Algebraische Zahlentheorie

gehalten von Prof. Dr. V. Paškūnas
an der Universität Duisburg-Essen im Sommersemester 2012

Stand: 18. Juli 2012

Aufgeschrieben von Johannes Hölken (johannes.hoelken@stud.uni-due.de)

Inhaltsverzeichnis

Kapitel I

Einleitung

Ganze Zahlen

Wie der Name der Vorlesung schon sagt, werden wir uns in dieser Vorlesung mit Zahlen befassen. Wenn wir an Zahlen denken, meinen wir oft die ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ als Teilmenge der rationalen oder reellen Zahlen. Wir wollen in dieser Vorlesung untersuchen, was „Ganzzahligkeit“ in beliebigen Körpern heißt und ob wir die spezifischen Eigenschaften der ganzen Zahlen auch in anderen Körpern wiederfinden. Dazu betrachten wir für einen beliebigen Körper K die Menge

$$\mathcal{O}_K := \left\{ \alpha \in K \,\middle|\, \text{Es gibt ein normiertes Polynom } P \in \mathbb{Z}[X] \text{ mit } P(\alpha) = 0 \right\}$$

Die ganzen Zahlen $\mathbb{Z}$ sind jedoch nicht nur eine Teilmenge von $\mathbb{Q}$, sondern bilden sogar einen Unterring von $\mathbb{Q}$ und tatsächlich können wir auch für die Verallgemeinerung zeigen, dass gilt:

Satz .1 *Sei K ein Körper, dann ist $\mathcal{O}_K$ ein Unterring von K. Das heißt aus $\alpha, \beta \in \mathcal{O}_K$ folgt stets, dass sowohl $\alpha + \beta \in \mathcal{O}_K$ als auch $\alpha \cdot \beta \in \mathcal{O}_K$ gelten.*

Daher nennen wir $\mathcal{O}_K$ auch den *Ganzheitsring* von K. Das dieser Ring $\mathcal{O}_K$ wirklich eine Verallgemeinerung der ganzen Zahlen ist, wollen wir schon hier betrachten:

Lemma .2 *Der Ganzheitsring der rationalen Zahlen ist genau der Ring der ganzen Zahlen.*
In Formeln $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Beweis. Sei $\alpha \in \mathbb{Q}$, dann ist α von der Form $\alpha = \frac{c}{d}$ mit $d \neq 0$ und $\mathrm{ggT}(d, c) = 1$. Das sie ganzen Zahlen $\mathbb{Z}$ eine Teilmenge von $\mathcal{O}_{\mathbb{Q}}$ ist, ist sofort klar, daher wollen wir nun die andere Inklusion zeigen. Sei dazu $\alpha = \frac{c}{d} \in \mathcal{O}_{\mathbb{Q}}$, dann gibt es ein normiertes Polynom $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ mit ganzzahligen Koeffizienten a_i und der Eigenschaft, dass $P(\alpha) = 0$ ist. Es gilt

$$P(\alpha) = 0 \quad \Leftrightarrow \quad c^n + c^{n-1} \cdot d \cdot a_{n-1} + c^{n-2} \cdot d^2 \cdot a_{n-2} + \ \ldots \ + d^n \cdot a_0 = 0$$

Also wird c^n von d geteilt. Da c und d aber Teilerfremd sind, folgt sofort, dass $d = \pm 1$ gilt. Damit ist α aber eine ganze Zahl. □

Wir haben nun also gesehen, dass der Ganzheitsring für $\mathbb{Q}$ wie gewünscht mit $\mathbb{Z}$ übereinstimmt. Nun wollen wir noch zeigen, dass der von uns definierte Ganzheitsring tatsächlich eine Verallgemeinerung der ganzen Zahlen ist, sich also auch auf andere Körper anwenden lässt. Dazu betrachten wir:

Lemma .3 *Sei $K := \mathbb{Q}(i) \subseteq \mathbb{C}$ mit $i^2 = -1$. Dann gilt $\mathcal{O}_K = \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.*

Beweis. Betrachte die natürliche Inklusion

$$\begin{array}{rcl} \iota : \mathbb{Q}[X] & \hookrightarrow & \mathbb{C} \\ X & \mapsto & i \\ q & \mapsto & q \end{array}$$

Dann ist ι ein Homomorphismus und es gilt

$$\mathrm{Bild}(\iota) \;=\; \mathbb{Q}(i) \;\cong\; {}^{\mathbb{Q}[X]}\!/_{(X^2+1)}$$

Mit dem *euklidischen Algorithmus* lässt sich leicht nachrechnen, dass die Menge $\left\{ \iota(1),\, \iota(X) \right\}$ eine Basis von $\mathbb{Q}(i)$ als $\mathbb{Q}$-Vektorraum bildet. Dann ist aber bereits jedes $\alpha \in \mathbb{Q}(i)$ eindeutig durch die Gleichung $\alpha = a + ib$ mit $a, b \in \mathbb{Q}$ bestimmt. Betrachte nun die komplexe Konjugation

$$\begin{array}{rccc} \kappa : & \mathbb{C} & \to & \mathbb{C} \\ & x + iy & \mapsto & x - iy \end{array}$$

Der Körper $\mathbb{Q}(i)$ ist invariant unter der komplexen Konjugation, das heißt falls $\alpha \in \mathbb{Q}(i)$, dann ist auch $\kappa(\alpha) = \overline{\alpha} \in \mathbb{Q}(i)$.
Sei nun $\alpha \in \mathcal{O}_{\mathbb{Q}}$, dann gibt es ein normiertes Polynom $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ mit ganzzahligen Koeffizienten a_i und der Eigenschaft, dass $P(\alpha) = 0$ ist. Aus der komplexen Analysis wissen wir, dass dann auch $\kappa(\alpha) = \overline{\alpha}$ eine Nullstelle von P ist. Also gilt $\alpha \in \mathcal{O}_{\mathbb{Q}(i)} \Leftrightarrow \overline{\alpha} \in \mathcal{O}_{\mathbb{Q}(i)}$. Mit Satz .1 folgt dann, dass auch $\alpha - \overline{\alpha}$, $\alpha + \overline{\alpha}$ und $\alpha \cdot \overline{\alpha}$ ganzzahlig in $\mathbb{Q}(i)$ sind. Insbesondere das Produkt ist interessant: Da wir die rationalen Zahlen durch die Menge $\mathbb{Q} = \left\{ \beta \in \mathbb{Q}(i) \,\middle|\, \beta = \overline{\beta} \right\}$ beschreiben können, gilt $\alpha \cdot \overline{\alpha} \in \mathcal{O}_{\mathbb{Q}(i)} \cap \mathbb{Q} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, denn $\alpha \cdot \overline{\alpha} = \overline{\alpha \cdot \overline{\alpha}}$. Sei nun $\alpha = a + ib$ mit $a, b \in \mathbb{Q}$ die eindeutige Darstellung bezüglich der oben gewählten Basis, dann folgt aus der soeben gezeigten Eigenschaft des Produktes und der ersten binomischen Formel, dass $2a$, $2b$, $a^2 + b^2 \in \mathbb{Z}$ gelten. Es gibt also ganze Zahlen a_1 und b_1 mit $a = \frac{a_1}{2}$ und $b = \frac{b_1}{2}$ sowie der Eigenschaft

$$a_1^2 + b_1^2 \;\equiv\; 0 \mod 4 \tag{.1}$$

Die Zahlen a_1 und b_1 können modulo 4 nur kongruent zu 0, 1, 2 oder 3 sein, daher können deren Quadrate modulo 4 nur Kongruent zu 0, 1, 0 oder 1 sein. Mit Formel (0.1) müssen a_1 und b_1 also gerade, das heißt durch zwei teilbar, sein. Damit sind aber bereits $a, b \in \mathbb{Z}$. Es folgt

$$\mathcal{O}_{\mathbb{Q}(i)} \;\subseteq\; \mathbb{Z}[i] \;:=\; \left\{ a + ib \,\middle|\, a, b \in \mathbb{Z} \right\} \;\subseteq\; \mathbb{Q}(i)$$

Die andere Inklusion ist auch in diesem Fall leicht. □

Eindeutige Zerlegung in Primfaktoren

Eine wichtige Eigenschaft der ganzen Zahlen ist die (bis auf Reihenfolge) eindeutige Primfaktorzerlegung. Das heißt für jede ganze Zahl $z \in \mathbb{Z} \setminus \{0\}$ gibt es endlich viele Primzahlen p_i, so dass gilt

$$z \;=\; (\pm 1) \cdot p_1 \cdot \ldots \cdot p_r$$

Diese Eigenschaft lässt sich im Allgemeinen nicht auf Ganzheitsringe übertragen.

Beispiel 1 *(Ganzheitsringe sind nicht immer faktoriell)*
Sei $K = \mathbb{Q}(\sqrt{-6})$, dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. Wir können die Zahl 6 in $\mathbb{Z}[\sqrt{-6}]$ darstellen durch

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

aber sowohl 2 und 3 als auch $\sqrt{-6}$ sind unzerlegbar (also prim) in $\mathbb{Z}[\sqrt{-6}]$.

Eine gute Annäherung an die Eigenschaft der ganzen Zahlen finden wir in der *Kummer-Theorie*:

Satz .4 *(Kummer)*
Sei K ein Körper und $\mathcal{O}_K$ sein Ganzheitsring, dann gilt: Jedes Ideal $\mathfrak{a} \lhd \mathcal{O}_K$ mit $\neq 0$ lässt sich (bis auf Reihenfolge) eindeutig faktorisieren als

$$\mathfrak{a} \;=\; \wp_1 \cdot \ldots \cdot \wp_r \qquad \text{mit } \wp \in \operatorname{Spec}(\mathcal{O}_K)$$

Es wird also nun, anstatt eine Zahl in ihre Primbestandteile zu zerlegen, ein Ideal in seine Primideal-Bestandteile zerlegt.

Beispiel 2 *(Faktorisierungen in Ganzheitsringen)*

- *Sei $K = \mathbb{Q}$ und $\mathcal{O}_k = \mathbb{Z}$. Wir wissen, dass $\mathbb{Z}$ ein Hauptidealring ist. Für $n \in \mathbb{Z}_{>1}$ gilt*

  $$(n) \in \operatorname{Spec}\mathbb{Z} \;\Leftrightarrow\; {}^{\mathbb{Z}}\!/_{(n)} \text{ ist Integritätsring } \;\Leftrightarrow\; n \text{ ist Primzahl}$$

  Damit erhalten wir in diesem Fall die gewünschte Übereinstimmung der beiden Faktorisierungen, denn n hat genau dann die Primfaktorzerlegung $n = (\pm 1) \cdot p_1 \cdot \ldots \cdot p_r$, wenn das Hauptideal (n) die Faktorisierung $(n) = (p_1) \cdot \ldots \cdot (p_r)$ besitzt.

- *Sei $K = \mathbb{Q}(\sqrt{-6})$ und $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. Betrachte zunächst den Isomorphismus*

  $$\begin{array}{rcl} {}^{\mathbb{Z}[X]}\!/_{(X^2+6)} & \xleftrightarrow{\sim} & \mathbb{Z}[\sqrt{-6}] \\ X & \mapsto & \sqrt{-6} \\ z & \mapsto & z \end{array}$$

  Die Ideale $\wp_1 := (2, \sqrt{-6})$ und $\wp_2 := (3, \sqrt{-6})$ sind Primideale von $\mathcal{O}_K$, denn

  $$\begin{array}{rcccccl} {}^{\mathcal{O}_K}\!/_{\wp_1} & \cong & {}^{\mathbb{Z}[X]}\!/_{(X, 2, X^2+6)} & \cong & {}^{\mathbb{Z}[X]}\!/_{(X, 2)} & \cong & \mathbb{F}_2 \\ {}^{\mathcal{O}_K}\!/_{\wp_2} & \cong & {}^{\mathbb{Z}[X]}\!/_{(X, 3, X^2+6)} & \cong & {}^{\mathbb{Z}[X]}\!/_{(X, 3)} & \cong & \mathbb{F}_3 \end{array}$$

  Betrachten wir nun die möglichen Produkte der Ideale

  $$\begin{array}{rcccccl} \wp_1^2 & = & \left(2^2, 2 \cdot \sqrt{-6}, (\sqrt{-6})^2\right) & = & \left(4, 2 \cdot \sqrt{-6}, -6\right) & = & (2) \\ \wp_2^2 & = & \left(3^2, 3 \cdot \sqrt{-6}, (\sqrt{-6})^2\right) & = & \left(9, 3 \cdot \sqrt{-6}, -6\right) & = & (3) \\ \wp_1 \cdot \wp_2 & = & \left(2 \cdot 3, 2 \cdot \sqrt{-6}, 3 \cdot \sqrt{-6}, (\sqrt{-6})^2\right) & & & = & (\sqrt{-6}) \end{array}$$

  dann sehen wir sofort, dass die Zerlegung

  $$(6) \;=\; \wp_1^2 \cdot \wp_2^2 \;=\; (\wp_1 \cdot \wp_2)^2$$

  eindeutig ist.

Klassengruppen

Nach der Untersuchung der Ganzheitsringe und Ihrer Eigenschaften wird das Studiom der Klassengruppen ein weiterer Schwerpunkt in dieser Vorlesung sein. Die historische Motivation dieser Theorie der Klassengruppen ist, wie so oft in der Zahlentheorie, der Versuch die Fermatsche Vermutung (auch Fermats großer Satz / großer Fermat) zu beweisen.

Um die Klassengruppen eines Ganzheitsrings zu definieren benötigen wir zunächst etwas Theorie. Sei K ein Körper und $\mathcal{O}_K$ sein Ganzheitsring, dann bezeichnen wir einen endlich erzeugten $\mathcal{O}_K$-Untermodul von K, der nicht der Nullmodul ist, als *gebrochenes Ideal* von K.

Bemerkung .5 *Sei K ein Körper, dann bilden die gebrochenen Ideale von K eine Gruppe mit*

- *der Multiplikation*
$$\mathfrak{a} \cdot \mathfrak{b} \;=\; \left\{ \sum_{i=1}^{r} a_i b_i \;\middle|\; a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b} \right\}$$
für gebrochene Ideale $\mathfrak{a}$ und $\mathfrak{b}$
- *dem neutralen Element $\mathcal{O}_K$ und*
- *den Inversen $\mathfrak{a}^{-1} := \left\{ a \in K \,\middle|\, a \cdot \mathfrak{a} \subseteq \mathcal{O}_K \right\}$.*

Weiter ist die Menge der Hauptideale $\left\{ \alpha \in \mathcal{O}_K \,\middle|\, \alpha \in K^* \right\}$ eine Untergruppe der Gruppe der gebrochenen Ideale.

Wir definieren nun die *Klassengruppe* als die Faktorgruppe

$$\mathcal{C}\ell_K \;:=\; \frac{\text{Gebrochene Ideale}}{\text{Hauptideale}}$$

Ein wichtiges Ergebnis dieses Abschnittes wird der folgende

Satz .6 *Sei K ein Körper. Die Klassenzahl $h_K := |\,\mathcal{C}\ell_K\,|$ ist endlich.*

Wir wollen zum Abschluss dieser Einleitung auch aus diesem Abschnitt ein schönes Ergebnis vorziehen:

Lemma .7 *Sei K ein Körper. Ist die Klassenzahl h_K gleich 1, so ist $\mathcal{O}_K$ ein Hauptidealring.*

Die Menge der ganzen Ideale $\left\{ \mathfrak{a} \lhd \mathcal{O}_K \;\middle|\; \mathfrak{a} \neq 0 \right\}$ ist in der Gruppe der gebrochenen Ideale enthalten. Für jedes gebrochene Ideal $\mathfrak{a}$ von K gibt es ein $\alpha \in K^*$, so dass $\alpha \cdot \mathfrak{a}$ ein ganzes Ideal ist, denn sei $\mathfrak{a}$ ein gebrochenes Ideal, dann ist $\mathfrak{a}$ von der Form

$$\mathfrak{a} \;=\; \mathcal{O}_K\, x_1 + \ldots + \mathcal{O}_K\, x_r \qquad \text{mit } x_i \in K^*$$

und es gibt ein $\alpha \in K^*$ so dass für alle $i = 1, \ldots, r$ das Produkt $\alpha \cdot x_i \in \mathcal{O}_K$ ist. Mit dieser Beobachtung ist es Sinnvoll die folgende Äquivalenzrelation einzuführen:

$$\mathfrak{a} \sim \mathfrak{b} \;\;:\Leftrightarrow\;\; \exists \alpha, \beta \in K^* \text{ mit } \beta \cdot \mathfrak{a} = \alpha \cdot \mathfrak{b}$$

Durch diese Äquivalenzrelation können wir die Klassengruppe auch schreiben als

$$\mathcal{C}\ell_K \;=\; \text{Ganze Ideale}/_{\sim}$$

Damit folgt leicht

$$\begin{aligned} h_K = 1 \quad &\Leftrightarrow \quad \mathcal{C}\ell_K = \{(1)\} \quad \Leftrightarrow \quad (\forall\, \mathfrak{a} \lhd \mathcal{O}_K : \ \mathfrak{a} \sim (1)) \\ &\Leftrightarrow \quad \mathcal{O}_K \text{ ist ein Hauptidealring} \end{aligned}$$

□

Kapitel II

Algebraische Grundlagen

In diesem Abschnitt werden wir die algebraischen Grundlagen dieser Vorlesung bereitstellen. Erstes wichtiges Zwischenziel ist der *Strucktursatz über endlich erzeugte Torsionsmoduln über Hauptidealringen*. Dazu der erste Abschnitt

0 Moduln über Hauptidealringen

In diesem Abschnitt bezeichne R immer einen kommutativen Ring mit Einselement.

Definition 0.1 *(Modul)*
Ein R-Modul M ist eine abelsche Gruppe zusammen mit einer Abbildung

$$\cdot : R \times M \to M$$

welche die Eigenschaften

i) *Für alle $x \in M$ gilt:* $1_R \cdot x = x$

ii) *Für alle $x, y \in M$ und alle $\alpha \in R$ gilt:* $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$

iii) *Für alle $x \in M$ und alle $\alpha, \beta \in R$ gilt:* $\alpha \cdot (\beta \cdot y) = (\alpha\beta) \cdot x$

iv) *Für alle $x \in M$ und alle $\alpha, \beta \in R$ gilt:* $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$

erfüllt. Wo ohne Misverständnisse möglich lassen wir den Punkt der Skalarmultiplikation $(\cdot)$ ebenso wie den Punkt der Ringmultiplikation weg.

Beispiel 3 *(Bekannte Ringe und ihre Moduln)*

- *Sei $R = K$ ein Körper, dann sind die K-Moduln genau die K-Vektorräume.*
- *Jede abelsche Gruppe A ist ein $\mathbb{Z}$-Modul, denn Sei $n \in \mathbb{Z}$, dann erfüllt die Abbildung*

$$n \cdot a := \begin{cases} \sum_{i=1}^{n} a & \text{falls } n > 0 \\ 0 & \text{falls } n = 0 \\ \sum_{i=1}^{|n|} -a & \text{falls } n < 0 \end{cases}$$

Die Bedingungen (i) - (iv) aus der Definition.

- *Die Ideale eines Rings R sind genau die R-Untermoduln von R*

Definition 0.2 *(Modul-Homomorphismen)*
Seien M, N zwei R-Moduln. Ein Homomorphismus $f : M \to N$ von R-Moduln ist ein R-linearer Homomorphismus der abelschen Gruppen M, N, das heißt für alle $\alpha \in R$ und alle $m \in m$ gilt zusätzlich zu den Gruppen-Homomorphieeigenschaften

$$f(\alpha m) \;=\; \alpha\, f(m)$$

Die Menge der R-Modul-Homomorphismen von M nach N bezeichnen wir mit $\mathrm{Hom}_R(M, N)$.

Anmerkung Die Menge $\mathrm{Hom}_R(M, N)$ bildet eine abelsche Gruppe und kann mit der Abbildung

$$(r\varphi)(x) \;:=\; r \cdot \varphi(x) \qquad \text{für alle } \varphi \in \mathrm{Hom}(M, N), \text{ alle } r \in R \text{ und alle } x \in M$$

selbst wieder als R-Modul aufgefasst werden.

Definition und Bemerkung 0.3 *(Direkte Summe zweier Moduln)*
Seien M, N zwei R-Moduln, dann nennen wir

$$M \oplus N \;:=\; \big\{\, (m, n) \,\big|\, m \in M \,\wedge\, n \in N \,\big\}$$

die direkte Summe der Moduln M und N. Die direkte Summe zweier R-Moduln wird selber zu einem R-Modul via

$$\alpha \cdot (m, n) \;:=\; (\alpha m, \alpha n)$$

für alle $\alpha \in R$, alle $m \in M$ und alle $n \in N$.

Beweis. Nachrechnen der Punkte (i) bis (iv) aus Definition 0.1. □

Bemerkung 0.4 *Seien M, N zwei R-Moduln mit $N \subseteq M$, dann ist auch der Quotient M/N ein R-Modul.*

Beweis. Rechne nach, dass die Abbildung

$$\alpha \cdot \overline{m} \;=\; \alpha \cdot \big(m + N\big) \;:=\; \alpha m + N$$

die Eigenschaften einer Skalarmultiplikation erfüllt. □

Definition 0.5 *(Endlich erzeugte / freie Moduln)*
Ein R-Modul M heißt endlich erzeugt, falls es eine Teilmenge $\{x_1, \ldots, x_n\} \subseteq M$ gibt, so dass

$$M \;=\; Rx_1 + \ldots + Rx_n$$

gilt. Das heißt, dass es für alle $m \in M$ Ringelemente $\alpha_1, \ldots, \alpha_n \in R$ so gibt, dass $m = \sum \alpha_i\, x_i$ ist.
In diesem Fall nennen wir die Menge $\{x_1, \ldots, x_n\} \subseteq M$ ein Erzeugendensystem von M.
Weiter heißt M frei oder freier Modul, falls es ein Erzeugendensystem $\{x_1, \ldots, x_n\} \subseteq M$ so gibt, dass für alle $m \in M$ eindeutige(!) Ringelemente $\alpha_1, \ldots, \alpha_n$ existieren mit $m = \sum \alpha_i\, x_i$.
In diesem Fall nennen wir das Erzeugendensystem auch eine Basis von M.

Anmerkung Im Unterschied zu Vektorräumen haben Moduln im Allgemeinen keine Basis. So sind zum Beispiel endliche abelsche Gruppen als $\mathbb{Z}$-Module nicht frei.

Bemerkung 0.6 *(Eigenschaften)*
Sei M ein endlich erzeugter R-Modul. Wähle eine Teilmenge $E := \{x_1, \ldots, x_n\} \subseteq M$ und betrachte die Abbildung

$$\begin{array}{rcccc} \varphi : R^n & := & R \oplus \ldots \oplus R & \to & M \\ & & (\alpha_1, \ldots, \alpha_n) & \mapsto & \alpha_1 x_1 + \ldots + \alpha_n x_n \end{array}$$

Es gelten

- *Die Menge E ist genau dann ein Erzeugendensystem von M, wenn φ surjektiv ist.*
- *Die Menge E ist genau dann eine Basis von M, wenn φ ein Isomorphismus ist.*

Beweis. Klar. □

Definition 0.7 *(Torsionselement, Torsionsmodul)*
Sei M ein R-Modul, dann heißt ein Element $x \in M$ ein Torsionselement, falls es ein $\alpha \in R\backslash\{0\}$ so gibt, dass $\alpha x = 0$ gilt. Die Menge aller Torsionselemente von M bezeichnen wir mit $\mathrm{M}_{\mathrm{Tor}}$.
Gilt für einen R-Modul $\mathrm{M}_{\mathrm{Tor}} = \{0\}$, so nennen wir M torsionsfrei.

Übungsaufgabe 1 *Sei R ein Integritätsbereich und M ein R-Modul. Beweisen Sie*

- $\mathrm{M}_{\mathrm{Tor}}$ *ist ein Untermodul von M.*
- $M/\mathrm{M}_{\mathrm{Tor}}$ *ist Torsionsfrei*

Einschub: Das Tensorprodukt

Auch in diesem Einschub bezeichne R immer einen kommutativer Ring mit Eins.

Notation 0.8 *Seien A, B und C drei R-Moduln. Wir bezeichnen die Menge der bilinearen Abbildungen von $A \times B$ nach C über R mit*

$$\mathrm{Bil}_R(A \times B, C) \;:=\; \left\{ f : A \times B \to C \,\middle|\, f \text{ ist } R\text{-linear in beiden Komponenten} \right\}$$

Bemerkung 0.9 *Seien A, B und C drei R-Moduln. Für jede bilineare Abbildung $f \in \mathrm{Bil}_R(A \times B, C)$ und alle $a \in A$ sowie alle $b \in B$ gelten*

$$f(a,0) \;=\; f(0,b) \;=\; 0$$

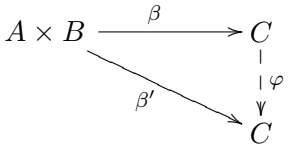
Beweis. Seien $f \in \mathrm{Bil}_R(A \times B, C)$ und $a \in A$. Wegen der Linearität von f in der zweiten Komponente gilt

$$f(a,0) + f(a,0) \;=\; f(a,0+0) \;=\; f(a,0)$$

Damit muss $f(a,0) = 0$ gelten. Die Behauptung für $f(0,b)$ folgt analog. □

Definition 0.10 *(Tensorprodukt)*
Seien A, B zwei R-Moduln. Ein Tensorprodukt von A und B über R ist ein R-Modul C zusammen mit einer bilinearen Abbildung $\beta \in \mathrm{Bil}_R(A \times B, C)$ derart, dass das Paar (β, C) die folgende universelle Abbildungseigenschaft (UAE) erfüllt:

Für alle Paare (β', C') von R-Moduln C' mit bilinearen Abbildungen $\beta' \in \mathrm{Bil}_R(A \times B, C')$ gibt es einen eindeutig bestimmten(!) R-Modulhomomorphismus $\varphi \in \mathrm{Hom}_R(C, C')$ mit $\varphi \circ \beta = \beta'$.
Das heißt, das folgende Diagramm kommutiert:



Anmerkung Seien A, B und C' irgendwelche R-Moduln und das Paar (β, C) erfülle die obige Definition eines Tensorprodukts von A und B, dann ist

$$\begin{array}{ccc} \mathrm{Hom}_R(C, C') & \to & \mathrm{Bil}_R(A \times B, C') \\ \phi & \mapsto & \phi \circ \beta \end{array}$$

ein Isomorphismus.

Bemerkung 0.11 *Sei I eine beliebige Menge. Wir setzen*

$$\mathbb{Z}^{(I)} \;:=\; \left\{ (x_i)_{i \in I} \subset \mathbb{Z} \;\middle|\; \text{fast alle } x_i = 0 \right\}$$

Dann ist $\mathbb{Z}^{(I)}$ eine abelsche Gruppe bezüglich komponentenweiser Addition.

Beweis. Nachrechnen der Gruppeneigenschaften. □

Beispiel 4 *In einigen Spezialfällen kann die oben eingeführte Gruppe expliziter angegeben werden:*

1. *Sei $I = \{1, \ldots, n\}$ eine endliche Menge, dann ist*

$$\mathbb{Z}^{(I)} \;=\; \bigoplus_{i=1}^{n} \mathbb{Z} \;=\; \mathbb{Z}^n$$

2. *Sei $I = \mathbb{N}$ dann ist*

$$\begin{array}{rcl} \mathbb{Z}^{(I)} = \mathbb{Z}^{(\mathbb{N})} & \to & \mathbb{Z}[X] \\ (a_0, a_1, \ldots) & \mapsto & \displaystyle\sum_{i \in I} a_i X^i \end{array}$$

   ein Isomorphismus von abelschen Gruppen (denn die Tupel (a_i) haben nur endlich viele Einträge ungleich Null).

Das obige Beispiel legt eine intuitivere Notation für Tupel aus $\mathbb{Z}^{(I)}$ nahe:

Notation 0.12 *Sei I eine beliebige Menge, dann führen wir für ein Element $(x_i)_{i \in I} \in \mathbb{Z}^{(I)}$ die folgende Schreibweise ein:*

$$(x_i)_{i \in I} \;:=\; \sum_{i \in I} x_i[i] \;=\; \sum_{i \in I} x_i i$$

Lemma 0.13 *Seien I eine Menge und A eine abelsche Gruppe, dann gilt*

$$\begin{array}{rcl} \mathrm{Abb}(I, A) =: \mathrm{Hom}_{Mengen}(I, A) & \xleftrightarrow{\sim} & \mathrm{Hom}_{Gruppen}(\mathbb{Z}^{(I)}, A) \\ \varphi & \mapsto & \phi\left(\displaystyle\sum_{i \in I} x_i[i]\right) := \sum_{i \in I} x_i \varphi(i) \\ \varphi(i) := \Phi(i) & \leftarrow\!\shortmid & \Phi \end{array}$$

Mit Hilfe dieser Konstruktion können wir nun die Existenz des Tensorproduktes Beweisen. Unteranderem dazu der folgende

Satz 0.14 *Für alle R-Moduln A und B existiert ein Tensorprodukt und ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Unter der Annahme, dass es ein Tensorprodukt gibt beweisen wir zunächst die Eindeutigkeit. Seien also (β, C) und (β', C') zwei Tensorprodukte von A und B. Die universelle Abbildungseigenschaft von (β, C) liefert uns einen eindeutig bestimmten Homomorphismus $\phi \in \mathrm{Hom}_R(C, C')$ mit $\beta' = \phi \circ \beta$. Andererseits liefert uns die universelle Abbildungseigenschaft von (β', C') einen ebenfalls eindeutig bestimmten Homomorphismus $\phi' \in \mathrm{Hom}(C', C)$ mit $\beta = \phi' \circ \beta'$. Insgesamt erhalten wir also die beiden Identitäten

$$\beta' \;=\; \phi \circ \phi' \circ \beta' \qquad \text{und} \qquad \beta \;=\; \phi' \circ \phi \circ \beta$$

Trivialerweise gelten auch $\beta' = id_{C'} \circ \beta'$ und $\beta = id_C \circ \beta$. Wegen der Eindeutigkeit der beiden Abbildungen ϕ und ϕ' folgt nun bereits, dass ϕ und ϕ' zueinander invers sind.

Wir wollen nun die Existenz beweisen, dazu werden wir das Tensorprodukt konstruktiv angeben. Wir konstruieren das Tensorprodukt zunächst als abelsche Gruppe durch

$$C \;:=\; A \otimes_R B \;:=\; {}^{\mathbb{Z}^{(A\times B)}}\!/_{\mathfrak{R}}$$

Wobei $\mathfrak{R} \lhd \mathbb{Z}^{(A\times B)}$ die Untergruppe sei, die erzeugt wird von den Elementen der Form

$$(a_1 + a_2, b) - (a_1, b) - (a_2, b), \quad (a, b_1 + b_1) - (a, b_1) - (a, b_2) \;\text{ und }\; (\lambda a, b) - (a, \lambda b)$$

wobei a, a_1, a_2 alle Elemente in A und b, b_1, b_2 alle Elemente in B und λ alle Elemente in R durchlaufen sollen. Als nächstes wollen wir zu der Menge $A \otimes_R B$ die zugehörige Abbildung konstruieren. Betrachte dazu

$$\begin{aligned} \beta : A \times B &\to A \otimes_R B \\ (a, b) &\mapsto a \otimes b \end{aligned}$$

Dann ist β eine bilinearform, denn es gelten für $a, a_1, a_2, b, b_1 b_2, \lambda$ aus den entsprechenden Bereichen:

$$\begin{aligned} \beta(a_1 + a_2, b) &= (a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b = \beta(a_1, b) + \beta(a_2, b) \\ \beta(a, b_1 + b_2) &= a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2 = \beta(a, b_1) + \beta(a, b_2) \\ \beta(\lambda a, b) &= \lambda a \otimes b = a \otimes \lambda b = \beta(a, \lambda b) \end{aligned}$$

Als nächsten Schritt wollen wir die abelsche Gruppe $A \otimes_R B$ zu einem R-Modul machen. Wir benötigen nur noch eine Skalarmultiplikation. Dazu setzen wir für $\lambda \in R$

$$\lambda \cdot \left(\sum_i a_i \otimes b_i \right) \;:=\; \sum_i \lambda(a_i \otimes b_i) \qquad \text{mit } a_i \in A \text{ und } b_i \in B$$

Die Assoziativität und Distributivität lässt sich dann leicht nachrechnen.

Behauptung Das Paar $(\beta, A \otimes_R B)$ erfüllt die universelle Abbildungseigenschaft des Tensorprodukts.

Sei C' ein R-Modul, dann induziert jede Bilinearform $\beta' \in \mathrm{Bil}_R(A \times B, C')$ einen Homomorphismus von abelschen Gruppen $\Phi_{\beta'} \in \mathrm{Hom}_{Gruppen}(\mathbb{Z}^{A\times B}, C')$ der durch

$$\Phi_{\beta'}(a, b) \;:=\; \beta'(a, b)$$

bestimmt ist. Da β' bilinear über R ist, werden insbesondere alle Erzeuger von $\mathfrak{R}$ unter β' auf die Null abgebildet, also ist $\mathfrak{R} \subseteq \mathrm{Ker}(\Phi_{\beta'})$. Wir erhalten eine weitere induzierte Abbildung

$$\begin{aligned} \phi_{\beta'} : {}^{\mathbb{Z}^{(A\times B)}}\!/_{\mathfrak{R}} = A \otimes_R B &\longrightarrow C' \\ (a \otimes b) &\mapsto \Phi_{\beta'}(a, b) = \beta'(a, b) \end{aligned}$$

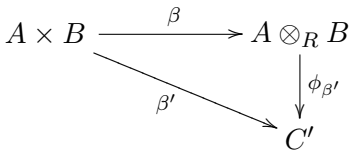
Sei $\lambda \in R$, dann gilt

$$\phi_{\beta'}\big(\lambda(a \otimes b)\big) \;=\; \beta'(\lambda a, b) \;=\; \lambda\, \beta'(a, b) \;=\; \lambda \phi_{\beta'}(a, b)$$

Auf gleiche Weise erbt $\phi_{\beta'}$ auch die anderen linearitätseigenschaften von β', also ist $\phi_{\beta'}$ ein R-Modulhomomorphismus von $A \otimes_R B$ nach C'. Wegen $\beta(a, b) = a \otimes b$ gilt weiter

$$(\phi_{\beta'} \circ \beta)(a, b) \;=\; \phi_{\beta'}(a \otimes b) \;=\; \beta'(a, b)$$

also kommutiert das folgende Diagramm:



Und damit ist der Satz gezeigt. □

Wir wollen im Folgenden einige Eigenschaften des Tensorprodukts angeben. Einige davon werden wir beweisen, bei anderen werden wir den Beweis einsparen, da sie für die weitere Vorlesung nicht von Relevanz sind. Es seien immer A, A_i, B, B_i, C, C' verschiedene R-Moduln.

(i) Wir können mit dem Tensorprodukt auf gewisse Art „rechnen“, denn es gelten

1. $A \otimes_R B \;\cong\; B \otimes_R A$
2. $\big(A \otimes_R B\big) \otimes_R C \;\cong\; A \otimes_R \big(B \otimes_R C\big)$
3. $\big(A_1 \oplus A_2\big) \otimes_R B \;\cong\; A_1 \otimes_R B \oplus A_2 \otimes_R B$
4. $A \otimes_R R \;\cong\; A$

Beweis. Die erste Aussage ist klar. der Isomorphismus, der uns die zweite Aussage gibt wird durch $(a \otimes b) \otimes c \;\mapsto\; a \otimes (b \otimes c)$ induziert. Auch die vierte Aussage können wir durch die Angabe der Abbildung $a \otimes \lambda \;\mapsto\; \lambda \cdot a$ nachweisen. Für Teil drei betrachte

$$\begin{array}{ccc} \mathrm{Bil}_R\big((A_1 \oplus A_2) \times B, C\big) & \cong & \mathrm{Bil}_R\big(A_1 \times B, C\big) \otimes \mathrm{Bil}_R\big(A_2 \times B, C\big) \\ \wr\| & & \wr\| \\ \mathrm{Hom}_R\big((A_1 \oplus A_2) \times B, C\big) & & \mathrm{Hom}_R\big(A_1 \times B, C\big) \otimes \mathrm{Hom}_R\big(A_2 \times B, C\big) \end{array}$$

□

(ii) Sei $\mathfrak{a} \lhd R$ ein Ideal, dann ist die Abbildung

$$\begin{array}{rcl} A \otimes_R {}^{R}\!/_{\mathfrak{a}} & \xrightarrow{\sim} & {}^{A}\!/_{\mathfrak{a}\,A} \\ a \otimes (\lambda + \mathfrak{a}) & \mapsto & \lambda a + \mathfrak{a}\,A \end{array}$$

ein Isomorphismus.

Beispiel 5 *Mit dieser Regel gilt*

$${}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \otimes_R {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \;\cong\; {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\!/_{2\,.\,\mathbb{Z}/3\mathbb{Z}} \;=\; \{0\}$$

(iii) Sei R ein Integritätsring und $K := \mathrm{Quot}(R)$ sein Quotientenkörper. Sei weiter $M = \mathrm{M}_{\mathrm{Tor}}$ ein R-Torsionsmodul, dann gilt

$$M \otimes_R K \;=\; \{0\}$$

Beweis. Der R-Modul $M \otimes_R K$ wird als abelsche Gruppe von der Menge

$$E \;:=\; \{\, m \otimes x \,|\, m \in M \wedge x \in K \,\}$$

erzeugt. Sei nun $m \otimes x \in E$ mit $m \neq 0_M$ und $x \neq 0_K$ und sei weiter $\lambda \in R \backslash \{0\}$ ein Annulator[1] von m. Betrachte die folgende Rechnung:

$$\begin{aligned} m \otimes x &= m \otimes \lambda\lambda^{-1}x = \lambda m \otimes \lambda^{-1}x \\ &= 0 \otimes \lambda^{-1}x = 0 \end{aligned}$$

□

(iv) Das Tensorprodukt ist funktoriell in beiden Komponenten, das heißt für R-Moduln A, B und C mit einem $\phi \in \mathrm{Hom}_R(B, C)$ gibt es einen Homomorphismus von R-Moduln

$$\begin{aligned} \varphi : A \otimes_R B &\to A \otimes_R C \\ a \otimes b &\mapsto a \otimes \phi(b) \end{aligned}$$

In der anderen Komponente gilt die Aussage analog.

(v) Sei S eine R-Algebra und A ein R-Modul, dann wird $A \otimes_R S$ ein S-Modul via

$$x(a \otimes \lambda) := a \otimes \lambda x \qquad \text{für alle } a \in A \text{ und alle } \lambda, x \in S$$

Ist insbesondere R ein Integritätsring und bezeichne $K := \mathrm{Quot}(R)$ den Quotientenkörper von R, dann ist für jeden R-Modul M das Tensorprodukt $M \otimes_R K$ ein K-Modul (also ein K-Vektorraum). Ist weiter M von der Menge $\{m_1, \ldots, m_n\} \subseteq M$ endlich erzeugt, dann ist $M \otimes_R K$ als K-Modul von $\{m_1 \otimes 1, \ldots, m_n \otimes 1\}$ endlich erzeugt.

Beweis. Die abelsche Gruppe $M \otimes_R K$ ist erzeugt von der Menge

$$E := \{\, m \otimes x \,|\, m \in M \wedge x \in K \,\}$$

Für alle $x \in K$ und alle $m \in M$ gilt $m \otimes x = x \cdot (m \otimes 1)$ weiter gibt es $\lambda_i \in R$ so dass $m = \lambda_1 m_1 + \ldots + \lambda_n m_n$ ist. Es gilt

$$m \otimes 1 = \big(\lambda_1 m_1 + \ldots \lambda_n m_n\big) \otimes 1 = \sum_{i=1}^{n} \lambda_i (m_i \otimes 1)$$

und damit gibt es für alle $y \in M \otimes_R K$ Elemente $x_i \in K$ mit

$$y = \sum_{i=1}^{n} x_i (m_i \otimes 1)$$

□

(vi) Seien A, B und C drei R-Moduln mit einem surjektiven Homomorphismus $\phi \in \mathrm{Hom}(B, C)$, dann ist auch

$$\phi' : A \otimes_R B \ni a \otimes b \mapsto a \otimes \phi(b) \in A \otimes_R C$$

surjektiv.

[1] Ein Element $\lambda \in R \backslash \{0\}$ heißt Annulator eines Torsionselements m, falls $\lambda m = 0_M$ gilt.

Definition 0.15 *(Rang endlich erzeugter Moduln)*
Sei R ein Integritätsring und $K := \mathrm{Quot}(R)$ sein Quotientenkörper. Wir setzen den Rang eines endlich erzeugten R-Moduls M als

$$\mathrm{rg}_R(M) \;:=\; \dim_K(M \otimes_R K)$$

Anmerkung Der Rang eines endlich erzeugten Moduls M ist immer kleinergleich der Anzahl der Elemente im minimalen Erzeugendensystem von M, das heißt

$$\mathrm{rg}_R(M) \;\leq\; \min\left\{ \sharp E \,\middle|\, E \text{ ist ein Erzeugendensystem von } M \right\}$$

Ist M sogar ein freier Modul, dann ist $\mathrm{rg}_R(M) = \sharp B$ wobei B eine R-Basis von M sei. Denn sei $n = \sharp B$, dann ist $M \cong R^n$ und damit folgt

$$M \otimes_R K \;\cong\; R^n \otimes_R K \;\cong\; (R \otimes_R K)^n \;\cong\; K^n$$

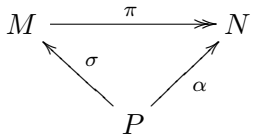
Definition 0.16 *(exakte Sequenz / Komplex)*[2]
Seien M_i für $i \in \mathbb{N}$ gegebene R-Moduln mit zugehörigen Homomorphismen $\varphi_i \in \mathrm{Hom}_R(M_i, M_{i+1})$. Eine Folge oder Sequenz der Form

$$\ldots \to M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \to \ldots$$

heißt:

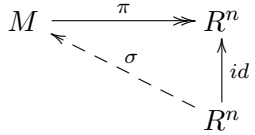
- *ein Komplex, falls* $\mathrm{Im}(\varphi_{i-1}) \subseteq \mathrm{Ker}(\varphi_i)$
- *eine exakte Sequenz oder exakt, falls* $\mathrm{Im}(\varphi_{i-1}) = \mathrm{Ker}(\varphi_i)$

Definition 0.17 *(Projektive Moduln)*[3]
Ein R-Modul P heißt projektiv, falls die folgende universelle Abbildungseigenschaft (UAE) gilt: Für alle R-Moduln M, N und für alle surjektiven R-Homomorphismen $\pi \in \mathrm{Hom}_R(M, N)$ sowie für alle $\alpha \in \mathrm{Hom}_R(P, N)$ gibt es einen Homomorphismus $\sigma \in \mathrm{Hom}_R(P, M)$, so dass gilt: $\pi \circ \sigma = \alpha$.



Lemma 0.18 *Jeder freie R-Modul ist projektiv.*

Beweis. Sei M ein freier R-Modul mit Basis $\{x_1, \ldots, x_n\} \subseteq M$. Dann gibt es eine surjektive Abbildung $\pi : M \twoheadrightarrow R^n$ mit der Eigenschaft $\pi(x_i) = e_i$, wobei e_i dasjenige Element aus R^n bezeichne, dass in der i-ten Komponente eine Eins hat und überall sonst nur Nullen. Betrachte das Diagramm



[2]Diese Definition stammt nicht aus der Vorlesung, sondern wurde von mir aus [L3] zum besseren Verständnis eingefügt.
[3]Diese Definition stammt nicht aus der Vorlesung, sondern wurde von mir aus [L3] zum besseren Verständnis eingefügt.

Wir wollen zeigen, dass es eine Abbildung $\sigma : R^n \to M$ gibt, die die Forderung $\pi \circ \sigma = id_{R^n}$ erfüllt. Setze dazu $\sigma(e_i) := x_i$, dann gilt

$$\sigma\big((\alpha_1, \ldots, \alpha_n)\big) \;=\; \sum_{i=1}^{n} \alpha_i \, x_i \qquad \text{für alle } (\alpha_1, \ldots, \alpha_n) \in R^n$$

Und damit ist die universelle Abbildungseigenschaft projektiver Moduln erfüllt. □

Notation 0.19 *Einen Hauptidealring, der gleichzeitig ein Integritätsbereich ist, wollen wir im weiteren einen Hauptidealbereich nennen und mit HIB abkürzen.*

Proposition 0.20 *Sei R ein Hauptidealbereich, dann ist jeder Untermodul $N \neq \{0\}$ eines endlich erzeugten freien R-Moduls M selber wieder ein freier R-Modul.*

Beweis. Induktiv über den Rang von M.

$\mathrm{rg}_R(M) = 1$ In diesem Fall gilt $M \cong R^1 = R$ also ist N isomorph zu einem ein Ideal $\mathfrak{a} \lhd R$. Da R ein Hauptidealring ist gibt es einen Erzeuger $a \in R$ mit $(a) = \mathfrak{a}$. Da R ein Integritätsring ist gibt es einen Isomorphismus $\psi : R \xrightarrow{\sim} aR = (a)$ und damit ist $N \cong \mathfrak{a} \cong R$ frei.

$\mathrm{rg}_R(M) = n$ Wir setzen voraus, dass die Behauptung für $m < n$ gilt. Betrachte die Projektion

$$\begin{array}{rcl} \pi : M \cong R^n & \to & R \\ (\alpha_1, \ldots, \alpha_n) & \mapsto & \alpha_n \end{array}$$

Nach Induktionsvoraussetzung ist $\ker(\pi) = R^{n-1}$ ein freier Modul vom Rang $n-1$. Betrachte die kurzen exakten Sequenzen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\pi) & \longrightarrow & M & \xrightarrow{\pi} & R & \longrightarrow & 0 \\ & & \cup & & \cup & & \cup & & \\ 0 & \longrightarrow & \ker(\pi) \cap N & \longrightarrow & N & \xrightarrow{\pi} & \pi(N) & \longrightarrow & 0 \end{array}$$

Auch der R-Modul $\ker(\pi) \cap N$ ist frei nach Induktionsvoraussetzung. Setze $\mathrm{rg}_R(\ker \pi \cap N) =: m < n$ und unterscheide

Sonderfall ($\pi(N) = \{0\}$) In diesem Fall ist $N \cong \ker(\pi) \cap N$ und damit frei.

Hauptfall ($\pi(N) \neq \{0\}$) In diesem Fall ist $\pi(N) \cong R$ ein freier Modul vom Rang 1. Mit Bemerkung 0.6 gilt dann

$$N \;\cong\; (\ker(\pi) \cap N) \oplus \pi(N) \;\cong\; R^m \oplus R \;\cong\; R^{m+1}$$

und damit folgt die Behauptung.

□

Folgerung 0.21 *Sei R ein Hauptidealbereich und M ein freier, endlich erzeugter R-Modul mit Untermodul N. Es gelten*

1. $\mathrm{rg}_R(N) \;\leq\; \mathrm{rg}_R(M)$
2. *N ist endlich erzeugt.*

Beweis. Teil 1 haben wir schon im Beweis der vorangegangenen Proposition gesehen. Für den Teil 2 betrachte noch einmal die Abbildung $\pi : R^n \twoheadrightarrow M$ aus Bemerkung 0.6:

$$\begin{array}{ccc} R^n & \xrightarrow{\pi} & M \\ \cup & & \cup \\ \pi^{-1}(N) & \xrightarrow{\pi} & N \end{array}$$

Aus der zuvor gezeigten Proposition 0.20 folgt nun, dass

$$\pi^{-1}(N) \;:=\; \left\{ \underline{x} \in R^n \,\middle|\, \pi(\underline{x}) \in N \right\}$$

ein freier Modul von endlichem Rang ist. Wähle ein endliches Erzeugendensystem $E \subset \pi^{-1}(N)$, dann ist $\pi(E)$ ein endliches Erzeugendensystem von N nach Bemerkung 0.6. □

Lemma 0.22 *Sei R ein Hauptidealbereich und M ein endlich erzeugter R-Modul, dann gilt: Ist M torsionsfrei, so ist M frei.*

Beweis. Wähle ein Erzeugendensystem $S \subseteq M$ von M und setze $T \subseteq S$ als eine maximal linearunabhängige Teilmenge von S, das heißt für T gelten

- Gibt es $\alpha_t \in R$ mit $\sum\limits_{t\in T} \alpha_t \cdot t \;=\; 0$ so sind notwendig alle $\alpha_t = 0$.
- Sei $s \in S$ beliebig, dann ist $T \cup \{s\}$ nicht mehr linear unabhängig.

Behauptung T ist nicht leer: Sei $s \in S\backslash\{0\}$, dann ist $\{s\}$ linear unabhängig, denn wegen der Torsionsfreiheit von M folgt aus $\alpha s = 0$ stets, dass $\alpha = 0$ gilt.
Da wir die Familie der linearunabhängigen Teilmengen von S via „$\subseteq$“ mit einer Halbordnung versehen können muss es eine maximal linearunabhängige Teilmengen geben, denn S ist endlich. Wir betrachten nun wieder zwei Fälle

Fall 1 ($T = S$) Die Abbildung

$$\begin{array}{ccc} \bigoplus\limits_{t\in T} R & \to & M \\ (r_t \,|\, t \in T) & \mapsto & \sum\limits_{t\in T} r_t \cdot t \end{array}$$

ist surjektiv, denn $T = S$ ist ein Erzeugendensystem und injektiv, da T linear unabhängig ist. Also ist die Abbildung ein Isomorphismus und damit ist M nach Bemerkung 0.6 frei.

Fall 2 ($T \neq S$) Für alle $y \in S\backslash T$ gibt es Elemente $\alpha_y \in R\backslash\{0\}$ derart, dass

$$\alpha_y y \;=\; \sum_{t\in T} \alpha_t \cdot t \;\in\; \sum_{t\in T} Rt \;=:\; N \;\subseteq M$$

gilt, denn $T \cup \{y\}$ ist eine linear abhängige Menge. Der M-Untermodul $N = \sum_{t\in T} Rt$ ist frei nach Proposition 0.20. Setze nun

$$\beta \;:=\; \prod_{y\in S\backslash T} \alpha_y$$

Dann ist $\beta x \in N$ für alle $x \in S$. Das heißt aber, da S ein Erzeugendensystem von M ist, dass $\beta M \subseteq N$ gilt. Da N frei und nach der Folgerung 0.21 auch endlich erzeugt ist, ist auch βM frei und endlich erzeugt.Da M nach Voraussetzung torsionsfrei ist, ist die Surjektion

$$M \ni m \;\mapsto\; \beta m \in \beta M$$

auch injektiv, also ist $M \cong \beta M$ frei. □

Folgerung 0.23 *Sei R ein Hauptidealbereich und M ein endlich erzeugter R Modul, dann gibt es einen Untermodul M_F von M mit*

- *M_F ist ein freier Modul*
- $M \;\cong\; \mathrm{M}_{\mathrm{Tor}} \oplus M_F$
- $\mathrm{rg}_R(M) \;=\; \mathrm{rg}_R(M_F)$

Beweis. Bezeichne $\pi : M \to {}^{M}\!/_{\mathrm{M}_{\mathrm{Tor}}}$ die natürliche Projektion. Nach Übungsaufgabe 1 ist ${}^{M}\!/_{\mathrm{M}_{\mathrm{Tor}}}$ ein endlich erzeugter torsionsfreier Untermodul von M und damit nach Lemma 0.22 ein freier und nach Lemma 0.18 ein projektiver Modul. Also gibt es eine Abbildung

$$\sigma : {}^{M}\!/_{\mathrm{M}_{\mathrm{Tor}}} \;\to\; M \qquad \text{mit } id_M : M \xrightarrow{\pi} {}^{M}\!/_{\mathrm{M}_{\mathrm{Tor}}} \xrightarrow{\sigma} M$$

Setze $M_F := \mathrm{Bild}(\sigma)$, dann gilt $M \cong \mathrm{M}_{\mathrm{Tor}} \oplus M_F$ nach Isomorphiesatz.
Zum Nachweis der Aussage über den Rang sei $K := \mathrm{Quot}(R)$ der Quotientenkörper von R, dann gilt

$$M \otimes_R K \;=\; \left(\mathrm{M}_{\mathrm{Tor}} \otimes_R K\right) \;\oplus\; \left(M_F \otimes_R K\right)$$

Da es für alle $x \in \mathrm{M}_{\mathrm{Tor}}$ ein $\alpha \in R\backslash\{0\}$ mit $\alpha x = 0$ gibt und α in K eine Einheit ist gilt für alle $x \in \mathrm{M}_{\mathrm{Tor}}$

$$x \otimes 1 \;=\; x \otimes \alpha \cdot \alpha^{-1} \;=\; \alpha x \otimes \alpha^{-1} \;=\; 0 \otimes \alpha^{-1} \;=\; 0$$

Also ist $\mathrm{M}_{\mathrm{Tor}} \otimes_R K \;=\; 0$ und damit folgt die Behauptung. □

Anmerkung Die Bildung von $\mathrm{M}_{\mathrm{Tor}}$ ist kanonisch, die Bildung von M_F jedoch nicht, da σ nicht kanonisch ist.

Da wir $M_F \;\cong\; R \oplus \ldots \oplus R$ schon recht gut verstehen wollen wir nun die Struktur von endlich erzeugten Torsionsmoduln besser verstehen lernen. In Vorbereitung darauf werden wir zunächst den Elementarteilersatz zeigen. Doch zuerst noch eine kurze

Erinnerung. Aus der Algebra Vorlesung wissen wir, dass es in Hauptidealbereichen R immer einen größten gemeinsamen Teiler gibt. Das heißt für alle $a, b \in R$ gibt es ein $d \in R$ mit

- d teilt sowohl a also auch b.
- Wenn es ein anderes Element $d' \in R$ gibt das ebenfalls a und b teilt, dann teilt d' auch d.

Insbesondere ist der größte gemeinsame Teiler bis auf Multiplikation mit einer Einheit $\epsilon \in R^\times$ eindeutig bestimmt. Wir schreiben dann auch $d := \mathrm{ggT}(a, b)$. Da R ein Hauptidealring ist gilt weiter

$$(a, b) = (d) \qquad \Leftrightarrow\; \exists\, \alpha, \beta \in R :\;\; \alpha a + \beta b = d$$

Zwei Elemente $a, b \in R$ heißen Teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$ oder äquivalent $(a, b) = R$ gelten.

Satz 0.24 *(Elementarteilersatz für Basen)*
Sei R ein Hauptidealbereich und M ein freier R-Modul von endlichem Rang. Sei weiter $N \subset M$ ein Untermodul von M mit $\mathrm{rg}_R(M) = n = \mathrm{rg}_R(M)$.
Dann gibt es eine R-Basis $\{x_1, \ldots, x_n\}$ von M und Elemente $d_1, \ldots, d_n \in R$ mit

1. *Die d_i sind geordnet durch d_i teilt d_{i+1} und*
2. *Die Menge $\{d_1x_1, \ldots, d_nx_n\}$ ist eine R-Basis von N.*

Beweis. Wähle eine R-Basis $\{x_1, \ldots, x_n\}$ von M und eine R-Basis $\{y_1, \ldots, y_n\}$ von N. Da N als M Untermodul insbesondere eine Teilmenge von M ist können wir jedes Element von N als linearkombination der Basiselemente von M schreiben. Insbesondere für die Basiselemente y_i von N gilt also

$$y_i \;=\; \sum_{j=1}^{n} a_{i,j}x_j \qquad \text{mit } a_{i,j} \in R$$

Auf diesem Wege erhalten wir eine Matrix $A := (a_{i,j}) \in \mathrm{Mat}_{n\times n}(R)$.

Anmerkung Wie in der linearen Algebra über Körpern kann auch die Basiswechselmatrix über Ringen aus $\mathrm{Gl}_n(R)$ gewählt werden, denn für zwei Basen $\{b_i\}$ und $\{b'_i\}$ eines R-Moduls seien $C, C' \in \mathrm{Mat}_{n\times n}(R)$ Matritzen mit $b = C'b'$ und $b' = Cb$. Dann gelten auch $b = C'Cb$ und $b' = CC'b'$.

Also ist die folgende Reformulierung des Elementarteilersatzes sinnvoll:

Satz 0.25 *(Elementarteilersatz für Matritzen)*
Sei $A \in \mathrm{Mat}_{n\times n}(R)$ eine Matrix, dann gibt es invertierbare Matrizen $B, C \in \mathrm{Gl}_n(R)$ mit

$$B \cdot A \cdot C \;=\; \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

wobei jedes d_i seinen diagonalen Nachfolger d_{i+1} teilt.

Dies ist wirklich eine Reformulierung des Elementarteilersatzes, denn die Basen $\{\, By_i \,|\, i = 1 \ldots n\}$ für N und $\{\, Cx_i \,|\, i = 1 \ldots n\}$ für M sind wirklich die Basen der anderen Version.

Notation 0.26 *(Länge einer Zahl)*
Sei R ein faktorieller Ring und $a \in R\backslash\{0\}$, dann setzen wir die Länge von a als die (mit Vielfachheit gezählte) Anzahl der Primfaktoren von a, also sei

$$a \;=\; \epsilon \cdot \prod_{i=1}^{n} \pi_i$$

die Primfaktorzerlegung von a mit einer Einheit $\epsilon \in R^\times$ und nicht notwendig verschiedenen Primelementen $p_i \in R$, dann ist die Länge von a gesetzt als $l(a) := n$.

