Algebraische Zahlentheorie

Vorlesung an der HU Berlin
im Sommersemester 2017

Thomas Krämer

Dateiversion vom 9.10.2017

Inhaltsverzeichnis

KAPITEL I

Einführung: Faktorielle Ringe

Den Begriff *Algebraische Zahlentheorie* kann man auf zwei verschiedene Weisen verstehen:

- Zunächst als algebraische Theorie der Zahlen, also das Studium der ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\} \subset \mathbb{Q}$ mit Methoden der Algebra.
- Allgemeiner aber auch als Theorie algebraischer Zahlen, also das Studium von Zahlringen in algebraischen Körpererweiterungen $K/\mathbb{Q}$.

In diesem Kapitel werden wir sehen, wie die erste Perspektive in natürlicher Weise auf die zweite führt und welche Fragen sich hierbei ergeben.

1. Summen zweier Quadrate

Welche natürlichen Zahlen $p \in \mathbb{N}$ lassen sich als $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ schreiben? Betrachten wir der Einfachheit halber den Fall von Primzahlen. Die kleinsten ungeraden Primzahlen, welche sich als Summe zweier Quadrate schreiben lassen, sind

$$\begin{aligned} 5 &= 2^2 + 1^2 \\ 13 &= 3^2 + 2^2 \\ 17 &= 4^2 + 1^2 \\ 29 &= 5^2 + 2^2 \\ 37 &= 6^2 + 1^2 \\ 41 &= 5^2 + 4^2 \\ 53 &= 7^2 + 2^2 \\ 61 &= 6^2 + 5^2 \\ 73 &= 8^2 + 3^2 \\ 89 &= 8^2 + 5^2 \\ 97 &= 9^2 + 4^2 \\ &\vdots \end{aligned}$$

Ein Muster wird erkennbar, wenn man diese Primzahlen auf einem Primzahlsieb markiert:

	3	5	7		11	13			17	19	
	23			29	31				37		
41	43		47			53				59	
61			67		71	73				79	
	83			89					97		
101	103		107	109		113					
			127		131				137	139	
				149	151				157		
	163		167			173				179	
181					191	193			197	199	

Alle ungeraden Zahlen der Form $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ haben Rest 1 bei Division durch 4, denn

$$x^2 \equiv \begin{cases} 0 \mod 4 & \text{für} \quad x \in 2\mathbb{Z}, \\ 1 \mod 4 & \text{für} \quad x \in 1 + 2\mathbb{Z}. \end{cases}$$

Ist p eine Primzahl, so gilt auch die Umkehrung; dies besagt das folgende 1640 von Fermat formulierte Kriterium, dessen erste Beweise von Euler, Lagrange und Gauss stammen:

SATZ 1.1. *Eine Primzahl $p \neq 2$ hat die Form $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ genau dann, wenn $p = 4m + 1$ für eine natürliche Zahl $m \in \mathbb{N}$ ist.*

Beweis. Sei $p = 4m + 1$ prim für ein $m \in \mathbb{N}$. Wir betrachten den endlichen Körper

$$\mathbb{F}_p \;=\; \mathbb{Z}/p\mathbb{Z} \;=\; \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}.$$

Aus der Algebra ist bekannt, dass die multiplikative Gruppe $\mathbb{F}_p^\times = (\mathbb{F}_p \setminus \{0\},\ \cdot\ )$ dieses Körpers zyklisch von der Ordnung $p - 1$ ist. Sei $\zeta \in \mathbb{Z}$ eine ganze Zahl, deren Restklasse $\overline{\zeta} \in \mathbb{F}_p$ ein Erzeuger dieser zyklischen Gruppe, also eine primitive $(p-1)$-te Einheitswurzel ist. Für die Restklasse der ganzen Zahl $x = \zeta^m \in \mathbb{Z}$ gilt dann offenbar

$$\overline{x}^2 \;=\; \overline{\zeta}^{(p-1)/2} = -1,$$

d.h.

$$p \mid (x^2 + 1).$$

Wir wollen jetzt diese Teilbarkeit und die Primzahleigenschaft von p ausnutzen und dazu $x^2 + 1$ in nichttrivialer Weise als ein Produkt zweier Faktoren schreiben. Dies ist offenbar in $\mathbb{Z}$ nicht immer möglich; aber $x^2 + 1 = (x + i)(x - i)$ in dem größeren Ring

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

Wir werden sehen, dass in diesem Ring der sogenannten *Gauß'schen ganzen Zahlen* eine ähnliche Primfaktorzerlegung wie für gewöhliche ganze Zahlen existiert:

- Jedes $z \in \mathbb{Z}[i]$ lässt sich als Produkt sogenannter *irreduzibler Elemente* schreiben, von denen sich kein von ± 1 und $\pm i$ verschiedener Faktor mehr abspalten lässt.
- Diese Zerlegung ist *eindeutig* bis auf die Reihenfolge der Faktoren und bis auf Multiplikation beliebiger Faktoren mit ± 1 und $\pm i$.

Im nächsten Abschnitt werden wir diese Eigenschaften in dem allgemeinen Begriff eines faktoriellen Ringes präzisieren. Zurück zu unserem Beweis:

Per Konstruktion gilt $p \mid (x+i)(x-i)$. Wäre die Zahl p ein irreduzibles Element von $\mathbb{Z}[i]$, so müsste sie wegen der Eindeutigkeit der Primfaktorzerlegung einen der beiden Faktoren des Produktes $(x + i)(x - i)$ teilen, was wegen $(x \pm i)/p \notin \mathbb{Z}[i]$ unmöglich ist. Also existiert eine Zerlegung

$$p \;=\; z \cdot w \quad \text{mit} \quad z, w \;\in\; \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}.$$

Durch Anwenden der Norm $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z},\ x \mapsto x \cdot \overline{x}$ auf beiden Seiten erhalten wir dann

$$p^2 \;=\; N(z) \cdot N(w) \quad \text{mit} \quad N(z), N(w) \;\in\; \mathbb{Z} \setminus \{\pm 1\}.$$

Da p eine Primzahl ist, folgt $p = N(z)$. Dies liefert eine Darstellung von $p = a^2 + b^2$ als Summe zweier Quadrate, indem man $z = a + ib$ mit $a, b \in \mathbb{Z}$ schreibt. □

Übung 1.2. Wir können nun auch die Darstellbarkeit beliebiger natürlicher Zahlen als Summe zweier Quadrate diskutieren:

(1) Wir haben gesehen, dass jede Primzahl $p \equiv 1 \mod 4$ in dem Ring $\mathbb{Z}[i]$ als Produkt zweier irreduzibler Faktoren zerfällt. Man überlege sich, dass jede Primzahl $p \equiv 3 \mod 4$ in diesem Ring irreduzibel bleibt.

(2) Jede natürliche Zahl ist ein Produkt $n = \prod_{p\,\mathrm{prim}} p^{\nu_p}$ von Primzahlen p mit Vielfachheiten $\nu_p \geq 0$. Man finde hiervon ausgehend ein notwendiges und hinreichendes Kriterium für die Existenz einer Darstellung $n = x^2+y^2$ als Summe von Quadraten ganzer Zahlen $x, y \in \mathbb{Z}$.

Übung 1.3. Man benutze die eindeutige Primfaktorzerlegung in $\mathbb{Z}[i]$, um alle ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $y^2 = x^3 - 4$ zu finden.

2. Faktorielle Ringe

Wir wollen nun die oben benutzten Teilbarkeitsregeln präzisieren. Zunächst sei daran erinnert, dass ein *Ring* eine Menge R mit binären Verknüpfungen $+$ und $\cdot$ ist, welche folgenden Axiomen genügen:

- $(R, +)$ ist eine abelsche Gruppe,
- $(R, \cdot\,)$ ist ein Monoid, d.h. die Verknüpfung $\cdot$ ist assoziativ und es gibt ein Einselement $1 \in R$ mit $1 \cdot a = a = a \cdot 1$ für alle $a \in R$,
- es gilt das Distributivgesetz $a \cdot (b + c) = ab + ac$ und $(b + c) \cdot a = ba + ca$ für alle $a, b, c \in R$.

Ein Ring R heißt *kommutativ*, wenn $ab = ba$ für alle $a, b \in R$ gilt. Wir bezeichnen mit

$$R^\times \;=\; \left\{\, r \in R \;\mid\; \exists s \in R \;\text{ mit }\; rs = sr = 1 \,\right\}$$

die Gruppe der multiplikativ invertierbaren Elemente eines Ringes R. Diese Gruppe heißt *Einheitengruppe* und ihre Elemente werden *Einheiten* des Ringes genannt. So gilt etwa

- $\mathbb{Z}^\times = \{\pm 1\}$,
- $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$,
- $K^\times = K \setminus \{0\}$ für Körper K,
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{m} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(m, n) = 1\}$,
- $Mat_{n\times n}(k)^\times = Gl_n(k) = \{M \in Mat_{n\times n}(k) \mid \det(M) \neq 0\}$, etc.

Im Folgenden werden wir uns primär für *Integritätsringe* interessieren, d.h. für kommutative Ringe $R \neq \{0\}$ mit der Eigenschaft $ab \neq 0$ für alle $a, b \in R \setminus \{0\}$.

Beispiel 2.1. Es ist $\mathbb{Z}/n\mathbb{Z}$ ein Integritätsring genau für n prim oder $n = 0$.

Beispiel 2.2. Körper sind Integritätsringe. Teilringe eines Integritätsrings sind wieder Integritätsringe. Umgekehrt bettet sich jeder Integritätsring R in einen Körper ein, den *Quotientenkörper* $K = Quot(R)$; formal lässt sich dieser als Menge der Äquivalenzklassen

$$Quot(R) \;=\; \big\{(a, b) \in R^2 \mid b \neq 0\big\}/\approx$$

bezüglich der Äquivalenzrelation $(a, b) \approx (c, d) \iff ad = bc$ definieren. So gilt beispielsweise

$$Quot(\mathbb{Z}) \;=\; \mathbb{Q}, \quad Quot(\mathbb{Z}[i]) \;=\; \mathbb{Q}(i), \quad \text{usw.}$$

DEFINITION 2.3. Sei R ein Integritätsring. Man bezeichnet ein Element $a \in R$ als *Teiler* von $c \in R$ und schreibt $a \mid c$, falls $c = ab$ für ein $b \in R$ ist. Ist dabei b eine Einheit, so nennt man a *assoziiert* zu c und schreibt $a \sim c$. Ein *echter Teiler* von c ist ein Teiler, welcher weder eine Einheit noch assoziiert zu c ist.

Der Begriff einer Primzahl lässt sich in diesem Kontext auf zwei verschiedene Weisen verallgemeinern:

DEFINITION 2.4. Sei R ein Integritätsring. Ein Element $c \in R \setminus R^\times \cup \{0\}$ heißt

- *irreduzibel*, falls c keine echten Teiler besitzt,
- *prim*, wenn für alle $a, b \in R$ gilt: Aus $c \mid ab$ folgt $c \mid a$ oder $c \mid b$.

BEISPIEL 2.5. Im vorigen Abschnitt haben wir gesehen, dass in $R = \mathbb{Z}[i]$ eine Primzahl $p \in \mathbb{N}$ genau dann irreduzibel bleibt, wenn sie von der Form $p = 4m + 3$ für eine natürliche Zahl $m \in \mathbb{N}$ ist.

LEMMA 2.6. *In Integritätsringen R ist jedes Primelement irreduzibel.*

Beweis. Sei $c \in R$ nicht irreduzibel, also $c = ab$ mit echten Teilern $a, b \in R$ und somit $c \mid ab$. Wäre c prim in R, so müsste $c \mid a$ oder $c \mid b$ gelten. Nach Vertauschen der beiden Teiler können wir oBdA $c \mid a$ annehmen, sei also $a = cb'$ mit $b' \in R$. Es folgt

$$0 \;=\; c - ab \;=\; c \cdot (1 - bb')$$

und damit $bb' = 1$, weil R ein Integritätsring und $c \neq 0$ ist. Also ist $b \in R^\times$ eine Einheit und somit kein echter Teiler im Widerspruch zur Annahme. □

DEFINITION 2.7. Ein *faktorieller Ring* ist ein Integritätsring R, in welchem jedes Element $r \in R \setminus (R^\times \cup \{0\})$ ein endliches Produkt von Primelementen ist. Dies lässt sich äquivalent auch durch folgende zwei Axiome charakterisieren:

(1) Jedes $r \in R \setminus (R^\times \cup \{0\})$ ist ein endliches Produkt irreduzibler Elemente.
(2) Jedes irreduzible Element von R ist prim.

Dabei stellt die zweite Eigenschaft sicher, dass die Faktorisierung in irreduzible Elemente im Wesentlichen eindeutig ist:

PROPOSITION 2.8. *Sei R ein Integritätsring, $p_1, \ldots, p_r \in R$ prim, $q_1, \ldots, q_s \in R$ irreduzibel und*

$$p_1 \cdots p_r \;=\; q_1 \cdots q_s.$$

Dann gilt $r = s$, und nach eventuellem Umnumerieren hat man $p_i \sim q_i$ für alle i.

Beweis. Nach Annahme ist $p_1 \mid q_1 \cdots q_s$. Da p_1 prim ist, folgt nach eventuellem Umnumerieren $p_1 \mid q_1$. Die Irreduzibilität von q_1 liefert nun $p_1 \sim q_1$, also $p_1 = \epsilon q_1$ mit $\epsilon \in R^\times$ und somit

$$p_1 \cdot (p_2 \cdots p_r - \epsilon q_2 \cdots q_s) \;=\; 0.$$

Da R ein Integritätsring ist, muß der eingeklammerte Ausdruck verschwinden, und die Behauptung folgt nun durch Induktion über $\min\{s, r\}$, indem man q_2 durch das hierzu assoziierte Element ϵq_2 ersetzt. □

3. Euklidische und Hauptidealringe

Wie sieht man einem Integritätsring R an, ob er faktoriell ist? In $R = \mathbb{Z}$ spielt die Division mit Rest für den Euklidischen Algorithmus eine zentrale Rolle. Dies motiviert den folgenden Begriff:

DEFINITION 3.1. Ein Integritätsring R heißt *Euklidisch* bezüglich einer gegebenen Abbildung $N : R \longrightarrow \mathbb{N}_0$, wenn gilt:

(1) Es ist $N(a) = 0$ genau für $a = 0$.
(2) Für alle $a, b \in R$, $b \neq 0$ gibt es $c, r \in R$ mit $a = bc + r$ und $N(r) < N(b)$.

Wir wollen die klassischen Argumente für $\mathbb{Z}$ übertragen, um zu sehen, dass jeder Euklidische Ring R faktoriell ist. Erinnern wir uns zunächst, dass im klassischen Fall aus dem Euklidischen Algorithmus folgt, dass für $a, c \in \mathbb{Z}$ die Menge der Linearkombinationen

$$\mathfrak{a} \;=\; \left\{\, ra + sc \;\mid\; r, s \in \mathbb{Z} \,\right\} \;\subseteq\; \mathbb{Z}$$

genau aus den ganzzahligen Vielfachen des größten gemeinsamen Teilers $\mathrm{ggT}(a, c)$ besteht. Diese Teilmenge ist ein Ideal:

DEFINITION 3.2. Ein *Ideal* eines kommutativen Ringes R ist eine Untergruppe $\mathfrak{a}$ von $(R, +)$, die unter Multiplikation mit beliebigen Ringelementen stabil ist; wir schreiben dann $\mathfrak{a} \trianglelefteq R$. In diesem Fall trägt $R/\mathfrak{a}$ eine natürliche Ringstruktur, und die Quotientenabbildung $\varphi : R \twoheadrightarrow R/\mathfrak{a}$ ist ein Ringhomomorphismus mit $\ker(\varphi) = \mathfrak{a}$. Umgekehrt ist für jeden beliebigen Ringhomomorphismus $\psi : R \to S$ der Kern $\ker(\psi)$ ein Ideal von R. Man kann also Ideale äquivalent auch als die Kerne von Ringhomomorphismen definieren. Für Ringelemente $a_1, \ldots, a_n \in R$ bezeichnen wir mit

$$(a_1, \ldots, a_n) \;=\; \left\{\, r_1 a_1 + \cdots + r_n a_n \;\mid\; r_1, \ldots, r_n \in R \,\right\} \;\trianglelefteq\; R$$

das von diesen erzeugte Ideal. Ein *Hauptideal* ist ein Ideal der Form (a) mit $a \in R$; ist jedes Ideal von R ein Hauptideal, so heißt R ein *Hauptidealring*.

Die oben zitierte Folgerung aus dem Euklidischen Algorithmus besagt, dass $\mathbb{Z}$ ein Hauptidealring ist. Allgemeiner gilt:

PROPOSITION 3.3. *Jeder Euklidische Ring R ist ein Hauptidealring.*

Beweis. Sei R ein Euklidischer Ring bezüglich $N : R \longrightarrow \mathbb{N}_0$. Für $\mathfrak{a} \trianglelefteq R$ wähle man $a \in \mathfrak{a} \setminus \{0\}$ mit

$$N(r) \;\geq\; N(a) \quad \text{für alle} \quad r \;\in\; \mathfrak{a} \setminus \{0\}.$$

Diese Minimalitätseigenschaft impliziert durch Division mit Rest r im Euklidischen Ring R, dass jedes Element von $\mathfrak{a}$ durch a teilbar sein muß, d.h. es ist $\mathfrak{a} = (a)$. □

SATZ 3.4. *Jeder Hauptidealring R ist faktoriell.*

Beweis. Wir zeigen zunächst, dass jedes Element von R ein endliches Produkt von irreduziblen Elementen ist. Wäre dies nicht der Fall, so könnten wir eine unendliche Folge $a_1, a_2, a_3, \cdots \in R$ finden, sodass a_{n+1} ein echter Teiler von a_n ist für alle n. Dann wäre

$$(a_1) \;\subsetneq\; (a_2) \;\subsetneq\; (a_3) \;\subsetneq\; \cdots$$

eine unendliche echt aufsteigende Folge von Idealen in R. Andererseits wäre auch die Vereinigung

$$\mathfrak{a} \;=\; \bigcup_{n \geq 1} (a_n) \;\trianglelefteq\; R$$

ein Ideal. Da R ein Hauptidealring ist, gäbe es ein $a \in R$ mit $\mathfrak{a} = (a)$. Wegen $a \in \mathfrak{a}$ wäre $a \in (a_n)$ für ein $n \in \mathbb{N}$ und somit $\mathfrak{a} = (a_n)$ im Widerspruch dazu, dass alle Inklusionen in der obigen Folge von Idealen strikt sind.

Zu zeigen bleibt, dass jedes irreduzible Element $c \in R$ prim ist. Seien $a, b \in R$ und $c \mid ab$. Da R ein Hauptidealring ist, gilt

$$(a, c) \;=\; (d) \quad \text{für ein} \quad d \;\in\; R.$$

Wegen $c \in (d)$ ist d ein Teiler von c. Da irreduzible Elemente keine echten Teiler haben, bleiben nur zwei Fälle: Entweder ist $d \in R^\times$ und somit $(a, c) = R$. In diesem Fall hat man

$$1 \;=\; ra + sc \quad \text{für geeignete} \quad r, s \;\in\; R$$

und c ist somit ein Teiler von $b = rab + scb$ wie gewünscht. Oder es ist $d \sim c$. In diesem Fall ist $(a, c) = (c)$ und somit insbesondere c ein Teiler von a. □

4. Beispiele und Ausblick

Abschließend seien einige einfache Beispiele betrachtet. Das folgende Lemma mit $d = 1$ liefert die Rechtfertigung für unsere naive Rechnung in den Gauß'schen ganzen Zahlen zu Beginn dieses Kapitels:

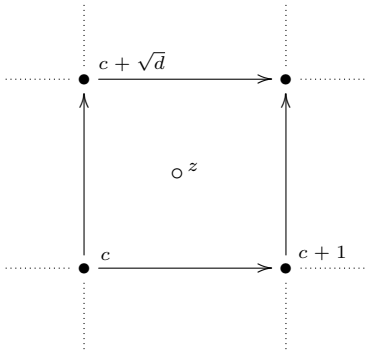
LEMMA 4.1. *Der Ring $R = \mathbb{Z}[\sqrt{d}]$ ist für $d \in \{-1, -2\}$ Euklidisch bezüglich der Funktion*

$$N(z) \;=\; z\overline{z}.$$

Beweis. Offenbar ist $N(z) = 0$ genau für $z = 0$. Für die Division mit Rest genügt es wegen der Multiplikativität der Norm zu zeigen, dass für alle $a, b \in R$ mit $b \neq 0$ ein $c \in R$ existiert mit

$$N(a/b - c) \;<\; 1.$$

Dazu genügt es zu zeigen, dass es zu jeder komplexen Zahl $z \in \mathbb{C}$ einen Punkt $c \in R$ im Abstand $|z - c| < 1$ gibt:



Für $d \in \{-1, -2\}$ ist dies offenbar der Fall: Der schlimmstmögliche Punkt z liegt in der Mitte einer Masche des Gitters $R = \mathbb{Z}[\sqrt{d}]$ und sein Abstand vom nächsten Gitterpunkt ist $\frac{1}{2}\sqrt{1 - d} < 1$. □

Im Fall $d > 0$ kann man den Absolutbetrag komplexer Zahlen durch den Betrag der Norm

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} : \quad \mathbb{Q}(\sqrt{d}) \;\longrightarrow\; \mathbb{Q}, \quad a + b\sqrt{d} \;\mapsto\; (x + y\sqrt{d})(x - y\sqrt{d}) \quad \text{für} \quad x, y \in \mathbb{Q}$$

ersetzen und erhält auch hier einige Euklidische Beispiele:

LEMMA 4.2. *Der Ring $R = \mathbb{Z}[\sqrt{d}]$ ist für $d \in \{2, 3\}$ Euklidisch bezüglich der Funktion*

$$N: \quad R \longrightarrow \mathbb{N}_0, \quad z \mapsto |N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(z)|.$$

Beweis. Wie im Beweis von Lemma 4.1 genügt es zu zeigen, dass für alle $a, b \in R$ mit $b \neq 0$ ein $c \in R$ mit $N(a/b - c) < 1$ existiert. Wegen $a/b \in \mathbb{Q}(\sqrt{d})$ können wir dabei

$$a/b = x + y\sqrt{d} \quad \text{mit} \quad x, y \in \mathbb{Q}$$

schreiben. Zu zeigen ist dann die Existenz von ganzen Zahlen $m, n \in \mathbb{Z}$, sodass die Ungleichung

$$\Big|(x-m)^2 - d \cdot (y-n)^2\Big| = N\Big((x-m) + (y-n)\sqrt{d}\Big) < 1$$

gilt. Hierzu genügt es im Fall $d \in \{2, 3\}$ offenbar, $m, n \in \mathbb{Z}$ mit $|x-m|, |y-n| \leq 1/2$ zu wählen. □

BEMERKUNG 4.3. Man kann zeigen, dass $\mathbb{Z}[\sqrt{d}]$ für quadratfreies $d \in \mathbb{Z}$ genau dann Euklidisch bezüglich

$$z \mapsto |N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(z)|$$

ist, wenn

$$d \in \big\{-2, -1, 2, 3, 6, 7, 11, 19\big\}$$

gilt. Es gibt jedoch viele weitere Beispiele von quadratischen Zahlringen $\mathbb{Z}[\sqrt{d}]$, die zwar nicht Euklidisch bezüglich der obigen Funktion, aber bezüglich geeigneter anderer Funktionen sind. Dies ist etwa für $d = 14$ der Fall, vgl. Harper (2004).

ÜBUNG 4.4. Man zeige, dass für $4 \mid (d-1)$ das Minimalpolynom von $\alpha = \frac{1+\sqrt{d}}{2}$ ganzzahlige Koeffizienten besitzt und die Norm auf $R = \mathbb{Z}[\alpha]$ ganzzahlige Werte annimmt. Man beweise, dass R für $d \in \{-3, -7, -11\}$ Euklidisch unter der Norm ist, für $d = -15$ aber nicht einmal faktoriell. Für $d = -19$ ist R ein Hauptidealring, aber bezüglich keiner Funktion N Euklidisch (vgl. Übungsblatt 2).

Bezeichnen wir einen Teilring $R \subset K$ einer endlichen Körpererweiterung $K/\mathbb{Q}$ mit $N_{K/\mathbb{Q}}(R) \subseteq \mathbb{Z}$ als *Norm-Euklidisch*, wenn er Euklidisch bezüglich $z \mapsto |N_{K/\mathbb{Q}}(z)|$ ist, so zeigen obige Beispiele, dass für die ersten beiden der folgenden Implikationen die Umkehrung im Allgemeinen nicht gilt:

$$\text{Norm-Euklidisch} \implies \text{Euklidisch} \implies \text{Hauptidealring} \implies \text{Faktorieller Ring}$$

In beliebigen Integritätsringen gilt auch für die letzte Implikation die Umkehrung im Allgemeinen nicht, dies ist für uns aber weniger wichtig:

BEMERKUNG 4.5. In der Algebra zeigt man, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist. Auf diese Weise erhält man Beispiele von faktoriellen Ringen, die keine Hauptidealringe sind. Allerdings werden wir später sehen, dass der Ganzheitsring eines algebraischen Zahlkörpers faktoriell ist genau dann, wenn er ein Hauptidealring ist (vgl. Lemma II.4.9).

Der Ausgangspunkt der algebraischen Zahlentheorie liegt in der Beobachtung, dass nicht jeder Zahlring faktoriell ist: Beispielsweise ist der Ring $R = \mathbb{Z}[\sqrt{-5}]$ nicht faktoriell, denn

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

sind zwei verschiedene Faktorisierungen in irreduzible, paarweise nicht-assoziierte Elemente von R. Es war die Idee von Ernst Kummer (1810-1893), das Versagen der eindeutigen Primfaktorzerlegung durch die Einführung gewisser *idealer Zahlen* zu

beheben. In obigem Beispiel würde man etwa ideale Zahlen $\alpha, \beta, \gamma, \delta$ einführen mit der Eigenschaft

$$2 \;=\; \alpha\beta, \quad 3 \;=\; \gamma\delta, \quad 1+\sqrt{-5} \;=\; \alpha\gamma, \quad 1-\sqrt{-5} \;=\; \beta\delta$$

und so die beiden verschiedenen obigen Faktorisierungen auf eine gemeinsame ideale Faktorisierung zurückführen. Während Kummers ideale Zahlen ein gedankliches Konstrukt und präzise schwer faßbar blieben, hatte Richard Dedekind (1831-1916) die bahnbrechende Idee, statt einer idealen Zahl die Gesamtheit aller durch sie teilbaren Elemente von R zu betrachten; dies führte ihn zum heutigen Begriff eines *Ideals*, einem der Ausgangspunkte der modernen Algebra. Die Rolle von Ringelementen wird dabei ersetzt durch die von diesen erzeugten Hauptidealen, und an die Stelle von Primfaktorzerlegungen treten Zerlegungen eines Ideals als Produkt von Primidealen; hierbei ist das Produkt von zwei Idealen $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ definiert als

$$\mathfrak{a} \cdot \mathfrak{b} \;=\; \left\{ \textstyle\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\} \;\trianglelefteq\; R.$$

Bevor wir im nächsten Kapitel die Dedekind'sche Theorie von Zahlringen genauer entwickeln, sei sie am obigem Beispiel illustriert:

ÜBUNG 4.6. Man finde Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d} \trianglelefteq R = \mathbb{Z}[\sqrt{-5}]$ mit

$$(2) \;=\; \mathfrak{a} \cdot \mathfrak{b}, \quad (3) \;=\; \mathfrak{c} \cdot \mathfrak{d}, \quad (1+\sqrt{-5}) \;=\; \mathfrak{a} \cdot \mathfrak{c}, \quad (1-\sqrt{-5}) \;=\; \mathfrak{b} \cdot \mathfrak{d}.$$

KAPITEL II

Ganzheitsringe von Zahlkörpern

In diesem Kapitel werden wir die Dedekind'sche Idealtheorie von Zahlkörpern entwickeln und dabei

- eine intrinsische Definition des Ganzheitsringes $R = \mathfrak{o}_K$ für algebraische Zahlkörper $K/\mathbb{Q}$ geben, welche die obigen Beispiele verallgemeinert;
- zeigen, dass sich jedes Ideal eines solchen Ringes im Wesentlichen eindeutig als Produkt von Primidealen schreiben lässt;
- mit der Klassengruppe ein Maß dafür einführen, wie weit der Ring $\mathfrak{o}_K$ davon entfernt ist, ein Hauptidealring oder faktoriell zu sein.

1. Ganze Ringerweiterungen

Sei K/k eine Körpererweiterung. Ein Element $\alpha \in K$ heißt *algebraisch über* k, wenn es ein $n \in \mathbb{N}$ und $c_0, c_1, \ldots, c_{n-1} \in k$ gibt mit

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \;=\; 0.$$

Dies ist genau dann der Fall, wenn der von α erzeugte Erweiterungskörper $k(\alpha)$ endlichen Grad

$$[k(\alpha) : k] \;=\; \dim_k(k(\alpha)) \;<\; \infty$$

hat. Man nennt K/k eine *algebraischen Körpererweiterung*, wenn sie die folgenden äquivalenten Bedingungen erfüllt:

- Jedes Element $\alpha \in K$ ist algebraisch über k,
- Es ist $K = \bigcup_\nu K_\nu$ Vereinigung endlicher Körpererweiterungen K_ν/k.

In der algebraischen Zahlentheorie interessieren uns *algebraischen Zahlkörper*, die endlichen Körpererweiterungen $K/\mathbb{Q}$. In Verallgemeinerung der Gauß'schen ganzen Zahlen wollen wir jedem solchen algebraischen Zahlkörper einen Teilring $\mathfrak{o}_K \subset K$ mit $Quot(\mathfrak{o}_K) = K$ zuordnen, welcher die Rolle von $\mathbb{Z} \subset \mathbb{Q}$ übernimmt. Die weiter unten eingeführte Norm und Spur sollten auf diesem Teilring ganzzahlige Werte annehmen,

$$\begin{array}{ccc} K & \overset{N_{K/\mathbb{Q}}}{\underset{tr_{K/\mathbb{Q}}}{\rightleftarrows}} & \mathbb{Q} \\ \uparrow & & \uparrow \\ \mathfrak{o}_K & \dashrightarrow & \mathbb{Z} \end{array}$$

Allgemeiner sollten für $\alpha \in \mathfrak{o}_K$ alle Koeffizienten des charakteristischen Polynoms von α in $\mathbb{Z}$ liegen. Wir bezeichnen eine algebraische Zahl $\alpha \in K$ als *ganz*, wenn sie im Sinn der folgenden Definition ganz über $\mathbb{Z}$ ist:

Definition 1.1. Ein Element α eines kommutativen Ringes S heißt *ganz* über einem Teilring $R \subseteq S$, wenn es ein $n \in \mathbb{N}$ und Koeffizienten $c_0, c_1, \ldots, c_{n-1} \in R$ gibt mit

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \;=\; 0.$$

Man nennt $R \subseteq S$ eine *ganze Ringerweiterung* und sagt kurz, dass S ganz über R sei, wenn alle Elemente $\alpha \in S$ ganz über R sind.

Im Falle von Körpererweiterungen stimmt dies genau mit dem obigen Begriff der Algebraizität überein. Ebenso wie dort hat man auch für ganze Elemente in Ringerweiterungen mehrere alternative Charakterisierungen, wobei Vektorräume durch Moduln zu ersetzen sind:

DEFINITION 1.2. Sei R ein kommutativer Ring. Ein *R-Modul* ist eine abelsche Gruppe $(M, +)$ mit einer Verknüpfung

$$R \times M \longrightarrow M, \quad (r, m) \mapsto r \cdot m,$$

sodass für alle $r, s \in R$, $m, n \in M$ gilt:

$$\begin{aligned} 1 \cdot m &= m, \\ r \cdot (s \cdot m) &= (r \cdot s) \cdot m, \\ (r + s) \cdot m &= r \cdot m + s \cdot m, \\ r \cdot (m + n) &= r \cdot m + r \cdot n. \end{aligned}$$

Ein R-Modul M heißt *endlich erzeugt*, wenn ein $n \in \mathbb{N}$ und $m_1, \ldots, m_n \in M$ existieren mit

$$M = Rm_1 + \cdots + Rm_n := \{ r_1 m_1 + \cdots + r_n m_n \mid r_\nu \in R \}.$$

Man sagt dann auch, dass die Elemente $m_1, \ldots, m_n$ den R-Modul M *erzeugen*.

PROPOSITION 1.3. *Für kommutative Ringe $R \subseteq S$ und $\alpha \in S$ sind äquivalent:*

(1) *Das Element $\alpha \in S$ ist ganz über R.*
(2) *Der von α erzeugte Teilring $R[\alpha] \subseteq S$ ist ein endlich erzeugter R-Modul.*
(3) *Es gibt einen endlich erzeugten R-Untermodul $M \subseteq S$ mit*

$$1 \in M \quad \text{und} \quad \alpha \cdot M \subseteq M.$$

Beweis. (1) $\Longrightarrow$ (2): Wenn $\alpha \in S$ einer Gleichung $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$ mit $c_\nu \in R$ genügt, kann man jede Potenz α^m für $m \geq n$ als R-Linearkombination der Elemente $1, \alpha, \ldots, \alpha^{n-1}$ schreiben. Diese Elemente erzeugen also den Ring $R[\alpha]$ als R-Modul:

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1} \subseteq S.$$

Für (2) $\Longrightarrow$ (3) kann man offenbar $M = R[\alpha]$ wählen. Um (3) $\Longrightarrow$ (1) zu zeigen, wollen wir den Satz von Cayley-Hamilton auf den durch die Multiplikation mit α gegebenen R-linearen Endomorphismus

$$M \longrightarrow M, \quad m \mapsto \alpha \cdot m$$

anwenden, um aus dem charakteristischen Polynom eine Ganzheitsgleichung für α zu bekommen. Zunächst schreiben wir

$$M = Rm_1 + \cdots + Rm_n \quad \text{mit} \quad m_1, \ldots, m_n \in M.$$

Wegen $1 \in M$ dürfen wir dabei $m_1 = 1$ annehmen. Die Annahme $\alpha \cdot M \subseteq M$ liefert nun ein Gleichungssystem

$$\begin{aligned} \alpha m_1 &= r_{11} m_1 + \cdots + r_{n1} m_n \\ &\vdots \\ \alpha m_n &= r_{n1} m_1 + \cdots + r_{nn} m_n \end{aligned}$$

mit $r_{ij} \in R$, welches sich in Matrixnotation schreiben lässt als

$$A \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \;=\; 0 \quad \text{mit} \quad A \;=\; \begin{pmatrix} \alpha - r_{11} & & -r_{1n} \\ & \ddots & \\ -r_{n1} & & \alpha - r_{nn} \end{pmatrix}$$

Wir betrachten die komplementäre Matrix

$$A^* \;=\; \Big((-1)^{i+j} \cdot \det(A_{ij})\Big)_{i,j=1,\ldots,n}$$

wobei die Matrix A_{ij} aus A durch Streichen der i-ten Spalte und j-ten Zeile entsteht und ihre Determinante durch die übliche Entwicklungsformel definiert wird. Wie in der linearen Algebra sieht man

$$A \cdot A^* \;=\; A^* \cdot A \;=\; \det(A) \cdot \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

und somit

$$\det(A) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \;=\; 0.$$

Wegen $m_1 = 1$ folgt $\det(A) = 0$, und dies liefert nach Entwicklung der Determinante wie gewünscht eine Ganzheitsgleichung der Form $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 \;=\; 0$ mit $c_0, c_1, \ldots, c_{n-1} \in R$. □

KOROLLAR 1.4. *Seien $R \subseteq S \subseteq T$ Erweiterungen kommutativer Ringe.*

(1) *Die Menge $\{\alpha \in S \mid \alpha \text{ ganz über } R\} \subseteq S$ ist ein Teilring, d.h. Summen und Produkte ganzer Elemente sind wieder ganz.*
(2) *Wenn die Ringerweiterungen $R \subseteq S$ und $S \subseteq T$ beide ganz sind, dann ist auch $R \subseteq T$ ganz (und umgekehrt).*

Beweis. Sind $\alpha, \beta \in S$ ganz über R, so sind die Ringe $R[\alpha], R[\beta] \subseteq S$ endlich erzeugte R-Moduln, etwa

$$R[\alpha] \;=\; Ra_1 + \cdots + Ra_n \quad \text{und} \quad R[\beta] \;=\; Rb_1 + \cdots + Rb_m$$

mit $a_i, b_j \in S$. Dann wird der Teilring

$$M \;=\; R[\alpha, \beta] \;\subseteq\; S$$

als R-Modul erzeugt von den endlich vielen Elementen der Form $a_i \cdot b_j$. Somit folgt mit Kriterium (3) in Prop. 1.3, dass alle Elemente dieses Teilrings ganz über R sind. Das gilt insbesondere für die Elemente $\alpha \pm \beta$, $\alpha \cdot \beta \in M$, also folgt (1). Der Beweis von (2) ist analog. □

DEFINITION 1.5. Für Erweiterungen $R \subseteq S$ kommutativer Ringe nennt man den Teilring $\{\alpha \in S \mid \alpha \textit{ ganz über } R\}$ den *ganzen Abschluß von R in S*. Stimmt dieser ganze Abschluß mit dem ursprünglichen Ring R überein, so sagt man auch, R sei *ganz abgeschlossen in S*. Ist R ein Integritätsring und $S = Quot(R)$, so wird der Zusatz *in S* meist weggelassen.

BEISPIEL 1.6. Faktorielle Ringe R sind ganz abgeschlossen: Sei $\alpha = \frac{a}{b} \in Quot(R)$ ganz über R für $a, b \in R$, $b \neq 0$. Nach Kürzen des Bruchs können wir annehmen, dass a und b keine gemeinsamen Primteiler besitzen. Für geeignete $c_\nu \in R$ hat man aber eine Ganzheitsgleichung

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + +c_1\alpha + c_0 \;=\; 0$$

und somit

$$a^n \;=\; -b \cdot (c_{n-1}a^{n-1} + \cdots + c_1 a b^{n-2} + b^{n-1}),$$

sodass jeder Primteiler von b auch ein solcher von a sein müsste. Also hat b keine Primteiler und muß somit eine Einheit sein, und daraus folgt $\alpha \in R$.

LEMMA 1.7. *Für jede Erweiterung $R \subseteq T$ kommutativer Ringe ist der ganze Abschluß $\{\alpha \in T \mid \alpha$ ganz über $R\}$ ganz abgeschlossen in T.*

Beweis. Das folgt unmittelbar aus der Aussage (2) im Korollar 1.4. □

In Erweiterungen von ganz abgeschlossenen Integritätsringen lässt sich die Ganzheit von Elementen anhand ihres Minimalpolynoms prüfen:

LEMMA 1.8. *Es sei R ein ganz abgeschlossener Integritätsring und S sein ganzer Abschluß in einer endlichen Erweiterung K/k von $k = Quot(S)$. Dann gilt*

(1) $K = Quot(S) = \{\frac{s}{r} \mid s \in S, r \in R\}$,

(2) $S = \big\{\alpha \in K \mid$ *das Minimalpolynom von α über k liegt in $R[x] \subseteq k[x]$*$\big\}$.

Beweis. (1) Jedes $\alpha \in K$ ist algebraisch über $k = Quot(R)$ und erfüllt somit eine Gleichung

$$r_n\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_1\alpha + r_0 \;=\; 0 \quad \text{mit} \quad r_1, \ldots, r_n \;\in\; R, \quad r_n \;\neq\; 0.$$

Multiplikation dieser Gleichung mit r_n^{n-1} liefert eine Ganzheitsgleichung für das Element $s = r_n\alpha$, und hieraus folgt die Behauptung.

(2) Wenn ein Element $\alpha \in K$ ganz über R ist, dann auch alle Konjugierten $\sigma(\alpha)$ mit $\sigma \in Gal(\overline{k}/k)$, weil eine Ganzheitsgleichung mit Koeffizienten in $R \subseteq k$ invariant unter der Galoisoperation ist. Dann sind also alle Nullstellen des Minimalpolynoms von α, und somit auch alle Koeffizienten diese Polynoms, ganz über R. Andererseits liegen diese Koeffizienten aber in $k = Quot(R)$, und weil R ganz abgeschlossen ist, folgt die Behauptung. □

Nach diesen allgemeinen Erörterungen kommen wir nun zu unserem eigentlichen Ziel zurück, dem Studium ganzer algebraischer Zahlen:

DEFINITION 1.9. Für Zahlkörper $K/\mathbb{Q}$ ist der *Ganzheitsring* $\mathfrak{o}_K \subset K$ definiert als der Teilring aller ganzen algebraischen Zahlen in dem Zahlkörper, d.h. der ganze Abschluß von $\mathbb{Z}$ in K.

Nach dem obigen Lemma gilt $K = Quot(\mathfrak{o}_K)$. Das einfachste Beispiel sind die Ganzheitsringe quadratischen Zahlkörper:

LEMMA 1.10. *Sei $K = \mathbb{Q}(\sqrt{d})$ für eine quadratfreie ganze Zahl $d \in \mathbb{Z}$. Dann hat man*

$$\mathfrak{o}_K \;=\; \mathbb{Z}[\alpha] \quad \textit{mit} \quad \alpha \;=\; \begin{cases} \frac{1+\sqrt{d}}{2} & \text{falls} \quad d \equiv 1 \mod 4, \\ \sqrt{d} & \text{falls} \quad d \equiv 2, 3 \mod 4. \end{cases}$$

Beweis. Jedes $\beta \in K$ lässt sich eindeutig in der Form $\beta = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$ schreiben und erfüllt

$$\beta^2 \;-\; 2x \cdot \beta \;+\; (x^2 - dy^2) \;=\; 0.$$

Für $y \neq 0$ ist dieses Polynom das Minimalpolynom von β, und Teil (2) von Lemma 1.8 zeigt, dass $\beta \in \mathfrak{o}_K$ gilt genau für $2x \in \mathbb{Z}$ und $x^2 - dy^2 \in \mathbb{Z}$. Hieraus folgt die Behauptung. □

2. Norm, Spur und Diskriminante

Die obigen Ganzheitsringe sind sogenannte *Gitter in K*, d.h. endlich erzeugte freie $\mathbb{Z}$-Untermoduln vom Rang $n = [K : \mathbb{Q}]$. Wir werden sehen, dass dies ganz allgemein für die Ganzheitsringe beliebiger Zahlkörper gilt. Hierzu wählen wir zunächst eine $\mathbb{Q}$-Basis $\beta_1, \ldots, \beta_n$ von K und finden nach Lemma 1.8 ein $N \in \mathbb{N}$

mit $\alpha_\nu = N\beta_\nu \in \mathfrak{o}_K$ für $\nu = 1, 2, \ldots, n$. Auf diese Weise erhalten wir immerhin ein Untergitter

$$\Lambda \;=\; \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \;\subseteq\; \mathfrak{o}_K,$$

Ist $[\mathfrak{o}_K : \Lambda] < \infty$, und wie kann man diesen Index explizit kontrollieren? Erinnern wir uns zunächst an einige Grundbegriffe der Algebra:

DEFINITION 2.1. Für endliche separable Körpererweiterungen K/k und $\alpha \in K$ ist die Skalarmultiplikation

$$m_\alpha : \quad K \longrightarrow K, \quad x \mapsto \alpha \cdot x$$

ein k-linearer Endomorphismus, und wir definieren die *Norm* und die *Spur* von α durch

$$N_{K/k}(\alpha) \;=\; \det(m_\alpha), \quad tr_{K/k}(\alpha) \;=\; tr(m_\alpha).$$

Weiter definieren wir das *charakteristische Polynom von* α in der Erweiterung K/k durch

$$\begin{aligned} \chi_{K/k}(\alpha, x) &= \det(x \cdot id_K - m_\alpha) \\ &= x^n - tr_{K/k}(\alpha)\, x^{n-1} + \cdots + (-1)^n N_{K/k}(\alpha). \end{aligned}$$

Zu seiner Berechnung fixieren wir einen algebraischen Abschluß $\iota : k \hookrightarrow \overline{k}$.

SATZ 2.2. *Sei K/k eine endliche separable Erweiterung, und es bezeichne Σ die Menge aller Einbettungen $\sigma : K \hookrightarrow \overline{k}$ mit $\sigma|_k = \iota$. Für $\alpha \in K$ gilt dann*

$$\chi_{K/k}(\alpha, x) \;=\; \prod_{\sigma \in \Sigma} (x - \sigma(\alpha)).$$

Insbesondere ist $tr_{K/k}(\alpha) = \sum_{\sigma\in\Sigma} \sigma(\alpha)$ und $N_{K/k}(\alpha) = \prod_{\sigma\in\Sigma} \sigma(\alpha)$.

