, wobei $|\ |_\infty$ der übliche Absolutbetrag auf $\mathbb{Q}$ ist. Da sowohl $|\ |$ als auch $|\ |_\infty^a$ Gruppenhomomorphismen von $\mathbb{Q}^\times$ nach $\mathbb{R}_+$ sind, und diese auf einem Erzeugendensystem von $\mathbb{Q}$, nämlich auf den Primzahlen und -1, übereinstimmen, folgt $|\ | = |\ |_\infty^a$.

Fall 2: Es gibt ein $n > 1$ mit $|n| \leq 1$. Dann ist $N = 1$, und (8.1) liefert $|m| \leq 1$ für alle $m > 1$. Also ist die Bewertung nicht-archimedisch nach Satz 8.1.4. Es ist leicht zu sehen, daß für jede nicht-archimedische Bewertung von K die Menge

$$A := \{a \in K \mid |a| \leq 1\}$$

ein Unterring von K ist, mit genau einem maximalen Ideal

$$\mathfrak{m} := \{a \in K \mid |a| < 1\}.$$

Also ist A ein lokaler Ring. Für mehr Details siehe Abschnitt 5.3 in [1]. Es gilt $\mathbb{Z} \subseteq A$. Ist $ab \in \mathfrak{m}$, also $|a||b| = |ab| < 1$, so folgt entweder $|a| < 1$ oder $|b| < 1$, also $a \in \mathfrak{m}$ oder $b \in \mathfrak{m}$. Deshalb ist $\mathfrak{m}$ ein Primideal in A, und deshalb $\mathfrak{m} \cap \mathbb{Z}$ ein Primideal in $\mathbb{Z}$. Es kann nicht Null sein, sonst wäre die Bewertung trivial. Also ist $\mathfrak{m} \cap \mathbb{Z} = (p)$ für eine rationale Primzahl p. Ist m nicht durch p teilbar, so ist $m \notin \mathfrak{m}$, und deshalb $|m| = 1$. Mit $a = \log_{|p|}(\frac{1}{p})$ gilt $|p|^a = \frac{1}{p}$. Dann ist

$$|mp^r|^a = |m|^a|p|^{ar} = |p|^{ar} = \frac{1}{p^r} = |mp^r|_p.$$

Also gilt $|\ |^a = |\ |_p$ auf $\mathbb{Z}$, und damit auch auf $\mathbb{Q}$ wegen Multiplikativität. Somit sind $|\ |$ und $|\ |_p$ äquivalent. □

8.3 Diskrete Bewertungen

Definition 8.6. Eine Exponentialbewertung ν auf K heißt *diskret*, falls $\nu(K^\times) \subseteq \mathbb{R}$ diskret ist. Eine Absolut-Bewertung $|\ |$ heißt *diskret*, falls $|K^\times| \subseteq \mathbb{R}_+$ diskret ist.

Ist $\nu(K^\times)$ diskret in $\mathbb{R}$, so ist es ein Gitter in $\mathbb{R}$, und deshalb von der Form $\mathbb{Z}c$ für ein $c \in \mathbb{R}$. Dabei ist c das kleinste positive Element in $\mathbb{Z}c$. Wir können die Bewertung normieren, indem wir anstatt ν die äquivalente Bewertung $\nu' = \frac{1}{c}\nu$ betrachten. Dann heißt ν' *normiert*, und $\nu' \colon K^\times \to \mathbb{Z}$ ist ein surjektiver Gruppenhomomorphismus.

Beispiel 8.3.1. *Die p-adische Bewertung $|\ |_p$ auf $\mathbb{Q}$ ist diskret, und die zugehörige Exponentialbewertung ν_p, definiert durch*

$$\nu_p\left(\pm\prod_{q\in\mathbb{P}} q^{n_q}\right) = n_p$$

ist diskret und normiert.

Wir assoziieren zu jeder nicht-archimedischen Bewertung einen lokalen Bewertungsring, wie im Beweis von Satz 8.2.1.

Definition 8.7. Sei $|\ |$ eine nicht-archimedische Bewertung auf K, und ν eine assoziierte Exponentialbewertung. Es seien

$$\begin{aligned} A &= \{a \in K \mid |a| \leq 1\} = \{a \in K \mid \nu(a) \geq 0\} \\ U &= \{a \in K \mid |a| = 1\} = \{a \in K \mid \nu(a) = 0\} \\ \mathfrak{m} &= \{a \in K \mid |a| < 1\} = \{a \in K \mid \nu(a) > 0\}. \end{aligned}$$

Dann heißt A der *Bewertungsring* zu $|\ |$, oder zu ν, U die *Einheitengruppe* von A, und $A/\mathfrak{m}$ der Restklassenkörper von A.

Diese Bezeichnungen sind gerechtfertigt, denn A ist in der Tat ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, und U besteht aus Einheiten in A. Das Ideal $\mathfrak{m}$ ist deshalb maximal, weil es aus den Nicht-Einheiten besteht, denn für $a \in A$ mit $a \notin \mathfrak{m}$ gilt ja $|a| = 1$, und daher $|1/a| = 1/|a| = 1$, und somit $1/a \in A$, also a Einheit in A.

Bemerkung 8.3.2. Jede nicht-archimedische Bewertung auf einem Zahlkörper K ist diskret. Aber es gibt auch nicht-archimedische Bewertungen, die *nicht* diskret sind. Dazu sei $K = \overline{\mathbb{Q}}$ ein algebraischer Abschluß von $\mathbb{Q}$. Die p-adische Bewertung $|\ |_p \colon \mathbb{Q} \to \mathbb{R}$ lässt sich auf viele Weisen auf $\overline{\mathbb{Q}}$ fortsetzen. Allerdings gilt dann

$$|\overline{\mathbb{Q}}^\times|_p = \{p^r \mid r \in \mathbb{Q}\},$$

und das ist keinesfalls diskret in $\mathbb{R}_+$. Zum Beispiel ist $p^{1/n} \in \overline{\mathbb{Q}}^\times$ für alle n, also $1/\sqrt[n]{p} \in |\overline{\mathbb{Q}}^\times|$ mit $\lim_{n\to\infty} 1/\sqrt[n]{p} = 1$.

Lemma 8.3.3. *Sei $|\ |$ eine nicht-archimedische Bewertung auf einem Körper K. Dann ist $|\ |$ genau dann diskret, wenn $\mathfrak{m}$ ein Hauptideal ist.*

Beweis. Sei $|\ |$ diskret. Wähle ein $\pi \in \mathfrak{m}$ mit $|\pi|$ maximal. Das ist möglich, weil $|K^\times|$ diskret ist, und nach oben beschränkt ist. Sei $a \in \mathfrak{m}$. Dann gilt

$$\left|\frac{a}{\pi}\right| = \frac{|a|}{|\pi|} \leq 1,$$

also $a/\pi \in A$. Also gilt $a = \pi \cdot \frac{a}{\pi} \in \pi A$. Somit ist $\mathfrak{m} = \pi A$ ein Hauptideal in A. Sei umgekehrt $\mathfrak{m} = (\pi)$ ein Hauptideal. Dann ist $|K^\times| \leq \mathbb{R}_+$ die von $|\pi|$ erzeugte Untergruppe, also isomorph zu $\mathbb{Z}$. □

Beispiel 8.3.4. *Die p-adische Bewertung $|\ |_p$ auf $\mathbb{Q}$ ist diskret und ihr zugehöriger Bewertungsring ist*

$$A = \mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid (n,p) = 1\},$$

mit maximalem Ideal $\mathfrak{m} = pA$ und Restklassenkörper $A/pA \simeq \mathbb{F}_p$.

Das maximale Ideal $\mathfrak{m}$ ist also, wie erwartet, ein Hauptideal.

Allgemeiner sei K ein Zahlkörper mit Ganzzahlring $\mathcal{O}_K$, und $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. Dann ist die Abbildung $\nu_\mathfrak{p} \colon K^\times \to \mathbb{Z}$ mit $\nu_\mathfrak{p}(a) = n_\mathfrak{p}$,

$$a\mathcal{O}_K = \prod_{\mathfrak{q} \text{ prim}} \mathfrak{q}^{n_\mathfrak{q}}$$

eine Exponentialbewertung, und

$$|a|_\mathfrak{p} = N(\mathfrak{p})^{-\nu_\mathfrak{p}(a)} = (\#\mathcal{O}_K/\mathfrak{p})^{-\nu_\mathfrak{p}(a)}$$

eine zugehörige Absolut-Bewertung mit Bewertungsring

$$A = (\mathcal{O}_K)_\mathfrak{p} = \left\{ \frac{a}{b} \in K \mid a \in \mathcal{O}_K,\, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}.$$

Dieser Ring ist gerade die Lokalisierung von $\mathcal{O}_K$ nach $\mathfrak{p}$. Das maximale Ideal von A ist das Hauptideal $\mathfrak{p}A$, und der Restklassenkörper ist $A/\mathfrak{p}A$, welcher wegen Satz 6.1.7 isomorph zu dem üblichen Restklassenkörper (Definition 6.4) $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ von $\mathfrak{p}$ ist,

$$(\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} \simeq \mathcal{O}_K/\mathfrak{p}.$$

Definition 8.8. Ein *diskreter Bewertungsring* ist ein Integritätsbereich A, der ein Bewertungsring einer diskreten Bewertung auf dem Quotientenkörper K von A ist.