Wir wollen nun den Elementarteilersatz in der Version für Matrizen beweisen.
Sei dazu $A = (a_{i,j}) =\in \mathrm{Mat}_{n\times n}(R)\backslash\{0\}$ eine Matrix. Setze $l(A) := \min\{l(a_{i,j}) | a_{i,j} \neq 0\}$. Wähle nun zu A zwei invertierbare Matrizen $B, C \in \mathrm{Gl}_n(R)$ so dass $l(BAC)$ minimal ist. Bezeichne

$$A' \;:=\; BAC$$

und gelte ohne Einschränkung, dass $a'_{1,1}$ bereits das Element mit der minimalen Länge ist (sonst vertausche entsprechend Zeilen und Spalten in A').

Behauptung *Das Element $a'_{1,1}$ teilt alle Elemente der ersten Zeile sowie auch alle Elemente der ersten Spalte von A'. Das heißt für alle $1 \leq i, j \leq n$ gelten $a'_{1,1}|a'_{1,j}$ und $a'_{1,1}|a'_{i,1}$.*

Beweis. Es geügt zu zeigen, dass $a'_{1,1}$ ein anderes Element der Zeile oder der Spalte teilt. Danach kann die Konstruktion mit den anderen Elementen wiederhohlt werden. Sei also $d = \mathrm{ggT}(a'_{1,1}, a'_{1,2})$ der größte gemeinsame Teiler, dann gibt es Ringelemente $x, y \in R$ mit $d = xa'_{1,1} + ya'_{1,2}$. Wir setzen:

$$B \;:=\; A' \cdot \begin{pmatrix} x & -\frac{a_{1,2}}{d} & & & \\ y & -\frac{a_{1,2}}{d} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \;\in\; \mathrm{Gl}_n(R)$$

Das B invertierbar ist, ist klar, da die obere 2×2-Blockmatrix die Determinante 1 hat. Es gilt

$$A' \cdot B \;=\; \begin{pmatrix} d & * & \dots & * \\ * & * & & * \\ \vdots & & \ddots & \\ * & & & * \end{pmatrix}$$

Weil $d = xa'_{1,1} + ya'_{1,2}$ ist und die Länge von $a'_{1,1}$ minimal ist muss $l(A) = l(a'_{1,1}) \leq l(d)$ gelten. Also teilt $a'_{1,1}$ den größten gemeinsamen Teiler und muss so bereits selber $a'_{1,2}$ teilen. $\diamond$

Es darf nun ohne Einschränkung angenommen werden, dass A' bereits von der folgenden Form ist

$$A' \;=\; \begin{pmatrix} a'_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \boxed{A''} & \\ 0 & & & \end{pmatrix} \qquad \text{mit einer Matrix } A'' \in \mathrm{Mat}_{n-1\times n-1}(R)$$

Durch schrittweise Wiederholung erhalte eine Matrix

$$A^{(n)} \;=\; \begin{pmatrix} a'_{1,1} & & & \\ & a''_{1,1} & & \\ & & \ddots & \\ & & & a^{(n)}_{1,1} \end{pmatrix}$$

Setze $d_i := a^{(i)}_{1,1}$ Wir wollen nun zeigen, dass d_1 den diagonalen Nachfolger d_2 teilt, dann folgt der Rest der Behauptung durch Induktion. Betrachte

$$\begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \cdot A \;=\; \begin{pmatrix} d_1 & d_2 & & & \\ & d_2 & & & \\ & & d_3 & & \\ & & & \ddots & \\ & & & & d_3 \end{pmatrix}$$

Ersetze nun d_1 durch $\mathrm{ggT}(d_1, d_2)$. Mit dem gleichen Argument wie oben folgt dann aus der minimalen Länge von $d_1 = a'_{a,a}$, dass d_1 den Nachfolger d_2 teilen muss. $\square$

Jetzt haben wir alles zusammen um endlich erzeugte Torsionsmoduln, und damit den Torsionsanteil in jeden endlich erzeugten Modul, besser zu verstehen. Es gilt der folgende

Satz 0.27 *(Struktursatz über endlich erzeugte Torsionsmoduln über Hauptidealringen)*
Sei R ein Hauptidealbereich und $M = \mathrm{M}_{\mathrm{Tor}}$ ein endlich erzeugter Torsionsmodul über R. Es gelten

1. *Sei $\pi \in R$ ein Primelement, dann setzen wir die Menge der π-primären Elemente von M als*

$$M(\pi) \ := \ \left\{ x \in M \,\middle|\, \exists n \in \mathbb{N} : \pi^n \cdot x = 0 \right\} \subset M$$

   mit dieser Notation gilt

$$M \ \cong \ \bigoplus_{\pi \in R \text{ prim}} M(\pi)$$

   Insbesondere ist $M(\pi)$ also auch ein Untermodul von M.

2. *Ist M ein π-Torsionsmodul von R, also wenn es ein $n \in \mathbb{N}$ gibt, so dass $\pi^n M = \{0\}$ gilt, dann gibt es natürliche Zahlen $r_1, \ldots, r_k \in \mathbb{N}$ mit*

$$M \ \cong \ {}^{R}\!\diagup_{(\pi^{r_1})} \oplus \ldots \oplus {}^{R}\!\diagup_{(\pi^{r_k})}$$

   und die Zahlen r_i sind bis auf Reihenfolge eindeutig bestimmt.

Beweis. Für den Nachweis von Teil 1 setze $M(r) \ := \ \left\{ x \in M \,\middle|\, \exists n \in \mathbb{N} : r^n \cdot x = 0 \right\}$ für $r \in R$. Seien nun $a, b \in R$ zwei Teilerfremde Elemente, dann ist die folgende Abbildung

$$\begin{aligned} \varphi : M(a) \otimes M(b) \ &\to \ M(a,b) \\ (x,y) \ &\mapsto \ x + y \end{aligned}$$

ein R-Modulisomorphismus. Die Homomorphieeigenschaft lässt sich schnell nachrechnen. Sei $(x,y) \in \mathrm{Ker}(\varphi)$, dann gilt $x = -y$ und ausserdem gibt es Zahlen $n, m \in \mathbb{N}$ mit $a^n x = 0$ und $b^m y = 0$. Setze $N := \max(n,m)$.
Da a und b Teilerfremd sind, sind auch a^N und b^N teilerfremd, also gibt es $\alpha, \beta \in R$ mit $1 = \alpha a^N + \beta b^N$. Multipliziere diese Gleichung mit x durch und erhalte

$$x \ = \ \alpha a^N x + \beta b^N x \ \overset{x=-y}{=} \ \alpha a^N x - \beta b^N y \ = \ 0$$

denn a^N annuliert x und b^N annuliert y. Damit ist (x,y) genau dann im Kern von φ, wenn $x = -y = 0$ gilt. Also ist φ injektiv.
Sei nun $z \in M(a,b)$, dann gibt es ein $N \in \mathbb{N}$ so dass $(ab)^N z \ = \ 0$ ist. Wegen der Teilerfremdheit von a und b gilt dann wieder mit α und β wie zuvor

$$z \ = \ \alpha \underbrace{a^N z}_{\in M(a)} + \beta \underbrace{b^N z}_{\in M(b)}$$

Also ist φ auch surjektiv.
Allgemein gibt es ein Element $a \in R \backslash \{0\}$ so dass für alle $x \in M$ gilt $a \cdot x = 0$, denn M ist endlich erzeugt also wähle echte Annulatoren (also nicht die Null) der Erzeuger von M, dann annuliert das Produkt dieser Annulatoren den ganzen Modul. Da R ein Integritätsring ist, ist dieses Produkt ungleich Null. Betrachte nun die Primfaktorzerlegung von a

$$a \ = \ \epsilon \cdot \pi_1^{r_1} \cdot \ldots \cdot \pi_s^{r_s} \qquad \text{mit Primelementen } \pi_i \in R \text{ und einer Einheit } \epsilon \in R^\times$$

Da alle π paarweise verschieden, und damit teilerfremd, sind folgt mit dem oben gezeigten Isomorphismus

$$M \;=\; M(a) \;\cong\; \bigoplus_{i=1}^{s} M(\pi_i)$$

Für den Nachweis des zweiten Teils benutzen wir den zuvor gezeigten Elementarteilersatz 0.24. Wir müssen zunächst zwei freie R-Moduln konstruieren, die den Voraussetzungen des Satzes genügen. Da M ein endlich erzeugter Modul ist gibt es eine surjektive Abbildung

$$\alpha : F_0 \;\twoheadrightarrow\; M$$

von einem endlich erzeugten freien Modul F_0 nach M. Insbesondere ist nach Lemma 0.22 aber auch $\mathrm{Ker}(\alpha) =: F_1$ ein freier Modul von endlichem Rang. Da M nach Voraussetzung ein π-Torsionsmodul ist liegt für genügend großes $N \in \mathbb{N}$ der Modul $\pi^N F_0$ im Kern der Abbildung. Da $\pi^N F_0 \to F_0$ ein Isomorphismus ist gilt

$$\mathrm{rg}_R(F_0) \;=\; \mathrm{rg}_R(\pi^N F_0) \;\leq\; \mathrm{rg}_R(F_1) \;\leq\; \mathrm{rg}_R(F_0)$$

was nichts anderes heißt als $\mathrm{rg}_R(F_0) = \mathrm{rg}_R(F_1)$. Wir können nun den Elementarteilersatz anwenden und finden eine R-Basis $\{x_1, \ldots, x_n\}$ von F_0 so dass gelten

$$\begin{aligned} F_0 &= Rx_1 \oplus \ldots \oplus Rx_n \\ F_1 &= Rd_1x_1 \oplus \ldots \oplus Rd_1x_n \end{aligned}$$

Aus dem Homomorphiesatz erhalten wir hieraus

$$M \;\cong\; {}^{F_0}\!/_{F_1} \;\cong\; \bigoplus_{i=1}^{n} {}^{R}\!/_{(d_i)}$$

Wegen $\pi^N M = 0$ gilt auch $\pi^N {}^{R}\!/_{(d_i)} = 0$ für alle $i = 1, \ldots, n$. Insbesondere teilt also jedes d_i die Primpotenz π^N. Da R ein Hauptidealbereich ist gibt es zu jedem $i \in \{1, \ldots, n\}$ ein $r_i \in \mathbb{N}$ mit

$$(\pi^{r_i}) \;=\; (d_i)$$

Die Eindeutigkeit bis auf Reihenfolge war der Inhalt einer Übungsaufgabe. □

Folgerung 0.28 *(Hauptsatz über endlich erzeugte abelsche Gruppen)*
Jede endliche abelsche Gruppe ist als $\mathbb{Z}$-Modul isomorph zu einem Produkt zyklischer Gruppen von Primpotenzordnung.

Beweis. Dies ist ein Spezialfall von Satz 0.27 mit $R = \mathbb{Z}$. □

1 Gauß'sche Zahlen

Wir betrachten im Folgenden Untermengen der komplexen Zahlen $\mathbb{C}$. Daher bezeichne i immer die imaginäre Einheit mit $i^2 = -1$. Die Menge

$$\mathbb{Q}(i) \;:=\; \left\{ a + bi \,\middle|\, a, b \in \mathbb{Q} \right\} \;\subset\; \mathbb{C}$$

ist ein Unterkörper von $\mathbb{C}$, denn

$$\mathbb{Q}(i) \;\cong\; \mathbb{Q}[X] \big/ (X^2 + 1)$$

und das Polynom X^2+1 ist irreduzibel in $\mathbb{Q}[X]$. Dies haben wir schon im Lemma .3 in der Einleitung gesehen. Ebenfalls haben wir dort schon den Ring der Gauß'schen Zahlen betrachtet:

Definition 1.1 *(Ring der Gauß'schen Zahlen)*
Wir nennen den Unterring

$$\mathbb{Z}[i] \;:=\; \left\{ a + bi \,\middle|\, a, b \in \mathbb{Z} \right\} \;\subseteq\; \mathbb{Q}(i)$$

den Ring der Gauß'schen Zahlen.

Lemma 1.2 *Die Normfunktion*

$$\begin{aligned} N : \mathbb{Q}(i) &\to \mathbb{Q} \\ z &\mapsto z\overline{z} \end{aligned}$$

mit $\overline{z}$ ist das komplexe Konjugat zu z, wird durch Einschränkung auf den Unterring $\mathbb{Z}[i]$ zu einer Multiplikativen Norm von $\mathbb{Z}[i]$ nach $\mathbb{Z}$.

Beweis. Sei $z = x + yi \in \mathbb{Q}(i)$, dann ist $\overline{z} = x - yi$. Für das Produkt gilt $z\overline{z} = x^2 + y^2$ nach binomischer Formel. Aus der komplexen Analysis ist bekannt, dass die komplexe Konjugation multiplikativ ist, das heißt für alle $w, z \in \mathbb{Q}(i)$ gilt $\overline{wz} = \overline{w} \cdot \overline{z}$. Betrachte nun die Einschränkung, das heißt sei $a + bi \in \mathbb{Z}[i]$, dann ist $N(a + bi) \;=\; a^2 + b^2 \in \mathbb{Z}$. □

Lemma 1.3 *Es gibt nur vier Gauß'sche Einheiten, konkret gilt*

$$(\mathbb{Z}[i])^\times \;:=\; \{\pm 1, \pm i\}$$

Beweis. Sei $u \in \mathbb{Z}[i]$ eine Gauß'sche Zahl, dann ist u genau dann eine Einheit, wenn es eine weitere Gaußsche Zahl $v \in \mathbb{Z}[i]$ so gibt, dass gilt $u \cdot v = 1$. Betrachte die Norm

$$N(uv) \;=\; N(u) \cdot N(v) \;=\; 1$$

Nach Lemma 1.2 sind $N(u)$ und $N(v)$ positive ganze Zahlen, also muss $N(u) = 1$ gelten. Welche Gauß'schen Zahlen haben die Norm 1? Schreibe $u = a + bi$ mit $a, b \in \mathbb{Z}$, dann ist nach der obigen Überlegung $u = a + bi$ genau dann eine Einheit, wenn $a^2 + b^2 = 1$ ist. Dies erfüllen nur die Zahlen $1, -1, i, -i \in \mathbb{Z}[i]$. □

Lemma 1.4 *Für alle $y \in \mathbb{Q}(i)$ gibt es ein $\alpha \in \mathbb{Z}[i]$ derart, dass $N(\alpha - y) \leq \frac{1}{2}$ ist.*

Beweis. Geometrisch betrachtet bilden die Gauß'schen Zahlen ein Punktegitter in der komplexen Ebene mit Abstand 1. Das heißt jede Zahl $y \in \mathbb{Q}(i)$ liegt in einem Quadrat mit Eckpunkten aus $\mathbb{Z}[i]$ der Kantenlänge 1. Den größten Abstand, denn zwei dieser Eckpunkte haben können, ist die Diagonale des Quadrats. Die länge der Diagonale eines Quadrats mit Kantenlänge 1 ist $\sqrt{2}$. Damit gibt es immer einen Eckpunkt, der höchstens $\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$ von y entfernt ist. Sei nun $\alpha \in \mathbb{Z}[i]$ dieser Eckpunkt, dann gilt

$$N(y-\alpha) \;=\; |y-\alpha|^2 \;\leq\; \left(\frac{1}{\sqrt{2}}\right)^2 \;=\; \frac{1}{2}$$

□

Lemma 1.5 *Der Ring der Gauß'schen Zahlen $\mathbb{Z}[i]$ ist euklidisch.*
Das heißt für alle $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$ gibt es Zahlen $q, r \in \mathbb{Z}[i]$ mit $\alpha = q\beta + r$ und $N(r) < N(\beta)$.

Beweis. Seien $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$, dann dürfen wir $\frac{\alpha}{\beta} \in \mathbb{Q}(i)$ betrachten. Nach Lemma 1.4 gibt es ein $q \in \mathbb{Z}[i]$ so dass gilt

$$N\left(\frac{\alpha}{\beta} - q\right) \;\leq\; \frac{1}{2} \;\Leftrightarrow\; N(\alpha - q\beta) \;\leq\; \frac{1}{2} \cdot N(\beta)$$

Setze $r := \alpha - q\beta$, dann ist $N(r) < N(\beta)$ und es gilt

$$q\beta + r \;=\; q\beta + \alpha - q\beta \;=\; \alpha$$

□

Folgerung 1.6 *Der Ring der Gauß'schen Zahlen ist ein Hauptidealring.*

Beispiel 6 *(Größter gemeinsamer Teiler und Euklidischer Algorithmus in $\mathbb{Z}[i]$)*

- *Wir suchen den größten gemeinsamen Teiler von $\alpha = 3 + 4i$ und $\beta = 5 + i$. Betrachten wir die Normen*

  $$N(\alpha) = 9 + 16 = 25 \quad \text{und} \quad N(\beta) = 25 + 1 = 26$$

  fällt auf, dass diese in $\mathbb{Z}$ teilerfremd sind. Hätten α und β einen gemeinsamen Teiler größer als 1, so müsste die Norm dieses Teilers sowohl die Norm von β als auch die Norm von α teilen. Dies kann jedoch nicht sein, also müssen auch α und β teilerfremd sein und ihr größter gemeinsamer Teiler ist also 1.

- *Wir suchen nun den größten gemeinsamen Teiler von $\alpha = 3 + 4i$ und $\beta = 5 + 10i$. Die Normen*

  $$N(\alpha) = 9 + 16 = 25 \quad \text{und} \quad N(\beta) = 25 + 100 = 125$$

  sind nicht Teilerfremd. Betrachte die folgende Rechnung in $\mathbb{Q}(i)$

  $$\begin{aligned} \frac{\beta}{\alpha} \;&=\; \frac{5+10i}{3+4i} \cdot \frac{3-4i}{3-4i} \;=\; \frac{15+40+i(30-20)}{25} \\ &=\; \frac{55+10i}{25} \;=\; \frac{11+2i}{5} \;=\; 2\frac{1}{5} + \frac{2}{5}i \end{aligned}$$

Wie in Lemma 1.5 suchen wir nun eine Zahl, so dass die Norm der Differenz kleiner $\frac{1}{2}$ ist. Wie wir aus der obigen Rechnung ablesen können wird $2 \in \mathbb{Z}[i]$ diese Aufgabe erfüllen, denn

$$N\left(\frac{\beta}{\alpha} - 2\right) \;=\; \frac{1}{25} + \frac{4}{25} \;=\; \frac{1}{5} \;<\; \frac{1}{2}$$

Wir gehen weiter analog zum Beweis des Lemmas vor und setzen $\alpha_1 := \beta - 2\alpha = -1 + 2i$. Untersuche nun, ob α_1 ein Teiler von α in $\mathbb{Z}[i]$ ist. Wir rechnen wieder in $\mathbb{Q}(i)$:

$$\begin{aligned} \frac{\alpha}{\alpha_1} &= \frac{3+4i}{-1+2i} \cdot \frac{-1-2i}{-1-2i} = \frac{-3+9-i(4+6)}{5} \\ &= \frac{5-10i}{5} = 1-2i \;\in \mathbb{Z}[i] \end{aligned}$$

Also teilt α_1 tatsächlich α in $\mathbb{Z}[i]$. Betrachte nun die euklidischen Algoritmus. Es gilt

$$\begin{aligned} \beta \;=\; 5+10i &= 2\cdot\alpha + \alpha_1 \\ &= 2\cdot(3+4i) + (-1+2i) \\ \alpha \;=\; 3+4i &= \alpha_1 \cdot (1-2i) + 0 \\ &= (-1+2i)\cdot(1-2i) + 0 \end{aligned}$$

Damit ist $\alpha_1 = 1 + 2i$ ein größter gemeinsamer Teiler von α und β.

Konvention *Wir bezeichnen nur die positiven Primelemente in $\mathbb{Z}$ als Primzahlen.*

Definition 1.7 *(Rationale Primzahlen)*
Sei $p \in \mathbb{Z}$ eine Primzahl. Falls es ein Primelemt $\pi \in \mathbb{Z}[i]$ so gibt, dass p von π in $\mathbb{Z}[i]$ geteilt wird, dann nennen wir p eine rationale Primzahl.

Satz 1.8 *(Primzahlen in $\mathbb{Z}[i]$)*

1. *Jede Gauß'sche Primzahl, also jedes Primelement in $\mathbb{Z}[i]$, teilt genau eine Primzahl in $\mathbb{Z}$.*
2. *Rationale Primzahlen $p \in \mathbb{Z}$ zerlegen sich wie folgt in $\mathbb{Z}[i]$:*
   - **(a)** *Für $p = 2$ gilt: $2 = (1+i)(1-i) = -i(1+i)^2$*
   - **(b)** *Für $p \equiv 1 \pmod 4$ gilt: $p = \pi_p\overline{\pi_p} = a^2 + b^2$ mit einer Gauß'schen Primzahl $\pi_p = a + ib$*
   - **(c)** *Für $p \equiv 3 \pmod 4$ gilt: p ist prim in $\mathbb{Z}[i]$*

Beweis. Zum Nachweis von **Teil 1** sei $\pi \in \mathbb{Z}[i]$ eine Gauß'sche Primzahl. Dann hat π insbesondere nicht die Norm 1, denn sonst wäre π eine Einheit. Betrachte also Primfaktorzerlegung von $N(\pi)$ in $\mathbb{Z}$. Es gilt

$$N(\pi) \;=\; \pi\overline{\pi} \;=\; \epsilon \cdot \prod_{j=1}^{s} p_j \qquad \text{mit Primzahlen } p_i \in \mathbb{Z} \text{ und } \epsilon \in \{\pm 1\}$$

Da $\mathbb{Z}[i]$ ein Hauptidealring und π ein Primelement in $\mathbb{Z}[i]$ ist gibt es ein $j \in \{1, \ldots, s\}$ mit π teilt p_j. Dann muss aber auch $N(\pi)$ ein Teiler von $N(p_j)$ sein, also gilt $N(\pi) = p$ oder $N(\pi) = p^2$ für eine Primzahl $p \in \mathbb{Z}$.

Vor den Nachweis von **Teil 2** stellen wir eine kurze

Bemerkung 1.9 *Sei $\alpha \in \mathbb{Z}[i]$ mit der Eigenschaft, dass die Norm von α eine Primzahl $p \in \mathbb{Z}$ ist. Dann ist α ein Primelement in $\mathbb{Z}[i]$.*

Beweis. Wie jede Gauß'sche Zahl können wir α als Produkt zweier Gauß'scher zahlen $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$ schreiben. Da die Norm multiplikativ ist gilt dann

$$p \;=\; N(\alpha) \;=\; N(\alpha_1 \cdot \alpha_2) \;=\; N(\alpha_1) \cdot N(\alpha_2)$$

Da $p \in \mathbb{Z}$ eine Primzahl ist, folgt aus obiger Rechnung, dass entweder $N(\alpha_1) = 1$ gilt, also α_1 eine Einheit in $\mathbb{Z}[i]$ ist, oder das $N(\alpha_2) = 1$ gilt, also α_2 eine Einheit in $\mathbb{Z}[i]$ ist. □

Mit dieser Bemerkung folgt **(a)** leicht, denn wir sehen nun sofort, dass $1 + i$ wegen

$$N(1+i) \;=\; (1+i) \cdot (1-i) \;=\; 1+1 \;=\; 2$$

eine Gauß'sche Primzahl ist. Weiter sehen wir auch, dass 2 von $1 + i$ geteilt wird, also eine rationale Primzahl ist.
Für **(b)** seien $p \in \mathbb{Z}$ eine Primzahl und $\pi = a + bi \in \mathbb{Z}[i]$ eine Gauß'sche Zahl mit $N(\pi) = p \neq 2$ und $p \equiv 1 \,(\text{mod } 4)$.
Behauptung -1 ist ein Quadrat in $\mathbb{F}_p$
Beweis. $\mathbb{F}_p^\times$ ist zyklisch, also gibt es ein $\gamma \in \mathbb{F}_p$ mit $< \gamma >= \mathbb{F}_p^\times$ und $\gamma^{p-1} = 1$. Es gilt

$$1 \;=\; \gamma^{p-1} \;=\; \left(\gamma^{\frac{p-1}{2}}\right)^2 \;\Longrightarrow\; \gamma^{\frac{p-1}{2}} \;=\; \pm 1$$

Da die Ordnung von γ gleich der Ordnung von $\mathbb{F}_p^\times$ gleich $p - 1$ ist, kann $\gamma^{\frac{p-1}{2}}$ nicht eins sein. Setze

$$x \;:=\; \gamma^{\frac{p-1}{4}}$$

dann ist $x^2 = -1$ in $\mathbb{F}_p$. ◇
Mit dieser Behauptung gibt es ein $a \in \mathbb{Z}$ mit $a^2 \equiv -1 \,(\text{mod } p)$. Dies heißt aber, dass $a^2 + 1$ von p in $\mathbb{Z}[i]$ geteilt wird. Angenommen p wäre ein Primelement in $\mathbb{Z}[i]$. Da $a^2+1 = (a+i)(a-i)$ von p geteilt wird, würde p dann sowohl $a + i$ als auch $a - i$ in $\mathbb{Z}[i]$ teilen, da p invariant unter der Konjugation ist. Damit teilte p aber auch $2a$ in $\mathbb{Z}[i]$, was zur Folge hätte, dass a modulo p kongruent zu 0 wäre, was falsch ist, da $0 \neq -1 \in \mathbb{F}_p$. Damit kann eine rationale Primzahl p, die modulo 4 kongruent zu 1 ist, in $\mathbb{Z}[i]$ nicht prim sein. Es gibt eine Gauß'sche Primzahl $\pi_1 \in \mathbb{Z}[i]$ die p in $\mathbb{Z}[i]$ teilt, aber nach obiger Überlegung nicht gleich p ist. Damit wird auch $N(p) = p^2$ von $N(\pi_1)$ geteilt. Nach Voraussetzung gilt dann also: $N(\pi_1)$ teilt $\big(N(\pi)\big)^2$. Damit folgt sofort dass $\pi_1 = \pi$ oder $\pi_1 = \overline{\pi}$ und $p = \pi\overline{\pi}$.
Zum Nachweis von **(c)** sei $p \in \mathbb{Z}$ eine Primzahl die modulo 4 kongruent zu 3 ist. Angenommen p wäre nicht prim in $\mathbb{Z}[i]$, dann gäbe es eine Gauß'sche Primzahl $\pi \in \mathbb{Z}[i]$ die p teilt, also Norm $N(\pi) = p$ hat. Nach Teil (b) ist dann $p = \pi \cdot \overline{\pi}$ modulo 4 kongruent zu 1. □

Folgerung 1.10 *Die Primelemente von $\mathbb{Z}[i]$ sind (bis auf Multiplikation mit einer Einheit):*

(i) $1 + i$

(ii) $\pi = a + bi$ *mit* $a > |b|$ *und* $N(\pi) = a^2 + b^2 = p$ *ist prim in* $\mathbb{Z}$ *und* $p \equiv 1$ *(mod* 4*)*

(iii) $\pi = p$ *wobei* $p \in \mathbb{Z}$ *eine Primzahl mit* $p \equiv 3$ *(mod* 4*) ist.*

Definition und Bemerkung 1.11 *Wir definieren die Abbildung*

$$\begin{aligned}\left(\frac{-1}{*}\right) : \mathbb{N} &\to \{0, \pm 1\} \\ n &\mapsto \left(\frac{-1}{n}\right)\end{aligned}$$

durch $\left(\frac{-1}{1}\right) := 1$ *und für eine Primzahl* $p \in \mathbb{Z}$ *setzen wir*

$$\left(\frac{-1}{p}\right) := \begin{cases} 0 & \text{falls } p = 2 \\ 1 & \text{falls } p \equiv 1 \,(\text{mod } 4) \\ -1 & \text{falls } p \equiv 3 \,(\text{mod } 4) \end{cases}$$

Für die oben definierte Abbildung gelten

- $\left(\frac{-1}{*}\right)$ *ist multiplikativ.*
- $\left(\frac{-1}{n}\right) = 0$ *für alle* $n \in \mathbb{N}$*, die von* 2 *geteilt werden.*
- $\left(\frac{-1}{*}\right)$ *ist periodisch modulo* 4*.*

Beweis. Definiere die Abbildung zunächst auch auf allen anderen natürlichen Zahlen, dazu sei zu $n \in \mathbb{N}$

$$n = p_1 \cdot \ldots \cdot p_t$$

die Primfaktorzerlegung. Wir setzen

$$\left(\frac{-1}{n}\right) := \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_t}\right)$$

dann ist $\left(\frac{-1}{*}\right)$ wohldefiniert und die ersten beiden Eigenschaften folgen automatisch. Für die letzte Eigenschaft sei $n \in \mathbb{N}$ ungerade, das heißt 2 teilt nicht n. Sortiere die Primfaktorzerlegung von n in $\mathbb{Z}$ wie folgt

$$n = p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_k \qquad \text{mit } p_j \equiv 1 \ (4) \text{ und } q_j \equiv 3 \ (4)$$

Dann ist

$$n \equiv (-1)^k \pmod 4$$

Damit gilt $\left(\frac{-1}{n}\right) = (-1)^k$ und es ist alles gezeigt, denn

$$\begin{aligned} n \equiv 1 \ (4) &\quad \Leftrightarrow \quad k \text{ ist gerade} \\ n \equiv 3 \ (4) &\quad \Leftrightarrow \quad k \text{ ist ungerade} \end{aligned}$$

□

Anmerkung Die Abbildung $\left(\frac{-1}{*}\right)$ ist ein Beispiel für einen primitiven Dirichlet Charakter modulo 4.

Definition 1.12 *(Norm eines Ideals)*
Sei $\mathfrak{a} \lhd \mathbb{Z}[i]$ *ein Ideal. Da* $\mathbb{Z}[i]$ *ein Hauptidealring ist, gibt es ein* $a \in \mathbb{Z}[i]$ *mit* $\mathfrak{a} = (a)$*. Wir setzen*

$$N(\mathfrak{a}) := a\overline{a}$$

Definition 1.13 *Für $s \in \mathbb{C}$ mit Realteil $\Re(s) > 1$ definieren wir*

$$\zeta(s) \;:=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1.1}$$

$$L\left(s, \left(\frac{-1}{*}\right)\right) \;:=\; \sum_{n=1}^{\infty} \frac{\left(\frac{-1}{n}\right)}{n^s} \tag{1.2}$$

$$\zeta_{\mathbb{Q}(i)}(s) \;:=\; \sum_{\substack{\mathfrak{a} \lhd \mathbb{Z}[i] \\ \mathfrak{a} \neq (0)}} \frac{1}{\left(N(\mathfrak{a})\right)^s} \tag{1.3}$$

Anmerkung In der Vorlesung „analytische Zahlentheorie“ wird gezeigt, dass diese Reihen für $s \in \mathbb{C}$ mit $\Re(s) > 1$ absolut konvergieren und uniform sind auf Kompakta. Die erste Reihe dieser Definition nennen wir auch die Riemannsche ζ-Funktion.

Satz 1.14 *Für $s \in \mathbb{C}$ mit $\Re(s) > 1$ gilt*

$$\zeta_{\mathbb{Q}(i)}(s) \;=\; \zeta(s) \cdot L\left(s, \left(\frac{-1}{*}\right)\right)$$

Beweis. Bezeichne die Menge der Primzahlen in $\mathbb{Z}$ mit $\mathbb{P}$. Mit der geometrischen Reihe gelten

$$\zeta(s) \;=\; \prod_{p \in \mathbb{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) \;=\; \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$$

und

$$\begin{aligned} L\left(s, \left(\frac{-1}{*}\right)\right) \;&=\; \prod_{p \in \mathbb{P}} \left(1 + \frac{\left(\frac{-1}{p}\right)}{p^s} + \frac{\left(\frac{-1}{p}\right)^2}{p^{2s}} + \ldots\right) \;=\; \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\left(\frac{-1}{p}\right)}{p^s}} \\ &=\; \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1\ (4)}} \frac{1}{1 - \frac{1}{p^s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3\ (4)}} \frac{1}{1 + \frac{1}{p^s}} \end{aligned}$$

In Folgerung 1.10 haben wir die Primzahlen in $\mathbb{Z}[i]$ bestimmt. Damit gilt nun für das Produkt

$$\zeta(s) \cdot L\left(s, \left(\frac{-1}{*}\right)\right) \;=\; \frac{1}{1 - \frac{1}{2^s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1\ (4)}} \frac{1}{\left(1 - \frac{1}{p^s}\right)^2} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3\ (4)}} \frac{1}{1 + \frac{1}{p^{2s}}} \tag{1.4}$$

In Satz 1.8 haben wir gesehen, dass es zu jeder Primzahl $p \in \mathbb{P}$ genau ein Primelement in $\pi \in \mathbb{Z}[i]$ gibt mit

$$N(\pi) \;=\; \begin{cases} 2 & \text{falls } p = 2 \\ p & \text{falls } p \equiv 1\ (4) \\ p^2 & \text{falls } p \equiv 3\ (4) \end{cases}$$

Damit können wir in Gleichung (1.4) zu Normen von Primidealen übergehen, und erhalten

$$\zeta(s) \cdot L\left(s, \left(\frac{-1}{*}\right)\right) \;=\; \prod_{(\pi) \in \mathrm{Spec}(\mathbb{Z}[i])} \frac{1}{1 - \frac{1}{N(\pi)^s}} \;=\; \sum_{\substack{\mathfrak{a} \lhd \mathbb{Z}[i] \\ \mathfrak{a} \neq 0}} \frac{1}{N(\mathfrak{a})^s} \;=\; \zeta_{\mathbb{Q}(i)}(s)$$

□

Definition und Bemerkung 1.15 *Für $n \in \mathbb{N}$ setzen wir*

$$R(n) \;:=\; \sharp\left(\left\{ (a,b) \in \mathbb{Z}^2 \;\middle|\; n = a^2 + b^2 \right\} \Big/ \sim \right)$$

wobei $\sim$ die folgende Äquivalenzrelation sei

$$(a,b) \sim (x,y) \;:\Leftrightarrow\; (x,y) \in \big\{(a,b),(-b,a),(-a,-b),(b,-a)\big\}$$

Beweis. Rechne nach, das $\sim$ eine Äquivalenzrelation ist. Zeige also

1. $(a,b) \sim (a,b)$ und
2. falls $(a,b) \sim (d,c)$ gilt, dann gilt auch $(d,c) \sim (a,b)$ sowie
3. aus $(a,b) \sim (d,c)$ und $(d,c) \sim (x,y9$ folgt stets $(a,b) \sim (x,y)$.

Lemma 1.16 *Für $n \in \mathbb{N}$ gilt*

$$R(n) \;=\; \sharp\big\{\; \mathfrak{a} \lhd \mathbb{Z}[i] \;\big|\; N(\mathfrak{a}) = n \,\big\}$$

Beweis. Wenn wir $n \in \mathbb{N}$ als die Summe der Quadrate von zwei ganzen Zahlen a, b darstellen können, dann gilt

$$n \;=\; a^2 + b^2 \;=\; N(a+bi)$$

Weiter wissen wir, dass zwei Elemente in $\mathbb{Z}[i]$ genau dann das selbe Hauptideal erzeugen, wenn sie assoziiert sind, das heißt wenn sie sich nur um eine Einheit unterscheiden. Da $\mathbb{Z}[i]$ ein Hauptidealring ist und die Multiplikation mit einer Einheit die Norm nicht verändert folgt die Bahauptung. □

Satz 1.17 *Für $n \in \mathbb{N}$ gilt*

$$R(n) \;=\; \sum_{\substack{d \in \mathbb{N} \\ d \,|\, n}} \left(\frac{-1}{d} \right)$$

Beweis. Sei $s \in \mathbb{C}$ mit $\Re(s) > 1$. Wir rechnen

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{R(n)}{n^s} \quad &= \quad = \sum_{\substack{\mathfrak{a} \lhd \mathbb{Z}[i] \\ \mathfrak{a} \neq 0}} \frac{1}{N(\mathfrak{a})^s} \;=\; \zeta_{\mathbb{Q}(i)}(s) \\
&\overset{\text{Satz 1.14}}{=} \zeta(s) \cdot L\left(s, \left(\frac{-1}{*}\right)\right) \overset{(*)}{=} \sum_{(k,l) \in \mathbb{N}^2} \frac{1}{k^s} \cdot \frac{\left(\frac{-1}{l}\right)}{l^s} \\
&= \quad \sum_{n=1}^{\infty} \frac{\sum\limits_{d \,|\, n} \left(\frac{-1}{d}\right)}{n^s}
\end{aligned}$$

Wobei wir für die Gleichheit bei $(*)$ benutzen, dass die Abbildung $\mathbb{N} \times \mathbb{N} \ni (k,l) \mapsto kl \in \mathbb{N}$ bijektiv ist. □

Beispiel 7 *Wir wollen natürliche Zahlen untersuchen.*

($n = 99$) *n hat die Primfaktorzerlegung $n = 99 = 3^2 \cdot 11$, damit erhalten wir die Menge der natürlichen Teiler von n erhalten wir daraus*

$$T(n) \;=\; \{1, 3, 3^2, 11, 3 \cdot 11, 3^2 \cdot 11\}$$

Mit dem soeben gezeigten Satz gilt dann

$$R(n) \;=\; \sum_{d \in T(n)} \left(\frac{-1}{d}\right) \;=\; 1 - 1 + 1 - 1 + 1 - 1 \;=\; 0$$

Also lässt sich n nicht als Summe zweier Quadrate in $\mathbb{Z}$ darstellen.

($n = 45$) *Die Primfaktorzerlegung von n ist $n = 45 = 3^2 \cdot 5$. Als Menge der natürlichen Teiler von n erhalten wir daraus*

$$T(n) \;=\; \{1, 3, 3^2, 5, 3 \cdot 5, 3^2 \cdot 5\}$$

Wir betrachten wieder die Summe

$$R(n) \;=\; \sum_{d \in T(n)} \left(\frac{-1}{d}\right) \;=\; 1 - 1 + 1 - 1 + 1 + 1 \;=\; 2$$

Damit muss es also zwei Möglichkeiten geben $n = 45$ als die Summe zweier Quadrate darzustellen. Leicht sehen wir, dass sich 5 als mit $5 = 1 + 2^2$ als Summe zweier Quadrate schreiben lässt. Damit erhalten wir

$$45 \;=\; 3^2 \cdot 5 \;=\; 3^2 \cdot (1 + 2^2) \;=\; 3^2 + 6^2$$

die erste Lösung. Nach Definition 1.15 sind (a, b) und (b, a) nicht in Relation, also ist die durch Vertauschung gewonnene Darstellung $6^2 + 3^2 = 45$ die andere Möglichkeit.

2 Ganze algebraische Zahlen

In diesem Kapitel werden wir ganze Zahlen in Ringen betrachten. Wir werden dabei viele Parallelen zu algebraischen Zahlen über einem Körper entdecken können. Diese Ähnlichkeit beginnt schon mit der grundlegenden

Definition 2.1 *(Ganze Zahlen)*
Sei A ein Ring und L ein Körper mit $A \subseteq L$. Wir nennen $b \in L$ ganz über A, falls es ein normiertes Polynom

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_o \;\in A[X]$$

so gibt, dass $f(b) = 0$ ist.

Anmerkung Die Voraussetzung, das unsere Ringe immer Unterringe von Körpern sind, impliziert bereits, dass wir nur kommutative Integritätsringe betrachten.

Beispiel 8 *Mit $A = \mathbb{Z}$ und $L = \mathbb{Q}$ gilt: $b \in \mathbb{Q}$ ist genau dann ganz über $\mathbb{Z}$, wenn $b \in \mathbb{Z}$ ist.*

Wir wollen zeigen, dass wir mit unserer Ganzheits-Definition den im Beispiel betrachteten Sachverhalt gültig verallgemeinern können.

Bemerkung 2.2 *Sei A ein Hauptidealbereich und $L = \mathrm{Quot}(A)$ sein Quotientenkörper, es gilt: Genau dann ist $b \in L$ ganz über A, wenn $b \in A$ ist.*

Beweis. Sei $b \in L\backslash\{0\}$, dann gibt es teilerfremde Elemente $c, d \in A\backslash\{0\}$ so dass wir b darstellen können als $b = \frac{c}{d}$. Nach Definition 2.1 ist b genau dann ganz über A, wenn es Elemente $a_0, \ldots, a_{n-1} \in A$ so gibt, dass $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$ gilt. Betrachte

$$\begin{aligned} 0 &= b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 && \mid \cdot d^n \\ \Leftrightarrow 0 &= c^n + a_{n-1}c^{n-1}d + \ldots + a_1 b d^{n-1} + a_0 d^n \\ \Leftrightarrow c^n &= d \cdot \left(a_{n-1}c^{n-1} + \ldots + a_1 b d^{n-2} + a_0 d^{n-1}\right) \end{aligned}$$

Also wird c^n von d geteilt. Dann teilt d aber auch c, weshalb, weil d und c teilerfremd sind, d bereits eine Einheit von A sein muss. Damit folgt sofort, dass $b \in A$ ist. □

Beispiel 9 *Mit $A = \mathbb{Z}[i]$ und $L = \mathbb{Q}(i)$ erhalten wir aus der Bemerkung sofort, dass $b \in \mathbb{Q}(i)$ genau dann ganz über $\mathbb{Z}[i]$ ist, wenn b ein Element in $\mathbb{Z}[i]$ ist, denn $\mathbb{Z}[i]$ ist ein Hauptidealbereich.*

Satz 2.3 *(Satz über ganze Elemente)*
Seien A ein Ring und L ein Körper mit $A \subset L$. Dann ist $\alpha \in L$ genau dann ganz über A, wenn es einen endlich erzeugten A-Modul $0 \neq M \subseteq L$ mit $\alpha M \subseteq M$ gibt.

Beweis. Nemen wir zunächst an, dass $\alpha \in L$ ganz über A sei. Nach Definition gibt es dann Elemente $a_0, \ldots, a_{n-1} \in A$ mit $f(\alpha) := \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Setze

$$M \;:=\; A + A\alpha + A\alpha^2 + \ldots + A\alpha^{n-1} \;\subseteq L$$

Multiplizieren wir diesen Modul nun mit α verschieben sich die Exponenten um je einen nach oben, das heißt

$$\alpha M \;=\; A\alpha + A\alpha^2 + A\alpha^2 + \ldots + A\alpha^n$$

Da aber $f(\alpha) = 0$ gilt, ist α^n bereits in M enthalten, also gilt $\alpha M \subseteq M$.
Nimm nun an, dass es einen endlich erzeugten A-Modul

$$0 \neq M := A\alpha_1 + \ldots + A\alpha_n \qquad \text{mit } \alpha_i \in L$$

mit $\alpha M \subseteq M$ gibt. Unter diesen Voraussetzungen erhalten wir n Gleichungen

$$\begin{aligned} \alpha \cdot \alpha_1 &= a_{1,1}\alpha_1 + \ldots + a_{1,n}\alpha_n \\ \vdots & \qquad\qquad \vdots \\ \alpha \cdot \alpha_n &= a_{n,1}\alpha_n + \ldots + a_{n,n}\alpha_n \end{aligned}$$

Fasse die Koeffizienten $a_{i,j}$ in natürlicher Weise in der Matrix $B := (a_{i,j})_{1 \leq i,j \leq n}$ zusammen. Bezeichne E die $(n \times n)$-Einheitsmatrix und $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n)^t$), dann erhalten wir das homogene Gleichungssystem

$$(B - \alpha E) \cdot \underline{\alpha} = 0$$

Damit gilt $\det(B - \alpha E) = 0$ und α ist Nullstelle von $f(X) := \det(B - XE) \in A[X]$. Dieses Polynom hat den Leitkoeffizienten $(-1)^n \in A^\times$, also ist α ganz über A. □

Definition 2.4 *(Ganzer Abschluss)*
Sei L ein Körper und $A \subseteq L$ ein Unterring, dann nennen wir

$$\overline{A} := \left\{ \alpha \in L \,\middle|\, \alpha \text{ ist ganz über } A \right\}$$

einen ganzen Abschluss von A in L. Weiter heißt A ganz abgeschlossen in L, wenn $A = \overline{A}$ ist.
Ein Ring A heißt ganz abgeschlossen (ohne Nennung eines Oberkörpers) wenn A ganz abgeschlossen in seinem Quotientenkörper $\mathrm{Quot}(A)$ *ist.*

Beispiel 10 *Ein ganzer Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(i)$ ist $\mathbb{Z}[i]$ aber $\mathbb{Z}$ ist ganz abgeschlossen, denn $\mathbb{Z} = \overline{\mathbb{Z}}$ im Quotientenkörper* $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

Dieses Beispiel zeigt zwei Dinge: Zum einen kann ein Ring ganz abgeschlossen - also im Quotientenkörper ganz abgeschlossen - sein, aber je nach Körper in dem wir diesen Ring betrachten größere ganze Abschlüsse besitzen. Zum Anderen sind offenbar manche ganzen Abschlüsse selber Ringe. Den letzten Umstand wollen wir im folgenden Satz genauer untersuchen.

Definition 2.5 *(Ganze Ringe)*
Sei L ein Körper und seien $A \subseteq B \subseteq L$ zwei Unterringe. Wir sagen B ist ganz über A, wenn jedes Element $b \in B$ ganz über A ist.

Satz 2.6 *Sei L ein Körper und $A \subset L$ ein Unterring. Bezeichne B einen ganzen Abschluss von A in L, dann ist B ein Ring.*

Beweis. Seien $x, y \in B$. Da x und y ganz sind über A gibt es nach Satz 2.3 zwei endlich erzeugte A-Moduln $M, N \subseteq L$ mit $xM \subseteq M$ und $yN \subseteq N$. Setze

$$MN := M \cdot N := \left\{ \sum_{i=1}^{d} m_i n_i \,\middle|\, d \in \mathbb{N} \wedge m_i \in M \wedge n_i \in N \right\}$$

Da A kommutativ ist, ist leicht zu sehen, dass MN ein A-Modul ist. Sind weiter $\{x_1 \ldots, x_s\} \subseteq M$ und $\{y_1, \ldots, y_t\} \subseteq N$ zwei A-Erzeugendensysteme von M und N, so wird MN von der Menge $\{x_1, \ldots, x_s, y_1, \ldots, y_t\}$ über A endlich erzeugt.

Behauptung Es gelten $(x+y) \cdot MN \subseteq MN$ und $xy \cdot MN \subseteq MN$.

Beweis. Betrachte

$$\begin{aligned} (x+y) \cdot \sum_{i=1}^{d} m_j\, n_j &= \sum_{i=1}^{d} \underbrace{x\, m_i}_{\in M} n_i + \sum_{i=1}^{d} \underbrace{y\, n_i}_{\in N} m_i \qquad \in MN \\ (xy) \cdot \sum_{i=1}^{d} m_j\, n_j &= \sum_{i=1}^{d} \underbrace{x\, m_i}_{\in M} \underbrace{y\, n_i}_{\in N} \qquad \in MN \end{aligned}$$

$\diamond$

Damit gilt für alle $x, y \in B$, dass auch $x+y$ und $x \cdot y$ ganz über A sind und damit in B liegen. Da alle Elemente aus A ganz über A sind, und A ein Ring ist, sind $0, 1 \in B$ klar. $\square$

Bisher haben wir nur ganze Zahlen betrachtet. Wir haben als Parallele zu den algebraischen Zahlen feststellen könen, dass ganze Zahlen Nullstellen normierter Polynome sind. Nun wollen wir untersuchen ob wir noch mehr Zusammenhänge finden können.

Lemma 2.7 *Sei A ein Integritätsring und $K = \mathrm{Quot}(A)$ sein Quotientenkörper sowie L/K eine algebraische Körpererweiterung. Bezeichne B einen ganzen Abschluss von A in L, dann gibt es für alle $\lambda \in L$ Elemente $b \in B$ und $a \in A$ mit $\lambda = \frac{b}{a}$. Insbesondere ist $L = \mathrm{Quot}(B)$ der Quotientenkörper von B.*

Beweis. Sei $\lambda \in L$, dann ist λ algebraisch über K. Also gibt es $k_0, \ldots\ k_{n-1} \in K$ mit

$$\lambda^n + k_{n-1}\lambda^{n-1} + \ldots + k_0 \;=\; 0$$

Da $K = \mathrm{Quot}(A)$ der Quotientenkörper von A ist, gibt es ein $a \in A \backslash \{0\}$ mit $a \cdot k_i \in A$ für alle $i = 0, \ldots, n-1$. Multiplizieren wir die oben erhaltene Gleichung nun mit a^n durch so gilt

$$(a\lambda)^n + k_{n-1}a(a\lambda)^{n-1} + \ldots + k_0 a^n \;=\; 0$$

Damit haben wir ein normiertes Polynom in $A[X]$ gefunden, das $a\lambda$ als Nullstelle hat, also ist $a\lambda$ ganz über A. $\square$

Anmerkung Dieses Lemma zeigt ausserdem $L = B \otimes_A K$.
(Hierzu siehe eine der kommenden Übungsaufgaben)

Bemerkung 2.8 *Sei L ein Körper und $A \subseteq L$ ein Unterring. Dann sind $b_1, \ldots, b_n \in L$ genau dann ganz über A, wenn $B = A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul ist. Wobei $A[b_1, \ldots, b_n]$ das Bild von $A[X_1, \ldots, X_n]$ unter der Evaluationsabbildung sei, das heißt $A[b_1, \ldots, b_n] := \mathrm{Im}(\mathrm{ev})$ mit*

$$\begin{aligned} \mathrm{ev} : A[X_1, \ldots, X_n] &\to L \\ X_i &\mapsto b_i \end{aligned}$$

Beweis. Angenommen $B = A[b_1, \ldots, b_n]$ ist endlich erzeugter A-Modul, dann ist nichts zu zeigen, denn

$$X_i \cdot A[X_1, \ldots, X_n] \subseteq A[X_1, \ldots, X_n] \qquad \text{für alle } i = 1, \ldots, n$$

Also ist $b_i B \subseteq B$ und für jedes i und damit sind alle b_i ganz über A.
In der anderen Richtung ist mehr zu zeigen. Seien nun also $b_1, \ldots, b_n$ ganz über A. Wir wollen einen Induktionsbeweis führen. Für den Induktions Anfang gilt: Für jedes über A ganze Element $b \in L$ gibt es ein normiertes Polynom $p \in A[X]$ mit $\deg(p) = d$, so dass gilt

$$A[X]/(p) \twoheadrightarrow A[b]$$

Das heißt die Menge $\{1, b, b^2, \ldots, b^d\}$ erzeugt $A[b]$ als A-Modul.
Für den Induktionsschritt nimm an, dass $R = A[b_1, \ldots, b_{n-1}]$ ein endlich erzeugter A-Modul ist. Beachte, dass R selber ein Ring ist, also gilt nach dem Induktionsanfang, dass $R[b_n]$ ein endlich erzeugter R-Modul ist, denn wegen $A[X] \subset R[X]$ ist b_n auch ganz über R. Da R als A-Modul endlich erzeugt ist, ist dann auch $R[b_n] = A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt. □

Lemma 2.9 *Sei L ein Körper und seien $A \subseteq B \subseteq C \subseteq L$ Unterringe, dann gilt: Ist B ganz über A und ist weiter C ganz über B, dann ist C auch ganz über A.*

Beweis. Sei $c \in C$, dann gibt es Elemente $b_0, \ldots, b_{n-1} \in B$ mit

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

Da B ganz über A ist, ist $A[b_0, \ldots, b_{n-1}]$ nach Bemerkung 2.8 ein endlich erzeugter A-Modul. Da c ganz über B ist, ist dann auch $A[b_0, \ldots, b_{n-1}][c]$ ein endlich erzeugter A-Modul. Mit der Bemerkung ist c dann auch ganz über A. □

Bemerkung 2.10 *(Ganze Abschlüsse von $\mathbb{Z}$ in Zahlkörpern vom Grad 2)*
Sei $K/\mathbb{Q}$ eine Körpererweiterung von Grad 2 und $\mathcal{O}_K$ ein ganzer Abschluss von $\mathbb{Z}$ in K. Dann gibt es ein quadratfreies $d \in \mathbb{Z}$ derart, dass $K = \mathbb{Q}(\sqrt{d})$ ist und es gilt

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \equiv 3, 2 \quad (4) \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & \text{falls } d \equiv 1 \quad (4) \end{cases}$$

Beweis. Wir konstruieren zunächst $d \in \mathbb{Z}$. Sei dazu $\alpha \in K \setminus \mathbb{Q}$, dann ist $\{1, \alpha\}$ eine $\mathbb{Q}$-Basis von K. Wir können nun zum Beispiel α^2 bezüglich dieser Basis darstellen als $\alpha^2 = a\alpha + b$ mit $a, b \in \mathbb{Q}$. Setze $\alpha' := \alpha - \frac{a}{2}$, dann ist $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$. Betrachten nun noch einmal α^2

$$\begin{aligned} & \alpha^2 = \left(\alpha' + \frac{a}{2}\right)^2 = a\left(\alpha' + \frac{a}{2}\right) + b \\ \Rightarrow \quad & \alpha'^2 + a\alpha' + \frac{a^2}{4} = a\alpha' + \frac{a^2}{2} + b \\ \Rightarrow \quad & \alpha'^2 = \frac{a^2}{4} + b =: q \in \mathbb{Q} \end{aligned}$$

Damit erhalten wir $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha') = \mathbb{Q}(\sqrt{q})$. Wir können dieses $q \in \mathbb{Q}$ nun darstellen als

$$q = \frac{x^2 \cdot d}{y} \qquad \text{mit } \mathrm{ggT}(x^2 d, y) = 1 \text{ und } x, y, d \in \mathbb{Z} \text{ und } d \text{ ist quadratfrei}$$

Wir erhalten schließlich $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha') = \mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{d})$ und haben das gesuchte quadratfreie $d \in \mathbb{Z}$ gefunden. Nun wollen wir $\mathcal{O}_K$ genauer untersuchen. Da $K/\mathbb{Q}$ insbesondere galoisch vom Grad 2 ist, gibt es ausser der Identität nur die Konjugation

$$\sigma : K \ni a + b\sqrt{d} \mapsto a - b\sqrt{d} \in K$$

in der Galoisgruppe von $K/\mathbb{Q}$. Für $\beta \in K$ gilt:

$$\beta \in \mathcal{O}_K \;\Leftrightarrow\; \sigma(\beta) \in \mathcal{O}_K$$

denn aus der Galoistheorie wissen wir

$$\beta^n + \sum_{i=0}^{n-1} \beta^i a_i \;=\; 0 \;\Leftrightarrow\; \sigma(\beta)^n + \sum_{i=0}^{n-1} \sigma(\beta)^i a_i \;=\; 0$$

Definiere die Abbildungen Spur (Tr) und Norm (N) via

$$\begin{array}{rccl} Tr: & K & \to & \mathbb{Q} \\ \beta = a + b\sqrt{d} & \mapsto & \beta + \sigma(\beta) \;=\; a + b\sqrt{d} + a - b\sqrt{d} \;=\; 2a & \\ N: & K & \to & \mathbb{Q} \\ \beta = a + b\sqrt{d} & \mapsto & \beta \cdot \sigma(\beta) \;=\; (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) \;=\; a^2 - b^2 d & \end{array}$$

Für alle $\beta \in K$ gilt $\beta^2 - Tr(\beta) \cdot \beta + N(\beta) \;=\; 0$, also ist β genau dann ganz über $\mathbb{Z}$ (also $\beta \in \mathcal{O}_K$), wenn $Tr(\beta) \in \mathbb{Z}$ und $N(\beta) \in \mathbb{Z}$ gelten. Das heißt $\beta = a + b\sqrt{d}$ ist genau dann ganz über $\mathbb{Z}$, wenn $2a$ und $a^2 + b^2 d$ ganze Zahlen sind. Sei $\beta = a + b\sqrt{d} \in \mathcal{O}_K$. Setze $e := 2a$ und $f := 2b$, dann sind e und $\frac{e^2}{4} - \frac{df^2}{4}$ ganze Zahlen. Also gilt $df^2 \in \mathbb{Z}$ und, da d quadratfrei ist, sogar $f \in \mathbb{Z}$. Insgesamt erhalten wir

$$e^2 - 4f^2 \in 4\,\mathbb{Z} \quad \text{und} \quad e^2 \;\equiv\; df^2 \;\; (4) \tag{2.5}$$

Wir erinnern uns an unsere Defninitionen $e = 2a$ und $f = 2b$ und betrachten d modulo 4.

Falls $d \equiv 1 \;(4)$ **gilt,** so erhalten wir aus Gleichung (2.5), dass genau dann $a^2 \;\equiv\; b^2 \;(4)$ ist, wenn $a \equiv b \;(2)$ ist.

Falls $d \equiv 2 \;(4)$ **oder** $d \equiv 3 \;(4)$ **gilt,** dann erhalten wir aus Gleichung (2.5), dass genau dann $a \;\equiv\; b \;(4)$ ist, wenn $a^2 \equiv b^2 d \;(4)$ ist.