Beweis. Für $d = [k(\alpha) : k]$ bilden die Potenzen $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine k-Basis von $k(\alpha)$. Somit bilden die

$$\gamma_{ij} \;=\; \alpha^i \cdot \beta_j \quad \text{für} \quad i \;=\; 0, 1, \ldots, d-1 \quad \text{und} \quad j \;=\; 1, \ldots, n$$

eine k-Basis von K, wenn $\beta_1, \ldots, \beta_n$ eine $k(\alpha)$-Basis von K ist. Bezüglich der γ_{ij} ist die Matrix des Endomorphismus m_α in Blockdiagonalform mit e identischen Blöcken $m_\alpha|_{k(\alpha)}$. Somit folgt

$$\chi_{K/L}(\alpha, x) \;=\; (p_\alpha(x))^e$$

wobei $p_\alpha(x) \in k[x]$ das Minimalpolynom von α bezeichnet. Da K/k eine separable Körpererweiterung ist, gilt

$$p_\alpha(x) \;=\; \prod_{\sigma' \in \Sigma'} (x - \sigma'(\alpha)),$$

wobei Σ' die Menge aller Einbettungen $\sigma' : k(\alpha) \hookrightarrow \overline{k}$ mit $\sigma'|_k = \iota$ bezeichnet. Jede dieser Einbettungen setzt sich auf genau $n = [K : k(\alpha)]$ verschiedene Weisen zu einer Einbettung $K \hookrightarrow \overline{k}$ fort, somit folgt die Behauptung. □

BEMERKUNG 2.3. Wegen $m_{\alpha\beta} = m_\alpha \circ m_\beta$ und $m_{\alpha+\beta} = m_\alpha + m_\beta$ sind Norm und Spur Homomorphismen:

$$\begin{aligned} N_{K/k} : \quad K^\times &\longrightarrow k^\times \\ tr_{K/k} : \quad (K, +) &\longrightarrow (k, +) \end{aligned}$$

Insbesondere wird durch

$$\langle \cdot, \cdot \rangle : \quad K \times K \longrightarrow k, \quad (x, y) \mapsto tr_{K/k}(xy)$$

eine symmetrische Bilinearform auf dem k-Vektorraum K erklärt. Ist K/k separabel, so ist diese Bilinearform nichtausgeartet:

$$K \longrightarrow K^\vee = \mathrm{Hom}_k(K, k), \quad x \mapsto \langle x, \cdot \rangle$$

ist ein Isomorphismus wegen $\langle x, y \rangle \neq 0$ für $x \neq 0$, $y = 1/x$.

Im Fall eines Zahlkörpers K über $k = \mathbb{Q}$ nehmen die Norm und die Spur nach Satz 2.2 auf $\mathfrak{o}_K$ ganzzahlige Werte an, da Galoiskonjugierte, Summen und Produkte von ganzen Elementen wieder ganz sind. Insbesondere schränkt sich die obige Bilinearform ein zu

$$\langle \cdot, \cdot \rangle : \quad \mathfrak{o}_K \times \mathfrak{o}_K \longrightarrow \mathbb{Z}.$$

Wir können nun Gittertheorie anwenden:

PROPOSITION 2.4. *Der Ganzheitsring $\mathfrak{o}_K \subset K$ ist ein Gitter.*

Beweis. Wir haben als Konsequenz aus Lemma 1.8 bereits bemerkt, dass der Ganzheitsring jedenfalls ein Untergitter $\Lambda \subseteq \mathfrak{o}_K$ enthält. Das hierzu *duale Gitter* ist definiert als

$$\Lambda^* = \{\alpha \in K \mid \langle \alpha, \beta \rangle \in \mathbb{Z} \text{ für alle } \beta \in \Lambda\}.$$

Dies ist offenbar wiederum ein Gitter, denn es wird erzeugt von einer bezüglich $\langle \cdot, \cdot \rangle$ zu einer $\mathbb{Z}$-Basis von Λ dualen $\mathbb{Q}$-Vektorraumbasis von K. Die Ganzzahligkeit der Spur liefert Inklusionen

$$\Lambda \subseteq \mathfrak{o}_K \subseteq \mathfrak{o}_K^* \subseteq \Lambda^*$$

und somit folgt die Behauptung. □

DEFINITION 2.5. Eine *Ganzheitsbasis* des Zahlkörpers K vom Grad $n = [K : \mathbb{Q}]$ ist ein Tupel von $\alpha_\nu \in \mathfrak{o}_K$ mit $\mathfrak{o}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

Für Zahlkörper höheren Grades ist eine solche Ganzheitsbasis im Allgemeinen schwierig zu finden. Ein Maß für den Index eines von $\mathbb{Q}$-linear unabhängigen ganzen Elementen $\alpha_1, \ldots, \alpha_n \in \mathfrak{o}_K$ erzeugten Untergitters bietet jedoch die Gram-Matrix der Spurform auf diesem Gitter:

DEFINITION 2.6. Für endliche separable Körpererweiterungen K/k definieren wir die *Diskriminante* von $\alpha_1, \ldots, \alpha_n \in K$ unter Benutzung der Spurform $\langle \cdot, \cdot \rangle$ durch

$$d_{K/k}(\alpha_1, \ldots, \alpha_n) = \det\big(\langle \alpha_i, \alpha_j \rangle\big)_{1 \leq i,j \leq n}.$$

Über $k = \mathbb{Q}$ setzen wir

$$d_\Lambda = d(\alpha_1, \ldots, \alpha_n) \quad \text{für Gitter} \quad \Lambda = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i \subset K,$$

und im Fall $\Lambda = \mathfrak{o}_K$ bezeichnen wir $d_K = d_\Lambda$ als *Diskriminante des Zahlkörpers K*.

Die Wohldefiniertheit von d_Λ folgt aus der Beobachtung, dass je zwei $\mathbb{Z}$-Basen des Gitters Λ durch eine Transformationsmatrix $M \in Gl_n(\mathbb{Z})$ mit $\det(M) \in \{\pm 1\}$ ineinander überführt werden, und aus

LEMMA 2.7. *Für $(\alpha'_1, \ldots, \alpha'_n) = (\alpha_1, \ldots, \alpha_n) \cdot M$ mit $M \in Gl_n(k)$ und $\alpha_\nu \in K$ hat man*

$$d_{K/k}(\alpha'_1, \ldots, \alpha'_n) = \det(M)^2 \cdot d_{K/k}(\alpha_1, \ldots, \alpha_n).$$

Beweis. Aus dem Transformationsverhalten von Bilinearformen in der linearen Algebra folgt $A' = MAM^t$ für die Matrizen $A' = (\langle \alpha'_i, \alpha'_j \rangle)_{i,j}$ und $A = (\langle \alpha_i, \alpha_j \rangle)_{i,j}$, wobei M^t die Transponierte von M bezeichnet. □

LEMMA 2.8. *Sei K ein Zahlkörper.*

(1) *Sind $\Lambda' \subseteq \Lambda$ zwei Gitter in K, so gilt $d_{\Lambda'} = m^2 \cdot d_\Lambda$ für $m := [\Lambda : \Lambda']$.*
(2) *Wenn $\alpha_1, \ldots, \alpha_n \in \mathfrak{o}_K$ existieren, deren Diskriminante $d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ quadratfrei ist, folgt*

$$\mathfrak{o}_K \;=\; \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Beweis. (1) Nach dem Elementarteilersatz für Untermoduln endlich erzeugter freier $\mathbb{Z}$-Moduln können wir ganze Zahlen $e_i \in \mathbb{Z}$ und Gittervektoren $\lambda_i \in \Lambda$ finden mit

$$\Lambda' \;=\; \mathbb{Z} \cdot e_1\lambda_1 \oplus \cdots \oplus \mathbb{Z} \cdot e_n\lambda_n \;\subseteq\; \Lambda \;=\; \mathbb{Z} \cdot \lambda_1 \oplus \cdots \oplus \mathbb{Z} \cdot \lambda_n.$$

Ein Isomorphismus zwischen den beiden Gittern ist in diesen Gitterbasen gegeben durch eine Diagonalmatrix $M = \operatorname{diag}(e_1, \ldots, e_n)$. Daher ist Lemma 2.7 anwendbar mit $m = \det(M)$. Die Behauptung (2) folgt aus der Aussage (1), indem man $\Lambda = \mathfrak{o}_K$ und $\Lambda' = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ wählt. □

Zur Berechnung von Diskriminanten in endlichen separablen Erweiterungen K/k seien schließlich noch zwei allgemeine Formeln angegeben:

LEMMA 2.9. *Seien K/k eine separable Körpererweiterung und $\sigma_1, \ldots, \sigma_n$ ihre Einbettungen in einen algebraischen Abschluß $\overline{k}/k$.*

(1) *Für $\alpha_1, \ldots, \alpha_n \in K$ gilt*

$$d_{K/k}(\alpha_1, \ldots, \alpha_n) \;=\; \Big(\det\big(\sigma_i(\alpha_j)\big)_{1 \le i,j \le n}\Big)^2$$

(2) *Für $K = k(\alpha)$ ist*

$$d_{K/k}(\alpha) \;:=\; d(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \;=\; \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

Beweis. Teil (1) folgt aus $(\langle \alpha_i, \alpha_j \rangle)_{i,j} = M \cdot M^t$ für die Matrix $M = (\sigma_i(\alpha_j))_{i,j}$, und (2) folgt mittels einer Vandermonde-Determinante (Übung). □

KOROLLAR 2.10 (Stickelberger). *Für Zahlkörper K gilt $d_K \equiv 0$ oder $1 \mod 4$.*

Beweis. Wir wählen eine Ganzheitsbasis $\alpha_1, \ldots, \alpha_n \in \mathfrak{o}_K$ und betrachten die Determinante

$$\det\big(\sigma_i(\alpha_j)\big)_{1 \le i,j \le n} \;=\; d_+ - 2\,d_- \quad \text{mit} \quad d_\pm \;=\; \sum_{\pi \in \mathfrak{S}_\pm} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}),$$

wobei wir $\mathfrak{S}_+ = \mathfrak{S}_n$ und $\mathfrak{S}_- = \{\sigma \in \mathfrak{S}_n \mid sgn(\sigma) = -1\}$ gesetzt haben. Aus obigem Lemma folgt

$$d_K \;=\; (d_+ - 2d_-)^2 \;=\; d_+^2 + 4 \cdot (d_-^2 - d_+d_-).$$

Als ganze algebraische Zahl, die invariant unter der Galoisoperation von $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ ist, ist $d_+ \in \mathbb{Z}$. Also liegt $d_-^2 - d_+d_- = (d_K - d_+^2)/4$ in $\mathbb{Q}$ und folglich als ganze algebraische Zahl in $\mathbb{Z}$. Hieraus folgt die Behauptung mit $d_K \equiv d_+^2 \mod 4$. □

BEISPIEL 2.11. Für $K = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$ folgt aus Lemma 1.10, dass

$$d_K \;=\; \begin{cases} d & \text{für } d \equiv 1 \mod 4, \\ 4d & \text{für } d \equiv 2, 3 \mod 4. \end{cases}$$

3. Noethersche Ringe

Wir wollen nun die Idealtheorie in Ganzheitsringen von Zahlkörpern entwickeln und die nötigen Eigenschaften zunächst axiomatisch fassen. Sei R ein kommutativer Ring. Für Hauptidealringe haben wir in Satz I.3.4 die Existenz von Faktorisierungen in irreduzible Elemente letztlich daraus erhalten, dass diese Ringe Noethersch im Sinn der folgenden Definition sind:

DEFINITION 3.1. Ein R-Modul M heißt *Noethersch*, wenn jede aufsteigende Kette von R-Untermoduln

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots \subseteq M$$

stationär wird, d.h. $\mathfrak{a}_{n+1} = \mathfrak{a}_n$ für alle genügend großen $n \gg 0$ gilt. Der Ring R heißt Noethersch, wenn er als Modul über sich selbst Noethersch ist, d.h. wenn jede aufsteigende Kette von Idealen in ihm stationär wird.

LEMMA 3.2. *Für R-Moduln M sind äquivalent:*

(1) *M ist Noethersch.*
(2) *Jeder R-Untermodul $N \subseteq M$ ist endlich erzeugt.*

Beweis. Ist $N \subseteq M$ ein R-Untermodul, welcher nicht endlich erzeugt ist, so können wir induktiv eine unendliche Folge von Elementen $n_1, n_2, n_3, \cdots \in N$ finden mit

$$n_{i+1} \notin \mathfrak{a}_i := Rn_1 + \cdots + Rn_i \quad \text{für alle} \quad i \in \mathbb{N},$$

Dies liefert eine unendliche, nicht stationär werdende Kette von R-Untermoduln, also kann M nicht Noethersch sein. Ist umgekehrt M nicht Noethersch, so existiert eine unendliche Kette von R-Untermoduln

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \cdots \subseteq M,$$

die nicht stationär wird. Dann ist

$$N := \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$$

offenbar ein R-Untermodul von M, welcher nicht endlich erzeugt ist: Gäbe es ein endliches System von Erzeugern, so wären alle diese in einem Modul $\mathfrak{a}_n$ für genügend großes $n \gg 0$ enthalten und somit würde die Kette stationär. □

KOROLLAR 3.3. *Für exakte Sequenzen*

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

von R-Moduln ist M ist Noethersch genau dann, wenn M' und M'' es sind.

Beweis. Jede Kette von Untermoduln $\mathfrak{a}'_n \subseteq M'$ bzw. $\mathfrak{a}''_n \subseteq M''$ liefert eine Kette von Untermoduln

$$\mathfrak{a}_n = i(\mathfrak{a}'_n) \subseteq M \quad \text{bzw.} \quad \mathfrak{a}_n = p^{-1}(\mathfrak{a}''_n) \subseteq M.$$

Wenn M Noethersch ist, wird letztere stationär, daher muß auch die ursprüngliche Kette stationär werden und somit sind M' und M'' Noethersch. Ist umgekehrt letzteres der Fall, so erhält man aus jeder Kette von Untermoduln $\mathfrak{a}_n \subseteq M$ zwei Ketten von Untermoduln

$$\mathfrak{a}'_n = i^{-1}(\mathfrak{a}_n) \subseteq M' \quad \text{und} \quad \mathfrak{a}''_n = p(\mathfrak{a}_n) \subseteq M''.$$

Wenn M' und M'' Noethersch sind, werden diese beiden Ketten stationär und die Exaktheit der Sequenz zeigt, dass dann die ursprüngliche Kette ebenfalls stationär werden muß. Somit ist M Noethersch. □

KOROLLAR 3.4. *Für Noethersche Ringe R gilt:*

(1) *Ein R-Modul M ist genau dann Noethersch, wenn er endlich erzeugt ist.*
(2) *Ist S/R eine endliche Ringerweiterung, d.h. ist der Ring S als R-Modul endlich erzeugt, so ist auch S ein Noetherscher Ring.*

Beweis. (1) Nach Lemma 3.2 gilt ganz allgemein, dass Noethersche R-Moduln endlich erzeugt sind. Für die Umkehrung müssen wir voraussetzen, dass der Ring R Noethersch ist (sonst wäre $M = R$ ein Gegenbeispiel). Nach Korollar 3.3 sind dann die freien R-Moduln

$$R^n = R \times \cdots \times R \quad \text{für } n \in \mathbb{N}$$

und alle ihre Quotienten, d.h. alle endlich erzeugten R-Moduln, Noethersch.

(2) Ist S/R eine endliche Ringerweiterung, so ist S als R-Modul endlich erzeugt und somit Noethersch nach Teil (1). Da jede aufsteigende Kette von S-Untermoduln auch eine solche von R-Untermoduln ist, ist S dann a fortiori auch als S-Modul Noethersch und folglich ein Noetherscher Ring. □

Tatsächlich gilt eine sehr viel stärkere Aussage als in Teil (2):

SATZ 3.5 (Hilbertscher Basissatz). *Ist R ein Noetherscher Ring, dann auch jede endlich erzeugte R-Algebra S.*

Beweisidee. Per Definition ist jede endliche erzeugte R-Algebra S ein Quotient eines Polynomrings $R[x_1, \ldots, x_n]$ für ein $n \in \mathbb{N}$, daher genügt es, den Fall $S = R[x]$ zu behandeln. Sei dazu ein Ideal $\mathfrak{a} \trianglelefteq R[x]$ gegeben. Da R Noethersch ist, ist das Ideal

$$\mathfrak{b} \;=\; \big\{ r \in R \mid r \text{ ist Leitkoeffizient eines Polynomes } f(x) \in \mathfrak{a} \big\} \;\trianglelefteq\; R$$

endlich erzeugt. Wir wählen $f_1(x), \ldots, f_n(x) \in \mathfrak{a}$, deren Leitkoeffizienten $\mathfrak{b}$ erzeugen, und für

$$0 \;\leq\; \mu \;\leq\; \max\{\deg(f_1), \ldots, \deg(f_n)\}$$

setzen wir

$$\mathfrak{b}_\mu \;=\; \big\{ r \in R \mid r \text{ ist Leitkoeffizient eines } g(x) \in \mathfrak{a} \text{ mit } \deg(g) \leq \mu \big\} \;\trianglelefteq\; R$$

Auch diese Ideale sind alle endlich erzeugt, und für jedes der $\mathfrak{b}_\mu$ wählen wir endlich viele Polynome $g_{\mu\nu}(x) \in \mathfrak{a}$, deren Leitkoeffizienten es erzeugen. Man überlegt sich leicht, dass jedes Polynom in dem Ideal $\mathfrak{a}$ eine $R[x]$-Linearkombination der $f_\alpha(x)$ und $g_{\mu\nu}(x)$ ist, also ist $\mathfrak{a} \trianglelefteq R[x]$ endlich erzeugt. □

Wir kommen hier mit der schwächeren Aussage (2) in Korollar 3.4 aus. So folgt mit Proposition 2.4, dass Ganzheitsringe von Zahlkörpern Noethersch sind, allgemeiner erhält man folgendes

PROPOSITION 3.6. *Sei R ein Hauptidealring, S sein ganzer Abschluß in einer endlichen separablen Körpererweiterung $K/k = Quot(S)$ vom Grad $n = [K : k]$.*

$$\begin{array}{ccc} S & \hookrightarrow & K \\ | & & | \\ R & \hookrightarrow & k \end{array}$$

Dann ist $S \simeq R^n$ als R-Modul. Somit ist S/R endlich und S ein Noetherscher Ring.

Beweis. Ersetzt man im Beweis von Proposition 2.4 überall $\mathbb{Z}$ durch R, so erhält man Einbettungen

$$\Lambda \;\subseteq\; S \;\subseteq\; \Lambda^* \;=\; \big\{\alpha \in K \mid tr_{K/k}(\alpha\beta) \in R \text{ für alle } \beta \in R\big\}$$

wobei Λ und damit auch Λ^* ein freier R-Modul vom Rang n ist. Wegen $S \subseteq \Lambda^*$ folgt nach dem Elementarteilersatz für Untermoduln endlich erzeugter freier Moduln über Hauptidealringen, dass S ein freier R-Modul vom Rang $m \leq n$ ist, und $m = n$ wegen $\Lambda \subseteq S$. Dass S Noethersch ist, folgt aus Korollar 3.4. □

4. Dedekind-Ringe

Wir haben bereits bemerkt, dass in einem Noetherschen Integritätsring jedes Element ein Produkt von irreduziblen ist. Um ein idealtheoretisches Analogon von faktoriellen Ringen zu finden, führen wir die folgenden Begriffe ein:

Definition 4.1. Ein Ideal $\mathfrak{p} \trianglelefteq R$ heißt ein *echtes* Ideal, wenn es vom Einsideal verschieden ist, und wir schreiben dann $\mathfrak{p} \triangleleft R$. Ein echtes Ideal $\mathfrak{p} \triangleleft R$ heißt

- *prim*, wenn $ab \notin \mathfrak{p}$ für alle $a, b \in R \setminus \mathfrak{p}$ gilt,
- *maximal*, wenn es kein echtes Ideal $\mathfrak{a} \triangleleft R$ mit echter Inklusion $\mathfrak{p} \subsetneq \mathfrak{a}$ gibt.

Ein Hauptideal $(a) \trianglelefteq R$ ist prim genau dann, wenn a ein Primelement oder Null ist. Ist R ein Hauptidealring, dann sind die maximalen Ideale genau die von den irreduziblen Elementen erzeugten Ideale (Übung). Allgemein gilt offenbar:

$$\mathfrak{p} \triangleleft R \text{ ist } \begin{cases} \text{prim} \\ \text{maximal} \end{cases} \iff R/\mathfrak{p} \text{ ist ein } \begin{cases} \text{Integritätsring} \\ \text{Körper} \end{cases}$$

Insbesondere ist jedes maximale Ideal prim. Wir können nun den zentralen Begriff dieses Kapitels einführen:

Definition 4.2. Ein *Dedekind-Ring* ist ein ganz abgeschlossener, Noetherscher Integritätsring, in dem jedes von Null verschiedene Primideal maximal ist.

Allgemeiner definiert man die *Dimension* eines kommutativen Ringes R als das Supremum

$$\dim(R) \;=\; \sup\big\{n \in \mathbb{N} \mid \exists \text{ Primideale } \mathfrak{p}_i \triangleleft R \text{ mit } 0 \neq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n\big\}.$$

Ein Dedekind-Ring ist also ein ganz abgeschlossener, Noetherscher Integritätsring der Dimension 1. Die letzte Bedingung ist von der vorigen unabhängig: Es gibt sogar Noethersche Ringe R mit $\dim(R) = \infty$ (Nagata)!

Offenbar ist jeder Hauptidealring ein Dedekind-Ring. Allgemeiner erhält man aus Dedekindringen weitere Dedekind-Ringe, indem man den ganzen Abschluß in endlichen separablen Erweiterungen ihres Quotientenkörpers bildet:

Proposition 4.3. *Sei R ein Dedekind-Ring und S sein ganzer Abschluß in einer endlichen separablen Erweiterung K/k des Quotientenkörpers $k = Quot(S)$; dann ist S ein Dedekind-Ring.*

Beweis. Offenbar ist S ein ganz abgeschlossener Integritätsring. Außerdem ist dieser Ring Noethersch, denn wie in Proposition 3.6 sieht man, dass S Untermodul eines freien R-Moduls von endlichem Rang und damit insbesondere endlich erzeugt als R-Modul ist; hierfür haben wir nicht den Elementarteilersatz, sondern lediglich duale Basen für die Spurform verwendet. Zu zeigen bleibt also nur, dass jedes von Null verschiedene Primideal $\mathfrak{p} \triangleleft S$ maximal ist. Sei $0 \neq \alpha \in \mathfrak{p}$. Da α ganz über R ist, erfüllt es eine Gleichung

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \;=\; 0 \quad \text{mit} \quad n \in \mathbb{N},\; c_0, c_1, \ldots, c_{n-1} \;\in\; R.$$

Nach Division durch eine geeignete Potenz von α dürfen wir dabei $c_0 \neq 0$ annehmen, sodass also

$$0 \neq c_0 \in \mathfrak{m} := \mathfrak{p} \cap R$$

gilt. Aber $\mathfrak{m} \lhd R$ ist ein Primideal, und in Hauptidealringen ist jedes von Null verschiedene Primideal maximal. Folglich ist der Restklassenring $\kappa_R = R/\mathfrak{m}$ ein Körper. Andererseits ist S/R eine ganze Ringerweiterung, somit ist die Erweiterung von Integritätsringen

$$\kappa_R = R/\mathfrak{m} \hookrightarrow \kappa_S = S/\mathfrak{p}$$

ebenfalls ganz. Aber ein Integritätsring, der ganz über einem Körper ist, ist selber ein Körper (Übung)! Also ist κ_S ein Körper, und damit ist $\mathfrak{p} \lhd S$ maximal. □

Unser Hauptinteresse liegt auf Ganzheitsringen algebraischer Zahlkörper, wir nehmen jedoch einen allgemeineren Standpunkt ein, welcher auch *Funktionenkörper* umfasst, d.h. endliche Erweiterungen des Körpers $k(x)$ der rationalen Funktionen über einem gegebenen Körper k. Wir werden sehen, dass sich diese in vieler Hinsicht ähnlich wie Zahlkörper verhalten; diese auf André Weil (1906-1996) zurückgehende Analogie zwischen Zahlentheorie und algebraischer Geometrie hat sich als extrem fruchtbar für beide Seiten erwiesen.

Beispiel 4.4. Algebraische Zahlkörper $K/\mathbb{Q}$ und Funktionenkörper $K/k(x)$ werden zusammenfassend als *globale Körper* bezeichnet. Ihr *Ganzheitsring* $\mathfrak{o}_K \subset K$ ist definiert als der ganze Abschluß

- von $\mathbb{Z}$ in K, falls $K/\mathbb{Q}$ ein Zahlkörper ist,
- von $k[x]$ in K, falls $K/k(x)$ ein Funktionenkörper ist.

Nach Proposition 4.3 sind alle diese Ganzheitsringe Dedekind-Ringe.

Im Folgenden sei stets R ein Dedekind-Ring. Wir wollen zeigen, dass jedes Ideal von R sich im Wesentlichen eindeutig als Produkt von Primidealen schreibt. Dabei ist das Produkt $\mathfrak{ab}$ von Idealen $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ definiert als das von den $\alpha\beta$ mit $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}$ erzeugte Ideal. Wir bezeichnen mit

$$\mathfrak{a}^e = \mathfrak{a} \cdots \mathfrak{a}$$

das e-fache Produkt eines Ideals mit sich selbst für $e \in \mathbb{N}$. Die Multiplikation von Idealen ist assoziativ, kommutativ und besitzt das Einsideal $(1) = R$ als neutrales Element. Um Ideale invertieren zu können, benötigen wir die folgende

Definition 4.5. Unter einem *gebrochenen Ideal* von R verstehen wir einen endlich erzeugten R-Untermodul $\mathfrak{b}$ von $K = Quot(R)$. Die Ideale im früheren Sinn bezeichnen wir zur Vermeidung von Verwechslungen auch als *ganze Ideale* von R.

Für jedes ganze Ideal $\mathfrak{a} \trianglelefteq R$ und jedes $\beta \in K$ ist $\beta \cdot \mathfrak{a} = \{\alpha\beta \mid \alpha \in \mathfrak{a}\} \subseteq K$ ein gebrochenes Ideal. Umgekehrt gibt es wegen der endlichen Erzeugtheit für jedes gebrochene Ideal $\mathfrak{b} \subseteq K$ ein $\alpha \in K$, sodass $\alpha \cdot \mathfrak{b} \trianglelefteq R$ ein ganzes Ideal ist.

Satz 4.6. *Die gebrochenen Ideale $\mathfrak{b} \neq (0)$ jedes Dedekind-Ringes R bilden eine Gruppe bezüglich der Multiplikation.*

Beweis. Wir müssen zeigen, dass jedes gebrochene Ideal $\mathfrak{b} \neq (0)$ ein Inverses bezüglich der Multiplikation von Idealen besitzt. Wir tun dies drei Schritten:

(1) Für jedes von Null verschiedene ganze Ideal $\mathfrak{a} \lhd R$ gilt $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$ mit geeigneten Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \lhd R$. Denn andernfalls könnten wir ein bezüglich der Inklusion maximales Gegenbeispiel $\mathfrak{a} \lhd R$ finden (weil R Noethersch ist); dabei ist $\mathfrak{a}$ nicht prim, es existieren also $\alpha, \beta \in R \setminus \mathfrak{a}$ mit $\alpha\beta \in \mathfrak{a}$. Dann gilt

$$\mathfrak{a} \supsetneq \mathfrak{a}_1\mathfrak{a}_2$$

für die beiden von α_i und $\mathfrak{a}$ erzeugten Ideale $\mathfrak{a}_i = (\mathfrak{a}, \alpha_i) \trianglelefteq R$. Diese Ideale sind echt größer als $\mathfrak{a}$ und enthalten somit wegen der Maximalität von $\mathfrak{a}$ ein Produkt von Primidealen; dann enthält aber auch $\mathfrak{a}$ ein solches Produkt, ein Widerspruch.

(2) Zu jedem von Null verschiedene Primideal $\mathfrak{p} \triangleleft R$ existiert ein multiplikatives Inverses als gebrochenes Ideal. Denn durch

$$\mathfrak{p}^{-1} \;=\; \{\alpha \in K \mid \alpha\beta \in R \text{ für alle } \beta \in \mathfrak{p}\}$$

wird ein gebrochenes Ideal definiert: Für $\beta \in \mathfrak{p} \setminus (0)$ ist $\beta \cdot \mathfrak{p}^{-1} \trianglelefteq R$ ein Ideal des Noetherschen Ringes R, also endlich erzeugt, womit die endliche Erzeugtheit von $\mathfrak{p}^{-1}$ folgt. Wegen $R \subseteq \mathfrak{p}^{-1}$ ist

$$\mathfrak{p} \;\subseteq\; \mathfrak{p} \cdot \mathfrak{p}^{-1} \;\subseteq\; R,$$

und da $\mathfrak{p}$ als von Null verschiedenes Primideal in einem Dedekind-Ring maximal ist, muß in einer der beiden obigen Inklusionen Gleichheit gelten. Gilt Gleichheit in der zweiten Inklusion, so sind wir fertig; wir nehmen also $\mathfrak{p} = \mathfrak{p} \cdot \mathfrak{p}^{-1}$ an. Für festes $\beta \in \mathfrak{p} \setminus (0)$ sei $n \in \mathbb{N}$ minimal mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \;\subseteq\; (\beta) \;\subseteq\; \mathfrak{p} \quad \text{für Primideale} \quad \mathfrak{p}_1, \ldots, \mathfrak{p}_n \;\triangleleft\; R.$$

Ein solches n existiert nach Teil (1). Mindestens eines der $\mathfrak{p}_i$ muß in $\mathfrak{p}$ enthalten sein, denn sonst gäbe es für jedes i ein $\alpha_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, es wäre aber $\alpha_1 \cdots \alpha_n \in \mathfrak{p}$ im Widerspruch dazu, dass $\mathfrak{p}$ ein Primideal ist. Nach Umnumerieren der Faktoren dürfen wir $\mathfrak{p}_1 \subseteq \mathfrak{p}$ und damit $\mathfrak{p}_1 = \mathfrak{p}$ annehmen, da jedes von Null verschiedene Primideal von R maximal ist. Wegen der Minimalität von n ist $\mathfrak{p}_2 \cdots \mathfrak{p}_n \not\subseteq (\beta)$, sei also $\alpha \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \setminus (\beta)$. Somit ist

$$\alpha \cdot \mathfrak{p} \;\subseteq\; \mathfrak{p}_1 \cdots \mathfrak{p}_n \;\subseteq\; (\beta), \quad \text{also} \quad \gamma \;:=\; \alpha/\beta \;\in\; \mathfrak{p}^{-1} \setminus R$$

Andererseits ist aber

$$\gamma \cdot \mathfrak{p} \;\subseteq\; \mathfrak{p}^{-1} \cdot \mathfrak{p} \;=\; \mathfrak{p},$$

wobei die letzte Gleichung nach Annahme gilt. Das Cayley-Hamilton-Argument aus dem Beweis von Proposition 1.3 liefert nun

$$\det\Big((\gamma \cdot id_{\mathfrak{p}} - m_\gamma) : \mathfrak{p} \longrightarrow \mathfrak{p}\Big) \;=\; 0$$

und damit eine Ganzheitsgleichung für γ (die Bedingung, dass der entsprechende Modul das Einselement enthält, ist in Integritätsringen für Cayley-Hamilton nicht erforderlich). Da R ganz abgeschlossen ist, folgt $\gamma \in R$, ein Widerspruch.

(3) Jedes von Null verschiedene gebrochene Ideal von R ist invertierbar. Da jedes gebrochene Ideal ein skalares Vielfaches eines echten Ideals ist, genügt es offenbar, diese Aussage für ganze Ideale zu zeigen. Angenommen, $\mathfrak{a} \triangleleft R$ wäre ein maximales nicht invertierbares ganzes Ideal. Sei $\mathfrak{p} \triangleleft R$ ein maximales und damit primes Ideal, welches $\mathfrak{a}$ enthält. Dann gilt

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

Im Fall $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$ zeigt ein analoges Argument wie in (2), dass $\mathfrak{p}^{-1} \subseteq R$ und damit $R = \mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathfrak{p}$ gilt, was absurd ist. Also ist $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$, und wegen der Maximalität von $\mathfrak{a}$ unter allen nicht-invertierbaren Idealen besitzt dann $\mathfrak{p}^{-1}\mathfrak{a}$ ein Inverses gebrochenes Ideal $\mathfrak{b}$. Dann ist $\mathfrak{b}\mathfrak{p}^{-1}$ ein Inverses für $\mathfrak{a}$, Widerspruch. □

Wir sagen, ein Ideal $\mathfrak{a} \trianglelefteq R$ *teilt* ein Ideal $\mathfrak{b} \trianglelefteq R$, und schreiben $\mathfrak{a} \mid \mathfrak{b}$, wenn ein Ideal $\mathfrak{c} \trianglelefteq R$ existiert mit der Eigenschaft $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. Die Tatsache, dass die von Null gebrochenen Ideale eine Gruppe bilden, zeigt insbesondere:

$$\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b}\mathfrak{a}^{-1} \subseteq R \iff \mathfrak{b} \subseteq \mathfrak{a}.$$

Eine weitere einfache Konsequenz ist das Hauptresultat dieses Kapitels, die Existenz und Eindeutigkeit der Primfaktorzerlegung für Ideale in Dedekind-Ringen:

SATZ 4.7. *Sei R ein Dedekind-Ring.*

(1) *Für jedes Ideal $\mathfrak{a} \trianglelefteq R$ gibt es paarweise verschiedene Primideale $\mathfrak{p}_i \triangleleft R$ und $e_i \in \mathbb{N}$ mit*

$$\mathfrak{a} \;=\; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

und diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

(2) *Dasselbe gilt für gebrochene Ideale, wenn man $e_i \in \mathbb{Z} \setminus \{0\}$ zulässt.*

Beweis. (1) Würde eine solche Produktzerlegung nicht für alle Ideale $\mathfrak{a} \triangleleft R$ existieren, so wähle man ein maximales Gegenbeispiel $\mathfrak{a} \trianglelefteq R$. Dieses ist enthalten in einem maximalen Ideal $\mathfrak{p} \supseteq \mathfrak{a}$. Dann ist

$$\mathfrak{p}^{-1}\mathfrak{a} \;\triangleleft\; R$$

ein ganzes Ideal, das $\mathfrak{a}$ strikt enthält (aus $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$ würde $\mathfrak{p} = R$ folgen). Folglich ist $\mathfrak{p}^{-1}\mathfrak{a}$ ein Produkt von Primidealen und somit gilt dasselbe auch für das Ideal $\mathfrak{a}$ im Widerspruch zur Annahme.

Um die Eindeutigkeit zu sehen, schreiben wir die Primfaktorzerlegungen ohne Exponenten, indem wir mehrfach auftretende Faktoren zulassen. Gegen seien also Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \triangleleft R$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_n \triangleleft R$ (nicht notwendig verschieden) mit der Eigenschaft

$$\mathfrak{a} \;=\; \mathfrak{p}_1 \cdots \mathfrak{p}_m \;=\; \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

Dann ist $m > 0$, weil sich das Einsideal offenbar nur als leeres Produkt schreiben lässt, und somit auch $n > 0$. Wenn $\mathfrak{p}_1 \neq \mathfrak{q}_j$ für alle j wäre, so gäbe es für jedes j ein $\alpha_j \in \mathfrak{q}_j \setminus \mathfrak{p}_1$, dann wäre aber

$$\alpha_1 \cdots \alpha_n \;\in\; \mathfrak{a} \setminus \mathfrak{p}_1$$

im Widerspruch zu $\mathfrak{a} \subseteq \mathfrak{p}_1$. Nach Umnumerieren können wir folglich $\mathfrak{p}_1 = \mathfrak{q}_1$ annehmen und erhalten nach Multiplikation mit $\mathfrak{p}_1^{-1} = \mathfrak{q}_1^{-1}$ die Eindeutigkeit der Zerlegung per Induktion über $\min\{m, n\}$.

(2) Wegen der endlichen Erzeugtheit existiert für jedes gebrochene Ideal $\mathfrak{b} \subset K$ ein Ringelement $\alpha \in R \setminus \{0\}$, sodass $\mathfrak{a} := \alpha \cdot \mathfrak{b} \trianglelefteq R$ ein ganzes Ideal ist. Nach Teil (1) können wir

$$\mathfrak{a} \;=\; \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n} \quad \text{und} \quad (\alpha) \;=\; \mathfrak{p}_1^{g_1} \cdots \mathfrak{p}_n^{g_n} \quad \text{mit} \quad f_i, g_i \in \mathbb{N}_0$$

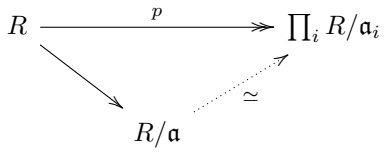
und Primidealen $\mathfrak{p}_i \triangleleft R$ schreiben. Dies liefert eine Produktzerlegung $\mathfrak{b} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ mit ganzzahligen Exponenten $e_i = f_i - g_i \in \mathbb{Z}$, und die Zerlegung wird bis auf die Reihenfolge der Faktoren eindeutig, wenn wir alle Faktoren mit Exponent $e_i = 0$ weglassen (dies folgt aus der Eindeutigkeit in (1) nach Multiplikation mit einem gemeinsamen Nenner, welcher alle auftretenden Ideale ganz macht). □

KOROLLAR 4.8 (Chinesischer Restsatz). *Ist R ein Dedekindring und $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$ mit $e_i \in \mathbb{N}$ und paarweise verschiedenen Primidealen $\mathfrak{p}_i \triangleleft R$, dann hat man einen natürlichen Isomorphismus*

$$R/\mathfrak{a} \;\xrightarrow{\sim}\; \prod_{i=1}^{n} R/\mathfrak{p}_i^{e_i}.$$

Beweis. Per Induktion über n genügt es zu zeigen: Sind zwei Ideale $\mathfrak{a}_1, \mathfrak{a}_2 \triangleleft R$ teilerfremd in dem Sinne, dass ihre beiden Primfaktorzerlegungen kein gemeinsames

Primideal enthalten, dann induzieren die Quotientenabbildungen $p_i : R \twoheadrightarrow R/\mathfrak{a}_i$ einen Epimorphismus $p = (p_1, p_2)$ mit Kern $\mathfrak{a} := \mathfrak{a}_1\mathfrak{a}_2$.



In der Tat: Das von den $\mathfrak{a}_i$ erzeugte Ideal $(\mathfrak{a}_1, \mathfrak{a}_2)$ muß das Einsideal sein, da es sonst in einem maximalen Ideal $\mathfrak{p} \lhd R$ enthalten wäre und dann $\mathfrak{a}_i \subseteq \mathfrak{p}$ für $i = 1, 2$ wäre im Widerspruch zur Teilerfremdheit. Also folgt

$$1 \;=\; \alpha_1 + \alpha_2 \quad \text{mit} \quad \alpha_1 \in \mathfrak{a}_1 \quad \text{und} \quad \alpha_2 \in \mathfrak{a}_2.$$

Dann ist $p(\alpha_2) = (1, 0)$ und $p(\alpha_1) = (0, 1)$, somit ist p surjektiv. Für den Kern gilt andererseits per Definition

$$\ker(p) \;=\; \mathfrak{a}_1 \cap \mathfrak{a}_2,$$

und $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$ wegen der Teilerfremdheit und der Charakterisierung der Teilbarkeit von Idealen durch Inklusion (Übung). □

KOROLLAR 4.9. *Für Dedekind-Ringe R sind äquivalent:*

(1) *R ist faktoriell,*

(2) *R ist ein Hauptidealring.*

Beweis. Hauptidealringe sind faktoriell nach Satz I.3.4. Sei umgekehrt R ein faktorieller Ring. Wenn R ein Dedekind-Ring ist, ist jedes Ideal ein Produkt von Primidealen, wir müssen also nur sehen, dass jedes Primideal $\mathfrak{p} \lhd R$ ein Hauptideal ist. In faktoriellen Ringen ist jedes von Null verschiedene Element eine Einheit oder ein Produkt von Primelementen. Für $\mathfrak{p} \neq (0)$ gibt es Primelemente $p_1, \ldots, p_n \in R$ mit $p_1 \cdots p_n \;\in\; \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, muß $p_i \in \mathfrak{p}$ für ein i sein. Dies liefert eine Inklusion

$$(0) \;\neq\; (p_i) \;\subseteq\; \mathfrak{p}$$

von Primidealen. Weil in Dedekind-Ringen jedes von Null verschiedene Primideal maximal ist, folgt $\mathfrak{p} = (p_i)$ und wir sind fertig. □

DEFINITION 4.10. Sei R ein Dedekind-Ring und $K = Quot(R)$. Wir bezeichnen mit I_R die Gruppe der von Null verschiedenen gebrochenen Ideale von R. Wir haben eine natürliche Abbildung $\varphi : K^\times \longrightarrow I_R$, welche einem Element das hiervon erzeugte gebrochene Hauptideal zuordnet, und wir bezeichnen den Quotienten als die *Idealklassengruppe* $C_R = I_R/R^\times$ des Dedekind-Rings.

Offenbar ist ein gebrochenes Hauptideal $(\alpha) = \alpha \cdot R$ mit $\alpha \in K^\times$ genau dann das Einsideal, wenn $\alpha \in R^\times$ eine Einheit des Dedekind-Ringes ist. Dies liefert eine exakte Sequenz

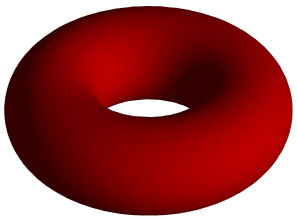
$$0 \;\longrightarrow\; R^\times \;\longrightarrow\; K^\times \;\longrightarrow\; I_R \;\longrightarrow\; C_R \;\longrightarrow\; 0.$$

deren äußere Terme das Herz der algebraischen Zahlentheorie bilden:

- Die Einheitengruppe $R^\times$ kontrolliert den Unterschied zwischen Elementen des Ringes und den hiervon erzeugten Hauptidealen.
- Die Klassengruppe C_R ist ein Maß dafür, wie weit der Ring R davon entfernt ist, ein Hauptidealring und damit faktoriell zu sein.

Im nächsten Kapitel werden wir die Struktur dieser Gruppen für Ganzheitsringe von Zahlkörpern studieren und insbesondere sehen, dass hier die Einheitengruppe endlich erzeugt und die Klassengruppe sogar endlich ist. Dies ist allerdings ein Spezifikum von Zahlkörpern und bleibt für Funktionenkörper im Allgemeinen nicht richtig, wie das Beispiel elliptischer Kurven zeigt:

BEISPIEL 4.11. Sei $\Lambda \subset \mathbb{C}$ ein Gitter, d.h. eine additive Untergruppe, die von zwei $\mathbb{R}$-linear unabhängigen Vektoren erzeugt wird. Der Quotient $E = \mathbb{C}/\Lambda$ ist eine sogenannte *elliptische Kurve*, eine kompakte Riemannsche Fläche, welche homöomorph zu einem zweidimensionalen reellen Torus $(\mathbb{R}/\mathbb{Z})^2$ ist:



Sei $0 \in E$ der Ursprung und $E^* = E \setminus \{0\} \subset E$ sein Komplement. Wir betrachten den Ring

$$S \;=\; \big\{\, f : E^* \;\longrightarrow\; \mathbb{C} \;\mid\; f \text{ holomorph} \,\big\}$$

der holomorphen Funktionen auf diesem Komplement. Unter der Abbildung $\mathbb{C} \twoheadrightarrow E$ entsprechen solche Funktionen bijektiv den sogenannten *elliptischen Funktionen*, meromorphen Funktionen $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ mit Polen höchstens in Λ und mit der Periodizität

$$f(z+\lambda) \;\equiv\; f(z) \quad \text{für alle} \quad \lambda \;\in\; \Lambda.$$

In der Funktionentheorie zeigt man, dass jede elliptische Funktion sich als Polynom in der Weierstraß-Funktion

$$\wp(z) \;=\; \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \Big(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \Big)$$

und ihrer Ableitung $\wp'(z)$ schreibt. Diese Ableitung erfüllt eine Differentialgleichung der Form

$$(\wp')^2 \;=\; 4 \cdot \wp^3 + a \cdot \wp + b \quad \text{mit Konstanten} \quad a, b \;\in\; \mathbb{C},$$

also ist

$$S \;=\; \mathbb{C}[\wp, \wp'] \;\simeq\; \mathbb{C}[x,y]/(y^2 - 4x^3 - ax - b) \;\supset\; R \;=\; \mathbb{C}[x]$$

eine ganze Ringerweiterung. Tatsächlich ist $S = \mathfrak{o}_K$ für den Funktionenkörper K in folgendem Diagramm:

$$\begin{array}{ccc} S = \mathbb{C}[\wp, \wp'] & \hookrightarrow & K = \mathbb{C}(\wp, \wp') \\ \big| & & \big| \\ R = \mathbb{C}[x] & \hookrightarrow & k = \mathbb{C}(x) \end{array}$$

Wie sehen die maximalen Ideale in diesem Ganzheitsring $S \simeq \mathfrak{o}_K$ aus? Offenbar ist für jedes $p \in E^*$ das Ideal

$$\mathfrak{m}_p \;=\; \big\{\, f \in S \;\mid\; f(p) \;=\; 0 \,\big\} \;\lhd\; S$$

maximal, denn die Auswertung elliptischer Funktionen am Punkt p liefert einen Isomorphismus $S/\mathfrak{m}_p \simeq \mathbb{C}$. Man kann sich überlegen, dass jedes maximale Ideal von dieser Form ist, die eindeutige Primfaktorzerlegung von Idealen in Dedekindringen liefert also eine Identifikation

$$I_S \;=\; \bigoplus_{p\in E^*} \mathbb{Z},$$

sodass $\varphi : K^\times \longrightarrow I_S$ einer meromorphen Funktion f die Ordnung $\nu_p(f) \in \mathbb{Z}$ ihrer Null- oder Polstellen an den Punkten $p \in E^*$ zuordnet. Es gilt nun genauer der folgende klassische

Satz 4.12 (Abel-Jacobi). *Das Bild der Abbildung φ ist genau der Kern der Summationsabbildung*

$$\bigoplus_{p\in E^*} \mathbb{Z} \;\longrightarrow\; E, \quad (n_p)_{p\in E^*} \;\mapsto\; \sum_{p\in E^*} n_p \cdot p \;\in\; E.$$

Somit hat die exakte Sequenz von Einheiten- und Idealklassengruppe hier die folgende Form:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S^\times & \longrightarrow & K^\times & \longrightarrow & I_S & \longrightarrow & C_S & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \| & & \\ & & \mathbb{C}^\times & & \mathbb{C}(\wp,\wp')^\times & & \bigoplus_{p\in E\setminus\{0\}} \mathbb{Z} & & E & & \end{array}$$

Insbesondere ist keine dieser beiden Gruppen endlich erzeugt! Im nächsten Kapitel werden wir sehen, dass sich die Situation für Zahlkörper sehr von derjenigen für Funktionenkörper unterscheidet.