Folgende Charakterisierung diskreter Bewertungsringe haben wir in Theorem 5.3.16 in [1] erhalten.

Theorem 8.3.5. *Sei A ein Intergritätsbereich, der kein Körper ist. Dann sind folgende Aussagen äquivalent.*

(1) A ist ein diskreter Bewertungsring.

(2) A ist ein lokaler Hauptidealring.

(3) A ist ein faktorieller Ring mit bis auf Assoziierte eindeutigem irreduziblen Element.

(4) A ist ein Noetherscher lokaler Ring, dessen maximales Ideal ein Hauptideal ist.

(5) A ist ein lokaler Dedekindring.

8.4 Vervollständigungen

Sei K ein Körper mit einer nicht-trivialen Bewertung $|\ |$. Dann ist $d(a,b) = |a-b|$ eine Metrik auf K, und eine Folge (a_n) von Elementen aus K heißt eine *Cauchyfolge*, falls es für jedes $\varepsilon > 0$ ein N gibt mit

$$d(a_n, a_m) < \varepsilon$$

für alle $n, m > N$.

Beispiel 8.4.1. *Sei $K = \mathbb{Q}$ versehen mit der 5-adischen Metrik. Dann ist die Folge $a_n = \frac{1}{2^n}$ keine Cauchyfolge. Hingegen ist*

$$4, 34, 334, 3334, 33334, \ldots$$

eine Cauchyfolge.

Es gilt $d(a_n, a_{n+1}) = |2^{-(n+1)}|_5 = 5^0 = 1$, also ist (a_n) keine Cauchyfolge. Bei der zweiten Folge hat man für alle $m > n$

$$d(b_m, b_n) = 5^{-n}.$$

Diese Cauchyfolge konvergiert gegen $\frac{2}{3} \in \mathbb{Q}$, weil

$$3 \cdot 4 = 12,\ 3 \cdot 34 = 102,\ 3 \cdot 334 = 1002,\ 3 \cdot 3334 = 10002, \ldots$$

also $3 \cdot a_n - 2 \to 0$ für $n \to \infty$ in der 5-adischen Topologie.

Definition 8.9. Ein bewerteter Körper $(K, |\ |)$ heißt *vollständig*, wenn jede Cauchyfolge einen (notwendig eindeutigen) Limes in K hat.

Es ist wohlbekannt, daß $\mathbb{Q}$ bezüglich der Absolut-Bewertung nicht vollständig ist. Ebenso ist auch $\mathbb{Q}$ bezüglich jeder p-adischen Bewertung nicht vollständig. Der Satz von Ostrowski impliziert also folgendes Lemma.

Lemma 8.4.2. *Der Körper $\mathbb{Q}$ ist nicht vollständig bezüglich jeder seiner Absolut-Bewertungen.*

Beweis. Sei $|\ |$ eine Bewertung auf $\mathbb{Q}$. Wegen Theorem 8.2.1 müssen wir nur zeigen, daß $(\mathbb{Q}, |\ |_\infty)$ und $(\mathbb{Q}, |\ |_p)$ nicht vollständig sind. Im ersten Fall konstruiere eine Folge (a_n) mit rationalen a_n rekursiv durch $a_1 = 1$ und

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}.$$

Das ist eine Cauchyfolge in $\mathbb{Q}$ bezüglich des Absolutbetrags, die gegen keine rationale Zahl konvergiert. Hätte sie nämlich einen Limes x, so würde der notwendig $x^2 = 2$ erfüllen.
Sei nun $\mathbb{Q}$ versehen mit der p-adischen Metrik. Sei $a \in \mathbb{Z}$ mit $1 < a < p-1$. Dann ist die Folge

$$a_n = a^{p^n}$$

eine Cauchyfolge, die keinen Limes in $\mathbb{Q}$ hat. Es gilt

$$a_{n+1} - a_n = a^{p^{n+1}} - a^{p^n} = a^{p^n}(a^{\varphi(p^{n+1})} - 1),$$

und nach dem kleinen Satz von Fermat gilt $p^{n+1} \mid a^{\varphi(p^{n+1})} - 1$. Es folgt $|a_{n+1} - a_n|_p < p^{-n-1}$, und (a_n) ist eine Cauchyfolge. Für eine nicht-archimedische Bewertung $|\ |$ ist (a_n) nämlich genau dann eine Cauchyfolge, wenn

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0$$

gilt. Hätte sie einen Limes $x \in \mathbb{Q}$, so wäre $|x-a|_p < 1$ und $x^p = x$, Denn $x = \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} a_n^p = x^p$. Wegen $x \neq 0$ haben wir $x^{p-1} = 1$ und $x \in \mathbb{Q}$, also $x = 1$. Da $|x-a|_p < 1$ folgt $p \mid (x-a)$, also $p \mid (1-a)$. Dann ist $1 - a = pk$ für ein $k \in \mathbb{Z}$, d.h., $a = pk + 1$. Falls $k > 0$ dann folgt $a > p$, und falls $k < 0$, so folgt $a < 1$, im Widerspruch zu $1 < a < p - 1$. □

Um zu zeigen, daß $\mathbb{Q}$ mit der p-adischen Metrik unvollständig ist, reichte es auch, irrationale Elemente in $\mathbb{Q}_p$ zu finden. Dabei benutzt man das Henselsche Lemma. In der Tat besitzt $\mathbb{Q}_p$ für $p > 3$ alle primitiven $(p-1)$-sten Einheitswurzeln, und für $p = 2$ ist $\sqrt{-7} \in \mathbb{Q}_2 \setminus \mathbb{Q}$, für $p = 3$ ist $\sqrt{7} \in \mathbb{Q}_3 \setminus \mathbb{Q}$.

Der metrische Raum $(\mathbb{Q}, |\ |_\infty)$ und der ultrametrische Raum $(\mathbb{Q}, |\ |_p)$ sind also nicht vollständig. Sie können aber, wie jeder metrische Raum, in natürlicher Weise vervollständigt werden. Bevor wir dazu kommen, wollen wir noch erwähnen, daß die p-adische Metrik sich sehr von der Euklidischen Metrik unterscheidet.

Lemma 8.4.3. *Sei $|\ |$ eine nicht-archimedische Bewertung auf K. Sind $x, a, b \in K$ gegeben mit $|x-b| < |x-a|$, so folgt $|b-a| = |x-a|$. Jedes Dreieck in dem ultrametrischen Raum $(K; |\ |)$ ist also gleichschenklig.*

Beweis. Es gilt dann

$$\begin{aligned} |b-a| &= |b-x+x-a| = \max\{|b-x|, |x-a|\} \\ &= |x-a|. \end{aligned}$$

□

Ein kuriose Folgerung ist auch, daß jeder Punkt in einem Ball

$$B(x,r) = \{y \in K \mid |x-y| < r\}$$

automatisch Mittelpunkt ist. Damit sind Bälle, die sich schneiden, schon ineinander enthalten.

Theorem 8.4.4. *Sei K ein Körper mit Absolut-Bewertung $|\ |$. Dann existiert ein vollständiger bewerteter Körper $\widehat{K}$, der K als dichten Teilkörper enthält, und die Bewertung von K auf $\widehat{K}$ fortsetzt. Er hat die universelle Eigenschaft in folgendem Sinne. Jeder Homomorphismus $K \to L$ in einen vollständigen, bewerteten Körper L, der die Bewertung von K fortsetzt, lässt sich eindeutig zu einem Homomorphismus $\widehat{K} \to L$ fortsetzen.*

Beweis. Der Satz ist ein Spezialfall eines allgemeinen Satzes über die Vervollständigung metrischer Räume. Wir führen daher den Beweis nur in denjenigen Einzelheiten aus, die uns hier interessieren. Sei R der Ring der Cauchyfolgen in K, und

$$\mathcal{M} = \{(a_n) \in R \mid a_n \to 0\}$$

das Ideal der Nullfolgen. Es ist leicht zu sehen, daß $\mathcal{M}$ ein maximales Ideal ist. Man erhält also einen Körper

$$\widehat{K} = R/\mathcal{M},$$

der aus den Äquivalenzklassen solcher Cauchyfolgen besteht. Man hat eine kanonische Einbettung $K \hookrightarrow \widehat{K}$, indem man jedes $a \in K$ auf die konstante Cauchyfolge $(a) = (a, a, a, \ldots)$ abbildet bzw. auf deren Äquivalenzklasse a in $\widehat{K}$ abbildet. Die Bewertung $|\ |$ von K lässt sich $\widehat{K}$ fortsetzen, indem man für die Klasse a der Cauchyfolge (a_n) definiert

$$|a| = \lim_{n\to\infty} |a_n|.$$

Dieser Limes existiert wegen der Vollständigkeit von $\mathbb{R}$, da die Folge $(|a_n|)$ eine Cauchyfolge in $\mathbb{R}$ ist. In der Tat, $||a_m| - |a_n|| \leq |a_m - a_n|$. Nun kann man leicht zeigen, daß $\widehat{K}$ bezüglich seiner Bewertung vollständig ist. Die universelle Eigenschaft besagt insbesondere, daß $\widehat{K}$ bis auf kanonischen Isomorphismus eindeutig ist. Das Bild von K ist dicht in $\widehat{K}$, weil der Abschluß $\overline{K}$ in $\widehat{K}$ auch vollständig ist, und wie $\widehat{K}$ die universelle Eigenschaft erfüllt. Damit ist $\overline{K} \simeq \widehat{K}$. □