Wir können also $\mathcal{O}_K$ beschreiben als

$$\mathcal{O}_K \;=\; \left\{ \frac{a + b\sqrt{d}}{2} \,\middle|\, a, b \in \mathbb{Z} \wedge a \equiv b \;(2) \right\} \;=\; \left\{ a' + b' \left(\frac{1 + \sqrt{d}}{2} \right) \,\middle|\, a', b' \in \mathbb{Z} \right\}$$

falls $d \equiv 1 \;(4)$ gilt, und als

$$\mathcal{O}_K \;=\; \left\{\, a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Z} \,\right\}$$

falls $d \equiv 2 \;(4)$ oder $d \equiv 3 \;(4)$ gelten. □

Beispiel 11 *In unserem Standartbeispiel $K = \mathbb{Q}(i)$ erhalten wir wegen $i^2 = -1$ und $-1 \equiv 3 \;(4)$ auch auf diesem Wege wieder den Ring der Gauß'schen Zahlen $\mathbb{Z}[i]$ als ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(i)$.*

3 Körpertheorie (Wdh.)

Im Folgenden wollen wir ein paar körpertheoretische Ergebnisse der Algebra I Vorlesung zur Verfügung stellen. In diesem kurzen Abschnitt werden einige Tatsachen nur ohne Beweis angegeben, andere Beweise sind nur skizziert. Für ein genaues Studium betrachte zum Beispiel [L4].

Satz 3.1 *(Ergebnisse der Körpertheorie)*
Sei L/K eine Körpererweiterung, dann gelten:

1. *Per Definition ist L/K genau dann separabel, wenn für alle $\alpha \in L$ gilt: Das zu α gehörige Minimalpolynom $m_\alpha \in K[X]$ hat keine mehrfache Nullstelle.*
   Dies ist genau dann der Fall, wenn
   $$\mathrm{ggT}(m_\alpha, m'_\alpha) \;=\; 1$$
   also wenn m_α und seine formale Ableitung m'_α teilerfremd in $K[X]$ sind.
   Ist K ein Körper der Charakteristik Null, so ist jeder Erweiterungskörper L über K separabel.

2. *Per Definition ist L/K genau dann normal, wenn für alle normierten und irreduzieblen Polynome $f \in K[X]$ gilt: Hat f eine Nullstelle in L, so zerfällt f über L in Linearfaktoren.*

3. *Sei $\alpha \in L$ ein Element, dann ist $K(\alpha)$ ein Zwischenkörper von K und L, also $K \subseteq K(\alpha) \subseteq L$. Die Abbildung*
   $$\begin{array}{rcl} K[X]\big/_{(m_\alpha)} & \to & K(\alpha) \\ X & \mapsto & \alpha \end{array}$$
   ist ein Körperisomorphismus über K. Damit erhalten wir eine Bijektion
   $$\begin{array}{ccc} \mathrm{Hom}_K\big(K(\alpha), L\big) & \overset{1:1}{\longleftrightarrow} & \big\{\, \beta \in L \,\big|\, m_\alpha(\beta) = 0 \,\big\} \\ X & \mapsto & \beta \end{array}$$
   Also gibt es ebensoviele K-lineare Abbildungen von $K(\alpha)$ nach L, wie es Nullstellen vom Minimalpolynom m_α in L gibt.
   Falls L/K normal ist, zerfällt das Polynom m_α über L in Linearfaktoren, das heißt
   $$m_\alpha(X) \;=\; (X - a_1) \cdot \ldots \cdot (X - a_n) \;\in L[X]$$
   Ist weiter $K(\alpha)/K$ separabel, so sind die Nullstellen a_i sogar paarweise verschieden. Es gilt
   $$\sharp\,\mathrm{Hom}_K\big(K(\alpha), L\big) \;=\; n \;=\; \deg(m_\alpha) \;=\; \big[K(\alpha) : L\big]$$
   Damit erhalten wir im Fall L/K normal und $K(\alpha)/K$ separabel die Darstellung
   $$m_\alpha(X) \;=\; \prod_{\sigma \in \mathrm{Hom}_K(K(\alpha), L)} \big(X - \sigma(\alpha)\big)$$

4. *Sei L/K endlich und separabel und sei weiter L'/L eine beliebige normale Körpererweiterung, dann gilt*
   $$\sharp\,\mathrm{Hom}_K(L, L') \;=\; [L : K]$$

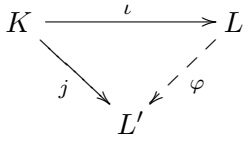
5. *Sei L/K eine separable und normale Körpererweiterung, dann nennen wir L/K eine Galoiserweiterung.*

Ein weiters wichtiges Konstrukt der Körpertheorie sind die algebraischen Zahlen. Im Vorangegangenen Abschnitt haben wir ganze Zahlen und ganze Abschlüsse betrachtet. Wir haben gesehen, dass es Parallelen zwischen algebraischen und ganzen Zahlen gibt. Aus der Körpertheorie kennen wir das dem ganzen Abschluss ähnliche Konzept des algebraischen Abschlusses. Wir wollen diese Erinnerung etwas auffrischen, dazu die folgende

Definition 3.2 *(Algebraischer Abschluss)*
Sei K ein Körper. Ein algebraischer Abschluss von K ist ein Paar (L, ι), wobei L ein Körper und $\iota : K \hookrightarrow L$ eine Einbettung[4] *ist, das die folgenden Eigenschaften erfüllt:*

(i) *L ist algebraisch Abgeschlossen, das heißt jedes Polynom in $L[X]$ zerfält über L in Linearfaktoren*

(ii) *Zu jedem weiteren Paar (L', j), mit einem algebraisch abgeschlossenem Körper L' und einer Einbettung $j : K \to L'$, gibt es einen K-Homomorphismus $\varphi : L \to L'$ so dass das folgende Diagramm kommutiert*



Diese Eigenschaft nennen wir die universelle Abbildungseigenschaft des algebraischen Abschlusses.

Satz 3.3 *Zu jedem Körper K existiert ein algebraischer Abschluss und ist bis auf Isomorphie eindeutig bestimmt.*

Beweisskizze. Die Existenz wird konstruktiv gezeigt. Dazu wird K Schrittweise erweitert, bis jede Nullstelle enes jeden Polynomes in $K[X]$ in L liegt. Die Eindeutigkeit folgt auf bekannte Weise aus der universellen Abbildungseigenschaft.

Notation 3.4 *Sei K ein Körper, dann schreiben wir $\overline{K}$ für seinen algebraischen Abschluss.*

Bemerkung 3.5 *Sei K ein Körper, dann ist die Körpererweiterung $\overline{K}/K$ normal.*

Bemerkung 3.6 *Der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ ist viel kleiner (bezüglich der Enthaltenseinsrelation) als $\mathbb{C}$.*

Beweis. π und e sind transzendent über $\mathbb{Q}$, damit auch nicht in $\overline{\mathbb{Q}}$ enthalten. □
Genauer gilt sogar: $\overline{\mathbb{Q}}$ ist abzählbar und $\mathbb{C}$ ist es nicht.

[4] Einbettung = injektiver Homomorphismus

Kapitel III

Zahlkörper und Ganzheitsringe

4 Spur und Norm

Der Begriff der Norm ist uns im Laufe der Vorlesung bereits mehrfach begegnet. In Abschnitt 1 definierten wir die Normabbildung

$$\begin{array}{rcl} N : \mathbb{Q}(i) & \to & \mathbb{Q} \\ z & \mapsto & z\overline{z} \end{array}$$

und auch in der Bemerkung über ganze Abschlüsse in Zahlkörpern von Grad 2 2.10 haben wir eine Normfunktion definiert. Die Spur kennen wir noch aus der linearen Algebra als Spur einer Matrix. Beide Funktionen wollen wir hier in allgemeiner Form definieren und einige ihrer Eigenschaften studieren. Wir beginnen mit einer

Definition 4.1 *(Spur und Norm)*
Sei L/K eine endliche Körpererweiterung. Für alle $\alpha \in L$ ist die Multiplikation mit α

$$\begin{array}{rcl} A_\alpha : L & \to & L \\ x & \mapsto & \alpha \cdot x \end{array}$$

eine K-lineare Abbildung. Wir definieren

$$\begin{array}{rcll} Tr_K^L(\alpha) & := & Tr(A_\alpha) & \text{als die Spur von } \alpha \\ N_K^L(\alpha) & := & \det(A_\alpha) & \text{als die Norm von } \alpha \end{array}$$

Bemerkung 4.2 *(Triviale Eigenschaften)*

1. *Die Abbildung $Tr_K^L : L \to K$ ist ein Gruppenhomomorphismus von $(L, +)$ nach $(K, +)$.*
2. *Die Abbildung $N_K^L : L^* \to K^*$ ist ein Gruppenhomomorphismus von $(L^*, \cdot)$ nach $(K^*, \cdot)$.*
3. *Ist $\alpha \in K$, so gilt $A_\alpha = \alpha \cdot E$ wobei E die Einheitsmatrix bezeichne. Damit erhalten wir*

$$Tr_K^L(\alpha) \;=\; [L : K] \cdot \alpha \quad \text{und} \quad N_K^L(\alpha) \;=\; \alpha^{[L:K]}$$

4. *Sei L/K eine Körpererweiterung vom Grad n und bezeichne $\chi_\alpha(X) \in K[X]$ das charakteristische Polynom von A_α, also*

$$\chi_\alpha(X) := \det(XE - A_\alpha) = X^n + \sum_{i=0}^{n-1} a_i X^i$$

dann gelten

$$Tr_K^L(\alpha) = -a_{n-1} \quad \text{und} \quad N_K^L(\alpha) = (-1)^n a_0$$

Beweis. Es ist nichts zu zeigen.
Als Vorbereitung für den nächsten wichtigen Satz ziehen wir einen technischen Schritt in einem allgemeinerem Lemma nach vorne:

Lemma 4.3 *Sei R ein Ring und seien $a_0, \ldots, a_{n-1} \in R$, dann hat jede $n \times n$-Matrix der Form*

$$A = \begin{pmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ \vdots & & \ddots & 1 & \\ & & & 0 & 1 \\ -a_0 & -a_1 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

mit Einsen auf der ersten oberen Nebendiagonalen, ein charakteristisches Polynom der Form

$$\chi_A(X) = X^n + a_{n-1}X^{n-1} + \ldots + Xa_1 + a_0 \in R[X]$$

Beweis. Wir wollen zeigen, dass

$$\chi_A(X) = \det(XE - A) = \det \begin{pmatrix} X & -1 & & & \\ 0 & \ddots & \ddots & & \\ \vdots & & \ddots & -1 & \\ & & & X & -1 \\ a_0 & a_1 & \ldots & a_{n-2} & X + a_{n-1} \end{pmatrix}$$

von der oben behaupteten Form ist. Dies wollen wir per Induktion über die Dimension n beweisen.

Falls ($n = 1$): Es ist nichts zu zeigen, denn $A = (-a_0)$ und $\det(XE - A) = X + a_0$.

Falls ($n = 2$): Es gilt

$$\det(XE - A) = \det \begin{pmatrix} X & -1 \\ a_0 & X + a_1 \end{pmatrix} = X(X + a_1) + a_0 = X^2 + a_1 X + a_0$$

Falls ($n = 3$): Auch hier gilt die Behauptung, denn

$$\det(XE - A) = \det \begin{pmatrix} X & -1 & 0 \\ 0 & X & -1 \\ a_0 & a_1 & X + a_2 \end{pmatrix} = X^3 + a_2 X^2 + a_1 X + a_0$$

Falls ($n > 3$): Angenommen für alle $m < n$ gelte die Behauptung. Mit dem Laplace'schen Entwicklungssatz gilt dann

$$\begin{aligned}
\det(XE - A) &= X \cdot \det \underbrace{\begin{pmatrix} -1 & & & \\ X & \ddots & & \\ & \ddots & -1 & \\ & & X & -1 \\ a_1 & \dots & a_{n-2} & X + a_{n-1} \end{pmatrix}}_{= X^{n-1} + \sum_{i=0}^{n-2} a_{i+1} X^i} \\
&\quad + (-1)^{n-1} \cdot a_0 \cdot \det \underbrace{\begin{pmatrix} -1 & & \\ X & \ddots & \\ & \ddots & -1 \\ & & X \end{pmatrix}}_{= (-1)^{n-1}} \\
&= X^n + \sum_{i=0}^{n-1} a_i X^i
\end{aligned}$$

□

Satz 4.4 *Sei L/K eine endliche separable Körpererweiterung und sei $\alpha \in L$ ein Element mit zugehörigem Minimalpolynom $\mathfrak{m}_\alpha \in K[X]$. Es gelten*

$$\chi_\alpha(X) = \mathfrak{m}_\alpha(X)^{[L:K(\alpha)]} = \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \big(X - \sigma(\alpha)\big) \tag{4.1}$$

$$Tr_K^L(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(\alpha) \tag{4.2}$$

$$N_K^L(\alpha) = \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(\alpha) \tag{4.3}$$

Beweis. Wir zeigen zunächst Gleichung (4.1), da wir die anderen beiden Gleichungen aus dieser ableiten wollen. Dazu konstruieren wir eine K-Basis von L, so dass A_α besonders „einfach" wird. Sei

$$\mathfrak{m}_\alpha(X) =: X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

Die Menge $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ ist eine K-Basis von $K(\alpha)$. Wähle nun eine Basis $\{\beta_1, \ldots, \beta_m\}$ von L als $K(\alpha)$-Vektorraum, dann ist

$$B := \big\{\beta_1, \beta_1\alpha, \beta_1\alpha^2, \ldots, \beta_1\alpha^{n-1}, \beta_2, \beta_2\alpha, \ldots, \beta_m\alpha^{n-1}\big\}$$

eine Basis von L als K-Vektorraum. Betrachte für $i \in \{1, \ldots, m\}$

$$\alpha \cdot \big(\beta_i \alpha^j\big) = \beta_i \alpha^{j+1} \begin{cases} \in B & \text{falls } j < n-1 \\ \beta_i(-a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}) & \text{falls } j = n-1 \end{cases}$$

Also hat A_α bezüglich B die Blockmatrixform

$$A_\alpha \;=\; \begin{pmatrix} \boxed{M} & & & \\ & \boxed{M} & & \\ & & \ddots & \\ & & & \boxed{M} \end{pmatrix}$$

Mit einer $n\times n$-Matrix M der Form

$$M \;=\; \begin{pmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ \vdots & & \ddots & 1 & \\ & & & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

Mit dem zuvor gezeigtem Lemma 4.3 gilt dann $\chi_\alpha \;=\; \mathfrak{m}_\alpha^m$ mit $m = [L : K(\alpha)]$.

Betrachte das nebenstehende Diagramm:
Da L/K endlich und separabel ist, ist auch $L/K(\alpha)$ endlich und separabel. Da $\overline{K}$ normal ist, gibt es für jedes $\sigma : K(\alpha) \hookrightarrow \overline{K}$ genau $m = [L : K(\alpha)]$ Einbettungen $\tau : L \hookrightarrow \overline{K}$ die Fortsetzungen von σ sind, das heißt $\tau_{|_{K(\alpha)}} = \sigma$.

Damit erhalten wir:

$$\begin{array}{ccc} L & \xrightarrow{\tau} & \overline{K} \\ \big| & & \big\| \\ K(\alpha) & \xrightarrow{\sigma} & \overline{K} \\ \big| & & \big\| \\ K & \xrightarrow{\iota} & \overline{K} \end{array}$$

$$\begin{aligned} \prod_{\tau\in\mathrm{Hom}_K(L,\overline{K})} \big(X-\tau(\alpha)\big) \;&=\; \prod_{\sigma\in\mathrm{Hom}_K(K(\alpha),\overline{K})} \left(\prod_{\substack{\tau\in\mathrm{Hom}_K(L,\overline{K}) \\ \tau|_{K(\alpha)}=\sigma}} \big(X-\tau(\alpha)\big) \right) \\ &=\; \prod_{\sigma\in\mathrm{Hom}_K(K(\alpha),\overline{K})} \big(X-\sigma(\alpha)\big)^m \;=\; \mathfrak{m}_\alpha(X)^m \end{aligned}$$

Damit haben wir die Formel (4.1) gezeigt und wissen nun

$$\chi_\alpha(X) \;=\; \prod_{\sigma\in\mathrm{Hom}_K(L,\overline{K})} \big(X-\sigma(\alpha)\big) \;=\; X + b_{N-1}X^{N-1} + \ldots + b_0$$

Wir erinnern uns an die Formeln, die wir für Spur und Norm bereits in Bemerkung 4.2 Punkt 4 festgehalten haben, damit gelten

$$Tr_K^L(\alpha) \;=\; -b_{N-1} \;=\; \sum_{\sigma\in\mathrm{Hom}_K(L,\overline{K})} \sigma(\alpha) \tag{4.2}$$

$$N_K^L(\alpha) \;=\; (-1)^n b_0 \;=\; \prod_{\sigma\in\mathrm{Hom}_K(L,\overline{K})} \sigma(\alpha) \tag{4.3}$$

Damit haben wir alle drei Formeln bewiesen. □

Folgerung 4.5 *Seien $M/L/K$ endliche separable Körpererweiterungen, dann gelten*

(a) $Tr_K^L \circ Tr_L^M \;=\; Tr_K^M$

(b) $N_K^L \circ N_L^M \;=\; N_K^M$

Beweis. Wir zeigen diese Eigenschaft nur für die Spur unter Benutzung der Gleichung (4.2). Die Eigenschaft für die Norm folgt vollständig analog aus Gleichung (4.3) des vorangegangenen Satzes 4.4. Sei $\alpha \in M$, dann gilt

$$\begin{aligned} Tr_K^M(\alpha) &= \sum_{\tau \in \mathrm{Hom}_K(M,\overline{K})} \tau(\alpha) \\ &= \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sum_{\substack{\tau \in \mathrm{Hom}_K(M,\overline{K}) \\ \tau_{|_L} = \sigma}} \tau(\alpha) \\ &= \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma\big(Tr_L^M(\alpha)\big) \;=\; Tr_K^L \circ Tr_L^M(\alpha) \end{aligned}$$

□

Wir wollen Spur und Norm noch auf eine andere Weise beschreiben dazu benötigen wir ein wenig Theorie von Bilinearformen.

Definition 4.6 *(Dualraum)*
Sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Wir nennen

$$V^* \;:=\; \mathrm{Hom}(V, K)$$

den zu V dualen Raum.

Definition 4.7 *((nicht ausgeartete) symmetrische Biliniearform)*
Sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Wir nennen

$$(\cdot,\cdot) : V \times V \to K$$

eine symmetrische Bilinearform auf V, wenn für alle $v, w \in V$ und alle $\lambda \in K$ gelten

$$(v, \lambda w) \;=\; (\lambda v, w) \;=\; \lambda \cdot (v, w) \;=\; \lambda \cdot (w, v)$$

Weiter heißt eine symmetrische Bilinearform $(\cdot,\cdot)$ auf V nicht ausgeratet, falls

$$\begin{aligned} \varphi : V &\to V^* \\ v &\mapsto [w \mapsto (v, w)] \end{aligned}$$

ein K-Vektorraumisomorphismus ist.

Lemma 4.8 *Sei K ein Körper und V ein endlichdimensionaler K-Vektorraum mit K-Basis $\{v_1, \ldots, v_n\}$ und $(\cdot, \cdot)$ eine symmetrische Bilinearform auf V. Es sind äquivalent*

(i) *$(\cdot, \cdot)$ ist nicht ausgeartet.*

(ii) *V besitzt eine bzüglich $(\cdot, \cdot)$ orthogonale Basis $\{v_1^*, \ldots, v_n^*\}$ zu $\{v_1, \ldots, v_n\}$, das heißt $(v_i^*, v_j) = \delta_{ij} \in \{0, 1\}$.*

(iii) *Die Matrix $A := \big((v_i, v_j)\big)_{1 \leq i,j \leq n}$ ist invertierbar.*

Beweis. Sei $\{\delta_1, \ldots, \delta_n\}$ eine zu $\{v_1, \ldots, v_n\}$ duale K-Basis von V^*, das heißt es gelte $\delta_i(v_j) = \delta_{i,j}$.
Wir zeigen nun zunächst die äquivalenz von **(i)** und **(ii)**:
Genau dann existiert eine orthogonalen Basis $\{v_1^*, \ldots, v_n^*\}$ wie in **(ii)**, wenn alle δ_i der dualen Basis D im Bild von $\varphi : V \to V^*$ aus Definition 4.7 liegen. Damit ist die Abbildung φ aber surjektiv. Da die Dimensionen von V und V^* gleich sind, ist jede surjektive Abbildung zwischen ihnen ein Isomorphismus. Per Definition gilt nun: Genau dann ist $(\cdot, \cdot)$ nicht ausgeartet, wenn φ ein Isomorphismus ist.
Nun wollen wir zeigen, dass **(i)** und **(ii)** äquivalent sind zu **(iii)**:
Da $\{v_1, \ldots, v_n\}$ eine Basis von V ist existieren für alle $v \in V$ Körpererlemente $\lambda_1, \ldots, \lambda_n \in K$ mit

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

Wir wollen nun untersuchen, wie sich der Isomorphismus

$$\begin{aligned} \varphi : V &\to V^* \\ v &\mapsto \varphi_v := [w \mapsto (v, w)] \end{aligned}$$

aus Definition 4.7 auf den Basiselementen v_i verhält. Betrachte

$$\begin{aligned} \varphi_{v_i}(v) &= \varphi_{v_i}\big(\lambda_1 v_1 + \ldots + \lambda_n v_n\big) \\ &= \sum_{j=1}^{n} \lambda_j \cdot (v_i, v_j) \end{aligned}$$

Damit erhalten wir

$$\varphi_{v_i}(v_j) = \sum_{j=1}^{n} (v_i, v_j) \cdot \delta_{ij}$$

Da φ nach Voraussetzung **(i)** ein Isomorphismus ist, ist $\{\varphi_{v_1}, \ldots, \varphi_{v_n}\}$ eine Basis des Dualraums V^*. Die Matrix $A := \big((v_i, v_j)\big)_{1 \leq i,j \leq n}$ ist genau dann invertierbar, wenn $\{\varphi_{v_1}, \ldots, \varphi_{v_n}\}$ eine Basis des Dualraums V^* ist. □

Definition und Satz 4.9 *(Spurform)*
Sei L/K eine endliche separable Körpererweiterung vom Grad n. Dann ist die Spurform

$$\begin{aligned} Tr_K^L : L \times L &\to K \\ (x, y) &\mapsto Tr_K^L(xy) \end{aligned}$$

eine nicht ausgeartete symmetrische Bilinearform.

Beweis. Nach dem Satz vom Primitiven Element[1] gibt es ein $\theta \in L$ mit $L = K(\theta)$. Dann ist die Menge $B = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ eine K-Basis von L. Wir wollen das vorangegangenene Lemma anwenden, und wollen zeigen, dass die Determinante der Matrix

$$M \;=\; \left(Tr_K^L(\theta^{i+j})\right)_{1\le i,j\le n}$$

nicht Null ist, denn dann ist M invertierbar. Nach Satz 4.4 gilt

$$Tr_K^L(\theta^{i+j}) \;=\; \sum_{\sigma\in \mathrm{Hom}_K(L,\overline{K})} \sigma(\theta)^i \cdot \sigma(\theta)^j$$

Nummeriere nun die Einbettungen

$$\mathrm{Hom}_K(L,\overline{K}) \;=\; \{\sigma_1, \ldots, \sigma_n\}$$

Mit der Notation $\theta_i := \sigma_i(\theta)$ erhalten wir

$$M \;=\; \left(Tr_K^L(\theta^{i+j})\right)_{1\le i,j\le n} \;=\; N \cdot N^T$$

Mit der Matrix

$$N \;=\; \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \theta_1^2 & \theta_2^2 & \cdots & \theta_n^2 \\ & & \vdots & \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix}$$

Damit gilt für die Determinante

$$\det(M) \;=\; \det(NN^T) \;=\; (-1)^{\binom{n}{2}} \det(N)^2 \;\overset{(1)}{=}\; (-1)^{\binom{n}{2}} \prod_{j=1}^{n} \prod_{\substack{i=1 \\ i\neq j}}^{n} (\theta_i - \theta_j) \;\overset{(2)}{\neq}\; 0$$

Wir müssen noch zwei Dinge Begründen:

- Die Gleichheit unter (1) ist die Vandermond'sche Determinante
- Die Ungleichheit unter (2) folgt aus der Separabilität von L/K, denn aus $\sigma_i(\theta) = \sigma_j(\theta)$ folgt stets, dass bereits $i = j$ gilt.

□

Definition 4.10 *(Diskriminante)*
Sei L/K eine endliche separable Körpererweiterung und sei $\{w_1, \ldots, w_n\}$ eine K-Basis von L. Wir nennen

$$d(w_1, \ldots, w_n) \;:=\; \det\left(\sigma_i(w_j)\right)^2 \;=\; \det\left(Tr_K^L(w_i w_j)\right)$$

mit $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \overline{K})$, die Diskriminante von $\{w_1, \ldots, w_n\}$.

Anmerkung Wegen des Quadrates hängt die Diskriminante nicht von der Reihenfolge der σ_i und w_j ab.

[1] Siehe zum Beispiel [L4] Seite 60.

Definition 4.11 *(Zahlkörper, Ganzheitsring)*
Eine endliche Körpererweiterung K von $\mathbb{Q}$ nennen wir einen Zahlkörper, und bezeichnen mit $\mathcal{O}_K$ den ganzen Abschluss von $\mathbb{Z}$ in K. Wir nennen $\mathcal{O}_K$ den Ganzheitsring von K.

Definition und Satz 4.12 *(Ganzheitsbasis)*
Sei K ein Zahlkörper mit Erweiterungsgrad $[K:\mathbb{Q}] = n$, dann ist $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang n, das heißt es gibt Elemente $w_1, \ldots, w_n \in \mathcal{O}_K$ so dass

$$\mathcal{O}_K \;=\; w_1\,\mathbb{Z} \oplus \ldots \oplus w_n\,\mathbb{Z}$$

und die $\mathbb{Z}$-Basis $\{w_1, \ldots, w_n\}$ nennen wir eine Ganzheitsbasis von $\mathcal{O}_K$.

Beweis. Es genügt zu zeigen, dass $\mathcal{O}_K$ endlich erzeugter $\mathbb{Z}$-Modul ist, denn wir wissen bereits

(i) Für alle $x \in K$ gibt es ein $a \in \mathbb{Z}\setminus\{0\}$ mit $x \cdot a \in \mathcal{O}_K$

(ii) $\mathcal{O}_K$ muss als Untermenge eines Körpers torsionsfrei sein.

Ist $\mathcal{O}_K$ nun endlich erzeugt, so ist $\mathcal{O}_K$ wegen **(ii)** frei mit einer Basis $\{w_1, \ldots, w_m\}$. Wegen **(i)** gilt dann $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \;=\; K$ also

$$\mathrm{rg}(\mathcal{O}_K) \;:=\; \dim_{\mathbb{Q}}(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}) \;=\; [K:\mathbb{Q}] \;=\; n$$

somit muss $m = n$ gelten. Zeigen wir also, dass $\mathcal{O}_K$ über $\mathbb{Z}$ endlich erzeugt ist. Dazu sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Q}$-Basis von K mit $\alpha_i \in \mathcal{O}_K$. Diese kann wegen **(i)** so gewählt werden. Sei dann $\{\alpha_1^*, \ldots, \alpha_n^*\}$ eine zu $\{\alpha_1, \ldots, \alpha_n\}$ bezüglich der Spurform $Tr_{\mathbb{Q}}^K$ orthogonale Basis, also $Tr_{\mathbb{Q}}^K(\alpha_i\alpha_j^*) = \delta_{ij}$.
Wähle nun $c \in \mathbb{Z}\setminus\{0\}$ so, dass für alle $i = 1, \ldots, n$ gilt $c \cdot \alpha_i^* \in \mathcal{O}_K$. Dann gilt für alle $x \in \mathcal{O}_K$ und alle $i = 1, \ldots, n$

$$c \cdot \alpha_i^* \cdot x \;\in \mathcal{O}_K \;\;\Rightarrow\;\; Tr_{\mathbb{Q}}^K(c\alpha_i^* x) \;\in \mathbb{Z} \;\;\Rightarrow\;\; Tr_{\mathbb{Q}}^K(\alpha_i^* x) \;\in \frac{1}{c}\,\mathbb{Z}$$

Da $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis ist, gibt es $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ derart, dass

$$x \;=\; \sum_{i=1}^{n} \lambda_i \alpha_i$$

Damit erhalten wir

$$\begin{aligned} Tr_{\mathbb{Q}}^K(x \cdot \alpha_i^*) \;&=\; Tr_{\mathbb{Q}}^K\left(\alpha_i^* \cdot \sum_{j=1}^{n} \lambda_j \alpha_j\right) \;=\; \sum_{j=1}^{n} \lambda_j Tr_{\mathbb{Q}}^K(\alpha_i^* \alpha_j) \\ &=\; \lambda_i \;\in \frac{1}{c}\,\mathbb{Z} \end{aligned}$$

Es gelten also

$$\alpha_1\,\mathbb{Z} + \ldots + \alpha_n\,\mathbb{Z} \;\subseteq\; \mathcal{O}_K \;\subseteq\; \frac{1}{c}\big(\alpha_1\,\mathbb{Z} \oplus \ldots \oplus \alpha_n\,\mathbb{Z}\big)$$

Damit ist $\mathcal{O}_K$ als Untermodul eines endlich erzeugten freien $\mathbb{Z}$-Moduls selber endlich erzeugt über $\mathbb{Z}$.
□

Anmerkung Wir können den obigen Satz auch allgemeiner Formulieren, nämlich:

Sei R ein Hauptidealbereich und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Seien weiter L/K eine endliche separable Körpererweiterung und S der ganze Abschluss von R in L. Dann ist S ein freier R-Modul von Rang $\mathrm{rg}(S) = n = [L : K]$.

Denn. Da im Beweis des Satzes nur die allgemeinen Ergebnisse

- Endlich erzeugte, torsionsfreie Moduln über Hauptiealbereichen sind frei (Lemma 0.22)
- Die Spurform ist nicht ausgeartet (Satz 4.9)
- Für alle $x \in L$ gilt $x = \frac{s}{r}$ mit $s \in S$ und $r \in R$

benutzt wurden kann der Beweis der allgemeineren Aussage analog geführt werden.

Definition 4.13 *(Diskriminante von Zahlkörpern)*
Sei K ein Zahlkörper und sei $\{w_1, \ldots, w_n\}$ eine Ganzheitsbasis von $\mathcal{O}_K$. Wir nennen

$$D_K \;:=\; d(w_1, \ldots, w_n) \;:=\; \det\Big(\big(\sigma_i(w_j)\big)_{1\le i,j\le n}\Big)^2$$

mit $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, die Diskriminante von K.

Lemma 4.14 *Sei K ein Zahlkörper, dann ist die Diskriminante D_K von K unabhängig von der Wahl der Ganzheitsbasis.*

Beweis. Seien $\{w_1, \ldots, w_n\}$ und $\{w'_1, \ldots, w'_n\}$ zwei Ganzheitsbasen, dann finden wir zu jedem w'_i Elemente $a_{i,j} \in \mathbb{Z}$ mit

$$w'_i \;=\; \sum_{j=1}^{n} a_{i,j} w_j$$

Ebenso finden wir Elemente $b_{i,j} \in \mathbb{Z}$ mit

$$w_i \;=\; \sum_{j=1}^{n} b_{i,j} w'_j$$

Wir erhalten zwei Matrizen $A := (a_{i,j}), B := (b_{i,j}) \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$, die zueinander Invers sind, das heißt

$$\det(AB) \;=\; \det(id) \;=\; 1$$

Also können beide Matritzen nur entweder 1 oder -1 als Determinante haben. Da $K/\mathbb{Q}$ endlich ist nummeriere die $\mathbb{Q}$-Homomorphismen $\sigma : K \to \mathbb{C}$ durch, dann gilt für alle $k = 1, \ldots, n$

$$\sigma_k(w'_i) \;=\; \sum_{j=1}^{n} a_{i,j} \sigma_k(w_j)$$

Damit erhalten wir aber

$$\det\Big(\big(\sigma_k(w_j)\big)_{1\le k,j\le n}\Big) \;=\; \det(A) \cdot \det\Big(\big(\sigma_k(w'_j)\big)_{1\le k,j\le n}\Big)$$

Also unterscheiden sich die Determinanten höchstens im Vorzeichen. Da die obige Determinante quadriert wird, fällt dieser Unterschied wieder weg, daher folgt die Behauptung. □

Beispiel 12 *(Diskriminanten von Zahlkörpern vom Grad 2)*
Sei K ein Zahlkörper mit $K = \mathbb{Q}(\sqrt{d})$ für ein quadratfreies $d \in \mathbb{Z}$. Wir haben bereits gezeigt, dass

$$\mathcal{O}_K \;=\; \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \equiv 3,2 \quad (4) \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & \text{falls } d \equiv 1 \qquad (4) \end{cases}$$

Damit erhalten wir als Ganzheitsbases

$$\begin{aligned} \left\{1, \sqrt{d}\right\} \qquad & \text{falls } d \;\equiv\; 2,3 \;\; (4) \\ \left\{1, \frac{\sqrt{d}+1}{2}\right\} \qquad & \text{falls } d \;\equiv\; 1 \;\; (4) \end{aligned}$$

Die einzigen beiden $\mathbb{Q}$-Homomorphismen von K nach $\mathbb{C}$ sind die Identität und die komplexe Konjugation, damit erhalten wir als zu betrachtende Matrizen

$$A_1 \;=\; \begin{pmatrix} 1 & \frac{\sqrt{d}+1}{2} \\ 1 & \frac{-\sqrt{d}+1}{2} \end{pmatrix} \qquad \text{und} \qquad A_{2,3} \;=\; \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}$$

Wobei natürlich A_1 im Fall $d \;\equiv\; 1 \;(4)$ und $A_{2,3}$ im Fall $d \;\equiv\; 2,3 \;(4)$ zu betrachten sind. Es gelten $\det(A_1) \;=\; -\sqrt{d}$ und $\det(A_{2,3}) \;=\; -2\sqrt{d}$. Damit erhalten wir als Diskriminante

$$D_K \;=\; \begin{cases} 4d & \text{falls } d \;\equiv\; 2,3 \;\; (4) \\ d & \text{falls } d \;\equiv\; 1 \;\; (4) \end{cases}$$

Bemerkung 4.15 *Sei $p > 2$ eine Primzahl. Wir betrachten den von der primitiven p-ten Einheitswurzel $\xi \;=\; e^{\frac{2\pi i}{p}} \;\in \mathbb{C}$ erzeugten Zahlkörper $K = \mathbb{Q}(\xi)$. Es gelten:*

(i) *Der Ganzheitsring von $\mathbb{Q}(\xi)$ ist $\mathbb{Z}[\xi]$.*

(ii) *Die Diskriminante von $\mathbb{Q}(\xi)$ ist*

$$D_{\mathbb{Q}(\xi)} \;=\; \begin{cases} p^{p-2} & \text{falls } p \;\equiv\; 1 \;\; (4) \\ -p^{p-2} & \text{falls } p \;\equiv\; 3 \;\; (4) \end{cases}$$

Beweis. Für den Beweis der beiden Teile erinnern wir uns zunächst an die Algebra Vorlesung. Wir kennen das Minimalpolynom $f_\xi \in \mathbb{Z}[X]$

$$\begin{aligned} f_\zeta(X) \;\;=:\;\; f(X) \;&=\; X^{p-1} + X^{p-2} + \ldots + X + 1 \\ &=\; \frac{X^P - 1}{X - 1} \;=\; \prod_{j=1}^{p-1}(X - \xi^j) \;=\; \prod_{j=1}^{p-1}\big(X - \sigma_j(\xi)\big) \end{aligned}$$

mit $\{\sigma_1, \ldots, \sigma_{p-1}\} \;=\; \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Weiter wissen wir, dass $\{1, \xi, \xi^2, \ldots, \xi^{p-2}\}$ die Nullstellen von $X^p - 1$ sind. Damit sind diese Elemente insbesondere ganz über $\mathbb{Z}$. Für $1 \leq r \leq p-2$ setze nun $\pi_r := 1 - \xi^r$, dann gilt

$$N_{\mathbb{Q}}^K(\pi_r) \;=\; \prod_{j=1}^{p-1}\big(1 - \sigma_j(\xi^r)\big) \;=\; f(1) \;=\; p$$

Weil für alle $r \in \mathbb{Z}$, die von p in $\mathbb{Z}$ nicht geteilt werden, gilt $\sigma_j(\xi^r) = \sigma_j(\xi)^r = (\xi^r)^j$ gilt insbesondere für alle $1 \leq r \leq p-2$:

$$f(X) = \prod_{j=1}^{p-1} \left(X - \sigma_j(\xi^r)\right)$$

Behauptung 1 *Für alle $1 \leq r \leq p-2$ gilt: π_r ist irreduzibel in $\mathcal{O}_K$, das heißt wenn es zwei Elemente $a, b \in \mathcal{O}_K$ mit $\pi_r = a \cdot b$ gibt, so folgt stets, dass entweder a oder b eine Einheit in $\mathcal{O}_K$ ist.*

Beweis. Seien $a, b \in \mathcal{O}_K$ mit $ab = \pi_r$, so folgt

$$p = N_{\mathbb{Q}}^K(\pi_r) = N_{\mathbb{Q}}^K(ab) = N_{\mathbb{Q}}^K(a) \cdot N_{\mathbb{Q}}^K(b)$$

Da p eine Primzahl ist, muss entweder $N_{\mathbb{Q}}^K(a) = \pm 1$ oder $N_{\mathbb{Q}}^K(b) = \pm 1$ gelten. Somit muss entweder a oder b bereits eine Einheit in $\mathcal{O}_K$ sein. ◇

Durch ausmultiplizieren sehen wir, dass für $r = 1, \ldots, p-2$ gilt

$$\pi_r = \pi_1 \cdot (1 + \xi + \ldots + \xi^{r-1})$$

Da sowohl π_r als auch π_1 nach der Behauptung irreduzibel sind, muss $(1 + \xi + \ldots + \xi^{r-1})$ eine Einheit in $\mathcal{O}_K$ sein. Damit erhalten wir

$$p = f(1) = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_{p-1} = \varepsilon \cdot \pi_1^{p-1} \qquad \text{mit einem } \varepsilon \in \mathcal{O}_K^\times \qquad (*)$$

Behauptung 2 *Sei $c \in \mathbb{Z}$ eine Zahl, die von $\pi := \pi_1$ in $\mathcal{O}_K$ geteilt wird, dann wird c in $\mathbb{Z}$ von p geteilt. In Formeln:*

$$\pi \,|\, c \text{ in } \mathcal{O}_K \quad \Rightarrow \quad p \,|\, c \text{ in } \mathbb{Z}$$

Beweis. Wenn π die Zahl c in $\mathcal{O}_K$ teilt, dann wird die Norm von c in $\mathbb{Z}$ von der Norm von π geteilt. Es gelten $N_{\mathbb{Q}}^K(\pi) = p$ und $N_{\mathbb{Q}}^K(c) = c^{p-1}$. Damit folgt die Behauptung aus der Primeigenschaft von p. ◇

Behauptung 3 *Für alle $r \in \mathbb{Z}$ gilt für die Spur*

$$Tr_{\mathbb{Q}}^K(\xi^r) = \begin{cases} -1 & \text{falls } r \not\equiv 0 \ \ (p) \\ p-1 & \text{falls } r \equiv 0 \ \ (p) \end{cases}$$

Beweis. Wir betrachten die beiden Fälle

($r \equiv 0 \ \ (p)$): In diesem Fall ist $\xi^r = 1$. Es gilt also

$$Tr_{\mathbb{Q}}^K(\xi^r) = Tr_{\mathbb{Q}}^K(1) = [K : \mathbb{Q}] = p - 1$$

($r \not\equiv 0 \ \ (p)$): In diesem Fall ist $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ das Charakteristische Polynom von ξ^r über K. Alle Koeffizienten des Polynoms sind 1, also insbesondere der Zweithöchste. Mit Bemerkung 4.2 Teil 4 gilt dann

$$Tr_{\mathbb{Q}}^K(\xi^r) = -a_{p-2} = -1$$

◇

Jetzt haben wir alles beisammen um Teil **(i)** zu beweisen: Sei $x \in \mathcal{O}_K$, dann ist

$$x \;=\; a_0 + a_1\xi + \ldots + a_{p-1}\xi^{p-1} \qquad \text{mit Elementen } a_i \in \mathbb{Q}$$

Mit der zuvor bewiesenen Behauptung 3 gelten dann

$$\begin{aligned} Tr_{\mathbb{Q}}^{K}(\xi\, x) &= -\sum_{j=0}^{p-2} a_j \\ Tr_{\mathbb{Q}}^{K}(\xi^r\, x) &= (p-1)a_r - \sum_{\substack{j=0 \\ j\neq r}}^{p-2} a_j \qquad \text{für } r = 1, \ldots, p-2 \end{aligned}$$

Aus diesem beiden Gleichungen erhalten wir

$$Tr_{\mathbb{Q}}^{K}(\xi^r\, x - \xi\, x) \;=\; pa_r \qquad \text{für } r = 1, \ldots, p-2$$

Da wir nun über $\mathbb{Z}$ sind gibt es Elemente $b_1, \ldots, b_{p-2} \in \mathbb{Z}$ mit

$$p \cdot x \;=\; b_0 + b_1\xi + \ldots + b_{p-1}\xi^{p-1}$$

Substituiere $\xi = 1 - \pi$ und erhalte

$$p \cdot x \;=\; c_0 + c_1\pi + \ldots + c_{p-1}\pi^{p-1} \qquad \text{mit Elementen } c_i \in \mathbb{Z}$$

Also gilt, dass π das Produkt $p \cdot x$ in $\mathcal{O}_K$ teilt. Also teilt π insbesondere auch das c_0 in $\mathcal{O}_K$. Mit Behauptung 2 folgt dann, dass p das c_0 in $\mathbb{Z}$ teilt, das heißt es gibt ein $c_0' \in \mathbb{Z}$ mit $p \cdot c_0' = c_0$. Damit gilt

$$p(x - c_0') \;=\; \pi\big(c_1 + c_2\pi + \ldots + c_{p-2}\pi^{p-3}c_{p-2}\big)$$

Nun gilt nach $(*)$ aber, dass p von π^{p-2} in $\mathcal{O}_K$ geteilt wird, also teilt π auch die Summe $c_1 + \pi c_2 + \ldots + c_{p-2}\pi^{p-3}$ in $\mathcal{O}_K$. Dann teilt π insbesondere das Element c_1 in $\mathcal{O}_K$ Als folgt wieder nach Behauptung 2: p teilt c_1 in $\mathbb{Z}$.
Diese Argumentation wiederholen wir nun immer wieder und erhalten schließlich, dass die Primzahl p jedes c_i teilt. Dann muss aber $x \in \mathbb{Z}[\xi]$ gelten.

Für den Nachweis von Teil **(ii)** fehlt uns noch eine Aussage, die wir als Übungsaufgabe stellen:

Übungsaufgabe 2 *Sei $\alpha \in \mathbb{C}$, dann betrachte den Zahlkörper $K := \mathbb{Q}(\alpha)$ über $\mathbb{Q}$.*
Sei $[K : \mathbb{Q}] = n$ und sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von α über $\mathbb{Q}$. Zeige: Dann gilt

$$d(1, \alpha, \ldots, \alpha^{n-1}) \;=\; \begin{cases} +N_{\mathbb{Q}}^{K}\big(f'(\alpha)\big) & \text{falls } n \;\equiv\; 0, 1 \;\; (4) \\ -N_{\mathbb{Q}}^{K}\big(f'(\alpha)\big) & \text{falls } n \;\equiv\; 2, 3 \;\; (4) \end{cases}$$

wobei $f'(\alpha)$ die formale Ableitung von f an der Stelle α sei.

Mit dieser Übungsaufgabe erhalten wir zunächst

$$D_K \;=\; d(1, \xi, \ldots, \xi^{p-1}) \;\in\; \big\{\, \pm N_{\mathbb{Q}}^{K}\big(f'(\xi)\big) \,\big\}$$

Betrachten wir zunächst die Ableitung des Minimalpolynoms

$$\begin{aligned} f(X) = \frac{X^p - 1}{X - 1} \quad &\Rightarrow \quad (X^p - 1) \;=\; f(X) \cdot (X - 1) \\ &\Rightarrow \quad pX^{p-1} \;=\; f(X) + (X - 1) \cdot f'(X) \\ &\Rightarrow \quad p\xi^{p-1} \;=\; (\xi - 1) \cdot f'(X) \\ &\Rightarrow \quad f'(X) \;=\; \frac{p\xi^{p-1}}{\xi - 1} \end{aligned}$$

Damit erhalten wir

$$N_{\mathbb{Q}}^K\big(f'(\xi)\big) \;=\; \frac{p^{p-1}}{N_{\mathbb{Q}}^K(\pi)} \;=\; p^{p-2}$$

Betrachten wir nun die Fallunterscheidung aus der Übungsaufgabe folgt

$$D_{\mathbb{Q}(\xi)} \;=\; \begin{cases} p^{p-2} & \text{falls } p \equiv 1 \ (4) \\ -p^{p-2} & \text{falls } p \equiv 3 \ (4) \end{cases}$$

Denn die Fälle $p \equiv 0 \ (4)$ und $p \equiv 2 \ (4)$ können wegen $p > 2$ nicht auftreten. □

Anmerkung Diese Bemerkung zeigt implizit:

$$\mathbb{Q}(\xi) \;\supseteq\; \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{falls } p \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-p}) & \text{falls } p \equiv 3 \ (4) \end{cases}$$

Bemerkung 4.16 *Sei R ein Hauptidealbereich und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Seien weiter L/K eine endliche separable Körpererweiterung und S der ganze Abschluss von R in L. Wähle eine K-Basis $\{\alpha_1, \ldots, \alpha_n\} \subset S$ von L. Setze $D := d(\alpha_1, \ldots, \alpha_n)$, dann gilt*

$$R\alpha_1 \oplus \ldots \oplus R\alpha_n \;\subset\; S \;\subset \frac{1}{D}\big(R\alpha_1 \oplus \ldots \oplus R\alpha_n\big)$$

Beweis. Sei $\{\alpha_1^*, \ldots, \alpha_n^*\}$ die zu $\{\alpha_1, \ldots, \alpha_n\}$ bezüglich der Spurform Tr_K^L orthogonale Basis. Wir haben bereits im Beweis von Satz 4.12 gezeigt, dass für $c \in R\backslash\{0\}$, mit der Eigenschaft $c \cdot \alpha_i^* \in S$ für alle $i = 1, \ldots, n$, gilt

$$R\alpha_1 \oplus \ldots \oplus R\alpha_n \;\subset\; S \;\subset \frac{1}{c}\big(R\alpha_1 \oplus \ldots \oplus R\alpha_n\big)$$

Wir wollen im folgenden also zeigen, dass $D = d(\alpha_1, \ldots, \alpha_n)$ diese Eigenschafen hat. Setze dazu $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n)$ und $\underline{\alpha}^* := (\alpha_1^*, \ldots, \alpha_n^*)$. Es gibt eine Basiswechselmatrix $A = (a_{i,j}) \in \mathrm{Gl}_N(K)$ mit $\underline{\alpha}^* = A\underline{\alpha}$ also gilt

$$\begin{aligned} \alpha_i^* \quad &= \quad \sum_{j=1}^{n} a_{i,j} \cdot \alpha_j && \text{für alle } i = 1, \ldots, n \\ \Rightarrow \quad \alpha_k \alpha_i^* \quad &= \quad \sum_{j=1}^{n} a_{i,j} \cdot \alpha_j \alpha_k && \text{für alle } i, k = 1, \ldots, n \\ \Rightarrow \quad \delta_{i,k} \quad &=: \; Tr_K^L(\alpha_i^* \alpha_k) \;=\; \sum_{j=1}^{n} a_{i,j} \cdot Tr_K^L(\alpha_j \alpha_k) && \text{für alle } i, k = 1, \ldots, n \\ \Rightarrow \quad A \quad &= \Big(\big(Tr_K^L(\alpha_i \alpha_k)\big)_{1 \le i,k \le n}\Big)^{-1} \end{aligned}$$

Lemma *Sei $n \in \mathbb{N}$ und R ein kommutativer Ring, dann gibt es für $1 \leq i, j \leq n$ Polynome*

$$P_{i,j}(\underline{X}) \ \in \ \mathbb{Z}[X_{1,1}, \ldots, X_{1,n}, X_{2,1}, \ldots, X_{n,n}]$$

So dass für alle Matrizen $A \in \mathrm{Mat}_{n\times n}(R)$ gilt

$$A \cdot \Big(P_{i,j}(\underline{X})\Big)_{1\leq i,j\leq n} \ = \ \det(A) \cdot id_n$$

wobei id_n die $n \times n$-Einheitsmatrix bezeichne.

Beweis. Einen Beweis mit einem Körper K finden Sie in gäniger Literatur zur Linearen Algebra.

Mit diesem Lemma finden wir Polynome $P_{l,j}(\underline{X})$ so dass gilt

$$\begin{aligned} A \ &= \ \Big(\big(Tr_K^L(\alpha_i\alpha_k)\big)_{1\leq i,k\leq n}\Big)^{-1} \\ &= \ \frac{\Big(P_{l,j}\big(\, Tr_K^L(\alpha_i\alpha_k) \,\big|\, 1 \leq i,k \leq n \,\big)\Big)_{1\leq l,j\leq n}}{\det\Big(\big(Tr_K^L(\alpha_i\alpha_k)\big)_{1\leq i,k\leq n}\Big)} \ \in \mathrm{Mat}_{n\times n}\big(\frac{1}{D}R\big) \end{aligned}$$

Also hat A Einträge aus $\frac{1}{D}R$ und damit folgt die Behauptung. □

Satz 4.17 *Seien L und K endliche Zahlkörper über $\mathbb{Q}$ mit*

$$[KL : \mathbb{Q}] \ = \ [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$$

das heißt es gilt $K \cap L = \mathbb{Q}$. Sei weiter $d = \mathrm{ggT}(D_K, D_L)$ der größte gemeinsame Teiler der Diskriminanten von K und L. Dann gilt

$$\mathcal{O}_{LK} \ \leq \ \frac{1}{d} \cdot \mathcal{O}_K \cdot \mathcal{O}_L$$

Insbesondere gilt, falls D_K und D_L teilerfremd sind,

$$\mathcal{O}_{LK} \ = \ \mathcal{O}_K \cdot \mathcal{O}_L$$

Beweis. Seien $\{\alpha_1, \ldots, \alpha_m\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ und $\{\beta_1, \ldots, \beta_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_L$, dann ist $\{\, \alpha_i\beta_j \,|\, i = 1 \ldots m \ \wedge \ j = 1 \ldots m \,\}$ eine $\mathbb{Q}$-Basis vom Kompositum LK. Mit dieser Überlegung hat jedes $\alpha \in \mathcal{O}_{LK}$ eine Dartstellung der Form

$$\alpha \ = \ \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{m_{i,j}}{r} \cdot \alpha_i\beta_j \qquad \text{mit } r, m_{i,j} \in \mathbb{Z} \text{ und } \mathrm{ggT}\left(r, \mathrm{ggT}(m_{i,j})\right) = 1$$

Behauptung *Das r aus dieser Darstellung teilt D_K*

Beweis. Ohne Einschränkung sei $KL \subseteq \mathbb{C}$. Wegen der Voraussetzung $K \cap L = \mathbb{Q}$ gibt es für alle $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ eine Fortsetzung $\tilde{\sigma} \in \mathrm{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ mit $\tilde{\sigma}_{|_K} = \sigma$ und $\tilde{\sigma}_{|_L} = id_L$. Damit gilt für alle $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$

$$\tilde{\sigma}(\alpha) \ = \ \sum_{i=1}^{m} \underbrace{\sum_{j=1}^{n} \frac{m_{i,j}}{r} \cdot \beta_j}_{=: x_i \in L} \cdot \sigma(\alpha_i) \ = \ \sum_{i=1}^{m} x_i \cdot \sigma(\alpha_i)$$

Nummeriere nun die Einbettungen $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_m\}$ und setze $A := \big(\sigma_k(\alpha_i)\big)_{1 \le i,k \le m}$. Es gilt

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \;=\; A^{-1} \cdot \begin{pmatrix} \tilde{\sigma}_1(\alpha) \\ \vdots \\ \tilde{\sigma}_n(\alpha) \end{pmatrix}$$

Denn wegen $\det(A)^2 \;=\; D_K \neq 0$ ist A invertierbar. Mit dem im vorangegangenen Beweis zitierten Lemma gibt es sogar eine Matrix $A' \in \mathrm{Mat}_{m \times m}(\mathcal{O}_K)$ mit

$$A^{-1} \;=\; \frac{A'}{\det(A)}$$

Also gibt es für alle $i = 1, \ldots, m$ ganze Elemente $\delta_i \in \mathcal{O}_{KL}$ mit

$$L \;\ni\; D_K \cdot x_i \;=\; \delta_i \cdot \det(A) \;\in\; \mathcal{O}_{KL}$$

Das heißt aber, dass $D_K \cdot x_i$ für alle $i = 1, \ldots, n$ sowohl im ganzen Abschluss von $\mathbb{Z}$ in KL als auch in L liegen, also gilt $D_K \cdot x_i \in \mathcal{O}_L$ für alle $i = 1, \ldots, n$. Nach Definition der x_i gilt also

$$D_K \cdot x_i \;=\; \sum_{j=1}^{n} \frac{m_{i,j} D_K}{r} \cdot \beta_j \;\in \mathcal{O}_L$$

Da $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ ist mit r das die Produkte $m_{i,j} D_K$ für alle $j = 1, \ldots, n$ und alle $i = 1, \ldots, m$ teilen. Also teilt r den größten gemeinsamen Teiler der $m_{i,j}$ und D_K. Da wir r gerade so gewählt haben, dass r und $\mathrm{ggT}(m_{i,j})$ teilerfremd sind, muss r also D_K teilen, $\diamond$

Aus Symmetriegründen teilt r dann auch D_L, also teilt r den größten gemeinsamen Teiler d von D_K und D_L.

Insgesamt haben wir gezeigt: Ist $\alpha \in \mathcal{O}_{KL}$ so gilt

$$\alpha = \frac{1}{r} \sum_{i=1}^{m} \sum_{j=1}^{n} m_{i,j} \cdot \alpha_i \beta_j \;\in\; \frac{1}{r}\, \mathcal{O}_K \cdot \mathcal{O}_L \;\subseteq\; \frac{1}{d}\, \mathcal{O}_K \cdot \mathcal{O}_L$$

$\square$

Lemma 4.18 *Sei V ein n-dimensionaler $\mathbb{Q}$-Vektorraum und*

$$(\cdot, \cdot) : V \times V \to \mathbb{Q}$$

eine nicht ausgeartete Bilinearform. Sei weiter M ein endlich erzeugter $\mathbb{Z}$-Modul mit der Eigenschaft, dass es für jedes $v \in V$ ein $\lambda \in \mathbb{Q} \setminus \{0\}$ so gibt, dass $\lambda v \in M$ ist, und sei $N \subseteq M$ ein Untermodul mit

$$\mathrm{rg}_{\mathbb{Z}}(N) \;=\; \mathrm{rg}_{\mathbb{Z}}(M) \;=\; \dim_{\mathbb{Q}}(V)$$

Seien schließlich $d(M)$ und $d(N)$ die Diskriminanten von M und N bezüglich $(\cdot, \cdot)$, also

$$d(M) \;:=\; \det\Big(\big((v_i, v_j)\big)_{1 \le i,j \le n}\Big)$$

mit $M \;=\; \mathbb{Z}\, v_1 \oplus \ldots \oplus \mathbb{Z}\, v_n$. Dann gilt

$$d(N) \;=\; (M : N)^2 \cdot d(M)$$

Beweis. Nach dem Elementarteilersatz (Satz 0.24) gibt es $d_1, \ldots, d_n \in \mathbb{Z}$ mit

- d_i teilt d_j für alle $i, j = 1, \ldots, n$ mit $i \leq j$.
- $N \;=\; \mathbb{Z}\, d_1 v_1 \oplus \ldots \oplus \mathbb{Z}\, d_n v_n$

Bezeichne $D := \operatorname{diag}(d_1, \ldots, d_n)$ die $n \times n$-Diagonalmatrix mit den Diagonaleinträgen d_1 bis d_n, dann gilt

$$d(N) \;=\; \det\Big(D \cdot \big((v_i, v_j)\big)_{1 \leq i,j \leq n} \cdot D\Big) \;=\; (d_1 \cdot \ldots \cdot d_n)^2 \cdot d(M)$$

Weiter gilt

$$(M : N) \;=\; \sharp\Big({}^{M}\!/_{N}\Big) \;=\; \sharp\Big({}^{\mathbb{Z}}\!/_{d_1} \otimes \ldots \otimes {}^{\mathbb{Z}}\!/_{d_n}\Big) \;=\; d_1 \cdot \ldots \cdot d_n$$

□

Lemma 4.19 *Sei K ein Zahlkörper und $\{0\} \neq \mathfrak{a} \subseteq K$ ein endlich erzeugter $\mathcal{O}_K$-Modul, dann gelten*

a) *$\mathfrak{a}$ ist ein freier Modul vom Rang $\operatorname{rg}_{\mathcal{O}_K}(\mathfrak{a}) \;=\; [K : \mathbb{Q}] \;=\; n$.*

b) *Ist $\mathfrak{a}' \subseteq \mathfrak{a}$ ein Untermodul mit $\{0\} \neq \mathfrak{a}$, dann ist*

$$d(\mathfrak{a}) \;=\; (\mathfrak{a} : \mathfrak{a}')^2 \cdot d(\mathfrak{a})$$

mit $d(\mathfrak{a}') := d(\alpha_1, \ldots, \alpha_n)$ für eine $\mathcal{O}_K$ Basis $\{\alpha_1, \ldots, \alpha_n\}$ von $\mathfrak{a}$.

