

Algebraische Zahlentheorie I

Prof. Dr. Uwe Jannsen
Wintersemester 2007/08

Inhaltsverzeichnis

1	Die Gaußschen Zahlen	1
2	Algebraische Zahlkörper und ganze Zahlen	4
3	Norm, Spur und Diskriminante	8
4	Ideale in Dedekindringen	17
5	Primzerlegungen in Erweiterungen	23
6	Zyklotomische Körper	30
7	Zyklotomische Körper und die Fermat-Vermutung	35
8	Primzerlegung und Galoistheorie	43
9	Das quadratische Reziprozitätsgesetz	53
10	Minkowski-Theorie	57
11	Die Klassengruppe	69
12	Die Einheitengruppe	73
13	Lokalisierungen	79
14	Diskriminante und Verzweigung	82
15	Bewertungen	87
16	Komplettierungen	93
17	Vollständige nicht-archimedische Körper	99
18	Zahlkörper und ihre Komplettierungen	104

1 Die Gaußschen Zahlen

Dies sind die Elemente des Rings

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C},$$

$i = \sqrt{-1}$. Sein Studium zeigt bereits einige Aspekte der algebraischen Zahlentheorie.

1.1 $\mathbb{Q}(i) = \mathbb{Q}[i]$ ist eine Körpererweiterung von \mathbb{Q} mit Grad $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ (i ist algebraisch über \mathbb{Q} mit Minimalpolynom $x^2 + 1$).

1.2 Als abelsche Gruppe ist $\mathbb{Z}[i] \cong \mathbb{Z}^2$, eine freie abelsche Gruppe vom Rang 2.

1.3 $\mathbb{Q}(i)$ identifiziert sich mit dem Quotientenkörper von $\mathbb{Z}[i]$, vermöge

$$\begin{aligned} \text{Quot}(\mathbb{Z}[i]) &\xrightarrow{\sim} \mathbb{Q}(i) \\ \frac{a + bi}{c + di} &\longmapsto (a + bi) \cdot (c + di)^{-1} \quad (\text{für } (c, d) \neq (0, 0)). \end{aligned}$$

Für $\alpha = a + bi \in \mathbb{Q}(i)$ definiere

- die Norm $N(\alpha) = (a + bi)(a - bi) = a^2 + b^2$
- die Spur $T(\alpha) = (\alpha + bi) + (a - bi) = 2a$.

Dann ist $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ und $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

Lemma 1.4 (a) $\alpha = a + bi \in \mathbb{Z}[i]$ ist Einheit in $\mathbb{Z}[i]$ genau dann, wenn $N(\alpha) \in \{\pm 1\}$.

(b) Die Einheiten in $\mathbb{Z}[i]$ sind $1, -1, i, -i$.

Beweis: (a) α Einheit, $\beta = c + di$ Inverses $\Rightarrow \alpha\beta = 1 \Rightarrow 1 = N(1) = N(\alpha) \cdot N(\beta) \Rightarrow N(\alpha)$ Einheit in $\mathbb{Z} \Rightarrow N(\alpha) \in \{\pm 1\}$. Umgekehrt ist in $\mathbb{Q}(i)$ für $\alpha = a + bi \neq 0$

$$\alpha^{-1} = \frac{a - bi}{N(\alpha)} \in \mathbb{Q}(i)$$

und dies liegt in $\mathbb{Z}[i]$ für $N(\alpha) \in \{\pm 1\}$.

(b) $a, b \in \mathbb{Z}$, $a^2 + b^2 \in \{\pm 1\} \Rightarrow (a, b) = (1, 0)$ oder $(-1, 0)$ oder $(0, 1)$ oder $(0, -1)$.

Lemma 1.5 $\mathbb{Z}[i]$ ist euklidisch, also insbesondere faktoriell (ZPE-Ring).

Beweis: $\mathbb{Z}[i]$ ist euklidisch bezüglich der Funktion

$$\begin{aligned} \mathbb{Z}[i] &\longrightarrow \mathbb{N} \cup \{0\} \\ \alpha &\longmapsto N(\alpha) \end{aligned}$$

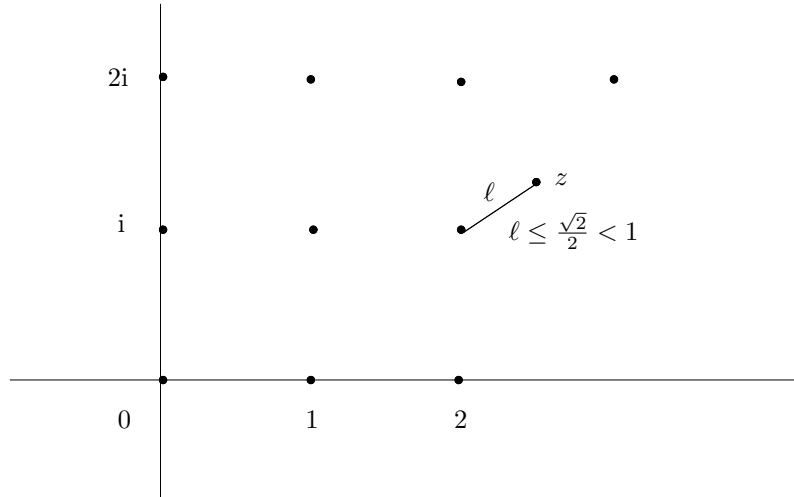
Sind nämlich $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, so gibt es $\gamma \in \mathbb{Z}[i]$ mit

$$\alpha = \gamma\beta + \delta, \quad N(\delta) < N(\beta).$$

Denn es ist $|\alpha| = \sqrt{N(\alpha)}$ der gewöhnliche Betrag in \mathbb{C} , und es genügt, ein $\gamma \in \mathbb{Z}[i]$ zu finden mit

$$\left| \frac{\alpha}{\beta} - \gamma \right| < 1.$$

Dies gilt aber für jede Zahl $z \in \mathbb{C}$ an Stelle von $\frac{\alpha}{\beta}$, da die Masche des Gitters $\mathbb{Z}[i]$ in \mathbb{C} die Diagonale der Länge $\sqrt{2}$ hat



Wir erhalten hieraus die zahlentheoretische Anwendung

Satz 1.6 Eine Primzahl $p \neq 2$ ist genau dann Summe von 2 Quadraten in \mathbb{Z} ,

$$p = a^2 + b^2, \quad a, b \in \mathbb{Z},$$

wenn $p \equiv 1 \pmod{4}$.

Bemerkung: (Allgemein kann man zeigen: $n = \pm p_1^{n_1} \dots p_r^{n_r} \in \mathbb{Z}$ ist Summe von 2 Quadraten $\Leftrightarrow n > 0$ und n_i gerade für $p_i \equiv 3(4)$).

Beweis: Die Idee ist, die Gleichung $p = a^2 + b^2$ zu deuten als

$$p = a^2 + b^2 = (a + bi)(a - bi) = N(a + bi).$$

Wir zeigen

Satz 1.7 Für eine Primzahl $p \neq 2$ sind äquivalent:

- (i) $p \equiv 1 \pmod{4}$.
- (ii) Es gibt ein $x \in \mathbb{Z}$ mit $-1 \equiv x^2 \pmod{p}$ (“-1 ist ein quadratischer Rest modulo p ”).
- (iii) p ist zerlegt in $\mathbb{Z}[i]$, d.h., kein Primelement in $\mathbb{Z}[i]$.
- (iv) $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$.

Beweis: (iv) \Rightarrow (i): Sei $p = a^2 + b^2$. Von den Zahlen a und b muss dann eine gerade und eine ungerade sein, da p ungerade ist. Wir benutzen nun die folgende Beobachtung, die noch öfter nützlich sein wird:

$$(1.7.1) \quad \begin{array}{l} \text{Ist } m \text{ gerade, so ist } m \equiv 0 \text{ oder } 2 \pmod{4}, \text{ also } m^2 \equiv 0 \pmod{4}. \\ \text{Ist } m \text{ ungerade, so ist } m \equiv 1 \text{ oder } 3 \pmod{4}, \text{ also } m^2 \equiv 1 \pmod{4}. \end{array}$$

Hieraus folgt $p = a^2 + b^2 \equiv 1 \pmod{4}$.

(i) \Rightarrow (ii): Wir erinnern uns (aus der Algebra), dass die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch von der Ordnung $p - 1$ ist. Nach der Theorie der zyklischen Gruppen ist also für $a \in \mathbb{Z}$, $(a, b) = 1$ und $\bar{a} = a \pmod{p}$

$$\bar{a} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2 \Leftrightarrow \bar{a}^{\frac{p-1}{2}} = 1.$$

Für $a = -1$ ist also $\overline{-1}$ ein Quadrat genau dann, wenn $(-1)^{\frac{p-1}{2}} = 1$, also wenn $p \equiv 1 \pmod{4}$.

(ii) \Rightarrow (iii): Sei $x \in \mathbb{Z}$ mit $-1 \equiv x^2 \pmod{p}$. Dann

$$p \mid x^2 + 1 = (x + i) \cdot (x - i).$$

Aber $p \nmid (x + i), (x - i)$ (denn $\frac{x \pm i}{p} \notin \mathbb{Z}[i]$). Also ist p kein Primelement im faktoriellen Ring $\mathbb{Z}[i]$.

(iii) \Rightarrow (iv): Sei $p = \alpha \cdot \beta$ mit Nicht-Einheiten $\alpha, \beta \in \mathbb{Z}[i]$. Dann ist

$$p^2 = N(p) = N(\alpha) \cdot N(\beta).$$

Nach 1.4. (a) sind $N(\alpha), N(\beta)$ keine Einheiten in \mathbb{Z} ; es gilt also $p = N(\alpha) = a^2 + b^2$ für $\alpha = a + bi$.

Wir betrachten noch eine andere Anwendung der Gaußschen Zahlen:

Satz 1.8 Die ganzzahligen Lösungen der Gleichung

$$x^2 + y^2 = z^2$$

mit $x, y, z > 0$ und $(x, y, z) = 1$ (pythagoräische Tripel) sind gegeben durch die Tripel mit

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

mit $u, v \in \mathbb{Z}$, $u > v > 0$ und $(u, v) = 1$, u, v nicht beide ungerade, bzw. durch die Tripel die man durch Vertauschung von x und y erhält.

Beweis: Diese Konstruktion liefert natürlich Pythagoräische Tripel. Umgekehrt schreiben wir die Gleichung als

$$z^2 = (x + yi)(x - yi) = N(x + yi).$$

Wir behaupten, dass dann

$$x + yi = \varepsilon \cdot \alpha^2$$

mit $\alpha \in \mathbb{Z}[i]$ und ε Einheit in $\mathbb{Z}[i]$. (Mit $\alpha = u + vi$ ergibt sich dann $\{x, y\} = \{\pm u^2 - v^2, \pm 2uv\}$).

Im faktoriellen Ring $\mathbb{Z}[i]$ genügt es zu zeigen: ist π ein Primelement mit $\pi \mid x + yi$, so teilt π die Zahl $x + yi$ mit einer geraden Potenz. Dies gilt für z^2 , also genügt es zu zeigen $\pi \nmid x - yi$.

Wir bemerken, dass z ungerade ist: x und y sind nicht beide gerade – da $(x, y, z) = 1$ – und nicht beide ungerade, da sonst $z^2 \equiv 2 \pmod{4}$ (nach (1.7.1)), was nicht sein kann.

Angenommen $\pi \mid x + yi, x - yi$. Dann folgt $\pi \mid 2x, \pi \mid z$. Andererseits sind $2x, z$ relativ prim (z ungerade, x, y, z relativ prim), also $r2x + sz = 1$ für $r, s \in \mathbb{Z}$. Es folgt $\pi \mid 1$ in $\mathbb{Z}[i]$; Widerspruch!

2 Algebraische Zahlkörper und ganze Zahlen

Definition 2.1 (a) Ein algebraischer Zahlkörper ist ein Körper K von endlichem Grad über \mathbb{Q} . Seine Elemente heißen algebraische Zahlen.

(b) Eine algebraische Zahl heißt ganz, wenn sie Nullstelle eines normierten Polynoms $f(x) \in \mathbb{Z}[x]$ ist.

Allgemeiner, für Ringe (kommutativ, mit Eins):

Definition 2.2 Sei $A \subseteq B$ eine Ringerweiterung.

(a) Ein Element $b \in B$ heißt ganz über A , wenn es einer Gleichung (*Ganzheitsgleichung*)

$$(2.2.1) \quad b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

mit $n \in \mathbb{N}$ und Koeffizienten $a_0, \dots, a_{n-1} \in A$ genügt.

(b) B heißt ganz über A , wenn alle Elemente $b \in B$ ganz über A sind.

Proposition 2.3 Für eine Ringerweiterung $A \subseteq B$ und ein Element $b \in B$ sind äquivalent.

(i) b ist ganz über A .

(ii) Der Unterring $A[b] \subseteq B$ ist als A -Modul endlich erzeugt.

(iii) Es existiert ein endlich erzeugter A -Untermodul $M \subseteq B$ mit $1 \in M$ und $b \cdot M \subseteq M$.

Bemerkung: Sei A ein kommutativer Ring mit Eins. Ein A -Modul ist eine abelsche Gruppe $(M, +)$ mit einer Verknüpfung $A \times M \rightarrow M, (a, m) \mapsto am$, für die dieselben Regeln gilt wie bei Vektorräumen über einem Körper:

$$\begin{aligned} a(m_1 + m_2) &= am_1 + am_2 \\ (a_1 + a_2)m &= a_1m + a_2m \\ a(bm) &= (ab)m \\ 1m &= m \end{aligned}$$

für alle $a, a_1, a_2 \in A$ und $m, m_1, m_2 \in M$. Weiter heißt M endlich erzeugt, wenn es endlich viele Elemente $m_1, \dots, m_n \in M$ gibt mit

$$M = Am_1 + Am_2 + \dots + Am_n := \{a_1m_1 + \dots + a_nm_n \mid a_1, \dots, a_n \in A\}.$$

Dann heißt $\{m_1, \dots, m_n\}$ ein Erzeugendensystem von M .

Ist $A \subseteq B$ eine Ringerweiterung, so ist B durch die Multiplikation in B ein A -Modul.

Beweis von Proposition 2.3 : (i) \Rightarrow (ii): Sei

$$(*) \quad b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

und M der endlich erzeugte A -Modul $A + Ab + \dots + Ab^{n-1} \subseteq B$. Dann ist $b^n \in M$, und durch Multiplikation von $(*)$ und Induktion folgt $b^i \in M$ für alle $i \geq 0$, also $A[b] = M$.

(ii) \Rightarrow (iii) ist trivial.

(iii) \Rightarrow (i): Sei $M = Am_1 + \dots + Am_n$ ein endlich erzeugter A -Untermodule von B . Gilt $bM \subseteq M$, so erhalten wir ein Gleichungssystem

$$\begin{aligned} bm_1 &= a_{11}m_1 + \dots + a_{1n}m_n \\ &\dots \\ &\dots \\ &\dots \\ bm_n &= a_{n1}m_1 + \dots + a_{nn}m_n \end{aligned}$$

mit Koeffizienten $a_{ij} \in A$. Für die $(n \times n)$ -Matrix mit Koeffizienten in B

$$C = bE_n - (a_{ij}) = \begin{pmatrix} b - a_{11} & & -a_{1n} \\ & \ddots & \\ -a_{n1} & & b - a_{nn} \end{pmatrix}$$

($E_n = (n \times n)$ -Einheitsmatrix) gilt also

$$C \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Dabei wird die Anwendung einer $(n \times n)$ -Matrix auf einen Vektor aus B^n durch die üblichen, aus der Linearen Algebra für Körper bekannten Formeln definiert.

Wir benutzen nun aus der Linearen Algebra

Lemma 2.4 Sei $C = (c_{ij})$ eine $n \times n$ -Matrix über einem Ring A und sei $C^* = (c_{ij}^*)^t$ die komplementäre (oder adjungierte) Matrix, mit

$$c_{ij}^* = (-1)^{i+j} \det C_{ij},$$

wobei C_{ij} aus C durch Streichen der i -ten Zeile und j -ten Spalte entsteht. Dann ist

$$C^* \cdot C = C \cdot C^* = \det C \cdot E_n.$$

(Dies wird in der Linearen Algebra für Körper bewiesen; der Beweis ist aber rein formal und gilt in Ringen, wobei $\det C$ über die Laplace-Entwicklungsformel definiert wird).

Hieraus folgt bei uns

$$\det C \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Nach Voraussetzung ($1 \in M$) können wir $m_1 = 1$ wählen, dann folgt

$$0 = \det C = b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0$$

mit $a_i \in A$, also eine Ganzheitsgleichung für b .

Corollar 2.5 Endlich viele Elemente $b_1, \dots, b_n \in B$ sind genau dann ganz über A , wenn $A[b_1, \dots, b_n]$ endlich erzeugt als A -Modul ist.

Beweis: Sind $b_1, \dots, b_n \in B$ ganz über A , so folgt mit Induktion aus 2.3, dass $A[b_1, \dots, b_n]$ endlich erzeugter A -Modul ist: haben wir bereits gezeigt, dass $A' = A[b_1, \dots, b_{n-1}]$ endlich erzeugter A -Modul ist, so ist b_n ganz über A' und nach 2.3 also $A[b_1, \dots, b_n] = A'[b_n]$ endlich erzeugt als A' -Modul, also auch als A -Modul. Die Umkehrung folgt mit Kriterium 2.3 (iii), mit $M = A[b_1, \dots, b_n]$.

Bemerkung: Wir haben benutzt: Seien $A \subseteq A' \subseteq A''$ Ringerweiterungen. Ist A' endlich erzeugter A -Modul und A'' endlich erzeugter A' -Modul, so ist A'' endlich erzeugter A -Modul. Ist nämlich $\{m_1, \dots, m_r\} \subset A'$ ein Erzeugendensystem von A' als A -Modul und $\{n_1, \dots, n_s\} \subset A''$ ein Erzeugendensystem von A'' als A' -Modul, so ist $\{m_i \cdot n_j \mid i = 1, \dots, r, j = 1, \dots, s\}$ ein Erzeugendensystem von A'' als A -Modul.

Corollar 2.6 Seien $A \subseteq B \subseteq C$ zwei Ringerweiterungen. Dann ist C genau dann ganz über A , wenn B ganz über A und C ganz über B ist.

Beweis der nicht-trivialen Richtung: Seien B/A und C/B ganz, und sei $c \in C$. Gibt es eine Gleichung

$$c^n + b_{n-1}c^{n-1} + \dots + b_1c + b_0 = 0$$

mit $b_i \in B$, so ist c ganz über $\tilde{B} = A[b_0, \dots, b_{n-1}]$, also $\tilde{B}[c]$ endlich erzeugter \tilde{B} -Modul, und andererseits \tilde{B} nach 2.5 ein endlich erzeugter A -Modul. Daher ist $\tilde{B}[c]$ endlich erzeugter A -Modul, und c ganz über A nach Kriterium 2.3 (iii).

Definition 2.7 (a) Für eine Ringerweiterung $A \subseteq B$ heißt

$$\tilde{A} = \{b \in B \mid b \text{ ganz über } A\}$$

der ganze Abschluss von A in B . Nach 2.5 ist \tilde{A} wieder ein Ring! Man sagt, A ist ganz-abgeschlossen in B , wenn $\tilde{A} = A$.

(b) Ist A ein Integritätsring und $B = K$ sein Quotientenkörper, so heißt \tilde{A} einfach der ganze Abschluss (oder auch die Normalisierung) von A , und A heißt ganz-abgeschlossen (oder normal), wenn $\tilde{A} = A$.

Beispiele 2.8 (a) Sei L/K eine Körpererweiterung. Ein Element $b \in L$ ist genau dann ganz über K wenn b algebraisch über K ist.

(b) Jeder faktorielle Ring A ist ganz-abgeschlossen: Ist $\frac{a}{b} \in K = \text{Quot}(A)$ (mit $a \in A$, $b \in A \setminus \{0\}$) ganz über A und ist

$$\left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + a_0 = 0$$

mit $a_0, \dots, a_{n-1} \in A$, so gilt

$$a^n + a_{n-1}ba^{n-1} + \dots + a_1b^{n-1}a + a_0b^n = 0.$$

Jedes Primelement π , welches b teilt, teilt daher auch a ; durch Kürzen sieht man also: $\frac{a}{b} \in A$.

Proposition 2.9 Sei A ein ganz-abgeschlossener Integritätsbereich, K sein Quotientenkörper, L/K eine endliche Körpererweiterung und B der ganze Abschluss von A in L . Dann gilt:

- (a) B ist ganz-abgeschlossen.
- (b) Jedes $\beta \in L$ lässt sich schreiben als $\beta = \frac{b}{a}$, mit $b \in B$, $a \in A$, und es ist $\text{Quot}(B) \xrightarrow{\sim} L$.
- (c) Ein Element $\beta \in L$ ist genau dann in B , wenn sein Minimalpolynom $p(x)$ über K Koeffizienten in A hat.

Beweis: (a) folgt aus der ‘Transitivität’ 2.6.

(b) Sei $\beta \in L$. Dann gibt es eine Gleichung

$$a_n\beta^n + a_{n-1}\beta^{n-1} + \dots + a_1\beta + a_0 = 0$$

mit $n \geq 1$ und $a_0, \dots, a_n \in A$, $a_n \neq 0$.

Durch Multiplikation mit a_n^{n-1} erhält man eine Gleichung

$$(a_n\beta)^n + a'_{n-1}(a_n\beta)^{n-1} + \dots + a'_1(a_n\beta) + a'_0 = 0$$

mit $a'_i \in A$; es ist also $a_n\beta$ ganz über A , also in B .

(c) Sei β Nullstelle des normierten Polynoms $g(x) \in A[x]$. Dann ist $p(x)$ ein Teiler von $g(x)$ in $K[x]$. Alle Nullstellen β_1, \dots, β_n von $p(x)$ sind also ganz über A und damit auch alle Koeffizienten. Wegen der Ganz-Abgeschlossenheit von A ist $p(x) \in A[x]$. Die Umkehrung ist klar.

Definition 2.10 Sei K ein algebraischer Zahlkörper. Eine Zahl $\alpha \in K$ heißt ganz, wenn sie ganz über \mathbb{Z} ist. Der Ring

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz}\}$$

(also der ganze Abschluss von \mathbb{Z} im K) heißt der Ring der ganzen Zahlen in K .

Diese Zahlringe sind der Hauptgegenstand der algebraischen Zahlentheorie. Wir beschreiben sie nun für **quadratische Zahlkörper** $\mathbb{Q}(\sqrt{m})$ (also alle quadratischen Erweiterungen von \mathbb{Q} , siehe Übungsaufgabe 1).

Satz 2.11 Sei $m \in \mathbb{Z}$ quadratfrei und $K = \mathbb{Q}(\sqrt{m})$.

(a) Für $\alpha = a + b\sqrt{m} \in K$ ($a, b \in \mathbb{Q}$) setze

$$(2.11.1) \quad \begin{aligned} N(\alpha) &= a^2 + b^2m, \\ T(\alpha) &= 2a. \end{aligned}$$

Dann ist α genau dann ganz, wenn $N(\alpha), T(\alpha) \in \mathbb{Z}$.

(b) Es ist

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z}[\sqrt{m}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{m}, & \text{falls } m \equiv 2 \text{ oder } 3 \pmod{4}, \\ \mathcal{O}_K &= \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}, & \text{falls } m \equiv 1 \pmod{4}.\end{aligned}$$

Beweis: (a) Dies gilt für $b = 0$: $a \in \mathbb{Q}$ ist ganz falls a^2 und $2a$ ganz sind. Für $b \neq 0$ ist wegen

$$(\alpha - a)^2 = b^2m$$

das Polynom

$$x^2 - 2ax + a^2 - b^2m = 0$$

das Minimalpolynom von α über \mathbb{Q} . Dies liegt genau dann in $\mathbb{Z}[x]$, wenn $N(\alpha)$ und $T(\alpha)$ ganz sind.

(b) Natürlich sind 1 und \sqrt{m} immer ganz. Für $\alpha = \frac{1+\sqrt{m}}{2}$ ist $N(\alpha) = \frac{1-m}{4}$ und $T(\alpha) = 1$; dies liegt in \mathbb{Z} für $m \equiv 1 \pmod{4}$. Umgekehrt seien $a, b \in \mathbb{Q}$ und sei $a + b\sqrt{m}$ ganz, nach (a) also

$$\tilde{a} = 2a, \quad r = a^2 - b^2m \in \mathbb{Z}.$$

Dann ist $\tilde{a}^2 - 4mb^2 = 4r$. Sei $b = \frac{p}{q}$ mit $p, q \in \mathbb{Z}$, $(p, q) = 1$, $q > 0$. Aus der Gleichung

$$4mp^2 = (\tilde{a}^2 - 4r)q^2$$

folgt dann $q^2 \mid 4 \cdot m$. Wegen der Quadrat-Freiheit von m folgt $q = 1$ oder 2 , durch Betrachtung der Primfaktorzerlegung von q . Für $q = 1$ sind $b, 2a$ und a^2 ganz, also $a, b \in \mathbb{Z}$.

Sei $q = 2$. Dann ist p ungerade, und es ist

$$mp^2 = \tilde{a}^2 - 4r,$$

nach (1.7.1) also

$$m \equiv \tilde{a}^2 \equiv 0 \text{ oder } 1 \pmod{4}.$$

$m \equiv 0 \pmod{4}$ kann nicht sein, da m quadratfrei ist; also folgt $m \equiv 1 \pmod{4}$ und die Behauptung.

3 Norm, Spur und Diskriminante

Norm und Spur sind grundlegende Hilfsmittel für die algebraische Zahlentheorie.

Definition 3.1 Sei L/K eine endliche Körpererweiterung. Für $\alpha \in L$ betrachte die Multiplikation mit α

$$\begin{aligned}\varphi_\alpha : L &\longrightarrow L \\ x &\longmapsto \alpha \cdot x\end{aligned}$$

als K -Vektorraum-Endomorphismus von L . Dann heißen die Determinante bzw. Spur von φ_α

$$\begin{aligned}N_{L/K}(\alpha) &:= \det(\varphi_\alpha) \\ \text{Tr}_{L/K}(\alpha) &:= \text{tr}(\varphi_\alpha)\end{aligned}$$

die Norm bzw. Spur von α (für L/K).

Bemerkung 3.2 (a) Für das charakteristische Polynom

$$\begin{aligned}\chi(\varphi_\alpha, x) &= \det(id \cdot x - \varphi_\alpha) \\ &= x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0\end{aligned}$$

($n = [L : K]$) ist $a_{n-1} = -\text{Tr}_{L/K}(\alpha)$ und $(-1)^n a_0 = N_{L/K}(\alpha)$.

(b) Wegen $\varphi_{\alpha+\beta} = \varphi_\alpha + \varphi_\beta$ und $\varphi_{\alpha \cdot \beta} = \varphi_\alpha \circ \varphi_\beta$ sind

$$\begin{aligned}\text{Tr}_{L/K} &: L \longrightarrow K \\ N_{L/K} &: L^\times \longrightarrow K^\times\end{aligned}$$

Homomorphismen bezüglich $+$ bzw. \cdot .

Beispiele 3.3 (a) Sei $\beta \in K$. Bezüglich jeder K -Basis von L hat φ_β die Matrix

$$\begin{pmatrix} \beta & & & 0 \\ & \ddots & & \\ 0 & & & \beta \end{pmatrix}.$$

Es ist also $\text{Tr}_{L/K}(\beta) = n \cdot \beta$ und $N_{L/K}(\beta) = \beta^n$.

(b) Sei $L = \mathbb{Q}(\sqrt{m})$ für $m \in \mathbb{Z}$, m kein Quadrat. Dann ist für $\alpha = a + b\sqrt{m}$

$$\begin{aligned}\text{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) &= 2a, \\ N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) &= a^2 - b^2m\end{aligned}$$

(vergleiche (2.11.1)!). Denn: In der \mathbb{Q} -Basis $(1, \sqrt{m})$ von $\mathbb{Q}(\sqrt{m})$ hat φ_α die Matrix

$$\begin{pmatrix} a & bm \\ b & a \end{pmatrix}.$$

Für separable Erweiterungen haben wir:

Satz 3.4 Ist L/K endlich separabel und Σ die Menge aller K -Einbettungen $\sigma : L \rightarrow \overline{K}$ von L in einen algebraischen Abschluss \overline{K} von K , so gilt für $\alpha \in L$:

(a) $\chi(\varphi_\alpha, x) = \prod_{\sigma \in \Sigma} (x - \sigma\alpha).$

(b) $\text{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \Sigma} \sigma\alpha.$

(c) $N_{L/K}(\alpha) = \prod_{\sigma \in \Sigma} \sigma\alpha.$

Bemerkung Wir setzen im folgenden die Existenz eines algebraischen Abschlusses \overline{K} voraus, d.h., eines algebraisch abgeschlossenen Körpers, der algebraisch über K ist. In 3.4 und ähnlichen Situationen kann man \overline{K} immer durch eine "genügend große" normale Körpererweiterung N/K ersetzen, z.B. durch einen Zerfällungskörper von L/K . Man kann \overline{K} aber auch durch einen beliebigen algebraisch abgeschlossenen Körper über K ersetzen. In allen diesen Fällen gibt es n verschiedene K -Einbettungen von L in diesen Körper, $n = [L : K]$ (da L/K separabel ist).

Denn: $p_\alpha(x) \in K[x]$ ist irreduzibel und α ist eine Nullstelle von $p_\alpha(x)$. Ist $\tilde{\alpha}$ eine weitere Nullstelle in \overline{K} , so gibt es (siehe Algebra I, Satz 10.7 bzw. Satz 16.15) eine K -Einbettung $\sigma : K(\alpha) \rightarrow \overline{K}$ mit $\sigma(\alpha) = \tilde{\alpha}$. Diese ist offenbar eindeutig bestimmt, und die Zuordnung $\tilde{\alpha} \mapsto \sigma = \sigma_{\tilde{\alpha}}$ ist injektiv, also bijektiv, denn die Nullstellen von $p_\alpha(x)$ sind paarweise verschieden und es ist $\deg p_\alpha(x) = [K(\alpha) : K] = |\text{Hom}_K(K(\alpha), \overline{K})|$, da mit L/K auch $K(\alpha)/K$ separabel ist (vergleiche Algebra I, Corollar 16.16).

Die $\sigma\alpha$, also die Nullstellen von $p_\alpha(x)$, heißen auch die Konjugierten von α (vergleiche Algebra I, Definition 13.2).

Nun gibt es zu jedem τ_i genau d Einbettungen $\sigma : L \rightarrow \overline{K}$ mit $\sigma|_{K(\alpha)} = \tau_i$. Damit folgt

$$\begin{aligned} \prod_{\sigma \in \Sigma} (x - \sigma\alpha) &= \prod_{i=1}^m (x - \tau_i\alpha)^d = p_\alpha(x)^d && \text{(nach (3.4.2))} \\ &= \chi(\varphi_\alpha, x) && \text{(nach (3.4.1)).} \end{aligned}$$

(b) und (c) folgen sofort aus (a).

Corollar 3.5 ist L/K galoissch, mit Galoisgruppe G , so ist

$$(a) \chi(\varphi_\alpha, x) = \prod_{\sigma \in G} (x - \sigma\alpha),$$

$$(b) \text{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma\alpha,$$

$$(c) N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma\alpha.$$

Beweis: Ist $\iota : L \rightarrow \overline{K}$ eine feste K -Einbettung, so sind $\{\iota\sigma \mid \sigma \in G\}$ die $[L : K]$ vielen verschiedenen K -Einbettungen von L in \overline{K} .

Beispiele 3.6 (a) $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ (m kein Quadrat) ist galoissch mit Galoisgruppe $\{1, \sigma\}$, $\sigma\sqrt{m} = -\sqrt{m}$. Für $\alpha = a + b\sqrt{m}$ ist

$$\text{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = a + b\sqrt{m} + a - b\sqrt{m} = 2a$$

$$N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2m.$$

(b) Für $L = \mathbb{Q}(\sqrt[3]{5})$ sind die \mathbb{Q} -Einbettungen $L \hookrightarrow \mathbb{C}$ gegeben durch

$$\begin{aligned} 1 &: \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \sigma &: \sqrt[3]{5} \mapsto \zeta \cdot \sqrt[3]{5} \\ \tau &: \sqrt[3]{5} \mapsto \zeta^2 \sqrt[3]{5} \end{aligned}$$

wobei $\zeta = e^{\frac{2\pi i}{3}}$ eine primitive 3-te Einheitswurzel ist. Es folgt wegen $\zeta^4 = \zeta$:

$$\begin{aligned} \text{Tr}_{L/\mathbb{Q}}(a + b\sqrt[3]{5} + c\sqrt[3]{5}^2) &= 3a \\ N_{L/\mathbb{Q}}(a + b\sqrt[3]{5} + c\sqrt[3]{5}^2) &= (a + b\delta + c\delta^2)(a + \zeta b\delta + \zeta^2 c\delta^2)(a + \zeta^2 b\delta + \zeta c\delta^2) \\ &= \dots \end{aligned}$$

Corollar 3.7 Für endliche separable Körpererweiterungen $M/L/K$ gilt

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}, \quad \text{und} \quad N_{M/K} = N_{L/K} \circ N_{M/L}.$$

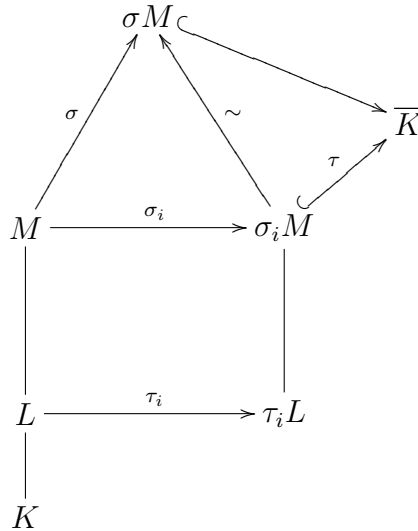
Beweis: Seien $\tau_1, \dots, \tau_m : L \rightarrow \overline{K}$ ($m = [L : K]$) die verschiedenen K -Einbettungen. Dann ist für $\alpha \in M$

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K(M, \overline{K})} \sigma \alpha = \sum_{i=1}^m \sum_{\substack{\sigma \\ \sigma|_L = \tau_i}} \sigma \alpha$$

Wählen wir für jedes τ_i ein $\sigma_i : M \rightarrow \overline{K}$ mit $\sigma_i|_L = \tau_i$ aus, so ist dies weiter

$$= \sum_{i=1}^m \mathrm{Tr}_{\sigma_i M / \tau_i L}(\sigma_i \alpha) = \sum_{i=1}^m \tau_i \mathrm{Tr}_{M/L}(\alpha) = \mathrm{Tr}_{L/K} \mathrm{Tr}_{M/L}(\alpha)$$

denn jedes $\sigma \in \mathrm{Hom}_K(M, \overline{K})$ mit $\sigma|_L = \tau_i$ lässt sich eindeutig schreiben als $\sigma = \tau \sigma_i$ mit einem $\tau \in \mathrm{Hom}_{\tau_i K}(\sigma_i, L, \overline{K})$:



Der Fall der Normen ist analog.

Bemerkung 3.8 Die Transitivität in 3.7 gilt auch für beliebige endliche (nicht notwendig separable) Körpererweiterungen (siehe Bosch “Algebra”, 4.7.).

Wir kommen nun zum Begriff der Diskriminante. Diese ist wichtig für die Bestimmung von Zahlringen und für die Verzweigungstheorie. Hierzu zunächst:

Lemma/Definition 3.9 Sei L/K eine endliche separable Körpererweiterung. Die **Diskriminante** einer K -Basis $\alpha_1, \dots, \alpha_n$ von L ist definiert als

$$d(\alpha_1, \dots, \alpha_n) := \det(\mathrm{Tr}_{L/K}(\alpha_i \cdot \alpha_j)) = [\det(\sigma_i \alpha_j)]^2,$$

wobei $\sigma_1, \dots, \sigma_n$ die verschiedenen K -Einbettungen $L \hookrightarrow \overline{K}$ sind.

Beweis der letzten Gleichheit:

$$(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) = \left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j) \right) = \left(\sum_{k=1}^n \sigma_k \alpha_i \cdot \sigma_k \alpha_j \right) = (\sigma_k \alpha_i)^t \cdot (\sigma_k \alpha_j) .$$

Die Behauptung folgt, da $\det(\sigma_i \alpha_j) = \det(\sigma_j \alpha_i)^t$.

Bemerkung Die Matrix $(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$ ist gerade die Fundamentalmatrix der symmetrischen K -Bilinearform

$$\begin{aligned} L \times L &\rightarrow K \\ (\alpha, \beta) &\mapsto \mathrm{Tr}_{L/K}(\alpha \beta) \end{aligned}$$

bezüglich der K -Basis $(\alpha_1, \dots, \alpha_n)$. Über die erste Gleichung in 3.9 ist die Diskriminante für jede endliche Körpererweiterung definiert.

Lemma 3.10 Für eine K -Basis der Form $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ (in diesem Fall ist α ein primitives Element für L/K , d.h., $L = K(\alpha)$) gilt

$$d(1, \alpha, \dots, \alpha^{m-1}) = \prod_{i < j} (\alpha_i - \alpha_j)^2 ,$$

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

Beweis: Sind $\sigma_1, \dots, \sigma_n : L = K(\alpha) \rightarrow \overline{K}$ die K -Einbettungen, so sind die Konjugierten von α gerade $\alpha_1 = \sigma_1 \alpha, \dots, \alpha_n = \sigma_n \alpha$. Es folgt

$$\det(\sigma_i \alpha^{j-1}) = \det(\alpha_i^{j-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{m-1} \\ & & \vdots & & \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{m-1} \end{pmatrix}$$

die Vandermondsche Determinante für $\alpha_1, \dots, \alpha_n$.

Bemerkung 3.11 Dies zeigt, dass $d(1, \alpha, \dots, \alpha^{m-1})$ die **Diskriminante des Minimalpolynoms** $p_\alpha(x)$ von α über K ist (siehe Algebra II, Definition 14.7). Hiermit folgt

$$d(1, \alpha, \dots, \alpha^{m-1}) = (-1)^{m(m-1)/2} \cdot N_{K(\alpha)/K}(p'_\alpha(\alpha)) ,$$

wobei $p'_\alpha(x)$ die formale Ableitung von $p_\alpha(x)$ ist (siehe Bosch "Algebra" 4.4 S. 174).

Lemma 3.12 Eine endliche Körpererweiterung L/K ist genau dann separabel, wenn die Spurform

$$\begin{aligned} \langle, \rangle &: L \times L \rightarrow K \\ (\alpha, \beta) &\mapsto \mathrm{Tr}_{L/K}(\alpha \cdot \beta) \end{aligned}$$

eine nicht-ausgeartete Bilinearform ist.

Beweis: Ist L/K separabel, so gibt es ein primitives Element $\delta \in L$, d.h., $L = K(\delta)$ (Algebra I, Satz 11.14). Dann ist $1, \delta, \dots, \delta^{n-1}$, mit $n = [L : K]$, eine K -Basis von L . Bezüglich dieser hat die Spurform die Fundamentalmatrix

$$M = (\mathrm{Tr}_{L/K}(\delta^{i-1} \cdot \delta^{j-1}))_{i,j=1,\dots,n} .$$

Seien $\sigma_1, \dots, \sigma_n : L \rightarrow \overline{K}$ die K -Einbettungen. Nach 3.9 und 3.10 ist dann

$$\det M = \det(\sigma_i \delta^{j-1})^2 = \prod_{i < j} (\sigma_i \delta - \sigma_j \delta)^2$$

und dies ist ungleich 0, falls L/K separabel ist (dann ist $\sigma_i \delta \neq \sigma_j \delta$ für $i \neq j$, siehe Beweis von 3.4). Aber $\det M \neq 0$ bedeutet gerade, dass die Spurform nicht-ausgeartet ist.

Ist aber L/K nicht separabel, so ist $\text{Tr}_{L/K} = 0$ (Bosch, "Algebra" 4.7.).

Corollar 3.13 Ist L/K endlich separabel, so ist für jede K -Basis $\alpha_1, \dots, \alpha_n$ von L

$$d(\alpha_1, \dots, \alpha_n) \neq 0.$$

Beweis: $d(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{L/K}(\alpha_i \cdot \alpha_j))$, die Determinante der Fundamentalmatrix der nicht-ausgearteten Spurform.

Wir notieren noch, wie sich die Diskriminante bei Basiswechsel verhält:

Lemma 3.14 L/K endlich separable Körpererweiterung, und seien $\{\alpha_1, \dots, \alpha_n\}, \{\alpha'_1, \dots, \alpha'_n\}$ K -Basen von L mit

$$\begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} = T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

für $T = (t_{ij}) \in GL_n(K)$. Dann gilt

$$d(\alpha'_1, \dots, \alpha'_n) = (\det T)^2 d(\alpha_1, \dots, \alpha_n).$$

Beweis: Dies folgt sofort aus dem Transformationsverhalten der Fundamentalmatrix einer symmetrischen Bilinearform bei Basiswechsel (siehe Lineare Algebra II, Lemma 16.6). Ein Beweis mittels der Einbettungen geht so: Sei $\{\sigma_1, \dots, \sigma_n\} = \text{Hom}_K(L, \overline{K})$, dann gilt

$$d(\alpha'_1, \dots, \alpha'_n) = (\det(\sigma_i \alpha'_j))^2 = \det [(\sigma_i \alpha_j) \cdot T^t]^2 = \det^2(\sigma_i \alpha_j) \cdot \det^2(T),$$

denn es ist $(\sigma_i \alpha'_j) = (\sigma_i(\sum_k t_{jk} \alpha_k)) = (\sum_k \sigma_i(\alpha_k) \cdot t_{jk}) = (\sigma_i \alpha_j) T^t$.

Wir betrachten nun einen ganz-abgeschlossenen Integritätsring A mit Quotientenkörper K und seinen ganzen Abschluss B in einer endlichen separablen Erweiterung L/K (vergl. 2.8.).

Wir bemerken:

Lemma 3.15 Sei $\beta \in B$. Dann gilt:

- (a) Alle Konjugierten $\sigma\beta$ ($\sigma : L \rightarrow \overline{K}$ K -Einbettung) sind wieder ganz über A (nicht notwendig in B !).
- (b) $\text{Tr}_{L/K}(\beta), N_{L/K}(\beta) \in A$.
- (c) $\beta \in B^\times \Leftrightarrow N_{L/K}(\beta) \in A^\times$.

Beweis: (a) Ist β Nullstelle des normierten Polynoms $f(x) \in A[x]$, so auch $\sigma\beta : f(\sigma\beta) = \sigma f(\beta) = 0$.

(b) $\text{Tr}_{L/K}(\beta) = \sum_{\sigma} \sigma\beta$ ist ganz über A , andererseits in K ; aber A war ganz-abgeschlossen. Analog für $N_{L/K}(\beta)$.

(c) “ \Rightarrow ” folgt aus der Multiplikativität der Norm. “ \Leftarrow ”: Sei $\alpha \in A$ mit $1 = \alpha \cdot N_{L/K}(\beta)$. Dann ist $1 = \alpha \cdot \prod_{\sigma} \sigma\beta$, weiter gibt es ein σ_0 mit $\sigma_0\beta = \beta$ (Wir nehmen an, dass alle L in \overline{K} liegen, eine Einbettung ist also die “Identität”). Damit folgt

$$\beta^{-1} = \alpha \cdot \prod_{\sigma \neq \sigma_0} \sigma\beta.$$

Nach (a) sind alle Faktoren der rechten Seite ganz über A , also gilt dies auch für $\beta^{-1} \in L$. Es folgt $\beta^{-1} \in B$.

Proposition 3.16 Sei $\alpha_1, \dots, \alpha_n$ eine K -Basis von L die in B liegt. Für die Diskriminante $d = d(\alpha_1, \dots, \alpha_n)$ gilt dann

$$d \cdot B \subseteq A\alpha_1 + \dots + A\alpha_n.$$

Beweis: Sei $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n \in B$ ($a_1, \dots, a_n \in K$). Dann gilt

$$\text{Tr}_{L/K}(\alpha_i \cdot \alpha) = \sum_{j=1}^n \text{Tr}_{L/K}(\alpha_i \cdot \alpha_j) \cdot a_j$$

für $i = 1, \dots, n$. Dies ist ein lineares Gleichungssystem für a_1, \dots, a_n , mit Matrix $M = (\text{Tr}_{L/K}(\alpha_i \cdot \alpha_j))$. Nach 3.15 (a) ist $\text{Tr}_{L/K}(\alpha_i \cdot \alpha), \text{Tr}_{L/K}(\alpha_i \cdot \alpha_j) \in A$ für alle i, j . Mit der Cramerschen Regel folgt

$$a_j = \frac{\tilde{a}_j}{d} \quad \text{mit} \quad \tilde{a}_j \in A,$$

da $d = \det M$, also $d \cdot \alpha \in A\alpha_1 + \dots + A\alpha_n$.

Definition 3.17 Ist B ein freier A -Modul mit Basis $\alpha_1, \dots, \alpha_n$, so heisst $\{\alpha_1, \dots, \alpha_n\}$ eine Ganzheitsbasis von B über A .

Bemerkung: Sei R ein kommutativer Ring mit Eins. Ein R -Modul M heißt frei vom Rang $n \in \mathbb{N}_0$, wenn es $m_1, \dots, m_n \in M$ gibt, so dass jedes $m \in M$ eine Darstellung $m = a_1m_1 + \dots + a_nm_n$ mit eindeutig bestimmten $a_i \in R$ hat (Äquivalent: (m_1, \dots, m_n) ist ein Erzeugendensystem und die m_i sind linear unabhängig: $\sum a_i m_i = 0$ mit $a_i \in R \Rightarrow$ alle $a_i = 0$). Das Tupel (m_1, \dots, m_n) heißt dann eine Basis von M . Offenbar ist M genau dann frei vom Rang n , wenn es einen Isomorphismus $M \cong R^n$ von R -Moduln gibt.

Satz 3.18 Ist A ein Hauptidealring und L/K separabel, so ist jeder endlich erzeugte B -Untermodule $M \neq 0$ von L freier A -Modul vom Rang $n = [L : K]$. Insbesondere besitzt B eine Ganzheitsbasis über A .