Korollar 8.4.5. *Eine Bewertung auf K ist genau dann nicht-archimedisch, wenn sie auf $\widehat{K}$ nicht-archimedisch ist. In diesem Fall gilt $|K| = |\widehat{K}|$.*

Beweis. Die Bewertung $|\ |$ auf K ist genau dann nicht-archimedisch, wenn sie beschränkte Werte auf $\{m1 \mid m \in \mathbb{Z}\}$ annimmt, siehe Satz 8.1.4. Da $|K|$ aber die Bewertung von K erweitert, und alle $m1$ in K liegen, gilt das Kriterium auch für $\widehat{K}$.
Sei $b \neq 0$ in $\widehat{K}$ gegeben. Dann exsitiert ein $c \in K$ mit $|b-c| < |c|$. Aus Lemma 8.4.3 folgt $|b| = |c|$, und daher $|K| = |\widehat{K}|$. □

Beispiel 8.4.6. *Die Vervollständigung von $\mathbb{Q}$ bezüglich $|\ |_\infty$ ist $\mathbb{R}$.*

Definition 8.10. Die Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Bewertung $|\ |_p$ wird mit $\mathbb{Q}_p$ bezeichnet, und heißt der Körper der *p-adischen Zahlen*. Sein Bewertungsring A wird mit $\mathbb{Z}_p$ bezeichnet, und heißt der Ring der ganzen p-adischen Zahlen.

Es ist also $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. Man kann sich p-adische Zahlen in $\mathbb{Q}_p$ als Äquivalenzklasse von Cauchyfolgen der Form

$$a_{-n}p^{-n} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots$$

mit ganzen Zahlen $0 \leq a_i < p$ vorstellen. Wenn die Koeffizienten mit negativem Index verschwinden, ist $a \in \mathbb{Z}_p$. Der Ring $\mathbb{Z}_p$ ist ein diskreter Bewertungsring, also ein Hauptidealring mit maximalem Ideal $p\mathbb{Z}_p$ und Quotientenkörper $\mathbb{Q}_p$. Es gilt $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$. Für alternative Beschreibungen von $\mathbb{Q}_p$ und $\mathbb{Z}_p$ als Limes projektiver Systeme siehe Beispiel 5.3.20 und nachfolgende Ausführungen in [1].

8.5 Lokale Körper

Ein lokaler Körper ist die Vervollständigung eines globalen Körpers bezüglich einer kanonischen Absolut-Bewertung. Die gängige Definition ist aber die folgende.

Definition 8.11. Ein *lokaler Körper* ist ein Körper, der ein vollständiger metrischer Raum bezüglich einer diskreten Bewertung ist und einen endlichen Restklassenkörper besitzt.

Zum Beispiel sind $\mathbb{R}$ und $\mathbb{C}$ lokale Körper. Sie heißen archimedisch. Dieses sind sogar die einzigen archimedischen lokalen Körper. Wenn die Bewertung nicht archimedisch ist, spricht man von nicht-archimedischen lokalen Körpern. Beispiele sind endliche Erweiterungen von $\mathbb{Q}_p$.

Beispiel 8.5.1. *Sei K ein Zahlkörper, $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$, und $K_\mathfrak{p}$ die Vervollständigung von K bezüglich der $\mathfrak{p}$-adischen Norm. Dann ist $K_\mathfrak{p}$ ein nicht-archimedischer lokaler Körper.*

Wir bezeichnen mit $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$ die Vervollständigung des Ringes $\mathcal{O}_K$ bezüglich der $\mathfrak{p}$-adischen Metrik. Man kann folgendes Resultat zeigen.

Satz 8.5.2. *Sei K ein globaler Körper mit Ganzzahlring $\mathcal{O}_K$, $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. Dann ist $\mathcal{O}_\mathfrak{p}$ ein diskreter Bewertungsring mit Quotientenkörper $K_\mathfrak{p}$ und endlichem Restklassenkörper $\mathcal{O}_K/\mathfrak{p}$. Der Ring $\mathcal{O}_\mathfrak{p}$ ist kompakt für die $\mathfrak{p}$-adische Metrik, und der Körper $K_\mathfrak{p}$ ist lokalkompakt.*

Ein metrischer Raum ist lokalkompakt, wenn jede beschränkte Folge eine konvergente Teilfolge hat. Die Kompaktheit von $\mathcal{O}_\mathfrak{p}$ zeigt man dadurch, daß man diesen Ring als inversen Limes von $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$ darstellt, der als abgeschlossene Teilmenge des unendlichen Produkts $\prod_n \mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$ kompakt ist, weil das Produkt nach den Satz von Tychonoff kompakt ist: alle Ringe $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$ sind endlich, also kompakt. Für $a \in K_\mathfrak{p}$ ist $a + \mathcal{O}_\mathfrak{p}$ eine offenen und kompakte Umgebung, also ist $K_\mathfrak{p}$ lokalkompakt.

Satz 8.5.3. *Sei K ein bewerteter Körper der Charakteristik Null. Dann sind folgende Aussagen äquivalent.*

(1) K ist ein lokaler Körper.

(2) K ist eine endliche Erweiterung von $\mathbb{Q}_p$.

(3) K ist vollständig, lokalkompakt und nicht diskret.

(4) K ist eine Vervollständigung $K_\mathfrak{p}$, wie in Beispiel 8.5.1.

Bemerkung 8.5.4. Es gibt auch einen analogen Satz für Körper der Charakteristik p. In diesem Fall ist K genau dann lokal, wenn K eine endliche Erweiterung von $\mathbb{F}_q((t))$ ist.

In der Zahlentheorie hat es sich als sehr nützlich herausgestellt, gewisse Probleme zuerst lokal zu untersuchen, also für lokale Körper, und dann global, also für globale Körper. Ein gutes Beispiel dafür ist der Satz von Hasse-Minkowski, der ein solches Kriterium für die Existenz von Nullstellen von quadratischen Formen liefert.

Theorem 8.5.5 (Hasse-Minkowski)**.** *Sei K ein globaler Körper und*

$$f(x) = a_1 x_1^2 + \cdots + a_n x_n^2$$

ein Polynom mit Koeffizienten in $K^\times$. Dann hat f genau dann eine nicht-triviale Nullstelle in K, wenn es eine nicht-triviale Nullstelle in jedem lokalen Körper hat, der als Vervollständigung von K bezüglich einer Absolut-Bewertung auftritt.

Hasse hat diesen Satz für $K = \mathbb{Q}$ in seiner Doktorarbeit von 1921 bewiesen, und 1924 auf alle Zahlkörper verallgemeinert. Wir wollen das Ergebnis für $\mathbb{Q}$ nochmals explizit nennen.

Korollar 8.5.6. *Sei $Q(x_1, \ldots, x_n)$ eine quadratische Form über $\mathbb{Q}$. Dann besitzt die Gleichung $Q(x_1, \ldots, x_n) = 0$ genau dann eine nicht-triviale Lösung über $\mathbb{Q}$, wenn sie eine nicht-triviale Lösung über $\mathbb{R}$ und allen p-adischen Körpern $\mathbb{Q}_p$ hat.*

Dabei meint *nicht-trivial*, daß nicht alle x_i gleich Null sind. Eine Richtung des Theorems ist einfach. Gibt es eine Lösung im globalen Körper K, so auch über dem lokalen Körper $K_\mathfrak{p}$. Die Umkehrung ist also die interessante Richtung. Zudem kann das Finden einer globalen Lösung viel schwieriger sein, als das von lokalen Lösungen. Der Übergang von globalen Körpererweiterungen zu lokalen Erweiterungen heißt auch *Lokal-Global-Prinzip*, und ist einer der wichtigsten Methoden der algebraischen Zahlentheorie.
In diesem Zusammenhang wollen wir noch das Henselsche Lemma nennen. Es gibt mehrere Versionen davon, weswegen manchmal von *Henselei* die Rede ist.

Lemma 8.5.7 (Hensel). *Sei K ein vollständiger, diskret bewerteter Körper mit diskretem Bewertungsring A, und maximalem Ideal $\mathfrak{m}$ von von A. Sei $f(t) \in A[t]$ ein Polynom, und a_0 eine einfache Nullstelle von f modulo $\mathfrak{m}$, also*

$$\begin{aligned} f(a_0) &\equiv 0 \mod \mathfrak{m}, \\ f'(a_0) &\not\equiv 0 \mod \mathfrak{m}. \end{aligned}$$

Dann gibt es eine eindeutiges $a \in A$ mit $f(a) = 0$ und $a \equiv a_0 \mod \mathfrak{m}$.