KAPITEL III

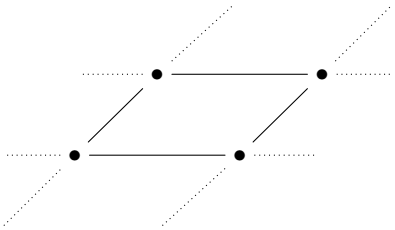
Geometrie der Zahlen

Wir wollen nun die Struktur der Ganzheitsringe $\mathfrak{o}_K$ in Zahlkörpern $K/\mathbb{Q}$ näher untersuchen. Dabei werden wir

- das Gitter $\mathfrak{o}_K$ in einen Euklidischen Vektorraum einbetten und die Größe der Gittermaschen zur Diskriminante d_K in Bezug setzen;
- ein allgemeines Kriterium für die Existenz von Gitterpunkten in genügend großen konvexen Teilmengen des Vektorraumes kennenlernen;
- als Anwendung die Struktur der Einheitengruppe $\mathfrak{o}_K^\times$ beschreiben und die Endlichkeit der Klassengruppe C_K beweisen.

1. Minkowski's Gittertheorie

Im vorigen Kapitel haben wir bereits eine Verbindung der Diskriminante von Zahlkörpern mit dem Volumen von Gittermaschen erwähnt; dies wollen wir im Folgenden präzisieren und dazu zunächst einige allgemeine Resultate über Gitter diskutieren. Dabei sei stets V ein endlich-dimensionaler reeller Vektorraum. Unter einem *Gitter* $\Lambda \subset V$ verstehen wir eine von einer Vektorraumbasis erzeugte additive Untergruppe,



d.h. eine freie abelsche Untergruppe vom Rang $n = \dim(V)$ mit der Eigenschaft, dass die Skalarmultiplikation

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} V$$

ein Isomorphismus ist. Mit der üblichen Topologie auf dem $\mathbb{R}$-Vektorraum V lässt sich dies auch folgendermaßen ausdrücken:

LEMMA 1.1. *Eine Untergruppe $\Lambda \subset V$ ist genau dann ein Gitter, wenn folgende beiden Eigenschaften gelten:*

- *$\Lambda \subset V$ ist diskret, d.h. besitzt in V keine Häufungspunkte,*
- *$\Lambda \subset V$ ist cokompakt, d.h. der Quotient V/Λ ist kompakt.*

Beweis. Für "$\Longrightarrow$" kann man nach Wahl einer Gitterbasis $\Lambda = \mathbb{Z}^n \subset V = \mathbb{R}^n$ annehmen, sodass offenbar $\Lambda \subset V$ diskret und $V/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^n$ kompakt ist.

Für "$\Longleftarrow$" beachte man zunächst, dass aus der Kompaktheit von V/Λ folgt, dass auch der Cokern der linearen Abbildung $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow V$ kompakt und somit trivial ist. Diese Abbildung ist also surjektiv und wir können daher eine in Λ liegende

Basis $e_1, \ldots, e_n \in \Lambda$ des $\mathbb{R}$-Vektorraumes V finden. Dann ist die hiervon erzeugte Untergruppe

$$\Lambda' \;=\; \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n \;\subseteq\; \Lambda$$

vom endlichen Index: Denn

$$V \;=\; \bigcup_{v\in\Lambda'} (M+v) \quad \text{für} \quad M \;=\; \big\{\lambda_1 e_1 + \cdots + \lambda_n e_n \mid \lambda_1, \ldots, \lambda_n \in [0,1]\big\},$$

und der Schnitt $M \cap \Lambda$ einer kompakten Menge M mit einer diskreten Menge Λ ist notwendigerweise endlich. Wir können somit eine natürliche Zahl $m \in \mathbb{N}$ finden mit $\Lambda \subseteq \frac{1}{m}\Lambda' \simeq \mathbb{Z}^n$ und folglich ist auch Λ eine endlich erzeugte freie abelsche Gruppe nach dem Elementarteilersatz. □

Um zu messen, wie "dicht" das Gitter $\Lambda \subset V$ liegt, nehmen wir an, dass V ein *Euklidischer Vektorraum* ist: Ein $\mathbb{R}$-Vektorraum mit einer positiv definiten und symmetrischen $\mathbb{R}$-Bilinearform

$$(\cdot,\cdot): \quad V \times V \;\longrightarrow\; \mathbb{R}.$$

Dieses Skalarprodukt definiert eine Metrik und somit auch eine Volumenform auf dem Euklidischen Vektorraum. Jede Orthonormalbasis $v = (v_1, \ldots, v_n) \in V^n$ gibt einen Isomorphismus

$$\varphi_v: \quad \mathbb{R}^n \;\xrightarrow{\sim}\; V, \quad (x_1, \ldots, x_n) \;\mapsto\; \sum_i x_i v_i,$$

welcher das Skalarprodukt und die Volumenform in das Standardskalarprodukt und die übliche Volumenform auf dem Euklidischen Raum $\mathbb{R}^n$ übersetzt. Wir bezeichnen eine Teilmenge $S \subseteq V$ als *meßbar*, wenn $\varphi_v^{-1}(S)$ meßbar für das Lebesgue-Maßes λ ist, und setzen dann

$$vol(S) \;:=\; \lambda(\varphi_v^{-1}(S)) \;\in\; \mathbb{R}_{\geq 0} \cup \{\infty\}.$$

Diese Begriffe hängen nicht von der Wahl der Orthonormalbasis ab:

LEMMA 1.2. *Die Meßbarkeit und das Volumen $vol(S)$ einer Teilmenge $S \subseteq V$ hängen nicht von der Orthonormalbasis v ab.*

Beweis. Der Wechsel zu einer anderen Vektorraumbasis $u = (u_1, \ldots, u_n) \in V^n$ ist durch eine Matrix $M = \varphi_u^{-1} \circ \varphi_v \in Gl_n(\mathbb{R})$ gegeben, dabei gilt also offenbar die Äquivalenz

$$\varphi_v^{-1}(S) \quad \text{meßbar} \quad\Longleftrightarrow\quad \varphi_u^{-1}(S) \;=\; M(\varphi_v^{-1}(S)) \quad \text{meßbar}$$

und im meßbaren Fall

$$vol(\varphi_u^{-1}(S)) \;=\; |\det(M)| \cdot vol(\varphi_v^{-1}(S))$$

wegen der Transformationsformel für Integrale. Wenn u und v Orthonormalbasen sind, so ist $\det(M) = \pm 1$ und damit folgt die Unabhängigkeit des Volumens von der gewählten Orthonormalbasis. □

Als Maß dafür, wie "dicht" ein Gitter $\Lambda \subset V$ liegt, können wir nun das Volumen einer Elementarmasche betrachten:

LEMMA 1.3. *Sei $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i \subset V$ ein Gitter. Dann hängt das Volumen einer Elementarmasche*

$$S \;=\; \Big\{ \sum_i x_i \alpha_i \;\mid\; x_i \in [0,1] \Big\}$$

nicht von der gewählten Gitterbasis ab und wird daher kurz durch $vol(\Lambda) = vol(S)$ bezeichnet. Es gilt

$$vol(\Lambda) \;=\; \sqrt{|\det(D)|} \quad \textit{für die Matrix} \quad D \;=\; \big((\alpha_i, \alpha_j)\big)_{1\leq i,j\leq n}.$$

Beweis. Die Unabhängigkeit von der gewählten Gitterbasis folgt mit demselben Argument wie das vorige Lemma. Um eine explizite Formel für das Volumen zu erhalten, sei $v = (v_1, \ldots, v_n) \in V^n$ eine Orthonormalbasis von V und $M \in Gl(V)$ die eindeutig bestimmte lineare Transformation, welche den Basiswechsel zu unserer gewählten Gitterbasis herstellt, d.h. es sei $\alpha_i = M(v_i)$ für $i = 1, 2, \ldots, n$. Dann gilt einerseits $vol(\Lambda) = |\det(M)|$ nach der Transformationsformel für Integrale. Für die Matrizen, welche das Skalarprodukt in diesen beiden Basen beschreiben, gilt andererseits

$$D \;=\; M^t \cdot E \cdot M \;=\; M^t \cdot M$$

für die Einheitsmatrix E mit Einträgen $(v_i, v_j) = \delta_{ij}$. Also ist $\det(D) = \det(M)^2$ und damit folgt die Behauptung. □

Wir kommen nun zum Hauptresultat dieses Kapitels, aus dem die Endlichkeit der Klassengruppe und die endliche Erzeugtheit der Einheitengruppe für Zahlkörper folgen werden. Hierzu machen wir folgende

Definition 1.4. Eine Teilmenge $S \subseteq V$ heißt

- *symmetrisch*, wenn für jeden Punkt $s \in S$ auch $-s \in S$ ist,
- *konvex*, wenn für alle Punkte $s, t \in S$ das Geradensegment zwischen diesen in S liegt:

$$[s,t] \;:=\; \big\{\lambda s + (1-\lambda)t \;\mid\; \lambda \in [0,1]\big\} \;\subseteq\; S.$$

Man kann zeigen, dass jede konvexe Teilmenge $S \subseteq V$ meßbar ist; wir lassen den Beweis hier aus, da die Meßbarkeit in allen unseren Anwendungen offensichtlich sein wird. Beispielsweise folgt aus der Dreiecksungleichung für die Norm $\|v\| = \sqrt{\langle v, v\rangle}$, dass für $r \geq 0$ die Kugel

$$B_r(0) \;=\; \big\{\, v \in V \;\mid\; \|v\| \leq r \,\big\}$$

konvex ist. Wir bezeichnen eine Teilmenge als *beschränkt*, wenn sie in einer solchen Kugel enthalten ist. Der Satz von Minkowski (1864-1909) gibt ein Kriterium für die Existenz von Gitterpunkten in genügend großen Teilmengen:

Satz 1.5 (Gitterpunktsatz von Minkowski). *Ist $\Lambda \subset V$ ein Gitter und $S \subseteq V$ symmetrisch und konvex mit*

$$2^n \cdot vol(\Lambda) \;<\; vol(S) \;<\; \infty$$

für $n = \dim(V)$, dann enthält S einen nichttrivialen Gitterpunkt: $S \cap \Lambda \neq \{0\}$.

Beweis. Es reicht, für die reskalierte Teilmenge $\frac{1}{2}S \subseteq S$ Gitterpunkte $\lambda, \mu \in \Lambda$ mit

$$\big(\lambda + \tfrac{1}{2}S\big) \cap \big(\mu + \tfrac{1}{2}S\big) \;\neq\; \varnothing \quad \text{und} \quad \lambda \;\neq\; \mu$$

zu finden: Denn

$$\lambda + \tfrac{1}{2}s \;=\; \mu + \tfrac{1}{2}t$$

mit $s, t \in S$ liefert

$$0 \;\neq\; \tfrac{1}{2}(s-t) \;=\; \mu - \lambda \;\in\; [s, -t] \cap \Lambda \;\subset\; S \cap \Lambda$$

wegen der vorausgesetzten Symmetrie und Konvexität. Wir argumentieren nun durch Widerspruch: Wären die Translate $\lambda + \frac{1}{2}S$ mit $\lambda \in \Lambda$ paarweise disjunkt, so würde dasselbe für ihre Durchschnitte mit einer Grundmasche $M \subset \Lambda$ gelten, sodass also

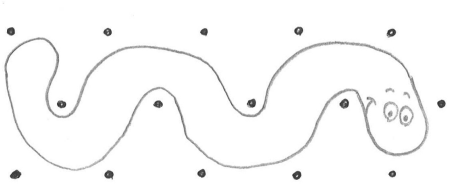
$$vol(\Lambda) \;=\; vol(M) \;\geq\; \sum_{\lambda\in\Lambda} vol\Big(M \cap \big(\lambda + \tfrac{1}{2}S\big)\Big) \;=\; \sum_{\lambda\in\Lambda} vol\Big(\big(M - \lambda\big) \cap \tfrac{1}{2}S\Big)$$

gelten würde. Aber die Translate $M - \lambda$ mit $\lambda \in \Lambda$ überdecken per Definition einer Grundmasche den gesamten Vektorraum, sodass die Summe auf der rechten Seite gleich

$$vol(\tfrac{1}{2}S) \;=\; 2^{-n} \cdot vol(S)$$

ist. Für $vol(S) > 2^n \cdot vol(\Lambda)$ liefert dies den gewünschten Widerspruch. □

Die Konvexität der Teilmenge $S \subseteq V$ kann im Gitterpunktsatz offenbar nicht ersatzlos gestrichen werden:



Auch die angegebene Schranke im Gitterpunktsatz ist optimal: Beispielsweise hat der offenen Würfel $S = (-1,1)^n \subset \mathbb{R}^n$ das Volumen $vol(S) = 2^n$ und enthält keinen nichttrivialen Gitterpunkt. Allerdings kann die strikte Ungleichung zu "$\geq$" abgeschwächt werden, wenn S kompakt ist:

KOROLLAR 1.6. *Ist $\Lambda \subset V$ ein Gitter und $S \subseteq V$ eine kompakte symmetrische konvexe Teilmenge mit*

$$vol(S) \;\geq\; 2^n \cdot vol(\Lambda)$$

für $n = \dim(V)$, dann enthält S einen nichttrivialen Gitterpunkt: $S \cap \Lambda \neq \{0\}$.

Beweis. Für jedes $m \in \mathbb{N}$ ist der Gitterpunktsatz 1.5 auf $S_m = (1 + \frac{1}{m}) \cdot S \subset V$ anwendbar wegen $vol(S_m) > vol(S_m)$. Wir erhalten somit eine Folge von ineinander geschachtelten Kompakta

$$S_1 \;\supset\; S_2 \;\supset\; S_3 \;\supset\; \cdots \;\supset\; S \;=\; \bigcap_{m \geq 1} S_m,$$

von denen jedes einen nichttrivialen Gitterpunkt enthält: Es ist $S_m \cap \Lambda \neq \{0\}$ für alle $m \geq 1$. Aber $\Lambda \subset V$ ist eine diskrete Teilmenge und besitzt daher nur endlich viele Schnittpunkte mit jeder gegebenen kompakten Menge. Also ist

$$S_1 \cap \Lambda \;\supseteq\; S_2 \cap \Lambda \;\supseteq\; S_3 \cap \Lambda \;\supseteq\; \cdots$$

eine absteigende Kette von endlichen nichtleeren Mengen und wird folglich stationär, d.h. es ist $S_m \cap \Lambda = S_{m+1} \cap \Lambda = \cdots \neq \{0\}$ für alle $m \gg 0$. Also gibt es einen nichttrivialen Gitterpunkt

$$0 \;\neq\; \lambda \;\in\; \bigcap_{m \geq 1} S_m \cap \Lambda \;=\; S \cap \Lambda$$

wie behauptet. □

2. Gitter in Zahlkörpern

Sei jetzt K eine Zahlkörper. Um Minkowski's Satz auf den Ganzheitsring $\mathfrak{o}_K$ anzuwenden, muß dieser als Gitter in einen Euklidischen Vektorraum V eingebettet werden. Ein Kandidat ist $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ mit der zur Definition der Diskriminante betrachteten Bilinearform

$$\langle \alpha, \beta \rangle \;:=\; tr_{K/\mathbb{Q}}(\alpha\beta) \;=\; \sum_{\sigma \in \Sigma} \sigma(\alpha\beta) \;=\; \sum_{\sigma \in \Sigma} \sigma(\alpha)\,\sigma(\beta),$$

wobei Σ die Menge aller Einbettungen des Zahlkörpers K in die komplexen Zahlen bezeichnet. Diese Bilinearform ist aber im Allgemeinen nicht positiv definit, also kein Skalarprodukt. Wir beheben dies durch komplexe Konjugation des zweiten Faktors und setzen

$$(\alpha, \beta) \;:=\; \sum_{\sigma \in \Sigma} \sigma(\alpha)\, \overline{\sigma(\beta)} \quad \text{für} \quad \alpha, \beta \;\in\; K.$$

Hierbei werden die folgenden Notationen nützlich sein.

Definition 2.1. Eine Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ heißt *reell*, wenn $\overline{\sigma} = \sigma$ gilt, und andernfalls *komplex*. Wir bezeichnen im Folgenden die reellen Einbettungen mit $\sigma_1, \ldots, \sigma_r$. Die komplexen Einbettungen treten offenbar in Paaren komplexer Konjugierter auf und wir fixieren ein Repräsentantensystem $\sigma_{r+1}, \ldots, \sigma_{r+s}$ für die Paare. Die zu den gewählten Repräsentanten konjugierten Einbettungen bezeichnen wir auch mit $\sigma_{r+s+\nu} = \overline{\sigma_{r+\nu}}$ für $\nu = 1, \ldots, s$.

Beispiel 2.2. Für den Zahlkörper $K = \mathbb{Q}(\sqrt[3]{2})$ ist $r = s = 1$; die Einbettungen sind gegeben durch

$$\sigma_1(\sqrt[3]{2}) \;=\; \sqrt[3]{2} \;\in\; \mathbb{R}, \qquad \sigma_2(\sqrt[3]{2}) \;=\; \zeta \cdot \sqrt[3]{2} \qquad \text{und} \qquad \sigma_3(\sqrt[3]{2}) \;=\; \overline{\zeta} \cdot \sqrt[3]{2},$$

wobei $\zeta \in \mathbb{C}$ eine primitive dritte Einheitswurzel bezeichnet.

Kommen wir zurück zum allgemeinen Fall und betrachten mit obiger Notation die $\mathbb{Q}$-lineare Einbettung

$$\begin{aligned} \iota : \quad K \;&\hookrightarrow V \;:=\; \mathbb{R}^r \times \mathbb{C}^s \\ \alpha \;&\mapsto \big(\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)\big). \end{aligned}$$

Dabei ist V ein *reeller* Vektorraum der Dimension $\dim_{\mathbb{R}}(V) = r + 2s = [K : \mathbb{Q}]$, und wir versehen ihn mit dem Skalarprodukt

$$(z, w)_V \;:=\; \sum_{i=1}^{r} z_i \cdot w_i \;+\; \sum_{i=r+1}^{r+s} tr_{\mathbb{C}/\mathbb{R}}(z_i \cdot \overline{w_i}),$$

das vom Standard-Skalarprodukt auf $\mathbb{R}^r$ und der Spur des Standard-Hermiteschen Produktes auf $\mathbb{C}^s$ induziert ist. Dieses Skalarprodukt ist $\mathbb{R}$-bilinear, positiv definit und erfüllt

$$(\iota(\alpha), \iota(\beta))_V \;=\; (\alpha, \beta) \quad \text{für} \quad \alpha, \beta \;\in\; K.$$

Wir können nun präzisieren, inwiefern die Diskriminante d_K ein Maß dafür bietet, wie *"dicht"* der Ganzheitsring $\mathfrak{o}_K$ in K liegt:

Lemma 2.3. *Das Bild $\Lambda := \iota(\mathfrak{o}_K) \subset V = \mathbb{R}^r \times \mathbb{C}^s$ des Ganzheitsringes ist ein Gitter mit*

$$vol(\Lambda) \;=\; \sqrt{|d_K|}.$$

Beweis. Wir wissen bereits, dass der Ganzheitsring $\mathfrak{o}_K = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i$ und damit auch Λ frei abelsch vom Rang n ist. Zu zeigen bleibt die Volumenformel. Lemma 1.3 liefert

$$vol(\Lambda) \;=\; \sqrt{|\det(A)|} \quad \text{mit} \quad A \;=\; \big((\alpha_i, \alpha_j)_{1 \le i,j \le n}\big).$$

Wegen

$$\begin{aligned} (\alpha_i, \alpha_j) \;&=\; \sum_{\nu=1}^{r} \sigma_\nu(\alpha_i)\, \sigma_\nu(\alpha_j) + \sum_{\nu=r+1}^{s} tr_{\mathbb{R}/\mathbb{C}}(\sigma_\nu(\alpha_i)\, \overline{\sigma_\nu(\alpha_j)}) \\ &=\; \sum_{\nu=1}^{n} \sigma_\nu(\alpha_i)\, \overline{\sigma_\nu(\alpha_j)} \end{aligned}$$

ist $A = M^t \cdot \overline{M}$ für die komplexe Matrix M mit Einträgen $M_{ij} = \sigma_i(\alpha_j)$, also insgesamt

$$vol(\Lambda) \;=\; |\det(M)|.$$

Mit $d_K = (\det(M))^2$ nach Lemma II.2.9 folgt nun die Behauptung. □

Allgemeiner können wir Gittertheorie auf beliebige von Null verschiedene Ideale anwenden, da diese endlichen Index im Ganzheitsring besitzen:

LEMMA 2.4. *Jedes Ideal* $(0) \neq \mathfrak{a} \trianglelefteq \mathfrak{o}_K$ *erfüllt* $\mathfrak{a} \cap \mathbb{Z} \neq (0)$ *und hat somit endlichen Index*

$$N(\mathfrak{a}) \;:=\; [\mathfrak{o}_K : \mathfrak{a}] \;<\; \infty.$$

Insbesondere ist $\iota(\mathfrak{a}) \subset V$ *ein Gitter mit Maschenvolumen* $vol(\Lambda) = N(\mathfrak{a}) \cdot \sqrt{|d_K|}$.

Beweis. Jedes $\alpha \in \mathfrak{a} \setminus (0)$ erfüllt eine Gleichung $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$ mit $c_i \in \mathbb{Z}$. Nach Division durch eine geeignete Potenz von α können wir dabei offenbar $c_0 \neq 0$ annehmen. Wegen

$$c_0 \;=\; -\alpha^n - c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha \;\in\; \mathfrak{a} \cap \mathbb{Z}$$

ist dann das auf der rechten Seite stehende Ideal nicht Null. Insbesondere ist der Quotientenring $\mathbb{Z}/\mathfrak{a} \cap \mathbb{Z}$ endlich, und $\mathfrak{o}_K/\mathfrak{a}$ ist als endlich erzeugter Modul über diesem endlichen Ring ebenfalls endlich. Aus dem Elementarteilersatz folgt, dass für Gitter Λ jede Untergruppe $\Lambda' \subseteq \Lambda$ vom endlichen Index wieder ein Gitter ist, mit

$$vol(\Lambda') \;=\; [\Lambda : \Lambda'] \cdot vol(\Lambda).$$

Für $\Lambda' = \iota(\mathfrak{a})$, $\Lambda = \iota(\mathfrak{o}_K)$ folgt die letzte Behauptung daher aus Lemma 2.3. □

Der im obigen Lemma auftretende Index $N(\mathfrak{a}) \in \mathbb{N}$ wird auch als die *Norm* des Ideals $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ bezeichnet. Das folgende Lemma besagt, dass es genügt, die Norm im Fall von Primidealen $\mathfrak{a} = \mathfrak{p}$ zu kennen; hier ist $\mathfrak{o}_K/\mathfrak{p}$ ein endlicher Körper und somit

$$\begin{array}{ccc} \mathfrak{o}_K/\mathfrak{p} & \xrightarrow{\sim} & \mathbb{F}_{p^f} \\ \big| & & \big| \\ \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} & \xrightarrow{\sim} & \mathbb{F}_p \end{array} \qquad \Longrightarrow \qquad N(\mathfrak{p}) \;=\; p^f$$

mit $f \in \mathbb{N}$ und der eindeutig bestimmten Primzahl $p \in \mathbb{N}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

LEMMA 2.5. *Für* $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ *mit Primidealen* $\mathfrak{p}_i \lhd \mathfrak{o}_K$ *und* $e_i \in \mathbb{N}$ *gilt die Formel*

$$N(\mathfrak{a}) \;=\; N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_n)^{e_n}.$$

Beweis. Der chinesische Restsatz (Korollar II.4.8) reduziert uns auf den Fall, dass $\mathfrak{a} = \mathfrak{p}^e$ für ein Primideal $\mathfrak{p} \lhd \mathfrak{o}_K$ und ein $e \in \mathbb{N}$ ist. Im Fall $e = 1$ ist hier nichts zu zeigen. Im allgemeinen Fall wollen wir Induktion über den Exponenten e benutzen. Die Sequenz

$$0 \;\longrightarrow\; \mathfrak{p}^{e-1}/\mathfrak{p}^e \;\longrightarrow\; \mathfrak{o}_K/\mathfrak{p}^e \;\longrightarrow\; \mathfrak{o}_K/\mathfrak{p}^{e-1} \;\longrightarrow\; 0$$

ist exakt und liefert

$$N(\mathfrak{p}^e) \;=\; |\mathfrak{p}^{e-1}/\mathfrak{p}^e| \cdot N(\mathfrak{p}^{e-1}).$$

Die Behauptung folgt nun induktiv, wenn wir zeigen können, dass $|\mathfrak{p}^{e-1}/\mathfrak{p}^e| = N(\mathfrak{p})$ ist. Hierzu sei $\beta \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$ beliebig vorgegeben. Wir behaupten, dass dann die Abbildung

$$\varphi: \quad \mathfrak{o}_K \;\longrightarrow\; \mathfrak{p}^{e-1}/\mathfrak{p}^e\,, \quad \alpha \;\mapsto\; \alpha\beta$$

surjektiv ist; denn in

$$\mathfrak{p}^e \overset{\neq}{\hookrightarrow} (\mathfrak{p}^e, \beta) \;=\; \big\{\pi + \alpha\beta \mid \pi \in \mathfrak{p}^e,\, \alpha \in \mathfrak{o}_K\big\} \hookrightarrow \mathfrak{p}^{e-1}$$

muß die zweite Inklusion eine Gleichheit sein, weil die erste Inklusion strikt ist und für die Primfaktorzerlegung des Ideals in der Mitte somit keine andere Möglichkeit bleibt. Offenbar ist $\mathfrak{p} \subseteq \ker(\varphi) \neq \mathfrak{o}_K$ und somit sogar $\mathfrak{p} = \ker(\varphi)$, weil $\mathfrak{p} \neq (0)$ maximal ist. Wir erhalten also einen Isomorphismus

$$\overline{\varphi}: \quad \mathfrak{o}_K/\mathfrak{p} \;\xrightarrow{\sim}\; \mathfrak{p}^{e-1}/\mathfrak{p}^e$$

und es folgt $|\mathfrak{p}^{e-1}/\mathfrak{p}^e| = N(\mathfrak{p})$ wie gewünscht. □

Korollar 2.6. *Die Idealnorm setzt sich eindeutig auf gebrochene Ideale fort zu einem multiplikativen Homomorphismus $N : I_K \longrightarrow \mathbb{Q}^\times$.*

Beweis. Nach dem vorigen Lemma ist die Idealnorm ein Homomorphismus von dem multiplikativen Monoid der ganzen Ideale $(0) \neq \mathfrak{a} \trianglelefteq \mathfrak{o}_K$ in den multiplikativen Monoid $\mathbb{Z}$, und hieraus folgt die Behauptung. □

Übung 2.7. Man folgere aus dem Elementarteilersatz, dass die obige Norm im Fall von Hauptidealen kompatibel ist mit der für Körperelemente: Für $\alpha \in K^\times$ hat man

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

3. Die Endlichkeit der Klassengruppe

Wir wollen nun Minkowski's Gitterpunktsatz auf Ideale des Ganzheitsringes $\mathfrak{o}_K$ anwenden.

Proposition 3.1. *Es gibt eine nur von r und s abhängige Konstante $c_{r,s} \in \mathbb{R}$, sodass jedes von Null verschiedene ganze Ideal $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ ein Element $\alpha \neq 0$ enthält mit*

$$|N_{K/\mathbb{Q}}(\alpha)| \;\leq\; c_{r,s} \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a}).$$

Beweis. Wir wollen Minkowski's Satz auf das Gitter $\Lambda = \iota(\mathfrak{a}) \subset V$ anwenden und betrachten

$$\|\cdot\|_1: \quad V \;=\; \mathbb{R}^r \times \mathbb{C}^s \;\longrightarrow\; \mathbb{R}, \quad \|v\|_1 \;=\; \sqrt[n]{\prod_{i=1}^{r} |v_i| \cdot \prod_{i=r+1}^{r+s} |v_i|^2}$$

mit

$$|N_{K/\mathbb{Q}}(\alpha)| \;=\; \|\iota(\alpha)\|_1^n \quad \text{für} \quad \alpha \;\in\; K.$$

Man beachte, dass die soeben definierte reellwertige Funktion $\|\cdot\|_1 : V \longrightarrow \mathbb{R}$ im Fall $r+s > 1$ nicht positiv definit ist und für $R > 0$ in diesem Fall die symmetrische Teilmenge

$$S_{1,R} \;=\; \big\{v \in V \mid \|v\|_1 \leq R\big\} \;\subset\; V$$

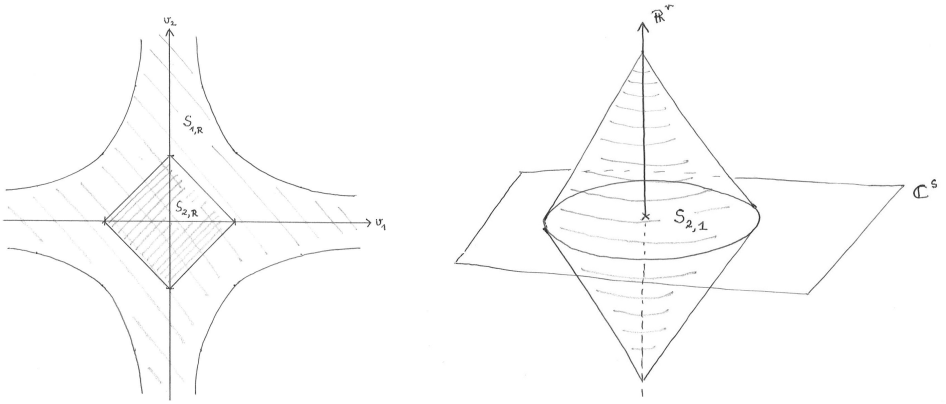
weder beschränkt noch konvex ist. Nach der Ungleichung zwischen arithmetischem und geometrischem Mittel gilt jedoch

$$\|v\|_2 \;:=\; \tfrac{1}{n} \cdot \Big(\sum_{i=1}^{r} |v_i| + 2 \sum_{i=r+1}^{r+s} |v_i|\Big) \;\geq\; \|v\|_1,$$

und die symmetrische Teilmenge

$$S_{2,R} \;=\; \big\{v \in V \mid \|v\|_2 \leq R\big\} \;\subset\; V$$

ist tatsächlich kompakt und konvex. Die folgende Skizze illustriert die Situation in den Fällen $r = 1, s = 0$ und $r = s = 1$:



Nach Minkowski's Gitterpunktsatz 1.6 existiert ein $\alpha \in \mathfrak{a} \setminus \{0\}$ mit $\iota(\alpha) \in S_{2,R}$, sobald

$$vol(S_{2,R}) \;\geq\; 2^n \cdot vol(\Lambda) \;=\; 2^n \cdot N(\mathfrak{a}) \cdot \sqrt{|d_K|}$$

gilt. Dies ist offenbar der Fall für $R \gg 0$, genauer erhält man durch Reskalieren offenbar

$$vol(S_{2,R}) \;=\; R^n \cdot vol(S_{2,1}).$$

Wenn R kleinstmöglich gewählt wird, sodass die obige Abschätzung gilt, folgt für die Norm

$$|N_{K/\mathbb{Q}}(\alpha)| \;=\; \|\iota(\alpha)\|_1^n \;\leq\; \|\iota(\alpha)\|_2^n \;\leq\; R^n \;=\; c_{r,s} \cdot N(\mathfrak{a}) \cdot \sqrt{|d_K|}$$

wobei die Konstante

$$c_{r,s} \;=\; vol(S_{2,1})^{-1} \cdot 2^n$$

nur von r und s abhängt (siehe unten für ihre explizite Berechnung). □

Bemerkung 3.2. Durch Induktion über r und Einführen von Polarkoordinaten für die s komplexen Koordinaten liefert explizite Integration $vol(S_{2,1}) = \frac{2^r \cdot \pi^s \cdot n^n}{n!}$ und somit

$$c_{r,s} \;=\; \Big(\frac{4}{\pi}\Big)^s \cdot \frac{n!}{n^n}\,.$$

Die Zahl $M_K = c_{r,s} \cdot \sqrt{|d_K|} \in \mathbb{R}$ wird auch als die *Minkowski-Konstante* von K bezeichnet. Im Spezialfall quadratischer Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit d quadratfrei ist

$$c_{r,s} \;=\; \begin{cases} 2/\pi & \text{falls } d < 0, \\ 1/2 & \text{falls } d > 0. \end{cases}$$

Mit $d_K = d$ für $d \equiv 1 \mod 4$ sowie $d_K = 4d$ sonst erhalten wir für $K = \mathbb{Q}(\sqrt{d})$ also die folgenden Minkowski-Konstanten:

$d =$	$\cdots$	-7	-6	-5	-3	-2	-1	$+2$	$+3$	$+5$	$+6$	$+7$	$\cdots$
$M_K \simeq$	$\cdots$	1,7	3.1	2.8	1.1	1.8	1.2	1.4	1.7	1.1	2.6	2.6	$\cdots$

Kommen wir nun zu allgemeinen Zahlkörpern K zurück. Eine erste Anwendung der Minkowski-Schranke ist das folgende

Korollar 3.3. *Es ist $|d_K| > 1$ für alle Zahlkörper $K \neq \mathbb{Q}$.*

Beweis. Für das größtmögliche Gitter $\mathfrak{a} = \mathfrak{o}_K$ liefert Proposition 3.1 mit $s \leq n/2$ die Abschätzung

$$1 \;\leq\; N(\alpha) \;\leq\; c_n \cdot \sqrt{|d_K|} \quad \text{mit} \quad c_n \;:=\; \Big(\frac{4}{\pi}\Big)^{\frac{n}{2}} \cdot \frac{n!}{n^n}\,.$$

Es genügt also, induktiv

$$c_n \;<\; 1 \quad \text{für alle} \quad n \;\geq\; 2$$

zu beweisen. Der Induktionsanfang ist offensichtlich mit dem Wert $c_2 = 2/\pi < 1$, und mit $c_{n+1}/c_n = \sqrt{4/\pi} \cdot (n/(n+1))^n < 1$ für alle n folgt die Behauptung. □

Wir wollen nun die Minkowski-Schranke in Proposition 3.1 für das Studium der Gruppe der gebrochenen Ideale des Dedekind-Ringes $R = \mathfrak{o}_K$ anwenden. Der Einfachheit halber bezeichnen wir diese Gruppe im Folgenden mit I_K statt I_R, analog für die Klassengruppe

$$C_K \;=\; I_K/K^\times$$

welche die Nicht-Faktorialität des Ganzheitsringes kontrolliert. Durch geschicktes Invertieren erhält man hierfür die folgende

Proposition 3.4. *Jede Element der Idealklassengruppe C_K lässt sich durch ein ganzes Ideal $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ mit Norm $N(\mathfrak{a}) \leq M_K$ repräsentieren.*

Beweis. Sei $\mathfrak{b} \in I_K$ ein gebrochenes Ideal. Dann ist auch das Inverse $\mathfrak{b}^{-1}$ ein gebrochenes Ideal. Indem wir $\mathfrak{b}$ durch $\beta \cdot \mathfrak{b}$ mit geeignetem $\beta \in K^\times$ ersetzen, können wir ohne Änderung der durch das gebrochene Ideal repräsentierten Klasse $[\mathfrak{b}] \in C_K$ erreichen, dass

$$\mathfrak{b}^{-1} \;\trianglelefteq\; \mathfrak{o}_K$$

ein ganzes Ideal ist. Nach Proposition 3.1 existiert daher ein von Null verschiedenes Element $\alpha \in \mathfrak{b}^{-1}$ mit $|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N(\mathfrak{b}^{-1})$. Dann ist $\mathfrak{a} = \alpha \cdot \mathfrak{b} \trianglelefteq \mathfrak{o}_K$ ein ganzes Ideal mit

$$N(\mathfrak{a}) \;=\; |N_{K/\mathbb{Q}}(\alpha)| \cdot N(\mathfrak{b}) \;\leq\; M_K$$

und $[\mathfrak{a}] = [\mathfrak{b}] \in C_K$ wie gewünscht. □

Korollar 3.5. *Die Klassengruppe C_K ist endlich.*

Beweis. Nach Proposition 3.4 genügt es zu zeigen, dass es für jedes feste $N \in \mathbb{N}$ höchstens endlich viele ganze Ideale $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ gibt mit $N(\mathfrak{a}) = N$. In der Tat ist für jedes solche Ideal

$$[\mathfrak{o} : \mathfrak{a}] \;=\; N \quad \text{und somit} \quad N \cdot \mathfrak{o} \;\subseteq\; \mathfrak{a},$$

also $\mathfrak{a} \mid (N)$. Schreibt man

$$(N) \;=\; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

mit Exponenten $e_i \in \mathbb{N}$ und paarweise verschiedenen Primidealen $\mathfrak{p}_i \trianglelefteq \mathfrak{o}_K$, so folgt aus der obigen Teibarkeit $\mathfrak{a} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$ mit $f_i \in \{0, 1, \ldots, e_i\}$ und somit bleiben nur endlich viele Möglichkeiten. □

Der Beweis des Korollars liefert zugleich eine effektive Schranke: Jedes Element der Klassengruppe C_K lässt sich durch einen Teiler $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ der endlich vielen Hauptideale

$$(N) \;\trianglelefteq\; \mathfrak{o}_K \quad \text{mit} \quad N \;=\; 2, 3, \ldots, \lfloor M_K \rfloor$$

repräsentieren. Für die Berechnung von Klassengruppen müssen also nur Relationen zwischen den Primidealen untersucht werden, die in der Faktorisierung dieser endlich vielen Hauptideale vorkommen, denn diese Primideale erzeugen C_K.

BEISPIEL 3.6. Sei $K = \mathbb{Q}(\sqrt{d})$. Für die Minkowski-Schranke prüft man dann leicht nach:

$$\lfloor M_K \rfloor \;=\; 1 \quad\Longleftrightarrow\quad d \;\in\; \{-7,-3,-2,-1,+2,+3,+5,+13\}$$

Für diese Werte von d ist also die Klassengruppe C_K trivial. Die Umkehrung dieser Aussage gilt aber nicht, beispielsweise sind die Klassengruppen C_K auch für die Werte $d \in \{-11,-19,-43,-67,-163\}$ trivial. Tatsächlich kann man zeigen, dass diese Liste alle Fälle trivialer Klassengruppen für Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit $d < 0$ erschöpft: Dieses *Klassenzahl-Eins-Problem* wurde 1952 von dem mathematischen Außenseiter Kurt Heegner gelöst. Sein Beweis fand aber wegen scheinbarer Lücken zur damaligen Zeit keine allgemeine Akzeptanz, was sich erst nach Heegners Tod mit der Arbeit von Stark ändern sollte; einen unabhängigen Beweis hat etwa zur gleichen Zeit Baker gegeben und für die hierin eingeführten neuen Techniken eine Fields-Medaille bekommen. Der Fall $d > 0$ ist komplizierter: Man vermutet, dass hier C_K für unendlich viele d trivial ist, aber dies ist bis heute offen.

BEISPIEL 3.7. Für $K = \mathbb{Q}(\sqrt{-5})$ ist für die Minkowski-Schranke $\lfloor M_K \rfloor = 2$, also wird die Klassengruppe in diesem Fall erzeugt von den Primidealen, die das von 2 erzeugte Hauptideal teilen. Man überlegt sich leicht, dass dieses Hauptideal die Form

$$(2) \;=\; (2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) \;=\; \mathfrak{p}^2 \quad \text{mit} \quad \mathfrak{p} \;=\; (2, 1+\sqrt{-5})$$

hat wegen

$$\begin{aligned} 2 \;&=\; (1+\sqrt{-5})(2-\sqrt{-5}) - 2\cdot 2 \;\in\; \mathfrak{p}^2 \\ (2) \;\ni\; (1+\sqrt{-5})(1-\sqrt{-5}) \;&=\; 2\cdot(-4), \end{aligned}$$

und $\mathfrak{p}$ ist ein Primideal, weil offenbar der Quotient $\mathfrak{o}_K/\mathfrak{p} \simeq \mathbb{F}_2$ ein Körper ist. Also wird die Klassengruppe von $\mathfrak{p}$ erzeugt und

$$C_K \;\simeq\; \mathbb{Z}/2\mathbb{Z}$$

weil $\mathfrak{o}_K$ nicht faktoriell und somit kein Hauptidealring ist.

BEISPIEL 3.8. Für $K = \mathbb{Q}(\sqrt{-30})$ ist $\lfloor M_K \rfloor = 3$, also wird die Klassengruppe hier erzeugt von den Primidealen, welche eines der Hauptideale (ν) mit $\nu \in \{2,3\}$ teilen. Es gilt

$$(\nu) \;=\; \mathfrak{p}_\nu^2 \quad \text{mit} \quad \mathfrak{p}_\nu \;=\; (\nu, \sqrt{-30})$$

mit einer ähnlichen Rechnung wie im vorigen Beispiel, und die $\mathfrak{p}_\nu$ sind Primideale, weil $\mathfrak{o}_K/\mathfrak{p}_\nu \simeq \mathbb{F}_\nu$ Körper sind. Diese Primideale sind keine Hauptideale, denn durch Betrachten der Norm sieht man, dass die Elemente $\nu = 2, 3$ in dem Ring $\mathfrak{o}_K$ irreduzibel sind, während offenbar $\sqrt{-30}$ nicht durch sie teilbar ist. Ähnlich zeigt man, dass auch das Produkt

$$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_3 \;&=\; (2, \sqrt{-30})(3, \sqrt{-30}) \\ &=\; (6, 2\sqrt{-30}, 3\sqrt{-30}, -30) \;=\; (6, \sqrt{-30}) \end{aligned}$$

kein Hauptideal ist. Somit ist

$$C_K \;\simeq\; \langle x, y \mid xy = yx, x^2 = y^2 = 1 \rangle \;\simeq\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

4. Der Einheitensatz von Dirichlet

Eine fiktive Quelle berichtet, dass sich in der Schlacht bei Hastings 1066 die angelsächsischen Truppen dem Heer der Normannen in 13 gleich großen Quadraten entgegengestellt und dann mit ihrem hinzueilenden König Harald II ein einziges unbesiegbares Quadrat gebildet hätten. Was würde dies über die angelsächsische Truppengröße

$$13\,y^2 + 1 \;=\; x^2$$

mit $x, y \in \mathbb{N}$ aussagen? Für jede Lösung der obigen Gleichung ist $x + y\sqrt{13} \in \mathfrak{o}_K^\times$ eine Einheit des Ganzheitsringes von $K = \mathbb{Q}(\sqrt{13})$, und hiervon ausgehend werden wir später alle solchen Lösungen finden.