Beweis. Der Modul $\mathfrak{a}$ ist als Untermenge eines Zahlkörpers torsionsfrei über $\mathbb{Z}$. Da $\mathfrak{a}$ endlich erzeugt ist gilt dann

$$\mathfrak{a} \;\cong\; \mathbb{Z}^{\otimes m} \;=\; \mathbb{Z}^m$$

Weiter ist $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Q}$ wegen $\mathfrak{a} \subseteq K$ ein $\mathbb{Q}$-Untervektorraum von K. Damit gilt $m \leq [K : \mathbb{Q}]$. Andererseits wähle ein $x \in \mathfrak{a} \setminus \{0\}$, dann ist

$$\mathcal{O}_K \;\ni\; y \;\mapsto\; xy \;\in\; \mathfrak{a}$$

injektiv und damit gilt insgesamt

$$m \;=\; \operatorname{rg}(\mathfrak{a}) \;\geq\; \operatorname{rg}(\mathcal{O}_K) \;=\; [K : \mathbb{Q}] \;\geq\; m$$

Für den zweiten Teil stellen wir fest:

- $\operatorname{rg}(\mathfrak{a}') = \operatorname{rg}(\mathfrak{a})$ nach **a)**, denn auch $\mathfrak{a}'$ ist endlich erzeugter $\mathcal{O}_K$-Modul
- K ist ein n-Dimensionaler $\mathbb{Q}$-Vektorraum und die Spurform $Tr^K_{\mathbb{Q}}$ ist nicht ausgeartet auf K.
- Für jedes $k \in K$ gibt es ein $\lambda \in \mathbb{Q}$ mit $\lambda k \in \mathfrak{a}$

damit folgt die Behauptung aus Lemma 4.18. □

Folgerung 4.20 *Sei K ein Zahlkörper mit $[K : \mathbb{Q}] = n$. Sei weiter $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ eine $\mathbb{Q}$-Basis von K mit über $\mathbb{Z}$ ganzen Elementen α_i. Es gilt:*
Ist $d(\alpha_1, \ldots, \alpha_n)$ quadratfrei, so ist $\mathcal{O}_K \;=\; \mathbb{Z}\, \alpha_1 \oplus \ldots \oplus \mathbb{Z}\, \alpha_n$.

Beweis. Die Inklusion $\mathbb{Z}\, \alpha_1 \oplus \ldots \oplus \mathbb{Z}\, \alpha_n \subseteq \mathcal{O}_K$ ist klar. Nach Lemma 4.19 gilt dann

$$d(\alpha_1, \ldots, \alpha_n) \;=\; \big(\mathcal{O}_K \;:\; \mathbb{Z}\, \alpha_1 \oplus \ldots \oplus \mathbb{Z}\, \alpha_n\big)^2 \cdot d(\mathcal{O}_K)$$

wenn $d(\alpha_1, \ldots, \alpha_n)$ quadratfrei ist muss $\big(\mathcal{O}_K \;:\; \mathbb{Z}\, \alpha_1 \oplus \ldots \oplus \mathbb{Z}\, \alpha_n\big) = 1$ gelten und damit folgt die Behauptung. □

5 Dedekindringe

Wir wissen, dass in allgemeinen Ringen die Zerlegung eines Ringelemntes in seine Primfaktoren nicht eindeutig sein muss. Wir haben bereits in der Einleitung im Beispiel 1 gesehen, dass auch Zahlringe hiervon keine Ausnahme bilden. In diesem Abschnitt wollen wir einen Ersatz für die eindeutige Zerlegung in Primelemente finden. Ziel ist also der

Satz *(Satz von Kummer)*
Sei K ein Körper und $\mathcal{O}_K$ sein Ganzheitsring, dann gilt: Jedes Ideal $\mathfrak{a} \lhd \mathcal{O}_K$ mit $\mathfrak{a} \neq 0$ lässt sich (bis auf Reihenfolge) eindeutig faktorisieren als

$$\mathfrak{a} \;=\; \wp_1 \cdot \ldots \cdot \wp_r \qquad \text{mit } \wp \in \operatorname{Spec}(\mathcal{O}_K)$$

Anstatt also eine Zahl in ihre Primbestandteile zu zerlegen, zerlegen wir Ideale in Primideal-Bestandteile. Dazu betrachten wir eine spezielle Sorte von Ringen

Definition 5.1 *(Dedekindring)*
Sei R ein Integritätsring. Wir nennen R einen Dedekindring oder dedekindsch, wenn die folgenden Bedingungen erfüllt sind

(D1) *Alle Ideale sind endlich erzeugt. (Das heißt R ist noethersch)*

(D2) *Jedes Primideal von R ausser dem Nullideal ist maximal. (Das heißt die Krull-Dimension von R ist Eins)*

(D3) *R ist ganz abgeschlossen in* $\operatorname{Quot}(R)$.

Satz 5.2 *Sei $K/\mathbb{Q}$ eine endliche Erweiterung, dann ist $\mathcal{O}_K$ dedekindsch.*

Beweis. Wegen $\mathcal{O}_K \subset K$ ist klar, dass $\mathcal{O}_K$ ein Integritätsring ist. Wir müssen also die drei Bedingungen der Definition nachprüfen. Da $K/\mathbb{Q}$ endlich ist, ist der Ganzheitsring $\mathcal{O}_K$ von K ein endlich erzeugter $\mathbb{Z}$-Modul. Weil $\mathbb{Z}$ noethersch ist, sind alle Ideale von $\mathcal{O}_K$ als $\mathbb{Z}$-Moduln endlich erzeugt. Da $\mathcal{O}_K$ selbst endlich über $\mathbb{Z}$ ist, sind alle Ideale von $\mathcal{O}_K$ endlich erzeugte $\mathcal{O}_K$-Moduln, also folgt **(D1)**. Sei $\wp \in \operatorname{Spec}(R)\backslash\{(0)\}$ und $\alpha \in \wp\backslash\{0\}$, dann gilt

$$\mathbb{Z} \;\ni\; N_{\mathbb{Q}}^{K}(\alpha) \;=\; \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(\alpha) \;\in\; (\alpha) \;\subseteq\; \wp$$

Also gibt es eine Primzahl $p \in \mathbb{N}$ mit $\wp \cap \mathbb{Z} = (p)$. Sei nun $\mathcal{O}_K = \mathbb{Z}\,\alpha_1 \oplus \ldots \oplus \mathbb{Z}\,\alpha_n$ dann ist

$$\mathcal{O}_K \big/ p\,\mathcal{O}_K \;\cong\; \mathbb{F}_p\,\overline{\alpha}_1 \oplus \ldots \oplus \mathbb{F}_p\,\overline{\alpha}_n$$

und die Abbildung

$$\mathcal{O}_K \big/ p\,\mathcal{O}_K \;\to\; \mathcal{O}_K \big/ \wp$$

ist surjektiv. Also ist $V := \mathcal{O}_K \big/ \wp$ ein $\mathbb{F}_p$-Vektorraum endlicher Dimension. Insbesondere hat V als endlichdimensionaler Vektorraum über einem endlichen Körper nur endlich viele Elemente.

Behauptung $V = \mathcal{O}_K \big/ \wp$ ist ein Körper.

Beweis. Sei $x \in V\backslash\{0\}$. Da V endlich ist muss sich die Folge $x, x^2, x^3, \ldots$ irgendwann wiederholen, also gibt es $i, j \in \mathbb{N}$ mit $i < j$ und $x^i = x^j$. Da V als Faktor von einem Ring nach einem Primideal ein Integritätsring ist, folgt nun $x^{i-j} = 1$, also ist x eine Einheit. $\diamond$

Diese Behauptung liefert den Nachweis von **(D2)**.
Sei $x \in \mathrm{Quot}(\mathcal{O}_K)$. Genau dann ist x ganz über OO_K, wenn das Minimalpolynom von x über $\mathbb{Q}$ ganzzahlige Koeffizienten hat, also aus $\mathbb{Z}[X]$ ist. Das heißt aber, dass $x \in \mathrm{Quot}(\mathcal{O}_K$ genau dann ganz über $\mathcal{O}_K$ ist, wenn $x \in \mathcal{O}_K$ liegt und $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K ist. Also ist $\mathcal{O}_K$ ganz abgeschlossen und damit folgt **(D3)**. □

Ab jetzt bezeichne R stets einen Dedekindring und $K := \mathrm{Quot}(R)$ seinen Quotientenkörper.

Lemma 5.3 *Sei $\mathfrak{a} \lhd R$ mit $\mathfrak{a} \neq (0)$ ein Ideal, dann gibt es vom Nullideal verschieden Primideale $\wp_1, \ldots, \wp_r \in \mathrm{Spec}(R)\backslash\{(0)\}$ mit*

$$\mathfrak{a} \supseteq \wp_1 \cdot \ldots \cdot \wp_r$$

Erinnerung Gemeint ist hierbei natürlich das Produkt von Idealen, das heißt seinen $\mathfrak{a}, \mathfrak{b} \lhd R$, dann ist

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^{N} a_i b_i \,\middle|\, N \in \mathbb{N} \wedge a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b} \right\}$$

Isnbesondere für Hauptideale $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$ gilt $(a) \cdot (b) = (ab)$.

Beweis. Wir betrachten die Menge von Idealen, für die das Lemma nicht gilt, und wollen zeigen, dass diese leer ist. Sei dazu

$$S := \left\{ \mathfrak{a} \lhd R \,\middle|\, \mathfrak{a} \neq (0) \text{ und } \mathfrak{a} \text{ enthält kein Produkt von Primidealen ungleich Null} \right\}$$

Angenommen S sei nicht leer. Da R noethersch ist enthält jede nicht leere Familie von Idealen ein maximales Element bezüglich der Inklusion „$\subseteq$“. Sei $\mathfrak{a}$ dieses maximale Element von S. Dieses Element ist kein Primideal, denn $\mathfrak{a} \subseteq \mathfrak{a}$ und $\mathfrak{a}$ enthält kein Produkt von Primidealen. Dann gibt es aber $r, s \in R\backslash\,\mathfrak{a}$ mit $r \cdot s \in \mathfrak{a}$. Mit diesen Ringelementen bilden wir neue Ideale $(r) + \mathfrak{a}$ und $(s) + \mathfrak{a}$, die je echt größer als $\mathfrak{a}$ sind, für deren Produkt aber gilt

$$\big((r) + \mathfrak{a}\big) \cdot \big((s) + \mathfrak{a}\big) = (rs) + \mathfrak{a} = \mathfrak{a} \qquad (*)$$

Da wir $\mathfrak{a}$ als das maximale Element in S gewählt haben und $(r) + \mathfrak{a}$ sowie $(s) + \mathfrak{a}$ echt größer als $\mathfrak{a}$ sind gibt es $\wp_1, \ldots, \wp_l, \mathfrak{q}_1, \ldots, \mathfrak{q}_k \in \mathrm{Spec}(R)\backslash\{(0)\}$ mit

$$\wp_1 \cdot \ldots \cdot \wp_l \subseteq (r) + \mathfrak{a} \quad \text{und} \quad \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_k \subseteq (s) + \mathfrak{a}$$

Wegen $(*)$ folgt dann aber sofort

$$\wp_1 \cdot \ldots \cdot \wp_l \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_k \subseteq \mathfrak{a}$$

Also ist $\mathfrak{a} \notin S$ was ein Widerspruch ist. Somit muss S leer sein. □

Lemma 5.4 *Sei $\mathfrak{a} \lhd R$ ein Ideal mit $\mathfrak{a} \neq (1)$, dann gibt es ein $\alpha \in K\backslash R$ mit $\alpha \cdot \mathfrak{a} \subseteq R$*

Beweis. Ohne Einschränkung sein $\mathfrak{a} \neq (0)$, sonst ist die Aussage trivial. Seien also $a \in \mathfrak{a}\backslash\{0\}$ und $r \in \mathbb{N}$ minimal[2], so dass $\wp_1 \cdot \ldots \cdot \wp_r \subseteq (a)$ für Primideale $\wp_i \in \mathrm{Spec}(R)\backslash\{(0)\}$.
Jedes Ideal ist in einem maximalen Ideal enthalten, also gibt es insbesondere ein maximales Ideal $\mathfrak{p} \in \mathrm{Spm}(R)$ mit $(a) \subseteq \mathfrak{a} \subseteq \mathfrak{p}$.

[2] Betrachte $(6) \supseteq (2) \cdot (3)$ aber $(3) \nsubseteq (6)$ und $(2) \nsubseteq (6)$

Behauptung $\mathfrak{p} \supseteq \wp_i$ *für ein* $i \in \{1, \ldots, r\}$

Beweis. Angenommen diese Behauptung gelte nicht, dann existierte zu jedem $i = 1 \ldots r$ ein $a_i \in \wp_i$ mit $a_i \notin \mathfrak{p}$ aber

$$\prod_{i=1}^{r} a_i \;\in\; \wp_1 \cdot \ldots \cdot \wp_r \;\subseteq\; (a) \;\subseteq\; \mathfrak{p}$$

Da $\mathfrak{p}$ insebsondere prim ist gäbe dann aber ein $j \in \{1, \ldots, r\}$ mit $a_j \in \mathfrak{p}$ was widersprüchlich ist. $\diamond$

Ohne Einschränkung gelte $\wp_1 \subseteq \mathfrak{p}$. Da R ein Dedekindring ist folgt aus Eigenschaft **(D2)**, dass $\wp_1 = \mathfrak{p}$ ist. Weiter ist wegen der Minimalität von r das Produkt $\wp_2 \cdot \ldots \cdot \wp_r$ nicht in (a) enthalten, daher gibt es ein $b \in \wp_2 \cdot \ldots \cdot \wp_r$ mit $b \notin (a)$. Damit haben wir ein Element $\alpha := \frac{b}{a} \in K \backslash R$ gefunden, das die Behauptung $\alpha \cdot \mathfrak{a} \subseteq R$ erfüllt, denn $\frac{b}{a} \cdot \mathfrak{a}$ ist genau dann Teilmenge von R, wenn $b \cdot \mathfrak{a}$ Teilmenge von (a) ist. Nach Wahl von b gilt

$$b\wp_1 \;\subseteq\; \wp_1 \cdot \wp_2 \cdot \ldots \cdot \wp_r \;\subseteq\; (a)$$

und wegen $\mathfrak{a} \subseteq \mathfrak{p} = \wp_1$ gilt weiter $b \cdot \mathfrak{a} \subseteq b\wp_1$. $\square$

Satz 5.5 *Sei* $\mathfrak{a} \lhd R$ *ein Ideal mit* $(0) \neq \mathfrak{a}$ *und sei weiter* $\alpha \in \mathfrak{a} \backslash \{0\}$. *Setze*

$$\mathfrak{b} \;:=\; \left\{ \beta \in R \,\middle|\, \beta\,\mathfrak{a} \subseteq (\alpha) \right\}$$

Dann gilt $\mathfrak{b} \cdot \mathfrak{a} = (\alpha)$.

Beweis. Durch das Nachrechnen der Idealaxiome folgt, dass $\mathfrak{b}$ ein Ideal ist. Nach Definition von $\mathfrak{b}$ gilt sofort die Inklusion $\mathfrak{b} \cdot \mathfrak{a} \subseteq (\alpha)$. Wir müssen also nur noch die andere inklusion zeigen. Setze dazu $\mathfrak{c} := \frac{1}{\alpha}\,\mathfrak{b}\,\mathfrak{a}$, dann ist $\mathfrak{c} \subseteq R$.

Fall I ($\mathfrak{c} = R$)**:** In diesem Fall folgt die Behauptung sofort.

Fall II ($\mathfrak{c} \neq R$)**:** In diesem Fall gibt es nach Lemma 5.4 ein Element $\gamma \in K \backslash R$ mit $\gamma \cdot \mathfrak{c} \subseteq R$. Es gelten

$$\mathfrak{b} \subseteq \mathfrak{c} \;\Rightarrow\; \gamma\,\mathfrak{b} \subseteq \gamma\,\mathfrak{c} \subseteq R \qquad \text{und} \qquad \gamma\,\mathfrak{c} \subseteq R \;\Leftrightarrow\; \gamma\,\mathfrak{b}\,\mathfrak{a} \subseteq (\alpha)$$

Also ist $\gamma\,\mathfrak{b} \;\subseteq\; \mathfrak{b}$. Da $\mathfrak{b}$ ein endlich erzeugtes Ideal von R nach **(D1)** ist, ist $\mathfrak{b}$ ein endlich erzeugter R-Modul. Mit Satz 2.3 ist γ also ganz über R. Da R ganz abgeschlossen ist, heißt das $\gamma \in R$. Dies ist ein Widerspruch, da γ aus $K \backslash R$ gewählt wurde.

Da der zweite Fall nicht auftreten kann, ist der Satz bewiesen. $\square$

Folgerung 5.6 *Seien* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \lhd R$ *Ideale mit* $\mathfrak{a} \neq (0)$*, dann gilt*

$$\mathfrak{a} \cdot \mathfrak{b} \;=\; \mathfrak{a} \cdot \mathfrak{c} \quad\Rightarrow\quad \mathfrak{b} \;=\; \mathfrak{c}$$

Beweis. Seien $\alpha \in \mathfrak{a} \backslash \{(0)\}$ und $\mathfrak{a}' := \left\{ \beta \in R \,\middle|\, \beta\,\mathfrak{a} \subseteq (\alpha) \right\}$. Nach dem vorangegangenen Satz gilt dann $\mathfrak{a}' \cdot \mathfrak{a} = (\alpha)$, also folgt

$$\alpha\,\mathfrak{b} \;=\; \mathfrak{a}'\,\mathfrak{a}\,\mathfrak{b} \;=\; \mathfrak{a}'\,\mathfrak{a}\,\mathfrak{c} \;=\; \alpha\,\mathfrak{c}$$

Da Dedekindringe Integritätsbereiche sind, folgt damit die Behauptung. $\square$

Definition und Folgerung 5.7 *(*$\mathfrak{a}$ *teilt* $\mathfrak{b}$*)*

Seien $\mathfrak{a}, \mathfrak{b} \lhd R$ *zwei Ideale. Wir sagen* $\mathfrak{a}$ *teilt* $\mathfrak{b}$ *und schreiben* $\mathfrak{a} \mid \mathfrak{b}$*, wenn es ein Ideal* $\mathfrak{c} \lhd R$ *mit* $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$ *gibt. In Dedekindringen gilt: Genau dann wird* $\mathfrak{b}$ *von* $\mathfrak{a}$ *geteilt, wenn* $\mathfrak{b} \subseteq \mathfrak{a}$ *ist.*

Beweis. Angenommen es gibt ein solches $\mathfrak{c} \lhd R$, dann gilt

$$\mathfrak{b} \;=\; \mathfrak{a}\cdot\mathfrak{c} \;\subseteq\; \mathfrak{a}R \;=\; \mathfrak{a}$$

Wir wollen nun die andere Implikation betrachten. Im Sonderfall $\mathfrak{a} = (0)$ folgt sofort, dass auch $\mathfrak{b} = (0)$ ist. Damit ist $\mathfrak{c} := (0)$ ein Ideal, mit der gesuchten Eigenschaft. Im Hauptfall sei $\alpha \in \mathfrak{a}\setminus\{0\}$. Wir setzen wieder $\mathfrak{a}' := \big\{\beta \in R \,\big|\, \beta\,\mathfrak{a} \subseteq (\alpha)\big\}$. Die Voraussetzung $\mathfrak{b} \subseteq \mathfrak{a}$ liefert zusammen mit Satz 5.5

$$\mathfrak{a}'\,\mathfrak{b} \;\subseteq\; \mathfrak{a}'\,\mathfrak{a} \;=\; (\alpha)$$

Mit Folgerung 5.6 gilt

$$\mathfrak{a}\cdot\mathfrak{c} \;=\; \frac{\mathfrak{a}'\,\mathfrak{a}}{\alpha}\cdot\mathfrak{b} \;=\; \mathfrak{b}$$

für $\mathfrak{c} := \frac{1}{\alpha}\,\mathfrak{a}\,\mathfrak{b} \lhd R$. □

Wir sind nun in der Lage den als Ziel vormulierten Satz zu beweisen:

Satz 5.8 *Sei $\mathfrak{a} \lhd R$ ein Ideal mit $(1) \neq \mathfrak{a} \neq (0)$, dann gibt es $\wp_1, \ldots, \wp_r \in \mathrm{Spec}(R)\setminus\{0\}$ mit*

$$\mathfrak{a} \;=\; \wp_1 \cdot \ldots \cdot \wp_r$$

und die $\wp_i$ sind bis auf Reihenfolge eindeutig bestimmt.

Beweis. Wir zeigen zunächst die Existenz. Dafür betrachten wir wieder die Famile der Ideale aus R für die der Satz nicht stimmt und wollen zeigen, dass diese leer sein muss. Sei also

$$S \;:=\; \big\{\; \mathfrak{a} \lhd R \,\big|\, (1) \neq \mathfrak{a} \neq (0) \text{ und } \mathfrak{a} \text{ hat keine Zerlegung in Primideale} \;\big\}$$

Angenommen S wäre nicht leer, dann hätte S ein maximales Element $\mathfrak{a}$ bezüglich der Inklusion „$\subseteq$“, denn R ist insbesondere noethersch. Unter dieser Annahme gäbe es ein maximales Ideal $\mathfrak{p} \in \mathrm{Spm}(R)$ mit $\mathfrak{a} \subset \mathfrak{p}$ und $\mathfrak{a} \neq \mathfrak{p}$ da sonst $\mathfrak{a}$ nicht aus S wäre. Mit Folgerung 5.7 gäbe es dann ein $\mathfrak{b} \lhd R$ mit

$$\mathfrak{a} \;=\; \mathfrak{p}\cdot\mathfrak{b} \quad \text{und} \quad \mathfrak{a} \subsetneq \mathfrak{b}$$

Da $\mathfrak{a}$ als das maximale Element von S gewählt wurde, wäre $\mathfrak{b}$ kein Element von S. Wir finden also eine Zerlegung $\wp_1, \ldots, \wp_r \in \mathrm{Spec}(R)\setminus\{(0)\}$ mit $\mathfrak{b} = \wp_1 \cdot \ldots \cdot \wp_r$. Dann erhielten wir aber mit

$$\mathfrak{a} \;=\; \mathfrak{p}\cdot\mathfrak{b} \;=\; \mathfrak{p}\cdot\wp_1 \cdot \ldots \cdot \wp_r$$

eine Zerlegung in Primideale von $\mathfrak{a}$. Damit wäre $\mathfrak{a} \notin S$ was ein Widerspruch ist.

Wir wollen nun die Eindeutigkeit zeigen. Dazu seinen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \mathrm{Spec}(R)\setminus\{(0)\}$ Primideale mit

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \;=\; \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$$

Mit Folgerung 5.7 ist dann $\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdot \ldots \cdot$"$_s$, also gibt es wegen der Primeigenschaft ein $i \in \{1, \ldots, s\}$ mit $\mathfrak{p}_1 \supset \mathfrak{q}_i$. Da R dedekindsch ist, sind beide Primideale maximal, und somit folgt $\mathfrak{p}_1 = \mathfrak{q}_i$. Ohne Einschränkung sei $i = 1$ (Ansonsten nummeriere die $\mathfrak{q}_j$ entsprechend um), dann ist

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \;=\; \mathfrak{p}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$$

Mit Folgerung 5.6 gilt dann

$$\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \;=\; \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$$

Wiederholen wir diesen Schritt insgesamt r mal folgt $r = s$ und $\mathfrak{p}_i = \mathfrak{q}_i$ für $i = 1, \ldots, r$. □

Beispiel 13 *Sei $R = \mathbb{Z}$. Wir wissen, dass $\mathbb{Z}$ ein Hauptidealring ist. Für $n \in \mathbb{Z}_{>1}$ gilt*

$$(n) \in \operatorname{Spec}\mathbb{Z} \;\Leftrightarrow\; {}^{\mathbb{Z}}\!/_{(n)} \text{ ist Integritätsring} \;\Leftrightarrow\; n \text{ ist Primzahl}$$

Damit erhalten wir in diesem Fall die gewünschte Übereinstimmung der beiden Faktorisierungen, denn n hat genau dann die Primfaktorzerlegung $n = (\pm 1) \cdot p_1 \cdot \ldots \cdot p_r$, wenn das Hauptideal (n) die Faktorisierung $(n) = (p_1) \cdot \ldots \cdot (p_r)$ besitzt.

Beispiel 14 *Sei $K = \mathbb{Q}(\sqrt{-5})$ dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, denn -5 ist kongruent zu 3 modulo 4. Anhand von*

$$21 \;=\; 3 \cdot 7 \;=\; (4 + \sqrt{5}) \cdot (4 - \sqrt{5})$$

sehen wir, dass wir keine eindeutige Primfaktorzerlegung erhalten. Wir wollen nun das Hauptideal (21) betrachten. Dazu setze

$$\wp_1 := (3, 1 + \sqrt{-5}) \qquad \wp_2 := (3, 1 - \sqrt{-5})$$
$$\wp_3 := (7, 3 + \sqrt{-5}) \qquad \wp_4 := (7, 3 - \sqrt{-5})$$

Wir wollen zeigen, dass diese Ideale Primideale sind. dabei nutzen wir die Isomorphie

$$\mathbb{Z}[\sqrt{-5}] \;\cong\; {}^{\mathbb{Z}[X]}\!/_{(X^2+5)}$$

aus. Um zu zeigen, dass die ersten beiden Ideale prim sind, betrachten wir den Ganzheitsring modulo 3. Mit der obigen Isomorphie erhalten wir

$${}^{\mathbb{Z}[\sqrt{-5}]}\!/_{(3)} \;\cong\; {}^{\mathbb{F}_3[X]}\!/_{(X^2+5)}$$

In $\mathbb{F}_3[X]$ können wir das Polynom $X^2 + 5$ weiter zerlegen. Es gilt

$$X^2 + 5 \;=\; X^2 - 1 \;=\; (X - 1)(X + 1) \qquad \text{in } \mathbb{F}_3[X]$$

Wir können nun die Isomorphiekette weiter Fortsetzen zu

$${}^{\mathbb{Z}[\sqrt{-5}]}\!/_{(3)} \;\cong\; {}^{\mathbb{F}_3[X]}\!/_{(X^2+5)} \;\cong\; {}^{\mathbb{F}_3[X]}\!/_{(X-1)} \times {}^{\mathbb{F}_3[X]}\!/_{(X+1)} \;\cong\; \mathbb{F}_3 \times \mathbb{F}_3$$

Damit sind $(3, X + 1), (3, X - 1) \lhd {}^{\mathbb{Z}[X]}\!/_{(X^2+5)}$ primideale. Diese korrespondieren via des oben angegebenen Isomorphismus $X \mapsto \sqrt{-5}$ zu den Idealen $\wp_1$ und $\wp_2$. Es gilt

$$\wp_1 \cdot \wp_2 \;=\; (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}) \;=\; (3^2, 3(\sqrt{-5} + 1), 3(\sqrt{-5} - 1), -5 - 1) \;=\; (3)$$

Nun wollen wir zeigen, dass auch die anderen beiden Ideale prim sind, dazu betrachten wir den Ganzheitsring modulo 7 und stellen mit der in $\mathbb{F}_7[X]$ gültigen Zerlegung $X^2 + 5 = (X - 3)(X + 3)$ fest, dass

$${}^{\mathbb{Z}[\sqrt{-5}]}\!/_{(7)} \;\cong\; {}^{\mathbb{F}_7[X]}\!/_{(X^2+5)} \;\cong\; {}^{\mathbb{F}_7[X]}\!/_{(X-3)} \times {}^{\mathbb{F}_7[X]}\!/_{(X+3)}$$

Wie gerade erhalten wir, dass $(7, X - 3), (7, X + 3) \lhd {}^{\mathbb{Z}[X]}\!/_{(X^2+5)}$ primideale sind. Betrachten wir nun das Produkt der beiden Ideale $\wp_3$ und $\wp_4$ erhalten wir

$$\wp_3 \cdot \wp_4 \;=\; (7, 3 + \sqrt{-5}) \cdot (7, 3 - \sqrt{-5}) \;=\; (7^2, 7(\sqrt{-5} - 3)(\sqrt{-5} + 3), -5 - 9) \;=\; (7)$$

Und damit haben wir die eindeutige Faktorisierung in Primideale

$$(21) \;=\; (3) \cdot (7) \;=\; \wp_1 \cdot \wp_2 \cdot \wp_3 \cdot \wp_4$$

gefunden.

Satz 5.9 *(Chinesischer Restsatz)*
Sei A ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \lhd A$ Ideale von A mit $\mathfrak{a}_i + \mathfrak{a}_j = A$ für $i \neq j$. Dann ist die Abbildung

$$\begin{array}{rcl} \varphi : A & \to & {}^{A}\!/_{\mathfrak{a}_1} \times \cdots \times {}^{A}\!/_{\mathfrak{a}_n} \\ a & \mapsto & (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n) \end{array}$$

ein surjektiver Ringhomomorphismus mit $\mathrm{Ker}(\varphi) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$. Insbesondere gilt

$${}^{A}\!/_{(\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n)} \;\cong\; {}^{A}\!/_{\mathfrak{a}_1} \times \cdots \times {}^{A}\!/_{\mathfrak{a}_n}$$

Beweis. Die Homomorphieeigenschaft und Wohldefiniertheit ergibt sich komponentenweise aus den natürlichen Projektionen. Nach Voraussetzung ist $\mathfrak{a}_1 + \mathfrak{a}_j = A$ für alle $j = 2, \ldots, n$. Damit gilt

$$\mathfrak{a}_1 + \big(\mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n \big) \;=\; A$$

Ohne Einschränkung kann also angenommen werden, dass $n = 2$ gilt. Wegen der Voraussetzung $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ gibt es Elemente $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$ mit $a_1 + a_2 = 1$. Dann gilt für alle $x \in A$

$$x \;=\; \underbrace{x \cdot a_1}_{\in \mathfrak{a}_1} + \underbrace{x \cdot a_2}_{\in \mathfrak{a}_2}$$

Wegen $a_i + \mathfrak{a}_i = \mathfrak{a}_i$ und $a_j + \mathfrak{a}_i = 1 + \mathfrak{a}_i$ für $i \in \{1, 2\}$ gelten

$$\begin{array}{rcccl} \varphi(a_1) & = & (a_1 + \mathfrak{a}_1, a_1 + \mathfrak{a}_2) & = & (0 + \mathfrak{a}_1, 1 + \mathfrak{a}_2) \\ \varphi(a_2) & = & (a_2 + \mathfrak{a}_1, a_2 + \mathfrak{a}_2) & = & (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2) \end{array}$$

Mit diesen Elementen können wir zu jedem $(b_1 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2) \in {}^{A}\!/_{\mathfrak{a}_1} \times {}^{A}\!/_{\mathfrak{a}_2}$ ein Urbild bezüglich φ angeben, denn φ ist ein Ringhomomorphismus. □

Definition 5.10 *(Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches von Idealen)*
Seien $\mathfrak{a}, \mathfrak{b} \lhd R$ Ideale. Ein Ideal $\mathfrak{c} \lhd R$ heißt

- *größter gemeinsamer Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, wenn $\mathfrak{c}$ sowohl $\mathfrak{a}$ als auch $\mathfrak{b}$ teilt und wenn, wann immer ein weiteres Ideal $\mathfrak{c}' \lhd R$ die beiden Ideale $\mathfrak{a}$ und $\mathfrak{b}$ teilt, dann teilt $\mathfrak{c}'$ auch $\mathfrak{c}$. In Formeln*

$$\mathfrak{c} \;=\; \mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) \;\;:\Leftrightarrow\;\; \Big[\big(\mathfrak{c} \,|\, \mathfrak{a} \wedge \mathfrak{c} \,|\, \mathfrak{b} \big) \;\wedge\; \big(\forall\, \mathfrak{c}' \lhd R : (\mathfrak{c}' \,|\, \mathfrak{a} \wedge \mathfrak{c}' \,|\, \mathfrak{b}) \Rightarrow \mathfrak{c}' \,|\, \mathfrak{c} \big) \Big]$$

- *kleinstes gemeinsames Vielfaches von $\mathfrak{a}$ und $\mathfrak{b}$, wenn sowohl $\mathfrak{a}$ als auch $\mathfrak{b}$ das Ideal $\mathfrak{c}$ teilen und wenn $\mathfrak{a}$ und $\mathfrak{b}$ ein weiteres Ideal $\mathfrak{c}' \lhd R$ teilen, dann wird $\mathfrak{c}'$ auch von $\mathfrak{c}$ geteilt. In Formeln*

$$\mathfrak{c} \;=\; \mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) \;\;:\Leftrightarrow\;\; \Big[\big(\mathfrak{a} \,|\, \mathfrak{c} \wedge \mathfrak{b} \,|\, \mathfrak{c} \big) \;\wedge\; \big(\forall\, \mathfrak{c}' \lhd R : (\mathfrak{a} \,|\, \mathfrak{c}' \wedge \mathfrak{b} \,|\, \mathfrak{c}') \Rightarrow \mathfrak{c} \,|\, \mathfrak{c}' \big) \Big]$$

Wie in den Formeln bereits genutzt schreiben wir wie bei Zahlen auch $\mathrm{ggT}(\cdot, \cdot)$ und $\mathrm{kgV}(\cdot, \cdot)$.

Anmerkung Diese Definition entspricht genau der Definition der entsprechenden Eigenschaften für Zahlen.

Lemma 5.11 *Seien $\mathfrak{a}, \mathfrak{b} \lhd R$ Ideale. In Dedekindringen gilt*

$$\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) \;=\; \mathfrak{a} + \mathfrak{b} \quad \text{und} \quad \mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) \;=\; \mathfrak{a} \cap \mathfrak{b}$$

Beweis. Nach Folgerung 5.7 gilt in Dedekindringen: $\mathfrak{c}$ teilt genau dann $\mathfrak{a}$, wenn $\mathfrak{a} \subseteq \mathfrak{c}$ ist. Es gelten:
- $\mathfrak{a} + \mathfrak{b}$ ist das kleinste Ideal in R, dass $\mathfrak{a}$ und $\mathfrak{b}$ enthält.
- $\mathfrak{a} \cap \mathfrak{b}$ ist das größte Ideal in R, dass in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten ist. □

Folgerung 5.12 *Zwei Ideale $\mathfrak{a}, \mathfrak{b} \lhd R$ sind genau dann Teilerfremd, wenn $\mathfrak{a} + \mathfrak{b} = (1) = R$ gilt.* □

Bemerkung 5.13 *Seien $\mathfrak{a}, \mathfrak{b} \lhd R$ zwei Ideale, dann finden wir nach Satz 5.8 paarweise verscheidene Primideale $\wp_1, \ldots, \wp_s \in \operatorname{Spec}(R) \backslash \{(0)\}$ so dass wir $\mathfrak{a}$ und $\mathfrak{b}$ zerlegen können in*

$$\mathfrak{a} \;=\; \wp_1^{a_1} \cdot \ldots \cdot \wp_s^{a_s} \quad \text{und} \quad \mathfrak{b} \;=\; \wp_1^{b_1} \cdot \ldots \cdot \wp_s^{b_s}$$

mit Exponenten $a_i, b_i \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Wir erhalten dann auch Darstellungen für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache als

$$\begin{aligned} \operatorname{ggT}(\mathfrak{a}, \mathfrak{b}) &= \wp_1^{m_1} \cdot \ldots \cdot \wp_s^{m_s} \quad \text{mit } m_i := \min\{a_i, b_i\} \\ \operatorname{kgV}(\mathfrak{a}, \mathfrak{b}) &= \wp_1^{M_1} \cdot \ldots \cdot \wp_s^{M_s} \quad \text{mit } M_i := \max\{a_i, b_i\} \end{aligned}$$

Folgerung 5.14 *Seien $\mathfrak{a}, \mathfrak{b} \lhd R$ zwei teilerfremde Ideale, dann ist $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.*

Beweis. Betrachte die Zerlegungen für $\mathfrak{a}$ und $\mathfrak{b}$ sowie für das kleinste gemeinsame Vielfache aus Bemerkung 5.13. Wenn $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, ist entweder immer $a_i = 0$ oder $b_i = 0$, also ist

$$\operatorname{kgV}(\mathfrak{a}, \mathfrak{b}) \;=\; \mathfrak{a} \cdot \mathfrak{b}$$

Mit Lemma 5.11 folgt nun die Behauptung □

Folgerung 5.15 *Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \lhd R$ paarweise Teilerfremde Ideale, dann gilt*

$$R\big/_{(\mathfrak{a}_1 \cdots \mathfrak{a}_n)} \;\cong\; R\big/_{\mathfrak{a}_1} \times \cdots \times R\big/_{\mathfrak{a}_n}$$

Beweis. Mit dem Chinesischen Restsatz 5.9 und der soeben gezeigten Folgerung 5.14 ist bereits alles gezeigt. □

Definition und Satz 5.16 *(Die absolute Norm)*
Sei $K/\mathbb{Q}$ eine endliche Erweiterung sowie $\mathfrak{a} \lhd \mathcal{O}_K$ ein Ideal mit $\mathfrak{a} \neq (0)$. Dann enthält $\mathcal{O}_K\big/_{\mathfrak{a}}$ nur endlich viele Elemente. Wir definieren die absolute Norm von $\mathfrak{a}$ durch

$$\mathbb{N}(\mathfrak{a}) \;:=\; \mathrm{N}(\mathfrak{a}) \;:=\; \sharp\left(\mathcal{O}_K\big/_{\mathfrak{a}}\right)$$

Beweis. Nach Voraussetzung ist $\mathfrak{a}$ nicht das Nullideal, also gibt es ein $\alpha \in \mathfrak{a} \backslash \{0\}$. Aus dem vorangegangen Abschnitt wissen wir

$$N_{\mathbb{Q}}^{K}(\alpha) \;=\; \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \sigma(\alpha) \;\in\; \mathfrak{a} \cap \mathbb{Q} \;=\; \mathfrak{a} \cap \mathbb{Z}$$

also ist insbesondere das Ideal $\mathfrak{a} \cap \mathbb{Z} \lhd \mathbb{Z}$ nicht das Nullideal. Dann gibt es aber ein $n \in \mathbb{N}$ mit

$$n\,\mathbb{Z} \;=\; (n) \;=\; \mathfrak{a} \cap \mathbb{Z}$$

Da $\mathcal{O}_K$ ein endlich erzeugter $\mathbb{Z}$-Modul ist, ist $\mathcal{O}_K\big/_{\mathfrak{a}}$ ein endlich erzeugter $\mathbb{Z}\big/_{n\,\mathbb{Z}}$ modul. Da aber $\mathbb{Z}\big/_{n\,\mathbb{Z}}$ nur endlich viele Elemente enthält folgt die Behauptung. □

Lemma 5.17 *Sei $K/\mathbb{Q}$ ein endlicher Erweiterungskörper. Seien $\wp \in \mathrm{Spec}(\mathcal{O}_K)\backslash\{(0)\}$ ein Primideal und $p \in \mathbb{Z}$ eine Primzahl. Die folgenden Aussagen sind äquivalent:*

(i) *p teilt die absolute Norm von $\wp$, also $p|\,\mathbb{N}(\wp)$*

(ii) *Die absolute Norm von $\wp$ ist eine natürliche Potenz von p, also $\mathbb{N}(\wp) = p^f$ mit $f \in \mathbb{N}$*

(iii) *Es gilt $\wp \cap \mathbb{Z} \;=\; p\,\mathbb{Z} \;=\; (p)$*

(iv) *$\wp$ teilt das von p in $\mathcal{O}_K$ erezugte Ideal, also $\wp | p\,\mathcal{O}_K$.*

Beweis. Da $\wp$ ein Primideal ungleich Null in einem Dedekindring ist, ist $\wp$ ein maximales ideal. Damit ist $\mathcal{O}_K/\wp$ ein Körper. Mit der Einbettung

$$A \;:=\; \mathbb{Z}/\wp\cap\mathbb{Z} \hookrightarrow \mathcal{O}_K/\wp$$

folgt, dass $\wp \cap \mathbb{Z}$ ein von Null verschiedenes Primideal in $\mathbb{Z}$ sein muss, denn A ist notwendig ein Integritätsring. Wir wissen, dann gibt es eine Primzahl $p \in \mathbb{Z}$ mit $(p) = \wp \cap \mathbb{Z}$. Nach Satz 5.16 ist $\mathcal{O}_K/\wp$ endlich über $\mathbb{Z}/p\,\mathbb{Z} =: \mathbb{F}_p$ erzeugt. Es gilt nun

$$\sharp\left(\mathcal{O}_K/\wp\right) \;=\; p^f \qquad \text{mit } f = \left[\mathcal{O}_K/\wp : \mathbb{F}_p\right]$$

Damit haben wir bereits **(i)**⇔**(ii)**⇔**(iii)** gezeigt. Für den letzten Punkt betrachte

$$\wp | p\,\mathcal{O}_K \;\Leftrightarrow\; p\,\mathcal{O}_K \subseteq \wp \;\Leftrightarrow\; p \in \wp\cap\mathbb{Z} \;\Leftrightarrow\; (p) = \wp\cap\mathbb{Z}$$

□

Anmerkung Mit diesem Beweis haben wir nicht nur die Äquivalenz der vier Aussagen gezeigt, sondern auch, dass es zu jedem Primideal undgleich Null in $\mathcal{O}_K$ eine solche Primzahl gibt.

Im nächsten Schritt wollen wir zeigen, dass die absolute Norm multiplikativ ist. Dazu benötigen wir aber noch die Theorie der gebrochenen Ideale. Ideale, die wir in Zukunft auch ganze Ideale nennen werden, können wir als Untermodul des Rings auffassen, wenn wir den Ring selber als einen Modul über sich selbst betrachten. Da wir zur Zeit nur Dedekindringe betrachten, ist jedes Ideal sogar ein endlich erzeugter Untermodul des Rings. In Analogie dazu stellen wir die folgende auf. Wir erinnern noch einmal an die Generalvoraussetzung in diesem Abschnitt: Mit R bezeichnen wir stets einen Dedekindring und mit $K = \mathrm{Quot}(R)$ seinen Quotientenkörper.

Definition 5.18 *(Gebrochenes Ideal)*
Ein gebrochenes Ideal $\mathfrak{a}$ von R ist ein endlich erzeugter R-Untermodul von $K = \mathrm{Quot}(R)$, das heißt

$$\mathfrak{a} \;=\; R\lambda_1 + \ldots + R\lambda_n \;\subseteq\; K$$

mit $\lambda_1, \ldots, \lambda_n \in K$.

Anmerkung Die (ganzen) Ideale von R sind natürlich auch endlich erzeugte R-Untermoduln von K. Dieses Phänomen kennen wir schon von ganzen Zahlen, die wir ja auch als rationale Zahlen auffassen können.

Lemma 5.19 *Sei $\mathfrak{a} \subseteq K$ ein R-Untermodul, dann ist $\mathfrak{a}$ genau dann ein gebrochenes Ideal von R, wenn es ein $\alpha \in R\backslash\{0\}$ so gibt, dass $\alpha \cdot \mathfrak{a} \subseteq R$ gilt.*

Beweis. Angenommen $\mathfrak{a}$ sei ein gebrochenes Ideal, also ein endlich erzeugter R-Modul, dann gibt es $\lambda_1, \ldots, \lambda_n \in K$ mit

$$\mathfrak{a} \;=\; R\lambda_1 + \ldots + R\lambda_n \;\subseteq\; K$$

Da $K = \mathrm{Quot}(R)$ ist, gibt es ein $\alpha \in R\backslash\{0\}$ so dass $\alpha \cdot \lambda_i \in R$ für alle $i = 1, \ldots, n$ gilt. Dieses α erfüllt die Behauptung.
Andererseits nimm an, $\alpha \in R\backslash\{0\}$ erfüllt die Bedingung $\alpha \cdot \mathfrak{a} \subseteq R$, dann gibt es $x_1, \ldots, x_n \in R$ mit

$$\alpha\,\mathfrak{a} \;=\; Rx_1 + \ldots + Rx_n$$

denn R ist ein Dedekindring, also insbesondere noethersch. Damit folgt aber

$$\mathfrak{a} \;=\; R\frac{x_1}{\alpha} + \ldots + R\frac{x_n}{\alpha}$$

□

Definition und Satz 5.20 *(Gruppe der gebrochenen Ideale)*
Sei $K = \mathrm{Quot}(R)$, dann heißt

$$I(K) \;:=\; \left\{\, \mathfrak{a} \subseteq K \;\middle|\; \mathfrak{a} \neq \{0\} \text{ und } \mathfrak{a} \text{ ist ein gebrochenes Ideal von } R \,\right\}$$

Gruppe der gebrochenen Ideale in K. Wobei die Gruppenverknüpfung durch

$$\mathfrak{a} \cdot \mathfrak{b} \;:=\; \left\{ \sum_{i=1}^{d} a_i b_i \;\middle|\; d \in \mathbb{N} \wedge a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b} \right\}$$

für $\mathfrak{a}, \mathfrak{b} \in I(K)$ gegeben ist. Weiter ist $R \in I(K)$ das neutrale Element und zu $\mathfrak{a} \in I(K)$ ist

$$\mathfrak{a}^{-1} \;:=\; \left\{\, x \in K \;\middle|\; x \cdot \mathfrak{a} \subseteq R \,\right\}$$

das inverse Element.

Beweis. Die Menge $I(K)$ ist unter der gegebenen Multiplikation abgeschlossen, denn für

$$\mathfrak{a} \;=\; Ra_1 + \ldots + Ra_n \quad \text{und} \quad \mathfrak{b} \;=\; Rb_1 + \ldots + Rb_m$$

ist

$$\mathfrak{a} \cdot \mathfrak{b} \;=\; \sum_{i=1}^{n} \sum_{j=1}^{m} Ra_i b_j$$

Insbesondere stimmt die Einschränkung der Multiplikation mit der uns bereits bekannten Multiplikation der ganzen Ideale überein. Es gilt $\mathfrak{a} \cdot R = \mathfrak{a} = R \cdot \mathfrak{a}$ für alle $\mathfrak{a} \in I(K)$, also ist R das neutrale Element. Für den Nachweis der Existenz inverser Elemente berachte das folgende

Lemma 5.21 *Sei $\mathfrak{a} \in I(K)$ ein gebrochenes Ideal. Es gibt ein gebrochenes Ideal $\mathfrak{b} \in I(K)$ mit*

$$\mathfrak{b} \cdot \mathfrak{a} = R$$

Beweis. Nach Lemma 5.19 gibt es ein $\alpha \in R\backslash\{0\}$ mit $\alpha \cdot \mathfrak{a} \subseteq R$. Wähle ein $\beta \in \alpha\,\mathfrak{a}$ mit $\beta \neq 0$ und setze $\mathfrak{a}' := \left\{ x \in R \,\middle|\, x \cdot \alpha\,\mathfrak{a} \subseteq (\beta) \right\}$. Wegen $(\beta) \subseteq \alpha\,\mathfrak{a}$ gilt $\mathfrak{a}' = \left\{ x \in K \,\middle|\, x \cdot \alpha\,\mathfrak{a} \subseteq (\beta) \right\} \subseteq K$. Nach Satz 5.5 gilt

$$\mathfrak{a}' \cdot (\alpha\,\mathfrak{a}) \;=\; (\beta)$$

Definiere nun

$$\mathfrak{b} \;:=\; \frac{\alpha}{\beta}\,\mathfrak{a}' \;=\; \left\{ x \in K \,\middle|\, \frac{\alpha x}{\beta}\,\mathfrak{a} \subseteq R \right\} \;=\; \left\{ y \in K \,\middle|\, y\,\mathfrak{a} \subseteq R \right\}$$

dann erfüllt $\mathfrak{b}$ die Behauptung, denn es gilt

$$\mathfrak{b} \cdot \mathfrak{a} \;=\; \frac{\alpha}{\beta}\,\mathfrak{a}'\,\mathfrak{a} \;=\; \frac{1}{\beta}(\beta) \;=\; (1) \;=\; R$$

$\diamond$

Mit diesem Lemma ist alles gezeigt. $\square$

Bemerkung 5.22 *Wenn $\wp \in \mathrm{Spec}(R)\backslash\{(0)\}$ ein Primideal ist, können wir spezielle gebrochene Ideale betrachten. Aus dem vorangegangenen Satz erhalten wir nun zunächst das Inverse zu $\wp$ als gebrochenes Ideal $\wp^{-1} = \left\{ x \in K \,\middle|\, x \cdot \wp \subseteq R \right\}$. Damit gilt für $n \in \mathbb{N}$*

$$(\wp^{-1})^n \cdot \wp^n \;=\; (\wp^{-1}\wp)^n \;=\; \big((1)\big)^n \;=\; (1^n) \;=\; (1) \;=\; R$$

Für alle natürlichen Potenzen $n \in \mathbb{N}$ gelten

1. $\wp^n \;\neq\; \wp^{n+1}$
2. *Es gibt keine ganzen Ideale, die echt zwischen $\wp^{n+1}$ und $\wp^n$ liegen*
3. *Sei $a \in \wp^n$ mit $a \notin \wp^{n+1}$, dann ist $\wp^n = (a) + \wp^{n+1}$*

Beweis. Für die erste Eigenschaft nimm an $\wp^i$ und $\wp^{i-1}$ wären gleich, dann gilt

$$\wp^i \;=\; \wp^{i-1} \quad\Leftrightarrow\quad \wp^i \cdot \wp^{-1} \;=\; \wp^{i-1} \cdot \wp^i \quad\Leftrightarrow\quad \wp \;=\; R$$

was ein Widerspruch ist, denn $\wp$ ist ein Primideal. Auch die zweite Eigenschaft beweisen wir indirekt. Nimm also an, es gäbe ein $\mathfrak{b} \lhd R$ mit $\wp^{i+1} \subsetneq \mathfrak{b} \subsetneq \wp^i$, dann folgt wie oben

$$\wp \subsetneq \mathfrak{b}\,\wp^{-i} \subsetneq R$$

Aber $R\!/\!_{\wp}$ ist ein Körper, denn $\wp$ ist als Primideal eines Dedekindrings maximal. Die dritte Aussage folgt aus den ersten beiden. $\square$

Lemma 5.23 *Da R nach Voraussetzung dedekindsch ist, gilt $\mathrm{Spec}(R)\backslash\{(0)\} = \mathrm{Spm}(R)$, denn alle von Null verschiedenen Primideale sind maximal. Die folgende Abbildung ist ein Isomorphismus*

$$\begin{array}{ccc} \displaystyle\bigoplus_{\wp \in \mathrm{Spm}(R)} \mathbb{Z} & \xrightarrow{\sim} & I(K) \\ (v_\wp)_{\wp \in \mathrm{Spm}(R)} & \mapsto & \displaystyle\prod_{\wp \in \mathrm{Spm}(R)} \wp^{v_\wp} \end{array}$$

Beweis. Die Abbildung ist wolhdefiniert, denn jedes Tupel $(v_\wp)_{\wp\in\mathrm{Spm}(R)}$ enthält nur endlich viele Einträge ungleich Null. Wir müssen nun noch zeigen, dass jedes von Null verschiedene gebrochene Ideal $\mathfrak{a} \in I(K)$ sich als eindeutiges Produkt von Primidealpotenzen schreiben lässt. Sei also $\mathfrak{a} \in I(K)$ ein gebrochenes Ideal mit $\mathfrak{a} \neq (0)$, dann gibt es ein $\alpha \in R$, so dass $\alpha\,\mathfrak{a} \lhd R$ ein ganzes Ideal ist. Nach Satz 5.8 gibt es dann $\mathfrak{q}_1, \ldots, \mathfrak{q}_n, \mathfrak{p}_1, \ldots, \mathfrak{p}_m \in \mathrm{Spm}(R)$ mit

$$(\alpha) \;=\; \mathfrak{q}_1^{w_1} \cdot \ldots \cdot \mathfrak{q}_n^{w_n} \qquad \text{und} \qquad \alpha\,\mathfrak{a} \;=\; \mathfrak{q}_1^{v_1} \cdot \ldots \cdot \mathfrak{p}_n^{v_n}$$

mit natürlichen Zahlen[3] $v_i, w_i \in \mathbb{N}$. Damit erhalten wir eine Darstellung

$$\mathfrak{a} \;=\; \mathfrak{q}_1^{-w_1} \cdot \ldots \cdot \mathfrak{q}_n^{-w_n} \cdot \mathfrak{q}_1^{v_1} \cdot \ldots \cdot \mathfrak{p}_n^{v_n}$$

Wir können also jedes $\mathfrak{a} \in I(K)$ als Produkt von Primidealpotenen darstellen. Diese Aussage ist gleichbedeutend mit der Aussage, dass die im Lemma vormulierte Abbildung surjektiv ist.
Betrachte nun zwei gleiche Produkte:

$$\begin{aligned}
&\prod_{\mathfrak{p}\in\mathrm{Spm}(R)} \mathfrak{p}^{v_\mathfrak{p}} \;=\; \prod_{\mathfrak{q}\in\mathrm{Spm}(R)} \mathfrak{q}^{w_\mathfrak{q}} \\
\Leftrightarrow\quad &\prod_{\substack{\mathfrak{p}\in\mathrm{Spm}(R)\\ v_\mathfrak{p}>0}} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\substack{\mathfrak{p}\in\mathrm{Spm}(R)\\ v_\mathfrak{p}<0}} \mathfrak{p}^{v_\mathfrak{p}} \;=\; \prod_{\substack{\mathfrak{q}\in\mathrm{Spm}(R)\\ w_\mathfrak{q}>0}} \mathfrak{q}^{w_\mathfrak{q}} \cdot \prod_{\substack{\mathfrak{q}\in\mathrm{Spm}(R)\\ w_\mathfrak{q}<0}} \mathfrak{q}^{w_\mathfrak{q}} \\
\Leftrightarrow\quad &\prod_{\substack{\mathfrak{p}\in\mathrm{Spm}(R)\\ v_\mathfrak{p}>0}} \mathfrak{p}^{v_\mathfrak{p}} \cdot \prod_{\substack{\mathfrak{q}\in\mathrm{Spm}(R)\\ w_\mathfrak{q}<0}} \mathfrak{q}^{-w_\mathfrak{q}} \;=\; \prod_{\substack{\mathfrak{q}\in\mathrm{Spm}(R)\\ w_\mathfrak{q}>0}} \mathfrak{q}^{w_\mathfrak{q}} \cdot \prod_{\substack{\mathfrak{p}\in\mathrm{Spm}(R)\\ v_\mathfrak{p}<0}} \mathfrak{p}^{-v_\mathfrak{p}}
\end{aligned}$$

Damit folgt die Injektivität der Abbildung aus der eindeutigen Faktorisierung für ganze Ideale nach Satz 5.8. □

Lemma 5.24 *Sei $\wp \in \mathrm{Spm}(R)$ und $n \in \mathbb{N}$, dann ist ${\wp^n}/{\wp^{n+1}}$ ein eindimensionaler ${R}/{\wp}$ Vektorraum.*

Beweis. Nach Bemerkung 5.22 gibt es ein $a \in \wp^n$ mit $a \notin \wp^{n+1}$ und $\wp^n = (a) + \wp^{n+1}$. Damit erzeugt aber das Bild von a in ${\wp^n}/{\wp^{n+1}}$ den R-Modul ${\wp^n}/{\wp^{n+1}}$. Die Modul-Skalarmultiplikation faktorisiert über $\wp$, also ist ${\wp^n}/{\wp^{n+1}}$ ein eindimesionaler Vektorraum über ${R}/{\wp}$ mit Basis $\{a + \wp^{n+1}\}$. □

Folgerung 5.25 *Ist für $\wp \in \mathrm{Spm}(R)$ der Restklassenkörper $\kappa(\wp) := {R}/{\wp}$ endlich, dann gelten*

$$\sharp\left({\wp^n}/{\wp^{n+1}}\right) \;=\; \sharp\left({R}/{\wp}\right) \qquad \text{und} \qquad \sharp\left({R}/{\wp^n}\right) \;=\; \sharp\left({R}/{\wp}\right)^n$$

für alle $n \in \mathbb{N}$.