Beweis. Es sei $\mathfrak{m} = (\pi)$. Wir konstruieren induktiv Nullstellen von f modulo π^n für alle $n \in \mathbb{N}$, also $a_n \in A$ mit

$$f(a_n) \equiv 0 \mod \pi^{n+1}.$$

Für $n = 0$ ist das unsere Annahme. Für den Induktionsschritt benutzen wir die Taylerreihenentwicklung von f, und erhalten

$$\begin{aligned} f(a_n + h\pi^{n+1}) &= f(a_n) + h\pi^{n+1} f'(a_n) + \frac{1}{2!}(h\pi^{n+1})^2 f''(a_n) + \cdots \\ &= f(a_n) + h\pi^{n+1} f'(a_n) \mod \pi^{n+2} \\ &\equiv 0 \mod \pi^{n+2} \end{aligned}$$

für

$$h := -\frac{f(a_n)}{\pi^{n+1}} \cdot \frac{1}{f'(a_n)}.$$

Man beachte, daß h wegen $f'(a_n) \not\equiv 0 \mod \pi$ wohldefiniert ist. Wir setzen $a_{n+1} = a_n + h\pi^{n+1}$ und erhalten wegen $f(a_n) \equiv 0 \mod \pi^{n+1}$ dann

$$f(a_{n+1}) = f(a_n + h\pi^{n+1}) \equiv 0 \mod \pi^{n+2}.$$

Damit ist der Induktionsschluß gezeigt. Nach Konstruktion konvergiert diese Folge. Sei $a \in A$ ihr Limes. Wegen $a \equiv a_n \mod \pi^n$ erhalten wir $f(a) \equiv f(a_n) \equiv 0 \mod \pi^{n+1}$ für alle $n \in \mathbb{N}$, und deshalb $f(a) = 0$. □

Für $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$, $\mathfrak{m} = (p) = p\mathbb{Z}_p$ und $A/\mathfrak{m} \simeq \mathbb{F}_p$ erhalten wir folgende Version.

Korollar 8.5.8. *Sei f ein Polynom in $\mathbb{Z}_p[t]$ und $a_0 \in \mathbb{Z}_p$ mit $f(a_0) \equiv 0 \mod p\mathbb{Z}_p$, aber $f'(a_0) \not\equiv 0 \mod p\mathbb{Z}_p$. Dann gibt es ein eindeutiges $a \in \mathbb{Z}_p$ mit $f(a) \equiv 0 \mod p\mathbb{Z}_p$ und $a \equiv 0 \mod p\mathbb{Z}_p$.*

Ist f in $\mathbb{Z}(t] \subseteq \mathbb{Z}_p[t]$, so bedeutet die Voraussetzung $f(a_0) = 0$ und $f'(a_0) \neq 0$ in $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. Dann gibt es ein eindeutiges $a \in \mathbb{Z}_p$ mit $f(a) = 0$ und $a_0 = a$ in $\mathbb{F}_p$. Hat man also eine Nullstelle von f in dem endlichen Körper $\mathbb{F}_p$, so kann man sie *liften* nach $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. Über Nullstellen von f über endlichen Körpern weiß man aber folgenden Satz.

Satz 8.5.9 (Chevalley-Warning). *Sei $K = \mathbb{F}_{p^r}$ ein endlicher Körper und $f \in K[x_1, \ldots, x_n]$ ein Polynom mit Totalgrad $\deg(f) < n$. Dann gilt für $V_K := \{x \in K^n \mid f(x) = 0\}$ die Kongruenz $\#V_K \equiv 0 \mod p$.*

Korollar 8.5.10. *Jede quadratische Form über einem endlichen Körper mit mindestens drei Variablen hat eine nicht-triviale Nullstelle.*

Beweis. Wegen $0 \in V_K$ gilt $\#V_K \geq p$ nach dem Satz von Chevalley-Warning, sofern $n > \deg(Q) = 2$. □

Beispiel 8.5.11. *Die quadratische Form*

$$Q(x, y, z) = 5x^2 + 7y^2 - 13z^2$$

hat nach dem Satz von Hasse-Minkowski eine nicht-triviale Nullstelle in $\mathbb{Q}$.

Offenbar hat

$$5x^2 + 7y^2 - 13z^2 = 0$$

eine nicht-triviale Lösung über $\mathbb{R}$. Jede quadratische Form mit mindestens drei Variablen hat nach einem Satz von Chevalley-Warning über jedem endlichen Körper eine nicht-triviale Nullstelle. Es gibt also $a, b, c \in \mathbb{Z}$ mit

$$5a^2 + 7b^2 - 13c^2 \equiv 0 \mod p.$$

Dabei ist zumindest eine der drei Zahlen a, b, c nicht durch p teilbar, da die Lösung ja nicht-trivial ist. Ohne Einschränkung dürfen wir $p \nmid a$ annehmen. Damit aber die quadratische Form wirklich mindestens drei Variablen hat, müssen wir außerdem

$$p \neq 5, 7, 13$$

annehmen. Nun wenden wir das Henselsche Lemma an, in Form von Korollar 8.5.8. Das Polynom $f(t) = 5t^2 + 7b^2 - 13c^2$ hat dann nach Chevalley-Warning eine Nullstelle a mit $f(a) \equiv 0 \mod (p)$. Dann ist

$$f'(a) = 10a \not\equiv 0 \mod (p)$$

falls $p \neq 2, 5$ gilt; $p \nmid a$ hatten wir ja ebenfalls angenommen. Nun folgt aus dem Henselschen Lemma die Existenz eines $\overline{a} \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$ mit $f(\overline{a}) = 0$, und damit ist $(\overline{a}, b, c)$ eine Lösung von $5x^2 + 7y^2 - 13z^2 = 0$ über $\mathbb{Q}_p$ für jede Primzahl ungleich $2, 5, 7, 13$. Für die Primzahlen $2, 5, 7, 13$ lässt sich aber die gleiche Idee anwenden, mit geeigneten Polynomen f. Insgesammt haben wir nicht-triviale Lösungen von $5x^2 + 7y^2 - 13z^2 = 0$ über jedem $\mathbb{Q}_p$ und $\mathbb{R}$ gefunden. Damit gibt es auch eine nicht-triviale Lösung über $\mathbb{Q}$.

Allerdings hätten wir eine solche Lösung hier auch leichter haben können. Die Form hat genau dann eine nicht-triviale rationale Lösung, wenn sie eine nicht-triviale ganzzahlige Lösung hat. Ganzzahlige Lösungen lassen sich auch mit dem Satz von Legendre für ternäre quadratische Formen entscheiden. Wegen

$$\left(\frac{7 \cdot 13}{5}\right) = \left(\frac{5 \cdot 13}{7}\right) = \left(\frac{5 \cdot 7}{13}\right) = 1$$

gibt es eine ganzzahlige Lösung, z.B.

$$(x, y, z) = (3, 1, 2).$$

Allerdings gibt es natürlich allgemeinere Fälle, wo kein Satz von Legendre gilt, und das obige Verfahren angewendet werden kann.
Interessant ist für ternäre quadratische Formen vielleicht noch die Frage, wie man eine nicht-triviale ganzzahlige Lösung findet. Dazu gibt es Algorithmen.

Satz 8.5.12 (Holzer 1950)**.** *Seien a, b, c quadratfreie ganze Zahlen. Falls die Gleichung $ax^2 + by^2 + cz^2 = 0$ eine nicht-trivale ganzzahlige Lösung hat, dann gibt es eine solche Lösung mit*

$$|x| \leq \sqrt{|bc|},\ |y| \leq \sqrt{|ca|},\ |z| \leq \sqrt{|ab|}.$$

Der Satz von Holzer lässt sich in einen Algorithmus zum Lösen von $ax^2+by^2+cz^2 = 0$ übersetzen: man suche in dem angegebenen Bereich. Entweder man findet eine Lösung, oder die Gleichung hat keine. Allerdings ist die Größe des Suchraums exponentiell in der Länge der Eingabe, welche $O(\log(|abc|))$ ist. Daher ist dieses Verfahren für die Praxis im allgemeinen nicht brauchbar. Für effizientere Algorithmen siehe [5]. Hier ist ein Beispiel aus [5]:

Beispiel 8.5.13. *Die Gleichung*

$$x^2 - 3101464826902737254 09y^2 + 113922743z^2 = 0$$

hat eine nicht-triviale ganzzahlige Lösung. Eine solche, die der Bedingung von Holzer genügt, ist

$$(x, y, z) = (70647575606369,\ 5679,\ 6632499416).$$

Leider läßt sich der Satz von Hasse-Minkowski nicht so einfach auf multivariate Polynome höheren Grades übertragen. Ein bekanntes Gegenbeispiel ist das folgende von Selmer.

Beispiel 8.5.14. *Die Gleichung*

$$3x^3 + 4y^3 + 5z^3 = 0$$

hat eine nicht-triviale Lösung über jedem Körper $\mathbb{Q}_p$ und über $\mathbb{R}$, aber nicht über $\mathbb{Q}$.

Der schwierige Teil dieser Aussage besteht darin zu zeigen, daß es keine nicht-triviale rationale Lösung gibt. Die Existenz der lokalen Lösungen folgt aus der Hasse-Weil-Schranke für endliche Körper; sie lassen sich aber auch konkret angeben:

$$(x, y, z) = (-1, \sqrt[3]{3/4}, 0),\ (0, \sqrt[3]{5/4}, -1),$$
$$(5, -2\sqrt[3]{15/4}, -3),\ (-1, 0, \sqrt[3]{3/5}).$$

Alle Lösungen gibt es in $\mathbb{R}$, und mindestens eine existiert in einem vorgegebenen Körper $\mathbb{Q}_p$.

Zuletzt wollen wir noch eine weitere Anwendung des Satzes von Hasse-Minkowski angeben.

