Skript zur Vorlesung

Algebraische Zahlentheorie
im WS 2022/23

von Dr. Andreas Demleitner

Version vom 15. April 2024

Literaturvorschläge:

- U. Jannsen: *Algebraische Zahlentheorie I*, Vorlesungsskript, WS 2007/08.
- S. Lang: *Algebraic Number Theory* (2. Auflage), Springer, 1994.
- J. Neukirch: *Algebraische Zahlentheorie*, Springer, 1992.
- P. Samuel: *Algebraic Theory of Numbers*, Dover, 2008.

Disclaimer: Dies ist ein Vorlesungsskript, kein Lehrbuch. Fehler passieren. Für Meldungen an andreas.demleitner@math.uni-freiburg.de bin ich sehr dankbar. ☺

Kapitel 0

Worum geht es?

Der *Hauptsatz der Arithmetik* besagt, dass jede natürliche Zahl, die größer als 1 ist, eindeutig als Produkt von Primzahlen geschrieben werden kann. Während man die Teilbarkeitsrelation auf beliebigen Integritätsringen[1] diskutieren kann, lässt sich der Hauptsatz der Arithmetik sich nicht auf beliebige Ringe verallgemeinern:

Beispiel 0.1. Betrachten Sie die Menge

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

wobei $\sqrt{-5}^2 = -5$ sei. Simples Nachrechnen ergibt, dass es sich bei $\mathbb{Z}[\sqrt{-5}]$ um einen Ring handelt. In diesem Ring gilt jedoch

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

d.h. die Zahl 6 kann auf zwei Art und Weisen als Produkt anderer Elemente geschrieben werden. (Dafür muss man noch nachweisen, dass diese beiden Darstellungen auch tatsächlich unterschiedlich bis auf Assoziiertheit sind.)

Diejenigen Ringe, in denen der Hauptsatz der Arithmetik funktioniert, heißen *faktoriell*. Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist demnach nicht faktoriell. Grob gesagt beschäftigt sich diese Vorlesung damit, den Hauptsatz der Arithmetik für Ringe wie $\mathbb{Z}[\sqrt{-5}]$ anzupassen. Dazu muss natürlich "Ringe wie $\mathbb{Z}[\sqrt{-5}]$" präzisiert werden. Das führt auf den Begriff des *Dedekindrings*. Wir werden zeigen, dass in Dedekindringen jedes Ideal $\neq (0)$ eindeutig als Produkt von Prim*idealen* geschrieben werden kann. Anhand einiger Beispiele illustrieren wir, wie Arithmetik in Dedekindringen genutzt wird, um nach ganzzahligen Lösungen von Gleichungen zu suchen:

(1) Sei p eine ungerade Primzahl. Wir interessieren uns dafür, wann

$$X^2 + Y^2 = p \tag{0.1}$$

ganzzahlig lösbar ist. Als ungerade Primzahl lässt sich p in der Form $p = 4n \pm 1$ schreiben. Da die Gleichung $X^2 + Y^2 \equiv -1 \pmod 4$ nicht lösbar ist (die Quadrate modulo 4 sind 0 und 1), ist eine notwendige Bedingung für die Lösbarkeit von (0.1), dass $p = 4n + 1$.
Ist $p = 4n + 1$ auch hinreichend? Wir bemerken zunächst, dass $(\mathbb{Z}/p\mathbb{Z})^*$ für

[1] d.h. nullteilerfreien, kommutativen Ringen $\neq \{0\}$ mit Einselement

$p = 4n+1$ zyklisch der Ordnung $4n$ ist. Es gibt also eine ganze Zahl $m \neq 0$, deren Klasse in $(\mathbb{Z}/p\mathbb{Z})^*$ die multiplikative Ordnung 4 hat. Es folgt $m^2 \equiv -1 \pmod{p}$, also ist m^2+1 durch p teilbar. Nun betrachten wir den Ring der Gaußschen Zahlen

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

Dieser ist ein Hauptidealring (Aufgabe 0.1.1), also auch faktoriell. In $\mathbb{Z}[i]$ gilt

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

Durch Vergleichen der Imaginärteile sieht man, dass p kein Teiler von $m+i$ und $m-i$ sein kann. Da p jedoch ihr Produkt m^2+1 teilt, ist p kein Primelement in $\mathbb{Z}[i]$. Nun ist $\mathbb{Z}[i]$ faktoriell, das heißt, dass p ebenfalls reduzibel ist. Es gibt also irreduzible Elemente $\pi_1, \ldots, \pi_k \in \mathbb{Z}[i]$, $k \geq 2$ mit

$$p = \pi_1 \cdot \ldots \cdot \pi_k.$$

Nehmen des Betrags und Quadrieren liefert

$$p^2 = |\pi_1|^2 \cdot \ldots \cdot |\pi_k|^2. \tag{0.2}$$

Schreibe $\pi_j = a_j + ib_j$, dann gilt

$$|\pi_j|^2 = a_j^2 + b_j^2 = (a_j + ib_j)(a_j - ib_j) = \pi_j \cdot \overline{\pi_j}.$$

Es folgt $|\pi_j|^2 \in \mathbb{Z}_{\geq 0}$ und $|\pi_j|^2 > 1$ (da π_j als irreduzibles Element keine Einheit ist). Im Hinblick auf (0.2) bedeutet dies $k = 2$ und

$$p = |\pi_j|^2 = a_j^2 + b_j^2 \qquad \text{für} \quad j = 1, 2.$$

Also ist p eine Summe von zwei Quadraten.

(2) Die berühmte Gleichung $X^p + Y^p = Z^p$ für $p \geq 3$ prim lässt sich im Kreisteilungskörper $\mathbb{Q}(\zeta_p)$ wie folgt umschreiben:

$$X^p + Y^p = \prod_{i=0}^{p-1} (X + \zeta_p^i Y) = Z^p.$$

Die Schwierigkeit des großen Satzes von Fermat liegt nun darin, dass der Ring $\mathbb{Z}[\zeta_p]$ für fast keine Primzahlen p faktoriell ist. In Abschnitt 6.3 werden wir uns erneut mit dem großen Satz von Fermat beschäftigen und Spezialfälle beweisen.

(3) Man betrachte die Gleichung $X^2+5 = Y^3$. Diese hat keine ganzzahligen Lösungen, was wir aber noch nicht beweisen können. Wie in den vorherigen Beispielen wäre ein erster Ansatz, die Gleichung in $\mathbb{Z}[\sqrt{-5}]$ zu

$$(X + \sqrt{-5})(X - \sqrt{-5}) = Y^3$$

umzuformen. Nun ist $\mathbb{Z}[\sqrt{-5}]$ aber nicht faktoriell, das heißt, dass uns diese Faktorisierung nicht helfen wird. Da wir aber eine eindeutige Faktorisierung in Prim*ideale* haben, können wir die Gleichung

$$(X + \sqrt{-5})(X - \sqrt{-5}) = (Y)^3$$

von *Idealen* in $\mathbb{Z}[\sqrt{-5}]$ studieren!

Innerhalb der Vorlesung gelten die folgenden Konventionen:

Konvention. Mit einem *Ring* sei immer ein kommutativer Ring $\neq \{0\}$ mit Eins gemeint. (In Spezialfällen wird es trotzdem sinnvoll sein, den Nullring auch als Ring zu betrachten, zum Beispiel möchten wir natürlich, dass der Faktorring eines Ringes nach einem Ideal erneut ein Ring ist. Verwirrungen sollten allerdings ausgeschlossen sein.) Ein Ringhomomorphismus bildet 1 auf 1 ab.

0.1 Übungen

Aufgabe 0.1.1. Ein nullteilerfreier Ring A heißt *euklidisch*, wenn es eine Abbildung

$$N\colon A \setminus \{0\} \to \mathbb{Z}_{>0} \qquad (\text{“Euklidische Normabbildung”})$$

mit der folgenden Eigenschaft gibt (“Division mit Rest”): Für je zwei Elemente $a, b \in A$, $b \neq 0$ gibt es $q, r \in A$ mit $a = qb + r$ und entweder $r = 0$ oder $N(r) < N(b)$.

(1) Sei A ein euklidischer Ring mit Norm N. Zeigen Sie, dass A ein Hauptidealring ist.
Hinweis: Sei $\mathfrak{a} \neq (0)$ ein Ideal von A. Wählen Sie ein Element $b \in \mathfrak{a} \setminus \{0\}$ mit $N(b)$ minimal.

(2) Zeigen Sie, dass $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$ bezüglich der Normabbildung $N(x + iy) = |x + iy|^2 = x^2 + y^2$ euklidisch ist.
Hinweis: Für jedes $z \in \mathbb{C}$ existiert ein $x + iy \in \mathbb{Z}[i]$ mit $|z - (x + iy)| \leq \frac{1}{\sqrt{2}}$. (Warum?)

Kapitel 1

Der Ganzheitsring

Der Begriff der "Ganzheit" dürfte Ihnen bereits geläufig sein.

Satz und Definition 1.1. Sei B/A eine Ringerweiterung. Für $b \in B$ sind die folgenden Aussagen äquivalent:

(1) Es gibt ein normiertes Polynom $0 \neq f \in A[X]$ mit $f(b) = 0$.

(2) Es ist $A[b]$ ein endlich-erzeugter A-Modul.

(3) Es gibt einen Teilring $A[b] \subset C \subset B$, der ein endlich-erzeugter A-Modul ist.

In diesem Falle heißt b *ganz* über A. Die Ringerweiterung B/A heißt *ganz*, wenn alle Elemente aus B ganz über A sind.

Beweis. Wir erinnern daran, dass $A[b_1, \ldots, b_k]$ die Menge der *polynomiellen* Ausdrücke in $b_1, \ldots, b_k$ ist. Aufgefasst als A-Modul wird $A[b_1, \ldots, b_k]$ also von den Elementen

$$b_1^{i_1} \cdot \ldots \cdot b_k^{i_k}, \qquad \text{mit} \quad i_j \geq 0$$

erzeugt.

"(1) $\implies$ (2):" Ist

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

ein normiertes Polynom mit b als Nullstelle, so gilt also

$$b^n = -(a_{n-1}b^{n-1} + \ldots + a_0),$$

d.h. b^n (und induktiv dann auch jede höhere Potenz) kann als A-Linearkombination von $\{1, b, \ldots, b^{n-1}\}$ geschrieben werden. Somit wird $A[b]$ von $\{1, b, \ldots, b^{n-1}\}$ erzeugt.

"(2) $\implies$ (3):" Man nehme $C = A[b]$.

"(3) $\implies$ (1):" Sei $\{x_1, \ldots, x_n\}$ ein Erzeugendensystem von C als A-Modul. Da $b \in C$, kann man bx_i wieder als Linearkombination bzgl. $\{x_1, \ldots, x_n\}$ schreiben:

$$bx_i = \sum_{j=1}^{n} a_{ij}x_j \qquad (a_{ij} \in A).$$

Für die Matrix M mit den Einträgen a_{ij} gilt also

$$(M - bI_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0. \tag{1.1}$$

Multiplizieren der Gleichung (1.1) mit der Adjunkten von $M - bI_n$ ergibt (vgl. Aufgabe 1.0.1):

$$\det(M - bI_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Mit anderen Worten ist $\det(M - bI_n)x_i = 0$ für jedes $i = 1, \ldots, n$. Da $\{x_1, \ldots, x_n\}$ ein Erzeugendensystem von C ist, gibt es $a_1, \ldots, a_n \in A$ mit

$$a_1x_1 + \ldots + a_nx_n = 1. \tag{1.2}$$

Multiplizieren wir (1.2) mit $\det(M - bI_n)$, so erhalten wir schließlich

$$\det(M - bI_n) = 0.$$

Da $\det(M - XI_n) \in A[X]$ normiert vom Grad n ist und b als Nullstelle hat, haben wir eine Ganzheitsgleichung für b gefunden. □

Proposition 1.2. *Sei B/A eine Ringerweiterung und $b_1, \ldots, b_n \in B$. Ist jedes b_i ganz über $A[b_1, \ldots, b_{i-1}]$ (also insbesondere, wenn $b_1, \ldots, b_n$ ganz über A sind), so ist $A[b_1, \ldots, b_n]$ ein endlich-erzeugter A-Modul.*

Beweis. Wir beweisen die Aussage durch Induktion über n. Der Fall $n = 1$ wurde bereits in Satz 1.1 diskutiert. Nehmen wir also an, dass $B' := A[b_1, \ldots, b_{n-1}]$ ein endlich-erzeugter A-Modul ist. Da b_n ganz über B' ist, ist $B'[b_n]$ ein endlich-erzeugter B'-Modul (Satz 1.1 (2)). Ist $\{x_1, \ldots, x_k\}$ ein B'-Erzeugendensystem von $B'[b_n]$ und $\{y_1, \ldots, y_m\}$ ein A-Erzeugendensystem von B', so ist

$$\{x_iy_j \mid 1 \leq i \leq k,\ 1 \leq j \leq m\}$$

ein A-Erzeugendensystem von $B'[b_n] = A[b_1, \ldots, b_n]$. □

Offensichtlich sind die Elemente aus $A \subset B$ ganz über A, denn $a \in A$ ist Nullstelle von $X - a \in A[X]$. Mehr Beispiele bekommen wir durch

Korollar 1.3. *Summen und Produkte ganzer Elemente sind ganz. Insbesondere bilden die Elemente von B, die ganz über A sind, einen Unterring $\overline{A}$ von B, der A enthält. Dieser heißt der* ganze Abschluss *von A in B.*

Beweis. Alle Elemente aus A sind ganz über A. Für über A ganze Elemente $b_1,\ b_2 \in B$ ist $A[b_1, b_2]$ nach Proposition 1.2 ein endlich-erzeugter A-Modul. Da

$$b_1 + b_2,\ b_1 - b_2,\ b_1b_2 \in A[b_1, b_2],$$

folgt die Behauptung aus Satz 1.1 (3). □

Ganz besonders werden wir den *Ganzheitsring* eines *algebraischen Zahlkörpers* studieren:

Definition 1.4.

(1) Ein *(algebraischer) Zahlkörper* ist eine endliche Körpererweiterung von $\mathbb{Q}$.

(2) Für einen Zahlkörper K bezeichnen wir den ganzen Abschluss von $\mathbb{Z}$ in K mit $\mathcal{O}_K$. Der Ring $\mathcal{O}_K$ heißt der *Ganzheitsring* von K.

Wir möchten daran erinnern, dass ein nullteilerfreier Ring A einen Quotientenkörper $\mathrm{Frac}(A)$ hat:

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} \mid a, b \in A,\ b \neq 0 \right\}, \qquad \frac{a_1}{b_1} = \frac{a_2}{b_2} \ :\Longleftrightarrow\ a_1 b_2 = a_2 b_1$$

Bezüglich der folgenden wohldefinierten (!) Addition und Multiplikation wird $\mathrm{Frac}(A)$ ein Körper:

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}, \qquad \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

Via der Abbildung $\iota\colon A \hookrightarrow \mathrm{Frac}(A)$, $a \mapsto \frac{a}{1}$ ist A ein Teilring von $\mathrm{Frac}(A)$. Ferner ist $\mathrm{Frac}(A)$ ist der kleinste Körper, der A enthält, im folgenden Sinne: Ist K ein Körper und $f\colon A \hookrightarrow K$ ein injektiver Ringhomomorphismus, so gibt es genau einen Körperhomomorphismus $\tilde{f}\colon \mathrm{Frac}(A) \to K$ mit $\tilde{f} \circ \iota = f$ für alle $a \in A$.

Definition 1.5. Ein nullteilerfreier Ring A heißt *ganz abgeschlossen* (oder *normal*), wenn A mit seinem ganzen Abschluss im Quotientenkörper $\mathrm{Frac}(A)$ übereinstimmt.

Wir zeigen, dass der Ganzheitsring eines Zahlkörpers ganz abgeschlossen ist.

Proposition 1.6. *Sind C/B und B/A ganze Ringerweiterungen, so ist auch C/A ganz.*

Beweis. Sei $c \in C$. Da c ganz über B ist, erfüllt c eine Ganzheitsgleichung der Form

$$c^n + b_{n-1} c^{n-1} + \ldots + b_0 = 0, \qquad \text{mit} \quad b_0, \ldots, b_{n-1} \in B.$$

Also ist c ganz über $A' := A[b_0, \ldots, b_{n-1}]$. Nach Satz 1.1 (2) ist $A'[c]$ ein endlich-erzeugter A'-Modul. Weil B/A ganz ist, impliziert Proposition 1.2, dass A' ein endlich-erzeugter A-Modul ist. Somit ist auch $A'[c] = A[b_0, \ldots, b_{n-1}, c]$ ein endlich-erzeugter A-Modul. Die Aussage folgt dann durch erneute Anwendung von Satz 1.1 (3). □

Korollar 1.7. *Ist K ein Zahlkörper, so ist $\mathcal{O}_K$ ganz abgeschlossen.*

Beweis. Sei $\mathcal{O}'$ der ganze Abschluss von $\mathcal{O}_K$ in seinem Quotientenkörper. Wir haben ganze Ringerweiterungen $\mathcal{O}_K/\mathbb{Z}$ und $\mathcal{O}'/\mathcal{O}_K$. Nach Proposition 1.6 ist $\mathcal{O}'/\mathbb{Z}$ ganz, d.h. $\mathcal{O}' \subset \mathcal{O}_K$. □

Bemerkung 1.8. Sei K ein Zahlkörper.

(1) Per Definition gilt

$$\mathcal{O}_K = \{\beta \in K \mid \text{ es gibt ein normiertes Polynom } P \in \mathbb{Z}[X] \text{ mit } P(\beta) = 0\}.$$

Weil die Erweiterung $K/\mathbb{Q}$ nun aber endlich ist, ist sie algebraisch. Jedes $\alpha \in K$ hat also ein Minimalpolynom $m_\alpha \in \mathbb{Q}[X]$. Dieses ist das eindeutig bestimmte

normierte Polynom minimalen Grades, das α als Nullstelle besitzt. Insbesondere teilt m_α jedes andere Polynom $\neq 0$, das α als Nullstelle besitzt.
Gilt sogar $m_\alpha \in \mathbb{Z}[X]$, so folgt gemäß obiger Beschreibung $\alpha \in \mathcal{O}_K$. Wenn umgekehrt ein normiertes Polynom $P \in \mathbb{Z}[X]$ mit $P(\alpha) = 0$ gegeben ist, so wissen wir, dass m_α ein Teiler von P ist. Da sowohl m_α als auch P normiert sind, besagt eine der Varianten des Lemmas von Gauß, dass $m_\alpha \in \mathbb{Z}[X]$ gilt.
Summa summarum haben wir also

$$\mathcal{O}_K = \{\beta \in K \mid m_\beta \in \mathbb{Z}[X]\}$$

gezeigt. Um zu überprüfen, ob ein Element von K ganz ist, müssen wir also nur das Minimalpolynom berechnen und schauen, ob es ganzzahlig ist.

(2) Der Quotientenkörper von $\mathcal{O}_K$ ist K, denn: Sei $\beta \in K$. Erneut betrachten wir das Minimalpolynom $m_\beta \in \mathbb{Q}[X]$. Multipliziert man die Gleichung $m_\beta(\beta) = 0$ mit dem Hauptnenner der Koeffizienten von m_β durch, so erhalten wir eine Gleichung der Form

$$a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_0 = 0, \qquad a_i \in \mathbb{Z}, \quad a_n \neq 0.$$

Multiplizieren mit a_n^{n-1} ergibt

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + a_{n-2}a_n(a_n\beta)^{n-2} + \ldots + a_n^{n-1}a_0 = 0.$$

Also ist $a_n\beta \in \mathcal{O}_K$. Es folgt $\beta = \frac{a_n\beta}{a_n} \in \mathrm{Frac}(\mathcal{O}_K)$. Das zeigt $K \subset \mathrm{Frac}(\mathcal{O}_K)$.

Beispiel 1.9. Trivialerweise gilt $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Beispiel 1.10. Sei $K = \mathbb{Q}(i)$. Wir behaupten, dass $\mathcal{O}_K$ gleich dem Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ ist. Für den Nachweis bemerken wir zunächst, dass $a + bi \in \mathbb{Q}(i)$ $(a, b \in \mathbb{Q})$ Nullstelle des normierten Polynoms

$$(X - (a + bi))(X - (a - bi)) = X^2 - 2aX + a^2 + b^2 \tag{1.3}$$

ist.

"$\mathbb{Z}[i] \subset \mathcal{O}_K$:" Sind $a, b \in \mathbb{Z}$, so ist das Polynom in (1.3) ganzzahlig und es folgt $a + bi \in \mathcal{O}_K$.

"$\mathcal{O}_K \subset \mathbb{Z}[i]$:" Sind umgekehrt $a, b \in \mathbb{Q}$, sodass (1.3) ganzzahlig ist, so folgt $2a, a^2+b^2 \in \mathbb{Z}$. Es gibt also $\tilde{a} \in \mathbb{Z}$ mit $a = \frac{\tilde{a}}{2}$. Es folgt

$$4(a^2 + b^2) = \tilde{a}^2 + 4b^2 \in 4\mathbb{Z}. \tag{1.4}$$

Es folgt $4b^2 \in \mathbb{Z}$, d.h. man kann $b = \frac{\tilde{b}}{2}$ mit $\tilde{b} \in \mathbb{Z}$ schreiben. Eingesetzt in (1.4) erhalten wir

$$\tilde{a}^2 + \tilde{b}^2 \equiv 0 \pmod 4. \tag{1.5}$$

Die einzigen Quadrate modulo 4 sind 0 und 1, und demnach kann (1.5) nur erfüllt sein, wenn $\tilde{a}^2 \equiv \tilde{b}^2 \equiv 0 \pmod 4$. Somit sind $\tilde{a}$ und $\tilde{b}$ gerade, d.h. $a, b \in \mathbb{Z}$.

In den folgenden Abschnitten werden wir die Struktur von Ganzheitsringen genauer untersuchen. Wir werden insbesondere zeigen, dass es sich dabei um *Dedekindringe* handelt.

1.0.1 Übungen

Aufgabe 1.0.1. Sei A ein beliebiger Ring.

(1) Zeigen Sie die Existenz eines nullteilerfreien Ringes R und eines surjektiven Ringhomomorphismus $\varphi\colon R \to A$.

Sei K ein Körper und $M \in \mathrm{Mat}(n \times n, K)$. Wir erinnern an die *Adjunkte* M^{adj} von M; dies ist die $(n \times n)$-Matrix, deren (j,i)-ter Eintrag $(-1)^{i+j}\det(M_{ij})$ ist, wobei M_{ij} die Streichmatrix ist, die aus M durch Streichen der i-ten Zeile und der j-ten Spalte entsteht. In der linearen Algebra beweist man dann die Formel

$$M^{\mathrm{adj}}M = MM^{\mathrm{adj}} = \det(M)I_n. \tag{1.6}$$

(2) Setzen Sie die Gültigkeit der Formel (1.6) für Körper voraus und beweisen Sie dann ihre Gültigkeit für Matrizen über dem Ring A.
Hinweis: Nach der vorherigen Teilaufgabe gibt es einen surjektiven Ringhomomorphismus $\varphi\colon R \to A$, wobei R wie in der vorherigen Teilaufgabe ist. Der Ring R hat einen Quotientenkörper.

Aufgabe 1.0.2. Finden Sie den Ganzheitsring von $\mathbb{Q}(\sqrt{3})$.

Aufgabe 1.0.3. Ist $\mathbb{Z}[\sqrt{5}]$ der Ganzheitsring von $\mathbb{Q}(\sqrt{5})$?

Aufgabe 1.0.4. Sei $K = \mathbb{Q}(\alpha)$, wobei α eine Nullstelle von $X^3 + X^2 - 2X + 8 \in \mathbb{Z}[X]$ sei. Finden Sie das Minimalpolynom von

$$\beta := \frac{\alpha + \alpha^2}{2}$$

über $\mathbb{Q}$. Ist β ganz?

Kapitel 2

Teilbarkeitstheorie und der Elementarteilersatz

Definition 2.1. Ein Ring[1] A heißt *Integritätsring* (oder *Integritätsbereich*), wenn A nullteilerfrei ist, d.h. wenn für alle $a, b \in A$ mit $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

Bemerkung 2.2. In einem Integritätsring A dürfen wir "kürzen": Sind $a \in A \setminus \{0\}$ und $b, c \in A$ mit $ab = ac$, dann erhalten wir $a(b - c) = 0$. Die Nullteilerfreiheit und $a \neq 0$ implizieren dann $b = c$.

Definition 2.3. Sei A ein Integritätsring und $a, b, \pi \in A$.

(1) Das Element π heißt *Primelement*, wenn $\pi \neq 0$, $\pi \notin A^*$ und wenn für alle $b_1, b_2 \in A$ mit $\pi \mid b_1 b_2$ gilt, dass $\pi \mid b_1$ oder $\pi \mid b_2$.

(2) Die Elemente $a, b \in A$ heißen *assoziiert*, wenn es eine Einheit $u \in A^*$ mit $a = u \cdot b$ gibt. (Weisen Sie zur Übung nach, dass es sich bei Assoziiertheit um eine Äquivalenzrelation handelt!)

(3) Das Element π heißt *irreduzibel*, wenn $\pi \neq 0$, $\pi \notin A^*$ und für alle $b_1, b_2 \in A$ mit $\pi = b_1 b_2$ gilt, dass $b_1 \in A^*$ oder $b_2 \in A^*$. (Slogan: "Eine Nichteinheit $\pi \neq 0$ ist irreduzibel, wenn jeder echte Teiler von π zu π assoziiert ist".)

Lemma 2.4. *Primelemente eines Integritätsrings sind stets irreduzibel.*

Beweis. Sei π ein Primelement des Integritätsrings A. Ferner seien $a, b \in A$ mit $\pi = ab$. Dann gilt also insbesondere $\pi \mid ab$. Da π prim ist, können wir ohne Einschränkung $\pi \mid a$ annehmen. Es gibt also ein $c \in A$ mit $c\pi = a$. Dann folgt

$$\pi = ab = bc\pi.$$

Durch Umstellen erhalten wir

$$(1 - bc)\pi = 0.$$

Da ein Integritätsbereich nullteilerfrei ist und $\pi \neq 0$, muss $bc = 1$ gelten, d.h. $b \in A^*$. Damit ist π irreduzibel. □

[1] kommutativ, $\neq \{0\}$, mit Einselement

Beispiel 2.5. Im Allgemeinen gilt die Umkehrung nicht, d.h. irreduzible Elemente sind nicht prim. Beispielsweise ist das Element $2 \in \mathbb{Z}[\sqrt{-5}]$ zwar irreduzibel, aber nicht prim – Details verifizieren Sie in Aufgabe 2.0.1.

Sei A ein Ring. Wir erinnern daran, dass ein *Primideal* von A ein Ideal $\mathfrak{p} \neq A$ mit der Eigenschaft

$$\forall a, b \in A\colon \qquad ab \in \mathfrak{p} \implies a \in \mathfrak{p} \quad \text{oder} \quad b \in \mathfrak{p}$$

ist. Ferner erinnern wir an

Lemma 2.6. *Sei A ein Ring und $\mathfrak{a} \subset A$ ein Ideal. Dann gilt:*

$$\mathfrak{a} \textit{ ist ein Primideal} \iff A/\mathfrak{a} \textit{ ist ein Integritätsring.}$$

Beweis. Es gilt für alle $c \in A$:

$$c \in \mathfrak{a} \iff c + \mathfrak{a} = 0 + \mathfrak{a} \text{ in } A/\mathfrak{a}.$$

Daraus folgen sofort beide Implikationen. □

Bemerkung 2.7. Sei A ein Ring.

(1) Das Ideal $(0) \subset A$ ist genau dann prim, wenn A ein Integritätsring ist.

(2) Ein Ideal $\mathfrak{a}$ von A ist genau dann maximal, wenn $A/\mathfrak{a}$ ein Körper ist. Lemma 2.6 sagt uns also, dass maximale Ideale auch prim sind.

Lemma 2.8. *Sei A ein Integritätsring und $\pi \in A$. Dann gilt:*

$$(\pi) \textit{ ist ein Primideal} \iff \pi = 0 \textit{ oder } \pi \textit{ ist ein Primelement.}$$

Beweis. Im Hinblick auf Bemerkung 2.7 (1) muss nur der Fall $\pi \neq 0$ betrachtet werden.

"$\Leftarrow$": Seien nun $\pi \in A$ ein Primelement und $a, b \in A$ mit $ab \in (\pi)$. Dann gibt es $c \in A$ mit $ab = c\pi$. Insbesondere gilt $\pi \mid ab$, also können wir ohne Einschränkung annehmen, dass π auch ein Teiler von a ist. Das heißt, dass es ein $d \in A$ mit $d\pi = a$ gibt, also $a \in (\pi)$. Also ist (π) ein Primideal.

"$\Rightarrow$": Ist $\pi \neq 0$ kein Primelement, so gibt es zwei Fälle:

(1) Ist $\pi \in A^*$, so ist $(\pi) = A$. Das Einsideal ist per Definition aber kein Primideal.

(2) Ist $\pi \notin A^*$, so gibt es $a, b \in A$ mit $\pi \mid ab$ (d.h. $ab \in (\pi)$), aber $\pi \nmid a$ (d.h. $a \notin (\pi)$) und $\pi \nmid b$ (d.h. $b \notin (\pi)$). Damit ist (π) kein Primideal.

□

Proposition 2.9. *Sei A ein Hauptidealring und $\pi \in A$ irreduzibel. Dann ist (π) ein maximales Ideal von A. Insbesondere gilt:*

(1) Die Begriffe "irreduzibel" und "Primelement" in Hauptidealringen überein.

(2) Jedes Primideal $\neq (0)$ in einem Hauptidealring ist maximal.

Beweis. Sei $\mathfrak{a} \subset A$ ein Ideal mit $(\pi) \subset \mathfrak{a} \subsetneq A$. Da A ein Hauptidealring ist, gibt es $a \in A \setminus A^*$ mit $\mathfrak{a} = (a)$. Wegen $(\pi) \subset \mathfrak{a} = (a)$ gilt $a \mid \pi$, d.h. es gibt ein $b \in A$ mit $ab = \pi$. Nun ist π irreduzibel und a keine Einheit (da $\mathfrak{a} = (a) \neq A$). Also folgt $b \in A^*$ und damit sind a und π assoziiert, d.h. $\mathfrak{a} = (a) = (\pi)$, was die Maximalität von (π) beweist. Die Aussagen (1) und (2) folgen nun zusammen mit Lemma 2.4 und Lemma 2.8. □

Definition 2.10. Ein Integritätsring A heißt faktoriell, wenn jedes $a \in A \setminus \{0\}$ eindeutig in der Form

$$a = u \cdot \pi_1 \cdot \ldots \cdot \pi_k$$

mit $u \in A^*$ und irreduziblen Elementen $\pi_1, \ldots, \pi_k$ geschrieben werden kann. "Eindeutig" heißt hierbei, dass die $\pi_1, \ldots, \pi_k$ bis auf Assoziiertheit eindeutig sind.

Beispiel 2.11. Da die positiven irreduziblen Elemente in $\mathbb{Z}$ genau die Primzahlen sind, ist $\mathbb{Z}$ faktoriell. Es ist Teil von Aufgabe 2.0.1 zu verifizieren, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist.

Genau wie in Hauptidealringen gilt die Implikation "irreduzibel $\implies$ prim" auch in faktoriellen Ringen:

Proposition 2.12. *Sei A faktoriell und $\pi \in A$. Dann gilt:*

$$\pi \text{ ist irreduzibel} \iff \pi \text{ ist prim.}$$

Beweis. Die Richtung "$\Leftarrow$" gilt unabhängig von der Faktorialität, vgl. Lemma 2.4. Für die Richtung "$\Rightarrow$" nehmen wir an, dass π irreduzibel ist. Ferner seien $a, b \in A \setminus \{0\}$ mit $\pi \mid ab$. Dann gibt es $c \in A$ mit $c\pi = ab$. Da A faktoriell ist, können wir a, b, c bis auf Einheiten als Produkt irreduzibler Elemente schreiben:

$$a = u \cdot p_1 \cdot \ldots \cdot p_k, \qquad b = v \cdot q_1 \cdot \ldots \cdot q_m, \qquad c = w \cdot r_1 \cdot \ldots \cdot r_n,$$

wobei $u, v, w \in A^*$ und p_i, q_j, r_ℓ irreduzibel seien. Die Gleichung $c\pi = ab$ liest sich dann wie folgt:

$$w \cdot r_1 \cdot \ldots \cdot r_n \cdot \pi = u \cdot v \cdot p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m.$$

Da die Zerlegung in irreduzible Elemente eindeutig ist, muss jedes r_ℓ auch auf der rechten Seite auftauchen. Wie in Bemerkung 2.2 können wir dann $r_1, \ldots, r_n$ auf beiden Seiten entfernen und erhalten eine Gleichung der Form

$$\pi = \pi_1' \cdot \ldots \cdot \pi_s'$$

mit irreduziblen Elementen $\pi_1', \ldots, \pi_s'$. Jedes der Elemente $\pi_1', \ldots, \pi_s'$ ist zu einem p_i oder q_j assoziiert, teilt also a oder b.
Nun nutzen wir erneut die eindeutige Faktorisierung in in irreduzible Elemente: Da π irreduzibel ist, kann auf der rechten Seite nur ein irreduzibles Element $\pi' = \pi_1'$ auftauchen, und dieses muss zu π assoziiert sein. Ist π' ein Teiler von a, so gilt $\pi \mid a$, andernfalls ist π' ein Teiler von b und wir erhalten $\pi \mid b$. Also ist π prim. □

Bemerkung 2.13. Da der Ring $\mathbb{Z}$ faktoriell ist, sind die Primzahlen ebenfalls Primelemente in $\mathbb{Z}$. Das rechtfertigt den Begriff "*Prim*element".

Da in Hauptidealringen und faktoriellen Ringen irreduzible Elemente jeweils prim sind, liegt das folgende Resultat nahe.

Satz 2.14. *Sei A ein Hauptidealring. Dann ist A faktoriell.*

Beweis. Wir zeigen zunächst die Existenz einer Faktorisierung in irreduzible Elemente. Sei $M \subset A \setminus \{0\}$ die Menge der Elemente, die keine Zerlegung in irreduzible Elemente besitzen. Wir wollen $M = \emptyset$ zeigen. Für einen Widerspruch nehmen wir an, dass $a \in M$ sei. Dann kann a weder eine Einheit noch irreduzibel sein, denn sonst wäre a seine eigene Zerlegung in irreduzible Elemente. Also gibt es Elemente $b, c \in A \setminus A^*$ mit $a = bc$. Dann muss mindestens eines der Elemente b und c in M enthalten sein – wären beide nicht in M enthalten, so wären b und c nämlich zu einem Produkt irreduzibler Elemente assoziiert, das Element a dann also auch. Ohne Einschränkung nehmen wir $b \in M$ an. Wir wiederholen den Prozess und schließen, dass b weder Einheit noch irreduzibel sein kann. Induktiv erhalten wir eine Folge von Elementen $(a_n)_{n\geq 0}$ in M mit

$$a_0 = a, \qquad \forall n \geq 0\colon \quad a_{n+1} \mid a_n, \qquad \text{und} \qquad a_{n+1} \text{ ist nicht zu } a_n \text{ assoziiert.}$$

Nun betrachten wir die echt (!) aufsteigende Kette der Hauptideale

$$(a) = (a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots \ .$$

Da $\mathfrak{a} = \bigcup_{n=0}^{\infty}(a_n)$ ein Ideal ist und A ein Hauptidealring ist, gibt es ein $d \in A$ mit $\mathfrak{a} = (d)$. Das Element d muss aber in einem der Ideale (a_N) enthalten sein. Wir erhalten den Widerspruch

$$\mathfrak{a} = (d) \subset (a_N) \subsetneq (a_{N+1}) \subset \mathfrak{a} = (d).$$

Also ist $M = \emptyset$, was die Existenz beweist.

Wir beweisen noch die Eindeutigkeit. Sei $a \in A \setminus \{0\}$ und

$$a = u \cdot \pi_1^{\nu_1} \cdot \ldots \cdot \pi_k^{\nu_k} = v \cdot \pi_1^{\mu_1} \cdot \ldots \cdot \pi_k^{\mu_k},$$

wobei $u, v \in A^*$, $\pi_1, \dots, \pi_k \in A$ irreduzibel und paarweise nicht assoziiert seien, sowie $\nu_i,\ \mu_j \geq 0$. Wir möchten $u = v$ und $\nu_i = \mu_i$ für $i = 1, \dots, k$ zeigen. Angenommen, es gälte $\nu_1 > \mu_1$, dann können wir wie in Bemerkung 2.2 kürzen und erhalten

$$u \cdot \pi_1^{\nu_1 - \mu_1} \cdot \pi_2^{\nu_2} \ldots \cdot \pi_k^{\nu_k} = v \cdot \pi_2^{\mu_2} \cdot \ldots \cdot \pi_k^{\mu_k}.$$

Da π_1 die linke Seite teilt, muss π_1 auch die rechte Seite teilen. Da π_1 irreduzibel ist und A ein Hauptidealring ist, ist π_1 prim und teilt somit v oder eines der Elemente $\pi_2, \dots, \pi_k$ (vgl. Proposition 2.9). Das ist aber nicht der Fall, da π_1 als irreduzibles Element keine Einheit teilt und $\pi_2, \dots, \pi_k$ nicht zu π_1 assoziiert sind – ein Widerspruch. Also gilt $\nu_i = \mu_i$ für alle i. Dann folgt aber sofort $u = v$. □

Bemerkung 2.15. Leicht modifiziert funktioniert der Existenzbeweis in Satz 2.14 auch, wenn A noethersch ist.

Bemerkung 2.16.

(1) Ist A faktoriell, so ist auch $A[X]$ faktoriell. Das folgt aus dem Lemma von Gauß.

(2) Nicht jeder faktorielle Ring ist ein Hauptidealring: Nach dem vorherigen Stichpunkt ist $\mathbb{Z}[X]$ faktoriell. Das Ideal $(2, X) \subset \mathbb{Z}[X]$ ist aber kein Hauptideal – machen Sie sich das klar!

(3) Zieht man Aufgabe 0.1.1 in Betracht, so haben wir Implikationen

$$\text{euklidisch} \implies \text{Hauptidealring} \implies \text{faktoriell}.$$

Im Allgemeinen gilt keine der Rückrichtungen. In der Tat ist $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ein nicht-euklidischer Hauptidealring (Nachweis später).

Zum Abschluss des Kapitels möchten wir noch den Elementarteilersatz diskutieren, den wir jedoch nicht beweisen werden.

Satz und Definition 2.17 (Elementarteilersatz)**.** Sei M ein freier $\mathbb{Z}$-Modul vom Rang r und $M' \subset M$ ein Untermodul. Dann existiert eine $\mathbb{Z}$-Basis $(m_1, \ldots, m_r)$ von M, ein $s \leq r$ und Zahlen $d_1, \ldots, d_s \in \mathbb{Z}_{>0}$ mit der Eigenschaft $d_i \mid d_{i+1}$ für alle i, sodass $(d_1 m_1, \ldots, d_s m_s)$ eine $\mathbb{Z}$-Basis von M' ist. Insbesondere ist M' frei vom Rang s. Die Zahlen $d_1, \ldots, d_s$ sind außerdem eindeutig bestimmt und heißen die *Elementarteiler* von M' in M.

Beweisskizze/Interpretation. Wie schon erwähnt, verzichten wir auf einen vollständigen Beweis, möchten aber die Philosophie hinter dem Resultat andeuten. Sei $(n_1, \ldots, n_r)$ eine $\mathbb{Z}$-Basis von M. Angenommen, wir wissen bereits, dass M' frei vom Rang $s \leq r$ ist, dann gibt es eine $\mathbb{Z}$-Basis $(n'_1, \ldots, n'_s)$ von M'. Diese können wir als A-Linearkombination von $(n_1, \ldots, n_r)$ schreiben:

$$n'_j = \sum_{i=1}^{r} a_{ij} n_i, \qquad a_{ij} \in \mathbb{Z}.$$

Sei $A = (a_{ij}) \in \mathrm{Mat}(r \times s, \mathbb{Z})$ (das ist also die darstellende Matrix der Inklusion $M' \to M$ bzgl. der angegebenen Basen). Die Aussage des Satzes ist es dann, dass es Matrizen $S \in \mathrm{GL}(r, \mathbb{Z})$ und $T \in \mathrm{GL}(s, \mathbb{Z})$ mit der Eigenschaft, dass

$$SAT = \begin{pmatrix} d_1 & 0 & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & \ldots & 0 & d_s \\ 0 & & \ldots & & 0 \\ \vdots & & & & \vdots \\ 0 & & \ldots & & 0 \end{pmatrix} \in \mathrm{Mat}(r \times s, \mathbb{Z})$$

und $d_i \mid d_{i+1}$ gibt. Mit anderen Worten: Durch Zeilen- und Spaltenumformungen über $\mathbb{Z}$ (!) kann A auf "Diagonal"form gebracht werden, □

Bemerkung 2.18.

(1) Allgemeiner gilt der Elementarteilersatz nicht nur für $\mathbb{Z}$-Moduln, sondern für Moduln über Hauptidealringen.

(2) Der Beweis des Elementarteilersatzes ist konstruktiv und ist hier zu finden.

Wir betrachten nun den Spezialfall $r = s$. In diesem Fall gilt mit der Notation aus obiger Beweisskizze $|\det(A)| = d_1 \cdot \ldots \cdot d_r$. Da ein $\mathbb{Z}$-Modul außerdem nichts anderes als eine abelsche Gruppe ist, ist in diesem Fall $M' \subset M$ eine Untergruppe von endlichem Index $(M : M') = |M/M'|$. Ist nun $(m_1, \ldots, m_r)$ eine $\mathbb{Z}$-Basis von M mit der Eigenschaft, dass $(d_1 m_1, \ldots, d_r m_r)$ eine $\mathbb{Z}$-Basis von M' ist, so haben wir einen Isomorphismus von Gruppen

$$\begin{aligned} &\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \to M/M', \\ &(c_1 + d_1\mathbb{Z}, \ldots, c_r + d_r\mathbb{Z}) \mapsto c_1 m_1 + \ldots + c_r m_r + M'. \end{aligned}$$

Wir haben also bewiesen:

Proposition 2.19. *In der obigen Situation gilt* $(M : M') = |\det(A)| = d_1 \cdot \ldots \cdot d_r$.

2.0.1 Übungen

Aufgabe 2.0.1. Betrachten Sie den Ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. In der Einleitung zum Skript wurde behauptet, dass dieser nicht faktoriell ist. Hier verifizieren Sie alle Details.

(1) Sei $N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ durch $N(a+b\sqrt{-5}) = a^2+5b^2$ definiert. Begründen Sie kurz, dass N multiplikativ ist, d.h. für alle $a, b, c, d \in \mathbb{Z}$ gilt

$$N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}).$$

(2) Zeigen Sie, dass ± 1 die einzigen Einheiten von $\mathbb{Z}[\sqrt{-5}]$ sind.

(3) Zeigen Sie, dass die Elemente $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ zwar irreduzibel, aber nicht prim sind.

(4) Folgern Sie, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist.

Aufgabe 2.0.2. Zeigen Sie, dass das Ideal $(2, X) \subset \mathbb{Z}[X]$ kein Hauptideal ist.

Aufgabe 2.0.3.

(1) Beweisen Sie den *Satz über rationale Nullstellen*:
Sei A ein faktorieller Ring mit Quotientenkörper K, sowie

$$f = a_n X^n + \ldots + a_1 X + a_0 \in A[X].$$

Ist $\alpha \in K$ eine Nullstelle von f, so gibt es $a, b \in A$, $b \neq 0$ mit $\alpha = \frac{a}{b}$ und $a \mid a_0$, $b \mid a_n$.

(2) Folgern Sie, dass faktorielle Ringe ganz abgeschlossen sind.

Aufgabe 2.0.4. Betrachte die $\mathbb{Z}$-lineare Abbildung $A \colon \mathbb{Z}^4 \to \mathbb{Z}^3$, die durch die folgende Matrix gegeben ist:

$$A = \begin{pmatrix} 1 & 1 & 6 & -3 \\ 3 & -2 & 6 & 4 \\ 4 & 3 & -2 & 5 \end{pmatrix}.$$

Studieren Sie den Beweis des Elementarteilersatzes und finden Sie die Elementarteiler von $\mathrm{im}(A) \subset \mathbb{Z}^4$.

Aufgabe 2.0.5. Sei $f\colon A \to B$ ein Ringhomomorphismus und $\mathfrak{p} \subset B$ ein Primideal. Verifizieren Sie, dass $f^{-1}(\mathfrak{p}) \subset A$ ein Primideal ist. Stimmt die Aussage auch, wenn man "Primideal" durch "maximales Ideal" ersetzt?

Aufgabe 2.0.6. Sei B/A eine ganze Ringerweiterung von Integritätsringen.

(1) Zeigen Sie:

$$B \text{ ist ein Körper } \iff A \text{ ist ein Körper.}$$

(2) Sei $\mathfrak{p} \subset B$ ein Primideal und $\mathfrak{p}' = \mathfrak{p} \cap A$. Zeigen Sie, dass $\mathfrak{p}'$ genau dann ein maximales Ideal von A ist, wenn $\mathfrak{p}$ ein maximales Ideal von B ist.

Sei K nun ein Zahlkörper.

(3) Folgern Sie, dass jedes Primideal $\neq (0)$ in $\mathcal{O}_K$ maximal ist. (Später werden wir dies noch mit anderen Methoden beweisen.)

Kapitel 3

Dedekindringe

3.1 Warum?

Motivation 3.1. In der Vorlesung "Kommutative Algebra" lernt man, was eine *affine Kurve* ist. Zum Zwecke dieser Motivation betrachten wir nur *ebene affine Kurven* über $\mathbb{C}$. Solche sind definiert als Nullstellenmengen eines nicht-konstanten Polynoms $f \in \mathbb{C}[x, y]$, in Formeln

$$X = \{(a, b) \in \mathbb{A}^2_{\mathbb{C}} \mid f(a, b) = 0\}.$$

Die Menge der *singulären Punkte* von X ist definiert durch

$$\mathrm{Sing}(X) = X \cap \left\{ (a, b) \in \mathbb{A}^2_{\mathbb{C}} \;\middle|\; \frac{\partial f}{\partial x}(a, b) = \frac{\partial f}{\partial y}(a, b) = 0 \right\}.$$

Des Weiteren kann man zu einer solchen Kurve X den *affinen Koordinatenring* $\mathbb{C}[X] = \mathbb{C}[x, y]/(f)$ assoziieren. Für jeden Punkt $p \in X$ ist

$$\mathfrak{m}_p = \{[g] \in \mathbb{C}[X] \mid g(p) = 0\}$$

ein maximales Ideal im Koordinatenring $\mathbb{C}[X]$. An diesem kann man *lokalisieren* – dadurch erhält man den *lokalen Ring*

$$\mathcal{O}_{X,p} := \mathbb{C}[X]_{\mathfrak{m}_p} = \left\{ \frac{g_1}{g_2} \;\middle|\; g_1, g_2 \in \mathbb{C}[X],\ g_2(p) \neq 0 \right\}.$$

In der Vorlesung "kommutative Algebra" wird nun bewiesen, dass $\mathcal{O}_{X,p}$ genau dann ein *diskreter Bewertungsring* ist, wenn $p \in X \setminus \mathrm{Sing}(X)$ ist. Wenn X eine glatte Kurve ist (das heißt $\mathrm{Sing}(X) = \emptyset$), dann heißt das, dass $\mathbb{C}[X]$ ein *Dedekindring* ist (zumindest, wenn X irreduzibel ist). Dieser Zusammenhang wird im Folgenden hergestellt. Während diskrete Bewertungsringe also die lokale Situation glatter affiner Kurven widerspiegeln, sind Dedekindringe das globale Äquivalent dazu. Es lohnt sich also, Dedekindringe genauer zu studieren.

Wir führen nun den Begriff des Dedekindrings ein.

Definition 3.2. Ein *Dedekindring* ist ein Integritätsbereich A mit den folgenden Eigenschaften:

(1) A ist noethersch,

(2) A ist ganz abgeschlossen,

(3) jedes Primideal $\neq (0)$ in A ist maximal, und

(4) A ist kein Körper.

Bemerkung. Die Bedingungen (3) und (4) kann man auch zu "A ist ein Ring der (Krull-)Dimension 1" zusammenfassen.

Bemerkung. Faktorielle Ringe sind automatisch ganz abgeschlossen (Aufgabe 2.0.3 (2)).

Wie in der Motivation angedeutet behaupte ich, dass Sie Dedekindringe bereits kennen.

Satz 3.3. *Sei A ein noetherscher Integritätsbereich der Dimension 1. Dann sind äquivalent:*

(1) A ist ein Dedekindring.

(2) Für alle Primideale $\mathfrak{p} \neq (0)$ in A ist der lokale Ring $A_\mathfrak{p}$ ein diskreter Bewertungsring.

Bevor wir den Beweis führen, wiederholen wir kurz die Lokalisierung von Moduln und diskrete Bewertungsringe.

Erinnerung. Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt *multiplikativ abgeschlossen*, wenn $1 \in S$ und wenn für alle $a, b \in S$ gilt, dass auch $ab \in S$. (Wichtigstes Beispiel: Ist $\mathfrak{p} \subset A$ ein Primideal, so ist $A \setminus \mathfrak{p}$ multiplikativ abgeschlossen.) Wir betrachten die folgende Relation auf $A \times S$:

$$(a_1, s_1) \sim (a_2, s_2) \iff \text{es gibt } t \in S, \text{ sodass } t \cdot (a_1 s_2 - a_2 s_1) = 0. \tag{3.1}$$

Dies ist eine Äquivalenzrelation. Die Menge der Äquivalenzklassen bezeichnen wir mit $S^{-1}A$, die Äquivalenzklasse von $(a, s) \in A \times S$ mit $\frac{a}{s}$. Mittels der wohldefinierten (!) Verknüpfungen

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}, \qquad \frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$$

wird $S^{-1}A$ zu einem Ring, der *Lokalisierung* von A an S. Im Spezialfall $S = A \setminus \mathfrak{p}$ für ein Primideal $\mathfrak{p} \subset A$ schreiben wir $A_\mathfrak{p}$ statt $(A \setminus \mathfrak{p})^{-1}A$ und sprechen von der Lokalisierung an $\mathfrak{p}$. (Beispiel: Ist A ein Integritätsring, so ist $\mathrm{Frac}(A) = A_{(0)}$.) Die Ringe $A_\mathfrak{p}$ sind *lokale Ringe*, d.h. sie haben genau ein maximales Ideal, nämlich

$$\mathfrak{p}A_\mathfrak{p} = \left\{ \frac{a}{s} \in A_\mathfrak{p} \;\middle|\; a \in \mathfrak{p},\ s \notin \mathfrak{p} \right\}.$$

Wir können auch einen A-Modul M an S lokalisieren, indem wir die Äquivalenzrelation (3.1) analog auf $M \times S$ definieren. So erhalten wir einen $S^{-1}A$-Modul $S^{-1}M$. Eine lineare Abbildung $f\colon M \to N$ von A-Moduln induziert eine lineare Abbildung

$$S^{-1}f\colon S^{-1}M \to S^{-1}N, \qquad \frac{m}{s} \mapsto \frac{f(m)}{s}$$

von $S^{-1}A$-Moduln. Ferner erinnern wir daran, dass für einen Homomorphismus $f\colon M \to N$ von A-Moduln äquivalent sind:

(1) f ist injektiv/surjektiv/ein Isomorphismus,

(2) für alle Primideale $\mathfrak{p} \subset A$ ist $f_{\mathfrak{p}} \colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ injektiv/surjektiv/ein Isomorphismus,

(3) für alle maximalen Ideale $\mathfrak{m} \subset A$ ist $f_{\mathfrak{m}} \colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ injektiv/surjektiv/ein Isomorphismus.

Man beweist nun leicht

Lemma 3.4. *Sei B/A eine Ringerweiterung und $\overline{A}$ der ganze Abschluss von A in B. Ist $S \subset A$ multiplikativ abgeschlossen, so ist $S^{-1}\overline{A}$ der ganze Abschluss von $S^{-1}A$ in $S^{-1}B$.*

Beweis. Sei $x \in \overline{A}$ und $s \in S$. Da x ganz über A ist, erfüllt x eine Gleichung der Form

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, \qquad a_i \in A.$$

Dann erfüllt $\frac{x}{s} \in S^{-1}\overline{A}$ die Gleichung

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s} \cdot \left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{a_0}{s^n} = 0.$$

Also ist $S^{-1}\overline{A}$ ganz über $S^{-1}A$.
Ist nun $b \in B$ und $t \in S$, sodass $\frac{b}{t} \in S^{-1}B$ ganz über $S^{-1}A$ ist, dann erfüllt $\frac{b}{t}$ eine Gleichung der Form

$$\left(\frac{b}{t}\right)^m + \frac{a'_{m-1}}{s_{m-1}} \cdot \left(\frac{b}{t}\right)^{m-1} + \ldots + \frac{a'_0}{s_0} = 0, \qquad a'_i \in A, \quad s_i \in S.$$

Sei $s := s_0 \cdot \ldots \cdot s_{m-1}$. Durchmultiplizieren der obigen Gleichung mit $(st)^m$ liefert eine Ganzheitsgleichung von bs über A. Es folgt $bs \in \overline{A}$, das heißt $\frac{b}{t} = \frac{bs}{st} \in S^{-1}\overline{A}$.

(Man bemerke die Ähnlichkeit zu Bemerkung 1.8 (2)). □

Erinnerung. Ein lokaler noetherscher Integritätsbereich $(A, \mathfrak{m})$ der Dimension 1 heißt *diskreter Bewertungsring*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(1) A ist ganz abgeschlossen,

(2) $\mathfrak{m}$ ist ein Hauptideal,

(3) Es ist $\mathfrak{m}/\mathfrak{m}^2$ ein 1-dimensionaler $A/\mathfrak{m}$-Vektorraum,

(4) Jedes Ideal $\neq (0)$ von A ist eine Potenz von $\mathfrak{m}$,

(5) Es gibt eine surjektive Abbildung ("Bewertung")

$$\nu \colon \operatorname{Frac}(A) \to \mathbb{Z} \cup \{\infty\},$$

sodass $A = \{x \in \operatorname{Frac}(A) \mid \nu(x) \geq 0\}$, und sodass die folgenden Bedingungen für alle $x, y \in \operatorname{Frac}(A)$ gelten:[1]

(a) $\nu(x) = \infty \iff x = 0$,

(b) $\nu(xy) = \nu(x) + \nu(y)$,

(c) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,

[1] Hierbei gelten die üblichen Rechenregeln $\infty + \infty = \infty$, $k + \infty = \infty + k = \infty$, sowie $\infty \geq \infty$ und $\infty \geq k$ für alle $k \in \mathbb{Z}$.

Für uns wird hauptsächlich die erste Eigenschaft relevant sein (d.h., dass diskrete Bewertungsringe ganz abgeschlossen sind), aber auch die letzte Eigenschaft wird eine Rolle spielen. Bedingung (3) ist wie folgt zu verstehen: Es ist $\mathfrak{m}^2$ ein A-Untermodul von $\mathfrak{m}$, also kann man den Quotientenmodul $\mathfrak{m}/\mathfrak{m}^2$ über A betrachten. Multipliziert man ein Element von $\mathfrak{m}/\mathfrak{m}^2$ jedoch mit einem Skalar aus $\mathfrak{m} \subset A$, so erhält man die triviale Klasse $0 + \mathfrak{m}^2$. Demnach kann man $\mathfrak{m}/\mathfrak{m}^2$ auch als Vektorraum über $A/\mathfrak{m}$ auffassen.

Nun beweisen wir Satz 3.3.

Beweis von Satz 3.3. Es ist nur zu zeigen, dass die ganze Abgeschlossenheit von A äquivalent zur ganzen Abgeschlossenheit von $A_\mathfrak{p}$ für jedes Primideal $\mathfrak{p}$ ist.
Sei $\overline{A}$ der ganze Abschluss von A und $\iota\colon A \hookrightarrow \overline{A}$ die Inklusion. Nach Lemma 3.4 ist $\overline{A}_\mathfrak{p}$ der ganze Abschluss von $A_\mathfrak{p}$. Es folgt

$$\begin{aligned} & A \text{ ist ganz abgeschlossen} \\ \iff & \iota \text{ ist ein Isomorphismus} \\ \iff & \iota_\mathfrak{p}\colon A_\mathfrak{p} \hookrightarrow \overline{A}_\mathfrak{p} \text{ ist ein Isomorphismus für alle Primideale } \mathfrak{p} \subset A \\ \iff & A_\mathfrak{p} \text{ ist für alle Primideale } \mathfrak{p} \subset A \text{ ganz abgeschlossen.} \end{aligned}$$

□

Als nächstes geben wir Beispiele von Dedekindringen.

Beispiel 3.5.

(1) Jeder Hauptidealring, der kein Körper ist, ist ein Dedekindring. Die ganze Abgeschlossenheit folgt hierbei aus Lemma 2.0.3 (2).

(2) Der Koordinatenring $\mathbb{C}[X]$ einer irreduziblen, glatten Kurve X über $\mathbb{C}$.