Beweis: Wir benutzen die folgende Konsequenz des *Elementarteilersatzes* (siehe Algebra II Satz 7.13 oder Bosch “Algebra” 2.9.):

(3.18.1) Ist A ein Hauptidealring, so ist jeder Untermodule M eines freien A -Moduls A^r vom Rang r selbst freier A -Modul vom Rang $s \leq r$.

Sei also nun $0 \neq M \subseteq L$ ein endlich erzeugter B -Untermodul und $\alpha_1, \dots, \alpha_n$ eine K -Basis von L . Ohne Einschränkung liegen alle α_i in B (vergl. 2.8. (b)). Nach 3.16 ist dann

$$dB \subseteq A\alpha_1 + A\alpha_2 + \dots + A\alpha_n =: M_0,$$

$d = d(\alpha_1, \dots, \alpha_n)$. Sei $\{\mu_1, \dots, \mu_r\}$ ein Erzeugendensystem von M als B -Modul. Es gibt (wieder nach 2.8 (b)) ein $a \in A$ mit $a \cdot \mu_i \in B$ für alle $i = 1, \dots, r$, also $a \cdot M \subseteq B$. Es folgt

$$adM \subseteq dB \subset M_0.$$

Offenbar ist M_0 ein freier A -Modul vom Rang n : $M_0 = A\alpha_1 \oplus A\alpha_2 \oplus \dots \oplus A\alpha_n \cong A^n$. Daher ist adM ein freier A -Modul vom Rang $s \leq n$. Wegen der A -Modul-Isomorphie $M \cong adM$, $x \mapsto adx$, gilt dies auch für M . Wir zeigen nun noch $s = n$. Für ein beliebiges Element $\mu \in M \setminus \{0\}$ gilt

$$B \cong \mu B \subseteq M$$

und

$$M_0 \subseteq B.$$

Es folgt also auch $n = \text{rg}(M_0) \leq s = \text{rg}(M)$, also $s = n$.

Corollar 3.19 Ist K ein algebraischer Zahlkörper, so ist der Ring \mathcal{O}_K der ganzen Zahlen in K ein freier \mathbb{Z} -Modul (= freie abelsche Gruppe) vom Rang $n = [K : \mathbb{Q}]$.

Lemma/Definition 3.20 Sei K ein algebraischer Zahlkörper. Die **Diskriminante von K** ist definiert als

$$d_K = d(\alpha_1, \dots, \alpha_n),$$

wobei $n = [K : \mathbb{Q}]$ und $\{\alpha_1, \dots, \alpha_n\}$ eine Ganzheitsbasis von \mathcal{O}_K über \mathbb{Z} ist, d.h., $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$. Man sagt auch "Ganzheitsbasis von K ". Dies ist unabhängig von der Wahl der Ganzheitsbasis.

Beweis der Behauptungen: Ist $\alpha'_1, \dots, \alpha'_n$ eine andere Basis, so gilt

$$\alpha'_i = \sum_{j=1}^n a_{ij} \alpha_j, \quad i = 1, \dots, n,$$

mit $a_{ij} \in \mathbb{Z}$, und die Übergangsmatrix $T = (a_{ij})$ liegt in $\text{GL}_n(\mathbb{Z})$, d.h., hat ein Inverses T^{-1} mit ganzzahligen Koeffizienten (die Transformationsmatrix in umgekehrter Richtung). Es folgt $\det(T) \in \mathbb{Z}^\times = \{+1, -1\}$ (denn es ist $\det T \cdot \det T^{-1} = 1$). Mit Lemma 3.14 folgt $d(\alpha'_1, \dots, \alpha'_n) = (\det T)^2 \cdot d(\alpha_1, \dots, \alpha_n) = d(\alpha_1, \dots, \alpha_n)$. q.e.d.

Wir berechnen die Diskriminante für quadratische Zahlkörper:

Satz 3.21 Sei $K = \mathbb{Q}(\sqrt{m})$ ein quadratischer Zahlkörper, $m \in \mathbb{Z}$ quadratfrei. Dann ist

$$\begin{aligned} d_K &= 4m, & \text{wenn } m &\equiv 2 \text{ oder } 3 \pmod{4}, \\ d_K &= m, & \text{wenn } m &\equiv 1 \pmod{4}. \end{aligned}$$

Beweis: Die Konjugierten von \sqrt{m} sind \sqrt{m} und $-\sqrt{m}$. Im ersten Fall ist $\{1, \sqrt{m}\}$ eine Ganzheitsbasis und

$$d_K = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2 \cdot \sqrt{m})^2 = 4m.$$

Im zweiten Fall ist $\{1, \frac{1+\sqrt{m}}{2}\}$ eine Ganzheitsbasis und

$$d_K = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = (-\sqrt{m})^2 = m.$$

4 Ideale in Dedekindringen

Sei K ein Zahlkörper mit Ring der ganzen Zahlen \mathcal{O}_K .

Lemma 4.1 \mathcal{O}_K ist ein noetherscher Ring.

Beweis Sei $\mathfrak{a} \subseteq \mathcal{O}_K$ ein Ideal. Da \mathcal{O}_K ein endlich erzeugter \mathbb{Z} -Modul ist, gilt dies auch für \mathfrak{a} . Dann ist \mathfrak{a} auch als \mathcal{O}_K -Modul endlich erzeugt

Wie in jedem noetherschen Ring lässt sich jede Nicht-Einheit $\alpha \in \mathcal{O}_K$ als ein Produkt von irreduziblen Elementen schreiben. Im allgemeinen ist \mathcal{O}_K aber nicht faktoriell:

Beispiele 4.2 (a) Der Ganzheitsring von $k = \mathbb{Q}(\sqrt{-5})$ ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In ihm lässt sich die Zahl 21 auf zwei verschiedene Weisen in Irreduzible zerlegen:

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

(siehe Übungsaufgabe 8).

(b) Allgemein ist \mathcal{O}_K nicht faktoriell für $K = \mathbb{Q}(\sqrt{-m}), m \geq 5$ quadratfrei, $m \equiv 1 \pmod{4}$ (Algebra II, Übungsaufgabe 17).

In \mathcal{O}_K hat man aber eine eindeutige Zerlegung für **Ideale** (im Primideale). Dies gilt allgemeiner für **Dedekindringe**:

Definition 4.3 Ein Ring R (kommutativ, mit 1) heißt Dedekindring, wenn gilt:

- (i) R ist noethersch.
- (ii) R ist ganz-abgeschlossener Integritätsring.
- (iii) Jedes Primideal $\mathfrak{p} \neq 0$ von R ist auch ein maximales Ideal.

Satz 4.4 \mathcal{O}_K ist ein Dedekindring.

Beweis Wir müssen nur noch (iii) zeigen. Sei $0 \neq \mathfrak{p}$ ein Primideal. Dann ist

$$\mathfrak{p} \cap \mathbb{Z} = (p) \quad \text{für eine Primzahl } p,$$

d.h., ein von Null verschiedenes Primideal in \mathbb{Z} . Denn: Der von $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ induzierte Ringhomomorphismus

$$\psi : \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$$

ist injektiv, also ist $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$ integer und damit $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal. Ist weiter $0 \neq \beta \in \mathfrak{p}$, so gibt es eine Ganzheitsgleichung

$$\beta^m + q_{m-1} \beta^{m-1} + \dots + a_1 \beta + a_0 = 0$$

mit $a_i \in \mathbb{Z}$, $a_0 \neq 0$. Dann ist $a_0 \in \mathfrak{p} \cap \mathbb{Z} \neq 0$.

Da \mathcal{O}_K endlich erzeugter \mathbb{Z} -Modul ist, wird $\mathcal{O}_K/\mathfrak{p}$ mittels ψ ein endlich erzeugter \mathbb{F}_p -Vektorraum, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$. Daher ist $\mathcal{O}_K/\mathfrak{p}$ endlich. Ein endlicher Integritätsring ist aber ein Körper; daher ist \mathfrak{p} ein maximales Ideal.

Wir betrachten nun einen beliebigen Dedekindring R ; K sei sein Quotientenkörper. Statt mit Elementen rechnen wir im Folgenden oft mit Idealen. Diese können wir auch addieren und multiplizieren:

Definition 4.5 Für zwei Ideale $\mathfrak{a}, \mathfrak{b} \subseteq R$ definieren wir die Summe durch

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

und das Produkt durch

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^n a_i \cdot b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

Dies sind beides wieder Ideale von R .

Damit gilt nun (für R Dedekindring!):

Satz 4.6 (eindeutige Zerlegung in Primideale) Jedes von 0 und R verschiedene Ideal $\mathfrak{a} \subseteq R$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$$

in ein Produkt von Primidealen $\mathfrak{p}_i \subseteq R$.

Lemma 4.7 Zu jedem Ideal $\mathfrak{a} \neq 0$ von R gibt es von Null verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ mit

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r.$$

Beweis: Sei M die Menge der Ideale $\neq 0$, für die dies falsch ist. Angenommen, M ist nicht leer. Da R noethersch ist, besitzt M dann ein maximales Element (Algebra I, Proposition 5.7), etwa \mathfrak{a} . Dieses ist kein Primideal, es gibt also Elemente $b_1, b_2 \in R$ mit $b_1 \cdot b_2 \in \mathfrak{a}$ aber $b_1, b_2 \notin \mathfrak{a}$.

Setzen wir $\mathfrak{a}_1 = \mathfrak{a} + (b_1)$, $\mathfrak{a}_2 = \mathfrak{a} + (b_2)$, so ist $\mathfrak{a} \subsetneq \mathfrak{a}_1$ und $\mathfrak{a} \subsetneq \mathfrak{a}_2$ und $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subseteq \mathfrak{a}$. Wegen der Maximalität von \mathfrak{a} enthalten \mathfrak{a}_1 und \mathfrak{a}_2 Primidealprodukte, und dasselbe würde für \mathfrak{a} folgen – Widerspruch!

Lemma 4.8 Sei $\mathfrak{p} \subseteq R$ ein Primideal und $0 \neq \mathfrak{a}$ ein Ideal. Ist

$$\mathfrak{p}^{-1} := \{x \in K = \text{Quot}(R) \mid x \cdot \mathfrak{p} \subseteq R\}$$

so gilt $\mathfrak{a} \not\subseteq \mathfrak{a}\mathfrak{p}^{-1}$.

Beweis Offenbar gilt $R \subseteq \mathfrak{p}^{-1}$. Wir behaupten zunächst $\mathfrak{p}^{-1} \neq R$: Sei $0 \neq a \in \mathfrak{p}$ und (nach 4.7)

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}, \mathfrak{p}_i \text{ Primideal,}$$

mit minimalem r ($(a) = Ra$ das von a erzeugte Hauptideal). Dann ist eins der \mathfrak{p}_i gleich \mathfrak{p} : Es genügt zu zeigen, dass ein \mathfrak{p}_i in \mathfrak{p} enthalten ist; wegen der Maximalität von \mathfrak{p}_i folgt dann $\mathfrak{p}_i = \mathfrak{p}$. Ist aber kein \mathfrak{p}_i in \mathfrak{p} enthalten, so gäbe es für jedes i ein $a_i \in \mathfrak{p}_i$ mit $a_i \notin \mathfrak{p}$. Aber dann ist $a_1 \cdots a_r \in \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}$ im Widerspruch dazu, dass \mathfrak{p} prim ist.

Sei also etwa $\mathfrak{p}_1 = \mathfrak{p}$. Wegen $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$ (Minimalität von r) gibt es ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ mit $b \notin (a)$, also $\frac{b}{a} \notin R$. Andererseits ist aber $b\mathfrak{p} \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a)$, also $\frac{b}{a}\mathfrak{p} \subseteq R$, d.h., $\frac{b}{a} \in \mathfrak{p}^{-1}$. Damit haben wir tatsächlich gezeigt, dass $R \subsetneq \mathfrak{p}^{-1}$.

Nun zur Behauptung des Lemmas: Sei $0 \neq \mathfrak{a} \subseteq R$ ein Ideal, und $\alpha_1, \dots, \alpha_n$ ein Erzeugendensystem von \mathfrak{a} . Angenommen, $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Dann ist für jedes $\beta \in \mathfrak{p}^{-1}$

$$\alpha_i \cdot \beta = \sum_{j=1}^n a_{ij} \alpha_j, \quad i = 1, \dots, n,$$

mit $a_{ij} \in R$. Für die Matrix

$$C = \beta \cdot E_n - (a_{ij})$$

gilt also

$$C \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0,$$

und aus 2.4 folgt mit $d = \det C$

$$d \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

Im Körper K folgt hieraus $d = 0$. Damit ist β Nullstelle des normierten Polynoms

$$\det(x \cdot E_n - (a_{ij})) \in R[x],$$

also ganz über R , also in R wegen der Ganz-Abgeschlossenheit von R . Es würde folgen $\mathfrak{p}^{-1} \subseteq R$, Widerspruch!

Wir kommen nun zum

Beweis von Satz 4.6 1) Existenz der Primzerlegung: Sei \mathcal{N} die Menge der von 0 und R verschiedenen Ideale, die keine Primzerlegung besitzen. Angenommen, \mathcal{N} ist nicht leer. Dann

besitzt \mathcal{N} wieder ein maximales Element \mathfrak{a} . Dieses liegt wiederum in einem maximalen Ideal \mathfrak{p} , und wir erhalten wegen $R \subseteq \mathfrak{p}^{-1}$

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R .$$

Nach 4.8 ist

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \text{ und } \mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R .$$

Da \mathfrak{p} maximales Ideal ist, folgt $\mathfrak{p}\mathfrak{p}^{-1} = R$. Da \mathfrak{a} in \mathcal{N} liegt, ist $\mathfrak{a} \neq \mathfrak{p}$ und daher $\mathfrak{a}\mathfrak{p}^{-1} \neq R$ (da sonst $\mathfrak{a} = \mathfrak{a}R = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = R\mathfrak{p} = \mathfrak{p}$). Wegen der Maximalität von \mathfrak{a} in \mathcal{N} besitzt daher $\mathfrak{a}\mathfrak{p}^{-1}$ eine Primzerlegung, etwa $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Es folgt dann $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, Widerspruch!

2) Eindeutigkeit der Primzerlegung: Wir benutzen

Lemma 4.9 In einem beliebigen Ring R gilt für Ideale $\mathfrak{a}, \mathfrak{b}$ und ein Primideal \mathfrak{p}

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p} .$$

Beweis Gilt $\mathfrak{a} \not\subseteq \mathfrak{p}$ und $\mathfrak{b} \not\subseteq \mathfrak{p}$, so existieren $a \in \mathfrak{a} \setminus \mathfrak{p}$ und $b \in \mathfrak{b} \setminus \mathfrak{p}$ und es folgt $ab \in \mathfrak{a}\mathfrak{b} \setminus \mathfrak{p}$, also $\mathfrak{a} \cdot \mathfrak{b} \not\subseteq \mathfrak{p}$.

Seien nun in unserem Dedekindring R

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

zwei Primzerlegungen des Ideals \mathfrak{a} . Wegen $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1$ enthält \mathfrak{p}_1 nach 4.9 einen der Faktoren \mathfrak{q}_i , o.E. \mathfrak{q}_1 , und es ist dann $\mathfrak{q}_1 = \mathfrak{p}_1$, da \mathfrak{q}_1 maximales Ideal ist. Wir multiplizieren mit \mathfrak{p}_1^{-1} und erhalten wegen

$$\mathfrak{p}_1\mathfrak{p}_1^{-1} = R$$

(Beweis wie oben: $\mathfrak{p}_1 \neq R \xrightarrow{4.8} \mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} \subseteq R \Rightarrow \mathfrak{p}_1\mathfrak{p}_1^{-1} = R$ da \mathfrak{p}_1 maximal)

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s .$$

Induktiv fortfahrend erhalten wir $r = s$ ($R = \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{q}_1$ ist nicht möglich) und, nach Umordnung, $\mathfrak{p}_i = \mathfrak{q}_i$.

Beispiel 4.10 Sei $K = \mathbb{Q}(\sqrt{7})$ mit dem Ring der ganzen Zahlen

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{7}] \cong \mathbb{Z}[t]/(t^2 - 7) .$$

Das Ideal (3) ist nicht prim: Wir haben Ringisomorphismen

$$\begin{aligned} \mathcal{O}_K/(3) &\cong \mathbb{Z}[t]/(t^2 - 7, 3) \cong (\mathbb{Z}/3\mathbb{Z})[t]/(t^2 - 7) \cong \mathbb{Z}/3\mathbb{Z}[t]/(t^2 - 1) \cong \mathbb{Z}/3\mathbb{Z}[t]/(t - 1)(t + 1) \\ &\cong \mathbb{Z}/3\mathbb{Z}[t]/(t - 1) \times \mathbb{Z}/3\mathbb{Z}[t]/(t + 1) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

Hieraus erhält man außerdem die Primzerlegung

$$(3) = \ker(\mathcal{O}_K \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = \mathfrak{p} \cap \mathfrak{q} \stackrel{(*)}{=} \mathfrak{p}\mathfrak{q}$$

mit $\mathfrak{p} = (3, \sqrt{7} - 1)$ und $\mathfrak{q} = (3, \sqrt{7} + 1)$ (vergleiche Übungsaufgaben). Die Gleichheit (*) folgt wegen $\mathfrak{p} \neq \mathfrak{q}$ aus den Überlegungen in der folgenden Bemerkung.

Bemerkung 4.11 Allgemein sagt man in einem Ring R (kommutativ, mit 1) für Ideale $\mathfrak{a}, \mathfrak{b}$

$$\mathfrak{a} \mid \mathfrak{b} \text{ (} \mathfrak{a} \text{ teilt } \mathfrak{b} \text{)} \Leftrightarrow \mathfrak{b} \subseteq \mathfrak{a}$$

(beachte, dass für Elemente a, b gilt: $a \mid b \Leftrightarrow b = a \cdot r$ für $r \in R \Leftrightarrow (b) \subseteq (a)$).
Für Primideale \mathfrak{p} gilt dabei nach 4.9

$$\mathfrak{p} \mid \mathfrak{a} \cdot \mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ oder } \mathfrak{p} \mid \mathfrak{b} .$$

Satz 4.6 sagt nun, dass in einem **Dedekindring** jedes Ideal $\mathfrak{a} \neq 0$, R eine eindeutige Produktdarstellung

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}, \nu_i > 0 ,$$

besitzt, wobei die \mathfrak{p}_i gerade die paarweise verschiedenen **Primteiler** von \mathfrak{a} sind: für $\mathfrak{p} \mid \mathfrak{a}$, \mathfrak{p} Primideal (wir sagen auch einfach: prim) folgt wie im Eindeutigkeitsbeweis $\mathfrak{p} = \mathfrak{p}_i$ für eins der \mathfrak{p}_i . Wegen $\mathfrak{p} \mathfrak{p}^{-1} = R$ folgt weiter für Ideale $\mathfrak{a}, \mathfrak{b} \subseteq R$

$$\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c} \text{ für ein Ideal } \mathfrak{c} .$$

Schreiben wir nämlich

$$\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{m_i}$$

$$\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$$

mit denselben \mathfrak{p}_i und nun $n_i \geq 0, m_i \geq 0$ (wobei $\mathfrak{p}^0 := R$) so gilt

$$\begin{aligned} \mathfrak{a} \mid \mathfrak{b} &\Leftrightarrow m_i \leq n_i \quad \forall i = 1, \dots, r \\ &\Leftrightarrow \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c} \quad \text{mit} \quad \mathfrak{c} = \prod_{i=1}^r \mathfrak{p}_i^{(n_i - m_i)} . \end{aligned}$$

Wir erhalten also eine befriedigende Teilertheorie für Ideale, obwohl dies für Elemente nicht gelten muss. Es gilt dabei $\mathfrak{a} + \mathfrak{b} = ggT(\mathfrak{a}, \mathfrak{b})$ und $\mathfrak{a} \cap \mathfrak{b} = kgV(\mathfrak{a}, \mathfrak{b})$.

Für Hauptideale (a) verwendet man oft Sprechweisen, die (a) durch a ersetzen: Man sagt $\mathfrak{p} \mid a$ für $\mathfrak{p} \mid (a)$ und $a = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ für $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, usw.

Diese Teilertheorie erhält ihre befriedigendste Formulierung durch die gebrochenen Ideale:

Sei wieder R ein Dedekindring, mit Quotientenkörper K .

Definition 4.12 (a) Ein **gebrochenes Ideal** in (oder von) K ist ein endlich erzeugter R -Untermodul von K .

(b) Für ein Element $a \in K^\times$ heißt $(a) := R \cdot a \subseteq K$ das zugehörige (gebrochene) **Hauptideal**.

(c) Das Produkt von gebrochenen Idealen $\mathfrak{a}, \mathfrak{b}$ wird definiert durch

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^n a_i \cdot b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\} .$$

Bemerkung 4.13 (a) Da R noethersch ist, ist ein R -Untermodul $0 \neq \mathfrak{c}$ von K genau dann ein gebrochenes Ideal, wenn es ein $0 \neq \beta \in R$ gibt mit $\beta \cdot \mathfrak{c} \subseteq R$. Die gebrochenen Ideale sind also alle von der Form $\mathfrak{c} = \frac{1}{\beta} \cdot \mathfrak{a}$, $\mathfrak{a} \subseteq R$ übliches Ideal und $\beta \in R \setminus \{0\}$.

(b) Für gebrochene Hauptideale $(\alpha), (\beta)$ gilt $(\alpha) \cdot (\beta) = (\alpha \cdot \beta)$.

(c) Die gebrochenen Ideale $\mathfrak{a} \subseteq R$, also die üblichen Ideale von R , heißen zur Unterscheidung auch **ganze Ideale**.

Satz 4.14 Die gebrochenen Ideale bilden mit dem Produkt aus 4.11 (c) eine abelsche Gruppe, die Idealgruppe I_K von K . Das neutrale Element ist $(1) = R$, das Inverse von \mathfrak{a} ist

$$\mathfrak{a}^{-1} = \{\beta \in K \mid \beta \cdot \mathfrak{a} \subseteq R\} .$$

Beweis: Assoziativität, Kommutativität sowie die Neutralität von (1) sind klar. Für ein Primideal \mathfrak{p} haben wir schon gesehen, dass $\mathfrak{p}\mathfrak{p}^{-1} = R$. Ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ ein ganzes Ideal, so ist also $\mathfrak{b} := \mathfrak{p}_1^{-1} \cdot \mathfrak{p}_2^{-1} \cdots \mathfrak{p}_r^{-1}$ ein Inverses. Wir zeigen nun $\mathfrak{b} = \mathfrak{a}^{-1}$. Wegen $\mathfrak{b} \cdot \mathfrak{a} = R$ ist $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Ist umgekehrt $\beta \in \mathfrak{a}^{-1}$, also $\beta \cdot \mathfrak{a} \subseteq R$, so ist $\beta \cdot R = \beta \mathfrak{a} \mathfrak{b} \subseteq \mathfrak{b}$, also $\beta \in \mathfrak{b}$, also auch $\mathfrak{a}^{-1} \subseteq \mathfrak{b}$. Ist schließlich \mathfrak{c} ein gebrochenes Ideal und $\beta \in R \setminus \{0\}$ mit $\beta \cdot \mathfrak{c} \subseteq R$, so ist offenbar $(\beta \cdot \mathfrak{c})^{-1} = \beta^{-1} \cdot \mathfrak{c}^{-1}$, also $R = \beta \cdot \mathfrak{c} \cdot \beta^{-1} \mathfrak{c}^{-1} = \mathfrak{c} \cdot \mathfrak{c}^{-1}$.

Corollar 4.15 Jedes gebrochene Ideal \mathfrak{a} in K besitzt eine eindeutige Produktdarstellung

$$\mathfrak{a} = \prod_{\mathfrak{p} \text{ Primideal } \neq 0} \mathfrak{p}^{n_{\mathfrak{p}}}$$

mit $n_{\mathfrak{p}} \in \mathbb{Z}$, $n_{\mathfrak{p}} = 0$ für fast alle \mathfrak{p} . Mit anderen Worten: I_K ist die freie abelsche Gruppe auf den Primidealen $\mathfrak{p} \neq 0$.

Beweis: Jedes gebrochene Ideal \mathfrak{a} ist nach 4.12 (a) Quotient $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ von zwei Idealen $\mathfrak{b}, \mathfrak{c} \subseteq R$. Diese besitzen Primzerlegungen, also auch \mathfrak{a} . Die Eindeutigkeit der Primzerlegung folgt sofort aus der Eindeutigkeit für ganze Ideale.

Bemerkung 4.16 Wir können die Teilertheorie auf gebrochene Ideale erweitern, indem wir definieren

$$\begin{aligned} \mathfrak{a} \mid \mathfrak{b} &\Leftrightarrow \mathfrak{b} \subseteq \mathfrak{a} \\ &\Leftrightarrow \mathfrak{b}\mathfrak{a}^{-1} \text{ ganz} . \end{aligned}$$

Wir schreiben auch $\mathfrak{b}/\mathfrak{a}$ für $\mathfrak{b}\mathfrak{a}^{-1}$.

Nach 4.12 (b) bilden die gebrochenen Hauptideale (α) , $\alpha \in K^\times$ eine Untergruppe $P_K \subseteq I_K$ der Idealgruppe.

Definition 4.17 Der Quotient

$$Cl_K := I_K/P_K$$

heißt die **Klassengruppe** von K .

Als ein Hauptresultat der algebraischen Zahlentheorie werden wir später zeigen, dass Cl_K endlich ist. Diese Gruppe und ihre Ordnung h_K (die **Klassenzahl** von K) sind wichtige Invarianten eines Zahlkörpers.

5 Primzerlegungen in Erweiterungen

Wir haben schon gesehen, dass es von Interesse ist zu wissen, welche Primideale \mathfrak{p} eines Zahlkörpers K in einer Erweiterung L von K Primideal bleiben. Ähnlich interessant und nützlich ist auch das genaue Zerlegungsgesetz.

Sei A ein Dedekindring mit Quotientenkörper K , L/K eine endliche Körpererweiterung und B der ganze Abschluss von A in L . (Beispiel: L/K Zahlkörper, $A = \mathcal{O}_K$, $B = \mathcal{O}_L$).

Lemma 5.1 B ist ein Dedekindring.

Beweis: B ist ganz abgeschlossen nach 2.8 (a). Wie im Beweis von 4.4 folgt weiter: Ist $\mathfrak{P} \neq 0$ ein Primideal von B , so ist $\mathfrak{p} = \mathfrak{P} \cap A$ von Null verschiedenes Primideal in A , und B/\mathfrak{P} ist eine ganze Ringerweiterung des Körpers A/\mathfrak{p} . Gäbe es in B/\mathfrak{P} ein nicht-triviales Primideal, so gäbe es nach dem gleichen Argument auch eins in A/\mathfrak{p} was nicht sein kann.

Dass B noethersch ist, beweisen wir nur für den Fall, dass L/K separabel ist (für den allgemeinen Fall siehe Neukirch 'Algebraische Zahlentheorie' I 12.8). Dann ist mit einer in B gelegenen K -Basis $\alpha_1, \dots, \alpha_n$ von L und $d = d(\alpha_1, \dots, \alpha_n)$

$$B \subseteq \frac{1}{d}(A\alpha_1 + \dots + A\alpha_n).$$

Der rechte A -Modul ist endlich erzeugt, also auch jedes Ideal von B als A -Modul (da A noethersch ist) also auch als B -Modul, d.h., als Ideal.

Lemma/Definition 5.2 Für ein Primideal $\mathfrak{P} \neq 0$ von B und ein Primideal $\mathfrak{p} \neq 0$ von A sind äquivalent:

- (a) $\mathfrak{P} \cap A = \mathfrak{p}$
- (a') $\mathfrak{P} \cap K = \mathfrak{p}$
- (b) $\mathfrak{p} \subseteq \mathfrak{P}$
- (c) $\mathfrak{p}B \subseteq \mathfrak{P}$
- (d) $\mathfrak{P} \mid \mathfrak{p}B$

Zu diesem Fall sagen wir \mathfrak{P} liegt über \mathfrak{p} (bzw. \mathfrak{p} liegt unter \mathfrak{P} , bzw. $\mathfrak{P}/\mathfrak{p}$).

Beweis: der Äquivalenzen:

$$(a) \Leftrightarrow (a'): B \cap K = A \Rightarrow \mathfrak{P} \cap K = \mathfrak{P} \cap B \cap K = \mathfrak{P} \cap A$$

$$(c) \Leftrightarrow (d) \text{ gilt nach Definition}$$

$$(b) \Leftrightarrow (c) \text{ ist klar}$$

$$(a) \Rightarrow (b) \text{ ist trivial}$$

$$(b) \Rightarrow (a) \mathfrak{p} \subseteq \mathfrak{P} \Rightarrow \mathfrak{p} \subseteq \mathfrak{P} \cap A; \text{ aber } \mathfrak{p} \text{ ist maximal und } \mathfrak{P} \cap A \neq A \text{ (da } 1 \notin \mathfrak{P}\text{)}.$$

Im Folgenden heißt "Primideal" immer "Primideal $\neq 0$ ". Jedes Primideal \mathfrak{P} von B liegt dann über genau einem Primideal \mathfrak{p} von A , nämlich $\mathfrak{p} = \mathfrak{P} \cap A$ (man sieht wie im Beweis von 5.1, dass dies $\neq 0$ ist). Umgekehrt gilt:

Lemma 5.3 Ist $\mathfrak{p} \subseteq A$ ein Primideal, so ist $\mathfrak{p}B \neq B$. Insbesondere gibt es ein Primideal \mathfrak{P} von B über \mathfrak{p} .

Beweis: Nach 4.8 ist $\mathfrak{p}^{-1} \supsetneq A$. Sei also $x \in \mathfrak{p}^{-1} \setminus A$, d.h., $x \in K \setminus A$ mit $x \cdot \mathfrak{p} \subseteq A$. Dann ist

$$x \cdot \mathfrak{p}B \subseteq A \cdot B = B$$

Wäre $\mathfrak{p}B = B$, so wäre also $x \in B \cap K = A$ – Widerspruch! Also ist $\mathfrak{p}B \subsetneq B$. Da B noethersch ist, gibt es also ein maximales Ideal $\mathfrak{P} \subseteq B$ mit $\mathfrak{p}B \subseteq \mathfrak{P}$.

Nach der eindeutigen Primzerlegung in B gibt es also eindeutig bestimmte, paarweise verschiedene Primideale $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ in B und natürliche Zahlen e_1, \dots, e_r mit

$$(5.4.1) \quad \mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

(man schreibt auch oft nur $\mathfrak{p} = \mathfrak{p}^{e_1} \cdots \mathfrak{P}_r^{e_r}$), wobei die \mathfrak{P}_i gerade die verschiedenen Primteiler von $\mathfrak{p}B$, also die verschiedenen $\mathfrak{P}_i/\mathfrak{p}$ sind.

Seien $k(\mathfrak{p}) = A/\mathfrak{p}$ und $k(\mathfrak{P}_i) = B/\mathfrak{P}_i$ die Restklassenkörper von \mathfrak{p} bzw. \mathfrak{P}_i (beide Ideale sind maximal!). Die Inklusion $A \subseteq B$ induziert wegen $\mathfrak{P}_i \cap A = \mathfrak{p}$ einen injektiven Ringhomomorphismus

$$(5.4.2) \quad k(\mathfrak{p}) \hookrightarrow k(\mathfrak{P}_i),$$

also eine Körpererweiterung $k(\mathfrak{P}_i)/k(\mathfrak{p})$.

Definition 5.4 (a) Die Zahl e_i heißt der **Verzweigungsindex** von \mathfrak{P}_i über \mathfrak{p} , Bezeichnung $e(\mathfrak{P}_i/\mathfrak{p})$.

(b) \mathfrak{P}_i heißt **unverzweigt** über \mathfrak{p} (oder in L/K), wenn $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ und wenn die Körpererweiterung $k(\mathfrak{P}_i)/k(\mathfrak{p})$ separabel ist.

(c) \mathfrak{p} heißt **unverzweigt** in L/K , wenn alle $\mathfrak{P}_i/\mathfrak{p}$ ($i = 1, \dots, r$) unverzweigt über \mathfrak{p} sind.

(d) Der **Restklassengrad** von \mathfrak{P}_i über \mathfrak{p} ist definiert als

$$f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [k(\mathfrak{P}_i) : k(\mathfrak{p})].$$

(e) \mathfrak{p} heißt **unzerlegt** in L/K , wenn $r = 1$, d.h., wenn es nur ein Primideal \mathfrak{P} über \mathfrak{p} gibt, und **träge**, wenn zusätzlich $e(\mathfrak{P}/\mathfrak{p}) = 1$ ist, d.h., wenn $\mathfrak{p}B$ prim ist.

(f) \mathfrak{p} heißt **voll zerlegt** in L/K , wenn $f(\mathfrak{P}_i/\mathfrak{p}) = 1$ und $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ für alle $i = 1, \dots, r$ ist.

Beispiel 5.5 Im Körper der Gaußschen Zahlen ist

$$2 = \mathbb{N}_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = -i(1+i)^2.$$

Dies zeigt, dass das Hauptideal $\mathfrak{p} = (1+i)$ prim ist (vgl. Übungsaufgabe 3 (i)) und dass

$$(2) = \mathfrak{p}^2.$$

Weiter ist

$$\mathbb{Z}[i]/\mathfrak{p} = \mathbb{Z}[i]/(1+i) \cong \mathbb{Z}[x]/(x^2+1, 1+x) \cong \mathbb{Z}/2\mathbb{Z}.$$

Die Einbettung der Restklassenkörper $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/(2) \hookrightarrow \mathbb{Z}[i]/\mathfrak{p}$ ist also ein Isomorphismus. Daher ist 2 (d.h., das Primideal (2)) verzweigt und unzerlegt in $\mathbb{Q}(i)/\mathbb{Q}$ mit nur einem Primideal $\mathfrak{p}/2$, wobei

$$e(\mathfrak{p}/2) = 2, f(\mathfrak{p}/2) = 1.$$

Für die Primzahl 3 ist dagegen nach 1.7 das Hauptideal (3) auch prim in $\mathbb{Q}(i)$ und

$$\mathbb{Z}[i]/(3) = \mathbb{Z}[i]/3 \cdot \mathbb{Z}[i] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

als \mathbb{Z} -Modul. Der Körper $\mathbb{Z}[i]/(3)$ hat also den Grad 2 über $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ (es ist also $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$, der Körper mit 9 Elementen). Daher ist 3 unverzweigt und unzerlegt, also träge in $\mathbb{Q}(i)/\mathbb{Q}$, und für das Primideal $\mathfrak{q} = (3)$ über 3 gilt

$$e(\mathfrak{q}/3) = 1, f(\mathfrak{q}/3) = 2.$$

Für die Primzahl 5 ist dagegen nach 1.7 das Primideal (5) zerlegt in $\mathbb{Q}(i)$, und zwar ist $5 = N_{\mathbb{Q}(i)/\mathbb{Q}}(2+i) = (2+i)(2-i)$, mit nicht-assoziierten Primelementen $2+i$ und $2-i$. Daher haben wir Primideale $\mathfrak{p}_1 = (2+i) \neq (2-i) = \mathfrak{p}_2$ und

$$(5) = \mathfrak{p}_1 \cdot \mathfrak{p}_2.$$

Weiter ist

$$\mathbb{Z}[i]/\mathfrak{p}_1 = \mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[x]/(x^2+1, 2+x) \cong \mathbb{Z}/5\mathbb{Z},$$

und ebenso folgt $\mathbb{Z}[i]/\mathfrak{p}_2 \cong \mathbb{Z}/5\mathbb{Z}$. Damit gilt für $i = 1, 2$

$$e(\mathfrak{p}_i/5) = 1, f(\mathfrak{p}_i/5) = 1.$$

Wie bestimmt man nun konkret die Zerlegung eines Primideals? Hier hilft in vielen Fällen die folgende Methode:

Sei L/K eine separable Erweiterung und $\beta \in B$ ein primitives Element (d.h., $L = K(\beta)$) mit Minimalpolynom

$$p(x) \in A[x].$$

Wir betrachten den Unterring

$$B' = A[\beta] \subseteq B.$$

Sein **Führer** wird definiert als das Ideal

$$\mathfrak{F} = \{b \in B \mid b \cdot B \subseteq B'\}.$$

Da B als A -Modul endlich erzeugt ist (Beweis von 5.1, L/K separabel), ist $\mathfrak{F} \neq 0$.

Satz 5.6 Sei \mathfrak{p} ein Primideal von A , welches teilerfremd zu \mathfrak{F} ist (d.h., $\mathfrak{p}B$ und \mathfrak{F} sind teilerfremd). Sei

$$\overline{p(x)} = \bar{p}_1(x)^{e_1} \cdots \bar{p}_r(x)^{e_r}$$

die Zerlegung der Reduktion

$$\overline{p(x)} = p(x) \pmod{\mathfrak{p}}$$

von $p(x)$ in irreduzible normierte Faktoren $\bar{p}_i(x)$ im Polynomring $A[x]/\mathfrak{p}A[x] \cong k(\mathfrak{p})[x]$, wobei die \bar{p}_i paarweise teilerfremd sind. Seien $p_i(x) \in A[x]$ normierte Polynome mit $\bar{p}_i(x) = p_i(x) \pmod{\mathfrak{p}}$. Dann sind

$$\mathfrak{P}_i = \mathfrak{p}B + p_i(\beta)B \quad (i = 1, \dots, r)$$

die verschiedenen über \mathfrak{p} liegenden Primideale in B . Weiter gilt $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, also

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

für den Verzweigungsindex von \mathfrak{P}_i über \mathfrak{p} , und der Restklassengrad von \mathfrak{P}_i über \mathfrak{p} ist

$$f(\mathfrak{P}_i/\mathfrak{p}) = \deg \bar{p}_i(x),$$

der Grad von \bar{p}_i .

Zum Beweis benutzen wir:

Lemma 5.7 Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal.

(a) Die Surjektion

$$\varphi : R \twoheadrightarrow R/\mathfrak{a}$$

induziert eine Bijektion

$$\begin{aligned} \varphi^{-1} : \{\text{Ideale von } R/\mathfrak{a}\} &\xrightarrow{\sim} \{\text{Ideale } \mathfrak{b} \subseteq R \text{ mit } \mathfrak{a} \subseteq \mathfrak{b}\} \\ \mathfrak{c} &\mapsto \varphi^{-1}(\mathfrak{c}) \end{aligned}$$

mit Umkehrabbildung $\mathfrak{b} \mapsto \varphi(\mathfrak{b})$. Dies induziert eine Bijektion

$$\varphi^{-1} : \{\text{Primideal von } R/\mathfrak{a}\} \xrightarrow{\sim} \{\text{Primideale } \mathfrak{p} \subseteq R \text{ mit } \mathfrak{a} \subseteq \mathfrak{p}\}.$$

(b) Sei R ein Dedekindring und $\mathfrak{a} \neq 0$. Dann hat R/\mathfrak{a} endlich viele Primideale $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ und es gibt eindeutig bestimmte $e_1, \dots, e_r \in \mathbb{N}$ mit der Eigenschaft: Für alle $e'_1, \dots, e'_r \in \mathbb{N}$ gilt

$$\mathfrak{q}_1^{e'_1} \cdots \mathfrak{q}_r^{e'_r} = 0 \quad \Leftrightarrow \quad e'_i \geq e_i \quad \text{für alle } i = 1, \dots, r.$$

Für die Primideale $\mathfrak{p}_i = \varphi^{-1}(\mathfrak{q}_i) \subseteq R$ gilt dann

$$\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}.$$

Beweis (a): Offenbar ist $\varphi^{-1}(\mathfrak{c})$ ein Ideal in R mit $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{c})$, und wegen der Surjektivität von φ gilt $\varphi(\varphi^{-1}(\mathfrak{c})) = \mathfrak{c}$. Umgekehrt gilt wegen der Surjektivität von φ für ein Ideal $\mathfrak{b} \subseteq R$ mit $\mathfrak{a} \subseteq \mathfrak{b}$, dass $\varphi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a} \subseteq R/\mathfrak{a}$ ein Ideal ist und dass $\varphi^{-1}(\mathfrak{b}/\mathfrak{a}) = \mathfrak{b}$. Wegen $R/\mathfrak{b} \cong (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ ist \mathfrak{b} genau dann ein Primideal, wenn dies für $\mathfrak{b}/\mathfrak{a} \subseteq R/\mathfrak{a}$ gilt.

(b) Ist $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ die Zerlegung in Primideale ($\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$, $e_i \in \mathbb{N}$), so gilt nach der Teilertheorie in R , dass $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ die Primideale von R sind, die \mathfrak{a} umfassen. Nach (a) sind $\mathfrak{q}_i = \mathfrak{p}_i/\mathfrak{a}$, für $i = 1, \dots, r$, gerade die Primideale von R/\mathfrak{a} . Weiter gilt für $e'_1, \dots, e'_r \in \mathbb{N}$

$$\begin{aligned} 0 &= \mathfrak{q}_1^{e'_1} \cdots \mathfrak{q}_r^{e'_r} = (\mathfrak{p}_1^{e'_1} \cdots \mathfrak{p}_r^{e'_r} + \mathfrak{a})/\mathfrak{a} \\ \Leftrightarrow \mathfrak{p}_1^{e'_1} \cdots \mathfrak{p}_r^{e'_r} &\subseteq \mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \\ \Leftrightarrow e'_i &\geq e_i \quad \text{für alle } i = 1, \dots, r. \end{aligned}$$

Offenbar sind e_1, \dots, e_r hierdurch eindeutig bestimmt.

Beweis von Satz 5.6: Wir wenden Lemma 5.7 auf $\mathfrak{p}B \subseteq B$ an und untersuchen $B/\mathfrak{p}B$.

Nach Voraussetzung ist $\mathfrak{F} + \mathfrak{p}B = B$. Wegen $\mathfrak{F} \subset B'$ ist also

$$B = B' + \mathfrak{p}B ;$$

d.h., die Abbildung

$$B' \rightarrow B/\mathfrak{p}B$$

ist surjektiv. Ihr Kern ist $B' \cap \mathfrak{p}B$, und dies ist gleich $\mathfrak{p}B'$, denn wegen $\mathfrak{F} + \mathfrak{p}B = B$ und $\mathfrak{F} \cdot B \subseteq B'$ ist $B' \cap \mathfrak{p}B \subseteq (\mathfrak{F} + \mathfrak{p}B) \cdot (B' \cap \mathfrak{p}B) \subseteq \mathfrak{p}B'$. Wir erhalten also einen Isomorphismus

$$(5.6.1) \quad B'/\mathfrak{p}B' \cong B/\mathfrak{p}B .$$

Andererseits induziert die Surjektion $A[x] \rightarrow B', x \mapsto \beta$, einen Isomorphismus

$$\begin{aligned} A[x]/(p(x)) &\xrightarrow{\sim} B' \\ x \bmod (p(x)) &\mapsto \beta \quad (\text{d.h., } f(x) \bmod (p(x)) \mapsto f(\beta)) . \end{aligned}$$

und durch Reduktion modulo \mathfrak{p} einen Ringisomorphismus

$$(5.6.2) \quad k(\mathfrak{p})[x]/(\overline{p(x)}) \cong B'/\mathfrak{p}B' .$$

Wegen $\overline{p(x)} = \prod_{i=1}^r \overline{p_i(x)}^{e_i}$ liefert der chinesische Restsatz weiter den Isomorphismus

$$(5.6.3) \quad k(\mathfrak{p})[x]/(\overline{p(x)}) \cong \bigoplus_{i=1}^r k(\mathfrak{p})[x]/(\overline{p_i(x)})^{e_i} ,$$

und mit Lemma 5.7, angewandt auf $(\overline{p(x)}) \subseteq k(\mathfrak{p})[x]$, folgt

- Die Primideale des Rings $k(\mathfrak{p})[x]/(\overline{p(x)})$ sind die durch $\overline{p_i(x)} \bmod (\overline{p(x)})$ erzeugten Hauptideale \mathfrak{q}_i .
- Es gilt $\mathfrak{q}_1^{e'_1} \dots \mathfrak{q}_r^{e'_r} = 0 \Leftrightarrow e'_i \geq e_i \quad \forall i$.

Über die durch (5.6.1) und (5.6.2) gegebene Isomorphie

$$(5.6.4) \quad \begin{aligned} k(\mathfrak{p})[x]/(\overline{p(x)}) &\xrightarrow{\phi} B/\mathfrak{p}B \\ f(x) &\mapsto f(\beta) \bmod \mathfrak{p} \end{aligned}$$

erhalten wir:

- Die Primideale in $B/\mathfrak{p}B$ sind die Hauptideale $(\overline{p_i(\beta)})$ für $\overline{p_i(\beta)} := p_i(\beta) \bmod \mathfrak{p}$
- Es gilt $(\overline{p_1(\beta)})^{e'_1} \dots (\overline{p_r(\beta)})^{e'_r}$ in $B/\mathfrak{p}B$ genau dann wenn $e'_i \geq e_i$ für alle i .

Sei nun

$$\varphi : B \twoheadrightarrow B/\mathfrak{p}B$$

die kanonische Surjektion. Dann gilt nach Lemma 5.7

- 1) Die Ideale $\mathfrak{P}_i = \varphi^{-1}(\overline{p_i(\beta)}) = p_i(\beta)B + \mathfrak{p}B$ ($i = 1, \dots, r$) sind gerade die verschiedenen Primideale von B , die $\mathfrak{p}B$ umfassen, also die verschiedenen Primteiler von $\mathfrak{p}B$.
- 2) $\mathfrak{p}B = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$.

Weiter haben wir Isomorphismen von $k(\mathfrak{p})$ -Vektorräumen

$$B/\mathfrak{P}_i \cong k(\mathfrak{p})[x]/(\overline{p_i}(x))$$

und damit

$$f(\mathfrak{P}_i/\mathfrak{p}) = \dim_{k(\mathfrak{p})} B/\mathfrak{P}_i = \deg \overline{p_i}(x).$$

Bemerkung 5.8 Wie wir gesehen haben, ist $\mathfrak{F} \neq 0$, also auch $\mathfrak{F} \cap A \neq 0$. Es gibt also $0 \neq a \in A$ mit $aB \subseteq B' = A[\beta]$ (explizit wähle A -Erzeugende β_1, \dots, β_n von B , schreibe sie als K -Linearkombinationen von $1, \beta, \dots, \beta^{n-1}$ (da $L = K(\beta)$), und finde a als Hauptnenner aller Koeffizienten). Ist \mathfrak{p} teilerfremd zu a (also $a \notin \mathfrak{p}$), so ist \mathfrak{p} teilerfremd zu \mathfrak{F} : $\mathfrak{p} + aA = A \Rightarrow \mathfrak{p}B + aB = \beta \Rightarrow \mathfrak{p}B + \mathfrak{F} = B$ wegen $a \in \mathfrak{F}$.