Beweis. Nach dem vorangegangen Lemma sind die $\kappa(\wp)$-Vektorräume $\kappa(\wp)$ und ${\wp^n}/{\wp^{n+1}}$ isomorph, damit müssen beide auch gleichviele Elemente haben und es folgt die erste Gleichung.
Weiter gibt es eine natürliche Surjektion

$$\varphi : {R}/{\wp^n} \;\twoheadrightarrow\; {R}/{\wp^{n+1}}$$

[3] Beachte $\mathbb{N} \neq \mathbb{N}_0 := \mathbb{N} \cup \{0\}$

mit $\mathrm{Ker}(\varphi = {\wp^{n-1}}/{\wp^n}$. Aus der Gruppentheorie wissen wir, dass für eine endliche abelsche Gruppe G mit Untergruppe H gilt

$$\sharp G \;=\; \sharp\left({G}/{H}\right) \cdot \sharp H$$

und damit folgt

$$\sharp\left({R}/{\wp^n}\right) \;=\; \sharp\left({R}/{\wp^{n-1}}\right) \cdot \sharp\left({\wp^{n-1}}/{\wp^n}\right) \;=\; \ldots \;=\; \sharp\left({R}/{\wp}\right)^n$$

□

Satz 5.26 *Sei $K/\mathbb{Q}$ eine endliche Körpererweiterung und seien $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ von Null verschiedene Ideale, dann gilt*

$$\mathbb{N}(\mathfrak{a}) \cdot \mathbb{N}(\mathfrak{b}) \;=\; \mathbb{N}(\mathfrak{a} \cdot \mathfrak{b})$$

Beweis. Wir betrachten zunächst einen Spezialfall: Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd, so gilt

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

nach Folgerung 5.15. Damit ist indesem Spezialfall nichts weiter zu zeigen.
Da $\mathcal{O}_K$ dedekindsch ist, können wir die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in Primideale faktorisieren. Wegen des oben schon gezeigten Spezialfalls genügt es also den Satz für Potenzen von Primidealen zu zeigen, das heißt wir zeigen:

$$\mathbb{N}(\wp^k) \;=\; \big(\mathbb{N}(\wp)\big)^k \qquad \text{mit } \wp \in \mathrm{Spec}(\mathcal{O}_K)\backslash\{(0)\} \text{ und } k \in \mathbb{N}$$

Behauptung 1 *Sei $a \in {\mathcal{O}_K}/{\wp^k}$. Ist a keine Einheit, so gilt $a \in {\wp}/{\wp^k}$.*

Beweis. Aus $x \in {\wp}/{\wp^k}$ folgt stets $1 - x \in \mathcal{O}_K^\times$, denn es gilt

$$(1-x)(1 + x + x^2 + \ldots + x^{k-1}) \;=\; 1 - x^k \;=\; 1 \qquad \text{in } {\mathcal{O}_K}/{\wp^k}$$

Für $a \in {\mathcal{O}_K}/{\wp^k}$ mit bezeichne $\overline{a} \in {\mathcal{O}_K}/{\wp}$ die Äquivalenzklasse. Gilt $\overline{a} \neq \overline{0}$ so gibt es ein $b \in {\mathcal{O}_K}/{\wp^k}$ mit Äquivalenzklasse $\overline{b} \in {\mathcal{O}_K}/{\wp}$ und $\overline{ab} = \overline{1}$. Also ist $a \cdot b$ kongruent 1 modulo $\wp$. Das heißt es gibt ein $u \in \left({\mathcal{O}_K}/{\wp^k}\right)^\times$ mit $ab = u$ und damit ist insbesondere

$$a \cdot (bu^{-1}) \;=\; 1 \quad \text{ in } {\mathcal{O}_K}/{\wp^k}$$

also ist a eine Einheit. ◇

Behauptung 2 ${\mathcal{O}_K}/{\wp^k}$ *ist ein Hauptidealring*

Beweis. Sei $a \in {\mathcal{O}_K}/{\wp^k}$. Nach Bemerkung 5.22 Teil 1 gibt es ein $n \in \{1, \ldots, k-1\}$ mit

$$a \in {\wp^n}/{\wp^k} \quad \text{ und } \quad a \notin {\wp^{n+1}}/{\wp^k}$$

das heißt $\wp^{n+1} \subsetneq \mathfrak{b} := (a, \wp^{n+1}) \subseteq \wp^n$. Mit dem zweiten Teil von Bemerkung 5.22 gibt es aber kein Ideal das echt zwischen $\wp^{n+1}$ und $\wp^n$ liegt, also muss $\mathfrak{b} = \wp^n$ gelten. Damit erhalten wir

$${\wp^n}/{\wp^k} \;=\; (a)$$

Da alle Ideale in $\mathcal{O}_K/\wp^k$ von dieser Form oder Produkte von Idealen dieser Form sind, folgt die Behauptung. $\diamond$

Sei nun $\wp \in \mathrm{Spec}(\mathcal{O}_K)\backslash\{(0)\}$. Wir müssen zeigen, dass

$$\sharp\left(\mathcal{O}_K/\wp^k\right) \;=\; \sharp\left(\mathcal{O}_K/\wp\right)^k$$

gilt. Dies haben wir aber bereits in Folgerung 5.25 für einen allgemeineren Fall gezeigt. $\square$

Folgerung 5.27 *Die absolute Norm lässt sich zu einem Gruppenhomomorphismus*

$$\begin{array}{rccc} \mathbb{N}: & I(K) & \to & \mathbb{Q}^*_{>0} \\ & \displaystyle\prod_{\wp\in\mathrm{Spm}(R)} \wp^{v_\wp} & \mapsto & \displaystyle\prod_{\wp\in\mathrm{Spm}(R)} \big(\mathbb{N}(\wp)\big)^{v_\wp} \end{array}$$

Wobei mit $\mathbb{Q}^*$ die multiplikative Gruppe in $\mathbb{Q}$ bezeichnet ist. $\square$

6 Die Idealklassengruppe und die Klassenzahl

Definition 6.1 *(Cokern)*
Seien G_1, G_2 abelsche Gruppe und $\phi : G_1 \to G_2$ ein Gruppenhomomorphismus, dann ist, wegen der Kommutativität, $\phi(G_1)$ nicht nur eine Untergruppe von G_2 sondern sogar ein Normalteiler. Wir definieren

$$\mathrm{Coker}(\phi) \;:=\; G_2/\phi(G_1)$$

Definition und Satz 6.2 *(Idealklassengruppe/ Klassenzahl)*
Sei R ein Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(R)$. Die Abbildung

$$\begin{array}{rcl} \varphi : K^* & \to & I(K) \\ \alpha & \mapsto & \alpha R \end{array}$$

ist ein Gruppenhomomorphismus mit $\mathrm{Ker}(\varphi) = R^\times$. Wir definieren die Idealklassengruppe von K als

$$\mathcal{C}\ell(K) \;:=\; \mathrm{Coker}(\varphi)$$

Weiter setzen wir die Klassenzahl als

$$h_K \;:=\; \sharp\mathcal{C}\ell(K)$$

Beweis. Mit Satz 5.20 wissen wir bereits, dass $I(K)$ eine Gruppe mit neutralem Element $(1) = R$ ist. Weiter gelten

- $(\alpha)\cdot(\beta) \;=\; (\alpha\beta)$ in $I(K)$ für $\alpha, \beta \in K^*$
- Nach Satz 5.20 sind Inverse von der Form

$$(\alpha)^{-1} \;:=\; \big\{x \in K \big| x\cdot(\alpha) \subseteq R\big\} \;=\; \alpha^{-1}\cdot\big\{x\in K\big|x\cdot R\subseteq R\big\} \;=\; \alpha^{-1}R$$

- Genau dann ist $\alpha R \;=\; R$, wenn $\alpha \in R^\times$ ist. $\square$

Bemerkung 6.3 *Wir können die Klassengruppe $\mathcal{C}\ell(K)$ von einem Zahlkörper K auch auf eine alternative Weise einführen: Betrachte die Äquivalenzrelation*

$$\mathfrak{a} \sim \mathfrak{b} \;:\Leftrightarrow\; \exists \alpha \in K^* : \; \mathfrak{a} = \alpha\,\mathfrak{b}$$

für $\mathfrak{a}, \mathfrak{b} \in I(K)$. Dann ist

$$\mathcal{C}\ell(K) \;=\; {}^{I(K)}\!/_{\sim}$$

und insbesondere gibt es für alle $\mathfrak{a} \in I(K)$ ein $\mathfrak{b} \in \mathcal{O}_K$ mit $\mathfrak{b} \in [\mathfrak{a}]_{\mathcal{C}\ell(K)}$.

Bemerkung 6.4 *In der Situation von Definition 6.2 gilt: Genau dann ist $\mathcal{C}\ell(K) = \{1\}$, wenn R ein Hauptidealring ist.*

Beweis. Jedes $\alpha \in R \backslash R^\times$ wird mit der Abbildung

$$\varphi : K^* \;\to\; I(K)$$

auf das Hauptideal $(\alpha) \lhd R$ geschickt. Es gilt: Die Klassengruppe von K ist genau dann einelementig, wenn die zugrundeliegende Abbildung φ surjektiv ist. Dies ist genau dann der Fall, wenn es für alle $\mathfrak{a} \in I(K)$ ein $\alpha \in K^*$ mit $\alpha R = \mathfrak{a}$ gibt. □

Unser nächstes Ziel ist es zu zeigen, dass die Klassengruppe $\mathcal{C}\ell(K)$ für Zahlkörper $K/\,\mathbb{Q}$ immer eine endliche Gruppe ist, also $h_K < \infty$ gilt.

Lemma 6.5 *Sei K ein Zahlkörper und $\alpha \in \mathcal{O}_K \setminus \{0\}$. Dann gilt*

$$\mathbb{N}\big((\alpha)\big) \;=\; \big|\, N_{\mathbb{Q}}^K(\alpha)\,\big|$$

Beweis. Zur besseren Unterscheidung bezeichne $\mathfrak{a} := (\alpha)$ das Hauptideal von α. Wir wissen nach Lemma 4.19

$$d(\mathfrak{a}) \;=\; d(\alpha\,\mathcal{O}_K) \;=\; (\mathcal{O}_K : \alpha\,\mathcal{O}_K)^2 \cdot d(\mathcal{O}_K) \;=\; \mathbb{N}(\mathfrak{a}) \cdot D_K \tag{6.1}$$

Weiter sei $\{w_1, \ldots, w_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul, dann ist

$$\mathfrak{a} \;=\; \alpha\,\mathcal{O}_K \;=\; \mathbb{Z}\,\alpha w_1 \oplus \ldots \oplus \mathbb{Z}\,\alpha w_n$$

Seien weiter $\sigma_1, \ldots, \sigma_n$ die $\mathbb{Q}$-Einbettungen von K in $\mathbb{C}$, dann erhalten wir etwas expliziter

$$\begin{aligned} d(\mathfrak{a}) \;=\; d(\alpha\,\mathcal{O}_K) \;&=\; \det\Big(\big[\sigma_j(\alpha w_i)\big]_{1\le i,j\le n}\Big)^2 \\ &=\; \det\left[\begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix} \cdot \big(\sigma_j(w_i)\big)_{1\le i,j\le n}\right]^2 \\ &=\; \big(\sigma_1(\alpha) \cdot \ldots \cdot \sigma_n(\alpha)\big)^2 \cdot D_K \;=\; \big|\, N_{\mathbb{Q}}^K(\alpha)\,\big| \cdot D_K \end{aligned} \tag{6.2}$$

Da $D_K \neq 0$ gilt, folgt die Behauptung aus den Gleichungen (6.1) und (6.2). □

Satz 6.6 *Sei K ein Zahlkörper. Es gibt ein $\lambda \in \mathbb{R}_+$ so dass für alle ganzen Ideale $\mathfrak{a} \lhd \mathcal{O}_K$ die nicht das Nullideal sind ein ganzes Element $\alpha \in \mathcal{O}_K \setminus \{0\}$ so existiert, dass*

$$\left| N_{\mathbb{Q}}^K(\alpha) \right| \ \leq \ \lambda \cdot \mathbb{N}(\mathfrak{a})$$

gilt.

Anmerkung Es ist wichtig zu sehen, dass λ unabhängig von $\mathfrak{a}$ ist!

Beweis. Seien $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ die n Einbettungen von K in $\mathbb{C}$ und sei $\{w_1, \ldots, w_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$. Setze

$$\lambda \ := \ \prod_{i=1}^{n} \left(\sum_{j=1}^{n} \left| \, \sigma_i(w_j) \, \right| \right)$$

dann ist $\lambda \in \mathbb{R}_+$. Sei nun $\alpha \in \mathcal{O}_K$ und $m \in \mathbb{N}$ eine natürliche Zahl mit

$$m^n \ \leq \ \mathbb{N}(\mathfrak{a}) \ \leq \ m^{n+1} \quad \Leftrightarrow \quad m = \lfloor \sqrt[n]{\mathbb{N}(\mathfrak{a})} \rfloor$$

wobei $\lfloor x \rfloor$ den ganzzahligen Anteil von x bezeichne. Definiere weiter

$$S \ := \ \left\{ \sum_{j=1}^{m} m_j w_j \, \middle| \, 0 \leq m_j \leq m \right\}$$

dann hat S genau $(m+1)^n$ Elemente. Wegen $\sharp S \ > \ \sharp \left({}^{\mathcal{O}_K}\!/_{\mathfrak{a}} \right) \ = \ \mathbb{N}(\mathfrak{a})$ ist die Abbildung

$$S \ni s \ \mapsto \ s + \mathfrak{a} \in {}^{\mathcal{O}_K}\!/_{\mathfrak{a}}$$

nicht injektiv. Damit finden wir dann ein

$$\alpha \ = \ \sum_{j=1}^{n} m_j w_i \qquad \text{mit } |m_j| \leq m \text{ für alle } j = 1, \ldots, n$$

denn aus $x + \mathfrak{a} = y + \mathfrak{a}$ folgt $x - y \in \mathfrak{a}$. Insgesamt gilt die folgende Abschätzung:

$$\begin{aligned} \left| N_{\mathbb{Q}}^K(\alpha) \right| \ &= \ \left| \prod_{i=1}^{n} \sigma_i(\alpha) \right| \ \overset{\Delta-UGL}{\leq} \ \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |m_j| \cdot \left| \sigma_i(w_j) \right| \right) \\ &\leq \ m^n \cdot \lambda \ \leq \ \mathbb{N}(\mathfrak{a}) \cdot \lambda \end{aligned}$$

□

Folgerung 6.7 *Sei K ein Zahlkörper, dann gilt: Jede Nebenklasse $C \in \mathcal{C}\ell(K)$ enthält ein ganzes Ideal $\mathfrak{a} \lhd \mathcal{O}_K$ mit $\mathbb{N}(\mathfrak{a}) \leq \lambda$ für $\lambda \in \mathbb{R}_+$ wie im vorherigen Satz 6.6.*

Beweis. Sei $C^{-1} \in \mathcal{C}\ell(K)$ eine Nebenklasse und $\mathfrak{b} \in \mathcal{O}_K$ ein ganzes Ideal mit $\overline{\mathfrak{b}} \in C^{-1}$ (dies kann für $\mathfrak{b} \in I(K)$ nach der Charakterisierung in Lemma 5.19 durch Multiplikation mit geeignetem $\beta \in \mathcal{O}_K$ immer erreicht werden). Dann ist $C^{-1} = \overline{\mathfrak{b}}$ das Bild von $\mathfrak{b}$ in $\mathcal{C}\ell(K)$. Sei weiter $\alpha \in \mathfrak{b}$ mit $\alpha \neq 0$ und

$$\left| N_{\mathbb{Q}}^K(\alpha) \right| \ \leq \ \lambda \cdot \mathbb{N}(\mathfrak{b})$$

Ein solches α finden wir nach dem Vorangegangenen Satz. Es gibt ein ganzes Ideal $\alpha \lhd \mathcal{O}_K$ mit $(\alpha) = \mathfrak{a} \cdot \mathfrak{b}$ also folgt

$$\big|\, N_{\mathbb{Q}}^K(\alpha) \,\big| \;=\; \mathbb{N}(\mathfrak{a}) \cdot \mathbb{N}(\mathfrak{b})$$

und wegen $\mathbb{N}(\mathfrak{b}) \neq 0$ dürfen wir dann schließen, dass

$$\mathbb{N}(\mathfrak{a}) \;=\; \frac{\big|\, N_{\mathbb{Q}}^K(\alpha) \,\big|}{\mathbb{N}(\mathfrak{b})} \;\leq\; \lambda$$

gilt. und aus $\mathfrak{a} \cdot \mathfrak{b} = (\alpha)$ folgt $\mathfrak{a} \cdot C^{-1} = \overline{(1)}$ in $\mathcal{C}\ell(K)$, also $\overline{\mathfrak{a}} \in C$. □

Folgerung 6.8 *Sei K ein Zahlkörper, dann ist $\mathcal{C}\ell(K)$ eine endliche Gruppe.*

Beweis. Die Projektion $\pi : I(K) \twoheadrightarrow \mathcal{C}\ell(K)$ ist in natürlicher Weise surjektiv und für alle gebrochenen Ieale $\mathfrak{a} \in I(K)$ finden wir nach Lemma 5.23 eine Zerlegung in von paarweise verschiedene nicht-null Primideale $\wp_1, \ldots, \wp_r \in \mathrm{Spm}(\mathcal{O}_K)$ von der Form

$$\mathfrak{a} \;=\; \wp_1^{v_1} \cdot \ldots \cdot \wp_r^{v_r} \;\in I(K)$$

Damit erhalten wir aus Satz 5.26 eine Zerlegung der absoluten Norm von $\mathfrak{a}$

$$\mathbb{N}(\mathfrak{a}) \;=\; \big(\mathbb{N}(\wp_1)\big)^{v_1} \cdot \ldots \cdot \big(\mathbb{N}(\wp_r)\big)^{v_r}$$

also genügt es nach der vorangegangenen Folgerung zu zeigen, dass es nur endlich viele Primideale $\wp \lhd \mathcal{O}_K$ gibt, die die Bedingung $\mathbb{N}(\wp) \leq \lambda$, mit $\lambda \in \mathbb{R}_+$ wie in Satz 6.6, erfüllen.
Nach Lemma 5.17 gibt es für jedes $\wp \in \mathrm{Spm}(\mathcal{O}_K)$ eine Primzahl p und eine natürliche Zahl $f \in \mathbb{N}$, so dass $\mathbb{N}(\wp) = p^f$ ist, aber die Menge

$$\big\{\, p^f \leq \lambda \,\big|\, p \text{ ist prim und } f \in \mathbb{N} \,\big\}$$

ist endlich. □

Beispiel 15 *Sei $K = \mathbb{Q}(\sqrt{2})$, dann ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ und $\{1, \sqrt{2}\}$ ist eine Ganzheitsbasis von $\mathcal{O}_K$. Mit $\lambda := (1 + \sqrt{2})^2$ gilt $5 \leq \lambda < 6$. Für alle $C \in \mathcal{C}\ell(K)$ gibt es ein $\mathfrak{a} \in \mathcal{O}_K$ mit $\mathbb{N}(\mathfrak{a}) \leq 5$ und $C = \overline{\mathfrak{a}} = [\mathfrak{a}]_{\mathcal{C}\ell(K)}$. Die absolute Norm von $\mathfrak{a}$ kann also nur die Werte $2,\ 3,\ 4$ und 5 annehen. Für jedes $\wp \in \mathrm{Spm}(\mathcal{O}_K)$ mit $\wp$ teilt $\mathfrak{a}$ liegen $2,\ 3$ oder 5 in $\wp$. Es gilt $2\,\mathcal{O}_K = (\sqrt{2}\,\mathcal{O}_K)^2$ also ist das von 2 in $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ erzeugte Ideal nicht prim, aber die ideale $3\,\mathcal{O}_K$ und $5\,\mathcal{O}_K$ sind prim, denn*

$$\mathbb{Z}[\sqrt{2}]\big/_{5\,\mathbb{Z}[\sqrt{2}]} \;\cong\; \mathbb{F}_5[X]\big/_{(X^2-2)} \quad \text{und} \quad \mathbb{Z}[\sqrt{2}]\big/_{3\,\mathbb{Z}[\sqrt{2}]} \;\cong\; \mathbb{F}_3[X]\big/_{(X^2-2)}$$

Also folgt aus $2\,\mathcal{O}_K$, $3\,\mathcal{O}_K$ oder $5\,\mathcal{O}_K$ teilt $\wp$, dass $\wp$ ein Hauptideal ist, also gilt $\overline{\wp} = [\wp]_{\mathcal{C}\ell(K)} = \overline{(1)}$ und damit folgt $\mathcal{C}\ell(K) = \{1\}$.
In diesem Beispiel konnten wir eine wichtige Eigenschaft von $\mathbb{Z}[\sqrt{2}]$ aus der Klassengruppe $\mathcal{C}\ell\left(\mathbb{Q}(\sqrt{2})\right)$ ablesen, nämlich das $\mathbb{Z}[\sqrt{2}]$ ein Hauptidealring ist.

7 Minkowski Theorie

Im Beispiel am Ende des letzten Abschnittes haben wir gesehen, dass uns die Klassengruppe eines Zahlkörpers K etwas über die Struktur des Ganzheitsrings $\mathcal{O}_K$ sagen kann. Leider ist das in Satz 6.6 konstruierte $\lambda \in \mathbb{R}_+$ sehr groß. In diesem Abschnitt wollen wir das kleinste λ konstruieren, dass die Eigenschaft für alle ganzen Ideale $\mathfrak{a} \lhd \mathcal{O}_K$, die nicht das Nullideal sind, gibt es ein ganzes Element $\alpha \in \mathcal{O}_K \setminus \{0\}$ so dass

$$\left| N_{\mathbb{Q}}^K(\alpha) \right| \ \leq \ \lambda \cdot \mathbb{N}(\mathfrak{a})$$

gilt, erfüllt. Hierzu benötigen wir die neue Konstruktion eines Gitters und einen Begriff vom Maß einer Menge. Letzteren werden wir hier nur motivieren und verweisen auf geeignete Lektüre (zum Beispiel ein Analysis III Skript).

Definition 7.1 *(Gitter)*
Ein Gitter in einem endlich dimensionalem $\mathbb{R}$-Vektorraum V ist eine additive Untergruppe $\Gamma \subset V$ mit den Eigenschaften

G1 *$\Gamma \subset V$ ist diskret.*

G2 *V/Γ ist kompakt.*

Anmerkung Wir sagen zu dieser Menge zwar „Gitter“ aber betrachten nur die „Eckpunkte“. Manchmal können wir nicht einmal von „Eckpunkten“ reden.

Beispiel 16 *Sei $V = \mathbb{R}$ und $\Gamma = \mathbb{Z}$, dann sind die Ganzzahligen Elemente von $\mathbb{R}$ die Gitterpunkte und es gilt*

$$V/\Gamma \ = \ \mathbb{R}/\mathbb{Z} \ \cong \ \partial K_1(0) \ =: \ S^1$$

mit S^1 bezeichne den Einheitskreis in $\mathbb{R}^2$. Dies zu sehen betrachte den Isomorphismus

$$\begin{array}{rccc} \phi : & \mathbb{R}/\mathbb{Z} & \to & S^1 \\ & \alpha & \mapsto & e^{2\pi i \alpha} \end{array}$$

Beispiel 17 *Sei $V = \mathbb{C}$ und $\Gamma = \mathbb{Z}[i]$, dann erhalten wir wieder die ganzzahligen Elemente von $\mathbb{C}$ als Gitterpunkte (diesmal können wir wegen der Dimension 2 tatsächlich von Knoten- oder Eckpunkten sprechen) die Ganzzahligen Elemente von $\mathbb{C}$. Analog zum Vorangegangenen Beispiel gilt*

$$V/\Gamma \ = \ \mathbb{C}/\mathbb{Z}[i] \ \cong \ S^1 \times S^1$$

Lemma 7.2 *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $\Gamma \subseteq V$ eine Untergruppe bezüglich $+$. Dann ist Γ genau dann ein Gitter, wenn Γ von der Form $\Gamma = \mathbb{Z}\, v_1 + \ldots + \mathbb{Z}\, v_n$ für eine $\mathbb{R}$-Basis $\{v_1, \ldots, v_n\}$ von V ist.*

Beweis. Sei $V_0 \subseteq V$ ein Untervektorraum, der von Γ aufgespannt wird. Falls $V_0 \neq V$ gilt, wähle einen komplimentären Vektorraum W mit $V = V_0 \oplus W$. Dann gilt

$$V/\Gamma \ \cong \ V_0/\Gamma \oplus W$$

weiter gibt es ein $m \in \mathbb{N}$ mit $0 < m < n$ und $W \cong \mathbb{R}^m$ also ist V/Γ nicht kompakt. Damit enthält Γ eine Basis $\{v_1, \ldots, v_n\}$ von V. Setze

$$\Gamma_0 \ := \ \mathbb{Z}\, v_1 + \ldots + \mathbb{Z}\, v_n$$

dann ist Γ_0 ein Gitter, denn Γ_0 ist diskret und

$$V/\Gamma_0 \;\cong\; RR/\mathbb{Z} \times \cdots \times \mathbb{R}/\mathbb{Z}$$

ist als Produkt kompakter Mengen kompakt. Da $\Gamma \subseteq V$ als diskrete Menge abgeschlossen ist, folgt

$$\Gamma/\Gamma_0 \;\subseteq\; V/\Gamma_0$$

ist ebenfalls wieder diskret und abgeschlossen, also kompakt. Diskrete kompakte Mengen sind endlich. Sei also

$$k \;:=\; \sharp\Big(\Gamma/\Gamma_0\Big)$$

dann gilt

$$\Gamma_0 \;\leq\; \Gamma \;\leq\; \frac{1}{k}\Gamma_0$$

und mit dem Elementarteilersatz folgt die Existenz einer Basis $\{w_1, \ldots, w_n\}$ von V mit

$$\Gamma \;=\; \mathbb{Z}\, w_1 + \ldots + \mathbb{Z}\, w_n$$

□

Definition 7.3 *(Euklidischer Raum)*
Das Tupel $(V, <\cdot,\cdot>)$ heißt n-dimensionaler euklidischer Raum, wenn V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $<\cdot,\cdot>$ eine nicht ausgeartete symmetrische und positiv definite Bilinearform auf V ist.

Konstruktion 7.4 *(Volumen / Maß)*
Sei $(V, <\cdot,\cdot>)$ ein n-dimensionaler euklidischer Raum, dann gibt es bezüglich $<\cdot,\cdot>$ eine Orthonormalbasis $\{e_1, \ldots, e_n\}$ von V, also eine Basis mit $<e_i, e_j> = \delta_{i,j} \in \{0, 1\}$.
Wir betrachten bezüglich dieser Basis einen Kubus mit Kantenlänge 1

$$Q[0,1] \;:=\; \Big\{ \sum_{i=1}^{n} x_i e_i \;\Big|\; 0 \leq x_i \leq 1 \Big\}$$

Wir setzen das Volumen dieses Einheitskubus als $vol(Q[0,1]) := 1$ und fordern das Volumen möge die folgenden Eigenschaften erfüllen

i) *Für $\lambda \in \mathbb{R}$ gelte*

$$vol\big(\lambda \cdot Q[0,1]\big) \;=\; vol\big(Q[0,|\lambda|]\big) \;=\; |\lambda|^n$$

ii) *Seien für $i \in I$ Mengen $X_i \subseteq V$ mit $X_j \cap X_j = \varnothing$ für $i \neq j$ gegeben, dann gelte*

$$\sum_{i \in I} vol(X_i) \;=\; vol\Big(\bigcup_{i \in I} X_i\Big)$$

Bemerkung 7.5 *Sei $(V, <\cdot,\cdot>)$ ein n-dimensionaler euklidischer Raum, und vol ein Volumen nach Konstruktion 7.4. Seien weiter $v_1, \ldots, v_n \in V$ dann Setze*

$$X \;:=\; \Big\{ \sum_{i=1}^{n} x_i v_i \;\Big|\; 0 \leq x_i \leq 1 \Big\}$$

Für das Volumen von X gilt

$$vol(X) \;=\; \big|\det(A)\big| \qquad \text{mit } v_i =: Ae_i$$

Beweis. Dieses Faktum übernehmen wir unbewiesen aus der Maßtheorie.

Auch wenn wir die Bemerkung nicht beweisen, wollen wir zumindest mit ein paar Beispielen motivieren, dass wir mit dem konstruierten Maß und der Bemerkung die schon bekannten Maße wiedererlangen. Betrachte dazu die folgenden Beispiele

Ab jetzt bezeichne vol stets ein Volumen nach Konstruktion 7.4.

Beispiel 18 *Sei $V = \mathbb{R}$ mit Bilinearform $< x, y >:= xy$ für $x, y \in \mathbb{R}$, dann ist $(V, < \cdot, \cdot >)$ ein eindimensionaler euklidischer Raum und das von uns Konstruierte Volumen entspricht der Länge der Strecken, denn für die Gerade zwischen 0 und $v \in \mathbb{R}$*

$$X_v \ := \ \{\, xv \,|\, 0 \leq x \leq 1 \,\}$$

gilt nach Bemerkung 7.5 $vol(x) = |v|$.

Beispiel 19 *Sei wieder $V = \mathbb{R}$ aber diesmal mit der Bilinearform $< x, y >:= 2xy$ für $x, y \in \mathbb{R}$. Auch in diesem Fall ist $(V, < \cdot, \cdot >)$ euklidisch. Weiter ist $\{\frac{1}{\sqrt{2}}\}$ eine Orthonormalbasis von V bezüglich der gegebenen Bilinearform. Für $a \in \mathbb{R}$ setze die Gerade X_a von 0 bis a wie eben, dann gilt*

$$X \ := \ X_a \cap X_b$$

ist die Gerade von a bis b und wir erhalten das Volumen

$$vol(X) \ = \ \sqrt{2}|b - a|$$

Beispiel 20 *Sei diesmal $V = \mathbb{R}^2$ mit dem Standartskalarprodukt $< (x_1, x_2), (y_1, y_2) >:= x_1y_1 + x_2y_2$. Dann ist $\left\{ \binom{1}{0}, \binom{0}{1} \right\}$ eine Orthonormalbasis bezüglich $< \cdot, \cdot >$ Seien nun $v_1 := \binom{a_{11}}{a_{21}}$ und $v_2 := \binom{a_{12}}{a_{22}}$, dann ist*

$$X \ = \ \{\, x_1v_1 + x_2v_2 \,|\, 0 \leq x_1, x_2 \leq 1 \,\}$$

Das Parallelogramm, dass von v_1, v_2 in $\mathbb{R}^2$ aufgespannt wird. Nach Bemerkung 7.5 ist das Volumen des Parallelogramms wie erwartet

$$vol(X) \ = \ \left| \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right| \ = \ |\, a_{11}a_{22} - a_{12}a_{21} \,|$$

Definition 7.6 *(Grundmasche)*
Sei $(V, < \cdot, \cdot >)$ ein n-dimensionaler euklidischer Raum und $\Gamma \subseteq V$ ein Gitter der Form

$$\Gamma \ = \ \mathbb{Z}\, v_1 + \ldots + \mathbb{Z}\, v_n$$

für eine $\mathbb{R}$-Basis $\{v_1, \ldots, v_n\}$ von V. Wir definieren die Grundmasche von Γ als

$$\mathcal{F} \ := \ \left\{ \sum_{i=1}^{n} x_i v_i \,\middle|\, 0 \leq x \leq 1 \right\} \ \subset \ V$$

Weiter setzen wir

$$vol\left({}^{V}\!/_{\Gamma} \right) \ := \ vol(\mathcal{F})$$

Lemma 7.7 *Sei $(V, < \cdot, \cdot >)$ ein n-dimensionaler euklidischer Raum und $\Gamma \subseteq V$ ein Gitter. Sei weiter $\{v_1, \ldots, v_n\}$ eine Basis von V. Dann gilt*

$$vol(\mathcal{F}) \;=\; vol\left(V\!/\Gamma\right) \;=\; \sqrt{\det\left(< v_i, v_j >_{1\leq i,j\leq n} \right)}$$

und das Volumen ist unabhängig von der Basiswahl.

Beweis. Sei $A \in \mathrm{Gl}_n(\mathbb{R})$ mit $v_i =: Ae_i$ wobei $\{e_1, \ldots, e_n\}$ eine Orthonormalbasis von V bezüglich $< \cdot, \cdot >$ ist. Ein Solches A finden wir nach den Erkenntnissen der linearen Algebra immer. Nach Bemerkung 7.5 gilt

$$vol(\mathcal{F}) \;=\; vol\left(V\!/\Gamma\right) \;=\; \left|\, \det(A) \,\right|$$

Nach der Wahl von A gilt

$$A^T A \;=\; \left(< v_i, v_j >_{1\leq i,j\leq n} \right)$$

und wir wissen bereits, dass

$$\det(A)^2 \;=\; \det\left(< v_i, v_j >_{1\leq i,j\leq n} \right)$$

unabhängig von der Basis ist. □

Definition 7.8 *(Messbar)*
Sei $(V, < \cdot, \cdot >)$ ein n-dimensionaler euklidischer Raum. Eine Menge $X \subseteq V$ heißt messbar, wenn $vol(X)$ definiert ist.

Lemma 7.9 *(Lemma von Blichfeld)*
Sei $(V, < \cdot, \cdot >)$ ein n-dimensionaler euklidischer Raum. Seien weiter $X \subset V$ messbar und $\Gamma \subseteq V$ ein Gitter mit $vol(X) > vol(\mathcal{F})$. Dann gibt es $u, v \in X$ mit $u \neq v$ und $u - v \in \Gamma$.

Beweis. Sei $\{v_1, \ldots, v_n\}$ eine Basis von V, so dass Γ von der Form $\Gamma = \mathbb{Z}\, v_1 + \ldots + \mathbb{Z}\, v_n$ ist. Setze

$$\mathcal{F}' \;=\; \Big\{ \sum_{i=1}^{n} x_i v_i \,\Big|\, 0 \leq x_i \leq 1 \Big\}$$

Dann ist

$$V \;=\; \dot{\bigcup}_{\gamma\in\Gamma} \gamma + \mathcal{F}' \;=\; \coprod_{\gamma\in\Gamma} \gamma + \mathcal{F}'$$

Damit erhalten wir auf natürliche Weise die Gleichung

$$\begin{aligned} X \;&=\; X \cap V \;=\; X \cap \coprod_{\gamma\in\Gamma} \gamma + \mathcal{F}' \;=\; \coprod_{\gamma\in\Gamma} (\gamma + \mathcal{F}') \cap X \\ &=\; \coprod_{\gamma\in\Gamma} \gamma + (X - \gamma) \cap \mathcal{F}' \end{aligned}$$

Wären nun alle Mengen der Form $(X - \gamma) \cap \mathcal{F}'$ disjunkt, so folgte nach Konstruktion 7.4 Forderung (ii) die Ungleichung

$$vol(X) \;=\; \sum_{\gamma\in\Gamma} vol\big((X - \gamma) \cap \mathcal{F}'\big) \;\leq\; vol(\mathcal{F}')$$

Da sich $\mathcal{F}$ und $\mathcal{F}'$ höchstens um eine Basis unterscheiden folgte mit dem vorangegangenen Lemma

$$vol(X) \;\leq\; vol(\mathcal{F}') \;=\; vol(\mathcal{F})$$

was ein Widerspruch zur Voraussetzung ist. Also sind nicht alle Mengen der Form $(X-\gamma)\cap\mathcal{F}'$ disjunkt und also gibt es $\gamma_1,\gamma_2\in\Gamma$ mit $\gamma_1\neq\gamma_2$ so dass es ein

$$a \;\in\; (X-\gamma_1)\cap(X-\gamma_2)\cap\mathcal{F}'$$

gibt. Setze nun $u := a+\gamma_1$ und $v := a+\gamma_2$, dann erfüllen $u,v\in X$ die Behauptung. □

Definition 7.10 *(Konvex)*
V ein $\mathbb{R}$-Vektorraum. Eine Teilmenge $X\subseteq V$ heißt konvex, wenn zu je zwei Punkten aus X auch die gesamte Verbindungsstrecke in X liegt, das heißt wenn für alle $x,y\in X$ gilt

$$\left\{\, tx+(1-t)y \,\middle|\, t\in[0,1]\,\right\} \;\subseteq\; X$$

Definition 7.11 *(Zentralsymmetrisch)*
V ein $\mathbb{R}$-Vektorraum. Eine Teilmenge $X\subseteq V$ heißt zentralsymmetrisch, wenn für jedes $x\in X$ auch $-x$ in X liegt.

Satz 7.12 *(Satz von Minkowski / Gitterpunktsatz)*
Sei $(V,<\cdot,\cdot>)$ ein n-dimensionaler euklidischer Raum. Seien $X\subseteq V$ eine konvexe zentralsymmetrische Teilmenge und $\Gamma\subseteq V$ ein Gitter mit

$$vol(X) \;>\; 2^n\cdot vol(\mathcal{F})$$

Dann enthält X einen Gitterpunkt $\gamma\in\Gamma$.
Ist X sogar kompakt in V, dann genügt die Voraussetzung

$$vol(X) \;\geq\; 2^n\cdot vol(\mathcal{F})$$

Beweis. Setze

$$Y \;:=\; \frac{1}{2}X \;=\; \left\{\, \frac{1}{2}x \,\middle|\, x\in X\,\right\}$$

dann gilt nach Voraussetzung

$$vol(Y) \;=\; \frac{1}{2^n}\cdot vol(X) \;>\; vol(\mathcal{F})$$

Nach dem Lemma von Blichfeld gibt es $u,v\in Y$ mit $u\neq v$ und $u-v\in\Gamma$. Nach Konstruktion sind $2u,2v\in X$ und wegen der zentralsymmetrie von X gilt dann auch $-2v\in X$. Für $t=\frac{1}{2}$ folgt aus der Konvexheit von X

$$\frac{1}{2}(2u)+\frac{1}{2}(-2v) \;=\; u-v \;\in X$$

Sei nun X kompakt und die Voraussetzung entsprechend abgeschwächt. Für jede natürliche Zahl $m\in\mathbb{N}$ setze $\left(1+\frac{1}{m}\right)X =: X_m$, dann gilt

$$vol(X_m) \;=\; \left(1+\frac{1}{m}\right)^n\cdot vol(X) \;>\; 2^n\cdot vol(\mathcal{F})$$

Da nun wieder echte Ungleichungen gelten, gibt es für alle $m \in \mathbb{N}$ ein $\gamma_m \in X_m \cap (\Gamma\backslash\{0\})$ nach dem bereits bewiesenen Teil. Für alle $m \in \mathbb{N}$ gilt weiter $X_m \subseteq 2X$ und $2X$ ist nach Voraussetzung kompakt. Damit ist

$$2X \cap (\Gamma\backslash\{0\}) \;=:\; W$$

als Schnitt einer diskreten und einer kompakten Menge endlich. Wir haben aber bereits gesehen, dass die Folge $(\gamma_m)_{m\in\mathbb{N}}$ vollständig in W liegt, also gibt es eine weitere Folge $(m_i)_{i\in\mathbb{N}}$ so dass $\gamma_{m_i} = \gamma_{m_j} := \gamma \in \Gamma\backslash\{0\}$. Dann ist aber

$$\gamma \;\in\; \bigcap_{i\in\mathbb{N}} \Big(1 + \frac{1}{m_i}\Big) X \;=\; X$$

□

Aus dem Einschub über das Tensorprodukt wissen wir, dass wir zu jedem Zahlkörper $K/\mathbb{Q}$ auf natürliche Weise einen $\mathbb{R}$-Vektorraum $K \otimes_{\mathbb{Q}} \mathbb{R} =: K_{\mathbb{R}}$ konstruieren können. Wir erhalten ebenfalls sofort eine Inklusion

$$\begin{aligned} j : K &\hookrightarrow K_{\mathbb{R}} \\ \lambda &\mapsto \lambda \otimes 1 \end{aligned}$$

Als nächsten Schritt wollen wir eine Bilinearform $< \cdot, \cdot >$ auf $K_{\mathbb{R}}$ konstruieren, so dass $(K_{\mathbb{R}}, < \cdot, \cdot >)$ euklidisch ist. Anschließend wollen wir zeigen, dass für $\mathfrak{a} \in \mathcal{O}_K$ die Untergruppe $j(\mathfrak{a}) \subset K_{\mathbb{R}}$ ein Gitter mit

$$vol\left(K_{\mathbb{R}}/j(\mathfrak{a})\right) \;=\; \sqrt{|D_K|} \cdot \mathbb{N}(\mathfrak{a})$$

ist. Anschließend wollen wir dann zeigen, dass uns die Minkowsky-Theorie ein $C_K \in \mathbb{R}_+$ liefert, so dass für alle $[\mathfrak{a}] \in \mathcal{C}\ell(K)$ ein $\alpha \in \mathfrak{a}\setminus\{0\}$ existiert mit

$$\left| N_{\mathbb{Q}}^K(\alpha) \right| \;\leq\; C_K \cdot \mathbb{N}(\mathfrak{a})$$

Definition und Bemerkung 7.13 *(Reelle und komplexe Homomorphismen)*
Sei K ein Zahlkörper. Wir führen die Notation $\Sigma := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ für die Menge der $\mathbb{Q}$-Homomorphismen von K nach $\mathbb{C}$ ein. Es gilt $\sharp\Sigma = [K : \mathbb{Q}]$. Betrachte nun die Galois-Gruppe von $\mathbb{C}\,/\,\mathbb{R}$

$$G \;:=\; \mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R}) \;=\; \{1, c\}$$

wobei 1 die Identität und c die komplexe Konjugation seien. Diese Gruppe operiert via

$$\begin{aligned} \omega : G \times \Sigma &\to \Sigma \\ (g, \sigma) &\mapsto g.\sigma := g(\sigma) := g \circ \sigma \end{aligned}$$

auf Σ. In Anlehnung an die Notation für komplexe Zahlen schreiben wir dann

$$c(\sigma) \;=:\; \overline{\sigma}$$

Weiter heißt $\sigma \in \Sigma$ genau dann reell, wenn $\sigma = \overline{\sigma}$ gilt. Ansonsten nennen wir σ komplex.
Aus der Galois-Theorie wissen wir, dass $\mathbb{C}^G = \mathbb{R}$ ist. damit gilt für $\sigma \in \Sigma$ reell: $\sigma(K) \subseteq \mathbb{R}$.

Generalvoraussetzung Bis zum Ende des Abschnittes setzen wir die folgenden Bezeichnungen fest:

- K ist ein Zahlkörper vom Grad $[K : \mathbb{Q}] = n$.
- $\Sigma := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.
- $c : \mathbb{C} \ni z \mapsto \overline{z} \in \mathbb{C}$ ist die komplexe Konjugation.
- $r := \sharp\{\, \sigma \in \Sigma \,|\, \overline{\sigma} = \sigma \,\}$ die Anzahl der reellen Homomorphismen in Σ.
- $s := \sharp\{\, (\sigma, \overline{\sigma}) \,|\, \sigma \in \Sigma \wedge \overline{\sigma} \neq \sigma \,\}$ die Anzahl der komplexen Homomorphismenpaare in Σ.

Anmerkung Für den Grad der Körpererweiterung von K über $\mathbb{Q}$ gilt:

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

Bemerkung 7.14 *Sei $K = \mathbb{Q}(\alpha)$ mit Minimalpolynom $f \in \mathbb{Q}[X]$ von α, dann sind*

$$r \;:=\; \sharp\{\, x \in \mathbb{R} \mid f(x) = 0\} \quad \text{und} \quad s \;:=\; \sharp\{\, z \in \mathbb{C} \setminus \mathbb{R} \mid f(z) = 0\}$$

Ist K ein Zahlkörper der konkreten Form $K = \mathbb{Q}(\sqrt{d})$ mit einem $d \in \mathbb{Q}$ quadratfrei, dann gelten

$$\begin{aligned} r = 2 \text{ und } s = 0 \qquad & \text{falls } d > 0 \\ r = 0 \text{ und } s = 1 \qquad & \text{falls } d > 0 \end{aligned}$$

Beweis. Der erste Teil folgt sofort aus Ergebnissen der Galois-Theorie. Ist $d > 0$ so zerfällt das Minimalpolynom $f(X) = X^2 - d$ über $\mathbb{R}$ in die Faktoren $X^2 - \sqrt{d}$ und $X^2 + \sqrt{d}$. Also hat f zwei reelle Nullstellen. Da $n = [K : \mathbb{Q}] = 2$ gilt, folgt der erste Fall. Ist nun $d < 0$ so ist das Minimalpolynom $f(X) = X^2 - d$ irreduzibel über $\mathbb{R}$. □

Mit den Begriffen aus Definition 7.13 und der Generalvoraussetzung können wir nun den Zielsatz dieses Abschnittest Formulieren:

Definition und Satz 7.15 *(Minkowski-Konstante/ Satz von Minkowski II)*
In jeder Idealklasse $C \in \mathcal{C}\ell(K)$ gibt es ein ganzes Ideal $\mathfrak{a} \lhd \mathcal{O}_K$ mit

$$\mathbb{N}(\mathfrak{a}) \;\leq\; C_K \cdot \sqrt{|D_K|}$$

wobei gilt

$$C_K \;:=\; \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s$$

Wir nennen $C_K \in \mathbb{R}_+$ die Minkowski-Konstante von K.

Anmerkung Die Stirlingsche-Formel besagt, dass es für alle $n \in \mathbb{N}$ ein $\theta \in \mathbb{R}$ mit $|\theta| \leq 1$ gibt, mit

$$\log(n!) \;=\; n \cdot \log(n) - n + \frac{\log(\pi)}{2} + \frac{\theta}{12n}$$

Damit erhalten wir die Formel

$$\frac{n!}{n^n} \;=\; \exp(-n) \cdot \exp\left(\frac{\log(\pi)}{2}\right) \cdot \exp\left(\frac{\theta}{12n}\right) \quad \overset{n\to\infty}{\longrightarrow} \quad 1$$

Beispiel 21 *Sei $K = \mathbb{Q}(\sqrt{-5})$. Mit dem Wissen der vorangegangenen Abschnitte erkennen wir, dass dann $D_K = -5$ und $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ sind. In Übungsaufgaben haben wir gesehen, dass es nicht immer leicht ist die Klassenzahl h_K zu berechnen. Wir wollen in diesem Beispiel zeigen, dass der Satz von Minkowski (II) auch hierfür hilfreich sein kann. Mit Bemerkung 7.14 gelten $r = 0$ und $s = 1$, denn -5 ist quadratfrei in $\mathbb{Q}$. Damit erhalten wir*

$$C_K \;=\; \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right)^1 \;=\; \frac{4}{\pi} \quad (???)$$

Insgesamt ist also

$$h_K \;\leq\; C_K \cdot \sqrt{|D_K|} \;=\; \frac{4}{\pi} \cdot \sqrt{5} \;<\; 3$$

Also muss $h_K \in \{1, 2\}$ gelten. Betrachte nun das von 2 in $\mathcal{O}_K$ erzeugte Ideal:

$$\mathcal{O}_K \big/ 2\,\mathcal{O}_K \;\cong\; \mathbb{F}_2[T] \big/ (T^2 + 5) \;=\; \mathbb{F}_2[T] \big/ (T+1)^2$$

Demnach ist $\wp = (2, 1 + \sqrt{-5})$ ein Primideal in $\mathcal{O}_K$ und damit ist $\mathcal{O}_K$ sicher kein Hauptidealring. Mit Bemerkung 6.4 kann dann h_K nicht 1 sein. Also folgt $h_K = 2$.

Damit wir den Satz 7.15 beweisen können müssen wir noch einige Schritte machen. Zuerst erinnern wir an die Konstruktion, mithilfe derer wir zum Zahlkörper K einen n-Dimensionalen $\mathbb{R}$-Vektorraum erhalten.

Bemerkung 7.16 *Setze $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$, dann ist $K_\mathbb{R}$ ein $\mathbb{R}$-Vektorraum der Dimension*

$$\dim_\mathbb{R}(K_\mathbb{R}) \;=\; \dim_\mathbb{Q}(K) \;=\; [K : \mathbb{Q}] \;=\; n$$

und der natürlichen Inklusion

$$\begin{aligned} j : K &\;\to\; K_\mathbb{R} \\ \lambda &\;\mapsto\; \lambda \otimes 1 \end{aligned}$$

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Q}$ Basis von K, dann ist

$$K \;=\; \underbrace{\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}}_{n\,-\,\text{mal}}$$

Damit folgt

$$K \otimes_\mathbb{Q} \mathbb{R} \;=\; \mathbb{Q} \otimes_\mathbb{Q} \mathbb{R} \oplus \ldots \oplus \mathbb{Q} \otimes_\mathbb{Q} \mathbb{R} \;\cong\; \mathbb{R} \otimes \ldots \otimes \mathbb{R}$$

und $\{j(\alpha_1), \ldots, j(\alpha_n)\}$ ist eine $\mathbb{R}$-Basis von $K_\mathbb{R}$. □

Auf K haben wir die Spurform

$$Tr_\mathbb{Q}^K : K \times K \;\to\; \mathbb{Q}$$

als symmetrische nicht-ausgeartete Bilinearform. Wir wollen diese nun zu einer Bilinearform auf $K_\mathbb{R}$ fortsetzen. Dazu betrachte die folgende

Konstruktion 7.17 *(Fortsetzung von Bilinearformen)*
Sei V ein endlich dimensionaler $\mathbb{Q}$-Vektorraum. Es gelten

(i) *Die Bilinearform*

$$< \cdot, \cdot >: V \times V \ \to \ \mathbb{Q}$$

ist genau dann symmetrisch und nicht-ausgeartetet, wenn

$$\begin{aligned} \varphi : V &\to V^* \\ v &\mapsto < \cdot, v > \end{aligned}$$

ein Isomorphismus von $\mathbb{Q}$-Vektorräumen ist. [Erinnerung: $V^* := \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$.]

(ii) *Im Anschluss an Satz 0.14 haben wir einige Eigenschaften des Tensorproduktes gezeigt. Insbesondere, dass es für R-Moduln A, B und C mit einem $\varphi \in \mathrm{Hom}_R(A, C)$ es einen Homomorphismus von R-Moduln*

$$\begin{aligned} \phi : A \otimes_R B &\to C \otimes_R B \\ a \otimes b &\mapsto \varphi(a) \otimes b \end{aligned}$$

gibt.

*Sei also $< \cdot, \cdot >$ eine symmetrische, nicht-ausgeartetete Bilinearform auf V, dann gibt es nach **(i)** einen Isomorphismus $\varphi : V \xrightarrow{\sim} V^*$. Mit **(ii)** ist dann auch*

$$\phi : V_{\mathbb{R}} := V \otimes_{\mathbb{Q}} \mathbb{R} \ \xrightarrow{\sim} V^* \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{Hom}_{\mathbb{R}}(V_{\mathbb{R}}, \mathbb{R}) = V_{\mathbb{R}}^*$$

*ein Ismorphismus. Dann ist aber nach **(i)***

$$< \cdot, \cdot >_{\mathbb{R}}: V_{\mathbb{R}} \times V_{\mathbb{R}} \ \to \ \mathbb{R}$$

eine nicht-ausgeartete, symmetrische Bilinearform auf $V_{\mathbb{R}}$. Genauer sei $\{v_1, \ldots, v_n\}$ eine $\mathbb{Q}$-Basis von V, dann lässt sich jedes Element von $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$ eindeutig schreiben als

$$\sum_{i=1}^{n} v_i \otimes \lambda_i$$

Betrachten wir nun die Fortsetzung $< \cdot, \cdot >_{\mathbb{R}}$ auf zwei Elementen $u, w \in V_{\mathbb{R}}$, dann gilt

$$\begin{aligned} < u, w >_{\mathbb{R}} &= \Big\langle \sum_{i=1}^{n} v_i \otimes \lambda_i \, , \, \sum_{j=1}^{n} v_j \otimes \mu_j \Big\rangle_{\mathbb{R}} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \mu_j \ < v_i \otimes 1 \, , \, v_j \otimes 1 \ >_{\mathbb{R}} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \mu_j \ < v_i, v_j > \end{aligned}$$

Die Fortsetzung ist also sogar kanonisch und mit der natürlichen Inklusion $j : V \hookrightarrow V_{\mathbb{R}}$ gilt

$$< x, y > \ = \ < j(x), j(y) >_{\mathbb{R}} \qquad \text{für alle } x, y \in V$$

Nach Konstruktion ist die Fortsetzung der Spurform eine symmetrische und nicht-ausgeartete Bilinearform auf $K_{\mathbb{R}}$. Leider ist diese Fortsetzung nicht notwendig positiv definit. Wir werden später eine Bilinearform auf $K_{\mathbb{R}}$ konstruieren, die tatsächlich positiv definit ist. Nehmen wir einmal an, wir hätten bereits gezeigt, dass es eine positiv definite symmetrische und nicht ausgeartete Bilinearform $< \cdot, \cdot >$ auf $K_{\mathbb{R}}$ gibt, dann wäre $(K_{\mathbb{R}}, < \cdot, \cdot >)$ ein euklidischer Raum und wir können den folgenden Satz formulieren und zeigen:

Satz 7.18 *Sei $\mathfrak{a} \in \mathcal{O}_K$ ein ganzes Ideal mit $\mathfrak{a} \neq 0$. Dann ist $j(\mathfrak{a})$ ein Gitter in $K_{\mathbb{R}}$ mit*

$$vol\Big(K_{\mathbb{R}}/j(\mathfrak{a})\Big) \;=\; \mathbb{N}(\mathfrak{a}) \cdot \sqrt{|D_K|}$$

bezüglich $< \cdot, \cdot >$.

Beweis. Es gilt

$$\mathfrak{a} \;=\; \mathbb{Z}\,\alpha_1 \oplus \ldots \oplus \mathbb{Z}\,\alpha_n$$

für eine $\mathbb{Q}$-Basis $\{\alpha_1, \ldots, \alpha_n\}$ von K. Die Menge $\{j(\alpha_1), \ldots, j(\alpha_n)\}$ ist eine $\mathbb{R}$-Basis von $K_{\mathbb{R}}$ mit

$$j(\mathfrak{a}) \;=\; \mathbb{Z}\,j(\alpha_1) \oplus \ldots \oplus \mathbb{Z}\,j(\alpha_n)$$

Damit ist $j(\mathfrak{a})$ ein Gillter in $K_{\mathbb{R}}$. Weiter gilt

$$\begin{aligned} vol\Big(K_{\mathbb{R}}/j(\mathfrak{a})\Big) \;&=\; \sqrt{\Big|\, \det\big(< j(\alpha_k), j(\alpha_l) >_{1\leq k,l\leq n} \big)\,\Big|} \;=\; \sqrt{\Big|\, \det\big(Tr^K_{\mathbb{Q}}(\alpha_k\alpha_l)_{1\leq k,l\leq n}\big)\,\Big|} \\ &=\; \sqrt{\big|d(\mathfrak{a})\big|} \;=\; \sqrt{\big(\mathbb{N}(\mathfrak{a})\big)^2 \cdot |D_K|} \;=\; \mathbb{N}(\mathfrak{a}) \cdot \sqrt{|D_K|} \end{aligned}$$

□

Wir wollen nun eine symmetrische nicht ausgeartete und positiv definite Bilinearform $< \cdot, \cdot >$ auf $K_{\mathbb{R}}$ konstruieren. Dazu müssen wir aber zunächst $K_{\mathbb{R}}$ besser verstehen. In den folgenden Lemmata wollen wir $K_{\mathbb{R}}$ konkreter beschreiben:

Lemma 7.19 *Die Abbildung*

$$\begin{aligned} \varphi : K \otimes_{\mathbb{Q}} \mathbb{C} \;&\to\; \prod_{\sigma\in\Sigma} \mathbb{C} \\ \lambda \otimes z \;&\mapsto\; \big(\sigma(\lambda)\big)_{\sigma\in\Sigma} \end{aligned}$$

ist ein Isomorphismus von $\mathbb{C}$-Vektorräumen. Wir schreiben $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C}$.