(3) Wir behaupten, dass $A = \mathbb{Z}[\sqrt{-5}]$ ein Dedekindring ist. Sicherlich ist A ein Integritätsbereich, der kein Körper ist. Da $\mathbb{Z}[X]$ noethersch ist (Hilbertscher Basissatz), ist $A = \mathbb{Z}[X]/(X^2+5)$ als Quotient eines noetherschen Rings noethersch. Um nachzuweisen, dass A ganz abgeschlossen ist, zeigen wir, dass $A = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ ist. Dazu betrachten wir ein Element $\gamma = a + b\sqrt{-5} \in \mathrm{Frac}(A) = \mathbb{Q}(\sqrt{-5})$ (wobei $a, b \in \mathbb{Q}$), das ganz, also Nullstelle eines Polynoms $\neq 0$ mit ganzzahligen Koeffizienten, ist. Wir schreiben $\overline{\gamma} := a - b\sqrt{-5}$. Dann gilt

$$(X - \gamma)(X - \overline{\gamma}) = X^2 - 2aX + a^2 + 5b^2.$$

Obiges Polynom hat genau dann ganzzahlige Koeffizienten, wenn $2a \in \mathbb{Z}$ und $a^2 + 5b^2 \in \mathbb{Z}$. Wie in Beispiel 1.10 impliziert dies, dass $a, b \in \mathbb{Z}$. Somit ist A in der Tat ganz abgeschlossen. Dass $\dim(A) = 1$ gilt, haben wir in Aufgabe 2.0.6 gesehen.

Spoiler. Wir werden bald sehen, dass Ganzheitsringe von Zahlkörpern Dedekindringe sind.

3.2 Primidealzerlegung

Wir wissen, dass der Ring $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist, es in diesem Ring also keine eindeutige Zerlegung in irreduzible Elemente gibt. Nutzt man die zusätzliche Struktur

von Dedekindringen, erhält man jedoch eine eindeutige Zerlegung in Prim*ideale*. Dafür müssen wir etwas arbeiten.

Lemma 3.6. *Sei A ein Ring und $\mathfrak{p} \subset A$ ein Primideal. Enthält $\mathfrak{p}$ ein Produkt $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$ von Idealen, so enthält $\mathfrak{p}$ eines der Ideale $\mathfrak{a}_i$.*

Beweis. Das ist Aufgabe 3.2.1. □

Lemma 3.7. *Sei A ein noetherscher Ring. Dann gilt:*

(1) Jedes Ideal von A enthält ein Produkt von Primidealen.

(2) Ist A ein Integritätsbereich, so enthält jedes Ideal $\neq (0)$ von A ein Produkt von Primidealen $\neq (0)$.

Beweis. Wir beweisen nur die zweite Aussage. Die erste Aussage wird analog bewiesen; man muss dazu nur drei Mal "$\neq (0)$" aus dem Beweis löschen – diese Stellen markieren wir farblich blau.
Wir beweisen die Aussage durch Widerspruch und nehmen dafür an, dass die Menge

$$M := \{\mathfrak{a} \subset A \mid \mathfrak{a} \neq (0) \text{ ist ein Ideal, das kein Produkt von Primidealen } \neq (0) \text{ enthält}\}$$

nicht leer ist. Als nicht-leere Menge von Idealen eines noetherschen Rings enthält M ein maximales Element $\mathfrak{b}$. Dieses Ideal $\mathfrak{b}$ ist nicht prim, sonst wäre $\mathfrak{b} \notin M$. Des Weiteren ist $\mathfrak{b} \neq A$. Demnach existieren $a_1, a_2 \in A \setminus \mathfrak{b}$ mit $a_1 a_2 \in \mathfrak{b}$. Die Ideale $\mathfrak{b} + (a_1)$ und $\mathfrak{b} + (a_2)$ enthalten $\mathfrak{b}$ als echtes Ideal und sind somit aufgrund der Maximalität von $\mathfrak{b}$ nicht in M enthalten. Es gibt somit Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$, die verschieden von (0) sind, sodass

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subset \mathfrak{b} + (a_1), \qquad \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subset \mathfrak{b} + (a_2).$$

Da jedoch $a_1 a_2 \in \mathfrak{b}$, folgt

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subset (\mathfrak{b} + (a_1))(\mathfrak{b} + (a_2)) \subset \mathfrak{b},$$

ein Widerspruch zu $\mathfrak{b} \in M$. □

Wie werden sehen, dass es sinnvoll ist, nicht nur "normale" Ideale zu betrachten.

Definition 3.8. Sei A ein Integritätsbereich mit Quotientenkörper K. Ein A-Untermodul $\mathfrak{a}$ von K heißt *gebrochenes Ideal*, wenn ein $d \in A \setminus \{0\}$ mit $d\mathfrak{a} \subset A$ existiert.

Bemerkung 3.9.

(1) Übliche Ideale in A sind gebrochene Ideale mit $d = 1$. Um sie von "echten" gebrochenen Idealen zu unterscheiden, nennen wir die Ideale in A oft *ganze Ideale*.

(2) Ist $\mathfrak{a}$ ein endlich-erzeugter A-Untermodul von K, so ist $\mathfrak{a}$ ein gebrochenes Ideal. Ist nämlich $\{x_1, \ldots, x_n\} \subset K$ ein Erzeugendensystem von I über A, so kann man $x_i = \frac{a_i}{d_i}$ mit $a_i, d_i \in A$ schreiben. Das Element $d = d_1 \cdot \ldots \cdot d_n$ hat dann die gewünschte Eigenschaft.

(3) Wenn A noethersch ist (z.B. ein Dedekindring), ist ein A-Untermodul von K genau dann ein gebrochenes Ideal, wenn er endlich erzeugt ist. Ist nämlich $\mathfrak{a} \subset K$ ein gebrochenes Ideal, so wähle man $d \neq 0$, sodass $d\mathfrak{a}$ ein Untermodul von A ist (also ein ganzes Ideal). Da A noethersch ist, ist so ist $d\mathfrak{a}$ endlich erzeugt, damit ist auch $\mathfrak{a}$ endlich erzeugt.

Wir wissen bereits, was das Produkt von ganzen Idealen ist. Für gebrochene Ideale machen wir das genau so.

Definition 3.10. Es seien $\mathfrak{a}_1, \mathfrak{a}_2$ gebrochene Ideale von A. Wir definieren das Produkt $\mathfrak{a}_1\mathfrak{a}_2$ als die Menge der endlichen Summen $\sum x_i y_i$ mit $x_i \in \mathfrak{a}_1$ und $y_i \in \mathfrak{a}_2$.

Bemerkung 3.11. Seien $\mathfrak{a}_1, \mathfrak{a}_2$ gebrochene Ideale.

(1) Offensichtlich gilt $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_2\mathfrak{a}_1$.

(2) Seien $d_1, d_2 \in A \setminus \{0\}$ so gewählt, dass $d_1\mathfrak{a}_1, d_2\mathfrak{a}_2 \subset A$. Dann sind $\mathfrak{a}_1 \cap \mathfrak{a}_2$, $\mathfrak{a}_1 + \mathfrak{a}_2$ und $\mathfrak{a}_1\mathfrak{a}_2$ wieder gebrochene Ideale, denn: dass es sich bei diesen Idealen um A-Untermoduln von K handelt, ist klar. Außerdem gilt

$$d_1(\mathfrak{a}_1 \cap \mathfrak{a}_2),\ d_2(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subset A, \qquad d_1 d_2(\mathfrak{a}_1 + \mathfrak{a}_2) \subset A, \qquad d_1 d_2 \mathfrak{a}_1 \mathfrak{a}_2 \subset A.$$

Wir nutzen jetzt die zusätzliche Struktur eines Dedekindrings.

Satz 3.12. *Sei A ein Dedekindring, $K = \mathrm{Frac}(A)$ und $\mathfrak{p} \neq (0)$ ein Primideal von A. Wir setzen*

$$\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subset A\}.$$

Dann ist $\mathfrak{p}^{-1}$ ein gebrochenes Ideal und es gilt $\mathfrak{p}^{-1}\mathfrak{p} = A$.

Beweis. Es ist klar, dass $\mathfrak{p}^{-1}$ ein A-Untermodul von K ist. Für jedes $d \in \mathfrak{p} \setminus \{0\}$ gilt per Definition $d\mathfrak{p}^{-1} \subset A$, also ist $\mathfrak{p}^{-1}$ ein gebrochenes Ideal. Wir müssen also nur noch $\mathfrak{p}^{-1}\mathfrak{p} = A$ zeigen. Per Definition von $\mathfrak{p}^{-1}$ ist die Inklusion "$\subset$" klar. Für die umgekehrte Inklusion bemerken wir zunächst, dass $A \subset \mathfrak{p}^{-1}$ gilt, da $\mathfrak{p}$ ein Ideal ist. Es folgt

$$\mathfrak{p} = A\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset A.$$

Also ist $\mathfrak{p}^{-1}\mathfrak{p}$ ein ganzes Ideal von A, das $\mathfrak{p}$ enthält. Als Primideal $\neq (0)$ in einem Dedekindring ist $\mathfrak{p}$ maximal, also folgt $\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}$ oder $\mathfrak{p}^{-1}\mathfrak{p} = A$. Wir müssen $\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}$ ausschließen. Wir nehmen also $\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}$ an und arbeiten auf einen Widerspruch hin. Für jedes $x \in \mathfrak{p}^{-1}$ haben wir dann $x\mathfrak{p} \subset \mathfrak{p}$ und damit auch

$$x^2\mathfrak{p} \subset x\mathfrak{p} \subset \mathfrak{p}, \qquad x^3\mathfrak{p} \subset x^2\mathfrak{p} \subset x\mathfrak{p} \subset \mathfrak{p}, \qquad \ldots,$$

also induktiv $x^m\mathfrak{p} \subset \mathfrak{p}$ für alle $m \geq 0$. Es folgt für beliebiges $d \in \mathfrak{p} \setminus \{0\}$:

$$\forall m \geq 0\colon \qquad dx^m \in A.$$

Mit anderen Worten: $A[x]$ ist ein gebrochenes Ideal. Nun verwenden wir, dass A noethersch ist, um zu schließen, dass $A[x]$ ein endlich-erzeugter A-Modul ist (Bemerkung 3.9 (3)). Das bedeutet, dass x ganz über A ist (Satz 1.1). Jedoch ist A ganz-abgeschlossen. Es folgt $x \in A$ und damit kann $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ nur gelten, wenn $\mathfrak{p}^{-1} = A$ gilt.
Wir schließen also noch $\mathfrak{p}^{-1} = A$ aus. Dafür sei $a \in \mathfrak{p} \setminus \{0\}$. Nach Lemma 3.7 enthält das Hauptideal $(a) \subset A$ ein Produkt von Primidealen $\neq (0)$. Sei $n \geq 1$ minimal mit der Eigenschaft, dass es n Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \neq (0)$ mit

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subset (a) \subset \mathfrak{p}.$$

gibt. Mit Lemma 3.6 folgt, dass $\mathfrak{p}$ eines der $\mathfrak{p}_i$ enthält, sagen wir $\mathfrak{p}_1 \subset \mathfrak{p}$. Da $\mathfrak{p}_1$ maximal ist, folgt $\mathfrak{p}_1 = \mathfrak{p}$. Wir setzen

$$\mathfrak{b} := \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n.$$

Die Minimalität von n impliziert, dass $\mathfrak{b} \nsubseteq (a)$. Wir können also ein $b \in \mathfrak{b}$ finden, das nicht in (a) enthalten ist. Da jedoch $\mathfrak{p}_1\mathfrak{b} = \mathfrak{p}\mathfrak{b} \subset (a)$ gilt, folgt $\mathfrak{p}ba^{-1} \subset A$. Es folgt also $ba^{-1} \in \mathfrak{p}^{-1}$ nach Definition von $\mathfrak{p}^{-1}$. Aus $b \notin (a)$ erhalten wir jedoch $ba^{-1} \notin A$, das heißt $\mathfrak{p}^{-1} \neq A$ wie gewünscht. □

Satz 3.13 (Dedekind)**.** *Sei A ein Dedekindring. Dann lässt sich jedes gebrochene Ideal $\mathfrak{b} \neq (0)$ eindeutig in der Form*

$$\mathfrak{b} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k}$$

schreiben[2]*, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ paarweise verschiedene Primideale des Ringes A sind und $\nu_1, \ldots, \nu_k \in \mathbb{Z} \setminus \{0\}$.*

Beweis. Wir beweisen zunächst die Existenz der Zerlegung. Sei dafür $\mathfrak{b} \neq (0)$ ein gebrochenes Ideal und $d \in A \setminus \{0\}$ so gewählt, dass $d\mathfrak{b} \subset A$. Dann gilt

$$\mathfrak{b} = (d\mathfrak{b})Ad^{-1} = (d\mathfrak{b})(Ad)^{-1},$$

weswegen es reicht, die Existenz der Primidealzerlegung für ganze Ideale zu beweisen. Ähnlich wie in den Beweisen von Lemma 3.7 und Satz 2.14 betrachten wir die Menge M der ganzen Ideale $\neq (0)$ von A, die kein Produkt von Primidealen sind und nehmen für einen Widerspruch an, dass M nicht leer ist. Da A noethersch ist, besitzt M dann ein maximales Element $\mathfrak{a}$. Da A selbst ein Produkt von Primidealen ist (das leere Produkt), gilt $\mathfrak{a} \neq A$. Es gibt also ein maximales Ideal $\mathfrak{m}$, das $\mathfrak{a}$ enthält. Es folgt mit Satz 3.12 nun aus $\mathfrak{a} \subset \mathfrak{m}$, dass

$$\mathfrak{a}\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = A. \tag{3.2}$$

Also ist $\mathfrak{a}\mathfrak{m}^{-1}$ ein ganzes Ideal.
Da $A \subset \mathfrak{m}^{-1}$ und $\mathfrak{a} = A\mathfrak{a}$, gilt aber auch $\mathfrak{a} \subset \mathfrak{a}\mathfrak{m}^{-1}$. Wir behaupten, dass $\mathfrak{a} \neq \mathfrak{a}\mathfrak{m}^{-1}$ gilt. Nehmen wir das Gegenteil $\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1}$ an, dann gilt für $x \in \mathfrak{m}^{-1}$ auch $x\mathfrak{a} \subset \mathfrak{a}$ und induktiv dann $x^n\mathfrak{a} \subset \mathfrak{a}$ für alle $n \geq 0$. Analog zum Beweis von Satz 3.12 erhalten wir dann $x \in A$. Das ist ein Widerspruch, da $\mathfrak{m}^{-1} \neq A$ (auch das haben wir im Beweis von Satz 3.12 gesehen – alternativ kann man es auch aus dem Ergebnis von Satz 3.12 folgern: Gälte $\mathfrak{m}^{-1} = A$, dann folgte der Widerspruch $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m} \neq A$).
Das zeigt also $\mathfrak{a} \subsetneq a\mathfrak{m}^{-1}$. Nun folgt aus der Maximalität von $\mathfrak{a}$, dass $\mathfrak{a}\mathfrak{m}^{-1} \notin M$. Gleichung (3.2) sagt aber, dass $\mathfrak{a}\mathfrak{m}^{-1}$ ein *ganzes* Ideal ist – als solches muss es also eine Zerlegung

$$\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

in Primideale besitzen. Multipliziert man beide Seiten mit $\mathfrak{m}$ und beachtet, dass $\mathfrak{m}\mathfrak{m}^{-1} = A$ gilt (Satz 3.12), so ist

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \cdot \mathfrak{m}$$

[2]Die Zerlegung von A selbst ist hierbei durch das leere Produkt gegeben. Für $\nu > 0$ und $\mathfrak{p} \neq (0)$ prim sei außerdem $\mathfrak{p}^{-\nu} := (\mathfrak{p}^{-1})^{\nu}$.

also eine Primidealzerlegung von $\mathfrak{a}$, ein Widerspruch zu $\mathfrak{a} \in M$.
Um die Eindeutigkeit der Zerlegung nachzuweisen, nehmen wir an, dass

$$\mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k} = \mathfrak{p}_1^{\mu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\mu_k}$$

für paarweise verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \subset A$, $\mathfrak{p}_i \neq (0)$ gilt. (Wir erlauben an dieser Stelle explizit, dass die ν_i und die μ_j auch 0 sein können – damit können wir erreichen, dass auf beiden Seiten der Gleichung dieselben Primideale auftauchen.) Aus Satz 3.12 folgt dann durch Umstellen

$$\mathfrak{p}_1^{\nu_1 - \mu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k - \mu_k} = A.$$

Wir beobachten, dass entweder $\nu_i = \mu_i$ für alle $i \in \{1, \ldots, k\}$ gilt (dann sind wir bereits fertig), oder die disjunkten (!) Mengen

$$I_+ := \{i \in \{1, \ldots, k\} \mid \nu_i - \mu_i > 0\} \text{ und } I_- := \{j \in \{1, \ldots, k\} \mid \nu_j - \mu_j < 0\}$$

sind beide (!) nicht leer. In letzterem Fall erhalten wir durch Umstellen

$$\prod_{i \in I_+} \mathfrak{p}_i^{\nu_i - \mu_i} = \prod_{j \in I_-} \mathfrak{p}_j^{\mu_j - \nu_j}.$$

Für $i_0 \in I_+$ enthält das Primideal $\mathfrak{p}_{i_0}$ also das Produkt $\prod_{j \in I_-} \mathfrak{p}_j^{\mu_j - \nu_j}$. Lemma 3.6 impliziert dann, dass $\mathfrak{p}_{i_0}$ ein $\mathfrak{p}_{j_0}$ für $j_0 \in I_-$ enthält. Jedoch sind beide der Ideale $\mathfrak{p}_{i_0}$ und $\mathfrak{p}_{j_0}$ maximal, also gleich – ein Widerspruch. □

Eine wichtige Folgerung aus dem Beweis ist:

Korollar 3.14. *Ein gebrochenes Ideal $\mathfrak{b} \neq (0)$ eines Dedekindrings A ist genau dann ganz, wenn in der Primidealzerlegung von $\mathfrak{b}$ nur nicht-negative Potenzen von Primidealen vorkommen.*

Beweis. Sei $\mathfrak{b} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k}$ die Primidealzerlegung. Gilt $\nu_1, \ldots, \nu_k \geq 0$, so ist $\mathfrak{b}$ natürlich ganz. Ist umgekehrt $\mathfrak{b}$ ganz, so haben wir im Beweis des Satzes von Dedekind 3.13 gesehen, dass dann $\nu_1, \ldots, \nu_k \geq 0$ gilt (wir haben die Menge der ganzen Ideale $\neq (0)$ betrachtet, die kein Produkt von Primidealen sind und gezeigt, dass diese Menge leer ist). □

Notation 3.15. Ist A ein Integritätsbereich und $(0) \neq \mathfrak{a}, \mathfrak{b} \subset A$ (ganze) Ideale, so schreibt man $\mathfrak{a} \mid \mathfrak{b}$, wenn $\mathfrak{b} \subset \mathfrak{a}$ gilt.

Die folgende Bemerkung erklärt die Notation.

Bemerkung 3.16. Sei A ein Integritätsbereich.

(1) Für $x, y \in A \setminus \{0\}$ gilt $(x) \mid (y)$ genau dann, wenn $x \mid y$.

(2) Die Teilbarkeitsrelation für ganze Ideale von A erfüllt dieselben Eigenschaften wie die Teilbarkeit von Ringelementen:

   (a) Reflexivität: Es gilt stets $\mathfrak{a} \mid \mathfrak{a}$.

   (b) Transitivität: Aus $\mathfrak{a} \mid \mathfrak{b}$ und $\mathfrak{b} \mid \mathfrak{c}$ folgt stets $\mathfrak{a} \mid \mathfrak{c}$.

(3) Seien A ein Dedekindring und $(0) \neq \mathfrak{a}, \mathfrak{b} \subset A$ ganze Ideale.

(a) $\mathfrak{a} \mid \mathfrak{b}$ bedeutet schlicht, dass jedes Primideal, das in der Primidealzerlegung von $\mathfrak{a}$ mit Exponent ν auftaucht, ebenfalls in der Primidealzerlegung von $\mathfrak{b}$ mit einem Exponenten $\geq \nu$ auftaucht. Das folgt aus Korollar 3.14.

(b) Insbesondere folgt aus $\mathfrak{a} \mid \mathfrak{b}$ die Existenz eines ganzen Ideals $\mathfrak{c}$ mit $\mathfrak{ac} = \mathfrak{b}$.

(c) Aus der Algebra kennen Sie den Begriff der Teilerfremdheit von Idealen: Die Ideale $\mathfrak{a}, \mathfrak{b}$ heißen teilerfremd, wenn $\mathfrak{a} + \mathfrak{b} = A$ gilt. Aus Aufgabe 3.2.7 folgt dann, dass die Ideale $\mathfrak{a}, \mathfrak{b}$ also genau dann teilerfremd sind, wenn es kein Primideal gibt, das beide Ideale teilt.

Beispiel 3.17. Wir betrachten den Dedekindring $\mathbb{Z}[\sqrt{-5}]$ und erinnern uns daran, dass ein Produkt von Idealen von allen Produkten der Erzeuger erzeugt wird. Demnach gilt

$$\begin{aligned}\left(2,\ 1+\sqrt{-5}\right)^2 &= \left(4,\ 2(1+\sqrt{-5}),\ -4+2\sqrt{-5}\right) = (2), \text{ und}\\ \left(3,\ 1+\sqrt{-5}\right)\left(3,\ -1+\sqrt{-5}\right) &= \left(9,\ -3+3\sqrt{-5},\ 3+3\sqrt{-5},\ 6\right) = (3).\end{aligned}$$

In Aufgabe 3.2.6 überlegen Sie sich, dass es sich bei den drei Idealen $\left(2,\ 1+\sqrt{-5}\right)$, $\left(3,\ 1+\sqrt{-5}\right)$ und $\left(3,\ -1+\sqrt{-5}\right)$ um Primideale handelt. Demnach ist die Primidealzerlegung von $(6) \subset \mathbb{Z}[\sqrt{-5}]$ durch

$$(6) = (2)(3) = \left(2,\ 1+\sqrt{-5}\right)^2\left(3,\ 1+\sqrt{-5}\right)\left(3,\ -1+\sqrt{-5}\right)$$

gegeben.

3.2.1 Übungen

Aufgabe 3.2.1. Beweisen Sie Lemma 3.6.

Aufgabe 3.2.2. Sei A ein Dedekindring und $(0) \neq \mathfrak{a} \subset A$ ein Ideal. Das Ziel dieser Aufgabe ist es zu beweisen, dass für jedes $x \in \mathfrak{a}\backslash\{0\}$ ein $y \in \mathfrak{a}$ existiert, sodass $\mathfrak{a} = (x, y)$. Gehen Sie wie folgt vor:

(1) Sei $\mathfrak{p} \subset A$ ein von (0) verschiedenes Primideal. Zeigen Sie, dass durch

$$\varphi\colon A_\mathfrak{p}/\mathfrak{p}^n A_\mathfrak{p} \to A/\mathfrak{p}^n, \qquad \frac{a}{b} + \mathfrak{p}^n A_\mathfrak{p} \mapsto (a+\mathfrak{p}^n)(b+\mathfrak{p}^n)^{-1} \qquad (a, b \in A,\ b \notin \mathfrak{p})$$

ein wohldefinierter Isomorphismus von Ringen beschrieben ist.

(2) Sei $(0) \neq \mathfrak{b} \subset A$ ein Ideal. Zeigen Sie, dass jedes Ideal in $A/\mathfrak{b}$ ein Hauptideal ist. *Hinweis:* Reduzieren Sie auf den Fall $\mathfrak{b} = \mathfrak{p}^n$ (Chinesischer Restsatz!) und wenden Sie die vorherige Teilaufgabe an.

(3) Folgern Sie die zu zeigende Aussage, indem Sie die vorherige Teilaufgabe auf ein geeignetes Ideal $\mathfrak{b}$ anwenden.

Aufgabe 3.2.3. Zeigen Sie, dass Dedekindringe genau dann Hauptidealringe sind, wenn sie faktoriell sind.

Aufgabe 3.2.4. Es sei A ein Dedekindring und $\mathfrak{a}_1, \mathfrak{a}_2 \neq (0)$ zwei ganze Ideale. Zeigen Sie, dass ein gebrochenes Ideal $\mathfrak{b} \neq (0)$ existiert, das zu $\mathfrak{a}_2$ teilerfremd ist, sodass $\mathfrak{a}_1\mathfrak{b}$ ein Hauptideal ist.

Aufgabe 3.2.5.

(1) Sei A ein Dedekindring und $\mathfrak{a} \neq (0)$ ein gebrochenes Ideal von A. Wir fixieren endlich viele paarweise verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \neq (0)$ von A. Zeigen Sie, dass ein $\alpha \in \mathfrak{a}$ mit der Eigenschaft $\nu_i(\mathfrak{a}) = \nu_i((\alpha))$ für alle $1 \leq i \leq n$ existiert. Hierbei bezeichnet $\nu_i(\mathfrak{b})$ den Exponenten von $\mathfrak{p}_i$ in der Primfaktorisierung eines gebrochenen Ideals $\mathfrak{b} \neq (0)$ von A.
Hinweis: Verwenden Sie die Aussage von Aufgabe 3.2.4.

(2) Folgern Sie die Aussage von Aufgabe 3.2.2 aus der obigen Teilaufgabe.

Aufgabe 3.2.6.

(1) Zeigen Sie, dass die Ideale

$$\left(2,\ 1+\sqrt{-5}\right),\ \left(3,\ 1+\sqrt{-5}\right) \text{ und } \left(3,\ -1+\sqrt{-5}\right)$$

prim in $\mathbb{Z}[\sqrt{-5}]$ sind.

(2) Zeigen Sie, dass das Ideal (5) in $\mathbb{Z}[\sqrt{-5}]$ nicht prim ist und geben Sie – mit Begründung – ein Primideal $\mathfrak{p}$ an, das (5) enthält. Verifizieren Sie dann $(5) = \mathfrak{p}^2$.

Aufgabe 3.2.7. Sei A ein Dedekindring und $(0) \neq \mathfrak{a}, \mathfrak{b} \subset A$ ganze Ideale mit Primfaktorisierung

$$\mathfrak{a} = \mathfrak{p}_1^{\mu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\mu_k} \text{ und } \mathfrak{b} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k},$$

wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ paarweise verschiedene Primideale sind und $\mu_i, \nu_j \geq 0$. Zeigen Sie:

$$\mathfrak{a} + \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\min\{\mu_i, \nu_i\}}, \qquad \mathfrak{a} \cap \mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\max\{\mu_i, \nu_i\}}.$$

Aufgabe 3.2.8. Sei $R = \mathbb{Z}[\sqrt{-3}]$.

(1) Zeigen Sie, dass R kein Dedekindring ist, indem Sie nachweisen, dass R eine der Eigenschaften aus Definition 3.2 nicht erfüllt.

(2) Sei $\mathfrak{p} = \left(2,\ 1+\sqrt{-3}\right)$. Zeigen Sie, dass $\mathfrak{p}$ ein Primideal ist.

(3) Zeigen Sie, dass $\mathfrak{p}^2 = (2)\mathfrak{p}$ und $(2) \neq \mathfrak{p}$ gilt. Folgern Sie daraus, dass wenn es in R eine Primidealzerlegung gibt, dann ist diese nicht eindeutig.

(4) Zeigen Sie, dass das Ideal $(2) \subset R$ keine Zerlegung in Primideale besitzt.

Somit ist sowohl die Existenz als auch die Eindeutigkeit der Primidealzerlegung in Nicht-Dedekindringen nicht gegeben.

Aufgabe 3.2.9. Zeigen Sie: Ein Dedekindring, der kein Hauptidealring ist, besitzt unendlich viele maximale Ideale.
Hinweis: Chinesischer Restsatz.

Aufgabe 3.2.10. Sei A ein Dedekindring. Zeigen Sie, dass jedes gebrochene Ideal von A ein *projektiver A-Modul* ist. Hierbei heißt ein A-Modul P *projektiv*, wenn jeder surjektive A-Modulhomomorphismus $f\colon M \to P$ einen sogenannten *Schnitt* besitzt, das ist ein A-Modulhomomorphismus $g\colon P \to N$, der rechtsinvers zu f ist.

3.3 Die Klassengruppe

Eine entscheidende Folgerung aus dem Satz von Dedekind 3.13 ist

Korollar 3.18. *Die Menge der von* (0) *verschiedenen gebrochenen Ideale eines Dedekindrings* A *ist eine abelsche Gruppe* I_A *bzgl. der Multiplikation gebrochener Ideale.*

Beweis. Ist $\mathfrak{b} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{\nu_k}$ die Primidealzerlegung eines gebrochenen Ideals $\mathfrak{b} \neq (0)$, so gilt $\mathfrak{b}\mathfrak{b}^{-1} = A$ für $\mathfrak{b}^{-1} = \mathfrak{p}_1^{-\nu_1} \cdot \ldots \cdot \mathfrak{p}_k^{-\nu_k}$. □

Bemerkung. Genauer zeigt der Satz von Dedekind 3.13, dass I_A eine freie abelsche Gruppe ist, deren Basis durch die Menge der Primideale $\neq (0)$ von A gegeben ist.

Bemerkung. Für jedes Primideal $\mathfrak{p} \neq (0)$ in einem Dedekindring A hat man einen Gruppenhomomorphismus $\nu_\mathfrak{p} \colon I_A \to \mathbb{Z}$, der $\mathfrak{a} \in I_A$ den Exponenten von $\mathfrak{p}$ in der Primfaktorisierung von $\mathfrak{a}$ zuordnet.

Die Gruppe I_A enthält die Untergruppe P_A der gebrochenen Hauptideale. Es ist dann möglich, die Faktorgruppe $\mathrm{Cl}_A := I_A/P_A$ zu betrachten.

Definition 3.19. Die Gruppe $\mathrm{Cl}_A = I_A/P_A$ heißt die *Klassengruppe* von A.

Im Allgemeinen sind Klassengruppen jedoch sehr schwer zu berechnen – der Fakt, dass I_A bzw. Cl_A Gruppen sind, erlaubt jedoch, Arithmetik mit Idealen zu betreiben.

Bemerkung 3.20. Offensichtlich ist die Klassengruppe eines Dedekindrings genau dann trivial, wenn er ein Hauptidealring ist (oder, gemäß Aufgabe 3.2.3, wenn er faktoriell ist). Die Klassengruppe "misst" also, wie weit ein Ring davon entfernt ist, ein Hauptidealring zu sein.

Wir werden uns im weiteren Verlauf der Vorlesung (Abschnitt 5.2) beweisen, dass die Klassengruppe von Ganzheitsringen sogar endlich ist – das ist ein tiefes Resultat!

3.3.1 Übungen

Aufgabe 3.3.1. Zeigen Sie, dass die Klassengruppe von $\mathbb{Z}[\sqrt{-5}]$ ein Element der Ordnung 2 besitzt.

Aufgabe 3.3.2. Sei A ein Dedekindring. Ein endlich erzeugter A-Modul M heißt *lokal frei vom Rang* n, wenn für jedes maximale Ideal $\mathfrak{m} \subset A$ der Modul $M_\mathfrak{m}$ ein freier $A_\mathfrak{m}$-Modul vom Rang n ist. Lokal freie Moduln vom Rang 1 werden *invertierbar* genannt. Zeigen Sie:

(1) Die gebrochenen Ideale von A sind invertierbare Moduln.

(2) Das Tensorprodukt $- \otimes_A -$ induziert auf der Menge der Isomorphieklassen invertierbarer Moduln eine Gruppenstruktur (dazu müssen natürlich das neutrale Element sowie das Inverse beschrieben werden). Die resultierende Gruppe $\mathrm{Pic}(A)$ wird die *Picard-Gruppe* von A genannt.

(3) Die natürliche Abbildung $\mathrm{Cl}_A \to \mathrm{Pic}(A)$ ist ein Isomorphismus.

Kapitel 4

Zahlkörper: Die Basics

Das Studium der Ganzheitsringe algebraischer Zahlkörper ist der Hauptgegenstand der algebraischen Zahlentheorie. In diesem Kapitel definieren wir Stück für Stück die nötigen Begriffe.

Beispiel 4.1. Wir erinnern daran, dass algebraische Zahlkörper endliche Körpererweiterungen von $\mathbb{Q}$ sind. Aus der Algebra kennen Sie viele Beispiele:

- $\mathbb{Q}$ selbst.
- Quadratische Zahlkörper: $\mathbb{Q}(\sqrt{d})$ für $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei (siehe auch Aufgabe 4.1.1).
- Kreisteilungskörper: $\mathbb{Q}(\zeta_m)$, wobei ζ_m eine primitive $m$te Einheitswurzel ist.
- $\mathbb{Q}[X]/(f)$ mit $f \in \mathbb{Q}[X]$ irreduzibel.

4.1 Einbettungen von Körpern

Aus Ihrer Algebravorlesung kennen Sie den *Fortsetzungssatz für Körperhomomorphismen*, den wir hier in einem Spezialfall wiederholen möchten.

Satz 4.2. *Sei L/K eine separable Körpererweiterung vom Grad n. Dann gibt es für einen fixierten algebraischen Abschluss $\overline{K}$ genau n verschiedene Körperhomomorphismen $L \hookrightarrow \overline{K}$, die die Identität auf K fortsetzen.*

Beweis. Nach dem Satz vom primitiven Element (der anwendbar ist, da L/K endlich und separabel ist) gibt es ein $\alpha \in L$, sodass $L = K[\alpha] \cong K[X]/(m_\alpha)$: Hierbei ist ein Isomorphismus durch $\alpha \mapsto X + (m_\alpha)$ gegeben.
x Wir beweisen nun zunächst, dass es mindestens n Einbettungen gibt. Da L/K separabel ist, sind die n Nullstellen $\alpha_1, \dots, \alpha_n \in \overline{K}$ des Minimalpolynoms m_α von α paarweise verschieden. Der Kern des Einsetzungsmorphismus $\mathrm{ev}_{\alpha_j} \colon K[X] \to \overline{K}$, $P \mapsto P(\alpha_j)$ enthält m_α; somit erhalten wir nach dem Homomorphiesatz induzierte Ringhomomorphismen $K[X]/(m_\alpha) \to \overline{K}$. Schließlich bekommen wir Abbildungen $\sigma_j \colon L \to \overline{K}$, die α auf α_j abbilden. Diese sind injektiv, da L ein Körper ist.
Es bleibt zu zeigen, dass es höchstens n Einbettungen gibt. Wenn $\sigma \colon L \hookrightarrow \overline{K}$ eine Einbettung ist, die id_K fortsetzt, dann gilt

$$m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0,$$

und somit ist $\sigma(\alpha)$ eine der Nullstellen $\alpha_1, \ldots, \alpha_n$. Wir haben bereits gesehen, dass σ durch das Bild von α eindeutig bestimmt ist. □

Bemerkung 4.3. Im Spezialfall eines Zahlkörpers K spricht man oft von den *komplexen Einbettungen* von K, das heißt von Körperhomomorphismen $K \hookrightarrow \mathbb{C}$.
Sei $\sigma\colon K \hookrightarrow \mathbb{C}$ eine solche Einbettung. Dann ist die komplex konjugierte Abbildung

$$\overline{\sigma}\colon K \hookrightarrow \mathbb{C}, \qquad a \mapsto \overline{\sigma(a)}$$

ebenfalls eine komplexe Einbettung. Die Einbettung σ heißt *reell*, falls $\sigma = \overline{\sigma}$ gilt. Das ist äquivalent dazu, dass das Bild von σ in $\mathbb{R}$ enthalten ist. Wenn σ nicht reell ist, so ist $\{\sigma, \overline{\sigma}\}$ ein Paar komplex konjugierter Einbettungen. Bezeichnet r die Anzahl der reellen Einbettungen von K und s die Anzahl der Paare komplex konjugierter Einbettungen, so erhalten wir also

$$[K : \mathbb{Q}] = r + 2s.$$

Das Tupel (r, s) heißt der *Typ* von K. Der Körper K heißt *total reell*, falls $r = n$ ist (also wenn $s = 0$ ist) und *total imaginär*, wenn $s = \frac{n}{2}$ ist (also wenn $r = 0$ ist).

Die komplexen Einbettungen eines Zahlkörpers werden im Verlauf der Vorlesung eine wichtige Rolle spielen. Die Höhepunkte stellen sicherlich die Endlichkeit der Klassenzahl (Abschnitt 5.2) und der Einheitensatz von Dirichlet (Abschnitt 5.4) dar.

Beispiel 4.4.

(1) Sei $K = \mathbb{Q}[X]/(X^2+1) = \mathbb{Q}[\sqrt{-1}]$, wobei $\sqrt{-1} = X + (X^2+1)$ die Klasse von X in K sei. Dann sind die zwei Einbettungen $K \hookrightarrow \mathbb{C}$ durch $\sqrt{-1} \mapsto \pm i$ gegeben. Der Typ von K ist also $(0, 1)$ und K ist total imaginär.

(2) Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das nur reelle Nullstellen hat. Dann ist $K = \mathbb{Q}[X]/(f)$ total reell.

(3) Sei $K = \mathbb{Q}(\alpha)$, wobei α eine Nullstelle von $X^3 - 2$ ist. Die drei komplexen Einbettungen von K sind dann durch

$$\alpha \mapsto \sqrt[3]{2}, \qquad \alpha \mapsto \omega\sqrt[3]{2}, \qquad \alpha \mapsto \omega^2\sqrt[3]{2}$$

mit $\omega = \exp\left(\frac{2\pi i}{3}\right)$ gegeben. Nur die erste dieser drei Einbettungen ist reell, damit ist K vom Typ $(1, 1)$.

4.1.1 Übungen

Aufgabe 4.1.1. Sei K ein quadratischer Zahlkörper, d.h. $[K : \mathbb{Q}] = 2$. Zeigen Sie, dass ein quadratfreies $d \in \mathbb{Z} \setminus \{0, 1\}$ mit $K = \mathbb{Q}(\sqrt{d})$ existiert. Finden Sie d in den Fällen $K = \mathbb{Q}(i), \mathbb{Q}(\zeta_3), \mathbb{Q}(\alpha)$, wobei α eine Nullstelle von $\frac{1}{5}X^2 + 2X + 2 \in \mathbb{Q}[X]$ ist.

Aufgabe 4.1.2. Sei K ein Zahlkörper. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(1) K ist total imaginär und enthält einen total reellen Teilkörper F mit $[K : F] = 2$.

(2) Es gibt $\rho \in \mathrm{Aut}(K) \setminus \{\mathrm{id}_K\}$, sodass $\sigma \circ \rho = \overline{\sigma}$ für alle Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$ gilt.

(3) Es gibt eine nicht-triviale Involution ρ von K, sodass $\sigma \circ \rho = \overline{\sigma}$ für alle Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$ gilt.

(4) K kann in der Form $K = F[\alpha]$ geschrieben werden, wobei F ein total reeller Körper ist und $\alpha \in K$, sodass $\alpha^2 \in F$ und $\sigma(\alpha^2) < 0$ für alle Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$.

Ein Zahlkörper K, der die obigen äquivalenten Bedingungen erfüllt, heißt *CM-Körper*. Die Abkürzung "CM" steht für *complex multiplication*.

Aufgabe 4.1.3. Zeigen Sie die folgenden Aussagen:

(1) Teilkörper von CM-Körpern sind entweder wieder CM-Körper oder total reell.

(2) Sei L ein Körper und $K_1, K_2 \subset L$ zwei CM-Körper, so ist der kleinste Teilkörper K_1K_2 von L, der K_1 und K_2 enthält, wieder ein CM-Körper.

(3) Sei K ein CM-Körper. Wir fixieren eine Einbettung $K \subset \mathbb{C}$. Zeigen Sie, dass der Galoisabschluss L von K in $\mathbb{C}$ ein CM-Körper ist.

Aufgabe 4.1.4. Bestimmen Sie alle $m \geq 1$, für die der Kreisteilungskörper $K_m = \mathbb{Q}(\zeta_m)$ ein CM-Körper ist. Geben Sie in diesem Falle einen total reellen Teilkörper F_m von K_m an, sodass $[K_m : F_m] = 2$.

4.2 Norm und Spur

Sei A ein Ring und B ein Ring, der ein freier A-Modul vom Rang n ist[1]. Wir diskutieren Norm und Spur der Ringerweiterung B/A. Speziell wird uns natürlich der Fall $K/\mathbb{Q}$ interessieren.

Definition 4.5. Sei B/A wie oben. Für $\beta \in B$ betrachten wir die A-lineare Abbildung $L_\beta\colon B \to B$, $x \mapsto \beta x$. Dann ist die *Norm* von β definiert durch $N_{B/A}(\beta) = \det(L_\beta)$. Ähnlich ist die *Spur* von β definiert durch $\mathrm{tr}_{B/A}(\beta) = \mathrm{tr}(L_\beta)$.

Bemerkung 4.6. Sei B/A wie oben (d.h. B ist ein freier A-Modul vom Rang n). Es gelten folgende elementare Eigenschaften von Norm und Spur:

(1) Für $\beta \in B$ ist L_β eine A-lineare Abbildung, somit gilt $N_{B/A}(\beta), \mathrm{tr}_{B/A}(\beta) \in A$.

(2) Für $a \in A$ gilt $L_a = a \cdot \mathrm{id}_B$. Damit folgt $N_{B/A}(a) = a^n$ sowie $\mathrm{tr}_{B/A}(a) = n \cdot a$.

(3) Da für $\alpha, \beta \in B$ gilt, dass $L_{\alpha\beta} = L_\alpha \circ L_\beta$, ist die Norm nach dem Determinantenmultiplikationssatz multiplikativ, d.h. $N_{B/A}(\alpha\beta) = N_{B/A}(\alpha)N_{B/A}(\beta)$. Insbesondere gilt $N_{B/A}(\beta) \neq 0$, falls β eine Einheit ist.

(4) Da für $\alpha, \beta \in B$ gilt, dass $L_{\alpha+\beta} = L_\alpha + L_\beta$, ist die Spur additiv, d.h. $\mathrm{tr}_{B/A}(\alpha+\beta) = \mathrm{tr}_{B/A}(\alpha) + \mathrm{tr}_{B/A}(\beta)$.

(5) Die obigen Eigenschaften implizieren, dass durch $\langle \alpha, \beta \rangle = \mathrm{tr}_{B/A}(\alpha\beta)$ eine symmetrische A-Bilinearform auf B definiert wird. Sie wird die *Spurform* von B/A genannt.

Wir spezialisieren uns auf den Fall einer endlichen Körpererweiterung.

Lemma 4.7. *Sei L/K eine endliche Körpererweiterung von Körpern der Charakteristik 0. Ferner seien $[L : K] = n$ und $\alpha \in L$.*

[1] Es lässt sich zeigen, dass jeder Ring A (wobei "Ring" im Sinne dieser Vorlesung zu verstehen ist) die "Invariant Basis Number"-Eigenschaft hat, d.h aus $A^n \cong A^m$ folgt $n = m$. Das ist nicht trivial. Sprechen Sie mich an, wenn Sie an einem Beweis interessiert sind.

(1) Ist $m_\alpha = X^m + b_{m-1}X^{m-1} + \ldots + b_0 \in K[X]$ *das Minimalpolynom von* α*, so gilt:*

$$N_{L/K}(\alpha) = (-1)^n \cdot b_0^{n/m}, \qquad \mathrm{tr}_{L/K}(\alpha) = -\frac{n}{m} \cdot b_{m-1}.$$

(2) Sind $\sigma_1, \ldots, \sigma_n \colon L \hookrightarrow \overline{L}$ *die verschiedenen Einbettungen von* L*, so gilt:*

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Bevor wir mit dem Beweis starten, möchten wir anmerken, dass die Aussagen des Lemmas auch für allgemeine endliche separable Erweiterungen gelten (mit demselben Beweis). Wenn in (1) allerdings die Charakteristik von K ein Teiler von m ist, so ergibt es keinen Sinn, $\frac{n}{m}$ zu schreiben. Jedoch ist m ein Teiler von n, und somit bezeichnet $\frac{n}{m}$ eine natürliche Zahl k, und die Aussagen in (1) können dann zu

$$N_{L/K}(\alpha) = (-1)^n \cdot b_0^k \qquad \text{bzw.} \qquad \mathrm{tr}_{L/K}(\alpha) = -k \cdot b_{m-1}$$

umformuliert werden.

Beweis. Wir beweisen die beiden Aussagen simultan. Dafür betrachten wir zunächst den Spezialfall, in dem α ein primitives Element von L/K ist, d.h. $L = K(\alpha)$. In diesem Fall ist $m = \deg(m_\alpha) = n$ und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine K-Basis von L. Wir schreiben $L_\alpha(\alpha^i)$ in dieser Basis, um die darstellende Matrix von L_α zu berechnen:

$$L_\alpha(\alpha^i) = \alpha^{i+1} = \begin{cases} \alpha^{i+1}, & \text{falls } i \neq n-1 \\ -b_{n-1}\alpha^{n-1} - \ldots - b_0, & \text{falls } i = n-1. \end{cases}$$

Damit ist die darstellende Matrix von L_α gerade die Begleitmatrix

$$M := \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & -b_0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & -b_1 \\ 0 & 1 & 0 & \ldots & 0 & 0 & -b_2 \\ \vdots & & \ddots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 & -b_{n-1} \end{pmatrix}.$$

Elementare Eigenschaften von Begleitmatrizen zeigen, dass das charakteristische Polynom von M gerade $(-1)^n \cdot m_\alpha$ ist (alternativ bemerkt man, dass das charakteristische Polynom von M natürlich Koeffizienten in K hat und α als Nullstelle hat – da es außerdem den Grad n hat, folgt die Behauptung). Da L/K als Erweiterungen von Körpern der Charakteristik 0 separabel ist, hat m_α die n verschiedenen Nullstellen $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Die Matrix M hat über $\overline{K}$ also n verschiedene Eigenwerte, ist also diagonalisierbar und ähnlich zur Matrix

$$\mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

Damit folgen die Aussagen (1), (2) im Spezialfall $L = K(\alpha)$.

Im allgemeinen Fall (also $m \leq n$) wählen wir eine $K(\alpha)$-Basis $\{\beta_1, \ldots, \beta_k\}$ von L. Dann ist

$$\{\alpha^i \beta_j \mid i = 0, \ldots, m-1,\ j = 1, \ldots, k\} \tag{4.1}$$

eine K-Basis von L. Erneut bestimmen wir die darstellende Matrix von L_α bezüglich dieser Basis. Dafür fixieren wir $j \in \{1, \ldots, k\}$ und berechnen

$$L_\alpha(\alpha^i \beta_j) = \alpha^{i+1}\beta_j = \begin{cases} \alpha^{i+1}\beta_j, & \text{falls } i \neq m-1 \\ -b_{m-1}\alpha^{m-1}\beta_j - \ldots - b_0\beta_j, & \text{falls } i = m-1. \end{cases}$$

Die Rechnung zeigt, dass die Einschränkung des Endomorphismus L_α auf den K-Vektorraum $\beta_j K[\alpha] = \langle \beta_j, \alpha\beta_j, \ldots, \alpha^{m-1}\beta_j \rangle$ definiert, und dass die Darstellungsmatrix von $L_\alpha|_{\beta_j K[\alpha]}$ bezüglich der angegebenen Basis wieder gerade M ist. Aus (4.1) folgt, dass

$$L = \beta_1 K[\alpha] \oplus \ldots \oplus \beta_k K[\alpha]$$

als K-Vektorräume gilt. Insgesamt erhalten wir, dass die darstellende Matrix von L_α bezüglich der Basis (4.1) gerade die Blockdiagonalmatrix

$$\begin{pmatrix} M & 0 & 0 & \ldots & 0 \\ 0 & M & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \ldots & M \end{pmatrix}$$

ist. Die Anzahl der Blöcke auf der Diagonale ist hierbei $k = \frac{n}{m}$. Es folgt

$$\begin{aligned} N_{L/K}(\alpha) &= \det(L_\alpha) = \det(M)^k = \left(N_{K(\alpha)/K}(\alpha)\right)^k, \quad \text{und} \\ \operatorname{tr}_{L/K}(\alpha) &= \operatorname{tr}(L_\alpha) = k \cdot \operatorname{tr}(M) = k \cdot \operatorname{tr}_{K(\alpha)/K}(\alpha). \end{aligned}$$

Da wir $N_{K(\alpha)/K}(\alpha)$ und $\operatorname{tr}(K(\alpha)/K)$ bereits kennen, ist das Lemma bewiesen. □

Beispiel 4.8. Sei $K = \mathbb{Q}(\sqrt[4]{7})$. Das Minimalpolynom von $\sqrt[4]{7}$ über $\mathbb{Q}$ ist $X^4 - 7$. Also gilt

$$\operatorname{tr}_{K/\mathbb{Q}}(\sqrt[4]{7}) = 0 \qquad \text{und} \qquad N_{K/\mathbb{Q}}(\sqrt[4]{7}) = -7.$$

Da die Spur additiv ist, erhalten wir dadurch für $a, b, c, d \in \mathbb{Q}$:

$$\operatorname{tr}_{K/\mathbb{Q}}(a + b\sqrt[4]{7} + c\sqrt[4]{7}^2 + d\sqrt[4]{7}^3) = \operatorname{tr}_{K/\mathbb{Q}}(a) = 4a.$$

Die Norm ist nicht additiv. Stattdessen nutzen wir die vier Nullstellen $\sqrt[4]{7}$, $-\sqrt[4]{7}$, $i\sqrt[4]{7}$ und $-i\sqrt[4]{7}$ von $X^4 - 7$, um sie zu berechnen:

$$\begin{aligned} N_{K/\mathbb{Q}}(a + b\sqrt[4]{7} + c\sqrt[4]{7}^2 + d\sqrt[4]{7}^3) &= (a + b\sqrt[4]{7} + c\sqrt[4]{7}^2 + d\sqrt[4]{7}^3)(a - b\sqrt[4]{7} + c\sqrt[4]{7}^2 - d\sqrt[4]{7}^3) \\ &\quad (a + ib\sqrt[4]{7} - c\sqrt[4]{7}^2 - id\sqrt[4]{7}^3)(a - ib\sqrt[4]{7} - c\sqrt[4]{7}^2 + id\sqrt[4]{7}^3) \\ &= \text{wirklich keine Lust, das auszumultiplizieren.} \end{aligned}$$

Beispiel 4.9 (Wichtigstes Beispiel)**.** Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, also $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Das Minimalpolynom von $\sqrt{d}$ über $\mathbb{Q}$ ist $X^2 - d$. Somit gilt

$$N_{K/\mathbb{Q}}(\sqrt{d}) = -d \qquad \text{und } \operatorname{tr}_{K/\mathbb{Q}}(\sqrt{d}) = 0.$$

Allgemeiner gilt für $a, b \in \mathbb{Q}$:

$$N_{K/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \qquad \text{und } \operatorname{tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a.$$

4.2.1 Aufgaben

Aufgabe 4.2.1. Es sei L/K eine endliche Galoiserweiterung, $L \subset \mathbb{C}$. Zeigen Sie $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$ für $\alpha \in L$.

Aufgabe 4.2.2. Sei K ein Zahlkörper, $\alpha \in \mathcal{O}_K$. Zeigen Sie, dass $N_{K/\mathbb{Q}}(\alpha)$ und $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$ ganze Zahlen sind. Folgern Sie daraus, dass α genau dann eine Einheit in $\mathcal{O}_K$ ist, wenn $N_{K/\mathbb{Q}}(\alpha) \in \{\pm 1\}$ gilt.

4.3 Diskriminanten

Wir nutzen die im vorherigen Abschnitt eingeführte Spur, um die *Diskriminante* zu diskutieren.

Definition 4.10. Sei A ein Ring und B eine Ringerweiterung von A, die ein endlich erzeugter freier A-Modul mit Basis $\underline{e} = (e_1, \ldots, e_n)$ ist. Wir definieren die *Diskriminante* von B bzgl. der A-Basis $\underline{e}$ durch

$$d_{B/A}(\underline{e}) := d_{B/A}(e_1, \ldots, e_n) := \det\left(\left(\mathrm{tr}_{B/A}(e_i e_j)\right)_{1 \le i,j \le n}\right) \in A.$$

Bemerkung 4.11. Sei V ein endlich-dimensionaler euklidischer Vektorraum mit Skalarprodukt $(\ ,\ )$. Das Volumen des Parallelotops

$$\left\{ \sum_{i=1}^{n} \lambda_i v_i \mid 0 \le \lambda_i \le 1 \right\},$$

das durch $v_1, \ldots, v_n \in V$ aufgespannt wird, ist gleich der Gramschen Determinante

$$g(v_1, \ldots, v_n) = \sqrt{\det\left(((v_i, v_j))_{1 \le i,j \le n}\right)}.$$

Die Diskriminante aus Definition 4.10 kann also als ein algebraisches Analogon des Volumens verstanden werden, indem wir statt eines Skalarprodukts die A-wertige Bilinearform $\langle x, y \rangle = \mathrm{tr}_{B/A}(xy)$ auf B betrachten.

Wie üblich möchten wir von *der* Diskriminante von B sprechen – wir müssen also diskutieren, inwiefern die Wahl einer anderen Basis die Diskriminante ändert.

Lemma 4.12. *Sind $\underline{e} = (e_1, \ldots, e_n)$ und $\underline{e'} = (e'_1, \ldots, e'_n)$ zwei A-Basen von B, so gibt es eine Einheit $u \in A^*$ mit*

$$d_{B/A}(\underline{e'}) = u^2 d_{B/A}(\underline{e}).$$

Beweis. Wir können jedes e'_i als A-Linearkombination bzgl. $\underline{e}$ schreiben:

$$e'_i = \sum_{j=1}^{n} a_{ij} e_j.$$

Unter Verwendung der A-Bilinearität der Spur erhalten wir dann dann

$$\mathrm{tr}_{B/A}(e'_i e'_j) = \mathrm{tr}_{B/A}\left(\sum_{k=1}^{n} a_{ik} e_k \sum_{\ell=1}^{n} a_{j\ell} e_\ell\right) = \sum_{k=1}^{n}\sum_{\ell=1}^{n} a_{ik}\, \mathrm{tr}_{B/A}(e_i e_j) a_{j\ell}.$$

Es folgt also mit $U = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(A)$:

$$\left(\mathrm{tr}_{B/A}(e_i' e_j')\right)_{1\leq i,j\leq n} = U \left(\mathrm{tr}_{B/A}(e_i e_j)\right)_{1\leq i,j\leq n} U^t$$

und damit $d_{B/A}(\underline{e}') = \det(U)^2 d_{B/A}(\underline{e})$. Da $U \in \mathrm{GL}_n(A)$, ist $\det(U) \in A^*$.
(Man beachte, dass dies exakt derselbe Beweis ist, den man in der linearen Algebra führt, wenn man diskutiert, wie sich die darstellende Matrix einer Bilinearform ändert, wenn man die Basis wechselt.) □

Bemerkung 4.13. Betrachte die folgende Äquivalenzrelation $\sim$ auf A:

$$a \sim a' : \Longleftrightarrow \text{ es gibt ein } u \in A^* \text{ mit } a = u^2 a'.$$

Durch die Wahl einer beliebigen A-Basis erhalten wir somit ein Element $d_{B/A} \in A/\sim$, das *die Diskriminante* von B/A genannt wird. Insbesondere ist der Ausdruck "$d_{B/A} = 0$" sinnvoll. Für uns wird im weiteren Verlauf der Vorlesung vor allem der Fall $A = \mathbb{Z}$ wichtig sein – wegen $\mathbb{Z}^* = \{1, -1\}$ ist die Diskriminante dann sogar gänzlich unabhängig von der Wahl der Basis.

Sei K nun ein Zahlkörper mit $[K : \mathbb{Q}] = n$. Sei $M \subset K$ ein freier $\mathbb{Z}$-Untermodul vom Rang n mit $\mathbb{Z}$-Basis $(m_1, \ldots, m_n)$. Dann ist $(m_1, \ldots, m_n)$ auch eine $\mathbb{Q}$-Basis von K und wir können die *Diskriminante von* M durch

$$d_M := d_M(m_1, \ldots, m_n) := d_{K/\mathbb{Q}}(m_1, \ldots, m_n) = \det\left(\left(\mathrm{tr}_{K/\mathbb{Q}}(m_i m_j)\right)_{1\leq i,j\leq n}\right)$$

definieren. Analog zu Lemma 4.12 erhalten wir, dass d_M unabhängig von der Wahl der $\mathbb{Z}$-Basis von M ist:

Proposition 4.14. *Sei K ein Zahlkörper vom Grad n und $M', M \subset K$ freie $\mathbb{Z}$-Moduln vom Rang n. Ferner seien $\mathbb{Z}$-Basen $(m_1', \ldots, m_n')$ bzw. $(m_1, \ldots, m_n)$ von M' bzw. M gegeben. Dann gilt:*

(1) Es existiert ein $u \in \mathbb{Q} \setminus \{0\}$, sodass

$$d_{M'}(m_1', \ldots, m_n') = u^2 \cdot d_M(m_1, \ldots, m_n).$$

(2) Wenn zusätzlich $M' \subset M$ gilt, so kann man $u = (M : M')$ wählen, d.h. es gilt

$$d_{M'}(m_1', \ldots, m_n') = (M : M')^2 \cdot d_M(m_1, \ldots, m_n).$$

Insbesondere gilt: Die Diskriminante $d_M = d_M(m_1, \ldots, m_n)$ ist unabhängig von der Wahl der Basis von M.

Beweis. (1) Der gleiche Beweis wie bei Lemma 4.12 funktioniert. Wir wiederholen das Argument kurz. Wie bereits erwähnt sind $(m_1', \ldots, m_n')$ bzw. $(m_1, \ldots, m_n)$ auch $\mathbb{Q}$-Basen von K. Man kann also jedes m_i' als $\mathbb{Q}$-Linearkombination der m_j schreiben:

$$m_i' = \sum_{j=1}^{n} a_{ij} m_j, \qquad a_{ij} \in \mathbb{Q}.$$

Sei $U \in \mathrm{Mat}(n \times n, \mathbb{Q})$ die Matrix mit den Einträgen a_{ij}. Wie im Beweis von Lemma 4.12 folgt dann

$$d_{M'}(m_1', \ldots, m_n') = \det(U)^2 \cdot d_M(m_1, \ldots, m_n).$$

Mit $u = \det(U) \in \mathbb{Q} \setminus \{0\}$ folgt die Behauptung.