Allgemein bildet neben der Klassengruppe die Einheitengruppe $\mathfrak{o}_K^\times$ eine der wichtigsten Invarianten eines Zahlkörpers K. Auch hier gibt der Gitterpunktsatz von Minkowski nähere Information. Hierzu beachte man, dass die in Abschnitt 2 eingeführte Einbettung

$$\begin{aligned} \iota: \quad \mathfrak{o}_K \;&\hookrightarrow\; V \;=\; \mathbb{R}^r \times \mathbb{C}^s \\ \alpha \;&\mapsto\; \big(\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)\big) \end{aligned}$$

nicht nur $\mathbb{Q}$-linear, sondern auch ein Ringhomomorphismus ist, wenn $V = \mathbb{R}^r \times \mathbb{C}^s$ mit der Produkt-Ringstruktur ausgestattet wird. Also schränkt sich ι ein zu einer Einbettung

$$\iota: \quad \mathfrak{o}_K^\times \;\hookrightarrow\; (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$$

zwischen den Einheitengruppen der betreffenden Ringe. Da Einheiten $\alpha \in \mathfrak{o}_K^\times$ die Norm $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ haben, liegt das Bild dieser Einbettung in der abgeschlossenen Untergruppe

$$G \;:=\; \big\{\, v \in V^\times \mid \|v\|_1 \;=\; 1 \,\big\} \;\subset\; V^\times$$

welche durch

$$\|v\|_1 \;:=\; \sqrt[n]{\prod_{i=1}^{r} |v_i| \cdot \prod_{i=r+1}^{r+s} |v_i|^2} \qquad \text{mit} \qquad |N_{K/\mathbb{Q}}(\alpha)| \;=\; \|\iota(\alpha)\|_1^n$$

definiert wird wie im Beweis von Proposition 3.1. Um die multiplikative Struktur der Einheitengruppen in eine additive zu übersetzen, nutzen wir den Logarithmus und führen die Abbildung

$$\begin{aligned} \mathrm{Log}: \quad V^\times \;=\; (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \;&\longrightarrow\; \mathbb{R}^{r+s} \\ \big(z_1, \ldots, z_{r+s}\big) \;&\mapsto\; \big(\log|z_1|, \ldots, \log|z_r|, \ldots, \log|z_{r+s}|\,\big) \end{aligned}$$

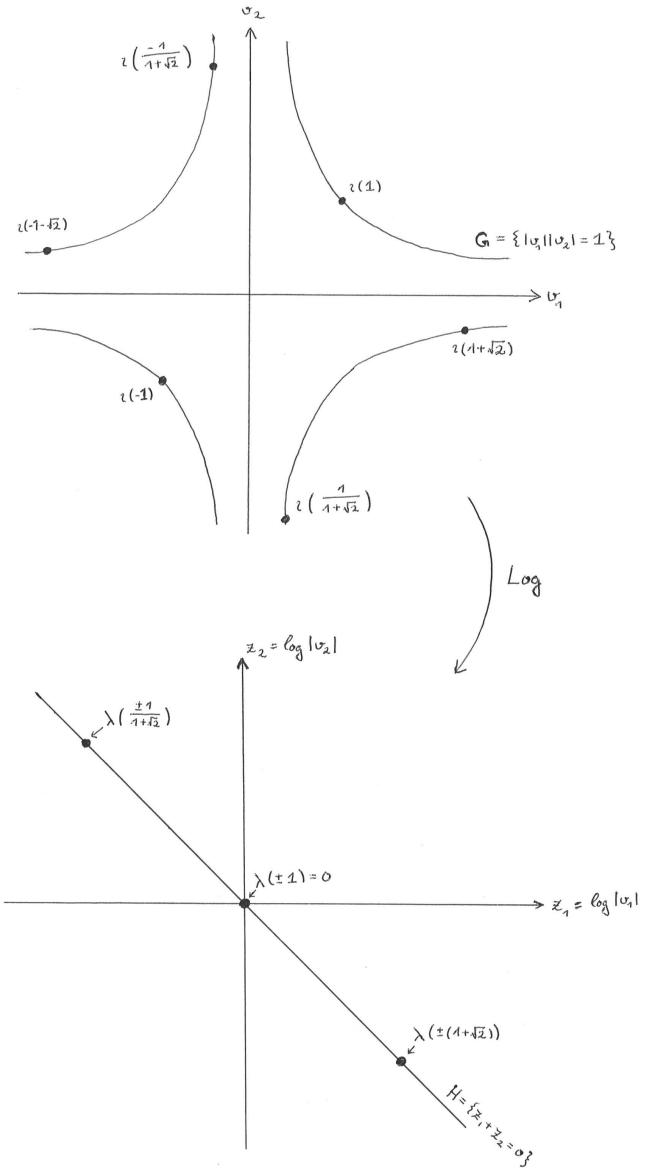
ein. Man beachte, dass der Logarithmus die multiplikative Untergruppe $G \subset V^\times$ auf die Hyperebene

$$H \;:=\; \big\{\, z \in \mathbb{R}^{r+s} \mid z \cdot h \;=\; 0 \,\big\} \quad \text{für} \quad h \;=\; \big(\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{2, 2, \ldots, 2}_{s}\big)$$

abbildet. Betrachten wir beispielsweise den quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{3})$, so hat man

$$\begin{aligned} \iota: \quad \mathfrak{o}_K \;=\; \mathbb{Z}[\sqrt{2}] \;\hookrightarrow\; V \;=\; \mathbb{R}^2, \qquad & a + b\sqrt{2} \;\mapsto\; \big(a + b\sqrt{2}, a - b\sqrt{2}\,\big), \\ \mathrm{Log}: \quad V^\times \;=\; (\mathbb{R}^\times)^2 \;\longrightarrow\; \mathbb{R}^2, \qquad & (v_1, v_2) \;\mapsto\; \big(\log|v_1|, \log|v_2|\,\big), \end{aligned}$$

und die Situation sieht wie in der folgenden Skizze aus:



Beim Eintragen weiterer Punkte wird schnell augenfällig, dass das Bild $\lambda(\mathfrak{o}_K^\times)$ hier eine zyklische Untergruppe der Geraden H bildet. Tatsächlich gilt für beliebige Zahlkörper K der folgende

SATZ 4.1. *Für die Zusammensetzung* $\lambda = \mathrm{Log} \circ \iota : \mathfrak{o}_K^\times \longrightarrow \mathbb{R}^{r+s}$ *gilt:*

(1) *Der Kern von* λ *ist die endliche zyklische Gruppe*

$$\mu_K \ := \ \big\{\, \alpha \in K^\times \mid \alpha^N = 1 \text{ für ein } N \in \mathbb{N} \,\big\}.$$

(2) *Das Bild von* λ *ist ein Gitter in der Hyperebene* $H \simeq \mathbb{R}^{r+s-1}$.

Beweis. (1) Offenbar wird der gesuchte Kern unter der Einbettung $\iota : K^\times \hookrightarrow V^\times$ auf die Teilmenge

$$\iota(\ker(\lambda)) \ = \ \iota(\mathfrak{o}_K^\times) \cap \mathrm{Log}^{-1}(0)$$

abgebildet. Letztere ist aber als Durchschnitt der diskreten Teilmenge $\iota(\mathfrak{o}_K^\times)$ mit der kompakten Menge $\mathrm{Log}^{-1}(0) = \{\, v \in V \mid |v_i| = 1 \,\text{für alle}\, i \,\}$ endlich, somit

ist auch $\ker(\lambda)$ eine endliche Gruppe. Als endliche Untergruppe der multiplikativen Gruppe eines Körpers ist dann $\ker(\lambda)$ zyklisch und erzeugt von einer Einheitswurzel; und umgekehrt liegt offenbar jede Einheitswurzel $\alpha \in K^\times$ im Kern von λ, da für Einheitswurzeln $|\sigma_i(\alpha)| = 1$ für alle i gilt.

(2) Zunächst ist das Bild $\lambda(\mathfrak{o}_K^\times) \subset H$ offenbar enthalten in der Hyperebene H weil

$$N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}^\times = \{\pm 1\} \quad \text{für alle Einheiten} \quad \alpha \in \mathfrak{o}_K^\times$$

gilt. Wir behaupten weiter, dass dieses Bild eine diskrete Teilmenge von H ist. Nach Translation genügt es, diese Behauptung in kleinen Umgebungen des Ursprungs zu zeigen; und für $C_\epsilon = \{ z \mid |z_i| \leq \epsilon \text{ für alle } i \}$ mit $\epsilon > 0$ ist der Schnitt $\lambda(\mathfrak{o}_K^\times) \cap C_\epsilon$ notwendigerweise endlich, weil

$$\iota(\mathfrak{o}_K^\times) \cap \mathrm{Log}^{-1}(C_\epsilon)$$

als Durchschnitt einer diskreten mit einer kompakten Teilmenge endlich ist.

Somit ist $\lambda(\mathfrak{o}_K^\times) \subset H$ eine diskrete Untergruppe. Zu zeigen bleibt, dass diese den gesamten reellen Untervektorraum $H \subset \mathbb{R}^{r+s}$ aufspannt. Nach Lemma 1.1 ist dies äquivalent dazu, dass der Quotient

$$H/\lambda(\mathfrak{o}_K^\times)$$

kompakt ist. Da stetige Bilder kompakter topologischer Räume kompakt sind, reicht es, die Kompaktheit von

$$G/\iota(\mathfrak{o}_K^\times)$$

zu zeigen. Hierzu wählen wir eine kompakte konvexe symmetrische Menge $S \subset V$ mit $vol(S) > 2^n\, vol(\Lambda)$ für $\Lambda = \iota(\mathfrak{o}_K)$, beispielsweise eine genügend große Kugel um den Ursprung. Als stetige Funktion nimmt $\| \cdot \|_1$ auf dem Kompaktum S ein Maximum

$$c := \max\{ \|v\|_1 \mid v \in S \} < \infty$$

an. Da es nur endlich viele ganze Ideale mit beschränkter Norm gibt und da ein Element bis auf Assoziiertheit eindeutig durch das von ihm erzeugte Hauptideal bestimmt ist, können wir Elemente $\gamma_1, \ldots, \gamma_N \in \mathfrak{o}_K$ finden, sodass jedes $\gamma \in \mathfrak{o}_K$ mit $|N_{K/\mathbb{Q}}(\gamma)| \leq c$ zu einem dieser Elemente assoziiert ist. Wir behaupten, dass dann

$$G \subset \bigcup_{i=1}^{N} \iota\big(\gamma_i^{-1} \cdot \mathfrak{o}_K^\times\big) \cdot S$$

gilt: Denn für $g \in G$ ist die entsprechend reskalierte Teilmenge $g^{-1}S$ auch kompakt, konvex und symmetrisch mit $vol(g^{-1}S) = vol(S)$, der Satz von Minkowski liefert also einen Gitterpunkt

$$0 \neq \iota(\alpha) = g^{-1}s \in \Lambda \cap g^{-1}S \quad \text{mit} \quad \alpha \in \mathfrak{o}_K,\, s \in S.$$

Wegen $\|g^{-1}\|_1 = 1$ gilt hierbei für die Norm die Abschätzung $|N_{K/\mathbb{Q}}(\alpha)| = \|s\|_1 \leq c$, sodass α assoziiert zu einem γ_i mit $i \in \{1, 2, \ldots, N\}$ ist und somit wie gewünscht folgt, dass

$$g = gs^{-1} \cdot s = \iota\big(\gamma_i^{-1} \cdot \gamma_i/\alpha\big) \cdot s \in \iota\big(\gamma_i^{-1} \cdot \mathfrak{o}_K^\times\big) \cdot S$$

ist. Die stetige Surjektion

$$G \cap \bigcup_{i=1}^{N} \iota(\gamma_i^{-1}) \cdot S \twoheadrightarrow G/\iota(\mathfrak{o}_K^\times)$$

zeigt dann, dass der Quotient auf der rechten Seite kompakt ist, denn die linke Seite ist als Schnitt einer abgeschlossenen Teilmenge $G \subset V$ mit einer kompakten Teilmenge ebenfalls kompakt. □

KOROLLAR 4.2 (Dirichlet'scher Einheitensatz). *Die Einheitengruppe von $\mathfrak{o}_K$ hat die Gestalt*

$$\mathfrak{o}_K^\times \simeq \mu_K \times \mathbb{Z}^m \quad \textit{mit} \quad m := r+s-1.$$

Beweis. Satz 4.1 liefert eine kurze exakte Sequenz $0 \to \mu_K \to \mathfrak{o}_K^\times \to \mathbb{Z}^m \to 0$, und da der rechts stehende Term $\mathbb{Z}^m$ eine freie abelsche Gruppe ist, lässt er sich als direkter Summand von $\mathfrak{o}_K^\times$ abspalten. □

Es gibt also Einheiten $\epsilon_1, \dots, \epsilon_m \in \mathfrak{o}_K^\times$ mit der Eigenschaft, dass jedes $\epsilon \in \mathfrak{o}_K^\times$ eindeutig als

$$\epsilon = \zeta \cdot \epsilon_1^{\nu_1} \cdots \epsilon_m^{\nu_m} \quad \text{mit} \quad \zeta \in \mu_K,\ \nu_1, \dots, \nu_m \in \mathbb{Z}$$

geschrieben werden kann. Man sagt in diesem Fall auch kurz, dass $\epsilon_1, \dots, \epsilon_m$ ein System von *Fundamentaleinheiten* des Zahlkörpers sei. Natürlich ist ein solches nicht eindeutig bestimmt, ebensowenig wie die Spaltung der obigen kurzen exakten Sequenz, die Ambiguität ist jedoch leicht zu beschreiben:

LEMMA 4.3. *Jedes weitere System von Fundamentaleinheiten $\tilde\epsilon_1, \dots, \tilde\epsilon_m$ erhält man durch Anwenden einer Matrix $A = (a_{ij}) \in Gl_m(\mathbb{Z})$ und Multiplikation mit geeigneten $\zeta_i \in \mu_K$,*

$$\tilde\epsilon_i = \zeta_i \cdot \epsilon_1^{a_{1i}} \cdots \epsilon_m^{a_{1i}} \quad \textit{für} \quad i = 1, 2, \dots, m.$$

Beweis. Sowohl die $\lambda(\epsilon_i)$ als auch die $\lambda(\tilde\epsilon_i)$ sind eine Gitterbasis von $\Lambda = \lambda(\mathfrak{o}_K^\times)$, und die Transformation zwischen zwei Basen eines Gitters vom Rang m ist durch eine Matrix $A \in Gl_m(\mathbb{Z})$ gegeben. Wegen $\mu_K = \ker(\lambda)$ folgt die Behauptung. □

BEISPIEL 4.4. Sei $K = \mathbb{Q}(\sqrt{d})$ für eine quadratfreie ganze Zahl $d \in \mathbb{Z}$.

(1) Für $d < 0$ sieht man leicht (Übung):

$$\mathfrak{o}_K^\times = \mu_K \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{für } d = -1, \\ \mathbb{Z}/6\mathbb{Z} & \text{für } d = -3, \\ \mathbb{Z}/2\mathbb{Z} & \text{sonst.} \end{cases}$$

(2) Für $d > 0$ ist

$$\mathfrak{o}_K^\times = \{\pm 1\} \times \{\, \epsilon^\nu \mid \nu \in \mathbb{Z} \,\} \simeq \{\pm 1\} \times \mathbb{Z}$$

für die eindeutig bestimmte sogenannte *Fundamentaleinheit* $\epsilon \in \mathfrak{o}_K^\times \subset \mathbb{R}^\times$ mit $\epsilon > 1$ (in der reellen Einbettung mit $\sqrt{d} > 0$).

Für reell-quadratische Zahlkörper kann man die Fundamentaleinheit mit folgender naiven Methode finden:

LEMMA 4.5. *Sei $d > 0$ eine quadratfreie ganze Zahl, und es sei $b \in \mathbb{N}$ minimal, sodass*

$$db^2 \pm e^2 \quad \textit{eine Quadratzahl } a^2 \textit{ mit } a \in \mathbb{N} \textit{ ist,}$$

wobei wir

$$e := \begin{cases} 2 & \textit{für } d \equiv 1 \mod 4, \\ 1 & \textit{für } d \equiv 2, 3 \mod 4 \end{cases}$$

setzen. Dann ist die Fundamentaleinheit des quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$ gegeben durch

$$\epsilon = \frac{a + b\sqrt{d}}{e}.$$

Beweis. Nach unserer Definition der Fundamentaleinheit erfüllt diese $\epsilon > 1$ und somit $\epsilon > \epsilon^{-1} > -\epsilon^{-1} > -\epsilon$. Da Einheiten die Norm ± 1 besitzen, erhalten wir wegen

$$(x + y\sqrt{d})^{-1} \;=\; \pm(x - y\sqrt{d}) \quad \text{für} \quad N_{K/\mathbb{Q}}(x + y\sqrt{d}) \;=\; \pm 1,$$

dass

$$\epsilon \;=\; \frac{a_1 + b_1\sqrt{d}}{e} \quad \text{mit ganzen Zahlen} \quad a_1, b_1 \;>\; 0$$

ist. Man sieht leicht, dass die Koeffizienten in allen höheren Potenzen von ϵ echt wachsen: Für $m > 1$ ist

$$\epsilon^m \;=\; \frac{a_m + b_m\sqrt{d}}{e} \quad \text{mit ganzen Zahlen} \quad a_m \;>\; a_{m-1} \quad \text{und} \quad b_m \;>\; b_{m-1}.$$

Insbesondere ist b_1 minimal, also $b_1 = b$ und damit auch $a_1 = a$. □

Beispiel 4.6. Für $K = \mathbb{Q}(\sqrt{13})$ liefert das obige Lemma mit $b = 1$, $a = 3$ die Fundamentaleinheit

$$\epsilon \;=\; \frac{3 + \sqrt{13}}{2} \;\in\; \mathfrak{o}_K^\times$$

mit Norm $N_{K/\mathbb{Q}}(\epsilon) = -1$. Insbesondere sind also die Elemente der Norm 1 in $\mathfrak{o}_K$ bis auf das Vorzeichen und Konjugation genau die geradzahligen Potenzen dieser Fundamentaleinheit. Jede ganzzahlige Lösung $(x, y) \in \mathbb{Z}^2$ von $x^2 - 13y^2 = 1$ muß damit die Form

$$x + y\sqrt{13} \;=\; \pm\Big(\frac{3 \pm \sqrt{13}}{2}\Big)^{2m} \quad \text{mit} \quad m \in \mathbb{N}_0$$

haben, aber nicht alle diese Potenzen liefern auch tatsächlich *ganzzahlige* Lösungen; die kleinsten Werte sind

$$\begin{aligned}
\Big(\frac{3 \pm \sqrt{13}}{2}\Big)^2 &= \frac{11 \pm 3\sqrt{13}}{2} \\
\Big(\frac{3 \pm \sqrt{13}}{2}\Big)^4 &= \frac{119 \pm 33\sqrt{13}}{2} \\
\Big(\frac{3 \pm \sqrt{13}}{2}\Big)^6 &= 649 \pm 180\sqrt{13}.
\end{aligned}$$

Dies liefert für die zu Beginn erwähnte angelsächsische Armee mit König Harald II eine Stärke von mindestens

$$649^2 \;=\; 13 \cdot 180^2 + 1 \;=\; 421\,201$$

Soldaten — so genau sollte man es mit dieser Angabe wohl doch nicht nehmen.

Das soeben benutzte Verfahren führt auch allgemein zum Ziel, und weiter als bis zur sechsten Potenz muß man dabei nie gehen:

Lemma 4.7. *Für quadratfreie ganze Zahlen $d > 0$ hat die sogenannte Pell'sche Gleichung*

$$x^2 - dy^2 = 1$$

unendlich viele nichtnegative ganzzahlige Lösungen $(x, y) \in \mathbb{N}_0^2$. Genauer existiert ein $\delta \in \{1, 2, 3, 6\}$, sodass die Lösungen bijektiv den Potenzen der Form

$$x + y\sqrt{d} \;=\; \epsilon^{m\delta} \quad \textit{mit} \quad m \in \mathbb{N}_0$$

entsprechen, wobei $\epsilon > 1$ die Fundamentaleinheit des Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$ ist.

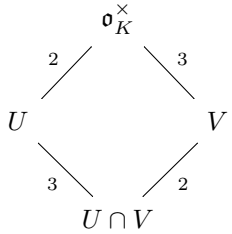
Beweis. Die Lösungen sind genau die Elemente im Durchschnitt $U \cap V \subseteq \mathfrak{o}_K^\times$ der Untergruppen

$$U := \left\{ \alpha \in \mathfrak{o}_K^\times \mid N_{K/\mathbb{Q}}(\alpha) = +1 \right\} \quad \text{und} \quad V := \mathbb{Z}[\sqrt{d}]^\times.$$

Die erste Untergruppe ist als Kern eines Gruppenhomomorphismus nach $\{\pm 1\}$ vom Index ≤ 2. Die zweite Untergruppe enthält den Kern $1+2\mathfrak{o}_K$ des Homomorphismus von Einheitengruppen

$$\mathfrak{o}_K^\times \twoheadrightarrow R^\times \quad \text{für} \quad R = \mathfrak{o}_K/2\mathfrak{o}_K.$$

Da R ein Ring mit vier Elementen ist, hat die Einheitengruppe $R^\times$ höchstens drei Elemente, also ist V eine Untergruppe vom Index 1 oder 3. Wir erhalten das Diagramm



wobei die Indizes der diagonalen Inklusionen jeweils Teiler der gegebenen Zahlen sind. Also ist $U \cap V \hookrightarrow \mathfrak{o}_K^\times$ eine Untergruppe vom Index $1, 2, 3$ oder 6. □

KAPITEL IV

Zerlegung und Verzweigung

Die Untersuchung von Summen zweier Quadrate hat uns auf Zerlegungen von Primzahlen in den Gauß'schen ganzen Zahlen geführt. Allgemeiner haben wir bei der Berechnung von Klassengruppen gesehen, dass die Zerlegung der von Primzahlen erzeugter Hauptideale in Ganzheitsringen von Zahlkörpern eine fundamentale Rolle spielt. Im Folgenden werden wir

- allgemeine Begriffe zur Beschreibung solcher Zerlegungen einführen,
- systematische Methoden zu ihrer Berechnung entwickeln,
- einen gruppentheoretischen Bezug zur Galoistheorie herstellen.

Im Gegensatz zum vorigen Kapitel kehren wir wieder zu einem allgemeinen Rahmen zurück, der neben Zahlkörpern auch Funktionenkörper umfasst.

1. Grundbegriffe und erste Beispiele

Im Folgenden sei stets R ein Dedekind-Ring und $K/k = Quot(R)$ eine endliche separable Erweiterung seines Quotientenkörpers. Nach Proposition II.4.3 ist der ganze Abschluß

$$S \;=\; \big\{\, \alpha \in K \mid \alpha \text{ ist ganz über } R \,\big\}$$

wieder ein Dedekind-Ring, ein typisches Beispiel sind die Ganzheitsringe $S = \mathfrak{o}_K$ von Zahlkörpern:

$$\begin{array}{ccc} S & \hookrightarrow & K \\ | & & | \\ R & \hookrightarrow & k \end{array}$$

Jedes Primideal des größeren Ringes definiert ein solches des kleineren Ringes:

LEMMA 1.1. *Sei $\mathfrak{P} \trianglelefteq S$ ein Ideal und $\mathfrak{p} = \mathfrak{P} \cap R$.*

(1) *Es ist $\mathfrak{P} \neq 0$ genau dann, wenn $\mathfrak{p} \neq 0$ ist.*
(2) *Ist $\mathfrak{P} \trianglelefteq S$ ein Primideal, dann ist auch $\mathfrak{p} \trianglelefteq R$ ein Primideal.*
(3) *Ein Primideal $\mathfrak{P} \trianglelefteq S$ ist maximal genau dann, wenn $\mathfrak{p} \trianglelefteq R$ maximal ist.*

Beweis. Übung; dies benutzt tatsächlich nur, dass S/R eine ganze Erweiterung von Integritätsringen ist. Die zentrale Aussage (1) folgt durch Betrachten konstanter Terme in Ganzheitsgleichungen. Man beachte jedoch, dass die Umkehrung von (2) auch im Fall von Dedekind-Ringen im Allgemeinen nicht gilt! □

Wir interessieren uns hier für die andere Richtung: Jedem Ideal $\mathfrak{a} \trianglelefteq R$ kann man das hiervon erzeugte Ideal

$$\mathfrak{a}S \;=\; \big\{\, a_1 s_1 + \cdots + a_m s_m \mid a_i \in \mathfrak{a}, s_i \in S \,\big\} \;=\; \bigcap_{\substack{\mathfrak{b} \trianglelefteq S \\ \mathfrak{b} \supseteq \mathfrak{a}}} \mathfrak{b} \;\trianglelefteq\; S$$

zuordnen. Auch wenn $\mathfrak{a} = \mathfrak{p}$ ein Primideal ist, muß das hiervon erzeugte Ideal $\mathfrak{p}S$ nicht mehr prim sein. Allgemein gilt

LEMMA 1.2. *Sei* $(0) \neq \mathfrak{p} \trianglelefteq R$ *ein Primideal. Dann gelten für Primideale* $\mathfrak{P} \trianglelefteq S$ *die Äquivalenzen*

$$\mathfrak{P} \mid \mathfrak{p}S \iff \mathfrak{p}S \subseteq \mathfrak{P} \iff \mathfrak{p} \subseteq \mathfrak{P} \iff \mathfrak{P} \cap R = \mathfrak{p}$$

und es gibt mindestens ein Primideal, das diese äquivalenten Eigenschaften besitzt.

Beweis. Die erste Äquivalenz haben wir bereits im Kapitel über Dedekindringe gesehen, die zweite ist trivial. Für die letzte Äquivalenz beachte man, dass $\mathfrak{p} \neq (0)$ maximal ist, sodass aus $\mathfrak{p} \subseteq \mathfrak{P} \cap R$ Gleichheit folgt wegen $1 \notin \mathfrak{P}$. Um zu sehen, dass ein $\mathfrak{P}$ mit obigen Eigenschaften existiert, müssen wir zeigen, dass $\mathfrak{p}S \neq S$ für alle echten Ideale $\mathfrak{p} \lhd R$ gilt. Wäre dies nicht der Fall, so könnte man eine Zerlegung des Einselementes $1 = p_1 s_1 + \cdots + p_m s_m$ mit $p_i \in \mathfrak{p}$, $s_i \in S$ finden. Durch Bilden der Norm erhielte man dann

$$1 = \sum_{i=1}^{N} \tilde{p}_i \cdot r_i \quad \text{mit} \quad \tilde{p}_i \in \mathfrak{p},$$

wobei die $r_i = r_i(s_1, \ldots, s_n)$ symmetrische Funktionen in den Galoiskonjugierten der s_j wären. Insbesondere wären alle $r_i \in R$ und somit $1 \in \mathfrak{p}$, ein Widerspruch. □

DEFINITION 1.3. Die Primideale $\mathfrak{P} \trianglelefteq S$ mit obigen äquivalenten Eigenschaften werden *Primideale über* $\mathfrak{p}$ genannt, und wir benutzen dafür auch die Notation $\mathfrak{P} \mid \mathfrak{p}$ statt $\mathfrak{P} \mid \mathfrak{p}S$. Wir definieren das *maximale Spektrum* $\mathrm{Spm}(S)$ als die Menge aller maximalen Ideale des kommutativen Ringes S, analog für $\mathrm{Spm}(R)$. Lemma 1.1 liefert eine Abbildung

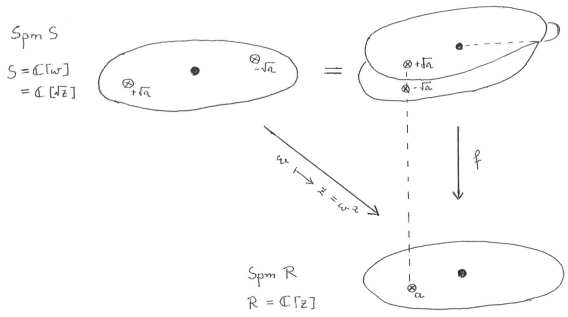
$$\begin{aligned} f: \quad \mathrm{Spm}(S) &\longrightarrow \mathrm{Spm}(R), \\ \mathfrak{P} &\mapsto \mathfrak{p} = \mathfrak{P} \cap R, \end{aligned}$$

und Lemma 1.2 besagt genau, dass diese Abbildung surjektiv ist und ihre Fasern die Form

$$f^{-1}(\mathfrak{p}) = \{ \text{Primideale } \mathfrak{P} \text{ über } \mathfrak{p} \} \subseteq \mathrm{Spm}(R)$$

besitzen. Für Funktionenkörper kann man dies geometrisch visualisieren:

BEISPIEL 1.4. Für $R = \mathbb{C}[z]$ ist jedes maximale Ideal ein Hauptideal $(z-a)$ mit einem $a \in \mathbb{C}$, wir können daher das maximale Spektrum $\mathrm{Spm}(R)$ mit der komplexen Ebene mit Koordinate z identifizieren. Für die ganze Ringerweiterung $S = R[\sqrt{z}]$ sieht dann die Situation folgendermaßen aus:



Die Faser über jedem Punkt $a \neq 0$ besteht aus zwei verschiedenen Punkten, die Faser über $a = 0$ ist aber ein einziger Punkt. In der Topologie und Funktionentheorie bezeichnet man solche Punkte als *Verzweigungspunkte*.

DEFINITION 1.5. Wie im obigen Beispiel sollten die Punkte der Fasern mit geeigneten Vielfachheiten gezählt werden, damit alle Fasern die gleiche Kardinalität besitzen. Hierzu führen wir folgende Begriffe ein:

(1) Wir schreiben

$$\mathfrak{p} \cdot S \;=\; \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} \quad \text{mit} \quad e_{\mathfrak{P}|\mathfrak{p}} \;\in\; \mathbb{N}$$

und nennen $e_{\mathfrak{P}|\mathfrak{p}}$ den *Verzweigungsindex* des Primideals $\mathfrak{P}$ über $\mathfrak{p}$.

(2) Ein Primideal $\mathfrak{P} \mid \mathfrak{p}$ heißt *unverzweigt* über $\mathfrak{p}$, wenn $e_{\mathfrak{P}|\mathfrak{p}} = 1$ gilt und die Erweiterung

$$\mathbb{F}_{\mathfrak{p}} \;=\; R/\mathfrak{p} \;\hookrightarrow\; \mathbb{F}_{\mathfrak{P}} \;=\; S/\mathfrak{P}$$

der Restklassenkörper separabel ist. Ist dies für alle Primideale $\mathfrak{P} \mid \mathfrak{p}$ der Fall, so heißt $\mathfrak{p}$ *unverzweigt* in K/k, andernfalls *verzweigt*.

(3) Man nennt $f_{\mathfrak{P}|\mathfrak{p}} = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}] \in \mathbb{N}$ den *Restklassengrad* von $\mathfrak{P} \mid \mathfrak{p}$.

(4) Ein Primideal $\mathfrak{p} \trianglelefteq R$ heißt in K/k

- *voll zerlegt*, wenn $e_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{p}} = 1$ für alle $\mathfrak{P} \mid \mathfrak{p}$ gilt,
- *unzerlegt*, wenn es nur ein einziges Primideal $\mathfrak{P} \mid \mathfrak{p}$ gibt,
- *voll verzweigt*, wenn es unzerlegt mit $f_{\mathfrak{P}|\mathfrak{p}} = 1$ ist,
- *träge*, wenn es unzerlegt mit $e_{\mathfrak{P}|\mathfrak{p}} = 1$, d.h. $\mathfrak{P} = \mathfrak{p}S$ prim ist.

Im Fall $R = \mathbb{Z}$ sagen wir auch, eine Primzahl $p \in \mathbb{N}$ sei in einem Zahlkörper $K/\mathbb{Q}$ unverzweigt, verzweigt, voll verzweigt, ..., wenn das von dieser Primzahl erzeugte Hauptideal $(p) \trianglelefteq \mathbb{Z}$ die entsprechende Eigenschaft besitzt.

BEISPIEL 1.6. In Hauptidealringen sind die von Null verschiedenen Primideale genau die von irreduziblen Elementen erzeugten Hauptideale. Unsere Beschreibung irreduzibler Elemente in $\mathfrak{o}_K = \mathbb{Z}[i]$ für den quadratischen Zahlkörper $K = \mathbb{Q}(i)$ zeigt dann:

(1) Jede Primzahl $p \equiv 3 \mod 4$ ist träge in K.

(2) Jede Primzahl $p \equiv 1 \mod 4$ ist voll zerlegt in K.

(3) Es ist $p = 2$ die einzige in K verzweigte Primzahl (und voll verzweigt).

Denn im ersten Fall ist p irreduzibel in $\mathfrak{o}_K$. Im zweiten und dritten Fall ist $p = a^2+b^2$ mit $a, b \in \mathbb{Z}$, also

$$p \cdot \mathfrak{o}_K \;=\; \mathfrak{p}_+\mathfrak{p}_- \quad \text{für die Primideale} \quad \mathfrak{p}_\pm \;=\; (a \pm ib) \;\trianglelefteq\; \mathfrak{o}_K,$$

und für $p \neq 2$ sind diese beiden Primideale verschieden voneinander.

BEISPIEL 1.7. Im quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{-5})$ zeigen elementare Rechnungen mit Idealen:

(1) Die Primzahl $p = 2$ ist voll verzweigt, $(2) = \mathfrak{p}^2$ für $\mathfrak{p} = (2, 1 + \sqrt{-5})$.

(2) Die Primzahl $p = 3$ ist voll zerlegt, $(3) = \mathfrak{p}_+\mathfrak{p}_-$ für $\mathfrak{p}_\pm = (3, 1 \pm \sqrt{-5})$.

(3) Die Primzahl $p = 5$ ist voll verzweigt, $(5) = \mathfrak{p}^2$ für $\mathfrak{p} = (\sqrt{-5})$.

(4) Die Primzahl $p = 7$ ist voll zerlegt, $(7) = \mathfrak{p}_+\mathfrak{p}_-$ für $\mathfrak{p}_\pm = (7, 1 \pm \sqrt{-5})$.

(5) Die Primzahl $p = 11$ ist träge, denn der Ring $\mathfrak{o}_K/(11) \simeq \mathbb{F}_{11}[x]/(x^2 + 5)$ besitzt keine Nullteiler.

Die Verbindung zu quadratischen Resten werden wir in Lemma 2.4 diskutieren.

In den obigen Beispielen ist p entweder voll zerlegt als Produkt zweier Primideale oder unzerlegt mit Verzweigungsindex und Restklassengrad $(e, f) \in \{(2,1),(1,2)\}$, also haben die Fasern der Abbildung

$$\mathrm{Spm}(S) \longrightarrow \mathrm{Spm}(R)$$

konstante Kardinalität, wenn man die Punkte mit den Vielfachheiten $e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}}$ zählt. Dies ist ein allgemeines Phänomen:

PROPOSITION 1.8. *Sei $n = [K : k]$. Dann gilt für alle Primideale $(0) \neq \mathfrak{p} \trianglelefteq R$ die Formel*

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}} = n,$$

wobei die Summation sich über alle Primideale $\mathfrak{P} \trianglelefteq S$ mit $\mathfrak{P} \mid \mathfrak{p}$ erstreckt.

Beweis. Der Einfachheit halber schreiben wir im Folgenden kurz $\mathfrak{p}S = \prod_i \mathfrak{P}_i^{e_i}$ mit $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$ und setzen $f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$. Der Chinesische Restsatz liefert uns dann einen Isomorphismus

$$\bigoplus_i S/\mathfrak{P}_i^{e_i} \simeq S/\mathfrak{p}S$$

von Vektorräumen über dem Restklassenkörper $\mathbb{F}_\mathfrak{p} = R/\mathfrak{p}$. Die Dimension dieser Vektorräume erhält man wie folgt:

(1) Um die Summanden auf der linken Seite zu kontrollieren, betrachten wir die Kompositionsreihen

$$\mathfrak{P}_i^{e_i} \subset \mathfrak{P}_i^{e_i-1} \subset \cdots \subset \mathfrak{P}_i \subset S.$$

Wie bei der Multiplikativität der Idealnorm in Lemma III.2.5 zeigt man, dass die sukzessiven Quotienten

$$\mathfrak{P}_i^{\nu-1}/\mathfrak{P}_i^{\nu} \simeq S/\mathfrak{P}_i$$

sind. Somit folgt

$$\dim_{\mathbb{F}_\mathfrak{p}} S/\mathfrak{P}_i^{e_i} = \sum_{\nu=1}^{e_i} \dim_{\mathbb{F}_\mathfrak{p}} \mathfrak{P}_i^{\nu-1}/\mathfrak{P}_i^{\nu} = e_i \cdot \dim_{\mathbb{F}_\mathfrak{p}} S/\mathfrak{P}_i = e_i \cdot f_i.$$

(2) Für den Beweis der behaupteten Formel genügt es nun zu zeigen, dass für die rechte Seite

$$\dim_{\mathbb{F}_\mathfrak{p}} S/\mathfrak{p}S = n$$

gilt. Hierzu erinnern wir uns zunächst daran, dass der Ring S als R-Modul endlich erzeugt ist. Also ist $m := \dim_{\mathbb{F}_\mathfrak{p}} S/\mathfrak{p}S < \infty$ und wir können Elemente $s_1, \ldots, s_m \in S$ finden, deren Restklassen

$$\overline{s}_1, \ldots, \overline{s}_m \in S/\mathfrak{p}S$$

eine $\mathbb{F}_\mathfrak{p}$-Basis von $S/\mathfrak{p}S$ bilden. Wir behaupten, dass $s_1, \ldots, s_m$ eine k-Basis von K bilden; dann ist insbesondere $m = n$ und wir sind fertig.

Hierzu zeigen wir zunächst, dass $s_1, \ldots, s_m$ linear unabhängig über k sind. Wäre dies nicht der Fall, so hätte man

$$r_1 s_1 + \cdots + r_m s_m = 0$$

für gewisse $r_i \in k$, nicht alle Null. Nach Multiplikation mit einem gemeinsamen Nenner können wir dabei $r_i \in R$ für alle i annehmen. Wir wählen nun ein $\alpha \in k$ mit der Eigenschaft

$$\alpha \cdot r_i \in R \text{ für alle } i, \text{ aber } \alpha \cdot r_i \notin \mathfrak{p} \text{ für mindestens ein } i.$$

Ein solches α existiert immer: Denn setzt man $\mathfrak{a} := (r_1, \ldots, r_m) \trianglelefteq R$, dann hat jedes $\alpha \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$ die gewünschten Eigenschaften. Durch Multiplikation der

ursprünglichen Relation mit einem solchen α und Reduktion modulo $\mathfrak{p}$ erhält man eine nichttriviale Relation

$$\overline{\alpha \cdot r_1} \cdot \overline{s}_1 + \cdots + \overline{\alpha \cdot r_m} \cdot \overline{s}_m \;=\; 0$$

im Widerspruch dazu, dass die $\overline{s}_i$ linear unabhängig über $\mathbb{F}_\mathfrak{p}$ sind.

Zu zeigen bleibt daher nur, dass $s_1, \ldots, s_m$ den k-Vektorraum K erzeugen. Hierzu betrachten wir den R-Untermodul

$$S_0 \;:=\; Rs_1 + \cdots + Rs_n \;\subseteq\; S.$$

Es gilt $S_0 + \mathfrak{p} \cdot S = S$, weil der Quotient $S/\mathfrak{p}S$ von den Basiselementen $\overline{s}_i$ erzeugt wird. Also ist

$$Q \;=\; \mathfrak{p} \cdot Q \quad \text{für den endlich erzeugten } R\text{-Modul} \quad Q \;:=\; S/S_0.$$

Nach Wahl von Erzeugern $q_1, \ldots, q_N$ für Q können wir also Elemente $a_{ij} \in \mathfrak{p}$ finden mit

$$q_i \;=\; \sum_{j=1}^{N} a_{ij} q_j \quad \text{für alle} \quad i.$$

Die a_{ij} müssen nicht eindeutig sein, aber wie im Beweis von Proposition II.1.3 liefert Multiplikation mit der komplementären Matrix $A^* = ((-1)^{i+j} \det(A_{ji}))$ zur Matrix $A = (\delta_{ij} - a_{ij})$, dass

$$d \cdot Q \;=\; \{0\} \quad \text{für} \quad d \;:=\; \det(A) \;\in\; R$$

ist. Also gilt

$$d \cdot S \;\subseteq\; S_0$$

und es folgt $k \cdot S_0 = K$, weil $d \neq 0$ wegen $d \equiv 1 \mod \mathfrak{p}$ ist. □

2. Eine explizite Formel von Dedekind

Der obige Beweis liefert zugleich eine effektive Methode, um die $e_{\mathfrak{P}|\mathfrak{p}}$ und $f_{\mathfrak{P}|\mathfrak{p}}$ zu berechnen. Hierzu schreiben wir unsere endliche separable Körpererweiterung in der Form $K = k(\alpha)$ mit $0 \neq \alpha \in K$, was nach dem Satz vom primitiven Element immer möglich ist. Nach Multiplikation mit einem Nenner dürfen wir $\alpha \in S$ annehmen und bezeichnen mit

$$p_\alpha(x) \;\in\; R[x]$$

das Minimalpolynom von α über k. Im Allgemeinen ist $R[\alpha] \subseteq S$ ein echter Teilring und somit nicht stabil unter der Multiplikation mit Elementen von S. Wir führen daher das Ideal

$$\mathfrak{b}_\alpha \;:=\; \left\{\, r \in R \;\mid\; r \cdot S \subseteq R[\alpha] \,\right\} \;\trianglelefteq\; R$$

ein. Dieses Ideal ist von Null verschieden, wie das folgende Lemma mit $\beta_i = \alpha^{i-1}$ zeigt:

LEMMA 2.1. *Für jede k-Basis $\beta_1, \ldots, \beta_n \in S$ von K existiert ein $r \in R \setminus \{0\}$ mit der Eigenschaft*

$$r \cdot S \;\subseteq\; R\beta_1 + \cdots + R\beta_n.$$

Beweis. Wir wissen aus dem Beweis von Proposition II.4.3, dass S ein endlich erzeugter R-Modul ist. Also ist $S = Rs_1 + \cdots + Rs_m$ für geeignete Erzeuger $s_i \in S$ und wir müssen $r \in R \setminus \{0\}$ finden mit

$$rs_i \;\in\; R\beta_1 + \cdots + R\beta_n$$

für alle i. Dazu schreiben wir $s_i = \sum_{j=1}^{n} c_{ij}\beta_j$ mit $c_{ij} \in k$. Wegen $k = Quot(R)$ gibt es ein $r \in R \setminus \{0\}$ mit $rc_{ij} \in R$ für alle i, j und wir sind fertig. □

Insbesondere ist das Ideal $\mathfrak{b}_\alpha \trianglelefteq R$ ein Produkt von Primidealen. Es hat um so weniger Teiler, je größer der von dem primitiven Element erzeugte Teilring $R[\alpha] \subseteq S$ ist, im Extremfall

$$S \;=\; R[\alpha] \quad\Longleftrightarrow\quad \mathfrak{b}_\alpha \;=\; (1).$$

Der folgende Satz bestimmt das Zerlegungsverhalten für alle Primideale bis auf die endlich vielen Teiler des obigen Ideals:

SATZ 2.2. *Sei $K = k(\alpha)$ für ein primitives Element $\alpha \in S$. Es sei $\mathfrak{p} \in \mathrm{Spm}(R)$ kein Teiler von $\mathfrak{b}_\alpha$, und die Reduktion* $\bmod \mathfrak{p}$ *des Minimalpolynoms von α zerlege sich als*

$$\overline{p}_\alpha(x) \;=\; \overline{q}_1(x)^{e_1} \cdots \overline{q}_g(x)^{e_g} \;\in\; \mathbb{F}_\mathfrak{p}[x]$$

mit paarweise verschiedenen irreduziblen und normierten Polynomen $\overline{q}_i(x) \in \mathbb{F}_\mathfrak{p}[x]$ und $e_i \in \mathbb{N}$. Dann gibt es paarweise verschiedene maximale Ideale $\mathfrak{P}_i \in \mathrm{Spm}(S)$ mit

$$\mathfrak{p} \cdot S \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \quad \textit{und} \quad \begin{cases} e_{\mathfrak{P}_i|\mathfrak{p}} \;=\; e_i, \\ f_{\mathfrak{P}_i|\mathfrak{p}} \;=\; \deg(\overline{q}_i(x)). \end{cases}$$

Explizit ist $\mathfrak{P}_i = (\mathfrak{p}, q_i(\alpha))$ für jeden Lift $q_i(x) \in R[x]$ von $\overline{q}_i(x) \in \mathbb{F}_\mathfrak{p}[x]$.