Beweis. Betrachte die Verkettung

$$\begin{aligned} \psi : K \;\overset{j}{\hookrightarrow}\; K \otimes_{\mathbb{Q}} \mathbb{C} \;&\overset{\varphi}{\to}\; \prod_{\sigma\in\Sigma} \mathbb{C} \\ \lambda \;\mapsto\; \lambda \otimes 1 \;&\mapsto\; \big(\sigma(\lambda)\big)_{\sigma\in\Sigma} \end{aligned}$$

Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Q}$-Basis von K, so ist $\{j(\alpha_1), \ldots, j(\alpha_n\}$ eine $\mathbb{C}$-Basis von $K \otimes_{\mathbb{Q}} \mathbb{C}$ und für jedes Basiselement α_i erhalten wir ein Tupel

$$\psi(\alpha_i) \;=\; \big(\sigma(\alpha_i)\big)_{\sigma\in\Sigma}$$

mit nur endlich vielen Einträgen ungleich Null. Insgesamt erhalten wir eine Matrix $A = \big(\psi(\alpha_i)\big)_{1\leq i\leq n}$ und A ist invertierbar. Also sind die Tupel $\psi(\alpha_i)$ eine Basis des $\mathbb{C}$-Vektorraums $\prod_{\sigma\in\Sigma} \mathbb{C}$. Also bildet φ eine Basis auf eine Basis ab und ist demnach ein Vektorraumisomorphismus. □

Lemma 7.20 *Die Galois-Gruppe von* $\mathbb{C}\,/\,\mathbb{R}$

$$G \;:=\; \mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R}) \;=\; \big\{1, c\big\}$$

wobei 1 *die Identität und* c *die komplexe Konjugation seien, operiert via*

$$\begin{array}{rcl} \omega : G \times K_{\mathbb{C}} & \to & K_{\mathbb{C}} \\ (g, \lambda \otimes z) & \mapsto & g(\lambda \otimes z) \;:=\; \lambda \otimes g(z) \end{array}$$

auf $K_{\mathbb{C}}$ *und es gilt*

$$K_{\mathbb{R}} \;=\; (K_{\mathbb{C}})^G \;=\; \big\{\, \lambda \otimes z \in K_{\mathbb{C}} \,\big|\, \lambda \otimes z = \lambda \otimes \overline{z} \,\big\}$$

Beweis. Die Galoisgruppe $G = \mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R})$ operiert $\mathbb{Q}$-linear auf $\mathbb{C}$, damit wird eine Operation von G auf $K_{\mathbb{C}}$ induziert. Betrachte

$$\begin{array}{ccc} K_{\mathbb{C}} & \to & K_{\mathbb{C}} \\ \| \wr & & \| \wr \\ c : \mathbb{C}^n & \to & \mathbb{C}^n \\ (z_1, \ldots, z_n) & \mapsto & (\overline{z}_1, \ldots, \overline{z}_2) \end{array}$$

□

Lemma 7.21 *Das folgende Diagramm kommutiert*

$$\begin{array}{ccc} K_{\mathbb{C}} & \xrightarrow{c} & K_{\mathbb{C}} \\ \| \wr & & \| \wr \\ \displaystyle\prod_{\sigma\in\Sigma} \mathbb{C} & \xrightarrow{c'} & \displaystyle\prod_{\sigma\in\Sigma} \mathbb{C} \end{array}$$

wobei c *die komplexe Konjugation bezeichne und*

$$c'\big((z_\sigma)_{\sigma\in\Sigma}\big) \;:=\; (\overline{z}_{\overline{\sigma}})_{\sigma\in\Sigma}$$

Beweis. Sei $\lambda \in K$ und $z \in \mathbb{C}$. Weiter bezeichne φ den Isomorphismus aus Lemma 7.19. Dann sind

$$\begin{array}{rcccl} c'\big(\varphi(\lambda \otimes z)\big) & = & c'\big(\big(\sigma(\lambda)\, z\big)_{\sigma\in\Sigma}\big) & = & \big(\sigma(\lambda)\, \overline{z}\big)_{\sigma\in\Sigma} \\ \varphi\big(c(\lambda \otimes z)\big) & = & \varphi(\lambda \otimes \overline{z}) & = & \big(\sigma(\lambda)\, \overline{z}\big)_{\sigma\in\Sigma} \end{array}$$

□

Folgerung 7.22 *Es gibt einen kanonischen Isomorphismus*

$$K_{\mathbb{R}} \;:=\; K \otimes_{\mathbb{Q}} \mathbb{R} \;\xrightarrow{\sim}\; \Big\{\, (z_\sigma)_{\sigma\in\Sigma} \in \prod_{\sigma\in\Sigma} \mathbb{C} \;\Big|\, \overline{z}_\sigma \,=\, z_\sigma \,\Big\}$$

Beweis. Nach Lemma 7.20 gilt $K_{\mathbb{R}} \,=\, (K_{\mathbb{C}})^{\mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R}}$. Die Menge $G := \{1, c'\}$, wobei 1 die Identität auf dem Produktraum und c' die Abbildung aus Lemma 7.21 ist, ist eine Gruppe, die via

$$\begin{array}{rcl} \omega : G \times \displaystyle\prod_{\sigma\in\Sigma} \mathbb{C} & \to & \displaystyle\prod_{\sigma\in\Sigma} \mathbb{C} \\ (g, \underline{z}) & \mapsto & g.\underline{z} \;:=\; g(\underline{z}) \end{array}$$

auf dem Produktraum $\prod_{\sigma\in\Sigma}\mathbb{C}$ operiert. Es gilt

$$\Big\{ (z_\sigma)_{\sigma\in\Sigma} \in \prod_{\sigma\in\Sigma}\mathbb{C} \;\Big|\; \overline{z}_\sigma \,=\, z_\sigma \Big\} \;=\; \Big(\prod_{\sigma\in\Sigma}\mathbb{C}\Big)^G$$

□

Folgerung 7.23 *Wir können nun $K_\mathbb{R}$ als Produktraum auffassen, denn es gilt*

$$\begin{aligned} K_\mathbb{R} \;&\cong\; \Big\{ (z_\sigma)_{\sigma\in\Sigma} \in \prod_{\sigma\in\Sigma}\mathbb{C} \;\Big|\; \overline{z}_\sigma \,=\, z_\sigma \Big\} \\ &\cong\; \mathbb{R}^r \times \mathbb{C}^s \;\cong\; \mathbb{R}^{r+2s} \;\cong\; \prod_{\sigma\in\Sigma}\mathbb{R} \end{aligned}$$

Beweis. Teile die Homomorphismen in Σ auf wie folgt:

$$\Sigma \;=\; \big\{ \underbrace{\sigma_1,\ldots,\sigma_r}_{reell}, \underbrace{\tau_1,\overline{\tau}_1,\ldots,\tau_n,\overline{\tau}_n}_{komplex} \big\}$$

und setze

$$x_\sigma \;:=\; z_\sigma \qquad x_\tau := \Re(z_\tau) \qquad x_{\overline{\tau}} := \Im(z_\tau)$$

wobei $\Re(z)$ der Realteil und $\Im(z)$ der Imaginärteil von $z \in \mathbb{C}$ sei. Dann folgt die Behauptung mit dem $\mathbb{R}$-Vektorraumisomorphismus

$$\begin{array}{ccccc} \big\{ (z,w) \in \mathbb{C}^2 \;\big|\; z = \overline{w} \big\} & \xrightarrow{\sim} & \mathbb{C} & \xrightarrow{\sim} & \mathbb{R}^2 \\ (z,w) & \mapsto & z & \mapsto & \big(\Re(z),\Im(z)\big) \end{array}$$

□

Mit diesem Verständnis von $K_\mathbb{R}$ als $\mathbb{R}^{r+2s}$ können wir nun eine symmetrische nicht ausgeartete Bilinearform $<\cdot,\cdot>$ auf $K_\mathbb{R}$ konstruieren, die positiv definit ist.

Konstruktion 7.24 *Sei $n = r + 2s \in \mathbb{N}$. Betrachte das Standart-Skalarprodukt $<\cdot,\cdot>_\mathbb{C}$ auf $\mathbb{C}^n$, dann erhalten wir hieraus mit Lemma 7.19 eine Hermitsche Form auf $\prod_{\sigma\in\Sigma}\mathbb{C}$*

$$\big\langle (z_\sigma)_{\sigma\in\Sigma}\,,\,(w_\sigma)_{\sigma\in\Sigma} \big\rangle \;=\; \sum_{\sigma\in\Sigma} z_\sigma \cdot \overline{w}_\sigma$$

Mit Folgerung 7.23 induziert diese hermitsche Form eine positiv definite, symmetrische und nicht ausgeartete Bilinearform $<\cdot,\cdot>$ auf $K_\mathbb{R}$ durch Einschränkung.
Explizit gilt für $v = (t_1,\ldots,t_r,x_1,y_1,\ldots,x_s,y_s) \in \mathbb{R}^{r+2s}$

$$<v,v> \;=\; \sum_{i=1}^{r} t_i^2 + 2\cdot\left(\sum_{i=1}^{s} x_i^2 \cdot y_i^2\right)$$

Mit der Einbettung

$$\begin{aligned} j : K &\hookrightarrow K_{\mathbb{R}} \\ a &\mapsto \big(\sigma(a)\big)_{\sigma\in\Sigma} \end{aligned}$$

Gilt für die Spurform

$$Tr_{\mathbb{Q}}^{K}(ab) \;=\; \sum_{\sigma\in\Sigma} \sigma(a)\cdot\sigma(b)$$

damit unterscheidet sich die fortgesetzte Spurform von der oben konstruierten kanonischen Form nur durch komplexe Konjugation in der zweiten Variable. Diese Konjugation sorgt dafür, dass die kanonische Form positiv definit ist.
Insbesindere, wenn K nur reelle Einbettungen σ hat, stimmen die kanonische und die fortgesetzte Spurform überein.

Satz 7.25 *Sei $\mathfrak{a} \lhd \mathcal{O}_K$ ein Ideal ungleich Null. Dann gibt es ein $a \in \mathfrak{a}\setminus\{0\}$ mit*

$$N_{\mathbb{Q}}^{K}(a) \;\leq\; C_K \cdot \sqrt{|D_K|}\cdot \mathbb{N}(\mathfrak{a})$$

Als Folgerung aus diesem Satz erhalten wir sofort den

Satz 7.15 *(Minkowski-Konstante/ Satz von Minkowski II)*
In jeder Idealklasse $C \in \mathcal{C}\ell(K)$ gibt es ein ganzes Ideal $\mathfrak{a} \lhd \mathcal{O}_K$ mit

$$\mathbb{N}(\mathfrak{a}) \;\leq\; C_K \cdot \sqrt{|D_K|} \qquad \text{wobei } \; C_K \;:=\; \frac{n!}{n^n}\cdot\left(\frac{4}{\pi}\right)^s$$

Beweis. Wir zeigen Zunächst, dass der Satz von Minkowski II aus Satz 7.25 folgt. Sei dazu $\mathfrak{b} \lhd \mathcal{O}_K$ ein Ideal mit Klasse $c^{-1} = [b] \in \mathcal{C}\ell(K)$. Mit dem Vorausgesetzen Satz gibt es dann ein $x \in \mathfrak{b}$ mit

$$\begin{aligned} & N_{\mathbb{Q}}^{K}(x) && \leq\; C_K \cdot \sqrt{|D_K|}\cdot \mathbb{N}(\mathfrak{b}) \\ \Leftrightarrow\; & \mathbb{N}(\mathfrak{b})^{-1}\cdot N_{\mathbb{Q}}^{K}(x) && \leq\; C_K\sqrt{|D_K|} \\ \Leftrightarrow\; & \mathbb{N}(x\,\mathfrak{b}^{-1}) && \leq\; C_K\sqrt{|D_K|} \end{aligned}$$

Denn

$$\mathbb{N}\big((x)\big) \;=\; \big(\mathcal{O}_K : (x)\big) \;=\; N_{\mathbb{Q}}^{K}(x)$$

Wir wollen nun den Satz beweisen. Da wir dies mithilfe des Gitterpunktsatzes 7.12 tun wollen, müssen wir eine Menge X konstruieren, die die Eigenschaften

- X ist kompakt, konvex und zentralsymmetrisch
- Es gilt $vol(X) \geq 2^n \cdot vol(\mathfrak{a})$

erfüllt, denn dann gibt es ein $a \in \big(X \cap \mathfrak{a}\setminus\{0\}\big)$. Wir setzen für $t \in \mathbb{R}_+$

$$X \;:=\; S(t) \;:=\; \left\{ (z_\sigma)_{\sigma\in\Sigma} \in K_{\mathbb{R}} \,\middle|\, \sum_{\sigma\in\Sigma} |z_\sigma| \;\leq\; t \right\}$$

In einer Übungsaufgabe haben wir gezeigt, dass

$$vol\big(S(t)\big) \;=\; \frac{t^n}{n!}\cdot 2^r\cdot\pi^s$$

gilt. Wir wollen nun, durch geschickte Wahl von t, erreichen, dass

$$vol\big(S(t)\big) \;=\; 2^n \cdot vol(\mathfrak{a})$$

gilt. Dazu wähle

$$t^n \;:=\; \frac{n!}{\pi^s} \cdot 2^{n-r} \cdot vol(\mathfrak{a}) \;=\; \frac{n! \cdot 2^{2s}}{\pi^s} \cdot vol(\mathfrak{a})$$

Dann gibt es nach dem Gitterpunktsatz ein $a \in S(t) \cap \big(\mathfrak{a} \setminus \{0\}\big)$. Wegen $a \in S(t)$ gilt dann

$$\sum_{\sigma \in \Sigma} |\sigma(a)| \;<\; t$$

Nach der verallgemeinerten Cauchy-Schwarzen Ungleichung gilt

$$\Big(N_{\mathbb{Q}}^K(a)\Big)^{\frac{1}{n}} \;=\; \Big(\prod_{\sigma \in \Sigma} |\sigma(a)|\Big)^{\frac{1}{n}} \;\leq\; \frac{1}{n} \cdot \sum_{\sigma \in \Sigma} |\sigma(a)| \;\leq\; \frac{t}{n}$$

Beim Übergang zur n-ten Potenz bleiben die Ungleichungen erhalten, daher folgt

$$\begin{aligned} N_{\mathbb{Q}}^K(a) \;&\leq\; \frac{t^n}{n^n} \;=\; \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot vol(\mathfrak{a}) \\ &=\; C_K \cdot vol\big(\mathcal{O}_K\big) \cdot [\mathcal{O}_K : \mathfrak{a}] \\ &=\; C_K \cdot \sqrt{|D_K|} \cdot \mathbb{N}(\mathfrak{a}) \end{aligned}$$

□

Folgerung 7.26 *Sei $\mathfrak{a} \lhd \mathcal{O}_K$ ein Ideal ungleich Null. Dann gibt es ein $a \in \mathfrak{a} \setminus \{0\}$ mit*

$$\frac{N_{\mathbb{Q}}^K(a)}{\mathbb{N}(\mathfrak{a})} \;\leq\; C_K \cdot \sqrt{|D_K|}$$

Insbesondere gilt für $C_K \cdot \sqrt{|D_K|} \;<\; 2$, dass für jedes $\mathfrak{a} \lhd \mathcal{O}_K$ ein $a \in \mathfrak{a}$ existiert, so dass $\mathfrak{a} = (a)$ ein Hauptideal ist. Damit ist $\mathcal{O}_K$ dann ein Hauptidealring.

Beispiel 22 *(Hauptialringeigenschaft von Ganzheitsringen I)*
Sei $K = \mathbb{Q}(\sqrt{d})$ für ein $d > 0$ quadratfrei. Dann ist $n = [K : \mathbb{Q}] = 2$ und beide Einbettungen

$$id, \sigma : \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{C}$$

sind reell. Also ist $r = 2$ und $s = 0$ und es gilt

$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \;=\; \frac{2}{2^2} \;=\; \frac{1}{2}$$

Damit erhalten wir die Bedingung

$$\frac{1}{2} \cdot \sqrt{|D_K|} \;<\; 2 \quad \Leftrightarrow \quad |D_K| \;<\; 16$$

Insbesondere sind also alle Ganzheitsringe $\mathcal{O}_K$ von $K = \mathbb{Q}(\sqrt{d})$ Hauptidealringe, nach Folgerung 7.26. Für $d \in \{2, 3, 5, 13\}$ erhalten wir Diskriminanten $D_K = \{8, 12, 5, 13\}$ damit sind die zugehörigen Ganzheitsringe Hauptidealringe.

Beispiel 23 *(Hauptialringeigenschaft von Ganzheitsringen II)*
Sei $K = \mathbb{Q}(\zeta_5)$ wobei ζ_5 eine primitive 5-te Einheitswurzel sei. Dann ist

$$n \;=\; [K : \mathbb{Q}] \;=\; [\mathbb{Q}(\zeta_5) : \mathbb{Q}] \;=\; 4$$

und alle Einbettungen

$$\sigma_1, \ldots, \sigma_4 : \mathbb{Q}(\zeta_5) \hookrightarrow \mathbb{C}$$

sind komplex. Damit sind $s = 2$ und $r = 0$. Weiter ist $D_K = 5^3 = 125$ und wir erhalten

$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D_K|} \;=\; \frac{4!}{4^4} \cdot \frac{4^2}{\pi^2} \cdot \left(\sqrt{5}\right)^3 \;=\; \frac{15 \cdot \sqrt{5}}{2 \cdot \pi^2} \;<\; 2$$

Damit ist $\mathcal{O}_K$ für $K = \mathbb{Q}(\zeta_5)$ ein Hauptidealring.

Beispiel 24 *Sei nun $K = \mathbb{Q}(\sqrt{-5})$, dann gelten $n = 2$, $s = 1$, $r = 0$ und $D_K = 20$. Damit erhalten wir*

$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D_K|} \;=\; \frac{2}{2^2} \cdot \frac{4}{\pi} \cdot (2 \cdot \sqrt{5}) \;=\; \frac{4 \cdot \sqrt{5}}{\pi} \;\approx\; 2,85 \;<\; 3$$

Also gibt es in jeder Idealklasse $C \in \mathcal{C}\ell(K)$ ein ganzes Ideal $\mathfrak{a} \in C$ mit $\mathbb{N}(\mathfrak{a}) \leq 2$. Angenommen $\mathbb{N}(\mathfrak{a}) = 2$, dann teilt $\mathfrak{a}$ das von 2 in $\mathcal{O}_K$ erzeugte Ideal, das heißt $2\,\mathcal{O}_K \subseteq \mathfrak{a}$. Damit definiert $\mathfrak{a}$ ein Ideal $\overline{\mathfrak{a}}$ in

$$\begin{aligned} \mathcal{O}_K \big/ 2\,\mathcal{O}_K \;&=\; \mathbb{Z}[\sqrt{-5}] \big/ (2) \;\cong\; \mathbb{F}_2[T] \big/ (t^2 + 5) \\ &\cong\; \mathbb{F}_2[T] \big/ (t^2 + 1) \;\cong\; \mathbb{F}_2[T] \big/ (t + 2)^2 \end{aligned}$$

insbesondere den letzten Ring kennen wir sehr gut und wissen, dass er nur die Ideale $(t + 1)$ und $(t + 1)^2 \cong \overline{2\,\mathcal{O}_K}$ enthält. Da $\mathbb{N}(2\,\mathcal{O}_K) = 4$ ist, gilt $\mathfrak{a} \neq 2\,\mathcal{O}_K$ also muss $\overline{\mathfrak{a}} \cong (t + 1)$ gelten und damit ist

$$\mathfrak{a} \;=\; (2, 1 + \sqrt{-5})$$

und $\mathfrak{a}$ ist das einzige Ideal mit Norm 2. Also ist $\sharp\,\mathcal{C}\ell(K) = h_K = 2$ und wir erhalten

$$\mathcal{C}\ell(K) \;=\; \mathbb{Z} \big/ 2\,\mathbb{Z} \qquad \text{für } K = \mathbb{Q}(\sqrt{-5})$$

Der Satz von Minkowski II hilft uns aber nicht nur bei der genaueren Beschreibung von Ganzheitsringen, sondern können wir auch einige Aussagen über die Diskriminante von Zahlkörpern schließen. Zum Beispiel die naheliegende, aber bisher noch nicht bewiesenen Aussage

Folgerung 7.27 *Wenn $K \neq \mathbb{Q}$ ist, dann gilt $|D_K| > 1$.*

Beweis. Nach dem Satz von Minkowski II gilt

$$1 \;\leq\; C_K \cdot \sqrt{|D_K|}$$

Dies können wir umformen zu

$$|D_K| \;\geq\; \left(\frac{n^n \cdot \pi^s}{n! \cdot 4}\right)^2 \;=:\; c_n$$

Wir wollnen nun per Induktion über $n = r + 2s$ schließen. Wegen

$$\left(\frac{\pi}{4}\right)^s \;\overset{s \to \infty}{\longrightarrow}\; 0$$

wähle s immer so groß wie möglich.

Induktions Anfang Für $n = 2$ gilt $s \leq 1$. Wähle also $s = 1$, dann ist

$$c_2 \;=\; \left(\frac{2^2 \cdot \pi}{2 \cdot 4}\right)^2 \;=\; \frac{\pi^2}{4} \;>\; 1$$

Induktions Schritt Wir schließen von n auf $n+1$. Betrachte den Quotienten

$$\begin{aligned}\frac{c_{n+1}}{c_n} &= \left(\frac{(n+1)^{n+1} \cdot n!}{(n+1)! \cdot n^n}\right)^2 \cdot \frac{\pi}{4} \;=\; \left(\left(\frac{n+1}{n}\right)^n\right)^2 \cdot \frac{\pi}{4} \\ &= \frac{\pi}{4} \cdot \left(1 + \frac{1}{n}\right)^{2n} \;\geq\; \frac{\pi}{4}(1+2) \;=\; \frac{3\pi}{4} \;>\; 1\end{aligned}$$

damit ist $c_{n+1} > c_n$. □

Bemerkung 7.28 *Die Folgerung impliziert*

$$\lim_{n \to \infty} \frac{1}{C_K} \;=\; \infty$$

Insbesondere haben für fest gewähltes $N \in \mathbb{N}$ alle Zahlkörper K mit $|D_K| \leq N$ einen beschränkten (endlichen) Erweiterungsgrad über $\mathbb{Q}$.

Folgerung 7.29 *Zu fest gewähltem $d \in \mathbb{N}$ gibt es nur endlich viele Zahlkörper $K/\mathbb{Q}$ mit $|D_K| = d$.*

Beweis. Nach der vorangegangenen Bemerkung ist $[K : \mathbb{Q}] \leq N$ für ein $N \in \mathbb{N}$. Wir suchen nun ein „möglichst kleines“ ganzes Element $\alpha \in \mathcal{O}_K$ mit $K = \mathbb{Q}(\alpha)$. Dazu beschränken wir uns zunächst auf den Fall, dass es komplexe Einbettungen von K in $\mathbb{C}$ gibt, also $s > 0$ ist. Dann wähle eine solche komplexe Einbettung $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \Sigma$ aus und setze

$$\Omega(t) \;:=\; \left\{ (z_\tau)_{\tau \in \Sigma} \;\middle|\; \begin{array}{rcll} |z_\sigma - z_{\overline{\sigma}}| & < & t \cdot \sqrt{|D_K|} & ① \\ |z_\sigma + z_{\overline{\sigma}}| & < & \frac{1}{2} & ② \\ |z_\tau| & < & \frac{1}{2} \;\; \forall\, \tau \in \Sigma \backslash \{\sigma, \overline{\sigma}\} & ③ \end{array} \right\}$$

Die so definierte Menge $\Omega(t)$ ist konvex und zentralsymmetrisch. Nach dem Satz von Minkowski gibt es für $t \in \mathbb{N}$ groß genug in Abhängigkeit von n und D_K eine ganz algebraische Zahl $\alpha \in \mathcal{O}_K$ mit

$$\alpha \;\in\; \Omega(t) \cap (\mathcal{O}_K \backslash \{0\})$$

Behauptung $\sigma(\alpha) \;\notin\; \{\, \overline{\sigma}(\alpha) \,\} \cup \{\, \tau(\alpha) \,|\, \tau \in \Sigma \backslash \{\sigma, \overline{\sigma}\} \,\}$

Wenn wir diese Behauptung zeigen können ist $K = \mathbb{Q}(\alpha)$. Wir wissen schon, dass $\alpha \in \mathcal{O}_K$ ist, also ist das Minimalpolynom μ_α aus $\mathbb{Z}[X]$ und die Koeffizienten von μ_α sind die elementarsymmetrischen Polynome in $\{\, z_\tau \,|\, \tau \in \Sigma \,\}$ aber die Absulotbeträge

$$|Re(z_\sigma)|, \;\; |Im(z_\sigma)| \;\text{ und }\; |z_\tau|_{\tau \in \Sigma \backslash \{\sigma, \overline{\sigma}}$$

sind beschränkt. Also sind auch die Koeffizienten beschränkt und es gibt nur endlich viele Möglichkeiten für μ_α.

Beweis der Behauptung. Angenommen $\sigma(\alpha) = \overline{\sigma}(\alpha)$, dann gelten

$$\begin{aligned} Im\big(\sigma(\alpha)\big) &= 0 && \text{nach } ① \\ Re\big(\sigma(\alpha)\big) &< \tfrac{1}{4} && \text{nach } ② \\ \forall\, \tau \in \Sigma \backslash \{\sigma, \overline{\sigma}\} \qquad \big|\tau(\alpha)\big| &< \tfrac{1}{2} && \text{nach } ③ \end{aligned}$$

Damit gilt aber für die Norm von α

$$N_{\mathbb{Q}}^{K}(\alpha) \;<\; 1$$

Dies ist ein Widerspruch, denn α ist ganz algebraisch.
Sei nun angenommen es gibt ein $\tau \in \Sigma\backslash\{\sigma, \overline{\sigma}\}$ mit $\sigma(\alpha) = \tau(\alpha)$. Dann ist

$$|\sigma(\alpha)| \;=\; |\tau(\alpha)| \;<\; \frac{1}{2} \qquad \text{nach } ③$$

Damit erhalten wir aber aus den Bedingungen

$$|\overline{\sigma(\alpha)}| \;<\; \frac{1}{2} \quad \text{und} \quad |\rho(\alpha)| \;<\; \frac{1}{4} \quad \forall\, \rho \in \Sigma\backslash\{\sigma, \overline{\sigma}, \tau\}$$

Damit erhalten wir für die Norm von α erneut einen Widerspruch, denn

$$N_{\mathbb{Q}}^{K}(\alpha) \;=\; \prod_{\rho\in\Sigma} \rho(\alpha) \;<\; 1$$

$\diamond$

Damit haben wir die Folgerung im Fall $s > 0$ bewiesen. Für den Fall $s = 0$ konstruiere eine ähnliche Hilfsmenge $\Omega(t)$ und schließe analog. $\square$

8 Der Dirichletsche Einheitssatz

In desem Abschnitt betrachten wir wieder eine endliche Körpererweiterung $K/\,\mathbb{Q}$, also einen Zahlkörper K mit $[K : \mathbb{Q}] = n = r + 2s$. Wie zuvor benutzen wir die Abkürzung

$$\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \;=:\; \Sigma$$

Weiter betrachten wir die aus dem vorangegangen Abschnitt bekannte Einbettung

$$\begin{array}{rccccc} j: & K & \hookrightarrow & K \otimes_{\mathbb{Q}} \mathbb{C} & \xrightarrow{\sim} & \prod_{\sigma\in\Sigma} \mathbb{C} \\ & \lambda & \mapsto & \lambda \otimes 1 & & \\ & & & \lambda \otimes z & \mapsto & \big(\sigma(\lambda) \cdot z\big)_{\sigma\in\Sigma} \\ & \lambda & & \longmapsto & & \big(\sigma(\lambda)\big)_{\sigma\in\Sigma} \end{array}$$

Bemerkung 8.1 *Der $\mathbb{C}$-Vektorraum $K \otimes_{\mathbb{Q}} \mathbb{C} =: K_{\mathbb{C}}$ ist ein Ring.*

Beweis. Die Multiplikation auf $K_{\mathbb{C}}$ wird induziert durch

$$(\lambda_1 \otimes z_1) \cdot (\lambda_2 \otimes z_2) \;=\; \lambda_1\lambda_2 \otimes z_1 z_2$$

$\square$

Damit ist der oben genannte Isomorphismus $K_{\mathbb{C}} \xrightarrow{\sim} \prod \mathbb{C}$ nicht nur ein Isomorphismus von abelschen Gruppen, sondern auch ein Ringisomorphismus. Damit gilt

$$K^* \;\hookrightarrow\; \big(K_{\mathbb{C}}\big)^{\times} \;\xrightarrow{\sim}\; \prod_{\sigma\in\Sigma} \mathbb{C}^*$$

Setze nun

$$\begin{aligned} l : \mathbb{C}^* &\to \mathbb{R} \\ z &\mapsto \log|z| \end{aligned}$$

dann ist l ein stetiger Gruppenhomomorphismus mit der Fortsetzung

$$\begin{aligned} \tilde{l} : K_{\mathbb{C}}^{\times} &\to \prod_{\sigma\in\Sigma} \mathbb{R} \\ (z_\sigma)_{\sigma\in\Sigma} &\mapsto \big(\log|z_\sigma|\big)_{\sigma\in\Sigma} \end{aligned}$$

Definiere nun noch die Abbildung

$$\begin{aligned} N : K_{\mathbb{C}}^{\times} &\to \mathbb{C}^* \\ (z_\sigma)_{\sigma\in\Sigma} &\mapsto \prod_{\sigma\in\Sigma} z_\sigma \end{aligned}$$

dann erhalten wir das kommutative Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^{\times} & \xrightarrow{\tilde{l}} & \prod\limits_{\sigma\in\Sigma} \mathbb{R} \\ \Big\downarrow{\scriptstyle N_{\mathbb{Q}}^K} & & \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \xrightarrow[\iota]{} & \mathbb{C}^* & \xrightarrow[l]{} & \mathbb{R} \end{array}$$

Wir wissen aus dem vorangegangen Abschnitt, dass die Galois-Gruppe $G := \mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R}) = \{1, c\}$ auf $K_{\mathbb{C}}$ operiert, und dass

$$K_{\mathbb{R}} \;=\; K \otimes_{\mathbb{Q}} \mathbb{R} \;=\; \big(K_{\mathbb{C}}\big)^G$$

gilt. Wenn wir nun die Galois-Gruppe G auf dem Diagramm via

$$\begin{aligned} c\big((z_\sigma)_{\sigma\in\Sigma}\big) &= (\overline{z}_{\overline{\sigma}})_{\sigma\in\Sigma} \qquad \text{wenn } (z_\sigma)_{\sigma\in\Sigma} \in K_{\mathbb{C}} \\ c\big((x_\sigma)_{\sigma\in\Sigma}\big) &= (x_{\overline{\sigma}})_{\sigma\in\Sigma} \qquad \text{wenn } (x_\sigma)_{\sigma\in\Sigma} \in \prod_{\sigma\in\Sigma} \mathbb{R} \end{aligned}$$

operieren lassen, erhalten wir das Folgende kommutative Diagramm **(D1)**:

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^{\times} & \xrightarrow{\tilde{l}} & \Big(\prod\limits_{\sigma\in\Sigma} \mathbb{R}\Big)^G \\ \Big\downarrow{\scriptstyle N_{\mathbb{Q}}^K} & & \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \xrightarrow[\iota]{} & \mathbb{R}^* & \xrightarrow[l]{} & \mathbb{R} \end{array}$$

Weiter gelten

$$\begin{aligned} \Big(\prod_{\sigma\in\Sigma} \mathbb{R}\Big)^G &= \underbrace{\mathbb{R}\times\ldots\times\mathbb{R}}_{r-\text{mal}} \times \underbrace{(\mathbb{R}\times\mathbb{R})^G \times \ldots \times (\mathbb{R}\times\mathbb{R})^G}_{s-\text{mal}} \\ (\mathbb{R}\times\mathbb{R})^G &= \big\{\, (x,x) \in \mathbb{R}^2 \;\big|\; x \in \mathbb{R} \,\big\} \end{aligned}$$

Aus diesen Gleichungen erhalten wir ein weiteres kommutatives Diagramm **D2)**:

$$\begin{array}{ccc} \Big(\prod_{\sigma\in\Sigma}\mathbb{R}\Big)^G & \xrightarrow{\sim} & \mathbb{R}^{r+s} \\ {\scriptstyle Tr}\downarrow & & \downarrow{\scriptstyle Tr'} \\ \mathbb{R} & \xrightarrow[id]{} & \mathbb{R} \end{array}$$

mit

$$Tr'\big((x_1,\ldots,x_{r+s})\big) \;:=\; \sum_{i=1}^{r+s} x_i$$

Damit können wir den fortgesetzten Homomorphismus $\tilde{l}$ im Diagramm **(D1)** explizit angeben, es gilt

$$\begin{array}{rccl} \tilde{l}: & K_{\mathbb{R}}^{\times} & \to & \mathbb{R}^{r+s} \\ & (z_\sigma)_{\sigma\in\Sigma} & \mapsto & \big(\log|z_{\sigma_1}|,\ldots,\log|z_{\sigma_r}|,(\log|z_{\tau_1}|)^2,\ldots,(\log|z_{\tau_s}|)^2\big) \end{array}$$

Die hier eingeführten Abbildungen und Mengen werden wir im gesamten Abschnitt verwenden. Weiter werden wir die Mengen

$$\begin{aligned} H &:= \left\{ x\in\Big(\prod_{\sigma\in\Sigma}\mathbb{R}\Big) \,\Big|\, Tr(x)=0 \right\} \;\cong\; \{\, x\in\mathbb{R}^{r+s} \,|\, Tr'(x)=0 \,\} \\ S &:= \{\, y\in K_{\mathbb{R}}^{\times} \,|\, N(y)\in\{\pm1\} \,\} \end{aligned}$$

gebrauchen. Es gilt

$$\dim_{\mathbb{R}}(H) \;=\; \dim_{\mathbb{R}}\Big[\Big(\prod_{\sigma\in\Sigma}\mathbb{R}\Big)^G\Big]-1 \;=\; \dim_{\mathbb{R}}\big(\mathbb{R}^{r+s}\big)-1 \;=\; r+s-1$$

Bemerkung 8.2 *Die Abbildung*

$$\varphi:\; \mathcal{O}_K^{\times} \xrightarrow{\;j\;} S \xrightarrow{\;\tilde{l}\;} H$$

ist ein Gruppenhomomorphismus.

Beweis. Die Einheiten im Ganzheitsring sind

$$\mathcal{O}_K^{\times} \;=\; \{\, x\in\mathcal{O}_K \,|\, N_{\mathbb{Q}}^K(x)\in\{\pm1\} \,\}$$

damit folgt $j(\mathcal{O}_K^{\times})\subset S$ aus dem Diagramm **(D1)**. Die andere Inklusion ist klar. φ ist als Komposition zweier Gruppenhomomorphismen ein Gruppenhomomorphismus. □

Wir wollen im Folgenden den Kern von φ bestimmen und anschließend zeigen, dass das Bild ein Gitter in H ist.

Lemma 8.3 *Sei die Gruppe der Einheitswurzeln in K mit $\mu(K)$ bezeichnet, dann gilt*

$$\mathrm{Ker}(\varphi) \;=\; \mathrm{Ker}(\tilde{l}\circ j) \;=\; \mu(K)$$

Beweis. Sei zunächst $\zeta \in \mu(K)$ eine Einheitswurzel, dann ist wegen $[K : \mathbb{Q}] = n$ spätestens die n-te Potenz von ζ wieder 1, das heißt $\zeta^n = 1$. Für alle $\sigma \in \Sigma$ gilt

$$\begin{aligned} \sigma(\zeta^n) &= \sigma(\zeta)^n &= 1 \\ \Rightarrow \quad n \cdot \log|\sigma(\zeta)| &= 0 \\ \Rightarrow \quad \log|\sigma(\zeta)| &= 0 \end{aligned}$$

Da die Abbildung $j : \mathcal{O}_K^\times \hookrightarrow S$ injektiv ist, folgt aus $\zeta \in \mathrm{Ker}(\tilde{l})$ bereits die gewünschte Inklusion $\mu(K) \subseteq \mathrm{Ker}(\varphi)$.
Wir wissen bereits, dass $j(\mathcal{O}_K)$ ein Gitter in $K_\mathbb{R}$ ist, also ist die Menge

$$M \;:=\; j(\mathcal{O}_K) \cap \left\{ (z_\sigma)_{\sigma\in\Sigma} \in K_\mathbb{R} \,\middle|\, |z_\sigma| \leq 1 \;\text{ für alle } \sigma \in \Sigma \right\}$$

endlich. Wegen $j\big(\mathrm{Ker}(\varphi)\big) \subseteq M$ ist dann auch $j\big(\mathrm{Ker}(\varphi)\big)$ endlich. Da j eine Einbettung ist, ist $\mathrm{Ker}(\varphi)$ eine endliche Untergruppe von $\mathcal{O}_K^\times$. Damit folgt die andere Inklusion $\mathrm{Ker}(\varphi) \subseteq \mu(K)$, denn jedes Element $x \in \mathrm{Ker}(\varphi)$ hat höchstens Ordung $\mathrm{Ord}(\mathcal{O}_K^\times) = n$, also gilt $x^n = 1$. □

Bemerkung 8.4 *Die Menge $\varphi(\mathcal{O}_K^\times)$ ist genau dann ein Gitter in H, wenn es Einheiten im Ganzheitsring $\varepsilon_1, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ so gibt, dass gelten*

1. *Die Menge $\{\varphi(\varepsilon_1), \ldots, \varphi(\varepsilon_{r+s-1})\}$ ist $\mathbb{R}$-linear unabhängig.*
2. *Die ε_i erzeugen $\varphi(\mathcal{O}_K^\times)$ über $\mathbb{Z}$, das heißt:*

$$\varphi(\mathcal{O}_K^\times) \;=\; \tilde{l}\big(j(\mathcal{O}_K^\times)\big) \;=\; \mathbb{Z}\,\varphi(\varepsilon_1) \otimes \ldots \otimes \mathbb{Z}\,\varphi(\varepsilon_{r+s-1})$$

Folgerung 8.5 *(Dirichletscher Einheitssatz)*
Es gilt die Isomorphie der folgenden abelschen Gruppen:

$$\mathcal{O}_K^\times \;\cong\; \mu(K) \times \mathbb{Z}^{r+s-1}$$

Konkret heißt das, dass es für alle $u \in \mathcal{O}_K^\times$ genau eine Einheitswurzel $\zeta \in \mu(K)$ und ganze Zahlen $n_i \in \mathbb{Z}$ so gibt, dass gilt

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

mit ε_i wie in der vorangegangenen Bemerkung.

Beweis. Sobald wir wissen, das $\varphi(\mathcal{O}_K^\times)$ ein Gitter in H ist erhalten wir die Aussage der Folgerung aus dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen. □

Wir wollen nun die Aussage, dass $\varphi(\mathcal{O}_K^\times)$ ein Gitter in H ist, schritweise in der nach Bemerkung 8.4 umgeformten Version beweisen.

Lemma 8.6 *$\varphi(\mathcal{O}_K^\times)$ ist eine diskrete Untergruppe von H.*

Beweis. Für alle $c \in \mathbb{R}_+$ setze

$$B_c \;:=\; \left\{ (x_\sigma)_{\sigma\in\Sigma} \in \mathbb{R}^{r+s} \,\middle|\, |x_\sigma| < c \quad \forall\, \sigma \in \Sigma \right\}$$

Es genüg nun zu zeigen, dass der Schnitt von B_c und $\varphi(\mathcal{O}_K^\times)$ endlich ist für alle $c \in \mathbb{R}_+$. Wir wissen bereits, dass $j(\mathcal{O}_K)$ ein Gitter in $K_\mathbb{R}$ ist und die Menge

$$l^{-1}(B_c) \;=\; \left\{ (z_\sigma)_{\sigma\in\Sigma} \in \prod_{\sigma\in\Sigma} \mathbb{C} \;\middle|\; \exp(-c) \,<\, |z_\sigma| \,<\, \exp(c)\ \forall \sigma \in \Sigma \right\}$$

ist offensichtlich beschränkt. Also ist $j(\mathcal{O}_K) \cap l^{-1}(B_c)$ eine endliche Menge. Dann ist aber erst recht die kleinere Menge $j(\mathcal{O}_K^\times) \cap l^{-1}(B_c)$ endlich. Wende nun l auf diese Menge an, dann ist

$$l\big(\, j(\mathcal{O}_K^\times) \cap l^{-1}(B_c)\,\big) \;=\; \big(j(\mathcal{O}_K^\times)\big) \cap B_c \;=\; \varphi(\mathcal{O}_K^\times) \cap B_c$$

endlich. □

Nach diesem Lemma gibt es also $\varepsilon_1, \ldots, \varepsilon_d \in \mathcal{O}_K^\times$ mit der Eigenschaft, dass die Menge $\big\{\, \varphi(\varepsilon_1),\, \ldots,\, \varphi(\varepsilon_d)\big\}$ linear unabhängig über $\mathbb{R}$ ist und

$$\varphi(\mathcal{O}_K^\times) \;=\; \mathbb{Z}\,\varphi(\varepsilon_1) \,\otimes\, \ldots \,\otimes\, \mathbb{Z}\,\varphi(\varepsilon_d)$$

Nach Lemma 7.2 ist dann aber $\varphi(\mathcal{O}_K^\times)$ ein Gitter im $\mathbb{R}$-Erzeugnis $< \varphi(\varepsilon_1), \ldots, \varphi(\varepsilon_d) >_{\mathbb{R}}$ der $\varphi(\varepsilon_i)$ in H. Damit müssen wir noch zeigen, dass $d = r + s - 1$ ist, dann ist $\varphi(\mathcal{O}_K^\times)$ ein Gitter in H nach Bemerkung 8.4. Auch diesen Beweis spalten wir in einige leichtere Aussagen auf:

Lemma 8.7 *Fixiere ein beliebiges $\tau \in \Sigma$, dann gibt es für alle Zahlen $\alpha \in \mathcal{O}_K \setminus\{0\}$ eine ganz-algebraische Zahl $\beta \in \mathcal{O}_K \setminus\{0\}$ mit*

$$\big|N_{\mathbb{Q}}^K(\beta)\big| \;\leq\; \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D_K|}$$

und

$$\log\big|\sigma(\beta)\big| \;<\; \log\big|\sigma(\alpha)\big| \qquad \text{für alle } \sigma \in \Sigma\setminus\{\tau, \overline{\tau}\}$$

Beweis. Definiere für alle $\sigma \in \Sigma$ reelle Zahlen $c_\sigma \in \mathbb{R}_+$ mit

(i) $c_\sigma \;=\; c_{\overline{\sigma}}$

(ii) Für alle $\sigma \in \Sigma\setminus\{\tau, \overline{\tau}\}$ gelte $0 \;<\; c_\sigma \;<\; \log|\sigma(\alpha)|$

(iii) Für das Produkt gilt

$$C \;:=\; \prod_{\sigma\in\Sigma} c_\sigma \;=\; \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D_K|}$$

Durch diese Bedingungen werden auch c_τ und $c_{\overline{\tau}}$ eindeutig bestimmt. Setze weiter

$$X \;:=\; \big\{\, (z_\sigma)_{\sigma\in\Sigma} \in K_{\mathbb{R}} \,\big|\, |z_\sigma| < c_\sigma \text{ für alle } \sigma \in \Sigma \,\big\}$$

dann erhalten wir die Gleichung

$$vol_{K_{\mathbb{R}}}(X) \;=\; 2^s \cdot vol_{\mathbb{R}^n}(\tilde{X})$$

mit einem in $\mathbb{R}^n$ verallgemeinertem Zylinder

$$\tilde{X} \;:=\; \left\{ (x_\sigma)_{\sigma\in\Sigma} \in \mathbb{R}^n \;\middle|\; \begin{array}{ll} |x_\sigma| \;<\; c_\sigma & \text{falls } \sigma \text{ reell} \\ x_\sigma^2 + x_{\overline{\sigma}}^2 \;<\; c_\sigma^2 & \text{falls } \sigma \text{ komplex} \end{array} \right\}$$

Aus der reellen Analysis kennen wir $vol_{\mathbb{R}^n}(\tilde{X})$ bereits, damit erhalten wir

$$\begin{aligned} vol_{K_{\mathbb{R}}}(X) \;&=\; 2^s \cdot vol_{\mathbb{R}^n}(\tilde{X}) \;=\; 2^s \cdot \prod_{\substack{\sigma\in\Sigma \\ \sigma \text{ reell}}} 2c_\sigma \cdot \prod_{\substack{\sigma\in\Sigma \\ \sigma \text{ komplex}}} c_\sigma \\ &=\; 2^{s+r} \cdot c \cdot \pi^s \;=\; 2^{2s+r} \cdot \sqrt{|D_K|} \;=\; 2^n \cdot vol\big(j(\mathcal{O}_K)\big) \end{aligned}$$

Mit dem Satz von Minkowski II 7.15 folgt nun die Existenz von β. □

Übungsaufgabe 3 *Sei K ein Zahlkörper über $\mathbb{Q}$. Zeigen Sie:*
Für $a \in \mathbb{N}$ gibt es nur endlich viele $\mathfrak{a} \lhd \mathcal{O}_K$ mit $\mathbb{N}(\mathfrak{a}) = a$.

Lemma 8.8 *Fixiere ein beliebiges $\tau \in \Sigma$, dann gibt es ein $u \in \mathcal{O}_K^\times$ mit*

$$\log|\sigma(u)| \;<\; 0 \qquad \text{für alle } \sigma \in \Sigma\backslash\{\tau, \overline{\tau}\}$$

Beweis. Wenn wir das vorangegangene Lemma 8.7 successive anwenden erhalten wir eine Folge $\alpha_1, \alpha_2, \ldots \in \mathcal{O}_K^\times$ mit

$$(1) \qquad \big|N_{\mathbb{Q}}^K(\alpha_i)\big| \;\leq\; \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D_K|} =: C \qquad \text{für } i = 1, 2, \ldots$$

$$(2) \qquad \log|\sigma(\alpha_i)| \;>\; \log|\sigma(\alpha_{i+1})| \qquad \text{für } i = 1, 2, \ldots \text{ und alle } \sigma \in \Sigma\backslash\{\tau, \overline{\tau}\}$$

Wegen $\mathbb{N}((a)) = N_{\mathbb{Q}}^K$ und (1) sind die Normen der Hauptideale (α_i) für alle $i = 1, 2 \ldots$ durch C nach oben beschränkt. Nach Übungsaufgabe 3 gibt es nur endlich viele Ideale $\mathfrak{a} \lhd \mathcal{O}_K$ deren Norm kleiner oder gleich C ist. Also gibt es $\hat{i} \in \mathbb{N}$, so dass für $\hat{i} < j$ gilt

$$(\alpha_{\hat{i}}) \;=\; (\alpha_j)$$

Wenn zwei Hauptideale gleich sind gibt es aber eine Einheit $u \in \mathcal{O}_K^\times$ mit $\alpha_j = u \cdot \alpha_{\hat{i}}$. Nach (2) gilt dann aber

$$\log|\sigma(u)| \;=\; \log|\sigma(\alpha_j)| \,-\, \log|\sigma(\alpha_{\hat{i}})| \;<\; 0 \qquad \text{für alle } \sigma \in \Sigma\backslash\{\tau, \overline{\tau}\}$$

□

Übungsaufgabe 4 *Seien $n, m \in \mathbb{N}$ natürliche Zahlen und $A := (a_{i,j}) \in \mathrm{Mat}_{m\times n}(\mathbb{R})$ eine Matrix mit*

$$(1) \qquad a_{i,i} > 0 \qquad \text{für alle } i = 1, \ldots, \min\{m, n\}$$

$$(2) \qquad a_{i,j} < 0 \qquad \text{für alle } i = 1, \ldots, m \text{ und } j = 1, \ldots, n \text{ mit } i \neq j$$

$$(3) \qquad \sum_{i=1}^{m} a_{i,j} = 0 \qquad \text{für alle } j = 1, \ldots, n$$

Zeigen Sie: Dann gilt $rg(A) \;=\; m - 1$

Satz 8.9 *Die Menge $\varphi(\mathcal{O}_K^\times) \;=\; l\big(j(\mathcal{O}_K^\times)\big)$ ist ein Gitter in H.*

Beweis. Wir betrachten noch einmal die Menge der Einbettungen von K nach $\mathbb{C}$ genauer:

$$\Sigma \;=\; \big\{\underbrace{\sigma_1, \ldots, \sigma_r}_{reell}, \underbrace{\tau_1, \overline{\tau}_1, \ldots, \tau_n, \overline{\tau}_n}_{komplex}\big\}$$

Mit dem vorangegangenen Lemma 8.7 gibt es dann Einheiten $\varepsilon_1, \ldots \varepsilon_{r+s} \in \mathcal{O}_K^\times$ so dass die Matrix

$$A \;:=\; \begin{pmatrix} \log|\sigma_1(\varepsilon_1)| & \log|\sigma_1(\varepsilon_2)| & \cdots & \log|\sigma_1(\varepsilon_{r+s})| \\ \vdots & \vdots & & \vdots \\ \log|\sigma_r(\varepsilon_1)| & \log|\sigma_r(\varepsilon_2)| & \cdots & \log|\sigma_r(\varepsilon_{r+s})| \\ \log|\tau_1(\varepsilon_1)| & \log|\tau_1(\varepsilon_2)| & \cdots & \log|\tau_1(\varepsilon_{r+s})| \\ \vdots & \vdots & & \vdots \\ \log|\tau_s(\varepsilon_1)| & \log|\tau_s(\varepsilon_2)| & \cdots & \log|\tau_s(\varepsilon_{r+s})| \end{pmatrix}$$

Die Eigenschaften (1), (2) und (3) von Übungsaufgabe 4 erfüllt. Damit folgt nun

$$\mathrm{rg}(A) \;=\; r+s-1$$

Und damit folgt aus Dimensionsgründen

$$H \;=\; <\varphi(\varepsilon_1),\ldots,\varphi(\varepsilon_{r+s-1})>_{\mathbb{R}}$$

Also enthält $\varphi(\mathcal{O}_K^\times)$ eine Basis von H. Nach Lemma 8.6 ist $\varphi(\mathcal{O}_K^\times)$ diskret in H. Insgesamt folgt dann mit Lemma 7.2 die Behauptung. □

Wir haben nun den Dirichletschen Einheitssatz 8.5 gezeigt. Dieser besagt, dass für die Einheitengruppe des Ganzheitsringes

$$\mathcal{O}_K^\times \;\cong\; \mu(K)\times\mathbb{Z}^{r+s-1} \qquad (*)$$

gilt. Wobei r die Anzahl der reellen einbettungen von K in $\mathbb{C}$ und s die Anzahl der Paare von komplexen Einbettungen von K in $\mathbb{C}$ ist. Weiter bezeichnet $\mu(K)$ die Gruppe der Einheitswurzeln in K. Aus $(*)$ erhalten wir, dass es $\varepsilon_1,\ldots,\varepsilon_{r+s-1}\in\mathcal{O}_K^\times$ git, so dass es für jede Einheit $u\in\mathcal{O}_K^\times$ eindeutig bestimmte $n_1,\ldots,n_{r+s-1}\in\mathbb{Z}$ und $\zeta\in\mu(K)$ gibt mit

$$u \;=\; \zeta\cdot\prod_{i=1}^{r+s-1}\varepsilon_i^{n_i}$$

Definition 8.10 *(Grundeinheit)*
Eine Einheit $\varepsilon\in\mathcal{O}_K^\times$ heißt Grundeinheit, falls gilt

$$<\pm\varepsilon^z \mid z\in\mathbb{Z}> \;=\; \mathcal{O}_K^\times$$

Anmerkung Ist $\varepsilon\in\mathcal{O}_K^\times$ eine Grundeinheit, dann sind $-\varepsilon$, $\frac{1}{\varepsilon}$ und $-\frac{1}{\varepsilon}$ die anderen Grundeinheiten.

Beispiel 25 *(Quadratische Körper)*
Sei $K=\mathbb{Q}(\sqrt{d})$ für ein $d\in\mathbb{Z}$ quadratfrei. Es gilt

$$\mu(K) \;=\; \mu\big(\mathbb{Q}(\sqrt{d})\big) \;=\; \begin{cases} \{\pm1,\pm i\} & \text{falls } d=-1 \\ \{\pm1,\pm\omega,\pm\omega^2\} & \text{falls } d=-3 \text{ mit } \omega=e^{\frac{2\pi i}{3}} \\ \{\pm1\} & \text{sonst}\end{cases}$$

Sei ζ eine Einheitswurzel von der Form $\zeta = e^{\frac{2\pi i}{n}}$. Aus Algebra I wissen wir, dass dann für die Eulersche-φ-Funktion gilt

$$\varphi(n) \;=\; \big[\mathbb{Q}(\zeta):\mathbb{Q}\big]$$

Ist $\zeta\in\mu(K)$, dann ist $\varphi(n)\le 2$. Was können wir nun für n schließen? Sei

$$n \;=\; p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$$

die Primfaktorzerlegung von n, dann gilt

$$\begin{aligned}\varphi(n) &= n\cdot\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}(p_1-1)\cdots p_k^{\alpha_k-1}(p_k-1) \;\le\; 2\end{aligned}$$

Diese Ungleichung kann aber nur erfüllt werden, wenn $n\in\{2,3,4\}$ ist. Damit können wir die Einheiten im Ganzheitsring $\mathcal{O}_K$ näher bestimmen.

Fall ($d < 0$): *In diesem Fall gibt es keine reelle Einbettung von K nach $\mathbb{C}$ und wir erhalten $r = 0$ und $s = 1$. Mit dem Dirichletschen Einheitssatz 8.5 gilt dann*

$$\mathcal{O}_K^\times \;\cong\; \mu(K) \times \mathbb{Z}^{r+s-1} \;=\; \mu(K) \times \mathbb{Z}^{0+1-1} \;=\; \mu(K)$$

Fall ($d > 0$): *In diesem Fall gibt es keine komplexen Einbettungen, also folgt $r = 2$ und $s = 0$. Weiter haben wir gesehen, dass für $d \notin \{-1, -3\}$ gilt $\mu(K) = \{\pm 1\}$ Mit dem Dirichletschen Einheitssatz 8.5 gilt dann*

$$\mathcal{O}_K^\times \;\cong\; \mu(K) \times \mathbb{Z}^{r+s-1} \;=\; \{\pm 1\} \times \mathbb{Z}^{2+0-1} \;=\; \{\pm 1\} \times \mathbb{Z}$$

Es gibt also insbesondere eine Grundeinheit ε in $\mathcal{O}_K^\times$, das heißt für jedes $u \in \mathcal{O}_K^\times$ gibt es ein $m \in \mathbb{Z}$ mit $u = \varepsilon^m$ oder $u = -\varepsilon^m$. Wir wollen nun die Grundeinheiten in $\mathcal{O}_K$ bestimmen Da $d > 0$ ist, ist $K \subseteq \mathbb{R}$ ein Unterkörper und d ist die positive Nullstelle von $X^2 - d$. Wir betrachten nun wieder bekannte Fallunterscheidungen modulo 4:

$d \equiv 2, 3\ (4)$: *Wir wissen schon, dass in diesem Fall $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ gilt. Weiter haben wir*

$$\begin{aligned} \mathcal{O}_K^\times &= \left\{ \lambda \in \mathcal{O}_K \;\middle|\; N_{\mathbb{Q}}^K(\lambda) \in \{\pm 1\} \right\} \\ &= \left\{ x + \sqrt{d}\, y \;\middle|\; x, y \in \mathbb{Z} \wedge |x^2 - dy^2| = 1 \right\} \end{aligned}$$

Wie finden wir nun die Grundeinheiten? Angenommen $\varepsilon = a + \sqrt{d}\, b$ mit $a, b \in \mathbb{N}$ wäre so eine Grundeinheit. Für $m \in \mathbb{Z}$ schreibe $\varepsilon^m =: a_m + \sqrt{d}\, b_m$, dann ist

$$b_{m+1} \;=\; ba_m + b_m a \;\Rightarrow\; b_{m+1} - b_m \;=\; ba_m + b_m(a-1) \;>\; 0$$

Algorithmus zur Bestimmung der Grundeinheiten in $\mathbb{Q}(\sqrt{d})$ mit $d \equiv 2, 3\ (4)$:

1. *Teste für $b = 1, 2, 3, \ldots$ ob $db^2 + 1$ oder $db^2 - 1$ ein Quadrat in $\mathbb{Z}$ ist.*
2. *Ist $db^2 + 1$ [bzw. $db^2 - 1$] ein Quadrat in $\mathbb{Z}$, so setze $a^2 := db^2 + 1$ [bzw. $a^2 := db^2 - 1$]*
3. *$\varepsilon = a + \sqrt{d}\, b$ ist eine Grundeinheit in $\mathcal{O}_K^\times$*

Mit der Anmerkung nach Definition 8.10 sind somit alle Grundeinheiten bestimmt.

***Beispiel** (Bestimmung von Grundeinheiten)*
Sei $d = 2$ dann teste $b = 1$. Es gelten

$$db^2 + 1 \;=\; 2 \cdot 1 + 1 = 3 \quad \text{und} \quad db^2 - 1 \;=\; 2 \cdot 1 - 1 = 1$$

also ist $db^2 + 1$ kein Quadrat in $\mathbb{Z}$ aber $db^2 - 1$ ist ein Quadrat. Setze also $a = 1$, dann ist $\varepsilon = a + \sqrt{d}\, b \;=\; 1 + \sqrt{2}$ eine Grundeinheit in $\mathbb{Z}[\sqrt{2}]^\times$.
Sei nun $d = 3$. Teste $b = 1$. Es gilt

$$db^2 + 1 \;=\; 3 \cdot 1 + 1 = 4 = 2^2$$

ist ein Quadrat in $\mathbb{Z}$. Setze also $a = 2$, dann ist dann ist $\varepsilon = a + \sqrt{d}\, b \;=\; 2 + \sqrt{3}$ eine Grundeinheit in $\mathbb{Z}[\sqrt{3}]^\times$.

$d \equiv 1\ (4)$**:** *Auch in diesem Fall haben wir den Ganzheitsring schon bestimmt. es gilt*

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] = \left\{ \frac{x+\sqrt{d}\,y}{2} \,\middle|\, x,y \in \mathbb{Z} \wedge x \equiv y\ (2) \right\} \\ &= \left\{ \frac{x-y}{2} + y\frac{\sqrt{d}+1}{2} \,\middle|\, x,y \in \mathbb{Z} \wedge x \equiv y\ (2) \right\}\end{aligned}$$

Wie im vorangegangen Fall wollen wir nun die Grundeinheiten bestimmen. Sei also

$$\varepsilon := \frac{1}{2} \cdot (a + \sqrt{d}\,b) \quad \text{mit } a,b \in \mathbb{Z}_+ \text{ und } a \equiv b\ (2)$$

eine Grundeinheit, dann setze wieder

$$\varepsilon^m =: \frac{1}{2^m} \cdot (a_m + \sqrt{d}\,b_m)$$

Mit der gleichen Rechnung wie oben erhalten wir auch hier $b_{m+1} > b_m$. Und für die Einheiten erhalten wir die Beschreibung

$$\begin{aligned}\mathcal{O}_K^\times &= \left\{ \lambda \in \mathcal{O}_K \,\middle|\, N_{\mathbb{Q}}^K(\lambda) \in \{\pm 1\} \right\} \\ &= \left\{ \frac{x+\sqrt{d}\,y}{2} \,\middle|\, x,y \in \mathbb{Z} \ \wedge\ |x^2 - dy^2| = 4 \ \wedge\ x \equiv y\ (2) \right\}\end{aligned}$$

Algorithmus zur Bestimmung der Grundeinheiten in $\mathbb{Q}(\sqrt{d})$ mit $d \equiv 1\ (4)$:

1. *Teste für $b = 1, 2, 3, \ldots$ ob $db^2 + 4$ oder $db^2 - 4$ ein Quadrat in $\mathbb{Z}$ ist.*
2. *Ist $db^2 + 4$ [bzw. $db^2 - 4$] ein Quadrat in $\mathbb{Z}$, so setze $a^2 := db^2 + 4$ [bzw. $a^2 := db^2 - 4$]*
3. *$\varepsilon = \frac{a+\sqrt{d}\,b}{2}$ ist eine Grundeinheit in $\mathcal{O}_K^\times$*

Mit der Anmerkung nach Definition 8.10 sind somit alle Grundeinheiten bestimmt.