Insbesondere können wir $a = d := d(1, \beta, \dots, \beta^{n-1})$ nehmen, denn wir haben gesehen (Proposition 3.15), dass $dB \subseteq A \oplus A\beta \oplus \dots \oplus A\beta^{n-1} = B'$, also $d \in \mathfrak{F}$. Ist also \mathfrak{p} prim zur Diskriminante $d(1, \beta, \dots, \beta^{n-1})$, so können wir Satz 5.6 anwenden.

Wir betrachten nun noch zwei wichtige Eigenschaften der Verzweigungsindizes und Restklassengrade.

Lemma 5.9 Sei M/L eine weitere endliche Erweiterung, C der ganze Abschluss von B in M und \mathfrak{Q} ein Primideal in C . Sei $\mathfrak{P} = \mathfrak{Q} \cap B$ und $\mathfrak{p} = \mathfrak{Q} \cap A = \mathfrak{P} \cap A$, so dass $\mathfrak{Q}/\mathfrak{P}/\mathfrak{p}$.

Dann gilt

$$(a) \quad e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P}) \cdot e(\mathfrak{P}/\mathfrak{p}).$$

$$(b) \quad f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P}) \cdot e(\mathfrak{P}/\mathfrak{p}).$$

Beweis: (a) folgt sofort aus der Eindeutigkeit der Primzerlegung, und die Gleichung (b) ist die Multiplikatивität des Grades für die Körpererweiterungen $k(\mathfrak{Q})/k(\mathfrak{P})/k(\mathfrak{p})$.

Die folgende Gleichung wird auch die **fundamentale Gleichung** genannt und ist sehr wichtig.

Satz 5.10 Sei L/K eine separable Erweiterung vom Grad n . Für ein Primideal \mathfrak{p} in A sei

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

die Primzerlegung von \mathfrak{p} in B , also $e_i = e(\mathfrak{P}_i/\mathfrak{p})$. Mit $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ gilt dann

$$\sum_{i=1}^r e_i \cdot f_i = n, \quad \text{also} \quad \sum_{i=1}^r e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = n.$$

Beweis: Nach dem chinesischen Restsatz hat man einen Isomorphismus

$$B/\mathfrak{p}B \cong \bigoplus_{i=1}^r B/\mathfrak{P}_i^{e_i},$$

denn die Ideale $\mathfrak{P}_i^{e_i}$ sind paarweise teilerfremd. Dies ist ein Isomorphismus von Vektorräumen über dem Körper $F = A/\mathfrak{p}$. Daher genügt es zu zeigen, dass

- (i) $\dim_F B/\mathfrak{p}B = n$.
- (ii) $\dim_F B/\mathfrak{P}_i^{e_i} = e_i \cdot f_i$.

Beweis von (i): Seien $\beta_1, \dots, \beta_m \in B$ so, dass die Restklassen $\overline{\beta}_1, \dots, \overline{\beta}_m \in B/\mathfrak{p}B$ eine F -Basis bilden (beachte, dass B nach dem Beweis von 5.1 ein endlich erzeugter A -Modul ist, also auch $\dim_F B/\mathfrak{p}B < \infty$). Wir zeigen, dass β_1, \dots, β_m dann eine K -Basis von L bilden; hieraus folgt $m = n$.

(a) β_1, \dots, β_m sind linear unabhängig: Angenommen

$$a_1\beta_1 + \dots + a_m\beta_m = 0$$

mit $a_1, \dots, a_m \in A$, nicht alle null. Für das Ideal

$$\mathfrak{a} = (a_1, \dots, a_m) \subseteq A$$

ist dann $\mathfrak{a} \neq 0$ und daher $\mathfrak{a}^{-1}\mathfrak{p} \subsetneq \mathfrak{a}^{-1}$. Sei $\alpha \in \mathfrak{a}^{-1}$ mit $\alpha \notin \mathfrak{a}^{-1}\mathfrak{p}$, also $\alpha \cdot \mathfrak{a} \not\subseteq \mathfrak{p}$ ($\alpha \cdot \mathfrak{a} \subseteq \mathfrak{p} \Rightarrow \alpha A = \alpha \mathfrak{a} \mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}\mathfrak{p}$). Dann ist $\alpha a_1, \dots, \alpha a_m \in A$, aber nicht alle $\alpha a_i \in \mathfrak{p}$. Dies gibt eine nicht-triviale Linearkombination

$$\overline{\alpha a_1} \cdot \overline{\beta}_1 + \dots + \overline{\alpha a_m} \cdot \overline{\beta}_m = 0$$

in $B/\mathfrak{p}B$ – Widerspruch!

(b) β_1, \dots, β_m erzeugen L über K : Sei $M = A\beta_1 + \dots + A\beta_m \subseteq B$ und $N = B/M$. Da $\overline{\beta}_1 = \beta_1 + \mathfrak{p}B, \dots, \overline{\beta}_m = \beta_m + \mathfrak{p}B$ den B -Modul $B/\mathfrak{p}B$ erzeugen, gilt $M + \mathfrak{p}B = B$, also $N/\mathfrak{p}N \cong B/\mathfrak{p}B + M = 0$. Da L/K separabel ist, ist B ein endlich erzeugter A -Modul, also auch N .

Sei $(\gamma_1, \dots, \gamma_k)$ ein Erzeugendensystem von N als A -Modul; dann gibt es wegen $N = \mathfrak{p}N$ Elemente $a_{ij} \in \mathfrak{p}$ mit

$$\gamma_i = \sum_{j=1}^k a_{ij} \gamma_j \quad (i = 1, \dots, k).$$

Mit Lemma 2.4 folgt

$$d \cdot N = 0,$$

wobei $d = \det(E_k - a_{ij})$. Wegen $a_{ij} \in \mathfrak{p}$ für alle i, j folgt $E_k - (a_{ij}) \equiv E_k \pmod{\mathfrak{p}M_n(A)}$ und damit $d \equiv 1 \pmod{\mathfrak{p}}$. Daher ist $d \neq 0$. Es folgt $dB \subseteq M = A\beta_1 + \dots + A\beta_m$ und damit $L = dL = K\beta_1 + \dots + K\beta_m$.

Beweis von (ii): Wir haben eine absteigende Kette

$$(5.10.1) \quad B/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i^2/\mathfrak{P}_i^{e_i} \supseteq \dots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i}$$

von F -Vektorräumen. Der ν -te Quotient $(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{e_i})/(\mathfrak{P}_i^{\nu+1}/\mathfrak{P}_i^{e_i})$ dieser Kette ist isomorph zu $\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}$, und dies ist wiederum isomorph zu B/\mathfrak{P}_i : Ist nämlich $\beta \in \mathfrak{P}_i^\nu \setminus \mathfrak{P}_i^{\nu+1}$, so ist der Homomorphismus

$$\begin{aligned} \varphi : B &\longrightarrow \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1} \\ b &\longmapsto b \cdot \beta \pmod{\mathfrak{P}_i^{\nu+1}} \end{aligned}$$

surjektiv, da der ggT von $\mathfrak{P}_i^{\nu+1}$ und βB gleich \mathfrak{P}_i^ν ist ($\beta \in \mathfrak{P}_i^\nu \setminus \mathfrak{P}_i^{\nu+1} \Rightarrow \mathfrak{P}_i^\nu \mid \beta B$ und $\mathfrak{P}_i^{\nu+1} \nmid \beta B$), so dass $\mathfrak{P}_i^\nu = \beta B + \mathfrak{P}_i^{\nu+1}$. Weiter ist $\ker \varphi = \mathfrak{P}_i$, denn offenbar ist $\mathfrak{P}_i \subseteq \ker \varphi \subsetneq B$.

Der Homomorphiesatz liefert also einen Isomorphismus

$$\bar{\varphi} : B/\mathfrak{P}_i \xrightarrow{\sim} \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1} .$$

Damit folgt $\dim_F \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1} = \dim_F B/\mathfrak{P}_i = [k(\mathfrak{P}_i) : F] = f_i$ und

$$\dim_F B/\mathfrak{P}_i^{e_i} \stackrel{(*)}{=} \sum_{\nu=0}^{e_i-1} \dim_F [(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{e_i})/(\mathfrak{P}_i^{\nu+1}/\mathfrak{P}_i^{e_i})] = \sum_{\nu=0}^{e_i-1} \dim_F \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1} = e_i \cdot f_i .$$

Die Gleichung $(*)$ ergibt sich induktiv aus (5.10.1) und der Tatsache, dass $\dim V = \dim W + \dim V/W$ für ein Vektorraum V und einen Unterraum W .

Bemerkung 5.11 \mathfrak{p} heißt voll zerlegt (oder total zerlegt) in der Erweiterung L/K , wenn $e(\mathfrak{P}/\mathfrak{p}) = 1$ und $f(\mathfrak{P}/\mathfrak{p}) = 1$ für alle $\mathfrak{P}/\mathfrak{p}$. Für separables L/K ist dies also der Fall, wenn in der Zerlegung

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

$r = n = [L : K]$, so dass automatisch $e_i = 1 = f_i$ für alle $i = 1, \dots, r$.

Beispiel 5.12 Sei L/K eine quadratische separable Erweiterung, also $[L : K] = 2$. Wegen $\sum_{i=1}^r e_i f_i = 2$ sind nur folgende Fälle möglich:

- (a) $r = 1, e_1 = 2, f_1 = 1$: \mathfrak{p} ist verzweigt (und unzerlegt).
- (b) $r = 1, e_1 = 1, f_1 = 2$: \mathfrak{p} ist unzerlegt, mit Restklassengrad 2, und unverzweigt falls die Erweiterung $k(\mathfrak{P}_1)/k(\mathfrak{p})$ separabel ist.
- (c) $r = 2, e_i = 1, f_i = 1 (i = 1, 2)$: \mathfrak{p} ist voll zerlegt und unverzweigt.

Dies zeigt, dass im Beispiel 5.5 alle möglichen Zerlegungstypen vorkommen.

6 Zyklotomische Körper

Sei $n \in \mathbb{N}$.

Erinnerung 6.1 Sei K ein Körper. Jede endliche Untergruppe von K^\times ist zyklisch. Insbesondere ist die Gruppe

$$\mu_n(K) = \{\zeta \in K^\times \mid \zeta^n = 1\}$$

der **n-ten Einheitswurzeln in K** zyklisch. Ist K algebraisch abgeschlossen und $\text{char}(K)$ prim zu n , so ist $\mu_n(K)$ zyklisch von der Ordnung n .

Dies wird in der Algebra bewiesen (siehe z.B. Algebra I, Lemmas 14.4 und 15.6)

Im folgenden sei K ein Körper mit $\text{char}K \nmid n$, \overline{K} ein fester algebraischer Abschluss von K und $\mu_n = \mu_n(\overline{K})$ die Gruppe aller n -ten Einheitswurzeln in \overline{K} . Nach 6.1 ist nicht-kanonisch $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$. Jedes Erzeugende der zyklischen Gruppe μ_n heißt eine **primitive n -te Einheitswurzel**.

Satz 6.2 Sei ζ_n eine primitive n -te Einheitswurzel. Dann ist $K(\zeta_n)/K$ galoissch, und es gibt einen kanonischen injektiven Gruppenhomomorphismus

$$\chi : \text{Gal}(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times ;$$

daher ist die Galoisgruppe kanonisch isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Für $K = \mathbb{Q}$ ist

$$\chi : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times ,$$

ein Isomorphismus, insbesondere ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beweis: Dies wird in der Algebra bewiesen (siehe z. B. Algebra I, §15). Wir erinnern an einige Argumente und die Definition von χ : Mit ζ_n ist auch $\zeta_n^i \in K' := K(\zeta_n)$ für jedes $i \geq 0$; daher enthält K' alle n -ten Einheitswurzeln und das Polynom $x^n - 1$, dessen Nullstelle ζ_n ist, zerfällt in Linearfaktoren über K' , d.h., K'/K ist normal. Weiter ist K'/K separabel, da $x^n - 1$ separabel ist, wegen $\text{char}(K) \nmid n$. Sei $G = \text{Gal}(K'/K)$. Für $\sigma \in G$ ist $\sigma(\zeta_n)$ wieder in μ_n . Da μ_n zyklisch von der Ordnung n ist und ζ_n ein Erzeugendes, gibt es ein $a \in \mathbb{N}$ mit

$$\sigma(\zeta_n) = \zeta_n^a ,$$

und das Element

$$\chi(\sigma) := a \pmod n \in \mathbb{Z}/n\mathbb{Z}$$

ist eindeutig durch σ bestimmt ($\zeta_n^a = \zeta_n^b \Rightarrow \zeta_n^{a-b} = 1 \Rightarrow n = \text{ord}(\zeta_n) | a - b$). Weiter ist für $\tau \in G$

$$\chi(\sigma\tau) = \chi(\sigma) \cdot \chi(\tau) .$$

Daher ist $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ (betrachte $\tau = \sigma^{-1}$), und

$$\begin{array}{ccc} \chi : & G & \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ & \sigma & \longmapsto \chi(\sigma) \end{array}$$

ein Gruppenhomomorphismus, den man auch den **zyklotomischen Charakter** nennt. Dabei gilt

$$\sigma(\zeta) = \zeta^{\chi(\sigma)} \quad \forall \zeta \in \mu_n$$

(denn $\sigma(\zeta_n^i) = \sigma(\zeta_n)^i = (\zeta_n^{\chi(\sigma)})^i = (\zeta_n^i)^{\chi(\sigma)} = \zeta_n^{i\chi(\sigma)}$). Insbesondere ist χ injektiv ($\chi(\sigma) = 1 \Rightarrow \chi(\zeta_n^i) = \zeta_n^i$ für alle $i \geq 0 \Rightarrow \sigma(x) = x$ für alle $x \in K(\zeta_n)$). Es bleibt zu zeigen, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Hierfür siehe z.B. Algebra I Corollar 15.13 (b).

Beweis: Sei $f(x)$ das Minimalpolynom von ζ_n über \mathbb{Q} . Es genügt zu zeigen, dass jede primitive n -te Einheitswurzel Nullstelle von f ist (da dann $\deg f(x) = \varphi(n) = \text{Anzahl der primitiven } n\text{-ten Einheitswurzeln}$ ist). Nun teilt $f(x)$ das Polynom $x^n - 1$; es gibt also ein Polynom h mit

$$x^n - 1 = f \cdot h .$$

Da f normiert ist, ist auch h normiert und in $\mathbb{Z}[x]$ (Polynomdivision).

1. Schritt Sei p eine Primzahl, $p \nmid n$. Dann ist ζ_n^p Nullstelle von f , d.h., $f(\zeta_n^p) = 0$.

Beweis: ζ_n^p ist wieder primitive Einheitswurzel. Ist $f(\zeta_n^p) \neq 0$, so ist $h(\zeta_n^p) = 0$, also ζ_n Nullstelle von $h(x^p)$. Hieraus folgt wiederum $f|h(x^p)$, also etwa

$$h(x^p) = f \cdot g,$$

wobei wieder g normiert und in $\mathbb{Z}[x]$ ist. Durch Reduktion modulo p folgt für die Restklassen in $\mathbb{Z}/p\mathbb{Z}[x]$:

$$\bar{h}(x)^p = \bar{h}(x^p) = \bar{f}(x) \cdot \bar{g}(x).$$

Hieraus folgt, dass $\bar{f}(x)$ und $\bar{h}(x)$ nicht teilerfremd in $\mathbb{F}_p[x]$ sind ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Körper mit p Elementen). Daher hat das Polynom

$$x^n - 1 = \bar{f}(x) \cdot \bar{h}(x)$$

mehrfache Nullstellen über \mathbb{F}_p – Widerspruch dazu, dass $\text{char } \mathbb{F}_p = p \nmid n$, s.o.!

2. Schritt Jede primitive n -te Einheitswurzel ζ' ist Nullstelle von $f(x)$.

Beweis: Es ist $\zeta' = \zeta_n^m$ mit $\text{ggT}(m, n) = 1$. Zerlegt man m in ein Produkt von Primzahlen, so sind diese alle prim zu n , und der 1. Schritt zeigt induktiv, dass $f(\zeta_n^m) = 0$.

Definition 6.3 Das Minimalpolynom $\phi_n(x)$ einer primitiven Einheitswurzel (und damit von allen primitiven Einheitswurzeln) über \mathbb{Q} heißt das **n -te Kreisteilungspolynom** (oder zyklotomische Polynom), und $\mathbb{Q}(\zeta_n)$ heißt der **n -te Kreisteilungskörper** (oder zyklotomische Körper).

Beispiel 6.4 (a) Wegen $\deg \phi_n(x) = \varphi(n)$ und $\varphi(p) = p - 1$ für eine Primzahl p ist offenbar

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

(b) Allgemeiner ist für $n = p^\nu$, p prim

$$\begin{aligned} \phi_{p^\nu}(x) &= \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = \phi_p(x^{p^{\nu-1}}) \\ &= x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \dots + x^{p^{\nu-1}} + 1. \end{aligned}$$

Wir bestimmen nun den Ring ganzer Zahlen in $\mathbb{Q}(\zeta_n)$.

Lemma 6.5 Sei $n = \ell^\nu \neq 2$ eine Primzahlpotenz, $\zeta = \zeta_n$ eine primitive n -te Einheitswurzel, $\lambda = 1 - \zeta$, und $d = \ell^{\nu-1}(\ell - 1) = \varphi(\ell^\nu) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.

(a) Dann hat die \mathbb{Q} -Basis $1, \zeta, \zeta^2, \dots, \zeta^{d-1}$ von $K = \mathbb{Q}(\zeta)$ die Diskriminante

$$d(1, \zeta, \zeta^2, \dots, \zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \cdot \ell^m,$$

wobei $m = \ell^{\nu-1}(\nu\ell - \nu - 1)$.

(b) Im Ring \mathcal{O}_K der ganzen Zahlen von K gilt

$$(\ell) = (\lambda)^d.$$

Beweis (a): Nach 3.11 bzw. Übungsaufgabe 13 ist

$$d(1, \zeta, \dots, \zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \cdot N_{K/\mathbb{Q}}(\phi'_n(\zeta)).$$

Differenziert man die Gleichung

$$(x^{\ell^{\nu-1}} - 1)\phi_n(x) = x^{\ell^{\nu}} - 1$$

und setzt ζ ein, so folgt

$$(\zeta_{\ell} - 1)\phi'_n(\zeta) = \ell^{\nu} \cdot \zeta^{-1},$$

wobei $\zeta_{\ell} := \zeta^{\ell^{\nu-1}}$ eine primitive ℓ -te Einheitswurzel ist.

Wegen $\phi_{\ell}(x) = x^{\ell-1} + \dots + x + 1 = \prod_{i=1}^{\ell-1} (x - \zeta_{\ell}^i)$ gilt

$$N_{\mathbb{Q}(\zeta_{\ell})/\mathbb{Q}}(\zeta_{\ell} - 1) = \prod_{i=1}^{\ell-1} (\zeta_{\ell}^i - 1) = (-1)^{\ell-1} \phi_{\ell}(1) = (-1)^{\ell-1} \cdot \ell.$$

Weiter ist nach 3.2 (a)

$$\begin{aligned} N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) &= (-1)^d \cdot (\text{nullter Koeffizient von } \phi_n(x)) \\ &= 1 \text{ wegen } \ell^{\nu} \neq 2. \end{aligned}$$

Es folgt

$$\begin{aligned} d(1, \zeta, \dots, \zeta^{d-1}) &= (-1)^{\frac{d(d-1)}{2}} \cdot \ell^{\nu d} \cdot \ell^{-\ell^{\nu-1}} \\ &= (-1)^{\frac{d(d-1)}{2}} \cdot \ell^{\ell^{\nu-1}(\nu\ell - \nu - 1)}. \end{aligned}$$

(b): Setzen wir $x = 1$ in

$$\phi_n(x) = x^{\ell^{\nu-1}(\ell-1)} + \dots + x^{\ell^{\nu-1}} + 1,$$

so folgt

$$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^{\times}} (1 - \zeta^a) = \ell.$$

Für jedes a gilt dabei

$$1 - \zeta^a = \varepsilon_a \cdot (1 - \zeta)$$

mit der ganzen Zahl

$$\varepsilon_a = \frac{1 - \zeta^a}{1 - \zeta} = \zeta^{a-1} + \zeta^{a-2} + \dots + \zeta + 1.$$

Ist $a' \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ mit $a' \cdot a = 1$, so ist

$$\frac{1 - \zeta}{1 - \zeta^a} = \frac{1 - (\zeta^a)^{a'}}{1 - \zeta^a} = (\zeta^a)^{a'-1} + \dots + \zeta^a + 1$$

ebenfalls ganz, somit ist ε_a eine Einheit in \mathcal{O}_K .

Es folgt

$$\ell = \varepsilon \cdot (1 - \zeta)^{\varphi(n)},$$

mit der Einheit $\varepsilon = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^{\times}} \varepsilon_a$, also

$$(\ell) = (\lambda)^d$$

für die assoziierten Hauptideale.

Bemerkung 6.6 Wegen $d = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ zeigt die fundamentale Gleichung 5.10, dass $(\lambda)/\ell$ ein Primideal vom Restklassengrad 1 ist, welches unzerlegt und verzweigt in K/\mathbb{Q} ist.

Satz 6.7 Sei $n \in \mathbb{N}$. Für den Ring \mathcal{O}_K der ganzen Zahlen in $K = \mathbb{Q}(\zeta_n)$ ist $1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}$ eine Ganzheitsbasis, d.h., es ist

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n] = \mathbb{Z} \oplus \mathbb{Z} \zeta_n \oplus \dots \oplus \mathbb{Z} \zeta_n^{\varphi(n)-1} .$$

Beweis für den Fall, dass $n = \ell^\nu$ eine Primzahlpotenz ist (für den allgemeinen Fall siehe Neukirch ‘Algebraische Zahlentheorie’ Beweis von Satz 10.2):

Wegen $d(1, \zeta, \dots, \zeta^{d-1}) = \pm \ell^m$, m wie in Lemma 6.5, erhalten wir nach Proposition 3.16

$$\ell^m \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K .$$

Setzen wir $\lambda = 1 - \zeta \in \mathbb{Z}[\zeta]$, so ist nach 6.6

$$\mathcal{O}_K / \lambda \mathcal{O}_K \cong \mathbb{Z} / \ell \mathbb{Z} ,$$

also $\mathcal{O}_K = \mathbb{Z} + \lambda \mathcal{O}_K$ und damit auch

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda \mathcal{O}_K .$$

Induktiv (mit λ multiplizieren und wieder einsetzen) folgt

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda^i \mathcal{O}_K$$

für alle $i \geq 0$. Für $i = m\varphi(n)$ folgt wegen $(\lambda^{\varphi(n)}) = (\ell)$

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \ell^m \mathcal{O}_K = \mathbb{Z}[\zeta] .$$

Wir können nun das Zerlegungsgesetz in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ vollständig beschreiben – es ist sehr übersichtlich:

Satz 6.8 Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n , und für jede Primzahl p sei $n^{(p)} = n/p^{\nu_p}$ (also $n = p^{\nu_p} \cdot n^{(p)}$ mit $p \nmid n^{(p)}$). Weiter sei f_p die kleinste natürliche Zahl mit

$$p^{f_p} \equiv 1 \pmod{n^{(p)}} ,$$

d.h., f_p sei die Ordnung von p in $(\mathbb{Z}/n^{(p)}\mathbb{Z})^\times$. Dann ist die Zerlegung von p in $K = \mathbb{Q}(\zeta_n)$

$$(p) = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^{\varphi(p^{\nu_p})} ,$$

wobei $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ verschiedene Primideale in $\mathbb{Q}(\zeta_n)$ vom gleichen Grad f_p sind. Es ist also $f(\mathfrak{p}_i/p) = f_p$ und $e(\mathfrak{p}_i/p) = \varphi(p^{\nu_p})$ für alle $i = 1, \dots, r$, und $r = \varphi(n^{(p)})/f_p$.

Beweis: Wegen $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ ist der Führer von $\mathbb{Z}[\zeta_n]$ gleich 1, und wir können für alle p den Satz 5.6 anwenden. Danach zerfällt das Primideal (p) wie das Minimalpolynom $\phi_n(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Wir haben also zu zeigen, dass für $\bar{\phi}_n(x) = \phi_n(x) \pmod p$

$$\bar{\phi}_n(x) = (p_1(x) \cdots p_r(x))^{\varphi(p^{\nu_p})}$$

ist, wobei p_1, \dots, p_r verschiedene irreduzible Polynome über $\mathbb{Z}/p\mathbb{Z}$ sind, die alle den Grad f_p haben. Sei $m = n^{(p)}$, also $n = p^{\nu_p} \cdot m$, $p \nmid m$. Ist $\{\xi_i\}$ die Menge aller primitiven m -ten Einheitswurzeln und $\{\eta_j\}$ die Menge aller primitiven p^{ν_p} -ten Einheitswurzeln, so ist $\{\xi_i \cdot \eta_j\}$ wegen $\mu_n = \mu_{p^{\nu_p}} \times \mu_m$ die Menge aller primitiven n -ten Einheitswurzeln.

Daher ist

$$\phi_n(x) = \prod_{i,j} (x - \xi_i \cdot \eta_j) .$$

Wegen $x^{p^{\nu_p}} - 1 \equiv (x - 1)^{p^{\nu_p}} \pmod p$ ist dabei $\eta_j \equiv 1 \pmod{\mathfrak{p}}$ für jedes Primideal \mathfrak{p}/p von $\mathbb{Q}(\zeta_n)$. Also ist

$$\phi_n(x) \equiv \phi_m(x)^{\varphi(p^{\nu_p})} \pmod p .$$

Wegen $\varphi(n) = \varphi(p^{\nu_p})\varphi(m)$ haben wir also nur noch den Fall $n = m$ zu betrachten, also den Fall $p \nmid n$ (denn f_p ist auch die Ordnung von p in $(\mathbb{Z}/m\mathbb{Z})^\times$). Dann gilt wegen $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p \nmid n$, dass $x^n - 1 \pmod p$ lauter verschiedene Nullstellen in einem Zerfällungskörper von $\mathbb{Z}/p\mathbb{Z}$ hat. Die Abbildung

$$\begin{aligned} \mu_n(\mathbb{Q}(\zeta_n)) &\longrightarrow \mu_n(k(\mathfrak{p})) \\ \zeta &\longmapsto \zeta \pmod{\mathfrak{p}} \end{aligned}$$

ist also ein Isomorphismus für jedes Primideal \mathfrak{p}/p von $\mathbb{Q}(\zeta_n)$. Der kleinste Erweiterungskörper von \mathbb{F}_p , der μ_n enthält, ist $\mathbb{F}_{p^{f_p}}$, denn $\mathbb{F}_{p^r}^\times$ ist zyklisch von der Ordnung $p^r - 1$. Da $k(\mathfrak{p})$ über \mathbb{F}_p von ζ_n erzeugt wird, folgt $k(\mathfrak{p}) \cong \mathbb{F}_{p^{f_p}}$ für alle \mathfrak{p}/p . Weiter zerfällt $\phi_n(x)$ als Teiler von $x^n - 1$ auch in lauter verschiedene irreduzible Faktoren modulo p , und die Behauptung folgt.

Corollar 6.9 Sei p eine ungerade Primzahl.

- (a) p ist genau dann verzweigt in $\mathbb{Q}(\zeta_n)$, wenn $p|n$.
- (b) p ist genau dann voll zerlegt in $\mathbb{Q}(\zeta_n)$, wenn $p \equiv 1 \pmod n$.

Beweis (a): $\varphi(p^{\nu_p}) \neq 1 \Leftrightarrow \nu_p \neq 0$.

(b) $\varphi(p^{\nu_p}) = 1 = f_p \Leftrightarrow p \equiv 1 \pmod n$.

Corollar 6.10 (a) 2 ist genau dann verzweigt in $\mathbb{Q}(\zeta_n)$, wenn $4|n$.

(b) 2 ist genau dann voll zerlegt in $\mathbb{Q}(\zeta_n)$, wenn $n \leq 2$.

Beweis (a): $\varphi(2^r) \neq 1 \Leftrightarrow r \geq 2$.

(b): $\varphi(2^{\nu_2}) = 1 = f_2 \Leftrightarrow n = 1$ oder 2 .

7 Zyklotomische Körper und die Fermat-Vermutung

Die Fermat-Vermutung lautet:

F_n : Sei $n > 2$. Die Gleichung

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

besitzt keine nicht-triviale ganzzahlige Lösung, d.h., keine Lösung mit $x, y, z \in \mathbb{Z}$ und $xyz \neq 0$.

Bemerkungen 7.1 (a) Es ist dasselbe, nach Lösungen in \mathbb{Q} zu fragen; umgekehrt genügt es, Lösungen in \mathbb{Z} mit $\text{ggT}(x, y, z) = 1$ zu betrachten.

(b) $F_n \Rightarrow F_{n \cdot m}$ für alle $m \geq 1$:

$$\begin{aligned} x^{n \cdot m} + y^{n \cdot m} &= z^{n \cdot m} \\ \Rightarrow (x^m)^n + (y^m)^n &= (z^m)^n. \end{aligned}$$

Also genügt es, F_4 und F_p für alle ungeraden Primzahlen p zu zeigen.

(c) F_4 wurde in Übungsaufgabe 2 gezeigt.

(d) Die Fermat-Vermutung wurde 1994 von Andrew Wiles und Richard Taylor bewiesen. Die Methoden kommen aus der Algebraischen Zahlentheorie, aber auch aus der Algebraischen Geometrie.

Klassischerweise unterscheidet man zwei Fälle der Fermat-Vermutung F_p , p ungerade Primzahl:

1. Fall Die Gleichung

$$x^p + y^p = z^p$$

hat keine Lösung $x, y, z \in \mathbb{Z}$ mit $p \nmid xyz$.

2. Fall Die Gleichung

$$x^p + y^p = z^p$$

hat keine Lösung mit $x, y, z \in \mathbb{Z}$, $p \nmid xy$, $p \mid z$.

Der 2. Fall ist im allgemeinen schwerer zu beweisen. Für den 1. Fall gilt

Satz 7.2 Der erste Fall der Fermat-Vermutung gilt für $p = 3$.

Beweis: Wir benutzen:

$$x \in \mathbb{Z}, x \not\equiv 0 \pmod{3} \Rightarrow x^3 \equiv \pm 1 \pmod{9}.$$

Denn $x \equiv 1 \pmod{3} \Rightarrow x = 1 + 3a$, $a \in \mathbb{Z} \Rightarrow x^3 = 1 + 3 \cdot 3a + 3 \cdot (3a)^2 + (3a)^3 \equiv 1 \pmod{9}$.
Ist nun $x \equiv -1 \pmod{3}$, so folgt $-x \equiv 1 \pmod{3}$ und $x^3 = -(-x)^3 \equiv -1 \pmod{9}$.

Für $x^3 + y^3 = z^3$, $3 \nmid xyz$ gilt also $x^3 + y^3 \equiv -2, 0$, oder $2 \pmod{9}$, aber $z^3 \equiv \pm 1 \pmod{9}$ – Widerspruch!

Bemerkungen 7.3 (a) Analog kann man den 1. Fall der Fermat-Vermutung für $p = 5$ zeigen; durch Kongruenzen modulo 25.

(b) Für $p = 7$, oder allgemeiner für jedes $p \equiv 1 \pmod{3}$ hat $x^p + y^p \equiv z^p \pmod{p^\nu}$ Lösungen mit $p \nmid xyz$ für jedes $\nu \geq 1$ (Übungsaufgabe).

Wir betrachten nun den 1. Fall der Fermat-Gleichung für eine beliebige ungerade Primzahl p . Seien $x, y, z \in \mathbb{Z}$ mit

$$(7.4.1) \quad x^p + y^p = z^p ,$$

$p \nmid xyz$, x, y und z paarweise teilerfremd. Sei $\zeta = \zeta_p$ eine primitive p -te Einheitswurzel. Aus der Gleichung

$$X^p - 1 = \prod_{i=0}^{p-1} (X - \zeta^i)$$

erhalten wir ($X = -\frac{x}{y}$ setzen und mit $-y^p$ multiplizieren)

$$(7.4.2) \quad x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y) .$$

Lemma 7.4 Die Ideale $(x + \zeta^i y)$, $i = 0, \dots, p-1$, sind paarweise teilerfremd in $\mathbb{Z}[\zeta]$.

Beweis: Sei \mathfrak{P} ein Primideal in $\mathbb{Z}[\zeta]$ mit $\mathfrak{P} \mid (x + \zeta^i y)$, $(x + \zeta^j y)$, wobei $i \neq j$. Dann gilt

$$\mathfrak{P} \mid (x - \zeta^j y) - (x - \zeta^i y) = (\zeta^i y - \zeta^j y) = \varepsilon(1 - \zeta) \cdot y$$

mit einer Einheit ε , vergleiche den Beweis von 6.5 (b). Weiter ist $(1 - \zeta)$ ein Primideal (siehe Bemerkung 6.6). Es folgt

$$\mathfrak{P} = (1 - \zeta) \text{ oder } \mathfrak{P} \mid y .$$

Ebenso gilt

$$\mathfrak{P} \mid \zeta^i(x - \zeta^j y) - \zeta^j(x - \zeta^i y) = \zeta^i x - \zeta^j x = \varepsilon \cdot (1 - \zeta)x ,$$

also

$$\mathfrak{P} = (1 - \zeta) \text{ oder } \mathfrak{P} \mid x .$$

Für $\mathfrak{P} \neq (1 - \zeta)$ folgt $\mathfrak{P} \mid x$ und $\mathfrak{P} \mid y$, was wegen der Teilfremdheit von x und y nicht sein kann. Also ist $\mathfrak{P} = (1 - \zeta)$, und liegt insbesondere über p (Bemerkung 6.6).

Es folgt

$$x + y \equiv x + \zeta^i y \equiv 0 \pmod{\mathfrak{P}} ,$$

also

$$x + y \equiv 0 \pmod{p}$$

wegen $\mathfrak{P} \cap \mathbb{Z} = (p)$. Es folgt

$$z \equiv z^p = x^p + y^p \equiv x + y \equiv 0 \pmod{p} ,$$

denn in $\mathbb{Z}/p\mathbb{Z}$ gilt $a^p = a$ für jedes a . Dies ist aber ein Widerspruch zu $p \nmid z$.

Lemma 7.5 (Sei wieder $\zeta = \zeta_p$) Ist $\mathbb{Z}[\zeta]$ faktoriell, so gilt

$$x + \zeta y = \varepsilon \cdot \alpha^p$$

mit $\alpha \in \mathbb{Z}[\zeta]$ und ε Einheit in $\mathbb{Z}[\zeta]$.

Beweis: Wir betrachten die Gleichung

$$(7.5.1) \quad \prod_{i=0}^{p-1} (x + \zeta^i y) = z^p,$$

die aus (7.4.1) und (7.4.2) folgt. Ist π ein Primelement in $\mathbb{Z}[\zeta]$ mit $\pi \mid x + \zeta y$, so folgt $\pi \mid z^p$, also auch $\pi \mid z$. Ist π^i die genaue Potenz, die z teilt, so ist π^{ip} die genaue Potenz, die z^p teilt, und damit auch die $x + \zeta^i y$ teilt, da π wegen Lemma 7.4 die $x + \zeta^i y$ für $i = \{0, \dots, p-1\} \setminus \{1\}$ nicht teilt.

Wir wollen dies nun zu einem Widerspruch führen. Hierfür brauchen wir einige Vorbereitungen.

Lemma 7.6 Sei $\alpha \in \mathbb{C}$ eine ganze algebraische Zahl. Haben alle Konjugierten von α den Absolutbetrag 1, so ist α eine Einheitswurzel.

Beweis: Das Minimalpolynom von α ist ganzzahlig und hat Grad $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, und seine Koeffizienten sind elementarsymmetrische Polynome in den n Konjugierten von α , sind also beschränkt durch eine Konstante, die nur von n abhängt. Dasselbe gilt für alle Potenzen α^ν von α , da $\alpha^\nu \in \mathbb{Q}(\alpha)$, so dass $[\mathbb{Q}(\alpha^\nu) : \mathbb{Q}] \leq n$ ist. Da die Konjugierten durch das charakteristische Polynom bestimmt sind und es nur endlich viele Möglichkeiten für diese Polynome gibt, ist die von α erzeugte zyklische Untergruppe $\{\alpha^\nu \mid \nu \in \mathbb{Z}\}$ endlich.

Lemma 7.7 Für $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$ ist

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

Beweis: Wegen $(m, n) = 1$ ist $\zeta_{mn} := \zeta_m \cdot \zeta_n$ primitive $m \cdot n$ -te Einheitswurzel und

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{m \cdot n}).$$

In dem kommutativen Diagramm

$$\begin{array}{ccccc} G = \text{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}) & \xrightarrow{\varphi} & \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \times & \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \downarrow \sim \chi & & \downarrow \sim \chi & & \downarrow \sim \chi \\ (\mathbb{Z}/mn\mathbb{Z})^\times & \xrightarrow{\sim} & (\mathbb{Z}/m\mathbb{Z})^\times & \times & (\mathbb{Z}/n\mathbb{Z})^\times \end{array}$$

sind die vertikalen Isomorphismen die zyklotomischen Charaktere (siehe 6.1) und die horizontalen Pfeile von den natürlichen Projektionen induziert.

Es folgt, dass φ ein Isomorphismus ist. Hieraus folgt, dass jedes Element in G sich schreiben lässt als $\sigma \cdot \tau$, wobei $\sigma|_{\mathbb{Q}(\zeta_n)} = 1$ und $\tau|_{\mathbb{Q}(\zeta_m)} = 1$. Daher ist $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})^G = \mathbb{Q}$.

Corollar 7.8 Die Einheitswurzeln in $\mathbb{Q}(\zeta_n)$ sind von der Form $\pm \zeta_n^a$, $a \geq 1$. (d.h., die Gruppe der Einheitswurzeln in $\mathbb{Q}(\zeta_n)$ ist $\mu_n \cdot \mu_2$).

Beweis: Sei η eine Einheitswurzel in $\mathbb{Q}(\zeta_n)$ mit maximaler Ordnung $m = \prod_p p^{\mu_p}$, und sei $n = \prod_p p^{\nu_p}$. Dann folgt $\mathbb{Q}(\zeta_{p^{\nu_p}}) = \mathbb{Q}(\zeta_{p^{\mu_p}})$ für alle p . Für ungerades p impliziert dies $\mu_p = \nu_p$, für gerades p geht dies nur für $\nu_p = \mu_p$ oder $\nu_p = 0, \mu_p = 2$.

Im Folgenden denken wir uns $\mathbb{Q}(\zeta_p)$ fest in \mathbb{C} eingebettet, etwa $\zeta_p = e^{\frac{2\pi i}{p}}$. Die komplexe Konjugation $z \mapsto \bar{z}$ bildet ζ_p auf ζ_p^{-1} ab, also $\mathbb{Q}(\zeta_p)$ in sich. Wir können sie also als ein Element $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ auffassen (es ist das eindeutige Element in $(\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung 2). Die folgenden Aussagen gelten für beliebiges ungerades p – es wird nicht benutzt, dass $\mathbb{Z}[\zeta_p]$ faktoriell ist.

Lemma 7.9 Sei ε eine Einheit in $\mathbb{Z}[\zeta_p]$.

(a) Es ist $\varepsilon/\bar{\varepsilon} = \zeta_p^a$ für ein $a \in \mathbb{Z}$.

(b) Es ist $\varepsilon = \varepsilon_0 \cdot \zeta_p^r$ für ein $r \in \mathbb{Z}$ und ε_0 mit $\bar{\varepsilon}_0 = \varepsilon_0$ (ε_0 **reelle** Einheit).

Beweis: (a) Die Zahl $\varepsilon/\bar{\varepsilon}$ ist ganz algebraisch und hat komplexen Absolutbetrag 1. Da $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ abelsch ist, vertauscht σ und daher die komplexe Konjugation mit allen $\tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Daher haben auch alle Konjugierten von $\varepsilon/\bar{\varepsilon}$ Betrag 1. (Es ist $\tau\varepsilon/\tau\bar{\varepsilon} = \tau\varepsilon/\overline{\tau\varepsilon}$) Nach 7.6 ist $\varepsilon/\bar{\varepsilon}$ eine Einheitswurzel, und nach 7.8 ist $\varepsilon/\bar{\varepsilon} = \pm \zeta_p^a, a \in \mathbb{Z}$.

Angenommen, $\varepsilon/\bar{\varepsilon} = -\zeta_p^a$ ($\zeta := \zeta_p$). Sei $\varepsilon = b_0 + b_1\zeta + \dots + b_{p-2}\zeta^{p-2}$ mit $b_i \in \mathbb{Z}$. Dann ist

$$\varepsilon \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{1 - \zeta}.$$

Ebenso ist

$$\begin{aligned} \bar{\varepsilon} &= b_0 + b_1\zeta^{-1} + \dots + b_{p-2}\zeta^{-p+2} \\ &\equiv b_0 + \dots + b_{p-2} \equiv \varepsilon \pmod{1 - \zeta} \\ &\equiv -\zeta^a \bar{\varepsilon} \equiv -\bar{\varepsilon} \pmod{1 - \zeta}. \end{aligned}$$

Es folgt

$$1 - \zeta \mid 2\bar{\varepsilon}.$$

Da $\bar{\varepsilon}$ Einheit ist, folgt $1 - \zeta \mid 2$, im Widerspruch dazu, dass $(1 - \zeta) \cap \mathbb{Z} = p > 2$.

(b): Da p ungerade ist, gibt es $r \in \mathbb{Z}$ mit $2r \equiv a \pmod{p}$. Dann gilt $\varepsilon = \zeta^{2r}\bar{\varepsilon}$ und damit

$$\zeta^{-r}\varepsilon = \zeta^r \cdot \bar{\varepsilon} = \overline{\zeta^{-r}\varepsilon},$$

also $\varepsilon = \zeta^r \cdot \varepsilon_0$ mit $\varepsilon_0 = \zeta^{-r}\varepsilon = \bar{\varepsilon}_0$.

Satz 7.10 Ist $p \geq 5$ prim und $\mathbb{Z}[\zeta_p]$ faktoriell, so gilt der erste Fall der Fermat-Vermutung für p .

Beweis: Sei wieder $\zeta = \zeta_p$. Ausgehend von Lemmas 7.5 und 7.9 haben wir eine Gleichung

$$x + \zeta y = \varepsilon \cdot \alpha^p = \zeta^r \cdot \varepsilon_0 \cdot \alpha^p$$

mit $r \geq 0$ und einer Einheit ε_0 mit $\bar{\varepsilon}_0 = \varepsilon_0$. Ist $\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$, so gilt wegen $(a + b)^p \equiv a^p + b^p \pmod{p}$ und $\zeta^p = 1$

$$\alpha^p \equiv a_0^p + a_1^p + \dots + a_{p-2}^p = a \pmod{p}$$

mit $a \in \mathbb{Z}$. Es folgt

$$x + \zeta y = \zeta^r \cdot \varepsilon_0 \cdot \alpha^p \equiv \zeta^r \cdot \varepsilon_0 \cdot a \pmod{p}$$

und andererseits

$$x + \zeta^{-1}y = \overline{x + \zeta y} \equiv \zeta^{-r} \varepsilon_0 \cdot a \pmod{p}.$$

Es folgt

$$x + \zeta y - \zeta^{2r}(x + \zeta^{-1}y) \equiv 0 \pmod{p},$$

also

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0 \pmod{p}.$$

1. Fall Sind $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ paarweise verschieden, so ist notwendigerweise $p \geq 5$, und $\{1, \zeta, \zeta^{2r}, \zeta^{2r-1}\}$ Teil einer \mathbb{Z} -Basis von $\mathbb{Z}[\zeta]$ (wegen $1 + \zeta + \dots + \zeta^{p-1} = 0$ ist jede Teilmenge von $\{1, \dots, \zeta^{p-1}\}$ von $p-2$ Elementen eine \mathbb{Z} -Basis von $\mathbb{Z}[\zeta]$). Dann folgt

$$x \equiv 0 \pmod{p} \text{ und } y \equiv 0 \pmod{p}.$$

im Widerspruch zu $p \nmid xy$.

2. Fall Ist $\zeta^{2r} = 1$, so folgt

$$\zeta y - \zeta^{p-1}y \equiv 0 \pmod{p},$$

also $y - \zeta^{p-2}y \equiv 0 \pmod{p}$, also

$$y \equiv 0 \pmod{p}$$

im Widerspruch zu $p \nmid xy$.

3. Fall Ist $\zeta^{2r} = \zeta$ ($\Leftrightarrow \zeta^{2r-1} = 1$), so ist

$$x - y + \zeta(x - y) \equiv 0 \pmod{p},$$

also $x - y \equiv 0 \pmod{p}$.

4. Fall Ist $\zeta^{2r-1} = \zeta$, so folgt

$$x - \zeta^2 x \equiv 0 \pmod{p}$$

also $x \equiv 0 \pmod{p}$ im Widerspruch zu $p \nmid xy$.

Es folgt also in jedem Fall $x \equiv y \pmod{p}$. Da wir mit $x^p + y^p = z^p$ auch die Gleichung

$$x^p + (-z)^p = (-y)^p$$

haben, folgt genauso

$$x \equiv -z \pmod{p}.$$

Außerdem gilt wegen $a^p \equiv a \pmod{p}$

$$x + y \equiv z \pmod{p}.$$

Zusammen folgt $-2z \equiv z \pmod{p}$, also

$$p \mid 3z.$$

Ist $p \geq 5$, so folgt $p \mid z$, im Widerspruch zur Annahme. Damit ist Satz 7.10 bewiesen.

Bemerkungen 7.11 (a) Nach Montgomery und Uchida ist $\mathbb{Z}[\zeta_p]$ genau für $p \leq 19$ faktoriell.

(b) Insbesondere ist $\mathbb{Z}[\zeta_{23}]$ nicht faktoriell (vergl. spätere Übungsaufgabe).