Beweis. Nach Annahme sind die beiden Ideale $\mathfrak{p}S$ und $\mathfrak{b}_\alpha S$ teilerfremd. Somit erhalten wir $S = \mathfrak{b}_\alpha S + \mathfrak{p}S \subseteq R[\alpha] + \mathfrak{p}S$, und folglich ist der zusammengesetzte Ringhomomorphismus

$$\begin{array}{ccccc} R[\alpha] & \hookrightarrow & S & \twoheadrightarrow & S/\mathfrak{p}S \\ & \searrow & & \nearrow_{\varphi} & \end{array}$$

surjektiv. Dann ist aber auch der hiervon durch Reduktion modulo $\mathfrak{p}$ induzierte Homomorphismus

$$\mathbb{F}_\mathfrak{p}[x]/(\overline{p}_\alpha(x)) \;\simeq\; R[\alpha]/\mathfrak{p}R[\alpha] \xrightarrow{\;\overline{\varphi}\;} S/\mathfrak{p}S$$

surjektiv und damit sogar bijektiv, denn nach Proposition 1.8 haben die links und rechts stehenden Vektorräume über dem Körper $\mathbb{F}_\mathfrak{p}$ dieselbe Dimension.

Zum Vergleich beider Seiten wenden wir folgende allgemeine Beobachtung für Dedekind-Ringe A und Ideale $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \trianglelefteq A$ mit paarweise verschiedenen maximalen Idealen $\mathfrak{p}_i \in \mathrm{Spm}(A)$ an:

(1) Die maximalen Ideale des Quotienten $\overline{A} = A/\mathfrak{a}$ sind genau die Ideale der Form $\overline{\mathfrak{p}}_i = \mathfrak{p}_i/\mathfrak{a}$, und diese sind ebenfalls paarweise verschieden.
(2) Die Quotientenabbildung liefert einen Isomorphismus $A/\mathfrak{p}_i \simeq \overline{A}/\overline{\mathfrak{p}}_i$.
(3) Die $e_i \in \mathbb{N}$ sind eindeutig bestimmt dadurch, dass für beliebige $\overline{e}_i \in \mathbb{N}$ gilt:

$$\overline{\mathfrak{p}}_1^{\overline{e}_1} \cdots \overline{\mathfrak{p}}_g^{\overline{e}_g} \;=\; (0) \quad\Longleftrightarrow\quad \overline{e}_i \;\geq\; e_i \;\text{ für } i = 1, \ldots, g.$$

Der Beweis dieser Tatsachen beruht darauf, dass die Ideale von $\overline{A}$ bijektiv den $\mathfrak{a}$ enthaltenden Idealen von A entsprechen. Für (2) genügt die Surjektivität, da auf beiden Seiten Körper stehen, und (3) folgt aus der Beziehung zwischen Inklusion und Teilbarkeit für Ideale in Dedekind-Ringen. Als Konsequenz von (1),(2),(3) halten wir fest:

BEMERKUNG. Durch den Ring $\overline{A}$ sind die Zahl g der Faktoren, die Exponenten e_i bis auf die Reihenfolge, und die zu den jeweiligen maximalen Idealen gehörigen Restklassenkörper $A/\mathfrak{p}_i$ bis auf Isomorphismus eindeutig bestimmt.

Wir wollen dies auf die Quotientenringe $\overline{A}_i = A_i/\mathfrak{a}_i$ in folgenden beiden Fällen anwenden:

- einerseits für $A_1 = \mathbb{F}_\mathfrak{p}[x] \supseteq \mathfrak{a}_1 = (\overline{p}_\alpha(x)) = \prod_i (\overline{q}_i(x))^{e_i}$,
- andererseits für $A_2 = S \supseteq \mathfrak{a}_2 = \mathfrak{p}S = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$.

Da die Quotientenringe durch den Isomorphismus $\overline{\varphi} : \overline{A}_1 \xrightarrow{\sim} \overline{A}_2$ miteinander identifiziert werden, erhalten wir unter Benutzung der obigen Bemerkung, dass es genau g verschiedene Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_g \mid \mathfrak{p}$ gibt und dass bei geeigneter Numerierung

$$e_{\mathfrak{P}_i|\mathfrak{p}} \;=\; e_i \quad \text{und} \quad S/\mathfrak{P}_i \;\simeq\; \mathbb{F}_\mathfrak{p}[x]/(\overline{q}_i(x))$$

für alle i gilt. Dieser letzte Körperisomorphismus ist per Konstruktion kompatibel mit der Struktur von $\mathbb{F}_\mathfrak{p}$-Algebren, sodass auch $f_{\mathfrak{P}|\mathfrak{p}} = \deg(\overline{q}_i(x))$ folgt. Es bleibt die Formel

$$\mathfrak{P}_i \;=\; (\mathfrak{p}, q_i(x))$$

zu zeigen. Hierzu beachte man, dass das auf der rechten Seite stehenden Ideal das Ideal $\mathfrak{p}S$ enthält und somit das volle Urbild eines Ideals von $\overline{S} = S/\mathfrak{p}S$ ist. Das letztere Ideal ist aber gleich $\overline{\mathfrak{P}}_i = \mathfrak{P}_i/\mathfrak{p}S$, weil die Restklasse von x unter dem Isomorphismus

$$\mathbb{F}_\mathfrak{p}[x]/(\overline{p}_\alpha(x)) \;\simeq\; S/\mathfrak{p}S$$

derjenigen von α entspricht. Damit folgt die behauptete Formel. □

Der für uns interessanteste Spezialfall betrifft die Zerlegung von Primzahlen in Zahlkörpern:

KOROLLAR 2.3. *Sei $K = \mathbb{Q}(\alpha)$ für eine ganze algebraische Zahl $\alpha \in \mathbb{C}$ und p eine Primzahl mit*

$$p \nmid [\mathfrak{o}_K : \Lambda] \quad \textit{für} \quad \Lambda = \mathbb{Z}[\alpha].$$

Das Minimalpolynom von α zerlege sich modulo p als $f_\alpha(x) \equiv \prod_{i=1}^g q_i(x)^{e_i} \bmod p$ mit $q_i(x) \in \mathbb{Z}[x]$, wobei die $\overline{q}_i(x) \in \mathbb{F}_p[x]$ paarweise verschieden, normiert und irreduzibel seien. Dann ist

$$p \cdot \mathfrak{o}_K \;=\; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \quad \textit{mit} \quad \mathfrak{p}_i \;=\; (p, q_i(\alpha)) \quad \textit{und} \quad \begin{cases} e_{\mathfrak{p}_i|\mathfrak{p}} \;=\; e_i, \\ f_{\mathfrak{p}_i|\mathfrak{p}} \;=\; \deg(\overline{q}_i(x)). \end{cases}$$

Beweis. Offenbar gilt hier $\mathfrak{b}_\alpha = \{m \in \mathbb{Z} \mid m\mathfrak{o}_K \subseteq \Lambda\} \ni N = [\mathfrak{o}_K : \Lambda]$. Für $p \nmid N$ ist also $(p) \nmid \mathfrak{b}_\alpha$ und somit folgt die Behauptung. □

Wir können nun auch die Beziehung zu quadratischen Resten in Beispiel 1.7 allgemeiner verstehen. Hierzu führen wir für $d \in \mathbb{Z}$ und für Primzahlen p das Legendre-Symbol

$$\left(\frac{d}{p}\right) \;=\; \begin{cases} +1 & \text{falls } d \equiv x^2 \not\equiv 0 \bmod p \text{ mit } x \in \mathbb{Z} \text{ ist}, \\ 0 & \text{falls } d \equiv 0 \bmod p \text{ ist}, \\ -1 & \text{sonst}, \end{cases}$$

ein und erhalten folgendes

LEMMA 2.4. *Sei $K = \mathbb{Q}(\sqrt{d})$ für eine quadratfreie ganze Zahl $d \in \mathbb{Z}$. Dann ist eine ungerade Primzahl*

$$p \;\neq\; 2 \quad \textit{in } K \quad \begin{cases} \textit{voll zerlegt} \\ \textit{verzweigt} \\ \textit{träge} \end{cases} \quad \textit{genau für} \quad \left(\frac{d}{p}\right) \;=\; \begin{cases} +1, \\ 0, \\ -1. \end{cases}$$

Andererseits ist

$$p = 2 \quad \textit{in } K \quad \begin{cases} \textit{voll zerlegt} \\ \textit{verzweigt} \\ \textit{träge} \end{cases} \quad \textit{genau für} \quad d \equiv \begin{cases} 1 \mod 8, \\ 2,3 \mod 4, \\ 5 \mod 8. \end{cases}$$

Beweis. Für $\alpha = \sqrt{d}$ und $\Lambda = \mathbb{Z}[\alpha]$ ist der Index $[\mathfrak{o}_K : \Lambda] \in \{1, 2\}$, somit ist das obige Korollar auf alle ungeraden Primzahlen p anwendbar und liefert die Behauptung mit $f_\alpha(x) = x^2 - d$. Für $d \equiv 2, 3 \bmod 4$ wissen wir sogar $\mathfrak{o}_K = \Lambda$, also zeigt in diesem Fall dasselbe Argument, dass die Primzahl $p = 2$ voll verzweigt ist wegen $x^2 - 2 \equiv x^2$ und $x^2 - 3 \equiv (x-1)^2 \bmod 2$.

Es bleibt nur der Fall $p = 2$ und $d \equiv 1 \bmod 4$. Hier ist $\mathfrak{o}_K = \mathbb{Z}[\beta]$ für $\beta = \frac{1+\sqrt{d}}{2}$ mit Minimalpolynom

$$f_\beta(x) = x^2 - x + \tfrac{1-d}{4} \in \mathbb{Z}[x].$$

Dieses Polynom hat zwei verschiedene oder gar keine Nullstellen modulo $p = 2$, je nachdem ob $d \equiv 1 \bmod 8$ oder $d \equiv 5 \bmod 8$ ist, das Korollar liefert also auch hier die Behauptung. □

Bemerkung 2.5. Sowohl der voll zerlegte als auch der träge Fall treten bei festem d jeweils für unendlich viele Primzahlen p auf; eine genauere Aussage werden wir später mit dem quadratischen Reziprozitätsgesetz beweisen. Verzweigt sind andererseits nur die endlich vielen Teiler der Diskriminante d_K. Wir werden später sehen, dass dies für beliebige Zahlkörper richtig bleibt.

Bemerkung 2.6. Der Ring $\mathfrak{o}_K$ muß für die Anwendung von Korollar 2.3 nicht unbedingt explizit bekannt sein: Beispielsweise kann man das Korollar direkt auf alle Primzahlen

$$p \nmid d_{K/\mathbb{Q}}(\alpha) = [\mathfrak{o}_K : \mathbb{Z}[\alpha]]^2 \cdot d_K$$

anwenden. Dazu müssen *nicht* die einzelnen Faktoren auf der rechten Seite berechnet werden, die Formel

$$d_{K/\mathbb{Q}}(\alpha) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

aus Lemma II.2.9 genügt! Für Primzahlen $p \mid d_K$ lässt sich dieser Trick zwar nie anwenden, da hier stets $p \mid d_{K/k}(\alpha)$ ist; in günstigen Fällen kann man aber mit etwas mehr Arbeit trotzdem ein primitives Element $\beta \in \mathfrak{o}_K$ finden mit $p \nmid [\mathfrak{o}_K : \mathbb{Z}[\beta]]$, Beispiele hierfür haben wir in den Übungen gesehen.

Beispiel 2.7. Sei $K = \mathbb{Q}(\alpha)$ mit $\alpha^3 = 10$. Die Einbettungen $\sigma_\nu : K \hookrightarrow \mathbb{C}$ sind gegeben durch

$$\sigma_\nu(\alpha) = \zeta^\nu \cdot \sqrt[3]{10} \quad \text{für } \nu = 1, 2, 3, \quad \text{mit} \quad \zeta = e^{2\pi i/3} \quad \text{und} \quad \sqrt[3]{10} \in \mathbb{R}.$$

Somit folgt

$$\begin{aligned} d_{K/\mathbb{Q}}(\alpha) &= \sqrt[3]{10}^6 \cdot \prod_{\nu<\mu} (\zeta^\nu - \zeta^\mu)^2 = 10^2 \cdot (1-\zeta)^2 \cdot (1-\zeta^2)^2 \cdot (\zeta - \zeta^2)^2 \\ &= 10^2 \cdot \underbrace{(1 - 2\zeta + \zeta^2)}_{-3\zeta} \cdot \underbrace{(1 - 2\zeta^2 + \zeta^4)}_{-3\zeta^2} \cdot \underbrace{(\zeta^2 - 2\zeta^3 + \zeta^4)}_{-3} = -10^2 \cdot 3^3 \end{aligned}$$

wegen $1 + \zeta + \zeta^2 = 0$, somit ist der Index $N = [\mathfrak{o}_K : \mathbb{Z}[\alpha]]$ ein Teiler von 30. Da das Minimalpolynom

$$f_\alpha(x) = x^3 - 10$$

ein Eisenstein-Polynom bezüglich der beiden Primzahlen $p \in \{2,5\}$ ist, wissen wir andererseits aus den Übungsaufgaben, dass der Index durch keine dieser beiden Primzahlen teilbar ist. Also gilt $N \in \{1,3\}$, und Korollar 2.3 ist auf alle $p \neq 3$ anwendbar:

$$\begin{aligned}(2) &= \mathfrak{P}_1^3 \quad \text{mit} \quad \mathfrak{P}_1 = (2,\alpha) \trianglelefteq \mathfrak{o}_K,\\ (5) &= \mathfrak{P}_2^3 \quad \text{mit} \quad \mathfrak{P}_2 = (5,\alpha) \trianglelefteq \mathfrak{o}_K,\\ (7) &= \mathfrak{P}_3 \quad \text{bleibt ein Primideal in } \mathfrak{o}_K,\\ &\vdots\end{aligned}$$

Für die Primzahl $p = 3$ würde Anwenden des Korollars auf α ebenfalls totale Verzweigung voraussagen, dies ist aber *nicht* richtig. Tatsächlich ist hier $N = 3$, und die korrekte Zerlegung von $p = 3$ erhält man durch Anwenden des Korollars auf

$$\beta = \frac{1+\alpha+\alpha^2}{3} \in \mathfrak{o}_K \quad \text{mit Minimalpolynom} \quad f_\beta(x) = x^3 - x^2 - 3x - 3.$$

Es ist

$$(3) = \mathfrak{P}^2 \cdot \mathfrak{Q} \quad \text{mit} \quad \mathfrak{P} = (3,\beta),\ \mathfrak{Q} = (3,\beta-1) \trianglelefteq \mathfrak{o}_K = \mathbb{Z}[\beta].$$

Es ist eine instruktive Übungsaufgabe, diese Zerlegung von Hand nachzuprüfen; wer hätte sie ohne das Korollar 2.3 erraten?

Warnung. Die obige Methode führt oft, aber nicht immer zum Ziel. Es gibt beispielsweise Zahlkörper $K/\mathbb{Q}$ mit der Eigenschaft, dass der Index $[\mathfrak{o}_K : \mathbb{Z}[\beta]]$ gerade ist für alle $\beta \in \mathfrak{o}_K$!

3. Galoiserweiterungen: Zerlegungsgruppen

In diesem Abschnitt setzen wir stets voraus, dass die Körpererweiterung K/k eine Galoiserweiterung ist. Dann hat die Zerlegung von Primidealen eine besondere Symmetrie, da für festes $\mathfrak{p} \in \operatorname{Spm}(R)$ alle Primideale $\mathfrak{P} \mid \mathfrak{p}$ konjugiert unter der Operation der Galoisgruppe sind:

Proposition 3.1. *Sei K/k eine Galoiserweiterung und $\mathfrak{p} \in \operatorname{Spm}(R)$. Dann operiert die Galoisgruppe $G = Gal(K/k)$ transitiv auf der Menge der sämtlichen Primideale*

$$\mathfrak{P}_1, \dots, \mathfrak{P}_g \trianglelefteq S \quad \textit{mit} \quad \mathfrak{P}_i \mid \mathfrak{p}.$$

Beweis. Die Galoisgruppe G operiert trivial auf dem Teilkörper $k \subseteq K$, also insbesondere auf R, und erhält daher dessen ganzen Abschluß:

$$G \curvearrowright S = \{\, s \in K \mid s \text{ ist ganz über } R \,\}$$

Für $\mathfrak{P} \in \operatorname{Spm}(S)$ ist

$$\sigma\mathfrak{P} = \{\, \sigma(\alpha) \mid \alpha \in \mathfrak{P} \,\} \in \operatorname{Spm}(S)$$

ebenfalls ein maximales Ideal, und dabei gilt offenbar $\mathfrak{P} \cap R = \sigma\mathfrak{P} \cap R$, sodass wir eine Operation der Galoisgruppe auf der Menge aller Primideale über dem festen Primideal $\mathfrak{p} \in \operatorname{Spm}(R)$ erhalten.

Angenommen, die Operation wäre nicht transitiv, es wäre etwa $\sigma\mathfrak{P}_1 \neq \mathfrak{P}_2$ für alle $\sigma \in G$. Nach dem Chinesischen Restsatz können wir dann ein Element $\alpha \in S$ finden mit

$$\alpha \equiv 0 \mod \mathfrak{P}_2, \quad \alpha \equiv 1 \mod \sigma\mathfrak{P}_1 \quad \text{für alle} \quad \sigma \in G.$$

Die erste Bedingung liefert

$$N_{K/k}(\alpha) \;=\; \prod_{\sigma\in G}\sigma(\alpha) \;=\; \alpha\cdot\prod_{\sigma\neq id}\sigma(\alpha) \;\in\; \mathfrak{P}_2\cap R \;=\; \mathfrak{p},$$

die zweite Bedingung aber $\sigma(\alpha)\notin\mathfrak{P}_1$ für alle $\sigma\in G$ und somit wegen der Primalität von $\mathfrak{P}_1$ auch

$$N_{K/k}(\alpha) \;=\; \prod_{\sigma\in G}\sigma(\alpha) \;\notin\; \mathfrak{P}_1.$$

Wegen $\mathfrak{p}=\mathfrak{P}_1\cap R$ liefert dies einen Widerspruch. □

KOROLLAR 3.2. *In obiger Situation hängen die Zahlen $e=e_{\mathfrak{P}_i|\mathfrak{p}}$ und $f=f_{\mathfrak{P}_i|\mathfrak{p}}$ nicht von i ab. Insbesondere ist $[K:k] \;=\; efg$.*

Beweis. Für $\sigma\in G$ erhält man aus der Eindeutigkeit der Primfaktorisierung von Idealen wegen

$$\prod_{\mathfrak{P}|\mathfrak{p}}(\sigma\mathfrak{P})^{\,e_{\sigma\mathfrak{P}|\mathfrak{p}}} \;=\; \prod_{\mathfrak{P}|\mathfrak{p}}\mathfrak{P}^{\,e_{\mathfrak{P}|\mathfrak{p}}} \;=\; \mathfrak{p}S \;=\; \sigma(\mathfrak{p}S) \;=\; \prod_{\mathfrak{P}|\mathfrak{p}}(\sigma\mathfrak{P})^{\,e_{\mathfrak{P}|\mathfrak{p}}}$$

sofort $e_{\sigma\mathfrak{P}|\mathfrak{p}}=e_{\mathfrak{P}|\mathfrak{p}}$. Für die entsprechenden Restklassenkörper induziert σ einen Isomorphismus

$$\sigma: \quad \mathbb{F}_{\mathfrak{P}} \;=\; S/\mathfrak{P} \;\xrightarrow{\sim}\; \mathbb{F}_{\sigma\mathfrak{P}} \;=\; S/\sigma\mathfrak{P}$$

von $\mathbb{F}_{\mathfrak{p}}$-Algebren, somit folgt für die Restklassengrade ebenfalls $f_{\sigma\mathfrak{P}|\mathfrak{p}}=f_{\mathfrak{P}|\mathfrak{p}}$. Die Behauptung folgt nun aus der Transitivität der Galoisoperation. □

DEFINITION 3.3. Wir fixieren im Folgenden ein Primideal $\mathfrak{P}\mid\mathfrak{p}$ von S und bezeichnen

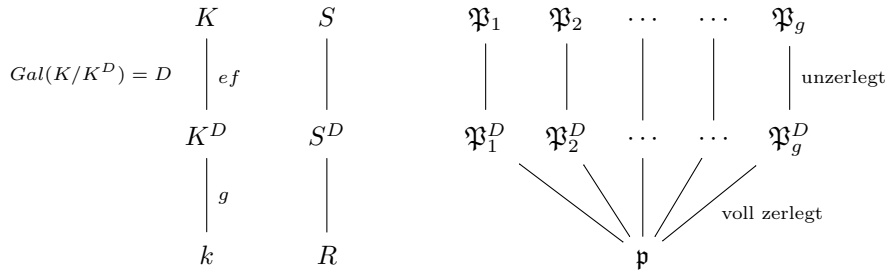
$$D \;:=\; G_{\mathfrak{P}} \;:=\; \big\{\,\sigma\in G\mid\sigma\mathfrak{P}=\mathfrak{P}\,\big\} \;\subseteq\; G \;=\; Gal(K/k)$$

als die *Zerlegungsgruppe* des gewählten Primideals. Bis auf Konjugation hängt diese nicht von der getroffenen Wahl ab, denn $G_{\sigma\mathfrak{P}}=\sigma G_{\mathfrak{P}}\sigma^{-1}$ für $\sigma\in G$. Wir nennen den Fixkörper

$$K^D \;=\; \big\{\,\alpha\in K\mid\sigma(\alpha)=\alpha \text{ für alle } \sigma\in D\,\big\} \;\subseteq\; K$$

auch den *Zerlegungskörper* des Primideals.

Wir haben also einen Turm von Erweiterungen, wobei der Fixring $S^D=S\cap K^D$ der ganze Abschluß von R in K^D und daher auch ein Dedekind-Ring ist. Wir behaupten nun, dass dies die Galoiserweiterung in einen voll zerlegten und einen unzerlegten Teil aufspaltet:



Genauer gilt:

SATZ 3.4. *Mit den obigen Notationen ist*

(1) $\mathfrak{Q}=\mathfrak{P}\cap K^D$ *unzerlegt in* K/K^D *mit* $e_{\mathfrak{P}|\mathfrak{Q}}=e$ *und* $f_{\mathfrak{P}|\mathfrak{Q}}=f$,

(2) $\mathfrak{p}$ *voll zerlegt in der Erweiterung* K^D/k *mit* $e_{\mathfrak{Q}|\mathfrak{p}}=f_{\mathfrak{Q}|\mathfrak{p}}=1$.

Beweis. Offenbar ist K/K^D eine Galoiserweiterung, und da $Gal(K/K^D) = D$ definitionsgemäß das gegebene Primideal $\mathfrak{P}$ stabilisiert, zeigt die Transitivität der Operation in Proposition 3.1, dass dieses das einzige Primideal über $\mathfrak{O}$ ist. Somit ist $\mathfrak{O}$ in der Körpererweiterung K/K^D unzerlegt, und dasselbe gilt dann auch für alle seine Galoiskonjugierten. Da nun das Primideal $\mathfrak{P}$ genau g verschiedene Galoiskonjugierte besitzt, hat $\mathfrak{O}$ ebensoviele Galoiskonjugierte. Es ist aber

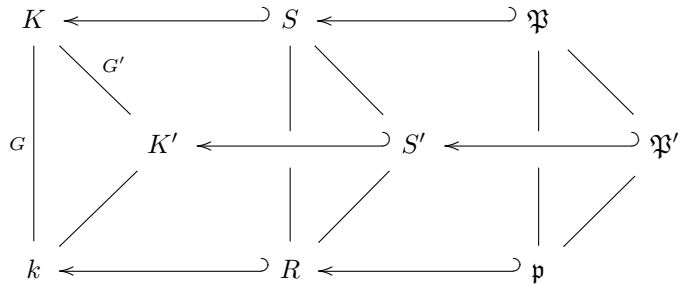
$$g \;=\; |G/D| \;=\; [K^D : k]$$

und somit folgt wie behauptet, dass das Primideal $\mathfrak{p}$ in der Erweiterung K^D/K voll zerlegt ist. Da Verzweigungsindices und Restklassengrade multiplikativ in Türmen von Erweiterungen sind (Übung), folgt $e_{\mathfrak{P}|\mathfrak{O}} = e_{\mathfrak{P}|\mathfrak{O}} \cdot 1 = e_{\mathfrak{P}|\mathfrak{O}} \cdot e_{\mathfrak{O}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}} = e$ und $f_{\mathfrak{P}|\mathfrak{O}} = f$ wie behauptet. □

Der obige Formalismus ist allgemeiner auch für endliche separable, aber nicht notwendig normale Körpererweiterungen anwendbar, indem man zur Galoishülle übergeht. Sei also K' ein Zwischenkörper der Galoiserweiterung K/k, wobei die Untergruppe

$$G' \;=\; Gal(K/K') \;=\; \left\{\, \sigma \in G : \sigma|_{K'} = id_{K'} \right\} \;\hookrightarrow\; G \;=\; Gal(K/k)$$

nicht normal sein muß. Wir haben die folgende Situation, wobei wir $S' = S \cap K'$ und $\mathfrak{P}' = \mathfrak{P} \cap K' = \mathfrak{P} \cap S'$ setzen:



Dabei ist S' als ganzer Abschluß von R in K' wieder ein Dedekind-Ring. Für die Zerlegungsgruppen gilt

$$D' \;=\; \left\{\, \sigma \in G' \mid \sigma\mathfrak{P} = \mathfrak{P} \,\right\} \;=\; G' \cap D \;\subset\; D \;=\; \left\{\, \sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P} \right\}$$

und wir erhalten das folgende Resultat.

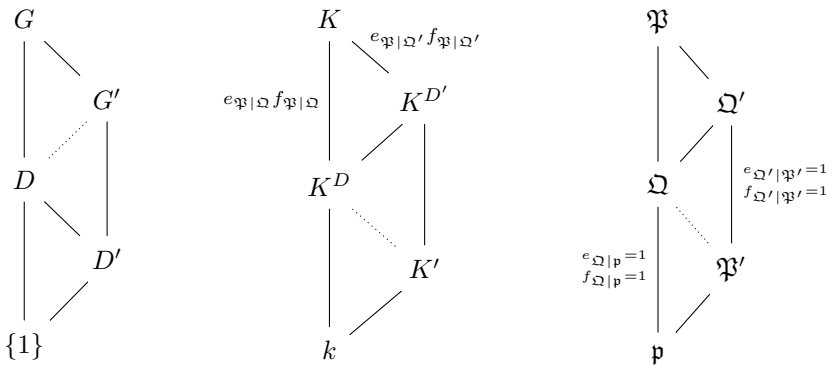
Satz 3.5. *In obiger Situation sind äquivalent:*

(1) $D \subseteq G'$
(2) $K' \subseteq K^D$
(3) $e_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{p}} = 1$

Beweis. Die Äquivalenz der ersten beiden Eigenschaften ist klar, weil K' nach Galoistheorie der Fixkörper von G' ist: Denn (1) ist die gepunktete Inklusion im folgenden Diagramm von Galois- und Zerlegungsgruppen, und (2) ist die gepunktete Inklusion im Diagramm der Fixkörper. Wir fügen diesen Diagrammen noch eines der Primideale unter $\mathfrak{P}$ hinzu, wobei wir

$$\mathfrak{O} \;=\; \mathfrak{P} \cap K^D \quad \text{und} \quad \mathfrak{O}' \;=\; \mathfrak{P} \cap K^{D'}$$

setzen:



Durch Anwenden von Satz 3.4 für die Verzweigungsindices und Restklassengrade der Zerlegungskörper in den Galoiserweiterungen K/k und K/K' erhält man die Identitäten

$$e_{\mathfrak{O}|\mathfrak{p}} \;=\; f_{\mathfrak{O}|\mathfrak{p}} \;=\; 1 \quad \text{und} \quad e_{\mathfrak{O}'|\mathfrak{P}'} \;=\; f_{\mathfrak{O}'|\mathfrak{P}'} \;=\; 1.$$

Gilt (2), so erhalten wir aus den ersten beiden Gleichungen sowie der gepunkteten Inklusion und der Multiplikativität der Verzweigungsindices und Restklassengrade in Türmen

$$e_{\mathfrak{P}'|\mathfrak{p}} \;=\; \frac{e_{\mathfrak{O}|\mathfrak{p}}}{e_{\mathfrak{O}|\mathfrak{P}'}} \;=\; 1 \quad \text{und} \quad f_{\mathfrak{P}'|\mathfrak{p}} \;=\; \frac{f_{\mathfrak{O}|\mathfrak{p}}}{f_{\mathfrak{O}|\mathfrak{P}'}} \;=\; 1$$

und somit gilt (3). Ist umgekehrt letzteres der Fall, dann erhalten wir auf dieselbe Weise

$$e_{\mathfrak{O}'|\mathfrak{O}} \;=\; \frac{e_{\mathfrak{O}'|\mathfrak{p}}}{e_{\mathfrak{O}|\mathfrak{p}}} \;=\; \frac{e_{\mathfrak{O}'|\mathfrak{P}'} \cdot e_{\mathfrak{P}'|\mathfrak{p}}}{e_{\mathfrak{O}|\mathfrak{p}}} \;=\; 1 \quad \text{und analog} \quad f_{\mathfrak{O}'|\mathfrak{O}} \;=\; 1.$$

Dies liefert

$$\left[K^{D'} : K^D\right] \;=\; \frac{[K : K^D]}{[K : K^{D'}]} \;=\; \frac{e_{\mathfrak{P}|\mathfrak{O}} \cdot f_{\mathfrak{P}|\mathfrak{O}}}{e_{\mathfrak{P}|\mathfrak{O}'} \cdot f_{\mathfrak{P}|\mathfrak{O}'}} \;=\; e_{\mathfrak{O}'|\mathfrak{O}} \cdot f_{\mathfrak{O}'|\mathfrak{O}} \;=\; 1,$$

also

$$K^{D'} = K^D$$

und für den Fixkörper $K' = K^{G'}$ folgt die Inklusion (2). □

Dies liefert ein rein galoistheoretisches Kriterium für die volle Zerlegtheit eines Primideals in einem beliebigen Zwischenkörper K' der Erweiterung K/k, sobald die Zerlegungsgruppen

$$G_{\mathfrak{P}} \;=\; \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\} \;\subseteq\; G \;=\; Gal(K/k)$$

alle bekannt sind:

KOROLLAR 3.6. *Es ist $\mathfrak{p} \in \mathrm{Spm}(R)$ im Zwischenkörper K' von K/k voll zerlegt genau dann, wenn gilt:*

$$G_{\mathfrak{P}} \;\subseteq\; G' \;=\; Gal(K/K') \quad \textit{für alle} \quad \mathfrak{P} \mid \mathfrak{p}.$$

Beweis. Ein Primideal $\mathfrak{p} \in \mathrm{Spm}(R)$ ist definitionsgemäß in K' voll zerlegt genau dann, wenn $e_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{p}} = 1$ für alle Primideale $\mathfrak{P}' \mid \mathfrak{p}$ ist. Für ganze Erweiterungen ist die Abbildung

$$\left\{\mathfrak{P} \in \mathrm{Spm}(S) :\; \mathfrak{P} \mid \mathfrak{p}\right\} \;\longrightarrow\; \left\{\mathfrak{P}' \in \mathrm{Spm}(S') :\; \mathfrak{P}' \mid \mathfrak{p}\right\}, \quad \mathfrak{P} \;\mapsto\; \mathfrak{P}' \;=\; \mathfrak{P} \cap S'$$

surjektiv, und somit folgt die behauptete Äquivalenz aus Satz 3.5. □

4. Galoiserweiterungen: Trägheitsgruppen

Im vorigen Abschnitt haben wir ein Primideal $\mathfrak{P} \mid \mathfrak{p}$ fixiert und hiervon ausgehend die Galoiserweiterung K/k in einen voll zerlegten und einen unzerlegten Anteil aufgespalten. Wir wollen den letzteren nun weiter in einen voll verzweigten und einen unverzweigten Anteil zerlegen. Hierzu betrachten wir in $G = Gal(K/k)$ die Zerlegungsgruppe

$$D \;=\; G_{\mathfrak{P}} \;=\; \left\{\, \sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P} \,\right\} \;\simeq\; Gal(K/K^D).$$

Jedes Element dieser Zerlegungsgruppe erhält per Definition das Primideal $\mathfrak{P}$ und operiert somit auf dem Restklassenkörper $\mathbb{F}_{\mathfrak{P}} = S/\mathfrak{P}$. Diese Operation fixiert den Teilkörper $\mathbb{F}_{\mathfrak{p}} = R/\mathfrak{p}$, liefert also einen Homomorphismus $\varphi : D \to Aut(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, und das Pendant zur Transitivität im vorigen Abschnitt ist

Proposition 4.1. *Die Körpererweiterung $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ ist normal. Ist sie separabel, so ist obiger Homomorphismus surjektiv:*

$$\varphi : \quad D \;\twoheadrightarrow\; Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Beweis. Für die Normalität der Körpererweiterung müssen wir zeigen: Wenn ein irreduzibles Polynom $q(x) \in \mathbb{F}_{\mathfrak{p}}[x]$ im größeren Körper eine Nullstelle $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ besitzt, zerfällt es über dem größeren Körper komplett in Linearfaktoren. Hierzu liften wir die Nullstelle zu einem $\alpha \in S$ und bezeichnen mit $p_\alpha(x) \in R[x]$ sein Minimalpolyom. Da K/k eine Galoiserweiterung und somit insbesondere normal ist, zerfällt dieses Minimalpolynom $p_\alpha(x)$ wegen $p_\alpha(\alpha) = 0$ über dem Körper K komplett in Linearfaktoren. Da Galoiskonjugierte von ganzen Elementen ganz sind, zerfällt $p_\alpha(x)$ dann schon über S komplett in Linearfaktoren. Somit zerfällt die Reduktion

$$\overline{p}_\alpha(x) \;=\; \big(\, p_\alpha(x) \mod \mathfrak{p} \,\big) \in \mathbb{F}_{\mathfrak{p}}[x]$$

über $\mathbb{F}_{\mathfrak{P}}$ ebenfalls in Linearfaktoren. Andererseits ist aber wegen $\overline{p}_\alpha(\overline{\alpha}) = 0$ diese Reduktion teilbar durch das Minimalpolynom von $\overline{\alpha}$ über $\mathbb{F}_{\mathfrak{p}}$. Offenbar ist das letztere Minimalpolynom gerade $q(x) \in \mathbb{F}_{\mathfrak{p}}[x]$, also zerfällt auch dieses über $\mathbb{F}_{\mathfrak{P}}$ vollständig in Linearfaktoren. Damit ist die Erweiterung $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ normal.

Sei jetzt $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ außerdem separabel. Um die Surjektivität von $D \to Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ zu sehen, können wir die Erweiterung K/k durch K/K^D ersetzen, da dies die Zerlegungsgruppen und Restklassenkörper nicht ändert:

$$\begin{array}{ccc} K & & S \longrightarrow\!\!\!\!\!\rightarrow \mathbb{F}_{\mathfrak{P}} \\ {\scriptstyle D}\big| & & \big| \quad\quad \big| \\ K^D & & S^D \twoheadrightarrow \mathbb{F}_{\mathfrak{P}^D} \\ \big| & & \big| \quad\quad \big\| \\ k & & R \longrightarrow\!\!\!\!\!\rightarrow \mathbb{F}_{\mathfrak{p}} \end{array}$$

Wir können also annehmen, dass die Zerlegungsgruppe $D = G$ ist. Wegen der Separabilität können wir ein primitives Element $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ finden mit $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}(\overline{\alpha})$; wie oben sei $q(x) \in \mathbb{F}_{\mathfrak{p}}[x]$ das Minimalpolynom dieses primitiven Elementes, und wir wählen einen Lift $\alpha \in S$ mit Minimalpolynom $p_\alpha(x) \in S[x]$. Da $q(x)$ ein Teiler von $\overline{p}_\alpha(x)$ ist, gilt

$$\overline{p}_\alpha(\overline{\beta}) \;=\; 0 \quad \text{für jedes} \quad \overline{\beta} \;\in\; \mathbb{F}_{\mathfrak{P}} \quad \text{mit} \quad q(\overline{\beta}) \;=\; 0.$$

Daher lässt sich jede solche Nullstelle zu einem Ringelement $\beta \in S$ mit $p_\alpha(\beta) = 0$ liften. Da K/k eine Galoiserweiterung ist, existiert dann ein Automorphismus $\sigma \in G$

mit $\sigma(\alpha) = \beta$, und

$$\overline{\sigma}(\overline{\alpha}) \;=\; \overline{\beta} \quad \text{für das Bild} \quad \overline{\sigma} \;\in\; Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Da $\overline{\beta} \in \mathbb{F}_{\mathfrak{P}}$ ein beliebiges Galoiskonjugiertes der gegebenen Nullstelle $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ war, folgt die Surjektivität der Abbildung $G \to Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. □

Bemerkung 4.2. Die Erweiterung $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ ist automatisch separabel, wenn $\mathbb{F}_{\mathfrak{p}}$ ein sogenannter *perfekter Körper* ist, d.h. jedes irreduzible Polynom $f(x) \in \mathbb{F}_{\mathfrak{p}}[x]$ im algebraischen Abschluß $\overline{\mathbb{F}}_{\mathfrak{p}}$ nur einfache Nullstellen hat. Dies ist genau dann der Fall, wenn gilt:

(1) $char(\mathbb{F}_{\mathfrak{p}}) = 0$, oder

(2) $char(\mathbb{F}_{\mathfrak{p}}) = p > 0$, und die Abbildung $\Phi : \mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{p}}, \alpha \mapsto \alpha^p$ ist surjektiv.

Die für uns wichtigsten Beispiele sind

(1) Funktionenkörper K mit $char(K) = 0$, und

(2) Zahlkörper $K/\mathbb{Q}$, weil für letztere der Körper $\mathbb{F}_{\mathfrak{p}}$ endlich ist. Endliche Körper sind perfekt, da jeder Körperhomomorphismus Φ injektiv ist.

Im Folgenden setzen wir stets voraus, dass die Erweiterung $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ separabel ist.

Definition 4.3. Ist $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ in der Situation von Proposition 4.1 separabel, so bezeichnen wir

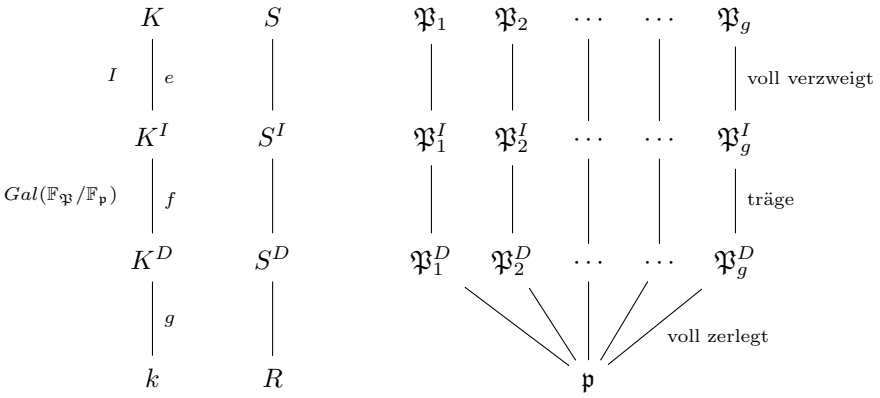
$$I \;:=\; I_{\mathfrak{P}} \;:=\; \ker\big(D \twoheadrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})\big)$$

als *Trägheitsgruppe* und den Fixkörper

$$K^I \;=\; \big\{\, \alpha \in K \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in I \,\big\}$$

als *Trägheitskörper* des gewählten Primideals $\mathfrak{P} \mid \mathfrak{p}$.

Auch hier ist der Fixring S^I wieder ein Dedekind-Ring. Wir können nun den unzerlegten Teil des Turmes von Erweiterungen aus Satz 3.4 weiter in einen trägen und einen voll verzweigten Anteil aufspalten und erhalten insgesamt das folgende Bild:



Genauer gilt:

Satz 4.4. *Mit den obigen Notationen ist*

(1) *K/K^I eine Galoiserweiterung mit $Gal(K/K^I) \simeq I$, und $\mathfrak{P}^I$ darin voll verzweigt mit*

$$e_{\mathfrak{P}|\mathfrak{P}^I} \;=\; e \quad \textit{und} \quad f_{\mathfrak{P}|\mathfrak{P}^I} \;=\; 1.$$

(2) K^I/K^D *Galoiserweiterung mit* $Gal(K^I/K^D) \simeq Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, *und* $\mathfrak{P}^D$ *darin träge mit*

$$e_{\mathfrak{P}^I|\mathfrak{P}^D} = 1 \quad \textit{und} \quad f_{\mathfrak{P}^I|\mathfrak{P}^D} = f.$$

Beweis. Offenbar ist K/K^D eine Galoiserweiterung mit $Gal(K/K^D) = D$. Diese Gruppe enthält I als normale Untergruppe, genauer haben wir nach Proposition 4.1 eine exakte Sequenz

$$1 \longrightarrow I \longrightarrow D \longrightarrow Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) \longrightarrow 1.$$

Somit ist auch K^I/K^D eine Galoiserweiterung und die Galoisgruppen haben die angegebene Form. Insbesondere ist

$$\big[K^I : K^D\big] = \big|Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})\big| = \big[\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}\big] = f$$

und somit

$$\big[K : K^I\big] = \frac{[K : K^D]}{[K^I : K^D]} = \frac{ef}{f} = e.$$

Es genügt nun

$$\mathbb{F}_\mathfrak{P} = \mathbb{F}_{\mathfrak{P}^I}$$

zu bemerken. Dies folgt daraus, dass die Trägheitsgruppe I einerseits der Kern des Reduktionshomomorphismus von Galoisgruppen, andererseits aber auch selbst eine Galoisgruppe ist:

$$I = \ker\big(Gal(K/K^D) \twoheadrightarrow Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_{\mathfrak{P}^D})\big) = Gal(K/K^I)$$

In dem kommutativen Diagramm

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I \cap Gal(K/K^I) & \xrightarrow{id} & Gal(K/K^I) & \longrightarrow & Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_{\mathfrak{P}^I}) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & Gal(K/K^D) & \longrightarrow & Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_{\mathfrak{P}^D}) & \longrightarrow & 1
\end{array}$$

sind somit die entsprechend markierten Pfeile die Identität, und damit liefert die Exaktheit der ersten Zeile wie gewünscht $Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_{\mathfrak{P}^I}) = 1$. □

Ähnlich wie für Verzweigungsgruppen kann man den obigen Formalismus von Trägheitsgruppen auch auf nicht notwendig normale Teilerweiterungen $K'/k \subset K/k$ ausdehnen. Wie zuvor sei

$$S' = S \cap K' \quad \text{und} \quad \mathfrak{P}' = \mathfrak{P} \cap S' \in \operatorname{Spm}(S').$$

Wir betrachten

$$\begin{aligned}
G' &= Gal(K/K'), & G &= Gal(K/k), \\
D' &= G' \cap D, & D &= \big\{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\big\}, \\
I' &= G' \cap I, & I &= \ker\big(D \longrightarrow Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})\big).
\end{aligned}$$

und erhalten das folgende Resultat:

Satz 4.5. *In obiger Situation sind äquivalent:*

(1) $I \subseteq G'$

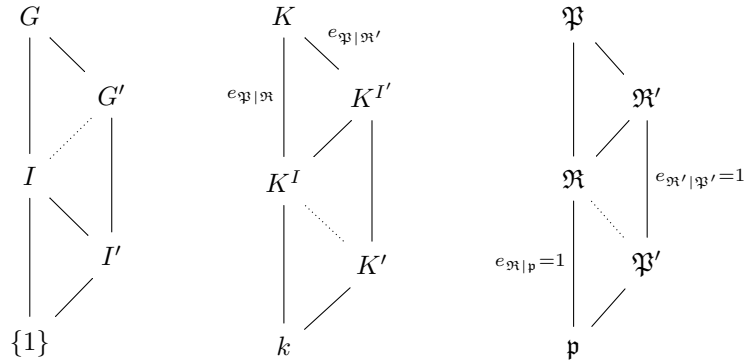
(2) $K' \subseteq K^I$

(3) $e_{\mathfrak{P}'|\mathfrak{p}} = 1$

Beweis. Die Äquivalenz der ersten beiden Eigenschaften ist klar, weil K' nach Galoistheorie der Fixkörper von G' ist. Wir betrachten nun folgende Diagramme, wobei wir

$$\mathfrak{R} \;=\; \mathfrak{P} \cap K^D \quad \text{und} \quad \mathfrak{R}' \;=\; \mathfrak{P} \cap K^{D'}$$

setzen:



Die angegebenen Körpergrade und Verzweigungsindices folgen aus Satz 4.4. Analog zu Satz 3.5 erhalten wir dann aus der Multiplikativität der Verzweigungsindices die Äquivalenzen

$$I \subseteq G' \iff I' = I \iff K^I = K^{I'} \iff e_{\mathfrak{P}|\mathfrak{R}'} = e_{\mathfrak{P}|\mathfrak{R}} \iff e_{\mathfrak{P}'|\mathfrak{p}} = 1$$

und damit folgt die Behauptung. □

Dies liefert ein rein galoistheoretisches Kriterium für die Unverzweigtheit eines Primideals in einem beliebigen Zwischenkörper K' der Erweiterung K/k, sobald die Trägheitsgruppen

$$I_{\mathfrak{P}} \;=\; \ker(D_{\mathfrak{P}} \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})) \;\subseteq\; G \;=\; Gal(K/k)$$

alle bekannt sind:

KOROLLAR 4.6. *Es ist $\mathfrak{p} \in \mathrm{Spm}(R)$ im Zwischenkörper K' von K/k unverzweigt genau dann, wenn gilt:*

$$G_{\mathfrak{P}} \;\subseteq\; G' \;=\; Gal(K/K') \quad \textit{für alle} \quad \mathfrak{P} \mid \mathfrak{p}.$$

Beweis. Ein Primideal $\mathfrak{p} \in \mathrm{Spm}(R)$ ist definitionsgemäß in K' unverzweigt genau dann, wenn $e_{\mathfrak{P}'|\mathfrak{p}} = 1$ für alle Primideale $\mathfrak{P}' \mid \mathfrak{p}$ ist. Für ganze Erweiterungen ist die Abbildung

$$\big\{\mathfrak{P} \in \mathrm{Spm}(S) :\; \mathfrak{P} \mid \mathfrak{p}\big\} \;\longrightarrow\; \big\{\mathfrak{P}' \in \mathrm{Spm}(S') :\; \mathfrak{P}' \mid \mathfrak{p}\big\}, \quad \mathfrak{P} \;\mapsto\; \mathfrak{P}' \;=\; \mathfrak{P} \cap S'$$

surjektiv, und somit folgt die behauptete Äquivalenz aus Satz 4.5. □

Im Fall von Zahlkörpern K/k sind die Restklassenkörper endlich, und in diesem Fall lässt sich die zugehörige Galoisgruppe $Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ expliziter beschreiben. Wir erinnern zunächst daran, dass es bis auf Isomorphie für jede Primzahlpotenz $q = p^\nu$ genau einen Körper $\mathbb{F}_q$ mit q Elementen gibt. Die endlichen Erweiterungskörper dieses Körpers sind genau die Körper $\mathbb{F}_{q^n}$ mit $n \in \mathbb{N}$, und es gilt:

LEMMA 4.7. *Sei $q = p^\nu$ eine Primzahlpotenz und $n \in \mathbb{N}$. Dann ist $\mathbb{F}_{q^n}/\mathbb{F}_q$ eine Galoiserweiterung und*

$$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \;\simeq\; \mathbb{Z}/n\mathbb{Z}$$

ist zyklisch, erzeugt von dem Automorphismus $\Phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \alpha \mapsto \alpha^q$.