(2) Sei U wie in Teil (1). Aus dem Elementarteilersatz (genauer Proposition 2.19) folgt $|\det(U)| = (M : M')$.
Die Unabhängigkeit von der Wahl der Basis folgt, indem man im eben gezeigten Resultat den Fall $M = M'$ betrachtet. □

Bemerkung 4.15. Ist K ein Zahlkörper vom Grad n und $M \subset \mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang n, dann ist $d_M \in \mathbb{Z}$. Das folgt aus der Tatsache, dass ganze Elemente eine ganzzahlige Spur haben (vgl. Aufgabe 4.2.2).

In der Schule haben Sie den Begriff der Diskriminante sicherlich bereits im Kontext des Lösens einer quadratischen Gleichung $aX^2 + bX + c = 0$ ($a, b, c \in \mathbb{R}$, $a \neq 0$) gehört. Die Diskriminante eines solchen quadratischen Polynoms war $b^2 - 4ac$. Je nachdem, ob sie positiv, null oder negativ ist, hat die Gleichung zwei reelle, eine reelle oder keine reelle Lösung. Hängt diese Diskriminante mit den oben eingeführten Diskriminantenbegriffen zusammen? Wenn ja, wie? Um diese Frage zu beantworten, müssen wir erst einmal definieren, was die Diskriminante eines Polynoms überhaupt ist.

Definition 4.16. Sei A ein Integritätsbereich und

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in A[X], \qquad a_n \neq 0.$$

In einer Ringerweiterung von A zerfällt f in Linearfaktoren, $f = a_n \cdot (X - \beta_1) \cdot \ldots \cdot (X - \beta_n)$. Die *Diskriminante* von f ist dann durch

$$\Delta(f) := a_n^{2n-2} \cdot \prod_{i<j} (\beta_i - \beta_j)^2$$

definiert.

Bemerkung 4.17.

(1) Durch das Quadrat in der Definition der Diskriminante hängt $\Delta(f)$ nicht von der Nummerierung der $\beta_1, \ldots, \beta_n$ ab.

(2) Aus der Definition ist sofort klar, dass f genau dann keine mehrfachen Nullstellen hat, wenn $\Delta(f) \neq 0$.

(3) Ist insbesondere L/K eine endliche, separable Körpererweiterung und $\alpha \in L$, so ist $\Delta(m_\alpha) \neq 0$.

Beispiel 4.18. Sei $A = \mathbb{R}$, $f = aX^2 + bX + c$ mit $a \neq 0$. Dann ist

$$\Delta(f) = a^2 \cdot \left(\frac{2\sqrt{b^2 - 4ac}}{2a} \right)^2 = b^2 - 4ac.$$

Wie hängen nun die Diskriminantenbegriffe zusammen? Um die Frage zu beantworten, spezialisieren wir uns auf den Fall, in dem L/K eine endliche, separable Körpererweiterung ist. Nach Satz 4.2 gibt es dann genau $n = [L : K]$ verschiedene Einbettungen

$$\sigma_1, \ldots, \sigma_n \colon L \hookrightarrow \overline{K}$$

über K. Ist $\{\alpha_1, \dots, \alpha_n\}$ eine K-Basis von L, so ist die Diskriminante bzgl. dieser Basis ja gerade durch die Determinante der Matrix mit den Einträgen

$$\mathrm{tr}_{L/K}(\alpha_i\alpha_j) \overset{\text{Lemma 4.7 (2)}}{=} \sum_{\ell=1}^{n} \sigma_\ell(\alpha_i)\sigma_\ell(\alpha_j)$$

gegeben. Es folgt

$$\left(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j} = (\sigma_i(\alpha_j))_{i,j}^T \cdot (\sigma_i(\alpha_j))_{i,j}$$

und damit auch

$$d_{L/K}(\alpha_1, \dots, \alpha_n) = \det((\sigma_i(\alpha_j))_{i,j})^2. \tag{4.2}$$

Wir nutzen nun erneut die Separabilität von L/K aus: Diese erlaubt uns, ein primitives Element α von L/K wählen. In diesem Fall ist also $\{1, \alpha, \dots, \alpha^{n-1}\}$ eine K-Basis von L. Gleichung (4.2) liest sich in diesem Fall wie folgt:

$$d_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \dots & \sigma_1(\alpha)^{n-1} \\ \vdots & & & \vdots \\ 1 & \sigma_n(\alpha) & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 \overset{(*)}{=} \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \Delta(m_\alpha).$$

In Schritt $(*)$ haben wir die Formel für die Vandermonde-Determinante verwendet.

Fazit. Ist $L = K(\alpha)$, so ist die Diskriminante der "Potenzbasis" $\{1, \alpha, \dots, \alpha^{n-1}\}$ gleich der Diskriminante von $m_\alpha \in K[X]$, dem Minimalpolynom von α.

Schließlich erhalten wir aus der gesamten Diskussion noch die wichtige Folgerung

Korollar 4.19. *Sei K ein Zahlkörper vom Grad n und $M \subset K$ ein freier $\mathbb{Z}$-Modul vom Rang n. Dann ist $d_M \neq 0$.*

Beweis. Sei α ein primitives Element von K. Die Diskussion oben impliziert, dass die Diskriminante des $\mathbb{Z}$-Moduls $M' := \langle 1, \alpha, \dots, \alpha^{n-1} \rangle_{\mathbb{Z}}$ gerade

$$d_{M'} = \Delta(m_\alpha) \neq 0$$

ist. Proposition 4.14 (1) sagt uns nun, dass sich d_M und $d_{M'}$ lediglich um ein Element aus $\mathbb{Q}\backslash\{0\}$ unterscheiden. Also folgt $d_M \neq 0$ aus der schon bewiesenen Tatsache $d_{M'} \neq 0$. □

Spoiler. Im nächsten Abschnitt werden wir beweisen, dass $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang $[K : \mathbb{Q}]$ ist. Die Diskriminante $d_K := d_{\mathcal{O}_K}$ des $\mathbb{Z}$-Moduls $\mathcal{O}_K$ wird im weiteren Verlauf der Vorlesung eine zentrale Rolle spielen.

4.3.1 Übungen

Aufgabe 4.3.1. Sei B eine Ringerweiterung von $\mathbb{Z}$, sodass B ein endlich erzeugter freier $\mathbb{Z}$-Modul vom Rang n ist. Ferner seien $(\beta_1, \dots, \beta_n)$ eine $\mathbb{Z}$-Basis von B und p eine Primzahl. Zeigen Sie, dass $(\overline{\beta}_n, \dots, \overline{\beta}_n)$ eine $\mathbb{F}_p$-Basis von $\overline{B} := B/pB$ ist. Hierbei

bezeichnet $\overline{\beta}_i$ die Klasse von β_i in $\overline{B}$.
Folgern Sie dann aus der obigen Aussage, dass die Reduktion der Diskriminante

$$d_{B/\mathbb{Z}}(\beta_1, \ldots, \beta_n)$$

modulo p gerade

$$d_{\overline{B}/\mathbb{F}_p}(\overline{\beta}_1, \ldots, \overline{\beta}_n)$$

ist.

Aufgabe 4.3.2. Es sei A ein Ring und B_1, B_2 Ringe, die ebenfalls endlich erzeugte freie A-Moduln sind. Zeigen Sie: $d_{(B_1 \times B_2)/A} = d_{B_1/A} \cdot d_{B_2/A}$.
Hinweis: Wie bekommt man eine A-Basis von $B_1 \times B_2$, wenn man A-Basen von B_1 und B_2 hat?

4.4 Der Ganzheitsring als Dedekindring

Sei K ein Zahlkörper und

$$\mathcal{O}_K = \{\alpha \in K \mid m_\alpha \in \mathbb{Z}[X]\}$$

der Ganzheitsring von K. In diesem Abschnitt möchten wir den folgenden Satz beweisen:

Satz 4.20. *Der Ganzheitsring $\mathcal{O}_K$ eines Zahlkörpers K ist ein Dedekindring.*

Wir erinnern daran, dass ein Dedekindring ein noetherscher, ganz abgeschlossener Integritätsbereich der Dimension 1 ist. Es ist klar, dass $\mathcal{O}_K$ ein Integritätsbereich ist. Die ganze Abgeschlossenheit wurde bereits in Korollar 1.7 bewiesen. Des Weiteren haben wir in Aufgabe 2.0.6 gesehen, dass jedes Primideal $\neq (0)$ in $\mathcal{O}_K$ maximal ist. Da $\mathcal{O}_K$ ebenfalls kein Körper ist, zeigt das, dass $\mathcal{O}_K$ die Dimension 1 hat. Um Satz 4.20 zu beweisen, müssen wir also nur noch nachweisen, dass $\mathcal{O}_K$ noethersch ist. Im Zuge unserer Diskussion wird sich ein weiterer Beweis dafür ergeben, dass $\mathcal{O}_K$ ein Ring der Dimension 1 ist.

Kurzzusammenfassung des Kapitels:
Wir beweisen, dass jedes Ideal $\mathfrak{a} \neq (0)$ von $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$ ist.
Ist diese Aussage gezeigt, erhalten wir sofort, dass $\mathcal{O}_K$ noethersch ist: Wenn $\mathfrak{a}$ nämlich endlich erzeugt über $\mathbb{Z}$ ist, dann sicherlich auch über dem größeren Ring $\mathcal{O}_K$ (d.h. als Ideal).
Des Weiteren impliziert der Spezialfall des Elementarteilersatzes (Proposition 2.19) dann, dass $\mathcal{O}_K/\mathfrak{a}$ für jedes Ideal $\mathfrak{a} \neq (0)$ endlich ist. Ist $\mathfrak{a}$ ein Primideal, so ist $\mathcal{O}_K/\mathfrak{a}$ insbesondere ein endlicher Integritätsbereich, also ein Körper, was beweist, dass $\mathfrak{a}$ maximal ist.

Sei K ein Zahlkörper vom Grad n und $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Q}$-Basis von K. Da K der Quotientenkörper von $\mathcal{O}_K$ ist, können wir durch Multiplikation mit den Nennern ohne Beschränkung der Allgemeinheit annehmen, dass $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. In dieser Situation haben wir dann

Lemma 4.21. *Sei $M \subset \mathcal{O}_K$ der freie $\mathbb{Z}$-Modul, der von $\alpha_1, \ldots, \alpha_n$ erzeugt wird. Dann ist $\mathcal{O}_K \subset d_M^{-1} M$.*

Beweis. Sei $\alpha \in \mathcal{O}_K$. Da $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Q}$-Basis von K ist, gibt es $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ mit

$$\alpha = \lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n. \tag{4.3}$$

Zu zeigen ist $d_M\lambda_i \in \mathbb{Z}$ für $i \in \{1, \ldots, n\}$. Wir schreiben

$$b_i := \mathrm{tr}_{K/\mathbb{Q}}(\alpha\alpha_i) \in \mathbb{Z} \qquad \text{(vgl. Aufgabe 4.2.2)}.$$

Wir setzen die Linearkombination (4.3) von α in b_i ein und nutzen die $\mathbb{Q}$-Linearität der Spur:

$$b_i = \mathrm{tr}_{K/\mathbb{Q}}\left(\sum_{j=1}^{n} \lambda_j\alpha_i\alpha_j\right) = \sum_{j=1}^{n} \lambda_j \,\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j). \tag{4.4}$$

Da $\alpha_i\alpha_j \in \mathcal{O}_K$, folgt $\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$ (hier nutzen wir wieder Aufgabe 4.2.2). Schreiben wir T für die Matrix mit den ganzzahligen Einträgen $\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$, so lässt sich (4.4) also zu

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = T \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \tag{4.5}$$

umschreiben. Per Definition der Diskriminante gilt nun $d_M = \det(T)$. Nach Korollar 4.19 gilt außerdem $d_M \neq 0$, also folgt $T \in \mathrm{GL}_n(\mathbb{Q})$. Nach der Cramerschen Regel ist $T^{-1} \in \mathrm{GL}_n(\mathbb{Q})$ durch

$$T^{-1} = \frac{1}{\det(T)} \cdot T^{\mathrm{adj}} = \frac{1}{d_M} \cdot T^{\mathrm{adj}}$$

gegeben – hierbei ist $T^{\mathrm{adj}} \in \mathrm{Mat}(n \times n, \mathbb{Z})$ die Adjunkte von T. Aus (4.5) erhält man schließlich

$$d_M \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = T^{\mathrm{adj}} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{Z}^n.$$

□

Satz 4.22. *Der Ganzheitsring $\mathcal{O}_K$ eines Zahlkörpers K vom Grad n ist ein freier $\mathbb{Z}$-Modul vom Rang n.*

Beweis. Wir verwenden weiterhin die Notationen, die vor und in Lemma 4.21 eingeführt wurden. Nach dem zitierten Lemma ist $\mathcal{O}_K$ im freien $\mathbb{Z}$-Modul $d_M^{-1}M$ vom Rang n enthalten. Nach dem Elementarteilersatz 2.17 ist $\mathcal{O}_K$ dann ebenfalls ein freier $\mathbb{Z}$-Modul vom Rang $m \leq n$. Das gleiche Argument liefert wegen $M \subset \mathcal{O}_K$ allerdings, dass $n \leq m$, also $n = m$. □

Die folgende Definition ergibt somit Sinn.

Definition 4.23. Eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ heißt eine *Ganzheitsbasis von K*.

Bemerkung 4.24. Eine Ganzheitsbasis eines Zahlkörpers K ist auch eine $\mathbb{Q}$-Basis von K (denn setzt man eine $\mathbb{Q}$-Linearkombination von $0 \in K$ an, so kann man diese mit einer ganzen Zahl durchmultiplizieren, um eine $\mathbb{Z}$-Linearkombination zu erhalten).

Notation 4.25. Als endlich erzeugter und freier $\mathbb{Z}$-Modul hat $\mathcal{O}_K$ nun eine Diskriminante, die wir verkürzt mit d_K bezeichnen werden.

Allgemeiner können wir nun beweisen

Korollar 4.26. *Ist $\mathfrak{a} \neq (0)$ ein Ideal von $\mathcal{O}_K$, so ist $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$.*

Beweis. Wir beweisen die Behauptung zunächst für Hauptideale (a), $a \neq 0$. In diesem Fall ist $\mathcal{O}_K \to (a)$, $x \mapsto ax$ ein Isomorphismus von $\mathbb{Z}$-Moduln. Da $\mathcal{O}_K$ frei vom Rang n ist (Satz 4.22), ist (a) dann ebenfalls frei vom Rang n.
In der allgemeinen Situation wählen wir $0 \neq a \in \mathfrak{a}$. Dann haben wir Inklusionen $(a) \subset \mathfrak{a} \subset \mathcal{O}_K$. Da sowohl (a) als auch $\mathcal{O}_K$ frei vom Rang n sind, muss nach dem Elementarteilersatz 2.17 dann auch $\mathfrak{a}$ frei vom Rang n sein. □

Wie in der Zusammenfassung des Kapitels bereits erwähnt, erhalten wir daraus fast in Gänze den Beweis von Satz 4.20:

Korollar 4.27. *Der Ganzheitsring eines Zahlkörpers ist noethersch.*

Beweis. Jedes Ideal $\neq (0)$ darin ist ein freier $\mathbb{Z}$-Modul vom endlichen Rang, also insbesondere endlich erzeugt als $\mathbb{Z}$-Modul. Demnach ist es sicherlich auch endlich erzeugt als $\mathcal{O}_K$-Modul. □

Korollar 4.28. *Ist $(0) \neq \mathfrak{a}$ ein Ideal in $\mathcal{O}_K$, so ist $\mathcal{O}_K/\mathfrak{a}$ ein endicher Ring.*

Beweis. Sowohl $\mathcal{O}_K$ als auch $\mathfrak{a}$ sind freie $\mathbb{Z}$-Moduln desselben endlichen Rangs. Die Behauptung folgt dann sofort aus Proposition 2.19. □

Schließlich liefern wir noch wie angekündigt einen weiteren Beweis dafür, dass jedes Primideal $\mathfrak{p} \neq (0)$ in $\mathcal{O}_K$ maximal ist. Da $\mathcal{O}_K/\mathfrak{p}$ nach Korollar 4.28 und Lemma 2.6 ein endlicher Integriätsbereich ist, genügt es dafür, das folgende Lemma zu zeigen:

Lemma 4.29. *Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Sei A ein endlicher Integritätsbereich. Für $a \in A \setminus \{0\}$ betrachten wir die Abbildung $L_a \colon A \to A$, $x \mapsto ax$. Diese ist injektiv, denn aus $ax_1 = ax_2$ für $x_1, x_2 \in A$ folgt $a(x_1 - x_2) = 0$ und da $a \neq 0$, folgt $x_1 = x_2$ aus der Nullteilerfreiheit. Als injektive Abbildung zwischen endlichen Mengen ist L_a auch surjektiv. Insbesondere gibt es ein $b \in A$ mit $L_a(b) = ab = 1$, also haben wir ein multiplikatives Inverses von a gefunden.
(Man beachte, dass der gleiche Beweis allgemeiner zeigt, dass jedes Element $\neq 0$ in einem endlichen Ring entweder Nullteiler oder Einheit ist.) □

Der Beweis von Satz 4.20 ist damit vollständig. Insbesondere hat jetzt also jedes gebrochene Ideal $\neq (0)$ in Zahlkörpern eine eindeutige Primidealfaktorisierung.

Bemerkung 4.30. In der Tat gilt ein allgemeineres Ergebnis als das in Satz 4.20:

Satz. *Sei A ein Dedekindring der mit Quotientenkörper K und L/K eine endliche Erweiterung von K. Wenn K die Charakteristik 0 hat, dann ist der ganze Abschluss $\overline{A}$ von A in L ein Dedekindring.*

Bei Satz 4.20 handelt es sich um den Spezialfall $A = \mathbb{Z}$. Um den Satz zu beweisen, benötigt man etwas andere Methoden. Wir skizzieren den Beweis hier nur:

- Eine bekannte Folgerung aus dem Going-Up Theorem ist, dass die Krull-Dimension eines Ringes gleich bleibt, wenn man zu einer ganzen Ringerweiterung übergeht. Da nun A die Krull-Dimension 1 hat und $A \subset \overline{A}$ ganz ist, folgt, dass $\overline{A}$ ebenfalls die Krull-Dimension 1 hat.
- Um zu beweisen, dass $\overline{A}$ noethersch ist, ist ein wenig Wissen über noethersche Moduln notwendig. Nothersche Moduln sind dadurch charakterisiert, dass all ihre Untermoduln endlich erzeugt sind. Wenn man also beweist, dass $\overline{A}$ ein noetherscher A-Modul ist, dann sind die Ideale von $\overline{A}$ endlich erzeugte A-Moduln, also sicherlich auch endlich erzeugt als Ideale. (Man bemerke die Ähnlichkeit zu Korollar 4.26 bzw. Korollar 4.27!)

4.4.1 Übungen

Aufgabe 4.4.1. Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$. Zeigen Sie: Es ist $\{1, \theta\}$ eine Ganzheitsbasis von $\mathcal{O}_K$, wobei

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

Insbesondere gilt $\mathcal{O}_K = \mathbb{Z}[\theta]$. Bestimmen Sie außerdem die Diskriminante von $K = \mathbb{Q}(\sqrt{d})$ in Abhängigkeit von d.

Aufgabe 4.4.2. Sei $K = \mathbb{Q}(\sqrt{-19})$.

(1) Nutzen Sie Aufgabe 4.2.2, um die Einheiten in $\mathcal{O}_K$ zu bestimmen.

(2) Bestimmen Sie das Minimalpolynom m_α von $\alpha = \frac{1+\sqrt{-19}}{2}$ und zeigen Sie, dass das Bild von m_α in $(\mathbb{Z}/2\mathbb{Z})[X]$ und $(\mathbb{Z}/3\mathbb{Z})[X]$ jeweils irreduzibel ist.

(3) Zeigen Sie, dass $\mathcal{O}_K$ nicht euklidisch ist. Nehmen Sie dafür an, dass $n \colon \mathcal{O}_K \setminus \{0\} \to \mathbb{N}$ eine euklidische Normfunktion ist und wählen Sie ein Element $0 \neq a \in \mathcal{O}_K \setminus \mathcal{O}_K^*$, sodass $n(a)$ minimal unter den Elementen aus $\mathcal{O}_K \setminus (\mathcal{O}_K^* \cup \{0\})$ ist. Teilen Sie dann ein $b \in \mathcal{O}_K$ mit Rest durch a, um einen Widerspruch herzuleiten.

Aufgabe 4.4.3. Entscheiden Sie auf die folgenden zwei Art und Weisen, ob $\alpha := \frac{3+2\sqrt{6}}{1-\sqrt{6}}$ eine ganze algebraische Zahl ist:

(1) Schreiben Sie α als $\mathbb{Q}$-Linearkombination einer Ganzheitsbasis von $\mathbb{Q}(\sqrt{6})$. Handelt es sich um eine ganzzahlige Linearkombination?

(2) Berechnen Sie das Minimalpolynom von α über $\mathbb{Q}$. Hat es ganzzahlige Koeffizienten?

Aufgabe 4.4.4. Sei $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$.

(1) Finden Sie ein primitives Element für K.

(2) Zeigen Sie, dass K *nicht monogen* ist, d.h. dass kein α mit $\mathcal{O}_K = \mathbb{Z}[\alpha]$ existiert.

Aufgabe 4.4.5. Sei K ein Zahlkörper, d_K seine Diskriminante. Zeigen Sie:

$$d_K \equiv 0 \pmod 4 \qquad \text{oder} \qquad d_K \equiv 1 \pmod 4.$$

Hinweis: Seien $\sigma_1, \ldots, \sigma_n$ die komplexen Einbettungen von K und $\{\omega_1, \ldots, \omega_n\}$ eine Ganzheitsbasis von K. Nach der Leibniz-Formel für die Determinante können wir schreiben

$$\det(\sigma_i(\omega_j)) = \underbrace{\sum_{\pi \in A_n} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)})}_{=:P} - \underbrace{\sum_{\pi \notin A_n} \prod_{i=1}^{n} \sigma_i(\omega_{\pi(i)})}_{=:N}.$$

Dann gilt also $d_K = (P-N)^2 = (P+N)^2 - 4PN$. Warum reicht es dann, $P+N, PN \in \mathbb{Z}$ zu zeigen?

Aufgabe 4.4.6. Sei α eine Nullstelle von $X^3 - X - 2 \in \mathbb{Z}[X]$ und $K = \mathbb{Q}(\alpha)$. Zeigen Sie, dass $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
Hinweis: Offensichtlich gilt $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$. Für die umgekehrte Inklusion können Sie Proposition 4.14 und Aufgabe 4.4.5 verwenden.

4.5 Die Idealnorm

Wir haben im vorherigen Abschnitt gesehen, dass der Ganzheitsring $\mathcal{O}_K$ eines Zahlkörpers K ein Dedekindring ist. Dafür haben wir insbesondere Korollar 4.28 bewiesen, welches die folgende Definition motiviert.

Definition 4.31. Sei K ein Zahlkörper und $\mathfrak{a} \neq (0)$ ein Ideal in $\mathcal{O}_K$. Dann definieren wir die *Norm* von $\mathfrak{a}$ als $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$.

Wir diskutieren nun einige elementare Eigenschaften der Idealnorm, welche größtenteils Umformulierungen von Aussagen sind, die wir bereits bewiesen haben.

Bemerkung 4.32. Das Ergebnis aus Proposition 4.14 lässt sich nun zu

$$d_{\mathfrak{a}} = N(\mathfrak{a})^2 \cdot d_K$$

umschreiben.

Das untenstehende Resultat rechtfertigt den Begriff "Idealnorm".

Proposition 4.33. *Sei $\alpha \in \mathcal{O}_K \setminus \{0\}$, dann gilt $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Beweis. Da $\mathcal{O}_K$ und (α) frei vom selben Rang n sind, gibt es Elementarteiler $d_1, \ldots, d_n$ mit $d_1 \geq 1$ und $d_i \mid d_{i+1}$ und eine $\mathbb{Z}$-Basis $(\alpha_1, \ldots, \alpha_n)$ von $\mathcal{O}_K$, sodass $(d_1\alpha_1, \ldots, d_n\alpha_n)$ eine $\mathbb{Z}$-Basis von (α) ist (vgl. Elementarteilersatz 2.17). Damit gilt

$$N((\alpha)) = |\mathcal{O}_K/(\alpha)| = d_1 \cdot \ldots \cdot d_n.$$

Wir erhalten also einen Isomorphismus von $\mathbb{Z}$-Moduln

$$\begin{aligned}\psi\colon \mathcal{O}_K &\to (\alpha),\\ \alpha_i &\mapsto d_i\alpha_i.\end{aligned}$$

Andererseits ist $(\alpha\alpha_1, \ldots, \alpha\alpha_n)$ ebenfalls eine $\mathbb{Z}$-Basis von (α). Somit gibt es einen Automorphismus φ von (α), der $d_i\alpha_i$ auf $\alpha\alpha_i$ abbildet. Da es sich bei φ um einen Automorphismus des $\mathbb{Z}$-Moduls (α) handelt, ist $\det(\varphi) \in \mathbb{Z}^* = \{1, -1\}$. Die Hintereinanderschaltung von

$$\begin{aligned}\varphi \circ \psi\colon \mathcal{O}_K &\to (\alpha),\\ \alpha_i &\mapsto \alpha\alpha_i\end{aligned}$$

mit der Inklusion $\iota\colon (\alpha) \hookrightarrow \mathcal{O}_K$ ist schlicht die Multiplikationsabbildung L_α mit α, und $\det(\psi \circ \iota) = d_1 \cdot \ldots \cdot d_n$. Mit der Definition der Norm folgt also

$$\pm|\mathcal{O}_K/(\alpha)| \overset{\text{Prop. 2.19}}{=} \pm d_1 \cdot \ldots \cdot d_n = \det(\varphi)\det(\psi \circ \iota) = \det(\varphi \circ \psi \circ \iota) = \det(L_\alpha) = N_{K/\mathbb{Q}}(\alpha).$$

□

Proposition 4.34. *Sei L/K eine Erweiterung von Zahlkörpern und sei $\mathfrak{P} \neq (0)$ ein Primideal von $\mathcal{O}_L$. Dann ist $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ ein Primideal $\neq (0)$ von $\mathcal{O}_K$ und es gibt eine ganze Zahl $f \geq 1$ mit $N(\mathfrak{P}) = N(\mathfrak{p})^f$.*

Beweis. Das Ideal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ ist das Urbild von $\mathfrak{P}$ unter der Inklusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$. Da Urbilder von Primidealen wieder Primideale sind, ist $\mathfrak{p}$ ein Primideal. Wir zeigen, dass $\mathfrak{p} \neq (0)$ ist. Dazu wählen wir $\alpha \in \mathfrak{P} \setminus \{0\}$ und betrachten das Minimalpolynom

$$m_\alpha = X^m + b_{m-1}X^{m-1} + \ldots + b_0 \in \mathbb{Z}[X]$$

von α über $\mathbb{Q}$. Da $\alpha \neq 0$, ist $b_0 \neq 0$. Aus $m_\alpha(\alpha) = 0$ folgt

$$b_0 = -(\alpha^m + b_{m-1}\alpha^{m-1} + \ldots + b_1\alpha) \in \mathfrak{P} \cap \mathbb{Z} \subset \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p},$$

was $\mathfrak{p} \neq (0)$ zeigt.
Nun ist $\mathcal{O}_L/\mathfrak{P}$ ein $\mathcal{O}_K$-Modul, der von $\mathfrak{p}$ annihiliert wird (d.h. multipliziert man ein Element aus $\mathcal{O}_L/\mathfrak{P}$ mit einem Skalar aus $\mathfrak{p}$, so ist das Ergebnis 0). Somit ist $\mathcal{O}_L/\mathfrak{P}$ ein $\mathcal{O}_K/\mathfrak{p}$-Vektorraum, der endlich-dimensional sein muss, weil $|\mathcal{O}_L/\mathfrak{P}| < \infty$. □

Korollar 4.35. *Ist K ein Zahlkörper und $\mathfrak{p} \neq (0)$ ein Primideal von $\mathcal{O}_K$, dann ist $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p und $N(\mathfrak{p})$ ist eine Potenz von p.*

Beweis. Der Beweis von Proposition 4.34 sagt uns, dass $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p gilt. Weiterhin sagt er uns, dass der Kern von $\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ gerade $p\mathbb{Z}$ ist. Also hat der endliche Körper $\mathcal{O}_K/\mathfrak{p}$ die Charakteristik p.
(Natürlich hätten wir dasselbe Ergebnis auch aus $N(\mathfrak{p}) = N(p\mathbb{Z})^f$ und Proposition 4.33 schließen können. Aber Vorsicht: Da $p\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ ist, ist $N(p\mathbb{Z})$ gleich $N_{\mathbb{Q}/\mathbb{Q}}(p) = p$ und nicht gleich $N_{K/\mathbb{Q}}(p) = \pm p^{[K:\mathbb{Q}]}$.) □

Schließlich beweisen wir:

Proposition 4.36. *Die Idealnorm ist vollständig multiplikativ, das heißt für je zwei Ideale* $\mathfrak{a}, \mathfrak{b} \neq (0)$ *von* $\mathcal{O}_K$ *gilt* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Beweis. Da $\mathcal{O}_K$ ein Dedekindring ist, lässt sich $\mathfrak{b}$ eindeutig als Produkt von maximalen Idealen schreiben. Es genügt also, $N(\mathfrak{am}) = N(\mathfrak{a})N(\mathfrak{m})$ für ein maximales Ideal $\mathfrak{m}$ zu zeigen. Nach dem zweiten Isomorphiesatz für Ringe gilt

$$(\mathcal{O}_K/\mathfrak{am}) \,/\, (\mathfrak{a}/\mathfrak{am}) \cong \mathcal{O}_K/\mathfrak{a},$$

also auch

$$|\mathfrak{a}/\mathfrak{am}| \cdot N(\mathfrak{a}) = N(\mathfrak{am}). \tag{4.6}$$

Nun ist $\mathfrak{a}/\mathfrak{am}$ ein $\mathcal{O}_K$-Modul, der von $\mathfrak{m}$ annihiliert wird. Wir können $\mathfrak{a}/\mathfrak{am}$ also auch als einen Vektorraum über dem endlichen Körper $\mathcal{O}_K/\mathfrak{m}$ betrachten. Die Untervektorräume von $\mathfrak{a}/\mathfrak{am}$ entsprechen den $\mathcal{O}_K$-Untermoduln von $\mathfrak{a}$, die $\mathfrak{am}$ enthalten. Genauer sind die Untervektorräume von der Form $\mathfrak{q}/\mathfrak{am}$, wobei $\mathfrak{am} \subset \mathfrak{q} \subset \mathfrak{a}$ ein Ideal von $\mathcal{O}_K$ ist. Die Eindeutigkeit der Primidealfaktorisierung impliziert nun aber wegen der Maximalität von $\mathfrak{m}$, dass $\mathfrak{q} = \mathfrak{a}$ oder $\mathfrak{q} = \mathfrak{am}$ gelten muss. Somit hat der $\mathcal{O}_K/\mathfrak{m}$-Vektorraum $\mathfrak{a}/\mathfrak{am}$ nur zwei Untervektorräume, muss also die Dimension 1 haben. Es folgt

$$|\mathfrak{a}/\mathfrak{am}| = |\mathcal{O}_K/\mathfrak{m}| = N(\mathfrak{m}).$$

Eingesetzt in (4.6) liefert das die Behauptung. □

Bemerkung. Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale $\neq (0)$, so liefert der Isomorphismus

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$$

aus dem chinesischen Restsatz einen einfacheren Beweis der Multiplikativität.

Die Multiplikativität der Norm stellt nun sicher, dass die folgende Definition sinnvoll ist.

Definition 4.37. Sei $\mathfrak{a} \neq (0)$ ein ganzes Ideal in $\mathcal{O}_K$. Dann definieren wir die *Norm* des gebrochenen Ideals $\mathfrak{a}^{-1}$ als $N(\mathfrak{a}^{-1}) := N(\mathfrak{a})^{-1}$.

Die Idealnorm ist somit für alle gebrochenen Ideale $\neq (0)$ definiert und vollständig multiplikativ, d.h. für je zwei gebrochene Ideale $\mathfrak{a}, \mathfrak{b} \neq (0)$ gilt $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

4.5.1 Übungen

Aufgabe 4.5.1. Sei K ein Zahlkörper und $\mathfrak{a} \subset \mathcal{O}_K$ ein ganzes Ideal $\neq (0)$. Zeigen Sie: Ist $N(\mathfrak{a})$ eine Primzahl, so ist $\mathfrak{a}$ ein Primideal. Gilt die Umkehrung?

4.6 Primfaktorisierung in Ganzheitsringen

Sei L/K eine Erweiterung von Zahlkörpern. Die grundsätzliche Fragestellung, die uns in diesem Kapitel beschäftigt, ist, wie die Primfaktorisierung von $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$ aussieht – hierbei ist $\mathfrak{p} \neq (0)$ ein Primideal in $\mathcal{O}_K$. Beispiele haben wir bereits in Aufgabe 3.2.6 gesehen, doch wie kommt man auf die dort angegebene Zerlegung?

Definition 4.38. Sei L/K eine Erweiterung von Zahlkörpern und sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Sei

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$$

die Primfaktorisierung des von $\mathfrak{p}$ erzeugten Ideals in $\mathcal{O}_L$. (Wie üblich seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ paarweise verschiedene Primideale und $e_1, \ldots, e_r \geq 1$.)

(1) Man definiert den *Verzweigungsindex* von $\mathfrak{P}_i$ über $\mathfrak{p}$ als $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$.

(2) Das Primideal $\mathfrak{p}$ heißt in L *verzweigt*, falls einer der Verzeigungsindizes $e(\mathfrak{P}_i|\mathfrak{p})$ größer als 1 ist, ansonsten heißt $\mathfrak{p}$ in L *unverzweigt* .

(3) Nach Proposition 4.34 ist $N(\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$ für ein $f_i \geq 1$. Die Zahl $f_i = f(\mathfrak{P}_i|\mathfrak{p})$ heißt der *Trägheitsgrad* von $\mathfrak{P}_i$ über $\mathfrak{p}$.

(4) Das Primideal $\mathfrak{p}$ heißt *träge* in L, falls einer der Trägheitsgrade $f(\mathfrak{P}_i|\mathfrak{p})$ größer als 1 ist.

Satz 4.39. *Sei $[L : K] = n$. Mit der Notation aus Definition 4.38 gilt die sogenannte* fundamentale Gleichung

$$n = \sum_{i=1}^{r} e_i f_i.$$

Beweis. Es gilt

$$N(\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}) \overset{\text{Prop. 4.36}}{=} N(\mathfrak{P}_1)^{e_1} \cdot \ldots \cdot N(\mathfrak{P}_r)^{e_r} = N(\mathfrak{p})^{\sum_{i=1}^{r} e_i f_i}.$$

Es genügt also,

$$N(\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})^n \tag{4.7}$$

zu zeigen. Definitionsgemäß gilt

$$N(\mathfrak{p}\mathcal{O}_L) = |\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L|.$$

Fassen wir $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ als Vektorraum über dem Körper $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ auf, so ist (4.7) gezeigt, wenn wir

$$\dim_{k(\mathfrak{p})}(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$$

nachweisen. Da $\mathcal{O}_L$ ein endlich erzeugzer $\mathcal{O}_K$-Modul ist, ist $\dim_{k(\mathfrak{p})}(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) < \infty$. Deshalb ist es möglich, eine (endliche) Menge $\{\alpha_1, \ldots, \alpha_m\} \subset \mathcal{O}_L$ so zu wählen, dass die die Menge der Restklassen $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_m\} \subset \mathcal{O}_L/p\mathcal{O}_L$ eine $k(\mathfrak{p})$-Basis bilden. Es genügt zu zeigen, dass $\{\alpha_1, \ldots, \alpha_m\}$ eine K-Basis von L ist (dann gilt insbesondere $m = n$). Angenommen, $\{\alpha_1, \ldots, \alpha_m\}$ wäre K-linear abhängig, dann gibt es auch eine nicht-triviale Linearkombination über $\mathcal{O}_K$:

$$\lambda_1\alpha_1 + \ldots + \lambda_m\alpha_m = 0, \qquad \lambda_i \in \mathcal{O}_K, \quad \text{nicht alle gleich } 0.$$

Wir möchten jetzt modulo $\mathfrak{p}$ reduzieren, um einen Widerspruch zu erhalten. Das Problem ist, dass die λ_i in $\mathfrak{p}$ enthalten sein können – deshalb bedienen wir uns eines kleinen Tricks. Betrachte das Ideal $\mathfrak{a} = (\lambda_1, \ldots, \lambda_m) \subset \mathcal{O}_K$. Wir wählen ein $\lambda \in \mathfrak{a}^{-1}$, sodass $\lambda \notin \mathfrak{a}^{-1}\mathfrak{p}$.

Dann gilt also $\lambda\mathfrak{a} \not\subseteq \mathfrak{p}$ und man erhält durch Multiplikation mit λ die nicht-triviale Linearkombination

$$\lambda\lambda_1\alpha_1 + \ldots + \lambda\lambda_m\alpha_m = 0.$$

Nun gilt $\lambda\lambda_i \in \mathcal{O}_K \setminus \mathfrak{p}$ (das folgt aus der Definition von $\mathfrak{a}$ und λ), also liefert die Reduktion modulo $\mathfrak{p}$ eine nicht-triviale Linearkombination von $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_m\}$ über $k(\mathfrak{p})$, ein Widerspruch.
Es bleibt zu zeigen, dass $\{\alpha_1, \ldots, \alpha_m\}$ ein K-Erzeugendensystem von L ist. Dazu imitieren wir den Beweis von Lemma 4.21. Betrachte den freien $\mathcal{O}_K$-Untermodul M von $\mathcal{O}_L$, der von $\{\alpha_1, \ldots, \alpha_m\}$ erzeugt wird. Sei $N := \mathcal{O}_L/M$ der Faktormodul. Da $\mathcal{O}_L = M + \mathfrak{p}\mathcal{O}_L$, gilt $\mathfrak{p}N = N$. Sei $\{\beta_1, \ldots, \beta_k\} \subset \mathcal{O}_L$ ein $\mathcal{O}_K$-Erzeugendensystem von N. Wegen $\mathfrak{p}N = N$ gibt es also $a_{ij} \in \mathfrak{p}$, sodass für alle $i \in \{1, \ldots, k\}$ gilt:

$$\beta_i = \sum_{j=1}^{k} a_{ij}\beta_j.$$

Sei $A = (a_{ij})_{i,j}$, sodass also

$$(I_k - A)\begin{pmatrix}\beta_1\\ \vdots \\ \beta_k\end{pmatrix} = 0$$

gilt. Durch Multiplikation mit der Adjunkten von $I_k - A$ bekommen wir nun aus der Cramerschen Regel $d\beta_i = 0$, wobei $d := \det(I_k - A)$. Das beweist $dN = \{0\}$, d.h. $d\mathcal{O}_L \subset M$. Da nun A Einträge in $\mathfrak{p}$ hat, gilt außerdem $d \equiv 1 \pmod{\mathfrak{p}}$, also gilt $d \neq 0$. Insgesamt haben wir nun gezeigt, dass

$$\mathcal{O}_L \subset \frac{1}{d}M.$$

Also ist $\{\alpha_1, \ldots, \alpha_m\}$ ein K-Erzeugendensystem von L. □

Definition 4.40. Ein Primideal $\mathfrak{p} \neq (0)$ von $\mathcal{O}_K$ heißt in L ...

(1) ... *total zerfallend*, wenn $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ für alle Primideale $\mathfrak{P} \subset \mathcal{O}_L$ gilt, die $\mathfrak{p}\mathcal{O}_L$ teilen. Die fundamentale Gleichung impliziert, dass es hier genau $n = [L : K]$ verschiedene Primideale gibt, die $\mathfrak{p}\mathcal{O}_L$ teilen.

(2) ... *total verzweigt*, wenn $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$ für ein Primideal $\mathfrak{P} \subset \mathcal{O}_L$ gilt. Hier gilt also $e(\mathfrak{P}|\mathfrak{p}) = n$ und $f(\mathfrak{P}|\mathfrak{p}) = 1$.

(3) ... *total träge*, wenn $\mathfrak{p}\mathcal{O}_L = \mathfrak{P} \subset \mathcal{O}_L$ ein Primideal ist. In diesem Fall ist also $e(\mathfrak{P}|\mathfrak{p}) = 1$ und $f(\mathfrak{P}|\mathfrak{p}) = n$.

Slogan: "Je kleiner der Trägheitsgrad, desto fleißiger zerfällt $\mathfrak{p}\mathcal{O}_L$ in Primideale."

Bemerkung. Sei L/K eine Erweiterung von Zahlkörpern und $\alpha \in \mathcal{O}_L$. Dann hat das Minimalpolynom m_α von α über K Koeffizienten in $\mathcal{O}_K$.
Das sieht man wie folgt ein. Ist $g \in \mathcal{O}_K[X] \setminus \{0\}$ ein Polynom mit $g(\alpha) = 0$, so gilt für

alle Einbettungen $\sigma\colon L \hookrightarrow \overline{K}$ über K, dass $g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$. Also sind alle $\sigma(\alpha)$ ebenfalls ganz über $\mathcal{O}_K$. Da nun

$$m_\alpha = \prod_{\sigma\colon L \hookrightarrow \overline{K}} (X - \sigma(\alpha))$$

gilt, sind die Koeffizienten von m_α also Polynome in den $\sigma(\alpha)$ und damit Elemente von $\mathcal{O}_K$.

Wir beweisen nun das Hauptergebnis dieses Abschnitts. Satz 4.41 beschreibt die Primfaktorisierung von $\mathfrak{p}\mathcal{O}_L$ unter der zusätzlichen Voraussetzung $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ für ein $\alpha \in \mathcal{O}_L$. Leider ist diese Voraussetzung selten erfüllt – wir werden deshalb noch Verallgemeinerungen kennenlernen.

Satz 4.41. *Es sei ein primitives Element $\alpha \in \mathcal{O}_L$ von L/K mit der Eigenschaft*

$$\mathcal{O}_L = \mathcal{O}_K[\alpha]$$

gegeben. Für ein Primideal $\mathfrak{p} \neq (0)$ von $\mathcal{O}_K$ sei $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ und $\overline{m}_\alpha \in k(\mathfrak{p})[X]$ die Reduktion des Minimalpolynoms $m_\alpha \in \mathcal{O}_K[X]$ modulo $\mathfrak{p}$. Das Polynom $\overline{m}_\alpha$ habe die folgende Zerlegung in irreduzible Faktoren:

$$\overline{m}_\alpha = \overline{q}_1^{e_1} \cdot \ldots \cdot \overline{q}_r^{e_r},$$

wobei $e_i \geq 1$ und die $\overline{q}_i \in k(\mathfrak{p})[X]$ irreduzibel, normiert und paarweise verschieden seien. Dann gibt es paarweise verschiedene Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \subset \mathcal{O}_L$, die $\mathfrak{p}\mathcal{O}_L$ teilen, sodass

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$$

und $f(\mathfrak{P}_i|\mathfrak{p}) = \deg(\overline{q}_i)$. Konkret: Ist $q_i \in \mathcal{O}_K[X]$ ein Repräsentant von $\overline{q}_i$, so gelten die obigen Aussagen für

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + (q_i(\alpha)).$$

x

Beweis. Nach Voraussetzung gilt

$$\mathcal{O}_L = \mathcal{O}_K[\alpha] \cong \mathcal{O}_K[X]/(m_\alpha).$$

Der Trick ist nun, den folgenden Isomorphismus zu nutzen:

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] \cong \mathcal{O}_K[X]/(\mathfrak{p} + (m_\alpha)) \cong k(\mathfrak{p})[X]/(\overline{m}_\alpha).$$

Die verknüpfte Abbildung ist hierbei wie folgt gegeben:

$$\begin{aligned} &\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \to k(\mathfrak{p})[X]/(\overline{m}_\alpha), \\ &\alpha + \mathfrak{p}\mathcal{O}_L \mapsto X + (\overline{m}_\alpha). \end{aligned}$$

Bevor wir mit dem Beweis fortfahren, möchten wir erläutern, warum der obige Isomorphismus für das Argument entscheidend ist. Unser Ziel ist es ja, die Primteiler von $\mathfrak{p}\mathcal{O}_L$ zu beschreiben. Wir suchen also die Primideale von $\mathcal{O}_L$, die $\mathfrak{p}\mathcal{O}_L$ enthalten. Diese entsprechen genau den Primidealen im Quotienten $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Da jedoch $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong$

$k(\mathfrak{p})[X]/(\overline{m}_\alpha)$ gilt, können wir alternativ auch die Primideale von $k(\mathfrak{p})[X]/(\overline{m}_\alpha)$ bestimmen! Das vereinfacht die Aufgabe enorm, weil $k(\mathfrak{p})[X]$ ein Hauptidealring ist.

Gehen wir nun zurück zum Beweis. Nach dem Chinesischen Restsatz ist die kanonische Abbildung

$$k(\mathfrak{p})[X]/(\overline{m}_\alpha) \to \prod_{j=1}^{r} k(\mathfrak{p})[X]/(\overline{q}_j^{e_j})$$

ein Ringisomorphismus. Insgesamt haben wir also einen Isomorphismus

$$\varphi\colon \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \to \prod_{j=1}^{r} k(\mathfrak{p})[X]/(\overline{q}_j^{e_j}). \tag{4.8}$$

Wir studieren nun einen einzelnen Faktor $k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$ näher. Die Ideale in $k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$ entsprechen den Idealen von $k(\mathfrak{p})[X]$, die $\overline{q}_i^{e_i}$ enthalten. Da $\overline{q}_i$ irreduzibel ist und $k(\mathfrak{p})[X]$ Hauptidealring, hat der Ring $k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$ also genau die $e_i + 1$ Ideale

$$(\overline{q}_i^{\ell})/(\overline{q}_i^{e_i}) \qquad \text{für} \quad \ell = 0, \dots, e_i.$$

Insbesondere hat $k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$ genau ein Primideal, nämlich $\mathfrak{q}_i := (\overline{q}_i)/(\overline{q}_i^{e_i})$. Das Produkt $\prod_{j=1}^{r} k(\mathfrak{p})[X]/(\overline{q}_j^{e_j})$ besitzt demnach genau r verschiedene Primideale. Diese korrespondieren zu den r Faktoren des Produkts.

Wegen der Isomorphie (4.8) hat der Ring $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ also ebenfalls genau r verschiedene Primideale. Mit anderen Worten: Es gibt genau r verschiedene Primideale $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ von $\mathcal{O}_L$, die $\mathfrak{p}\mathcal{O}_L$ teilen. Diese sind gerade durch $\mathfrak{P}_i := \varphi_i^{-1}(\mathfrak{q}_i)$, wobei φ_i die verknüpfte Abbildung

$$\mathcal{O}_L \xrightarrow{\text{Quot.}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \xrightarrow{\varphi} \prod_{j=1}^{r} k(\mathfrak{p})[X]/(\overline{q}_j^{e_j}) \xrightarrow{i\text{-te Proj.}} k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$$

$$\mathcal{O}_L \xrightarrow{\varphi_i} k(\mathfrak{p})[X]/(\overline{q}_i^{e_i})$$

ist. Definitionsgemäß gilt $\varphi_i(\alpha) = X + (\overline{q}_j^{e_j})$ und damit folgt die behauptete explizite Beschreibung

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + (q_i(\alpha)).$$

Um die restlichen Aussagen zu zeigen, sei nun

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{P}_r^{\nu_r}$$

die Primfaktorisierung. Analog zu oben liefert der Chinesische Restsatz dann einen Isomorphismus

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{j=1}^{r} \mathcal{O}_L/\mathfrak{P}_j^{\nu_j}.$$

Wie oben sehen wir, dass jeder Faktor $\mathcal{O}_L/\mathfrak{P}_i^{\nu_i}$ genau $\nu_i + 1$ Ideale hat. Zusammen mit (4.8) erhalten wir

$$\prod_{j=1}^{r} \mathcal{O}_L/\mathfrak{P}_j^{\nu_j} \cong \prod_{j=1}^{r} k(\mathfrak{p})[X]/(\overline{q}_j^{e_j}).$$

Nach Definition der $\mathfrak{P}_i$ wird der i-te Faktor der linken Seite auf den i-ten Faktor der rechten Seite abgebildet. Der i-te Faktor der linken Seite hat $\nu_i + 1$ Ideale, während der i-te Faktor der rechten Seite gerade $e_i + 1$ Ideale besitzt. Das zeigt schließlich $\nu_i = e_i$ und wir erhalten wie gewünscht

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

Wir zeigen nun die Aussage über die Trägheitsgrade. Wegen

$$\mathcal{O}_L/\mathfrak{P}_i \cong (\mathcal{O}_L/\mathfrak{P}_i^{e_i})/(\mathfrak{P}_i/\mathfrak{P}_i^{e_i}) \cong (k(\mathfrak{p})[X]/(\overline{q}_i^{e_i}))/((\overline{q}_i)/(\overline{q}_i^{e_i})) \cong k(\mathfrak{p})[X]/(\overline{q}_i)$$

ist $\mathcal{O}_L/\mathfrak{P}_i$ ein $\deg(\overline{q}_i)$-dimensionaler $k(\mathfrak{p})$-Vektorraum, was

$$N(\mathfrak{P}_i) = |\mathcal{O}_L/\mathfrak{P}_i| = |k(\mathfrak{p})|^{\deg(\overline{q}_i)} = N(\mathfrak{p})^{\deg(\overline{q}_i)},$$

also $f(\mathfrak{P}_i|\mathfrak{p}) = \deg(\overline{q}_i)$ zeigt.

□

Beispiel 4.42. Wir betrachten die Erweiterung $\mathbb{Q}(i)/\mathbb{Q}$. Dann gilt $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, die Voraussetzung von Satz 4.41 ist also erfüllt. Es ist $X^2 + 1 \in \mathbb{Z}[X]$ das Minimalpolynom von i. Sei p eine Primzahl. Nach Satz 4.41 bestimmt das Zerfallen von $X^2 + 1$ modulo p die Primfaktorisierung von $p\mathbb{Z}[i]$. Wir unterscheiden mehrere Fälle:

- Wir betrachten zunächst den Fall $p = 2$. Es gilt

  $$\overline{X^2 + 1} = (X + \overline{1})^2 \in \mathbb{F}_2[X].$$

  Somit gilt $2\mathbb{Z}[i] = (2, i+1)^2 = (i+1)^2$, wobei im letzten Schritt verwendet wurde, dass das Quadrat von $i + 1$ gleich $2i$ ist und damit 2 im von $i + 1$ erzeugten Ideal liegt. Somit ist 2 in $\mathbb{Q}(i)$ total verzweigt.

- Sei p nun ungerade[2]. Dann gilt $p = 4k - 1$ oder $p = 4k + 1$ für ein $k \in \mathbb{Z}$. Wir behandeln beide Fälle separat:

  - Falls $p = 4k - 1$, so ist $|\mathbb{F}_p^*| = 4k - 2$ nicht durch 4 teilbar, und damit enthält $\mathbb{F}_p^*$ kein Element der Ordnung 4. Mit anderen Worten: Es gibt kein $a \in \mathbb{Z}$, sodass $a^2 \equiv -1 \pmod{p}$. Es folgt, dass

    $$\overline{X^2 + 1} \in \mathbb{F}_p[X]$$

    irreduzibel ist. Also ist $p\mathbb{Z}[i]$ prim und p ist total träge in $\mathbb{Q}(i)$.

  - Falls $p = 4k + 1$, so ist $|\mathbb{F}_p^*| = 4k$ durch 4 teilbar. Da $\mathbb{F}_p^*$ außerdem zyklisch ist, enthält $\mathbb{F}_p^*$ ein Element $\overline{a}$ der Ordnung 4 . Es gilt also $\overline{a}^2 = \overline{-1}$ in $\mathbb{F}_p$. Es folgt

    $$\overline{X^2 + 1} = (X - \overline{a})(X + \overline{a}) \in \mathbb{F}_p[X]$$

[2] Vielleicht erinnert Sie dieser Stichpunkt an das quadratische Reziprozitätsgesetz.

Sei $a \in \mathbb{Z}$ Repräsentant von $\overline{a}$. Dann gilt also

$$p\mathbb{Z}[i] = (p,\ a+i) \cdot (p,\ a-i).$$

Da diese Ideale verschieden sind, ist p in $\mathbb{Q}(i)$ total zerfallend. Dieser Stichpunkt sollte Sie im Übrigen an das Beispiel aus der Einleitung erinnern!

Die folgende Bemerkung bereitet Korollar 4.44 vor.

Bemerkung 4.43. Sei A ein Integritätsring. Wie bereits in Bemerkung 4.17 festgestellt, bleibt die Diskriminante eines Polynoms symmetrisch in den Nullstellen. Der Hauptsatz über elementarsymmetrische Polynome zeigt, dass es ein Polynom $\Delta_n \in A[X_0, \ldots, X_n]$ gibt, sodass für alle Polynome

$$f = a_n X^n + \ldots + a_0 \in A[X], \qquad a_n \neq 0$$

gilt, dass

$$\Delta(f) = \Delta_n(a_0, \ldots, a_n).$$

Insbesondere folgt damit $\Delta(f) \in A$. Ist nun $\mathfrak{p} \subset A$ ein Primideal und $a_n \notin \mathfrak{p}$, so erhalten wir

$$\overline{\Delta(f)} = \overline{\Delta_n(a_0, \ldots, a_n)} = \overline{\Delta}_n(\overline{a}_0, \ldots \overline{a}_n) = \Delta(\overline{f}) \in A/\mathfrak{p},$$

wobei $\overline{(-)}$ Restklassen modulo $\mathfrak{p}$ bezeichnet.

Nun erhalten wir eine essentielle Folgerung aus In der Situation aus Satz 4.41:

Korollar 4.44. *Sei K ein Zahlkörper und $\alpha \in \mathcal{O}_K$ ein primitives Element von K, sodass $\mathcal{O}_K = \mathbb{Z}[\alpha]$ gilt. Dann ist eine Primzahl $p \in \mathbb{Z}_{>0}$ genau dann in K verzweigt, wenn p die Diskriminante d_K teilt.*

Beweis. Sei

$$\overline{m}_\alpha = \overline{q}_1^{e_1} \cdot \ldots \cdot \overline{q}_r^{e_r}$$

die Faktorisierung der Reduktion $\overline{m}_\alpha \in \mathbb{F}_p[X]$. Es gilt

$$p \nmid \Delta(m_\alpha) \iff \overline{\Delta(m_\alpha)} \overset{\text{Bem. 4.43}}{=} \Delta(\overline{m}_\alpha) \in \mathbb{F}_p \setminus \{0\} \overset{\mathbb{F}_p \text{ separabel}}{\iff} e_1 = \ldots = e_r = 1. \quad (4.9)$$

Die Voraussetzung $\mathcal{O}_K = \mathbb{Z}[\alpha]$ impliziert außerdem, dass $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Ganzheitsbasis von $\mathcal{O}_K$ ist. Es gilt also

$$d_K = d_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(m_\alpha), \quad (4.10)$$

vgl. die Diskussion vor Korollar 4.19. Durch Kombination von (4.9) und (4.10) folgt also

$$p \nmid d_K \iff e_1 = \ldots = e_r = 1.$$

Die Behauptung folgt nun aus Satz 4.41, nach welchem die Verzweigungsindizes in der Primfaktorisierung von $p\mathcal{O}_K$ ja gerade die $e_1, \ldots, e_r$ sind. □

Bemerkung. Die Voraussetzung "$\mathcal{O}_K = \mathbb{Z}[\alpha]$" in Korollar 4.44 ist lästig. Wir werden im nächsten Abschnitt sehen, dass man sie weglassen kann.

Bemerkung. Man kann sich die Frage stellen, wieso wir Korollar 4.44 nur im Falle $K/\mathbb{Q}$ formuliert haben. Der Grund dafür ist, dass wir im Beweis verwendet haben, dass $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul ist. Haben wir ein endliche Erweiterung L/K, sodass $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ für ein α, so muss $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul sein. (Ist $\mathcal{O}_K$ jedoch ein Hauptidealring, so ist $\mathcal{O}_L$ ein freier $\mathcal{O}_K$-Modul und wir könnten Korollar 4.44 auf diese Situation mit demselben Beweis verallgemeinern.) Wie sich die Situation im allgemeinen Fall verhält, schildern wir in Abschnitt 4.7.

Beispiel 4.45. Die Diskriminante von $\mathbb{Q}(i)$ ist -4, also verzweigt nur 2 in $\mathbb{Q}(i)$. Das bestätigt unser Ergebnis aus Beispiel 4.42.

Wie bereits bemerkt, hat Satz 4.41 den Nachteil, dass er nur für monogene Erweiterungen L/K gilt (d.h., dass $\mathcal{O}_L$ von der Form $\mathcal{O}_K[\alpha]$ sein muss). Eine genaue Inspektion des Beweises zeigt, dass man diese Voraussetzung etwas abschwächen kann.

Definition 4.46. Sei $\alpha \in \mathcal{O}_L$ ein primitives Element von L/K (damit haben wir also $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$ und $\mathrm{Frac}(\mathcal{O}_K[\alpha]) = L$). Dann setzen wir

$$\mathfrak{C} := \{\gamma \in \mathcal{O}_L \mid \gamma\mathcal{O}_L \subset \mathcal{O}_K[\alpha]\}.$$

Bemerkung 4.47.

(1) Bei $\mathfrak{C}$ handelt es sich um ein Ideal $\neq (0)$, vgl. Aufgabe 4.6.2.

(2) Für $\gamma \in \mathfrak{C}$ gilt insbesondere $\gamma \cdot 1 \in \mathcal{O}_K[\alpha]$. Es folgt $\mathfrak{C} \subset \mathcal{O}_K[\alpha]$. Also ist $\mathfrak{C}$ auch ein Ideal von $\mathcal{O}_K[\alpha]$.

(3) Es gilt $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ genau dann, wenn $\mathfrak{C} = \mathcal{O}_L$ gilt.