(c) Ein Dedekindring A ist genau dann faktoriell, wenn er Hauptidealring ist. Denn:

Jeder Hauptidealring ist faktoriell. Sei umgekehrt A faktoriell, und sei \mathfrak{a} ein Ideal in A . Dann gibt es ein Ideal $\mathfrak{b} \subseteq A$, so dass $\mathfrak{a}\mathfrak{b} = (a)$ ein Hauptideal ist ($\mathfrak{a} \cdot \mathfrak{a}^{-1} = A$; wähle $a \in A$ mit $\mathfrak{b} := a \cdot \mathfrak{a}^{-1} \subseteq A$). Ist $a = \prod_{i=1}^n \pi_i^{n_i}$, mit Primelementen π_i , so ist $(a) = \prod_{i=1}^n (\pi_i)^{n_i}$, wobei die Ideale (π_i) Primideale sind. Dann ist \mathfrak{a} nach der eindeutigen Primzerlegung Produkt von Primidealen, die Hauptideale sind, also selbst Hauptideal.

Dies heißt also, dass $\mathbb{Q}(\zeta_p)$ genau für alle $p \leq 19$ Klassenzahl 1 hat ($\Leftrightarrow \mathbb{Z}[\zeta_p]$ HIR).

Die Faktorialität von $\mathbb{Z}[\zeta_p]$ wurde nur in Lemma 7.5 gebraucht. Kummer bemerkte, dass eine schwächere Eigenschaft genügt:

Definition 7.12 Eine ungerade Primzahl p heißt **regulär**, wenn p nicht die Klassenzahl von $\mathbb{Q}(\zeta_p)$ teilt (und sonst irregulär).

Wir benutzen hier die später bewiesene Tatsache, dass die Klassengruppe $Cl_K = I_K/P_K$ von (gebrochenen) Idealen modulo Hauptidealen endlich ist; ihre Ordnung heißt die Klassenzahl von K .

Satz 7.13 (Kummer) Ist p eine reguläre Primzahl, so gilt der erste Fall der Fermat-Vermutung für p .

Beweis: Sei $\zeta = \zeta_p$. Aus der Gleichung (7.5.1):

$$\prod_{i=0}^{p-1} (x - \zeta^i y) = z^p$$

und der Teilerfremdheit der Faktoren links (Lemma 7.4) folgt zumindest die Idealgleichung

$$(x - \zeta y) = \mathfrak{a}^p$$

für ein Ideal $\mathfrak{a} \subseteq \mathbb{Z}[\zeta]$ (eindeutige Primzerlegung für die **Primideale**). Dies bedeutet, dass \mathfrak{a}^p ein Hauptideal ist, d.h., dass die Klasse von \mathfrak{a} in $Cl_{\mathbb{Q}(\zeta_p)}$ die Ordnung 1 oder p hat. Da die Ordnung von $Cl_{\mathbb{Q}(\zeta_p)}$ nach Voraussetzung prim zu p ist, muss \mathfrak{a} schon selbst ein Hauptideal sein, d.h., es gilt

$$x - \zeta y = \varepsilon \cdot \alpha^p$$

für eine Einheit ε und ein Element $\alpha \in \mathbb{Z}[\zeta_p]$. Ab hier geht der Beweis wie eben.

Bemerkungen 7.14 (a) Dieser Satz ist auf sehr viel mehr Primzahlen anwendbar; z.B. ist 23 eine reguläre Primzahl. Unter 100 sind nur 37, 59 und 67 irregulär.

(b) Experimentelle und heuristische Argumente zeigen, dass wahrscheinlich ungefähr $e^{-1/2} \approx 61$ % aller Primzahlen regulär sind und 39 % irregulär. Tatsächlich weiß man aber

bis heute nicht, ob es wirklich unendlich viele reguläre Primzahlen gibt. Dagegen hat Jensen 1915 bewiesen, dass es jedenfalls unendlich viele irreguläre Primzahlen gibt!

(c) Der Beweis der Fermat-Vermutung für $p = 3$ im zweiten Fall kann mit ähnlichen Methoden wie in Satz 7.10 durchgeführt werden (siehe unten).

(d) Durch Verfeinerung der Methoden kann man auch den zweiten Fall der Fermat-Vermutung für alle reguläre Primzahlen p zeigen (E. Kummer).

Satz 7.15 (Euler, Gauss) Die Fermat'sche Vermutung gilt für $p = 3$.

Beweis: Wegen 7.2 brauchen wir nur noch den zweiten Fall der Fermat'schen Vermutung zu behandeln. Seien $x, y, z_0 \in \mathbb{Z}$, paarweise teilerfremd, mit

$$x^3 + y^3 = z_0^3,$$

wobei $z_0 = 3^i z$, $3 \nmid z$, $i \geq 1$. Wir können annehmen, dass i minimal ist, und werden zeigen, dass es eine Lösung mit kleinerem i gibt. Sei $\zeta = \zeta_3$ eine primitive dritte Einheitswurzel. Dann ist nach (7.4.2)

$$(7.15.1) \quad (x+y)(x+\zeta y)(x+\zeta^2 y) = 3^{3i} z^3.$$

Wir benutzen, dass $\mathbb{Z}[\zeta]$ faktoriell und $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$ ist (Übungsaufgabe 20). Nach 6.5 ist $(3) = (1-\zeta)^2$, und $1-\zeta$ prim in $\mathbb{Z}[\zeta]$. Wir untersuchen die Teilbarkeit durch $1-\zeta$. Aus

$$x+y \equiv x^3+y^3 \equiv z_0^3 \equiv 0 \pmod{3}$$

folgt auch $x+y \equiv 0 \pmod{1-\zeta}$ in $\mathbb{Z}[\zeta]$. Daher gilt

$$x+\zeta y \equiv x+y \equiv 0 \pmod{1-\zeta},$$

entsprechend folgt $x+\zeta^2 y \equiv 0 \pmod{1-\zeta}$. Andererseits gilt $x+\zeta y, x+\zeta^2 y \not\equiv 0 \pmod{3}$, denn hieraus würde folgen $x \equiv y \equiv 0 \pmod{3}$ (da $1, \zeta$ Basis von $\mathbb{Z}[\zeta]$), im Widerspruch zur Annahme. Also werden $x+\zeta y$ und $x+\zeta^2 y$ genau zur 1. Potenz durch $1-\zeta$ geteilt, und nach Gleichung (7.15.1) wird $x+y$ genau durch $(1-\zeta)^{6i-2} = 3^{3i-1}$ geteilt.

Wie in Lemma 7.4 folgt nun, dass die Zahlen in $\mathbb{Z}[\zeta]$

$$\frac{x+y}{1-\zeta}, \frac{x-\zeta y}{1-\zeta}, \frac{x+\zeta^2 y}{1-\zeta}$$

paarweise teilerfremd sind. Schreiben wir nun

$$\frac{x+y}{1-\zeta} \cdot \frac{x+\zeta y}{1-\zeta} \cdot \frac{x+\zeta^2 y}{1-\zeta} = \frac{z_0}{1-\zeta}^3,$$

so folgt also, dass in den drei Faktoren links jeder Primfaktor in einer durch 3 teilbaren Potenz aufgeht, d.h., jeder Faktor ist assoziiert zu einer dritten Potenz. Zusammengefasst ist

$$1) \quad x+y = \varepsilon_0 \cdot 3^{3i-1} \cdot \alpha_0^3$$

$$2) \quad x+\zeta y = \varepsilon_1 \cdot (1-\zeta) \cdot \alpha_1^3$$

$$3) \quad x+\zeta^2 y = \varepsilon_2 \cdot (1-\zeta) \cdot \alpha_2^3$$

mit Einheiten ε_i und Zahlen α_i in $\mathbb{Z}[\zeta]$, $3 \nmid \alpha_0$.

a) Es ist

$$\varepsilon_1 \cdot (1-\zeta) \alpha_1^3 \stackrel{2)}{=} x+\zeta y \stackrel{1)}{=} x \cdot (1-\zeta) + \zeta \cdot \varepsilon_0 \cdot 3^{3i-1} \alpha_0^3$$

also

$$\begin{aligned} \varepsilon_1 \cdot \alpha_1^3 &= x + \zeta \cdot \varepsilon_0 \cdot 3^{3i-2} \cdot \frac{3}{1-\zeta} \cdot \alpha_0^3 \\ &\equiv x \pmod{3}. \end{aligned}$$

Da $\alpha_1^3 \equiv a_1 \pmod{3}$ für ein $a_1 \in \mathbb{Z}$ (s.o.), $3 \nmid a_1$, ist $\varepsilon_1 \equiv e_1 \pmod{3}$ für ein $e_1 \in \mathbb{Z}$ (schreibe $\varepsilon_1 = e_1 + \zeta e_2$). Wegen $\varepsilon_1 = \pm \zeta^a$ für ein $a \geq 0$ 7.9 (b) folgt $\varepsilon_1 = (\pm 1)$. Wegen $(\pm 1) = (\pm 1)^3$ können wir annehmen, dass $\varepsilon_1 = 1$. Ebenso ist o.E. $\varepsilon_2 = 1$.

b) Es ist ebenfalls $\varepsilon_0 = \pm \zeta^r$ mit $r \in \mathbb{Z}$. Wegen

$$1 = \frac{x+y}{x+y} = \frac{\varepsilon_0}{\bar{\varepsilon}_0} \cdot \frac{\alpha_0}{\bar{\alpha}_0}^3$$

ist $\varepsilon/\bar{\varepsilon}_0 = \zeta^r/\zeta^{-r} = \zeta^{2r}$ eine dritte Potenz; wegen $\zeta^3 = 1$ folgt $r \equiv 0 \pmod{3}$, also $\varepsilon_0 = \pm 1$, also auch o.E. $\varepsilon_0 = 1$.

c) Dann ist o.E. $\alpha_0 \in \mathbb{Z}$: sei $\alpha_0 = s + \zeta t$ mit $s, t \in \mathbb{Z}$, dann ist nämlich wegen 1) und $\varepsilon_0 = 1$

$$\begin{aligned}\alpha_0^3 &= s^3 + 3s^2t\zeta + 3st^2\zeta^2 + t^3 \in \mathbb{Z} \\ &= (s^2 + t^3 - 3st^2) + (3st^2t - 3st^2)\zeta \in \mathbb{Z},\end{aligned}$$

also $3st(s-t) = 0$. Für $s = 0$ können wir $\alpha_0 = t$ setzen, für $t = 0$ ist bereits $\alpha_0 \in \mathbb{Z}$, und für $s = t$ ist $\alpha_0 = s \cdot (1 + \zeta) = -s \cdot \zeta^2$, also o.E. $\alpha_0 = -s$. Dabei gilt immer $3 \nmid \alpha_0$.

d) Sei $\alpha_1 = a + b\zeta$ mit $a, b \in \mathbb{Z}$. Dann ist

$$\begin{aligned}x + \zeta y &= (1 - \zeta)\alpha_1^3 \\ &= (1 - \zeta)(a^3 + 3a^2b\zeta + 3ab^2\zeta^2 + b^3) \\ &= a^3 + 3a^2b\zeta - 3ab^2 - 3ab^2\zeta + b^3 \\ &\quad - a^3\zeta + 3a^2b + 3a^2b\zeta - 3ab^2 - b^2\zeta \\ &= (a^3 + 3a^2b - 6ab^2 + b^3) \\ &\quad + (-a^3 + 6a^2b - 3ab^2 - b^3)\zeta.\end{aligned}$$

Es folgt $a \cdot b \neq 0$ und $\text{ggT}(a, b) = 1$, denn sonst wären x und y nicht teilerfremd.

e) Nach der obigen Rechnung ist

$$x + y = 9ab(a - b).$$

f) Wegen $x + y = 3^{3i-1} \cdot \alpha_0^3$ mit $\alpha_0 \in \mathbb{Z}$ erhalten wir die Gleichung in \mathbb{Z}

$$ab(a - b) = (3^{i-1})^3 \alpha_0^3.$$

Da a, b und $a - b$ paarweise teilerfremd sind, sind a, b und $a - b$ jeweils dritte Potenzen in \mathbb{Z} , und zwar ist

$$\{a, b, a - b\} = \{a_1^3, b_1^3, (3^{i-1} \cdot c_1)^3\}$$

mit a_1, b_1, c_1 paarweise teilerfremd und $3 \nmid c_1$. Wegen $a + (-b) = a - b$, $a + (b - a) = b$ und $b + (a - b) = a$ ergibt dies jedenfalls eine Gleichung

$$(\pm a_1)^3 + (\pm b_1^3) = (3^{i-1} c_1)^3$$

mit a_1, b_1, c_1 paarweise teilerfremd und $3 \nmid c_1$, im Widerspruch zur Minimalität von i (bzw. für $i = 1$, zur Unlösbarkeit im 1. Fall).

8 Primzerlegung und Galoistheorie

Sei wieder allgemein A ein Dedekindring mit Quotientenkörper K , L/K eine endliche Erweiterung und B der ganze Abschluss von A in L .

Nun sei aber L/K galoissch mit Galoisgruppe G . Dann operiert G auf B (für jedes $b \in B$ und jedes $\sigma \in G$ ist σb wieder ganz über A), und für ein Primideal \mathfrak{P} von B , welches über dem Primideal \mathfrak{p} von A liegt ($\mathfrak{P} \cap A = \mathfrak{p}$) und $\sigma \in G$ ist $\sigma\mathfrak{P}$ wieder ein Primideal über \mathfrak{p} . Denn der von σ induzierte Isomorphismus

$$B/\mathfrak{P} \xrightarrow{\sigma} B/\sigma\mathfrak{P}$$

zeigt, dass $\sigma\mathfrak{P}$ ein Primideal ist, und weiter gilt $\sigma\mathfrak{P} \cap A = \sigma(\mathfrak{P} \cap A) = \mathfrak{p}$. Wir nennen $\sigma\mathfrak{P}$ ein zu \mathfrak{P} konjugiertes Primideal.

Satz 8.1 Für jedes Primideal $\mathfrak{p} \subseteq A$ operiert die Galoisgruppe G transitiv auf der Menge der über \mathfrak{p} gelegenen Primideale \mathfrak{P} von B , d.h., für $\mathfrak{P}, \mathfrak{P}' | \mathfrak{p}$ gibt es ein $\sigma \in G$ mit $\mathfrak{P}' = \sigma\mathfrak{P}$.

Beweis: Seien \mathfrak{P} und \mathfrak{P}' Primideale über \mathfrak{p} . Angenommen, $\sigma\mathfrak{P} \neq \mathfrak{P}'$ für alle $\sigma \in G$. Nach dem chinesischen Restsatz gibt es dann ein $b \in B$ mit

$$b \equiv 0 \pmod{\mathfrak{P}'}, \quad b \equiv 1 \pmod{\sigma\mathfrak{P}} \quad \text{für alle } \sigma \in G.$$

Dann gilt $N_{L/K}(b) = \prod_{\sigma \in G} \sigma b \in \mathfrak{P}' \cap A = \mathfrak{p}$. Andererseits ist $x \notin \sigma\mathfrak{P}$ für alle $\sigma \in G$, also $\sigma x \notin \mathfrak{P}$ für alle $\sigma \in G$, und daher $\prod_{\sigma \in G} \sigma x \notin \mathfrak{P} \cap A = \mathfrak{p}$ – Widerspruch!

Definition 8.2 Sei \mathfrak{P} ein Primideal von B . Dann heißt

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

die **Zerlegungsgruppe** von \mathfrak{P} über K (oder in G) und der zugehörige Fixkörper

$$Z_{\mathfrak{P}} := L^{G_{\mathfrak{P}}} = \{\beta \in L \mid \sigma\beta = \beta \quad \forall \sigma \in G_{\mathfrak{P}}\}$$

der **Zerlegungskörper** von \mathfrak{P} über K (oder in L/K).

Liegt \mathfrak{P} über \mathfrak{p} , so ist $G_{\mathfrak{P}}$ gerade die Standgruppe von \mathfrak{P} unter der Operation von G auf der Menge

$$\{\mathfrak{P}' \mid \mathfrak{P}' \subseteq B \text{ Primideal mit } \mathfrak{P}' \cap A = \mathfrak{p}\}$$

aller Primideale über \mathfrak{p} . Wegen der Transitivität der Operation ($\{\mathfrak{P}' \mid \mathfrak{p}\}$ ist ein Orbit unter G) haben wir eine Bijektion

$$\begin{array}{ccc} G/G_{\mathfrak{P}} & \xrightarrow{\sim} & \{\mathfrak{P}' \mid \mathfrak{p}\} \\ \bar{\sigma} & \longmapsto & \sigma\mathfrak{P}. \end{array}$$

Hieraus erhalten wir offenbar

Proposition 8.3 (a) Der Index $(G : G_{\mathfrak{P}})$ ist die Anzahl der Primideale $\mathfrak{P} \mid \mathfrak{p}$, also gleich der Zahl r in der Primzerlegung

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

von \mathfrak{p} in L/K . Insbesondere gilt:

(b) $G_{\mathfrak{P}} = \{1\} \Leftrightarrow Z_{\mathfrak{P}} = L \Leftrightarrow \mathfrak{p}$ ist voll zerlegt in L/K .

(c) $G_{\mathfrak{P}} = G \Leftrightarrow Z_{\mathfrak{P}} = K \Leftrightarrow \mathfrak{p}$ ist unzerlegt in L/K .

(d) Sei $\sigma \in G$. Dann ist die Zerlegungsgruppe von $\sigma\mathfrak{P}$ gerade

$$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}.$$

Corollar 8.4. Sind f_1, \dots, f_r die Trägheitsgrade und e_1, \dots, e_r die Verzweigungsindizes in der Primzerlegung

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

so ist $e_1 = \dots = e_r$ und $f_1 = \dots = f_r$. Insbesondere gilt mit $e = e(\mathfrak{P}_i/\mathfrak{p})$ und $f = f(\mathfrak{P}_i/\mathfrak{p})$

$$r \cdot e \cdot f = n := [L : K],$$

wobei

$$r = (G : G_{\mathfrak{P}}) .$$

Beweis: Für $\mathfrak{P}/\mathfrak{p}$ und $\sigma \in G$ haben wir einen $k(\mathfrak{p})$ -Isomorphismus

$$B/\mathfrak{P} \xrightarrow{\sigma} B/\sigma\mathfrak{P} .$$

Dies liefert die Gleichheit der f_i . Weiter gilt

$$\mathfrak{P}' \mid \mathfrak{p}B \Leftrightarrow (\sigma\mathfrak{P})' = \sigma\mathfrak{P}' \mid \sigma\mathfrak{p}B = \mathfrak{p}B .$$

Dies zeigt die Gleichheit der e_i . Der Rest ist klar.

Der Zerlegungskörper hat dabei die folgende Bedeutung für die Primzerlegung:

Satz 8.5 Sei $\mathfrak{P}_Z := \mathfrak{P} \cap Z_{\mathfrak{P}}$ das unter \mathfrak{P} gelegene Primideal von $Z_{\mathfrak{P}}$. Dann gilt:

- (a) \mathfrak{P}_Z ist unzerlegt in $L/Z_{\mathfrak{P}}$.
- (b) \mathfrak{P} hat in $L/Z_{\mathfrak{P}}$ den Verzweigungsindex $e = e(\mathfrak{P}/\mathfrak{p})$ und den Trägheitsgrad $f = f(\mathfrak{P}/\mathfrak{p})$.
- (c) Verzweigungsindex und Trägheitsgrad von \mathfrak{P}_Z in $Z_{\mathfrak{P}}/K$ sind beide 1.

Bild:

$$\begin{array}{ccc}
 \mathfrak{P} & L & \mathfrak{P} \\
 \left| \begin{array}{c} e, f \\ \\ e, f \end{array} \right. & \left| \begin{array}{c} ef \\ \\ r \end{array} \right. & \left| \begin{array}{c} e, f \\ \\ e=f=1 \end{array} \right. \\
 \mathfrak{p} & Z_{\mathfrak{P}} & \mathfrak{P}_Z \\
 & \left| \begin{array}{c} r \\ \\ \end{array} \right. & \\
 & K & \mathfrak{p}
 \end{array}$$

Beweis: (a) Wegen $\text{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$ ist die Menge der über \mathfrak{P}_Z liegenden Primideale

$$\{\mathfrak{P}'/\mathfrak{P}_Z\} = G_{\mathfrak{P}} \cdot \mathfrak{P} = \{\mathfrak{P}\} .$$

(b) Es ist

$$n = r \cdot e \cdot f$$

mit $n = (G : 1) = [L : K]$ und $r = (G : G_{\mathfrak{P}}) = [Z_{\mathfrak{P}} : K]$. Es folgt $ef = (G_{\mathfrak{P}} : 1) = [L : Z_{\mathfrak{P}}]$. Sei e' (bzw. f') der Verzweigungsindex (bzw. Trägheitsgrad) von \mathfrak{P} in $L/Z_{\mathfrak{P}}$. Dann gilt $e' \mid e$ und $f' \mid f$; andererseits ist $[L : Z_{\mathfrak{P}}] = e'f'$. Also gilt $e' = e$ und $f' = f$. Hieraus folgt auch (c).

Wir notieren noch:

Lemma 8.6 Sei L' ein Zwischenkörper von L/K , $B' = B \cap L'$ (= ganzer Abschluss von A in L'), $\mathfrak{P}' = \mathfrak{P} \cap L'$ und $\mathfrak{p} = \mathfrak{P} \cap K$.

(a) Für die Zerlegungsgruppen $G_{\mathfrak{P}} \subseteq G = \text{Gal}(L/K)$ und $G'_{\mathfrak{P}} \subseteq G' = \text{Gal}(L/L')$ gilt

$$G'_{\mathfrak{P}} = G_{\mathfrak{P}} \cap G' .$$

Wir hatten die Formel für die Primzerlegung von $\mathfrak{p} \subseteq A$

$$n = ref$$

für eine Galoiserweiterung L/K , und

$$r = (G : G_{\mathfrak{P}}),$$

wobei $\mathfrak{P} \subseteq B$ ein beliebiges Primideal über \mathfrak{p} ist. Der Verzweigungsindex $e = e(\mathfrak{P}/\mathfrak{p})$ und der Trägheitsgrad $f = f(\mathfrak{P}/\mathfrak{p})$ haben auch galoistheoretische Interpretationen:

Wir bemerken dazu, dass jedes $\sigma \in G_{\mathfrak{P}}$ wegen $\sigma B \subseteq B$ und $\sigma \mathfrak{P} \subseteq \mathfrak{P}$ einen Automorphismus

$$\begin{aligned} \bar{\sigma} : k(\mathfrak{P}) = B/\mathfrak{P} &\longrightarrow B/\mathfrak{P} = k(\mathfrak{P}) \\ b \bmod \mathfrak{P} &\longmapsto \sigma b \bmod \mathfrak{P} \end{aligned}$$

induziert, der natürlich $k(\mathfrak{p}) = A/\mathfrak{p} \subseteq k(\mathfrak{P})$ elementweise festläßt.

Satz 8.8 Die Erweiterung $k(\mathfrak{P})/k(\mathfrak{p})$ ist normal. Ist $k(\mathfrak{P})/k(\mathfrak{p})$ separabel (dies gilt z.B. falls $k(\mathfrak{p})$ endlich ist), so ist der Homomorphismus

$$\begin{aligned} G_{\mathfrak{P}} &\rightarrow Gal(k(\mathfrak{P})/k(\mathfrak{p})) \\ \sigma &\mapsto \bar{\sigma} : (b \bmod \mathfrak{P} \mapsto \sigma b \bmod \mathfrak{P}) \end{aligned}$$

surjektiv.

Beweis: Für $\tilde{\beta} \in k(\mathfrak{P})$ wähle $\beta \in B$ mit $\tilde{\beta} = \beta \bmod \mathfrak{P}$. Sei $p(x)$ das Minimalpolynom von β über K und $q(x)$ das Minimalpolynom von $\tilde{\beta}$ über $k(\mathfrak{p})$. Für $\bar{p}(x) := p(x) \bmod \mathfrak{p}$ gilt dann $\tilde{p}(\beta) = 0$, also $q(x) \mid p(x)$. Nach Voraussetzung zerfällt $p(x)$ in Linearfaktoren über L , also gilt dies auch für $\bar{p}(x)$ über $k(\mathfrak{P})$, und für den Teiler $q(x)$. Daher ist $k(\mathfrak{P})/k(\mathfrak{p})$ normal.

Für die zweite Behauptung können wir die Erweiterung L/K durch $L/Z_{\mathfrak{P}}$ ersetzen, da diese Erweiterungen dieselben Zerlegungsgruppen für \mathfrak{P} haben und außerdem für $\mathfrak{P}_0 = \mathfrak{P} \cap Z_{\mathfrak{P}}$ gilt $k(\mathfrak{P}_0) = k(\mathfrak{p})$.

Es ist also o.E. $G = G_{\mathfrak{P}}$. Sei $\tilde{\beta}$ ein primitives Element für $k(\mathfrak{P})/k(\mathfrak{p})$. Dann gilt mit den Bezeichnungen von oben: Ist $\tilde{\sigma} \in Gal(k(\mathfrak{P})/k(\mathfrak{p}))$, so ist $\tilde{\sigma}\tilde{\beta}$ Nullstelle von $q(x)$, also auch von $\bar{p}(x)$. Es gibt also eine Nullstelle β' von $p(x)$ in L mit $\tilde{\sigma}\tilde{\beta} = \beta' \bmod \mathfrak{P}$. Da β' ein Konjugiertes von β ist, gibt es ein $\sigma \in G (= G_{\mathfrak{P}})$ mit $\beta' = \sigma\beta$. Es gilt also $\sigma\beta \equiv \tilde{\sigma}\tilde{\beta} \bmod \mathfrak{P}$, und da $\tilde{\beta}$ ein primitives Element von $k(\mathfrak{P})/k(\mathfrak{p})$ ist, folgt, dass $\tilde{\sigma}$ das Bild von σ unter

$$G_{\mathfrak{P}} \rightarrow Gal(k(\mathfrak{P})/k(\mathfrak{p}))$$

ist.

Definition 8.9 Für ein Primideal $\mathfrak{P}/\mathfrak{p}$ von L heißt

$$I_{\mathfrak{P}} := \ker(G_{\mathfrak{P}} \rightarrow Gal(k(\mathfrak{P})/k(\mathfrak{p})))$$

die **Trägheitsgruppe** von \mathfrak{P} über K (oder in G) und der Fixkörper

$$T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}} = \{\beta \in L \mid \sigma\beta = \beta \ \forall \sigma \in I_{\mathfrak{P}}\}$$

der **Trägheitskörper** von \mathfrak{P} über K (oder in L/K).

Wir haben also ein Galoisdiagramm

$$\begin{array}{ccc}
 L & & 1 \\
 | & & | \\
 T_{\mathfrak{P}} & & I_{\mathfrak{P}} \\
 | & & | \\
 Z_{\mathfrak{P}} & & G_{\mathfrak{P}} \\
 | & & | \\
 K & & G
 \end{array}
 \quad
 \begin{array}{l}
 \\
 \\
 \cong \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \\
 \\
 \\
 \\
 \end{array}$$

und eine exakte Sequenz

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \longrightarrow 1 .$$

Erinnerung: Eine Sequenz $G_1 \xrightarrow{\alpha} G_2 \xrightarrow{\beta} G_3$ von Gruppen und Gruppenhomomorphismen heißt exakt, wenn $\text{im}(\alpha) = \ker(\beta)$. Eine Sequenz

$$1 \rightarrow G_1 \xrightarrow{\alpha} G_2 \xrightarrow{\beta} G_3 \rightarrow 1$$

heißt exakt, wenn sie an allen Stellen exakt ist. Das bedeutet α ist injektiv, β ist surjektiv und $\text{im}(\alpha) = \ker(\beta)$, so dass sich G_1 mit einem Normalteiler von G_2 identifiziert und der Homomorphiesatz einen Isomorphismus $G_2/G_1 \xrightarrow{\sim} G_3$ induziert.

Satz 8.10 Sei $k(\mathfrak{P})/k(\mathfrak{p})$ separabel. Dann gilt:

(a) Die Erweiterung $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ ist normal, und es ist

$$\text{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) .$$

(b) Es ist

$$(G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f \quad (= f(\mathfrak{P}/\mathfrak{p}))$$

und

$$(I_{\mathfrak{P}} : 1) = [L : T_{\mathfrak{P}}] = e \quad (= e(\mathfrak{P}/\mathfrak{p})) .$$

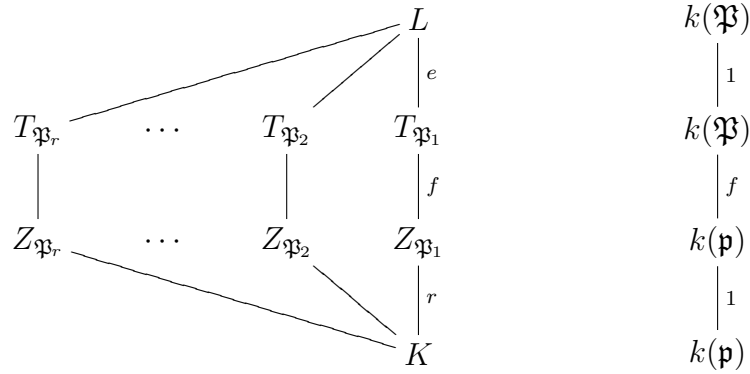
(c) Für die Primideale $\mathfrak{P}_T = \mathfrak{P} \cap T_{\mathfrak{P}}$ und $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ gilt dabei

$$\begin{array}{l}
 e(\mathfrak{P}/\mathfrak{P}_T) = e, \quad f(\mathfrak{P}/\mathfrak{P}_T) = 1 \\
 e(\mathfrak{P}_T/\mathfrak{P}_Z) = 1, \quad f(\mathfrak{P}_T/\mathfrak{P}_Z) = f .
 \end{array}$$

(d)

$$\begin{array}{l}
 I_{\mathfrak{P}} = \{1\} \Leftrightarrow L = T_{\mathfrak{P}} \Leftrightarrow \mathfrak{P} \text{ ist unverzweigt in } L/K \\
 \Leftrightarrow \mathfrak{p} \text{ ist unverzweigt in } L/K .
 \end{array}$$

Bild:



Beweis: (a) ist klar nach Galoistheorie, da $I_{\mathfrak{P}} \trianglelefteq G_{\mathfrak{P}}$ Normalteiler ist, mit

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) .$$

(b) Die erste Aussage ist klar nach (a); die zweite folgt wegen $[L : Z_{\mathfrak{P}}] = ef$.

(c) Wir zeigen zunächst:

Behauptung $k(\mathfrak{P}_T) = k(\mathfrak{P})$.

Beweis: Da $I_{\mathfrak{P}}$ auch die Trägheitsgruppe von \mathfrak{P} über $T_{\mathfrak{P}}$ ist, so folgt mit 8.8

$$\{1\} = \text{Gal}(L/T_{\mathfrak{P}})/I_{\mathfrak{P}} \xrightarrow{\sim} \text{Gal}(k(\mathfrak{P})/k(\mathfrak{P}_T)) ,$$

also $k(\mathfrak{P}) = k(\mathfrak{P}_T)$. Es folgt

$$f(\mathfrak{P}/\mathfrak{P}_T) = 1 \quad f(\mathfrak{P}_T/\mathfrak{P}_Z) = f .$$

Die Verzweigungsindizes berechnen sich nun aus der fundamentalen Gleichung und (a).

(d) ist nun klar, zusammen mit $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p})$ für $\mathfrak{P}, \mathfrak{P}'/\mathfrak{p}$ (da L/K galoissch ist).

Analog zu 8.6 haben wir

Lemma 8.11 Sei L' ein Zwischenkörper von L/K und $\mathfrak{P}' = \mathfrak{P} \cap L'$. Dann gilt

(a) Für die Trägheitsgruppen $I_{\mathfrak{P}} \subseteq G = \text{Gal}(L/K)$ und $I'_{\mathfrak{P}} \subseteq G' = \text{Gal}(L/L')$ gilt

$$I'_{\mathfrak{P}} = I_{\mathfrak{P}} \cap G' .$$

(b) $I_{\mathfrak{P}} \subseteq \text{Gal}(L/L') \Leftrightarrow L' \subseteq T_{\mathfrak{P}} \Leftrightarrow e(\mathfrak{P}'/\mathfrak{p}) = 1$.

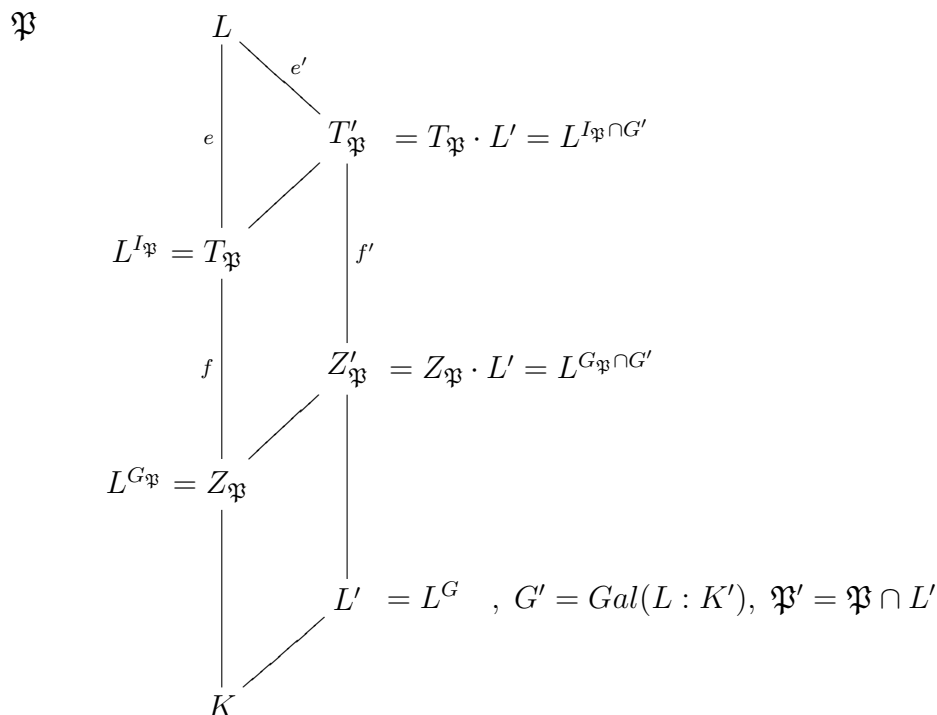
(c) Ist L'/K galoissch, so gilt für die Trägheitsgruppe $I_{\mathfrak{P}'}$ von \mathfrak{P}' in $\overline{G} = \text{Gal}(L'/K)$

$$I_{\mathfrak{P}'} = \text{Bild von } I_{\mathfrak{P}} \text{ in } \overline{G} .$$

Beweis: (a) Wir haben das kommutative Diagramm

$$\begin{array}{ccc} G'_{\mathfrak{P}} = G_{\mathfrak{P}} \cap \text{Gal}(L/L') & \longrightarrow & \text{Gal}(k(\mathfrak{P})/k(\mathfrak{P}')) \\ \downarrow & & \downarrow \\ G_{\mathfrak{P}} & \longrightarrow & \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \end{array}$$

(b) Die erste Äquivalenz gilt nach Galoistheorie. Weiter haben wir das Körperdiagramm



Hierbei haben die Körpererweiterungen die angegebenen Körpergrade, mit $e = e(\mathfrak{P}/\mathfrak{p})$ und $e' = e(\mathfrak{P}/\mathfrak{P}')$ (nach 8.10 (c)).

Es folgt

$$\begin{aligned}
 I_{\mathfrak{P}} \subseteq G' = \text{Gal}(L/L') &\Leftrightarrow I'_{\mathfrak{P}} = I_{\mathfrak{P}} \cap G' = I_{\mathfrak{P}} \\
 \Leftrightarrow T_{\mathfrak{P}} = T'_{\mathfrak{P}} &\stackrel{(1)}{\Leftrightarrow} e = e(\mathfrak{P}/\mathfrak{p}) = e' = e(\mathfrak{P}/\mathfrak{P}') \stackrel{(2)}{\Leftrightarrow} e(\mathfrak{P}'/\mathfrak{p}) = 1.
 \end{aligned}$$

Die Äquivalenz (1) gilt, da immer $T_{\mathfrak{P}} \subseteq T'_{\mathfrak{P}}$, und die Äquivalenz (2) gilt wegen $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}')e(\mathfrak{P}'/\mathfrak{p})$.

(c) Wir haben das kommutative Diagramm mit exakten Zeilen und Spalten

$$\begin{array}{ccccc}
 & G'_{\mathfrak{P}} & \twoheadrightarrow & \text{Gal}(k(\mathfrak{P})/k(\mathfrak{P}')) & \\
 & \downarrow & & \downarrow & \\
 I_{\mathfrak{P}} \subset & G_{\mathfrak{P}} & \twoheadrightarrow & \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) & \\
 \downarrow \alpha & \downarrow \beta \text{ 8.6} & & \downarrow & \\
 I_{\mathfrak{P}'} \subset & G_{\mathfrak{P}'} & \twoheadrightarrow & \text{Gal}(k(\mathfrak{P}')/k(\mathfrak{p})) &
 \end{array}$$

Es folgt durch einfache ‘Diagrammjagd’, dass α wohldefiniert und surjektiv ist. (Ist $x \in I'_{\mathfrak{P}}$, so hat x Bild 1 in $\text{Gal}(k(\mathfrak{P}')/k(\mathfrak{p}))$). Hieraus folgt, dass $\beta(x)$ in $I_{\mathfrak{P}'}$ liegt, so dass $\alpha = \beta \mid I'_{\mathfrak{P}}$ Bild in $I_{\mathfrak{P}'}$ hat. Surjektivität von α : Sei $y \in I_{\mathfrak{P}'}$ und $z \in G_{\mathfrak{P}}$ mit $\beta(z) = y$ (β ist nach 8.6 (c) surjektiv). Sei t das Bild von z in $\text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Da t Bild 1 in $\text{Gal}(k(\mathfrak{P}')/k(\mathfrak{p}))$ hat (wegen $y \in I_{\mathfrak{P}'}$) liegt t in $\text{Gal}(k(\mathfrak{P})/k(\mathfrak{P}'))$ und hat ein Urbild w in $G'_{\mathfrak{P}}$. Dann hat zw^{-1} Bild 1 in $\text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, liegt also in $I_{\mathfrak{P}}$, und wegen $\beta(w) = 1$ gilt $\beta(zw^{-1}) = \beta(z) = y$. Also ist $\alpha(zw^{-1}) = y$.)

Bemerkung 8.12 Analog zu Bemerkung 8.7 folgt, dass für ein Primideal \mathfrak{p} in K die folgenden Bedingungen äquivalent sind

- (i) \mathfrak{p} ist unverzweigt in L'/K .
- (ii) $I_{\mathfrak{P}} \subseteq G' = \text{Gal}(L/L')$ für alle $\mathfrak{P}/\mathfrak{p}$ in L .

Im Fall von Zahlkörpern sind die Restklassenkörper $k(\mathfrak{p}), k(\mathfrak{P}) \dots$ endlich und die dort auftretenden Galoisgruppen sehr einfach und gut zu beschreiben:

Erinnerung 8.13 (a) Sei F ein endlicher Körper. Dann ist $\text{char } F = p > 0$ und F ist eine endliche Erweiterung des Körpers $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ mit p Elementen. Ist $n = [F : \mathbb{F}_p]$, so hat F p^n Elemente.

(b) Sei p eine Primzahl und $n \in \mathbb{N}$. Dann gibt es bis auf Isomorphie genau einen Körper \mathbb{F}_{p^n} mit p^n Elementen. \mathbb{F}_{p^n} ist der Zerfällungskörper des Polynoms $X^{p^n} - X$ über \mathbb{F}_p und besteht aus allen Nullstellen dieses Polynoms.

(c) $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist galoisch mit zyklischer Galoisgruppe der Ordnung n , die erzeugt wird vom (absoluten) Frobenius-Automorphismus

$$\begin{aligned} Fr_p : \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ a &\longmapsto a^p . \end{aligned}$$

(d) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$. In diesem Fall ist $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ zyklisch vom Grad $d := \frac{n}{m}$ und $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ erzeugt vom **relativen Frobenius-Automorphismus** von $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$

$$\begin{aligned} Fr_{p^m} = (Fr_p)^m : \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ a &\longmapsto a^{p^m} . \end{aligned}$$

Dies wird in der Algebra bewiesen (siehe z.B. Algebra I §14).

Beweis: (a) Der Primkörper ist endlich und also von der Form \mathbb{F}_p mit einer Primzahl p , und der \mathbb{F}_p -Vektorraum \mathbb{F}_p^n hat p^n Elemente.

(b) Für $f(x) = X^{p^n} - X \in \mathbb{F}_p[x]$ ist $f'(x) = -1$, also ist f separabel. Sei F der Zerfällungskörper von $f(x)$. Sind a, b Nullstellen von $f(x)$ in F , so auch $a \pm b$ und $a \cdot b$; die Menge N der Nullstellen bildet also einen endlichen integren Unterring von F , ist also ein Körper. Damit ist $F = N$ und besteht aus p^n Elementen. Ist umgekehrt F ein Körper mit p^n Elementen, so ist F^\times zyklisch von der Ordnung $p^n - 1$. Für $q \in F^\times$ gilt also $a^{p^n-1} = 1$ (s. 7.1); es ist also

$$(*) \quad a^{p^n} - a = 0$$

für alle $a \in F$. Damit enthält F den Zerfällungskörper von $f(x)$, und ist ihm gleich aus Gradgründen.

(c) Wir wissen bereits, dass $\mathbb{F}_{p^n}/\mathbb{F}_p$ galoissch ist. Fr_p ist ein Ringhomomorphismus, also injektiv, da \mathbb{F}_{p^n} ein Körper ist, also surjektiv aus Mächtigkeitsgründen. Weil $a^p = a$ für $a \in \mathbb{F}_p$ "kleiner Fermat", aber siehe auch (b), ist Fr_p die Identität auf \mathbb{F}_p . Wegen $(Fr_p)^n(x) = x^{p^n} = x$ für alle $x \in \mathbb{F}_{p^n}$ ist die Ordnung von $Fr_p \leq n$. Wäre $Fr_p^m = \text{id}$ für $m < n$, so wäre $x^{p^m} = x$ für alle $x \in \mathbb{F}_{p^n}$, also \mathbb{F}_{p^n} in \mathbb{F}_{p^m} enthalten – Widerspruch zu $m < n$. Somit hat $Fr_p \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ die Ordnung $n = |\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| : 1$, erzeugt also diese Gruppe.

(d) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Rightarrow m = [\mathbb{F}_{p^m} : \mathbb{F}_p] \mid [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Gilt umgekehrt $m|n$, so teilt das Polynom $X^{p^m} - X$ das Polynom $X^{p^n} - X$ (der Quotient ist $(X^{p^m})^{p^{n-m}} + (X^{p^m})^{(p^{n-m}-1)} + \dots + X^{p^m} + 1$). Es gilt also $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Die zweite Aussage folgt wie in (c) aus $\mathbb{F}_{p^m} \subseteq (\mathbb{F}_{p^n})^{\langle Fr_{p^m} \rangle}$ und $\text{ord}(Fr_{p^m}) = \frac{n}{m} = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$.

Sei nun L/K eine Galoiserweiterung von **Zahlkörpern**, mit Galoisgruppe G .

Definition 8.14 Für jedes Primideal \mathfrak{P} in L , welches unverzweigt über K ist, definiere den Frobenius-Automorphismus $Fr_{\mathfrak{P}} \in G$ als das eindeutig bestimmte Element in der Zerlegungsgruppe $G_{\mathfrak{P}}$, welches unter dem Isomorphismus

$$G_{\mathfrak{P}} \xrightarrow{\sim} Gal(k(\mathfrak{P})/k(\mathfrak{p}))$$

($I_{\mathfrak{P}}$ ist trivial nach 8.10 (d)) auf den relativen Frobenius-Automorphismus von $k(\mathfrak{P})/k(\mathfrak{p})$ abgebildet wird, $\mathfrak{p} = \mathfrak{P} \cap K$ das unter \mathfrak{P} liegende Primideal in K .

Definition 8.15 Für einen Zahlkörper K und ein Primideal \mathfrak{p} in K definiere seine **Norm** durch

$$N(\mathfrak{p}) := |k(\mathfrak{p})|$$

(die Mächtigkeit des endlichen Körpers $k(\mathfrak{p})$).

Damit haben wir offenbar:

Lemma 8.16 In der Situation von 8.14 ist der Frobenius (-Automorphismus) $Fr_{\mathfrak{P}} \in G$ eindeutig bestimmt durch die Eigenschaften:

- (i) $Fr_{\mathfrak{P}} \mathfrak{P} = \mathfrak{P}$.
- (ii) $Fr_{\mathfrak{P}} b \equiv b^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ für alle $b \in \mathcal{O}_L$.

Beweis: (i) $\Leftrightarrow Fr_{\mathfrak{P}} \in G_{\mathfrak{P}}$.

(ii) \Leftrightarrow unter $G_{\mathfrak{P}} \rightarrow Gal(k(\mathfrak{P})/k(\mathfrak{p}))$ gilt $Fr_{\mathfrak{P}} \mapsto Fr_{N(\mathfrak{p})}$.

Bemerkungen 8.17 (a) Bedingung (i) folgt aus (ii).

(b) Für $\sigma \in G$ folgt sofort aus den Definitionen, dass gilt (vgl. 8.3. (d))

$$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}, \quad I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1},$$

sowie für unverzweigtes $\mathfrak{P}/\mathfrak{p}$

$$Fr_{\sigma\mathfrak{P}} = \sigma Fr_{\mathfrak{P}} \sigma^{-1}.$$

(c) Insbesondere hängen für **abelsches** G die Gruppen $G_{\mathfrak{P}}$, $I_{\mathfrak{P}}$ und das Element $Fr_{\mathfrak{P}}$ nicht von der Wahl von \mathfrak{P} (über \mathfrak{p}) ab, sondern nur von \mathfrak{p} . Sie werden dann auch mit $G_{\mathfrak{p}}$, $I_{\mathfrak{p}}$ und $Fr_{\mathfrak{p}}$ bezeichnet.