***Beispiel** (Bestimmung von Grundeinheiten)*
Sei $d = 5$ dann teste $b = 1$. Es gilt

$$db^2 + 4 = 5 \cdot 1 + 4 = 9 = 3^2$$

Setze also $a := 3$, dann ist $\varepsilon = \frac{3+\sqrt{5}}{2}$ eine Grundeinheit.

Folgerung 8.11 *Für eine in $\mathbb{Z}$ quadratfreie Zahl $d \in \mathbb{N}$ mit $d \equiv 2, 3\ (4)$ sind die in $\mathbb{Z}$ liegenden Lösungen der Gleichung $|x^2 - dy^2| = 1$ gegeben durch*

$$|x + \sqrt{d}\,y| = (a + \sqrt{d}\,b)^m$$

für ein $m \in \mathbb{Z}$.

Beweis. Die Aussage folgt direkt aus dem entsprechenden Fall des vorangegangenen Beispiels. □

Bemerkung 8.12 *Sei $K = \mathbb{Q}(\sqrt{d})$ für ein $d \in \mathbb{N}$ quadratfrei. Bezeichne $D := D_K$ die Diskriminante von K, dann gilt*

$$\mathcal{O}_K^\times = \left\{ \frac{t+\sqrt{D}\,u}{2} \,\middle|\, t,u \in \mathbb{Z} \ \wedge\ |t^2 - Du^2| = 4 \right\}$$

Beweis. Wir haben bereits gezeigt, dass

$$D \;:=\; D_K \;=\; \begin{cases} 4d & \text{falls } d \equiv 2,3 \ (4) \\ d & \text{falls } d \equiv 1 \ (4) \end{cases}$$

Damit ist im Fall $d \equiv 1 \ (4)$ nichts mehr zu zeigen. Für $d \equiv 2,3 \ (4)$ ist t wegen

$$|t^2 - 4du^2| \;=\; 4$$

durch 2 teilbar und es gilt

$$N_{\mathbb{Q}}^K\Big(\frac{t+\sqrt{D}\,u}{2}\Big) \;=\; N_{\mathbb{Q}}^K\Big(\frac{t}{2}+u\sqrt{d}\Big) \;=\; \Big(\frac{t}{2}\Big)^2 - du^2 \;\in\; \{\pm 1\}$$

□

Beispiel 26 *Bestimme alle Lösungen $(x,y) \in \mathbb{Z}^2$ der Gleichung*

$$x^2 - 2y^2 \;=\; 7$$

Wir wollen diese Problemstellung so interpretieren, dass wir sie in den uns jetzt bekannten Ringen untersuchen können. Eine geeignete Umformung des Problems wäre also:
Bestimme alle Elemente $x+\sqrt{2}\,y \in \mathbb{Z}[\sqrt{2}]$ mit

$$N_{\mathbb{Q}}^k\big(x+\sqrt{2}\,y\big) \;=\; 7 \;=\; \mathbb{N}\big((x+\sqrt{2}\,y)\big)$$

Wir betrachten also Elemente in $K=\mathbb{Q}(\sqrt{2})$. Da 7 eine Primzahl ist betrachte zunächst das von 7 in $\mathcal{O}_K$ aufgespannte Ideal:

$$7\,\mathcal{O}_K \;=\; (3+\sqrt{2})\cdot(3-\sqrt{2})$$

Also enthält die Menge

$$\big\{\, u\cdot(3+\sqrt{2}), u\cdot(3-\sqrt{2}) \,\big|\, u \in \mathcal{O}_K^\times \;\wedge\; N_{\mathbb{Q}}^K(u)=1 \,\big\}$$

alle gesuchten Lösungen. Im vorangegangenen langen Beispiel haben wir gezeigt, dass $\varepsilon = 1+\sqrt{2}$ eine Grundeinheit von $\mathbb{Z}[\sqrt{2}]^\times$ ist. Damit ist

$$\big\{\, u\cdot(3+\sqrt{2}), u\cdot(3-\sqrt{2}) \,\big|\, u \in \{\pm(1+\sqrt{2})^n \,|\, n \text{ gerade } \} \,\big\}$$

die gesuchte Lösungsmenge, denn für gerades n gilt

$$N_{\mathbb{Q}}^K(u) \;=\; N_{\mathbb{Q}}^K\big((1+\sqrt{2})^n\big) \;=\; N_{\mathbb{Q}}^K(1+\sqrt{2})^n \;=\; (-1)^n \;=\; 1$$

Wir wollen als nächstes den Regulator von einem endlichen Erweiterungskörper $K/\,\mathbb{Q}$ einführen. Für dessen Herleitung betrachte wieder die Abbildung

$$\varphi : \mathcal{O}_K^\times \;\hookrightarrow\; K^* \;\xrightarrow{\;j\;}\; \big(K\otimes_{\mathbb{Q}}\mathbb{R}\big)^\times \;\xrightarrow{\;l\;}\; \Big(\bigoplus_{\sigma\in\Sigma}\mathbb{R}\Big)^{\mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R})} \;\xrightarrow{\sim}\; \mathbb{R}^{r+s}$$

Wir haben die Menge

$$H \;=\; \ker\Big[Tr:\Big(\bigoplus_{\sigma\in\Sigma}\mathbb{R}\Big)^{\mathrm{Gal}(\mathbb{C}\,/\,\mathbb{R})} \to \mathbb{R}\Big]$$

eingeführt und in Satz 8.9 gezeigt, dass $\varphi(\mathcal{O}_K^\times)$ ein Gitter in $H \subseteq \mathbb{R}^{r+s}$ ist. Auf dem $\mathbb{R}$-Vektorraum $\mathbb{R}^{r+s}$ haben wir das standart Skalarprodukt $< \cdot, \cdot >$. Durch Einschränkung dieses Skalarproduktes auf H wird $(H, < \cdot, \cdot >_{|H})$ zu einem euklidischen Raum. Wir können also Mengen in H messen. Seien nun $\varepsilon_1, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ so, dass

$$\varphi(\mathcal{O}_K^\times) \;=\; \mathbb{Z}\,\varphi(\varepsilon_1) + \ \ldots\ + \mathbb{Z}\,\varphi(\varepsilon_{r+s-1})$$

Setze $\lambda := \frac{1}{\sqrt{r+s}} \cdot (1, \ldots, 1) \in \mathbb{R}^{r+s}$, dann ist $< \lambda, \lambda >= 1$ und das Erzeugnis $< \lambda >_{\mathbb{R}}$ von λ über $\mathbb{R}$ steht senkrecht auf H, das heißt für alle $x \in < \lambda >_{\mathbb{R}}$ und alle $h \in H$ gilt $< x, h >= 0$. Definiere weiter die Matrix

$$M \;:=\; \begin{pmatrix} \lambda_1 & \varphi(\varepsilon_1)_1 & \cdots & \varphi(\varepsilon_{r+s-1})_1 \\ \vdots & \vdots & & \vdots \\ \lambda_{r+s} & \varphi(\varepsilon_1)_{r+s} & \cdots & \varphi(\varepsilon_{r+s-1})_{r+s} \end{pmatrix} \in \mathrm{Mat}_{r+s\times r+s}(\mathbb{R})$$

Definition 8.13 *(Minoren)*
Sei $A \in \mathrm{Mat}_{n\times m}(\mathbb{R})$ eine Matrix, dann bezeichne $A^{i,j}$ die $n-1 \times m-1$ Untermatrix von A, die durch streichen der i-ten Zeile und j-ten Spalte aus A entsteht. Wir nennen diese Unermatrizen auch die Minoren von A.

Betrachte nun

$$\begin{aligned} vol_H\big(\,\varphi(\mathcal{O}_K^\times)\,\big) &= vol_H\Big(\Big\{\sum_{i=1}^{r+s} t_i\,\varphi(\varepsilon_i)\;\Big|\; 0 \le t_i \le 1\Big\}\Big) \\ &= vol_{\mathbb{R}^{r+s}}\Big(\Big\{\sum_{i=1}^{r+s-1} t_i\,\varphi(\varepsilon_i) + t_0\lambda\;\Big|\; 0 \le t_i \le 1\Big\}\Big) \\ &= \big|\det(M)\big| \end{aligned}$$

Wähle ein $i \in \{1, \ldots, r+s\}$ beliebig und fixiere in M die i-te Spalte. Addiere nun alle anderen Zeilen einmal zur i-ten Zeile hinzu, dann erhalten wir die Matrix

$$\tilde{M} \;:=\; \begin{pmatrix} \lambda_1 & \varphi(\varepsilon_1)_1 & \cdots & \varphi(\varepsilon_{r+s-1})_1 \\ \vdots & \vdots & & \vdots \\ \lambda_{i-1} & \varphi(\varepsilon_1)_{i-1} & \cdots & \varphi(\varepsilon_{r+s-1})_{i-1} \\ \frac{r+s}{\sqrt{r+s}} & 0 & \cdots & 0 \\ \lambda_{i+1} & \varphi(\varepsilon_1)_{i+1} & \cdots & \varphi(\varepsilon_{r+s-1})_{i+1} \\ \vdots & \vdots & & \vdots \\ \lambda_{r+s} & \varphi(\varepsilon_1)_{r+s} & \cdots & \varphi(\varepsilon_{r+s-1})_{r+s} \end{pmatrix} \in \mathrm{Mat}_{r+s\times r+s}(\mathbb{R})$$

wobei aber die Determinanten von M und $\tilde{M}$ gleich sind und es gilt

$$\big|\det(M)\big| \;=\; \big|\det(\tilde{M})\big| \;=\; \big|\sqrt{r+s}\big| \cdot \Big|\prod_{j=1}^{r+s} \det(M^{i,j})\Big|$$

Mit diesem Maß für das Gitter $\varphi(\mathcal{O}_K^\times)$ in H haben wir die Herleitung des Regulators abgeschlossen:

Definition 8.14 *(Regulator von K)*
Wir nennen

$$R_K \;:=\; \frac{vol\Big(H \big/ \varphi(\mathcal{O}_K^\times)\Big)}{\sqrt{r+s}}$$

den Regulator von K.

Beispiel 27 *Wir betrachten wieder einen quadratischen Körper $K := \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}_+$ quadratfrei. Dann vereinfacht sich die Abbildung φ zu*

$$\begin{array}{rccccc} \varphi : \mathcal{O}_K^\times & \to & K^* & \hookrightarrow & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}^2 \\ & & \lambda & \mapsto & \big(\sigma_1(\lambda),\sigma_2(\lambda)\big) & & \\ & & & & (x,y) & \mapsto & \big(\log|x|,\log|y|\big) \end{array}$$

Denn $\sharp\Sigma = 2$. Fixiere nun eine Grundeinheit $\varepsilon \in \mathcal{O}_K^\times$, dann ist

$$\varphi(\varepsilon) \;=\; \Big(\log\big|\sigma_1(\varepsilon)\big|, \log\big|\sigma_2(\varepsilon)\big|\Big) \;\in\; H \;=\; \big\{(x,-x)\,\big|\,x\in\mathbb{R}\,\big\}$$

Wir wissen bereits, dass $r = 2$ und $s = 0$ gilt. Für die Matrix M gilt damit

$$M \;=\; \begin{pmatrix} \frac{1}{\sqrt{2}} & \log\big|\sigma_1(\varepsilon)\big| \\ \frac{1}{\sqrt{2}} & \log\big|\sigma_2(\varepsilon)\big| \end{pmatrix}$$

Und wir erhalten den Regulator

$$R_K \;=\; R_{\mathbb{Q}(\sqrt{d})} \;=\; \Big|\log\big|\sigma_1(\varepsilon)\big|\Big| \;=\; \Big|\log\big|\sigma_2(\varepsilon)\big|\Big|$$

Konkret gilt zum Beispiel für $d = 2$

$$R_K \;=\; R_{\mathbb{Q}(\sqrt{2})} \;=\; \log\big(1+\sqrt{2}\big)$$

Kapitel IV

Primzahlen und Primideale

9 Lokalisierung und lokale Ringe

In diesem Abschnitt wollen wir die Konstruktion des Quotientenkörper verallgemeinern. Dabei erhalten wir Ringe, die nur ein einziges maximales Ideal enthalten und in diesem Sinne einfacher als die Ursprungsringe sind. Weiter können wir viele Eigenschaften „lokal“ nachweisen, d.h. wenn die Eigenschaft auf allen Lokalisierungen gilt, dann gilt sie auch auf dem Ursprungsring und umgekehrt.

Definition 9.1 *(Multiplikatives System)*
Sei A ein Ring. Eine Menge $S \subset A$ heißt multiplikativ oder multiplikatives System in A, falls gelten

(i) $1_A \in S$

(ii) *Für alle $x, y \in S$ ist auch $x \cdot y \in S$.*

Beispiel 28 *Sei A ein Ring.*

- *Sei $f \in A$, dann ist $S = \{1, f, f^2, \ldots\}$ multiplikativ.*
- *Sei $\wp \in \mathrm{Spec}(A)$, dann ist $S = A \backslash \wp$ multiplikativ.*
- *Die Mengen $\{0, 1\}$, A sind multiplikativ.*

Konstruktion 9.2 *(Lokalisierung von Ringen)*
Sei A ein Ring und $S \subseteq A$ dann definiere eine Äquivalenzrelation[1] *auf $A \times S$ via*

$$(a, s) \sim (b, t) \quad :\Leftrightarrow \quad \exists u \in S : \; u(at - bs) = 0$$

Die Äquivalenzklassen (a, s) bezüglich dieser Relation bezeichnen wir mit $\frac{a}{s}$ und die Menge aller Äquivalenzklassen mit $S^{-1}A$. Mit den Abbildungen

$$\begin{array}{rcl} + : S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ \left(\frac{a}{s}, \frac{b}{t}\right) & \mapsto & \frac{at + bs}{st} \end{array}$$

und

$$\begin{array}{rcl} \cdot : S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ \left(\frac{a}{s}, \frac{b}{t}\right) & \mapsto & \frac{ab}{st} \end{array}$$

wird $S^{-1}A$ zu einem Ring. Für die Wohldefiniertheit der Abbildungen $+$ und $\cdot$ ist wie üblich die Unabhängigkeit von der Wahl der Vertreter in den Äquivalenzklassen zu zeigen. Dies lässt sich unter Verwendung der Definition der Äquivalenzrelation aber leicht nachrechnen.
Wir nennen $S^{-1}A$ die Lokalisierung von A in S.

Bemerkung 9.3 *Sei A ein Ring und $S \subseteq A$ ein multiplikatives System mit $0 \in S$, dann ist $S^{-1}A$ der Nullring.*

Beweis. Ist $0 \in S$, so ist die Bedingung $u(at - bs) = 0$ für alle $a, b \in A$ und alle $t, s \in S$ mit $u = 0$ erfüllt, also enthält der Ring $S^{-1}A$ nur ein Element. □

Anmerkung Diese Konstruktion verallgemeinert tatsächlich die Quotientenkörper, denn ist A ein Integritätsring und ist $S = A\backslash\{0\}$, so ist die Bedingung, dass es ein $u \in S$ mit $u(at - bs) = 0$ gibt, Äquivalent dazu, dass $(at - bs) = 0$ ist.

Bemerkung 9.4 *Sei A ein Integritätsring und $S = A\backslash\{0\}$ sowie $T \subset S$ zwei multiplikative Systeme, dann gilt*

$$A \; \subset \; T^{-1}A \; \subset \; \mathrm{Quot}(A) = S^{-1}A$$

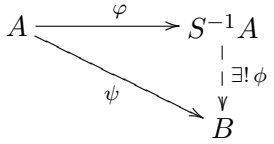
Insbesondere ist also $T^{-1}A$ nullteilerfrei.

Lemma 9.5 *Sei A ein Ring und $S \subseteq A$ multiplikativ. Die Abbildung*

$$\begin{array}{rcl} \varphi : A & \to & S^{-1}A \\ a & \mapsto & \frac{a}{1} \end{array}$$

[1] Es lässt sich leicht Nachrechnen, dass die hier definierte Relation tatsächlich eine Äquivalenzrelation ist.

hat den Kern $\{\, a \in A \,|\, \exists u \in S \,:\, ua = 0 \,\}$*. Insbesondere ist diese Abbildung im allgemeinen oft nicht injektiv!*
Desweiteren besitzt diese Abbildung eine universelle Eigenschaft. Das heißt für alle A*-Algebren* B *mit Ringhomomorphismus* $\psi : A \to B$*, für welchen* $\psi(S) \subseteq B^\times$ *gilt, gibt es einen eindeutig bestimmten Ringhomomorphismus* $\phi : S^{-1}A \to B$ *mit* $\phi \circ \varphi = \psi$*. Mit anderen Worten: Das untenstehende Diagramm kommutiert*



Beweis. Betrachte zunächst den Kern von φ es gilt

$$\begin{aligned} a \in \mathrm{Ker}(\varphi) \quad &\Leftrightarrow \quad \frac{a}{1} \;=\; \frac{0}{1} \text{ in } S^{-1}A \\ &\Leftrightarrow \quad \exists\, u \in S \,:\, u(1 \cdot a - 0) \;=\; ua \;=\; 0 \end{aligned}$$

Für den Nachweis der universellen Eigenschaft setze

$$\phi\Big(\frac{a}{s}\Big) \;:=\; \psi(a) \cdot \big(\psi(s)\big)^{-1}$$

Diese definition ist wohldefiniert, denn $\psi(S) \subset B^\times$ also gibt es multiplikative inverse zu $\psi(s)$ für $s \in S$. Weiter erfüllt die Abbildung ϕ die Kommutativität des Diagramms, denn

$$\phi \circ \varphi(a) \;=\; \phi\Big(\frac{a}{1}\Big) \;=\; \psi(a) \cdot \big(\psi(1)\big)^{-1} \;=\; \psi(a)$$

□

Konstruktion 9.6 *(Lokalisierung von Moduln)*
Sei A *ein Ring und* $S \subseteq A$ *multiplikativ. Weiter sei* M *ein* A*-Modul, dann definiere eine Äquivalenzrelation auf* $M \times S$ *via*

$$(m, s) \sim (n, t) \;\;:\Leftrightarrow\;\; \exists u \in S :\; u(mt - ns) = 0_M$$

Die Äquivalenzklassen (m, s) *bezüglich dieser Relation bezeichnen wir mit* $\frac{m}{s}$ *und die Menge aller Äquivalenzklassen mit* $S^{-1}M$*. Bezüglich der Abbildung*

$$\begin{aligned} + : S^{-1}M \times S^{-1}M \quad &\to \quad S^{-1}M \\ \Big(\frac{m}{s}, \frac{n}{t}\Big) \quad &\mapsto \quad \frac{mt + ns}{st} \end{aligned}$$

ist $S^{-1}M$ *eine abelsche Gruppe. Diese wird via*

$$\begin{aligned} \cdot : A \times S^{-1}M \quad &\to \quad \S^{-1}M \\ \Big(a, \frac{m}{s}\Big) \quad &\mapsto \quad \frac{am}{s} \end{aligned}$$

zu einem A*-Modul und via*

$$\begin{aligned} \bullet : S^{-1}A \times S^{-1}M \quad &\to \quad S^{-1}M \\ \Big(\frac{a}{s}, \frac{m}{t}\Big) \quad &\mapsto \quad \frac{am}{st} \end{aligned}$$

auch zu einem $S^{-1}A$*-Modul*[2]*.*

[2]Die Wohldefiniertheit der Abbildungen $+, \cdot, \bullet$ ist wie in der vorangegangenen Konstruktion wieder leicht.

Notation 9.7 *Seien A ein Ring und M ein A-Modul.*

- *Für $f \in A$ sei $S := \{1, f, f^2, \ldots\}$. Wir schreiben*

$$A_f \;:=\; S^{-1}A \qquad \text{und} \qquad M_f \;:=\; S^{-1}M$$

- *Für $\wp \in \operatorname{Spec}(A)$ sei $S := A \backslash \wp$. Wir schreiben*

$$A_\wp \;:=\; S^{-1}A \qquad \text{und} \qquad M_\wp \;:=\; S^{-1}M$$

Lemma 9.8 *Seien A ein Ring, $S \subseteq A$ multiplikativ und M, N zwei A-Moduln mit Modulhomomorphismus $f : M \to N$. Dann ist*

$$\begin{array}{rcl} S^{-1}f : S^{-1}M & \to & S^{-1}N \\ \dfrac{m}{s} & \mapsto & \dfrac{f(m)}{s} \end{array}$$

ein Homomorphismus von $S^{-1}A$ Moduln mit

$$\operatorname{Ker}(S^{-1}f) \;=\; S^{-1}\operatorname{Ker}(f) \qquad \text{und} \qquad \operatorname{Im}(S^{-1}f) \;=\; S^{-1}\operatorname{Im}(f)$$

Folgerung 9.9 *Seien A ein Ring, $S \subseteq A$ multiplikativ und ist*

$$0 \;\to\; M_1 \;\to\; M_2 \;\to\; M_3 \;\to\; 0$$

eine kurze exakte Sequenz von A-Moduln, so ist

$$0 \;\to\; S^{-1}M_1 \;\to\; S^{-1}M_2 \;\to\; S^{-1}M_3 \;\to\; 0$$

eine kurze exakte Sequenz von $S^{-1}A$-Moduln.

Notation 9.10 *Sei A ein Ring und $S \subseteq A$ multiplikativ. Bezüglich der Abbildung*

$$\begin{array}{rcl} \varphi : A & \to & S^{-1}A \\ a & \mapsto & \dfrac{a}{1} \end{array}$$

aus Lemma 9.5 setzen wir für Ideale $\mathfrak{a}_S \lhd S^{-1}A$

$$\mathfrak{a}_S \cap A \;:=\; \varphi^{-1}(\mathfrak{a}_S)$$

Lemma 9.11 *Sei A ein Ring und $S \subseteq A$ multiplikativ. Es gelten*

a) *Für alle Ideale $\mathfrak{a}_S \lhd S^{-1}A$ gilt: $S^{-1}(\mathfrak{a}_S \cap A) \;=\; \mathfrak{a}_S$ und die Abbildung*

$$\begin{array}{rcl} \varphi^a : \left\{\, \mathfrak{a}_S \lhd S^{-1}A \,\right\} & \to & \left\{\, \mathfrak{a} \lhd A \,\right\} \\ \mathfrak{a}_S & \mapsto & \varphi^{-1}(\mathfrak{a}_S) =: (\mathfrak{a}_S \cap A) \end{array}$$

injektiv. Insbesondere bildet φ^a Primideale wieder auf Primideale ab.

b) *Sei $\mathfrak{a} \lhd A$ dann sind äquivalent*

- **(i)** *Es gibt ein $\mathfrak{a}_S \lhd S^{-1}A$ mit $\mathfrak{a}_S \cap A \;=\; \mathfrak{a}$*
- **(ii)** *Es gilt $\mathfrak{a} \;=\; S^{-1}\,\mathfrak{a} \cap A$*
- **(iii)** *Die Menge $\pi(S)$ mit $\pi : A \twoheadrightarrow {}^{A}\!/_{\mathfrak{a}}$ ist Nullteilerfrei*

c) *Die Einschränkung von φ^a auf das Primspektrum von $S^{-1}A$ induziert eine Bijektion*

$$\operatorname{Spec}(S^{-1}A) \;\overset{1:1}{\longleftrightarrow}\; \left\{ \wp \in \operatorname{Spec}(A) \,\middle|\, \wp \cap S = \varnothing \right\}$$

Beweis. Für den Nachweis von Teil **(a)** betrachte

$$\mathrm{Ker}(\varphi^a) \;=\; \left\{\; \mathfrak{a}_S \in S^{-1}A \,\middle|\, \varphi^{-1}(\mathfrak{a}_S) = (0) \;\right\} \;=\; (0)$$

also ist φ^a injektiv. Sei nun $\mathfrak{P} \in \mathrm{Spec}(S^{-1}A)$ und sei $ab \in \mathfrak{P} \cap A$. Wegen der Primeigenschaft von $\mathfrak{P}$ sind ist entweder $\varphi(a) \in \mathfrak{P}$ oder $\varphi(b) \in \mathfrak{P}$. Ohne Einschränkung sei $\varphi(a) \in \mathfrak{P}$, dann gilt aber $\varphi^{-1}\left(\varphi(a)\right) = a \in \varphi^{-1}(\mathfrak{P})$, also ist $\mathfrak{P} \cap A$ prim.
Für Teil **(b)** müssen wir Äquivalenzen zeigen. Wir betrachten zunächst den Sonderfall $0 \in S$ und haben nichts zu zeigen, da $S^{-1}A = \{0\}$ als einziges Ideal das Nullideal enthält. Sei also $0 \notin S$, dann ist S in A Nullteilerfrei. Die Implikation „**(ii)** $\Rightarrow$ **(i)**“ ist trivial und die Gegenrichtung folgt aus der Injektivität von φ^a. Wir wollen nun den Schritt von **(ii)** nach **(iii)** betrachten. Im Sonderfall $\mathfrak{a} = A$ ist nichts zu zeigen, sei also ohne Einschränkung $\mathfrak{a} \neq A$. Es gilt $\pi(S)$ ist genau dann Nullteilerfrei, wenn $S \cap \mathfrak{a} = \varnothing$. Angenommen $x \in S \cap \mathfrak{a}$, dann gilt $1 \in S^{-1}\,\mathfrak{a}$ also ist $S^{-1}\,\mathfrak{a} = S^{-1}A$. Nach Voraussetzung gilt

$$\mathfrak{a} \;=\; S^{-1}\,\mathfrak{a} \cap A \;=\; S^{-1}A \cap A \;=\; A$$

Dies ist aber Widersprüchlich, also ist $\mathfrak{a} \cap S = \varnothing$. Wir müssen nun noch von **(iii)** auf **(i)** oder **(ii)** schließen. Nach Voraussetzung ist $\pi(S)$ Nullteilerfrei, also haben S und $\mathfrak{a}$ leeren Schnitt. Betrachte nun

$$\varphi^{-1}(S^{-1}\,\mathfrak{a}) \;=\; \left\{\, a \in A \,\middle|\, \frac{a}{1} \in S^{-1}\,\mathfrak{a} \,\right\} \;=\; \left\{\, a \in A \,\middle|\, \exists\, s \in S \,:\, sa \in \mathfrak{a} \,\right\} \;=\; \mathfrak{a}$$

Für Teil **(c)** ist nach den Teilen **(a)** und **(b)** nichts zu zeigen. □

Bemerkung 9.12 *Sei R ein Ring, dann bezeichnen wir die Menge der endlich erzeugten Ideale von R mit $I(R)$. Diese Menge wird bezüglich $+$ zu einer Gruppe. Ist R noethersch, so sind alle Ideale von R endlich erzeugt.*

Satz 9.13 *Sei A ein Dedekindring und $S \subset A$ eine multiplikative Teilmenge, dann ist auch $S^{-1}A$ dedekindsch. Bezeichne weiter $K = \mathrm{Quot}(A)$ den Quotientenkörper von A, dann ist*

$$S^{-1}\,\mathfrak{a} \;=\; \mathfrak{a}(S^{-1}A) \;=\; \left\{\, \frac{x}{s} \in K \,\middle|\, x \in \mathfrak{a} \wedge s \in S \,\right\}$$

das von $\mathfrak{a} \lhd A$ in $S^{-1}A$ erzeugte Ideal. Ide Abbildung

$$\begin{aligned} loc : I(A) &\;\to\; I(S^{-1}A) \\ \mathfrak{a} &\;\mapsto\; S^{-1}\,\mathfrak{a} \end{aligned}$$

induziert den Isomorphismus

$$I(S^{-1}A) \;\xrightarrow{\sim}\; \left\{\, \wp_1 \cdots \wp_r \,\middle|\, r \in \mathbb{N} \wedge \wp_i \in \mathrm{Spec}(A) \,\wedge\, \wp_i \cap S = \varnothing \,\right\} \leq I(A)$$

Beweis. Wir zeigen zunächst, dass $S^{-1}A$ dedekindsch ist. Dass $S^{-1}A$ noethersch ist folgt sofort aus der entsprechenden Eigenschaft von A und Lemma 9.11 Teil **(b)**. Da A ein Integritätsring ist, gilt

$$A \;\subseteq\; S^{-1}A \;\subseteq\; K \;=\; \mathrm{Quot}(A) \;=\; \mathrm{Quot}(S^{-1}A)$$

Sei nun $x \in K$ ein über $S^{-1}A$ ganzes Element, das heißt es gilt

$$0 \;=\; x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \ldots + \frac{a_1}{s_1}x + \frac{a_0}{s_0} \qquad \text{mit } a_i \in A \text{ und } s_i \in S$$

Dann ist $s_{n-1} \cdots s_1 \cdot s_0 \cdot x$ ganz über A. Da A ganzabgeschlossen ist, gilt sogar $s_{n-1} \cdots s_1 \cdot s_0 \cdot x \in A$ also ist $s_{n-1} \cdots s_1 \cdot s_0 \cdot x \in S^{-1}A$ und damit ist auch $S^{-1}A$ ganz abgeschlossen. Wir müssen nun nurnoch zeigen, dass jedes Primideal undgleich Null von $S^{-1}A$ ein maximales Ideal ist. Sei dazu $\mathfrak{m} \in \mathrm{Spm}(S^{-1}A)$ ein maximales Ideal mit

$$\mathfrak{P} \subseteq \mathfrak{m} \qquad \text{für ein } \mathfrak{P} \in \mathrm{Spec}(S^{-1}A)$$

Die Abbildung φ^a aus Lemma 9.11 ist Inklusionserhaltend, also gilt

$$\mathfrak{P} \cap A \subseteq \mathfrak{m} \cap A$$

Da A dedekindsch ist muss entweder $\mathfrak{P} \cap A = (0)$ sein, und damit folgt nach Lemma 9.11

$$\mathfrak{P} = S^{-1}(\mathfrak{P} \cap A) = (0)$$

oder $\mathfrak{P} \cap A = \mathfrak{m} \cap A$. In diesem Fall folgte aber

$$\mathfrak{p} = S^{-1}(\mathfrak{P} \cap A) = S^{-1}(\mathfrak{m} \cap A) = \mathfrak{m}$$

Damit ist $S^{-1}A$ ein Dedekindring. Wir betrachten nun den zweiten Teil der Aussage. Es gilt loc ist surjektiv, denn sei $\mathfrak{a}_S \in I(S^{-1}A)$, dann ist nach Lemma 9.11 $\mathfrak{a}_S \cap A$ ein Urbild. Betrachte

$$\begin{aligned} \mathrm{Ker}(loc) &= \left\{ \mathfrak{a} \in I(A) \,\middle|\, S^{-1}A = S^{-1}\mathfrak{a} \right\} = \left\{ \mathfrak{a} \in I(A) \,\middle|\, A = (S^{-1}\mathfrak{a}) \cap A \right\} \\ &= \left\{ \mathfrak{a} \in I(A) \,\middle|\, \exists\, a \in \mathfrak{a},\, s \in S : \frac{a}{s} = 1 \right\} = \left\{ \mathfrak{a} \in I(A) \,\middle|\, \mathfrak{a} \cap S \neq \varnothing \right\} \end{aligned}$$

Sei nun U die in $I(A)$ von den Primidealen $\wp \in \mathrm{Spec}(A)$, die mit S leeren Schnitt haben erzeugte Untergruppe, das heißt

$$U := \left\{ \wp_1 \cdots \wp_r \,\middle|\, r \in \mathbb{N} \wedge \wp_i \in \mathrm{Spec}(A) \wedge \wp_i \cap S = \varnothing \right\} \leq I(A)$$

Die Einschränkung von loc auf U ist offensichtlich surjektiv. Es gelten

$$I(A) \cong \bigoplus_{\wp \in \mathrm{Spm}(A)} \mathbb{Z} \quad \text{und} \quad \mathrm{Ker}(loc) \cong \bigoplus_{\substack{\wp \in \mathrm{Spm}(A) \\ \wp \cap S \neq \varnothing}} \mathbb{Z}$$

Mit Teil **(c)** von Lemma 9.11 gilt dann auch

$$I(S^{-1}A) \cong \bigoplus_{\substack{\wp \in \mathrm{Spm}(A) \\ \wp \cap S = \varnothing}} \mathbb{Z}$$

□

Definition 9.14 *(Lokaler Ring)*
Einen Ring R mit nur einem einzigen Maximalideal $\mathfrak{m}$ nennen wir einen lokalen Ring. Wir benutzen die folgenden Schreibweisen:
$(R, \mathfrak{m})$ *für den lokalen Ring mit Maximalideal $\mathfrak{m}$ sowie*
$(R, \mathfrak{m}, \kappa)$ *für $R, \mathfrak{m}$ wie oben und $\kappa = {}^{R}\!/_{\mathfrak{m}}$*

Lemma 9.15 *Sei A ein Ring und $\wp \in \operatorname{Spec}(A)\backslash\{(0)\}$ ein Primideal. Dann ist $A_\wp = S^{-1}A$ mit $S := A\backslash\wp$ ein lokaler Ring. Das maximale Ideal ist das von $\wp$ in $A_\wp$ erzeugte Ideal*

$$\wp A_\wp \;=\; \left\{ \frac{a}{s} \,\middle|\, a \in \wp \,\wedge\, s \in A\backslash\wp \right\}$$

Beweis. nach Lemma 9.11 gibt es eine Bijektion

$$\begin{array}{ccc} \left\{\, \mathfrak{a} \lhd A \,\middle|\, \mathfrak{a} \cap (A\backslash\wp) = \varnothing \,\right\} & \overset{1:1}{\longleftrightarrow} & \left\{\, \mathfrak{b} \lhd A_\wp \,\right\} \\ \mathfrak{a} & \mapsto & \mathfrak{a}\, A_\wp \\ \varphi^a(\mathfrak{b}) & \hookleftarrow & \mathfrak{b} \end{array}$$

Es gilt offensichtlich

$$\mathfrak{a} \cap (A\backslash\wp) \;=\; \varnothing \quad\Leftrightarrow\quad \mathfrak{a} \;\subseteq\; \wp$$

Das heißt jedoch genau, dass alle Ideale von $A_\wp$ in $\wp A_\wp$ enthalten sind. □

Bemerkung 9.16 *Sei A ein Ring und $\mathfrak{m} \lhd A$ ein Ideal. Es gilt: Genau dann ist $(A, \mathfrak{m})$ ein lokaler Ring, wenn $A\backslash\,\mathfrak{m} = A^\times$ ist.*

Beweis. Sei $(A, \mathfrak{m})$ ein lokaler Ring und sei $x \in A\backslash\,\mathfrak{m}$. Dann ist $(x) = A$, denn $(x) \nsubseteq \mathfrak{m}$. Also ist $x \in A^\times$. Sei nun $A\backslash\,\mathfrak{m} = A^\times$ und sei $\mathfrak{a} \lhd A$ mit $\mathfrak{a} \neq A$. Dann ist $\mathfrak{a} \cap A^\times = \varnothing$ also nach Voraussetzung $\mathfrak{a} \subseteq \mathfrak{m}$. □

Lemma 9.17 *Sei A ein Ring und $\wp \in \operatorname{Spec}(A)$, dann gibt es gibt eine injektive Abbildung*

$$A\!\diagup_{\wp} \;\hookrightarrow\; A_\wp\!\diagup_{\wp A_\wp} \;=\; \operatorname{Quot}\left(A\!\diagup_{\wp}\right) \;=:\; \kappa(\wp)$$

und $\left(A_\wp, \wp A_\wp, \kappa(\wp)\right)$ ist ein lokaler Ring. Ist $\wp$ insbesondere maximal, so gilt $A\!\diagup_{\wp} = \kappa(\wp)$.

Beweis. Setze $S := A\backslash\wp$ und sei $\overline{S}$ das Bild von S unter der natürlichen Projektion

$$\pi : A \;\twoheadrightarrow\; A\!\diagup_{\wp}$$

Dann gelten

$$S^{-1}\left(A\!\diagup_{\wp}\right) \;=\; \overline{S}^{\,-1}\left(A\!\diagup_{\wp}\right) \quad \text{und} \quad \overline{S} \;=\; \left(A\!\diagup_{\wp}\right)\backslash\{0\}$$

Da $\wp$ ein Primideal von A ist, ist der Quotient ein Integritätsring und es gibt eine natürliche Inklusion

$$A\!\diagup_{\wp} \;\hookrightarrow\; \operatorname{Quot}\left(A\!\diagup_{\wp}\right)$$

□

Definition 9.18 *(Diskreter Bewertungsring)*
Wir nennen einen lokalen Ring einen diskreten Bewertungsring, wenn er ein Hauptidealring ist. Häufig wird dies mit DVR *für* diskrete valuation ring *abgekürzt.*

Bemerkung 9.19 *Sei $(A, \mathfrak{m})$ ein diskreter Bewertungsring, dann gibt es ein m in A mit $(m) = \mathfrak{m}$ und für alle $x \in A\backslash\{0\}$ gibt es eine Einheit $u \in A^\times$ und ein $n \in \mathbb{N}_0$ so dass $x = u \cdot m^n$.*

Beweis. Wir betrachten zwei Fälle

($x \notin \mathfrak{m}$): Nach Bemerkung 9.16 ist jedes Element $x \in A\backslash\,\mathfrak{m}$ eine Einheit, setze also $n = 0$, dann gilt:

$$x \;=\; x \cdot m^0 \;=\; x \;\in A^\times$$

($x \in \mathfrak{m}$): Es gibt ein $x_1 \in A$ mit $x = x_1 m$. Wir unterscheiden wieder

> **($x \notin \mathfrak{m}$):** Wie oben gilt $x_1 \in A^\times$, damit ist $x = x_1 \cdot m^1$ von er behaupteten Form.
>
> **($x \in \mathfrak{m}$):** In diesem Fall gibt es ein $x_2 \in A$ mit $x_1 = x_2 \cdot m$ also $x = x_2 \cdot m^2$.

Dieses Verfahren bricht entweder ab, oder wir erhalten wir eine Kette

$$(x) \;\subseteq\; (x_1) \;\subseteq\; (x_2) \;\subseteq\; (x_3) \;\subseteq\; \ldots$$

von Hauptidealen. Da A ein Hauptidealring ist, ist A insbesondere noethersch. Also gibt es ein $n \in \mathbb{N}$ ab dem die Kette stationär wird, das heißt $(x_n) = (x_{n+1})$. Dann gibt es aber eine Einheit $u \in A^\times$ mit $x_n = u \cdot x_{n+1}$. Nach Konstruktion gilt aber auch $x_{n+1} = x_n \cdot m$ also ist $x_n \cdot (u - m) = 0$. Weil aber $u - m$ nicht in $\mathfrak{m}$ liegt, folgt die Behauptung. □

Definition und Folgerung 9.20 *(Bewertung)*
Sei $\big(A, (m)\big)$ ein nullteilerfreier diskreter Bewertungsring, dann ist die Abbildung

$$\begin{array}{rcl} v : A & \to & \mathbb{Z} \cup \{\infty\} \\ x & \mapsto & v(x) \end{array}$$

eindeutig durch die Gleichung $x = u \cdot m^{v(x)}$ für ein $u \in A^\times$ und die konvention $v(0) := \infty$ bestimmt. Wir nennen v die Bewertung. Es gelten

(i) $v(xy) \;=\; v(x) + v(y)$

(ii) $v(x) \;=\; \max\big\{\, n \in \mathbb{N}_0 \;\big|\; x \in (m)^n \,\big\}$
Insbesondere hängt also v nicht von einer Wahl eines Erzeugers von (m) ab.

(iii) $v(x+y) \;\geq\; \min\big\{\, v(x),\, v(y) \,\big\}$ *und*
$v(x+y) \;=\; \min\big\{\, v(x),\, v(y) \,\big\}$, *falls* $v(x) \neq v(y)$

Satz 9.21 *Sei A ein Dedekindring und $\wp \in \mathrm{Spm}(A)$ ein maximales Ideal, dann ist $A_\wp$ ein nullteilerfreier diskreter Bewertungsring.*

Beweis. Nach Lemma 9.17 ist $A_\wp$ ein loakler Ring und nach Satz 9.13 ist $A_\wp$ dedekindsch. Da in Dedekindringen alle Primideale, die nicht (0) sind, maximale Ideale sind, gibt es nur zwei Primideale in $A_\wp$ nämlich

$$\mathrm{Spec}(A_\wp) \;=\; \big\{(0),\, \wp A_\wp\big\}$$

Weil sich in Dedekindringen jedes beliebige Ideal eindeutig in Primideale zerlegen lässt, enthält

$$\big\{\, (\wp A_\wp)^n \,\big|\, n \in \mathbb{N} \,\big\} \cup \{(0)\}$$

alle Ideale von $A_\wp$. Es gilt $\wp A_\wp \neq (\wp A_\wp)^2$ wähle also $\alpha \in \wp A_\wp \backslash (\wp A_\wp)^2$. Nach obiger Überlegung gibt es dann ein $m \in \mathbb{N}$ mit $(\alpha) = (\wp A_\wp)^m$. Weil aber $\alpha \notin (\wp A_\wp)^2$ kann m nicht größer als 1 sein. Also ist $(\alpha) = \wp A_\wp$ und die Menge der Ideale von $A_\wp$ ist

$$\left\{ (\alpha^n) \,\middle|\, n \in \mathbb{N} \right\} \cup \{(0)\}$$

□

Lemma 9.22 *Sei A ein Dedekindring und seien $\mathfrak{a} \lhd A$ ein Ideal mit $\mathfrak{a} \neq (0)$ und $\wp \in \mathrm{Spm}(A)$. Es gilt: Genau dann ist*

$$\mathfrak{a}\, A_\wp \;=\; (\wp A_\wp)^m \qquad \text{für ein } m \in \mathbb{N}$$

wenn $\mathfrak{a} = \wp^m \cdot \mathfrak{b}$ für ein $\mathfrak{b} \lhd A$ mit $\wp \nmid \mathfrak{b}$.

Beweis. Angenommen $\mathfrak{b}$ ist so ein Ideal, dann gilt

$$\mathfrak{a}\, A_\wp \;=\; (\wp^m A_\wp) \cdot (\mathfrak{b}\, A_\wp) \;=\; \left\{ \frac{a}{s} \in \kappa(\wp) \,\middle|\, a \in \mathfrak{a} \text{ und } s \in A \backslash \wp \right\}$$

Weiter können wir die Bedingung $\wp \nmid \mathfrak{b}$ übersetzen in

$$\wp \nmid \mathfrak{b} \quad\Leftrightarrow\quad \mathfrak{b} \not\subseteq \wp \quad\Leftrightarrow\quad \exists\, x \in \mathfrak{b} \cap (A \backslash \wp)$$

Dann liegt aber $1 = \frac{x}{x}$ im Ideal $bA_\wp$ und es gilt

$$\mathfrak{a}\, A_\wp \;=\; (\wp^m A_\wp) \cdot (\mathfrak{b}\, A_\wp) \;=\; \wp^m A_\wp \;=\; (\wp A_\wp)^m$$

Für den Nachweis der anderen Implikationsrichtung können alle hier gegebenen Argumente rückwerts gelesen werden. □

Wenn A ein dedekindscher Ring ist, dann gibt es für alle $\wp \in \mathrm{Spm}(A)$ eine Abbildung

$$v_\wp : \kappa(\wp)^* \;\twoheadrightarrow\; \mathbb{Z}$$

Und es gilt $\kappa(\wp) = \mathrm{Quot}(A_\wp) = \mathrm{Quot}(A)$. Wir haben gezeigt, dass $A_\wp$ ein nullteilerfreier diskreter Bewertungsring ist, also kann $v_\wp$ auf ganz $\kappa(\wp)$ fortgesetzt werden. Für $x \in \kappa(\wp)^*$ gibt es eine Darstellung $x = \frac{a}{b}$ mit $a, b \in A_\wp \backslash \{0\}$ und es gilt

$$v_\wp(x) \;=\; v_\wp(a) \,-\, v_\wp(b)$$

Wir erhalten eine exakte Sequenz

$$0 \;\to\; A_\wp^\times \;\to\; \kappa(\wp)^* \;\xrightarrow{v_\wp}\; \mathbb{Z} \;\to\; 0$$

Und für alle gebrochenen Ideale der Form (x) für ein $x \in \kappa(\wp)^* = \mathrm{Quot}(A)^*$ gilt

$$(x) \;=\; \prod_{\wp \in \mathrm{Spm}(A)} \wp^{v_\wp(x)}$$

Dabei sind nur endlich viele $v_\wp$ ungleich Null.

Übungsaufgabe 5 *Sei A ein Dedekindring und $\wp \in \mathrm{Spm}(A)$ ein maximales Ideal, dann gelten*

$$\begin{aligned} A_\wp &= \left\{ x \in \mathrm{Quot}(A) \,\middle|\, v_\wp(x) \geq 0 \right\} \\ \wp A_\wp &= \left\{ x \in \mathrm{Quot}(A) \,\middle|\, v_\wp(x) > 0 \right\} \end{aligned}$$

Folgerung 9.23 *Sei A ein Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(A)$, dann gilt*

$$A \;=\; \left\{ x \in K \,\middle|\, v_p(x) \geq 0 \text{ für alle } \wp \in \mathrm{Spm}(A) \right\}$$

Satz 9.24 *Sei A ein Dedekindring, dann gilt*

$$A \;=\; \bigcap_{\wp \in \mathrm{Spm}(A)} A_\wp \;=: B \;\subseteq\; \mathrm{Quot}(A)$$

Beweis. Sei $x \in B$, dann gibt es ganze Zahlen $n_1, \ldots, n_r \in \mathbb{Z}$ mit

$$(x) \;=\; xA \;=\; \wp_1^{n_1} \cdots \wp_r^{n_r} \qquad \text{für Primideale } \wp_i \in \mathrm{Spec}(A)$$

Für alle $i = 1, \ldots, r$ gilt dann

$$(x)\wp_i \;=\; (xA_{\wp_i}) \;=\; (\wp_i A_{\wp_i})^{n_i}$$

weil weiter x in jedem der $A_{\wp_i}$ liegt folgt dann aus Übungsaufgabe 5, dass $n_i \geq 0$ für alle $i = 1, \ldots, r$ ist. Also ist $x \in A$ und damit folgt $B \subseteq A$. Die andere Inklusion ist aber trivial, also folgt die Behauptung. □

Lemma 9.25 *Sei A ein Integritätsring, und $K := \mathrm{Quot}(A)$ sein Quotientenkörper. Dann ist*

$$A \;=\; \bigcap_{\mathfrak{m} \in \mathrm{Spm}(A)} A_\mathfrak{m} \;\subseteq\; K$$

Beweis. Für alle $\mathfrak{m} \in \mathrm{Spm}(A)$ gilt die Inklusionskette $A \subseteq A_\mathfrak{m} \subseteq K$, also ist

$$A \;\subseteq\; \bigcap_{\mathfrak{m} \in \mathrm{Spm}(A)} A_\mathfrak{m}$$

Für die andere Inklusion sei nun x ein Element aus dem Schnitt. Setze

$$\mathfrak{a} \;:=\; \left\{ a \in A \,\middle|\, a \cdot x \in A \right\}$$

Dann ist $\mathfrak{a}$ offensichtlich ein Ideal in A.

Behauptung *Für alle Primideale $\wp \in \mathrm{Spec}(A)\backslash\{(0)\}$ gilt*

$$\mathfrak{a}\, A_\wp \;=\; \left\{ a \in A_\wp \,\middle|\, a \cdot x \in A_\wp \right\}$$

Beweis. Sei $\frac{a}{s} \in A_\wp$ mit $a \in A$ und $s \in A\backslash\wp$, dass die Eigenschaft $\frac{a}{s} \cdot x \in A_\wp$ erfüllt. Dann gibt es ein $b \in A$ und ein $t \in A\backslash\wp$ mit

$$\frac{ax}{s} \;=\; \frac{s}{t} \quad\Rightarrow\quad tax \;=\; sb \in A \quad\Rightarrow\quad ta \in \mathfrak{a}$$

dann lag aber bereits unser Element $\frac{a}{s} = \frac{at}{st}$ im Ideal $\mathfrak{a}\, A_\wp$, was die Behauptung war. ◇

Mit der Behauptung gilt nun für alle Maximalideale $m \in \mathrm{Spm}(A)$

$$\mathfrak{a}\, A_\mathfrak{m} \;=\; \left\{ a \in A_\mathfrak{m} \,\middle|\, a \cdot x \in A_\mathfrak{m} \right\} \;=\; A_\mathfrak{m}$$

Dann ist aber $\mathfrak{a} \cap (A \setminus \mathfrak{m}) = \varnothing$ für alle $m \in \mathrm{Spm}(A)$ und damit ist $\mathfrak{a}$ in keinem Maximalideal von A enthalten und insbesondere auch selber nicht maximal. Also muss $\mathfrak{a} = A$ gelten und so folgt $x = 1 \cdot x \in A$. □

Damit erhalten wir ein einfacheres Kriterium um zu entscheiden, wann ein Ring dedekindsch ist. Wir können zeigen, dass die Eigenschaft „dedekindsch zu sein“ in gewissem Sinne eine lokale Eigenschaft ist:

Satz 9.26 *Sei A ein noetherscher Integritätsring. Genu dann ist A ein Dedekindring, wenn für alle Primideale $\wp \in \mathrm{Spec}(A)\backslash\{(0)\}$ die Lokalisierung $A_\wp$ ein diskreter Bewertungsring ist.*

Beweis. Wir haben bereits in Satz 9.21 die Implikation

$$A \text{ ist dedekindsch} \quad \Rightarrow \quad A_\wp \text{ ist diskreter Bewertungsring für alle } \wp \in \mathrm{Spm}(A)$$

gesehen. Wir müssen also nur noch die andere Implikation zeigen und setzen also voraus, dass $A_\wp$ für alle $\wp \in \mathrm{Spec}(A)\backslash\{(0)\}$ ein diskreter Bewertungsring ist. Wegen $\mathrm{Spm}(A) \subseteq \mathrm{Spec}(A)\backslash\{(0)\}$ folgt aus Lemma 9.25

$$A \;=\; \bigcap_{\wp \in \mathrm{Spec}(A)\backslash\{(0)\}} A_\wp \;\subseteq\; \mathrm{Quot}(A)$$

Als ersten Schritt zeigen wir nun, dass A ein dedekindring ist. Dazu prüfen wir die in Definition 5.1 spezifizierten Eigenschaften nach:

- Da A ein noetherscher Integritätsring ist, sind alle lokalisierungen $A_\wp$ Hauptidealbereiche, also sind alle $A_\wp$ ganz abgeschlossen. Damit ist auch A ganz abgeschlossen, denn für ein ein ganzes $x \in \mathrm{Quot}(A)$ gibt es $a_{n-1}, \ldots, a_0 \in A$ mit

  $$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \;=\; 0$$

  Dann ist aber x in jedem $A_\wp$, denn diese sind ganz abgeschlossen, also liegt x auch im Schnitt der $A_\wp$ also in A.

- Sei $\mathfrak{m} \in \mathrm{Spm}(A)$, dann gibt es eine Bijektion

  $$\begin{array}{ccc} \{\, \wp \in \mathrm{Spec}(A) \mid \wp \subseteq \mathfrak{m} \,\} & \overset{1:1}{\longleftrightarrow} & \mathrm{Spec}(A_\mathfrak{m}) \\ \mathfrak{p} & \mapsto & \mathfrak{p}\, A_\mathfrak{m} \\ \mathfrak{q} \cap A & \hookleftarrow & \mathfrak{q} \end{array}$$

  Weil aber $A_\mathfrak{m}$ ein lokaler Ring ist, gilt für alle $\mathfrak{p} \in \mathrm{Spec}(A)$

  $$\mathfrak{p}\, A_\mathfrak{m} \;=\; \begin{cases} (0) & \Rightarrow \;\; \mathfrak{p} = (0) \\ \mathfrak{m}\, A_\mathfrak{m} & \Rightarrow \;\; \mathfrak{p} = \mathfrak{m} \end{cases}$$

  Also ist jedes Primideal $\mathfrak{p} \in \mathrm{Spec}(A)$ entweder das Nullideal oder maximal.

Da wir die Eigenschaft, dass A noethersch ist, bereits vorausgesetzt hatten folgt somit die Aussage des Satzes. □

Lemma 9.27 *Sei A ein Ring und $\mathfrak{m} \in \mathrm{Spm}(A)$ ein maximales Ideal. Zu jedem $x \in A\backslash\,\mathfrak{m}$ und jedem $n \in \mathbb{N}$ gibt es ein $y \in A\backslash\,\mathfrak{m}$ mit $xy \in 1 + \mathfrak{m}^n$.*

Beweis. Wir betrachten die natürliche Projektion

$$\pi : A \;\twoheadrightarrow\; {}^{A}\!/_{\mathfrak{m}}$$

Wir bezeichnen das Bild von x unter π mit $\pi(x) = \overline{x}$. Wegen $x \notin \mathfrak{m}$ gilt $\overline{x} \neq \overline{0}$. Weil $\mathfrak{m}$ maximal ist, ist der Quotient ein Körper, wähle also $y \in A$ so, dass $\pi(y) = \overline{y} = \overline{x}^{-1}$ gilt. Dann ist aber $xy \in 1 + \mathfrak{m}$. Da $\mathfrak{m}$ insbesondere auch prim ist, muss also entweder x oder y bereits in $1 + \mathfrak{m}$ liegen. Ohne Einschränkung gelte $x \in 1 + \mathfrak{m}$, dann gibt es aber ein $a \in \mathfrak{m}$ mit $x = 1 - a$ und es gilt

$$(1-a) \cdot (1 + a + a^2 + \ldots + a^{n-1}) \;=\; 1 - a^n \;\equiv\; 1 \;\text{ modulo } \mathfrak{m}^n$$

Setze also $y' := 1 + a + a^2 + \ldots + a^{n-1}$, dann ist $xy' \in 1 + \mathfrak{m}^n$. □

Lemma 9.28 *Sei A ein Ring, M ein A-Moul sowie $\mathfrak{m} \in \mathrm{Spm}(A)$ ein maximales Ideal. Dann gilt für alle $n \in \mathbb{N}$*

$$M/\mathfrak{m}^n M \;\cong\; M_{\mathfrak{m}}/\mathfrak{m}^n M_{\mathfrak{m}}$$

Beweis. Die kurze Sequenz

$$0 \;\to\; \mathfrak{m}^n M \;\to\; M \;\to\; M/\mathfrak{m}^n M \;\to\; 0$$

ist offensichtlich exakt. Lokalisieren erhält Exaktheit nach Folgerung 9.9, also ist auch

$$0 \;\to\; \mathfrak{m}^n M_{\mathfrak{m}} \;\to\; M_{\mathfrak{m}} \;\to\; M_{\mathfrak{m}}/\mathfrak{m}^n M_{\mathfrak{m}} \;\to\; 0$$

eine kurze exakte Sequenz. Wir erhalten die Isomorphie

$$\left(M/\mathfrak{m}^n M\right)_{\mathfrak{m}} \;\cong\; M_{\mathfrak{m}}/\mathfrak{m}^n M_{\mathfrak{m}}$$

Wir wollen nunzeigen, dass auch die folgende Isomorphie gilt:

$$\left(M/\mathfrak{m}^n M\right)_{\mathfrak{m}} \;\cong\; M/\mathfrak{m}^n M$$

Dazu betrachte ein typisches Element aus dem linken Quotienten. Etwa

$$\frac{a+\mathfrak{m}^n}{x} \;\in\; \left(M/\mathfrak{m}^n M\right)_{\mathfrak{m}}$$

mit $x \in A\setminus \mathfrak{m}$. Nach vorangegangenem Lemma 9.27 gibt es ein $y \in A\setminus \mathfrak{m}$ mit $xy \in 1+\mathfrak{m}^n$. Damit gilt

$$\frac{a+\mathfrak{m}^n}{x} \;=\; \frac{ya+\mathfrak{m}^n}{1}$$

Also ist die Abbildung

$$\begin{array}{rcl} l : M/\mathfrak{m}^n M & \to & \left(M/\mathfrak{m}^n M\right)_{\mathfrak{m}} \\ \lambda & \mapsto & \dfrac{\lambda}{1} \end{array}$$

surjektiv. Sei nun

$$a+\mathfrak{m}^n \;\in\; M/\mathfrak{m}^n M \quad \text{mit } \; l(a+\mathfrak{m}^n) \;=\; 0$$

dann gibt es ein $x \in A\setminus \mathfrak{m}$ so dass $xa+\mathfrak{m}^n \;=\; 0+\mathfrak{m}^n$ gilt. Mit dem Lemma zuvor finden wir nun wieder ein $y \in A\setminus \mathfrak{m}$ mit $xy \in 1+\mathfrak{m}^n$. hiermit gilt

$$a+\mathfrak{m}^n \;=\; xya+\mathfrak{m}^n \;=\; \mathfrak{m}^n$$

also ist $a \in \mathfrak{m}^n$ und die Abbildung l ist auch injektiv, was die Behauptung zeigt. □

10 Verhalten von Primidealen in Körpererweiterungen

In diesem Abschnitt haben wir wieder ein paar Bezeichnungen, die wir über den ganzen Abschnitt beibehalten wollen:

> A bezeichne in diesem Abschnitt einen Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(A)$. Weiter sei L/K eine endliche separable Körpererweiterung $B := \overline{A}$ bezeichne den ganzen Abschluss von A in L.