Satz 8.5.15 (Drei-Quadrate-Satz von Gauß)**.** *Sei n eine positive ganze Zahl. Dann sind äquivalent:*

(1) $n = a^2 + b^2 + c^2$ *für ganze Zahlen* a, b, c.

(2) n *hat nicht die Form* $4^\ell(8k + 7)$ *für* $k, \ell \in \mathbb{Z}_{\geq 0}$.

(3) $-n$ *ist kein Quadrat in* $\mathbb{Q}_2$.

Beweis. Wir skizzieren hier nur einige Ideen zum Beweis.
(1) $\Rightarrow$ (2): Diese Richtung ist leicht. Wir zeigen die Verneinung. Wenn n von der Form $4^\ell(8k - 1)$ ist, dann kann n *nicht* die Summe dreier Quadrate sein. Dazu bemerkt man zunächst folgende Tatsache. Wäre $4n = x_1^2 + x_2^2 + x_3^2$ die Summe dreier Quadrate, so auch n, und zwar $n = (x_1/2)^2 + (x_2/2)^2 + (x_3/2)^2$, weil alle x_i gerade Zahlen sein müssten. Deshalb muß man nur zeigen, daß $n = 8k + 7$ nicht Summe von drei Quadraten sein kann. Da aber ein Quadrat stets kongruent $0, 1, 4 \mod 8$ sein muß, kann die Summe dreier Quadrate nicht kongruent $7 \mod 8$ sein.
(2) $\Rightarrow$ (1) Hier zeigt man zunächst, daß wenn n die Summe dreier rationaler Quadrate ist, n auch die Summe dreier ganzzahliger Quadrate ist. Dann betrachtet man die nicht-ausgeartete quadratische Form

$$Q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 - nx_4^2$$

Die Gleichung $Q(x) = 0$ hat sicherlich eine nicht-triviale Nullstelle in $\mathbb{R}$, aber auch in jedem Körper $\mathbb{Q}_p$. Wenn p eine ungerade Primzahl ist, kann man das leicht folgern, weil mindestens drei der Koeffizienten der diagonalen quadratischen Form p-adische Einheiten sind, und es dann immer eine nicht-triviale Nullstelle in $\mathbb{Q}_p$ gibt. Für $p = 2$ benutzt man ein weiteres Argument, das mit quadratischen Resten zu tun hat. Jedenfalls kann man dann den Satz von Hasse-Minkowski anwenden, und erhält eine nicht-triviale rationale Lösung, bei der $x_4 \neq 0$ sein muß. Wir können also durch x_4^2 teilen, und erhalten eine Darstellung von n als Summe dreier rationaler Quadrate, und dann auch eine ganzzahlige Darstellung. □

9 Der Satz von Kronecker-Weber

Der Satz von Kronecker-Weber besagt, daß jede endliche abelsche Erweiterung von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten ist. Dabei bedeutet abelsche Erweiterung, daß die Erweiterung galoissch mit abelscher Galoisgruppe ist. Das Resultat wurde zuerst von Kronecker um 1853 formuliert, aber nicht vollständig bewiesen. Es gab eine Lücke im Fall, wo der Grad des Zahlkörpers eine Zweierpotenz ist. Weber veröffentlichte einen Beweis um 1886, der aber ebenfalls eine Lücke hatte. Ein vollständiger Beweis wurde 1896 von Hilbert gegeben.
Der Satz gehört in die sogenannte *Klassenkörpertheorie*, die abelsche Erweiterungen globaler Körper studiert. Diese Theorie ist ein wesentlicher Zweig der algebraischen Zahlentheorie. Mindestens drei Themen haben die Entwicklung der Klassenkörpertheorie am Ende des 19-ten Jahrhunderts angeregt: die Beziehungen zwischen abelschen Erweiterungen und Idealklassengruppen, Dichtigkeitssätze für Primzahlen und L-Reihen, sowie Reziprozitätsgesetze.
Die Resultate der allgemeinen Klassenkörpertheorie implizieren den Satz von Kronecker-Weber direkt. Das können wir hier nicht ausführen. Wir versuchen vielmehr, einen elementaren Beweis des Satzes von Kronecker-Weber zu skizzieren, der das Global-Lokal-Prinzip benutzt. Eine ausführliche Darstellung dieses Beweises findet man in [12]. Es gibt noch verschiedene andere Beweise des Satzes, elementare und weniger elementare.

9.1 Vorbereitungen

Sind K und L endliche Erweiterungen eines Körpers k, so heißt der kleinste Körper, der K und L enthält das *Kompositum* von K und L, und wird mit KL bezeichnet. Das folgende Lemma findet man zum Beispiel in [7]:

Lemma 9.1.1. *Es seien K und L endliche Galoiserweiterungen eines Körpers k. Dann sind $K \cap L$ und KL ebenfalls endliche Galoiserweiterungen von k, und die Gruppe $Gal(KL/k)$ ist isomorph zur der Untergruppe*

$$\{(\varphi, \psi) \in Gal(K/k) \times Gal(L/k) \mid \varphi_{|K\cap L} = \psi_{|K\cap L}\}$$

von $Gal(K/k) \times Gal(L/k)$.

Korollar 9.1.2. *Es seien K und L endliche Galoiserweiterungen eines Körpers k mit $K \cap L = k$. Dann gilt*

$$Gal(KL/k) \simeq Gal(K/k) \times Gal(L/k).$$

Sei L/K eine Erweiterung von lokalen Körpern. Falls $\mathbb{R} \subseteq K$, so gibt es nur drei Möglichkeiten $\mathbb{R}/\mathbb{R}$, $\mathbb{C}/\mathbb{R}$ und $\mathbb{C}/\mathbb{C}$. Für die Erweiterung $\mathbb{C}/\mathbb{R}$ definiert man den Verzweigungsindex $e(\mathbb{C}/\mathbb{R}) = 2$, und den Restklassengrad $f(\mathbb{C}/\mathbb{R}) = 1$. Wir wollen aber ab jetzt annehmen, daß $\mathbb{Q}_p \subseteq K$ gilt, für eine feste Primzahl p. Wir nennen dann solche Körper p-adisch.

Definition 9.1. Sei E/F eine Erweiterung von p-adischen Körpern mit lokalen Ganzzahlringen $\mathcal{O}_{\mathfrak{p}_E}$ und $\mathcal{O}_{\mathfrak{p}_F}$, maximalen Idealen $\mathfrak{p}_E$ und $\mathfrak{p}_F$ und Restklassenkörpern $\kappa(\mathfrak{p}_E) = \mathcal{O}_{\mathfrak{p}_E}/\mathfrak{p}_E$ und $\kappa(\mathfrak{p}_F) = \mathcal{O}_{\mathfrak{p}_F}/\mathfrak{p}_F$. Dann heißt

$$f(E/F) := [\kappa(\mathfrak{p}_E) : \kappa(\mathfrak{p}_F)]$$

der *Restklassengrad* von E/F. Der *Verzweigungsgrad* $e = e(E/F)$ ist definiert durch

$$\mathfrak{p}_F \mathcal{O}_E = \mathfrak{p}_E^e.$$

Die Erweiterung E/F heißt *unverzweigt*, falls $e(E/F) = 1$ gilt. Sie heißt allgemeiner *zahm verzweigt*, falls $p \nmid e(F/E)$ gilt für $p = \mathrm{char}(\kappa(\mathfrak{p}_F))$. Sie heißt *total verzweigt*, falls $f(E/F) = 1$.

Es gilt der lokale Gradsatz, also $[E : F] = e(E/F)f(E/F)$.

Lemma 9.1.3. *Es sei L/K eine Erweiterung von Zahlkörpern, P ein Primideal von $\mathcal{O}_L$, daß über dem Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ liegt. Es seien L_P und $K_\mathfrak{p}$ die Vervollständigungen von L und K bezüglich der P-adischen und $\mathfrak{p}$-adischen Metrik. Bezeichne die Vervollständigungen von $\mathcal{O}_L$ und $\mathcal{O}_K$ mit $\mathcal{O}_P$ und $\mathcal{O}_\mathfrak{p}$. Dann sind die Restklassenkörper von L_P und L isomorph, ebenso die von $K_\mathfrak{p}$ und K, und es gilt*

$$e(L_P \mid K_\mathfrak{p}) = e(P \mid \mathfrak{p}),$$
$$f(L_P \mid K_\mathfrak{p}) = f(P \mid \mathfrak{p}).$$

Beweis. Die Restklassenkörper $\kappa(P) = \mathcal{O}_P/\mathfrak{p}_L \simeq \mathcal{O}_L/P = k(P)$ und $\kappa(\mathfrak{p}) = \mathcal{O}_\mathfrak{p}/\mathfrak{p}_K \simeq \mathcal{O}_K/\mathfrak{p} = k(\mathfrak{p})$ sind isomorph, siehe Satz 8.5.2. Daher stimmen auch die Restklassengrade überein. Der Gradsatz in der lokalen Version besagt

$$[L_P : K_\mathfrak{p}] = e(L_P \mid K_\mathfrak{p}) \cdot f(L_P \mid K_\mathfrak{p}).$$

Daraus folgt auch die zweite Behauptung. □

Lemma 9.1.4. *Sei E/F eine Galoiserweiterung p-adischer Körper. Dann operiert $Gal(E/F)$ auf $\mathcal{O}_{\mathfrak{p}_E}$ und induziert einen surjektiven Gruppenhomomorphismus*

$$Gal(E/F) \to Gal(\kappa(\mathfrak{p}_E)/\kappa(\mathfrak{p}_F))$$

mit Kern $I(E/F)$. Es gilt

$$\#I(E/F) = e(E/F),$$
$$\#Gal(\kappa(\mathfrak{p}_E)/\kappa(\mathfrak{p}_F)) = f(E/F).$$

Die Teilerweiterung $E^{I(E/F)}/F$ ist unverzweigt.