Beispiel 8.18 Sei $n \in \mathbb{N}$ und $\zeta = \zeta_n$ eine primitive Einheitswurzel, und sei p eine Primzahl, die n nicht teilt. Dann ist p unverzweigt in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (siehe 6.8-6.10), und es ist

$$Fr_p = p \pmod{n} \in (\mathbb{Z}/n\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Denn für $\alpha = \sum a_i \zeta^i \in \mathbb{Z}[\zeta]$ ($a_i \in \mathbb{Z}$) gilt für das zu $p \pmod{n}$ gehörige Element $\sigma_p \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$$\sigma_p \alpha = \sum a_i \zeta^{ip} \equiv \left(\sum a_i \zeta^i \right)^p \pmod{p\mathbb{Z}[\zeta]},$$

so dass die Behauptung aus der Charakterisierung 8.16 folgt. Insbesondere ist die Zerlegungsgruppe $G_p = \langle p \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ vgl. Übungsaufgabe 25.

Bemerkung 8.19 Ist L/K eine Galoiserweiterung von Zahlkörpern und ist \mathfrak{P} ein Primideal in L welches unverzweigt in L/K ist, so ist die Zerlegungsgruppe $G_{\mathfrak{P}}$ von \mathfrak{P} in $G = \text{Gal}(L/K)$ *zyklisch*, denn wegen $I_{\mathfrak{P}} = 1$ ist $G_{\mathfrak{P}} \cong \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ für $\mathfrak{p} = \mathfrak{P} \cap K$, und die letztere Galoisgruppe ist zyklisch (erzeugt vom relativen Frobenius-Automorphismus), da $k(\mathfrak{p})$ und $k(\mathfrak{P})$ endlich sind. Insbesondere kann \mathfrak{p} nicht träge in L/K sein, wenn G nicht zyklisch ist.

9 Das quadratische Reziprozitätsgesetz

Definition 9.1 Seien $a, b \in \mathbb{Z}$. Dann heißt a **quadratischer Rest modulo b** , wenn die Gleichung

$$a \equiv x^2 \pmod{b}$$

mit $x \in \mathbb{Z}$ lösbar ist. Äquivalent hierzu ist, dass die diophantische Gleichung

$$x^2 + yb = a$$

eine Lösung $x, y \in \mathbb{Z}$ hat.

Aus dem chinesischen Restsatz folgt sofort

Lemma 9.2 Seien $m, n \in \mathbb{Z}$, $(m, n) = 1$. Dann gilt für $a \in \mathbb{Z}$
 a quadratischer Rest modulo mn
 $\Leftrightarrow a$ quadratischer Rest modulo m **und** modulo n .

Hiernach kann man auf den Fall $b = p^r$ für eine Primzahl p reduzieren. Eine weitere Reduktion zeigt dann, dass es genügt, a prim zu p zu betrachten (Übungsaufgabe). In diesem Fall gilt

Lemma 9.3 Sei p eine Primzahl und $a \in \mathbb{Z}$ mit $(a, p) = 1$. Dann gilt für $\nu \geq 1$:

(a) Ist p ungerade, so ist a quadratischer Rest modulo p^ν genau dann, wenn a quadratischer Rest modulo p ist.

(b) Für $p = 2$ gilt

$$a \text{ quadratischer Rest modulo } 2^\nu \Leftrightarrow \begin{cases} \text{immer, wenn } \nu = 1, \\ a \equiv 1 \pmod{4}, & \text{falls } \nu = 2, \\ a \equiv 1 \pmod{8}, & \text{falls } \nu \geq 3. \end{cases}$$

Beweis: Übungsaufgabe.

Es genügt also, im Folgenden den Fall zu betrachten, wo $b = p$ eine ungerade Primzahl ist und a prim zu p .

Definition 9.4 Für eine ungerade Primzahl p und eine ganze Zahl a , $(a, p) = 1$, definiere das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a \text{ quadratischer Rest mod } p \\ -1, & \text{sonst.} \end{cases}$$

Lemma 9.5 (a) Das Legendre-Symbol ist multiplikativ, d.h., für $a, b \in \mathbb{Z}$, $p \nmid a \cdot b$, gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

(b) Es gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Beweis: Nach Definition gilt für $\bar{a} = a \pmod{p} \in \mathbb{F}_p^\times$

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \bar{a} \in (\mathbb{F}_p^\times)^2.$$

Hieraus ergibt sich (a) (z.B. durch Fallunterscheidung), da $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ zyklisch von der Ordnung 2 ist, also isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

Da \mathbb{F}_p^\times zyklisch von der Ordnung $p-1$ ist und $p-1$ gerade ist, gilt weiter $(\mathbb{F}_p^\times)^{\frac{p-1}{2}} = \mu_2(\mathbb{F}_p) = \{\pm 1\}$, und $\bar{a} \in (\mathbb{F}_p^\times)^2 \Leftrightarrow \bar{a}^{\frac{p-1}{2}} = 1$, nach der Theorie der endlichen zyklischen Gruppen.

Damit folgt (b). (Hieraus folgt wiederum (a), da

$$\begin{array}{ccc} \{\pm 1\} & \xrightarrow{\sim} & \mu_2(\mathbb{F}_p) \\ y & \mapsto & y \pmod{p} \end{array}$$

ein Isomorphismus ist).

Bemerkung 9.6 Natürlich hängt $\left(\frac{a}{p}\right)$ nur von $a \pmod{p}$ ab. Wir können also $\left(\frac{\cdot}{p}\right)$ als Homomorphismus

$$\begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \{\pm 1\} \\ \bar{a} & \longmapsto & \left(\frac{a}{p}\right) \end{array}$$

auffassen.

Wichtig ist der folgende Zusammenhang mit dem Zerlegungsgesetz in quadratischen Zahlkörpern.

Satz 9.7 Für quadratfreies a und $(p, 2a) = 1$ gilt

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow p \text{ ist zerlegt in } \mathbb{Q}(\sqrt{a})$$

$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow p \text{ ist träge in } \mathbb{Q}(\sqrt{a})$$

Beweis: Die zweite Aussage wurde in Übungsaufgabe 10 bewiesen. Da p prim zu $2a$ ist, also unverzweigt in $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ ist (Übungsaufgabe 24; die Diskriminante von $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ ist a oder $4a$), folgt die erste Behauptung.

Der folgende Satz erlaubt nicht nur eine leichte Berechnung des Legendre-Symbols, sondern hat auch die Entwicklung der algebraischen Zahlentheorie stark beeinflusst.

Satz 9.8 (Quadratisches (oder Gaußsches) Reziprozitätsgesetz) Für zwei verschiedene ungerade Primzahlen p und q gilt

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}}.$$

Weiter gelten die sogenannten "Ergänzungssätze"

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beispiel 9.9 Hiermit ist es leicht, Legendre-Symbole auszurechnen: z.B. ist

$$\begin{aligned} \left(\frac{59}{97}\right) &= (-1)^{\frac{59-1}{2} \cdot \frac{97-1}{2}} \left(\frac{97}{59}\right) \\ &= \left(\frac{38}{59}\right) = \left(\frac{2}{59}\right) \left(\frac{19}{59}\right) \\ &= (-1)^{\frac{59^2-1}{8}} \cdot (-1)^{\frac{19-1}{2} \cdot \frac{59-1}{2}} \left(\frac{59}{19}\right) \\ &= \left(\frac{2}{19}\right) = (-1)^{\frac{19^2-1}{8}} = -1. \end{aligned}$$

Beachte: Wegen $(a + 8n)^2 = a^2 + 16an + 64n^2$ gilt

$$a \equiv b \pmod{8} \Rightarrow a^2 \equiv b^2 \pmod{16}.$$

Es folgt

$$a \equiv \begin{cases} 1 \\ 3 \\ 5 \\ 7 \end{cases} \pmod{8} \Rightarrow a^2 \equiv \begin{cases} 1 \\ 9 \\ 9 \\ 1 \end{cases} \pmod{16} \Rightarrow \frac{a^2-1}{8} \equiv \begin{cases} 0 \\ 1 \\ 1 \\ 0 \end{cases} \pmod{2}$$

Zum Beweis von 9.8 benutzen wir:

Proposition 9.10 Sei p eine ungerade Primzahl und $p^* := (-1)^{\frac{p-1}{2}} \cdot p$. Dann ist $\mathbb{Q}(\sqrt{p^*})$ der eindeutig bestimmte quadratische Zahlkörper, der in $\mathbb{Q}(\zeta_p)$ enthalten ist, ζ_p eine primitive p -te Einheitswurzel.

Beweis: Da $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch von der Ordnung $p-1$ ist und $p-1$ von 2 geteilt wird, gibt es genau einen quadratischen Zahlkörper, der in $\mathbb{Q}(\zeta_p)$ enthalten ist. Nach 6.5 gilt nun für die Diskriminante von $1, \zeta_p, \dots, \zeta_p^{p-2}$:

$$d(1, \zeta_p, \dots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} \cdot p^{p-2}.$$

Wegen $2 \mid (p-1)$ und $2 \nmid (p-2)$ ist die rechte Seite gleich $p^* \cdot p^{p-3} = p^* \cdot \left(p^{\frac{p-3}{2}}\right)^2$.

Andererseits ist nach Definition 3.9 die Diskriminante jeder \mathbb{Q} -Basis von $\mathbb{Q}(\zeta_p)$ ein Quadrat in $\mathbb{Q}(\zeta_p)$; explizit ist

$$d(1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}) = \left[\det (\zeta_p^{ij})_{\substack{i=0, \dots, p-2 \\ j=1, \dots, p-1}} \right]^2.$$

Es folgt, dass p^* eine Wurzel in $\mathbb{Q}(\zeta_p)$ besitzt, dass also $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$.

Beweis von 9.8: Wir behandeln zuerst die Spezialfälle.

1) Nach 9.5 (b) ist $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Da $p \neq 2$ ist, ist die Abbildung $\{\pm 1\} \xrightarrow{\sim} \mu_2(\mathbb{F}_p)$ ein Isomorphismus; es folgt also $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ in \mathbb{Z} .

2) Zur Berechnung von $\left(\frac{2}{p}\right)$ rechnen wir in $\mathbb{Z}[i]$. Wegen $(1+i)^2 = 2i$ gilt

$$(1+i)^p = (1+i) \left((1+i)^2\right)^{\frac{p-1}{2}} = (1+i) i^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}}.$$

Hieraus folgt wegen $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}$ und $(1+i)^p \equiv 1+i^p \pmod{p}$

$$1+i \cdot (-1)^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \cdot (1+i) \cdot i^{\frac{p-1}{2}} \pmod{p}.$$

Hieraus ergibt sich für $\frac{p-1}{2}$ gerade

$$1+i \equiv \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p-1}{4}} (1+i), \text{ also}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

Für $\frac{p-1}{2}$ ungerade ist $\frac{p+1}{2}$ gerade, und wegen $i^{\frac{p-1}{2}} = -i^{\frac{p+1}{2}} \cdot i$ gilt

$$1-i \equiv \left(\frac{2}{p}\right) (-1)^{\frac{p+1}{4}} (1-i), \text{ also}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}.$$

Im ersten Fall ist $(-1) = (-1)^{\frac{p+1}{2}}$, und im zweiten Fall ist $(-1) = (-1)^{\frac{p-1}{2}}$. Es ist also in jedem Fall

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p+1)(p-1)}{2 \cdot 4}}.$$

3) Wir kommen nun zur eigentlichen Reziprozitätsformel. Wegen 1) genügt es, die folgende Gleichheit zu zeigen

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Dazu betrachten wir das Galoisdiagramm

$$\begin{array}{ccccc} \mathbb{Q}(\zeta_p) & & 1 & & \\ \downarrow \frac{p-1}{2} & & \downarrow & & \\ \mathbb{Q}(\sqrt{p^*}) & H = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*})) & = & (\mathbb{Z}/p\mathbb{Z})^\times & \\ \downarrow 2 & & \downarrow & & \cap \\ \mathbb{Q} & G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & = & (\mathbb{Z}/p\mathbb{Z})^\times & \end{array}$$

Dann gelten die Äquivalenzen:

$$\begin{aligned} & \left(\frac{p^*}{q}\right) = 1 \\ \Leftrightarrow^{9.7} & q \text{ (voll) zerlegt in } \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}. \\ \Leftrightarrow^{8.6(b)} & \text{Für die Zerlegungsgruppe } G_q \subseteq G \text{ von } q \text{ gilt } G_q \subseteq H. \\ \Leftrightarrow & q \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2 = (\mathbb{F}_p^\times)^2 \text{ (denn es ist } G_q = \langle q \rangle \text{ nach 8.18)} \\ \Leftrightarrow & \left(\frac{q}{p}\right) = 1 \quad (\text{nach Definition}) \end{aligned}$$

q.e.d.

10 Minkowski-Theorie

Sei V ein endlich-dimensionaler \mathbb{R} -Vektorraum.

Definition 10.1 (a) Ein **Gitter** in V ist eine Untergruppe der Form

$$\Lambda = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m,$$

wobei v_1, \dots, v_m linear unabhängige Vektoren in V sind. Dann heißt (v_1, \dots, v_m) eine Basis von Λ und

$$M = M_{\underline{v}} = \left\{ \sum_{i=1}^m x_i v_i \mid x_i \in \mathbb{R}, \quad 0 \leq x_i < 1 \right\}$$

eine Grundmasche des Gitters.

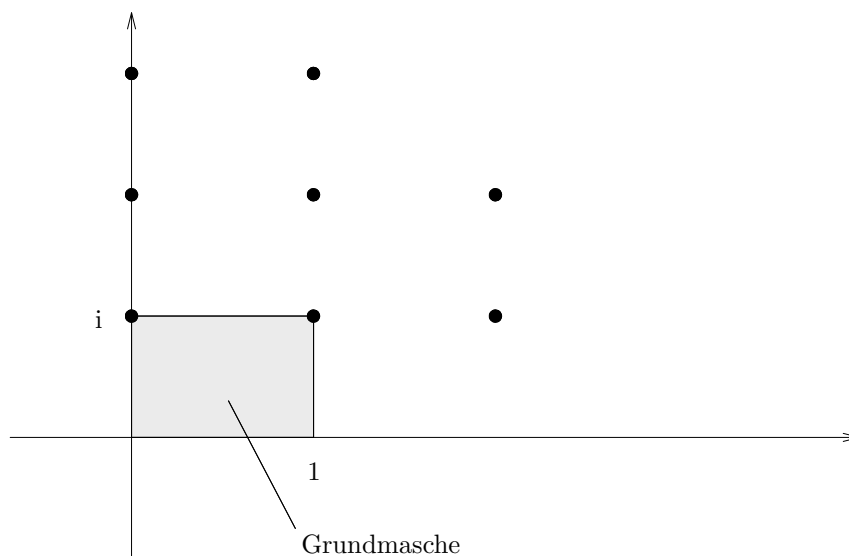
(b) Λ heißt vollständig (oder \mathbb{Z} -Struktur von V), wenn $m = n$ ist, d.h., wenn (v_1, \dots, v_m) eine Basis von V ist.

Wir bemerken noch, dass $M \subseteq V$ ein Repräsentantensystem für V/Λ bildet; anders ausgedrückt, ist

$$(10.1.1) \quad V = \bigcup_{\lambda \in \Lambda} \lambda + M_0$$

(disjunkte Vereinigung), denn mit der Gauß-Klammer $[x] = \max\{n \in \mathbb{Z} \mid n \leq x\}$ gilt $\sum y_i v_i = \sum [y_i] v_i + \sum (y_i - [y_i]) v_i$.

Beispiel 10.2 $\mathbb{Z} \oplus \mathbb{Z}i \subseteq \mathbb{C}$ ist ein vollständiges Gitter



Lemma 10.3 Eine Untergruppe $\Lambda \subseteq V$ ist genau dann ein Gitter, wenn Λ diskret (bezüglich der Relativtopologie von V) ist.

Beweis Offenbar ist Λ genau dann diskret, wenn jedes $\lambda \in \Lambda$ eine Umgebung $U \subseteq V$ besitzt mit $U \cap \Lambda = \{\lambda\}$.

1) Sei Λ ein Gitter und $\lambda = \sum_{i=1}^m a_i v_i \in \Lambda = \bigoplus_{i=1}^m \mathbb{Z} v_i$. Sei v_1, \dots, v_m zu einer Basis v_1, \dots, v_n von V ergänzt. Dann ist

$$U = \left\{ \sum_{i=1}^n x_i v_i \in V \mid |x_i - a_i| < 1 \quad \text{für alle } i = 1, \dots, m \right\}$$

eine offene Umgebung von λ mit $U \cap \Lambda = \{\lambda\}$.

2) Sei umgekehrt $\Lambda \subseteq V$ eine diskrete Untergruppe und $\lambda \in \Lambda$. Sei V_0 der lineare Unterraum von V , der durch die Menge Λ aufgespannt wird. Sei v_1, \dots, v_m eine in Λ gelegene Basis von V_0 , und betrachte das Gitter

$$\Lambda_0 = \mathbb{Z} v_1 \oplus \dots \oplus \mathbb{Z} v_m \subseteq \Lambda.$$

Λ_0 ist ein vollständiges Gitter in V_0 . Wir behaupten nun, dass der Index $(\Lambda : \Lambda_0)$ endlich ist: Seien λ_i ($i \in I$) Repräsentanten für die Nebenklassen in Λ/Λ_0 . Da Λ_0 vollständiges Gitter in V_0 ist, gilt nach (10.1.1)

$$V_0 = \bigcup_{\lambda \in \Lambda_0} \lambda + M_0 \quad , \quad \text{mit der Grundmasche} \quad M_0 = \left\{ \sum_{i=1}^m x_i v_i \mid x_i \in [0, 1[\right\}.$$

Daher ist für jedes $i \in I$

$$\lambda_i = \lambda_{0i} + m_i \quad , \quad \text{mit } \lambda_{0i} \in \Lambda_0, \quad m_i \in M_0 .$$

Da die $m_i = \lambda_i - \lambda_{0i} \in \Lambda$ diskret in der beschränkten Menge M_0 liegen, muss ihre Anzahl endlich sein; es ist also Λ/Λ_0 endlich.

Mit $N = (\Lambda : \Lambda_0)$ gilt dann $N\Lambda \subseteq \Lambda_0$, also

$$\Lambda \subseteq \frac{1}{N} \cdot \Lambda_0 = \mathbb{Z} \left(\frac{1}{N} v_1 \right) \oplus \dots \oplus \mathbb{Z} \left(\frac{1}{N} v_m \right) .$$

nach dem Elementarteilersatz (siehe (3.18.1)) ist Λ also eine endlich erzeugte freie abelsche Gruppe, also

$$\Lambda = \mathbb{Z}w_1 \oplus \dots \oplus \mathbb{Z}w_r$$

mit einer \mathbb{Z} -Basis $w_1, \dots, w_r \in V_0, r \leq m$. Da die w_i ebenfalls V_0 aufspannen, ist $r = m$, und w_1, \dots, w_m sind linear unabhängig über \mathbb{R} , d.h., Λ ist ein vollständiges Gitter in V_0 .

Lemma 10.4 Ein Gitter $\Lambda \subseteq V$ ist genau dann vollständig, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt mit

$$(10.4.1) \quad \bigcup_{\lambda \in \Lambda} \lambda + M = V .$$

Beweis Ist Λ vollständig, so können wir für M die Grundmasche nehmen.

Sei andererseits M beschränkt mit (10.4.1) und $V_0 \subseteq V$ der durch Λ aufgespannte Unterraum.

Behauptung $V = V_0$

Beweis Sei $v \in V$. Wegen (10.4.1) ist für jedes $n \in \mathbb{N}$

$$n \cdot v = \lambda_n + a_n \quad , \quad \text{mit } \lambda_n \in \Lambda \text{ und } a_n \in M .$$

Da M beschränkt ist, ist $\frac{a_n}{n}$ eine Nullfolge und

$$v = \lim_{n \rightarrow \infty} \frac{a_n}{n} + \lim_{n \rightarrow \infty} \frac{\lambda_n}{n} = \lim_{n \rightarrow \infty} \frac{\lambda_n}{n} \in V_0 ,$$

da V_0 abgeschlossen in V ist.

Sei nun V ein **euklidischer** Vektorraum, also ein endlich-dimensionaler \mathbb{R} -Vektorraum, mit einer symmetrischen, positiv definierten Bilinearform

$$\langle , \rangle : \quad V \times V \rightarrow \mathbb{R} .$$

Dann haben wir auf V einen Volumenbegriff (genauer ein Haarsches Maß, d.h., ein translationsinvariantes Maß), wie folgt: Ist $\underline{v} = (v_1, \dots, v_n)$ eine Orthonormalbasis von V , so ist

$$\varphi = \varphi_{\underline{v}} : \mathbb{R}^n \xrightarrow{\sim} V$$

$$e_i \mapsto v_i \quad (e_i \text{ der } i\text{-te Einheitsvektor})$$

da \underline{v} eine Orthonormalbasis war. Es ist also wegen

$$M_{\underline{w}} = A \cdot M_{\underline{v}}, \text{ wobei } M_{\underline{v}} = \left\{ \sum_{i=1}^n x_i v_i \mid x_i \in [0, 1[\right\}$$

und $\text{vol}(M_{\underline{v}}) = 1$ nach (10.4.3)

$$(10.4.4) \quad \text{vol}(M_{\underline{w}}) = |\det(\langle w_i, w_j \rangle)|^{\frac{1}{2}},$$

was eine algebraische Beschreibung des Volumens liefert.

Definition 10.5 Ist Λ das von den Vektoren w_1, \dots, w_n aufgespannte Gitter, so setze

$$\text{vol}(\Lambda) := \text{vol}(M_{\underline{w}}) \quad (= |\det(\langle w_i, w_j \rangle)|^{\frac{1}{2}})$$

Da für eine andere \mathbb{Z} -Basis von Λ die Übergangsmatrix in $Gl_n(\mathbb{Z})$ liegt und somit Determinante ± 1 hat, hängt dies nicht von der Basis, sondern nur von Λ ab.

Lemma 10.6 Ist $\Lambda' \subseteq \Lambda$ ein Untergitter von endlichem Index, so gilt

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

Beweis Sind \underline{w} und \underline{w}' Basen von Λ bzw. Λ' , und ist A die Übergangsmatrix von \underline{w} nach \underline{w}' , so ist $A \in Gl_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$ und $\Lambda' = A \cdot \Lambda$. Hieraus folgt

$$\text{vol}(\Lambda') = |\det A| \cdot \text{vol}(\Lambda).$$

Andererseits gilt nach dem Lemma 10.9 unten

$$(\Lambda : \Lambda') = |\det A|.$$

Definition 10.7 Sei K ein Körper und $n \in \mathbb{N}$. Dann heißen Matrizen von der Form

$$E_i(\lambda) = i \text{ --- } \begin{pmatrix} & & & i & & \\ & & & | & & \\ 1 & & & & & \\ & \ddots & & & & 0 \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ 0 & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}, \quad i \in \{1, \dots, n\}, \lambda \in K^\times$$

(λ an der Stelle (i, i)), oder von der Form

$$E_{k\ell}(\lambda) = k \text{ --- } \begin{pmatrix} & & & \ell & & \\ & & & | & & \\ 1 & & & & & \\ & \ddots & & & & \\ & & & \lambda & & 0 \\ & & & & & \\ 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad i, k \in \{1, \dots, n\}, \quad i \neq k, \quad \lambda \in K$$

(λ an der Stelle (k, ℓ)) **Elementarmatrizen.**

Satz 10.8 Jede Matrix $A \in GL_n(K)$ ist Produkt von Elementarmatrizen.

Beweis Ist

$$E_i(\lambda)A = A',$$

so geht A' aus A hervor, indem die i -te Zeile von A mit λ multipliziert wird. Für

$$E_{k\ell}(\lambda)A = A''$$

entsteht A'' aus A , indem das λ -fache der ℓ -ten Zeile von A auf die k -te Zeile von A aufaddiert wird. Diese beiden Operationen erzeugen alle Zeilentransformationen. Aus dem Gaußschen Eliminationsverfahren folgt also, dass es Elementarmatrizen B_1, \dots, B_m gibt mit

$$B_m \dots B_1 A = \begin{pmatrix} 1 & & & \\ & \ddots & & 0 \\ & & \ddots & \\ 0 & & & \ddots \\ & & & & 1 \end{pmatrix} = E.$$

Damit gilt $A = B_1^{-1} \dots B_m^{-1}$, und die B_i^{-1} sind wieder Elementarmatrizen, wie man leicht sieht.

Lemma 10.9 Sei $U \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$. Dann ist $\mathbb{Z}^n/U\mathbb{Z}^n$ endlich, und es gilt

$$|\mathbb{Z}^n/U\mathbb{Z}^n| = |\det A|.$$

Beweis Sind $U_1, U_2 \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$, so auch $U_1 U_2$, und gilt die Behauptung für zwei Matrizen in $\{U_1, U_2, U_1 U_2\}$, so auch für die dritte. Dies folgt aus der exakten Sequenz

$$0 \rightarrow \Lambda/U_2\Lambda \xrightarrow{U_1} \Lambda/U_1 U_2 \Lambda \rightarrow \Lambda/U_1 \Lambda \rightarrow 0$$

für $\Lambda = \mathbb{Z}^n$ und der daraus folgenden Beziehung

$$|\Lambda/U_1 U_2 \Lambda| = |\Lambda/U_1 \Lambda| \cdot |\Lambda/U_2 \Lambda|$$

sowie der entsprechenden Gleichung

$$|\det U_1 U_2| = |\det U_1| \cdot |\det U_2|.$$

Ist nun $U \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$, so gibt es nach 10.8 Elementarmatrizen $B_1, \dots, B_m \in GL_n(\mathbb{Q})$ mit $U = B_1 \dots B_m$. Es gibt $a_i \in \mathbb{Z} \setminus \{0\}$ mit $a_i B_i \in M_n(\mathbb{Z})$ und mit $a = \prod a_i$ gilt

$$(aE)U = aU = \prod_{i=1}^m a_i B_i.$$

Nach der Vorbemerkung genügt es daher, die Behauptung für Matrizen der Form $U = aB$ zu zeigen mit $a \in \mathbb{Z} \setminus \{0\}$ und $B \in Gl_n(\mathbb{Q})$ Elementarmatrix. Für $U = aE_i(\lambda)$ mit $b = a\lambda \in \mathbb{Z}$ gilt aber

$$U = \begin{pmatrix} a & & & & \\ & \ddots & & & \\ & & a & & \\ & & & b & \\ & & & & a \\ & 0 & & & \ddots \\ & & & & & a \end{pmatrix},$$

und $\mathbb{Z}^n/U\mathbb{Z}^n \cong (\mathbb{Z}/a\mathbb{Z})^{n-1} \times \mathbb{Z}/b\mathbb{Z}$ mit Ordnung $a^{n-1}b = \det U$. Für $U = aE_{k\ell}(\lambda)$ mit $b = a\lambda \in \mathbb{Z}$ gilt

$$U = \begin{pmatrix} a & & & & \\ & \ddots & & & \\ & & b & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}.$$

Für $U' = aE_{k\ell}(-\lambda)$ sieht man leicht, dass $U\mathbb{Z}^n = U'\mathbb{Z}^n$; andererseits gilt $U \cdot U' = a^2E$. Wegen $\det UU' = a^{2n} = |\mathbb{Z}^n/UU'\mathbb{Z}^n|$ folgt nun die Behauptung für U .

Wir kommen nun zum grundlegenden Satz von Minkowski.

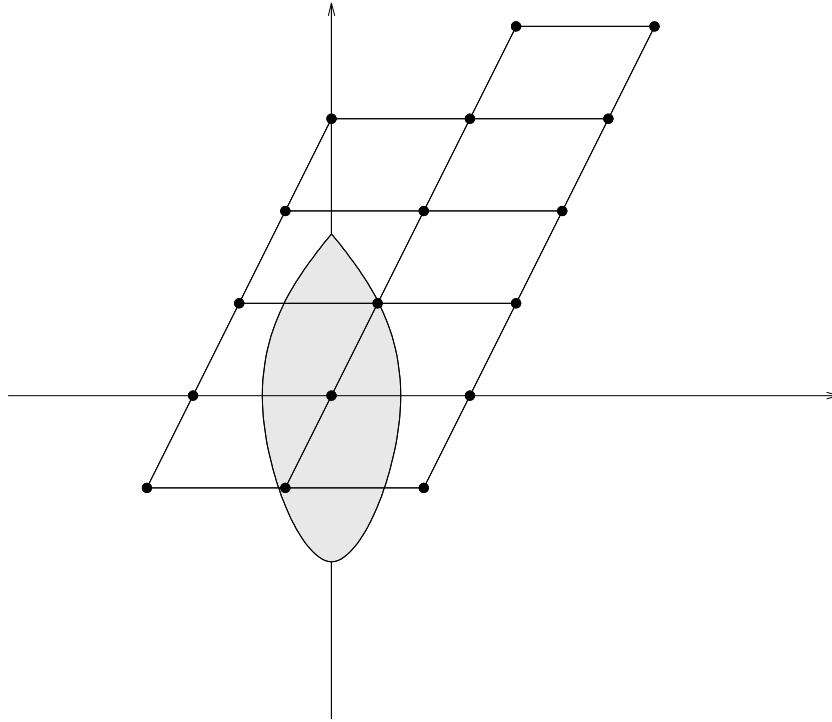
Definition 10.10 Eine Teilmenge $M \subseteq V$ heißt

- (a) konvex, wenn für je zwei $x, y \in M$ die Verbindungsstrecke $\{x + t(y - x) \mid 0 \leq t \leq 1\}$ ganz in M liegt,
- (b) zentralsymmetrisch, wenn mit $x \in M$ auch $-x \in M$ ist.

Satz 10.11 (Minkowskischer Gitterpunktsatz) Sei Λ ein vollständiges Gitter in einem euklidischen Vektorraum V der Dimension n und $M \subseteq V$ eine zentral-symmetrische, konvexe Teilmenge. Ist

$$\text{vol}(M) > 2^n \cdot \text{vol}(\Lambda),$$

so erhält M mindestens einen Punkt $\lambda \in \Lambda \setminus \{0\}$.



Beweis Es genügt zu zeigen, dass Gitterpunkte $\lambda_1 \neq \lambda_2$ in Λ gibt mit

$$\left(\lambda_1 + \frac{1}{2}M\right) \cap \left(\lambda_2 + \frac{1}{2}M\right) \neq \emptyset.$$

Dann gibt es nämlich $x_1, x_2 \in M$ mit

$$\lambda_1 + \frac{1}{2}x_1 = \lambda_2 + \frac{1}{2}x_2,$$

und es ist

$$\Lambda \ni \lambda_1 - \lambda_2 = \frac{1}{2}x_1 - \frac{1}{2}x_2 \in M,$$

als Mittelpunkt der Strecke zwischen $x_1, -x_2 \in M$.

Angenommen, die Mengen $\lambda + \frac{1}{2}M$ ($\lambda \in \Lambda$) sind alle disjunkt. Dann gilt dies auch für den Durchschnitt mit einer Grundmasche M_0 von Λ , d.h., es ist

$$\text{vol}(M_0) \geq \sum_{\lambda \in \Lambda} \text{vol}\left(M_0 \cap \left(\lambda + \frac{1}{2}M\right)\right).$$

Nun ist aber $\text{vol}(M_0 \cap (\lambda + \frac{1}{2}M)) = \text{vol}((M_0 - \lambda) \cap \frac{1}{2}M)$, da sich das Volumen bei Translation mit $-\lambda$ nicht ändert. Da die $M_0 - \lambda$ ganz V , also auch $\frac{1}{2}M$ überdecken, folgt

$$\text{vol}(\Lambda) = \text{vol}(M_0) \geq \sum_{\lambda \in \Lambda} \text{vol}\left((M_0 - \lambda) \cap \frac{1}{2}M\right) = \text{vol}\left(\frac{1}{2}M\right) = \frac{1}{2^n} \text{vol}(M),$$

Widerspruch zur Annahme!

In der Zahlentheorie tauchen solche Gitter wie folgt auf.

Sei K ein Zahlkörper und $n = [K : \mathbb{Q}]$.

Nach der Algebra besitzt K n verschiedene \mathbb{Q} -Einbettungen nach \mathbb{C} .

Definition 10.12 Eine Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ heißt **reell**, wenn $\sigma(K) \subseteq \mathbb{R}$, und **komplex** sonst.

Seien $\rho_1, \dots, \rho_r : K \hookrightarrow \mathbb{R}$ die reellen Einbettungen von K . Für jede komplexe Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ ist wegen $\sigma(K) \not\subseteq \mathbb{R}$ die komplex konjugierte Einbettung $\bar{\sigma}$, definiert durch $\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)}$, wobei $z \mapsto \bar{z}$ die komplexe Konjugation ist, ungleich σ . Daher können wir die komplexen Einbettungen in Paaren

$$\sigma_1, \bar{\sigma}_1, \sigma_2, \bar{\sigma}_2, \dots, \sigma_s, \bar{\sigma}_s$$

gruppieren. Damit ist also

$$(10.12.1) \quad n = r + 2s.$$

Für jeden Zahlkörper K sei $r = r(K)$ die Anzahl der reellen Einbettungen und sei $s = s(K)$ die Anzahl der Paare komplex konjugierter Einbettungen. (In (älterer) deutscher Literatur verwendet man oft r_1 und r_2 hierfür).

Beispiel 10.13 Der Zahlkörper $\mathbb{Q}(\sqrt[3]{5})$ hat eine reelle und zwei komplexe Einbettungen (es ist also $r = s = 1$): $\alpha = \sqrt[3]{5}$ ist primitives Element, mit Minimalpolynom $x^3 - 5$, und die Einbettungen in \mathbb{C} entstehen dadurch, indem man α auf die Nullstellen von $X^3 - 5$ in \mathbb{C} abbildet. Diese sind

$$\sqrt[3]{5} \quad (\text{die reelle Wurzel}), \quad e^{\frac{2\pi i}{3}} \sqrt[3]{5}, \quad e^{\frac{2\pi i \cdot 2}{3}} \sqrt[3]{5}.$$

Dies zeigt die Behauptung.

Wir fixieren nun eine Nummerierung

$$\underbrace{\rho_1, \dots, \rho_r}_{\text{reell}}, \quad \underbrace{\sigma_1, \bar{\sigma}_1, \sigma_2, \bar{\sigma}_2, \dots, \sigma_s, \bar{\sigma}_s}_{\text{komplex}}$$

der Einbettungen $K \hookrightarrow \mathbb{C}$ und definieren die Abbildung

$$\begin{aligned} j : K &\hookrightarrow \mathbb{R}^r \times \mathbb{C}^s =: V(K) \\ \alpha &\mapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \sigma_1(\alpha), \dots, \sigma_n(\alpha)) \end{aligned}$$

$V(K)$ ist ein n -dimensionaler \mathbb{R} -Vektorraum. Wir schreiben die Elemente als (x', x'') mit $x' \in \mathbb{R}^r$ und $x'' \in \mathbb{C}^s$, und machen $V(K)$ zu einem euklidischen Vektorraum durch das Skalarprodukt

$$\langle x, y \rangle = \sum_{i=1}^r x'_i y'_i + \sum_{j=1}^s \text{Tr}_{\mathbb{C}/\mathbb{R}}(x''_j \overline{y''_j})$$

d.h., durch die kanonischen reellen Skalarprodukte auf \mathbb{R}^r und \mathbb{C}^s (Ist \langle, \rangle hermitesches Skalarprodukt auf einem \mathbb{C} -Vektorraum, so ist $\text{Tr}_{\mathbb{C}/\mathbb{R}} \langle, \rangle$ euklidisches Skalarprodukt).

Proposition 10.14 Fassen wir j als Inklusion auf, so ist \mathcal{O}_K ein vollständiges Gitter in $V(K)$, und es ist

$$\text{vol}(\mathcal{O}_K) = \sqrt{|d_K|},$$

wobei d_K die Diskriminante von K ist.

Beweis Ist $\alpha_1, \dots, \alpha_n$ eine \mathbb{Z} -Basis von \mathcal{O}_K , so ist

$$(10.14.1) \quad \det(\langle \alpha_i, \alpha_j \rangle) \neq 0$$

genau dann, wenn $(\alpha_1, \dots, \alpha_n)$ ein vollständiges Gitter in $V(K)$ aufspannt: Ist nämlich $\sum_i \lambda_i \alpha_i = 0$ in $V(K)$ mit $\lambda_1, \dots, \lambda_n \in \mathbb{R}$, nicht alle gleich 0, so ist $\sum_i \lambda_i \langle \alpha_i, \alpha_j \rangle = 0$ für alle α_j , d.h., die Zeilen der Matrix $(\langle \alpha_i, \alpha_j \rangle)$ wären linear abhängig und die Diskriminante gleich null. Gilt aber (10.14.1), so ist nach 10.5

$$\text{vol}(\mathcal{O}_K) = |\det(\langle \alpha_i, \alpha_j \rangle)|^{\frac{1}{2}}.$$

Wir berechnen nun

$$\begin{aligned} \langle \alpha_i, \alpha_j \rangle &= \sum_{k=1}^r \rho_k \alpha_i \rho_k \alpha_j + \text{Tr}_{\mathbb{C}/\mathbb{R}} \left(\sum_{\ell=1}^s \sigma_\ell \alpha_i \overline{\sigma_\ell \alpha_j} \right) \\ &= \sum_{k=1}^r \rho_k \alpha_i \rho_k \alpha_j + \sum_{\ell=1}^s \sigma_\ell \alpha_i \overline{\sigma_\ell \alpha_j} + \sum_{\ell=1}^s \overline{\sigma_\ell \alpha_i} \sigma_\ell \alpha_j \\ &= \sum_{k=1}^n \tau_k \alpha_i \cdot \overline{\tau_k \alpha_j}, \end{aligned}$$

wobei $\tau_1, \dots, \tau_n : K \hookrightarrow \mathbb{C}$ die verschiedenen Einbettungen sind. Hier haben wir benutzt, dass $\text{Tr}_{\mathbb{C}/\mathbb{R}}|z| = z + \bar{z}$ ist. Mit der Matrix

$$A = (\tau_i \alpha_j)$$

ist also

$$(\langle \alpha_i, \alpha_j \rangle) = A^t \cdot \bar{A}.$$

Andererseits ist nach Definition 3.9

$$(\det A)^2 = d(\alpha_1, \dots, \alpha_n),$$

die Diskriminante von $\alpha_1, \dots, \alpha_n$, und da diese Elemente eine \mathbb{Z} -Basis von \mathcal{O}_K bilden, ist

$$d(\alpha_1, \dots, \alpha_n) = d_K,$$

die Diskriminante von K , und diese ist nach 3.13 ungleich null. Es folgt (10.14.1) und

$$\text{vol}(\mathcal{O}_K) = |\det(A^t \cdot \bar{A})|^{\frac{1}{2}} = |\det(A)| = |d_K|^{\frac{1}{2}}.$$

Lemma/Definition 10.15 Für ein gebrochenes Ideal $\mathfrak{a} \subseteq K$ definiere die Norm durch

$$N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{n_i},$$

wobei $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$ die Primidealzerlegung von \mathfrak{a} ist (also die \mathfrak{p}_i Primideale und $n_i \in \mathbb{Z}$) und

$$N(\mathfrak{p}) = (\mathcal{O}_K : \mathfrak{p}) = |k(\mathfrak{p})|,$$

wie in 8.15 definiert. Für ein ganzes Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ gilt dann

$$N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

Für $\alpha \in K^\times$ gilt

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

Beweis der Behauptungen: 1) Aus der Definition folgt sofort

$$(10.15.1) \quad N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$$

für gebrochene Ideale $\mathfrak{a}, \mathfrak{b} \subseteq K$. Ist nun $\mathfrak{a} \subseteq \mathcal{O}_K$, so gilt mit den obigen Bezeichnungen $n_i \geq 0$ für alle i , und der chinesische Restsatz liefert einen Isomorphismus

$$\mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^r \mathcal{O}_K/\mathfrak{p}_i^{n_i},$$

da die \mathfrak{p}_i nach Voraussetzung paarweise teilerfremd sind. Hieraus folgt

$$|\mathcal{O}_K/\mathfrak{a}| = \prod_{i=1}^r |\mathcal{O}_K/\mathfrak{p}_i^{n_i}|,$$

und es genügt, die Gleichung

$$(10.15.2) \quad |\mathcal{O}_K/\mathfrak{p}^n| = N(\mathfrak{p})^n$$

für jedes Primideal $\mathfrak{p} \subseteq \mathcal{O}_K$ und jedes $n \geq 0$ zu zeigen. Wir verwenden Induktion über n . Die Aussage ist trivial für $n = 0$ und gilt nach Definition für $n = 1$. Ist $n > 1$, so haben wir eine exakte Sequenz

$$0 \rightarrow \mathfrak{p}^{n-1}/\mathfrak{p}^n \rightarrow \mathcal{O}_K/\mathfrak{p}^n \rightarrow \mathcal{O}_K/\mathfrak{p}^{n-1} \rightarrow 0,$$

und nach dem Beweis von 5.10 einen Isomorphismus

$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{n-1}/\mathfrak{p}^n.$$

Mit der Induktionsvoraussetzung folgt

$$|\mathcal{O}_K/\mathfrak{p}^n| = |\mathfrak{p}^{n-1}/\mathfrak{p}^n| \cdot |\mathcal{O}_K/\mathfrak{p}^{n-1}| = N(\mathfrak{p})N(\mathfrak{p})^{n-1}$$

und damit (10.15.2) für n .

2) Ist nun $\alpha \in \mathcal{O}_K \setminus \{0\}$, so ist die Abbildung

$$\begin{aligned} \alpha & : \mathcal{O}_K & \rightarrow & \mathcal{O}_K \\ & x & \mapsto & \alpha x \end{aligned}$$

\mathbb{Z} -linear, und wird mittels einer \mathbb{Z} -Basis von $\mathcal{O}_K \cong \mathbb{Z}^n$ durch eine Matrix $U_\alpha \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$ repräsentiert. Nach Lemma 10.9 gilt

$$|\mathcal{O}_K/(\alpha)| = |\mathcal{O}_K/\alpha\mathcal{O}_K| = |\det(U_\alpha)|.$$

Andererseits ist U_α auch die Matrix der \mathbb{Q} -linearen Abbildung

$$\begin{aligned} \alpha &: K \rightarrow K \\ x &\mapsto x \end{aligned}$$

(bezüglich derselben Basis), und nach Definition gilt

$$N_{K/\mathbb{Q}}(\alpha) = \det(U_\alpha).$$

Dies zeigt die zweite Behauptung von 10.15 für α . Ist nun $\alpha \in K^\times$ beliebig und $\alpha = \beta/\gamma$ mit $\beta, \gamma \in \mathcal{O}_K \setminus \{0\}$, so folgt mit (10.15.1)

$$N((\alpha)) = \frac{N((\beta))}{N((\gamma))} = \frac{|N_{K/\mathbb{Q}}(\beta)|}{|N_{K/\mathbb{Q}}(\gamma)|} = N_{K/\mathbb{Q}}(\alpha),$$

wobei die letzte Gleichung wegen der Multiplikativität von $N_{K/\mathbb{Q}}$ gilt.

Mit Lemma 10.6 folgt nun leicht aus Proposition 10.14

Corollar 10.16 Jedes gebrochene Ideal $\mathfrak{a} \subseteq K$ ist (vermöge j) ein vollständiges Gitter in $V(K)$, und es gilt

$$\text{vol}(\mathfrak{a}) = \sqrt{|d_K|} N(\mathfrak{a}).$$

Bemerkung 10.17 Identifizieren wir

$$\begin{aligned} \mathbb{C} &\xrightarrow{\sim} \mathbb{R}^2 \\ z &\mapsto (\text{Re}z, \text{Im}z), \end{aligned}$$

so lautet die Einbettung j

$$\begin{aligned} j &: K \hookrightarrow \mathbb{R}^{r+2s} = \mathbb{R}^n \\ \alpha &\mapsto (\rho_1\alpha, \dots, \rho_r\alpha, \text{Re}(\sigma_1\alpha), \text{Im}(\sigma_1\alpha), \text{Re}(\sigma_2\alpha), \dots, \text{Re}(\sigma_s\alpha), \text{Im}(\sigma_s\alpha)). \end{aligned}$$

So wird die Einbettung bei Minkowski und in vielen Zahlentheorie-Büchern geschrieben, wobei dann die Standard-euklidische Norm auf \mathbb{R}^n gewählt wird, nämlich

$$\langle x, y \rangle_E = \sum_{i=1}^n x_i y_i.$$

Diese liefert das übliche Lebesgue-Maß vol_L auf \mathbb{R}^n . Unsere Metrik liefert

$$\langle x, y \rangle = \sum_{i=1}^n a_i x_i y_i$$

mit $a_i = 1$ für $i = 1, \dots, r$ und $a_i = 2$ für $i > r$.

Da dieses Skalarprodukt durch Transformation mit der Matrix

$$\left(\begin{array}{cccc} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \sqrt{2} \\ & & & & \ddots \\ & & & & & \sqrt{2} \end{array} \right) \left. \begin{array}{l} \vphantom{\left(} \right\} r \\ \vphantom{\left(} \right\} 2s \end{array} \right.$$

erhalten wird, gilt

$$\text{vol}(M) = 2^s \cdot \text{vol}_L(M).$$

11 Die Klassengruppe

Sei wieder K ein Zahlkörper, $n = [K : \mathbb{Q}]$.

Proposition 11.1 In jedem Ideal $\mathfrak{a} \neq 0$ von \mathcal{O}_K gibt es ein Element $\alpha \neq 0$ mit

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M \cdot N(\mathfrak{a}),$$

wobei

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

die **Minkowski-Schranke** ist (und $s = s(K)$ die Anzahl der Paare komplexer Einbettungen).

Beweis Wir wenden den Gitterpunktsatz an, wobei wir die Menge

$$M_c := M_c^{r,s} := \left\{ x \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^r |x'_i| + \sum_{j=1}^s 2 \cdot |x''_j| \leq c \right\}$$

für ein reelles $c > 0$ betrachten.