Mit der obigen Notation gilt:

Satz 4.48. *Ist $\mathfrak{p} \neq (0)$ ein Primideal von $\mathcal{O}_K$, sodass*

$$\mathfrak{p}\mathcal{O}_L + \mathfrak{C} = \mathcal{O}_L,$$

so gilt die Aussage von Satz 4.41 auch für $\mathfrak{p}$.

Beweis. Im Beweis von Satz 4.41 wurde die Voraussetzung "$\mathcal{O}_L = \mathcal{O}_K[\alpha]$" nur dazu verwendet, um

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] \cong k(\mathfrak{p})[X]/(\overline{m}_\alpha)$$

zu erhalten. Es genügt also, zu zeigen, dass die verkettete Abbilduing

$$\mathcal{O}_K[\alpha] \xrightarrow{\text{Inkl.}} \mathcal{O}_L \xrightarrow{\text{Quot.}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L, \qquad \mathcal{O}_K[\alpha] \xrightarrow{\varphi} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

einen Isomorphismus $\mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ induziert. Wir zeigen also, dass φ surjektiv ist und den Kern $\mathfrak{p}\mathcal{O}_K[\alpha]$ hat. Ist das bewiesen, liefert der Homomorphiesatz einen Isomorphismus $\mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$.

Zur Surjektivität von φ: Wegen $\mathfrak{p}\mathcal{O}_L + \mathfrak{C} = \mathcal{O}_L$ lässt sich $\beta \in \mathcal{O}_L$ in der Form $\beta = x + y$ mit $x \in \mathfrak{p}\mathcal{O}_L$ und $y \in \mathfrak{C}$ schreiben. Es folgt $\beta + \mathfrak{p}\mathcal{O}_L = y + \mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Da

$\mathfrak{C} \subset \mathcal{O}_K[\alpha]$, gilt auch $y \in \mathcal{O}_K[\alpha]$ und wir haben $\varphi(y) = \beta + \mathfrak{p}\mathcal{O}_L$.

Zu $\ker(\varphi) = \mathfrak{p}\mathcal{O}_K[\alpha]$: Nach Definition von φ gilt

$$\ker(\varphi) = \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha].$$

Es folgt sofort $\mathfrak{p}\mathcal{O}_K[\alpha] \subset \ker(\varphi)$. Für die umgekehrte Inklusion behaupten wir die Gültigkeit der Implikation

$$\mathfrak{p}\mathcal{O}_L + \mathfrak{C} = \mathcal{O}_L \implies \mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C} = \mathcal{O}_K[\alpha] \qquad (*)$$

Diese sieht man wie folgt: Ist $\mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C}$ ein echtes Ideal von $\mathcal{O}_K[\alpha]$, so gibt es ein maximales Ideal $\mathfrak{m} \subset \mathcal{O}_K[\alpha]$, das $\mathfrak{p}\mathcal{O}_K[\alpha]$ und $\mathfrak{C}$ enthält. Dann enthält $\mathfrak{m}\mathcal{O}_L$ aber auch $\mathfrak{p}\mathcal{O}_L$ und $\mathfrak{C}\mathcal{O}_L$. Da $\mathfrak{C}$ ein Ideal von $\mathcal{O}_L$ ist, gilt $\mathfrak{C}\mathcal{O}_L = \mathfrak{C}$, also folgt $\mathfrak{p}\mathcal{O}_L + \mathfrak{C} \subset \mathfrak{m}\mathcal{O}_L \neq \mathcal{O}_L$. Das beweist $(*)$.

Wir erhalten nun die folgende Inklusionskette:

$$\begin{aligned}
\ker(\varphi) = \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha] &= \mathcal{O}_K[\alpha] \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \\
&\overset{(*)}{=} (\mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C})(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \\
&\overset{(1)}{\subset} \mathfrak{p}\mathcal{O}_K[\alpha] \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) + \mathfrak{C} \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \\
&\overset{(2)}{\subset} \mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C} \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \\
&\overset{(3)}{\subset} \mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C}\mathfrak{p}\mathcal{O}_L \\
&\overset{(4)}{=} \mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C}\mathfrak{p} \\
&\overset{(5)}{\subset} \mathfrak{p}\mathcal{O}_K[\alpha].
\end{aligned}$$

Wir rechtfertigen die einzelnen Schritte:

(1) Das Ideal $(\mathfrak{p}\mathcal{O}_K[\alpha] + \mathfrak{C})(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha])$ wird von allen Elementen der Form $(x + c) \cdot y$ mit $x \in \mathfrak{p}\mathcal{O}_K[\alpha]$, $c \in \mathfrak{C}$ und $y \in \mathcal{O}_K[\alpha] \cap \mathfrak{p}\mathcal{O}_L$ erzeugt.
Analog wird $\mathfrak{p}\mathcal{O}_K[\alpha] \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) + \mathfrak{C} \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha])$ von allen Elementen der Form $x \cdot y_1 + c \cdot y_2$ mit $x \in \mathfrak{p}\mathcal{O}_K[\alpha]$, $c \in \mathfrak{C}$ und $y_1, y_2 \in \mathcal{O}_K[\alpha] \cap \mathfrak{p}\mathcal{O}_L$ erzeugt. Das zeigt die Inklusion.

(2) ist klar, da $\mathfrak{p}\mathcal{O}_K[\alpha] \cdot (\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \subset \mathfrak{p}\mathcal{O}_K[\alpha]$.

(3) folgt ebenfalls sofort, da $\mathcal{O}_K[\alpha] \cap \mathfrak{p}\mathcal{O}_L \subset \mathfrak{p}\mathcal{O}_L$.

(4) Es ist $\mathfrak{C}$ ein Ideal von $\mathcal{O}_L$, und damit gilt $\mathfrak{C}\mathcal{O}_L = \mathfrak{C}$.

(5) erhalten wir aus $\mathfrak{C} \subset \mathcal{O}_K[\alpha]$. □

Beispiel 4.49. Sei $K = \mathbb{Q}(\alpha)$, wobei α eine Nullstelle von $f = X^3 + X^2 - 2X + 8 \in \mathbb{Q}[X]$ ist. In Aufgabe 1.0.4 haben wir gesehen, dass f irreduzibel ist, und dass

$$\beta := \frac{\alpha + \alpha^2}{2} \in \mathcal{O}_K$$

gilt. Wir behaupten, dass $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ gilt. Die Inklusion "$\supset$" ist klar. Für die andere Inklusion nutzen wir:

Trick: *Ist $M \subset \mathcal{O}_K$ ein freier Untermodul von maximalem Rang mit quadratfreier Diskriminante d_M, so gilt $M = \mathcal{O}_K$.*

Begründung: Nach Proposition 4.14 (2) gilt $d_M = (\mathcal{O}_K : M)^2 \cdot d_K$, und da d_M quadratfrei ist, muss $(\mathcal{O}_K : M) = 1$, also $\mathcal{O}_K = M$ gelten.

Wir wenden dies auf den Untermodul

$$M := \langle 1, \alpha, \beta \rangle_{\mathbb{Z}} \subset \mathbb{Z}[\alpha, \beta] \subset \mathcal{O}_K.$$

an. Wir bemerken dafür zunächst, dass M frei vom Rang 3 ist: Wäre $\{1, \alpha, \beta\}$ nämlich linear abhängig, dann gäbe es $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$, nicht alle gleich 0, sodass

$$\lambda_1 + \lambda_2\alpha + \lambda_3\frac{\alpha + \alpha^2}{2} = \lambda_1 + \left(\lambda_2 + \frac{\lambda_3}{2}\right) \cdot \alpha + \frac{\lambda_3}{2} \cdot \alpha^2 = 0.$$

In diesem Fall ist α also Nullstelle eines rationalen Polynoms vom Grad ≤ 2, was der Irreduzibilität von f widerspricht. Damit ist M also tatsächlich frei vom Rang 3.

Wir berechnen nun die Diskriminante von M. Die darstellende Matrix von $L_\alpha \colon K \to K$, $x \mapsto \alpha x$ bzgl. der Basis $\{1, \alpha, \alpha^2\}$ ist die Begleitmatrix

$$C := \begin{pmatrix} 0 & 0 & -8 \\ 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix}.$$

Dann folgt, dass L_{α^2} die darstellende Matrix

$$C^2 = \begin{pmatrix} 0 & -8 & 8 \\ 0 & 2 & -10 \\ 1 & -1 & 3 \end{pmatrix}.$$

hat. Mittels $\alpha^3 = -\alpha^2 + 2\alpha - 8$ und $\alpha^4 = -\alpha^3 + 2\alpha^2 - 8\alpha = 3\alpha^2 - 10\alpha + 8$ berechnen wir noch

$$\begin{aligned} \alpha\beta &= \frac{\alpha^2 + \alpha^3}{2} = \alpha - 4, \\ \beta^2 &= \frac{\alpha^4 + 2\alpha^3 + \alpha^2}{4} = \frac{2\alpha^2 - 6\alpha - 8}{4} = \frac{1}{2}\alpha^2 - \frac{3}{2}\alpha - 2. \end{aligned}$$

Nun berechnen wir die Spuren:

$$\begin{aligned} &\mathrm{tr}_{K/\mathbb{Q}}(1) = 3, \\ &\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = -1 \qquad \text{(vgl. auch Lemma 4.7)}, \\ &\mathrm{tr}_{K/\mathbb{Q}}(\alpha^2) = 5, \\ &\mathrm{tr}_{K/\mathbb{Q}}(\beta) = \frac{1}{2}\left(\mathrm{tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{tr}_{K/\mathbb{Q}}(\alpha^2)\right) = 2, \\ &\mathrm{tr}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{tr}_{K/\mathbb{Q}}(\alpha) - 12 = -13, \\ &\mathrm{tr}_{K/\mathbb{Q}}(\beta^2) = \frac{1}{2}\,\mathrm{tr}_{K/\mathbb{Q}}(\alpha^2) - \frac{3}{2}\,\mathrm{tr}_{K/\mathbb{Q}}(\alpha) - 6 = -2. \end{aligned}$$

Schließlich erhalten wir

$$d_M = \det \begin{pmatrix} \mathrm{tr}_{K/\mathbb{Q}}(1) & \mathrm{tr}_{K/\mathbb{Q}}(\alpha) & \mathrm{tr}_{K/\mathbb{Q}}(\beta) \\ \mathrm{tr}_{K/\mathbb{Q}}(\alpha) & \mathrm{tr}_{K/\mathbb{Q}}(\alpha^2) & \mathrm{tr}_{K/\mathbb{Q}}(\alpha\beta) \\ \mathrm{tr}_{K/\mathbb{Q}}(\beta) & \mathrm{tr}_{K/\mathbb{Q}}(\alpha\beta) & \mathrm{tr}_{K/\mathbb{Q}}(\beta^2) \end{pmatrix} = \det \begin{pmatrix} 3 & -1 & 2 \\ -1 & 5 & -13 \\ 2 & -13 & -2 \end{pmatrix} = -503.$$

Nach Proposition 4.14 (2) gilt nun aber

$$-503 = d_M = (\mathcal{O}_K : M)^2 \cdot d_K.$$

Da 503 eine Primzahl ist (also insbesondere quadratfrei), muss also $(\mathcal{O}_K : M) = 1$ und $d_K = -503$ gelten. Mit anderen Worten: Es gilt tatsächlich $\mathcal{O}_K = M = \mathbb{Z}[\alpha, \beta]$! Insbesondere ist $\mathbb{Z}[\alpha]$ echt in $\mathcal{O}_K$ enthalten, und somit benötigen wir den stärkeren Satz 4.48, um Primfaktorisierungen in $\mathcal{O}_K$ berechnen zu können.

Sei $\mathfrak{C} = \{\gamma \in \mathcal{O}_K \mid \gamma\mathcal{O}_K \subset \mathbb{Z}[\alpha]\}$. Wegen $2\mathcal{O}_K \subset \mathbb{Z}[\alpha]$ ist $2 \in \mathfrak{C}$, d.h. $\mathfrak{C} \mid 2\mathcal{O}_K$. Jede Primzahl $p \neq 2$ ist also teilerfremd zu $\mathfrak{C}$.
Beispielsweise für $p = 503$ ist $\overline{f} = (X + 299)(X + 354)^2 \in \mathbb{F}_{503}[X]$ die Zerlegung in irreduzible Faktoren. Also ist die Primfaktorisierung von $503\mathcal{O}_K$ wie folgt gegeben:

$$503\mathcal{O}_K = (503,\ \alpha + 299) \cdot (503,\ \alpha + 354)^2.$$

Für $p = 2$ behaupten wir $2\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ für die paarweise verschiedenen Primideale

$$\mathfrak{p}_1 = (2, \alpha, \beta), \qquad \mathfrak{p}_2 = (2, \alpha, \beta - 1), \qquad \mathfrak{p}_3 = (2, \alpha - 1, \beta - 1).$$

Um nachzuweisen, dass $2\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ ist, bemerken wir zunächst, dass die $\mathfrak{p}_i$ sicherlich $2\mathcal{O}_K$ teilen. Außerdem sind $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ paarweise teilerfremd, denn

$$\begin{aligned} 1 &= \beta - (\beta - 1) \in \mathfrak{p}_1 + \mathfrak{p}_2, \\ 1 &= \beta - (\beta - 1) \in \mathfrak{p}_1 + \mathfrak{p}_3, \\ 1 &= \alpha - (\alpha - 1) \in \mathfrak{p}_2 + \mathfrak{p}_3. \end{aligned}$$

Aus der paarweisen Teilerfremdheit folgt

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \mid 2\mathcal{O}_K.$$

Als nächstes behaupten wir, dass $\mathfrak{p}_i \neq \mathcal{O}_K$ für $i = 1, 2, 3$ gilt. Dafür genügt es, für jedes $i = 1, 2, 3$ ein $x_i \in K \setminus \mathcal{O}_K$ mit $x_i\mathfrak{p}_i \subset \mathcal{O}_K$ anzugeben. Man rechnet nach, dass beispielsweise

$$x_1 = \frac{\beta + 1}{2}, \qquad x_2 = \frac{\beta - 1}{2}, \qquad x_3 = \frac{\alpha}{2}$$

die geforderten Eigenschaften haben: Klarerweise sind die x_i nicht in $\mathcal{O}_K$ enthalten, weil die Darstellung von x_i als Linearkombination bzgl. der Ganzheitsbasis $\{1, \alpha, \beta\}$ von $\mathcal{O}_K$ nicht ganzzahlig ist. Außerdem gilt

$$\begin{aligned} &2x_1 = \beta + 1 \in \mathcal{O}_K, && \alpha x_1 = \alpha - 2 \in \mathcal{O}_K, && \beta x_1 = -1 - \alpha + \beta \in \mathcal{O}_K, \\ &2x_2 = \beta - 1 \in \mathcal{O}_K, && \alpha x_2 = -\alpha - 2 \in \mathcal{O}_K, && (\beta - 1)x_2 = 1 + \alpha - \beta \in \mathcal{O}_K, \\ &2x_3 = \alpha \in \mathcal{O}_K, && (\alpha - 1)x_3 = \beta - \alpha \in \mathcal{O}_K, && (\beta - 1)x_3 = -\alpha - 2 \in \mathcal{O}_K. \end{aligned}$$

Also ist $\mathfrak{p}_i \neq \mathcal{O}_K$ für $i = 1, 2, 3$.

Wir weisen nun "$2\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$" und "$\mathfrak{p}_i$ prim" auf zwei Arten nach:

Möglichkeit 1: Die fundamentale Gleichung 4.39 impliziert, dass es höchstens $3 = [K : \mathbb{Q}]$ verschiedene Primideale gibt, die $2\mathcal{O}_K$ teilen. Da die $\mathfrak{p}_i$ paarweise verschieden sind, $2\mathcal{O}_K$ teilen und $\neq \mathcal{O}_K$ sind, müssen die $\mathfrak{p}_i$ also prim sein und $2\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ folgt.

Möglichkeit 2: Die Multiplikativität der Norm impliziert

$$N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3) \mid N(2\mathcal{O}_K) = |N_{K/\mathbb{Q}}(2)| = 2^3.$$

Da $\mathfrak{p}_i \neq \mathcal{O}_K$, gilt $N(\mathfrak{p}_i) > 1$. Es muss also $N(\mathfrak{p}_i) = 2$ für $i = 1, 2, 3$ gelten. Das zeigt, dass die $\mathfrak{p}_i$ Primideale sind (da dann $\mathcal{O}_K/\mathfrak{p}_i$ ein Ring mit zwei Elementen ist, also isomorph zu $\mathbb{Z}/2\mathbb{Z}$ sein muss). Also folgt $N(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3) = N(2\mathcal{O}_K)$ und damit muss $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 = 2\mathcal{O}_K$ gelten.

Zum Ende das Kapitels möchten wir noch die Tricks und Kniffe festhalten, die wir für unsere Berechnungen verwendet haben:

Tricks 4.50. Sei K ein Zahlkörper.

(1) Es ist im Allgemeinen schwierig, $\mathcal{O}_K$ genau zu bestimmen. Oftmals funktioniert jedoch der folgende Ansatz:

Schritt 1: Man finde einen $\mathbb{Z}$-Untermodul $M \subset \mathcal{O}_K$ vom Rang n durch Angabe einer expliziten $\mathbb{Z}$-Basis von M, von dem man vermutet, dass er bereits $\mathcal{O}_K$ ist.

Schritt 2: Man berechne die Diskriminante d_M.

Schritt 3: Nach Proposition 4.14 (2) gilt $d_M = (\mathcal{O}_K : M)^2 \cdot d_K$. Ist d_M also quadratfrei, so folgt sofort $\mathcal{O}_K = M$. Ist d_M nicht quadratfrei, so hat man noch die Chance, Aufgabe 4.4.5 zu nutzen: Diese besagt nämlich, dass

$$d_K \equiv 0 \pmod 4 \qquad \text{oder} \qquad d_K \equiv 1 \pmod 4$$

gilt. Zusammen mit $d_M = (\mathcal{O}_K : M)^2 \cdot d_K$ liefert das also Informationen über den Index $(\mathcal{O}_K : M)$ und zeigt vielleicht, dass dieser 1 ist. Schlägt diese Methode auch fehl, so gilt entweder $\mathcal{O}_K \neq M$, oder man hat Pech und muss andere Methoden nutzen, um $\mathcal{O}_K = M$ zu zeigen.

(2) Ist $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal, sodass $N(\mathfrak{a}) = p$ eine Primzahl p ist, so ist $\mathfrak{a}$ ein Primideal (siehe auch Aufgabe 4.5.1).

Begründung 1: Da für ein ganzes Ideal $\mathfrak{b} \neq (0)$ genau dann $N(\mathfrak{b}) = 1$ gilt, wenn $\mathfrak{b} = \mathcal{O}_K$ ist, ist $N(\mathfrak{a})$ keine Primzahl, wenn $\mathfrak{a}$ kein Primideal ist.

Begründung 2: Es genügt allgemeiner zu zeigen, dass jeder endliche Ring A mit $|A| = p$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist. Betrachte hierfür den Ringhomomorphismus $\varphi\colon \mathbb{Z} \to A$, $1 \mapsto 1$. Es gilt $\ker(\varphi) = n\mathbb{Z}$ für ein $n \geq 2$. Der Homomorphiesatz induziert dann eine injektive Abbildung $\overline{\varphi}\colon \mathbb{Z}/n\mathbb{Z} \to A$. Da $\overline{\varphi}$ injektiv ist, muss n ein Teiler von $|A| = p$ sein. Es folgt $n = p$ und $\overline{\varphi}$ ist ein Isomorphismus.

(3) Hat man Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ gefunden, die $p\mathcal{O}_K$ für eine Primzahl p teilen, so lohnt es sich oft, die Normen von $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ und $p\mathcal{O}_K$ zu vergleichen und/oder die fundamentale Gleichung zu nutzen, um $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \mathfrak{p}_r$ zu zeigen.

4.6.1 Übungen

Aufgabe 4.6.1. Zeigen Sie, dass der Ganzheitsring eines Zahlkörpers unendlich viele Primideale hat.

Aufgabe 4.6.2. Sei L/K Erweiterung von Zahlkörpern und $\alpha \in \mathcal{O}_L$ ein primitives Element. Zeigen Sie: $\mathfrak{C} = \{\gamma \in \mathcal{O}_L \mid \gamma\mathcal{O}_L \subset \mathcal{O}_K[\alpha]\}$ ist ein Ideal $\neq (0)$ von $\mathcal{O}_L$.

Aufgabe 4.6.3. Sei $K = \mathbb{Q}(\sqrt{-19})$. Berechnen Sie die Primidealzerlegung von $p\mathcal{O}_K$ für $p = 2, 3, 5, 7$.

Aufgabe 4.6.4. Sei α eine Nullstelle von $X^3 - X - 2 \in \mathbb{Z}[X]$ und $K = \mathbb{Q}(\alpha)$. In Aufgabe 4.4.6 haben Sie verifiziert, dass $\mathcal{O}_K = \mathbb{Z}[\alpha]$ gilt und dafür $d_K = -104$ gezeigt. Sei nun p eine Primzahl. Erläutern Sie kurz, warum eine der folgenden fünf Möglichkeiten eintritt:

(i) p ist in K total zerfallend,

(ii) p ist in K total verzweigt,

(iii) p ist in K total träge,

(iv) $p\mathcal{O}_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2$ für Primideale $\mathfrak{p}_1 \neq \mathfrak{p}_2$ von $\mathcal{O}_K$,

(v) $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ für Primideale $\mathfrak{p}_1 \neq \mathfrak{p}_2$ von $\mathcal{O}_K$.

Gibt es für jede der fünf Möglichkeiten eine entsprechende Primzahl p? Wenn ja, so geben Sie diese explizit an und begründen Sie Ihre Antwort. Wenn nein, beweisen Sie die Nichtexistenz.
Hinweis: Die größte Primzahl, die Sie probieren sollten, ist die 31. Wenn Sie eine gute Nudel sein möchten, können Sie auch noch die Primidealzerlegung von $p\mathcal{O}_K$ in den einzelnen Fällen angeben, notwendig für die Lösung ist das allerdings nicht.

Aufgabe 4.6.5. Sei $\alpha \notin \mathbb{Q}$ eine Nullstelle von $X^4 - \frac{3}{2}X^3 + \frac{1}{2}X^2 + X - \frac{1}{2} \in \mathbb{Q}[X]$ und $K = \mathbb{Q}(\alpha)$.

(1) Finden Sie $\mathcal{O}_K$.

(2) Berechnen Sie die Primidealzerlegungen von $p\mathcal{O}_K$ für $p \in \{2, 5, 23\}$. Geben Sie in allen Fällen die Verzweigungsindizes und Trägheitsgrade an.

Aufgabe 4.6.6. Sei L/K eine Körpererweiterung von Zahlkörpern und F ein Zwischenkörper. Sei $\mathfrak{P} \neq (0)$ ein Primideal in $\mathcal{O}_L$ und $\mathfrak{P}_F := \mathfrak{P} \cap \mathcal{O}_F$, $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$. Zeigen Sie:

$$f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}_F) \cdot f(\mathfrak{P}_F|\mathfrak{p}) \qquad \text{und} \qquad e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}_F) \cdot e(\mathfrak{P}_F|\mathfrak{p}).$$

4.7 Diskriminante und Verzweigung

Sei K ein Zahlkörper. In Korollar 4.44 haben wir gesehen, dass unter der Voraussetzung

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \text{ für ein } \alpha \in \mathcal{O}_K \tag{4.11}$$

eine Primzahl p genau dann in K verzweigt, wenn $p \mid d_K$. In diesem Kapitel zeigen wir, dass dieselbe Folgerung auch ohne die Voraussetzung (4.11) gilt.
Des Weiteren skizzieren wir der Vollständigkeit halber, wie sich die Situation allgemein, das heißt, in einer Erweiterung L/K von Zahlkörpern darstellt. Da wir dies für den weiteren Verlauf der Vorlesung nicht benötigen werden, verzichten wir hier auf vollständige Beweise. Stattdessen erklären wir, wie der Beweis im Spezialfall $K/\mathbb{Q}$ angepasst werden muss.

Das Ziel ist es, den folgenden Satz zu beweisen:

Satz 4.51. *Sei K ein Zahlkörper und p eine Primzahl. Dann gilt:*

$$p \text{ ist in } K \text{ verzweigt} \iff p \mid d_K.$$

Insbesondere verzweigen in K nur endlich viele Primzahlen.

Wie zu erwarten ist, wird der Beweis etwas aufwendiger als jener von Korollar 4.44. Wir benötigen vorbereitende Lemmata, die im Wesentlichen den Aufgaben 4.3.1 und 4.3.2 entsprechen:

Lemma 4.52. *Sei B ein Ring, der ein freier A-Modul vom Rang n ist. Sei $\mathfrak{a} \subset A$ ein Ideal, $\overline{A} := A/\mathfrak{a}$ und $\overline{B} := B/\mathfrak{a}B$. Ist $(\beta_1, \ldots, \beta_n)$ eine A-Basis von B, so ist $(\overline{\beta}_1, \ldots, \overline{\beta}_n)$ eine $\overline{A}$-Basis von $\overline{B}$, wobei $\overline{\beta}_i$ das Bild von β_i in $\overline{B}$ sei. Des Weiteren gilt*

$$d_{B/A}(\beta_1, \ldots, \beta_n) + \mathfrak{a}B = d_{\overline{B}/\overline{A}}(\overline{\beta}_1, \ldots, \overline{\beta}_n).$$

Beweis. Wir zeigen zunächst, dass dass $(\overline{\beta}_1, \ldots, \overline{\beta}_n)$ eine $\overline{A}$-Basis von $\overline{B}$ ist. Dass es sich um ein Erzeugendensystem handelt, ist klar. Es bleibt die lineare Unabhängigkeit zu zeigen. Seien dazu $x_1, \ldots, x_n \in A$ mit

$$\overline{x}_1\overline{\beta}_1 + \ldots + \overline{x}_n\overline{\beta}_n = 0 \in \overline{B}$$

gegeben. Dann folgt

$$x_1\beta_1 + \ldots + x_n\beta_n \in \mathfrak{a}B. \tag{4.12}$$

Wir behaupten, dass alle x_i in $\mathfrak{a}$ liegen. Aus (4.12) erhalten wir die Existenz von $y_1, \ldots, y_m \in \mathfrak{a}$ und $\gamma_1, \ldots, \gamma_m \in B$ mit

$$x_1\beta_1 + \ldots + x_n\beta_n = y_1\gamma_1 + \ldots + y_m\gamma_m.$$

Da $\{\beta_1, \ldots, \beta_n\}$ eine A-Basis von B ist, kann jedes γ_j als A-Linearkombination von $\{\beta_1, \ldots, \beta_n\}$ geschrieben werden, sagen wir

$$\gamma_j = \sum_{\ell=1}^{n} a_{j\ell}\beta_\ell.$$

Es folgt

$$x_1\beta_1 + \ldots + x_n\beta_n = (y_1a_{11} + \ldots + y_ma_{m1})\beta_1 + \ldots + (y_1a_{1n} + \ldots + y_ma_{mn})\beta_n.$$

Aus der Eindeutigkeit der Basisdarstellung erhalten wir mittels Koeffizientenvergleich schließlich

$$x_i = y_1a_{1i} + \ldots + y_ma_{mi} \in \mathfrak{a}$$

für jedes i, wie behauptet. Also ist $(\overline{\beta}_1, \ldots, \overline{\beta}_n)$ eine $\overline{A}$-Basis von $\overline{B}$.

Betrachte nun für $\beta \in B$ dann die Multiplikationsabbildung $L_\beta \colon B \to B$. Da $L_\beta(\mathfrak{a}B) \subset \mathfrak{a}B$, induziert L_β einen Endomorphismus

$$\begin{aligned} \overline{L}_\beta \colon \overline{B} &\to \overline{B}, \\ \overline{x} &\mapsto \overline{\beta x}. \end{aligned}$$

Aus der Definition folgt, dass $\overline{L}_\beta = L_{\overline{\beta}}$. Es folgt also

$$\overline{\mathrm{tr}_{B/A}(\beta)} = \mathrm{tr}_{\overline{B}/\overline{A}}(\overline{\beta}).$$

Daraus folgt dann die Behauptung. □

Lemma 4.53. *Seien B_1/A und B_2/A Ringerweiterungen, sodass B_1 und B_2 freie A-Moduln endlichen Ranges sind. Dann gilt $d_{(B_1 \times B_2)/A} = d_{B_1/A} \cdot d_{B_2/A}$.*

Beweis. Sei $(e_1, \ldots, e_m)$ eine A-Basis von B_1 und $(f_1, \ldots, f_n)$ eine A-Basis von B_2. Dann ist $((e_1, 0), \ldots, (e_m, 0), (0, f_1), \ldots, (0, f_n))$ eine A-Basis von $B_1 \times B_2$ – der Übersichtlichkeit wegen schreiben wir e_i bzw. f_j für $(e_i, 0)$ bzw. $(0, f_j)$. Die Diskriminante bezüglich der angegebenen Basis ist die Determinante der Block-Diagonalmatrix

$$\begin{pmatrix} \left(\mathrm{tr}_{(B_1 \times B_2)/A}(e_i e_k)\right)_{1 \le i,k \le m} & 0 \\ 0 & \left(\mathrm{tr}_{(B_1 \times B_2)/A}(f_j f_\ell)\right)_{1 \le k,\ell \le n} \end{pmatrix}$$

Es genügt dann,

$$\mathrm{tr}_{(B_1 \times B_2)/A}(\beta_1, 0) = \mathrm{tr}_{B_1/A}(\beta_1) \quad \text{bzw.} \quad \mathrm{tr}_{(B_1 \times B_2)/A}(0, \beta_2) = \mathrm{tr}_{B_2/A}(\beta_2)$$

für alle $\beta_1 \in B_1$ bzw. $\beta_2 \in B_2$ zu zeigen. Das folgt aber sofort, da für $\beta_1 \in B_1$ die darstellende Matrix der A-linearen Multiplikationsabbildung $L_{(\beta_1,0)} \colon B_1 \times B_2 \to B_1 \times B_2$ bzgl. der Basis $(e_1, \ldots, e_m, f_1, \ldots, f_n)$ die Blockdiagonalmatrix

$$\begin{pmatrix} M & 0 \\ 0 & 0 \end{pmatrix}$$

ist, wobei M die darstellende Matrix von $L_{\beta_1} \colon B_1 \to B_1$ bzgl. $(e_1, \ldots, e_m)$ ist. Mit β_2 funktioniert das natürlich analog. □

Beweis von Satz 4.51. Wir betrachten $\mathcal{O}_K$ als freien $\mathbb{Z}$-Modul vom Rang n und erinnern daran, dass definitionsgemäß $d_K = d_{\mathcal{O}_K} = d_{\mathcal{O}_K/\mathbb{Z}}(\alpha_1, \ldots, \alpha_n)$ für eine Ganzheitsbasis $(\alpha_1, \ldots, \alpha_n)$ gilt. Nach Lemma 4.52 ist $\overline{\mathcal{O}} := \mathcal{O}_K/p\mathcal{O}_K$ ein $\mathbb{F}_p$-Vektorraum der Dimension n und es gilt

$$p \mid d_K \iff d_{\overline{\mathcal{O}}/\mathbb{F}_p} = 0. \tag{4.13}$$

Sei $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die Primidealzerlegung, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathcal{O}_K$ paarweise verschiedene Primideale seien und $e_i \ge 1$. Nach dem Chinesischen Restsatz gilt

$$\overline{\mathcal{O}} \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \ldots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}.$$

Wir wenden nun Lemma 4.53 an und erhalten mit $\overline{\mathcal{O}}_i := \mathcal{O}_K/\mathfrak{p}_i^{e_i}$:

$$d_{\overline{\mathcal{O}}/\mathbb{F}_p} = \prod_{i=1}^{r} d_{\overline{\mathcal{O}}_i/\mathbb{F}_p}. \tag{4.14}$$

Aus (4.13) und (4.14) bekommen wir

$$p \mid d_K \iff \text{es gibt ein } i \in \{1, \dots, r\} \text{ mit } d_{\overline{\mathcal{O}}_i/\mathbb{F}_p} = 0.$$

Die Äquivalenz im Satz folgt also, wenn wir die folgenden beiden Aussagen zeigen:

(a) Wenn $e_i = 1$, so ist $d_{\overline{\mathcal{O}}_i/\mathbb{F}_p} \neq 0$, und

(b) Wenn $e_i > 1$, so ist $d_{\overline{\mathcal{O}}_i/\mathbb{F}_p} = 0$.

Zu (a): Falls $e_i = 1$, so ist $\overline{\mathcal{O}}_i = \mathcal{O}_K/\mathfrak{p}_i$ ein endlicher Körper. Die Erweiterung $\overline{\mathcal{O}}_i/\mathbb{F}_p$ ist also separabel. Sei α ein primitives Element der Erweiterung. Dann ist $\{1, \alpha, \dots, \alpha^{m-1}\}$ eine $\mathbb{F}_p$-Basis von $\overline{\mathcal{O}}_i$, wobei $m = [\overline{\mathcal{O}}_i : \mathbb{F}_p]$. Wir haben in der Diskussion vor Korollar 4.19 gesehen, dass

$$d_{\overline{\mathcal{O}}_i/\mathbb{F}_p}(1, \alpha, \dots, \alpha^{m-1}) = \Delta(m_\alpha) \neq 0$$

gilt. Das zeigt (a).

Zu (b): Falls $e_i > 1$, so wählen wir ein Element $b \in \mathfrak{p}_i \setminus \mathfrak{p}_i^{e_i}$. Dann gilt $b^{e_i} \in \mathfrak{p}_i^{e_i}$, und damit definiert die Klasse β von b in $\overline{\mathcal{O}}_i = \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ ein nicht-triviales nilpotentes. Für alle $\gamma \in \overline{\mathcal{O}}_i$ ist dann $\beta\gamma$ ebenfalls nilpotent. Somit definiert

$$L_{\beta\gamma} \colon \overline{\mathcal{O}}_i \to \overline{\mathcal{O}}_i, \qquad x \mapsto \beta\gamma x$$

für alle γ einen nilpotenten Endomorphismus des $\mathbb{F}_p$-Vektorraums $\overline{\mathcal{O}}_i$. Da nilpotente Endomorphismen die Spur 0 haben[3], gilt also für alle γ:

$$\mathrm{tr}_{\overline{\mathcal{O}}_i/\mathbb{F}_p}(\beta\gamma) = \mathrm{tr}(L_{\beta\gamma}) = 0.$$

Schließlich ergänzen wir β zu einer $\mathbb{F}_p$-Basis $\{\beta, \gamma_1, \dots, \gamma_\ell\}$ von $\overline{\mathcal{O}}_i$. Die Diskriminante bezüglich dieser Basis ist dann

$$d_{\overline{\mathcal{O}}_i/\mathbb{F}_p}(\beta, \gamma_1, \dots, \gamma_m) = \det \begin{pmatrix} \mathrm{tr}_{\overline{\mathcal{O}}_i|\mathbb{F}_p}(\beta^2) & \mathrm{tr}_{\overline{\mathcal{O}}_i|\mathbb{F}_p}(\beta\gamma_1) & \dots & \mathrm{tr}_{\overline{\mathcal{O}}_i|\mathbb{F}_p}(\beta\gamma_\ell) \\ \vdots & & & \vdots \end{pmatrix} = 0,$$

da sämtliche Einträge der ersten Zeile gleich 0 sind. Das zeigt dann (b).
Die zweite Aussage ("in K verzweigen nur endlich viele Primzahlen") folgt nun sofort, da $d_K \neq 0$ (das haben wir in Korollar 4.19 gesehen) und d_K somit nur endlich viele Primteiler hat. □

[3] Ist f ein nilpotenter Endomorphismus eines Vektorraums V der Dimension n, so ist $\mathrm{tr}(f)$ die Summe der Eigenwerte von f (in einem algebraischen Abschluss, mit Vielfachheiten gezählt). Es genügt also zu zeigen, dass f nur den Eigenwert 0 hat. Sei λ ein Eigenwert von f mit zugehörigem Eigenvektor $v \in V \setminus \{0\}$, so folgt aus der Nilpotenz $0 = f^n(v) = \lambda^n v$, also $\lambda = 0$.

Spoiler. In Abschnitt 5.2 werden wir sehen, dass $|d_K| \geq 2$ für alle Zahlkörper $K \neq \mathbb{Q}$ gilt. Somit verzweigt mindestens eine Primzahl in K. (Mit Hilfe von Aufgabe 4.4.5 erhalten wir sogar $|d_K| \geq 3$.)

Im Beweis von Satz 4.51 wurde essentiell verwendet, dass $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang $[K : \mathbb{Q}]$ ist. Aus diesem Grund verallgemeinert sich der Beweis nicht direkt auf den relativen Fall L/K, in dem wir eine Erweiterung von Zahlkörpern betrachten. Zunächst einmal muss erklärt werden, mit welchem Objekt wir die Diskriminante ersetzen.

Definition 4.54. Sei L/K eine Erweiterung von Zahlkörpern. Dann definiert man das *(relative) Diskriminantenideal* $\mathfrak{d}_{L/K}$ von L/K als das Ideal von $\mathcal{O}_K$, das von allen Diskriminanten $d_{L/K}(\underline{e})$ erzeugt wird, wobei $\underline{e} \subset \mathcal{O}_L$ eine K-Basis von L ist.

Bemerkung 4.55.

(1) Da das Minimalpolynom eines Elements $\alpha \in \mathcal{O}_L$ über K sogar Koeffizienten in $\mathcal{O}_K$ hat, gilt $\mathrm{tr}_{L/K}(\alpha) \in \mathcal{O}_K$ (vgl. auch Lemma 4.7). Also ist $\mathfrak{d}_{L/K}$ tatsächlich ein Ideal von $\mathcal{O}_K$.

(2) Ist $\alpha \in \mathcal{O}_L$ ein primitives Element von L/K, so ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine K-Basis von L. Es gilt also $d_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) \in \mathfrak{d}_{L/K}$. Da wir in der Diskussion vor Korollar 4.19 gesehen haben, dass $d_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(m_\alpha) \neq 0$ gilt, erhalten wir $\mathfrak{d}_{L/K} \neq (0)$.

(3) Ist $\mathcal{O}_L$ ein freier $\mathcal{O}_K$-Modul vom Rang $n = [L : K]$ (das gilt z.B. für $K = \mathbb{Q}$, oder allgemeiner, wenn $\mathcal{O}_K$ ein Hauptidealring ist), so wissen wir, dass sich je zwei Diskriminanten $d_{L/K}(\underline{e})$ und $d_{L/K}(\underline{e}')$ für K-Basen $\underline{e}, \underline{e}' \subset \mathcal{O}_L$ von L um ein Quadrat von $\mathcal{O}_K^*$ unterscheiden (dieses Element aus $\mathcal{O}_K^*$ ist die Determinante der Basiswechselmatrix von $\underline{e}$ auf $\underline{e}'$). Damit ist $\mathfrak{d}_{L/K}$ ein Hauptideal. Insbesondere gilt für einen Zahlkörper K, dass $\mathfrak{d}_{K/\mathbb{Q}} = (d_K)$.

(4) Ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul, so muss $\mathfrak{d}_{L/K}$ kein Hauptideal sein: Der Basiswechsel von $\underline{e}$ auf $\underline{e}'$ ist nämlich hier im Allgemeinen keine invertierbare Matrix mit Koeffizienten in $\mathcal{O}_K$, sondern mit Koeffizienten in K. Mit anderen Worten: Obwohl die Diskriminanten $d_{L/K}(\underline{e})$ und $d_{L/K}(\underline{e}')$ beides Elemente von $\mathcal{O}_K$ sind, unterscheiden sie sich um ein Quadrat aus K^*. Da $\mathfrak{d}_{L/K}$ aber ein Ideal in $\mathcal{O}_K$ ist, reicht i.A. nicht nur ein Erzeuger.

Satz 4.51 verallgemeinert sich dann wie folgt:

Satz 4.56. *Sei L/K eine Erweiterung von Zahlkörpern und $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann gilt:*

$$\mathfrak{p} \text{ ist in } L \text{ verzweigt} \iff \mathfrak{p} \mid \mathfrak{d}_{L/K}.$$

Insbesondere verzweigen in L nur endlich viele Primideale $\neq (0)$ von $\mathcal{O}_K$.

Beweisskizze. Wie bereits erwähnt, ist das größte Problem, dass $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul ist. Wir führen den Satz aber auf diesen Fall zurück, indem wir die lokalisierten Ringe

$$\mathcal{O}_{K,\mathfrak{p}} := (\mathcal{O}_K)_{\mathfrak{p}} \qquad \text{und} \qquad \mathcal{O}_{L,\mathfrak{p}} := (\mathcal{O}_L)_{\mathfrak{p}}$$

betrachten. Als Lokalisierung eines Dedekindrings an einem Primideal ist $\mathcal{O}_{K,\mathfrak{p}}$ ein diskreter Bewertungsring, also insbesondere ein Hauptidealring (vgl. Satz 3.3 und die

Erinnerung auf S. 19). Da $\mathcal{O}_L$ sogar der ganze Abschluss von $\mathcal{O}_K$ in L ist[4], folgt mit Lemma 3.4, dass $\mathcal{O}_{L,\mathfrak{p}}$ der ganze Abschluss von $\mathcal{O}_{K,\mathfrak{p}}$ ist.
Sei nun $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_{L,\mathfrak{p}}$ eine K-Basis von L. Sei M der freie $\mathcal{O}_{K,\mathfrak{p}}$-Modul, der von $\{\alpha_1, \ldots, \alpha_n\}$ erzeugt wird. Wie in Lemma 4.21 beweist man dann, dass

$$M \subset \mathcal{O}_{L,\mathfrak{p}} \subset d^{-1}M \qquad \text{mit} \quad d := d_{L/K}(\alpha_1, \ldots, \alpha_n)$$

gilt. Da der Elementarteilersatz 2.17 auch für Hauptidealringe gültig ist und sowohl M als auch $d^{-1}M$ freie $\mathcal{O}_{K,\mathfrak{p}}$-Moduln vom Rang $n = [L : K]$ ist, ist $\mathcal{O}_{L,\mathfrak{p}}$ auch frei vom Rang n. Die Aussage des Satzes folgt dann, indem man die folgenden Äquivalenzen zeigt:

$$\begin{aligned} & \mathfrak{p} \text{ ist in } L \text{ verzweigt} \\ \iff & \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \text{ teilt das Hauptideal } \left(d_{\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}}(\alpha_1, \ldots, \alpha_n)\right) \\ \iff & \mathfrak{p} \text{ teilt } \mathfrak{d}_{L/K}. \end{aligned}$$

Wir verzichten an dieser Stelle auf einen Beweis, möchten aber betonen, dass der Nachweis nicht schwierig ist. □

[4]Das folgt so: Sei C der ganze Abschluss von $\mathcal{O}_K$ in L. Dann haben wir ganze Ringerweiterungen $\mathbb{Z} \subset \mathcal{O}_K \subset C$, und nach Proposition 1.6 ist $C/\mathbb{Z}$ ganz, d.h. $C \subset \mathcal{O}_L$

Kapitel 5

Minkowski-Theorie

Das nächste große Ziel, ist es, die Endlichkeit der Klassengruppe $\mathrm{Cl}_K := \mathrm{Cl}_{\mathcal{O}_K}$ für einen Zahlkörper K zu beweisen. Das wird in Abschnitt 5.2 geschehen. Die Beweismethoden erlauben uns auch, weitere interessante Resultate zu beweisen, wie etwa die Sätze von Minkowski und Hermite (Abschnitt 5.3) und den Einheitensatz (Abschnitt 5.4).

5.1 Gittertheorie und Gitter in der Zahlentheorie

Im Folgenden sei V stets ein endlich-dimensionaler $\mathbb{R}$-Vektorraum der Dimension n.

Definition 5.1. Eine additive Untergruppe $\Lambda \subset V$ heißt ein *Gitter* in V, wenn es $\mathbb{R}$-linear unabhängige Vektoren $\underline{v} = (v_1, \ldots, v_m)$ von V gibt, sodass $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$. Die Menge $M = M_{\underline{v}} = \{\sum_{i=1}^m x_i v_i \mid 0 \leq x_i < 1\}$ heißt *Grundmasche* von Λ. Ein Gitter Λ heißt *vollständig*, wenn $\underline{v}$ Basis von V ist, d.h. wenn $m = n$.

Ein Gitter ist also ein endlich erzeugter $\mathbb{Z}$-Untermodul von V, der von einer linearen unabhängigen Teilmenge von V aufgespannt wird.

Bemerkung 5.2. Die Grundmasche M eines vollständigen Gitters $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ bildet ein Repräsentantensystem für V/Λ, d.h.

$$V = \bigsqcup_{m \in M} (m + \Lambda) = \bigsqcup_{\lambda \in \Lambda} (\lambda + M).$$

(Mit dem Symbol "$\sqcup$" bezeichnen wir eine disjunkte Vereinigung.)
Begründung: Jedes $x \in \mathbb{R}$ kann man eindeutig in der Form $x = m + y$ mit $m \in \mathbb{Z}$ und $y \in [0, 1)$ schreiben. Konkret:

$$m = \lfloor x \rfloor := \max\{k \in \mathbb{Z} \mid k \leq x\} \qquad \text{und} \qquad y = x - m.$$

Ist nun $v = \sum_{i=1}^n x_i v_i \in V$ mit $x_i \in \mathbb{R}$, so können wir

$$v = \underbrace{\sum_{i=1}^n \lfloor x_i \rfloor v_i}_{\in \Lambda} + \underbrace{\sum_{i=1}^n (x_i - \lfloor x_i \rfloor) v_i}_{\in M}$$

schreiben.

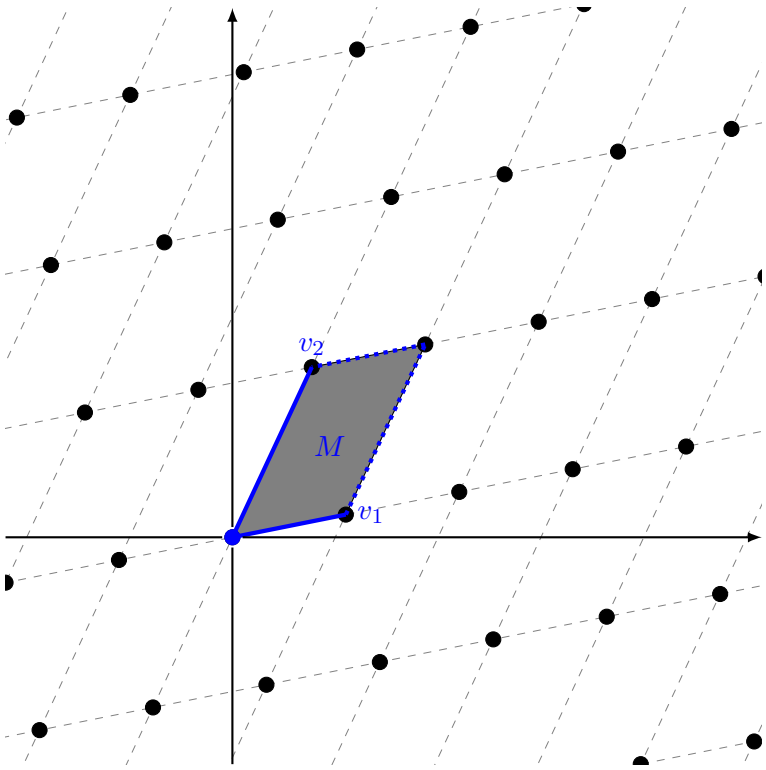


Abbildung 5.1: Das vollständige Gitter $\mathbb{Z}v_1 \oplus \mathbb{Z}v_2$ im $\mathbb{R}^2$ mit Grundmasche M.

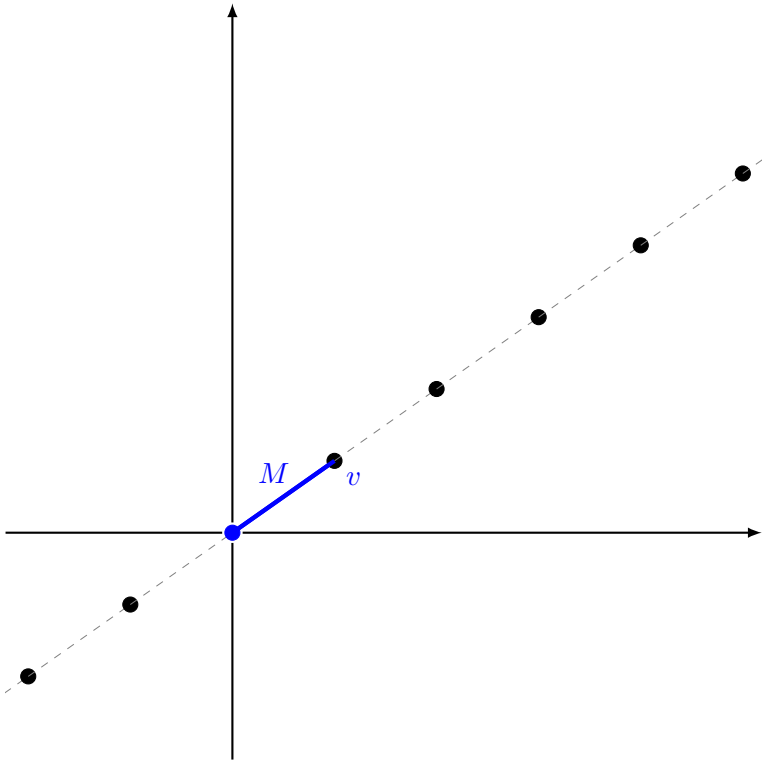


Abbildung 5.2: Das unvollständige Gitter $\mathbb{Z}v$ im $\mathbb{R}^2$ mit Grundmasche M.

Satz 5.3. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum, dann gilt:*

(1) Eine Untergruppe $\Lambda \subset V$ ist genau dann ein Gitter, wenn Λ diskret ist.

(2) Ist $\Lambda \subset V$ ein Gitter, so ist Λ genau dann vollständig, wenn eine beschränkte Menge $M \subset V$ mit $\bigcup_{\lambda\in\Lambda}(\lambda + M) = V$ existiert.

Vor dem Beweis gehen wir kurz auf die verwendeten topologischen Begriffe ein:

- Durch die Wahl irgendeiner Norm auf V erhalten wir eine Topologie auf V. Da auf endlich-dimensionalen $\mathbb{R}$-Vektorräumen alle Normen äquivalent sind, hängt diese Topologie nicht von der Wahl der Norm ab. Des Weiteren erlaubt uns die gewählte Norm von "Beschränktheit" zu sprechen, wie bereits in Satz 5.3 (2) geschehen.
- Ist X ein topologischer Raum und Y eine Teilmenge von X, so wird durch

$$W \subset Y \text{ heißt } \textit{offen} \text{ in } Y \iff \text{ es gibt } U \subset X \text{ offen mit } W = U \cap Y$$

  eine Topologie auf Y definiert, die die *Relativtopologie* auf Y genannt wird.
- Eine Teilmenge Y eines topologischen Raums heißt *diskret*, wenn die Relativtopologie auf Y die diskrete Topologie ist, d.h. alle Einpunktmengen $\{y\}$ mit $y \in Y$ sind offen in Y. Mit der Definition der Relativtopologie ist das äquivalent dazu, dass es für jedes $y \in Y$ eine offenes $U \subset X$ gibt, sodass $Y \cap U = \{y\}$. ("Alle Punkte in Y sind isoliert in X".)

Beweis. (1) Sei zunächst Λ ein Gitter. Dann gibt es $\mathbb{R}$-linear unabhängige Vektoren $\{v_1, \dots, v_m\} \subset V$, sodass $\Lambda = \mathbb{Z}v_1 \oplus \dots \mathbb{Z}v_m$¸. Wir ergänzen $\{v_1, \dots, v_m\}$ zu einer $\mathbb{R}$-Basis $\{v_1, \dots, v_n\}$ von V. Sei nun $\lambda = \sum_{i=1}^{m} a_i v_i \in \Lambda$, wobei $a_i \in \mathbb{Z}$. Für die in V offene Menge

$$U = \left\{ \sum_{i=1}^{n} x_i v_i \;\middle|\; |x_i - a_i| < 1 \text{ ¸für } i = 1, \dots, m \right\}$$

gilt dann $U \cap \Lambda = \{\lambda\}$, also ist Λ diskret.

Ist umgekehrt $\Lambda \subset V$ diskret, so betrachten wir den Untervektorraum V_0 von V, der von Λ erzeugt wird. Sei $\{v_1, \dots, v_m\} \subset \Lambda$ eine Basis von V_0 und $\Lambda_0 \subset \Lambda$ das Gitter mit der Basis $\{v_1, \dots, v_m\}$. Wir behaupten, dass $\Lambda_0 \subset \Lambda$ eine Untergruppe von endlichem Index ist. Dafür bemerken wir zunächst, dass

$$V_0 = \bigcup_{\lambda\in\Lambda_0} (\lambda + \overline{M_0}) \quad \text{mit } \overline{M_0} = \left\{ \sum_{i=1}^{m} x_i v_i \;\middle|\; 0 \le x_i \le 1 \right\}$$

gilt, weil Λ_0 ein vollständiges Gitter in V_0 ist. Wir wählen nun ein Repräsentantensystem $(\mu_i)_{i\in I}$ von Λ/Λ_0. Dann lässt sich μ_i für jedes $i \in I$ also in der Form

$$\mu_i = \lambda_{0i} + m_i, \qquad \text{wobei} \quad \lambda_{0i} \in \Lambda_0,\ m_i \in \overline{M_0}$$

schreiben. Die Differenzen $m_i = \mu_i - \lambda_{0i}$ sind also sowohl im Kompaktum $\overline{M_0}$ als auch in der diskreten Menge Λ enthalten. Da Λ als diskrete Untergruppe von V außerdem abgeschlossen ist, kann es nur endlich viele verschiedene m_i geben. (Die Details überlassen wir hier als Übungsaufgabe, vgl. Aufgabe 5.1.1.) Da die Klasse von m_i in Λ/Λ_0 gleich der von μ_i ist, folgt wie gewünscht, dass Λ/Λ_0 endlich ist.

Nun folgt, dass Λ ein Gitter ist: Mit $N = (\Lambda : \Lambda_0)$ haben wir dann $N\Lambda \subset \Lambda_0$, das heißt

$$\Lambda_0 \subset \Lambda \subset N^{-1}\Lambda_0.$$

Da Λ_0 und $N^{-1}\Lambda_0$ frei vom Rang m sind, zeigt der Elementarteilersatz 2.17, dass Λ ebenfalls frei vom Rang m ist. Des Weiteren zeigt er, dass man eine $\mathbb{Z}$-Basis von Λ durch geeignete Skalierung einer $\mathbb{Z}$-Basis von $N^{-1}\Lambda_0$ erhält. Da eine (und damit jede) $\mathbb{Z}$-Basis von $N^{-1}\Lambda_0$ durch ein System linear unabhängiger Vektoren von V gegeben ist, hat Λ auch eine $\mathbb{Z}$-Basis, die durch ein System linear unabhängiger Vektoren von V gegeben ist. Also ist Λ ein Gitter.