Beweis. Der Beweis verläuft wie im Zahlkörperfall, siehe Satz 6.3.6, nur einfacher. □

Lemma 9.1.5. *Sei L/K eine endliche Galoiserweiterung von Zahlkörpern, $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$ und P ein Primideal in $\mathcal{O}_L$, das über $\mathfrak{p}$ liegt. Dann gilt*

$$Gal(L_P/K_\mathfrak{p}) \simeq D_P,$$
$$I(L_P/K_\mathfrak{p}) \simeq I_P.$$

Lemma 9.1.6. *Sind L_1/K und L_2/K Galoiserweiterungen p-adischer lokaler Körper mit $L = L_1L_2$ und $e(L_1/K) = 1$. Dann folgt $e(L/K) = e(L_2/K)$. Insbesondere folgt aus der Unverzweigtheit von L_2/K dann auch die von L/K.*

9.2 Reduktion auf die lokale Version

Unser Ziel ist es nun, die globale Version von Kronecker-Weber aus der lokalen herzuleiten. Das ist wiederum ein Beispiel für das Lokal-Global-Prinzip. Dazu formulieren wir erst einmal die lokale und globale Version.

Theorem 9.2.1 (Lokaler Kronecker-Weber)**.** *Sei $K/\mathbb{Q}_p$ eine endliche abelsche Körpererweiterung. Dann gibt es eine primitive n-te Einheitswurzel mit $K \subseteq \mathbb{Q}_p(\zeta_n)$.*

Beweis. Siehe Abschnitt 9.3. Übrigens gilt die lokale Version auch für $\mathbb{Q}_\infty = \mathbb{R}$, was aber nicht viel aussagt, weil es nur die endlichen Erweiterungen $\mathbb{R}/\mathbb{R}$ und $\mathbb{C}/\mathbb{R}$ gibt. □

Theorem 9.2.2 (Globaler Kronecker-Weber)**.** *Sei $K/\mathbb{Q}$ eine endliche abelsche Körpererweiterung. Dann gibt es eine primitive n-te Einheitswurzel mit $K \subseteq \mathbb{Q}(\zeta_n)$.*

Beweis. Es sei $K/\mathbb{Q}$ eine endliche, abelsche Erweiterung. Sei S die Menge der rationalen Primzahlen, für die $\mathfrak{p} = (p)$ in K verzweigt. Es gilt $S = \{p \in \mathbb{P} \mid p \mid d\}$ für die absolute Diskriminante d von K, siehe Satz 6.4.1. Sei P über $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ und betrachte die Vervollständigungen K_P und $\mathbb{Q}_p$. Dann ist $Gal(K_P/\mathbb{Q}_p) \simeq D_P \subseteq Gal(K/\mathbb{Q})$ ebenfalls abelsch, und $K_P/\mathbb{Q}_p$ ist eine abelsche Erweiterung. Nach Theorem 9.2.1 gibt es eine primitive n_p-te Einheitswurzel ζ_{n_p} mit $K_P \subseteq \mathbb{Q}_p(\zeta_{n_p})$. Sei p^{e_p} die genaue p-Potenz in n_p. Wir setzen

$$n := \prod_{p \in S} p^{e_p}.$$

Wir wollen nun $K \subseteq \mathbb{Q}(\zeta_n)$ zeigen. Dazu setzen wir

$$L := K(\zeta_n)$$

und zeigen $L = \mathbb{Q}(\zeta_n)$. Wegen Lemma 9.1.1 ist $Gal(L/\mathbb{Q})$ eine Untergruppe der abelschen Gruppe $Gal(K/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, also selbst abelsch. Also ist auch $L/\mathbb{Q}$ eine endliche, abelsche Erweiterung. Sie ist unverzweigt außerhalb S. Wenn nämlich (p) verzweigt ist

über L, so auch über K und daher $p \in S$. Sei L_Q die Vervollständigung an einem passenden Primideal Q über (p), also mit

$$\mathbb{Q}_p \subseteq K_P \subseteq L_Q.$$

Dann gilt, mit $(m,p) = 1$,

$$L_Q = K_P(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}m}) = \mathbb{Q}_p(\zeta_{p^{e_p}})\mathbb{Q}_p(\zeta_m).$$

Hierbei ist die Erweiterung $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ unverzweigt, und $\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p$ total verzweigt. Da aber $\mathbb{Q}(\zeta_{p^{e_p}})/\mathbb{Q}$ rein verzweigt ist über p, mit $e = \varphi(p^{e_p})$, siehe Lemma 7.2.1, so folgt aus Lemma 9.1.3

$$e(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p) = e = \varphi(p^{e_p}).$$

Damit hat die Trägheitsgruppe

$$I_p = I(L_Q/\mathbb{Q}_p)$$

genau $\varphi(p^{e_p})$ Elemente wegen Lemma 9.1.4. Sei nun I die Untergruppe von $Gal(L/\mathbb{Q})$, die von allen I_p mit $p \in S$ erzeugt wird. Da diese Gruppen abelsch sind, ist I das Bild von $\prod_p I_p$ unter der natürlichen Abbildung. Es gilt nun

$$\#I \leq \prod_{p\in S} \#I_p = \prod_{p\in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Nach Konstruktion von I ist die Erweiterung $L^I/\mathbb{Q}$ unverzweigt, wobei L^I der Fixkörper ist. Deshalb gilt $L^I = \mathbb{Q}$ nach Satz 6.4.3, dem Satz von Hermite-Minkowski. Also ist

$$[L : \mathbb{Q}] = \#I \leq \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Wegen $\mathbb{Q}(\zeta_n) \subseteq L$ folgt $L = \mathbb{Q}(\zeta_n)$. □

9.3 Beweis der lokalen Version

Sei $K/\mathbb{Q}_p$ eine endliche abelsche Erweiterung. Wir beginnen zuerst wieder mit ein paar Vorbereitungen.

Lemma 9.3.1. *Sei L/K eine unverzweigte Erweiterung von p-adischen Körpern vom Grad n. Dann gilt $L = K(\zeta_{q-1})$, wobei $q = p^n$ die Kardinalität des Restklassenkörpers von L ist.*

Beweis. Sei $e = e(L/K)$ und $f = f(L/K)$. Da L/K unverzweigt ist, gilt $e = 1$ und $n = [L : K] = f$. Die Erweiterung L/K ist genau dann galoissch, wenn die Erweiterung der Restklassenkörper $k(\mathfrak{p}_L)/k(\mathfrak{p}_E)$ galoissch ist. Da letztere eine endliche Erweiterung von endlichen Körpern ist, ist sie galoissch mit zyklischer Galoisgruppe. Nach Lemma 9.1.4 haben wir die Isomorphie

$$Gal(L/K) \simeq Gal(k(\mathfrak{p}_L)/k(\mathfrak{p}_E)).$$

Die Erweiterung $k(\mathfrak{p}_L)/k(\mathfrak{p}_E)$ hat als Galoiserweiterung ein primitives Element $\alpha \in k(\mathfrak{p}_L)$, mit $k(\mathfrak{p}_L) = k(\mathfrak{p}_E)(\alpha)$. Es ist eine primitive $(q-1)$-te Einheitswurzel, mit $(q-1, p) = 1$, und daher Nullstelle von $f(t) = t^n - 1$. Da $q-1$ und p teilerfremd sind, ist $f'(\alpha) \not\equiv 0 \mod \mathfrak{p}_L$, und wir können das Lemma von Hensel auf f anwenden. Es gibt also eine Nullstelle $\beta \in \mathcal{O}_{\mathfrak{p}_L}$ mit $f(\beta) \equiv 0 \mod \mathfrak{p}_L$ und $\beta \equiv \alpha \mod \mathfrak{p}_L$. Dann ist β eine Einheitswurzel und

$$[K(\beta) : K] \geq [k(\mathfrak{p}_E)(\alpha) : k(\mathfrak{p}_E)] = [k(\mathfrak{p}_L) : k(\mathfrak{p}_E)] = [L : K].$$

Also folgt $L = K(\beta) = K(\zeta_{q-1})$. □

Lemma 9.3.2. *Sei L/K eine total und zahm verzweigte Erweiterung von endlichen Erweiterungen von $\mathbb{Q}_p$ mit $[L : K] = e$. Dann existiert ein Erzeuger π des maximalen Ideals $\mathfrak{p}_K$ des Bewertungsringes von K mit $L = K(\pi^{1/e})$.*