1) Wie in der Analysis bewiesen wird, gilt die Ungleichung zwischen arithmetischem und geometrischem Mittel von n nicht-negativen Zahlen.

$$\frac{1}{n} \sum_{i=1}^n a_i \geq \left(\prod_{i=1}^n a_i \right)^{\frac{1}{n}}$$

2) Hieraus folgt $\frac{1}{n} \|x\|_1 \geq \|x\|^{\frac{1}{n}}$ für

$$\begin{aligned} \|x\|_1 &= \sum_{i=1}^r |x'_i| + \sum_{j=1}^s 2|x''_j| && \text{und} \\ \|x\| &= \prod_{i=1}^r |x'_i| \cdot \prod_{j=1}^s |x''_j|^2. \end{aligned}$$

Für $\alpha \in K^\times$ gilt aber

$$(11.1.1) \quad \|j(\alpha)\| = \left| \prod_{\tau: K \hookrightarrow \mathbb{C}} \tau(\alpha) \right| = |N_{K/\mathbb{Q}}(\alpha)|.$$

Für $\alpha \in K^\times \cap M_c$ ist also

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{c}{n}\right)^n.$$

3) M_c ist zentralsymmetrisch (klar!) und konvex, denn $\|x\|_1$ erfüllt die Dreiecksungleichung $\|x+y\|_1 \leq \|x\|_1 + \|y\|_1$ und die Beziehung $\|t \cdot x\|_1 = t \cdot \|x\|_1$ für $t \geq 0$. Damit folgt: Sind $x, y \in M$, also $\|x\|_1, \|y\|_1 \leq c$, so gilt für $t \in [0, 1]$

$$\|(1-t)x + ty\|_1 \leq (1-t)\|x\|_1 + t\|y\|_1 \leq (1-t) \cdot c + tc = c,$$

also $(1-t)x + ty \in M_c$.

4) *Behauptung:* $\text{vol}(M_c) = 2^r \cdot \pi^s \cdot \frac{c^n}{n!}$.

Beweis: Sei $V^{r,s}(c) = \text{vol}(M_c^{r,s})$ für $r, s \in \mathbb{N}_0$, wobei wir $V^{0,0}(c) := 1$ setzen. Offenbar ist $V^{r,s}(c) = c^{r+2s} \cdot V^{r,s}(1)$. Wir führen Induktion über r und s . Für $r > 0$ ist

$$\begin{aligned} V_{r,s}(1) &= 2 \cdot \int_0^1 V_{r-1,s}(1-t) dt \\ &= 2 \cdot V_{r-1,s}(1) \cdot \int_0^1 (1-t)^{r-1+2s} dt = \frac{2}{r+2s} \cdot V_{r-1,s}(1); \end{aligned}$$

es genügt also, $V_{0,s}(1)$ zu berechnen. Für $s > 0$ ist hier

$$\begin{aligned} V_{0,s}(1) &= 2 \cdot \int_{x^2+y^2 \leq \frac{1}{4}} V_{0,s-1}(1-2\sqrt{x^2+y^2}) dx dy \\ &= 2 \cdot V_{0,s-1}(1) \cdot \int_0^{\frac{1}{2}} \int_0^{2\pi} (1-2r)^{2(s-1)} r dr d\varphi \quad (\text{Polarkoordinaten}) \\ &= 2 \cdot V_{0,s-1}(1) 2\pi \int_0^{\frac{1}{2}} \frac{1}{2} u^{2(s-1)} \frac{1}{2} (1-u) du \quad (u = 1-2r) \\ &= 2 \cdot V_{0,s-1}(1) \cdot \frac{\pi}{2} \cdot \left(\frac{1}{2s-1} - \frac{1}{2s}\right) = V_{0,s-1}(1) \pi \frac{1}{(2s-1)(2s)}, \end{aligned}$$

so dass die Behauptung induktiv folgt.

5) Wir benötigen die folgende Verschärfung des Gitterpunktsatzes:

Satz 11.2 Ist V ein euklidischer Vektorraum der Dimension n und $\Lambda \subseteq V$ ein vollständiges Gitter und $M \subseteq V$ kompakt, so gibt es einen Punkt in $\Lambda \setminus \{0\} \cap M$, wenn

$$\text{vol}(M) = 2^n \cdot \text{vol}(\Lambda).$$

Beweis (vergleiche Übungsaufgabe 36) Für jedes $m \in \mathbb{N}$ ist $\text{vol}((1 + \frac{1}{m}) \cdot M) = (1 + \frac{1}{m})^n \cdot \text{vol}(M) > 2^n \cdot \text{vol}(\Lambda)$, und es gibt nach dem Gitterpunktsatz 10.11 ein $\lambda_m \in \Lambda \setminus \{0\}$,

$\lambda_m \in (1 + \frac{1}{m}) \cdot M$. Die Folge der λ_m liegt in Λ und in der beschränkten Menge $2 \cdot M$, nimmt also nur endlich viele Werte an. Es gibt also ein $\lambda = \lambda_{m_0} \in \Lambda$ mit $\lambda \in \bigcap_{m \geq 1} (1 + \frac{1}{m})M = \overline{M} = M$.

6) Da M_c kompakt ist, gibt es nach 11.2 also ein $\alpha \in \mathfrak{a} \setminus \{0\}$ mit $\alpha \in M_c$, wenn

$$2^r \cdot \pi^s \frac{c^n}{n!} = \text{vol}(\mathfrak{a}) = 2^n \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a}).$$

Für dieses c und α ist nach 2)

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{c}{n}\right)^n = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a}).$$

Damit ist Proposition 11.1 bewiesen.

Corollar 11.3 In jeder Idealklasse, d.h., jedem Element der Klassengruppe $Cl_K = I_K/P_K$ gibt es ein ganzes Ideal \mathfrak{a} mit

$$N(\mathfrak{a}) \leq M = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

Beweis Sei \mathfrak{b} ein beliebiger Repräsentant der Klasse, und sei $\gamma \in \mathcal{O}_K$ mit $\mathfrak{c} = \gamma \cdot \mathfrak{b}^{-1} \subseteq \mathcal{O}_K$. Nach 11.1 gibt es dann ein $\alpha \in \mathfrak{c} \setminus \{0\}$ ($\Leftrightarrow \mathfrak{c} \mid (\alpha)$) mit

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M \cdot N(\mathfrak{c}) = M \cdot |N_{K/\mathbb{Q}}(\gamma)| \cdot N(\mathfrak{b}^{-1}).$$

Das Ideal $\mathfrak{a} = \alpha \cdot \mathfrak{c}^{-1} = \alpha \gamma^{-1} \cdot \mathfrak{b}$ ist dann ganz (wegen $\mathfrak{c} \mid (\alpha)$) mit $N(\mathfrak{a}) \leq M$.

Lemma 11.4 Es gibt nur endlich viele *ganze* Ideale $\mathfrak{a} \subseteq \mathcal{O}_K$ mit beschränkter Norm.

Beweis Ist $N(\mathfrak{a}) = p_1^{n_1} \dots p_r^{n_r}$, so gibt es nur endlich viele Möglichkeiten für die n_i und die p_i , und über letzteren liegen nur endlich viele Primideale in K ; insgesamt gibt es also nur endlich viele Möglichkeiten für die Primzerlegung von \mathfrak{a} .

Corollar 11.5 Für jeden Zahlkörper K ist die Klassengruppe Cl_K endlich.

Beweis: Nach 11.3 und 11.4 gibt es endlich viele Ideale, die alle Idealklassen repräsentieren.

Corollar 11.3 liefert nicht nur das qualitative Ergebnis 11.5 der Endlichkeit von Cl_K , sondern auch ein konstruktives Verfahren zur Berechnung von Cl_K , da man nur endlich viele Primideale untersuchen muss:

Beispiel 11.6 (a) Für den imaginär-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{-7})$ ist $d_K = -7$. Jede Idealklasse enthält also ein ganzes Ideal \mathfrak{a} mit Norm

$$N\mathfrak{a} := N(\mathfrak{a}) \leq \frac{2!}{4} \cdot \frac{4}{\pi} \cdot \sqrt{7} = 1,68\dots,$$

also das triviale Ideal \mathcal{O}_K . K hat also die Klassenzahl 1.

(b) Für den imaginär-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{-5})$ ist $d_K = -20$. Jede Idealklasse enthält also ein ganzes Ideal \mathfrak{a} mit Norm

$$N\mathfrak{a} \leq \frac{2!}{4} \cdot \frac{4}{\pi} \sqrt{20} = 2,84\dots,$$

also mit Norm ≤ 2 . Die Klassengruppe wird also von den Primidealen über 2 erzeugt. Wir wenden wie üblich Satz 5.6 zur Bestimmung der Primideale über 2 an. Es ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ und $x^2 + 5 \equiv x^2 + 1 \equiv (x + 1)^2 \pmod{2}$, also nach 5.6

$$2 \cdot \mathcal{O}_K = (2, \sqrt{-5} + 1)^2$$

die Primzerlegung von 2 in K . Damit erzeugt $\mathfrak{p} = (2, \sqrt{-5} + 1)$ die Klassengruppe, und \mathfrak{p}^2 ist prinzipal, d.h., trivial in der Klassengruppe. Aber \mathfrak{p} selbst ist kein Hauptideal: Angenommen $\mathfrak{p} = (\alpha)$, so wäre nach 10.15 $|N_{K/\mathbb{Q}}(\alpha)| = N\mathfrak{p} = 2$, also $N_{K/\mathbb{Q}}(\alpha) = \pm 2$. Schreiben wir

$$\alpha = a + b\sqrt{-5} \quad , \quad a, b \in \mathbb{Z},$$

so erhalten wir

$$a^2 + 5b^2 = \pm 2,$$

was nicht möglich ist. Die Klassenzahl von K ist also 2.

Bemerkung 11.7 Es wurde bereits von Gauss (1777-1855) vermutet, aber erst von Heegner (1952), Baker (1966) und Stark (1967) bewiesen, dass es genau 9 imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit Klassenzahl 1 gibt, nämlich für $d = -1, -2, -3, -7, -11, -19, -43, -67$ und -163 . Es wird vermutet, dass es unendlich viele reell-quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit Klassenzahl 1 gibt (es gibt 38 für $2 \leq d \leq 100$: $d = 2, 3, 5, 6, 7, 11, \dots, 93, 94, 97$); man weiss aber noch nicht einmal, ob es überhaupt unendlich viele Zahlkörper K mit Klassenzahl 1 gibt.

Satz 11.8 Für jeden Zahlkörper $K \neq \mathbb{Q}$ ist $|d_K| > 1$.

Beweis Aus 11.1 folgt für $\mathfrak{a} = \mathcal{O}_K$

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

also

$$\sqrt{|d_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{\frac{n}{2}} =: a_n,$$

wegen $\frac{\pi}{4} < 1$ und $\frac{n}{2} \geq s$. Wegen $a_2 = \frac{\pi}{2} > 1$ und

$$\frac{a_{n+1}}{a_n} = \left(1 + \frac{1}{n}\right)^n \cdot \left(\frac{\pi}{4}\right)^{\frac{1}{2}} > 1 \quad \text{für } n \geq 2$$

ist aber $a_n > 1$ für alle $n \geq 2$, also $\sqrt{|d_K|} > 1$.

Bemerkung 11.9 Wir werden später hieraus ableiten, dass es keine unverzweigte (d.h., für alle Primideale unverzweigte) Erweiterung K/\mathbb{Q} außer $K = \mathbb{Q}$ gibt. Für beliebige Zahlkörper K gibt es im Allgemeinen unverzweigte Erweiterungen L/K . Ist H/K die maximale abelsche,

unverzweigte Erweiterung, so zeigt man zum Beispiel in der **Klassenkörpertheorie**, dass es einen Isomorphismus

$$\begin{aligned} Cl_K &\xrightarrow{\sim} Gal(H/K) \\ [\mathfrak{p}] &\longmapsto Fr_{\mathfrak{p}} \end{aligned}$$

gibt (das ‘‘Hilbert-Artin’sche Reziprozitatsgesetz’’); insbesondere ist H/K endlich und im allgemeinen nicht-trivial.

12 Die Einheitengruppe

Sei wieder K ein Zahlkorper, $n = [K : \mathbb{Q}]$, $r = r(K)$ die Anzahl der reellen Einbettungen und $s = s(K)$ die Anzahl der Paare konjugierter komplexer Einbettungen. Wir wollen \mathcal{O}_K^\times , die Gruppe der Einheiten in \mathcal{O}_K , studieren.

Die Einbettung von Ringen (!)

$$\begin{aligned} j : \mathcal{O}_K &\rightarrow \mathbb{R}^r \times \mathbb{C}^s \\ \alpha &\mapsto (\rho_1\alpha, \dots, \rho_r\alpha, \sigma_1\alpha, \dots, \sigma_s\alpha) \end{aligned}$$

induziert einen injektiven Gruppenhomomorphismus

$$j : \mathcal{O}_K^\times \hookrightarrow (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s.$$

(beachte: $\mathcal{O}_K^\times \subsetneq \mathcal{O}_K \setminus \{0\}$; z.B. $\mathbb{Z}^\times = \{\pm 1\} \subsetneq \mathbb{Z} \setminus \{0\}$, aber $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$).

Weiter haben wir einen Gruppenhomomorphismus

$$\begin{aligned} \ell : (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s &\longrightarrow (\mathbb{R}_+^\times)^{r+s} \xrightarrow[\sim]{\log} \mathbb{R}^{r+s} \\ (x_i) &\longmapsto (||x_i||) \longmapsto (\log ||x_i||), \end{aligned}$$

wobei $||x_i||$ die Absolutnorm ist: $||x_i|| = |x_i|$ fur $x_i \in \mathbb{R}$ und $||x_i|| = |N_{\mathbb{C}/\mathbb{R}}(x_i)| = |x_i\bar{x}_i| = |x_i|^2$ fur $x_i \in \mathbb{C}$. Durch Komposition erhalten wir

$$\begin{aligned} \lambda = \ell \circ j : \mathcal{O}_K^\times &\longrightarrow \mathbb{R}^{r+s} \\ \alpha &\longmapsto (\log ||\rho_1\alpha||, \dots, \log ||\rho_r\alpha||, \log ||\sigma_1\alpha||, \dots, \log ||\sigma_s\alpha||) \end{aligned}$$

Lemma 12.1 $\ker \lambda = \mu(K)$, die Gruppe der Einheitswurzeln in K .

Beweis Dies folgt sofort aus Lemma 7.6, denn es gilt $\alpha \in \ker \lambda \Leftrightarrow |\rho\alpha| = 1$ fur alle Einbettungen $\rho : K \hookrightarrow \mathbb{C}$.

Lemma 12.2 $\lambda(\mathcal{O}_K^\times) \subseteq H = \{x \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r+s} x_i = 0\}$.

Beweis Es ist für $\alpha \in \mathcal{O}_K^\times$ und $x = \lambda(\alpha)$

$$\begin{aligned} \sum_{i=1}^{r+s} \log \|x_i\| &= \log \prod_{i=1}^{r+s} \|x_i\| \\ &= \log \left(\prod_{i=1}^r |\rho_i \alpha| \cdot \prod_{i=1}^s |\sigma_i \alpha \bar{\sigma}_i \alpha| \right) \\ &= \log \left(\left| \prod_{\tau: K \hookrightarrow \mathbb{C}} \tau \alpha \right| \right) = \log(|N_{K/\mathbb{Q}}(\alpha)|) = 0, \end{aligned}$$

da $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ für eine Einheit α .

Proposition 12.3 $\lambda(\mathcal{O}_K^\times)$ ist ein vollständiges Gitter im $(r + s - 1)$ -dimensionalen \mathbb{R} -Vektorraum H , insbesondere also ein freier \mathbb{Z} -Modul vom Rang $r + s - 1$.

Beweis 1) Nach der Rangformel für die surjektive lineare Abbildung $\sum : \mathbb{R}^{r+s} \rightarrow \mathbb{R}$, $x \mapsto \sum x_i$, ist $H = \ker \sum$ ein Untervektorraum der Dimension $r + s - 1$.

2) $\lambda(\mathcal{O}_K^\times)$ ist Gitter: es genügt zu zeigen, dass die beschränkte Menge

$$K_\varepsilon = \{(x_i) \in \mathbb{R}^{r+s} \mid |x_i| \leq \varepsilon \text{ für alle } i\}$$

für jedes $\varepsilon > 0$ nur endlich viele Elemente von $\lambda(\mathcal{O}_K^\times)$ enthält: ist dann ε' kleiner als jedes $|x_i| \neq 0$ für diese Punkte, so ist $K_{\varepsilon'} \cap \lambda(\mathcal{O}_K^\times) = \{0\}$, und durch Translation sieht man, dass jeder Punkt von $\lambda(\mathcal{O}_K^\times)$ diskret in \mathbb{R}^{r+s} liegt.

Das Urbild von K_ε unter ℓ ist aber die kompakte Menge

$$\{x \in \mathbb{R}^r \times \mathbb{C}^s \mid e^{-\varepsilon} \leq \|x_i\| \leq e^\varepsilon\},$$

die nur endlich viele Elemente von \mathcal{O}_K , also erst recht von \mathcal{O}_K^\times enthält.

3) $\Lambda = \lambda(\mathcal{O}_K^\times)$ ist vollständiges Gitter in H : Nach 10.4 genügt es zu zeigen, dass es eine beschränkte Menge $M \subseteq H$ gibt mit

$$(12.3.1) \quad \bigcup_{\mu \in \Lambda} \mu + M = H.$$

Wir betrachten dazu den surjektiven Homomorphismus

$$S = \{x \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \mid \|x\| = \prod_{i=1}^{r+s} \|x_i\| = 1\} \xrightarrow{\ell} H,$$

und konstruieren eine beschränkte Menge $N \subseteq S$ mit

$$(12.3.2) \quad \bigcup_{\alpha \in \mathcal{O}_K^\times} j(\alpha) \cdot N = S$$

(Beachte: Wegen $\|j(\alpha)\| = |N_{K/\mathbb{Q}}(\alpha)|$, siehe (11.1.1), und $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ für $\alpha \in \mathcal{O}_K^\times$ gilt $j(\mathcal{O}_K^\times) \subseteq S$). Setzen wir $M = \ell(N)$, so ist M ebenfalls beschränkt (wegen $\prod \|x_i\| = 1$ sind die Beträge $\|x_i\|$ sowohl nach oben als auch nach unten beschränkt, also auch $\log \|x_i\|$) und es gilt (12.3.1).

Zur Konstruktion von N fixieren wir ein Tupel $c = (c_1, \dots, c_{r+s})$ von Zahlen $c_i > 0$ und betrachten

$$N_c = \{x \in V(K) = \mathbb{R}^r \times \mathbb{C}^s \mid |x_i| \leq c_i \text{ für alle } i\}.$$

Dann ist N_c zentralsymmetrisch, konvex, mit Volumen

$$(12.3.3) \quad \begin{aligned} \text{vol}(N_c) &= 2^s \cdot \text{vol}_L(N_c) = 2^s \cdot \prod_{i=1}^r 2c_i \cdot \prod_{i=r+1}^{r+s} \pi c_i^2 \\ &= 2^{r+s} \cdot \pi^s \cdot \|c\|, \end{aligned}$$

wobei $\|x\| = \prod_{i=1}^r |x_i| \prod_{j=r+1}^{r+s} |x_j|^2$ wie oben.

Sei nun c so gewählt, dass

$$\text{vol}(N_c) > 2^n \cdot \text{vol}(\mathcal{O}_K),$$

d.h., nach (12.3.3) und Proposition 10.14, mit

$$\|c\| > \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|}.$$

Nach dem Gitterpunktsatz gibt es dann ein $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit $j\alpha \in N_c$. Für dieses α gilt

$$|N_{K/\mathbb{Q}}(\alpha)| = \|j\alpha\| \leq \|c\|.$$

Es gibt also nur endlich viele Möglichkeiten für $N_{K/\mathbb{Q}}(\alpha)$.

Wir bemerken nun

Lemma 12.4 Bis auf Assoziierte gibt es nur endlich viele $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit vorgegebener Norm $N_{K/\mathbb{Q}}(\alpha) = a \in \mathbb{Z} \setminus \{0\}$.

Beweis Da zwei Elemente $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ genau dann assoziiert sind, wenn $(\alpha) = (\beta)$ für die zugehörigen Hauptideale, folgt die Behauptung aus der entsprechenden Tatsache für Ideale (Lemma 11.4).

Es gibt also endlich viele Zahlen $\alpha_1, \dots, \alpha_m \in \mathcal{O}_K \setminus \{0\}$, so dass jedes $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit $|N_{K/\mathbb{Q}}(\alpha)| \leq \|c\|$ zu einem der Elemente α_i assoziiert ist. Wir behaupten nun, dass wir die Menge

$$N = \left(\bigcup_{i=1}^m j(\alpha_i)^{-1} \cdot N_c \right) \cap S$$

für (12.3.2) nehmen können. Offenbar ist N beschränkt. Sei nun $y \in S$. Dann ist im Ring $V(K)$

$$\begin{aligned} y^{-1}N_c &= \{y^{-1}x \in V(K) \mid |x_i| \leq c_i \forall i\} \\ &= \{z \in V(K) \mid |z_i| \leq |y_i|^{-1} \cdot c_i \forall i\} \\ &= N_{|y|^{-1}c} \end{aligned}$$

(wobei $|y|^{-1}c = (|y_1|^{-1}c_1, \dots, |y_{r+s}|^{-1}c_{r+s})$), und wegen $\|y\| = 1$ auch

$$\text{vol}(N_{|y|^{-1}c}) = 2^{r+s} \cdot \pi^s \cdot \| |y|^{-1}c \| = 2^{r+s} \pi^s \|c\| = \text{vol}(N_c) > 2^s \cdot \text{vol}(\mathcal{O}_k).$$

Es gibt also nach dem Gitterpunktsatz ein $\beta \in \mathcal{O}_K \setminus \{0\}$ mit $j(\beta) \in y^{-1}N_c$. Weiter gilt

$$|N_{K/\mathbb{Q}}(\beta)| = \|j(\beta)\| \leq \|y^{-1}c\| = \|c\|.$$

Es gibt also ein α_i ($1 \leq i \leq m$) und eine Einheit $u \in \mathcal{O}_K^\times$ mit $\beta = u \cdot \alpha_i$. Zusammen folgt

$$y \in S \cap j(\beta)^{-1}N_c = S \cap j(u)^{-1}j(\alpha_i)^{-1}N_c.$$

Da y beliebig war, und $j(u) \in S$, folgt

$$S = \bigcup_{u \in \mathcal{O}_K^\times} j(u) \cdot N$$

q.e.d.

Corollar 12.5 (Dirichletscher Einheitensatz) Die Einheitengruppe \mathcal{O}_K^\times von K ist eine endlich erzeugte abelsche Gruppe vom Rang $r + s - 1$. Genauer gibt es einen Isomorphismus

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1},$$

d.h., es gibt Einheiten $\varepsilon_1, \dots, \varepsilon_{r+s-1}$, so dass jede Einheit $\varepsilon \in \mathcal{O}_K^\times$ eine eindeutige Darstellung

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

mit einer Einheitswurzel ζ und $n_1, \dots, n_{r+s-1} \in \mathbb{Z}$ besitzt. Ein solches System $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ heißt ein **System von Grundeinheiten** (für K).

Beweis Nach 12.1 und 12.3 haben wir eine exakte Sequenz

$$0 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \lambda(\mathcal{O}_K^\times) \rightarrow 0$$

mit $\lambda(\mathcal{O}_K^\times) \cong \mathbb{Z}^{r+s-1}$. Ist $\overline{\varepsilon}_1, \dots, \overline{\varepsilon}_{r+s-1}$ eine \mathbb{Z} -Basis von $\lambda(\mathcal{O}_K^\times)$ und sind $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ Urbilder in \mathcal{O}_K^\times , so leisten diese das Gewünschte.

Beispiel 12.6 Ist $K = \mathbb{Q}(\sqrt{-d})$, ($d > 0$), ein imaginärer quadratischer Zahlkörper, so ist $r = 0$ und $s = 1$, also $\mathcal{O}_K^\times = \mu(K)$ die Gruppe der Einheitswurzeln (vergleiche den Fall $\mathbb{Q}(\sqrt{-1})$ in §1). Für eine Primzahl p gilt wegen $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ und $\mu_3 \subseteq \mathbb{Q}(\sqrt{-3})$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-p})}^\times = \begin{cases} \mu_6 & , \quad p = 3 \\ \mu_2 & , \quad \text{sonst.} \end{cases}$$

Beispiel 12.7 (a) Für einen reell-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ ($d > 0$) gilt $r = 2, s = 0$, also

$$(12.7.1) \quad \mathcal{O}_K^\times = \mu_2 \times \mathbb{Z}.$$

(b) Ist ε_1 eine Grundeinheit, so sind $\varepsilon_1^{-1}, -\varepsilon_1$ und $-\varepsilon_1^{-1}$ die anderen möglichen Grundeinheiten. Fixieren wir eine Einbettung $\sigma : \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{R}$, so gibt es unter diesen vier Grundeinheiten genau eine Grundeinheit ε mit $\sigma(\varepsilon) > 1$ (für die anderen ε' gilt offenbar $\sigma(\varepsilon') < 1$). Wir nennen ε die **Grundeinheit des eingebetteten reell quadratischen Zahlkörpers K** .

Identifizieren wir zum Beispiel \sqrt{d} mit der positiven reellen Wurzel, so gilt $\varepsilon = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$, $x, y > 0$, und es ist $\{\varepsilon, \varepsilon^{-1}, -\varepsilon, -\varepsilon^{-1}\} = \{\pm x \pm y\sqrt{d}\}$.

(c) Nach Lemma 3.15 liegt ein Element α in einem Zahlkörper L genau dann in \mathcal{O}_L^\times , wenn $\alpha \in \mathcal{O}_L$ und $N_{L/\mathbb{Q}}(\alpha) \in \{\pm 1\}$. Für $K = \mathbb{Q}(\sqrt{d})$ erhalten wir: Ist $d \equiv 2, 3 \pmod{4}$, so ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, und die Einheiten in \mathcal{O}_K^\times sind die Zahlen $a + b\sqrt{d}$, wobei $(a, b) \in \mathbb{Z}^2$ eine Lösung der **Pellschen Gleichung** (oder Gleichung von Pell-Fermat)

$$(12.7.2) \quad a^2 - db^2 = \pm 1$$

ist.

Für $d \equiv 1 \pmod{4}$ ist $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, und \mathcal{O}_K^\times besteht aus den Zahlen $\alpha = \frac{1}{2}(a + b\sqrt{d})$ mit $(a, b) \in \mathbb{Z}^2$ eine Lösung der Gleichung

$$(12.7.3) \quad a^2 - db^2 = \pm 4$$

(Für solche (a, b) ist $Tr_{K/\mathbb{Q}}(\alpha) = a \in \mathbb{Z}$ und $N_{K/\mathbb{Q}}(\alpha) = \pm 1 \in \mathbb{Z}$, also $\alpha \in \mathcal{O}_K$; siehe Satz 2.11).

(d) Ist $d \equiv 2, 3 \pmod{4}$, $\sqrt{d} \in \mathbb{R}_+$ und $\varepsilon_1 = a_1 + b_1\sqrt{d}$ mit $a_1, b_1 \in \mathbb{N}$ die Grundeinheit von $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$, so sind wegen (12.7.1) alle Lösungen $(a, b) \in \mathbb{N}^2$ der Pellschen Gleichung (12.7.2) durch die Paare (a_n, b_n) mit $n \in \mathbb{N}$ und

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

gegeben. Die einfach zu berechnende Grundeinheit ε_1 kann also benutzt werden, um alle Lösungen der Pellschen Gleichung (12.7.2) zu bestimmen.

(d) Analoges gilt für $d \equiv 1 \pmod{4}$,

$$\frac{a_n + b_n\sqrt{d}}{2} = \left(\frac{a_1 + b_1\sqrt{d}}{2} \right)^n$$

und die “modifizierte Pellsche Gleichung” (12.7.3).

Lemma/Definition 12.8 Sei $vol(\lambda(\mathcal{O}_K^\times))$ das Volumen des Gitters $\lambda(\mathcal{O}_K^\times) \subseteq H$, wobei wir auf H die Einschränkung des üblichen euklidischen Skalarprodukts von \mathbb{R}^{r+s} nehmen. Ist $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ ein System von Grundeinheiten, und

$$\lambda(\varepsilon_j) = (\lambda_1(\varepsilon_j), \dots, \lambda_{r+s}(\varepsilon_j)) = (\log |\rho_1(\varepsilon_j)|, \dots, \log |\rho_r(\varepsilon_j)|, 2 \log |\sigma_1(\varepsilon_j)|, \dots, 2 \log |\sigma_s(\varepsilon_j)|),$$

so ist

$$vol(\lambda(\mathcal{O}_K^\times)) = \sqrt{r+s} \cdot R_K,$$

wobei

$$\begin{aligned} R_K &= \left| \det \begin{pmatrix} \lambda_1(\varepsilon_1) & \dots & \lambda_1(\varepsilon_{r+s-1}) \\ \vdots & & \vdots \\ \lambda_{r+s-1}(\varepsilon_1) & \dots & \lambda_{r+s-1}(\varepsilon_{r+s-1}) \end{pmatrix} \right| \\ &= \left| \det \begin{pmatrix} \lambda_1(\varepsilon_1) & \dots & \lambda_1(\varepsilon_{r+s-1}) \\ \widehat{\lambda_i(\varepsilon_1)} & \dots & \widehat{\lambda_i(\varepsilon_{r+s-1})} \\ \lambda_{r+s}(\varepsilon_1) & \dots & \lambda_{r+s}(\varepsilon_{r+s-1}) \end{pmatrix} \right| \end{aligned}$$

der **Regulator** des Zahlkörpers K ist. Hier ist die zweite Matrix der $(r + s - 1) \times (r + s - 1)$ -Minor der Matrix $(\lambda_i(\varepsilon_j))$, der durch Weglassen der i -ten Zeile erhalten wird. (i beliebig). Insbesondere hängt R_K nicht von der Wahl des Grundeinheitensystems oder der Nummerierung der Einbettungen ab.

Beweis Es ist

$$\text{vol}(\lambda(\mathcal{O}_K^\times)) = \text{vol}_{r+s-1}(M_{(\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_{r+s-1}))}),$$

wobei $M_{(v_1, \dots, v_{r+s-1})}$ das von v_1, \dots, v_{r+s-1} aufgespannte Parallelepiped ist. Der Vektor $v = \frac{1}{\sqrt{r+s}}(1, \dots, 1) \in \mathbb{R}^{r+s}$ steht senkrecht auf H und hat die Länge 1. Daher ist

$$\text{vol}_{r+s-1}(M_{(\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_{r+s-1}))}) = \text{vol}_{r+s}(M_{(\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_{r+s-1}), v)}).$$

Letzteres ist in \mathbb{R}^{r+s} mit dem Standardvolumen gleich dem Determinantenbetrag der Matrix

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \dots & \lambda_1(\varepsilon_{r+s-1}) & \frac{1}{\sqrt{r+s}} \\ \lambda_{r+s}(\varepsilon_1) & \dots & \lambda_{r+s}(\varepsilon_{r+s-1}) & \frac{1}{\sqrt{r+s}} \end{pmatrix}$$

(dies folgt z.B. aus der Transformationsformel). Addieren wir zur i -ten Zeile die restlichen Zeilen, so erhalten wir dort die Zeile $(0, \dots, 0, \frac{r+s}{\sqrt{r+s}})$, und die Behauptung folgt durch Entwicklung nach dieser Zeile.

Beispiel 12.9 Für einen reell-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, mit Grundeinheit ε_1 ist für eine beliebige Einbettung $\sigma : \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{R}$

$$R_K = |\log |\sigma(\varepsilon_1)||,$$

und dies ist gleich $\log \sigma(\varepsilon_1)$, wenn man die eindeutig bestimmte Grundeinheit ε_1 mit $\sigma(\varepsilon_1) > 1$ wählt.

Bemerkung 12.10 Die **Dedekind'sche Zetafunktion** eines Zahlkörpers K wird definiert als die für komplexe Zahlen s mit $\text{Re}(s) > 1$ konvergente Reihe

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{ganzes Ideal}}} \frac{1}{N\mathfrak{a}^s}.$$

Für $K = \mathbb{Q}$ ist dies gerade die **Riemannsche Zetafunktion**

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

Man kann zeigen, dass $\zeta_K(s)$ eine meromorphe Fortsetzung auf ganz \mathbb{C} besitzt, mit genau einem Pol bei $s = 1$. Dieser Pol ist von erster Ordnung, und man hat

$$\text{Res}_{s=1} \zeta_K(s) = \frac{[2^r (2\pi)^s]}{w \cdot \sqrt{|d_K|}} \cdot h \cdot R,$$

wobei $w = |\mu(K)|$ die Anzahl der in K enthaltenen Einheitswurzeln ist, $h = h_K = |Cl_K|$ die Klassenzahl und $R = R_K$ der oben definierte Regulator. Dies nennt man die **analytische Klassenzahlformel**.

Dies kann man zu Berechnungen benutzen, da man die linke Seite durch **Artin'sche L -Reihen** ausrechnen kann. Zum Beispiel erhält man so für einen reell-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ mit Diskriminanten-Betrag $D = |d_K|$ die Formel

$$h = \frac{1}{\log \varepsilon} \cdot \left| \sum_{\substack{k \in (\mathbb{Z}/D\mathbb{Z})^\times \\ k < D/2}} \chi(k) \log \sin \frac{k\pi}{D} \right|,$$

wobei $\chi(k) = \left(\frac{k}{D}\right)$ das sogenannte Jacobi-Symbol ist, und ε die Grundeinheit > 1 .

13 Lokalisierungen

Sei A ein Integritätsring mit Quotientenkörper K .

Lemma/Definition 13.1 (i) Eine Teilmenge $S \subseteq A \setminus \{0\}$ heißt **multiplikativ** (oder **multiplikativ abgeschlossen**), wenn $1 \in S$ und wenn für alle $a, b \in S$ auch ab in S liegt.

(ii) Sei $S \subseteq A \setminus \{0\}$ multiplikativ. Die Menge

$$S^{-1}A = \left\{ \frac{a}{s} \in K \mid a \in A, s \in S \right\}$$

heißt die Lokalisierung von A nach S und ist ein Unterring von K , der A enthält.

Beweis der Behauptungen: Für $a, a' \in A$ und $s, s' \in S$ gilt $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \in S^{-1}A$ und $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} \in S^{-1}A$. Weiter gilt $A \subseteq S^{-1}A$ wegen $1 \in S$.

Bemerkung 13.2 Die obigen Begriffe lassen sich auf beliebige kommutative Ringe mit Eins verallgemeinern (siehe Algebra II, §10), und die unten in 13.4 und 13.5 gezeigten Aussagen gelten dann entsprechend.

Definition 13.3 Für einen kommutativen Ring R mit Eins sei $Spec(R)$ die Menge aller Primideale von R , genannt das **Spektrum** von R .

Satz 13.4 Sei $S \subseteq A \setminus \{0\}$ multiplikativ und $A' = S^{-1}A$.

(a) Für jedes Ideal $\mathfrak{a}' \subseteq A'$ gilt $(\mathfrak{a}' \cap A)A' = \mathfrak{a}'$.

(b) Die Abbildung

$$\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$$

ist eine Inklusions-erhaltende Bijektion zwischen der Menge $Spec(A')$ und der Menge $M_S = \{\mathfrak{p} \in Spec(A) \mid \mathfrak{p} \cap S = \emptyset\}$. Die Umkehrabbildung ist $\mathfrak{p} \mapsto \mathfrak{p}A'$.

Beweis (a): Offenbar gilt $(\mathfrak{a}' \cap A)A' \subseteq \mathfrak{a}'$, da \mathfrak{a}' ein A' -Ideal ist. Umgekehrt sei $x \in \mathfrak{a}'$, etwa $x = \frac{a}{s}$ mit $a \in A$ und $s \in S$. Da \mathfrak{a}' ein Ideal ist und $A \subseteq A'$, ist $a = s \cdot \frac{a}{s} \in \mathfrak{a}' \cap A$ und daher $x = \frac{a}{s} = a \cdot \frac{1}{s} \in (\mathfrak{a}' \cap A)A'$.

(b): Da die Abbildung

$$A/(\mathfrak{p}' \cap A) \rightarrow A'/\mathfrak{p}'$$

injektiv ist, ist $A/(\mathfrak{p}' \cap A)$ nullteilerfrei; weiter ist $1 \notin \mathfrak{p}' \cap A$, und es folgt, dass $\mathfrak{p}' \cap A$ ein Primideal in A ist. Weiter gilt $\mathfrak{p}' \cap S = \emptyset$, denn wäre $s \in S \cap \mathfrak{p}'$, so wäre $1 = \frac{1}{s} \cdot s \in \mathfrak{p}'$ – Widerspruch! Also ist $\mathfrak{p} = \mathfrak{p}' \cap A$ ein Primideal mit $\mathfrak{p} \cap S = \emptyset$.

Sei umgekehrt $\mathfrak{p} \subseteq A$ ein Primideal mit $\mathfrak{p} \cap S = \emptyset$. Wir zeigen, dass $\mathfrak{p}' = \mathfrak{p}A'$ ein Primideal in A' ist und $\mathfrak{p} = \mathfrak{p}' \cap A$. Dann folgt die Behauptung, da die Abbildungen $\varphi : \mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ und $\psi : \mathfrak{p} \mapsto \mathfrak{p}A'$ (eingeschränkt auf M_S) nach dem Bewiesenen zueinander inverse Bijektionen sind.

Wir behaupten zuerst

$$\mathfrak{p}A' = \left\{ \frac{p}{s} \mid p \in \mathfrak{p}, s \in S \right\}.$$

Für die nicht-triviale Richtung sei nämlich $x \in \mathfrak{p}A'$; dann gilt

$$x = \sum_{i=1}^n \frac{a_i}{s_i} p_i \quad \text{mit } a_i \in A, s_i \in S, p_i \in \mathfrak{p},$$

und daher $x = \frac{p}{s}$ mit $s = s_1 \cdot \dots \cdot s_n \in S$ und

$$p = \sum_{i=1}^n b_i p_i \in \mathfrak{p}, \quad b_i = \frac{a_i s}{s_i} \in A.$$

Es folgt nun leicht, dass $1 \notin \mathfrak{p}A'$ (denn sonst wäre $1 = \frac{p}{s}$ mit $p \in \mathfrak{p}$ und $s \in S$ und $s = p \in \mathfrak{p} \cap S = \emptyset$ – Widerspruch!) und dass $\mathfrak{p}A'$ ein Primideal ist: Seien $\frac{a}{s}, \frac{b}{t} \in A'$ ($a, b \in A, s, t \in S$) mit $\frac{a}{s} \frac{b}{t} \in \mathfrak{p}A'$, also

$$\frac{ab}{st} = \frac{p}{u} \quad \text{mit } p \in \mathfrak{p} \text{ und } u \in S,$$

also $abu = pst \in \mathfrak{p}$. Wegen $\mathfrak{p} \cap S = \emptyset$ ist $u \notin \mathfrak{p}$, und es folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d.h., $a/s \in \mathfrak{p}A'$ oder $b/t \in \mathfrak{p}A'$.

Es bleibt noch $\mathfrak{p}A' \cap A = \mathfrak{p}$ zu zeigen. Für die nicht-triviale Inklusion sei $x \in \mathfrak{p}A' \cap A$, etwa $x = \frac{p}{s}$ mit $p \in \mathfrak{p}$ und $s \in S$. Es folgt $sx = p \in \mathfrak{p}$, wegen $S \cap \mathfrak{p} = \emptyset$ also $x \in \mathfrak{p}$.

Corollar 13.5 Ist A noethersch, so auch $A' = S^{-1}A$.

Beweis Nach 13.4 (a) ist die Abbildung

$$\mathfrak{a}' \mapsto \mathfrak{a}' \cap A$$

eine *Injektion* von der Menge der Ideale in A' in die Menge der Ideale von A . Es folgt, dass in A' die aufsteigende Kettenbedingung für Ideale (siehe Algebra I, Prop. 5.7) gilt, weil dies in A gilt.

Satz 13.6 Sei R ein Integritätsring, der A enthält, sei $S \subseteq A \setminus \{0\}$ eine multiplikative Teilmenge und B der ganze Abschluss von A in R . Dann ist $S^{-1}B$ der ganze Abschluss von $S^{-1}A$ in $S^{-1}R$.

Beweis Sei $\frac{b}{s} \in S^{-1}B$ ($b \in B, s \in S$) und sei

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0 \quad (a_i \in A)$$

eine Ganzheitsgleichung für b über A . Dann ist (Division durch s^n)

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_1}{s^{n-1}} \frac{b}{s} + \frac{a_0}{s^n} = 0$$

eine Ganzheitsgleichung für $\frac{b}{s}$ über $S^{-1}A$. Umgekehrt sei $\frac{x}{s} \in S^{-1}R$ ($x \in R, s \in S$) ganz über $S^{-1}A$ und

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}} \left(\frac{x}{s}\right)^{n-1} + \dots + \frac{a_1}{t_1} \frac{x}{s} + \frac{a_0}{t_0} = 0$$

eine entsprechende Ganzheitsgleichung, mit $a_i \in A, t_i \in S$. Dann folgt durch Multiplikation mit $(st_0t_1 \cdots t_{n-1})^n$, dass $xt_0 \cdots t_{n-1} \in R$ ganz über A ist, also in B liegt. Damit folgt

$$\frac{x}{s} = \frac{xt_0 \cdots t_{n-1}}{st_0 \cdots t_{n-1}} \in S^{-1}B.$$

Corollar 13.7 Ist A ganz abgeschlossen, so auch $S^{-1}A$ für jede multiplikative Teilmenge $S \subseteq A \setminus \{0\}$.

Beweis: Anwendung von 13.6 auf $R = K = \text{Quot}(A)$.

Satz 13.8 Ist A ein Dedekindring, so auch jede Lokalisierung $S^{-1}A$.

Beweis Nach 13.5 und 13.7 ist $S^{-1}A$ wieder noethersch und ganz abgeschlossen. Nach Satz 13.4 (b) ist jedes Primideal $0 \neq \mathfrak{p}' \subseteq S^{-1}A$ maximal, denn es ist $\mathfrak{p} = \mathfrak{p}' \cap A \neq 0 = 0 \cap A$, also maximal; für ein Primideal $\mathfrak{q} \supsetneq \mathfrak{p}'$ wäre aber $\mathfrak{q}' \cap A \supsetneq \mathfrak{p}' \cap A$.

Lemma/Definition 13.9 Sei $\mathfrak{p} \subseteq A$ ein Primideal in einem Integritätsring A . Dann ist $A \setminus \mathfrak{p}$ eine multiplikative Teilmenge und

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$$

heißt die **Lokalisierung von A nach \mathfrak{p}** . Der Ring $A_{\mathfrak{p}}$ hat genau ein maximales Ideal, nämlich $\mathfrak{p}A_{\mathfrak{p}}$.

Beweis der Behauptungen: Die Multiplikativität von $A \setminus \mathfrak{p}$ folgt sofort aus den Eigenschaften eines Primideals. Weiter liefert Satz 13.4 (b) eine Inklusions-erhaltende Bijektion

$$\text{Spec}(A_{\mathfrak{p}}) \rightarrow M_{\mathfrak{p}} = \{\mathfrak{q} \subseteq A \mid \mathfrak{q} \text{ Primideal und } \mathfrak{q} \subseteq \mathfrak{p}\},$$

denn es gilt $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$ genau dann, wenn $\mathfrak{q} \subseteq \mathfrak{p}$. Da die Menge $M_{\mathfrak{p}}$ genau ein maximales Element hat, nämlich \mathfrak{p} , hat $A_{\mathfrak{p}}$ genau ein maximales Primideal, nämlich $\mathfrak{p}A_{\mathfrak{p}}$, welches nach 13.4 (b) unter der erwähnten Bijektion auf \mathfrak{p} abgebildet wird.

Lemma 13.10 Ist $\mathfrak{m} \subseteq A$ maximales Ideal, so ist die kanonische Abbildung

$$A/\mathfrak{m} \xrightarrow{\sim} A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$$

ein Isomorphismus. Allgemeiner sei B ein Integritätsring, der A als Unterring enthält und $B_{\mathfrak{m}} = (A \setminus \mathfrak{m})^{-1}B$. Dann ist der Ringhomomorphismus $\varphi : B/\mathfrak{m}B \rightarrow B_{\mathfrak{m}}/\mathfrak{m}B_{\mathfrak{m}}$ ein Isomorphismus.

Beweis Es genügt, die zweite Behauptung zu zeigen. Wir zeigen zuerst die Surjektivität. Sei $x = \frac{b}{s} \in B_{\mathfrak{m}}$ ($b \in B$, $s \in A \setminus \mathfrak{m}$) und \bar{x} die Restklasse von x in $B_{\mathfrak{m}}/\mathfrak{m}B_{\mathfrak{m}}$. Da $s \notin \mathfrak{m}$ und da \mathfrak{m} maximal ist, also A/\mathfrak{m} ein Körper, gibt es ein $c \in A$ mit $cs \equiv 1 \pmod{\mathfrak{m}}$. Es folgt

$$\frac{b}{s} - cb = (1 - cs)\frac{b}{s} \in \mathfrak{m}B_{\mathfrak{m}},$$

also $\varphi(cb) = \bar{x}$. Für die Injektivität haben wir zu zeigen, dass $B \cap \mathfrak{m}B_{\mathfrak{m}} = \mathfrak{m}B$. Für die nichttriviale Richtung sei $x \in \mathfrak{m}B_{\mathfrak{m}}$. Wie im Beweis von 13.4 (b) folgt, dass $x = \frac{m}{s}$ mit $m \in \mathfrak{m}B$ und $s \in A \setminus \mathfrak{m}$. Wie oben gibt es ein $c \in A$ mit $cs = 1 + a$, wobei $a \in \mathfrak{m}$. Ist nun $x \in B$, so folgt $sx = m \in \mathfrak{m}B$ und

$$x = csx - ax \in \mathfrak{m}B.$$

Satz 13.11 Ist A ein Dedekindring und $\mathfrak{p} \subseteq A$, $\mathfrak{p} \neq 0$, ein Primideal, so ist $A_{\mathfrak{p}}$ ein Hauptidealring. Genauer gibt es ein Primelement $\pi \in A_{\mathfrak{p}}$, so dass alle Ideale in $A_{\mathfrak{p}}$ von der Form $(\pi^n) = \pi^n A_{\mathfrak{p}}$ für ein $n \in \mathbb{N}_0$ sind.