Beweis. Das Polynom $f(x) = x^{q^n} - x \in \mathbb{F}_q[x]$ hat im algebraischen Abschluß $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$ keine mehrfachen Nullstellen, denn seine Ableitung ist $f'(x) = -1$. Der von den Nullstellen dieses Polynoms in $\overline{\mathbb{F}}_q$ erzeugte Zerfällungskörper ist also separabel und normal über $\mathbb{F}_q$, also eine Galoiserweiterung. Andererseits gilt

$$f(\alpha) \;=\; 0 \quad \text{für alle} \quad \alpha \;\in\; \mathbb{F}_{q^n}$$

wegen $|\mathbb{F}_{q^n}^\times| = q^n - 1$ (kleiner Satz von Fermat), wegen $\deg(f) = q^n$ besteht $\mathbb{F}_{q^n}$ also genau aus den Nullstellen von $f(x)$ und stimmt somit mit dem oben konstruierten Zerfällungskörper überein. Die Behauptung über die Struktur der Galoisgruppe folgt aus $|Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, weil der Automorphismus Φ nach dem kleinen Satz von Fermat die genaue Ordnung n besitzt. □

Sei K/k eine Galoiserweiterung von Zahlkörpern und $\mathfrak{P} \mid \mathfrak{p}$ ein unverzweigtes Primideal. Dann ist die Trägheitsgruppe $I_\mathfrak{P}$ trivial, und wir erhalten somit einen Isomorphismus

$$\varphi : \quad G_\mathfrak{P} \;\xrightarrow{\sim}\; Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$$

der Zerlegungsgruppe mit der Galoisgruppe der Restklassenkörpererweiterung. Es sei $\Phi \in Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ wie oben definiert durch $\Phi(\alpha) = \alpha^q$ mit $q = N(\mathfrak{p})$. Dann heißt

$$Fr_\mathfrak{P} \;=\; \varphi^{-1}(\Phi) \;\in\; G_\mathfrak{P}$$

das *Frobenius-Element* des betrachteten Primideals.

Lemma 4.8. *Das Frobenius-Element $Fr_\mathfrak{P} \in G = Gal(K/k)$ ist eindeutig durch die Eigenschaft*

$$Fr_\mathfrak{P}(\alpha) \;\equiv\; \alpha^q \mod \mathfrak{P} \quad \textit{für alle } \alpha \in \mathfrak{o}_K.$$

bestimmt. Die Konjugationsklasse dieses Frobenius-Elementes hängt nur von dem unten liegenden Primideal $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$ ab, denn $Fr_{\sigma\mathfrak{P}} = \sigma\, Fr_\mathfrak{P}\, \sigma^{-1}$ für $\sigma \in G$.

Beweis. Man beachte, dass die angegebene Kongruenzbedingung insbesondere impliziert, dass $Fr_\mathfrak{P}$ in der Zerlegungsgruppe $G_\mathfrak{P}$ von $\mathfrak{P} \mid \mathfrak{p}$ liegt. Die behauptete Eindeutigkeit folgt dann, weil φ ein Isomorphismus dieser Zerlegungsgruppe mit der Galoisgruppe der Restklassenkörpererweiterung ist. Die Formel für $Fr_{\sigma\mathfrak{P}}$ ist klar, weil die Isomorphismen φ mit der Galoisoperation kompatibel sind. □

Ist $G = Gal(K/k)$ eine abelsche Gruppe, so hängt das Frobenius-Element $Fr_\mathfrak{P}$ nach dem obigen Lemma nur von $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_k$ ab, und wir bezeichnen es dann auch mit $Fr_\mathfrak{p}$. Im einfachsten Beispiel quadratischer Zahlkörper erhalten wir:

Beispiel 4.9. Sei $K = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$, und sei $\sigma \in Gal(K/\mathbb{Q})$ gegeben durch

$$\sigma(a + b\sqrt{d}) \;=\; a - b\sqrt{d} \quad \text{für} \quad a, b \;\in\; \mathbb{Q}.$$

Für $p \nmid d_K$ prim gilt dann

$$Fr_p \;=\; \begin{cases} id_K & \text{falls } p \text{ in } K/\mathbb{Q} \text{ voll zerlegt ist,} \\ \sigma & \text{falls } p \text{ in } K/\mathbb{Q} \text{ träge ist.} \end{cases}$$

KAPITEL V

Beispiele und Anwendungen

1. Kreisteilungskörper

Sei k ein Körper und $n \in \mathbb{N}$ mit $char(k) \nmid n$. Bekanntlich sind alle endlichen Untergruppen der multiplikativen Gruppe eines Körpers zyklisch, insbesondere ist die Gruppe

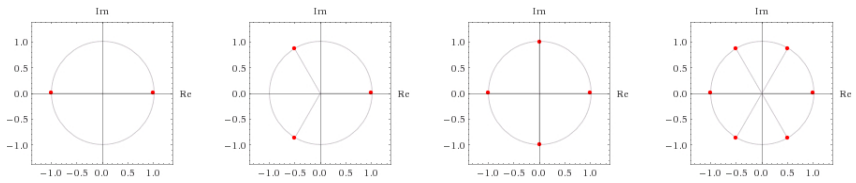
$$\mu_n(\overline{k}) \;=\; \{\alpha \in \overline{k}^\times \mid \alpha^n = 1\}$$

der n-ten Einheitswurzeln in einem algebraischen Abschluß $\overline{k}$ von k zyklisch. Unter einer *primitiven n-ten Einheitswurzel* versteht man einen beliebigen Erzeuger dieser Gruppe. Wir fixieren im Folgenden einen solchen Erzeuger $\zeta_n \in \mu_n(\overline{k})$. Der hiervon erzeugte Körper

$$K \;=\; k(\zeta_n)$$

hängt offenbar nicht von der gewählten primitiven Einheitswurzel ab und wird auch als *n-ter Kreisteilungskörper über k* bezeichnet. Einige Beispiele haben wir schon kennen gelernt:

$$\mathbb{Q}(\zeta_2) = \mathbb{Q} \qquad \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \qquad \mathbb{Q}(\zeta_4) = \mathbb{Q}(i) \qquad \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$$



Für $n \notin \{1, 2, 3, 4, 6\}$ ist allerdings der Körpergrad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] > 2$. Die Bedeutung der Kreisteilungskörper für die Zahlentheorie liegt darin, dass ihre Galoisgruppen dennoch eine sehr einfache Struktur haben:

LEMMA 1.1. *Für alle Kreisteilungskörper $K = k(\zeta_n)$ mit $char(k) \nmid n$ ist K/k eine Galoiserweiterung, und es existiert eine natürliche Einbettung*

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

der Galoisgruppe in die Einheitengruppe des Restklassenringes $\mathbb{Z}/n\mathbb{Z}$.

Beweis. Da ζ_n eine primitive n-te Einheitswurzel ist, gilt $\mu_n(\overline{k}) \subset K$. Also ist K der Zerfällungskörper des Polynoms $f(x) = x^n - 1$ und als solcher insbesondere normal über k. Die Erweiterung ist auch separabel, denn wegen $char(k) \nmid n$ ist die Ableitung

$$f'(\alpha) \;=\; n\alpha^{n-1} \;=\; 0 \quad \text{nur für} \quad \alpha \;=\; 0,$$

sodass $f(x)$ im algebraischen Abschluß keine mehrfachen Nullstellen besitzt. Also ist K/k eine Galoiserweiterung. Um die Galoisgruppe zu beschreiben, nutzen wir den Isomorphismus

$$\mu_n(\overline{k}) \;=\; \langle \zeta_n \rangle \;\xrightarrow{\sim}\; \mathbb{Z}/n\mathbb{Z}, \quad \zeta_n^a \;\mapsto\; \overline{a} \;=\; (a \bmod n).$$

Dieser gibt für jeden Automorphismus $\sigma \in Gal(K/k)$ ein eindeutiges $\chi(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ mit der Eigenschaft

$$\sigma(\zeta_n) \;=\; \zeta_n^a \quad \text{für} \quad \overline{a} \;=\; \chi(\sigma).$$

Für $\tau \in Gal(K/k)$ gilt

$$\zeta_n^{\chi(\sigma\tau)} \;=\; (\sigma\tau)(\zeta_n) \;=\; \sigma(\tau(\zeta_n)) \;=\; \sigma(\zeta_n^{\chi(\tau)}) \;=\; (\sigma(\zeta_n))^{\chi(\tau)} \;=\; \zeta_n^{\chi(\sigma)\chi(\tau)}$$

und somit

$$\chi(\sigma\tau) \;=\; \chi(\sigma)\chi(\tau),$$

wir erhalten also einen Homomorphismus von der Galoisgruppe in die Einheiten des Restklassenrings:

$$\chi: \quad Gal(K/k) \;\longrightarrow\; (\mathbb{Z}/n\mathbb{Z})^\times$$

Dieser Homomorphismus ist injektiv, weil ein Automorphismus $\sigma \in Gal(K/k)$ schon eindeutig durch das Bild $\sigma(\zeta_n) \in K$ bestimmt ist. □

Man beachte, dass die obige konstruierte Einbettung kein Isomorphismus sein muß, dies hängt vom Grundkörper k ab. Beispielsweise gilt:

- Es ist $Gal(\mathbb{R}(\zeta_n)/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z} \not\simeq (\mathbb{Z}/n\mathbb{Z})^\times$ für $n > 6$.
- Auch für endliche Körper ist $\chi(Gal(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p)) = \langle p \bmod n\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ im Allgemeinen eine echte Inklusion.

Der für uns interessanteste Fall ist allerdings der Grundkörper $k = \mathbb{Q}$, und hier kann man mehr sagen:

PROPOSITION 1.2. *Für Kreisteilungskörper $K = \mathbb{Q}(\zeta_n)$ ist die obige Einbettung ein Isomorphismus*

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

Beweis. Sei $f(x) \in \mathbb{Z}[x]$ das Minimalpolynom von ζ_n. Um die Surjektivität des obigen Homomorphismus zu zeigen, müssen wir

$$f(\zeta_n^a) \;=\; 0 \quad \text{für alle} \quad \overline{a} \;\in\; (\mathbb{Z}/n\mathbb{Z})^\times$$

zeigen, denn aus der Galoistheorie wissen wir, dass die Gruppe $Gal(K/k)$ transitiv auf den Nullstellen des Minimalpolynoms operiert. Indem wir das Element $a \in \mathbb{Z}$ als Produkt von Primzahlen $p \nmid n$ schreiben, reduzieren wir die zu beweisende Aussage auf den Fall einer solchen Primzahl $a = p$. Wir argumentieren nun durch Widerspruch: Angenommen,

$$f(\zeta_n^p) \;\neq\; 0 \quad \text{für eine Primzahl} \quad p \nmid n.$$

Wegen $\zeta_n^n = 1$ ist das Minimalpolynom $f(x)$ ein Teiler von $x^n - 1$, wir schreiben also

$$x^n - 1 \;=\; f(x) \cdot h(x) \quad \text{mit} \quad h(x) \;\in\; \mathbb{Z}[x]$$

und erhalten aus obiger Annahme

$$h(\zeta_n^p) \;=\; 0,$$

also ist $f(x) \mid h(x^p)$ und somit

$$h(x^p) \;=\; f(x) \cdot g(x) \quad \text{für ein} \quad g(x) \in \mathbb{Z}[x].$$

Modulo p folgt

$$(\overline{h}(x))^p \;=\; \overline{h}(x^p) \;=\; \overline{f}(x) \cdot \overline{g}(x) \;\in\; \mathbb{F}_p[x]$$

und somit

$$\mathrm{ggT}(\overline{h}(x), \overline{f}(x)) \;\neq\; 1.$$

Dann besitzt aber das Polynom

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

eine mehrfache Nullstelle im algebraischen Abschluß von $\mathbb{F}_p$, was aber für $p \nmid n$ nicht möglich ist, wie wir bereits beim Beweis der Separabilität im vorigen Lemma gesehen haben. □

BEMERKUNG 1.3. Insbesondere ist für jeden Teilkörper $K' \subseteq K = \mathbb{Q}(\zeta_n)$, welcher eine Galoiserweiterung von $\mathbb{Q}$ ist, die Galoisgruppe $Gal(K'/\mathbb{Q})$ abelsch. Der berühmte *Satz von Kronecker-Weber* besagt, dass sich umgekehrt jeder Zahlkörper mit abelscher Galoisgruppe in einen Kreisteilungskörper einbettet. Man beachte aber, dass die analoge Aussage über Zahlkörpern $k \neq \mathbb{Q}$ im Allg. nicht gilt!

Ab jetzt betrachten wir immer den Fall $k = \mathbb{Q}$. Wir bezeichnen mit $\Phi_n(x) \in \mathbb{Z}[x]$ das Minimalpolynom einer primitiven n-ten Einheitswurzel $\zeta_n \in \mathbb{C}$ und nennen dies auch das *n-te Kreisteilungspolynom*. Der Beweis von Proposition 1.2 hat gezeigt, dass

$$\Phi_n(x) \;=\; \prod_{\substack{\zeta \in \mu_n(\mathbb{C}) \\ \text{primitiv}}} (x - \zeta)$$

gilt, insbesondere hängt das obige Kreisteilungspolynom nicht von der gewählten primitiven Einheitswurzel ab. Der Grad dieses Polynomes ist gegeben durch die sog. *Eulersche φ-Funktion*

$$\begin{aligned} \varphi(n) \;&=\; |(\mathbb{Z}/n\mathbb{Z})^\times| \\ &=\; \prod_{p|n} |(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times| \\ &=\; \prod_{p|n} p^{e_p-1}(p-1) \quad \text{für} \quad n \;=\; \prod_p p^{e_p} \quad \text{mit} \quad e_p \;\in\; \mathbb{N}_0. \end{aligned}$$

Betrachten wir einige Beispiele:

(1) Für Primzahlen $n = p$ ist

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

(2) Für Primzahlpotenzen $n = p^\nu$ ist

$$\Phi_n(x) \;=\; \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} \;=\; x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \cdots + x^{p^{\nu-1}} + 1.$$

(3) Für allgemeinere $n \in \mathbb{N}$ gibt es keine einfache Formel für $\Phi_n(x)$, aber die obige Darstellung als Produkt über alle primitiven Einheitswurzeln liefert die rekursive Formel

$$\Phi_n(x) \;=\; \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}.$$

Im Folgenden wollen wir den Ganzheitsring und die Zerlegung von Primzahlen im Kreisteilungskörper $K = \mathbb{Q}(\zeta_n)$ ausrechnen. Der Einfachheit halber beschränken wir uns zunächst auf Einheitswurzeln von Primpotenzordnung:

PROPOSITION 1.4. *Sei $K = \mathbb{Q}(\zeta_n)$ für eine Primzahlpotenz $n = \ell^\nu \neq 2$. Dann ist*

$$d_{K/\mathbb{Q}}(\zeta_n) \;=\; (-1)^{\binom{d}{2}} \cdot \ell^m \quad \textit{mit} \quad d \;=\; \varphi(n), \quad m \;=\; \ell^{\nu-1}(\nu\ell - \nu - 1).$$

Beweis. Wir wollen die aus den Übungen bekannte Formel für die Diskriminante als Norm

$$d_{K/\mathbb{Q}}(\zeta_n) \;=\; (-1)^{\binom{d}{2}} \cdot N_{K/\mathbb{Q}}(\Phi_n'(\zeta_n))$$

verwenden. Durch Ableiten von

$$(x^{n/\ell}-1)\cdot\Phi_n(x) \;=\; x^n-1$$

und anschließendes Einsetzen der primitiven n-ten Einheitswurzel $x=\zeta_n$ erhalten wir zunächst

$$(\zeta_\ell-1)\cdot\Phi_n'(\zeta_n) \;=\; n\cdot\zeta_n^{-1}$$

wobei $\zeta_\ell=\zeta_n^{n/\ell}$ offenbar eine primitive ℓ-te Einheitswurzel ist. Die Norm der linken Seite ist

$$\begin{aligned} N_{K/\mathbb{Q}}(\zeta_\ell-1) &= N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}\big(N_{K/\mathbb{Q}(\zeta_\ell)}(\zeta_\ell-1)\big)\\ &= \big(N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\zeta_\ell-1)\big)^{d/(\ell-1)}\\ &= \big((-1)^{\ell-1}\cdot\Phi_\ell(1)\big)^{d/(\ell-1)}\\ &= (-1)^d\cdot\ell^{d/(\ell-1)} \end{aligned}$$

die der rechten Seite

$$\begin{aligned} N_{K/\mathbb{Q}}(\ell^\nu\cdot\zeta_n^{-1}) &= N_{K/\mathbb{Q}}(\ell^\nu)\cdot N_{K/\mathbb{Q}}(\zeta_n^{-1})\\ &= \ell^{\nu d}\cdot(-1)^d\cdot\Phi_n(0)\\ &= (-1)^d\cdot\ell^{\nu d} \end{aligned}$$

Indem wir beide Terme durcheinander teilen, erhalten wir für die gesuchte Norm der Ableitung die Formel

$$N_{K/\mathbb{Q}}(\Phi_n'(\zeta_n)) \;=\; \frac{\ell^{\nu d}}{\ell^{d/(\ell-1)}}$$

und die Behauptung folgt wegen $\nu d=\ell^{\nu-1}(\nu\ell-\nu)$ und $d/(\ell-1)=\ell^{\nu-1}$. □

Wir erhalten nun den gesuchten Ganzheitsring und das Zerlegungsgesetz für den obigen Kreisteilungskörper wie folgt.

Satz 1.5. *Im Kreisteilungskörper $K=\mathbb{Q}(\zeta_n)$ mit $n=\ell^\nu$ gilt:*

(1) *Es ist $\mathfrak{o}_K=\mathbb{Z}[\zeta_n]$.*

(2) *Jede Primzahl $p\neq\ell$ ist unverzweigt: $p\cdot\mathfrak{o}_K=\prod_{i=1}^g\mathfrak{p}_i$ für $g=\varphi(n)/f$ verschiedene Primideale $\mathfrak{p}_i\in\operatorname{Spm}(\mathfrak{o}_K)$, deren Restklassengrad gegeben ist durch*

$$f \;=\; \min\{\nu\mid p^\nu\equiv 1 \mod n\}.$$

(3) *Die Primzahl ℓ ist voll verzweigt mit*

$$(\ell) \;=\; \mathfrak{p}^{\varphi(n)} \quad \textit{für das Primideal} \quad \mathfrak{p} \;=\; (1-\zeta_n).$$

Beweis. (1) Der Index $N=[\mathfrak{o}_K:\mathbb{Z}[\zeta_n]]$ ist einerseits ein Teiler von $d_{K/\mathbb{Q}}(\zeta_n)$ und somit nach obiger Proposition eine Potenz der Primzahl ℓ. Andererseits hat man aber $\mathbb{Z}[\zeta_n]=\mathbb{Z}[\zeta_n-1]$, und das Minimalpolynom des Elementes ζ_n-1 ist offenbar

$$\Phi_n(x+1) \;=\; \frac{(x+1)^n-1}{(x+1)^{n/\ell}-1} \;\equiv\; \frac{x^n}{x^{n/\ell}} \;\equiv\; x^{\varphi(n)} \mod \ell,$$

also ein Eisenstein-Polynom bezüglich der Primzahl ℓ. Wie wir in den Übungen gesehen haben, gilt dann $\ell\nmid N$ und somit folgt wie behauptet $N=1$.

(2) Wegen $\mathfrak{o}_K=\mathbb{Z}[\zeta_n]$ ist Korollar IV.2.3 anwendbar. Für Primzahlen $p\neq\ell$ ist offenbar

$$\Phi_n'(\zeta) \;\not\equiv\; 0 \mod p\cdot\mathfrak{o}_K$$

für alle $\zeta\in\mu_n(K)$, somit besitzt das modulo p reduzierte Polynom $\overline{\Phi}_n(x)\in\mathbb{F}_p[x]$ keine mehrfachen Nullstellen im algebraischen Abschluß $\overline{\mathbb{F}}_p$ und folglich ist die

Primzahl p in K unverzweigt. Um den Restklassengrad der Primideale $\mathfrak{p} \mid (p)$ zu berechnen, schreiben wir

$$\mathbb{F}_{\mathfrak{p}} \;=\; \mathfrak{o}_K/\mathfrak{p} \;=\; \mathbb{F}_p[\overline{\zeta}_n] \;\subset\; \overline{\mathbb{F}}_p,$$

wobei $\overline{\zeta}_n \in \mathbb{F}_{\mathfrak{p}}$ das Bild der primitiven Einheitswurzel ζ_n bezeichne. Da dieses Bild ebenfalls eine primitive n-te Einheitswurzel ist, ist der Restklassenkörper $\mathbb{F}_{\mathfrak{p}}$ der kleinste Teilkörper von $\overline{\mathbb{F}}_p$, welcher alle n-ten Einheitswurzeln enthält. Für $\nu \in \mathbb{N}$ ist aber $\mathbb{F}_{p^\nu}^\times$ eine zyklische Gruppe der Ordnung $p^\nu - 1$, insbesondere gelten die Äquivalenzen

$$\mu_n(\overline{\mathbb{F}}_p) \;\subseteq\; \mathbb{F}_{p^\nu} \quad\Longleftrightarrow\quad n \mid (p^\nu - 1) \quad\Longleftrightarrow\quad p^\nu \equiv 1 \mod n$$

und somit ist der Restklassengrad f die multiplikative Ordnung von p mod n.

(3) Offenbar gilt

$$\prod_{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times} (1 - \zeta_n^a) \;=\; \Phi_n(1) \;=\; \sum_{i=0}^{\ell-1} x^{i \cdot \ell^{\nu-1}}|_{x=1} \;=\; \ell,$$

und dabei ist

$$1 - \zeta_n^a \;=\; \varepsilon_a \cdot (1 - \zeta_n) \quad \text{mit} \quad \varepsilon_a \;=\; \frac{1 - \zeta_n^a}{1 - \zeta_n} \;=\; \zeta_n^{a-1} + \cdots + \zeta_n + 1 \;\in\; \mathfrak{o}_K.$$

Es ist sogar $\varepsilon_a \in \mathfrak{o}_K^\times$, denn für das Inverse $\overline{b} = \overline{a}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gilt mit $ab \equiv 1 \mod n$ auch

$$\varepsilon_a^{-1} \;=\; \frac{1 - \zeta_n}{1 - \zeta_n^a} \;=\; \frac{1 - \zeta_n^{ab}}{1 - \zeta_n^a} \;=\; \zeta_n^{a(b-1)} + \cdots + \zeta_n^a + 1 \;\in\; \mathfrak{o}_K.$$

Somit sind alle Faktoren auf der linken Seite der obigen Produktzerlegung von ℓ zueinander assoziiert, und es folgt die Behauptung. □

Insbesondere ist die Trägheitsgruppe einer Primzahl p in der Erweiterung $K/\mathbb{Q}$ gegeben durch

$$I \;=\; \begin{cases} Gal(K/\mathbb{Q}) & \text{für } p = \ell, \\ \{1\} & \text{für } p \neq \ell, \end{cases}$$

wir brauchen uns im Folgenden also nur für die Zerlegungsgruppe $D \hookrightarrow Gal(K/\mathbb{Q})$ von Primzahlen $p \neq \ell$ zu interessieren. Diese sind unverzweigt und der Frobenius ist gegeben durch die Restklasse $\overline{p} = p \mod n$:

$$\begin{array}{ccc} \mathrm{Fr}_p & \longmapsto & \overline{p} \\ \cap & & \cap \\ Gal(K/\mathbb{Q}) & \xrightarrow{\sim} & (\mathbb{Z}/n\mathbb{Z})^\times \end{array}$$

Betrachten wir noch die Extremfälle von voller Zerlegtheit und Trägheit, wo die Zerlegungsgruppe trivial oder die volle Galoisgruppe ist. Unter einer *Primitivwurzel* mod n verstehen wir im Folgenden einen Erzeuger der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ falls diese Gruppe zyklisch ist.

KOROLLAR 1.6. *Sei $K = \mathbb{Q}(\zeta_n)$ mit $n = \ell^\nu$. Für Primzahlen p gilt dann:*

(1) *Es ist p voll zerlegt in K genau dann, wenn $p \equiv 1 \mod n$ ist.*

(2) *Es ist p träge in K genau dann, wenn p eine Primitivwurzel mod n ist.*

Beweis. Der Fall $p \mid n$ ist wegen der Unverzweigtheit ausgeschlossen, wir können also $p \neq \ell$ annehmen. Die multiplikative Ordnung f von $\overline{p} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ist gleich Eins genau dann, wenn $p \equiv 1 \bmod n$ ist. Andererseits ist diese Ordnung gleich $\varphi(n)$ genau dann, wenn p eine Primitivwurzel $\bmod n$ ist. □

In der Algebra zeigt man, dass die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ für $n = \ell^\nu$ zyklisch ist genau dann, wenn $\ell \neq 2$ oder $\nu \in \{1, 2\}$ ist; in allen diesen Fällen existieren also Primitivwurzeln und der träge Fall tritt dementsprechend auf.

Beispiel 1.7. (a) Da $(\mathbb{Z}/8\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nicht zyklisch ist, gibt es mod 8 keine Primitivwurzel und das obige Korollar zeigt, dass in $K = \mathbb{Q}(\zeta_8)$ keine Primzahl träge ist. Das irreduzible Polynom

$$\Phi_8(x) \;=\; x^4 + 1 \;\in\; \mathbb{Z}[x]$$

ist also modulo *jeder* Primzahl p reduzibel:

$$\begin{aligned} x^4 + 1 \;&\equiv\; (x+1)^4 \mod 2, \\ &\equiv\; (x^2 + x - 1)(x^2 - x - 1) \mod 3, \\ &\equiv\; (x^2 + 2)(x^2 - 1) \mod 5, \\ &\;\;\vdots \\ &\equiv\; (x+2)(x+8)(x+9)(x+15) \mod 17, \quad \text{usw.} \end{aligned}$$

Für $p \neq 2$ ist dieses Polynom in $\mathbb{F}_p[x]$ quadratfrei. Nach dem obigen Korollar tritt andernfalls genau eine der folgenden beiden Möglichkeiten auf:

- Für $p \equiv 1 \bmod 8$ zerfällt $\overline{\Phi}_8(x) \in \mathbb{F}_p[x]$ als Produkt von Linearfaktoren und dann ist p voll zerlegt im Kreisteilungskörper $K = \mathbb{Q}(\zeta_8)$.
- Andernfalls ist $\overline{\Phi}_8(x) \in \mathbb{F}_p[x]$ ein Produkt zweier irreduzibler quadratischer Polynome, und dementsprechend ist das Ideal $p \cdot \mathfrak{o}_K$ ein Produkt zweier Primideale vom Restklassengrad $f = 2$.

(b) Die Gruppe $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$ ist zyklisch mit Primitivwurzeln $\overline{2}, \overline{3} \bmod 5$ und es gilt

$$(\mathbb{Z}/5\mathbb{Z})^\times \;=\; \langle\,\overline{2}\,\rangle \;=\; \langle\,\overline{3}\,\rangle \;\simeq\; \mathbb{Z}/4\mathbb{Z} \;\supset\; \langle\,\overline{4}\,\rangle \;\simeq\; \mathbb{Z}/2\mathbb{Z} \;\supset\; \langle\,\overline{1}\,\rangle \;\simeq\; \{0\}.$$

Hier ist das reduzierte Polynom $\overline{\Phi}_5(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_p[x]$ für $p \neq 5$ quadratfrei, und das obige Korollar liefert folgende Möglichkeiten:

- Für $p \equiv 2, 3 \bmod 5$ ist das Polynom $\overline{\Phi}_5(x) \in \mathbb{F}_p[x]$ irreduzibel, und p ist somit träge in $K = \mathbb{Q}(\zeta_5)$. Insbesondere ist in diesem Fall also die Zerlegungsgruppe die volle Galoisgruppe $D = Gal(K/\mathbb{Q})$.
- Für $p \equiv 1 \bmod 5$ zerfällt $\overline{\Phi}_5(x) \in \mathbb{F}_p[x]$ als Produkt von Linearfaktoren, beispielsweise

  $$\Phi_5(x) \;\equiv\; (x+2)(x+6)(x+7)(x+8) \mod 11,$$

  und p ist im Kreisteilungskörper $K = \mathbb{Q}(\zeta_5)$ voll zerlegt mit $D = \{1\}$.
- Für $p \equiv 4 \bmod 5$ zerfällt $\overline{\Phi}_5(x) \in \mathbb{F}_p[x]$ in zwei irreduzible quadratische Faktoren, etwa

  $$\Phi_5(x) \;\equiv\; (x^2 + 5x + 1)(x^2 + 15x + 1) \mod 19,$$

  und $p \cdot \mathfrak{o}_K$ ist Produkt zweier Primideale vom Restklassengrad $f = 2$. Die Zerlegungsgruppe $D \subset Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times$ ist hier die eindeutige Untergruppe vom Index zwei, welche aus den Quadraten besteht.

Man beachte, dass der Erzeuger der Zerlegungsgruppe im letzten Fall die komplexe Konjugation ist, wir erhalten hier somit als Zerlegungskörper den quadratischen Teilkörper

$$K^D \;=\; K \cap \mathbb{R} \;=\; \mathbb{Q}(\zeta_5 + \overline{\zeta_5}) \;\stackrel{!}{=}\; \mathbb{Q}(\sqrt{5}) \quad \text{wegen} \quad \mathrm{Re}(\zeta_5) \;=\; \frac{\sqrt{5}-1}{4}.$$

Die Beziehung zwischen Kreisteilungskörpern und quadratischen Zahlkörpern wird im nächsten Abschnitt noch genauer untersucht.

2. Quadratische Reziprozität

Die Zerlegung von Primzahlen in Kreisteilungskörpern gibt eine konzeptionelle Erklärung für das quadratische Reziprozitätsgesetz. Der Ausgangspunkt hierfür ist die folgende, durch das letzte Beispiel motivierte Beobachtung:

PROPOSITION 2.1. *Sei p eine ungerade Primzahl. Dann enthält $K = \mathbb{Q}(\zeta_p)$ genau einen quadratischen Teilkörper k, und explizit ist dieser Teilkörper gegeben durch*

$$k \;=\; \mathbb{Q}(\sqrt{p^*}) \quad \textit{mit} \quad p^* \;=\; (-1)^{\frac{p-1}{2}}\, p.$$

Beweis. Da p eine ungerade Primzahl ist, ist die Galoisgruppe hier zyklisch von gerader Ordnung:

$$Gal(K/\mathbb{Q}) \;\simeq\; (\mathbb{Z}/p\mathbb{Z})^\times \;\simeq\; \mathbb{Z}/(p-1)\mathbb{Z}.$$

Insbesondere besitzt sie eine eindeutig bestimmte Untergruppe vom Index 2, also gibt es genau einen quadratischen Teilkörper k von K. Um diesen explizit zu bestimmen, betrachten wir die Diskriminante. Aus Proposition 1.4 erhalten wir einerseits

$$\begin{aligned} d_{K/\mathbb{Q}}(\zeta_p) &= (-1)^{\frac{(p-1)(p-2)}{2}} \cdot p^{p-2} \\ &= (-1)^{\frac{p-1}{2}} \cdot p \cdot p^{p-3} \\ &= p^{p-3} \cdot p^* \\ &= m^2 \cdot p^* \quad \text{mit} \quad m = p^{\frac{p-3}{2}} \in \mathbb{Z}, \end{aligned}$$

andererseits ist

$$d_{K/\mathbb{Q}}(\zeta_p) \;=\; \alpha^2 \quad \text{mit} \quad \alpha \;=\; \prod_{0 \le \mu < \nu < p} (\zeta_p^\mu - \zeta_p^\nu) \;\in\; \mathfrak{o}_K$$

ein Quadrat in K nach Lemma II.2.9. Beides zusammen liefert $\sqrt{p^*} = \pm\alpha/m \in K$ und damit die Behauptung. □

Als direktes Korollar erhalten wir nun das auf Euler zurückgehende quadratische Reziprozitätsgesetz, dessen erste Beweise von Gauss stammen und das seitdem eine Fülle verschiedener Beweise gefunden hat, seine tiefere Bedeutung aber erst im Rahmen von Kreisteilungskörpern offenbart. Aus elementarer Sicht geht es darum, das Legendre-Symbol

$$\left(\frac{d}{p}\right) \;=\; \begin{cases} +1 & \text{falls } d \equiv x^2 \not\equiv 0 \mod p \text{ mit } x \in \mathbb{Z} \text{ ist,} \\ 0 & \text{falls } d \equiv 0 \mod p \text{ ist,} \\ -1 & \text{sonst,} \end{cases}$$

für festes $d \in \mathbb{Z}$ und variable Primzahlen p effektiv zu berechnen: Wir wollen also wissen, modulo welcher Primzahlen eine gegebene ganze Zahl ein quadratischer Rest ist — ein Problem, das wir bereits im Zusammenhang mit der Zerlegung von

Primzahlen im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ angetroffen haben. Für jedes p ist das Legendre-Symbol

$$\left(\frac{\cdot}{p}\right): \quad (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$

ein Homomorphismus, wir können uns daher auf den Fall von Primzahlen $d = q$ beschränken. Das quadratische Reziprozitätsgesetz besagt dann, dass die gesuchten Legendre-Symbole für variables p nur von den endlich vielen Restklassen $\overline{p} \in \mathbb{Z}/q\mathbb{Z}$ abhängen. Genauer gilt:

Satz 2.2 (Quadratische Reziprozität). *Sind $p \neq q$ zwei ungerade Primzahlen, dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{1}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{2}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{3}$$

Beweis. Wir beweisen zunächst die sogenannten Ergänzungssätze (2), (3). Dabei folgt (2) aus der Tatsache, dass $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ zyklisch von der Ordnung $p-1$ ist und somit

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \quad \text{für alle} \quad a \in (\mathbb{Z}/p\mathbb{Z})^\times$$

gilt. Für (3) benutzen wir dieselbe Formel, berechnen die Potenzen von 2 mod p aber einfacher im Zahlring $\mathbb{Z}[i]$ modulo $p \cdot \mathbb{Z}[i]$. Wegen $(1+i)^2 = 2i$ hat man hier die Identität

$$2^{\frac{p-1}{2}} = \Big((1+i)^2 \cdot (-i)\Big)^{\frac{p-1}{2}} = (1+i)^{p-1} \cdot (-i)^{\frac{p-1}{2}}$$

und somit folgt

$$\begin{aligned}
(1+i) \cdot 2^{\frac{p-1}{2}} &= (1+i)^p \cdot (-i)^{\frac{p-1}{2}} \\
&\equiv (1+i^p) \cdot (-i)^{\frac{p-1}{2}} \mod p\,\mathbb{Z}[i] \\
&= (1+(-1)^{\frac{p-1}{2}} \cdot i) \cdot (-i)^{\frac{p-1}{2}} \\
&= i^{\frac{p-1}{2}} \cdot ((-1)^{\frac{p-1}{2}} + i).
\end{aligned}$$

Die rechte Seite hängt offenbar nur von p mod 8 ab. Ein Vergleich des Realteils auf beiden Seiten folgt

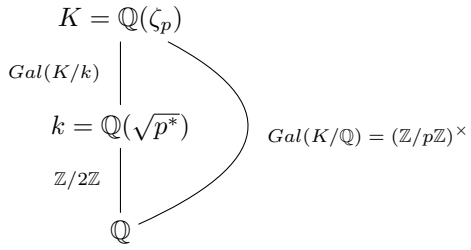
$$2^{\frac{p-1}{2}} \mod p \equiv \begin{cases} +1 \mod p & \text{für } p \equiv \pm 1 \mod 8, \\ -1 \mod p & \text{für } p \equiv \pm 3 \mod 8, \end{cases}$$

und die rechte Seite ist gleich $(-1)^{\frac{p^2-1}{8}}$ wie gewünscht.

Es bleibt der eigentlich interessante Teil, die Aussage (1) zu zeigen. Nach (3) ist diese äquivalent zu

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \quad \text{mit} \quad p^* = (-1)^{\frac{p-1}{2}} p.$$

Um die letzte Gleichheit von Legendre-Symbolen zu zeigen, betrachten wir den Körperturm



und bemerken, dass dieser die Galoisgruppe $Gal(K/k) \subset Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ mit der Untergruppe der Quadrate identifiziert, da die Einheitengruppe auf der rechten Seite zyklisch ist und somit genau eine Untergruppe vom Index zwei enthält. Wir erhalten die Äquivalenzen

$$\begin{aligned}
\left(\frac{p^*}{q}\right) \;=\; 1 \quad &\iff \quad q \text{ voll zerlegt in } k/\mathbb{Q} \\
&\iff \quad \text{Die Zerlegungsgruppe } \langle \mathrm{Fr}_q \rangle \text{ von } q \text{ ist enthalten in } Gal(K/k) \\
&\overset{!}{\iff} \quad \overline{q} = q \mod p \quad \text{ist ein Quadrat in} \quad (\mathbb{Z}/p\mathbb{Z})^\times \\
&\iff \quad \left(\frac{q}{p}\right) \;=\; 1
\end{aligned}$$

und damit die Behauptung. □

Beispiel 2.3. In $K = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$ ist nach Lemma IV.2.4 eine Primzahl

$$p \;\neq\; 2 \quad \begin{cases} \text{voll zerlegt} \\ \text{verzweigt} \\ \text{träge} \end{cases} \quad \text{genau für} \quad \left(\frac{d}{p}\right) \;=\; \begin{cases} +1, \\ \;\;0, \\ -1. \end{cases}$$

Aus dem quadratischen Reziprozitätsgesetz folgt nun, dass die rechte Seite nur von der Restklasse $p \bmod 4 \cdot d$ abhängt, und zugleich erhalten wir hieraus eine effektive Methode zu ihrer konkreten Berechnung für gegebenes d. So ist für $d = 15 = 3 \cdot 5$ beispielsweise

$$\left(\frac{15}{p}\right) \;=\; \left(\frac{3}{p}\right) \cdot \left(\frac{5}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot \left(\frac{p}{5}\right),$$

und die rechte Seite lässt sich leicht explizit berechnen: Für $p \in \{3, 5\}$ ist sie Null, sonst ist

$$\left(\frac{p}{3}\right) \;=\; \begin{cases} +1, & p \equiv 1 \mod 3, \\ -1, & p \equiv 2 \mod 3, \end{cases} \qquad \left(\frac{p}{5}\right) \;=\; \begin{cases} +1, & p \equiv 1, 4 \mod 5, \\ -1, & p \equiv 2, 3 \mod 5, \end{cases}$$

und somit

$$\left(\frac{15}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \cdot \begin{cases} +1, & p \equiv 1, 2, 4, 8 \mod 15, \\ -1, & p \equiv 7, 11, 13, 14 \mod 15. \end{cases}$$

Man beachte, dass die rechte Seite wegen des zusätzlichen Vorzeichens $(-1)^{\frac{p-1}{2}}$ insgesamt von $p \bmod 60$ abhängt.

Beispiel 2.4. Das quadratische Reziprozitätsgesetz erlaubt es auf einfache Weise nachzuprüfen, ob eine Zahl ein quadratischer Rest modulo einer gegebenen großen Primzahl $p \gg 0$ ist, ohne dabei alle Restklassen modulo p zu durchlaufen. So ist etwa

$$\left(\frac{27}{2017}\right) \;=\; \left(\frac{3}{2017}\right)^3 \;=\; \left(\frac{3}{2017}\right) \overset{!}{=} \left(\frac{2017}{3}\right) \;=\; \left(\frac{1}{3}\right) \;=\; +1$$

wegen $2017 \equiv 1 \bmod 3$, also ist 27 ein quadratischer Rest modulo $p = 2017$. Von Hand wäre das schwieriger nachzuprüfen, tatsächlich ist die kleinste Darstellung als Quadrat $774^2 = 599\,076 = 297 \cdot 2017 + 27 \equiv 27 \bmod 2017$.

3. Fermat's letzter Satz für reguläre Primzahlen

In diesem Abschnitt wollen wir als Anwendung der Kreisteilungskörper einige Spezialfälle von Fermat's letztem Satz beweisen, der berühmten Randbemerkung von Fermat (um 1640) in seinem Exemplar von Diophant's Arithmetik:

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere: Cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

Mit anderen Worten: Für $n \geq 3$ besitzt die Gleichung $x^n + y^n = z^n$ keine Lösungen $(x, y, z) \in \mathbb{Z}^3$ mit der Eigenschaft $xyz \neq 0$. Wie Fermat sich seinen nicht mehr auf den Rand passenden wunderbaren Beweis vorstellte, kann man nur spekulieren. Bekanntlich wurde der erste vollständige Beweis erst 1994 von Wiles und Taylor in Zusammenhang mit tiefliegenden Vermutungen über die Modularität elliptischer Kurven bewiesen. Wir sind hier bescheidener und betrachten lediglich einige Spezialfälle, die auf Kummer zurückgehen und eng mit der Theorie der Kreisteilungskörper verbunden sind.

Zunächst folgt aus der Fermat-Fermutung für den Exponent n auch die für jedes Vielfache von n wegen

$$x^{en} + y^{en} \;=\; z^{en} \quad\Longrightarrow\quad (x^e)^n + (y^e)^n \;=\; (z^e)^n \quad \text{für} \quad e \in \mathbb{N}.$$

Der Fall $n = 4$ lässt sich mit elementaren Methoden ausschließen und sei dem Leser als Übungsaufgabe überlassen, wir können also annehmen, dass $n = p$ eine ungerade Primzahl ist. Gabriel Lamé hat 1847 den folgenden Bezug zur Theorie der Kreisteilungskörper hergestellt:

LEMMA 3.1. *Wenn $x^p + y^p = z^p$ mit $x, y, z \in \mathbb{Z}$ ist, so hat man in $K = \mathbb{Q}(\zeta_p)$ eine Faktorisierung*

$$z^p \;=\; \prod_{\nu=1}^{p} (x + \zeta_p^\nu y).$$

Beweis. Wir können oBdA $y \neq 0$ und nach Division der Gleichung durch y^p sogar $y = 1$ annehmen. Nun durchlaufen die $-\zeta_p^\nu$ für $\nu = 1, 2, \ldots, p$ genau die Nullstellen des Polynoms $x^p + 1$, also folgt die Behauptung. □

Lamé bemerkte weiter, dass für $xyz \neq 0$ keine Faktoren auf der rechten Seite einen echten gemeinsamen Teiler besitzen können, und folgerte, dass jedes der Elemente $x + \zeta_p^\nu$ eine p-te Potenz sein müsse, woraus er einen Widerspruch ableiten konnte. Die Grundlage dieses Argumentes war jedoch die implizite Annahme, dass der Ganzheitsring $\mathfrak{o}_K$ faktoriell sei, was im Allgemeinen falsch ist! Dies war schon Kummer bekannt:

BEISPIEL 3.2. Für $K = \mathbb{Q}(\zeta_{23})$ ist $h_K > 1$ (Übungsaufgabe).