Beweis. Nach Voraussetzung gilt $f = f(E/F) = 1$ und

$$e(L/K) = [L : K] = ef = e$$

mit $p \nmid e$. Seien π_L und π_K Primelemente, die die maximalen Ideale $\mathfrak{p}_L$ und $\mathfrak{p}_K$ erzeugen. Dann gilt $K(\pi_L) = L$, wegen $K(\pi_L) \subseteq L$, und da die Erweiterung $L/K(\pi_L)$ ebenfalls Verzweigungsindex e hat, also $[L : K(\pi_L)] = e = [L : K]$ gilt. Nach Definition gilt

$$\pi_L^e = u\pi_K$$

für eine Einheit $u \in \mathcal{O}_{\mathfrak{p}_L}^\times$. Wegen $f = 1$ gilt $\kappa(\mathfrak{p}_L) = \kappa(\mathfrak{p}_K)$ für die Restklassenkörper. Also gibt es eine Einheit $v \in \mathcal{O}_{\mathfrak{p}_K}^\times$ mit $\overline{u} = \overline{v}$ für die Restklassen. Das Element $x = v\pi_k/\pi_L^e$ hat Restklasse $\overline{x} = \overline{1} \in \kappa(\mathfrak{p}_L)$. Nun können wir das Lemma von Hensel auf $f(t) = t^e - x$ anwenden, das ja eine Nullstelle bei $\overline{1} \in \kappa(\mathfrak{p}_L)$ hat. Diese Nullstelle ist einfach, weil die Ableitung $\overline{e}\overline{t}^{e-1}$ außerhalb von $\overline{0}$ nicht verschwindet, wegen $p \nmid e$. Es gibt also ein $y \in \mathcal{O}_{\mathfrak{p}_L}^\times$ mit $y^e = x$. Setzen wir nun $\pi = v\pi_K$, so erhalten wir

$$L = K(y\pi_L) = K(\sqrt[e]{v\pi_K}) = K(\sqrt[e]{\pi}).$$

□

Lemma 9.3.3. *Die Erweiterung $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ist total verzweigt mit Verzweigungsindex $e = p - 1$, und kann als $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{1/(p-1)})$ geschrieben werden.*

Beweis. Sei $L = \mathbb{Q}_p(\zeta_p)$ und $K = \mathbb{Q}_p$. Dann ist das maximale Ideal von $\mathcal{O}_{\mathfrak{p}_L}$ durch $\mathfrak{p}_L = (\pi_L)$ mit $\pi_L = 1 - \zeta_p$ gegeben. Es gilt $\mathfrak{p}_K = (p) = (1 - \zeta_p)^{p-1}$. Der Beweis verläuft jetzt wie in Lemma 9.3.2. Es ist

$$u^{-1} = \frac{\pi_K}{\pi_L^e} = \frac{p}{(1 - \zeta_p)^{p-1}}.$$

Wir behaupten, daß $u^{-1} \equiv -1 \mod \mathfrak{p}_L$ ist. Dann kann man $v = -1$ nehmen und erhält wie oben $L = K(\sqrt[e]{v\pi_K}) = K(\sqrt[p-1]{-p})$. Die Behauptung folgt aber aus dem Satz von Wilson und $\zeta_p \equiv 1 \mod \mathfrak{p}_L$:

$$\frac{p}{(1-\zeta_p)^{p-1}} = \prod_{i=1}^{p-1} \frac{1-\zeta_p^i}{1-\zeta_p} = \prod_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \zeta_p^j \right) \equiv (p-1)! \equiv -1 \mod \mathfrak{p}_L.$$

□

Jetzt können wir den Beweis des lokalen Kronecker-Weber Theorems skizzieren. Da die abelsche Gruppe $Gal(K/\mathbb{Q}_p)$ nach dem Hauptsatz ein Produkt von zyklischen Gruppen von Primzahlpotenzordnung ist, können wir K als Kompositum von Erweiterungen von $\mathbb{Q}_p$ schreiben, deren Galoisgruppe zyklisch von Primzahlpotenzordnung ist, siehe Lemma 9.1.1. Deshalb dürfen wir also ohne Einschränkung annehmen, daß $Gal(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r$ gilt für eine Primzahl q und ein $r \in \mathbb{N}$.

Fall 1: $q \neq p$**.**

Sei L die maximal unverzweigte Teilerweiterung von K. Sie ist durch den Fixkörper der Trägheitsgruppe gegeben. Wegen Lemma 9.3.1 gilt

$$L = \mathbb{Q}_p(\zeta_n)$$

für ein $n \in \mathbb{N}$. Sei $e = [K : L]$. Da e eine Potenz von q ist, gilt $p \nmid e$. Also ist K total und zahm verzweigt über L. Deshalb existiert nach Lemma 9.3.2 ein $\pi \in \mathcal{O}_{\mathfrak{p}_L}$ mit $\mathfrak{p}_L = (\pi)$ und $K = L(\pi^{1/e})$. Da $L/\mathbb{Q}_p$ unverzweigt ist, erzeugt auch p das maximale Ideal $\mathfrak{p}_L = (\pi)$. Also können wir $\pi = -pu$ schreiben, mit einer Einheit $u \in \mathcal{O}_{\mathfrak{p}_L}^\times$. Auch $L(u^{1/e})/L$ ist unverzweigt, weil $(e, p) = 1$ gilt und u eine Einheit ist, und deshalb die Diskriminante von $f(t) = t^e - u$ nicht durch p teilbar ist. Insbesondere ist die Erweiterung $L(u^{1/e})/\mathbb{Q}_p$ unverzweigt, und somit abelsch. Damit ist $K(u^{1/e})/\mathbb{Q}_p$ das Kompositum von zwei abelschen Erweiterungen $K/\mathbb{Q}_p$ und $L(u^{1/e})/\mathbb{Q}_p$, also selbst abelsch. Damit ist auch jede Teilerweiterung abelsch, insbesondere auch $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$.

Weil die Erweiterung $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ galoissch ist, muss sie alle e-ten Wurzeln von $-p$ enthalten, also alle e-ten Einheitswurzeln (wir können zwei Wurzeln durch einander teilen, um eine e-te Einheitswurzel zu erhalten). Aber $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ ist total verzweigt, während $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ unverzweigt ist. Das ist ein Widerspruch, es sei denn $\mathbb{Q}_p(\zeta_e)$ ist schon gleich $\mathbb{Q}_p$, d.h., $\zeta_e \in \mathbb{Q}_p$. Das kann aber nur für $e \mid p-1$ gelten, da der Restklassenkörper $\mathbb{F}_p$ von $\mathbb{Q}_p$ nur die $(p-1)$-ten Einheitswurzeln enthält.

Es gilt, wie oben erwähnt, $K \subseteq L((-p)^{1/e}, u^{1/e})$. Aber einerseits ist $L(u^{1/e})$ unverzweigt über L, also $L(u^{1/e}) = L(\zeta_m)$ für ein m wegen Lemma 9.3.1; andererseits gilt aber wegen $e \mid p-1$ auch

$$\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$$

wegen Lemma 9.3.3. Zusammengenommen bedeutet das

$$K \subseteq L((-p)^{1/e}, u^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n, \zeta_p, \zeta_m) \subseteq \mathbb{Q}_p(\zeta_{mnp}).$$

Fall 2: $q = p \neq 2$.

Sei $K/\mathbb{Q}_p$ eine endliche abelsche Erweiterung. Wie oben erwähnt, dürfen wir

$$Gal(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r = \mathbb{Z}/p^r$$

annehmen. Wir können zwei weitere Erweiterungen von $\mathbb{Q}_p$ mit dieser Galoisgruppe konstruieren, nämlich eine unverzweigte Erweiterung $K_u/\mathbb{Q}_p$ vom Grad p^r, und eine total verzweigte Erweiterung $K_r/\mathbb{Q}_p$ vom Grad p^r. In der Tat, $K_u = \mathbb{Q}_p(\zeta_{p^{p^r}-1})$ ist unverzweigt vom Grad p^r, und hat daher eine zyklische Galoisgruppe der Ordnung p^r. Sei K_r der Teilkörper vom Index $p-1$ von $\mathbb{Q}_p(\zeta_{p^{r+1}})$. Die Erweiterung $\mathbb{Q}_p(\zeta_{p^{r+1}})/\mathbb{Q}_p$ hat den Grad $p^r(p-1)$. Wegen $p > 2$ ist die Galoisgruppe zyklisch. Damit ist die Erweiterung $K_r/\mathbb{Q}_p$ total verzweigt mit zyklischer Galoisgruppe $\mathbb{Z}/p^r$. Wegen $K_r \cap K_u = \mathbb{Q}_p$ gilt nach Korollar 9.1.2

$$Gal(K_rK_u/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^r)^2.$$

Nun gilt entweder $K \subseteq K_rK_u \subseteq \mathbb{Q}_p(\zeta_{p^{r+1}(p^{p^r}-1)})$, oder $K \not\subseteq K_rK_u$. Im zweiten Fall hätten wir

$$Gal(K(\zeta_{p^{p^r}-1}, \zeta_{p^{r+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^r)^2 \times \mathbb{Z}/p^s$$

für ein $s > 0$. Diese Gruppe hat $(\mathbb{Z}/p)^3$ als Quotienten, also erhielten wir eine Erweiterung von $\mathbb{Q}_p$ mit Galoisgruppe $(\mathbb{Z}/p)^3$. Das ist wegen Lemma 9.3.5 unmöglich. Wir sind also fertig, wenn wir dieses Lemma bewiesen haben. Dazu brauchen wir allerdings noch folgendes Lemma aus der Kummertheorie.