(2) Ist Λ vollständig, so können wir für M die Grundmasche von Λ wählen. Ist umgekehrt M beschränkt und es gilt $\bigcup_{\lambda\in\Lambda}(\lambda + M) = V$, so betrachten wir erneut den Untervektorraum $V_0 \subset V$, der von Λ erzeugt wird. Zu zeigen ist natürlich $V_0 = V$. Hierfür fixieren $v \in V$ und betrachten die Folge $(kv)_{k\geq 1}$ in V. Nach Voraussetzung gibt es für jedes $k \geq 1$ ein $\lambda_k \in \Lambda$ und ein $m_k \in M$ mit

$$kv = \lambda_k + m_k.$$

Da M beschränkt ist, ist $(m_k/k)_{k\geq 1}$ eine Nullfolge. Damit gilt mit dem Grenzübergang $k \to \infty$:

$$v = \lim_{k\to\infty} \frac{\lambda_k}{k} + \lim_{k\to\infty} \frac{m_k}{k} = \lim_{k\to\infty} \frac{\lambda_k}{k} \in V_0,$$

da V_0 als Untervektorraum eines endlich-dimensionalen $\mathbb{R}$-Vektorraums abgeschlossen ist und somit alle seine Häufungspunkte enthält. □

Im Folgenden sei nun $\langle\ ,\ \rangle\colon V \times V \to \mathbb{R}$ ein Skalarprodukt, d.h. eine positiv definite und symmetrische Bilinearform. Wenn $\underline{v} = (v_1, \ldots, v_n)$ eine Orthonormalbasis bzgl. $\langle\ ,\ \rangle$ ist, so ist die Abbildung

$$\varphi_{\underline{v}}\colon \mathbb{R}^n \to V, \qquad e_i \mapsto v_i,$$

eine Isometrie, wobei $\mathbb{R}^n$ hier mit dem Standardskalarprodukt versehen und e_i der i-te Standardbasisvektor ist. Diese Isometrie erlaubt es uns, den Begriff der Lebesgue-Messbarkeit auf Teilmengen von V auszudehnen: Wir nennen $X \subset V$ *Lebesgue-messbar*, wenn $\varphi_{\underline{v}}^{-1}(X) \subset \mathbb{R}^n$ Lebesgue-messbar ist. Ist $X \subset V$ Lebesgue-messbar, so haben wir also einen Volumenbegriff

$$\mathrm{vol}_{\underline{v}}(X) := \mathrm{vol}\left(\varphi_{\underline{v}}^{-1}(X)\right),$$

wobei vol das Lebesgue-Maß auf $\mathbb{R}^n$ ist. Das Volumen $\mathrm{vol}_{\underline{v}}$ hängt a priori von der Wahl der Orthonormalbasis $\underline{v} = (v_1, \ldots, v_n)$ ab. Um die Unabhängigkeit von der Wahl der Orthonormalbasis zu zeigen, erinnern wir an die Transformationsformel:

Erinnerung. (Spezialfall des Transformationssatzes und interessante Folgerungen.)
Sei $Y \subset \mathbb{R}^n$ und $A \in \mathrm{GL}_n(\mathbb{R})$, so ist Y genau dann Lebesgue-messbar, wenn $A(Y)$ Lebesgue-messbar ist. In diesem Fall gilt

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

Mit $A = c \cdot I_n$ *und* $c > 0$ *gilt also, dass* $\mathrm{vol}(cY) = c^n \cdot \mathrm{vol}(Y)$*, wobei* $cY := A(Y)$*. Insbesondere ist* $\mathbb{R}_{>0} \to \mathbb{R}$*,* $c \mapsto \mathrm{vol}(cY)$ *stetig und falls* $\mathrm{vol}(Y) > 0$*, so gilt*

$$\lim_{c \searrow 0} \mathrm{vol}(cY) = 0 \qquad \textit{sowie} \qquad \lim_{c \to \infty} \mathrm{vol}(cY) = \infty.$$

In diesem Fall impliziert der Zwischenwertsatz, dass es für alle $x_0 > 0$ *ein* $c_0 > 0$ *mit* $\mathrm{vol}(c_0 Y) = x_0$ *gibt.*

Ist nun $\underline{w} = (w_1, \ldots, w_n)$ beliebige Basis von V, so können wir wie üblich

$$w_j = \sum_{i=1}^{n} a_{ij} v_i \qquad \text{mit } a_{ij} \in \mathbb{R}$$

schreiben. Bezeichne mit $A \in \mathrm{GL}_n(\mathbb{R})$ die Matrix mit den Einträgen a_{ij}. Wir haben ein kommutatives Diagramm

$$\begin{array}{ccc} e_j & \mathbb{R}^n \xrightarrow{\varphi_{\underline{v}}} V & v_j \\ \big\downarrow & \big\downarrow A \quad \searrow^{\varphi_{\underline{w}}} \quad \big\downarrow A & \big\downarrow \\ \sum_{i=1}^n a_{ij} e_i & \mathbb{R}^n \xrightarrow{\varphi_{\underline{v}}} V & w_j = \sum_{i=1}^n a_{ij} v_i \end{array}$$

Das Diagramm zeigt $A \circ \varphi_{\underline{v}} = \varphi_{\underline{w}} = \varphi_{\underline{v}} \circ A$. Nach dem Transformationssatz ist $\varphi_{\underline{v}}^{-1}(X)$ genau dann Lebesgue-messbar, wenn

$$\varphi_{\underline{w}}^{-1}(X) = (\varphi_{\underline{v}} \circ A)^{-1}(X) = A^{-1}(\varphi_{\underline{v}}^{-1}(X))$$

Lebesgue-messbar ist. In diesem Falle gilt dann auch

$$\mathrm{vol}\left(\varphi_{\underline{w}}^{-1}(X)\right) = |\det(A)|^{-1} \cdot \mathrm{vol}\left(\varphi_{\underline{v}}^{-1}(X)\right).$$

Ist nun $\underline{w}$ selbst eine Orthonormalbasis so bildet A eine Orthonormalbasis auf eine weitere ab, woraus $A \in O(n)$ folgt. Insbesondere gilt hier $|\det(A)| = 1$. Damit erhalten wir für ein messbares $X \subset V$:

$$\mathrm{vol}_{\underline{w}}(X) = |\det(A)|^{-1} \cdot \mathrm{vol}_{\underline{v}}(X) = \mathrm{vol}_{\underline{v}}(X).$$

Unser Volumensbegriff ist damit wie gewünscht unabhängig von der Wahl der Orthonormalbasis. Wir schreiben im Folgenden also schlicht $\mathrm{vol}(X)$ für messbare Teilmengen $X \subset V$.

Definition 5.4. Wenn $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ ein vollständiges Gitter ist, dann definiere das *Volumen* von Λ als das Volumen der Grundmasche bzgl. $\underline{v} = (v_1, \ldots, v_n)$, also $\mathrm{vol}(\Lambda) := \mathrm{vol}(M_{\underline{v}})$.

Auch hier müssen wir uns Gedanken über die Wohldefiniertheit machen. Wählt man eine weitere $\mathbb{Z}$-Basis $\underline{w} = (w_1, \ldots, w_n)$ von Λ, so kann man wieder $w_j = \sum_{i=1}^n a_{ij} v_i$ schreiben, wobei $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$. Als ganzzahlig invertierbare Matrix gilt wieder $|\det(A)| = 1$ und somit folgt die Unabhängigkeit von der Wahl der Basis erneut wie oben durch die Transformationsformel.

Bemerkung. Eigentlich haben wir in Definition 5.4 das *Ko*volumen eines Gitters Λ definiert, d.h. das Volumen des Quotienten V/Λ – in Bemerkung 5.2 haben wir ja gesehen, dass $M_{\underline{v}}$ ein Repräsentantensystem von V/Λ ist.

Glücklicherweise ist es sehr leicht, das Volumen eines Gitters zu berechnen:

Lemma 5.5. *Es seien $\underline{v} = (v_1, \ldots, v_n)$ und $\underline{w} = (w_1, \ldots, w_n)$ Basen von V. Seien $\Lambda_{\underline{v}}$ bzw. $\Lambda_{\underline{w}}$ die durch $\underline{v}$ bzw. $\underline{w}$ erzeugten Gitter. Ferner sei $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{R})$ die Basiswechselmatrix von $\underline{w}$ auf $\underline{v}$, das heißt*

$$w_j = \sum_{i=1}^{n} a_{ij} v_i \qquad \text{für alle} \quad j = 1, \ldots, n.$$

Dann gilt:

(1) Es ist $\mathrm{vol}(\Lambda_{\underline{w}}) = |\det(A)| \cdot \mathrm{vol}(\Lambda_{\underline{v}})$.

(2) Das Volumen von Gittern lässt sich wie folgt berechnen:

$$\mathrm{vol}(\Lambda_{\underline{w}}) = \sqrt{\det\left((\langle w_i, w_j\rangle)_{i,j}\right)}.$$

Beweis. (1) Bezeichnen $M_{\underline{v}}$ bzw. $M_{\underline{w}}$ die Grundmaschen von $\Lambda_{\underline{v}}$ bzw. $\Lambda_{\underline{w}}$, dann gilt $M_{\underline{w}} = A \cdot M_{\underline{v}}$ und damit folgt aus der Transformationsformel sofort

$$\mathrm{vol}(\Lambda_{\underline{w}}) = \mathrm{vol}(M_{\underline{w}}) = \mathrm{vol}(A \cdot M_{\underline{v}}) = |\det(A)| \cdot \mathrm{vol}(M_{\underline{v}}) = |\det(A)| \cdot \mathrm{vol}(\Lambda_{\underline{v}}).$$

(2) Ist $\underline{v} = (v_1, \ldots, v_n)$ eine Orthonormalbasis von $(V, \langle\ ,\ \rangle)$, so gilt

$$\mathrm{vol}(\Lambda_{\underline{v}}) = \mathrm{vol}(M_{\underline{v}}) = \mathrm{vol}(\varphi_{\underline{v}}^{-1}(M_{\underline{v}})) = 1, \tag{5.1}$$

da $\varphi_{\underline{v}}^{-1}(M_{\underline{v}}) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \le x_i < 1\}$ als Würfel im $\mathbb{R}^n$ der Seitenlänge 1 das Volumen 1 hat. Des Weiteren gilt für alle $1 \le i, j \le n$:

$$\langle w_i, w_j\rangle = \sum_{k,\ell=1}^{n} a_{ki} a_{\ell j} \underbrace{\langle v_k, v_\ell\rangle}_{=\delta_{k\ell}} = \sum_{k=1}^{n} a_{ki} a_{kj}.$$

Also gilt

$$(\langle w_i, w_j\rangle)_{i,j} = A^t \cdot A$$

und damit insbesondere auch

$$|\det(A)| = \sqrt{\det\left((\langle w_i, w_j\rangle)_{i,j}\right)}. \tag{5.2}$$

(Das sollte Sie an Bemerkung 4.11 erinnern.) Schließlich erhalten wir

$$\mathrm{vol}(\Lambda_{\underline{w}}) \overset{(1)}{=} |\det(A)| \cdot \mathrm{vol}(M_{\underline{v}}) \overset{(5.1)}{=} |\det(A)| \overset{(5.2)}{=} \sqrt{\det\left((\langle w_i, w_j\rangle)_{i,j}\right)}.$$

□

Bemerkung 5.6. Sei $(w_1, \ldots, w_n) \subset V$ ein $\mathbb{Z}$-linear unabhängiges System. Dann folgt *nicht*, dass $\mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_n$ ein Gitter ist (zum Beispiel ist $\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$ kein Gitter in $\mathbb{R}$)! Allerdings ist $\Lambda = \mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_n$ genau dann ein vollständiges Gitter in V, wenn

$$\det\left((\langle w_i, w_j\rangle)_{i,j}\right) \neq 0.$$

Gilt nämlich $x_1 w_1 + \ldots + x_n w_n = 0$ mit $x_1, \ldots, x_n \in \mathbb{R}$, nicht alle gleich 0, so folgt für jedes $j = 1, \ldots, n$:

$$x_1\langle w_1, w_j\rangle + \ldots + x_n\langle w_n, w_j\rangle = 0,$$

d.h. die Zeilen der Matrix $(\langle w_i, w_j \rangle)_{i,j}$ sind linear abhängig. Wenn umgekehrt Λ vollständig ist, so gibt es eine Basis $(v_1, \ldots, v_n)$ von V, sodass

$$\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n.$$

Da $(v_1, \ldots, v_n)$ sogar eine Basis von V ist, muss $(w_1, \ldots, w_n)$ auch eine Basis von V sein[1]. Man entnimmt dem Beweis von Lemma 5.5 (2) nun die Aussage $\det((\langle w_i, w_j \rangle)_{i,j}) \neq 0$.

Proposition 5.7. *Ist $\Lambda \subset V$ ein vollständiges Gitter und $\Lambda' \subset \Lambda$ ein Untergitter vom endlichen Index, so ist Λ' vollständig und es gilt*

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

Beweis. Da Λ' endlichen Index in Λ hat, folgt mit Proposition 2.19, dass Λ' denselben Rang wie Λ hat, nämlich $n = \dim(V)$. Nach dem Elementarteilersatz 2.17 gibt es eine $\mathbb{Z}$-Basis $(v_1, \ldots, v_n)$ von Λ und Zahlen $d_1, \ldots, d_n \in \mathbb{Z}_{>0}$, sodass $(d_1 v_1, \ldots, d_n v_n)$ eine $\mathbb{Z}$-Basis von Λ' ist. Insbesondere ist Λ' ebenfalls vollständig. Nach Proposition 2.19 folgt dann

$$|\Lambda/\Lambda'| = d_1 \cdot \ldots \cdot d_n = \det(A),$$

wobei $A = \mathrm{diag}(d_1, \ldots, d_n)$ die Basiswechselmatrix von $(v_1, \ldots, v_n)$ auf $(d_1 v_1, \ldots, d_n v_n)$ ist. Mit Lemma 5.5 (1) folgt nun

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

□

Bevor wir zum Hauptergebnis dieses Abschnitts kommen, erinnern wir an die folgenden Definitionen.

Definition 5.8. Sei $X \subset V$ eine Teilmenge.

(1) Man nennt X *konvex*, wenn für alle $x, y \in X$ gilt, dass die Verbindungsstrecke $\{tx + (1-t)y \mid t \in [0,1]\}$ in X enthalten ist.

(2) Man nennt X *zentralsymmetrisch*, wenn für alle $x \in X$ gilt, dass $-x \in X$.

Satz 5.9 (Gitterpunktsatz von Minkowski)**.** *Sei $\Lambda \subset V$ ein vollständiges Gitter und $X \subset V$ konvex und zentralsymmetrisch. Gilt $\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(\Lambda)$, so enthält X einen von 0 verschiedenen Gitterpunkt von Λ.*

Beweis. Wir zeigen zunächst, dass es genügt, die Existenz von Gitterpunkten $\lambda_1 \neq \lambda_2$ mit

$$\left(\lambda_1 + \frac{1}{2}X\right) \cap \left(\lambda_2 + \frac{1}{2}X\right) \neq \emptyset \tag{5.3}$$

zu beweisen. Sind nämlich $x_1, x_2 \in X$ mit $\lambda_1 + \frac{1}{2}x_1 = \lambda_2 + \frac{1}{2}x_2$ gegeben, so folgt

$$\underbrace{\lambda_1 - \lambda_2}_{\in \Lambda \setminus \{0\}} = \frac{1}{2}(x_2 - x_1).$$

[1] Insbesondere ist eine $\mathbb{Z}$-Basis eines vollständigen Gitters auch immer eine Vektorraumbasis.

Nun beobachten wir, dass $\frac{1}{2}(x_2 - x_1)$ der Mittelpunkt der Strecke zwischen x_2 und $-x_1$ ist. Aus der Zentralsymmetrie von X folgt $-x_1 \in X$ und aus der Konvexität schließlich $\lambda_1 - \lambda_2 = \frac{1}{2}(x_2 - x_1) \in X$.

Wir weisen also (5.3) nach. Für einen Widerspruch nehmen wir an, dass die Mengen $\lambda + \frac{1}{2}X$ für $\lambda \in \Lambda$ paarweise disjunkt sind. Sei M die Grundmasche von Λ. Aus unserer Annahme folgt

$$\operatorname{vol}(\Lambda) \overset{\text{Def.}}{=} \operatorname{vol}(M) \geq \sum_{\lambda \in \Lambda} \operatorname{vol}\left(M \cap \left(\lambda + \frac{1}{2}X\right)\right). \tag{5.4}$$

Da Volumina translationsinvariant sind, folgt für alle $\lambda \in \Lambda$ durch Translation um $-\lambda$:

$$\operatorname{vol}\left(M \cap \left(\lambda + \frac{1}{2}X\right)\right) = \operatorname{vol}\left((M - \lambda) \cap \frac{1}{2}X\right). \tag{5.5}$$

Da die Mengen $M - \lambda$ ganz V überdecken, überdecken sie auch $\frac{1}{2}X \subset V$. Wir erhalten nun den gewünschten Widerspruch durch

$$\operatorname{vol}(\Lambda) = \operatorname{vol}(M) \overset{(5.4),\,(5.5)}{\geq} \sum_{\lambda \in \Lambda} \operatorname{vol}\left((M - \lambda) \cap \frac{1}{2}X\right) = \operatorname{vol}\left(\frac{1}{2}X\right) = \left(\frac{1}{2}\right)^n \cdot \operatorname{vol}(X).$$

□

Bemerkung 5.10. Die Schranke im Gitterpunktsatz ist im Allgemeinen optimal. Ist X jedoch kompakt, so kann "$>$" zu "$\geq$" abgeschwächt werden, vgl. Aufgabe 5.1.3.

Wir möchten den Gitterpunktsatz auf die folgende zahlentheoretische Situation anwenden: Sei K ein Zahlkörper vom Grad n. Aus Abschnitt 4.1 wissen wir, dass

$$n = r + 2s,$$

wobei r die Anzahl der reellen Einbettungen und s die Anzahl der Paare echt komplexer Einbettungen von K ist. Seien nun

- $\rho_1, \ldots, \rho_r$ die reellen Einbettungen,
- $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$ die echt komplexen Einbettungen

von K. Wir bekommen dann eine Abbildung

$$\begin{aligned} j\colon K &\hookrightarrow K_{\mathbb{R}} := \mathbb{R}^r \times \mathbb{C}^s, \\ \alpha &\mapsto (\rho_1(\alpha), \ldots, \rho_r(\alpha), \sigma_1(\alpha), \ldots, \sigma_s(\alpha)). \end{aligned}$$

Um Volumina von Gittern in $K_{\mathbb{R}}$ studieren zu können, brauchen wir noch ein Skalarprodukt auf $K_{\mathbb{R}}$. Wir schreiben $(x', x'') \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$, wobei $x' = (x'_1, \ldots, x'_r) \in \mathbb{R}^r$ und $x'' = (x''_1, \ldots, x''_s) \in \mathbb{C}^s$ und definieren

$$\begin{aligned} &\langle\ ,\ \rangle\colon K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}, \\ &\langle (x', x''), (y', y'') \rangle := \left(\sum_{i=1}^{r} x'_i y'_i\right) + \left(\sum_{j=1}^{s} \operatorname{tr}_{\mathbb{C}/\mathbb{R}}(x''_j \overline{y''_j})\right). \end{aligned} \tag{5.6}$$

Beachtet man, dass $\operatorname{tr}_{\mathbb{C}/\mathbb{R}}\colon \mathbb{C} \to \mathbb{R}$ durch $z \mapsto z + \overline{z}$ gegeben ist, haben wir:

Bemerkung 5.11. Es gilt für alle $(x', x''), (y', y'') \in K_{\mathbb{R}}$:

$$\langle (x', x''), (y', y'') \rangle = \left(\sum_{i=1}^{r} x_i' y_i' \right) + 2 \cdot \left(\sum_{j=1}^{s} \left(\operatorname{Re}(x_j'') \operatorname{Re}(y_j'') + \operatorname{Im}(x_j'') \operatorname{Im}(y_j'') \right) \right).$$

Identifiziert man $\mathbb{C}$ auf die übliche Art mit $\mathbb{R}^2$, so entspricht das Skalarprodukt (5.6) auf $K_{\mathbb{R}}$ also bis auf den Faktor 2 in den komplexen Variablen dem Standardskalarprodukt auf $\mathbb{R}^r \times \mathbb{C}^s$. Das Volumen einer Menge $X \subset K_{\mathbb{R}}$ bzgl. (5.6) unterscheidet sich somit um den Faktor 2^s vom Volumen von X bzgl. des Standardskalarprodukts auf $\mathbb{R}^r \times \mathbb{C}^s$, in Formeln (mit hoffentlich selbsterklärender Notation):

$$\operatorname{vol}(X) = 2^s \cdot \operatorname{vol}_{\text{Standard}}(X).$$

Im Folgenden werden wir mit "vol(X)" stets das Volumen von $X \subset K_{\mathbb{R}}$ bzgl. des Skalarprodukts (5.6) meinen. Um vol(X) jedoch explizit zu berechnen, ist es aber oft einfacher, das Volumen von X bzgl. des Standardskalarprodukts zu berechnen und das Ergebnis mit 2^s zu multiplizieren.

Der Grund, wieso wir nicht einfach das Standardskalarprodukt auf $K_{\mathbb{R}}$ betrachten, wird in den folgenden Resultaten deutlich.

Bemerkung 5.12. Es seien $\alpha_1, \alpha_2 \in K$ und $w_1 := j(\alpha_1)$, $w_2 = j(\alpha_2) \in K_{\mathbb{R}}$. Dann vereinfacht sich das Skalarprodukt von w_1, w_2 wie folgt:

$$\begin{aligned}
\langle w_1, w_2 \rangle &= \sum_{i=1}^{r} \rho_i(\alpha_1)\rho_i(\alpha_2) + \operatorname{tr}_{\mathbb{C}/\mathbb{R}} \left(\sum_{j=1}^{s} \sigma_j(\alpha_1)\overline{\sigma_j(\alpha_2)} \right) \\
&= \sum_{i=1}^{r} \rho_i(\alpha_1)\rho_i(\alpha_2) + \sum_{j=1}^{s} \sigma_j(\alpha_1)\overline{\sigma_j(\alpha_2)} + \sum_{j=1}^{s} \overline{\sigma_j(\alpha_1)}\sigma_j(\alpha_2) \\
&= \sum_{k=1}^{n} \tau_k(\alpha_1)\overline{\tau_k(\alpha_2)},
\end{aligned}$$

wobei $\tau_1, \ldots, \tau_n$ *alle* verschiedenen komplexen Einbettungen von K sind.

Auf welches vollständige Gitter in $K_{\mathbb{R}}$ wollen wir nun den Gitterpunktsatz anwenden? Erinnern Sie sich außerdem daran, dass die Diskriminante ein algebraischer Volumenbegriff ist (Bemerkung 4.11)?

Proposition 5.13. *Sei K ein Zahlkörper und $j\colon K \hookrightarrow K_{\mathbb{R}}$ wie oben. Dann ist $j(\mathcal{O}_K)$ ein vollständiges Gitter in $K_{\mathbb{R}}$ und es gilt* $\operatorname{vol}(\mathcal{O}_K) := \operatorname{vol}(j(\mathcal{O}_K)) = \sqrt{|d_K|}$.

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine Ganzheitsbasis von $\mathcal{O}_K$. Wir schreiben $w_i := j(\alpha_i) \in K_{\mathbb{R}}$. Dann gilt $j(\mathcal{O}_K) = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$. Nach Bemerkung 5.12 gilt für $1 \leq i, j \leq n$:

$$\langle w_i, w_j \rangle = \sum_{k=1}^{n} \tau_k(\alpha_i)\overline{\tau_k(\alpha_j)}, \tag{5.7}$$

wobei $\tau_1, \ldots, \tau_n$ die verschiedenen komplexen Einbettungen von K sind. Bezeichnet $A \in \operatorname{Mat}(n \times n, \mathbb{C})$ die Matrix, deren (k, ℓ)-ter Eintrag $\tau_k(\alpha_\ell)$ ist, so zeigt Gleichung (5.7) also

$$(\langle w_i, w_j \rangle)_{i,j} = A^t \cdot \overline{A},$$

woraus

$$\sqrt{\det\left((\langle w_i, w_j\rangle)_{i,j}\right)} = |\det(A)| \tag{5.8}$$

folgt. Andererseits ist $A^t \cdot A$ die Matrix mit dem (i,j)-ten Eintrag

$$\sum_{k=1}^{n} \tau_k(\alpha_i)\tau_k(\alpha_j) \overset{\text{Lemma 4.7}}{=} \operatorname{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j).$$

Man erhält also

$$|\det(A)| = \det\left((\operatorname{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j}\right) = \sqrt{|d_K|}. \tag{5.9}$$

Zusammen liefern nun (5.8) und (5.9):

$$\sqrt{\det\left((\langle w_i, w_j\rangle)_{i,j}\right)} = \sqrt{|d_K|} \overset{\text{Kor. 4.19}}{\neq} 0.$$

Aus Bemerkung 5.6 folgt nun, dass $j(\mathcal{O}_K)$ ein vollständiges Gitter ist, und schließlich erhalten wir mit Lemma 5.5 (2) die gewünschte Aussage $\operatorname{vol}(\mathcal{O}_K) = \sqrt{|d_K|}$. □

Weitere Beispiele von vollständigen Gittern in $K_\mathbb{R}$ sind durch gebrochene Ideale gegeben.

Korollar 5.14. *Jedes gebrochene Ideal $\mathfrak{a} \neq (0)$ von K ist vermöge $j\colon K \hookrightarrow K_\mathbb{R}$ ein vollständiges Gitter mit Volumen*

$$\operatorname{vol}(\mathfrak{a}) := \operatorname{vol}(j(\mathfrak{a})) = \sqrt{|d_K|} \cdot N(\mathfrak{a}).$$

Beweis. Sie finden das mit entsprechendem Hinweis in Aufgabe 5.1.4. □

5.1.1 Übungen

Aufgabe 5.1.1. Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Ergänzen Sie die folgenden Details im Beweis von Satz 5.3 (1):

(1) Ist $\Lambda \subset V$ eine diskrete Untergruppe, so ist Λ abgeschlossen in V.

Anleitung: Sei $||\cdot||$ irgendeine Norm auf V. Da Λ diskret ist, gibt es ein $\varepsilon > 0$ mit $B_\varepsilon(0) \cap \Lambda = \{0\}$, wobei $B_\varepsilon(0)$ der ε-Ball um 0 bzgl. $||\cdot||$ ist. Folgern Sie für $B := B_{\varepsilon/2}(0)$:

$$B - B := \{x - y \mid x, y \in B\} \subset B_\varepsilon(0).$$

Sei nun $v \in V \setminus \Lambda$ und $v + B := \{v + y \mid x \in B\}$. Wenn nun $(v + B) \cap \Lambda = \emptyset$, sind Sie fertig – warum?
Andernfalls gibt es ein $\lambda \in (v + B) \cap \Lambda$. Zeigen Sie dann $(v + B) \cap \Lambda = \{\lambda\}$ und folgern Sie daraus die Behauptung.

Aufgabe 5.1.2. Geben Sie ein Beispiel einer kompakten Menge $K \subset \mathbb{R}$ und einer diskreten Menge $Y \subset \mathbb{R}$ an, sodass $K \cap Y$ nicht endlich ist. (Begründung!)

Aufgabe 5.1.3. Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum, $\Lambda \subset V$ ein vollständiges Gitter und $X \subset V$. Zeigen Sie:

(1) Ist X kompakt, zentralsymmetrisch und konvex mit $\mathrm{vol}(X) = 2^n \cdot \mathrm{vol}(\Lambda)$, so enthält X einen Gitterpunkt $\neq 0$ von Λ.
Hinweis: Betrachten Sie $X_a := aX$ für $a > 1$.

(2) Die Schranke im Gitterpunktsatz kann nicht verbessert werden: Geben Sie für jedes n ein vollständiges Gitter $\Lambda \subset \mathbb{R}^n$ und eine konvexe, zentralsymmetrische Menge X mit $\mathrm{vol}(X) = 2^n \cdot \mathrm{vol}(\Lambda)$ an, sodass X keinen von Null verschiedenen Gitterpunkt enthält.

Aufgabe 5.1.4. Beweisen Sie Korollar 5.14.
Hinweis: Bemerkung 4.32 und Proposition 5.7 könnten helfen.

Aufgabe 5.1.5 (Vier-Quadrate-Satz von Lagrange)**.** Sei p eine Primzahl.

(1) Zeigen Sie, dass ganze Zahlen u, v mit $u^2 + v^2 + 1 \equiv 0 \pmod{p}$ existieren.
Hinweis: Für $p = 2$ ist die Aussage klar. Für p ungerade zählen Sie jeweils die Elemente der Mengen

$$S = \{u^2 \pmod{p} \mid u \in \mathbb{Z}\} \qquad \text{und} \qquad S' = \{-1 - v^2 \pmod{p} \mid v \in \mathbb{Z}\}.$$

(2) Für $u, v \in \mathbb{Z}$ mit $u^2 + v^2 + 1 \equiv 0 \pmod{p}$ definieren wir

$$\Lambda_{u,v} := \{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv ua + vb \pmod{p} \quad \text{und} \quad d \equiv ub - va \pmod{p}\}.$$

Zeigen Sie, dass $\Lambda_{u,v}$ ein vollständiges Gitter in $\mathbb{R}^4$ mit Volumen $\leq p^2$ ist.

(3) Zeigen Sie, dass p als Summe von vier Quadratzahlen geschrieben werden kann.
Hinweis: Ein (offener) Ball mit Radius R im $\mathbb{R}^4$ hat das Volumen $\frac{\pi^2}{2} \cdot R^4$. Für $R = \sqrt{2p}$ lässt sich also der Gitterpunktsatz 5.9 anwenden.

(4) Zeigen Sie, dass jedes $n \in \mathbb{Z}_{>0}$ als Summe von vier Quadratzahlen geschrieben werden kann.
Hinweis: Nutzen Sie, dass die euklidische Norm auf $\mathbb{R}^4$ der (multiplikativen!) Norm der Quaternionen entspricht, das heißt für $(a, b, c, d) \in \mathbb{R}^4$ gilt

$$||(a, b, c, d)||^2 = |a + bi + cj + dk|^2.$$

Erläuterung: Die Quaternionen $\mathbb{H}$ bilden einen 4-dimensionalen $\mathbb{R}$-Vektorraum mit Basis $\{1, i, j, k\}$, der vermöge der durch die folgenden Rechenregeln definierte Multiplikation

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji, \quad ij = k, \quad i, j, k \text{ kommutieren mit reellen Zahlen}$$

zu einer $\mathbb{R}$-Algebra wird. Man kann zeigen, dass $\mathbb{H}$ ein Schiefkörper ist (der wegen der nicht gegebenen Kommutativität der Multiplikation kein Körper ist).

5.2 Endlichkeit der Klassenzahl

Wir verwenden weiterhin die Notation aus dem vorherigen Abschnitt: K ist ein Zahlkörper vom Grad $n = r + 2s$, wobei r die Anzahl an reellen Einbettungen und s die Anzahl der Paare komplexer Einbettungen von K ist.
Wir haben in Abschnitt 3.3 gesehen, dass die Menge der gebrochenen Ideale $\neq (0)$ modulo der Untergruppe der gebrochenen Hauptideale von $\mathcal{O}_K$ bezüglich der Multiplikation eine abelsche Gruppe Cl_K bildet. Wir werden in diesem Abschnitt sehen, dass die Ordnung $h_K := |\,\mathrm{Cl}_K\,|$ dieser Gruppe, die *Klassenzahl*, sogar endlich ist. Der Beweis dieses tiefen Resultats besteht aus zwei Schritten:

(1) Beweise, dass jede Idealklasse von Cl_K durch ein (ganzes) Ideal von $\mathcal{O}_K$ mit Norm $\leq M_K$ repräsentiert ist. Hierbei ist M_K die *Minkowski-Schranke*, die nur von K abhängt.

(2) Beweise, dass es nur endlich viele ganze Ideale mit beschränkter Norm gibt.

Wir beginnen mit dem ersten (und dem kompliziertesten) Schritt. Dieser wird eine Konsequenz der folgenden Proposition sein.

Proposition 5.15. *Sei $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Dann gibt es $\alpha \in \mathfrak{a} \setminus \{0\}$ mit*

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

Hierbei ist $M_K := \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|d_K|}$ die Minkowski-Schranke *von K.*

Beweis. Wir erinnern an die Abbildung $j\colon K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$, die durch die r reellen Einbettungen und die Wahl von s paarweise nicht komplex konjugierten Einbettungen gegeben ist. Nach Korollar 5.14 ist $j(\mathfrak{a})$ ein vollständiges Gitter in $K_{\mathbb{R}}$ mit Volumen $\mathrm{vol}(\mathfrak{a}) = \sqrt{|d_K|} \cdot N(\mathfrak{a})$.

Für $c > 0$ betrachten wir die kompakte und zentralsymmetrische Menge

$$X_c := X_c^{r,s} := \left\{ (x', x'') \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum_{i=1}^{r} |x_i'| + \sum_{j=1}^{s} 2|x_j''| \leq c \right\}.$$

Wir weisen noch nach, dass X_c konvex ist. Sei dazu

$$||x||_1 := \sum_{i=1}^{r} |x_i'| + \sum_{j=1}^{s} 2|x_j''|, \qquad x = (x', x'') \in K_{\mathbb{R}}$$

die 1-Norm auf $K_{\mathbb{R}}$. Dann gilt für $t \in [0,1]$ und $x, y \in X_c$:

$$||(1-t)x + ty||_1 \leq (1-t)||x||_1 + ||t||_1 \leq (1-t)c + tc = c,$$

d.h. $(1-t)x + ty \in X_c$, was die gewünschte Konvexität von X_c beweist.

Ist $\alpha \in K \setminus \{0\}$, sodass $j(\alpha) \in X_c$, so erhält man die folgende Abschätzung mit Hilfe der AM-GM-Ungleichung:

$$\begin{aligned} |N_{K/\mathbb{Q}}(\alpha)| = \left| \prod_{\tau\colon K \hookrightarrow \mathbb{C}} \tau(\alpha) \right| &= \left(\left(\prod_{\tau\colon K \hookrightarrow \mathbb{C}} |\tau(\alpha)| \right)^{1/n} \right)^n \\ &\leq \left(\frac{1}{n} \sum_{\tau} |\tau(\alpha)| \right)^n \leq \left(\frac{c}{n} \right)^n. \end{aligned} \tag{5.10}$$

Das Ziel ist es nun, die Formel

$$\mathrm{vol}(X_c) = 2^r \cdot \pi^s \cdot \frac{c^n}{n!} \tag{5.11}$$

zu beweisen. Wir nehmen zunächst an, dass die Gültigkeit von (5.11) bewiesen ist und folgern daraus die Aussage der Proposition. Wähle dafür $c \in \mathbb{R}_{>0}$ so, dass

$$\mathrm{vol}(X_c) = 2^n \cdot \mathrm{vol}(\mathfrak{a}) = 2^n \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a}).$$

Dann folgt mit der Kompaktheit von X_c und Bemerkung 5.10, dass X_c einen Gitterpunkt $j(\alpha) \in j(\mathfrak{a}) \setminus \{0\}$ enthält. Nach (5.10) gilt für die Norm von α die Abschätzung

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{c}{n}\right)^n = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a}),$$

wie behauptet. (Unsere Wahl von c impliziert, dass $c^n = n! \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a})$.)

Wir müssen also nur noch (5.11) verifizieren. Dafür setzen wir

$$V^{r,s}(c) := \operatorname{vol}_{\text{Standard}}(X_c^{r,s}) \text{ und } V^{0,0}(c) := 1.$$

Dann gilt also im Hinblick auf Bemerkung 5.11:

$$\operatorname{vol}(X_c^{r,s}) = 2^s \cdot V^{r,s}(c).$$

Demnach können wir äquivalenterweise

$$V^{r,s}(c) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{c^n}{n!} \tag{5.12}$$

nachweisen. Mit der Transformationsformel des Lebesgue-Integrals folgt

$$V^{r,s}(c) = c^{r+2s} \cdot V^{r,s}(1).$$

Da ja $n = r + 2s$ gilt, genügt es also, (5.12) für $c = 1$ zu beweisen. Für $r > 0$ schreiben wir $X_1^{r,s}$ zunächst wie folgt um:

$$\begin{aligned} X_1^{r,s} &= \left\{ (x', x'') \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum_{i=1}^{r} |x_i'| + \sum_{j=1}^{s} 2|x_j''| \leq 1 \right\} \\ &= \left\{ (x', x'') \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum_{i=1}^{r-1} |x_i'| + \sum_{j=1}^{s} 2|x_j''| \leq 1 - |x_r'| \right\}. \end{aligned}$$

Für $(x', x'') \in X_1^{r,s}$ gilt also $x_r' \in [-1, 1]$. Ist umgekehrt $y \in [-1, 1]$, so gibt es sicherlich $x_1', \ldots, x_{r-1}' \in \mathbb{R}$ und $x'' \in \mathbb{C}^s$, sodass $((x_1', \ldots, x_{r-1}', y), x'') \in X_1^{r,s}$. Damit erhalten wir

$$V^{r,s}(1) = 2 \cdot \int_0^1 V^{r-1,s}(1-t)\,\mathrm{d}t = 2 \cdot V^{r-1,s}(1) \cdot \int_0^1 (1-t)^{r-1+2s}\,\mathrm{d}t = \frac{2}{r+2s} \cdot V^{r-1,s}(1).$$

Induktiv erhalten wir somit für $r > 0$ die Gleichheit

$$V^{r,s}(1) = \frac{2^r}{(r+2s) \cdot (r-1+2s) \cdot \ldots \cdot (2s+1)} \cdot V^{0,s}(1). \tag{5.13}$$

Wir berechnen also noch $V^{0,s}(1)$ für $s > 0$. Ähnlich wie oben bemerken wir

$$X_1^{0,s} = \left\{ x'' \in \mathbb{C}^s \;\middle|\; \sum_{j=1}^{s} 2|x_j''| \leq 1 \right\} = \left\{ x'' \in \mathbb{C}^s \;\middle|\; 2\sum_{j=1}^{s-1} |x_j''| \leq 1 - 2|x_s''| \right\},$$

Also gilt

$$x_s'' \in \overline{B_{1/2}(0)} \iff \text{ es gibt } x_1'', \ldots, x_{s-1}'' \in \mathbb{C} \text{ mit } (x_1'', \ldots, x_s'') \in X_1^{0,s},$$

wobei $\overline{B_{1/2}(0)} \subset \mathbb{C}$ den abgeschlossenen Kreis mit Mittelpunkt 0 und Radius 1/2 bezeichnet.

Mit diesen Überlegungen folgt unter Verwendung von Polarkoordinaten $x = R\cos\varphi$, $y = R\sin\varphi$:

$$\begin{aligned} V^{0,s}(1) &= \iint_{\overline{B_{1/2}(0)}} V^{0,s-1}\left(1 - 2\sqrt{x^2+y^2}\right) \mathrm{d}x\,\mathrm{d}y \\ &= V^{0,s-1}(1) \cdot \int_0^{\frac{1}{2}} \int_0^{2\pi} (1-2R)^{2(s-1)} \cdot R\,\mathrm{d}\varphi\,\mathrm{d}R \\ &\overset{u:=1-2R}{=} 2\pi \cdot V^{0,s-1}(1) \cdot \int_0^1 \frac{1}{2} u^{2(s-1)} \cdot \frac{1}{2}(1-u)\,\mathrm{d}u \\ &= \frac{\pi}{2} \cdot V^{0,s-1}(1) \cdot \left(\frac{1}{2s-1} - \frac{1}{2s}\right) = \frac{\pi}{2} \cdot V^{0,s-1}(1) \cdot \frac{1}{(2s-1)2s}. \end{aligned}$$

Somit erhalten wir induktiv

$$V^{0,s}(1) = V^{0,0}(1) \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{(2s)!} = \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{(2s)!}. \tag{5.14}$$

Aus den Gleichungen (5.13) und (5.14) erhalten wir schließlich

$$V^{r,s}(1) = \frac{2^r}{(r+2s)\cdot(r-1+2s)\cdot\ldots\cdot(2s+1)} \cdot V^{0,s}(1) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{(r+2s)!} = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{n!}.$$

Das beweist (5.12) und damit auch die Proposition. □

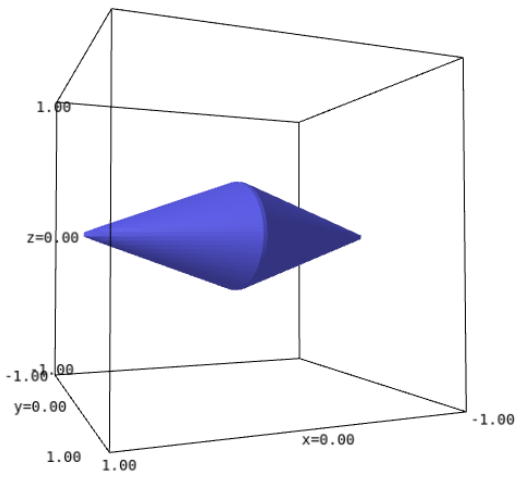


Abbildung 5.3: Ein Bild der Menge $X_1^{1,1} \subset \mathbb{R} \times \mathbb{C} = \mathbb{R}^3$.

Als Folgerung erhalten wir die Aussage des ersten Schrittes unserer Vorgehensweise:

Korollar 5.16. *In jeder Idealklasse* $[\mathfrak{b}] \in \mathrm{Cl}_K$ *gibt es ein ganzes Ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *mit* $N(\mathfrak{a}) \leq M_K$.

Beweis. Sei $0 \neq d \in \mathcal{O}_K$ so, dass $\mathfrak{c} := d\mathfrak{b}^{-1} \subset \mathcal{O}_K$. Nach Proposition 5.15 gibt es ein $\alpha \in \mathfrak{c} \setminus \{0\}$ mit

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N(\mathfrak{c}). \tag{5.15}$$

Wir setzen $\mathfrak{a} := \alpha\mathfrak{c}^{-1}$. Wegen $\alpha \in \mathfrak{c}$ gilt insbesondere $\mathfrak{c} \mid (\alpha)$. Es folgt dann aus der Primidealfaktorisierung, dass $\mathfrak{a}$ ein ganzes Ideal ist. Außerdem gilt

$$\mathfrak{a} = \alpha\mathfrak{c}^{-1} = (\alpha d^{-1})\mathfrak{b},$$

also $[\mathfrak{a}] = [\mathfrak{b}]$ in Cl_K und

$$N(\mathfrak{a}) = N((\alpha)) \cdot N(\mathfrak{c}^{-1}) = |N_{K/\mathbb{Q}}(\alpha)| \cdot N(\mathfrak{c}^{-1}) \overset{(5.15)}{\leq} M_K \cdot N(\mathfrak{c}^{-1}) \cdot N(\mathfrak{c}) = M_K.$$

□

Schließlich erledigen wir den zweiten Beweisschritt.

Lemma 5.17. *Sei $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ ein Primideal und p eine Primzahl. Dann gilt:*

$$N(\mathfrak{p}) = p^f \text{ für ein } f \geq 1 \iff \mathfrak{p} \mid p\mathcal{O}_K.$$

Insbesondere gilt es nur endlich viele Primideale von $\mathcal{O}_K$, deren Norm eine Potenz von p ist.

Beweis. Falls $\mathfrak{p}$ ein Teiler von $p\mathcal{O}_K$ ist, so folgt (mit der Multiplikativität der Idealnorm), dass $N(\mathfrak{p})$ die Zahl

$$N(p\mathcal{O}_K) \overset{\text{Prop. 4.33}}{=} |N_{K/\mathbb{Q}}(p)| = p^n \qquad \text{mit} \quad n = [K : \mathbb{Q}]$$

teilt.
Ist umgekehrt $N(\mathfrak{p})$ eine Potenz von p, so erhalten wir mit Korollar 4.35, dass

$$p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}.$$

Es folgt

$$p\mathcal{O}_K = (\mathfrak{p} \cap \mathbb{Z})\mathcal{O}_K \subset \mathfrak{p},$$

also $\mathfrak{p} \mid p\mathcal{O}_K$.

□

Bemerkung. Die Aussage von Lemma 5.17 kann leicht auf die relative Situation verallgemeinert werden (in der man statt einem Zahlkörper K eine Erweiterung L/K von Zahlkörpern betrachtet).

Proposition 5.18. *Für jedes $C > 0$ gibt es nur endlich viele ganze Ideale $\neq (0)$ von $\mathcal{O}_K$ mit Norm $\leq C$.*

Beweis. Da sich jedes ganze Ideal $\neq (0)$ von $\mathcal{O}_K$ sich eindeutig als Produkt von Primidealen schreiben lässt, die Idealnorm multiplikativ ist und die Norm eines Primideals $\neq (0)$ eine ganze Zahl ≥ 2, genügt es zu zeigen, dass es nur endlich viele *Prim*ideale mit beschränkter Norm gibt.
Da $N(\mathfrak{p})$ eine Potenz der durch $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ definierten Primzahl ist, gibt es nur endlich viele verschiedene Möglichkeiten für p. Für jedes dieser endlich vielen p's gibt es nach Lemma 5.17 nur endlich viele Primideale, deren Norm eine Potenz von p ist. □

Die Endlichkeit der Klassenzahl ist eine unmittelbare Konsequenz.

Satz 5.19 (Endlichkeit der Klassenzahl)**.** *Die Klassengruppe* Cl_K *ist endlich.*

Beweis. Nach Korollar 5.16 kann jede Idealklasse von einem ganzen Ideal mit beschränkter Norm repräsentiert werden. Nach Proposition 5.18 gibt es nur endlich viele ganze Ideale mit beschränkter Norm. □

Korollar 5.20. *Es existiert ein* $k \in \mathbb{Z}_{>0}$*, sodass für jedes ganze Ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *gilt, dass* $\mathfrak{a}^k$ *ein Hauptideal ist.*

Beweis. Sei $k := h_K < \infty$. Dann ist $(0)^k = (0)$ ein Hauptideal. Für $\mathfrak{a} \neq (0)$ ist die Ordnung von $[\mathfrak{a}] \in \mathrm{Cl}_K$ ein Teiler der Gruppenordnung h_k.
(Dieses k ist natürlich nicht optimal – es funktioniert beispielsweise auch die Zahl

$$k = \mathrm{kgV}(\{\mathrm{ord}([\mathfrak{b}]) \mid [\mathfrak{b}] \in \mathrm{Cl}_K\}),$$

die im Allgemeinen echt kleiner als h_K ist.) □

Beispiel 5.21. In der Tat liefert der Beweis auch Informationen über die Klassenzahl:

(1) Sei K ein Zahlkörper mit $M_K < 2$, dann ist $\mathcal{O}_K$ ein Hauptidealring.

Begründung: Wir haben gezeigt, dass jede Klasse $[\mathfrak{b}] \in \mathrm{Cl}_K$ durch ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}_K$ mit $N(\mathfrak{a}) \leq M_K < 2$ repräsentiert wird. Das einzige ganze Ideal mit der Norm 1 ist aber $\mathcal{O}_K$ selbst und damit ist Cl_K die triviale Gruppe.
Sei beispielsweise $K = \mathbb{Q}(\sqrt{13})$, dann ist

$$M_K = \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right)^0 \cdot \sqrt{13} = \frac{\sqrt{13}}{2} < \frac{\sqrt{16}}{2} = 2.$$

Also ist $\mathcal{O}_K$ ein Hauptidealring.

(2) Sei $K = \mathbb{Q}(\sqrt{-5})$. Aus Aufgabe 3.3.1 wissen wir bereits, dass Cl_K ein Element der Ordnung 2 hat, nämlich die Klasse von $(2, \sqrt{-5}+1)$. Die Gruppe Cl_K kann somit nicht trivial sein, aber welche Gruppe ist Cl_K genau? Nun, die Ungleichung

$$\frac{1}{2} \cdot \frac{4}{3} \cdot \sqrt{20} = \frac{4}{3}\sqrt{5} < 3 < \pi$$

impliziert durch Umstellen

$$M_K = \frac{1}{2} \cdot \frac{4}{\pi} \cdot \sqrt{20} < 3.$$

Somit wird jede Idealklasse in Cl_K durch ein ganzes Ideal repräsentiert, das die Norm 1 oder 2 hat. Eine nicht-triviale Idealklasse in Cl_K wird also durch ein ganzes Ideal $\mathfrak{a}$ repräsentiert, das die Norm 2 hat. In diesem Fall gilt $\mathfrak{a} \mid 2\mathcal{O}_K$. In Beispiel 3.17 haben wir bereits die Primfaktorzerlegung

$$2\mathcal{O}_K = (2, \sqrt{-5}+1)^2$$

berechnet. Es folgt $\mathfrak{a} = (2, \sqrt{-5}+1)$ und damit $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$ mit Erzeuger $[\mathfrak{a}]$.

Bemerkung 5.22. Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper ($d \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei).

(1) Ist $d < 0$, also K total imaginär, so heißt d eine *Heegner-Zahl*, wenn $h_K = 1$. Es stellt sich heraus, dass es lediglich die folgenden neun Heegner-Zahlen gibt:

$$-1, \quad -2, \quad -3, \quad -7, \quad -11, \quad -19, \quad -43, \quad -67, \quad -163.$$

(2) Im Kontrast zur obigen Liste ist noch nicht bekannt, ob es unendlich viele $d > 0$ (d.h. total reelle quadratische Zahlkörper K) mit Klassenzahl 1 gibt. Die folgenden $d < 100$ liefern quadratische Zahlkörper mit Klassenzahl 1:

2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33,
37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73,
77, 83, 86, 89, 93, 94, 97.

Wie die Folge weitergeht, kann hier eingesehen werden.

Bemerkung. Eine natürliche Fragestellung ist: Gegeben eine endliche, abelsche Gruppe A, gibt es einen Zahlkörper K mit $\mathrm{Cl}_K \cong A$? Antwort: Keine Ahnung. Das Problem ist noch weit offen. Teilantworten kann man im Falle von total imaginären quadratischen Zahlkörpern geben:

(1) Das "class number 100" Problem, welches von Mark Watkins gelöst wurde, bestimmt die Klassengruppen aller imaginär quadratischer Zahlkörper mit Klassenzahl ≤ 100. Die Klassifikation zeigt insbesondere, dass es genau fünf abelsche Gruppen der Ordnung ≤ 100 bis auf Isomorphie gibt, die nicht als Klassengruppe von total imaginären quadratischen Zahlkörpern auftreten können, beispielsweise $(\mathbb{Z}/3\mathbb{Z})^3$.

(2) Ist K ein total imaginärer quadratischer Zahlkörper, so ist die 2-Torsionsuntergruppe[2] von Cl_K isomorph zu $(\mathbb{Z}/2\mathbb{Z})^{\delta-1}$, wobei δ die Anzahl der verschiedenen Primteiler der Diskriminante d_K ist.

Bemerkung. Man beobachtet, dass wir im obigen Beweis der Endlichkeit der Klassenzahl wirklich entscheidend die Struktur von K als Zahlkörper genutzt haben. Dementsprechend liegt es nahe, zu fragen, ob die Klassengruppe von (Quotientenkörpern von) allgemeinen Dedekindringen ebenfalls endlich ist. Die Antwort ist "nein". Wir werden das hier nicht beweisen, aber beispielsweise ist die Klassengruppe des Koordinatenrings der affinen Kurve $y^2 = x^3 + ax + b$ über $\mathbb{C}$ mit $4a^3 + 27b^2 \neq 0$ (diese Bedingung garantiert, dass die Kurve glatt ist) nicht endlich.

Bemerkung. Im Beweis von Proposition 5.18 haben wir verwendet, dass es nur endlich viele Primideale in $\mathcal{O}_K$ gibt, die über einer fixierten Primzahl liegen. Das Ganze gilt viel allgemeiner: Ist $f\colon A \to B$ ein endlicher Ringhomomorphismus (d.h., bezüglich der skalaren Multiplikation $a *_f b := f(a)b$ mit $a \in A$ und $b \in B$ ist B ein endlich erzeugter A-Modul) und $\mathfrak{p} \subset A$ ein Primideal, so gibt es nur endlich viele Primideale $\mathfrak{q} \subset B$ mit $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. Wie zu erwarten ist, ist der Beweis komplizierter als in unserem Spezialfall. Wir geben den Beweis hier nicht, möchten aber auf die geometrische Bedeutung der Aussage hinweisen: Die Aussage heißt, dass die induzierte Abbildung

$$f^*\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A), \qquad \mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$$

zwischen den zugehörigen affinen Schemata endliche Fasern hat.

[2]Die m-Torsionsuntergruppe in einer (multiplikativ geschriebenen) abelschen Gruppe G ist die Untergruppe bestehend aus allen $g \in G$ mit $g^m = 1$.

5.2.1 Übungen

Aufgabe 5.2.1. Bestimmen Sie die Klassenzahl von $K = \mathbb{Q}(\sqrt{-23})$.

Aufgabe 5.2.2. Zeigen Sie, dass die quadratischen Zahlkörper mit den Diskriminanten

$$5, \quad 8, \quad 12, \quad 13, \quad -3, \quad -4, \quad -7, \quad -8, \quad -11$$

jeweils die Klassenzahl 1 haben.

Aufgabe 5.2.3. Verifzieren Sie, dass $K = \mathbb{Q}(\sqrt{-19})$ die Klassenzahl 1 hat, ohne Bemerkung 5.22 zu verwenden.

Aufgabe 5.2.4. Zeigen Sie, dass die Gleichung $x^2+5 = y^3$ keine ganzzahligen Lösungen hat, indem Sie die Gleichung von Idealen $(x^2 + 5) = (y)^3$ in $\mathcal{O}_K$ für $K = \mathbb{Q}(\sqrt{-5})$ untersuchen.

Aufgabe 5.2.5. Sei K ein Zahlkörper. Zeigen Sie, dass es eine endliche Körpererweiterung L/K gibt, sodass jedes gebrochene Ideal von $\mathcal{O}_K$ in L zu einem Hauptideal wird (d.h. für jedes gebrochene Ideal $\mathfrak{a}$ von $\mathcal{O}_K$ ist $\mathfrak{a}\mathcal{O}_L$ ein gebrochenes Hauptideal von $\mathcal{O}_L$).
Hinweis: Korollar 5.20. Finden Sie zunächst eine Erweiterung von K, in der *ein* gegebenes gebrochenes Ideal ein Hauptideal wird.

5.3 Die Sätze von Minkowski und Hermite

Der Beweis der Endlichkeit der Klassenzahl liefert noch weitere interessante Resultate, die wir in diesem Abschnitt beweisen möchten. Wir nutzen weiterhin die Notation aus den vorherigen Abschnitten, das heißt:

- K ist ein Zahlkörper vom Grad n,
- $\rho_1, \dots, \rho_r$ sind die reellen Einbettungen von K und $\sigma_1, \overline{\sigma}_1, \dots, \sigma_s, \overline{\sigma}_s$ sind die echt komplexen Einbettungen von K,
- Die Abbildung $j\colon K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$ ist durch

  $$\alpha \mapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \sigma_1(\alpha), \dots, \sigma_s(\alpha)).$$

  gegeben.

Satz 5.23 (Minkowski)**.** *Sei $K \neq \mathbb{Q}$ ein Zahlkörper, dann gilt $|d_K| \geq 2$. Insbesondere verzweigen in K mindestens eine und höchstens endlich viele Primzahlen.*

Beweis. Wir wenden Proposition 5.15 auf $\mathfrak{a} = \mathcal{O}_K$ an und erhalten ein $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit

$$\sqrt{|d_K|} \geq \frac{n^n}{n!} \cdot \left(\frac{\pi}{4}\right)^s \cdot |N_{K/\mathbb{Q}}(\alpha)| \geq \frac{n^n}{n!} \cdot \left(\frac{\pi}{4}\right)^{n/2}.$$

Hierbei haben wir $N(\mathcal{O}_K) = 1$, $s \leq n/2$ und $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$ benutzt. Für

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

erhalten wir

$$\frac{a_{n+1}}{a_n} = \sqrt{\frac{\pi}{4}} \cdot \left(1 + \frac{1}{n}\right)^n. \tag{5.16}$$

Da $\left(1+\frac{1}{n}\right)^n$ eine monoton wachsende Folge ist[3], deren Folgenglieder ≥ 2 sind, ist die rechte Seite von (5.16) größer gleich $2\sqrt{\frac{\pi}{4}} = \sqrt{\pi} > 1$. Somit ist (a_n) ebenfalls monoton wachsend. Es gilt also

$$\sqrt{|d_K|} \geq a_2 = \frac{\pi}{2} > 1.$$

Somit ist $|d_K| \geq 2$. Da d_K also mindestens einen Primteiler hat, folgt die Aussage aus Satz 4.51. □

Da für die im Beweis des Satzes von Minkowski 5.23 definierte Folge (a_n) gilt, dass

$$\frac{a_{n+1}}{a_n} \geq \sqrt{\pi} \qquad \text{für alle } n \geq 2,$$

divergiert (a_n) bestimmt gegen unendlich. Da außerdem $\sqrt{|d_K|} \geq a_n$ für $n = [K : \mathbb{Q}]$ gilt, erhalten wir aus dieser Überlegung:

Korollar 5.24. *Es gilt $|d_K| \to \infty$ für $[K : \mathbb{Q}] \to \infty$.*

Satz 5.25 (Hermite)**.** *Sei $M > 0$. Dann gibt es nur endlich viele Zahlkörper K mit $|d_K| < M$.*

Beweis. Sei $n \in \mathbb{Z}_{>0}$ gegeben. Nach Korollar 5.24 reicht es zu zeigen, dass es nur endlich viele Zahlkörper K vom Grad n und gegebener Diskriminante D gibt. Dafür unterscheiden wir zwei Fälle:

Fall 1: Der Körper K habe eine reelle Einbettung ρ_1. In diesem Fall betrachten wir für $c > 0$ die folgende Teilmenge von $K_{\mathbb{R}}$:

$$X_c := \left\{ (x', x'') \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; |x'_1| < c \text{ und } |x'_2|, \ldots, |x'_r| < 1,\ |x''_1|, \ldots, |x''_s| < 1 \right\}.$$

Wenn wir c groß genug wählen, können wir sicherlich

$$\operatorname{vol}(X_c) > 2^n \operatorname{vol}(\mathcal{O}_K) = 2^n \sqrt{D}$$

erreichen. Da X_c außerdem konvex und zentralsymmetrisch ist, impliziert der Gitterpunktsatz von Minkowski 5.9, dass es ein $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit $j(\alpha) \in X_c$ gibt. Für dieses α gilt

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| = |\rho_1(\alpha)| \cdot \underbrace{|\rho_2(\alpha)|}_{<1} \cdot \ldots \cdot \underbrace{|\rho_r(\alpha)|}_{<1} \cdot \underbrace{|\sigma_1(\alpha)|}_{<1} \cdot \underbrace{|\overline{\sigma}_1(\alpha)|}_{<1} \cdot \ldots \cdot \underbrace{|\sigma_s(\alpha)|}_{<1} \cdot \underbrace{|\overline{\sigma}_s(\alpha)|}_{<1}.$$

Wir erhalten $|\rho_1(\alpha)| > 1$.
Der nächste Schritt besteht darin, zu beweisen, dass α ein primitives Element von $K/\mathbb{Q}$ ist. Das sieht man so: Nach dem Fortsetzungssatz gibt es genau $[K : \mathbb{Q}(\alpha)]$ Fortsetzungen von $\rho_1|_{\mathbb{Q}(\alpha)}$ auf K. Eine solche Fortsetzung ist natürlich ρ_1 selbst. Gäbe es eine andere

[3] Das folgt etwa aus der AM-GM-Ungleichung: Mit $x_1 = 1$ und $x_2 = \ldots = x_{n+1} = 1 + \frac{1}{n}$ erhält man

$$\sqrt[n+1]{x_1 \cdot \ldots \cdot x_{n+1}} = \left(1 + \frac{1}{n}\right)^{n/(n+1)} \leq \frac{x_1 + \ldots + x_{n+1}}{n+1} = 1 + \frac{1}{n+1}.$$

Fortsetzung, so müsste dies eine der restlichen Einbettungen $\rho_2, \dots, \rho_r, \sigma_1, \overline{\sigma}_1, \dots, \sigma_s, \overline{\sigma}_s$ sein. Jedoch gilt ja

$$|\rho_1(\alpha)| > 1 \quad \text{und} \quad |\rho_2(\alpha)|, \dots, |\rho_r(\alpha)| < 1,\ |\sigma_1(\alpha)| = |\overline{\sigma}_1(\alpha)|, \dots, |\sigma_s(\alpha)| = |\overline{\sigma}_s(\alpha)| < 1.$$

Also muss $[K : \mathbb{Q}(\alpha)] = 1$ sein, d.h. $K = \mathbb{Q}(\alpha)$.
Schließlich untersuchen wir das Minimalpolynom m_α von α. Wir wissen, dass die Nullstellen von α in $\mathbb{C}$ gerade $\rho_1(\alpha), \dots, \rho_r(\alpha)$, $\sigma_1(\alpha), \dots, \overline{\sigma}_s(\alpha)$ sind. Da $\alpha \in X_c$, sind die Koeffizienten von m_α also lediglich in Abhängigkeit von c beschränkt. Da α ganz ist, ist $m_\alpha \in \mathbb{Z}[X]$ und damit gibt es nur endlich viele Möglichkeiten für m_α, also auch nur endlich viele Möglichkeiten für K.