Die Klassenzahlen von Kreisteilungskörpern sind nicht einfach zu berechnen und bis heute nicht völlig verstanden. Ein Resultat von Montgomery und Uchida (1971) besagt, dass $h_K = 1$ genau für die Primzahlen $p \leq 19$ gilt. Die folgende Liste zeigt einige weitere auftretende Klassenzahlen; die Besonderheit von $p = 37$ wird weiter unten diskutiert:

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	$\cdots$
h_K	1	1	1	1	1	1	1	3	8	9	37	121	211	695	$\cdots$

Kummer hat bemerkt, dass sich im Fall $p \nmid h_K$ das Argument von Lamé reparieren lässt, da dann die Nicht-Trivialität der Klassengruppe C_K keinen Einfluß auf das Verhalten p-ter Potenzen hat. Dies führt auf folgende

DEFINITION 3.3. Eine Primzahl p heißt *regulär*, falls $p \nmid h_K$ für $K = \mathbb{Q}(\zeta_p)$ ist.

Man vermutet, dass etwa 69 % aller Primzahlen regulär sind. Allerdings ist bis heute nicht einmal bekannt, ob es überhaupt unendlich viele reguläre Primzahlen gibt! Von Kummer stammt das folgende Kriterium:

$$p \text{ ist regulär} \quad \Longleftrightarrow \quad p \text{ teilt den Zähler einer Bernoulli-Zahlen } B_n \text{ mit } n \leq p-3.$$

wobei die B_n durch

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

definiert sind. Man kann zeigen, dass alle Bernoulli-Zahlen rational sind, so gilt zum Beispiel

$$B_{37} \;=\; -\,\frac{37 \cdot 683 \cdot 305065927}{2 \cdot 5 \cdot 51}$$

und $p = 37$ ist somit eine irreguläre Primzahl. Die kleinsten irregulären Primzahlen sind

$$p \;=\; 37, 59, 67, 101, 103, 131, \ldots$$

und man weiß, dass es unendlich viele irreguläre Primzahlen gibt; ein elementarer Beweis findet sich in Carlitz, Note on irregular primes.

Im Folgenden kehren wir lieber zu positiven Nachrichten zurück und bemerken zunächst, dass die von Lamé beobachtete Teilerfremdheit im *idealtheoretischen* Sinne richtig bleibt. Wir betrachten hierzu das von $\pi = 1 - \zeta_p$ erzeugte Primideal und beweisen allgemeiner

LEMMA 3.4. *Sei $K = \mathbb{Q}(\zeta_p)$ für eine Primzahl p. Für $x, y \in \mathfrak{o}_K$ und $\mathfrak{a} = (x, y)$ sind die Ideale*

$$\mathfrak{a}^{-1} \cdot (x + \zeta_p^{\nu} y) \;\trianglelefteq\; \mathfrak{o}_K \quad \textit{für} \quad 0 \leq \nu < p$$

entweder paarweise teilerfremd, oder es gilt: Alle diese Ideale sind teilbar durch (π) und je zwei von ihnen besitzen keine weiteren gemeinsamen Teiler.

Beweis. Sei $0 \leq \nu < \mu < p$ und $\mathfrak{d} = \mathrm{ggT}(\mathfrak{a}^{-1}(x+\zeta_p^{\nu} y), \mathfrak{a}^{-1}(x+\zeta_p^{\mu} y)) \trianglelefteq \mathfrak{o}_K$. Dann gilt

$$\begin{aligned} \pi y \;\sim\; (1-\zeta_p^{\mu-\nu}) \cdot y \;&=\; \zeta_p^{-\nu} \cdot ((x+\zeta_p^{\nu} y) - (x+\zeta_p^{\mu} y)) \;\in\; \mathfrak{a}\mathfrak{d} \quad \Longrightarrow \quad \mathfrak{a}\mathfrak{d} \mid (\pi x), \\ \pi x \;\sim\; (1-\zeta_p^{\mu-\nu}) \cdot x \;&=\; (x+\zeta_p^{\mu} y) - \zeta_p^{\mu-\nu}(x+\zeta_p^{\nu} y) \;\in\; \mathfrak{a}\mathfrak{d} \quad \Longrightarrow \quad \mathfrak{a}\mathfrak{d} \mid (\pi y). \end{aligned}$$

Wegen $\mathfrak{a} = (x, y)$ folgt $\mathfrak{a}\mathfrak{d} \mid \pi\mathfrak{a}$ und somit $\mathfrak{d} \mid (\pi)$. Da das Ideal (π) maximal ist, folgt hieraus

$$\mathfrak{d} = (1) \quad \text{oder} \quad \mathfrak{d} = (\pi).$$

Im letzten Fall ist

$$\mathfrak{a}^{-1} \cdot (x + \zeta_p^{\nu+1} y) \;\subseteq\; \underbrace{\mathfrak{a}^{-1} \cdot (x + \zeta_p^{\nu} y)}_{\subseteq \mathfrak{d} = (\pi)} \;+\; \underbrace{\mathfrak{a}^{-1} \cdot \zeta_p^{\nu} y}_{\subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}_K} \cdot \underbrace{(1 - \zeta_p)}_{= (\pi)} \;\subseteq\; (\pi)$$

und damit induktiv $(\pi) \mid \mathfrak{a}^{-1}(x + \zeta_p^{\gamma} y)$ für alle γ wie behauptet. □

Im Fall *regulärer* Primzahlen hat Kummer aus diesen Ideal-Faktorisierungen tatsächliche Faktorisierungen von Elementen konstruieren und erhielt damit den folgenden

SATZ 3.5. *Sei $p > 2$ eine reguläre Primzahl. Dann hat die Gleichung $x^p + y^p = z^p$ keine ganzzahligen Lösungen $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$.*

Beweis. Angenommen, es gäbe eine ganzzahlige Lösung (x, y, z) mit $xyz \neq 0$, wobei wir oBdA $\mathrm{ggT}(x, y) = 1$ annehmen können. Wir wollen einen Widerspruch herbeiführen und unterscheiden dazu zwei Fälle:

① *Der Fall $p \nmid xyz$.* Für $p = 3$ ist dann $x^3, y^3, z^3 \equiv \pm 1 \bmod 9$ und es kann keine Lösung der Fermat-Gleichung vorliegen. Wir nehmen daher im Folgenden $p \geq 5$ an. Durch Vertauschen von y und $-z$ kann dann $x \not\equiv y \bmod p$ erreicht werden, was später nützlich sein wird. Aus Lemma 3.1 erhalten wir

$$(z)^p \;=\; \prod_{\nu=0}^{p-1} (x + \zeta_p^\nu y) \;\trianglelefteq\; \mathfrak{o}_K \quad \text{in} \quad K \;=\; \mathbb{Q}(\zeta_p).$$

Wegen $p \nmid z$ sind die hierbei auftretenden Ideale $(x + \zeta_p^\nu) \trianglelefteq \mathfrak{o}_K$ nach Lemma 3.4 paarweise teilerfremd. Aus der eindeutigen Primfaktorzerlegung von Idealen folgt somit

$$(x + \zeta_p y) \;=\; \mathfrak{a}^p \quad \text{für ein Ideal} \quad \mathfrak{a} \trianglelefteq \mathfrak{o}_K.$$

Da auf der linken Seite ein Hauptideal steht, erhalten wir in der Klassengruppe C_K die Relation $[\mathfrak{a}]^p = 1$ und somit $[\mathfrak{a}] = 1$, denn für reguläre Primzahlen p enthält die Klassengruppe wegen

$$p \nmid h_K \;=\; |C_K|$$

keine p-Torsion. Als triviales Element der Klassengruppe ist dann $\mathfrak{a}$ ein Hauptideal, also

$$\mathfrak{a} \;=\; (\alpha) \quad \text{für ein} \quad \alpha \in \mathfrak{o}_K$$

und somit

$$x + \zeta_p y \;=\; \epsilon \cdot \alpha^p \quad \text{für eine Einheit} \quad \epsilon \in \mathfrak{o}_K^\times.$$

Schreibt man

$$\alpha \;=\; c_0 + c_1\zeta_p + \cdots + c_{p-2}\zeta_p^{p-2} \quad \text{mit} \quad c_0, \ldots, c_{p-2} \in \mathbb{Z},$$

so gilt offenbar

$$\alpha^p \;\equiv\; c_0^p + c_1^p + \cdots + c_{p-2}^p \;\equiv\; \overline{\alpha}^p \mod p$$

und somit

$$(x + \zeta_p y) - \eta \cdot (x + \zeta_p^{-1} y) \;\equiv\; 0 \mod p$$

mit $\eta = \overline{\epsilon}/\epsilon$. Wir wollen aus der letzten Kongruenz die Teilbarkeit $p \mid xy$ folgern im Widerspruch zur Annahme. Hierzu bemerken wir zunächst, dass die Einheit η die Eigenschaft

$$|\sigma(\eta)| \;=\; 1 \quad \text{für alle} \quad \sigma \in Gal(K/\mathbb{Q})$$

besitzt, also im Kern der Abbildung

$$\lambda \;=\; \mathrm{Log} \circ \iota : \quad \mathfrak{o}_K^\times \;\longrightarrow\; \mathbb{R}^{r+s+1}$$

aus Satz III.4.1 liegt und somit eine Einheitswurzel ist. Die einzigen in $K = \mathbb{Q}(\zeta_p)$ enthaltenen Einheitswurzeln sind aber die $2p$-ten Einheitswurzeln: Tatsächlich gilt ganz allgemein

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_p) \;=\; \mathbb{Q} \quad \text{für} \quad \mathrm{ggT}(m, n) \;=\; 1,$$

denn $\zeta_m\zeta_n$ ist eine primitive mn-te Einheitswurzel, also ist $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ und dabei gilt Gleichheit wegen $\varphi(mn) = \varphi(m)\varphi(n)$, was die Behauptung zeigt. In unserem Fall folgt

$$\eta \;=\; \pm\zeta_p^\nu \quad \text{für ein} \quad \nu \;\in\; \{0, 1, \dots, p-1\}.$$

Durch Reduktion dieser Identität modulo des Primideals $(1-\zeta_p)$ findet man das Vorzeichen $\eta = +\zeta_p^\nu$ und die für den gesuchten Widerspruch zu betrachtende Kongruenz wird zu

$$x \,+\, \zeta_p y \,-\, \zeta_p^\nu x \,-\, \zeta_p^{\nu-1} y \;\equiv\; 0 \mod p.$$

Nun bilden je $p-1$ verschiedene Potenzen der primitiven Einheitswurzel ζ_p eine Ganzheitsbasis für den Ring $\mathfrak{o}_K$. Für $p \nmid xy$ können die in der obigen Kongruenz auftretenden Potenzen also nicht alle verschieden sein, es muß also $\nu \in \{0, 1, 2\}$ gelten. Aber dann ist

$$(\zeta_p - \zeta_p^{-1})y \equiv 0 \quad \text{oder} \quad (1-\zeta_p)(x-y) \equiv 0 \quad \text{oder} \quad (1-\zeta_p^2)x \equiv 0 \mod p$$

im Widerspruch zu unserer Annahme $p \nmid xy$ und $x \not\equiv y \bmod p$.

⑪ *Der Fall $p \mid xyz$.* Wir nehmen oBdA $p \mid z$, $p \nmid xy$ an und wollen aus der gegebenen Lösung induktiv eine neue Lösung konstruieren, sodass die Teilbarkeit von z durch p in jedem Schritt verringert wird. Bei dem Abstiegsargument werden wir den ursprünglichen Rahmen verlassen und beweisen daher allgemeiner, dass die verallgemeinerte Fermat-Gleichung

$$x^p + y^p \;\sim\; z^p$$

keine Lösung

$$(x, y, z) \;\in\; \mathfrak{o}_K^3 \quad \text{mit} \quad xyz \;\neq\; 0 \quad \text{und} \quad \pi \mid z, \quad \pi \nmid xy$$

besitzt. Für eine beliebige solche Lösung definieren wir den Exponenten $n \in \mathbb{N}$ durch $\pi^n \| z$, also

$$\pi^n \mid z \quad \text{und} \quad \pi^{n+1} \nmid z.$$

Wir können die Lösung mit kleinstmöglichem Exponenten n wählen und wollen eine Lösung mit noch kleinerem Exponenten konstruieren, um einen Widerspruch zu erhalten. In der Faktorisierung

$$(z)^p \;=\; \prod_{\nu=0}^{p-1} (x + \zeta_p^\nu y) \;\trianglelefteq\; \mathfrak{o}_K$$

ist das Ideal auf der linken Seite durch π teilbar, daher liefert Lemma 3.4 eine Faktorisierung

$$(x + \zeta_p^\nu y) \;=\; \pi\mathfrak{a} \cdot \mathfrak{b}_\nu^p \quad \text{mit paarweise teilerfremden} \quad \mathfrak{b}_\nu \;\trianglelefteq\; \mathfrak{o}_K$$

und dem größten gemeinsamen Teiler

$$\mathfrak{a} \;=\; (x, y) \;\trianglelefteq\; \mathfrak{o}_K.$$

Bevor wir diesen größten gemeinsamen Teiler loswerden, wollen wir zunächst unsere Numerierung geeignet wählen: Wegen $\pi \nmid y$ durchlaufen die $x + \zeta_p^\nu y$ für $0 \le \nu < p$ genau die p verschiedenen Restklassen in $\pi\mathfrak{o}_K \bmod (\pi^2)$ und es ist genau eines dieser Elemente durch π^2 teilbar. Indem wir in unserer gegebenen Lösung y durch ein $\zeta_p^\mu y$ ersetzen, können wir

$$\pi^2 \mid (x+y) \quad \text{und somit} \quad \pi^{np-p+1} \| (x+y)$$

annehmen. Man beachte, dass dieses Argument zugleich $n > 1$ zeigt. Wir wählen nun ein ganzes Ideal $\mathfrak{c} \trianglelefteq \mathfrak{o}_K$ mit der Eigenschaft $[\mathfrak{c}] = [\mathfrak{b}_0]^{-1}$ in C_K. Dabei können wir

$$\mathfrak{a} \mid \mathfrak{c} \quad \text{und} \quad (\pi) \nmid \mathfrak{c}$$

erreichen (Übung). Nun gilt per Konstruktion $\mathfrak{a}^{-1} \cdot \mathfrak{c}^p = (\beta)$ für ein $\beta \in \mathfrak{o}_K$ und somit

$$\beta \cdot (x + \zeta_p^\nu y) \;=\; \pi \cdot (\mathfrak{c}\mathfrak{b}_\nu)^p \;\trianglelefteq\; \mathfrak{o}_K.$$

Wegen $p \nmid h_K$ folgt

$$\mathfrak{c}\mathfrak{b}_\nu \;=\; (\alpha_\nu) \quad \text{für ein} \quad \alpha_\nu \;\in\; \mathfrak{o}_K,$$

also

$$\beta \cdot (x + \zeta_p^\nu y) \;=\; \pi \cdot \epsilon_\nu \cdot \alpha_\nu^p \quad \text{mit} \quad \epsilon_\nu \;\in\; \mathfrak{o}_K^\times \quad \text{und} \quad \begin{cases} \pi^{n-1} \| \alpha_0, \\ \pi \nmid \alpha_1 \cdots \alpha_{p-1}. \end{cases}$$

Man beachte, dass $n > 1$ und somit $\pi \mid \alpha_0$ ist. Wenn wir eine neue Lösung unserer verallgemeinerten Fermat-Gleichung finden können, worin die Rolle von z durch α_0 ersetzt wird, sind wir fertig, da dies im Widerspruch zur Minimalität von n stehen würde. Bis auf eine lästige Einheit haben wir eine solche neue Lösung fast schon gefunden:

$$\begin{aligned} \alpha_1^p \;+\; \zeta_p \cdot \frac{\epsilon_{-1}}{\epsilon_1} \cdot \alpha_{-1}^p \quad &= \quad \frac{\beta(x + \zeta_p y)}{\pi \epsilon_1} + \frac{\beta(\zeta_p x + y)}{\pi \epsilon_1} \\ &= \quad (1 + \zeta_p) \cdot \frac{\beta(x + y)}{\pi \epsilon_1} \\ &= \quad \epsilon \cdot \alpha_0^p \quad \text{mit} \quad \epsilon \;=\; (1 + \zeta_p) \cdot \frac{\epsilon_0}{\epsilon_1} \;\in\; \mathfrak{o}_K^\times. \end{aligned}$$

Die Einheit ϵ auf der rechten Seite ist kein Problem, da wir diese bereits in unsere verallgemeinerte Kummer-Gleichung aufgenommen hatten. Wir sind daher fertig, wenn die Einheit $\zeta_p \cdot \epsilon_{-1}/\epsilon_1$ auf der linken Seite eine p-te Wurzel in $\mathfrak{o}_K^\times$ hat. Nun ist wegen

$$\alpha_1^p \;\equiv\; \alpha_{-1}^p \;\not\equiv 0 \mod p \quad \text{und} \quad \alpha_0^p \;\equiv\; 0 \mod p$$

offenbar

$$\zeta_p \cdot \frac{\epsilon_{-1}}{\epsilon_1} \;\equiv\; -1 \mod p,$$

und das im Anschluß an diesen Beweis diskutierte Lemma von Kummer zeigt, dass dann

$$\zeta \cdot \frac{\epsilon_{-1}}{\epsilon_1} \;=\; \eta^p \quad \text{für ein} \quad \eta \;\in\; \mathfrak{o}_K^\times$$

ist wie gewünscht. □

Am Ende des obigen Argumentes haben wir das sogenannte *Lemma von Kummer* benutzt, welches folgendes besagt:

Satz 3.6. *Sei $K = \mathbb{Q}(\zeta_p)$ für eine reguläre Primzahl $p \neq 2$. Wenn für eine Einheit $u \in \mathfrak{o}_K^\times$ eine ganze Zahl $a \in \mathbb{Z}$ existiert mit der Eigenschaft $u \equiv a \bmod p$, dann ist*

$$u \;=\; \eta^p \quad \textit{für ein} \quad \eta \;\in\; \mathfrak{o}_K^\times.$$

Beweisidee. Ein moderner, konzeptioneller Beweis dieser Aussage beruht auf Klassenkörpertheorie, hier kann daher nur skizzenhaft ein kurzer Ausblick gegeben werden: Zu jedem Zahlkörper K gibt es eine maximale abelsche und unverzweigte Erweiterung L/K, den sogenannten Hilbertschen Klassenkörper von K. Dieser besitzt die Eigenschaft, dass durch

$$C_K \;\xrightarrow{\sim}\; Gal(L/K), \quad [\mathfrak{p}] \;\mapsto\; Fr_{\mathfrak{p}}$$

ein Isomorphismus zwischen der Idealklassengruppe und der Galoisgruppe gegeben ist. Insbesondere gibt es also für Primzahlen $p \nmid h_K$ keine abelsche unverzweigte Erweiterung M/K vom Grad $[M : K] = p$.

Wir wenden dies auf $K = \mathbb{Q}(\zeta_p) \subseteq M = K(\sqrt[p]{u})$ an. Im Fall $\sqrt[p]{u} \notin K$ ist diese Erweiterung abelsch vom Grad

$$[M : K] \;=\; p,$$

und es bleibt nur nachzuprüfen, dass sie unverzweigt ist. Dies folgt aber aus unserer Voraussetzung $u \equiv a \bmod p$ mit $a \in \mathbb{Z}$ durch elementare Rechnung, Details finden sich etwa in [S. Lang, Cyclotomic Fields I and II, th. XIII.6.1]. □

KAPITEL VI

Diskriminanten und Verzweigung

Der Beweis von Satz V.3.6 (Kummer's Lemma) hat die Frage aufgeworfen, wie man die in einer gegebenen Erweiterung von Zahlkörpern verzweigten Primideale bestimmen kann. In diesem Kapitel werden wir sehen, dass

- eine Primzahl $p \in \{2, 3, 5, 7, \dots\}$ in einem Zahlkörper $K/\mathbb{Q}$ verzweigt ist genau dann, wenn sie die Diskriminante $d_K \in \mathbb{Z}$ teilt,
- allgemeiner für Erweiterungen K/k von Zahlkörpern zwar $\mathfrak{o}_K$ kein freier Modul über $\mathfrak{o}_k$ sein muß, aber *lokal* wie ein solcher aussieht,
- durch die entsprechenden lokalen Diskriminanten ein Ideal $\mathfrak{d}_{K/k} \trianglelefteq \mathfrak{o}_k$ definiert wird, das genau durch die verzweigten Primideale teilbar ist.

1. Der absolute Fall

Wir kehren wieder zum allgemeinen Setting von Kapitel IV zurück: Sei R ein Dedekind-Ring und $K/k = Quot(R)$ eine endliche separable Erweiterung. Nach Proposition II.4.3 ist

$$S \;=\; \big\{\, \alpha \in K \mid \alpha \text{ ist ganz über } R \,\big\}$$

wieder ein Dedekind-Ring:

$$\begin{array}{ccc} S & \hookrightarrow & K \\ | & & | \\ R & \hookrightarrow & k \end{array}$$

Sei jetzt $\mathfrak{p} \in \mathrm{Spm}(R)$ ein maximales Ideal. Wenn der Restklassenkörper $\mathbb{F}_\mathfrak{p} = R/\mathfrak{p}$ perfekt ist und der ganze Abschluß die Form $S = R[\alpha]$ mit $\alpha \in S$ besitzt, liefert die Formel von Dedekind in Satz IV.2.2 die folgenden Äquivalenzen, wobei $p_\alpha(x) \in R[x]$ das Minimalpolynom von α bezeichne:

$$\begin{array}{lcl} \mathfrak{p} \text{ verzweigt in } K/k & \iff & \text{Die Reduktion } \overline{p}_\alpha(x) \in \mathbb{F}_\mathfrak{p}[x] \\ & & \text{hat eine mehrfache Nullstelle in } \overline{\mathbb{F}}_\mathfrak{p} \\ & \iff & \text{Die Diskriminante von } \overline{p}_\alpha(x) \text{ ist Null} \\ & \iff & \text{Es ist } \mathfrak{p} \mid d_{K/k}(\alpha) = \displaystyle\prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \end{array}$$

Es gibt allerdings Beispiele, in welchen die Formel von Dedekind nicht anwendbar ist, das erste Beispiel stammt von ihm selbst:

Beispiel 1.1. Sei $\alpha \in \mathbb{C}$ eine Nullstelle von $f(x) = x^3 + x^2 - 2x + 8 \in \mathbb{Z}[x]$, und sei $K = \mathbb{Q}(\alpha)$. Dann ist

$$2 \mid [\mathfrak{o}_K : \mathbb{Z}[\beta]] \quad \text{für alle} \quad \beta \in \mathfrak{o}_K \setminus \mathbb{Z}.$$

Tatsächlich kann man nachprüfen, dass hier $2\mathfrak{o}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ ein Produkt von drei verschiedenen Primidealen ist. Da es nur zwei normierte lineare Polynome in $\mathbb{F}_2[x]$ gibt, kann ein Polynom vom Grad drei in $\mathbb{F}_2[x]$ niemals in paarweise verschiedene Linearfaktoren zerfallen. Daher kann das Kriterium von Dedekind hier niemals anwendbar sein, und es folgt $2 \mid [\mathfrak{o}_K : \mathbb{Z}[\beta]]$ für alle $\beta \in \mathfrak{o}_K \setminus \mathbb{Z}$.

Trotz solcher negativer Beispiele stellt sich heraus, dass die Diskriminante eines Zahlkörpers immer genau durch die verzweigten Primzahlen teilbar ist. Um dies allgemeiner zu formulieren, erinnern wir zunächst daran, dass S immer ein endlich erzeugter torsionsfreier R-Modul ist. Ist R ein Hauptidealring, beispielsweise $R = \mathbb{Z}$, so folgt

$$S \;=\; \bigoplus_{i=1}^{n} R \cdot \alpha_i \quad \text{für geeignete} \quad \alpha_1, \ldots, \alpha_n \;\in\; R,$$

die wir wie üblich auch als Ganzheitsbasis bezeichnen. Für den Beweis unseres Verzweigungskriteriums wird es hilfreich sein, einige Definitionen allgemeiner für beliebige Erweiterungen kommutativer Ringe mit dieser Eigenschaft zu fassen:

Definition 1.2. Sei $A \subset B$ eine Erweiterung kommutativer Ringe, sodass B ein freier A-Modul von endlichem Rang ist. Für Elemente $\beta \in B$ betrachten wir die Abbildung

$$m_\beta : \quad B \longrightarrow B, \quad b \mapsto \beta \cdot b$$

als Matrix in $\mathrm{Mat}_{n\times n}(A)$ mittels eines fest gewählten Isomorphismus $B \simeq A^n$ und definieren

$$tr_{B/A}(\beta) \;=\; tr_{B/A}(m_\beta) \;\in\; A$$

als die Spur dieser Matrix. Diese Spur hängt nicht vom gewählten Isomorphismus ab, denn je zwei verschiedene solche Isomorphismen werden durch Konjugation mit einer Matrix

$$\begin{aligned} M \;\in\; Gl(A) \;&=\; \big\{N \in \mathrm{Mat}_{n\times n}(A) \mid NN' = N'N = 1 \text{ für ein } N' \in \mathrm{Mat}_{n\times n}(A)\big\} \\ &=\; \big\{N \in \mathrm{Mat}_{n\times n}(A) \mid \det(N) \in A^\times\big\} \end{aligned}$$

ineinander überführt; die zweite Gleichung folgt aus der Cramer'schen Formel. Für beliebige $\alpha_1, \ldots, \alpha_n \in S$ erhalten wir die *Diskriminante*

$$d_{B/A}(\alpha_1, \ldots, \alpha_n) \;=\; \det\big(tr_{B/A}(\alpha_i\alpha_j)\big) \;\in\; R$$

und definieren das *Diskriminantenideal*

$$\mathfrak{d}_{B/A} \;=\; (d_{B/A}(\alpha_1, \ldots, \alpha_n)) \;\trianglelefteq\; A$$

als das Hauptideal, das von der Diskriminante einer beliebigen Basis $\alpha_1, \ldots, \alpha_n$ des freien A-Moduls B erzeugt wird. Man beachte, dass sich die Diskriminanten von je zwei solchen Basen nur um das Quadrat einer Einheit $\det(M) \in A^\times$ unterscheiden und $\mathfrak{d}_{B/A}$ somit nicht von der gewählten Basis abhängt.

Lemma 1.3. *Für $A \subseteq B$ wie oben gilt:*

(1) *Ist $\mathfrak{a} \trianglelefteq A$ ein Ideal, dann ist $\overline{B} = B/\mathfrak{a}B$ ein freier Modul über $\overline{A} = A/\mathfrak{a}$ und*

$$\begin{aligned} \overline{d_{B/A}(\alpha_1, \ldots, \alpha_n)} \;&=\; d_{\overline{B}/\overline{A}}(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) \;\in\; \overline{A} \quad \textit{für} \quad \alpha_i \in B, \\ \overline{\mathfrak{d}_{B/A}} \;&=\; \mathfrak{d}_{\overline{B}/\overline{A}}. \end{aligned}$$

(2) *Ist $B = B_1 \times B_2$ ein Produkt zweier A-Algebren B_i, die freie A-Moduln sind, dann gilt*

$$\mathfrak{d}_{B/A} \;=\; \mathfrak{d}_{B_1/A} \cdot \mathfrak{d}_{B_2/A}.$$

Beweis. (1) Für $B = \bigoplus_{i=1}^n A \cdot \alpha_i$ ist offenbar $\overline{B} = \bigoplus_{i=1}^n \overline{A} \cdot \overline{\alpha}_1$ und somit ist der Quotientenring ebenfalls ein freier Modul. Die Kompatibilität der Diskriminante mit der Quotientenabbildung folgt dann durch Reduktion von Matrizeneinträgen modulo $\mathfrak{a}$, was offenbar kompatibel mit der Spur ist.

(2) Der Produktring $B = B_1 \times B_2$ besitzt als A-Modul eine Basis $\alpha_1, \ldots, \alpha_n$ mit der Eigenschaft, dass

- $\alpha_1, \ldots, \alpha_m$ eine Basis des Untermoduls $B_1 \times \{0\} \subset B$ sind,
- $\alpha_{m+1}, \ldots, \alpha_n$ eine Basis des Untermoduls $\{0\} \times B_2 \subset B$ sind.

In dieser Basis hat die Matrix

$$\big(tr_{B/A}(\alpha_i\alpha_j)\big) \;=\; \begin{pmatrix} tr_{B/A}(\alpha_i\alpha_j)_{i,j\le m} & 0 \\ 0 & tr_{B/A}(\alpha_i\alpha_j)_{i,j>m} \end{pmatrix}$$

Blockform wegen $\alpha_i\alpha_j = 0$ für $i \le m < j$, und somit folgt die Behauptung. □

Nach diesen allgemeinen Bemerkungen kommen wir jetzt wieder zu unserem ursprünglichen Setting zurück: Sei R ein Dedekind-Ring und S sein ganzer Abschluß in einer endlichen separablen Erweiterung $K/k = Quot(R)$. Wie immer setzen wir voraus, dass die Restklassenkörper $R/\mathfrak{p}$ für alle maximalen Ideale $\mathfrak{p} \in \mathrm{Spm}(R)$ perfekt sind.

Satz 1.4. *Sei $\mathfrak{p} \in \mathrm{Spm}(R)$. Wenn der ganze Abschluß S ein freier R-Modul ist, dann gilt:*

$$\mathfrak{p} \text{ ist verzweigt in } S/R \quad\Longleftrightarrow\quad \mathfrak{p} \mid \mathfrak{d}_{S/R}$$

Beweis. Es ist $\overline{S} = S/\mathfrak{p}S$ ein freier Modul über $\overline{R} = R/\mathfrak{p}$, und das obige Lemma zeigt

$$\begin{aligned} \mathfrak{p} \mid \mathfrak{d}_{S/R} \quad &\Longleftrightarrow\quad \overline{\mathfrak{d}_{S/R}} \;=\; 0 \\ &\Longleftrightarrow\quad \mathfrak{d}_{\overline{S}/\overline{R}} \;=\; 0 \\ &\Longleftrightarrow\quad \mathfrak{d}_{(S/\mathfrak{P}^e)/\overline{R}} \;=\; 0 \quad \text{für mindestens ein } \mathfrak{P} \mid \mathfrak{p} \text{ und } e = e_{\mathfrak{P}|\mathfrak{p}}, \end{aligned}$$

wobei die letzte Äquivalenz aus dem chinesischen Restsatz folgt. Wir behaupten, dass die letzte Bedingung äquivalent zu $e > 1$ ist und damit genau dann eintritt, wenn das Primideal $\mathfrak{p}$ verzweigt: Denn im unverzweigten Fall ist $S/\mathfrak{P}^e = S/\mathfrak{P}$ ein Körper, und eine separable Erweiterung von $R/\mathfrak{p}$ wegen der Perfektheit, also ist die Spurform

$$(S/\mathfrak{P}) \times (S/\mathfrak{P}) \;\longrightarrow\; R/\mathfrak{p}, \quad (a,b) \;\mapsto\; tr(ab)$$

nichtausgeartet und

$$\mathfrak{d}_{(S/\mathfrak{P})/\overline{R}} \;\neq\; 0.$$

Ist andererseits $e > 1$, dann enthält der Quotientenring $S/\mathfrak{P}^e$ nilpotente Elemente; wählt man in

$$S/\mathfrak{P}^e \;=\; \bigoplus_{i=1}^n \overline{R} \cdot \overline{\alpha}_i$$

den ersten Basisvektor $\overline{\alpha}_1$ nilpotent, dann ist die Multiplikation mit $\overline{\alpha}_1\overline{\alpha}_i$ ein nilpotenter Endomorphismus und somit

$$tr(\overline{\alpha}_1\overline{\alpha}_j) \;=\; 0 \quad \text{für alle} \quad j.$$

Aber dann verschwindet die erste Zeile der Spurmatrix $(tr(\overline{\alpha}_i\overline{\alpha}_j))$ und somit auch ihre Determinante $d_?(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$ und das hiervon erzeugte Hauptideal $\mathfrak{d}$. □

KOROLLAR 1.5. *Sei $K/\mathbb{Q}$ ein beliebiger Zahlkörper. Für Primzahlen p gilt dann die Äquivalenz:*

$$p \text{ ist verzweigt in } K \quad \Longleftrightarrow \quad p \mid d_K.$$

Insbesondere gibt es keine unverzweigte endliche Erweiterung $K/\mathbb{Q}$.

Beweis. Nach Korollar III.3.3 aus der Minkowski-Schranke wissen wir $|d_K| > 1$ für alle $K \neq \mathbb{Q}$, das vorige Korollar liefert also die Behauptung. □

Wenn wir das obige Verzweigungskriterium vom absoluten Fall $k = \mathbb{Q}$ auf den relativen Fall beliebiger Erweiterungen K/k von Zahlkörpern ausdehnen wollen, ergibt sich das Problem, dass $\mathfrak{o}_K$ zwar ein endlich erzeugter und torsionsfreier, aber im Allgemeinen kein freier Modul über dem Ganzheitsring $\mathfrak{o}_k$ ist. Beispielsweise ist dies für

$$K \;=\; \mathbb{Q}(\sqrt{2}, \sqrt{-6}) \;\supset\; k \;=\; \mathbb{Q}(\sqrt{-6})$$

nicht der Fall, wie wir in den Übungsaufgaben sehen werden. Man beachte, dass hier $\mathfrak{o}_k = \mathbb{Z}[\sqrt{-6}]$ kein Hauptidealring ist; bekanntlich ist jeder endlich erzeugte torsionsfreie Modul über einem Hauptidealring frei. Im nächsten Abschnitt werden wir zeigen, dass Dedekind-Ringe sich *lokal* wie Hauptidealringe verhalten, und damit eine völlig neue Perspektive gewinnen.

2. Lokalisierung und Bewertungen

Der Grund für die Kompliziertheit von Zahlringen ist die Interaktion zwischen ihren verschiedenen maximalen Idealen. Gäbe es nur ein solches Ideal, dann wäre die Situation einfach:

LEMMA 2.1. *Jeder Dedekind-Ring R mit nur einem maximalen Ideal $\mathfrak{p} \in \operatorname{Spm}(R)$ ist ein Hauptidealring.*

Beweis. Wegen der Eindeutigkeit der Primfaktorzerlegung für Ideale von R hat man eine strikte Inklusion $\mathfrak{p}^2 \subset \mathfrak{p}$. Es gibt also ein $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ und wir behaupten, dass dann $\mathfrak{p} = (\pi)$ gilt: In der Tat ist einerseits $\mathfrak{p} \mid (\pi)$, andererseits aber $\mathfrak{p}^2 \nmid (\pi)$, und hieraus folgt die Behauptung, weil jedes von Null verschiedene Ideal eine Potenz des eindeutigen maximalen Ideals $\mathfrak{p}$ sein muß. Aus demselben Grund ist dann jedes Ideal von R ein Hauptideal. □

Ringe mit nur einem maximalen Ideal werden auch als *lokale Ringe* bezeichnet; die geometrische Motivation für diese Sprechweise werden wir im nächsten Kapitel diskutieren. Unser Ziel ist es nun, für beliebige Dedekind-Ringe R und ein maximales Ideal $\mathfrak{p} \in \operatorname{Spm}(R)$ mit Gewalt einen lokalen Ring $R_\mathfrak{p}$ zu konstruieren, indem wir alle Elemente der Menge

$$\Sigma \;=\; R \setminus \mathfrak{p}$$

zu Einheiten machen. Dies ist eine allgemeine Konstruktion:

DEFINITION 2.2. Sei A ein Integritätsring. Eine Teilmenge $\Sigma \subseteq A \setminus \{0\}$ wird als *multiplikativ abgeschlossen* bezeichnet, wenn $1 \in \Sigma$ ist und für alle $s_1, s_2 \in \Sigma$ auch $s_1 s_2 \in \Sigma$ ist. Dann ist

$$\Sigma^{-1}A \;=\; \big\{ a/s \in \operatorname{Quot}(A) \mid a \in A,\ s \in \Sigma \big\}$$

ein Teilring des Quotientenkörpers, die sogenannte *Lokalisierung* von A an Σ. Für Primideale $\mathfrak{p} \trianglelefteq R$ ist das Komplement $\Sigma = A \setminus \mathfrak{p}$ eine multiplikative Teilmenge und wir bezeichnen

$$A_\mathfrak{p} \;=\; (A \setminus \mathfrak{p})^{-1} A$$

auch als die *Lokalisierung* an dem gegebenen Primideal.

Beispielsweise erhält man durch Lokalisierung am Nullideal $A_{(0)} = \mathrm{Quot(A)}$. Ist andererseits $\mathfrak{p} \trianglelefteq A$ ein maximales Ideal, dann ist $A_{\mathfrak{p}}$ ein lokaler Ring mit dem eindeutigen maximalen Ideal

$$\mathfrak{p}A_{\mathfrak{p}} \trianglelefteq A_{\mathfrak{p}}.$$

In der Tat ist dies eine unmittelbare Konsequenz aus der Aussage (2) des folgenden Lemmas, wobei $\mathrm{Spec}(B)$ die Menge der Primideale von B bezeichnet:

LEMMA 2.3. *Sei $\Sigma \subseteq A\setminus\{0\}$ eine multiplikative Teilmenge und $A \hookrightarrow B = \Sigma^{-1}A$ die Lokalisierung. Dann gilt:*

(1) *Die Abbildung*

$$\big\{\mathit{Ideale}\ \mathfrak{b} \trianglelefteq B\big\} \hookrightarrow \big\{\mathit{Ideale}\ \mathfrak{a} \trianglelefteq A\big\}, \quad \mathfrak{b} \mapsto \mathfrak{a} = \mathfrak{b} \cap A,$$

ist injektiv und erhält die Inklusionsrelation von Idealen.

(2) *Für Primideale liefert dies eine Bijektion*

$$\mathrm{Spec}(B) \xrightarrow{\sim} \big\{\, \mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap \Sigma = \varnothing \,\big\}$$

mit Umkehrabbildung $\mathfrak{p} \mapsto \mathfrak{q} = \mathfrak{p} \cdot B \in \mathrm{Spec}(B)$.

Beweis. (1) Dass $\mathfrak{b} \mapsto \mathfrak{b} \cap A$ eine inklusionserhaltende Injektion ist, folgt aus der Umkehrformel

$$\mathfrak{b} = (\mathfrak{b} \cap A) \cdot B \quad \text{für} \quad \mathfrak{b} \trianglelefteq B.$$

Hierbei ist $\supseteq$ klar, für die umgekehrte Inklusion beachte man, dass jedes $b \in \mathfrak{b}$ als Element der Lokalisierung die Form $b = a/s$ mit $a \in A$ und $s \in \Sigma$ hat. Wegen $\mathfrak{b} \trianglelefteq B$ ist dabei $a = s \cdot b \in \mathfrak{b} \cap A$ und somit

$$b = sb \cdot s^{-1} \in (\mathfrak{b} \cap A) \cdot B$$

wie gewünscht. Es bleibt die Behauptung über Primideale zu zeigen.

(2) Für $\mathfrak{q} \in \mathrm{Spec}(B)$ ist offenbar $\mathfrak{p} = \mathfrak{q} \cap A \in \mathrm{Spec}(A)$ prim. Es ist $\mathfrak{p} \cap \Sigma = \varnothing$, weil sonst das Primideal $\mathfrak{q}$ wegen

$$\Sigma \subseteq B^\times$$

eine Einheit enthalten müsste. Sei jetzt umgekehrt $\mathfrak{p} \in \mathrm{Spec}(A)$ mit $\mathfrak{p} \cap \Sigma = \varnothing$ gegeben. Dann ist

$$\mathfrak{q} := \mathfrak{p} \cdot S = \Big\{\textstyle\sum_i \frac{p_i}{s_i} \mid p_i \in \mathfrak{p}, s_i \in \Sigma\Big\} = \big\{\tfrac{p}{s} \mid p \in \mathfrak{p}, s \in \Sigma\big\},$$

wie man durch Multiplikation der Elemente mit einem gemeinsamen Nenner leicht sieht. Insbesondere ist $\mathfrak{q} \neq S$ wegen $\mathfrak{p} \cap \Sigma = \varnothing$. Ebenso folgt, dass $\mathfrak{q}$ ein Primideal ist: Aus

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s} \quad \text{mit} \quad (a_i, s_i) \in A \times \Sigma \quad \text{und} \quad (p, s) \in \mathfrak{p} \times \Sigma$$

folgt $s \cdot a_1a_2 = s_1s_2 \cdot p \in \mathfrak{p}$ und somit a_i für mindestens ein $i \in \{1, 2\}$, denn $\mathfrak{p}$ ist prim und es gilt

$$s \notin \mathfrak{p} \quad \text{wegen} \quad \mathfrak{p} \cap \Sigma = \varnothing.$$

Also ist $\mathfrak{q}$ ein Primideal und man prüft leicht nach, dass $\mathfrak{p} = \mathfrak{q} \cap A$ ist. □

BEISPIEL 2.4. Für $A = \mathbb{Z}$ und Primzahlen p ist $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b\}$. Dieser lokale Ring ist ein Hauptidealring: Jedes von Null verschiedene Ideal darin besitzt die Form

$$p^\nu \cdot \mathbb{Z}_{(p)} \trianglelefteq \mathbb{Z}_{(p)} \quad \text{für ein} \quad \nu \in \mathbb{N}_0,$$

wie man durch Betrachten der kleinsten in allen Elementen des Ideals auftretenden Vielfachheit von p sieht, denn jede zu p teilerfremde ganze Zahl wird eine Einheit in $\mathbb{Z}_{(p)}$. Die Umkehrformel aus (1) besagt hier $(p^\nu \cdot \mathbb{Z}_{(p)}) \cap \mathbb{Z} = p^\nu\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Eine analoge Situation hat man allgemeiner für lokale Ringe $A_\mathfrak{p}$ zu maximalen Idealen $\mathfrak{p}$ von Dedekind-Ringen A. Dazu sei bemerkt, dass jede Lokalisierung eines Dedekind-Ringes wieder ein solcher ist:

LEMMA 2.5. *Sei A ein Integritätsring, $\Sigma \subseteq A\setminus\{0\}$ multiplikativ und $B = \Sigma^{-1}A$. Dann gilt:*

(1) *Ist A Noethersch, so auch B.*

(2) *Ist A ganz abgeschlossen, so auch B.*

(3) *Es ist* $\dim(B) \leq \dim(A)$.

Ist also A ein Dedekind-Ring, dann ist B ein Dedekind-Ring oder $B = Quot(A)$.

Beweis. (1) Der Schnitt einer unendlichen aufsteigenden Kette von Idealen in B ist eine aufsteigende Kette von Idealen in A. Wenn A Noethersch ist, wird letztere stationär. Dann zeigt die Umkehrformel im Beweis von Teil (1) des vorigen Lemmas, dass schon die Idealkette in B stationär wird.

(2) Sei $\beta \in Quot(B)$ und $\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta + b_0 = 0$ mit $b_\nu \in B$. Dann hat man

$$b_\nu \;=\; \frac{a_\nu}{s_\nu} \quad \text{mit} \quad a_\nu \;\in\; A,\; s_\nu \;\in\; \Sigma.$$

Für $s = s_0 \cdots s_{n-1}$ gilt

$$\begin{aligned} c_\nu \;&=\; s^{n-\nu}\cdot b_\nu \;\in\; A \quad \text{für} \quad \nu = 0, 1, \ldots, n-1, \\ \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 \;&=\; 0 \quad \text{für} \quad \alpha = s\cdot\beta \;\in\; Quot(B). \end{aligned}$$

Da A ganz abgeschlossen ist mit $Quot(A) = Quot(B)$, folgt $\alpha \in A$ und somit wie gewünscht $\beta = s^{-1}\alpha \in B$.