Beweis: Da \mathfrak{p} das einzige Primideal in A ist, welches in \mathfrak{p} enthalten ist, und ungleich 0 ist, besitzt $A_{\mathfrak{p}}$ nach 13.4 (b) nur ein Primideal $\neq 0$, nämlich $\mathfrak{P} = \mathfrak{p}A_{\mathfrak{p}}$. Nach der Idealtheorie für Dedekindringe ist also jedes Ideal in $A_{\mathfrak{p}}$ von der Form \mathfrak{P}^n mit $n \in \mathbb{N}_0$. Sei $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Dann gilt $(\pi) \subseteq \mathfrak{P}$ aber $(\pi) \not\subseteq \mathfrak{P}^2$, also muss $(\pi) = \mathfrak{P}$ gelten.

14 Diskriminante und Verzweigung

Definition 14.1 Sei A ein Dedekindring mit Quotientenkörper K . Sei L/K eine endliche separable Erweiterung und B der ganze Abschluss von A in L . Die **Diskriminante** $\mathfrak{d}_{B/A}$ von B über A ist definiert als das Ideal in A , welches von allen Diskriminanten $d(\beta_1, \dots, \beta_n)$ erzeugt wird, wobei $(\beta_1, \dots, \beta_n)$ eine in B gelegene K -Basis von L ist.

Bemerkung 14.2 (a) Nach Corollar 3.13 sind alle $d(\beta_1, \dots, \beta_n) \neq 0$, also $\mathfrak{d}_{B/A} \neq 0$.

(b) Ist B ein freier A -Modul (notwendigerweise vom Rang $n = [L : K]$), und ist $(\beta_1, \dots, \beta_n)$ eine A -Basis von B , also $B = A\beta_1 \oplus \dots \oplus A\beta_n$, so folgt aus Lemma 3.14, dass

$$\mathfrak{d}_{B/A} = (d(\beta_1, \dots, \beta_n))$$

(vergleiche auch 3.20). Im Allgemeinen ist $\mathfrak{d}_{B/A}$ aber kein Hauptideal.

(c) Ist L/K eine endliche Erweiterung von Zahlkörpern, so schreiben wir auch $\mathfrak{d}_{L/K}$ für $\mathfrak{d}_{\mathcal{O}_L/\mathcal{O}_K}$ und nennen dies die (relative) Diskriminante von L über K .

(d) Offenbar gilt für Zahlkörper K

$$\mathfrak{d}_{K/\mathbb{Q}} = (d_K),$$

wobei d_K die (absolute) Diskriminante von K ist (siehe 3.20).

Ziel dieses Abschnitts ist der folgende Satz:

Satz 14.2 Ein Primideal $\mathfrak{p} \subseteq A$ ist genau dann verzweigt in B/A , wenn $\mathfrak{p} \mid \mathfrak{d}_{B/A}$.

Bevor wir diesen Satz beweisen, notieren wir einige offensichtliche Folgerungen.

Corollar 14.3 Es gibt nur endlich viele Primideale, die in B/A verzweigen.

Corollar 14.4 Sei L/K eine Erweiterung von Zahlkörpern. Ein Primideal \mathfrak{p} in K ist genau dann verzweigt in L/K , wenn \mathfrak{p} die relative Diskriminante $\mathfrak{d}_{L/K}$ teilt. Insbesondere sind nur endlich viele \mathfrak{p} in L/K verzweigt.

Corollar 14.5 Sei K ein Zahlkörper. Eine Primzahl p ist genau dann in K verzweigt, wenn $p \mid d_K$.

Beispiele 14.6 (a) (vergleiche Übungsaufgabe 24) Sei $m \in \mathbb{Z} \setminus \{0\}$ quadratfrei und $K = \mathbb{Q}(\sqrt{m})$. Ist $m \equiv 2, 3 \pmod{4}$, so ist $d_K = 4m$ und eine Primzahl p genau dann verzweigt in K , wenn $p \mid 2m$. Ist $m \equiv 1 \pmod{4}$, so ist $d_K = m$ und p genau dann verzweigt in K , wenn $p \mid m$.

(b) Sei $n = \ell^\nu \neq 2$ eine Primzahlpotenz und $K = \mathbb{Q}(\zeta_n)$. Dann ist $d_K = \pm \ell^m$ für ein $m > 0$ (Lemma 6.5, Satz 6.7), also ist genau die Primzahl ℓ verzweigt in K (vergleiche 6.9 und 6.10).

Wie in Behauptung 11.9 angekündigt, erhalten wir nun auch:

Corollar 14.7 Es gibt keine unverzweigten Erweiterungen K/\mathbb{Q} außer der trivialen ($K = \mathbb{Q}$).

Beweis Nach Satz 11.8 gilt für $K \neq \mathbb{Q}$ immer $|d_K| > 1$, d.h., d_K hat immer Primteiler.

Zum Beweis von Satz 14.2 verallgemeinern wir die in §3 eingeführten Begriffe Norm, Spur und Diskriminante.

Sei A ein Ring (kommutativ, mit Eins), M ein freier A -Modul von endlichem Rang. Für jeden A -Modul-Endomorphismus $\varphi : M \rightarrow M$ sind dann die Determinante $\det(\varphi) \in A$, die Spur $\text{tr}(\varphi) \in A$ und das charakteristische Polynom $\chi(\varphi, x) \in A[x]$ definiert: Jede A -Basis (x_1, \dots, x_n) von M liefert einen Isomorphismus $M \cong A^n$ und eine Darstellung von φ durch eine $(n \times n)$ -Matrix $C = (a_{ij})$ mit Koeffizienten $a_{ij} \in A$, und man nimmt Determinante bzw. Spur bzw. charakteristisches Polynom dieser Matrix, nach den üblichen, aus der Linearen Algebra bekannten Regeln. Insbesondere ist

$$\text{tr}(\varphi) = \text{tr}(C) = \sum_{i=1}^n a_{ii},$$

die Determinante $\det(\varphi) = \det(C)$ kann mittels Leibniz-Regel oder Entwicklung nach Zeilen oder Spalten berechnet werden, und es gilt $\chi(\varphi, x) = \det(xid - C)$, mit Rechnung im Ring $A[x]$. Bei Übergang zu einer anderen Basis ändert sich C zu $D^{-1}CD$ für eine Matrix $D \in$

$Gl_n(A)$, und \det, tr und χ bleiben gleich, sind also unabhängig von φ . Für die Spur zeigt man zum Beispiel leicht $tr(C_1C_2) = tr(C_2C_1)$ und daher $tr(D^{-1}CD) = tr(C)$.

Definition 14.8 Sei B ein Ring und A ein Unterring von B derart, dass B ein freier A -Modul von endlichem Rang n ist.

(a) Für $\beta \in B$ sei

$$\begin{aligned} \varphi_\beta &: B \rightarrow B \\ x &\mapsto \beta x \end{aligned}$$

die A -lineare Abbildung, die durch Multiplikation mit β gegeben ist. Die Norm (bzw. Spur, bzw. das charakteristische Polynom) von β für B/A ist definiert als Determinante (bzw. Spur, bzw. charakteristisches Polynom) von φ_β :

$$\begin{aligned} N_{B/A}(\beta) &= \det(\varphi_\beta) \\ Tr_{B/A}(\beta) &= tr(\varphi_\beta) \\ \chi(\beta, x) &= \chi(\varphi_\beta, x). \end{aligned}$$

(b) Für $\beta_1, \dots, \beta_n \in B$ heißt

$$d(\beta_1, \dots, \beta_n) := \det(Tr_{B/A}(\beta_i\beta_j)) \in A$$

die **Diskriminante** von $(\beta_1, \dots, \beta_n)$.

(c) Ist $(\beta_1, \dots, \beta_n)$ eine A -Basis von B , so heißt das Hauptideal

$$\mathfrak{d}_{B/A} := (d(\beta_1, \dots, \beta_n))$$

die **Diskriminante** von B über A .

Bemerkung 14.9 (a) Wie in Lemma 3.14 gilt auch hier: Sind $\underline{\beta} = (\beta_1, \dots, \beta_n), \underline{\beta}' = (\beta'_1, \dots, \beta'_n) \in B^n$ und gilt $\beta'_i = \sum_{j=1}^n a_{ij}\beta_j$ mit $a_{ij} \in A$, so folgt

$$d(\beta'_1, \dots, \beta'_n) = (\det(a_{ij}))^2 d(\beta_1, \dots, \beta_n).$$

(b) Insbesondere gilt: Sind $\underline{\beta}$ und $\underline{\beta}'$ beides A -Basen von B , so ist $(a_{ij}) \in Gl_n(A)$, also $\det(a_{ij}) \in A^\times$ Einheit, also sind $d(\underline{\beta}')$ und $d(\underline{\beta})$ assoziiert. Dies zeigt, dass die obige Definition 14.8 (c) nicht von der Basis $(\beta_1, \dots, \beta_n)$ abhängt (vergleiche den Beweis von 3.20).

Lemma 14.10 Sei A ein Ring und seien B_1, \dots, B_q Ringe die A enthalten und freie A -Moduln von endlichem Rang sind. Dann gilt für den Produktring $B = \prod_{i=1}^q B_i$

$$\mathfrak{d}_{B/A} = \prod_{i=1}^q \mathfrak{d}_{B_i/A}$$

(Produkt der Ideale).

Beweis: Es genügt, dies für $q = 2$ zu zeigen; dann folgt die Behauptung durch Induktion über q . Seien (x_1, \dots, x_m) bzw. (y_1, \dots, y_n) A -Basen von B_1 bzw. B_2 . Identifizieren wir B_1

mit dem Unterring $B_1 \times \{0\}$ und B_2 mit $\{0\} \times B_2$, so ist $(x_1, \dots, x_m, y_1, \dots, y_n)$ eine A -Basis von $B = B_1 \times B_2$. Wegen $x_i y_i = 0$ ist $d(x_1, \dots, x_m, y_1, \dots, y_n)$ die Determinante der Matrix

$$\left(\begin{array}{c|c} \text{Tr}(x_i x_{i'}) & 0 \\ \hline 0 & \text{tr}(y_j y_{j'}) \end{array} \right),$$

also gleich $d(x_1, \dots, x_m) \cdot d(y_1, \dots, y_n)$.

Lemma 14.11 Sei B ein Ring, A ein Unterring und B frei als A -Modul, mit Basis (x_1, \dots, x_n) . Sei $\mathfrak{a} \subseteq A$ ein Ideal, und für $x \in B$ (bzw. $x \in A$) bezeichne \bar{x} die Restklasse von x in $B/\mathfrak{a}B$ (bzw. in A/\mathfrak{a}). Dann ist $(\bar{x}_1, \dots, \bar{x}_n)$ eine Basis von $B/\mathfrak{a}B$ über A/\mathfrak{a} , und es gilt

$$d(\bar{x}_1, \dots, \bar{x}_n) = \overline{d(x_1, \dots, x_n)}.$$

Beweis Die erste Behauptung ist klar. Für $\beta \in B$ gilt: Ist die Matrix für den Endomorphismus φ_β (Multiplikation mit β auf B) bezüglich (x_1, \dots, x_n) gleich (a_{ij}) , so ist die Matrix für die Multiplikation mit $\bar{\beta}$ auf $B/\mathfrak{a}B$ bezüglich $(\bar{x}_1, \dots, \bar{x}_n)$ gleich (\bar{a}_{ij}) . Es gilt also $\text{Tr}(\bar{\beta}) = \overline{\text{Tr}(\beta)}$. Daher gilt $\text{Tr}(\bar{x}_i \bar{x}_j) = \overline{\text{Tr}(x_i x_j)}$, und die Behauptung folgt durch Bildung der Determinante.

14.12 Wir kommen nun zum

Beweis von Satz 14.2: Sei A ein Dedekindring mit Quotientenkörper K , L/K eine endliche separable Erweiterung und sei B der ganze Abschluss von A in L . Sei $\mathfrak{d}_{B/A}$ die Diskriminante von B über A , sei $\mathfrak{p} \subseteq A$ ein Primideal, $\mathfrak{p} \neq 0$ und sei

$$(14.12.1) \quad \mathfrak{p}B = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$$

die Primzerlegung von \mathfrak{p} in B (\mathfrak{P}_i Primideal über \mathfrak{p} , $e_i \in \mathbb{N}$).

1) Sei $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}A$ wie in Definition 13.9 und $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$. Nach Satz 13.8 sind dies Dedekindringe, und nach Satz 13.6 ist $B_{\mathfrak{p}}$ der ganze Abschluss von $A_{\mathfrak{p}}$ in L . Weiter ist $A' = A_{\mathfrak{p}}$ nach Satz 13.11 ein Hauptidealring; nach Satz 3.18 ist also $B' = B_{\mathfrak{p}}$ ein freier A' -Modul vom Rang $n = [L : K]$. Sei (e_1, \dots, e_n) , mit $e_i \in B'$ eine A' -Basis von B' , und sei \bar{e}_i die Restklasse von e_i in $B'/\mathfrak{p}'B'$, wobei $\mathfrak{p}' = \mathfrak{p}A' = \mathfrak{p}A_{\mathfrak{p}}$. Nach Lemma 14.11 ist dann $B'/\mathfrak{p}'B'$ freier A'/\mathfrak{p}' -Modul mit Basis $(\bar{e}_1, \dots, \bar{e}_n)$, und es gilt

$$d(\bar{e}_1, \dots, \bar{e}_n) = d(e_1, \dots, e_n) \bmod \mathfrak{p}'.$$

Es existieren also die Diskriminanten für B' über A' und $B'/\mathfrak{p}'B'$ über A'/\mathfrak{p}' nach Definition 14.8 (c), und es gilt

$$\mathfrak{p}' \mid \mathfrak{d}_{B'/A'} \Leftrightarrow \mathfrak{d}_{(B'/\mathfrak{p}'B')/(A'/\mathfrak{p}')} = (0).$$

2) Andererseits gibt es nach Lemma 13.10 Isomorphismen $A/\mathfrak{p} \xrightarrow{\sim} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = A'/\mathfrak{p}'$ und $B/\mathfrak{p}B \xrightarrow{\sim} B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} = B'/\mathfrak{p}'B'$. Daher existiert auch die Diskriminante von $B/\mathfrak{p}B$ über A/\mathfrak{p} und ist gleich der Diskriminante von $B'/\mathfrak{p}'B'$ über A'/\mathfrak{p}' .

3) Nach (14.12.1) haben wir eine Isomorphie

$$B/\mathfrak{p}B \cong \prod_{i=1}^r B/\mathfrak{P}_i^{e_i}.$$

Da A/\mathfrak{p} ein Körper ist, sind alle $B/\mathfrak{P}_i^{e_i}$ endlich-dimensionale A/\mathfrak{p} -Vektorräume; es existieren also die jeweiligen Diskriminanten über A/\mathfrak{p} , und nach Lemma 14.10 gilt

$$(14.12.2) \quad \mathfrak{d}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = \prod_{i=1}^r \mathfrak{d}_{(B/\mathfrak{P}_i^{e_i})/(A/\mathfrak{p})}.$$

Wir behaupten nun

Behauptung 1: $\bar{\mathfrak{d}} := \mathfrak{d}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0) \Leftrightarrow \mathfrak{p}$ ist verzweigt in B/A .

Beweis: Nach (14.12.2) ist $\bar{\mathfrak{d}} \neq (0)$ genau dann, wenn alle $\mathfrak{d}_i := \mathfrak{d}_{(B/\mathfrak{P}_i^{e_i})/(A/\mathfrak{p})} \neq (0)$. Ist aber $\mathfrak{P}_i/\mathfrak{p}$ unverzweigt, so ist $e_i = 1$ und B/\mathfrak{P}_i eine endliche separable Körpererweiterung von $k(\mathfrak{p}) := A/\mathfrak{p}$; die Diskriminante ist also ungleich null nach Corollar 3.13. Ist aber $e_i > 1$, so gibt es ein nilpotentes Element $x \neq 0$ in $B/\mathfrak{P}_i^{e_i}$ und wir können dies zu einer $k(\mathfrak{p})$ -Basis $x_1 = x, x_2, \dots, x_m$ von $B_i := B/\mathfrak{P}_i^{e_i}$ ergänzen. Für alle $j = 1, \dots, m$ ist dann $x_1 x_j$ nilpotent; also ist die Multiplikation mit $x_1 x_j$ nilpotent auf dem $k(\mathfrak{p})$ -Vektorraum B_i . Nach der Linearen Algebra ist dann $\text{Tr}_{B_i/k(\mathfrak{p})}(x_1 x_j) = 0$; in der Matrix $(\text{Tr}_{B_i/k(\mathfrak{p})}(x_k x_j))$ ist also die erste Zeile null und es folgt, dass $d(x_1, \dots, x_m) = \det(\text{Tr}(x_k x_j)) = 0$, d.h., dass $\mathfrak{d}_i = (0)$. Ist schließlich $e_i = 1$ und der Körper B/\mathfrak{P}_i inseparabel über A/\mathfrak{p} , so ist $\mathfrak{d}_i = (0)$ nach Lemma 3.12.

4) Aus den Schritten 1) bis 3) folgt:

$$(14.12.3) \quad \mathfrak{p} \text{ ist verzweigt in } B/A \Leftrightarrow \mathfrak{p}' \mid \mathfrak{d}_{B'/A'}.$$

Satz 14.2 folgt also aus der folgenden Aussage:

Behauptung 2: $\mathfrak{p}' \mid \mathfrak{d}_{B'/A'} \Leftrightarrow \mathfrak{p} \mid \mathfrak{d}_{B/A}$.

Beweis: Wir bemerken, dass hier $\mathfrak{d}_{B/A}$ nach Definition 14.1 gebildet ist, da B im Allgemeinen kein freier A -Modul ist.

Sei wie oben (e_1, \dots, e_n) eine A' -Basis von B' , so dass $\mathfrak{d}_{B'/A'} = (d(e_1, \dots, e_n))$. Gilt $\mathfrak{p}' \mid \mathfrak{d}_{B'/A'}$, also $d(e_1, \dots, e_n) \in \mathfrak{p}'$, und ist (x_1, \dots, x_n) eine in B gelegene K -Basis von L , so gibt es wegen $B \subset B'$ Elemente $a'_{ij} \in A'$ mit $x_i = \sum a'_{ij} e_j$, und es folgt (siehe Bemerkung 14.9)

$$d(x_1, \dots, x_n) = [\det(a_{ij})]^2 d(e_1, \dots, e_n) \in \mathfrak{p}',$$

also $d(x_1, \dots, x_n) \in \mathfrak{p}$ wegen $\mathfrak{p}' \cap A = \mathfrak{p}A' \cap A = A$ (siehe 13.4 (b)). Da dies für alle in B gelegenen K -Basen (x_1, \dots, x_n) gilt, folgt $\mathfrak{d}_{B/A} \subseteq \mathfrak{p}$, d.h., $\mathfrak{p} \mid \mathfrak{d}_{B/A}$. Gilt umgekehrt $\mathfrak{d}_{B/A} \subseteq \mathfrak{p}$, so folgt $d(e_1, \dots, e_n) \in \mathfrak{p}'$. Schreibt man nämlich $e_i = \frac{y_i}{s}$ mit $y_i \in B$ und einem $s \in A \setminus \mathfrak{p}$ (Hauptnenner bilden!), so ist (y_1, \dots, y_n) eine in B gelegene K -Basis von L und es gilt

$$d(e_1, \dots, e_n) = s^{-2n} d(y_1, \dots, y_n) \in A' \mathfrak{d}_{B/A} \subseteq A' \mathfrak{p} = \mathfrak{p}'.$$

15 Bewertungen

Sei K ein Körper.

Definition 15.1 Eine (**Absolut-**) **Bewertung** auf K ist eine Abbildung

$$|\cdot|: K \rightarrow \mathbb{R}$$

mit den Eigenschaften

- (i) $|x| \geq 0$, und $|x| = 0 \Leftrightarrow x = 0$,
- (ii) $|x \cdot y| = |x| \cdot |y|$,
- (iii) $|x + y| \leq |x| + |y|$ (Dreiecksungleichung).

Beispiele 15.2 (a) Der übliche Absolutbetrag

$$\begin{aligned} |\cdot|: \mathbb{C} &\rightarrow \mathbb{R} \\ z &\mapsto |z| = \sqrt{z\bar{z}} \end{aligned}$$

ist eine Bewertung, entsprechend die Einschränkung von $|\cdot|$ auf \mathbb{R} . Allgemein erhält man für jeden Zahlkörper K und jede Einbettung $\sigma: K \hookrightarrow \mathbb{C}$ eine Bewertung $|\cdot|_\sigma$ durch

$$|\alpha|_\sigma = |\sigma(\alpha)|.$$

Offenbar ist $|\cdot|_\sigma = |\cdot|_{\bar{\sigma}}$.

(a) Sei p eine Primzahl. Dann hat man die p -adische Bewertung $|\cdot|_p$ auf \mathbb{Q} , definiert durch

$$|m| = p^{-n_p} \quad \text{für} \quad m = \pm \prod_{q \text{ prim}}^{n_q} q^{n_q}$$

falls $m \neq 0$, und $|0| = 0$. Die Eigenschaften (i) und (ii) sind klar, und für (iii) beachte man: Ist $m = \pm \prod_q q^{n_q}$, $m' = \pm \prod_q q^{n'_q}$, so gilt $m + m' = \pm \prod_q q^{n''_q}$ mit $n''_q \geq \min(n_q, n'_q)$. Ist ohne Einschränkung $n_p \leq n'_p$, so folgt

$$|m + m'|_p = p^{-n''_p} \leq p^{-n_p} = |m|_p \leq |m|_p + |m'|_p.$$

Ein **bewerteter Körper** ist ein Körper mit einer Bewertung. Ist $(K, |\cdot|)$ ein bewerteter Körper, so erhält man eine Metrik auf K durch

$$d(x, y) = |x - y|.$$

Addition und Multiplikation sind stetig bezüglich dieser Metrik (Beweis selbst!).

Eine Bewertung $|\cdot|$ heißt **trivial**, wenn $|x| = 1$ für alle $x \neq 0$ gilt.

Definition 15.3 Zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$ auf K heißen **äquivalent**, wenn es eine reelle Zahl $t > 0$ gibt mit

$$|x|_1 = |x|_2^t$$

für alle $x \in K$.

Dies ist offenbar eine Äquivalenzrelation.

Satz 15.4 Zwei Bewertungen sind genau dann äquivalent, wenn sie dieselbe Topologie definieren.

Beweis Gilt $|\cdot|_1 = |\cdot|_2^t$, so sind die Topologien offenbar gleich: Eine ε -Umgebung bezüglich $|\cdot|_2$ ist eine ε^t -Umgebung bezüglich $|\cdot|_1$.

Seien umgekehrt die von $|\cdot|_1$ und $|\cdot|_2$ definierten Topologien gleich. Für eine beliebige Bewertung $|\cdot|$ gilt nun

$$(15.4.1) \quad |x| < 1 \Leftrightarrow (x^n)_{n \geq 1} \text{ ist Nullfolge.}$$

Es folgt also für alle $x \in K$

$$(15.4.2) \quad |x|_1 < 1 \Leftrightarrow |x|_2 < 1.$$

Also ist $|\cdot|_2$ genau dann trivial, wenn dies für $|\cdot|_1$ gilt. Andernfalls gibt es ein Element $y \in K$ mit $|y|_1 > 1$.

Ist nun $x \in K \setminus \{0\}$, so ist $|x|_1 = |y|_1^\alpha$ für ein $\alpha \in \mathbb{R}$. Sei $\left(\frac{m_i}{n_i}\right)_{i \geq 1}$ eine Folge rationaler Zahlen ($m_i, n_i \in \mathbb{Z}$) mit $n_i > 0$, die strikt von oben gegen α konvergiert ($\frac{m_i}{n_i} > \alpha$). Dann ist

$$|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i},$$

also $|x^{n_i}/y^{m_i}|_1 < 1$. Mit (15.4.2) folgt ebenfalls $|x^{n_i}/y^{m_i}|_2 < 1$, durch Übergang zum Limes also $|x|_2 \leq |y|_2^\alpha$. Betrachten wir eine Folge, die strikt von unten gegen α konvergiert, so folgt genauso $|x|_2 \geq |y|_2^\alpha$. Damit gilt $|x|_2 = |y|_2^\alpha$. Für alle $x \in K^\times$ folgt dann

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2} =: t,$$

also

$$|x|_1 = |x|_2^t,$$

wobei $t > 0$ wegen $|y|_1 > 1$ und somit $|y|_2 > 1$.

Definition 15.5 Die Bewertung $|\cdot|$ heißt **nicht-archimedisch**, wenn $|n|$ für alle $n \in \mathbb{N}$ beschränkt ist, und somit **archimedisch**.

Beispiele 15.6 (a) Der übliche Betrag $|\cdot|$ auf \mathbb{R} oder \mathbb{C} , sowie die Bewertungen $|\cdot|_\sigma$ aus 15.2 (a) sind archimedisch.

(b) $|\cdot|_p$ auf \mathbb{Q} ist nicht-archimedisch, denn es ist $|n|_p \leq 1$ für alle $n \in \mathbb{N}$.

Proposition 15.7 Eine Bewertung $|\cdot|$ ist genau dann nicht-archimedisch, wenn sie die **verschärfte** (oder auch **ultra-metrische**) **Dreiecksungleichung**

$$(15.7.1) \quad |x + y| \leq \max\{|x|, |y|\}$$

erfüllt.

Beweis Gilt (15.7.1), so ist $|n| = |1 + \dots + 1| \leq |1| \leq |1| = 1$.

Sei umgekehrt $N \in \mathbb{N}$ mit $|n| \leq N$ für alle $n \in \mathbb{N}$. Seien $x, y \in K$, ohne Einschränkung $|x| \geq |y|$. Dann ist

$$|x + y|^n = \left| \sum_{\nu=0}^n \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leq \sum_{\nu=0}^n \binom{n}{\nu} |x|^\nu |y|^{n-\nu} \leq (n+1)N|x|^n,$$

also

$$|x + y| \leq \sqrt[n]{(n+1)N} \cdot |x|$$

Im Limes $n \rightarrow \infty$ folgt

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

Bemerkung 15.8 (a) Gilt die verschärfte Dreiecksungleichung (15.7.1), so folgt

$$(15.8.1) \quad |x| \neq |y| \Rightarrow |x + y| = \max\{|x|, |y|\}.$$

(Angenommen $|x| < |y|$ und $|x + y| < |y|$. Dann ist $|y| = |y + x - x| \leq \max\{|y + x|, |x|\} < |y|$ – Widerspruch!).

(b) Eine nicht-archimedische Bewertung ist also eine Abbildung

$$|\cdot| : K^\times \rightarrow \mathbb{R}_{>0}$$

mit

$$(1) |xy| = |x| |y|,$$

$$(2) |x + y| \leq \max\{|x|, |y|\}.$$

Allgemeiner betrachtet man auch Abbildungen

$$|\cdot| : K^\times \rightarrow G$$

in eine **total geordnete abelsche Gruppe** G mit den Eigenschaften (1) und (2). Solche werden Krull-Bewertungen genannt.

Wir betrachten hier aber im Folgenden immer Absolut-Bewertungen und nennen diese nur Bewertungen.

Lemma/Definition 15.9 (a) Ist K ein Körper und $|\cdot| : K \rightarrow \mathbb{R}$ eine *nicht-archimedische* Bewertung, so definieren wir die Funktion

$$v : K \rightarrow \mathbb{R} \cup \{\infty\}$$

durch

$$v(x) = \begin{cases} -\log |x| & , x \neq 0 \\ \infty & , x = 0. \end{cases}$$

Dann gilt

$$(i) v(x) = \infty \Leftrightarrow x = 0,$$

$$(ii) v(xy) = v(x) + v(y)$$

$$(iii) v(x + y) \geq \min(v(x), v(y))$$

(wobei wir für $a \in \mathbb{R}$ definieren $a + \infty = \infty$, $a < \infty$, $\infty + \infty = \infty$)

(b) Jede Funktion $v : K \rightarrow \mathbb{R} \cup \{\infty\}$ mit den Eigenschaften (i)-(iii) heißt eine **Exponential-Bewertung** von K , und zwei Exponential-Bewertungen v, v' heißen äquivalent, wenn $v = t \cdot v'$ mit einer reellen Zahl $t > 0$. Offenbar liefert die obige Zuordnung

$$| \cdot | \rightsquigarrow v = -\log | \cdot |$$

eine bijektive Beziehung zwischen nicht-archimedische Bewertungen und Exponential-Bewertungen, wobei sich die Äquivalenz entspricht. Wir nennen $| \cdot |$ und v auch assoziiert zueinander, wenn v und $-\log | \cdot |$ äquivalent sind.

Sei K ein Körper.

Proposition 15.10 Ist $| \cdot |$ eine nicht-archimedische Bewertung auf K und v eine assoziierte Exponential-Bewertung, so gilt:

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x| \leq 1\}$$

ist ein Unterring mit der Einheitengruppe

$$\mathcal{O}^\times = \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\}$$

und dem einzigen maximalen Ideal

$$\mathfrak{m} = \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\}.$$

Beweis: Klar/selbst!

Definition 15.11 \mathcal{O} heißt der **Bewertungsring** zu $| \cdot |$ (bzw. v), und \mathcal{O}/\mathfrak{m} heißt der **Restklassenkörper** von \mathcal{O} .

Bemerkung 15.12 Offenbar hängt \mathcal{O} nur von der Äquivalenzklasse der Bewertung ab.

Lemma/Definition 15.13 Ein kommutativer Ring R mit Eins heißt **lokal**, wenn er die folgende äquivalenten Bedingungen erfüllt:

(a) R besitzt genau ein maximales Ideal \mathfrak{m} .

(b) $R \setminus R^\times$ ist ein Ideal.

In diesem Fall ist $\mathfrak{m} = R \setminus R^\times$, und R/\mathfrak{m} heißt der **Restklassenkörper** von R .

Beweis der Behauptungen: Wir bemerken, dass für ein echtes Ideal $\mathfrak{a} \subsetneq R$ immer $\mathfrak{a} \cap R^\times = \emptyset$ ist, also $\mathfrak{a} \subseteq R \setminus R^\times$. Ist nun $R \setminus R^\times$ ein Ideal, so ist es also das eindeutig bestimmte maximale Ideal. Besitzt umgekehrt R genau ein maximales Ideal \mathfrak{m} , so gilt für jedes $x \in R \setminus R^\times$, dass $(x) \subseteq \mathfrak{m}$, also gilt $R \setminus R^\times \subseteq \mathfrak{m}$. Zusammen mit der Vorbemerkung folgt $R \setminus R^\times = \mathfrak{m}$; dies ist insbesondere ein Ideal.

Beispiele 15.14 (a) Nach 15.10 ist der Bewertungsring zu einer Bewertung ein lokaler Ring.
 (b) Sei A ein Integritätsring und $\mathfrak{p} \subseteq A$ ein Primideal. Dann ist nach 13.9 die Lokalisierung $A_{\mathfrak{p}}$ ein lokaler Ring (mit eindeutigem maximalem Ideal $\mathfrak{p}A_{\mathfrak{p}}$).

Im folgenden Beispiel kommen beide Fälle zusammen:

Beispiele 15.15 (a) Sei p eine Primzahl. Die Exponential-Bewertung zu $|\cdot|_p$ ist \tilde{v}_p mit

$$\tilde{v}_p(\pm \prod_{q \text{ prim}} q^{n_q}) = -\log(p^{-n_p}) = n_p \cdot \log p.$$

Die äquivalente Exponential-Bewertung v_p mit

$$v_p(\pm \prod_q q^{n_q}) = n_p$$

heißt die normierte Exponential-Bewertung von p oder die additive p -adische Bewertung. Der Bewertungsring zu $|\cdot|_p$ ist

$$\begin{aligned} \mathcal{O} &= \{\alpha \in \mathbb{Q} \mid v_p(\alpha) \geq 0\} \\ &= \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}, p \nmid b \right\} \\ &= \mathbb{Z}_{(p)}, \end{aligned}$$

die Lokalisierung nach dem Primideal (p) .

(b) Allgemeiner sei K ein Zahlkörper und \mathfrak{p} ein Primideal von K . Dann ist die Abbildung

$$\begin{aligned} v_{\mathfrak{p}} : K &\rightarrow \mathbb{Z} \cup \{\infty\} \\ v_{\mathfrak{p}}(\alpha) &= \begin{cases} \infty & , \text{ falls } \alpha = 0, \\ n_{\mathfrak{p}} & , \text{ falls } 0 \neq (\alpha) = \prod_{\mathfrak{q} \text{ Primideal}} \mathfrak{q}^{n_{\mathfrak{q}}} \end{cases} \end{aligned}$$

eine Exponential-Bewertung und

$$|\alpha|_{\mathfrak{p}} = N_{\mathfrak{p}}^{v_{\mathfrak{p}}(\alpha)}$$

eine zugehörige Absolutbewertung, wobei

$$N_{\mathfrak{p}} = |\mathcal{O}_K/\mathfrak{p}| < \infty.$$

Der zugehörige Bewertungsring ist der lokale Ring

$$\mathcal{O}_{\mathfrak{p}} := (\mathcal{O}_K)_{\mathfrak{p}} = \left\{ \frac{a}{b} \in K \mid a \in \mathcal{O}_K, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\},$$

die Lokalisierung von \mathcal{O}_K nach \mathfrak{p} (Beweis: Übungsaufgabe!).

Das maximale Ideal von $\mathcal{O}_{\mathfrak{p}}$ ist also

$$\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \left\{ \frac{a}{b} \in K \mid a \in \mathfrak{p}, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\},$$

und der Restklassenkörper ist $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Nach Lemma 13.10 ist die Abbildung

$$\mathcal{O}_K/\mathfrak{p} \rightarrow \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$$

ein Isomorphismus; der Restklassenkörper identifiziert sich also mit dem üblichen Restklassenkörper $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ von \mathfrak{p} .

Definition 15.16 (a) Eine Exponential-Bewertung v auf einem Körper K heißt **diskret**, wenn die **Wertegruppe** $\Gamma = v(K^\times)$ isomorph zu \mathbb{Z} ist. Der zugehörige Bewertungsring heißt dann diskreter Bewertungsring. Wir nennen auch jeden zugehörigen Absolutbetrag $|\cdot|$ diskret.

(b) Eine diskrete Exponential-Bewertung v heißt **normiert**, wenn $s = 1$.

Beispiele 15.17 (a) $|\cdot|_p$ auf \mathbb{Q} ist diskret; die zugehörige Exponential-Bewertung v_p aus 15.15 (a) ist normiert.

(b) Die Exponential-Bewertungen v_p aus 15.15 (b) sind diskret und normiert.

(c) Jede diskrete Exponential-Bewertung ist äquivalent zu einer normierten diskreten Exponential-Bewertung: Es gibt ein Erzeugendes s von Γ mit $s > 0$; dann ist also $\Gamma = \mathbb{Z} \cdot s$ und $\frac{1}{s}v$ normiert. Beachte: s ist das kleinste Element > 0 in Γ .

Definition 15.18 Sei v eine diskrete Exponential-Bewertung. Ein Element π mit minimalem positiven Wert $v(\pi)$ heißt **Primelement** (für v).

Lemma 15.19 Sei v diskrete Bewertung auf K mit Bewertungsring \mathcal{O} , und sei π ein Primelement.

(a) Jedes $x \in K^\times$ besitzt eine eindeutige Darstellung

$$x = u\pi^m$$

mit $m \in \mathbb{Z}$ und einer Einheit $u \in \mathcal{O}^\times$.

(b) $\mathfrak{p} = \pi\mathcal{O}$ ist das maximale Ideal von \mathcal{O} , und die von Null verschiedenen Ideale von \mathcal{O} sind die Ideale

$$\mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in K \mid v(x) \geq nv(\pi)\}$$

für $n \geq 0$. Insbesondere ist \mathcal{O} ein Hauptidealring.

Beweis Ohne Einschränkung sei v normiert und damit $v(\pi) = 1$ und $v(K^\times) = \mathbb{Z}$.

(a): Ist dann $x \in K^\times$ und $v(x) = m \in \mathbb{Z}$, so gilt für $u = x\pi^{-m}$: $v(u) = v(x) - mv(\pi) = m - m = 0$; also ist u eine Einheit und $x = u\pi^m$. Die Eindeutigkeit ist wegen $v(u\pi^m) = m$ klar.

(b): Sei $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ ein Ideal und $x \neq 0$ ein Element in \mathfrak{a} mit minimalem Wert $v(x) = n$. Dann ist $x = u\pi^n$ mit $u \in \mathcal{O}^\times$ also $\pi^n\mathcal{O} \subseteq \mathfrak{a}$. Ist $y = v\pi^m \in \mathfrak{a}$ mit $v \in \mathcal{O}^\times$, so ist $v(y) = m \geq n$, also $y = v\pi^{m-n}\pi^n \in \pi^n\mathcal{O}$. Es gilt also $\mathfrak{a} = \pi^n\mathcal{O}$. Daher ist offenbar auch $\mathfrak{p} := \pi\mathcal{O}$ maximales Ideal und $\mathfrak{p}^n = \pi^n\mathcal{O}$.

Man vergleiche dies mit Satz 13.11. Tatsächlich gilt

Satz 15.20 Für einen Integritätsring R sind äquivalent

(a) R ist ein diskreter Bewertungsring (d.h., der Bewertungsring einer diskreten Bewertung v auf $K = \text{Quot}(R)$) oder ein Körper.

- (b) R ist ein lokaler Dedekindring.
- (c) R ist ein lokaler Hauptidealring.

16 Kompletterungen

Definition 16.1 Ein bewerteter Körper $(K, | \cdot |)$ heißt **vollständig** (oder **komplett**), wenn jede Cauchyfolge $(a_n)_{n \in \mathbb{N}}$ in K gegen ein $a \in K$ konvergiert. (Cauchyfolgen und Konvergenz sind hier bezüglich der assoziierten Metrik $d(x, y) = |x - y|$ verstanden).

Konstruktion 16.2 Zu jedem bewerteten Körper $(K, | \cdot |)$ kann man in kanonischer Weise einen vollständigen bewerteten Körper $(\hat{K}, | \cdot |)$ definieren, der K als dichten Teilkörper enthält, wobei $| \cdot |$ auf \hat{K} eine Fortsetzung von $| \cdot |$ auf K ist. $(\hat{K}, | \cdot |)$ wird die **Kompletterung** (oder **Vervollständigung**) von $(K, | \cdot |)$ genannt.

Wir skizzieren die Konstruktion: Sei R der Ring der Cauchyfolgen in K . Darin bilden die Nullfolgen ein maximales Ideal N , und man setzt

$$\hat{K} = R/N.$$

Man erhält einen kanonischen (injektiven) Körperhomomorphismus

$$\begin{aligned} K &\rightarrow \hat{K} \\ a &\mapsto \text{Klasse } \underline{a} \text{ der konstanten Folge } (a). \end{aligned}$$

Die Bewertung $| \cdot |$ lässt sich auf \hat{K} fortsetzen, indem man für die Klasse a der Cauchyfolge $(a_n)_{n \in \mathbb{N}}$ definiert

$$|a| = \lim_{n \rightarrow \infty} |a_n|.$$

Dieser Limes existiert wegen der Vollständigkeit von \mathbb{R} , da wegen $||a_n| - |a_m|| \leq |a_n - a_m|$ die Folge $(|a_n|)_n$ eine Cauchyfolge in \mathbb{R} ist.

\hat{K} ist vollständig: Sei $(\overline{a^m})_{m \in \mathbb{N}}$ eine Cauchyfolge in \hat{K} , mit $a^m = (a_k^m)_{k \in \mathbb{N}} \in \mathcal{R}$. Für jedes $n \in \mathbb{N}$ gibt es dann ein $k_n \in \mathbb{N}$ mit

$$|a_k^n - a_{k'}^n| \leq \frac{1}{n} \quad \text{für } k, k' \geq k_n.$$

Dann ist $b = (a_{k_n}^n)$ eine Cauchyfolge mit $\lim_{m \rightarrow \infty} \overline{a^m} = \bar{b}$ in \hat{K} : Es ist

$$|a_{k_n}^n - a_{k_{n'}}^{n'}| = |\underline{a_{k_n}^n} - \underline{a_{k_{n'}}^{n'}}| \leq |\underline{a_{k_n}^n} - a^n| + |a^n - a^{n'}| + |a^{n'} - \underline{a_{k_{n'}}^{n'}}| \leq \frac{1}{n} + |a^n - a^{n'}| + \frac{1}{n'}.$$

Da (a^n) eine Cauchyfolge ist, gibt es für jedes $\varepsilon > 0$ ein $N_\varepsilon \in \mathbb{N}$, so dass $|a^n - a^{n'}|, \frac{1}{n}$ und $\frac{1}{n'} < \varepsilon$ für $n, n' \geq N_\varepsilon$. Also ist b eine Cauchyfolge.

Weiter gilt

$$|a^n - b| \leq |a^n - \underline{a_{n_k}^n}| + |\underline{a_{n_k}^n} - b| \leq \frac{1}{n} + 3\varepsilon \leq 4\varepsilon$$

für $n \geq N_\varepsilon$, also $\lim_{n \rightarrow \infty} a^n = b$.

K ist ein dichter Teilkörper: Ist a repräsentiert durch die Cauchy-Folge (a_n) , so ist $\lim_{n \rightarrow \infty} a_n = a$. Ist $(K_1, | \cdot |)$ ein weiterer vollständiger bewerteter Körper, der $(K, | \cdot |)$ als dichten Teilkörper enthält, so erhält man eine kanonische, bewertungserhaltende Körperisomorphie

$$\begin{aligned} \sigma : \hat{K} &\xrightarrow{\sim} K_1 \\ \text{Klasse von } (a_n) &\mapsto \lim_{n \rightarrow \infty} a_n. \end{aligned}$$

Beispiele 16.3 (a) \mathbb{R} und \mathbb{C} mit dem üblichen Betrag $| \cdot |_\infty$ sind vollständig, und \mathbb{R} ist die Vervollständigung von \mathbb{Q} bezüglich $| \cdot |_\infty$.

(b) Die Vervollständigung von \mathbb{Q} bezüglich $| \cdot |_p$ wird mit \mathbb{Q}_p bezeichnet und heißt der Körper der p -adischen Zahlen.

(c) Ist K ein Zahlkörper und \mathfrak{p} ein Primideal in K , so heißt die Vervollständigung von K bezüglich $| \cdot |_{\mathfrak{p}}$ die \mathfrak{p} -adische Vervollständigung und wird mit $K_{\mathfrak{p}}$ bezeichnet.

(d) Ist K ein Zahlkörper und $\sigma : K \hookrightarrow \mathbb{C}$ eine Einbettung, so ist die Kompletterung K_σ von K bezüglich $| \cdot |_\sigma$ isomorph zu \mathbb{R} , wenn σ reell ist (da $K_\sigma \hookrightarrow \mathbb{R}$ und da die Kompletterung von \mathbb{Q} bezüglich $| \cdot |_\sigma$ $\mathbb{Q} = | \cdot |_\infty$ bereits \mathbb{R} ist), und isomorph zu \mathbb{C} , wenn σ komplex ist (da $K_\sigma \hookrightarrow \mathbb{C}$ eine \mathbb{R} -Algebra ist, aber nicht in \mathbb{R} enthalten).

Wir studieren im Folgenden die \mathfrak{p} -adischen Kompletterungen von Zahlkörpern.

Sei R ein kommutativer Ring mit Eins und sei $\mathfrak{a} \subseteq R$ ein Ideal. Für alle $n \geq 1$ sei

$$\begin{aligned} \pi : R/\mathfrak{a}^{n+1} &\rightarrow R/\mathfrak{a}^n \\ x \bmod \mathfrak{a}^{n+1} &\mapsto x \bmod \mathfrak{a}^n \end{aligned}$$

die kanonische Surjektion.

Lemma/Definition 16.4 (a) Eine Familie (a_n) mit $x_n \in R/\mathfrak{a}^n$ heißt **kompatibel**, wenn $\pi_n(a_{n+1}) = a_n$ für alle $n \in \mathbb{N}$.

(b) Sei

$$\hat{R} := \hat{R}^{\mathfrak{a}} := \{(x_n) \in \prod_{n \in \mathbb{N}} R/\mathfrak{a}^n \mid \pi_n(x_{n-1}) = x_n \quad \forall n \in \mathbb{N}\}$$

die Menge aller kompatiblen Familien. Dann ist \hat{R} bezüglich der Verknüpfungen

$$(x_n) + (y_n) := (x_n + y_n)$$

ein Ring (also ein Unterring des Produktrings $\prod_n R/\mathfrak{a}^n$) und heißt die **\mathfrak{a} -adische Kompletterung** von R .

(c) Für $x = (x_n) \in \hat{R}$ nennen wir x_n auch die n -te Komponente von x und schreiben dafür $x \bmod \mathfrak{a}^n$. Die kanonischen Abbildungen

$$\begin{aligned} R &\rightarrow \hat{R} & , & & \hat{R} &\rightarrow R/\mathfrak{a}^n \\ y &\mapsto (y \bmod \mathfrak{a}^n) & , & & x &\mapsto x_n \end{aligned}$$

sind Ringhomomorphismen.

Bemerkungen 16.5 Man sagt auch, dass

$$\hat{R} = \varprojlim_n R/\mathfrak{a}^n$$

der projektive Limes des projektiven Systems (R/\mathfrak{a}^n) mit den Übergangsabbildungen π_n (bzw. $\pi_{m,n} : R/\mathfrak{a}^m \rightarrow R/\mathfrak{a}^n$ für $m \geq n$) ist. Dies ist ein Spezialfall des allgemeineren Begriffs eines projektiven Limes, siehe z.B. Algebra II, §2.

Lemma 16.6 Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein nilpotentes Ideal ($\mathfrak{a}^n = 0$ für ein $n \geq 0$). Dann gilt für $x \in R$

$$x \in R^\times \iff x \bmod \mathfrak{a} \in (R/\mathfrak{a})^\times .$$

Beweis “ \Rightarrow ” gilt immer (für jedes Ideal).

“ \Leftarrow ”: Ist $x \bmod \mathfrak{a}$ Einheit in R/\mathfrak{a} , so gibt es ein $y \in R$ mit

$$xy = 1 - a \quad , a \in \mathfrak{a} .$$

Ist nun $\mathfrak{a}^n = 0$, so gilt

$$(1 - a)(1 + a + a^2 + \dots + a^{n-1}) = 1 - a^n = 1 ,$$

also ist $y(1 + a + \dots + a^{n-1})$ ein Inverses von x in R .