Lemma 9.3.4. *Sei K ein Körper der Characteristik ℓ mit ℓ und n teilerfremd, $L = K(\zeta_n)$, und $M = L(a^{1/n})$ für ein $a \in L^\times$. Definiere einen Homomorphismus $\omega : Gal(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ durch die Relation $\zeta_n^{\omega(g)} = \zeta_n^g$. Dann ist M/K galoissch und abelsch genau dann wenn*

$$a^g/a^{\omega(g)} \in (L^\times)^n \qquad \forall g \in Gal(M/K). \tag{9.1}$$

Lemma 9.3.5. *Für $p > 2$ gibt es keine Erweiterung von $\mathbb{Q}_p$ mit Galoisgruppe $(\mathbb{Z}/p)^3$.*

Beweis. Es sei $\pi = \zeta_p - 1$ das uniformisierende Element von $\mathbb{Q}_p(\zeta_p)$. Aus $Gal(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p)^3$ folgt auch $Gal(K(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p)^3$, und $K(\zeta_p)$ ist abelsch über $\mathbb{Q}_p$ mit Galoisgruppe $(\mathbb{Z}/p)^\times \times (\mathbb{Z}/p)^3$. Wir können Kummertheorie anwenden auf $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$. Damit erhalten wir eine Untergruppe $B \subseteq \mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$, die isomorph zu $(\mathbb{Z}/p)^3$ ist. Damit folgt $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, B^{1/p})$. Sei $\omega\colon Gal(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times$ die kanonische Abbildung. Nach Lemma 9.3.4 gilt

$$b^g/b^{\omega(g)} \in (\mathbb{Q}_p(\zeta_p)^\times)^p \qquad \forall b \in B, g \in Gal(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p),$$

da $\mathbb{Q}_p(\zeta_p, b^{1/p}) \subseteq K(\zeta_p)$ ebenfalls abelsch ist über $\mathbb{Q}_p$. Wir erinnern an die Struktur von $\mathbb{Q}_p(\zeta_p)^\times$. Das maximale Ideal von $\mathbb{Z}_p[\zeta_p]$ ist erzeugt von π, und jede Einheit von $\mathbb{Z}_p[\zeta_p]$ ist kongruent zu einer $(p-1)$-ten Einheitswurzel modulo π. Also ist

$$\mathbb{Q}_p(\zeta_p)^\times = \pi^{\mathbb{Z}} \times (\zeta_{p-1})^{\mathbb{Z}} \times U_1,$$

wobei U_1 die Menge aller Einheiten von $\mathbb{Z}_p[\zeta_p]$, die kongruent zu 1 modulo π sind bezeichnet, und entsprechend

$$(\mathbb{Q}_p(\zeta_p)^\times)^p = \pi^{p\mathbb{Z}} \times (\zeta_{p-1})^{p\mathbb{Z}} \times U_1^p.$$

Wir wählen nun einen Repräsentanten $a \in L^\times$ eines von Null verschiedenen Elements von B. Ohne Einschränkung dürfen wir annehmen, daß $a = \pi^m u$ für ein $m \in \mathbb{Z}$ und ein$u \in U_1$ ist. Dann gilt

$$\frac{a^g}{a^{\omega(g)}} = \frac{(\zeta_p^{\omega(g)} - 1)^m}{\pi^{m\omega(g)}} \frac{u^g}{u^{\omega(g)}};$$

aber $v_\pi(\pi) = v_\pi(\zeta_p^{\omega(g)} - 1) = 1$. Also ist die Bewertung auf der rechten Seite gleich $m(1-\omega(g))$, welches nur ein Vielfaches von p für alle g sein kann, wenn $m \equiv 0 \pmod{p}$. Hier haben wir benutzt, daß p ungerade ist. Mit anderen Worten, wir hätten $m = 0$ und $a = u \in U_1$ wählen können.

Was $u^g/u^{\omega(g)}$ betrifft, so kann man leicht zeigen, daß U_1^p die Menge der Einheiten kongruent 1 modulo π^{p+1} ist (Übungsaufgabe). Wegen $\zeta_p = 1 + \pi + O(\pi^2)$ können wir $u = \zeta_p^b(1 + c\pi^d + O(\pi^{d+1}))$ schreiben, mit $c \in \mathbb{Z}$ und $d \geq 2$. Da $\pi^g/\pi \equiv \omega(g) \pmod{\pi}$ ist, erhalten wir

$$\begin{aligned} u^g &= \zeta_p^{b\omega(g)}(1 + c\omega(g)^d\pi^d + O(\pi^{d+1})), \\ u^{\omega(g)} &= \zeta_p^{b\omega(g)}(1 + c\omega(g)\pi^d + O(\pi^{d+1})). \end{aligned}$$

Aber beide müssen kongruent sein modulo π^{p+1}. Deswegen gilt entweder $d \geq p+1$ oder $d \equiv 1 \pmod{p-1}$, wobei letzteres nur für $d = p$ auftreten kann.

Insgesamt bedeutet das, daß die Menge der möglichen Elemente u erzeugt ist von ζ_p und $1 + \pi^p$. Diese beiden Elemente erzeugen aber nur eine Untergruppe von U_1/U_1^p, die isomorph zu $(\mathbb{Z}/p)^2$ ist, wogegen $B \cong (\mathbb{Z}/p)^3$ ist. Das ist ein Widerspruch. □

Fall 3: $p = q = 2$.

Dieser Fall geht eigentlich ähnlich wie der vorherige, bereitet aber mehr Schwierigkeiten, weil unter anderem $\mathbb{Q}_2$ sehr wohl eine Erweiterung mit Galoisgruppe $(\mathbb{Z}/2)^3$ zulässt. Allerdings läßt $\mathbb{Q}_2$ keine Erweiterung zu mit Galoisgruppe $(\mathbb{Z}/2)^4$ oder $(\mathbb{Z}/4)^3$. Damit läßt sich die Argumentation des vorherigen Falles auch hier durchführen. Wir verweisen auf [12]. Wer es selbst versuchen möchte, findet eine Anleitung in den folgenden Übungsaufgaben.

1. Man zeige, in der Notation des Beweises von Lemma 9.3.5, daß U_1^p genau die Menge der Einheiten ist, die kongruent 1 modulo π^{p+1} ist. (Hinweis: Für die erste Richtung schreibe man $u \in U_1$ als eine Potenz von ζ_p mal einer Einheit, die kongruent 1 modulo π^2 ist. Für die zweite Richtung benutze man die Binomialreihe für $(1 + x)^{1/p}$.)

2. Man zeige, daß es für jedes $r > 0$ eine Erweiterung von $\mathbb{Q}_2$ mit Galoisgruppe $\mathbb{Z}/2 \times (\mathbb{Z}/2^r)^2$ gibt, die in einem Körper $\mathbb{Q}_2(\zeta_n)$ enthalten ist.

3. Angenommen $K/\mathbb{Q}_2$ ist eine $\mathbb{Z}/2^r$-Erweiterung, die in keinem Körper $\mathbb{Q}_2(\zeta_n)$ enthalten ist. Man zeige, daß dann eine Erweiterung von $\mathbb{Q}_2$ exsitiert mit Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^4$ oder $(\mathbb{Z}/4\mathbb{Z})^3$.

4. Man beweise mittels Kummertheorie, daß es keine Erweiterung von $\mathbb{Q}_2$ mit Galoisgruppe $(\mathbb{Z}/2)^4$ gibt.

5. Man zeige, daß es keine Erweiterung von $\mathbb{Q}_2$ gibt mit Galoisgruppe $(\mathbb{Z}/4)^3$.
(Hinweis: Ansonsten gäbe es eine Erweiterung von $\mathbb{Q}_2$, die $\mathbb{Q}_2(\sqrt{-1})$ enthielte, mit Galoisgruppe $\mathbb{Z}/4$. Dann hätte die Gleichung $A^2 + B^2 = -1$ Lösungen in $\mathbb{Q}_2$, Widerspruch.)

Literaturverzeichnis

[1] D. Burde: *Commutative Algebra.* Vorlesungsskript (2009), 1–87.

[2] L. Claborn, *Every abelian group is a class group.* Pacific J. Math. **18**, No. 2 (1966), 219–222.

[3] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, **138** (1993). Springer-Verlag, Berlin.

[4] T. Coquand T, H. Lombardi: *A short proof for the Krull dimension of a polynomial ring.* American Math. Monthly. **112** (2005), no. 9, 826–829.

[5] J. E. Cremona, D. Rusin: *Efficient solution of rational conics.* Math. Comp. **72** (2003), no. 243, 1417–1441.

[6] K. Ireland, M. Rosen: *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics **84** (1990). Springer-Verlag, New York.

[7] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[8] H. Koch: *Zahlentheorie.* Vieweg-Verlag (1997).

[9] J. M. Masley, H. L. Montgomery: *Cyclotomic fields with unique factorization.* J. Reine Angew. Math. **287** (1976), 248–256.

[10] J. Neukirch: *Algebraische Zahlentheorie.* Grundlehren der mathematichen Wissenschaften (1992). Springer-Verlag, Berlin.

[11] H. M. Stark: *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. Journal **14** (1967), 1–27.

[12] L. C. Washington: *Introduction to cyclotomic fields.* Springer-Verlag (1997).