(3) ist klar nach Teil (2) des vorigen Lemmas. Ist nun A ein Dedekind-Ring, so folgt insgesamt, dass auch die Lokalisierung B ein Dedekind-Ring oder ein Körper ist, und im Körperfall muß offenbar $B = Quot(A)$ sein. □

KOROLLAR 2.6. *Ist A ein Dedekind-Ring und $\mathfrak{p} \in \mathrm{Spm}(A)$, dann ist der lokale Ring $A_\mathfrak{p}$ ein Hauptidealring.*

Beweis. Nach dem obigen Lemma ist $A_\mathfrak{p}$ ebenfalls ein Dedekind-Ring, und nach Lemma 2.1 ist jeder lokale Dedekind-Ring ein Hauptidealring. □

Lokale Hauptidealringe werden auch als *diskrete Bewertungsringe* bezeichnet, ihre Teilbarkeitstheorie ist sehr einfach: Ist A ein solcher Ring und $\pi \in A$ ein Erzeuger seines maximalen Ideals, so schreibt sich jedes $a \in Quot(A)\setminus\{0\}$ eindeutig als $a = \epsilon\cdot\pi^\nu$ mit $\epsilon \in A^\times$ und $\nu = \nu(a) \in \mathbb{Z}$. Die durch den Exponenten gegebene Funktion

$$\nu: \quad A\setminus\{0\} \;\longrightarrow\; \mathbb{Z}$$

ist eine *diskrete Bewertung* im Sinn der folgenden Definition:

DEFINITION 2.7. Eine *Bewertung* (oder *Exponentialbewertung*) eines Körpers K ist eine Funktion $K^\times \xrightarrow{\nu} \mathbb{R}$, die nicht konstant ist und

$$\begin{aligned} \nu(ab) \;&=\; \nu(a) + \nu(b), \\ \nu(a+b) \;&\geq\; \min\{\nu(a), \nu(b)\} \end{aligned}$$

für alle $a, b \in K^\times$ erfüllt. Mittels $\nu(0) := \infty$ setzt man diese zu $\nu : K \to \mathbb{R}\cup\{\infty\}$ fort. Dann wird durch

$$\{\,\alpha \in K \mid \nu(\alpha) \geq 0\,\}$$

ein Teilring von K definiert, der sogenannte *Bewertungsring von* v. Das Bild $v(K^\times)$ ist eine additive Untergruppe der reellen Zahlen, die *Wertegruppe von* v. Ist diese Untergruppe diskret, so heißt v eine *diskrete Bewertung*.

BEISPIEL 2.8. Sei A ein Dedekind-Ring. Für $0 \neq \alpha \in K = Quot(A)$ zerlegt sich das hiervon erzeugte gebrochene Ideal eindeutig als ein endliches Produkt von Primidealpotenzen

$$(\alpha) \;=\; \prod_{\mathfrak{p} \in \operatorname{Spm}(A)} \mathfrak{p}^{\nu_\mathfrak{p}(\alpha)} \qquad \text{mit Exponenten} \qquad \nu_\mathfrak{p}(\alpha) \in \mathbb{Z}.$$

Für jedes feste $\mathfrak{p} \in \operatorname{Spm}(A)$ ist dann

$$\nu_\mathfrak{p} : \quad K^\times \longrightarrow \mathbb{Z}$$

eine diskrete Bewertung, die sogenannte $\mathfrak{p}$-*adische Bewertung*. Ihr Bewertungsring ist die Lokalisierung

$$A_\mathfrak{p} \stackrel{!}{=} \big\{\alpha \in K \mid \nu_\mathfrak{p}(\alpha) \geq 0\big\}.$$

Die Idealtheorie von Dedekind-Ringen lässt sich daher äquivalent auch komplett in bewertungstheoretischer Sprache formulieren; dieser Standpunkt ist von zentraler Bedeutung für die moderne Zahlentheorie, seine mächtigen Anwendungen etwa in der Klassenkörpertheorie würden aber den Rahmen dieser Vorlesung sprengen und wir beschränken uns daher auf einen kurzen Ausblick im nächsten Kapitel.

3. Relative Diskriminanten

Zum Abschluß dieses Kapitels sei noch kurz erklärt, wie die soeben eingeführten Lokalisierungen eine Verallgemeinerung des Verzweigungskriteriums für beliebige Erweiterungen von Zahlkörpern erlauben. Wir nehmen die Situation von Abschnitt 1 wieder auf, d.h. R sei ein Dedekind-Ring und S sein ganzer Abschluß in einer endlichen separablen Erweiterung K von $k = Quot(R)$. Im Gegensatz zur vorigen Diskussion wollen wir aber nun nicht mehr voraussetzen, dass S ein freier R-Modul sei, und machen daher die folgende

DEFINITION 3.1. Das *Diskriminantenideal* der Erweiterung S/R ist definiert als das Ideal

$$\mathfrak{d}_{S/R} \;=\; \big\langle\, d_{S/R}(\alpha_1, \ldots, \alpha_n) \mid (\alpha_1, \ldots, \alpha_n) \in \mathscr{B}_{S/R} \,\big\rangle \;\trianglelefteq\; R$$

erzeugt von den Diskriminanten aller Basen in

$$\mathscr{B}_{S/R} \;=\; \big\{\, (\alpha_1, \ldots, \alpha_n) \in S^n \text{ Basis der Körpererweiterung } K/k \,\big\}.$$

Falls S ein freier R-Modul ist, stimmt dies mit unserer vorigen Definition überein, da eine Modulbasis insbesondere auch eine Basis der Körpererweiterung ist und ihre Diskriminante diejenige jeder anderen Basis in $\mathscr{B}_{S/R}$ teilt (Übung). Die obige Definition gilt jedoch ganz allgemein. Unser Beweis des Verzweigungskriteriums im allgemeinen Fall wird sich mittels des folgenden Lemmas auf den bereits bekannten Fall freier Moduln reduzieren:

LEMMA 3.2. *Sei* $\Sigma \subseteq R \setminus \{0\}$ *eine multiplikativ abgeschlossene Teilmenge. Dann gilt*

$$\mathfrak{d}_{S/R} \cdot \Sigma^{-1}R \;=\; \mathfrak{d}_{\Sigma^{-1}S/\Sigma^{-1}R}.$$

Beweis. Die Multiplikation mit beliebigen Skalaren aus der Teilmenge $\Sigma \subset k^\times$ berührt die Eigenschaft nicht, eine Basis von K/k zu sein. Somit gilt offenbar die Identität

$$\mathscr{B}_{\Sigma^{-1}S/\Sigma^{-1}R} \stackrel{!}{=} \{s^{-1} \cdot (\alpha_1, \ldots, \alpha_n) \mid s \in \Sigma, (\alpha_1, \ldots, \alpha_n) \in \mathscr{B}_{R/S}\} \;=\; \Sigma^{-1} \cdot \mathscr{B}_{R/S}$$

und wegen

$$d_{\Sigma^{-1}S/\Sigma^{-1}R}(s^{-1}\alpha_1,\ldots,s^{-1}\alpha_n) \;=\; s^{-2n}\cdot d_{S/R}(\alpha_1,\ldots,\alpha_n)$$

für $(\alpha_1,\ldots,\alpha_n)\in\mathscr{B}_{S/R}$ und $s\in\Sigma$ folgt die Behauptung. □

Diese Lokalisierungseigenschaft führt auf die folgende Verallgemeinerung des Verzweigungskriteriums:

SATZ 3.3. *Für* $\mathfrak{p}\in\operatorname{Spm}(R)$ *gilt:*

$$\mathfrak{p} \textit{ ist verzweigt in } S/R \quad\Longleftrightarrow\quad \mathfrak{p}\mid\mathfrak{d}_{S/R}$$

Beweis. Durch Lokalisierung an der multiplikativen Teilmenge $\Sigma=R\setminus\mathfrak{p}$ erhält man die Ringe $R_\mathfrak{p}\subseteq S_\mathfrak{p}=\Sigma^{-1}S$. Nach Lemma 2.5 sind dies Dedekind-Ringe und erfüllen ebenfalls die Annahmen dieses Kapitels. Außerdem ist aber $R_\mathfrak{p}$ als diskreter Bewertungsring ein Hauptidealring. Da jeder endlich erzeugte torsionsfreie Modul über einem Hauptidealring frei ist, ist folglich $S_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul. Wir erhalten nun

$$\begin{aligned}
\mathfrak{p}\text{ verzweigt in }S/R &\iff \mathfrak{p}\cdot S_\mathfrak{p}\text{ verzweigt in }S_\mathfrak{p}/R_\mathfrak{p}\quad(\text{wegen } S/\mathfrak{p}S\simeq S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p})\\
&\iff \mathfrak{p}\cdot R_\mathfrak{p}\mid\mathfrak{d}_{S_\mathfrak{p}/R_\mathfrak{p}}\quad(\text{Satz 1.4 für den freien } R_\mathfrak{p}\text{-Modul } S_\mathfrak{p})\\
&\iff \mathfrak{p}\mid\mathfrak{d}_{S/R}\quad(\text{weil } \mathfrak{d}_{S/R}\cdot R_\mathfrak{p}=\mathfrak{d}_{S_\mathfrak{p}/R_\mathfrak{p}}\text{ nach Lemma 3.2})
\end{aligned}$$

und somit folgt die Behauptung. □

KAPITEL VII

Lokale Körper

In diesem Kapitel werden wir die soeben eingeführten lokalen Techniken weiter ausbauen. Dabei werden wir

- einen topologischen Zugang zu Bewertungen entwickeln,
- von lokalen Ringen zu ihrer Vervollständigung übergehen,
- mit Hensels Lemma ein Kriterium zur Lösbarkeit von Gleichungen durch Potenzreihen kennenlernen.

1. Bewertungen

Der im vorigen Kapitel eingeführte Begriff der *Lokalisierung* kommt aus der algebraischen Geometrie, ist jedoch für ein lokales Arbeiten im Sinne der Analysis noch nicht fein genug. Um dies einzusehen, betrachten wir als konkretes Beispiel die Projektionsabbildung

$$f: \quad V := \{(x,y) \in \mathbb{R}^2 \mid y^2 = x+1\} \longrightarrow \mathbb{R}, \quad (x,y) \mapsto x.$$

Die Jacobi-Determinante dieser Abbildung im Punkt $(x,y) = (0,1)$ ist von Null verschieden, somit ist diese Abbildung in einer kleinen Umgebung dieses Punktes umkehrbar. Im Gegensatz zu f ist die lokale Umkehrfunktion aber nicht durch Polynome gegeben, verlässt also die Welt der algebraischen Geometrie. Sie besitzt jedoch die Potenzreihenentwicklung

$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{x^2}{8} + \cdots \in \mathbb{C}[[x]],$$

statt Lokalisierungen des Koordinatenringes im Sinne des vorigen Kapitels sollten wir also diesen Potenzreihenring betrachten. Der Übergang von einem Polynomen zu Potenzreihen ist ein Beispiel für den Prozess der *Vervollständigung*, den wir in diesem Kapitel diskutieren werden. Ein weiteres Beispiel ist der Übergang von $\mathbb{Q}$ zu $\mathbb{R}$, der für die Konvergenz von Cauchy-Folgen in der Analysis essentiell ist. Beide werden später Pate stehen für die Konstruktion eines Körpers $\mathbb{Q}_p$ der p-adischen Zahlen, dessen Elemente Potenzreihen

$$c_0 + c_1 \cdot p + c_2 \cdot p^2 + \cdots \quad \text{mit Koeffizienten} \quad c_n \in \{0,1,\ldots,p-1\}$$

sind und in der Zahlentheorie eine große Rolle spielen. Um derartige Potenzreihen studieren zu können, müssen wir zunächst etwas Bewertungstheorie entwickeln.

Um von der Konvergenz einer Reihe in einem Körper zu sprechen, brauchen wir ein Maß für die Größe der Restglieder:

Definition 1.1. Sei K ein Körper. Eine *Bewertung* von K ist eine auf $K^\times$ nicht konstante Abbildung

$$|\cdot|: \quad K \longrightarrow \mathbb{R}_{\geq 0},$$

sodass für alle $a, b \in K$ gilt:

(1) Es ist $|a| = 0$ genau für $a = 0$ (Definitheit).

(2) Es ist $|ab| = |a| \cdot |b|$ (Multiplikativität).

(3) Es ist $|a+b| \leq |a| + |b|$ (Dreiecksungleichung).

Man bezeichnet die Bewertung als *nichtarchimedisch*, wenn in (3) sogar die scharfe Dreiecksungleichung

$$|a+b| \leq \max\{|a|, |b|\}$$

gilt. Ist dies nicht der Fall, so bezeichnet man die Bewertung als *archimedisch*.

Beispielsweise ist der übliche Absolutbetrag $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$ eine archimedische Bewertung der reellen Zahlen. Tatsächlich ist die Terminologie motiviert durch das archimedische Axiom für die reellen Zahlen:

LEMMA 1.2. *Sei K ein Körper, und für $n \in \mathbb{N}$ bezeichne $n \cdot 1_K = 1_K + \cdots + 1_K$ die n-fache Summe seines Einselementes. Eine Bewertung*

$$|\cdot| : \quad K \longrightarrow \mathbb{R}_{\geq 0}$$

ist archimedisch genau dann, wenn die Menge aller $|n \cdot 1_K| \in \mathbb{R}_{\geq 0}$ beschränkt ist.

Beweis. Im nichtarchimedischen Fall liefert die scharfe Dreiecksungleichung die obere Schranke $|n \cdot 1_K| \leq |1_K|$ für alle $n \in \mathbb{N}$. Sei umgekehrt eine Schranke $c \in \mathbb{R}_{\geq 0}$ gegeben mit

$$|n \cdot 1_K| \ \leq \ c \quad \text{für alle} \quad n \ \in \ \mathbb{N}.$$

Für $a, b \in K$ folgt

$$\begin{aligned} |a+b|^n &= \Big| \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu} \Big| \\ &\leq \sum_{\nu=0}^{n} \Big| \binom{n}{\nu} \cdot 1_K \Big| \cdot |a|^\nu |b|^{n-\nu} \\ &\leq \sum_{\nu=0}^{n} c \cdot |a|^\nu |b|^{n-\nu} \ \leq \ (n+1) \cdot c \cdot \max\{|a|, |b|\}^n \end{aligned}$$

und somit

$$|a+b| \ \leq \ \sqrt[n]{c \cdot (n+1)} \cdot \max\{|a|, |b|\}$$

für alle $n \in \mathbb{N}$. Hieraus erhält man wie gewünscht die scharfe Dreiecksungleichung durch den Grenzübergang $n \to \infty$. □

BEISPIEL 1.3. Sei K ein Körper.

(1) Jede Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ liefert eine archimedische Bewertung von K mittels

$$|a|_\sigma \ := \ |\sigma(a)| \quad \text{für} \quad a \ \in \ K.$$

(2) Ist $\nu : K \to \mathbb{R} \cup \{\infty\}$ eine Exponentialbewertung (vgl. Definition VI.2.7), dann erhält man für jede feste Zahl $c \in (0,1)$ eine nichtarchimedische Bewertung durch

$$|a| \ := \ \begin{cases} c^{\nu(a)} & \text{für } a \in K^\times, \\ 0 & \text{für } a = 0. \end{cases}$$

Umgekehrt liefert jede nichtarchimedische Bewertung $|\cdot| : K \to \mathbb{R}_{\geq 0}$ und jedes $c \in (0,1)$ eine Exponentialbewertung via

$$\nu(a) \ := \ \begin{cases} \log_c |a| & \text{für } a \in K^\times, \\ \infty & \text{für } a = 0. \end{cases}$$

Es stellt sich natürlich die Frage, inwieweit die Bewertung in (2) von der Wahl der Konstanten $c \in (0,1)$ abhängt. Offenbar führen je zwei verschiedene Wahlen zu äquivalenten Bewertungen im folgenden Sinn:

DEFINITION 1.4. Zwei Bewertungen $|\cdot|_1, |\cdot|_2 : K \to \mathbb{R}_{\geq 0}$ heißen *äquivalent*, wenn ein $\lambda > 0$ existiert mit

$$|a|_1 \;=\; |a|_2^\lambda \quad \text{für alle} \quad a \in K.$$

Insbesondere definieren zwei solche Bewertungen dieselbe Topologie auf K, d.h. zu jedem $\epsilon_1 > 0$ gibt es ein $\epsilon_2 > 0$ mit

$$\{a \in K \mid |a|_1 < \epsilon_1\} \;\subseteq\; \{a \in K \mid |a|_2 < \epsilon_2\}$$

und umgekehrt. Tatsächlich gilt:

BEMERKUNG 1.5. Zwei Bewertungen von K sind äquivalent genau dann, wenn sie die gleiche Topologie auf K definieren.

Beweis. Übung. □

Für Zahlkörper entsprechen die Exponentialbewertungen nach Beispiel VI.2.8 genau den maximalen Idealen des Ganzheitsringes. Für jedes maximale Ideal fixieren wir im Folgenden eine nichtarchimedische Bewertung in ihrer Äquivalenzklasse, indem wir $c = 1/N(\mathfrak{p})$ in Beispiel 1.3 wählen:

DEFINITION 1.6. Sei K ein Zahlkörper. Für maximale Ideale $\mathfrak{p} \in \mathrm{Spm}(\mathfrak{o}_K)$ ist die $\mathfrak{p}$-*adische Bewertung* durch

$$|a|_\mathfrak{p} \;:=\; \begin{cases} N(\mathfrak{p})^{-\nu_\mathfrak{p}(a)} & \text{für } a \in K^\times, \\ 0 & \text{für } a = 0 \end{cases}$$

definiert. Im Fall $K = \mathbb{Q}$ schreiben wir auch $|a|_p$ statt $|a|_{(p)}$ für Primzahlen p und bezeichnen dies als die *p-adische Bewertung*. Explizit ist diese gegeben durch die Formel

$$\left|\frac{x}{y}\right|_p \;=\; p^{-(\nu_p(x)-\nu_p(y))} \quad \text{für} \quad x \in \mathbb{Z} \quad \text{und} \quad y \in \mathbb{N}.$$

Allgemein bezeichnet man eine Äquivalenzklasse von Bewertungen $|\cdot| : K \to \mathbb{R}_{\geq 0}$ auch als eine *Stelle* des Körpers K. Im Fall von Zahlkörpern bezeichnet man die Äquivalenzklassen nichtarchimedischer Bewertungen als *endliche Stellen*. Wir haben für solche Stellen v die Repräsentanten $|\cdot|_v = |\cdot|_\mathfrak{P}$ fixiert und schreiben $v \mid p$ im Fall $\mathfrak{p} \cap \mathbb{Z} = (p)$. Die Äquivalenzklassen archimedischer Bewertungen bezeichnet man als *unendliche Stellen*. Diese Stellen v sind durch die Bewertungen $|\cdot|_v = |\cdot|_\sigma$ für die Einbettungen $\sigma : K \hookrightarrow \mathbb{C}$ repräsentiert, wobei man symbolisch auch $v \mid \infty$ schreibt. Man beachte, dass je zwei konjugierte komplexe Einbettungen dieselbe Bewertung und damit auch dieselbe Stelle definieren — wir fixieren im Folgenden willkürlich jeweis eine der beiden als Repräsentant.

Der folgende sogenannte *schwache Approximationssatz* zeigt, dass sich je endlich viele verschiedene Stellen relativ unabhängig voneinander verhalten:

SATZ 1.7. *Sei K ein Zahlkörper, $\alpha_1, \ldots, \alpha_m \in K$, und es seien $v_1, \ldots, v_m$ endlich viele paarweise verschiedene Stellen. Dann gibt es ür jedes $\epsilon > 0$ ein $\alpha \in K$ mit*

$$|\alpha - \alpha_i|_{v_i} \;<\; \epsilon \quad \textit{für} \quad i \;=\; 1, \ldots, m.$$

Beweis. Nach der Minkowski-Theorie in Kapitel 2 definieren die Stellen $v \mid \infty$ eine Einbettung

$$\iota : \quad K \;\hookrightarrow\; V \;=\; \mathbb{R}^r \times \mathbb{C}^s$$

derart, dass das Bild des Ganzheitsringes ein Gitter ist. Also ist $\iota(K) \subset V$ eine dichte Teilmenge in dem Sinn, dass jede offene Kugel in V einen Punkt aus $\iota(K)$ enthält. Sei also $\beta \in K$ mit

$$|\beta - \alpha_i|_{v_i} \ < \ \frac{\epsilon}{2} \quad \text{für alle } i \text{ mit } v_i \mid \infty.$$

Wir wählen jetzt $N \in \mathbb{N}$, sodass $N \cdot (\beta - \alpha_i) \in \mathfrak{o}_K$ für alle i mit $v_i \nmid \infty$. Nach dem Chinesischen Restsatz können wir dann im Ganzheitsring ein Element $\gamma \in \mathfrak{o}_K$ finden mit

$$|\gamma + N \cdot (\beta - \alpha_i)|_{v_i} \ < \ \frac{\epsilon}{2} \cdot |N|_{v_i} \quad \text{für alle } i \text{ mit } v_i \nmid \infty.$$

Wir machen den Ansatz

$$\alpha \ := \ \frac{\gamma}{MN} + \beta \quad \text{mit geeignetem} \quad M \in \mathbb{N}.$$

Eine kurze Rechnung zeigt, dass die gewünschte Approximationseigenschaft von α erfüllt ist, wenn gilt:

(1) $|M|_{v_i} > \frac{2}{\epsilon} \cdot |\frac{\gamma}{N}|_{v_i}$ für alle i mit $v_i \mid \infty$,

(2) $|M-1|_{v_i} < \frac{\epsilon}{2} \cdot |\frac{MN}{\gamma}|_{v_i}$ für alle i mit $v_i \nmid \infty$.

Für $v_i \nmid \infty$ kann man dabei

$$|\alpha - \alpha_i|_{v_i} \ \leq \ \Big|\frac{\gamma}{N} + (\beta - \alpha_i)\Big|_{v_i} + \Big|\frac{\gamma}{MN} \cdot (M-1)\Big|_{v_i}$$

verwenden. Es bleibt daher nur noch zu bemerken, dass die Eigenschaften (1), (2) gelten, sobald $M-1$ genügend groß bezüglich des gewöhnlichen Absolutbetrags und zugleich hinreichend klein bezüglich aller Stellen $v_i \nmid \infty$ ist. □

Im Folgenden interessieren uns vor allem die nichtarchimedischen Bewertungen; die scharfe Dreiecksungleichung führt zu recht ungewöhnlichen Eigenschaften für die Kreisscheiben

$$D_R(a) \ = \ \{a \in K \mid |a| \leq R\} \quad \text{um} \quad a \in K \quad \text{mit Radius} \quad R > 0,$$

wie das folgende Lemma zeigt:

LEMMA 1.8. *Sei $|\cdot| : K \to \mathbb{R}_{\geq 0}$ eine nichtarchimedische Bewertung.*

(1) *Für alle $a, b \in K$ mit $|a| \neq |b|$ gilt $|a+b| = \max\{|a|, |b|\}$.*

(2) *Es gilt $D_R(a) = D_R(b)$ für alle $b \in D_R(a)$.*

(3) *Für $R' \leq R$ und $a' \in K$ ist*

$$D_R(a) \cap D_{R'}(a') \ = \ \begin{cases} D_{R'}(a') & \text{für } a' \in D_R(a), \\ \varnothing & \text{sonst.} \end{cases}$$

Beweis. Für (1) dürfen wir oBdA $|a| > |b|$ annehmen. Zweimaliges Anwenden der scharfen Dreiecksungleichung zeigt

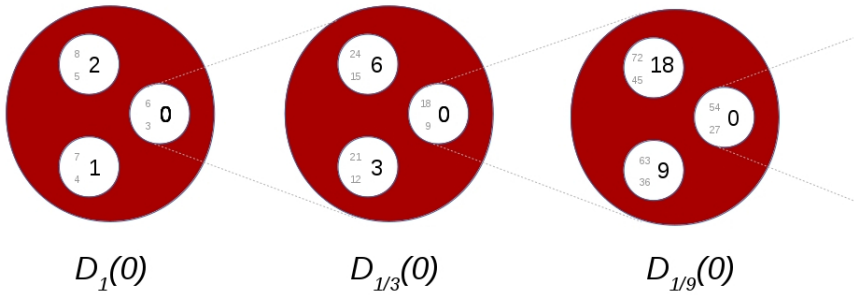
$$|a| \ = \ |a+b-b| \ \leq \ \max\{|a+b|, |b|\} \ \leq \ \max\{|a|, |b|\} \ = \ |a|,$$

also muß beidemale Gleichheit gelten. Für (2) sei $b \in D_R(a)$. Dann ist $|b-a| \leq R$, also folgt für alle $c \in D_R(b)$ mit der scharfen Dreiecksungleichung

$$|c-a| \ = \ |(c-b)+(b-a)| \ \leq \ \max\{|c-b|, |b-a|\} \ \leq \ R$$

und somit $D_R(b) \subseteq D_R(a)$. Die umgekehrte Inklusion erhält man ebenso. Teil (3) sei dem Leser als Übung überlassen. □

Beispiel 1.9. Nach dem obigen Lemma sind im nichtarchimedischen Fall zwei Kreisscheiben entweder disjunkt, oder eine ist in der anderen enthalten. Bezüglich der 3-adischen Bewertung $|\cdot|_3$ kann man sich z.B. die Lokalisierung $\mathbb{Z}_{(3)} \subset \mathbb{Q}$ wie folgt als unendlich löchrigen Schweizer Käse visualisieren, wobei wir in jedem Schritt um den Faktor 3 einzoomen:



In diesem Schweizer Käse sind einige Löcher gefüllt, beispielsweise konvergiert die folgende Reihe im 3-adischen Sinne:

$$1 - 3 + 9 - 27 + 81 - \cdots \;=\; \sum_{\nu=0}^{\infty} (-3)^\nu \;=\; \frac{1}{1-(-3)} \;=\; \frac{1}{4}.$$

Die meisten Löcher bleiben aber offen: Die meisten 3-adischen Cauchy-Folgen haben keinen rationalen Grenzwert. Im nächsten Kapitel werden wir für jede Primzahl p einen Erweiterungskörper $\mathbb{Q}_p \supset \mathbb{Q}$ konstruieren, sodass sich die p-adische Bewertung auf $\mathbb{Q}_p$ fortsetzt und dort jede Cauchy-Folge einen Grenzwert besitzt.

2. Vervollständigung: Topologische Beschreibung

Um die Löcher im obigen Schweizer Käse zu stopfen, gehen wir analog zur bekannten Konstruktion der reellen Zahlen mittels Cauchyfolgen rationaler Zahlen vor. Im Folgenden sei K ein beliebiger Körper. Wir fixieren eine archimedische oder nichtarchimedische Bewertung

$$|\cdot| : \quad K \longrightarrow \mathbb{R}_{\geq 0}.$$

Dann ist K ein metrischer Raum bezüglich der von der Bewertung induzierten Abstandsfunktion

$$d : \quad K \times K \longrightarrow \mathbb{R}_{\geq 0}, \quad d(x,y) \;:=\; |x-y|,$$

und wir können die folgende Definition aus der Analysis übernehmen:

Definition 2.1. Eine Folge $a_1, a_2, a_3, \ldots$ in K heißt *Cauchy-Folge*, wenn es zu jedem $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt mit

$$|a_m - a_n| \;<\; \epsilon \quad \text{für alle} \quad m, n \;\geq\; n_0.$$

Man nennt K *vollständig* bezüglich der gegebenen Bewertung, wenn jede solche Cauchy-Folge konvergiert, d.h. wenn es für jede solche Folge einen Punkt $a \in K$ gibt mit

$$\lim_{n\to\infty} |a_n - a| \;=\; 0.$$

Man schreibt dann auch kurz

$$a \;=\; \lim_{n\to\infty} a_n \;\in\; K$$

und bezeichnet $a \in K$ als den *Grenzwert* der Cauchy-Folge.

Jeder bewertete Körper lässt sich in minimaler Weise in einen vollständigen Körper, seine sogenannte *Vervollständigung*, einbetten:

PROPOSITION 2.2. *Zu jedem bewerteten Körper K gibt es eine bis auf kanonische Isomorphie eindeutige Einbettung*

$$K \;\hookrightarrow\; \hat{K}$$

in einen vollständigen bewerteten Körper, sodass gilt:

(1) *Die Bewertung auf $\hat{K}$ induziert die gegebene Bewertung auf K.*

(2) *Jedes Element $a \in \hat{K}$ ist Grenzwert einer Cauchy-Folge in K.*

Beweis. Sei $CF(K)$ der Ring der Cauchy-Folgen in K, ausgestattet mit der komponentenweisen Addition und Multiplikation. Offenbar bilden die gegen Null konvergenten Folgen ein Ideal $\mathfrak{N} \trianglelefteq CF(K)$, und wir definieren die Vervollständigung durch den Quotientenring

$$\hat{K} \;:=\; CF(K)/\mathfrak{N}.$$

Man prüft leicht nach, dass dies ein Körper ist, da sich jede von Null verschiedene Folge durch ein Element von $\mathfrak{N}$ so abändern lässt, dass alle Folgenglieder von Null verschieden sind. Durch

$$|a| \;:=\; \lim_{n\to\infty} |a_n| \quad \text{für} \quad a \;=\; \Big((a_n)_{n\in\mathbb{N}} \mod \mathfrak{N}\Big) \;\in\; \hat{K}$$

wird auf $\hat{K}$ eine Bewertung erklärt, und ein Diagonalargument zeigt, dass $\hat{K}$ mit dieser Bewertung ein vollständiger Körper ist. Dieser Körper enthält K mittels der Einbettung

$$K \;\hookrightarrow\; \hat{K}, \quad a \;\mapsto\; \Big((a)_{n\in\mathbb{N}} \mod \mathfrak{N}\Big)$$

welche ein Element auf die entsprechende konstante Folge schickt, und die übrigen Eigenschaften folgen nun leicht. □

Man beachte, dass die Vervollständigung $\hat{K}$ nicht nur von K, sondern auch von der Bewertung $|\cdot|$ auf K abhängt. Der Klarheit halber schreiben wir daher auch manchmal

$$\hat{K} \;=\; \widehat{(K, |\cdot|)},$$

wenn mehrere Bewertungen auf demselben Körper betrachtet werden.

BEISPIEL 2.3. Die Vervollständigung der rationalen Zahlen unter dem üblichen Absolutbetrag ist

$$\mathbb{R} \;\simeq\; \widehat{(\mathbb{Q}, |\cdot|)}.$$

Ist K allgemeiner ein Zahlkörper, dann erhält man für Einbettungen $\sigma : K \hookrightarrow \mathbb{C}$ die Vervollständigung

$$\widehat{(K, |\cdot|_\sigma)} \;\simeq\; \begin{cases} \mathbb{R} & \text{falls } \sigma \text{ reell ist,} \\ \mathbb{C} & \text{falls } \sigma \text{ komplex ist,} \end{cases}$$

denn die Einbettungen bewerteter Körper $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ induzieren $\mathbb{R} \subseteq \hat{K} \subseteq \mathbb{C}$.

Allgemeiner kann man zeigen, dass jeder vollständige archimedisch bewertete Körper isomorph zu $\mathbb{R}$ oder $\mathbb{C}$ mit einer Potenz des üblichen Absolutbetrages als Bewertung ist. Diesen sogenannten *Satz von Ostrowski* wollen wir hier nicht beweisen, sondern betrachten ab jetzt die nichtarchimedischen Bewertungen:

DEFINITION 2.4. Für Primzahlen p wird die Vervollständigung von $\mathbb{Q}$ bezüglich des p-adischen Absolutbetrags mit

$$\mathbb{Q}_p \;=\; \widehat{(\mathbb{Q}, |\cdot|_p)}$$

bezeichnet und heißt der Körper der *p-adischen Zahlen*. Allgemeiner betrachten wir für beliebige Zahlkörper K und jedes maximale Ideal $\mathfrak{p} \in \operatorname{Spm}(\mathfrak{o}_K)$ die $\mathfrak{p}$-adische Vervollständigung

$$K_\mathfrak{p} \;=\; \widehat{(K, |\cdot|_\mathfrak{p})}.$$

Die Elemente der soeben definierten Körper lassen sich ganz konkret durch Potenzreihenentwicklungen beschreiben, analog zur Dezimaldarstellung von reellen Zahlen. Tatsächlich ist die Situation im nichtarchimedischen Fall sogar viel einfacher:

LEMMA 2.5. *Sei K ein nichtarchimedisch bewerteter Körper. Für $a_1, a_2, \cdots \in K$ betrachten wir die Partialsummen*

$$s_n \;=\; a_1 + a_2 + \cdots + a_n.$$

Dann ist $(s_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge genau dann, wenn $\lim_{n\to\infty} a_n = 0$ ist.

Beweis. Die Implikation $\Rightarrow$ ist klar wegen $a_n = s_n - s_{n-1}$ und gilt natürlich ebenso auch für archimedische Bewertungen. Im nichtarchimedischen Fall erhält man $\Leftarrow$ aus

$$|s_m - s_n| \;=\; |a_{n+1} + \cdots + a_m| \;\leq\; \max\bigl\{|a_{n+1}|, \ldots, |a_m|\bigr\}$$

für $m \geq n$ wegen der scharfen Dreiecksungleichung. □

KOROLLAR 2.6. *Es sei K ein vollständiger nichtarchimedisch bewerteter Körper und $a_1, a_2, \ldots$ eine Folge von Elementen in K. Dann sind äquivalent:*

(1) *Die Reihe $\sum_{n=0}^{\infty} a_n$ konvergiert, d.h. es existiert $\lim_{N\to\infty} \sum_{n=0}^{N} a_n \in K$.*
(2) *Es ist $\lim_{n\to\infty} a_n = 0$.*

Beweis. Dies folgt direkt aus dem vorigen Lemma, da in vollständigen Körpern jede Cauchy-Folge konvergiert. □

Bezüglich der 3-adischen Bewertung erhält man etwa mittels der geometrischen Reihe

$$\frac{1}{4} \;=\; \frac{1}{1-(-3)} \;=\; \sum_{n=0}^{\infty} (-3)^n \quad \text{in} \quad \mathbb{Q}_3.$$

Hier ist der Grenzwert eine rationale Zahl. Dies ist aber natürlich nicht immer der Fall, beispielsweise werden wir später $\sqrt{7} = 1 + 1\cdot 3 + 1\cdot 3^2 + 2\cdot 3^4 + \cdots \in \mathbb{Q}_3$ sehen.

3. Vervollständigung: Algebraische Beschreibung

Im nichtarchimedischen Fall lässt sich die Vervollständigung aus dem vorigen Abschnitt auch algebraisch in der Sprache von Bewertungsringen beschreiben. Wir beginnen dazu mit der folgenden

DEFINITION 3.1. Sei K ein Körper und $|\cdot| : K \to \mathbb{R}_{\geq 0}$ eine nichtarchimedische Bewertung. Dann wird durch

$$\mathfrak{o} \;:=\; \{a \in K \mid\; |a| \leq 1\}$$

ein lokaler Ring definiert, der sogenannte *Bewertungsring* von $(K, |\cdot|)$. Das maximale Ideal

$$\mathfrak{m} \;:=\; \{a \in \mathfrak{o} \mid |a| < 1\}$$

nennt man auch das *Bewertungsideal*, und

$$\mathbb{F} \;:=\; \mathfrak{o}/\mathfrak{m}$$

den *Restklassenkörper*. Wir nennen die Bewertung $|\cdot|$ *diskret*, wenn die zugehörige Exponentialbewertung $\log|\cdot|$ diskret ist. Bewertungsideal und Bewertungsring der Vervollständigung bezeichnen wir mit

$$\hat{\mathfrak{m}} \;:=\; \{a \in \hat{K} \mid |a| < 1\} \;\trianglelefteq\; \hat{\mathfrak{o}} \;:=\; \{a \in \hat{K} \mid |a| \leq 1\}.$$

Der Restklassenkörper der Vervollständigung benötigt keine eigene Notation:

LEMMA 3.2. *In der obigen Situation gilt:*

(1) *Die Inklusion* $\mathfrak{o} \hookrightarrow \hat{\mathfrak{o}}$ *induziert einen Isomorphismus* $\mathfrak{o}/\mathfrak{m} \simeq \hat{\mathfrak{o}}/\hat{\mathfrak{m}}$.

(2) *Die Bewertung* $|\cdot|$ *ist diskret genau dann, wenn* $\mathfrak{m}$ *ein Hauptideal ist.*

(3) *Ist letzteres der Fall, dann induziert die Inklusion* $\mathfrak{o} \hookrightarrow \hat{\mathfrak{o}}$ *für jedes* $\nu \in \mathbb{N}$ *einen Isomorphismus*

$$\mathfrak{o}/\mathfrak{m}^\nu \;\simeq\; \hat{\mathfrak{o}}/\hat{\mathfrak{m}}^\nu.$$

Beweis. (1) Wegen $\mathfrak{m} = \mathfrak{o} \cap \hat{\mathfrak{m}}$ induziert die Inklusion $\mathfrak{o} \hookrightarrow \hat{\mathfrak{o}}$ jedenfalls einen injektiven Homomorphismus

$$\mathfrak{o}/\mathfrak{m} \;\hookrightarrow\; \hat{\mathfrak{o}}/\hat{\mathfrak{m}}$$

der entsprechenden Restklassenkörper. Um die Surjektivität zu sehen, beachte man, dass sich jedes Element $a \in \hat{\mathfrak{o}}$ als Grenzwert $a = \lim_{n\to\infty} a_n$ einer Folge von Elementen $a_n \in \mathfrak{o}$ schreiben lässt. Für $n \to \infty$ gilt dann offenbar $|a - a_n| \to 0$, also erhalten wir

$$a \equiv a_n \mod \hat{\mathfrak{m}} \quad \text{für alle genügend große} \quad n \gg 0$$

und hiermit folgt die behauptete Surjektivität.

(2) Ist $|\cdot|$ diskret, so ist die Wertegruppe $|K^\times| = \{|a| \mid a \in K^\times\} \subset \mathbb{R}^\times_{>0}$ zyklisch, erzeugt von einem Element $c \in (0,1)$. Wir wählen nun ein beliebiges Element $\pi \in \mathfrak{m}$ mit $|\pi| = c$. Dann ist

$$\mathfrak{m} \;=\; (\pi),$$

denn es gelten die Implikationen

$$a \in \mathfrak{m} \quad\Longrightarrow\quad |a| \leq c = |\pi| \quad\Longrightarrow\quad |a/\pi| \leq 1 \quad\Longrightarrow\quad a/\pi \in \mathfrak{o} \quad\Longrightarrow\quad a \in (\pi).$$

Insbesondere ist dann also $\mathfrak{m}$ ein Hauptideal. Die Umkehrung folgt analog.

(3) Per Konstruktion der Vervollständigung $\hat{K}$ mittels Cauchy-Folgen gilt für die Wertegruppen

$$|K^\times| \;=\; |\hat{K}^\times|,$$

mit K ist also auch $\hat{K}$ diskret bewertet. Sei $c \in (0,1)$ ein Erzeuger der gemeinsamen Wertegruppe. Für jedes $\nu \in \mathbb{N}$ folgt

$$\mathfrak{m}^\nu \;=\; \{a \in \mathfrak{o} \mid |a| \leq c^\nu\} \;=\; \mathfrak{o} \cap \{a \in \hat{\mathfrak{o}} \mid |a| \leq c^\nu\} \;=\; \mathfrak{o} \cap \hat{\mathfrak{m}}^\nu$$

und somit ist der Homomorphismus

$$\mathfrak{o}/\mathfrak{m}^\nu \;\hookrightarrow\; \hat{\mathfrak{o}}/\hat{\mathfrak{m}}^\nu$$

injektiv. Für die Surjektivität benutzen wir wieder, dass sich jedes Element von $\hat{\mathfrak{o}}$ als Grenzwert $a = \lim_{n\to\infty} a_n$ einer Folge von Elementen $a_n \in \mathfrak{o}$ schreibt. Damit gilt wie zuvor

$$|a - a_n| \;\to\; 0 \quad \text{für} \quad n \;\to\; \infty.$$

Da die Bewertung diskret ist, folgt

$$a - a_n \in \hat{\mathfrak{m}}^\nu \quad \text{für} \quad n \gg 0$$

und damit die behauptete Surjektivität. □

Im diskret bewerteten Fall können wir nun ein Analogon der Dezimaldarstellung reeller Zahlen formulieren. Dazu sei $\mathcal{R} \subset \mathfrak{o}^\times \cup \{0\}$ ein Repräsentantensystem für die Restklassen in $\mathbb{F} = \mathfrak{o}/\mathfrak{m}$, und wir fixieren einen Erzeuger π des Bewertungsideals $\mathfrak{m}$.

KOROLLAR 3.3. *Sei K ein diskret bewerteter Körper. Mit den obigen Notationen lässt sich dann jedes Element $a \in \hat{K}$ eindeutig in der Form $a = \sum_{\nu \geq \nu_0} c_\nu \cdot \pi^\nu$ mit Ziffern $c_\nu \in \mathcal{R}$ darstellen, wobei der Index $\nu_0 \in \mathbb{Z} \cup \{\infty\}$ eindeutig bestimmt ist durch*

$$|\pi|^{\nu_0} \;=\; |a|.$$

Beweis. Der Fall $a = 0$ ist trivial. Im Fall $a \neq 0$ können wir nach Multiplikation mit einer geeigneten Potenz von π annehmen, dass $\nu_0 = 0$ und $a \in \mathfrak{o}^\times$ ist. Nach dem vorigen Lemma existiert dann ein eindeutig bestimmter Repräsentant $c_0 \in \mathcal{R}$ mit $a \equiv c_0 \bmod \mathfrak{m}$. Anwenden des Lemmas auf $(a - c_0)/\pi$ liefert einen eindeutig bestimmten Repräsentanten $c_1 \in \mathcal{R}$ mit

$$a - c_0 \;\equiv\; c_1\pi \mod \mathfrak{m}^2$$

und induktiv fortfahrend erhalten wir eine eindeutige Folge von Ziffern $c_i \in \mathcal{R}$ mit der Eigenschaft

$$a - c_0 - c_1\pi - \cdots - c_\nu\pi^\nu \;\in\; \mathfrak{m}^{\nu+1} \quad \text{für alle} \quad \nu \in \mathbb{N}.$$

Die Behauptung folgt nun durch den Grenzübergang $\nu \to \infty$, wobei die erhaltene Reihe nach Korollar 2.6 konvergiert. □

BEISPIEL 3.4. Sei p eine Primzahl. Nach obigem Korollar hat jedes $a \in \mathbb{Q}_p^\times$ eine eindeutige *p-adische Entwicklung*

$$a \;=\; \sum_{\nu \geq \nu_0} c_\nu \cdot p^\nu \quad \text{mit} \quad c_\nu \in \{0, 1, \ldots, p-1\} \quad \text{und} \quad c_{\nu_0} \neq 0.$$

Solche p-adischen Entwicklungen erfüllen die üblichen Rechenregeln mit Übertrag, so ist etwa

$$(1 \cdot p^2 + 0 \cdot p^3 + \cdots) \cdot ((p-1) \cdot p^3 + 0 \cdot p^4 + \cdots) \;=\; 1 \cdot p^6 + 0 \cdot p^7 + \cdots \text{ in } \mathbb{Q}_p,$$

und als Übungsaufgabe kann man sich

$$1 + 2 + 4 + 8 + \cdots \;=\; -1 \text{ in } \mathbb{Q}_2$$

ohne explizite Benutzung der geometrischen Reihe überlegen.

Für eine formalere Beschreibung solcher Darstellungen in Stellenwertsystemen kann man den algebraischen Begriff eines *inversen Limes* verwenden. Wir wollen diesen hier nicht formal einführen, sondern lediglich den hier benötigten Spezialfall explizit notieren:

DEFINITION 3.5. Sei R ein kommutativer Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal. Für $n \in \mathbb{N}$ bezeichnen wir mit

$$p_n : \quad R/\mathfrak{a}^{n+1} \;\twoheadrightarrow\; R/\mathfrak{a}^n$$

den von der Identität id_R induzierten surjektiven Ringhomomorphismus. Dann ist die *$\mathfrak{a}$-adische Vervollständigung* von R definiert als der bezüglich dieser p_n gebildete inverse Limes

$$\varprojlim R/\mathfrak{a}^n \;:=\; \Big\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} R/\mathfrak{a}^n \;\mid\; p_n(a_{n+1}) = a_n \;\text{ für alle }\; n \Big\}.$$

In dieser Sprache können wir nun die Vervollständigung auf dem Niveau der Bewertungsringe in sehr einfacher Weise beschreiben:

KOROLLAR 3.6. *In der Situation von Korollar 3.3 ist der Bewertungsring der Vervollständigung gegeben durch*

$$\hat{\mathfrak{o}} \simeq \varprojlim \mathfrak{o}/\mathfrak{m}^n.$$

Beweis. Mittels der eindeutigen Darstellung aus Korollar 3.3 definieren wir einen Ringhomomorphismus

$$\varphi: \quad \hat{\mathfrak{o}} \to \varprojlim \mathfrak{o}/\mathfrak{m}^n$$

durch

$$\varphi\Big(\sum_{\nu\geq 0} c_\nu \pi^\nu\Big) := (a_n)_{n\in\mathbb{N}} \quad \text{mit} \quad a_n := \sum_{\nu=0}^{n-1} c_\nu \pi^\nu \mod \pi^n .$$

Mithilfe des Korollars prüft man leicht nach, dass φ bijektiv ist. □

4. Das Henselsche Lemma