Fall 2: Der Körper K ist total imaginär, d.h. $r = 0$. Dieser Fall wird analog bewiesen, indem wir die Menge

$$X_c := \left\{ x'' \in K_{\mathbb{R}} = \mathbb{C}^s \;\middle|\; |\operatorname{Im}(x_1'')| < c,\ |\operatorname{Re}(x_1'')| < 1 \text{ und } |x_2''|, \dots, |x_s''| < 1 \right\}$$

betrachten. Wie im ersten Fall erhalten wir $0 \neq \alpha \in \mathcal{O}_K$ mit $j(\alpha) \in X_c$ für c groß genug. Genau so zeigen wir $|\sigma_1(\alpha)| > 1$. Um "$K = \mathbb{Q}(\alpha)$" zu zeigen, bedarf es einer kleinen Änderung des Arguments: Wegen

$$|\sigma_2(\alpha)| = |\overline{\sigma}_2(\alpha)|, \dots, |\sigma_s(\alpha)| = |\overline{\sigma}_s(\alpha)| < 1$$

kann eine Fortsetzung von $\sigma_1|_{\mathbb{Q}(\alpha)}$ auf K nur σ_1 oder $\overline{\sigma}_1$ sein – wir müssen letzteres ausschließen. Das folgt jedoch sofort, da $j(\alpha) \in X_c$ und $|\sigma_1(\alpha)| > 1$ implizieren, dass $\operatorname{Im} \sigma_1(\alpha) \neq 0$, d.h. $\sigma_1(\alpha) \neq \overline{\sigma}_1(\alpha)$. Der Rest des Beweises funktioniert genau wie im ersten Fall. □

5.4 Die Einheitengruppe von Ganzheitsringen

In diesem Abschnitt beschäftigt uns die folgende Frage: Gegeben einen Zahlkörper K, wie lässt sich die Einheitengruppe $\mathcal{O}_K^*$ genauer beschreiben?

Beispiel 5.26.

- $\mathbb{Z}^* = \{1, -1\}$,
- Es gilt $1 + \sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})}^*$, da $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$.
- In jedem Zahlkörper K sind *Einheitswurzeln* leichte Beispiele von Einheiten in $\mathcal{O}_K$. Eine m-te Einheitswurzel von K ist definitionsgemäß eine Nullstelle des Polynoms $X^m - 1 \in \mathbb{Z}[X]$.

Zur Beantwortung der allgemeinen Frage nach der Struktur von $\mathcal{O}_K^*$ haben wir a priori zwei Ideen:

(1) Wir wissen nach Aufgabe 4.2.2, dass die Einheiten in $\mathcal{O}_K$ genau den ganzen Elementen mit Norm ± 1 entsprechen.

(2) Wir können erneut die Abbildung j aus den vorherigen beiden Abschnitten zu Rate ziehen:

$$\begin{aligned} j \colon K &\hookrightarrow K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s, \\ \alpha &\mapsto (\rho_1(\alpha), \dots, \rho_r(\alpha), \sigma_1(\alpha), \dots, \sigma_s(\alpha)). \end{aligned}$$

Hier sind wie üblich $\rho_1, \dots, \rho_r$ die reellen Einbettungen und $\sigma_1, \dots, \sigma_s$ paarweise nicht komplex konjugierte echt komplexe Einbettungen von K sind, sodass $n = [K : \mathbb{Q}] = r + 2s$.
Wir beobachten, dass $j(K^*) \subset (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$, also bekommen wir

$$j|_{\mathcal{O}_K^*} \colon \mathcal{O}_K^* \to (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s.$$

Wie üblich ist die Abbildung j gut geeignet, um den Gitterpunktsatz 5.9 zu nutzen. Jedoch handelt es sich bei Gittern um eine additive Untergruppe eines Vektorraums. Deshalb wandeln wir die multiplikative Gruppe $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$ gemäß

$$\begin{aligned} \ell \colon (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s &\to \mathbb{R}^{r+s}, \\ (x_1', \dots, x_r', x_1'', \dots, x_s'') &\mapsto \left(\ln\left(|x_1'|\right), \dots, \ln\left(|x_r'|\right), \ln\left(|x_1''|^2\right) \dots, \ln\left(|x_s''|^2\right)\right). \end{aligned}$$

in eine additive Gruppe um. Wir erhalten also einen injektiven Gruppenhomomorphismus

$$\begin{aligned} \lambda := \ell \circ j|_{\mathcal{O}_K^*} \colon \mathcal{O}_K^* &\to \mathbb{R}^{r+s}, \\ \alpha &\mapsto \left(\ln\left(|\rho_1(\alpha)|\right), \dots, \ln\left(|\rho_r(\alpha)|\right), \ln\left(|\sigma_1(\alpha)|^2\right), \dots, \ln\left(|\sigma_s(\alpha)|^2\right)\right), \end{aligned}$$

den wir im Folgenden genauer studieren werden. Dazu nutzen wir die kurze exakte Sequenz

$$1 \to \ker(\lambda) \to \mathcal{O}_K^* \xrightarrow{\lambda} \operatorname{im}(\lambda) \to 0.$$

Um $\mathcal{O}_K^*$ zu studieren, studieren wir also Kern und Bild von λ.

Wir bestimmen zunächst den Kern von λ.

Definition 5.27. Für einen Körper sei

$$\mu(F) = \{\zeta \in F^* \mid \text{es gibt } m \in \mathbb{Z}_{>0} \text{ mit } \zeta^m = 1\}$$

die *Gruppe der Einheitswurzeln* von F.

Beispiel 5.28. Der Zahlkörper K habe eine reelle Einbettung $\rho \colon K \hookrightarrow \mathbb{R}$. Dann gilt $\mu(K) = \{1, -1\}$, denn ist $\zeta \in \mu(K)$, so gibt es ein $m \in \mathbb{Z}_{>0}$ mit $\zeta^m = 1$. Es folgt

$$1 = \rho(1) = \rho(\zeta^m) = \rho(\zeta)^m,$$

d.h. $\rho(\zeta)$ ist eine Einheitswurzel in $\mathbb{R}$. Wir erhalten $\rho(\zeta) \in \{1, -1\}$, also $\zeta \in \{1, -1\}$.

Es stellt sich heraus, dass die Gruppe $\mu(K)$ der Einheitswurzeln von K gerade der Kern von $\lambda \colon \mathcal{O}_K^* \to \mathbb{R}^{r+s}$ ist:

Proposition 5.29. *Es gilt* $\ker(\lambda) = \mu(K)$.

Beweis. Sei $u \in \mathcal{O}_K^*$. Aus der Definition von λ folgt sofort:

$$\lambda(u) = 0 \iff |\tau(u)| = 1 \text{ für alle Einbettungen } \tau \colon K \hookrightarrow \mathbb{C}.$$

Die Aussage folgt dann sofort aus dem nächsten Lemma und der Erinnerung, dass die $\tau(u)$ gerade die Nullstellen des Minimalpolynoms von u sind. □

Lemma 5.30 (Kronecker)**.** *Sei $\alpha \in \mathbb{C}^*$ eine ganze algebraische Zahl, sodass alle Nullstellen des Minimalpolynoms von α den Absolutbetrag ≤ 1 haben. Dann ist α ist eine Einheitswurzel.*

Beweis. Seien $\alpha_1, \ldots, \alpha_m$ die komplexen Nullstellen des Minimalpolynoms m_α von α. Man betrachte die Folge von normierten Polynomen

$$P_\nu := \prod_{i=1}^{m} (X - \alpha_i^\nu), \qquad \nu \geq 1$$

vom Grad m. Durch Ausmultiplizieren sieht man, dass der Koeffizient $a_{\nu,k}$ von P_ν vor X^k $(0 \leq k < m)$ wie folgt gegeben ist:

$$a_{\nu,k} = (-1)^{m-k} \cdot \sum_{1 \leq i_1 < \ldots < i_{m-k} \leq m} \alpha_{i_1}^\nu \cdot \ldots \cdot \alpha_{i_{m-k}}^\nu.$$

Wir beobachten, dass die $a_{\nu,k}$ invariant unter der Operation von $\mathrm{Gal}(m_\alpha)$ sind – mit Galoistheorie folgt $a_{\nu,k} \in \mathbb{Q}$. Da aber $\alpha_1, \ldots, \alpha_m$ ganz algebraisch sind, sind auch alle $a_{\nu,k}$ ganz algebraisch. Mit $a_{\nu,k} \in \mathbb{Q}$ erhalten wir insgesamt $a_{\nu,k} \in \mathbb{Z}$.
Wir nutzen nun die Voraussetzung $|\alpha_1|, \ldots, |\alpha_m| \leq 1$, um den Betrag der ganzen Zahlen $a_{\nu,k}$ abzuschätzen:

$$|a_{k,\nu}| \overset{\text{Dreiecksugl.}}{\leq} \sum_{1 \leq i_1 < \ldots < i_{m-k} \leq m} |\alpha_{i_1}|^\nu \cdot \ldots \cdot |\alpha_{i_{m-k}}|^\nu \leq \sum_{1 \leq i_1 < \ldots < i_{m-k} \leq m} 1 = \binom{m}{m-k}. \tag{5.17}$$

Da die Abschätzung (5.17) nur von m, nicht aber von ν abhängt, sind die Polynome P_ν allesamt in der endlichen (!), von ν unabhängigen Menge

$$\left\{ X^m + b_{m-1}X^{m-1} + \ldots + b_1 X + b_0 \in \mathbb{Z}[X] \;\middle|\; \text{für alle } k = 0, \ldots, m-1 \text{ gilt } |b_k| \leq \binom{m}{m-k} \right\}$$

enthalten. Die Menge $\{P_\nu \mid \nu \geq 1\}$ ist also endlich. Die Menge der Nullstellen

$$N := \bigcup_{\nu \geq 1} \{\alpha_1^\nu, \ldots, \alpha_m^\nu\}$$

der Polynome P_ν ist also auch endlich. Da $\{\alpha^\nu \mid \nu \geq 1\}$ als Teilmenge von N auch endlich ist, gibt es $\nu_1 > \nu_2 \geq 1$ mit $\alpha^{\nu_2} = \alpha^{\nu_1}$, also $\alpha^{\nu_1 - \nu_2} = 1$. □

Bemerkung. Kroneckers Lemma 5.30 ist falsch, wenn α nicht als ganz vorausgesetzt ist. So gilt beispielsweise

$$m_\alpha = (X - \alpha)(X - \overline{\alpha}) = X^2 - \frac{6}{5}X + 1 \qquad \text{für} \quad \alpha = \frac{3 + 4i}{5} \in \mathbb{C},$$

d.h. α ist nicht ganz. Des Weiteren gilt $|\alpha| = |\overline{\alpha}| = 1$, aber α ist keine Einheitswurzel (denn Einheitswurzeln *sind* ganz).

Eine interessante Konsequenz des Beweises von Kroneckers Lemma 5.30 ist, dass $\mu(K)$ für jeden Zahlkörper K endlich ist. Fixiert man nämlich eine Einbettung $K \subset \mathbb{C}$, so hat jede Einheitswurzel $\zeta \in K$ den Absolutbetrag 1, und der Beweis zeigt, dass die

Koeffizienten von m_ζ in Abhängigkeit von $n = [K : \mathbb{Q}]$ beschränkt sind. Es gibt also nur endlich viele Möglichkeiten für m_ζ und damit auch nur endlich viele Einheitswurzeln in K.

Der Kern von $\lambda\colon \mathcal{O}_K^* \to \mathbb{R}^{r+s}$ ist nun also bestimmt. Um das Bild von λ zu finden, betrachten wir die Hyperebene

$$H := \left\{ (x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} \;\middle|\; \sum_{i=1}^{r+s} x_i = 0 \right\}$$

in $\mathbb{R}^{r+s}$ und starten mit der folgenden einfachen Beobachtung:

Lemma 5.31. *Es ist* $\operatorname{im}(\lambda) \subset H$.

Beweis. Sei $u \in \mathcal{O}_K^*$. Dann gilt:

$$\begin{aligned}
\sum_{i=1}^{r} \ln\left(|\rho_i(u)|\right) + \sum_{j=1}^{s} \ln\left(|\sigma_j(u)|^2\right) &= \ln\left(\prod_{i=1}^{r} |\rho_i(u)| \cdot \prod_{j=1}^{s} |\sigma_j(u)|^2 \right) \\
&= \ln\left(\prod_{i=1}^{r} |\rho_i(u)| \cdot \prod_{j=1}^{s} |\sigma_j(u)\overline{\sigma}_j(u)| \right) \\
&= \ln\left(\Big| \prod_{\tau\colon K \hookrightarrow \mathbb{C}} \tau(\alpha) \Big| \right) \overset{\text{Lem. 4.7}}{=} \ln |N_{K/\mathbb{Q}}(u)| = 0,
\end{aligned}$$

wobei wir im letzten Schritt verwendet haben, dass $N_{K/\mathbb{Q}}(u) \in \{\pm 1\}$, weil $u \in \mathcal{O}_K^*$. □

Wir möchten nun zeigen, dass $\operatorname{im}(\lambda)$ ein vollständiges Gitter in H ist. Dazu beweisen wir zunächst:

Lemma 5.32. *Für jedes $C > 0$ gibt es bis auf Assoziiertheit höchstens endlich viele $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit $|N_{K/\mathbb{Q}}(\alpha)| < C$.*

Beweis. Sei $\alpha \in \mathcal{O}_K \setminus \{0\}$ wie in der Aussage des Lemmas. Unter Verwendung von Proposition 4.33 folgt dann

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

Die Aussage folgt also aus der bereits bewiesenen Aussage "es gibt nur endlich viele ganze Ideale mit beschränkter Norm", vgl. Proposition 5.18. □

Proposition 5.33. *Das Bild von λ ist ein vollständiges Gitter in H.*

Beweis. Wir beweisen zunächst, dass $\operatorname{im}(\lambda)$ ein Gitter ist. Es genügt zu zeigen, dass für alle $\varepsilon > 0$ gilt:

$$|\operatorname{im}(\lambda) \cap Q_\varepsilon| < \infty, \tag{5.18}$$

wobei $Q_\varepsilon = \{(x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} \mid |x_i| \leq \varepsilon \text{ für } i = 1, \dots, r+s\}$. Wählt man nämlich ε klein genug, so folgt daraus $\operatorname{im}(\lambda) \cap Q_\varepsilon = \{0\}$. Durch Translation folgt dann die

Diskretheit von $\mathrm{im}(\lambda)$ und mit Satz 5.3 (1) erhalten wir dann, dass $\mathrm{im}(\lambda)$ ein Gitter ist. Wir weisen also nun (5.18) nach. Das Urbild von Q_ε unter $\ell\colon (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \to \mathbb{R}^{r+s}$ ist

$$A_\varepsilon := \{(x', x'') \in (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \mid e^{-\varepsilon} \leq |x_i'|, |x_j''|^2 \leq e^\varepsilon \text{ für } i = 1, \ldots, r,\ j = 1, \ldots, s\}.$$

Da A_ε kompakt ist und $j(\mathcal{O}_K)$ ein Gitter in $K_\mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ ist (vgl. Proposition 5.13), enthält A_ε nur endlich viele Elemente von $j(\mathcal{O}_K^*)$. Somit folgt auch, dass der Schnitt $\mathrm{im}(\lambda) \cap Q_\varepsilon$ endlich sein muss. Damit ist (5.18) also bewiesen.

Es bleibt zu zeigen, dass $\mathrm{im}(\lambda) \subset H$ vollständig ist. Gemäß Satz 5.3 (2) genügt es, eine beschränkte Menge $M \subset H$ mit

$$H = \bigcup_{\mu \in \mathrm{im}(\lambda)} (\mu + M) \tag{5.19}$$

zu finden. Wir schreiben für $x = (x', x'') \in K_\mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ verkürzt[4]

$$||y|| := \prod_{i=1}^{r} |x_i'| \cdot \prod_{j=1}^{s} |x_j''|^2$$

und beachten, dass die Einschränkung von ℓ auf

$$S := \left\{ x = (x', x'') \in (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \;\middle|\; ||x|| = 1 \right\}$$

eine Surjektion auf H definiert. Ist $N \subset S$ nun eine beschränkte Teilmenge, so ist $\ell(N)$ ebenfalls beschränkt, denn ist $x = (x', x'') \in N$, so impliziert die Beschränktheit von N, dass die Beträge $|x_i'|$ und $|x_j''|$ nicht beliebig groß werden können und wegen $||x|| = 1$ können sie deshalb auch nicht beliebig nahe an 0 herankommen.

Finden wir also eine beschränkte Teilmenge $N \subset S$ mit

$$\bigcup_{u \in \mathcal{O}_K^*} j(u) \cdot N = S, \tag{5.20}$$

so gilt auch (5.19) mit $M := \ell(N)$.

Zur Konstruktion einer geeigneten Menge N betrachten wir für $c = (c', c'') \in \mathbb{R}^{r+s}$ mit $c_i', c_j'' > 0$ die Menge

$$N_c := \{(x', x'') \in K_\mathbb{R} \mid |x_i'| < c_i',\ |x_j''| < c_j'' \text{ für } i = 1, \ldots, r,\ j = 1, \ldots, s\}.$$

Die konvexe und zentralsymmetrische Menge N_c ist das kartesische Produkt der r offenen Intervalle $(-c_i', c_i') \subset \mathbb{R}$ mit den s offenen Kreisscheiben $B_{c_j''}(0) \subset \mathbb{C}$. Also gilt[5]

$$\mathrm{vol}(N_c) = 2^{r+s} \cdot \pi^s \cdot ||c||.$$

Sei c nun so fixiert, dass $\mathrm{vol}(N_c) > 2^n \cdot \mathrm{vol}(\mathcal{O}_K)$ gilt.

Nach Lemma 5.32 gibt es $\beta_1, \ldots, \beta_m \in \mathcal{O}_K \setminus \{0\}$, sodass jedes $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit

$$|N_{K/\mathbb{Q}}(\beta)| < ||c||$$

[4] **Vorsicht:** Trotz der suggestiven Notation definiert $||\cdot||$ **keine** Norm auf $K_\mathbb{R}$!
[5] Um $||c||$ schreiben zu können, fassen wir $c \in \mathbb{R}^{r+s}$ als Element von $K_\mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ auf.

zu einem der $\beta_1, \ldots, \beta_m$ assoziiert ist. Wir weisen nun (5.20) für die beschränkte (!) Menge

$$N := \left(\bigcup_{i=1}^{m} j(\beta_i^{-1}) N_c \right) \cap S.$$

nach.

Hierfür bemerken wir zunächst, dass für alle $u \in \mathcal{O}_K^*$ gilt:

$$1 = |N_{K/\mathbb{Q}}(u)| = \prod_{i=1}^{r} |\rho_i(u)| \cdot \prod_{j=1}^{s} |\sigma_j(u)|^2 = ||j(u)||.$$

Wir erhalten somit $j(u) \in S$. Daher gilt $j(u)N \subset S$ für alle $u \in \mathcal{O}_K^*$.

Sei umgekehrt $y = (y', y'') \in S$. Zu zeigen ist, dass $u \in \mathcal{O}_K^*$ und $i \in \{1, \ldots, m\}$ mit

$$y \in j(u) \cdot \left(S \cap j(\beta_i^{-1}) N_c \right)$$

existieren. Wegen $j(u) \in S$ genügt es,

$$y \in j(u) j(\beta_i^{-1}) N_c \tag{5.21}$$

für ein $u \in \mathcal{O}_K^*$ und ein $i \in \{1, \ldots, m\}$ zu zeigen.

Wenn wir y als Einheit des Rings $K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$ (mit komponentenweiser Multiplikation) auffassen, so gilt:

$$\begin{aligned} y^{-1} N_c &= \{ y^{-1} x \in K_{\mathbb{R}} \mid x = (x', x''),\ |x_i'| < c_i',\ |x_j''| < c_j'' \text{ für } i = 1, \ldots, r,\ j = 1, \ldots, s \} \\ &= \{ (x', x'') \in K_{\mathbb{R}} \mid |x_i'| < |y_i'|^{-1} c_i',\ |x_j''| < |y_j''|^{-1} c_j'' \text{ für } i = 1, \ldots, r,\ j = 1, \ldots, s \} \\ &= N_{|y|^{-1}c} \qquad \text{mit} \quad |y|^{-1} c := (|y_1'|^{-1} \cdot c_1', \ldots, |y_r'|^{-1} \cdot c_r',\ |y_1''|^{-1} \cdot c_1'', \ldots |y_s''|^{-1} \cdot c_s''). \end{aligned}$$

Andererseits gilt wegen $||y|| = 1$ auch

$$\begin{aligned} \operatorname{vol}(N_{|y|^{-1}c}) &= 2^{r+s} \cdot \pi^s \cdot \left|\left| |y|^{-1} c \right|\right| \\ &= 2^{r+s} \cdot \pi^s \cdot ||y||^{-1} \cdot ||c|| \\ &= 2^{r+s} \cdot \pi^s \cdot ||c|| \\ &= \operatorname{vol}(N_c) \\ &> 2^n \cdot \operatorname{vol}(\mathcal{O}_K). \end{aligned}$$

Da $N_{|y|^{-1}c}$ außerdem konvex und zentralsymmetrisch ist, liefert der Gitterpunktsatz 5.9 ein $\alpha \in \mathcal{O}_K \setminus \{0\}$ mit

$$j(\alpha) \in N_{|y|^{-1}c} = y^{-1} N_c.$$

Wir haben also zweierlei Aussagen gezeigt:

(i) $y \in j(\alpha^{-1}) N_c$,

(ii) $|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r} |\rho_i(\alpha)| \cdot \prod_{j=1}^{s} |\sigma_j(\alpha)|^2 = ||j(\alpha)|| < \left|\left| |y|^{-1} c \right|\right| = ||c||$.

Wie bereits oben festgestellt, impliziert (ii), dass es ein β_i ($i \in \{1, \ldots, m\}$) und eine Einheit $u \in \mathcal{O}_K^*$ mit $\alpha = u^{-1} \cdot \beta_i$ gibt. Zusammen mit (i) bekommen wir

$$y \in j(\alpha^{-1})N_c = j(u)j(\beta_i^{-1})N_c.$$

Das beweist (5.21) und damit die Proposition. □

Als Folgerung erhalten wir den

Satz 5.34 (Dirichletscher Einheitensatz)**.** *Für einen Zahlkörper K mit r reellen und s Paaren echt komplexer Einbettungen gilt $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$. Insbesondere existieren $\varepsilon_1, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^*$, sodass sich jedes $u \in \mathcal{O}_K^*$ eindeutig in der Form*

$$u = \zeta \cdot \varepsilon_1^{\nu_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{\nu_{r+s-1}}$$

mit $\zeta \in \mu(K)$ und $\nu_i \in \mathbb{Z}$ schreiben lässt.

Beweis. In Proposition 5.29 und Proposition 5.33 haben wir gezeigt, dass wir eine exakte Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \mathrm{im}(\lambda) \to 0$$

haben, wobei $\mathrm{im}(\lambda)$ ein freier $\mathbb{Z}$-Modul vom Rang $r+s-1$ ist. Seien $\varepsilon_1, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^*$ so gewählt, dass $\{\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})\}$ eine $\mathbb{Z}$-Basis von $\mathrm{im}(\lambda)$ ist. Dann $\{\varepsilon_1, \ldots, \varepsilon_{r+s-1}\}$ eine $\mathbb{Z}$-linear unabhängige Teilmenge des multiplikativ geschriebenen $\mathbb{Z}$-Moduls $\mathcal{O}_K^*$, denn für alle $k_1, \ldots, k_{r+s-1} \in \mathbb{Z}$ mit

$$\varepsilon_1^{k_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{k_{r+s-1}} = 1$$

folgt ja

$$0 = \lambda(1) = \lambda\left(\varepsilon_1^{k_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{k_{r+s-1}}\right) = k_1 \cdot \lambda(\varepsilon_1) + \ldots + k_{r+s-1} \cdot \lambda(\varepsilon_{r+s-1}),$$

also $k_1, \ldots, k_{r+s-1} = 0$.

Ist nun $u \in \mathcal{O}_K^*$ beliebig, so gibt es eindeutig bestimmte $\nu_1, \ldots, \nu_{r+s-1} \in \mathbb{Z}$ mit

$$\lambda(u) = \nu_1 \cdot \lambda(\varepsilon_1) + \ldots + \nu_{r+s-1} \cdot \lambda(\varepsilon_{r+s-1}).$$

Jedoch gilt auch

$$\lambda\left(\varepsilon_1^{\nu_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{\nu_{r+s-1}}\right) = \nu_1 \cdot \lambda(\varepsilon_1) + \ldots + \nu_{r+s-1} \cdot \lambda(\varepsilon_{r+s-1}) = \lambda(u).$$

Es folgt $u \cdot \left(\varepsilon_1^{\nu_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{\nu_{r+s-1}}\right)^{-1} \in \ker(\lambda) = \mu(K)$, d.h.

$$u = \zeta \cdot \varepsilon_1^{\nu_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{\nu_{r+s-1}},$$

wie behauptet. □

Im Rest des Kapitels möchten wir uns den Fall quadratischer Zahlkörper genauer ansehen. Wir nehmen also im Folgenden stets

$$K = \mathbb{Q}(\sqrt{d}) \qquad \text{mit} \quad d \in \mathbb{Z} \setminus \{0, 1\} \text{ quadratfrei}$$

an. Des Weiteren möchten wir an die Beschreibung des Ganzheitsringes von K erinnern: Es gilt

$$\mathcal{O}_K = \mathbb{Z}[\theta] \qquad \text{mit} \quad \theta = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \pmod 4 \end{cases} \tag{5.22}$$

gilt, vgl. auch Aufgabe 4.4.1. Aus der obigen Beschreibung folgt sofort:

Lemma 5.35. *Sei $a + b\sqrt{d} \in \mathcal{O}_K$ mit $a, b \in \mathbb{Q}$.*

(1) Ist $d \equiv 2,3 \pmod 4$, so gilt $a, b \in \mathbb{Z}$.

(2) Ist $d \equiv 1 \pmod 4$, so gilt $a, b \in \frac{1}{2}\mathbb{Z}$. Ferner gilt $a \in \mathbb{Z}$ genau dann, wenn $b \in \mathbb{Z}$ gilt.

Beweis. Folgt sofort daraus, dass $\{1, \theta\}$ eine Ganzheitsbasis von K ist. □

Der imaginär quadratische Fall ist nun leicht behandelt.

Beispiel 5.36. Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}_{<0}$ quadratfrei. Dann ist K ein imaginär quadratischer Zahlkörper, d.h. $r = 0$ und $s = 1$. Der Einheitensatz 5.34 impliziert $\mathcal{O}_K^* = \mu(K)$ – insbesondere ist $\mathcal{O}_K^*$ endlich. In der Tat gilt mit $\omega = \frac{-1+\sqrt{-3}}{2}$:

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1, \ \pm\sqrt{-1}\}, & \text{falls } d = -1 \\ \{\pm 1, \ \pm\omega, \ \pm\omega^2\}, & \text{falls } d = -3 \\ \{\pm 1\}, & \text{sonst.} \end{cases}$$

Zur Verifikation betrachtet man ein Element $a+b\sqrt{d} \in \mathcal{O}_K$ (mit $a, b \in \mathbb{Q}$) und analysiert, wann

$$N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2 = a^2 + |d|b^2 = 1$$

eintritt. Die Details überlassen wir als Übungsaufgabe, vgl. Aufgabe 5.4.2.

Im Rest des Kapitels fokussieren wir uns auf den Fall reell quadratischer Zahlkörper, nehmen also $d > 0$ an. In diesem Fall ist $r = 2$ und $s = 0$. Der Einheitensatz 5.34 impliziert also

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}.$$

Da K reell ist, gilt $\mu(K) = \{1, -1\}$. Ist ε ein Erzeuger des freien Anteils von $\mathcal{O}_K^*$, so lässt sich also jede Einheit von $\mathcal{O}_K$ eindeutig in der Form $\pm\varepsilon^\nu$ für ein $\nu \in \mathbb{Z}$ schreiben. Deswegen wird ε auch eine *Grundeinheit* von K genannt. Neben ε sind die anderen möglichen Grundeinheiten $-\varepsilon$, ε^{-1} und $-\varepsilon^{-1}$. Betrachten wir K nun als Teilkörper von $\mathbb{R}$ (indem man $\sqrt{d}$ wie üblich mit der positiven Wurzel von d identifiziert), so gilt:

Lemma 5.37. *Genau eine der vier Grundeinheiten von K kann in der Form*

$$\varepsilon_0 = a_0 + b_0\sqrt{d} \qquad \text{mit} \quad a_0, b_0 \in \mathbb{Q}_{>0}$$

geschrieben werden. Des Weiteren wird ε_0 als diejenige Grundeinheit charakterisiert, die größer als 1 ist.

Beweis. Ein Element $u = a + b\sqrt{d} \in \mathcal{O}_K$ $(a, b \in \mathbb{Q})$ ist genau dann eine Einheit in $\mathcal{O}_K$, wenn a, b die *Pellsche Gleichung*

$$|N_{K/\mathbb{Q}}(u)| = |a^2 - db^2| = 1$$

erfüllen. In diesem Falle sind neben u also auch noch

$$a - b\sqrt{d}, \qquad -a + b\sqrt{d}, \qquad \text{und} \qquad -a - b\sqrt{d}$$

Einheiten. Des Weiteren gilt

$$u^{-1} = \frac{a - b\sqrt{d}}{N_{K/\mathbb{Q}}(u)}, \qquad -u^{-1} = \frac{-a + b\sqrt{d}}{N_{K/\mathbb{Q}}(u)}, \qquad \text{und} \qquad -u = -a - b\sqrt{d}.$$

Das zeigt, dass es unter den vier Grundeinheiten von K genau eine Grundeinheit ε_0 gibt, die in der Form $\varepsilon_0 = a_0 + b_0\sqrt{d}$ mit $a_0, b_0 > 0$ geschrieben werden kann. Nach Lemma 5.35 folgt aus $a_0, b_0 > 0$ sogar $a_0, b_0 \geq \frac{1}{2}$, daher ist $\varepsilon_0 > 1$. Es gilt dann $-\varepsilon_0, -\varepsilon_0^{-1} < 0$ und $0 < \varepsilon_0^{-1} < 1$, deshalb ist ε_0 die einzige Grundeinheit, die größer als 1 ist. □

Die Einheit $\varepsilon_0 = a_0 + b_0\sqrt{d}$ aus Lemma 5.37 wird dann *die* Grundeinheit von K genannt. Wir möchten beschreiben, wie man die Grundeinheit von K finden kann.

Lemma 5.38. *Sei $u = a + b\sqrt{d} \in \mathcal{O}_K^*$ mit $a, b \in \mathbb{Q}_{>0}$. Dann gilt $a \geq b$ und $db > a$.*

Beweis. Gälte $a < b$, so erhielten wir

$$\underbrace{N_{K/\mathbb{Q}}(u)}_{\in\{1,-1\}} = a^2 - db^2 < (1-d)b^2 \leq \begin{cases} 1 - d, & \text{falls } d \equiv 2, 3 \pmod 4 \\ \frac{1-d}{4}, & \text{falls } d \equiv 1 \pmod 4. \end{cases}$$

In beiden Fällen erhalten wir einen Widerspruch zu $|N_{K/\mathbb{Q}}(u)| = 1$.

Die zweite Abschätzung beweisen wir erneut durch Widerspruch. Gälte $db \leq a$, so muss $a \neq b$ gelten. Nach der eben bewiesenen Abschätzung gilt dann $a > b$ und nach Lemma 5.35 also

$$a - b \geq 1 \qquad \text{und} \qquad db \geq \begin{cases} 2, & \text{falls } d \equiv 2, 3 \pmod 4 \\ \frac{5}{2}, & \text{falls } d \equiv 1 \pmod 4. \end{cases}$$

Das liefert den Widerspruch

$$\underbrace{N_{K/\mathbb{Q}}(u)}_{\in\{1,-1\}} = a^2 - db^2 \geq db \cdot (a - b) \geq \begin{cases} 2, & \text{falls } d \equiv 2, 3 \pmod 4 \\ \frac{5}{2}, & \text{falls } d \equiv 1 \pmod 4. \end{cases}$$

□

Sei nun $\alpha = x + y\sqrt{d} \in \mathcal{O}_K$ mit $x, y \in \mathbb{Q}_{>0}$. Dann gilt für alle $u = a + b\sqrt{d} \in \mathcal{O}_K^*$ mit $a, b \in \mathbb{Q}_{>0}$ (also insbesondere auch für $u = \varepsilon_0$):

$$u\alpha = (a + b\sqrt{d}) \cdot (x + y\sqrt{d}) = ax + dby + (ay + bx)\sqrt{d}.$$

Lemma 5.35 impliziert, dass $x, y \geq \frac{1}{2}$ gilt. Also folgt zusammen mit $a \geq b > 0$ und $db > a$ (Lemma 5.38):

$$ax + dby \geq \frac{a + db}{2} > a \qquad \text{und} \qquad ay + bx \geq \frac{a + b}{2} \geq b.$$

Mit anderen Worten: Die "rationale Koordinate" von $u\alpha$ ist echt größer als jene von u, und die "irrationale Koordinate" von $u\alpha$ ist zumindest nicht kleiner als jene von u.

Unsere Überlegung zeigt:

Korollar 5.39. *Für jede Einheit $u = a+b\sqrt{d}$ von $\mathcal{O}_K$ mit $a, b \in \mathbb{Q}_{>0}$ gilt $a \geq a_0$, $b \geq b_0$. Ist $u \neq \varepsilon_0$, so gilt sogar $a > a_0$.*

Beweis. Da ε_0 Grundeinheit von K ist, kann u eindeutig in der Form $u = \pm\varepsilon_0^{\pm\nu}$ für ein $\nu \in \mathbb{Z}_{\geq 0}$ geschrieben werden. Natürlich kann $\nu = 0$ nicht sein, denn $u \notin \{1, -1\}$. Für $\nu \geq 1$ ist ε_0^ν von der Form $\varepsilon_0^\nu = a_\nu + b_\nu\sqrt{d}$ mit positiven Koeffizienten a_ν, b_ν. Dem Beweis von Lemma 5.37 entnimmt man, dass mindestens ein Koeffizient der Elemente

$$\varepsilon_0^{-\nu}, \qquad -\varepsilon_0^{-\nu}, \qquad \text{und} \qquad -\varepsilon_0^\nu$$

negativ ist. Da die Koeffizienten von u nach Voraussetzung positiv sind, muss also $u = \varepsilon_0^\nu$ gelten. Die obige Diskussion liefert dann die Aussage über die Koeffizienten von u. □

Wir haben jetzt gezeigt, dass die Grundeinheit von K als die Einheit mit positiven Koeffizienten charakterisiert wird, deren "rationale Koordinate" minimal ist. Das liefert einen leichten Bruteforce-Algorithmus, um ε_0 zu finden. Wir suchen nämlich nach einer Lösung $a_0, b_0 > 0$ der Pellschen Gleichung $|a_0^2 - db_0^2| = 1$, für die a_0 minimal ist und $a_0 + b_0\sqrt{d} \in \mathcal{O}_K$ gilt.

Wir illustrieren den Prozess an einem Beispiel.

Beispiel 5.40.

(1) Sei $d = 3$. Dann müssen wir nur ganzzahlige a_0 probieren. Wir starten mit $a_0 = 1$, überprüfen also, ob

$$|1 - 3b_0^2| = 1$$

eine Lösung $b_0 \in \mathbb{Z}_{>0}$ hat. Das ist nicht der Fall. Als nächstes überprüfen wir $a_0 = 2$. Die Gleichung

$$|4 - 3b_0^2| = 1$$

hat die positive ganzzahlige Lösung $b_0 = 1$. Also gilt $\varepsilon_0 = 2 + \sqrt{3}$.

(2) Sei $d = 5$. Da $d \equiv 1 \pmod 4$, müssen wir mit $a_0 = \frac{1}{2}$ starten. Wir überprüfen also, ob

$$\left|\frac{1}{4} - 5b_0^2\right| = 1$$

eine Lösung $b_0 \in \frac{1}{2}\mathbb{Z}_{>0}$ hat. Das ist tatsächlich der Fall: $b_0 = \frac{1}{2}$ ist eine Lösung. Also sind wir bereits fertig und es gilt $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$.

Bemerkung 5.41. Der obige Bruteforce-Algorithmus ist natürlich nicht sonderlich effizient. Eine wesentlich bessere Methode, um Pellsche Gleichungen zu lösen, ist die Methode der Kettenbruchentwicklungen.

Bemerkung/Fazit 5.42. Sei $u = a + b\sqrt{d} \in \mathcal{O}_K$ (wobei $K = \mathbb{Q}(\sqrt{d})$ immer noch reell quadratisch ist). Nach Lemma 5.35 gilt

$$\begin{cases} a, b \in \mathbb{Z}, & \text{falls } d \equiv 2, 3 \pmod 4 \\ a, b \in \frac{1}{2}\mathbb{Z}, \text{ und } a \in \mathbb{Z} \iff b \in \mathbb{Z}, & \text{falls } d \equiv 1 \pmod 4. \end{cases} \tag{5.23}$$

Wir haben außerdem gesehen, dass

$$u \in \mathcal{O}_K^* \iff |a^2 - db^2| = 1$$

gilt. Da $\mathcal{O}_K^*$ für K reell quadratisch eine unendliche Gruppe ist, hat die Pellsche Gleichung $|a^2 - db^2| = 1$ also stets unendlich viele Lösungen in a, b wie in (5.23).

5.4.1 Übungen

Aufgabe 5.4.1. Zeigen Sie, dass ein Zahlkörper K mit $[K : \mathbb{Q}]$ ungerade nur die Einheitswurzeln ± 1 besitzt.

Aufgabe 5.4.2. Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}_{<0}$ quadratfrei. Zeigen Sie:

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1, \ \pm\sqrt{-1}\}, & \text{falls } d = -1 \\ \{\pm 1, \ \pm\omega, \ \pm\omega^2\}, & \text{falls } d = -3 \\ \{\pm 1\}, & \text{sonst.} \end{cases}$$

Hierbei ist $\omega = \frac{-1+\sqrt{-3}}{2}$.

Aufgabe 5.4.3. Bestimmen Sie die Grundeinheiten von $\mathbb{Q}(\sqrt{d})$ für $d = 2, 6, 7$.

Aufgabe 5.4.4 (Die Schlacht bei Hastings vom 14.10.1066)**.** Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleich großen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. (...) Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen "Ut!", "Olicrosse!", "Godemite!" vorwärts. (...) (vgl. *Carmen de Hastingae Proelio* von Guy, Bischof von Amiens).

Schreiben Sie ein Computerprogramm (in einer Sprache Ihrer Wahl), das die Größe der Armee Harolds II. (inkl. Harold selbst) bestimmt und geben Sie diese an. Erklären Sie, warum Ihre gefundene Lösung tatsächlich die Armeegröße Harolds ist.

Anmerkungen:

- Sie können natürlich annehmen, dass Harold überhaupt eine Armee hatte, das heißt, dass die gesuchte Anzahl ≥ 2 ist.
- Laut Wikipedia wird die Weltbevölkerung im Jahre 1066 auf etwa 250–350 Millionen Menschen geschätzt.

Aufgabe 5.4.5. Sei L/K eine Erweiterung von Zahlkörpern. Zeigen Sie: Falls $L \neq K$, so ist der Index $(\mathcal{O}_L^* : \mathcal{O}_K^*)$ genau dann endlich, wenn L ein CM-Körper ist und K der total reelle Teilkörper von L.
Erinnerung: Ein CM-Körper ist eine quadratische Erweiterung eines total reellen Zahlkörpers, die total imaginär ist, vgl. Aufgabe 4.1.2.

Aufgabe 5.4.6. Sei $K \subset \mathbb{R}$ ein Zahlkörper. Zeigen Sie, dass $\mathcal{O}_K^*$ genau dann dicht in $\mathbb{R}$ ist, wenn $[K : \mathbb{Q}] \geq 4$ oder K total reell vom Grad 3 ist.

Kapitel 6

Kreisteilungskörper

6.1 Grundlagen

Wenn nicht anders erwähnt, sei im Folgenden stets K ein Körper der Charakteristik 0.

Notation 6.1. Mit $\zeta_n \in \overline{K}$ bezeichnen wir eine primitive n-te Einheitswurzel, das heißt, dass gilt:

- $\zeta_n^n = 1$,
- Für $0 < m < n$ gilt $\zeta_n^m \neq 1$.

Für einen Körper beliebiger Charakteristik definieren wir $\mu_n(K) = \{\zeta \in K^* \mid \zeta^n = 1\}$ die Gruppe der n-ten Einheitswurzeln in K. (Vorsicht: $\mu_n(K)$ enthält natürlich nicht ausschließlich *primitive* n-te Einheitswurzeln.)
Des Weiteren bezeichne $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ die Eulersche Phi-Funktion. Sie ist durch

$$\varphi(n) = |\{1 \leq a \leq n \mid \operatorname{ggT}(a,n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^*|$$

definiert und ist eine multiplikative zahlentheoretische Funktion, d.h. für teilerfremde natürliche Zahlen n, m gilt

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Ist p eine Primzahl und $\nu \geq 1$, so gilt $\varphi(p^\nu) = p^{\nu-1}(p-1)$. Man muss also nur die Zerlegung von n in Primfaktoren kennen, um $\varphi(n)$ zu berechnen.

Bemerkung 6.2. Für jeden Körper K ist die Gruppe $\mu_n(K)$ endlich und zyklisch, vgl. Aufgabe 6.1.1.

Bemerkung 6.3. Sei $0 \leq a < n$. Dann gilt:

$$\zeta_n^a \text{ ist primitive } n\text{-te Einheitswurzel} \iff \operatorname{ggT}(a,n) = 1.$$

Gilt nämlich $\operatorname{ggT}(a,n) = 1$, so gilt $(\zeta_n^a)^m = \zeta_n^{am} \neq 1$ für alle $0 < m < n$, da aus den Voraussetzungen $n \nmid am$ folgt. Ist umgekehrt $\operatorname{ggT}(a,n) = d > 1$, so gilt für $m := \frac{n}{d} \in \mathbb{Z}_{>0}$ natürlich $0 < m < n$ und $(\zeta_n^a)^m = (\zeta_n^n)^{a/d} = 1$, da $\frac{a}{d} \in \mathbb{Z}_{>0}$.

Beispiel 6.4. Es ist

$$\mu_n(\mathbb{C}) = \left\{ \exp\left(\frac{2\pi i a}{n}\right) \in \mathbb{C} \;\middle|\; 0 \leq a < n \right\}.$$

Satz 6.5. *Sei $K/\mathbb{Q}$ eine Körpererweiterung, dann ist $K(\zeta_n)/K$ galoissch und es gibt einen kanonischen injektiven Gruppenhomomorphismus (den* zyklotomischen Charakter*)*

$$\chi\colon \mathrm{Gal}(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

Ist $K = \mathbb{Q}$, so ist χ ein Isomorphismus. Insbesondere gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beweis. Der Körper $K(\zeta_n)$ ist der Zerfällungskörper von $X^n - 1 \in K[X]$, d.h. $K(\zeta_n)/K$ ist normal. Da die Charakteristik von K gleich 0 ist, ist die Erweiterung automatisch separabel. Klarerweise ist sie endlich. Insgesamt erhalten wir, dass $K(\zeta_n)/K$ galoissch ist.

Nach Aufgabe 6.1.1 ist $\mu_n(K(\zeta_n))$ eine zyklische Gruppe. Für $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$ gibt es somit ein eindeutig bestimmtes zu n teilerfremdes $0 \leq a < n$ mit $\sigma(\zeta_n) = \zeta_n^a$. Wir definieren dann $\chi(\sigma) = a + n\mathbb{Z}$. Es ist sofort ersichtlich, dass χ ein injektiver Gruppenhomomorphismus ist.
Die Aussage für $K = \mathbb{Q}$ ist aus der Algebra bekannt und wird hier deshalb nicht noch einmal bewiesen. □

Bemerkung 6.6. Aus den Rechenregeln für die Eulersche Phi-Funktion folgt

$$\varphi(1) = \varphi(2) = 1 \qquad \text{und} \qquad \varphi(n) \in 2\mathbb{Z} \text{ für alle } n \geq 3.$$

Somit gilt für alle $n \geq 3$, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ gerade ist. Diese einfache Beobachtung wird gelegentlich wichtig sein, wenn wir die Norm eines Elements $\alpha \in \mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ berechnen möchten: Ist $m_\alpha(0) = b_0$ und $\deg(m_\alpha) = m$, so gilt nach Lemma 4.7 (1) für alle $n \geq 3$:

$$N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\alpha) = (-1)^{\varphi(n)} \cdot b_0^{\varphi(n)/m} = b_0^{\varphi(n)/m}.$$

Aus Satz 6.5 folgt, dass das Minimalpolynom $\Phi_n \in \mathbb{Q}[X]$ von ζ_n über $\mathbb{Q}$ den Grad $\varphi(n)$ hat. Man nennt Φ_n das *n-te Kreisteilungspolynom*. Die Nullstellen von Φ_n sind gerade die primitiven n-ten Einheitswurzeln, d.h.

$$\Phi_n = \prod_{\substack{1 \leq a \leq n \\ \mathrm{ggT}(a,n)=1}} (X - \zeta_n^a).$$

Beispiel 6.7. Sei p eine Primzahl, dann gilt

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + X + 1.$$

Dass es sich bei dem oben angegebenen Polynom tatsächlich um das p-te Kreisteilungspolynom handelt, folgt aus Gradgründen oder aus dem Eisensteinkriterium angewendet auf $(X+1)^{p-1} + \ldots + (X+1) + 1$.
Ist ferner $\nu \geq 1$, so gilt

$$\Phi_{p^\nu} = \Phi_p(X^{p^{\nu-1}}) = X^{p^{\nu-1}(p-1)} + \ldots + X^{p^{\nu-1}} + 1,$$

denn ζ_p^ν ist Nullstelle des Polynoms $\Phi_p(X^{p^{\nu-1}})$ vom Grad $p^{\nu-1}(p-1) = \varphi(p^\nu)$. Im Allgemeinen sind Kreisteilungspolynome jedoch sehr schwer zu berechnen.

Bevor wir eine Anwendung des zyklotomischen Charakters geben, unterbrechen wir die aktuelle Diskussion für einen kurzen Exkurs über linear disjunkte Körper.

Lemma und Definition 6.8. *Seien $F \subset K, K' \subset L$ Körper. Dann sind die folgenden Aussagen äquivalent:*

(1) Jedes F-linear unabhängige System von K ist auch linear unabhängig über K'.

(2) Jedes F-linear unabhängige System von K' ist auch linear unabhängig über K.

Sind die beiden äquivalenten Aussagen (1) und (2) erfüllt, so heißen K und K' linear disjunkt (über F).

Beweis. Aufgrund der Symmetrie der beiden Implikationen genügt es, die Implikation "(1) $\implies$ (2)" zu zeigen. Dies beweisen wir mit einem Widerspruchsbeweis. Sei $m \in \mathbb{Z}_{>0}$ minimal gewählt, sodass es ein F-linear unabhängiges System $(x'_1, \dots x'_m) \subset K'$ gibt, das linear abhängig über K ist. Klarerweise haben wir $m \geq 2$. Die lineare Abhängigkeit von $(x'_1, \dots x'_m)$ über K impliziert, dass es eine nicht-triviale Relation

$$x_1 x'_1 + \dots + x_m x'_m = 0 \qquad \text{mit} \quad x_1, \dots, x_m \in K \tag{6.1}$$

gibt. Diese Relation besagt, dass $(x_1, \dots, x_m) \subset K$ linear abhängig über K' ist. Nach (1) ist $(x_1, \dots, x_m)$ auch linear abhängig über F. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass x_1 als F-Linearkombination von $x_2, \dots, x_m$ geschrieben werden kann, also

$$x_1 = a_2 x_2 + \dots + a_m x_m \qquad \text{mit} \quad a_2, \dots, a_m \in F. \tag{6.2}$$

Da nicht alle der $x_1, \dots x_m$ gleich 0 sind, sind wegen (6.2) nicht alle der $x_2, \dots, x_m$ gleich 0. Setzt man (6.2) in (6.1) ein, so erhält man

$$x_2(x'_2 + a_2 x'_1) + \dots + x_m(x'_m + a_m x'_1) = 0.$$

Also ist $(x'_2 + a_2 x'_1, \dots, x'_m + a_m x'_1)$ linear abhängig über K. Da das System jedoch linear unabhängig über F ist, erhalten wir einen Widerspruch zur Minimalität von m. □

Korollar 6.9. *Es seien $F \subset K, K' \subset L$ Körper. Sind K, K' linear disjunkt über F, so gilt $K \cap K' = F$.*

Beweis. Eine F-Basis B von $K \cap K'$ ist insbesondere eine F-linear unabhängige Teilmenge von K. Da K und K' linear disjunkt sind, ist B auch linear unabhängig über K'. Da je zwei Elemente aus $K \cap K'$ über K' linear abhängig sind, kann B also nur aus einem einzigen Element bestehen. □

Für Teilkörper K, K' eines Körpers L sei KK' der kleinste Teilkörper von L, der K und K' enthält. Er wird das *Kompositum* von K und K' genannt. Eine leichte Beobachtung ist, dass

$$[KK' : F] \leq [K : F] \cdot [K' : F]$$

gilt: Haben wir nämlich F-Basen $(x_i)_{i \in I} \subset K$ bzw. $(x'_j)_{j \in J}$ von K bzw. K' gegeben, so ist $(x_i x_j)$ sicherlich ein F-Erzeugendensystem von KK'.

Beispiel 6.10. Für $K = F(\alpha_1, \ldots, \alpha_r)$ und $K' = F(\alpha'_1, \ldots \alpha'_s)$ gilt

$$KK' = F(\alpha_1, \ldots, \alpha_r, \alpha'_1, \ldots, \alpha'_s).$$

Lemma 6.11. *Es seien $F \subset K, K' \subset L$ Körper, wobei wir K/F, K'/F als endlich voraussetzen. Dann sind die folgenden Aussagen äquivalent:*

(1) Die Körper K und K' sind linear disjunkt über F.

(2) Es gilt $[KK' : F] = [K : F] \cdot [K' : F]$.

Beweis. "(1) $\Longrightarrow$ (2):" Seien K, K' linear disjunkt. Fixieren wir F-Basen $(x_1, \ldots, x_m)$ von K bzw. $(x'_1, \ldots, x'_\ell)$ von K', so wissen wir, dass $(x_i x'_j)_{i,j}$ ein F-Erzeugendensystem von KK' ist, das aus $m \cdot \ell = [K : F] \cdot [K' : F]$ Elementen besteht. Es genügt also zu zeigen, dass $(x_i x'_j)_{i,j}$ auch F-linear unabhängig ist. Seien also $a_{ij} \in F$ mit

$$\sum_{i=1}^{m} \sum_{j=1}^{\ell} a_{ij} x_i x'_j = \sum_{j=1}^{\ell} \left(\sum_{i=1}^{m} a_{ij} x_i \right) x'_j = 0.$$

Da K und K' linear disjunkt sind, ist $(x'_1, \ldots, x'_\ell)$ auch linear unabhängig über K, die obige Gleichung impliziert also

$$\sum_{i=1}^{m} a_{i1} x_i = \ldots = \sum_{i=1}^{m} a_{i\ell} x_i = 0.$$

Nun ist $(x_1, \ldots, x_m) \subset K$ aber F-linear unabhängig, woraus wir $a_{ij} = 0$ für alle i, j ablesen.

"(2) $\Longrightarrow$ (1):" Es gelte umgekehrt $[KK' : F] = [K : F] \cdot [K' : F]$. Sei $(y'_1, \ldots, y'_r) \subset K'$ ein F-linear unabhängiges System. Wir müssen zeigen, dass es auch K-linear unabhängig ist. Seien dazu $y_1, \ldots, y_r \in K$ mit

$$y_1 y'_1 + \ldots + y_r y'_r = 0 \tag{6.3}$$

und $(x_1, \ldots, x_m) \subset K$ eine F-Basis. Schreibe

$$y_j = \sum_{i=1}^{m} a_{ij} x'_i \qquad \text{für } a_{ij} \in F. \tag{6.4}$$

Setzt man (6.4) in (6.3) ein, so bekommt man

$$\sum_{j=1}^{\ell} \sum_{i=1}^{m} a_{ij} x_i y'_j = 0.$$

Wegen $[KK' : F] = [K : F] \cdot [K' : F]$ ist $(x_i y'_j)_{i,j}$ nun F-linear unabhängig, d.h. man erhält $a_{ij} = 0$ für alle i, j. Eingesetzt in (6.4) liefert das $y_j = 0$ für alle j, wie gewünscht. □

Die Theorie der linear disjunkten Körper möchten wir natürlich auf Kreisteilungskörper anwenden, welche – wie wir in Satz 6.5 gesehen haben – galoissch über $\mathbb{Q}$ sind. Während im Allgemeinen durch $K \cap K' = F$ nicht garantiert wird, dass K und K' linear disjunkt über F sind, ist das im galoisschen Fall richtig:

Proposition 6.12. *Es seien $F \subset K, K' \subset L$ Körper, sodass K/F, K'/F endliche Galoiserweiterungen und L/F separabel sind. Dann gilt:*

(1) Die Erweiterung KK'/F ist galoissch und die Abbildung

$$\psi\colon \mathrm{Gal}(KK'/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(K'/F), \qquad \tau \mapsto (\tau|_K, \tau|_{K'})$$

ist ein injektiver Gruppenhomomorphismus. Gilt zusätzlich $K \cap K' = F$, so ist ψ ein Isomorphismus. In diesem Fall gilt insbesondere

$$\mathrm{Gal}(KK'/F) = \{\sigma\sigma' \mid \sigma \in \mathrm{Gal}(K/F), \sigma' \in \mathrm{Gal}(K'/F)\}.$$

(2) Die Körper K, K' sind genau dann linear disjunkt über F, wenn $K \cap K' = F$ gilt.

Beweis. (1) Wir erinnern daran, dass Galoiserweiterungen dadurch charakterisiert werden, dass sie Zerfällungskörper eines separablen Polynoms[1] sind. Sind f bzw. g also separable Polynome mit Zerfällungskörper K bzw. K', so ist $f \cdot g$ ein separables Polynom mit Zerfällungskörper KK'. Damit ist KK' galoissch.

Für die nächsten Aussagen bemerken wir zunächst, dass ψ wohldefiniert (denn jedes $\tau \in G$ bildet Nullstellen von f bzw. g wieder auf Nullstellen von f bzw. g ab, also gilt $\tau(K) \subset K$ bzw. $\tau(K') \subset K'$) und ein Gruppenhomomorphismus ist. Außerdem ist ψ injektiv, da ein $\sigma \in \mathrm{Gal}(KK'/F)$, das die Identität auf K und K' ist, auch die Identität auf KK' ist. Um nachzuweisen, dass ψ unter der Voraussetzung $K \cap K' = F$ ein Isomorphismus ist, müssen wir also nur zeigen:

$$K \cap K' = F \implies |\mathrm{Gal}(K/F)| \cdot |\mathrm{Gal}(K'/F)| = |G|. \tag{6.5}$$

Schreibe nun

$$H := \mathrm{Gal}(KK'/K), \qquad H' := \mathrm{Gal}(KK'/K').$$

Da $K = (KK')^H$ und $K' = (KK')^{H'}$ gilt, folgt $KK' \subset (KK')^{H \cap H'}$ und damit

$$KK' = (KK')^{H \cap H'}.$$

Die Galoiskorrespondenz impliziert nun

$$H \cap H' = \{\mathrm{id}_{KK'}\}. \tag{6.6}$$

Da K und K' jeweils galoissch über F sind, sind H und H' außerdem Normalteiler von G und es gilt

$$\mathrm{Gal}(K/F) \cong G/H, \qquad \mathrm{Gal}(K'/F) \cong G/H'.$$

Die Normalität von H und H' in G impliziert außerdem, dass

$$HH' = \{hh' \mid h \in H, h' \in H'\}$$

[1] Für uns ist ein separables Polynom ein nicht-konstantes Polynom f mit der Eigenschaft, dass jeder irreduzible Faktor von f keine mehrfachen Nullstellen hat. (Man beachte, dass f in manchen Lehrbüchern separabel genannt wird, wenn $\deg(f) \geq 1$ und f selbst keine mehrfachen Nullstellen hat – das unterscheidet sich von unserer Definition!)

eine Untergruppe von G ist. Des Weiteren gilt

$$|HH'| = \frac{|H| \cdot |H'|}{|H \cap H'|} \overset{(6.6)}{=} |H| \cdot |H'|, \tag{6.7}$$

vgl. Aufgabe 6.1.6. Da $H, H' \subset HH'$, gilt

$$(KK')^{HH'} \subset (KK')^H = K, \ (KK')^{H'} = K',$$

also $(KK')^{HH'} \subset K \cap K'$. Gilt nun $K \cap K' = F$, so erhalten wir also $(KK')^{HH'} = K \cap K'$ und die Galoiskorrespondenz liefert $HH' = G$. Zusammen mit (6.7) bekommen wir nun

$$|\mathrm{Gal}(K/F)| \cdot |\mathrm{Gal}(K'/F)| = |G/H| \cdot |G/H'| = |G|,$$

was genau der Aussage (6.5) entspricht.