Corollar 16.7 Sei R ein Integritätsring und \mathfrak{m} ein maximales Ideal, und sei $R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}R$ die Lokalisierung von R nach \mathfrak{m} . Dann ist für alle $n \in \mathbb{N}$ die Abbildung

$$\varphi_n : R/\mathfrak{m}^n \rightarrow R_{\mathfrak{m}}/\mathfrak{m}^n R_{\mathfrak{m}}$$

ein Isomorphismus, und die Kompletztierung

$$\hat{R} = \varprojlim_n R/\mathfrak{m}^n \xrightarrow{\sim} \varprojlim_n R_{\mathfrak{m}}/\mathfrak{m}^n R_{\mathfrak{m}} = \widehat{R}_{\mathfrak{m}}$$

ist ein lokaler Ring.

Beweis φ_n ist bijektiv: Dies folgt unter Benutzung von 16.6 genauso wie im Beweis von Lemma 13.10 (Fall $n = 1$).

\hat{R} ist lokal: Sei $x = (x_n)_{n \geq 1} \in \hat{R}$. Dann gilt

$$(16.7.1) \quad x \in \hat{R}^\times \iff x_1 \in (R/\mathfrak{m})^\times .$$

“ \Rightarrow ”: Allgemein gilt für jeden Ringhomomorphismus $\sigma : A \rightarrow B : a \in A^\times \Rightarrow \sigma(a) \in B^\times$.

“ \Leftarrow ”: Ist x_1 eine Einheit, so sind nach 16.6 alle x_n Einheiten (Es ist $R/\mathfrak{m} \cong (R/\mathfrak{m}^n)/(\mathfrak{m}/\mathfrak{m}^n)$, und für das Ideal $\mathfrak{m}/\mathfrak{m}^n \subseteq R/\mathfrak{m}^n$ ist $(\mathfrak{m}/\mathfrak{m}^n)^n = 0$). Ist nun $y_n \in R/\mathfrak{m}^n$ das (eindeutig bestimmte!) Inverse von x_n , so gilt $1 = \pi_n(x_{n+1} \cdot y_{n+1}) = \pi_n(x_{n+1}) \cdot \pi_n(y_{n+1}) = x_n \pi_n(y_{n+1})$, woraus wegen der Eindeutigkeit des Inversen $\pi_n(y_{n+1}) = y_n$ folgt. Also ist $y = (y_n)$ eine kompatible Familie, d.h., in \hat{R} , und es gilt $xy = 1$.

Aus (16.7.1) folgt nun (da R/\mathfrak{m} ein Körper ist)

$$\hat{R} \setminus \hat{R}^\times = \ker(\hat{R} \rightarrow R/\mathfrak{m}) ,$$

so dass $\hat{R} \setminus \hat{R}^\times$ ein Ideal ist, und die Behauptung folgt mit 15.13.

Sei \mathcal{O} ein Dedekindring, $0 \neq \mathfrak{p} \subseteq \mathcal{O}$ ein Primideal und $v_{\mathfrak{p}}$ die zugehörige diskrete Exponential-Bewertung (genauso definiert wie in 15.15 (b)):

$$v_{\mathfrak{p}}(\alpha) = n_{\mathfrak{p}}, \text{ falls } 0 \neq (\alpha) = \prod_{\mathfrak{q}} \mathfrak{q}^{n_{\mathfrak{q}}};$$

dabei interessiert uns vor allem der in 15.15 (b) behandelte Fall der Zahlkörper). Sei $K = \text{Quot}(\mathcal{O})$ der Quotientenkörper von \mathcal{O} , und sei $\hat{K}_{\mathfrak{p}}$ die Komplettierung von K bezüglich irgendeiner zu $v_{\mathfrak{p}}$ gehörigen Absolutbewertung $|\cdot|_{\mathfrak{p}}$ (z.B. $|\alpha|_{\mathfrak{p}} = e^{-v_{\mathfrak{p}}(\alpha)}$); aber die Komplettierung ist für jede äquivalente Bewertung dieselbe). Nach 16.2 ist $\hat{K}_{\mathfrak{p}}$ ein vollständig diskret bewerteter Körper, bezüglich einer kanonischen Fortsetzung $\hat{v}_{\mathfrak{p}}$ von $v_{\mathfrak{p}}$. Sei

$$\hat{\mathcal{O}}_{\mathfrak{p}} = \{a \in \hat{K}_{\mathfrak{p}} \mid v_{\mathfrak{p}}(a) \geq 0\}$$

der zugehörige Bewertungsring, und sei $\hat{\mathfrak{p}}$ das maximale Ideal darin.

Satz 16.8 (a) Für alle $n \geq 1$ sind die kanonischen Abbildungen

$$\mathcal{O}/\mathfrak{p}^n \rightarrow \hat{\mathcal{O}}_{\mathfrak{p}}/\hat{\mathfrak{p}}^n$$

Isomorphismen.

(b) Es ist $\hat{\mathfrak{p}}^n = \mathfrak{p}^n \hat{\mathcal{O}}_{\mathfrak{p}}$, und $\hat{\mathcal{O}}_{\mathfrak{p}}$ ist isomorph zur \mathfrak{p} -adischen Komplettierung von \mathcal{O} .

Beweis Sei $\mathcal{O}_{\mathfrak{p}} \subseteq K$ der Bewertungsring in K bezüglich $v_{\mathfrak{p}}$. Wie in 15.15 (b) folgt, dass $\mathcal{O}_{\mathfrak{p}}$ die Lokalisierung von \mathcal{O} nach dem Primideal \mathfrak{p} ist. Die Abbildung

$$\psi_n : \mathcal{O}_{\mathfrak{p}} \rightarrow \hat{\mathcal{O}}_{\mathfrak{p}}/\hat{\mathfrak{p}}^n$$

hat den Kern $\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}}$, wegen $\hat{v}_{\mathfrak{p}|K} = v_{\mathfrak{p}}$ (nach 15.19 (b) ist $\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}} = (\mathfrak{p} \mathcal{O}_{\mathfrak{p}})^n = \{x \in K \mid v_{\mathfrak{p}}(x) \geq n\}$ und $\hat{\mathfrak{p}}^n = \{x \in \hat{K}_{\mathfrak{p}} \mid \hat{v}_{\mathfrak{p}}(x) \geq n\}$).

Weiter ist ψ_n surjektiv: Da K dicht in $\hat{K}_{\mathfrak{p}}$ ist, gibt es zu jedem $a \in \hat{\mathcal{O}}_{\mathfrak{p}}$ ein $\alpha \in K$ mit

$$(16.8.1) \quad v_{\mathfrak{p}}(a - \alpha) \geq n.$$

Wegen $v_{\mathfrak{p}}(\alpha) \geq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(\alpha - a)) \geq 0$ ist dann $\alpha \in \mathcal{O}_{\mathfrak{p}}$, und wegen (16.8.1) gilt

$$a - \alpha \in \hat{\mathfrak{p}}^n.$$

Es ergibt sich also ein Isomorphismus

$$(16.8.2) \quad \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}} \xrightarrow{\sim} \hat{\mathcal{O}}_{\mathfrak{p}}/\hat{\mathfrak{p}}^n.$$

Zusammen mit dem Isomorphismus

$$\mathcal{O}/\mathfrak{p}^n \xrightarrow{\sim} \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}}$$

aus 16.7 ergibt sich die Behauptung (a).

(b): Die Wertegruppen sind gleich für die Bewertungen auf K und $\hat{K}_{\mathfrak{p}}$. Jedes Element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ist also ein Primelement für $\mathcal{O}_{\mathfrak{p}}$ und für $\hat{\mathcal{O}}_{\mathfrak{p}}$, und es folgt $(\hat{\mathfrak{p}})^n = \pi^n \hat{\mathcal{O}}_{\mathfrak{p}} = \mathfrak{p}^n \hat{\mathcal{O}}_{\mathfrak{p}}$ wegen $\mathfrak{p} \subseteq \hat{\mathfrak{p}}$. Die letzte Behauptung von (b) folgt aus (a) und dem folgenden Satz, angewendet auf $\mathcal{O}_{\mathfrak{p}}$.

Satz 16.9 Sei K ein vollständiger diskret bewerteter Körper mit zugehörigen Bewertungsring \mathcal{O} . Sei \mathfrak{m} das maximale Ideal in \mathcal{O} und $\hat{\mathcal{O}}$ die \mathfrak{m} -adische Kompletterung von \mathcal{O} . Dann ist die kanonische Abbildung

$$\varphi : \mathcal{O} \rightarrow \hat{\mathcal{O}}$$

ein Homöomorphismus. Hierbei trage $\hat{\mathcal{O}}$ die Unterraumtopologie bezüglich der Inklusion

$$\begin{aligned} \hat{\mathcal{O}} &\subseteq \prod_n \mathcal{O}/\mathfrak{m}^n \\ (x_n) &\mapsto (x_n), \end{aligned}$$

wobei das rechte Produkt die Produkttopologie trägt, bezüglich der diskreten Topologien auf den Faktoren $\mathcal{O}/\mathfrak{m}^n$.

Beweis Die Abbildung ist *injektiv*, denn der Kern ist $\bigcap_{n \geq 1} \mathfrak{m}^n = 0$ ($0 \neq \alpha \in \mathcal{O}, v(\alpha) = \nu \Rightarrow \alpha \in \mathfrak{m}^{\nu} \setminus \mathfrak{m}^{\nu+1}$).

Surjektivität: Ist $(x_n) \in \hat{\mathcal{O}}$ und wählen für jedes $n \geq 1$ ein $y_n \in \mathcal{O}$ mit $y_n \bmod \mathfrak{m}^n = x_n$, so ist $(y_n)_{n \geq 1}$ eine Cauchyfolge (für $m, n \geq N$ ist, wegen der Kompatibilität der $x_n, y_m \equiv y_n \equiv -y_N \bmod \mathfrak{m}^N$, also $v(y_m - y_n) \geq N$ für die normalisierte Bewertung v). Also existiert $y = \lim_{n \rightarrow \infty} y_n$ in K (da K vollständig ist), und es gilt $y \in \mathcal{O}$ (da alle $y_n \in \mathcal{O}$) und weiter $y \equiv y_n \bmod \mathfrak{m}^n$, also $y \bmod \mathfrak{m}^n = x_n$ für alle n .

In $\prod_n \mathcal{O}/\mathfrak{m}^n$ sind die Mengen

$$U_n = \{0\} \times \dots \times \{0\} \times \prod_{\nu \geq n} \mathcal{O}/\mathfrak{m}^{\nu}$$

(für $n \geq 1$) eine Umgebungsbasis der 0 (da die Topologie auf den $\mathcal{O}/\mathfrak{m}^{\nu}$ diskret sein sollte). Damit sind in $\hat{\mathcal{O}} \subseteq \prod_{\nu} \mathcal{O}/\mathfrak{m}^{\nu}$ die Mengen

$$\ker(\hat{\mathcal{O}} \rightarrow \mathcal{O}/\mathfrak{m}^n)$$

(für $n \geq 1$) eine Umgebungsbasis der 0. Unter der Bijektion φ entsprechen diese Mengen den Mengen

$$\mathfrak{m}^n \quad (n \geq 1),$$

die gerade eine Umgebungsbasis der 0 bilden. Es folgt, dass φ ein Homöomorphismus topologischer Gruppen ist (betrachte entsprechend auch die Umgebungsbasen für beliebige Elemente a ; hier entsprechen sich $a + \mathfrak{m}^n$ und $\varphi(a) + U_n$).

Wir geben noch eine etwas explizitere Beschreibung der betrachteten Körper.

Sei K ein vollständiger diskret bewerteter Körper mit Bewertungsring \mathcal{O} . Die folgende Eigenschaft unterscheidet diese Körper stark von den archimedischen Körpern \mathbb{R} oder \mathbb{C} .

Lemma 16.10 In K konvergiert jede Reihe

$$\sum_{n=1}^{\infty} a_n$$

deren Reihenglieder a_n gegen Null konvergieren.

Beweis Sei $\lim_{n \rightarrow \infty} a_n = 0$. Wir haben zu zeigen, dass dann die Partialsummen eine Cauchyfolge bilden. Ist aber $\varepsilon > 0$ und $|a_n| < \varepsilon$ für alle $n \geq N$, so gilt für alle $n \geq N$ und alle $M \geq 0$

$$|a_n + a_{n+1} + \dots + a_{n+M}| \leq \max_{i=0, \dots, M} |a_{n+i}| < \varepsilon$$

wegen der verschärften Dreiecksungleichung.

Satz 16.11 Sei $R \subseteq \mathcal{O}$, mit $0 \in R$, ein **Restsystem**, d.h., ein Repräsentantensystem für \mathcal{O}/\mathfrak{p} . Dann besitzt jedes $x \in K \setminus \{0\}$ eine eindeutige Darstellung als Reihe

$$x = \pi^m (a_0 + a_1 \pi + a_2 \pi^2 + \dots)$$

mit $m \in \mathbb{Z}$ und $a_i \in R, a_0 \neq 0$. Es ist in diesem Fall $v(x) = m$.

Beweis Sei $x = \pi^m \cdot u$ mit $m \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$ (siehe 15.19 (a)). Dabei ist $m = v(x)$. Wir zeigen nun durch Induktion, dass u für jedes $n \in \mathbb{N}$ eine Darstellung

$$(16.11.1) \quad u = a_0 + a_1 \pi + a_2 \pi^2 + \dots + a_{n-1} \pi^{n-1} + \pi^n \cdot b_n$$

mit eindeutigen $a_0, \dots, a_{n-1} \in R, a_0 \neq 0$ und $b_n \in \mathcal{O}$ besitzt.

Dies gilt offenbar für $n = 1$, nach Wahl des Restsystems: es gibt ein eindeutig bestimmtes $a_0 \in R \setminus \{0\}$ mit $u \equiv a_0 \pmod{\mathfrak{p}}$, und dann ist $u - a_0 = \pi \cdot b_1$ mit eindeutigem $b_1 \in \mathcal{O}$. Ist nun schon (16.11.1) gefunden, dann ist der Repräsentant $a_n \in R$ von $b_n \pmod{\pi \mathcal{O}}$ eindeutig bestimmt und

$$u = a_0 + a_1 \pi + \dots + a_n \pi^n + \pi^{n+1} b_{n+1}$$

mit einem eindeutig bestimmten $b_{n+1} \in \mathcal{O}$. Die Eindeutigkeit der a_i und b_i ergibt sich sukzessive durch Betrachtung von $u \pmod{\pi^i \mathcal{O}}, i = 1, \dots, n$. Wir erhalten hierdurch eine eindeutig bestimmte Reihe

$$\sum_{n=0}^{\infty} a_n \pi^n$$

die gegen u konvergiert, weil die Restglieder $\pi^n b_n$ gegen null gehen.

Beispiele 16.12 (a) Sei p eine Primzahl. Nach dem bisher Bewiesenen ist der Bewertungsring von \mathbb{Q}_p gleich

$$\mathbb{Z}_p = \hat{\mathbb{Z}}^{(p)},$$

die p -adische (= (p) -adische) Kompletterung von \mathbb{Z} . Wir haben Isomorphismen für alle n

$$\mathbb{Z}/p^n \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/p^n \mathbb{Z}_p,$$

insbesondere ist der Restklassenkörper (Fall $n = 1$) gleich $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Da $0, \dots, p - 1$ ein Restsystem für $\mathbb{Z}/p\mathbb{Z}$ ist, hat jede p -adische Zahl $\alpha \in \mathbb{Q}_p$ eine eindeutige Darstellung

$$\alpha = p^n(a_0 + a_1p + \dots + a_np^n + \dots)$$

mit $a_i \in \{0, \dots, p - 1\}, a_0 \neq 0, n \in \mathbb{Z}$. Es ist $\alpha \in \mathbb{Z}_p$ genau dann, wenn $n \geq 0$, wenn also

$$\alpha = \sum_{n=0}^{\infty} b_n p^n$$

mit $b_n \in \{0, \dots, p - 1\}$. Die Elemente in \mathbb{Z}_p heißen auch **ganze p -adische Zahlen**.

(b) Für alle $x \in p\mathbb{Z}_p$ (dem maximalen Ideal von \mathbb{Z}_p) konvergiert der p -adische Logarithmus

$$\log_p(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

und die p -adische Exponentialfunktion

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Dies ist nicht ganz offensichtlich, da $v_p(n!) \rightarrow \infty$ für $n \rightarrow \infty$, also $|n!|_p \rightarrow 0$ für $n \rightarrow \infty$; außerdem konvergiert $|n|_p$ nicht für $n \rightarrow \infty$. Es gilt aber $v_p\left(\frac{p^n}{n!}\right), v_p\left(\frac{x}{n}\right) \rightarrow \infty$ für $n \rightarrow \infty$, also $\left|\frac{x^n}{n}\right|_p, \left|\frac{x^n}{n!}\right|_p \rightarrow 0$.

17 Vollständige nicht-archimedische Körper

Sei $(K, |\cdot|)$ ein vollständiger nicht-archimedisch bewerteter Körper (mit $|\cdot|$ nicht-trivial). Sei \mathcal{O} der zugehörige Bewertungsring, mit maximalem Ideal \mathfrak{p} und Restklassenkörper $k = \mathcal{O}/\mathfrak{p}$.

Definition 17.1 Ein Polynom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathcal{O}[x]$$

heißt **primitiv**, wenn $f(x) \not\equiv 0 \pmod{\mathfrak{p}}$ ist, d.h., wenn

$$|f| := \max\{|a_0|, \dots, |a_n|\} = 1.$$

Satz 17.2 (“Henselsches Lemma”) Sei $f(x) \in \mathcal{O}[x]$ ein primitives Polynom. Besitzt $\bar{f}(x) = f(x) \pmod{\mathfrak{p}} \in k[x]$ eine Zerlegung

$$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$$

mit teilerfremden Polynomen $\bar{g}, \bar{h} \in k[x]$, so besitzt $f(x)$ eine Zerlegung

$$f(x) = g(x)h(x)$$

mit Polynomen $g, h \in \mathcal{O}[x]$, wobei $\deg g = \deg \bar{g}$ und

$$\bar{g} = g \bmod \mathfrak{p} \quad , \quad \bar{h} = h \bmod \mathfrak{p} .$$

Beweis: Sei $d = \deg f$ und $m = \deg \bar{g}$, so dass also $d - m \geq \deg \bar{h}$. Seien $g_0, h_0 \in \mathcal{O}[x]$ mit $\bar{g} = g_0 \bmod \mathfrak{p}, \bar{h} = h_0 \bmod \mathfrak{p}, \deg g_0 = \deg \bar{g} = m$ und $\deg h_0 \leq d - m$. Wegen $(\bar{g}, \bar{h}) = 1$ gibt es $a(x), b(x) \in \mathcal{O}[x]$ mit

$$ag_0 + bh_0 \equiv 1 \bmod \mathfrak{p} .$$

Für die Polynome

$$f - g_0h_0 \quad , \quad ag_0 + bg - 1 \quad \in \mathfrak{p}[x]$$

sei $\pi \in \mathfrak{p}$ ein Koeffizient mit maximalen Betrag $|\pi|$. Für die gesuchten Polynome g und h machen wir den Ansatz

$$\begin{aligned} g &= g_0 + p_1\pi + p_2\pi^2 + \dots \\ h &= h_0 + q_1\pi + q_2\pi^2 + \dots \end{aligned}$$

mit Polynomen $p_i, q_i \in \mathcal{O}[x]$ vom Grad $< m$ bzw. $\leq d - m$. Wegen der Vollständigkeit von K sind diese Reihen konvergiert und ergeben Polynome in $\mathcal{O}[x]$ vom Grad m bzw. $\leq d - m$, wobei nach Konstruktion $g \equiv g_0 \equiv \bar{g} \bmod \mathfrak{p}$ und $h \equiv h_0 \equiv \bar{h} \bmod \mathfrak{p}$ gilt. Dabei bestimmen wir induktiv die p_i und q_i derart, dass für die Polynome

$$\begin{aligned} g_n &= g_0 + p_1\pi + \dots + p_n\pi^n \\ h_n &= h_0 + q_1\pi + \dots + q_n\pi^n \end{aligned}$$

die Beziehung

$$(17.2.1) \quad f \equiv g_n h_n \bmod \pi^{n+1}$$

gilt. Durch Grenzübergang ergibt sich dann die gewünschte Gleichung $f = gh$.

Für $n = 0$ gilt (17.2.1) nach Wahl von g_0, h_0 und π . Gilt (17.2.1) für $n - 1$ und ist $n \geq 1$, so läuft (17.2.1) für n wegen

$$g_n = g_{n-1} + p_n\pi \quad , \quad h_n = h_{n-1} + q_n\pi$$

auf die Beziehung

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \bmod \pi^{n+1}$$

hinaus, also nach Division durch π^n auf die Konvergenz

$$(17.2.2) \quad f_n \equiv (g_{n-1}q_n + h_{n-1}p_n) \bmod \pi ,$$

wobei $f_n := (f - g_{n-1}h_{n-1})/\pi^n \in \mathcal{O}[x]$ nach Induktionsvoraussetzung.

Nach Wahl von π gilt $g_0a + h_0b \equiv 1 \bmod \pi$ und damit

$$(17.2.2') \quad g_0af_n + h_0bf_n \equiv f_n \bmod \pi ,$$

aber die Grade von af_n und bf_n könnten noch falsch sein. Mittels Polynomdivision durch $g_0(x)$ (in $K[x]$) erhalten wir

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x)$$

mit $\deg p_n < \deg g_0 = m$. Wegen $\deg g_0 = \deg \bar{g}_0 = m$ ist der führende Koeffizient von g_0 eine Einheit in \mathcal{O} , so dass $q(x) \in \mathcal{O}[x]$, und wir erhalten die Kongruenz

$$(17.2.3) \quad g_0(af_n + h_0q) + h_0p_n \equiv f_n \pmod{\pi}.$$

Streichen wir noch aus dem Polynom $af_n + h_0q$ alle durch π teilbaren Koeffizienten heraus, so erhalten wir ein Polynom q_n , das zusammen mit p_n die Kongruenz (17.2.2) erfüllt, wobei wegen $\deg f_n \leq d$, $\deg h_0p_n < (d-m) + m = d$ und $\deg g_0 = m$ gilt: $\deg q_n = \deg \bar{q}_n \leq d-m$.

Beispiel 17.3 (a) Sei p eine Primzahl. Das Polynom $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ zerfällt über dem Restklassenkörper $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ in verschiedene Linearfaktoren. Nach mehrfacher Anwendung des Henselschen Lemmas (auf den vollständigen bewerteten Körper $(\mathbb{Q}_p, |\cdot|_p)$ mit Bewertungsring \mathbb{Z}_p) zerfällt es also auch über \mathbb{Q}_p in (notwendigerweise) paarweise teilerfremde Linearfaktoren. Also enthält \mathbb{Q}_p die Gruppe μ_{p-1} aller $(p-1)$ -ten Einheitswurzeln. Weiter bildet die Menge $\mu_{p-1} \cup \{0\}$ ein Restsystem. Dabei ist $\mu_{p-1} \rightarrow \mathbb{F}_p^\times$ ein Isomorphismus bezüglich der Multiplikation; man spricht auch von einem **multiplikativen Restsystem**.

(b) Allgemeiner folgt, dass für einen Zahlkörper K und ein Primideal \mathfrak{p} für K die \mathfrak{p} -adische Komplettierung $K_{\mathfrak{p}}$ die $(q-1)$ -ten Einheitswurzeln enthält, wobei $q = N\mathfrak{p}$ die Mächtigkeit des Restklassenkörpers $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ ist. Hierbei ist $\mathcal{O}_{\mathfrak{p}}$ der Bewertungsring von $|\cdot|_{\mathfrak{p}}$ in $K_{\mathfrak{p}}$, also die \mathfrak{p} -adische Komplettierung von \mathcal{O}_K . Dieser Ring heißt auch der Ring der ganzen Zahlen in $K_{\mathfrak{p}}$. Weiter ist $\mu_{q-1} \cup \{0\}$ ein multiplikatives Restsystem für $K_{\mathfrak{p}}$.

Corollar 17.4 Für jedes irreduzible Polynom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$$

gilt

$$|f| = \max\{|a_0|, |a_1|\}.$$

Insbesondere gilt $f \in \mathcal{O}[x]$, falls $a_n = 1$ und $a_0 \in \mathcal{O}$.

Beweis Nach Multiplikation mit einem geeigneten Element $\alpha \in K^\times$ (nämlich dem Inversen eines Koeffizienten a_i mit $|a_i| = |f|$) können wir annehmen, dass $f \in \mathcal{O}[x]$ und $|f| = 1$. Sei a_r der Koeffizient mit minimalem r , so dass $|a_r| = 1$. Dann gilt

$$f(x) \equiv x^r(a_r + a_{r+1}x + \dots + a_n x^{n-r}) \pmod{\mathfrak{p}}$$

mit $a_r \equiv 0 \pmod{\mathfrak{p}}$. Wäre nun $\max\{|a_0|, |a_n|\} < 1$, so wäre $0 < r < n$, und x^r wäre teilerfremd zum Polynom in der Klammer, und nach dem Henselschen Lemma wäre $f(x)$ zerlegbar – Widerspruch! Der Zusatz ist klar, da $f \in \mathcal{O}[x]$ wenn $|f| = 1$.

Als Anwendung erhalten wir die folgende Aussage, die im Kontrast zur Situation von Zahlkörpern steht, wo für eine Erweiterung L/K , ein Primideal \mathfrak{p} für K und zwei verschiedene Primideale $\mathfrak{P}, \mathfrak{P}'$ für L über \mathfrak{p} zwei Fortsetzungen $|\cdot|_{\mathfrak{P}}$ und $|\cdot|_{\mathfrak{P}'}$ von $|\cdot|_{\mathfrak{p}}$ existieren, die verschieden sind (vergleiche Übungsaufgabe 52 (ii)).

Satz 17.5 Ist L/K eine endliche Erweiterung, so lässt sich $|\cdot|_{\mathfrak{p}}$ in eindeutiger Weise zu einer Bewertung $|\cdot|$ auf L fortsetzen. Diese ist durch

$$|\alpha| = \sqrt[r]{|N_{L/K}(\alpha)|} \quad \text{für } \alpha \in L$$

gegeben, wobei $n = [L : K]$. Der bewertete Körper $(L, | \cdot |)$ ist wieder vollständig.

Beweis: Existenz der Fortsetzung: Sei \mathcal{O} der Bewertungsring $| \cdot |$ in K , und sei \mathcal{O}_L der ganze Abschluss von \mathcal{O} in L . Dann gilt

$$(17.5.1) \quad \mathcal{O}_L = \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}\}.$$

Denn: Sei $\alpha \in L$ und

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in K[x]$$

das Minimalpolynom von α über K . Ist nun $\alpha \in \mathcal{O}_L$, so ist $f \in \mathcal{O}[x]$ und damit auch $N_{L/K}(\alpha) = \pm a_0 \in \mathcal{O}$. Ist umgekehrt $a_0 = \pm N_{L/K}(\alpha) \in \mathcal{O}$, so liegt f nach 17.4 in $\mathcal{O}[x]$, und damit ist α ganz über \mathcal{O} , d.h., in \mathcal{O}_L .

Wir zeigen nun, dass durch $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ eine Bewertung auf L gegeben ist. Die Bedingungen $|\alpha| = 0 \Leftrightarrow \alpha = 0$ und $|\alpha\beta| = |\alpha||\beta|$ gelten offensichtlich. Die verschärfte Dreiecksungleichung

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\},$$

wobei ohne Einschränkung $\alpha, \beta \neq 0$ sei, läuft nach Division durch $\max\{|\alpha|, |\beta|\}$, auf eine Beziehung

$$|\alpha| \leq 1 \quad \Leftrightarrow \quad |\alpha + 1| \leq 1$$

hinaus. Nach Definition und nach (17.5.1) bedeutet dies aber die Beziehung

$$\alpha \in \mathcal{O}_L \quad \Leftrightarrow \quad \alpha + 1 \in \mathcal{O}_L,$$

was gilt, da \mathcal{O}_L ein Ring mit Eins ist.

Also ist $| \cdot |$ eine Bewertung auf L , die $| \cdot |$ auf K fortsetzt, da für $a \in K$ gilt: $N_{L/K}(a) = a^n$.

Eindeutigkeit der Fortsetzung: Sei $| \cdot |'$ eine weitere Fortsetzung von $| \cdot |$ auf L , mit Bewertungsring \mathcal{O}' . Sei \mathfrak{P} bzw. \mathfrak{P}' das maximale Ideal von \mathcal{O}_L bzw. \mathcal{O}' (wir haben oben gesehen, dass $\mathcal{O}_L = \{\alpha \in L \mid |\alpha| \leq 1\}$, also gleich dem Bewertungsring von $| \cdot |$ auf L ist). Wir zeigen zuerst, dass $\mathcal{O}_L \subseteq \mathcal{O}'$. Sei $\alpha \in \mathcal{O}_L \setminus \mathcal{O}'$, und sei

$$f(x) = x^d + a_1x^{d-1} + \dots + a_d$$

das Minimalpolynom von α über K . Dann ist (wegen $\alpha \in \mathcal{O}_L$) $a_1, \dots, a_d \in \mathcal{O}$ und (wegen $K \setminus \mathcal{O}' = \{\beta \in K \mid |\beta|' > 1\}$) $\alpha^{-1} \in \mathfrak{P}'$, also $1 = -a_1\alpha^{-1} - \dots - a_d(\alpha^{-1})^d \in \mathfrak{P}'$ – Widerspruch! Also gilt $\mathcal{O}_L \subset \mathcal{O}'$, und damit auch $\mathfrak{P} \subset \mathfrak{P}'$, da $\mathcal{O}_L \cap \mathfrak{P}'$ ein von null verschiedenes Ideal in \mathcal{O}_L ist (da $| \cdot |$ auf K nicht-trivial ist), und damit $\mathfrak{P} = \mathcal{O}_L \cap \mathfrak{P}' \subseteq \mathfrak{P}'$. Dies bedeutet aber die Beziehung

$$|\alpha| < 1 \quad \Leftrightarrow \quad |\alpha|' < 1 \quad \text{für alle } \alpha \in L,$$

und damit die Äquivalenz von $| \cdot |$ und $| \cdot |'$; siehe den Beweis von Satz 15.4, wo nur die Implikation $|x|_1 < 1 \Rightarrow |x|_2 < 1$ benutzt wurde, um die Äquivalenz von $| \cdot |_1$ und $| \cdot |_2$ zu zeigen.

Die Gleichheit von $| \cdot |$ und $| \cdot |'$ auf L folgt nun aus dem folgenden Lemma.

Lemma 17.6 Sei K ein Körper, $| \cdot |$ eine nicht-triviale Bewertung auf K , sei L/K eine Körpererweiterung und seien $| \cdot |_1$ und $| \cdot |_2$ zwei Fortsetzungen von $| \cdot |$ auf L . Sind $| \cdot |_1$ und $| \cdot |_2$ äquivalent, so ist $| \cdot |_1 = | \cdot |_2$.

Beweis: Ist $|x|_1 = |x|_2^t$ für alle $x \in L$ mit einem $t > 0$, so folgt $|x| = |x|^t$ für alle $x \in K$. Ist $| \cdot |$ nicht-trivial, so folgt hieraus $t = 1$.

Wir fahren mit dem Beweis von 17.5 fort, wobei $(K, | \cdot |)$ wieder vollständig nicht-archimedisch bewertet ist.

Die **Vollständigkeit** von $(L, | \cdot |)$ folgt aus dem nächsten Satz.

Satz 17.7 Sei $(V, \| \cdot \|)$ ein endlich-dimensionaler normierter K -Vektorraum, d.h., $\| \cdot \|: V \rightarrow \mathbb{R}_{\geq 0}$ sei eine Abbildung mit den Eigenschaften

- (i) $\| x \| = 0 \Leftrightarrow x = 0$ für alle $x \in V$.
- (ii) $\| ax \| = |a| \cdot \| x \|$ für alle $a \in K, x \in V$.
- (iii) $\| x + y \| \leq \| x \| + \| y \|$ für alle $x, y \in V$.

Dann ist V (bezüglich der Metrik $d(x, y) = \| x - y \|$) vollständig.

Hieraus folgt in der Situation von 17.5 tatsächlich die Vollständigkeit von L , denn die Fortsetzung von $| \cdot |$ auf L definiert eine Norm auf dem n -dimensionalen K -Vektorraum L .

Beweis von Satz 17.7: Sei v_1, \dots, v_n eine K -Basis von V und $\| \cdot \|_{\infty}$ die zugehörige Maximumsnorm auf V :

$$\left\| \sum_{i=1}^n a_i v_i \right\|_{\infty} := \max\{|a_1|, \dots, |a_n|\}.$$

Es folgt aus der Vollständigkeit von K , dass V mit dieser Maximumsnorm vollständig ist. Daher genügt es zu zeigen, dass jede Norm $\| \cdot \|$ auf V zu $\| \cdot \|_{\infty}$ äquivalent ist, d.h., dass es Konstanten $\rho, \rho' > 0$ gibt mit

$$\rho \| x \|_{\infty} \leq \| x \| \leq \rho' \| x \|_{\infty}.$$

Für ρ' können wir aber $\|v_1\| + \dots + \|v_n\|$ wählen. Die Existenz von ρ folgt mit vollständiger Induktion über $n = \dim_K V$, wobei der Fall $n = 1$ mit $\rho = \|v_1\|$ gilt. Sei für $\dim V = n - 1$ alles bewiesen. Ist nun $\dim V = n$, so ist für jedes $i \in \{1, \dots, n\}$ der Unterraum

$$V_i = Kv_1 + \dots + Kv_{i-1} + Kv_{i+1} + \dots + Kv_n$$

nach Induktionsvoraussetzung bezüglich der Einschränkung von $\| \cdot \|$ vollständig, also abgeschlossen in V . Damit ist auch $v_i + V_i$ abgeschlossen. Wegen

$$0 \notin \bigcup_{i=1}^n (v_i + V_i) =: M$$

gibt es eine zu M disjunkte offene Umgebung von 0, d.h. (durch Betrachtung einer ρ -Umgebung von 0), es gibt ein $\rho > 0$ mit

$$\|v_i + w_i\| \geq \rho$$

für alle $i \in \{1, \dots, n\}$ und alle $w_i \in V_i$. Für $x = \sum_{i=1}^n a_i v_i \in V \setminus \{0\}$ und r so gewählt dass $|a_r| = \max\{|a_1|, \dots, |a_n|\} = \|x\|_{\infty}$ gilt dann

$$\|a_r^{-1} x\| = \left\| \frac{a_1}{a_r} v_1 + \dots + v_r + \dots + \frac{a_n}{a_r} v_n \right\| \geq \rho,$$

so dass

$$\|x\| \geq \rho \|x\|_\infty.$$

18 Zahlkörper und ihre Kompletzierungen

Sei K ein Körper.

Definition 18.1 Eine (Prim-)Stelle von K ist die Äquivalenzklasse $\langle | \rangle$ einer Bewertung $| \cdot |$ auf K .

Wir bezeichnen Stellen oft mit Buchstaben v, w, \dots , was nicht mit den Exponentialbewertungen verwechselt werden sollte.

Definition 18.2 Sei L/K eine Körpererweiterung und v eine Stelle von K .

(a) Eine Stelle w von L heißt Fortsetzung von v , wenn $w|_K$ gleich v ist, d.h., wenn für eine (und damit jede) Bewertung $| \cdot |'$ von L , die w repräsentiert, die Einschränkung $| \cdot |'_K$ in v liegt.

(b) Sei L/K eine Galoiserweiterung mit Galoisgruppe G . Für eine Bewertung $| \cdot |$ auf L mit $\sigma \in G$ sei ${}^\sigma | \cdot |$ die Bewertung, die durch ${}^\sigma |x| = |\sigma^{-1}x|$ definiert wird. Für eine Stelle $w = \langle | \cdot |' \rangle$ von L sei $\sigma w = \langle {}^\sigma | \cdot |' \rangle$ (Dies ist wohldefiniert, da für $| \cdot |' \sim | \cdot |''$ offenbar ${}^\sigma | \cdot |' \sim {}^\sigma | \cdot |''$).

(c) Für eine Stelle w von L heißt

$$G_w = \{\sigma \in G \mid \sigma w = w\}$$

die **Zerlegungsgruppe** von w in G .

(d) Ist w nicht-archimedisch, so heißt

$$I_w = \{\sigma \in G_w \mid |\sigma x - x|_w < 1 \text{ für alle } x \in L \text{ mit } |x|_w \leq 1\}$$

die Trägheitsgruppe von w in $\text{Gal}(L/K)$. Hierbei sei $| \cdot |_w$ eine Bewertung, die w repräsentiert.

Bemerkungen 18.3 (a) Offenbar hängt I_w in 18.2 (d) nicht von der Wahl von $| \cdot |_w$ ab; weiter sieht man leicht, dass I_w eine Untergruppe von G_w ist.

(b) Ist $w|_K$ nicht-trivial, so folgt aus Lemma 17.6

$$G_w = \{\sigma \in G \mid {}^\sigma | \cdot |_w = | \cdot |_w\}$$

falls $w = \langle | \cdot |_w \rangle$.

Beispiele 18.4 (a) Sei L/K eine Galoiserweiterung von Zahlkörpern mit Galoisgruppe G und $\mathfrak{P} \subseteq \mathcal{O}_L$ ein Primideal. Sei w die durch $| \cdot |_{\mathfrak{P}}$ gegebene Stelle. Dann ist

$$G_w = G_{\mathfrak{P}} = \{\tau \in G \mid \tau \mathfrak{P} = \mathfrak{P}\}$$

die übliche Zerlegungsgruppe von \mathfrak{P} . Denn für $\tau \in G$ gilt $\tau|_{\mathfrak{P}} = |_{\tau\mathfrak{P}}$, und \mathfrak{P} ist durch w eindeutig bestimmt (vergleiche auch Übungsaufgabe 52): Es ist $\mathfrak{P} = \{x \in L \mid |x|_{\mathfrak{P}} < 1\}$, und es gilt für Bewertungen $| \cdot |$ und $| \cdot |'$

$$(18.4.1) \quad | \cdot | \sim | \cdot |' \Leftrightarrow (|x| < 1 \Leftrightarrow |x|' < 1 \quad \forall x \in K)$$

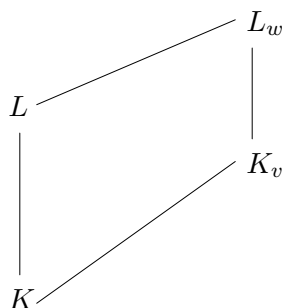
(vergleiche den Beweis von 15.4). Ebenso ist

$$I_w = I_{\mathfrak{P}} = \{\tau \in G_{\mathfrak{P}} \mid \sigma x \equiv x \pmod{\mathfrak{P}}\}$$

die übliche Trägheitsgruppe von L/K .

(b) Nun sei $\sigma : L \hookrightarrow \mathbb{C}$ eine Einbettung und $| \cdot |_{\sigma}$ die zugehörige Bewertung. Für $\rho \in G$ ist dann $\rho|_{\sigma} = |_{\sigma\rho^{-1}}$. Gilt $\rho|_{\sigma} = |_{\sigma}$, also auch $\rho^{-1}|_{\sigma} = |_{\sigma}$, so folgt (vergleiche Übungsaufgabe 52 (iii)) $\sigma\rho = \sigma$ oder $\sigma\rho = \bar{\sigma} = c\sigma$, wobei c die komplexe Konjugation auf \mathbb{C} ist. Im ersten Fall ist $\rho = id$; im zweiten Fall ist $\sigma\rho^2 = c\sigma\rho = c^2\sigma = \sigma$, also $\rho^2 = id$. Weiter gilt $\rho = \rho'$ falls $\sigma\rho = \sigma\rho'$. Die Zerlegungsgruppe hat also die Ordnung 1 oder 2.

Sei L/K eine Körpererweiterung, v eine Stelle von K , w eine Fortsetzung von v auf L . Seien K_v und L_w die Kompletterungen von K bezüglich v bzw. von L bezüglich w . Es ist klar, dass wir eine Einbettung $K_v \hookrightarrow L_w$ erhalten, und weiter ein Körperdiagramm



(die Striche stehen wie üblich für Einbettungen). Die Fortsetzungen von v bzw. w auf K_v bzw. L_w seien wieder mit v bzw. w bezeichnet.

Satz 18.5 Es gibt kanonische Isomorphismen

$$\begin{aligned}
 G_w(L/K) &\cong Gal(L_w/K_v) \\
 I_w(L/K) &\cong I_w(L_w/K_v).
 \end{aligned}$$

Beweis Nach 17.5 ist die Fortsetzung von v auf K_v zu w auf L_w eindeutig. Daher lässt jedes $\sigma \in Gal(L_w/K_v)$ die Stelle w fest, und wir erhalten durch Einschränkung einen Homomorphismus

$$\varphi : Gal(L_w/K_v) \rightarrow G_w(L/K)$$

(da L/K galoissch ist, gilt $\sigma|_L(L) \subseteq L$), der $I_w(L_w/K_v)$ in $I_w(L/K)$ abbildet. Da jedes $\sigma \in Gal(L_w/K_v)$ stetig bezüglich w ist und L dicht in L_w liegt, ist φ injektiv. Umgekehrt ist auch jedes $\sigma \in G_w(L/K)$ stetig bezüglich w und setzt sich daher eindeutig zu einem Isomorphismus der Kompletterung L_w fort, der K_v festlässt, weil der in K_v dichte Körper

K festgelassen wird, und der in $I_w(L_w/K_v)$ liegt, wenn σ in $I_w(L/K)$ liegt. Dies zeigt, dass φ surjektiv ist und auch einen Isomorphismus der Trägheitsgruppen induziert.

Wir erhalten auch eine “lokale” Beschreibung der Diskriminante.

Sei A ein Dedekindring, $\mathfrak{p} \subseteq A$ ein Primideal, $A_{\mathfrak{p}}$ die Lokalisierung und $\hat{A}_{\mathfrak{p}}$ die Komplette- rung. Dann haben wir gesehen: Die maximalen Ideale von $A_{\mathfrak{p}}$ bzw. $\hat{A}_{\mathfrak{p}}$ sind $\mathfrak{p}' = \mathfrak{p}A_{\mathfrak{p}}$ bzw. $\hat{\mathfrak{p}} = \mathfrak{p}\hat{A}_{\mathfrak{p}}$. Weiter gilt für alle $n \in \mathbb{N}$

$$(18.6.1) \quad \hat{\mathfrak{p}}^n \cap A_{\mathfrak{p}} = \mathfrak{p}'^n \quad , \quad \mathfrak{p}'^n \cap A = \mathfrak{p}^n .$$

Für ein Ideal $\mathfrak{a} = \prod_{\mathfrak{q}} \mathfrak{q}^{n_{\mathfrak{q}}}$ gilt weiter $\mathfrak{a}A_{\mathfrak{p}} = (\mathfrak{p}')^{n_{\mathfrak{p}}}$, $\mathfrak{a}\hat{A}_{\mathfrak{p}} = \hat{\mathfrak{p}}^{n_{\mathfrak{p}}}$. Wir können also $n_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{a})$ herausbekommen, indem wir in $A_{\mathfrak{p}}$ oder $\hat{A}_{\mathfrak{p}}$ rechnen.

Sei nun L eine endliche separable Erweiterung von $K = \text{Quot}(A)$ und B der ganze Abschluss von A in L .

Satz 18.6 Sei $\mathfrak{p} \subseteq A$ ein Primideal. Dann gilt

$$v_{\mathfrak{p}}(\mathfrak{d}_{B/A}) = v_{\mathfrak{p}}(\mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}) = \sum_{\mathfrak{P}/\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{d}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}}) ,$$

wobei $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$ die Lokalisierung von B nach \mathfrak{p} ist und $\hat{B}_{\mathfrak{P}}$ die \mathfrak{P} -adische Kom- plettierung von B . (Wir bezeichnen die normierten Exponentialbewertungen auf $A_{\mathfrak{p}}$ und $\hat{A}_{\mathfrak{p}}$ wieder mit $v_{\mathfrak{p}}$).

Beweis Die erste Gleichheit folgt unter Benutzung von (18.6.1) wie im Beweis der Behaup- tung 2 im Beweis von 14.2; Abschnitt 14.12: Es gilt

$$(18.6.2) \quad \mathfrak{p}^n \mid \mathfrak{d}_{B/A} \quad \Leftrightarrow \quad (\mathfrak{p}')^n \mid \mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} .$$

Die zweite Gleichheit folgt so: Ist e_1, \dots, e_n eine $A_{\mathfrak{p}}$ -Basis von $B_{\mathfrak{p}}$, so sind die Bilder e_1, \dots, e_n auch eine $\hat{A}_{\mathfrak{p}}$ -Basis der \mathfrak{p} -adischen Komplette- rung

$$\hat{B}_{\mathfrak{p}} = \varprojlim_m B_{\mathfrak{p}}/\mathfrak{p}^m B_{\mathfrak{p}}$$

von $B_{\mathfrak{p}}$; hieraus folgt

$$(18.6.3) \quad \mathfrak{d}_{\hat{B}_{\mathfrak{p}}/\hat{A}_{\mathfrak{p}}} = \mathfrak{d}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}\hat{A}_{\mathfrak{p}} .$$

Ist nun $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ die Primzerlegung von y in B , so ist nach dem chinesischen Restsatz kanonisch

$$\begin{array}{ccc} B_{\mathfrak{p}}/\mathfrak{p}^m B_{\mathfrak{p}} & \xrightarrow{\sim} & \prod_{i=1}^r B_{\mathfrak{p}}/\mathfrak{P}_i^{me_i} B_{\mathfrak{p}} \\ \parallel \wr & & \parallel \wr \\ B/\mathfrak{p}^m B & \xrightarrow{\sim} & \prod_{i=1}^r B/\mathfrak{P}_i^{me_i} B . \end{array}$$

Hieraus folgt die Isomorphie

$$\hat{B}_{\mathfrak{p}} \cong \prod_{i=1}^r \hat{B}_{\mathfrak{p}_i}.$$

Zusammen mit Lemma 14.10 folgt

$$(18.6.4) \quad \mathfrak{d}_{\hat{B}_{\mathfrak{p}}/\hat{A}_{\mathfrak{p}}} = \prod_{i=1}^r \mathfrak{d}_{\hat{B}_{\mathfrak{p}_i}/A_{\mathfrak{p}}}.$$

Aus (18.6.3) und (18.6.4) folgt die zweite Gleichheit in Satz 18.6.