(2) Eine Implikation wurde bereits in Korollar 6.9 bewiesen (und nutzt nicht, dass K, K' galoissch über F sind). Die andere Implikation, nämlich

$$\text{“}K \cap K' = F \implies K, K' \text{ sind linear disjunkt”},$$

folgt sofort aus

$$[KK' : F] = |\mathrm{Gal}(KK'/F)| \overset{(1)}{=} |\mathrm{Gal}(K/F)| \cdot |\mathrm{Gal}(K'/F)| = [K : F] \cdot [K' : F]$$

und Lemma 6.11. □

Im Zahlkörperfall kann man die Diskriminante linear disjunkter Körper in Spezialfällen in Abhängigkeit der beiden einzelnen Diskriminanten angeben:

Satz 6.13. *Seien $K, K' \subset \mathbb{C}$ Zahlkörper, die linear disjunkt und jeweils galoissch über $\mathbb{Q}$ sind. Ferner seien $\{\omega_1, \dots, \omega_m\}$ bzw. $\{\omega'_1, \dots, \omega'_\ell\}$ Ganzheitsbasen von K bzw. K'. Dann gilt: Sind die Diskriminanten d_K und $d_{K'}$ teilerfremd, so ist $\{\omega_i \omega'_j\}_{i,j}$ eine Ganzheitsbasis von KK' und die Diskriminante von KK' ist durch*

$$d_{KK'} = d_K^\ell \cdot d_{K'}^m$$

gegeben.

Beweis. Aus Lemma 6.11 folgt, dass $\{\omega_i \omega'_j\}_{i,j}$ eine $\mathbb{Q}$-Basis von KK' ist. Für jedes $\alpha \in \mathcal{O}_{KK'}$ gibt es also $a_{ij} \in \mathbb{Q}$ mit

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{n'} a_{ij} \omega_i \omega'_j.$$

Wir müssen $a_{ij} \in \mathbb{Z}$ zeigen. Hierfür schreiben wir $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_m\}$ bzw. $\mathrm{Gal}(K'/\mathbb{Q}) = \{\sigma'_1, \dots, \sigma'_\ell\}$. Dann gilt $\mathrm{Gal}(KK'/\mathbb{Q}) = \{\sigma_i \sigma'_j \mid 1 \le i \le m, \ 1 \le j \le \ell\}$ (hier nutzen wir, dass $K, K'/\mathbb{Q}$ galoissch und linear disjunkt sind, vgl. Proposition 6.12). Setzen wir

$$T := (\sigma'_\ell(\omega'_j))_{\ell,j} \in \mathrm{Mat}(\ell \times \ell, \mathcal{O}_{K'}), \qquad a := \begin{pmatrix} \sigma'_1(\alpha) \\ \vdots \\ \sigma'_\ell(\alpha) \end{pmatrix}, \qquad b := \begin{pmatrix} \sum_{i=1}^m a_{i1} \omega_i \\ \vdots \\ \sum_{i=1}^n a_{i\ell} \omega_i \end{pmatrix},$$

so gilt $d_{K'} = \det(T)^2$ (vgl. die Diskussion vor Korollar 4.19) und $Tb = a$. Mit der Cramerschen Regel folgt $\det(T)b = T^{\mathrm{adj}}a$, also erhält man

$$d_{K'}b = \det(T)T^{\mathrm{adj}}a.$$

Da die Einträge von T^{adj} und a Elemente von ganz sind, sind die Einträge

$$d_{K'}\beta_j = \sum_{i=1}^{m} d_{K'}a_{ij}\omega_i$$

von $d_{K'}b$ ebenfalls ganz. Da $\{\omega_1, \ldots, \omega_m\}$ eine Ganzheitsbasis von K ist, folgt daraus nun $d_{K'}a_{ij} \in \mathbb{Z}$ für alle i, j. Durch Vertauschen der Rollen von K und K' erhält man analog $d_K a_{ij} \in \mathbb{Z}$ für alle i, j. Da $\mathrm{ggT}(d_K, d_{K'})$ nun teilerfremd sind, gibt es $r, s' \in \mathbb{Z}$ mit $rd_K + sd_{K'} = 1$. Nun folgt wie gewünscht

$$a_{ij} = rd_K a_{ij} + sd_{K'}a_{ij} \in \mathbb{Z}.$$

Wir berechnen noch die Diskriminante der Ganzheitsbasis $\{\omega_i\omega'_j\}$ von KK'. Wie bereits weiter oben erwähnt, ist

$$d_{KK'} = \det(M)^2, \qquad \text{wobei} \quad M := \left((\sigma_r\sigma'_s)(\omega_i\omega'_j)\right) = \left(\sigma_r(\omega_i)\sigma'_s(\omega'_j)\right).$$

Schreiben wir $Q = (\sigma_r(\omega_i))_{r,i}$, so können wir M via

$$M = \mathrm{diag}(\underbrace{Q, \ldots, Q}_{\ell \text{ mal}}) \cdot \begin{pmatrix} I_m \cdot \sigma'_1(\omega'_1) & \ldots & I_m \cdot \sigma'_1(\omega'_\ell) \\ \vdots & & \vdots \\ I_m \cdot \sigma'_\ell(\omega'_1) & \ldots & I_m \cdot \sigma'_\ell(\omega'_\ell) \end{pmatrix}$$

als $(\ell \times \ell)$-Blockmatrix von $(m \times m)$-Matrizen auffassen. Durch Zeilen- und Spaltenvertauschungen kann man die rechte Matrix in die Block-Diagonalmatrix

$$\mathrm{diag}(\underbrace{T, \ldots, T}_{m \text{ mal}}), \qquad \text{wobei} \quad T = (\sigma'_s(\omega'_j))_{s,j} \quad \text{(wie oben definiert)}$$

überführen. Man erhält also unter Beachtung von $d_K = \det(Q)^2$ und $d_{K'} = \det(T)^2$:

$$d_{KK'} = \det(M)^2 = \det(Q)^{2\ell} \cdot \det(T)^{2m} = d_K^{\ell} \cdot d_{K'}^{m}.$$

□

Bemerkung. Die Voraussetzung "galoissch" in Satz 6.13 ist nicht notwendig, es reicht "linear disjunkt".

Die obigen Resultate wenden wir jetzt auf den Kontext von Kreisteilungskörpern an.

Proposition 6.14. *Es seien $n, m \in \mathbb{Z}_{>0}$ und $d := \mathrm{ggT}(n, m)$, $\ell = \mathrm{kgV}(n, m)$. Dann gilt*

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d) \qquad \textit{und } \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_\ell).$$

Insbesondere sind $\mathbb{Q}(\zeta_n)$ und $\mathbb{Q}(\zeta_m)$ linear disjunkt über $\mathbb{Q}(\zeta_d)$.

Beweis. Wir starten mit einer einfachen Vorüberlegung. Sind $n = \prod_{p \text{ prim}} p^{\nu_p}$ bzw. $m = \prod_{p \text{ prim}} p^{\mu_p}$ die Primfaktorisierungen von n bzw. m (d.h. fast alle ν_p bzw. μ_p sind gleich 0), so sind

$$d = \prod_{p \text{ prim}} p^{\min\{\nu_p,\mu_p\}} \qquad \text{bzw.} \qquad \ell = \prod_{p \text{ prim}} p^{\max\{\nu_p,\mu_p\}}$$

die Primfaktorisierungen von d bzw. ℓ. Wegen $\min\{\nu_p, \mu_p\} + \max\{\nu_p, \mu_p\} = \nu_p + \mu_p$ gilt dann $nm = d\ell$. Wir möchten

$$\varphi(n)\varphi(m) = \varphi(d)\varphi(\ell) \tag{6.8}$$

nachweisen. Aufgrund der Multiplikativität von φ müssen wir das nur für $n = p^{\nu_p}$ und $m = p^{\mu_p}$ nachrechnen:

$$\varphi(n)\varphi(m) = \begin{cases} p^{\nu_p+\mu_p-2} \cdot (p-1)^2, & \text{falls } \nu_p, \mu_p \geq 1 \\ p^{\nu_p-1} \cdot (p-1), & \text{falls } \nu_p \geq 1,\ \mu_p = 0 \\ p^{\mu_p-1} \cdot (p-1), & \text{falls } \mu_p \geq 1,\ \nu_p = 0 \\ 1, & \text{falls } \nu_p = \mu_p = 0. \end{cases}$$

Nun gilt jedoch auch:

$$\varphi(d) = \begin{cases} p^{\min\{\nu_p,\mu_p\}-1} \cdot (p-1), & \text{falls } \nu_p, \mu_p \geq 1 \\ 1, & \text{falls } \nu_p \geq 1,\ \mu_p = 0 \\ 1, & \text{falls } \mu_p \geq 1,\ \nu_p = 0 \\ 1, & \text{falls } \nu_p = \mu_p = 0 \end{cases} \qquad \text{und}$$

$$\varphi(\ell) = \begin{cases} p^{\max\{\nu_p,\mu_p\}-1} \cdot (p-1), & \text{falls } \nu_p, \mu_p \geq 1 \\ p^{\nu_p-1} \cdot (p-1), & \text{falls } \nu_p \geq 1,\ \mu_p = 0 \\ p^{\mu_p-1} \cdot (p-1), & \text{falls } \mu_p \geq 1,\ \nu_p = 0 \\ 1, & \text{falls } \nu_p = \mu_p = 0. \end{cases}$$

Insgesamt folgt $\varphi(n)\varphi(m) = \varphi(d)\varphi(\ell)$, wie behauptet.

Nun zum eigentlichen Beweis. Wir schreiben $F = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$. Während die Inklusion $\mathbb{Q}(\zeta_d) \subset F$ klar ist, genügt es für die andere Inklusion $[F : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d)$ zu zeigen. Nach Satz 6.5 ist $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n)$ galoissch und es gilt

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n)) = \{\sigma_a \colon \zeta_\ell \mapsto \zeta_\ell^a \mid 1 \leq a \leq \ell,\ \ \mathrm{ggT}(a, \ell) = 1,\ a \equiv 1 \pmod{n}\}.$$

Die Hauptbeobachtung ist nun, dass für jedes $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n))$ gilt:

$$\sigma_a|_{\mathbb{Q}(\zeta_m)} \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/F).$$

Dass F von σ_a fixiert wird, ist klar – man muss sich also noch klar machen, dass $\sigma_a(\zeta_m) \in \mathbb{Q}(\zeta_m)$ gilt. Da aus $\mathrm{ggT}(a,\ell) = 1$ jedoch $\mathrm{ggT}(a,m) = 1$ folgt, ist das ebenfalls klar. Da außerdem alle $\sigma_a|_{\mathbb{Q}(\zeta_m)}$ paarweise verschieden sind, erhält man nun zusammen mit der Gradformel

$$[\mathbb{Q}(\zeta_m) : F] = |\mathrm{Gal}(\mathbb{Q}(\zeta_m)/F)| \geq |\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n))| = [\mathbb{Q}(\zeta_\ell) : \mathbb{Q}(\zeta_n)] = \frac{\varphi(\ell)}{\varphi(n)} \overset{(6.8)}{=} \frac{\varphi(m)}{\varphi(d)}$$

und damit auch

$$\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : F] \cdot [F : \mathbb{Q}] \geq \frac{\varphi(m)}{\varphi(d)} \cdot [F : \mathbb{Q}],$$

also $[\mathbb{F} : \mathbb{Q}] \leq \varphi(d)$, wie gewünscht. Die Aussage über die lineare Disjunktheit von $\mathbb{Q}(\zeta_n)$ und $\mathbb{Q}(\zeta_m)$ über $\mathbb{Q}(\zeta_d)$ folgt nun aus Proposition 6.12 (2), da $\mathbb{Q}(\zeta_n)$ und $\mathbb{Q}(\zeta_m)$ galoissch über $\mathbb{Q}(\zeta_d)$ sind.

Es verbleibt, $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_\ell)$ zu zeigen. Da ζ_n und ζ_m beides ℓ-te Einheitswurzeln sind, ist die Inklusion "$\subset$" klar. Für die andere Inklusion genügt es, $[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = \varphi(\ell)$ zu zeigen. Mit Lemma 6.11 folgt nun aus der eben bewiesenen linearen Disjunktheit und der Gradformel:

$$\frac{[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}]}{\varphi(d)} = [\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_d)] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_d)] \cdot [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)] = \frac{\varphi(n)\varphi(m)}{\varphi(d)^2} \overset{(6.8)}{=} \frac{\varphi(\ell)}{\varphi(d)},$$

also $[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = \varphi(\ell)$, wie gewünscht. □

Vermutlich haben Sie schon damit gerechnet, dass das unten stehende Resultat gilt.

Proposition 6.15. *Die Einheitswurzeln in $\mathbb{Q}(\zeta_n)$ sind von der Form $\pm\zeta_n^a$, $1 \leq a \leq n$. Umgekehrt ist jedes Element von der Form $\pm\zeta_n^a$ eine Einheitswurzel von $\mathbb{Q}(\zeta_n)$.*

Beweis. Wegen $(\pm\zeta_n^a)^{2n} = 1$ sind die Elemente $\pm\zeta_n^a$ Einheitswurzeln. Umgekehrt sei m die maximale Ordnung einer Einheitswurzel von $\mathbb{Q}(\zeta_n)$ – solch ein m existiert, weil die Gruppe der Einheitswurzeln in einem Zahlkörper endlich ist. Es genügt zu zeigen, dass

$$m = \begin{cases} n, & \text{falls } n \text{ gerade ist} \\ 2n, & \text{falls } n \text{ ungerade ist} \end{cases}$$

gilt. Klar ist, dass n ein Teiler von m ist – wir können also $m = n \cdot k$ mit $k \in \mathbb{Z}_{>0}$ schreiben. Für $d := \mathrm{ggT}(n,k)$ gilt:

$$\varphi(m) = \varphi(nk) \overset{(*)}{=} \frac{d \cdot \varphi(n) \cdot \varphi(k)}{\varphi(d)} \geq \varphi(n) \cdot \varphi(k).$$

Die Gleichheit $(*)$ weist man hierbei wie die Gleichung (6.8) im Beweis von Proposition 6.14 nach. Da $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ und $\varphi(m) \geq \varphi(n)$ gilt, folgt

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

und damit $\varphi(m) = \varphi(n)$. Aus obiger Abschätzung bekommt man nun $\varphi(k) = 1$, d.h. $k \in \{1, 2\}$. Ist nun n gerade, so gilt $\varphi(2n) = 2\varphi(n) > \varphi(n)$, d.h. $k = 1$ und damit $m = n$. Für n ungerade gilt $\varphi(2n) = \varphi(n)$, d.h. $k = 2$ und damit $m = 2n$. □

6.1.1 Übungen

Aufgabe 6.1.1. Sei K ein beliebiger Körper.

(1) Zeigen Sie die aus Ihrer Algebravorlesung bekannte Aussage, dass endliche Untergruppen von K^* zyklisch sind.

(2) Zeigen Sie, dass $\mu_n(K)$ endlich ist.

(3) Folgern Sie, dass $\mu_n(K)$ zyklisch ist.

Aufgabe 6.1.2. Sei $n \geq 3$. Zeigen Sie, dass $\mathbb{Q}(\zeta_n)$ total imaginär ist, aber einen Teilkörper F mit $[\mathbb{Q}(\zeta_n) : F] = 2$ enthält, der total reell ist.

Aufgabe 6.1.3. In manchen Fällen lassen sich Kreisteilungspolynome aus anderen berechnen:

(1) Sei $n \in \mathbb{Z}_{>0}$ ungerade. Zeigen Sie $\Phi_{2n}(X) = \Phi_n(-X)$.

(2) Sei p eine Primzahl und $n \geq 1$. Zeigen Sie:

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p), & \text{falls } p|n \\ \Phi_n(X^p)/\Phi_n(X), & \text{falls } p \nmid n. \end{cases}$$

(3) Nutzen Sie die vorherige Teilaufgabe, um Φ_{p^ν} für $n \geq 1$ explizit anzugeben (p prim).

Aufgabe 6.1.4. Sei p eine Primzahl und $n \geq 1$ nicht durch p teilbar. Zeigen Sie die folgenden Aussagen:

(1) $\Phi_p(X^n) = \sum_{i=0}^{p-1} (X^p)^{e_i} X^i$ für geeignete Exponenten $e_i \geq 0$.

(2) $(X-1) \cdot \Phi_p(X^n) = \sum_{i=0}^{p-1} ((X^p)^{a_i} - (X^p)^{b_i}) X^i$ für geeignete Exponenten $a_i, b_i \geq 0$.

(3) Die Koeffizienten des Polynoms $\Phi_p(X^n)/\Phi_p(X)$ sind allesamt in der Menge $\{-1, 0, 1\}$ enthalten.

(4) Wenn n prim ist, dann liegen alle Koeffizienten von Φ_{pn} in $\{-1, 0, 1\}$.

Nutzen Sie Aufgabe 6.1.3 zusammen mit der obigen Teilaufgabe (4), um den folgenden Satz von Migotti zu beweisen:

(5) Falls $n = 2^a p^b q^c$ mit Primzahlen p, q, dann hat das Kreisteilungspolynom Φ_n nur Koeffizienten in $\{-1, 0, 1\}$.

(6) Folgern Sie, dass die Koeffizienten von Φ_n für $n < 105$ stets in der Menge $\{-1, 0, 1\}$ enthalten sind. In der Tat ist $n = 105$ der erste Fall, in dem das nicht mehr so ist, wie die verlinkte WolframAlpha-Rechnung zeigt.

Aufgabe 6.1.5. Es seien $K = \mathbb{Q}(\zeta_3 \sqrt[3]{2})$ und $K' = \mathbb{Q}(\sqrt[3]{2})$. Zeigen Sie, dass $K \cap K' = \mathbb{Q}$, aber dass K und K' nicht linear disjunkt über $\mathbb{Q}$ sind.

Aufgabe 6.1.6. Sei G eine Gruppe und U, V Untergruppen. Definiere $UV := \{uv \mid u \in U, v \in V\}$.

(1) Zeigen Sie, dass $|UV| = \frac{|U| \cdot |V|}{|U \cap V|}$ gilt.

(2) Zeigen Sie, dass UV genau dann eine Untergruppe von G ist, wenn $UV = VU$ gilt.

(3) Zeigen Sie: Ist U ein Normalteiler von G, so ist UV eine Untergruppe von G.

Aufgabe 6.1.7 (Spezialfall des Dirichletschen Primzahlsatzes)**.** Sei $b \in \mathbb{Z}_{>0}$. Zeigen Sie, dass es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{b}$ gibt.
Hinweis: Nehmen Sie an, es gäbe nur endlich viele solche Primzahlen. Sei P ihr Produkt. Nicht alle Zahlen $\Phi_b(xnP)$, $x \in \mathbb{Z}$ können 1 oder -1 sein. Sei $k \in \mathbb{Z}$ so, dass $\Phi_b(knP)$ durch eine Primzahl q teilbar ist. Leiten Sie einen Widerspruch her.
Bemerkung: In seiner allgemeinsten Form besagt der Dirichletsche Primzahlensatz, dass für zwei teilerfremde Zahlen $a, b \in \mathbb{Z}_{>0}$ gilt, dass

$$\sum_{\substack{p \text{ prim,} \\ p \equiv b \pmod{a}}} \frac{1}{p} = \infty.$$

Insbesondere gibt es unendlich viele Primzahlen der Form $an + b$. Der Beweis dieser Aussage basiert auf Methoden der analytischen Zahlentheorie.

Aufgabe 6.1.8 (Inverses Galoisproblem für abelsche Gruppen)**.** Sei A eine endliche, abelsche Gruppe. Zeigen Sie, dass es eine Galoiserweiterung $K/\mathbb{Q}$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong A$ gibt.
Hinweis: Verwenden Sie Aufgabe 6.1.7.

Bemerkung: Das inverse Galoisproblem ist ein noch ungelöstes Problem der Zahlentheorie, das danach fragt, ob es für jede endliche Gruppe G eine Galoiserweiterung $K/\mathbb{Q}$ mit Galoisgruppe $\cong G$ gibt. Für alle auflösbaren Gruppen und die meisten sporadischen Gruppen ist die Antwort "ja", noch offen ist der Fall der Mathieu-Gruppe M_{23}.

6.2 Das Zerlegungsgesetz

Gegeben eine natürliche Zahl n und eine Primzahl p, wie zerfällt p in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$? Diese Frage wird durch das Zerlegungsgesetz beantwortet. Zuerst müssen wir uns aber darüber Gedanken machen, welcher Ring $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ überhaupt ist.

Proposition 6.16. *Sei p eine Primzahl, $\nu \geq 1$ und $q = p^\nu \neq 2$. Sei $\zeta = \zeta_q$, sowie $\lambda = 1 - \zeta$ und $d := [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^\nu) = p^{\nu-1}(p-1)$. Dann gilt:*

(1) Die $\mathbb{Q}$-Basis $\{1, \zeta, \ldots, \zeta^{d-1}\}$ von $\mathbb{Q}(\zeta)$ hat die Diskriminante

$$d_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \cdot p^m \qquad \text{mit} \quad m = p^{\nu-1}(\nu p - \nu - 1).$$

(2) In $\mathcal{O}_{\mathbb{Q}(\zeta)}$ gilt $(p) = (\lambda)^d$. Insbesondere ist (λ) ein Primideal in $\mathcal{O}_{\mathbb{Q}(\zeta)}$ vom Trägheitsgrad 1 und p in $\mathbb{Q}(\zeta)$ total verzweigt.

Beweis. (1) Wegen

$$\Phi_q = \prod_{1 \leq a < q,\ p \nmid a} (X - \zeta^a)$$

gilt

$$\Phi_q'(\zeta) = \prod_{1 < a < q,\ p \nmid a} (\zeta - \zeta^a).$$

Sei nun $1 < a < q$ mit $p \nmid a$ gegeben. Da die komplexen Einbettungen von $\mathbb{Q}(\zeta)$ gerade durch $\zeta \mapsto \zeta^i$ für $1 \leq i < q$ mit $p \nmid i$ gegeben sind, folgt aus Lemma 4.7

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta - \zeta^a) = \prod_{1 \leq i < q,\ p \nmid i} (\zeta^i - \zeta^{ai})$$

und damit

$$\begin{aligned} N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi_q'(\zeta)) &= \prod_{\substack{1 \leq i < q \\ p \nmid i}} \prod_{\substack{1 < a < q \\ p \nmid a}} (\zeta^i - \zeta^{ai}) = \prod_{\substack{i \neq j \\ p \nmid i, j}} (\zeta^i - \zeta^j) \\ &= (-1)^{\frac{d(d-1)}{2}} \cdot \Delta(\Phi_q) = (-1)^{\frac{d(d-1)}{2}} \cdot d_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{d-1}). \end{aligned}$$

Es muss also nur noch $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi_q'(\zeta)) = p^m$ mit $m = p^{\nu-1}(\nu p - \nu - 1)$ nachgewiesen werden.

Differenzieren der Gleichung $(X^{p^{\nu-1}} - 1)\Phi_q = X^q - 1$ und anschließendes Einsetzen von ζ liefert

$$(\zeta_p - 1) \cdot \Phi_q'(\zeta) = q \cdot \zeta^{q-1} \qquad \text{mit} \quad \zeta_p := \zeta^{p^{\nu-1}}. \tag{6.9}$$

Um die Norm von $\Phi_q'(\zeta)$ zu berechnen, müssen wir also nur die Normen von $\zeta_p - 1$ und $q\zeta^{q-1}$ kennen. Beide Male können wir Lemma 4.7 dazu benutzen:

- Da das Minimalpolynom von ζ^{q-1} gerade Φ_q ist, folgt $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{q-1}) = 1$ (hier verwenden wir $q \neq 2$). Also gilt $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(q\zeta^{q-1}) = q^d = p^{\nu d}$.
- Das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist $\Phi_p = X^{p-1} + \ldots + 1$, also ist das Minimalpolynom von $\zeta_p - 1$ gerade $\Phi_p(X + 1)$, welches p als konstanten Koeffizienten hat. Es folgt also

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta_p - 1) = p^{d/(p-1)} = p^{p^{\nu-1}}.$$

Eingesetzt in (6.9) erhält man

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi_q'(\zeta)) = p^{\nu d - p^{\nu-1}} = p^m \qquad \text{mit} \quad m = p^{\nu-1}(\nu p - \nu - 1),$$

wie behauptet.

(2) Da

$$\Phi_q = X^{p^{\nu-1}(p-1)} + \ldots + X^{p^{\nu-1}} + 1 = \prod_{1 \leq a < q,\ p \nmid a} (X - \zeta^a),$$

folgt

$$p = \Phi_q(1) = \prod_{1 \leq a < q,\ p \nmid a} (1 - \zeta^a). \tag{6.10}$$

Für jedes $1 \leq a < q$ mit $p \nmid a$ gilt außerdem

$$1 - \zeta^a = \varepsilon_a \cdot (1 - \zeta) \qquad \text{für} \quad \varepsilon_a := \frac{1 - \zeta^a}{1 - \zeta} = \zeta^{a-1} + \ldots + \zeta + 1 \in \mathcal{O}_{\mathbb{Q}(\zeta)}. \tag{6.11}$$

Wir behaupten, dass $\varepsilon_a \in \mathcal{O}^*_{\mathbb{Q}(\zeta)}$ gilt. Dafür wählen wir $1 \leq b < q$ mit $ab \equiv 1 \pmod{q}$ und beobachten, dass

$$\varepsilon_a^{-1} = \frac{1-\zeta}{1-\zeta^a} = \frac{1-(\zeta^a)^b}{1-\zeta^a} = (\zeta^a)^{b-1} + \ldots + \zeta^a + 1 \in \mathcal{O}_{\mathbb{Q}(\zeta)}$$

gilt. Setzt man nun (6.11) in (6.10) ein, so bekommt man schließlich

$$p = \varepsilon \cdot \lambda^d \qquad \text{mit} \quad \varepsilon := \prod_{1 \leq a < q,\ p \nmid a} \varepsilon_a \in \mathcal{O}^*_{\mathbb{Q}(\zeta)}, \quad \lambda := 1 - \zeta.$$

Es folgt $(p) = (\lambda)^d$, wie behauptet. Der Zusatz, dass (λ) ein Primideal vom Trägheitsgrad 1 ist und p total verzweigt, folgt aus der fundamentalen Gleichung 4.39. □

Satz 6.17. *Sei p prim und $\nu \geq 1$, dann gilt $\mathcal{O}_{\mathbb{Q}(\zeta_{p^\nu})} = \mathbb{Z}[\zeta_{p^\nu}]$.*

Beweis. Wir können $p^\nu \neq 2$ annehmen und schreiben verkürzt $K := \mathbb{Q}(\zeta_{p^\nu})$. Nach Proposition 6.16 (1) gilt $d_{\mathbb{Z}[\zeta_{p^\nu}]} = \pm p^m$ für ein $m \in \mathbb{Z}_{>0}$, also mit Lemma 4.21 auch

$$p^m \mathcal{O}_K \subset \mathbb{Z}[\zeta_{p^\nu}] \subset \mathcal{O}_K. \tag{6.12}$$

Nach Proposition 6.16 (2) ist hat $(\lambda) = (1 - \zeta_{p^\nu})$ den Trägheitsgrad 1, also induziert die Einbettung $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ einen Isomorphismus

$$\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/(\lambda), \qquad x + p\mathbb{Z} \mapsto x + (\lambda).$$

Es folgt die Gleichheit

$$\mathcal{O}_K = \mathbb{Z} + \lambda \mathcal{O}_K$$

von $\mathbb{Z}$-Moduln. Insbesondere gilt auch

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^\nu}] + \lambda \mathcal{O}_K. \tag{6.13}$$

Wir erhalten

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^\nu}] + \lambda \mathcal{O}_K \overset{(6.13)}{=} \mathbb{Z}[\zeta_{p^\nu}] + \lambda \left(\mathbb{Z}[\zeta_{p^\nu}] + \lambda \mathcal{O}_K\right) = \mathbb{Z}[\zeta_{p^\nu}] + \lambda^2 \mathcal{O}_K.$$

Iteration des Einsetzens von (6.13) liefert also

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^\nu}] + \lambda^i \mathcal{O}_K \text{ für alle } i > 0.$$

Speziell für $i = m \cdot \varphi(p^\nu)$ bekommen wir wegen $(\lambda)^{\varphi(p^\nu)} = p\mathcal{O}_K$ (Proposition 6.16 (2)) schließlich

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^\nu}] + p^m \mathcal{O}_K \overset{(6.12)}{=} \mathbb{Z}[\zeta_{p^\nu}].$$

□

Wir verallgemeinern obiges Resultat zu allgemeinem n.

Satz 6.18. *Für $n \in \mathbb{Z}_{>0}$ ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.*

Beweis. Es ist klar, dass $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Für die umgekehrte Inklusion sei $n = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ die Primfaktorzerlegung[2] von n. Dann ist

$$\zeta_{(i)} := \zeta_n^{n/p_i^{\nu_i}} \text{ für } i = 1, \ldots, r$$

eine primitive $p_i^{\nu_i}$-te Einheitswurzel. Wegen

$$\mathrm{kgV}(p_1^{\nu_1}, \ldots, p_r^{\nu_r}) = n \qquad \text{und} \qquad \mathrm{ggT}(p_1^{\nu_1} \cdot \ldots \cdot p_{i-1}^{\nu_{i-1}}, p_i^{\nu_i}) = 1 \qquad \text{für} \quad i = 1, \ldots r$$

folgt mit Proposition 6.14:

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(1)}, \ldots, \zeta_{(r)}) \quad \text{und} \quad \mathbb{Q}(\zeta_{(1)}, \ldots, \zeta_{(i-1)}) \cap \mathbb{Q}(\zeta_{(i)}) = \mathbb{Q} \quad \text{für} \quad i = 1, \ldots, r.$$

Nach Satz 6.17 ist $\{1, \zeta_{(i)}, \ldots, \zeta_{(i)}^{\varphi(n/p_i^{\nu_i})-1}\}$ für jedes i eine Ganzheitsbasis von $\mathbb{Q}(\zeta_{(i)})$ über $\mathbb{Q}$. Nun besagt Proposition 6.16 (1), dass die Diskriminante von $\mathbb{Q}(\zeta_{(i)})$ bis auf ein Vorzeichen eine Potenz von p_i ist.

Durch sukzessives Anwenden von Satz 6.13 erhalten wir, dass

$$\left\{ \zeta_{(1)}^{j_1} \cdot \ldots \cdot \zeta_{(r)}^{j_r} \;\middle|\; \text{für alle } i = 1, \ldots, r \text{ gilt } 0 \le j_i < \varphi(n/p_i^{\nu_i}) - 1 \right\} \tag{6.14}$$

eine Ganzheitsbasis von $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ ist. Allerdings ist jedes der Elemente (6.14) eine Potenz von ζ_n. Demnach kann jedes $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ in der Form $g(\zeta_n)$ für ein Polynom $g \in \mathbb{Z}[X]$ geschrieben werden. □

Nun können wir das Zerlegungsgesetz formulieren und beweisen.

Satz 6.19. *Sei $n = \prod_{p \text{ prim}} p^{\nu_p}$ die Primfaktorzerlegung von $n \in \mathbb{Z}_{>0}$. Für eine Primzahl p setzen wir $n_{(p)} := n/p^{\nu_p}$. Weiter sei $f_p \ge 1$ minimal mit*

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

also $f_p = \mathrm{ord}_{(\mathbb{Z}/n_{(p)}\mathbb{Z})^*}(p)$. Dann gilt in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$:

$$p\mathcal{O}_{\mathbb{Q}(\zeta_n)} = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^{\varphi(p^{\nu_p})},$$

wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ paarweise verschiedene Primideale in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ sind, für die

$$f(\mathfrak{p}_1|p) = \ldots = f(\mathfrak{p}_r|p) = f_p \qquad \textit{und} \qquad e(\mathfrak{p}_1|p) = \ldots = e(\mathfrak{p}_r|p) = \varphi(p^{\nu_p})$$

gilt. Insbesondere gilt $r f_p = \varphi(n_{(p)})$ für alle Primzahlen p.

Beweis. Wegen $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ ist Satz 4.41 anwendbar. Sei p eine Primzahl und $\overline{\Phi}_n$ die Reduktion von Φ_n modulo p. Wir schreiben verkürzt $\nu = \nu_p$ und $f = f_p$. Gemäß dem zitierten Satz müssen wir zeigen, dass

$$\overline{\Phi}_n = (h_1 \cdot \ldots \cdot h_r)^{\varphi(p^\nu)} \tag{6.15}$$

mit paarweise verschiedenen irreduziblen Polynomen $h_1, \ldots, h_r \in \mathbb{F}_p[X]$ gilt, die allesamt denselben Grad (nämlich f_p) haben. Schreiben wir $\mu_m := \mu_m(\mathbb{Q}(\zeta_n))$, so wissen wir, dass

[2] Standard terms and conditions apply: Natürlich nehmen wir $p_i \neq p_j$ für $i \neq j$ sowie $\nu_1, \ldots, \nu_r \in \mathbb{Z}_{>0}$ an.

μ_m zyklisch ist (Bemerkung 6.2), und dass die Ordnung von μ_m ein Teiler von m ist. Wegen $\mathrm{ggT}(p^\nu, n_{(p)}) = 1$ und $n = p^\nu \cdot n_{(p)}$ gilt dann mit dem Chinesischen Restsatz

$$\mu_{p^\nu} \times \mu_{n_{(p)}} \cong \mu_n.$$

Ein Isomorphismus ist hierbei durch Multiplikation gegeben. Bezeichnen wir die Elemente von μ_{p^ν} mit ξ_i und die Elemente von $\mu_{n_{(p)}}$ mit η_j, so besteht μ_n also genau aus den Produkten der Form $\xi_i\eta_j$. Insbesondere gilt

$$\Phi_n = \prod_{i,j}(X - \xi_i\eta_j). \tag{6.16}$$

Wegen $X^{p^\nu} - 1 \equiv (X-1)^{p^\nu} \pmod{p}$ ist $\xi_i \equiv 1 \pmod{\mathfrak{p}}$ für alle Primideale $\mathfrak{p}$, die $p\mathbb{Z}[\zeta_n]$ teilen. Also folgt mit (6.16):

$$\Phi_n \equiv \prod_j (X - \eta_j)^{\varphi(p^\nu)} \equiv \Phi_{n_{(p)}}^{\varphi(p^\nu)} \pmod{\mathfrak{p}}.$$

Da Φ_n und $\Phi_{n_{(p)}}$ ganzzahlige Koeffizienten haben, folgt daraus auch

$$\Phi_n \equiv \Phi_{n_{(p)}}^{\varphi(p^\nu)} \pmod{p}.$$

Da $\varphi(n) = \varphi(n_{p'})\varphi(p^\nu)$, müssen wir die Behauptung (6.15) nur noch für $p \nmid n$ (also $n = n_{(p)}$) zeigen. In diesem Fall hat $X^n - 1$ keine mehrfachen Nullstellen im algebraischen Abschluss $\overline{\mathbb{F}}_p$ (da die Ableitung nX^{n-1} des Polynoms wegen $p \nmid n$ modulo p nicht null wird), weshalb die Abbildung

$$\mu_n \to \mu_n(\mathbb{Z}[\zeta_n]/\mathfrak{p}), \qquad \zeta \mapsto \overline{\zeta} := \zeta + \mathfrak{p}$$

für alle Primideale $\mathfrak{p} \mid p\mathbb{Z}[\zeta_n]$ ein Isomorphismus ist. Insbesondere ist $\overline{\zeta}_n$ immer noch eine primitive n-te Einheitswurzel. Wir behaupten, dass

$$\mathbb{F}_p(\overline{\zeta}_n) = \mathbb{F}_{p^f} \tag{6.17}$$

gilt. Eine notwendige Bedingung dafür, dass $\mathbb{F}_{p^k}$ die primitive n-te Einheitswurzel $\overline{\zeta}_n$ enthält, ist, dass $n \mid (p^k - 1)$. Da f minimal mit $n \mid (p^f - 1)$ gewählt war, muss nur noch gezeigt werden, dass $\mathbb{F}_{p^f}$ tatsächlich eine primitive n-te Einheitswurzel enthält. Hier bemerken wir, dass $\mathbb{F}_{p^f}^*$ nach Aufgabe 6.1.1 eine zyklische Gruppe der Ordnung $p^f - 1$ ist – bezeichnet $x \in \mathbb{F}_{p^f}^*$ einen Erzeuger, so ist

$$x^{(p^f-1)/n} \in \mathbb{F}_{p^f}^*$$

eine primitive n-te Einheitswurzel. Das beendet den Nachweis von (6.17).

Da Φ_n ein Teiler von $X^n - 1$ ist und keine mehrfachen Nullstellen modulo p hat, hat $\overline{\Phi}_n$ keine mehrfachen Nullstellen, zerfällt also in paarweise verschiedene irreduzible Faktoren. Jeder dieser irreduziblen Faktoren ist aber Minimalpolynom einer primitiven n-ten Einheitswurzel. Wie wir jedoch gesehen haben, liefert die Adjunktion einer primitiven n-ten Einheitswurzel an $\mathbb{F}_p$ eine Körpererweiterung vom Grad f.

Die letzte Aussage (also $rf = \varphi(n_{(p)})$) folgt mit der fundamentalen Gleichung 4.39

$$rf\varphi(p^\nu) = \varphi(n) = \varphi(p^\nu)\varphi(n_{(p)}),$$

indem man noch durch $\varphi(p^\nu)$ teilt. □

Korollar 6.20. *Sei $p \neq 2$ eine Primzahl, dann gilt*

(1) p ist in $\mathbb{Q}(\zeta_n)$ verzweigt $\iff p \mid n$,

(2) p ist in $\mathbb{Q}(\zeta_n)$ total zerfallend $\iff p \equiv 1 \pmod{n}$.

Beweis. Die erste Aussage folgt sofort aus der für Primzahlen $p \neq 2$ gültigen Aussage "$\varphi(p^{\nu_p}) \geq 2 \iff \nu_p > 0$". Die zweite Aussage folgt sofort aus der Äquivalenz "$\varphi(p^{\nu_p}) = f_p = 1 \iff p \equiv 1 \pmod{n}$" für $p \neq 2$. □

Für die Primzahl 2 haben wir folgendes Resultat:

Korollar 6.21.

(1) 2 ist in $\mathbb{Q}(\zeta_n)$ verzweigt $\iff 4 \mid n$,

(2) 2 ist in $\mathbb{Q}(\zeta_n)$ total zerfallend $\iff n \leq 2$.

Beweis. Beide Aussagen folgen sofort aus "$\varphi(2^k) \neq 1 \iff k \geq 2$", "$n_{(2)}$ ist ungerade" und dem Zerlegungsgesetz. □

6.2.1 Übungen

Aufgabe 6.2.1. Sei p eine ungerade Primzahl. Zeigen Sie, dass $\mathbb{Q}(\zeta_p)$ einen quadratischen Teilkörper $\mathbb{Q}(\sqrt{d})$ (wie immer $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei) enthält und bestimmen Sie d in Abhängigkeit von p.

6.3 Der große Satz von Fermat

Die *Fermat-Vermutung* besagt, dass die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine Lösung in $x, y, z \in \mathbb{Q} \setminus \{0\}$ besitzt. Er wurde Ende der 1990er Jahre von Andrew Wiles und Richard Taylor bewiesen. Wir wollen hier einen einfachen Spezialfall der Fermatschen Vermutung beweisen. Dafür starten wir mit einfachen Vorüberlegungen:

(1) Statt nach nicht-trivialen rationalen Lösungen kann man in der Fermat-Vermutung auch nach nicht-trivialen *ganzzahligen* Lösungen fragen. Diese beiden Formulierungen sind äquivalent, da man eine nicht-triviale rationale Lösung mit dem Hauptnenner durchmultiplizieren kann, um eine nicht-triviale ganzzahlige Lösung zu bekommen.

(2) Sind $x, y, z \in \mathbb{Z} \setminus \{0\}$ und $n \geq 3$ mit $x^n + y^n = z^n$, so gilt

$$\left(\frac{x}{\mathrm{ggT}(x,y,z)}\right)^n + \left(\frac{y}{\mathrm{ggT}(x,y,z)}\right)^n = \left(\frac{z}{\mathrm{ggT}(x,y,z)}\right)^n.$$

Wir können also $\mathrm{ggT}(x, y, z) = 1$ annehmen. Wegen $x^n + y^n = z^n$ ist das sogar äquivalent dazu, dass x und y (oder je zwei der Zahlen x, y, z) teilerfremd sind.

(3) Die Fermat-Vermutung für n impliziert für alle $m \geq 1$ die Fermat-Vermutung für mn: Bilden $x, y, z \in \mathbb{Z} \setminus \{0\}$ nämlich eine nicht-triviale Lösung zum Exponenten mn, so bilden y^m, y^m, z^m eine nicht-triviale Lösung zum Exponenten n:

$$(x^m)^n + (y^m)^n = x^{mn} + y^{mn} = z^{mn} = (z^m)^n.$$

Es genügt also, die Fermatsche Vermutung für $n = 4$ und Primzahlen $n \geq 3$ zu beweisen. Im Folgenden konzentrieren wir uns auf die Fermatsche Vermutung mit Primzahlexponenten, Sie werden den Fall $n = 4$ in Aufgabe 6.3.2 behandeln.

Klassischerweise unterscheidet man beim Beweis der Fermat-Vermutung für Primzahlen $p \geq 3$ zwei Fälle, wobei der erste Fall wesentlich leichter zu behandeln ist als der zweite Fall:

(1) $x^p + y^p = z^p$ hat keine Lösung $x, y, z \in \mathbb{Z} \setminus \{0\}$ mit $\mathrm{ggT}(x, y) = 1$ und $p \nmid xyz$.

(2) $x^p + y^p = z^p$ hat keine Lösung $x, y, z \in \mathbb{Z} \setminus \{0\}$ mit $\mathrm{ggT}(x, y) = 1$ und $p \nmid x, y$, aber $p \mid z$.

Bemerkung. Es ist $x^p + y^p = z^p$ äquivalent zu $x^p + (-z)^p = (-y)^p$, die Bedingung "$p \mid z$" im zweiten Fall der Fermat-Vermutung ist also willkürlich gewählt und kann auch durch "p teilt eine der drei Zahlen x, y, z" ersetzt werden.

Im Folgenden konzentrieren wir uns lediglich auf den ersten Fall der Fermat-Vermutung.

Lemma 6.22. *Der erste Fall der Fermat-Vermutung gilt für $p = 3$.*

Beweis. Die Gruppe $(\mathbb{Z}/9\mathbb{Z})^*$ ist zyklisch und hat die Ordnung $\varphi(9) = 6$. Ist also $a \in \mathbb{Z}$ mit $3 \nmid a$, so gilt $a^3 \equiv \pm 1 \pmod 9$. Gilt $3 \mid a$, so gilt $a^3 \equiv 0 \pmod 9$. Die dritten Potenzen modulo 9 sind also -1, 0 und 1.
Gäbe es nun eine nicht-triviale Lösung x, y, z von $x^3 + y^3 = z^3$ mit $3 \nmid xyz$, dann ist $x^3 + y^3 \equiv -2, 0, 2 \pmod 9$. Es folgt $z^3 \equiv 0 \pmod 9$ und damit insbesondere $3 \mid z$, ein Widerspruch. □

Bemerkung 6.23.

(1) Für $p = 5$ lässt sich der erste Fall der Fermat-Vermutung analog zu obigem Lemma durch Kongruenzen modulo 25 beweisen. Sie werden das in Aufgabe 6.3.3 tun.

(2) Für $p \equiv 1 \pmod 3$ existieren für jedes $\nu \geq 1$ ganze Zahlen x, y, z mit $p \nmid xyz$ und $x^p + y^p \equiv z^p \pmod{p^\nu}$. (Für den Nachweis nutzt man, dass der Ring $\mathbb{Z}_p$ der ganzen p-adische Zahlen primitive dritte Einheitswurzeln enthält. Wir verzichten auf einen detaillierten Beweis.) Somit lässt sich der erste Fall der Fermat-Vermutung für $p \equiv 1 \pmod 3$ nicht durch Kongruenzen modulo p^ν beweisen.

Im Folgenden seien nun stets p eine ungerade Primzahl, $x, y, z \in \mathbb{Z}$ paarweise teilerfremd mit $x^p + y^p = z^p$ und $p \nmid xyz$. Das Ziel ist es, daraus einen Widerspruch herzuleiten.

Sei $\zeta = \zeta_p \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Dann gilt

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

Proposition 6.24. *Die Ideale $(x + \zeta^i y)$, $i = 0, \ldots, p-1$ sind paarweise teilerfremd in $\mathbb{Z}[\zeta]$.*

Beweis. Für einen Widerspruch nehmen wir an, dass es ein Primideal $(0) \neq \mathfrak{p} \subset \mathbb{Z}[\zeta]$ gibt, das $(x + \zeta^i y)$ und $(x + \zeta^j y)$ für $0 \leq i < j \leq p - 1$ teilt, das heißt, die beiden Elemente $x + \zeta^i y$ und $x + \zeta^j y$ sind in $\mathfrak{p}$ enthalten. Dann ist die Differenz

$$\zeta^i y - \zeta^j y = \zeta^i (1 - \zeta^{j-i}) y$$

ebenfalls in $\mathfrak{p}$ enthalten. Wie im Beweis von Proposition 6.16 (2) können wir

$$\zeta^i(1-\zeta^{j-i}) = \varepsilon(1-\zeta)$$

für $\varepsilon \in \mathbb{Z}[\zeta]^*$ schreiben. Es folgt also, dass $\mathfrak{p}$ auch das Ideal $((1-\zeta)y)$ teilt. Da $(1-\zeta)$ prim ist (vgl. ebenfalls Proposition 6.16 (2)), erhalten wir die zwei Möglichkeiten

$$\mathfrak{p} = (1-\zeta) \qquad \text{oder} \qquad \mathfrak{p} \mid y\mathbb{Z}[\zeta].$$

Gilt $\mathfrak{p} \mid y\mathbb{Z}[\zeta]$, so gilt wegen $\mathfrak{p} \mid (x+\zeta^i y)$ dann auch $\mathfrak{p} \mid x\mathbb{Z}[\zeta]$, was der Teilerfremdheit von x und y widerspricht. Also gilt $\mathfrak{p} = (1-\zeta)$. Insbesondere liegt $\mathfrak{p}$ über p (auch das ist Inhalt von Proposition 6.16 (2)). Damit folgt

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

also $x + y \equiv 0 \pmod{p}$. Mit dem kleinen Satz von Fermat erhalten wir schließlich

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

also $p \mid z$ – wir behandeln jedoch den ersten Fall der Fermat-Vermutung, ein Widerspruch. □

Proposition 6.25. *Ist $\mathbb{Z}[\zeta]$ faktoriell, so gibt es eine Einheit $\varepsilon \in \mathcal{O}^*_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]^*$ und $\alpha \in \mathbb{Z}[\zeta]$ mit $x + \zeta y = \varepsilon\alpha^p$.*

Beweis. Es genügt, die Aussage "Ist $\pi \in \mathbb{Z}[\zeta]$ ein Primelement, sodass $\pi^k \mid\mid (x+\zeta y)$ gilt[3], dann ist k ein Vielfaches von p" zu beweisen. Sei also $\pi \in \mathbb{Z}[\zeta]$ ein Primelement, das $x + \zeta y$ teilt. Wegen $\prod_{i=0}^{p-1}(x+\zeta^i y) = z^p$ teilt π dann auch z. Sei $\nu \geq 1$ mit $\pi^\nu \mid\mid z$. Dann folgt $\pi^{p\nu} \mid\mid z^p$. Da die Ideale $(x+\zeta^i y)$ für $i = 0, \ldots, p-1$ nach Proposition 6.24 paarweise teilerfremd sind folgt $\pi^{\nu p} \mid\mid (x+\zeta y)$, woraus die Behauptung folgt. □

Über Einheiten von $\mathbb{Z}[\zeta]$ lässt sich noch mehr sagen. Anwenden werden wir das natürlich in Kombination mit Proposition 6.25.

Proposition 6.26. *Sei $p \geq 5$ eine Primzahl, $\zeta = \zeta_p \in \mathbb{C}$ und $\varepsilon \in \mathbb{Z}[\zeta]^*$. Dann gilt:*

(1) Es ist $\frac{\varepsilon}{\overline{\varepsilon}} = \zeta^a$ für ein $a \in \mathbb{Z}$.

(2) Es gibt eine reelle Einheit ε_0 (d.h. $\varepsilon_0 = \overline{\varepsilon}_0$) und ein $r \in \mathbb{Z}$, sodass $\varepsilon = \varepsilon_0\zeta^r$.

Vor dem Beweis merken wir an, dass die Aussagen der Proposition auch für $p = 3$ gültig sind. Der Einheitensatz 5.34 impliziert aber, dass $\mathbb{Z}[\zeta_3]^*$ nur aus Einheitswurzeln besteht, deshalb sind die Aussagen in diesem Fall uninteressant.

Beweis. (1) Nach Satz 6.5 ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoissch mit abelscher Galoisgruppe. Da die komplexe Konjugation in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ enthalten ist, gilt für alle $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ damit

$$\left|\tau\left(\frac{\varepsilon}{\overline{\varepsilon}}\right)\right| = \left|\frac{\tau(\varepsilon)}{\tau(\overline{\varepsilon})}\right| = \left|\frac{\tau(\varepsilon)}{\overline{\tau(\varepsilon)}}\right| = 1.$$

[3] Diese Notation bedeutet: $\pi^k \mid (x+\zeta y)$, aber $\pi^{k+1} \nmid (x+\zeta y)$.

Nach Kroneckers Lemma 5.30 ist $\varepsilon/\overline{\varepsilon}$ also eine Einheitswurzel. Mit Proposition 6.15 folgt, dass es ein $a \in \mathbb{Z}$ gibt, sodass

$$\frac{\varepsilon}{\overline{\varepsilon}} = \pm\zeta^a.$$

Wir müssen zeigen, dass ein "$-$" hier nicht auftreten kann. Nehmen wir für einen Widerspruch an, dass $\varepsilon/\overline{\varepsilon} = -\zeta^a$ und schreiben

$$\varepsilon = b_0 + b_1\zeta + \ldots + b_{p-2}\zeta^{p-2} \qquad \text{für} \quad b_0, \ldots, b_{p-2} \in \mathbb{Z},$$

so erhalten wir $\overline{\varepsilon} = b_0 + b_1\zeta^{p-1} + \ldots + b_{p-2}\zeta^2$ und damit

$$\overline{\varepsilon} \equiv \varepsilon \overset{\text{Annahme}}{\equiv} -\zeta^a\overline{\varepsilon} \equiv -\overline{\varepsilon} \pmod{(1-\zeta)}.$$

Es folgt damit $2\overline{\varepsilon} \equiv 0 \pmod{(1-\zeta)}$, also $(1-\zeta) \mid 2$ (da $\overline{\varepsilon}$ eine Einheit ist), im Widerspruch zu $(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$, vgl. Proposition 6.16 (2).

(2) Sei $a \in \mathbb{Z}$, sodass $\varepsilon/\overline{\varepsilon} = \zeta^a$. Da p ungerade ist, gibt es ein $r \in \mathbb{Z}$ mit $2r \equiv a \pmod{p}$. Hieraus bekommt man nun sofort $\varepsilon = \zeta^{2r}\overline{\varepsilon}$ und $\varepsilon = \varepsilon_0\zeta^r$ mit

$$\varepsilon_0 := \zeta^{-r}\varepsilon = \zeta^r\overline{\varepsilon} = \overline{\varepsilon}_0.$$

□

Bemerkung 6.27. Sei $p \geq 5$. Dann gibt es keine teilerfremden $x, y, z \in \mathbb{Z} \setminus \{0\}$, die gleichzeitig $x \equiv y \equiv -z \pmod{p}$ und $x^p + y^p = z^p$ erfüllen. Aus den Voraussetzungen folgt nämlich $3z^p \equiv 0 \pmod{p}$, und wegen $p \geq 5$ dann auch $p \mid z$, woraus man auch $p \mid x$ und $p \mid y$ abliest. Befinden wir uns also im ersten Fall der Fermat-Vermutung, so ist mindestens eine der Kongruenzen

$$x \equiv y \pmod{p}, \qquad x \equiv -z \pmod{p}, \qquad y \equiv -z \pmod{p}$$

verletzt. Da $x^p+y^p = z^p$ auch zu $x^p+(-z)^p = (-y)^p$ und $y^p+(-z)^p = (-x)^p$ äquivalent ist, können wir ohne Einschränkung annehmen, dass $x \not\equiv y \pmod{p}$.

Nun kommen wir zum versprochenen Satz.

Satz 6.28. *Sei $p \geq 3$ eine Primzahl mit der Eigenschaft, dass $\mathbb{Z}[\zeta]$ faktoriell ist. Dann hat die Gleichung $x^p + y^p = z^p$ keine nicht-triviale Lösung mit $p \nmid xyz$.*

Beweis. Da der Fall $p = 3$ in Lemma 6.22 behandelt wurde, dürfen wir $p \geq 5$ annehmen. Für einen Widerspruch nehmen wir wie wie immer an, dass $x, y, z \in \mathbb{Z} \setminus \{0\}$ mit, $p \nmid xyz$ und $x^p + y^p = z^p$ existieren. Im Hinblick auf Bemerkung 6.27 dürfen wir auch $x \not\equiv y \pmod{p}$ annehmen. Nach Proposition 6.25 können wir

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

mit $\varepsilon \in \mathbb{Z}[\zeta]^*$ und $\alpha \in \mathbb{Z}[\zeta]$ schreiben. (Hierfür benötigen wir die Voraussetzung, dass $\mathbb{Z}[\zeta]$ faktoriell ist!) Mit Proposition 6.26 folgt dann

$$x + \zeta y = \varepsilon\alpha^p = \zeta^r\varepsilon_0\alpha^p, \tag{6.18}$$

wobei $\varepsilon_0 \in \mathbb{Z}[\zeta]^*$ eine reelle Einheit ist. Da $\alpha \in \mathbb{Z}[\zeta]$, gibt es ganze Zahlen $a_0, \ldots, a_{p-2}$ mit

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}.$$

Wegen der Gültigkeit des Freshman's Dream in Charakteristik p und wegen $\zeta^p = 1$ folgt

$$\alpha^p \equiv \underbrace{a_0^p + \ldots + a_{p-2}^p}_{=:a \in \mathbb{Z}} \pmod{p}. \tag{6.19}$$

Zusammen mit (6.18) erhalten wir somit

$$x + \zeta y \equiv \zeta^r \varepsilon_0 a \pmod{p}. \tag{6.20}$$

Andererseits gilt

$$x + \zeta^{-1} y = \overline{x + \zeta y} \equiv \zeta^{-r} \varepsilon_0 a \pmod{p}. \tag{6.21}$$

Mit Hilfe von (6.20) und (6.21) berechnen wir nun

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

also nach Umstellen und Ausmultiplizieren

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \pmod{p}. \tag{6.22}$$

Wir unterscheiden nun vier Fälle anhand dessen, welche der Einheitswurzeln $1,\ \zeta,\ \zeta^{2r}$ und ζ^{2r-1} zusammenfallen:

Fall 1: Wenn $1, \zeta, \zeta^{2r}$ und ζ^{2r-1} paarweise verschieden sind, so kann die vierelementige Menge $\{1,\ \zeta,\ \zeta^{2r},\ \zeta^{2r-1}\}$ zu einer $\mathbb{Z}$-Basis von $\mathbb{Z}[\zeta]$ ergänzt werden, denn aufgrund von $1 + \zeta + \ldots + \zeta^{p-1} = 0$ ist jede Teilmenge der Kardinalität $p-1$ von $\{1, \ldots, \zeta^{p-1}\}$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\zeta]$. Somit sind die Bilder von $\{1,\ \zeta,\ \zeta^{2r},\ \zeta^{2r-1}\}$ in $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ Teil einer $\mathbb{F}_p$-Basis ebendieses Vektorraumes. Aus (6.22) folgt nun jedoch $x \equiv y \equiv 0 \pmod{p}$, ein Widerspruch zur Annahme $p \nmid xyz$.

Fall 2: Wenn $\zeta^{2r} = 1$, so lässt sich (6.22) zu

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

umschreiben. Da ζ eine Einheit modulo p ist, folgt

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

und damit auch $p \mid y$, da $(1-\zeta^{-2}) = (1-\zeta)$ und $p\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}$ nach Proposition 6.16 (2). Wir erhalten erneut einen Widerspruch zur Annahme $p \nmid xyz$.

Fall 3: Ist $\zeta^{2r-1} = \zeta$, so folgt aus (6.22) wie im vorherigen Fall $x(1 - \zeta^2) \equiv 0 \pmod{p}$ und damit analog der Widerspruch $p \mid x$.

Fall 4: Wenn $\zeta^{2r-1} = 1$ (was äquivalent zu $\zeta^{2r} = \zeta$ ist), dann liefert Gleichung (6.22)

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

also $x - y \equiv 0 \pmod{p}$ (da $1 - \zeta$ ein echter Teiler von p ist, wie jetzt schon mehrfach benutzt). Jedoch waren x und y so gewählt, dass $x \not\equiv y \pmod{p}$, ein Widerspruch. □

Bemerkung 6.29. Es scheint so, als hätten wir den ersten Fall der Fermat-Vermutung jetzt für viele Primzahlen bewiesen. Ist das wirklich so? Leider nein! Ein Resultat von Montgomery und Uchida von 1964 besagt nämlich, dass $\mathbb{Z}[\zeta_p]$ genau dann faktoriell ist, wenn $p \leq 19$ ist.

Kummer bemerkte jedoch, dass die Voraussetzung "$\mathbb{Z}[\zeta_p]$ ist faktoriell" abgeschwächt werden kann.

Definition 6.30. Eine Primzahl $p \neq 2$ heißt *regulär*, wenn sie die Klassenzahl $h_{\mathbb{Q}(\zeta_p)}$ von $\mathbb{Q}(\zeta_p)$ nicht teilt.

Bemerkung 6.31. Im Hinblick auf Bemerkung 6.29 sind alle ungeraden Primzahlen ≤ 19 regulär. Die folgende Liste zeigt die regulären Primzahlen bis 100:

3, 5 , 7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 61, 71, 73, 79, 83, 89, 97.

Man sieht, dass es davon wesentlich mehr gibt, als nur die ungeraden Primzahlen bis 19. Wie die Folge der regulären Primzahlen weitergeht, können Sie unter A007703 in der OEIS einsehen.

Satz 6.32 (Kummer)**.** *Ist p eine reguläre Primzahl, so gilt der erste Fall der Fermat-Vermutung für p.*

Beweis. Im Beweis von Satz 6.28 wurde die Voraussetzung "$\mathbb{Z}[\zeta_p]$ ist faktoriell" lediglich benutzt, um $x + \zeta_p y = \varepsilon\alpha^p$ mit $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ und $\alpha \in \mathbb{Z}[\zeta_p]$ schreiben zu können (vgl. auch Proposition 6.25). Wenn wir also zeigen können, dass man $x + \zeta_p y$ auch für reguläre Primzahlen p in einer solchen Form schreiben können, sind wir fertig.

Wir schreiben wie üblich

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

Ist $z\mathbb{Z}[\zeta_p] = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die Primidealzerlegung, so folgt die Idealgleichung

$$z^p\mathbb{Z}[\zeta] = (z\mathbb{Z}[\zeta])^p = (\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r})^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y). \tag{6.23}$$

Nach Proposition 6.24 sind die Hauptideale $(x + \zeta_p^i y)$ paarweise teilerfremd. Zusammen mit Gleichung (6.23) impliziert das, dass jedes der Ideale $(x + \zeta_p^i y)$ die p-te Potenz eines Ideals von $\mathbb{Z}[\zeta]$ ist. Insbesondere gilt das für $i = 1$, d.h. $(x + \zeta_p y) = \mathfrak{a}^p$ für ein Ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta_p]$. Da $\mathfrak{a}^p$ ein Hauptideal ist, gilt also

$$[\mathfrak{a}]^p = [\mathfrak{a}^p] = [\mathbb{Z}[\zeta_p]] \in \mathrm{Cl}_{\mathbb{Q}(\zeta)}\,.$$

Die Ordnung von $[\mathfrak{a}]$ in der Klassengruppe ist also 1 oder p. Als reguläre Primzahl teilt p jedoch die Klassenzahl von $\mathbb{Q}(\zeta)$ nicht, das heißt, dass $\mathfrak{a} = (\alpha)$ ein Hauptideal sein muss. Da $(x + \zeta_p y) = \mathfrak{a}^p = (\alpha^p)$, muss es also eine Einheit $\varepsilon \in \mathbb{Z}[\zeta]^*$ mit $x + \zeta_p y = \varepsilon\alpha^p$ geben, wie behauptet. □

Bemerkung 6.33. Klassenzahlen bzw. -gruppen sind schwierig zu berechnen – wie findet man also möglichst effizient heraus, ob eine gegebene Primzahl $p \neq 2$ regulär

ist? Überraschenderweise gibt es das folgende, verhältnismäßig leichte Kriterium für die Regularität einer Primzahl: Definiere die *Bernoulli-Zahlen* B_k für $k \in \mathbb{Z}_{\geq 0}$ durch[4]

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

Es ist nicht schwer zu zeigen, dass alle B_k rationale Zahlen sind. Schreiben wir

$$B_k = \frac{a_k}{b_k} \qquad \text{mit} \quad a_k \in \mathbb{Z}, b_k \in \mathbb{Z}_{>0} \text{ und } \operatorname{ggT}(a_k, b_k) = 1,$$

so gilt für eine Primzahl $p \neq 2$ die folgende wundersame Aussage:

$$p \text{ ist regulär} \iff \text{für alle } k \in \{2, 4, 6, \ldots, p-3\} \text{ gilt: } p \nmid a_k.$$

Beispielsweise gilt $B_{12} = -\frac{691}{2730}$, also ist die Primzahl 691 irregulär. (Der Beweis der Äquivalenz der beiden Definitionen ist natürlich – wie zu erwarten – aufwendig.)

Bemerkung 6.34. Für $x \in \mathbb{R}$ bezeichne $\pi(x)$ bzw. $\pi_{\text{reg}}(x)$ die Anzahl der Primzahlen bzw. regulären Primzahlen $\leq x$. Eine noch weit offene Vermutung von Siegel (1964) besagt, dass

$$\limsup_{x \to \infty} \frac{\pi_{\text{reg}}(x)}{\pi(x)} = e^{-1/2} \approx 0,6065$$

gilt. Mit anderen Worten: Es wird vermutet, dass etwa 60,65% aller Primzahlen regulär sind. Fragen Sie mich nicht, aus welchen Heuristiken der Wert $e^{-1/2}$ entspringt – ich habe keine Ahnung. Zum heutigen Tage ist nämlich noch nicht einmal bekannt, ob es überhaupt unendlich viele reguläre Primzahlen gibt. Es ist jedoch bewiesen, dass es unendlich viele irreguläre Primzahlen gibt.

Bemerkung 6.35. Wir haben in (6.19) im Beweis von Satz 6.28 gesehen, dass p-te Potenzen von Elementen in $\mathbb{Z}[\zeta_p]$ modulo p kongruent zu ganzen Zahlen sind. Die Umkehrung gilt zwar nicht, aber es gilt Kummers Lemma:

Ist p reguläre Primzahl und $u \in \mathbb{Z}[\zeta_p]^*$ modulo p kongruent zu einer ganzen Zahl, so gibt es $v \in \mathbb{Z}[\zeta_p]^*$ mit $u = v^p$.

Im Beweis von Kummers Lemma muss eine Verbindung zwischen den Einheiten von $\mathbb{Z}[\zeta_p]$ und der Klassenzahl $h_{\mathbb{Q}(\zeta_p)}$ hergestellt werden – man kann sich also vorstellen, dass der Beweis etwas aufwendiger ist. Wir verzichten deshalb an dieser Stelle auf einen Beweis. Dennoch möchten wir bemerken, dass Kummers Lemma genutzt werden kann, um Fall (2) des großen Satzes von Fermat für reguläre Primzahlen zu beweisen. Der Vollständigkeit halber haben wir den Beweis des zweiten Falls der Fermat-Vermutung im folgenden Unterkapitel, Abschnitt **??**, ausformuliert.
Im Vergleich zum Beweis der Fermat-Vermutung in Gänze (d.h. auch für nicht-reguläre Primzahlen) sind Kummers Lemma und die Methoden dieses Kapitels jedoch eher mit dem Einmaleins zu vergleichen.

[4]Beachte: Die auf $\mathbb{R} \setminus \{0\}$ definierte Funktion $t \mapsto \frac{t}{e^t - 1}$ kann in 0 analytisch fortgesetzt werden, deshalb ergibt die Taylorentwicklung Sinn.

6.3.1 Übungen

Aufgabe 6.3.1. Sei $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ die Einheitskreislinie. Zeigen Sie, dass jeder Punkt $(x_0, y_0) \in S^1 \cap \mathbb{Q}^2$ in der Form

$$x_0 = \frac{u^2 - v^2}{u^2 + v^2}, \qquad y_0 = \frac{2uv}{u^2 + v^2}$$

mit $u, v \in \mathbb{Z}$ geschrieben werden kann.
Hinweis: Betrachten Sie die Geraden $y = t(x - 1)$ für $t \in \mathbb{Q}$.

Aufgabe 6.3.2. Beweisen Sie die Fermatsche Vermutung für $n = 4$.

Aufgabe 6.3.3. Beweisen Sie den ersten Fall der Fermatschen Vermutung für $p = 5$.

Aufgabe 6.3.4. Zeigen Sie ausgehend von der Definition regulärer Primzahlen anhand der Bernoulli-Zahlen (vgl. Bemerkung 6.33), dass es unendlich viele irreguläre Primzahlen gibt.

Kapitel 7

Hilbertsche Verzeigungstheorie

Im vorherigen Kapitel haben wir das Zerlegungsgesetz 6.19 für Kreisteilungskörper bewiesen. Inhalt des Zerlegungsgesetzes ist unter anderem, dass alle Primideale von $\mathbb{Z}[\zeta_n]$, die über einer gegebenen Primzahl liegen, die gleichen Verzweigungsindizes und Trägheitsgrade haben. Dabei handelt es sich natürlich nicht um Zufall, sondern um ein Resultat der *Hilbertschen Verzweigungstheorie*, die wir in diesem Kapitel entwickeln und diskutieren möchten.

Das grundlegende Setup innerhalb des gesamten Kapitels sei wie folgt. Es sei L/K eine Galoiserweiterung von Zahlkörpern vom Grad $n = [L : K]$. Mit $G = \mathrm{Gal}(L/K)$ sei die Galoisgruppe der Erweiterung bezeichnet. Wir fixieren außerdem eine Einbettung $L \subset \mathbb{C}$. Aus der Körpererweiterung $K \subset L$ erhalten wir eine Ringerweiterung $\mathcal{O}_K \subset \mathcal{O}_L$. Das folgende Lemma ist der Startpunkt der Verzweigungstheorie.

Lemma 7.1. *Die Galoisgruppe G operiert in natürlicher Weise auf $\mathcal{O}_L$.*

Beweis. Sei $\sigma \in G$. Ist $\alpha \in \mathcal{O}_L$ mit Minimalpolynom $m_\alpha \in \mathbb{Z}[X]$ über $\mathbb{Q}$ gegeben, dann ist $\sigma(\alpha)$ wieder eine Nullstelle von m_α, also $\sigma(\alpha) \in \mathcal{O}_L$. □

Korollar 7.2. *Ist $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal und $\sigma \in G$, so ist $\sigma(\mathfrak{P})$ wieder ein Primideal von $\mathcal{O}_L$.*

Beweis. Die Abbildung $\sigma|_{\mathcal{O}_L} : \mathcal{O}_L \to \mathcal{O}_L$ ist ein Automorphismus von $\mathcal{O}_L$. □

Definition 7.3. Die Ideale $\sigma(\mathfrak{P})$ ($\sigma \in G$) heißen die zu $\mathfrak{P}$ *konjugierten* Primideale von $\mathcal{O}_L$.

Das führt zur folgenden Frage: Wir fixieren ein Primideal $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ und das von $\mathfrak{p}$ erzeugte Ideal $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$. Dieses hat eine Primfaktorisierung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}, \qquad e_j \geq 1.$$

Wie verhält sich diese Zerlegung unter der Wirkung der Galoisgruppe G?

Satz 7.4. *Die Galoisgruppe G operiert transitiv auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$.*

Beweis. Wir stellen zunächst fest, dass G auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ operiert, da für $\sigma \in G$ gilt, dass $\sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{p})\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$.
Um die Transitivität der Operation zu beweisen, nehmen wir für einen Widerspruch an,

dass es $i \neq j$ mit $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$ für alle $\sigma \in G$ gibt. Der Chinesische Restsatz garantiert dann die Existenz von $\beta \in \mathcal{O}_L$ mit $\beta \equiv 0 \pmod{\mathfrak{P}_j}$ und $\beta \equiv 1 \pmod{\sigma(\mathfrak{P}_i)}$ für alle $\sigma \in G$. Man erhält dann

$$N_{L/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta) = \underbrace{\beta}_{\in \mathfrak{P}_j} \cdot \prod_{\sigma \in G \setminus \{\mathrm{id}_L\}} \sigma(\beta) \in \mathfrak{P}_j \cap \mathcal{O}_K = \mathfrak{p}.$$

Andererseits ist β in keinem der $\sigma(\mathfrak{P}_i)$ enthalten. Da $\mathfrak{P}_i$ ein Primideal ist, folgt also der gewünschte Widerspruch

$$\prod_{\sigma \in G} \sigma(\beta) \notin \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}.$$

□

Im weiteren Verlauf werden wir den Stabilisator der Wirkung von G auf der Menge der Primideale von $\mathcal{O}_L$ genau studieren.

Definition 7.5. Sei $\mathfrak{P} \subset \mathcal{O}_L$ eines der Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$.

(1) Der Stabilisator

$$G_{\mathfrak{P}} := D(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

heißt *Zerlegungsgruppe* von $\mathfrak{P}$ über K.

(2) Der Fixkörper $Z_{\mathfrak{P}} := L^{G_{\mathfrak{P}}} = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G_{\mathfrak{P}}\}$ heißt der zu $\mathfrak{P}$ gehörige *Zerlegungskörper*.

Bemerkung 7.6.

(1) Nach dem Hauptsatz der Galoistheorie haben wir $K \subset Z_{\mathfrak{P}} \subset L$ und dass $L/Z_{\mathfrak{P}}$ galoissch mit der Galoisgruppe $G_{\mathfrak{P}}$ ist.

(2) Für $\sigma \in G$ gilt $\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\sigma(\mathfrak{P})}$.

(3) Nach Satz 7.4 operiert G transitiv auf der Menge $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ der Primideale über $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$. Wir erhalten demnach für jedes $i \in \{1, \ldots, r\}$ eine Bijektion

$$\begin{aligned} \varphi_i \colon G/G_{\mathfrak{P}_i} &\to \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}, \\ \sigma G_{\mathfrak{P}_i} &\mapsto \sigma(\mathfrak{P}_i). \end{aligned}$$

Die Abbildungen φ_i sind verträglich mit der G-Operation, das heißt für $\tau, \sigma \in G$ gilt

$$\tau(\varphi_i(\sigma G_{\mathfrak{P}_i})) = \varphi_i(\tau\sigma\mathfrak{P}_i).$$

Wir erhalten sofort:

Korollar 7.7. *Sei* $(0) \neq \mathfrak{P} \subset \mathcal{O}_L$ *und* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. *Sei* $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$ *die Primfaktorisierung. Dann gilt:*

(1) $[K : Z_{\mathfrak{P}}] = (G : G_{\mathfrak{P}}) = r$,

(2) $G_{\mathfrak{P}} = \{\mathrm{id}_L\} \iff Z_{\mathfrak{P}} = L \iff r = n$, *d.h.* $\mathfrak{p}$ *zerfällt in* L *total,*

(3) $G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff r = 1$, *d.h.* $\mathfrak{p}$ *ist in* L unzerlegt.

Beweis. Die erste Aussage folgt sofort aus Bemerkung 7.6 (3) und Galoistheorie, die anderen beiden Aussagen folgen sofort aus Galoistheorie und der ersten Aussage. □

Satz 7.8. *Sei* $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ *ein Primideal und* $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$ *die Primfaktorisierung. Schreibe außerdem* $f_i := f(\mathfrak{P}_i|\mathfrak{p})$*. Dann gilt*

$$e_1 = \ldots = e_r \qquad \text{und} \qquad f_1 = \ldots = f_r.$$

Für $e := e_i$ *und* $f := f_i$ *gilt also insbesondere* $n = r \cdot e \cdot f$*.*

Beweis. Für jedes $\sigma \in G$ und jedes $\mathfrak{P} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ haben wir ein kommutatives Diagramm von Vektorräumen über $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$:

$$\begin{array}{ccc} \mathcal{O}_L/\mathfrak{P} & \longrightarrow & \mathcal{O}_L/\sigma(\mathfrak{P}) \\ \uparrow & & \uparrow \\ k(\mathfrak{p}) & = & k(\mathfrak{p}) \end{array}$$

Hierbei ist $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\sigma(\mathfrak{P})$ der durch σ induzierte Isomorphismus von Vektorräumen über $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$. Es folgt

$$f(\mathfrak{P}|\mathfrak{p}) \overset{\text{Def.}}{=} \dim_{k(\mathfrak{p})}(\mathcal{O}_L/\mathfrak{P}) = \dim_{k(\mathfrak{p})}(\mathcal{O}_L/\sigma(\mathfrak{P})) \overset{\text{Def.}}{=} f(\sigma(\mathfrak{P})|\mathfrak{p}).$$

Aus der Transitivität der G-Operation auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ (siehe Satz 7.4) folgt somit $f_1 = \ldots = f_r$. Die verbleibende Aussage $e_1 = \ldots = e_r$ folgt ebenfalls aus der Transitivität und der Beobachtung

$$\mathfrak{P}^\nu \text{ teilt } \mathfrak{p}\mathcal{O}_L \iff \sigma(\mathfrak{P}^\nu) = \sigma(\mathfrak{P})^\nu \text{ teilt } \sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L.$$

Die Gleichung $n = r \cdot e \cdot f$ folgt nun aus der fundamentalen Gleichung 4.39. □

Warum heißen Zerlegungskörper eigentlich Zerlegungskörper?

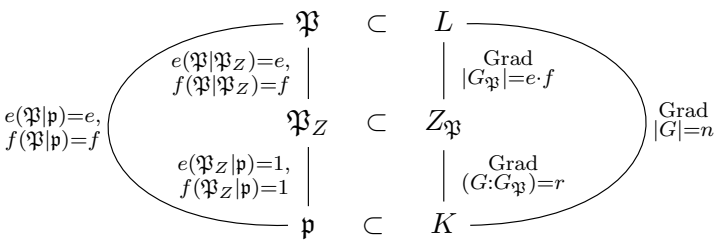
Satz 7.9. *Sei* $(0) \neq \mathfrak{P} \subset \mathcal{O}_L$ *ein Primideal,* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ *und* $\mathfrak{P}_Z := \mathfrak{P} \cap Z_\mathfrak{P}$*.*

(1) Es ist $\mathfrak{P}_Z$ *unzerlegt in* $L/Z_\mathfrak{P}$*, d.h.* $\mathfrak{P}_Z\mathcal{O}_L$ *ist eine Potenz von* $\mathfrak{P}$*,*

(2) Es gilt:

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{P}_Z) &= e, & f(\mathfrak{P}|\mathfrak{P}_Z) &= f, \\ e(\mathfrak{P}_Z|\mathfrak{p}) &= 1, & f(\mathfrak{P}_Z|\mathfrak{p}) &= 1. \end{aligned}$$

In einem Diagramm kann das Ergebnis des Satzes wie folgt zusammengefasst werden:



Es ist allerdings zu beachten, dass der Zerlegungskörper $Z_{\mathfrak{P}}$ von $\mathfrak{P}$ und nicht nur von $\mathfrak{p}$ abhängt. Die Primfaktorisierung von $\mathfrak{p}\mathcal{O}_{Z_{\mathfrak{P}}}$ enthält neben dem Faktor $\mathfrak{P}_Z$ (mit Verzweigungsindex 1 und Trägheitsindex 1) meist noch andere Faktoren, über die wir im Allgemeinen nichts sagen können (vgl. auch die Darstellungen unter Satz 7.14).

Beweis. (1) Da $Z_{\mathfrak{P}} = L^{G_{\mathfrak{P}}}$, gilt $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. Definitionsgemäß gilt außerdem für alle $\sigma \in G_{\mathfrak{P}}$, dass $\sigma(\mathfrak{P}) = \{\mathfrak{P}\}$. Da die Galoisgruppe $G_{\mathfrak{P}}$ transitiv auf der Menge der Primideale von $\mathcal{O}_L$ über $\mathfrak{P}_Z$ operiert (Satz 7.4), folgt die Aussage.

(2) Aus Satz 7.8, Korollar 7.7 und Galoistheorie erhalten wir

$$|G| = n = r \cdot e \cdot f,$$

wobei $r = (G : G_{\mathfrak{P}}) = [Z_{\mathfrak{P}} : K]$. Da also $|G| = |G_{\mathfrak{P}}| \cdot r$, folgt auch

$$|G_{\mathfrak{P}}| = e \cdot f = [L : Z_{\mathfrak{P}}]. \tag{7.1}$$

Außerdem gilt

$$e \cdot f \overset{(7.1)}{=} [L : Z_{\mathfrak{P}}] \overset{(1),\ \text{fund. Gl.}}{=} e(\mathfrak{P}|\mathfrak{P}_Z) \cdot f(\mathfrak{P}|\mathfrak{P}_Z). \tag{7.2}$$

Andererseits gilt nach Aufgabe 4.6.6 auch

$$e = e(\mathfrak{P}|\mathfrak{P}_Z) \cdot e(\mathfrak{P}_Z|\mathfrak{p}) \qquad \text{und} \qquad f = f(\mathfrak{P}|\mathfrak{P}_Z) \cdot f(\mathfrak{P}_Z|\mathfrak{p}),$$

was zusammen mit (7.2) nun $e(\mathfrak{P}|\mathfrak{P}_Z) = e$, $f(\mathfrak{P}|\mathfrak{P}_Z) = f$ und $e(\mathfrak{P}_Z|\mathfrak{p}) = f(\mathfrak{P}_Z|\mathfrak{p}) = 1$ beweist. □

Als nächstes möchten wir die Frage beantworten, wie sich die Zerlegungsgruppen verhalten, wenn wir zu einem Zwischenkörper übergehen.

Lemma 7.10. *Sei L' ein Zwischenkörper von L/K. Sei wie üblich $(0) \neq \mathfrak{P} \subset \mathcal{O}_L$ ein Primideal und $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Dann gilt mit $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{L'}$ und $G' = \mathrm{Gal}(L/L')$:*

(1) $G'_{\mathfrak{P}} = G_{\mathfrak{P}} \cap G'$,

(2) $G_{\mathfrak{P}} \subset G' \iff L' \subset Z_{\mathfrak{P}} \iff e(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p}) = 1$.

(3) Wenn L'/K galoissch ist und $\overline{G}_{\mathfrak{P}'} \subset \overline{G} := \mathrm{Gal}(L'/K)$ die Zerlegungsgruppe von $\mathfrak{P}'$ über K ist, so ist $\overline{G}_{\mathfrak{P}'}$ das Bild von $G_{\mathfrak{P}}$ unter der kanonischen Projektion $G \to \overline{G}$, $\sigma \mapsto \sigma|_{L'}$.

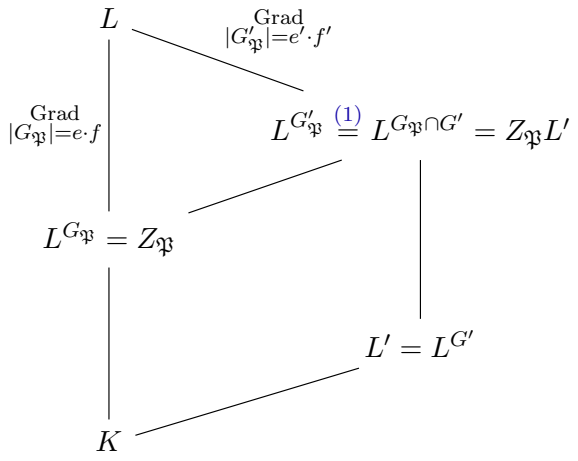
Beweis. (1) Es gilt definitionsgemäß

$$G'_{\mathfrak{P}} = \{\sigma \in G' \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} = \{\sigma \in G \mid \sigma \in G' \text{ und } \sigma(\mathfrak{P}) = \mathfrak{P}\} = G' \cap G_{\mathfrak{P}}.$$

(2) Die Galoiskorrespondenz liefert

$$G_{\mathfrak{P}} \subset G' \iff L' = L^{G'} \subset L^{G_{\mathfrak{P}}} = Z_{\mathfrak{P}}.$$

Für die zweite Äquivalenz betrachten wir das folgende Diagramm von Körpern, wobei wir $e' := e(\mathfrak{P}|\mathfrak{P}')$, $f' := f(\mathfrak{P}|\mathfrak{P}')$ schreiben:



Dass die Körpergrade wie angegeben sind, folgt beispielsweise aus dem Beweis von Satz 7.9. Das Diagramm zeigt:

$$L' \subset Z_{\mathfrak{P}} \iff L^{G'_{\mathfrak{P}}} = Z_{\mathfrak{P}} \iff e \cdot f = e' \cdot f' \overset{(*)}{\iff} e = e' \text{ und } f = f'.$$

Hierbei folgt Schritt $(*)$ erneut aus Aufgabe 4.6.6). Dieselbe Aufgabe impliziert jedoch auch

$$e(\mathfrak{P}'|\mathfrak{p}) = \frac{e}{e'} \qquad \text{und} \qquad f(\mathfrak{P}'|\mathfrak{p}) = \frac{f}{f'},$$

woraus wir die Behauptung ablesen.

(3) Sei $\sigma \in G$ und $\overline{\sigma} = \sigma|_{L'} \in \overline{G}$. Dann gilt:

$$\sigma \in G_{\mathfrak{P}} \overset{\text{Def.}}{\iff} \sigma(\mathfrak{P}) = \mathfrak{P} \overset{(**)}{\implies} \sigma(\mathfrak{P}') = \mathfrak{P}',$$

also $\overline{\sigma} \in \overline{G}_{\mathfrak{P}'}$. In Schritt $(**)$ wurde hierbei benutzt, dass L'/K galoissch ist, und damit $\sigma(\mathcal{O}_{L'}) = \mathcal{O}_{L'}$ gilt (vgl. Lemma 7.1). Das beweist, dass $\mathrm{im}(G_{\mathfrak{P}} \to \overline{G})$ in $\overline{G}_{\mathfrak{P}'}$ enthalten ist.

Ist umgekehrt $\tau \in \overline{G}_{\mathfrak{P}'} \subset \overline{G}$, so gibt es ein $\tau_1 \in G$ mit $\overline{\tau}_1 := \tau_1|_{L'} = \tau$ (da die Projektion $G \to \overline{G}$ surjektiv ist). Wir müssen zeigen, dass es ein $\tau_2 \in G' = \ker(G \to \overline{G})$ mit $\tau_2 \circ \tau_1 \in G_{\mathfrak{P}}$ gibt. Ein solches τ_2 erhalten wir wie folgt. Zuerst beobachten wir, dass

$$\tau_1(\mathfrak{P}) \cap \mathcal{O}_{L'} = \tau_1(\mathfrak{P} \cap \mathcal{O}_{L'}) = \tau_1(\mathfrak{P}') = \mathfrak{P}'$$

gilt. Da G' transitiv auf der Menge der Primideale über $\mathfrak{P}'$ operiert (Satz 7.4), gibt es also ein $\tau_2 \in G'$ mit $\tau_2(\tau_1(\mathfrak{P})) = \mathfrak{P}$, also $\tau_2 \circ \tau_1 \in G_{\mathfrak{P}}$, wie gewünscht. □

Wir erhalten ein gruppentheoretisches Kriterium, um volle Zerlegung für *beliebige* Erweiterungen L'/K von Zahlkörpern nachzuweisen (man kann L' nämlich stets in einen Körper L einbetten, sodass L/K galoissch ist):

Korollar 7.11. *In der Situation von Lemma 7.10*[1] *sind die folgenden Aussagen äquivalent:*

(1) $\mathfrak{p}$ *ist zerfällt in* L' *total, d.h.* $\mathfrak{p}\mathcal{O}_{L'}$ *ist ein Produkt von* $[L' : K]$ *paarweise verschiedenen Primidealen.*

[1] Man beachte, dass L'/K nicht notwendig galoissch sein muss.

(2) $G_{\mathfrak{P}} \subset G'$ *für alle Primideale* $\mathfrak{P} \subset \mathcal{O}_L$ *mit* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

Beweis. Für jedes Primideal $\mathfrak{P}' \subset \mathcal{O}_{L'}$, das über $\mathfrak{p}$ liegt, gibt es ein Primideal $\mathfrak{P} \subset \mathcal{O}_L$, das über $\mathfrak{P}'$ liegt. Nach Lemma 7.10 (2) gilt nun $e(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p}) = 1$ genau dann, wenn $G_{\mathfrak{P}} \subset G'$. □

Sei $\sigma \in G = \mathrm{Gal}(L/K)$ und $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal $\neq (0)$, das über dem Primideal $\mathfrak{p} \subset \mathcal{O}_K$ liegt. Definiere die Körper $k(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$ und $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$. Dann ist durch

$$\overline{\sigma}\colon k(\mathfrak{P}) \to k(\sigma(\mathfrak{P})), \qquad \alpha + \mathfrak{P} \to \sigma(\alpha) + \sigma(\mathfrak{P})$$

ein ein $k(\mathfrak{p})$-linearer Isomorphismus beschrieben (vgl. auch den Beweis von Satz 7.8). Für $\sigma \in G_{\mathfrak{P}}$ gilt also $\overline{\sigma} \in \mathrm{Aut}_{k(\mathfrak{p})}(k(\mathfrak{P}))$.

Proposition 7.12. *Die Erweiterung* $k(\mathfrak{P})/k(\mathfrak{p})$ *ist galoissch. Der Homomorphismus* $\varphi_{\mathfrak{P}}\colon G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, $\sigma \mapsto \overline{\sigma}$ *ist surjektiv.*

Beweis. Beide Körper der Erweiterung $k(\mathfrak{P})/k(\mathfrak{p})$ sind endlich, somit ist die Erweiterung galoissch[2].

Da die Zerlegungsgruppe von $\mathfrak{P}$ bzgl. L/K mit jener bzgl. $L/Z_{\mathfrak{P}}$ übereinstimmt und für $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ gilt, dass $f(\mathfrak{P}|\mathfrak{P}_Z) = f$ (Satz 7.9 (2)), folgt $k(\mathfrak{P}_Z) = k(\mathfrak{p})$. Wir dürfen also ohne Einschränkung $K = Z_{\mathfrak{P}}$ und damit auch $G = G_{\mathfrak{P}}$ annehmen.

Wir wählen nun ein primitives Element $\beta \in \mathcal{O}_L$ von L/K. Da L/K normal ist, zerfällt $q := m_\beta \in \mathcal{O}_K[X]$ über L in Linearfaktoren:

$$q = (X - \beta_1) \cdot \ldots \cdot (X - \beta_n), \qquad \beta_1 := \beta.$$

Reduzieren wir diese Gleichung modulo $\mathfrak{P}$, so erhalten wir

$$\overline{q} = (X - \overline{\beta}_1) \cdot \ldots \cdot (X - \overline{\beta}_n).$$

Da $L = K(\beta)$, folgt $k(\mathfrak{P}) = k(\mathfrak{p})(\overline{\beta})$. Ein Element $\tau \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ bildet $\overline{\beta}$ auf ein $\overline{\beta}_i$ ab und ist dadurch eindeutig festgelegt. Dann gilt für $\sigma \in G = G_{\mathfrak{P}}$, $\sigma(\beta) = \beta_i$ aber $\varphi_{\mathfrak{P}}(\sigma) = \tau$. □

Definition 7.13. Der Kern $I_{\mathfrak{P}}$ von $\varphi_{\mathfrak{P}}$ heißt *Trägheitsgruppe*[3] von $\mathfrak{P}$ über K. Der zugehörige Fixkörper $T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$ wird der *Trägheitskörper* von $\mathfrak{P}$ über K genannt.

Warum heißen Trägheitskörper eigentlich Trägheitskörper?

Satz 7.14. *Sei* $(0) \neq \mathfrak{P} \subset \mathcal{O}_L$ *ein Primideal,* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. *Dann gilt:*

(1) Die Erweiterung $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ *ist galoissch und* $\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}})$ *ist kanonisch isomorph zu* $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$.

(2) Es gilt $(G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f$ *und* $|I_{\mathfrak{P}}| = [L : T_{\mathfrak{P}}] = e$.

[2]Das sollte aus der Algebra bekannt sein: Bezeichnet p die Charakteristik der beiden Körper, so können wir $k(\mathfrak{P})$ mit $\mathbb{F}_{p^m}$ identifizieren. Es genügt dann nach Galoistheorie zu zeigen, dass $\mathbb{F}_{p^m}/\mathbb{F}_p$ Galois ist. Der Körper $\mathbb{F}_{p^m}$ ist aber der Zerfällungskörper von $X^{p^m} - X \in \mathbb{F}_p[X]$.

[3]engl. inertia = Trägheit, deshalb wird der Buchstabe I für die Trägheitsgruppe verwendet.

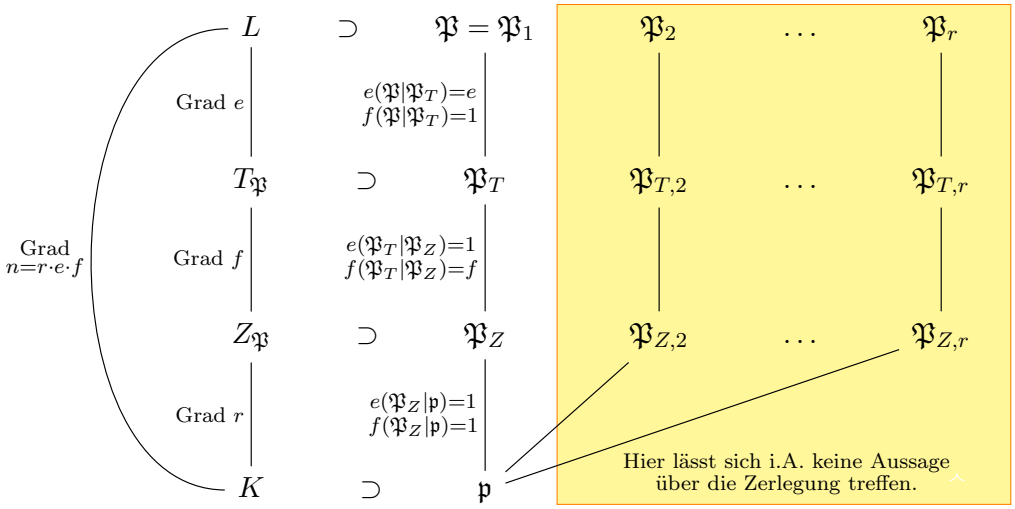
(3) Für die Primideale $\mathfrak{P}_T := \mathfrak{P} \cap \mathcal{O}_{T_\mathfrak{P}}$ *und* $\mathfrak{P}_Z := \mathfrak{P} \cap \mathcal{O}_{Z_\mathfrak{P}}$ *gilt*

$$e(\mathfrak{P}|\mathfrak{P}_T) = e, \qquad f(\mathfrak{P}|\mathfrak{P}_T) = 1,$$
$$e(\mathfrak{P}_T|\mathfrak{P}_Z) = 1, \qquad f(\mathfrak{P}_T|\mathfrak{P}_Z) = f.$$

Mit anderen Worten: $\mathfrak{P}_Z$ *ist total träge in* $T_\mathfrak{P}$ *und* $\mathfrak{P}_T$ *ist total verzweigt in* L.

(4) Es gilt $I_\mathfrak{P} = \{\mathrm{id}_L\} \iff L = T_\mathfrak{P} \iff e = 1$, *d.h.* $\mathfrak{p}$ *ist in* L *unverzweigt.*

Slogan: "Die Primfaktorisierung von $\mathfrak{P}_Z$ in $L/Z_\mathfrak{P}$ spaltet sich auf in einen total verzweigten Anteil und einen total trägen Anteil." Schreiben wir wie üblich $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdot \ldots \cdot \mathfrak{P}_r^e$ und $\mathfrak{P} = \mathfrak{P}_1$, so erhalten wir also insgesamt folgendes Diagramm:



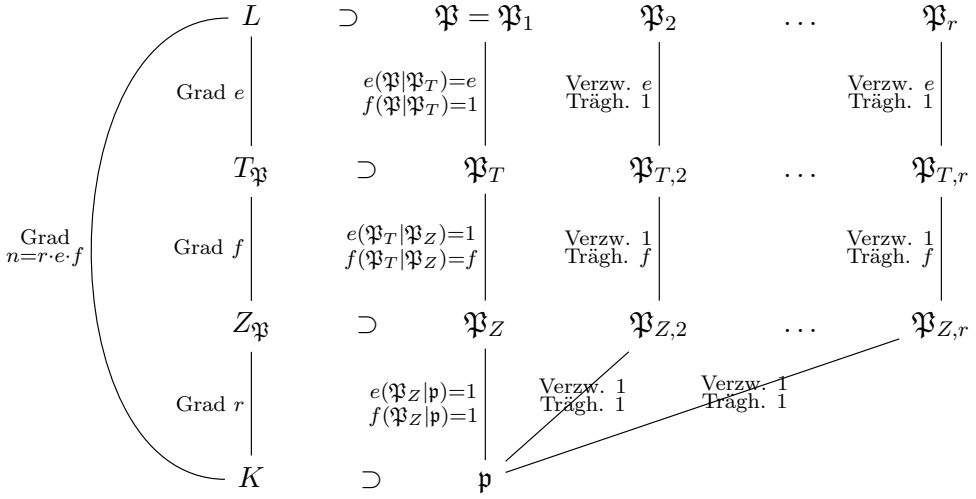
Um die Zerlegung der $\mathfrak{P}_{Z,i}$ (diese müssen nicht einmal paarweise verschieden sein) etc. zu studieren, muss man statt $Z_\mathfrak{P}$ bzw. $T_\mathfrak{P}$ natürlich $Z_{\mathfrak{P}_i}$ bzw. $T_{\mathfrak{P}_i}$ betrachten. Ist G allerdings abelsch, so folgt aus Bemerkung 7.6 (2) und Satz 7.4, dass

$$G_\mathfrak{P} = G_{\mathfrak{P}_1} = \ldots = G_{\mathfrak{P}_r}.$$

In diesem Fall folgt also auch

$$Z_\mathfrak{P} = Z_{\mathfrak{P}_1} = \ldots = Z_{\mathfrak{P}_r} \qquad \text{und} \qquad T_\mathfrak{P} = T_{\mathfrak{P}_1} = \ldots = T_{\mathfrak{P}_r}.$$

In diesem Fall kann man im gelben Teil des obigen Diagramm dieselben Verzweigungsindizes und Trägheitsgrade eintragen, wie links daneben:



In letzterem Fall sind $\mathfrak{P}_Z$ und die $\mathfrak{P}_{Z,i}$ (genau so wie die $\mathfrak{P}_T$ und die $\mathfrak{P}_{T,i}$) paarweise verschieden – das folgt aus der fundamentalen Gleichung 4.39 und den angetragenen Verzweigungsindizes und Trägheitsgraden.

Beweis von Satz 7.14. Die meisten Aussagen folgen aus Galoistheorie.

(1) Als Kern von $\varphi_\mathfrak{P}$ ist $I_\mathfrak{P}$ ein Normalteiler von $G_\mathfrak{P}$, somit liefert die Galoiskorrespondenz, dass $T_\mathfrak{P}/Z_\mathfrak{P}$ galoissch ist. Die Aussage über die Galoisgruppen folgt aus

$$\mathrm{Gal}(T_\mathfrak{P}/Z_\mathfrak{P}) \cong G_\mathfrak{P}/I_\mathfrak{P} \overset{\text{Prop. 7.12}}{\cong} \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

(2) Nach Galoistheorie gilt

$$[T_\mathfrak{P} : Z_\mathfrak{P}] = (G_\mathfrak{P} : I_\mathfrak{P}) = |G_\mathfrak{P}/I_\mathfrak{P}| \overset{(1)}{=} |\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))| = [k(\mathfrak{P}) : k(\mathfrak{p})] = f.$$

Die zweite Aussage folgt dann aus $|G_\mathfrak{P}| = e \cdot f$, siehe den Beweis von Satz 7.9.

(3) Zunächst überlegt man sich, dass $I_\mathfrak{P}$ auch die Trägheitsgruppe von $\mathfrak{P}$ über dem Trägheitskörper $T_\mathfrak{P}$ ist. Mit Proposition 7.12 folgt nun

$$\underbrace{\mathrm{Gal}(L/T_\mathfrak{P})/I_\mathfrak{P}}_{\text{triviale Gruppe}} \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}_T)),$$

d.h. $k(\mathfrak{P}) = k(\mathfrak{P}_T)$. Hieraus folgt $f(\mathfrak{P}|\mathfrak{P}_T) = 1$, also auch $f(\mathfrak{P}_T|\mathfrak{P}_Z) = f$. Die Aussage über die Verzweigungsindizes folgt nun aus

$$e(\mathfrak{P}|\mathfrak{P}_T) = e(\mathfrak{P}|\mathfrak{P}_T) \cdot f(\mathfrak{P}|\mathfrak{P}_T) \overset{(*)}{=} [L : T_\mathfrak{P}] \overset{(2)}{=} e \overset{\text{Aufg. 4.6.6}}{=} e(\mathfrak{P}|\mathfrak{P}_T) \cdot e(\mathfrak{P}_T|\mathfrak{P}_Z).$$

In Schritt $(*)$ wurde hierbei verwendet, dass $\mathfrak{P}_T\mathcal{O}_L$ eine Potenz von $\mathfrak{P}$ ist, was gilt, weil $\mathfrak{P}_Z\mathcal{O}_L$ eine Potenz von $\mathfrak{P}$ ist (Satz 7.9 (1)).

(4) Die erste Äquivalenz ist klar, die zweite folgt sofort aus (2). □

Wie bei Zerlegungskörpern kann man sich die Frage stellen, wie die Trägheitsgruppen von Zwischenkörpern aussehen.

Lemma 7.15. *Sei L' ein Zwischenkörper der endlichen Galoiserweiterung L/K. Sei wie üblich $(0) \neq \mathfrak{P} \subset \mathcal{O}_L$ ein Primideal und $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Dann gilt mit $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{L'}$ und $G' = \mathrm{Gal}(L/L')$:*

(1) Die Trägheitsgruppe $I'_\mathfrak{P}$ von $\mathfrak{P}$ über L' ist $I'_\mathfrak{P} = I_\mathfrak{P} \cap G'_\mathfrak{P}$.

(2) $I_\mathfrak{P} \subset G' \iff L' \subset T_\mathfrak{P} \iff e(\mathfrak{P}'|\mathfrak{p}) = 1$ (d.h. $\mathfrak{p}$ ist in L' unverzweigt).

(3) Ist L'/K galoissch und $\overline{G} = \mathrm{Gal}(L'/K)$, so ist $I_{\mathfrak{P}'}$ das Bild von $I_\mathfrak{P}$ unter der Projektion $G \to \overline{G}$, $\sigma \mapsto \sigma|_{L'}$.

Beweis. Die Aussagen (1) und (3) werden durch Diagrammjagd[4] bewiesen.

(1) Diese Aussage durch Analyse des folgenden kommutativen Diagramms mit exakten Zeilen (die Surjektivität folgt hierbei jeweils aus Proposition 7.12):

[4] Eine Beweismethode, bei der man Objekte "durch das Diagramm jagt". Beweise mittels Diagrammjagd sind schrecklich aufzuschreiben und es ist besser, wenn man versucht, sie selbst zu führen, als aufgeschriebene Beweise zu verstehen. Hat man selbst eine Hand voll Beweise mit Diagrammjagd geführt, so lassen sich die folgenden Diagrammjagden meist ohne Nachdenken durchführen.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I'_{\mathfrak{P}} & \longrightarrow & G'_{\mathfrak{P}} & \overset{\text{Lem. 7.10 (1)}}{=} & G_{\mathfrak{P}} \cap G' & \longrightarrow & \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}')) \longrightarrow 1 \\ & & \downarrow{\scriptstyle \iota} & & & & \downarrow & & \downarrow \\ 1 & \longrightarrow & I_{\mathfrak{P}} & \longrightarrow & G_{\mathfrak{P}} & \longrightarrow & & & \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \longrightarrow 1 \end{array}$$

Die blaue Inklusion ι ist hierbei wohldefiniert, da die Kommutativität des Diagramms und die Exaktheit der Zeilen implizieren, dass $x \in \ker\left(G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))\right) = I_{\mathfrak{P}}$ gilt. Die Wohldefiniertheit von ι stellt sicher, dass für $x \in I'_{\mathfrak{P}}$ gilt:

$$x \in I_{\mathfrak{P}} \qquad \text{und} \qquad x \in G', \qquad \text{also auch} \qquad x \in I_{\mathfrak{P}} \cap G'.$$

Ist umgekehrt $y \in I_{\mathfrak{P}} \cap G'$, so gilt insbesondere $y \in G_{\mathfrak{P}} \cap G' = G'_{\mathfrak{P}}$. Da außerdem $y \in I_{\mathfrak{P}}$, wird y in unteren Zeile auf $\mathrm{id}_{k(\mathfrak{P})} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ abgebildet. Da

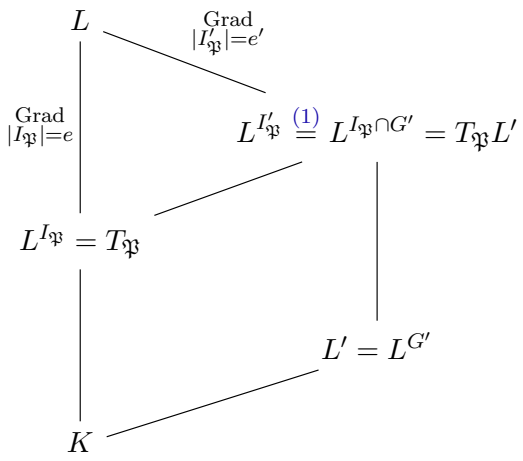
$$\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}')) \hookrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$$

injektiv ist, wird $y \in G'_{\mathfrak{P}}$ also auch in der oberen Zeile auf $\mathrm{id}_{k(\mathfrak{P})} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}'))$ abgebildet. Die Exaktheit der ersten Zeile impliziert nun $y \in I'_{\mathfrak{P}}$.

(2) Die erste Äquivalenz folgt sofort aus

$$I_{\mathfrak{P}} \subset G' \iff L' = L^{G'} \subset L^{I_{\mathfrak{P}}} = T_{\mathfrak{P}}.$$

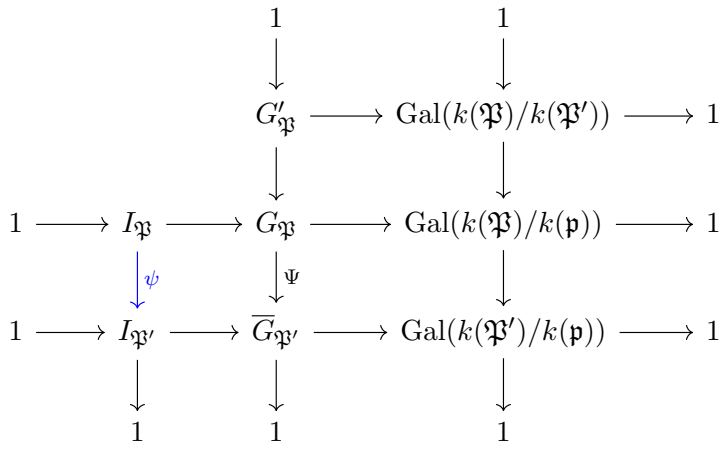
Für die zweite Äquivalenz betrachte man das folgende Körperdiagramm, wobei $e' := e(\mathfrak{P}|\mathfrak{P}')$:



Dass die Körpergrade wie angegeben sind, folgt aus Satz 7.14 (2). Aus dem Diagramm folgt nun sofort

$$L' \subset T_{\mathfrak{P}} \iff T_{\mathfrak{P}} L' = T_{\mathfrak{P}} \iff e = e' \overset{\text{Aufg. 4.6.6}}{\iff} e(\mathfrak{P}'|\mathfrak{p}) = 1.$$

(3) Wir ergänzen das Diagramm aus (1) zum folgenden Diagramm (wobei a priori noch nicht klar ist, weshalb die blaue Abbildung ψ wohldefiniert und surjektiv ist – das zeigen wir unter dem Diagramm):



Nach Lemma 7.10 (3) ist die Abbildung Ψ gerade die Einschränkung der Projektion $G \to \overline{G}$ auf $G_{\mathfrak{P}}$. Deshalb ist Ψ wohldefiniert und surjektiv. Wir beweisen nun durch Diagrammjagd, dass ψ wohldefiniert und surjektiv ist. Da ja $\psi = \Psi|_{I_{\mathfrak{P}}}$ gilt, entspricht die Wohldefiniertheit von ψ gerade der Inklusion $\mathrm{im}(I_{\mathfrak{P}} \to \overline{G}) \subset I_{\mathfrak{P}'}$ und die Surjektivität der umgekehrten Inklusion.

Wohldefiniertheit: Sei $x \in I_{\mathfrak{P}}$. Da die zweite Zeile des Diagramms exakt ist, wird x auf $\mathrm{id}_{k(\mathfrak{P})} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ abgebildet. Projiziert man nach $\mathrm{Gal}(k(\mathfrak{P}')/k(\mathfrak{p}))$, so erhält man natürlich $\mathrm{id}_{k(\mathfrak{P}')}$. Da das Diagramm kommutiert, wird $\Psi(x)$ unter

$$\overline{G}_{\mathfrak{P}'} \to \mathrm{Gal}(k(\mathfrak{P}')/k(\mathfrak{p}))$$

auch auf $\mathrm{id}_{k(\mathfrak{P}')}$ abgebildet. Da die dritte Zeile exakt ist, liegt $\Psi(x)$ also im Bild der Abbildung $I_{\mathfrak{P}'} \to \overline{G}_{\mathfrak{P}'}$, d.h. $\Psi(x) \in I_{\mathfrak{P}'}$. Das zeigt die Wohldefiniertheit von ψ.

Surjektivität: Ist $y \in I_{\mathfrak{P}'}$. Da Ψ surjektiv ist, können wir ein Urbild $x \in G_{\mathfrak{P}}$ von y wählen. Sei $\sigma \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ das Bild von x. Da das Diagramm kommutiert und die letzte Zeile exakt ist, ist das Bild von σ in $\mathrm{Gal}(k(\mathfrak{P}')/k(\mathfrak{p}))$ gerade $\mathrm{id}_{k(\mathfrak{P}')}$. Da die dritte Spalte exakt ist, gibt es also ein Urbild $\tau \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}'))$ von σ. Nun ist $G'_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{P}'))$ surjektiv, wir können also ein Urbild $z \in G'_{\mathfrak{P}}$ von τ wählen. Insgesamt erhalten wir, dass

$$xz^{-1} \in \ker(G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) = I_{\mathfrak{P}} \qquad \text{und} \qquad \Psi(xz^{-1}) = \Psi(x) = y.$$

Es ist also $xz^{-1} \in I_{\mathfrak{P}}$ ein Urbild von $y \in I_{\mathfrak{P}'}$, was die Surjektivität von ψ beweist. □

Ähnlich wie in Korollar 7.11 erhalten wir ein gruppentheoretisches Kriterium, um Unverzweigtheit in beliebigen Erweiterungen von Zahlkörpern nachzuweisen:

Korollar 7.16. *Mit der Notation von Lemma 7.15 sind äquivalent:*

(1) $\mathfrak{p}$ *ist in* L' *unverzweigt.*

(2) Es gilt $I_{\mathfrak{P}} \subset G'$ *für alle Primideale* $\mathfrak{P} \subset \mathcal{O}_L$ *über* $\mathfrak{p}$.

Beweis. Ist $\mathfrak{P}' \subset \mathcal{O}_{L'}$ ein Primideal über $\mathfrak{p}$, so gibt es ein Primideal $\mathfrak{P} \subset \mathcal{O}_L$ über $\mathfrak{P}'$. Nach Lemma 7.15 (2) gilt nun $e(\mathfrak{P}'|\mathfrak{p}) = 1$ genau dann, wenn $I_{\mathfrak{P}} \subset G'$ gilt. □

Wir beenden das Semester mit einer Anwendung der Verzweigungstheorie. Sei $|k(\mathfrak{p})| = q$. Es ist aus der Algebra-Vorlesung bekannt, dass $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ zyklisch ist und vom Frobenius-Homomorphismus

$$\mathrm{Frob}_q \colon k(\mathfrak{P}) \to k(\mathfrak{P}), \qquad x \mapsto x^q$$

erzeugt wird. Nach Proposition 7.12 ist $\varphi_{\mathfrak{P}} \colon G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ surjektiv, also können wir ein Urbild $\mathrm{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}}$ von Frob_q wählen. Ein solches Urbild wird ein *Frobeniuselement* genannt. Ist $\mathfrak{p}$ in L unverzweigt (d.h. $\varphi_{\mathfrak{P}}$ ist ein Ismorphismus, vgl. Satz 7.14 (4)), so ist die Konjugationsklasse von $\mathrm{Frob}_{\mathfrak{P}}$ in G schon durch $\mathfrak{p}$ bestimmt, da ja nach Bemerkung 7.6 (2) gilt:

$$\forall \sigma \in G\colon \qquad \sigma^{-1} G_{\mathfrak{P}} \sigma = G_{\sigma(\mathfrak{P})}, \qquad \text{also auch} \qquad \sigma^{-1} \circ \mathrm{Frob}_{\mathfrak{P}} \circ \sigma = \mathrm{Frob}_{\sigma(\mathfrak{P})}\,.$$

Des Weiteren beobachtet man, dass ein $\tau \in G$ genau dann ein Frobeniuselement ist, wenn die folgenden beiden Bedingungen erfüllt sind:

(1) $\tau(\mathfrak{P}) = \mathfrak{P}$, d.h. $\tau \in G_{\mathfrak{P}}$, und

(2) für alle $x \in \mathcal{O}_L$ gilt $\tau(x) \equiv x^q \pmod{\mathfrak{P}}$.

Der Dichtigkeitssatz von Cebotarev gibt Aufschluss darüber, für wie viele unverzweigte Primideale $\mathfrak{p} \subset \mathcal{O}_K$ eine Konjugationsklasse eines $\tau \in G$ ein Frobeniuselement enthält. Bevor wir ihn formulieren können, benötigen wir noch eine Definition.

Definition 7.17. Sei X eine Menge von Primidealen $\neq (0)$ von $\mathcal{O}_K$ und $\mathbb{P}$ die Menge aller Primideale $\neq (0)$ von $\mathcal{O}_K$. Dann heißt der Grenzwert

$$\delta(X) := \lim_{C \to \infty} \frac{|\{\mathfrak{p} \in X \mid N(\mathfrak{p}) \leq C\}|}{|\{\mathfrak{p} \in \mathbb{P} \mid N(\mathfrak{p}) \leq C\}|}$$

die *natürliche Dichtigkeit* von X, falls er existiert.

Klar ist, dass $\delta(X) = 0$, falls X endlich ist. Falls $\delta(X)$ existiert und positiv ist, so hat X also unendlich viele Elemente.

Satz 7.18 (Dichtigkeitssatz von Cebotarev)**.** *Sei L/K eine Galoiserweiterung von Zahlkörpern mit Galoisgruppe G. Für $\sigma \in G$ setzt man*

$$C_\sigma := \{\tau^{-1} \circ \sigma \circ \tau \mid \tau \in G\} \qquad \textit{(die Konjugationsklasse von } \sigma \in G\textit{)}, \qquad \textit{und}$$

$$X(\sigma) := \left\{ \mathfrak{p} \in \mathbb{P} \;\middle|\; \begin{array}{l} \mathfrak{p} \textit{ ist in } L \textit{ unverzweigt und } \sigma = \mathrm{Frob}_{\mathfrak{P}} \\ \textit{für ein Primideal } \mathfrak{P} \subset \mathcal{O}_L \textit{ mit } \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \end{array} \right\}.$$

Dann existiert $\delta(X(\sigma))$ und es gilt

$$\delta(X(\sigma)) = \frac{|C_\sigma|}{|G|}.$$

Der Beweis erfordert Methoden der analytischen Zahlentheorie und geht über den Umfang dieser Vorlesung hinaus. Um die Bedeutung des Dichtigkeitssatzes zu illustrieren, folgern wir den bekannten Dirichletschen Primzahlsatz aus ihm.

Satz 7.19 (Dirichletscher Primzahlsatz)**.** *Sei p eine Primzahl und $1 \leq a \leq n$ mit* $\mathrm{ggT}(a,n) = 1$. *Sei $X_{n,a} := \{p \text{ Primzahl} \mid p \equiv a \pmod{n}\}$. Dann gilt*

$$\delta(X_{n,a}) = \frac{1}{\varphi(n)}.$$

Insbesondere gibt es unendlich viele Primzahlen der Form $nk + a$.

Beweis. Sei p eine Primzahl, die n nicht teilt. Aus dem Zerlegungsgesetz 6.19 folgt, dass p dann unverzweigt in $\mathbb{Q}(\zeta_n)$ ist. Ferner gilt mit Satz 6.5, dass

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_b \colon \zeta_n \mapsto \zeta_n^b \mid \mathrm{ggT}(b,n) = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Wie wir oben gesehen haben, sind im Falle $p \nmid n$ also alle Frobeniuselemente $\mathrm{Frob}_{\mathfrak{P}}$ für $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ gleich (da sie konjugiert sind, aber $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ abelsch ist). Des Weiteren gilt definitionsgemäß

$$\sigma_p(\zeta_n) = \zeta_n^p \equiv \mathrm{Frob}_{\mathfrak{P}}(\zeta_n) \pmod{\mathfrak{P}}.$$

Also sind σ_p und $\mathrm{Frob}_{\mathfrak{P}}$ modulo $\mathfrak{P}$ gleich. Es folgt, dass σ_p die auf S. 125 angegebene Charakterisierung von Frobeniuselementen erfüllt. Also ist $\sigma_p = \mathrm{Frob}_{\mathfrak{P}}$. Da $\sigma_p = \sigma_a$ für $p \equiv a \mod n$ gilt, folgt insgesamt

$$p \in X_{n,a} \iff p \in X(\sigma_a).$$

Die Behauptung folgt also aus dem Dichtigkeitssatz von Cebotarev 7.18 angewendet auf σ_a (man beachte, dass $C_{\sigma_a} = \{\sigma_a\}$, weil $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ eine abelsche Galoisgruppe hat). □

7.0.1 Übungen

Aufgabe 7.0.1. Sei $L = \mathbb{Q}(i, \sqrt{5})$.

(1) Zeigen Sie, dass $L/\mathbb{Q}$ galoissch ist und bestimmen Sie die Galoisgruppe.

(2) Zeigen Sie, dass $\mathcal{O}_L = \mathbb{Z}[i, \frac{1+\sqrt{5}}{2}]$ gilt.

(3) Zeigen Sie, dass 2 und 5 die einzigen Primzahlen sind, die in L verzweigen.

(4) Berechnen Sie die Zerlegungs- und Trägheitsgruppen für alle Primideale $\mathfrak{P} \subset \mathcal{O}_L$, die über 2 und 5 liegen.