Wir haben in den letzten Abschnitten bereits gezeigt, dass dann auch B ein Dedekindring ist, den wir als endlich erzeugten A-Modul auffassen können. Weiter wissen wir, dass $\mathrm{Quot}(B) = L$ ist. Wir wollen in diesem Abschnitt untersuchen, wie die (Prim-)Ideale von B und A zusammenhängen, und welche Aussagen wir von A nach B „liften“ können und umgekehrt. Zunächsteinmal benötigen wir eine Sprechweise:

Definition 10.1 *Sei $\mathfrak{p} \in \mathrm{Spec}(A)$ ein Primideal, dann sagen wir ein Ideal $\mathfrak{P} \in \mathrm{Spec}(B)$ „liegt über“ $\mathfrak{p}$, wenn $\mathfrak{p} = \mathfrak{P} \cap A$ gilt. Wirschreiben dann auch $\mathfrak{P} \,/\, \mathfrak{p}$.*

Dass diese Sprechweise nicht leer, sondern sinnvoll ist zeigt der folgende

Satz 10.2 *Es gelten*

a) *Für alle $\mathfrak{P} \in \mathrm{Spec}(B)$ ist $\mathfrak{P} \cap A$ ein maximales Ideal in A.*

b) *Für alle $\mathfrak{p} \in \mathrm{Spm}(A)$ ist $\mathfrak{p}\,B \neq B$ und es gibt ein maximales Ideal $\mathfrak{P} \in \mathrm{Spm}(B)$ mit $\mathfrak{p} = \mathfrak{P} \cap A$.*

Beweis. . Für den Nachweis von **(a)** betrachte die Abbildung

$$A \;\hookrightarrow\; B \;\twoheadrightarrow\; {}^{B}\!/_{\mathfrak{P}}$$

Setze $\mathfrak{p} := \mathfrak{P} \cap A$, dann ist $\mathfrak{p}$ ein Primideal, da der Quotient ${}^{B}\!/_{\mathfrak{P}}$ ein Körper ist. Da A ein Dedekindring ist, genügt es nun zu zeigen, dass $\mathfrak{p}$ nicht das Nullideal ist. Sei dazu $x \in \mathfrak{P} \setminus \{0\}$ dann gibt es ein normiertes Polynom

$$f \;:=\; T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0 \;\in K[T]$$

und f ist das Minimalpolynom von $x \in L$ über K. Weil wir ein $x \neq 0$ gewählt haben ist auch $a_0 \neq 0$. Damit gilt

$$A \;\ni\; a_0 \;=\; -\big(x^n + a_{n-1}x^{n-1} + \ldots + a_1 x\big) \;\in\; \mathfrak{P} \cap A \;=\; \mathfrak{p}$$

Dann kann $\mathfrak{p}$ aber nicht das Nullideal sein und wir haben **(a)** gezeigt. Für Teil **(b)** sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann gilt $(\pi) := \pi A = \mathfrak{p}\,\mathfrak{a}$ für ein ideal $\mathfrak{a} \lhd A$ mit $\mathfrak{p} \nmid \mathfrak{a}$. Weil $(\pi) \nsubseteq \mathfrak{p}^2$ ist, teilt $\mathfrak{p}^2$ das Hauptideal (π) nicht. Also sind die Ideale $\mathfrak{p}$ und $\mathfrak{a}$ Teilerfremd, das heißt $\mathfrak{p} + \mathfrak{a} = A$. Damit muss es ein $p \in \mathfrak{p}$ und ein $a \in \mathfrak{a}$ geben, sodass $p + a = 1$ und es gilt $a \notin \mathfrak{p}$. Damit ist $a\,\mathfrak{p} \subseteq \mathfrak{a}\,\mathfrak{p} = \pi A$.
Angenommen das von $\mathfrak{p}$ in B erzeugte Ideal wäre bereits der ganze Ring, also $\mathfrak{p}\,B = B$, dann folgte aus der obigen Überlegung

$$aB \;=\; a\,\mathfrak{p}\,B \;\subseteq\; \mathfrak{a}\,\mathfrak{p}\,B \;=\; \pi B$$

Dann fänden wir aber ein $x \in B$ für das $a = \pi x$ gülte. Diese Gleichung könnten wir dann Umformen zu $x = \frac{a}{\pi} \in K \cap B = A$. Dann wäre aber $a = x\pi \in \mathfrak{p}$ und das haben wir oben bereits ausgeschlossen. Also muss $\mathfrak{p}\,B \neq B$ gelten.
Sei nun $\mathfrak{P} \in \mathrm{Spm}(A)$ ein maximales Ideal mit $\mathfrak{p}\,B \subseteq \mathfrak{P}$. Wir wissen nach Teil **(a)**, dass $\mathfrak{p} \cap A$ ein maximales Ideal in A sein muss. Weiter gilt $\mathfrak{p} \subseteq \mathfrak{P} \cap A$. Da aber auch $\mathfrak{p}$ ein maximales Ideal ist, folgt die Behauptung. □

Definition und Folgerung 10.3 *(Verzweigungsindex)*
Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ *dann gilt*

$$\mathfrak{p}\,B \;=\; \prod_{\substack{\mathfrak{P} \in \mathrm{Spm}(B) \\ \mathfrak{P} \cap A = \mathfrak{p}}} \mathfrak{P}^{e_{\mathfrak{P}}}$$

Wir nennen $e_{\mathfrak{P}} =: e(\mathfrak{P} \,/\, \mathfrak{p})$ *den Verzeigungsindex von* $\mathfrak{P}$ *über* $\mathfrak{p}$.

Beweis. Nach Satz 10.2 ist $\mathfrak{p}\,B \neq 0$ und B ist ein Dedekindring. Also können wir $\mathfrak{p}\,B$ eindeutig in Primideale $\mathfrak{P} \in \mathrm{Spm}(B)$ mit $\mathfrak{P} \subseteq \mathfrak{p}\,B$ faktorisieren. Jedes dieser Primideale kommt genau $e_{\mathfrak{P}}$-mal mit $e_{\mathfrak{P}} > 0$ in der Zerlegung vor. Weiter gilt

$$\mathfrak{P} \subseteq \mathfrak{p}\,B \quad\Leftrightarrow\quad \mathfrak{P} \mid \mathfrak{p}\,B \quad\Leftrightarrow\quad \mathfrak{p} = \mathfrak{P} \cap A$$

□

Definition 10.4 *(Trägheitsgrad)*
Wir definieren den Trägheitsgrad von $\mathfrak{P}$ *über* $\mathfrak{p} := \mathfrak{P} \cap A$ *als*

$$f(\mathfrak{P} \,/\, \mathfrak{p}) \;:=\; \left[{}^{B}\!/_{\mathfrak{P}} \,:\, {}^{A}\!/_{\mathfrak{p}} \right]$$

Anmerkung Diese Definition ist wohldefiniert, denn wir haben es hier tatsächlich mit einer Körpererweiterung zu tun. Wie bereits erwähnt können wir B als endlich erzeugten A-Modul auffassen. Dann ist aber auch ${}^{B}\!/_{\mathfrak{P}}$ ein endlich erzeugter A-Modul. Schließlich wird der Quotienten damit zu einem ${}^{A}\!/_{\mathfrak{p}}$-Vektorraum. Da sowohl $\mathfrak{P}$ als auch $\mathfrak{p}$ maximale Ideale sind, sind beide Quotienten Körper.

Satz 10.5 *Sei* $\mathfrak{p} \in \mathrm{Spm}(A)$ *und hierzu sei*

$$\mathfrak{p}\,B \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \qquad \text{mit } \mathfrak{P}_i \in \mathrm{Spm}(B) \text{ und } e_i > 0$$

die Primidealfaktorisierung von $\mathfrak{p}\,B$ *in paarweise verschiedene maximalideale von* B. *Seien weiter*

$$f_i \;:=\; f(\mathfrak{P}_i \,/\, \mathfrak{p}) \;:=\; \left[{}^{B}\!/_{\mathfrak{P}_i} \,:\, {}^{A}\!/_{\mathfrak{p}} \right]$$

die zugehörigen Trägheitsgrade, dann gilt

$$[L : K] \;=\; \sum_{i=1}^{r} f_i e_i$$

Beweis. Wir beweisen zwei Behauptungen, die zusammen den Satz ergeben.

Behauptung 1 $\dim_{{}^{A}\!/_{\mathfrak{p}}} \left({}^{B}\!/_{\mathfrak{p}\,B} \right) \;=\; \sum_{i=1}^{r} e_i f_i$.

Beweis. Mit dem chinesischen Restsatz 5.9 gilt

$${}^{B}\!/_{\mathfrak{p}\,B} \;\cong\; {}^{B}\!/_{\mathfrak{P}_1^{e_1}} \times \cdots \times {}^{B}\!/_{\mathfrak{P}_r^{e_r}}$$

Und alle auftretenden Quotienten sind ${}^{A}\!/_{\mathfrak{p}}$-Vektorräume. Für alle $i = 1, \ldots r$ gilt die Inklusionskette

$${}^{B}\!/_{\mathfrak{P}_i^{e_i}} \;\supseteq\; {}^{\mathfrak{P}_i}\!/_{\mathfrak{P}_i^{e_i}} \;\supseteq\; {}^{\mathfrak{P}_i^2}\!/_{\mathfrak{P}_i^{e_i}} \;\supseteq\; \cdots \;\supseteq\; {}^{\mathfrak{P}_i^{e_i-1}}\!/_{\mathfrak{P}_i^{e_i}}$$

fassen wir die Quotienten als B-Moduln auf, dann wissen wir dass gilt

$$\mathfrak{P}_i^l \big/ \mathfrak{P}_i^{l+1} \;\cong\; B \big/ \mathfrak{P}_i \qquad \text{für alle } l \in \mathbb{N}$$

Also gilt diese Isomorphie auch als $A/\mathfrak{p}$-Vektorraum. Dann folgt aber

$$\begin{aligned} \dim_{A/\mathfrak{p}} \left(B \big/ \mathfrak{P}_i^{e_i} \right) &= \sum_{l=0}^{e_i-1} \dim_{A/\mathfrak{p}} \left(\mathfrak{P}_i^l \big/ \mathfrak{P}_i^{l+1} \right) \\ &= e_i \cdot \dim_{A/\mathfrak{p}} \left(B \big/ \mathfrak{P}_i \right) \;=\; e_i f_i \end{aligned}$$

$\diamond$

Behauptung 2 $\dim_{A/\mathfrak{p}} \left(B \big/ \mathfrak{p}\, B \right) \;=\; [L:K]$

Beweis. Die Teilmenge

$$S := A \backslash \mathfrak{p} \;\subset\; A \;\subseteq B$$

ist ein multiplikatives System. Setze $B_\mathfrak{p} := S^{-1}B$. Da B über A endlich erzeugt ist, ist auch $B_\mathfrak{p}$ ein endlich erzeugter A-Modul. Weil weiter B ein Integritätsring mit Quotientenkörper L ist, gilt

$$B \;\subseteq\; B_\wp \;\subseteq\; L$$

Also ist B_{fp} insbesondere torsionsfrei. Wir haben im letzten Abschnitt gezeigt, dass $A_\mathfrak{p}$ ein Hauptidealring ist, also folgt mit dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen

$$B_\mathfrak{p} \;=\; A_\mathfrak{p}^{\otimes m} \;=\; A_\mathfrak{p}^m \quad \text{für ein } m \in \mathbb{N}$$

Weiter folgt dann mit Lemma 9.28

$$B \big/ \mathfrak{p}\, B \;\cong\; B_\mathfrak{p} \big/ \mathfrak{p}\, B_\mathfrak{p} \;\cong\; \left(A_\mathfrak{p} \big/ \mathfrak{p}\, A_\mathfrak{p} \right)^m \;\cong\; \left(A/\mathfrak{p} \right)^m$$

Damit ist also m die gesuchte Dimension. Weiter ist

$$L \;=\; B_\mathfrak{p} \otimes_{A_\mathfrak{p}} K \;\cong\; K^m$$

und damit folgt die Behauptung. $\diamond$

Offensichtlich ergeben die Aussagen der beiden Behauptungen zusammen gerade den Satz. $\square$

Definition 10.6 *(Voll zerlegt)*
Ein maximales Ideal $\mathfrak{p} \in \mathrm{Spm}(A)$ heißt voll zerlegt in L, wenn $\mathfrak{p}\, B$ in paarweise verschiedene Maximalideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_n \in \mathrm{Spm}(B)$ mit $n = [L:K]$ zerfällt. Das heißt wenn

$$\mathfrak{p}\, B \;=\; \mathfrak{P}_1 \cdots \mathfrak{P}_n$$

Folgerung 10.7 *Ist $\mathfrak{p} \in \mathrm{Spm}(A)$ voll zerlegt in L, so sind Trägheitsgrad und Verzeigungsindex gleich Eins für alle $\mathfrak{P} \in \mathrm{Spm}(B)$ mit $\mathfrak{P} \,/\, \mathfrak{p}$.*

Definition 10.8 *(Verzweigt, Unverzweigt)*
Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ *und sei hierzu* $\mathfrak{P} \in \mathrm{Spm}(B)$ *mit* $\mathfrak{P} \cap A = \mathfrak{p}$*, dann heißt* $\mathfrak{P} \,/\, \mathfrak{p}$ *unverzweigt, falls* $e(\mathfrak{P} \,/\, \mathfrak{p}) = 1$ *ist und die Körpererweiterung* ${}^{B}\!/_{\mathfrak{P}}\big/{}^{A}\!/_{\mathfrak{p}}$ *separabel ist.*
Enstprechend heißt $\mathfrak{P} \,/\, \mathfrak{p}$ *verzweigt, falls* $\mathfrak{P} \,/\, \mathfrak{p}$ *nicht unverzweigt ist, das heißt, wenn* $e(\mathfrak{P} \,/\, \mathfrak{p}) > 1$ *ist oder die Körpererweiterung* ${}^{B}\!/_{\mathfrak{P}}\big/{}^{A}\!/_{\mathfrak{p}}$ *nicht separabel ist.*
Weiter sei

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

die Primfaktorzerlegung des von $\mathfrak{p}$ *in* B *erzeugten Ideals in paarweise verschiedene Primfaktoren. Dann nennen wir* $\mathfrak{p}$ *in* L *(bzw.* B*) unverzweigt, wenn alle* $\mathfrak{P}_i \,/\, \mathfrak{p}$ *unverzweigt sind.*

Bemerkung 10.9 *Sei* K *ein endlicher Erweiterungskörper von* $\mathbb{Q}$*, dann ist* ${}^{\mathcal{O}_K}\!/_{\mathfrak{p}}$ *für* $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ *ein endlicher Körper. Sei nun* L/K *eine endliche separable Körpererweiterung und* B *der ganze Abschluss von* $\mathcal{O}_K$ *in* L*. Sei weiter* $\mathfrak{P} \in \mathrm{Spm}(B)$ *derart, dass* $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$*, dann ist*

$${}^{B}\!/_{\mathfrak{P}}\Big/{}^{\mathcal{O}_K}\!/_{\mathfrak{p}}$$

eine separable Körpererweiterung.

Satz 10.10 *Sei* $\theta \in B$ *ein primitives Element, das heißt* $L = K(\theta)$ *und sei* $g \in A[X]$ *das Minimalpolynom von* θ *über* K*. Setze*

$$\mathcal{F} \;:=\; \left\{\, a \in A \,\middle|\, a \cdot B \subseteq A[\theta] \,\right\} \;\lhd A$$

Sei weiter $\mathfrak{p} \in \mathrm{Spm}(A)$ *ein Primideal, dass* $\mathcal{F}$ *nicht teilt. Bezeichne weiter* $\overline{f} \in {}^{A}\!/_{\mathfrak{p}}[X]$ *das Bild von* $f \in A[X]$ *unter der natürlichen Projektion. Sei*

$$\overline{g} \;=\; \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r} \qquad \text{mit } \overline{g}_i \in {}^{A}\!/_{\mathfrak{p}}[X]$$

die Zerlegung von $\overline{g}$ *in paarweise verschiedene irreduzible und normierte Polynome.*
Dann sind die Primideale $\mathfrak{P}_i \in \mathrm{Spm}(B)$ *von* B*, die über* $\mathfrak{p}$ *liegen gegeben durch*

$$\mathfrak{P}_i \;=\; \mathfrak{p} + g_i(\theta) \cdot B \qquad \text{für } i = 1, \ldots, r$$

und es gelten

$$\mathfrak{p} \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \qquad \text{und} \qquad f(\mathfrak{P}_i \,/\, \mathfrak{p}) \;=\; \deg(\overline{g_i}) \text{ für alle } i = 1, \ldots, r$$

Beweis. Sei n der Grad von L über K, dann ist die Menge $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ eine K-Basis von L. Für alle $x \in L$ gibt es ein $a \in A$ mit $a \cdot x \in A[\theta]$, denn $K := \mathrm{Quot}(A)$ ist der Quotientenkörper von K. Da B über A endlich erzeugt ist, gibt es Elemente $\omega_1, \ldots, \omega_n \in B$ mit

$$B \;=\; A\omega_1 + \ldots + A\omega_n$$

Seien hierzu $a_1, \ldots, a_n \in A \backslash \{0\}$ mit $a_i \omega_i \in A[\theta]$ für alle $i = 1, \ldots, n$ gegeben, dann liegen alle a_i im oben definierten Ideal $\mathcal{F}$. Also ist $\mathcal{F}$ insbesondere nicht leer und es gilt

$$\mathcal{F}\, B \;\subseteq\; A[\theta] \;\subseteq\; B$$

Sei nun $\mathfrak{p} \in \mathrm{Spm}(A)$ wie oben gefordert, das heißt $\mathfrak{p} \nmid \mathcal{F}$, dann gilt $\mathfrak{p} + \mathcal{F} = A$. Also gibt es ein $p \in \mathfrak{p}$ und ein $f \in \mathcal{F}$ mit $1 = p + f$. Betrachte das folgende Diagramm

$$\begin{array}{ccccc} fB & \hookrightarrow & A[\theta] & \hookrightarrow & B \\ & \searrow & & & \downarrow \\ & & & & {}^{B}\!/_{\mathfrak{p}\,B} \end{array} \qquad \begin{array}{c} f \\ \downarrow \\ 1 \end{array}$$

Es gilt $fB \cap pB = fpB$ und damit erhalten wir insgesamt die Isomorphie

$${}^{A[\theta]}\!/_{\mathfrak{p}\,A[\theta]} \;\cong\; {}^{B}\!/_{\mathfrak{p}\,B}$$

Wei nun $\mathcal{F}$ nicht von $\mathfrak{p}$ geteilt wird können wir diese Isomorphie fortsetzen zu

$${}^{A[\theta]}\!/_{\mathfrak{p}\,A[\theta]} \;\cong\; {}^{B}\!/_{\mathfrak{p}\,B} \;\cong\; {}^{A[X]}\!/_{(\mathfrak{p},\,g)} \;\cong\; {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g})}$$

Mit dem Chinesischen Restsatz 5.9 folgt weiter

$${}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g})} \;\cong\; \prod_{i=1}^{r} {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g}_i)^{e_i}}$$

Wei $\mathfrak{p}$ ein Maximales Ideal von A und alle $\overline{g_i}$ irreduzible Polynome sind, sind für alle $i = 1, \ldots, r$ die Quotienten ${}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g}_i)}$ Körper, mit Erweiterungsgrad $\deg(\overline{g}_i)$ über ${}^{A}\!/_{\mathfrak{p}}$. Halte nun ein beliebiges $i \in \{1, \ldots, r\}$ fest und wähle ein Polynom $g_i \in A[X]$, so dass $\overline{g}_i$ das Bild von g_i unter der natürlichen Projektion ist. Setze

$$\mathfrak{P}_i \;:=\; \mathfrak{p}\,B + g_i(\theta)B$$

dann gilt

$${}^{B}\!/_{\mathfrak{P}_i} \;\cong\; {}^{B}\!/_{\mathfrak{p}\,B + g_i(\theta)B} \;{}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g}_i)}$$

also ist $\mathfrak{P}_i$ ein maximales Ideal. Betrachte weiter

$$B \;\twoheadrightarrow\; {}^{B}\!/_{\mathfrak{p}\,B} \;\cong\; {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g})} \;\twoheadrightarrow\; {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g},\,\overline{g}_i)}$$

Also ist $\mathfrak{P}_i$ das Urbild des Hauptideals $(\overline{g}_i) \lhd {}^{A}\!/_{\mathfrak{p}}[X]$ in B. Dann gilt

$$f(\mathfrak{P}_i \,/\, \mathfrak{p}) \;=\; \left[{}^{B}\!/_{\mathfrak{P}_i} \,:\, {}^{A}\!/_{\mathfrak{p}} \right] \;=\; \deg(\overline{g}_i)$$

Und das Bild von $\mathfrak{P}_i$ unter der natürlichen Projektion nach ${}^{{}^{A}\!/_{\mathfrak{p}}[X)}\!/_{(\overline{g})}$ ist das Ideal $(\overline{g}_i)^{e_i}$.

Zwischenstand: Wir haben gezeigt, dass die konstruierten Ideale $\mathfrak{P}_i$ die gewünschten Eigenschaften haben. Nun müssen wir nur noch zeigen, dass alle Ideale $\mathfrak{P} \in \mathrm{Spm}(B)$, die über $\mathfrak{p}$ liegen, sich auf diese Weise konstruieren lassen. Sei also $\mathfrak{P}$ ein Ideal über $\mathfrak{p}$, dann ist das Bild von $\mathfrak{P}$ in ${}^{B}\!/_{\mathfrak{p}\,B}$ ebenfalls ein maximales Ideal. Nach obiger Überlegung gilt aber die folgende Isomorphie

$${}^{B}\!/_{\mathfrak{p}\,B} \;\cong\; {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g})} \;\cong\; \prod_{i=1}^{r} {}^{{}^{A}\!/_{\mathfrak{p}}[X]}\!/_{(\overline{g}_i)^{e_i}}$$

also ist das Bild von $\mathfrak{P}$ unter der natürlichen Projektion nach ${}^{{}^{A}\!/_{\mathfrak{p}}[X)}\!/_{(\overline{g})}$ das Ideal $(\overline{g}_i)^{e_i}$ für ein $i\,\{1, \ldots, r\}$ und damit ist $\mathfrak{P} = \mathfrak{P}_i$ $\square$

Folgerung 10.11 *Es gibt nur endlich viele Ideale von A in B, die unverzweigt sind.*

Beweis. Seien die Bezeichnungen $A, B, K, L, \mathcal{F}, \theta, g, \overline{g}, \ldots$ wie in Satz 10.10. Es gibt nur endlich viele Ideale $\mathfrak{p} \in \mathrm{Spm}(A)$, die das Ideal $\mathcal{F}$ teilen, also können wir diese endliche Menge von Idealen ignorieren und ohne Einschränkung annehmen, dass $\mathfrak{p}$ das Ideal $\mathcal{F}$ nicht teilt. Bezeichne

$$D(g) \;:=\; D(1, \theta, \ldots, \theta^{n-1}) \;=\; \prod_{i=1}^{n} \prod_{\substack{j=1 \\ i<j}}^{n} \left(\theta_i - \theta_j\right)^2$$

mit $\theta_i := \sigma_i(\theta)$ für $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \overline{K})$ die Diskriminante von g. Nach Satz 10.10 gibt es Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathrm{Spm}(B)$ mit

$$\mathfrak{p} \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \qquad \text{mit } \mathfrak{P}_i \;=\; \mathfrak{p} + g_i(\theta) B$$

Behauptung $\mathfrak{p}$ *ist genau dann unverzweigt, wenn $\overline{g}$ das Produkt von paarweise verschiedenen separablen und irreduziblen Polynomen $\overline{g}_i \in {}^{A}\!/_{\mathfrak{p}}[X]$ ist.*

Beweis. Sei

$$\overline{g} \;=\; \overline{g}_1 \cdots \overline{g}_r$$

mit paarweise verschiedenen irreduziblen und separablen Polynomen $\overline{g}_i$. Nach Satz 10.10 gelten

$$e(\mathfrak{P}_i \,/\, \mathfrak{p}) \;=\; 1 \quad \text{und} \quad {}^{B}\!/_{\mathfrak{P}_i}/{}^{A}\!/_{\mathfrak{p}} \text{ ist separabel}$$

für alle $i = 1, \ldots, r$. Die Begründung über den vorangegangenen Satz funktioniert in beide Richtungen, also folgt die Behauptung. ◇

Das Polynom $\overline{g}$ zerfällt aber genau dann in paarweise verschiedene irreduzible Faktoren $\overline{g}_1, \ldots, \overline{g}_r$, wenn $\overline{g}$ keine mehrfachen Nullstellen in ${}^{A}\!/_{\mathfrak{p}}$ hat, also genau dann, wenn die Diskriminante von $\overline{g}$ nicht Null ist. Für die Diskriminante $D(\overline{g})$ von $\overline{g}$ gilt

$$D(\overline{g}) \;\equiv\; D(g) \;\text{ modulo } \mathfrak{p}$$

Insgesamt erhalten wir die Bedingung, dass $\mathfrak{p}$ unverweigt ist, wenn $\mathfrak{p} \nmid \mathcal{F}$ und $\mathfrak{p} \nmid D(g)$. Diese Bedingung wird aber nur von endlich vielen $\mathfrak{p}$ erfüllt. □

Beispiel 29 *(Zu Satz 10.10)*
Wir betrachten wieder unser Standartbeispiel eines quadratischen Körpers. Sei also $K = \mathbb{Q}(\sqrt{d})$ für ein quadratfreies $d \in \mathbb{Z}$, dann ist $\theta = \sqrt{d}$. Wie üblich unterscheiden wir die Fälle

$d \equiv 1\ (4)$ *In diesem Fall ist*

$$B \;=\; \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] \qquad \Longrightarrow \qquad \mathcal{F} \;=\; (2)$$

$d \equiv 2, 3\ (4)$ *Wir haben gezeigt, dass in diesem Fall $B = \mathbb{Z}[\sqrt{d}]$ gilt. Ist nun $p \in \mathbb{N}_{>2}$ eine Primzahl, dann haben wir die Isomorphie*

$${}^{\mathbb{Z}[\sqrt{d}]}\!/_{p\,\mathbb{Z}[\sqrt{d}]} \;\cong\; {}^{\mathbb{Z}[X]}\!/_{(X^2-d,\,p)} \;\cong\; {}^{\mathbb{F}_p[X]}\!/_{(X^2-d)}$$

Wir wollen nun die möglichen Settings für Satz 10.10 durchspielen.

Falls p teilt d: *In diesem Fall ist wegen der obige Isomorphie $r = 1$ und $\overline{g}_1 = \overline{g} = X$. Damit ergibt sich für das von p in $\mathbb{Z}[\sqrt{d}]$ erzeugte Ideal $p\,\mathbb{Z}[\sqrt{d}] \;=\; (p, \sqrt{d})^2$.*

Falls p teilt nicht d: *Diesen Fall müssen wir noch einmal zerlegen um eine genauere Aussage zu bekommen:*

1. *d ist ein Quadrat modulo p, das heißt es gibt ein $cin\,\mathbb{F}_p$ mit $d \;\equiv\; c^2\;(p)$. In desem Fall können wir die obige Isomorphie fortsetzen zu*

$$\mathbb{F}_p[X]\big/(X^2 - d) \;\cong\; \mathbb{F}_p \times \mathbb{F}_p$$

   wir erhalten die Zerlegung

$$\mathfrak{p} \;:=\; p\,\mathbb{Z}[\sqrt{d}] \;=\; (p, \sqrt{d} - c) \cdot (p, \sqrt{d} + c)$$

   und $\mathfrak{p}$ ist voll zerlegt.

2. *d ist kein Quadrat modulo p. In diesem Fall können wir die Isomorphie zu*

$$\mathbb{F}_p[X]\big/(X^2 - d) \;\cong\; \mathbb{F}_{p^2}$$

   fortsetzen und sehen sofort, dass $p\,\mathbb{Z}[\sqrt{d}]$ ein unverzweigtes Primideal mit $f\big(pB/(2)\big) = 2$ und $e\big(pB/(2)\big) = 1$.

Im ersten von uns betrachteten Fall ($d \;\equiv\; 1\;(4)$) können wir wegen der Bedingung $(p) \nmid \mathcal{F} = (2)$ nicht mit dem von 2 erzeugten Primideal umgehen. Betrachte aber

$$B \;=\; \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] \;\cong\; \mathbb{Z}[X]\Big/\Big(X^2 - X + \frac{1-d}{4}\Big)$$

Setze nun $a := \frac{1-d}{4}$, dann ist der Quotienten von B nach dem von 2 in B erzeugten Ideal

$$B\big/2B \;\cong\; \mathbb{F}_2[X]\big/(X^2 - X + a)$$

Wenn wir das Polynom $X^2 - X + a$ in $\mathbb{F}_2[X]$ untersuchen wollen, genügt es die folgenden Fälle zu betrachten:

($2 \mid a$): *In diesem Fall ist $a \;\equiv\; 0\;(2)$ also ist d wegen $d \;=\; 4a + 1$ sogar modulo 2 kongruent zu 1. Das Polynom vereinfacht sich zu*

$$X^2 - X \;=\; X \cdot (X - 1)$$

Damit erhalten wir

$$2B \;=\; \Big(2\,,\,\frac{\sqrt{d}+1}{2}\Big) \cdot \Big(2\,,\,\frac{\sqrt{d}+1}{2} - 1\Big)$$

($2 \nmid a$): *In diesem Fall ist das Polynom $X^2 - X + 1$ irreduzibel in $\mathbb{F}_2[X]$, also ist $2B$ prim in B.*

Beispiel 30 *(Zur Folgerung 10.11)*
Sei $p \in \mathbb{Z}$ eine Primzahl und $d \in \mathbb{Z}$ quadratfrei. Setze $K := \mathbb{Q}(\sqrt{d})$. Wir betrachten wieder die beiden Fälle

$d \equiv 1\ (4)$ *Wie im vorangegangen Beispiel gesehen ist*

$$B = \mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - X + a)$$

mit $a = \frac{d-1}{4}$. Die Diskriminante von $X^2 - X + a$ ist d also gilt mit der Folgerung:
Wenn (p) nicht (2) teilt, ist (p) genau dann Unverzweigt, wenn d von p geteilt wird.
Das einzige Primideal, das (2) teilt, ist (2) selber. Mit dem Nachtrag zum vorangegangen Beispiel wissen wir: Gilt $(2) = (p)$, genau dann ist (p) unverzweigt, wenn d von 2 geteilt wird.
Wir können also alles in einen Fall zusammenziehen und wissen nun:
(p) ist genau dann unverzweigt in $\mathcal{O}_K$, wenn d von p geteilt wird.

$d \equiv 2, 3\ (4)$ *In diesem Fall erhalten wir*

$$B = \mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - d)$$

Die Diskriminante des Polynoms $X^2 - d$ ist $4d$, also gilt mit der Folgerung:
(p) ist genau dann unverzweigt in $\mathcal{O}_K$, wenn $4d$ von p geteilt wird.

Definition 10.12 *(Voll verzeigt)*
Sei $\mathfrak{p}\, B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p}$ in B. Wir sagen $\mathfrak{p}$ ist voll verwzeigt, wenn $r = 1$ ist.

Bemerkung 10.13 *In der Situation von Definition 10.12 folgen aus der Bedingung $r = 1$:*

$$f(\mathfrak{P} \,/\, \mathfrak{p}) = 1 \quad \text{und} \quad e(\mathfrak{P} \,/\, \mathfrak{p}) = [L : K] = n$$

also ist $\mathfrak{p}\, B = \mathfrak{P}^n$ die Zerlegung von $\mathfrak{p}$ in B. Ist andererseits die Zerlegung von dieser Form, so folgt sofort $r = 1$, also sind diese Bedingungen äquivalent.

11 Das quadratische Reziprozitätsgesetz

Sei $p \in \mathbb{N}$ eine ungerade Primzahl, das heißt $p \neq 2$. Setze $L = \mathbb{Q}(\zeta_p)$ mit einer p-ten Einheitswurzel $\zeta_p := e^{\frac{2\pi i}{p}}$. Wir wissen

$$\mathcal{O}_L = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[X]/(\phi_p) \qquad \text{mit } \phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1$$

Ebenfalls kennen wir die Diskriminante

$$D_L = D(\phi_p) = (-1)^{p-1} 2 \cdot p^{p-2}$$

Für eine weitere Primzahl $l \in \mathbb{N}$ gilt mit Folgerung 10.11 aus dem letzten Abschnitt:
Genau dann ist (l) verzweigt in L, wenn D_L von l geteilt wird.
Die einzige Primzahl, die D_L teilen kann ist p und es gilt

$$p\, \mathcal{O}_L = (1 - \zeta_p)^{p-1}$$

Das Ideal $(1 - \zeta_p)$ ist ein Primideal in $\mathcal{O}_L$, also ist $\mathfrak{p}$ voll verzweigt. Wir halten die hier eingeführten Bezeichnungen für diesen Abschnitt fest.

Satz 11.1 *Sei $l \in \mathbb{N}$ eine Primzahl mit $l \neq p$ und sei*

$$l\,\mathbb{Z}[\zeta_p] \;=\; l\,\mathcal{O}_L \;=\; \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

die Primidealzerlegung von l in $\mathcal{O}_L$. Dann gilt

$$f(\mathfrak{P}_1\,/(l)) \;=\; \ldots \;=\; f(\mathfrak{P}_r\,/(l)) \;=:\; f_l$$

und f_l ist die kleinste Zahl mit $l^{f_l} \equiv 1$ mod p.
Insbesondere gilt

$$[L:\mathbb{Q}] \;=\; [\mathbb{Q}(\zeta_p):\mathbb{Q}] \;=\; p-1 \;=\; \sum_{i=1}^{r} e(\mathfrak{p}_i\,/(l)) \cdot f(\mathfrak{P}_i\,/(l)) \;=\; r \cdot f_l$$

Damit erhalten wir weiterhin eine Gleichung für r, denn es gilt $r \;=\; \frac{p-1}{f_l}$.

Beweis. Sei $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ ein Primideal, das über (l) liegt dann hat fp über (l) Verzweigungsindex $e(\mathfrak{P}\,/(l)) = 1$, denn l ist wegen $l \neq p$ unverzweigt. Es gilt also

$$f(\mathfrak{P}\,/(l)) \;=\; \left[\mathcal{O}_L\!\diagup_{\mathfrak{p}} \,:\, \mathbb{F}_l\right]$$

Behauptung $\mathcal{O}_L\!\diagup_{\mathfrak{P}}$ *ist der Zerfällungskörper von $X^p - 1$ über $\mathbb{F}_l$.*

Beweis. Es gilt

$$X^p - 1 \;=\; \prod_{i=0}^{p-1}(X - \zeta_p^i) \;\text{ in }\; \mathcal{O}_L \qquad \text{also} \qquad X^p - 1 \;=\; \prod_{i=0}^{p-1}(X - \overline{\zeta}_p^{\,i}) \;\text{ in }\; \mathcal{O}_L\!\diagup_{\mathfrak{P}}$$

Damit zerfällt $X^p - 1$ über $\mathcal{O}_L\!\diagup_{\mathfrak{P}}$. Dieser Körper ist aber gerade durch die Einheitswurzeln ζ_p^i erzeugt, denn

$$\mathbb{Z}[\zeta_p] \;\twoheadrightarrow\; \mathbb{Z}[\zeta_p]\!\diagup_{\mathfrak{P}} \;=\; \mathcal{O}_L\!\diagup_{\mathfrak{P}}$$

$\diamond$

Weiterhin zerfällt $X^p - 1$ genau dann über $\mathbb{F}_{l^{f_l}}$, wenn $\sharp\big(\mathbb{F}_{l^{f_l}}\big)^* = l^{f_l} - 1$ von p geteilt wird, nach dem Satz von Lagrange. Sei nun $f_l \in \mathbb{N}$ die kleinste Zahl für die gilt p teilt $l^{f_l} - 1$, dann ist $\mathbb{F}_{l^{f_l}}$ der Zerfällungskörper von $X^p - 1$. Da alle Zerfällungskörper bis auf eindeutige Isomorphie eindeutig sind, gilt dann wegen der Behauptung $f(\mathfrak{P}\,/(l)) \;=\; f_l$ für alle $\mathfrak{P}$ über (l). $\square$

Lemma 11.2 *Sei A ein Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(A)$.*
Weiter sei L/K eine endliche separable Körpererweiterung und $B := \overline{A}$ bezeichne den ganzen Abschluss von A in L. Sei hierzu M/L eine weitere endliche separable Körpererweiterung und $C := \overline{B}$ bezeichne den ganzen Abschluss von B in M. Weiter sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein Primideal. Wähle hierzu $\mathfrak{P} \in \mathrm{Spm}(B)$ mit $\mathfrak{P}$ liegt über $\mathfrak{p}$ und $\mathfrak{P}' \in \mathrm{Spm}(C)$ so dass $\mathfrak{P}'$ über $\mathfrak{P}$ liegt. Dann gelten

$$\begin{array}{ccccc} M & \supset & C & & \mathfrak{P}' \in \mathrm{Spm}(C) \\ \cup & & \cup & & \\ L & \supset & B & & \mathfrak{P} \in \mathrm{Spm}(B) \\ \cup & & \cup & & \\ K & \supset & A & & \mathfrak{p} \in \mathrm{Spm}(A) \end{array}$$

$$f(\mathfrak{P}'\,/\,\mathfrak{p}) \;=\; f(\mathfrak{P}'\,/\,\mathfrak{P}) \cdot f(\mathfrak{P}\,/\,\mathfrak{p}) \quad \text{und} \quad e(\mathfrak{P}'\,/\,\mathfrak{p}) \;=\; e(\mathfrak{P}'\,/\,\mathfrak{P}) \cdot e(\mathfrak{P}\,/\,\mathfrak{p})$$

Beweis. Für den Trägheitsgrad f betrachte den „Turm“ von Körpererweiterungen

$$A/\mathfrak{p} \subseteq B/\mathfrak{P} \subseteq C/\mathfrak{P}'$$

Mit dem Gradsatz folgt nun die Behauptung, denn

$$\left[C/\mathfrak{P}' : A/\mathfrak{p}\right] = \left[C/\mathfrak{P}' : B/\mathfrak{P}\right] \cdot \left[B/\mathfrak{P} : A/\mathfrak{p}\right]$$

Die Gleichung für den Verzweigungsindex e folgt aus der eindeutigen Faktorisierung in Primideale (Faktorisiere erst $\mathfrak{p}$ in B und faktorisiere dann jeden Faktor von $\mathfrak{p}\,B$ in C). □

Bemerkung 11.3 *Sei G eine endlich erzeugte zyklische Gruppe mit erzeugendem Element γ. Sei weiter n die Ordnung von G, dann gilt*

$$G = <\gamma> = \{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$$

Die Untergruppen von G sind gegeben durch

$$U_d = <\gamma^d> \leq G \qquad \text{mit } d|n = \sharp G$$

Dann ist natürlich $\sharp U_d = \frac{n}{d}$ und insbesondere gilt: Ist die Ordnung von G gerade, dann gibt es eine eindeutig bestimmte Untergruppe $H \leq G$ mit

$$[G : H] = 2 \quad \text{und} \quad H = \{\, g^2 \mid g \in G \,\} = <\gamma^2>$$

Ist weiter $U \leq G$ eine Untergruppe deren Index in G gerade ist, das heißt 2 teilt $[G : U]$, so ist U eine Untergruppe von H.

Definition 11.4 *(Legendre-Symbol)*
Sei $p \in \mathbb{N}$ eine ungerade Primzahl, dann bezeichnen wir die Abbildung

$$\begin{aligned} \left(\frac{*}{p}\right) : \mathbb{F}_p^* &\to \{\pm 1\} \\ a &\mapsto \left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ ein Quadrat in } \mathbb{F}_p \text{ ist.} \\ -1 & \text{falls } a \text{ kein Quadrat in } \mathbb{F}_p \text{ ist.} \end{cases} \end{aligned}$$

als das Legendre-Symbol.

Satz 11.5 *Sei $p \in \mathbb{N}$ eine ungerade Primzahl, dann setze $p^* := (-1)^{\frac{p-1}{2}} \cdot p$. Dann gilt*

$$p^* = \begin{cases} p & \text{falls } p \equiv 1\ (4) \\ -p & \text{falls } p \equiv 3\ (4) \end{cases}$$

Also ist $p^* \equiv 1\ (4)$ für alle Primzahlen $p > 2$. Weiter gilt: Die Körpererweiterung $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ enthält genau einen quadratischen Zwischenkörper $K = \mathbb{Q}(\sqrt{p^*})$.

Beweis. Setze $L := \mathbb{Q}(\zeta_p$. Die Erweiterung $L/\mathbb{Q}$ ist galoisch mit Galoisgruppe

$$G = \mathrm{Gal}(L/\mathbb{Q}) \cong \left(\mathbb{Z}/p\,\mathbb{Z}\right)^\times = \mathbb{F}_p^*$$

Diese Gruppe ist zyklisch. Nach Bemerkung 11.3 gibt es nur eine Untergruppe $H \leq G$ mit $[G : H] = 2$. Nach dem Hauptsatz der Galois-Theorie gibt es dann auch nur einen Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_p)$ mit $[K : \mathbb{Q}] = 2$, nämlich den Fixkörper $K = L^H = \big(\mathbb{Q}(\zeta_p)\big)^H$

Behauptung $K = \mathbb{Q}(\sqrt{p^*})$.

Diese Behauptung wollen wir auf drei alternativen Wegen zeigen. Wir beginnen mit

Beweis 1 (Vandermondsche Determinante)
Es gilt

$$\sqrt{D_L} = \sqrt{(-1)^{\frac{p-1}{2}} \cdot p^{p-2}} = p^{\frac{p-1}{2}} \cdot \sqrt{p^*} \in \mathbb{Q}(\zeta_p)$$

Beweis 2 (Verzweigtheit von Idealen)
Sei $l \in \mathbb{N}$ eine Primzahl mit $l \neq p$. Wir haben zu beginn dieses Abschnittes gesehen, dass (l) dann unverzweigt in $L = \mathbb{Q}(\zeta_p)$ ist. Nach dem vorangegangen Lemma 11.2 ist (l) dann auch in jedem Zwischenkörper von L und $\mathbb{Q}$ unverzweigt.
Insbesondere folgt also, dass alle Primzahlen $l \neq p$ unverzweigt in $\mathbb{Q}(\sqrt{d})$ sind. Wir erinnern uns an die Bedingungen dafür, dass (l) in $\mathbb{Q}(\sqrt{d})$ unverzweigt ist:

($d \equiv 1\ (4)$): (l) ist genau dann unverzweigt in $\mathbb{Q}(\sqrt{d})$, wenn d nicht von l geteilt wird.

($d \equiv 2, 3\,(4)$): (l) ist genau dann unverzweigt in $\mathbb{Q}(\sqrt{d})$, wenn $4d$ nicht von l geteilt wird.

Damit können wir den zweiten Fall direkt ausschließen, denn 2 teilt $4d$ und p ist ungerade. Im ersten Fall folgt aber schon, dass $d = p^*$ ist, denn d muss die folgenden Bedingungen erfüllen

1. d ist quadratfrei in $\mathbb{Z}$
2. $d \in \{\, \pm p^\alpha \mid \alpha \in \mathbb{N} \,\}$
3. $d \equiv 1$ modulo 4

Beweis 3 (Gaußsche Summen)
Wir wollen das kurz zuvor eingeführte Legendre-Symbol betrachten. Wir setzen

$$\tau := \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \cdot \zeta_p^a \in \mathbb{Q}(\zeta_p)$$

Behauptung 2 $\tau^2 = \left(\frac{-1}{p}\right) \cdot p$

Begründung. Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Betrachte

$$\begin{aligned}
\left(\frac{-1}{p}\right)\cdot\tau^2 &= \sum_{a,b\in\mathbb{F}_p}\left(\frac{-ab}{p}\right)\cdot\zeta_p^{a+b} \\
&\overset{c:=-b}{=} \sum_{a,c\in\mathbb{F}_p}\left(\frac{ac}{p}\right)\cdot\zeta_p^{a-c} = \sum_{a,c\in\mathbb{F}_p}\left(\frac{ac^{-1}}{p}\right)\cdot\zeta_p^{a-c} \\
&\overset{d:=ac^{-1}}{=} \sum_{d,c\in\mathbb{F}_p}\left(\frac{d}{p}\right)\cdot\zeta_p^{cd-c} \\
&= \sum_{\substack{d\in\mathbb{F}_p\\ d\neq 1}}\left(\frac{d}{p}\right)\sum_{c\in\mathbb{F}_p^*}\zeta_p^{c(d-1)} + \sum_{c\in\mathbb{F}_p^*}\left(\frac{1}{p}\right) \\
&= \sum_{\substack{d\in\mathbb{F}_p\\ d\neq 1}}\left(\frac{d}{p}\right)\sum_{c\in\mathbb{F}_p^*}\zeta_p^{c(d-1)} + (p-1)
\end{aligned}$$

Für $d \neq 1$ ist $z := \zeta_p^{d-1}$ eine primitive p-te Einheitswurzel. Es gilt

$$\sum_{c\in\mathbb{F}_p^*}\zeta_p^{c(d-1)} = \sum_{c\in\mathbb{F}_p^*} z^c = z + z^2 + \ldots + z^{p-1} = -1$$

Betrachte nun die andere Summe. Wähle hierzu ein $a \in \mathbb{F}_p^*$, welches kein Quadrat in $\mathbb{F}_p$ ist. Dann gilt

$$\left(\frac{a}{p}\right)\cdot\sum_{d\in\mathbb{F}_p}\left(\frac{d}{p}\right) = \sum_{d\in\mathbb{F}_p}\left(\frac{ad}{p}\right) \overset{b:=ad}{=} \sum_{b\in\mathbb{F}_p}\left(\frac{b}{p}\right)$$

Wir dürfen die Laufvariable b natürlich auch wieder d nennen und erhalten dann durch Subtraktion der beiden Seiten die Gleichung

$$\sum_{d\in\mathbb{F}_p}\left(\frac{d}{p}\right)\cdot\left(1-\left(\frac{a}{p}\right)\right) = 0$$

Nach Wahl von a ist $\left(1-\left(\frac{a}{p}\right)\right) = 2$ und wir rechnen in einem Integritätsring. Also muss

$$\sum_{d\in\mathbb{F}_p}\left(\frac{d}{p}\right) = 0$$

gelten. Dann erhalten wir aber

$$\sum_{\substack{d\in\mathbb{F}_p\\ d\neq 1}}\left(\frac{d}{p}\right) = -1$$

Damit folgt aber Behauptung 2 ◇

Behauptung 2 impliziert nun $\mathbb{Q}(p^*) = \mathbb{Q}(\tau) \subseteq \mathbb{Q}(\zeta_p)$, was einen dritten Beweis für die eingangs aufgestellte Behauptung lieftert. Insgesamt folgt damit auch der Satz. □

Satz 11.6 *Sei A ein Dedekindring mit Quotientenkörper $K = \mathrm{Quot}(A)$. Sei weiter L/K eine endliche galois Erweiterung mit $G := \mathrm{Gal}(L/K)$. Bezeichne B den ganzen Abschluss von A in L. Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein Primideal, dann operiert die Galoisgruppe G transitiv auf der Menge*

$$\{\, \mathfrak{P} \in \mathrm{Spm}(B) \mid \mathfrak{p} = \mathfrak{P} \cap B \,\}$$

der Primideale von B, die über $\mathfrak{p}$ liegen. Ist weiter

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

eine Zerlegung von $\mathfrak{p}$ in B, dann gelten

$$e_1 = e_2 = \ldots = e_r =: e \quad \text{und} \quad f_1 = f_2 = \ldots = f_r =: f$$

mit $f_i = f(\mathfrak{P}_i \,/\, \mathfrak{p})$. Insbesondere gilt $n = [L : K] = r \cdot e \cdot f$.

Beweis. Der Beweis dieses Satzes folgt im nächsten Abschnitt.

Satz 11.7 *Seien $l, p \in \mathbb{N}$ Primzahlen mit $l \neq p$ und $p > 2$. Setze*

$$L \;:=\; \mathbb{Q}(\zeta_p) \;\supseteq\; \mathbb{Q}(\sqrt{p^*}) \;=:\; K$$

und sei weiter $l\,\mathcal{O}_L \;=\; \mathfrak{P}_1 \cdots \mathfrak{P}_r$ die Primidealzerlegung des von l in $\mathcal{O}_L$ erzeugten Ideals. Die folgenden Bedingungen sind äquivalent:

(i) *Die Galoisgruppe $\mathrm{Gal}(L/K)$ operiert transitiv auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$.*

(ii) *r ist ungerade.*

(iii) *l ist träge in K, das heißt $l\,\mathcal{O}_K$ ist prim in $\mathcal{O}_K$.*

Beweis. Wir zeigen zunächst „**(i)** $\Leftrightarrow$ **(ii)**“. Betrachte dazu die Untergruppe

$$S \;:=\; \left\{\, g \in \mathrm{Gal}(L/\mathbb{Q}) \,\middle|\, g(\mathfrak{P}_1) \;=\; \mathfrak{P}_1 \,\right\} \;\leq\; \mathrm{Gal}(L/\mathbb{Q})$$

Nach Satz 11.6 operiert $\mathrm{Gal}(L/\mathbb{Q})$ transitiv auf $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$, damit folgt

$$\mathrm{Gal}(L/\mathbb{Q}) \;:\; S] \;=\; r$$

Mit dieser Vorüberlegung können wir nun schließen: $\mathrm{Gal}(L/K)$ operiert genau dann transitiv, wenn die Abbildung

$$\mathrm{Gal}(L/K) \;\to\; {}^{\mathrm{Gal}(L/\mathbb{Q})}\!/_{S}$$

surjektiv ist. Dies ist aber genau dann der Fall, wenn S keine Untergruppe von $\mathrm{Gal}(L/K)$ ist. S ist genau dann keine Untergruppe von $\mathrm{Gal}(L/K)$, wenn r ungerade ist.
Als nächstes zeigen wir „**(iii)** $\Leftrightarrow$ **(i)**“. Nach Voraussetzung ist $l\,\mathcal{O}_K$ ein Primideal. In diesem Fall ist $(l\,\mathcal{O}_K)\,\mathcal{O}_L \;=\; \mathcal{O}_L$ und mit Satz 11.6 folgt die Behauptung.
Wir müssen nun nur noch „**(i)** $\Leftrightarrow$ **(iii)**“ nachweisen. Dazu nehmen wir an, dass $l\,\mathcal{O}_K$ nicht prim sei, also etwa in die Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Spm}(\mathcal{O}_K$ zerfalle. Dann gäbe es Ideale $\mathfrak{P}_1, \mathfrak{P}_2 \in \mathrm{Spm}(\mathcal{O}_L)$ mit $\mathfrak{p}_i \;=\; \mathfrak{P}_i \cap \mathcal{O}_K$ für $i = 1, 2$. Nach Voraussetzunh operiert $\mathrm{Gal}(L/K)$ transitiv auf $\{\mathfrak{P}_1, \mathfrak{P}_2\}$, also gäbe es ein $g \in \mathrm{Gal}(L/K)$ mit $g(\mathfrak{P}_2) = \mathfrak{p}_1$ und wir erhielten die Gleichung

$$\mathfrak{p}_1 \;=\; \mathfrak{P}_1 \cap \mathcal{O}_K \;=\; g(\mathfrak{P}_2) \cap \mathcal{O}_K \;=\; g(\mathfrak{p}_2) \;=\; \mathfrak{p}_2$$

Dies wäre aber ein Widerspruch zur unverzweigtheit von l in K. □

Bemerkung 11.8 *Wir haben weiter oben in Definition 11.4 für eine ungerade Primzahl p das Legendre-Symbol als eine Abbildung*

$$\begin{aligned}\left(\frac{*}{p}\right) : \mathbb{F}_p^* &\to \{\pm 1\} \\ a &\mapsto \left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ ein Quadrat in } \mathbb{F}_p \text{ ist.} \\ -1 & \text{falls } a \text{ kein Quadrat in } \mathbb{F}_p \text{ ist.} \end{cases}\end{aligned}$$

eingeführt. Wir können den Definitionsbereich aber problemlos auf die Menge

$$\{\, a \in \mathbb{Z} \mid \mathrm{ggT}(a,p) = 1 \,\}$$

ausweiten. Es gilt dann

$$a \equiv b \ (p) \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Mit dem folgenden Satz sammeln wir die bisherigen Ergebnisse des Abschnittes ein und bereiten das Theorem über das quadratische Reziprozitätsgesetz vor.

Satz 11.9 *Seien $p, l \in \mathbb{N}$ Primzahlen mit $l \neq p$ und $p > 2$, dann sind die folgenden Aussagen äquivalent:*

1. $\left(\frac{l}{p}\right) = 1$
2. $l^{\frac{p-1}{2}} \equiv 1$ *modulo* (p)
3. *Ist $f_l \in \mathbb{N}$ die kleinste Zahl mit $l^{f_l} \equiv 1$ modulo (p), dann wird $\frac{p-1}{2}$ von f_l geteilt*
4. $\frac{p-1}{f_l}$ *ist gerade*
5. *Sei $l\,\mathbb{Z}[\zeta_p] = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ die Zerlegung des von l in $\mathbb{Z}[\zeta_p]$ erzeugten ideals, dann ist r gerade, denn $r = \frac{p-1}{f_l}$ nach Satz 11.1*
6. *l zerfällt in $\mathbb{Q}(\sqrt{p^*})$*
7. $X^2 - X + \frac{1-p^*}{4}$ *zerfällt in $\mathbb{F}_l$*
8. *<u>Entweder</u> ist $l \neq 2$ und es gilt $\left(\frac{p^*}{l}\right) = 1$ <u>oder</u> $l = 2$ und es gilt $p^* \equiv 1$ modulo (8)*

Bemerkung 11.10 *(Ergänzungssätze)*
Sei $p \in \mathbb{N}$ eine ungerade Primzahl, dann gelten

$$\left(\frac{2}{p}\right) = 1 \ \Leftrightarrow \ p^* \equiv 1 \ (8) \ \Leftrightarrow \ \begin{cases} p \equiv 1 \ (8) \\ p \equiv 7 \ (8) \end{cases}$$

$$\left(\frac{2}{p}\right) = -1 \ \Leftrightarrow \ p^* \equiv 5 \ (8) \ \Leftrightarrow \ \begin{cases} p \equiv 5 \ (8) \\ p \equiv 3 \ (8) \end{cases}$$

Es folgt der erste Ergänzungssatz

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Der zweite Ergänzungssatz ist klar

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Satz 11.11 *(Das quadratische Reziprozitätsgesetz)*
Seien $l, p \in \mathbb{N}_{>2}$ Primzahlen mit $l \neq p$, dann gilt

$$\left(\frac{l}{p}\right) \cdot \left(\frac{p}{l}\right) \;=\; (-1)^{\frac{p-1}{2}\,\frac{l-1}{2}}$$

Beweis. Nach dem Vorangegangenen Satz gilt

$$\begin{aligned}\left(\frac{p}{l}\right) \;&=\; \left(\frac{l^*}{p}\right) \;=\; \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) \\ &=\; \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} \left(\frac{l}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \left(\frac{l}{p}\right)\end{aligned}$$

Wegen $\left|\left(\frac{l}{p}\right)\right| = 1$ folgt die Behauptung. □

Lemma 11.12 *Sei $(G, +)$ eine endliche abelsche Gruppe. Dann ist G genau dann zyklisch, wenn für alle Primzahlen p, die die Ordnung von G teilen, gilt*

$$\sharp\left\{\, g \in G \,\middle|\, g^p = 1 \,\right\} \;=\; 1$$

Beweis. Sei $\sharp G = n < \infty$ dann betrachte die Primfaktorzerlegung

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

in paarweise verschiedene Primzahlen p_i. Via

$$z \cdot g \;:=\; \begin{cases} \underbrace{g + \ldots + g}_{z\text{ -mal}} & \text{falls } z > 0 \\ \underbrace{(-g) + \ldots + (-g)}_{|z|\text{ -mal}} & \text{falls } z < 0 \\ 0_G & \text{falls } z = 0 \end{cases}$$

können wir G als einen endlich erzeugten Torsionsmodul über $\mathbb{Z}$ auffassen. Mit dem Struktursatz über endlich erzeugte Torsionsmoduln über Hauptidealringen folgt nun

$$G \;\cong\; G_1 \times \ldots \times G_r \qquad \text{mit } \sharp G_i \;=\; p_i^{\alpha_i}$$

Wir können diese Gruppen noch einmal weiter zerlegen in

$$G_i \;\cong\; G_{i,1} \times \ldots \times G_{i,r_i} \quad \text{mit } G_{i,j} \;=\; {}^{\mathbb{Z}}\!/_{p^{a_{i,j}}\,\mathbb{Z}}$$

Insgesamt gilt: Die Gruppe G ist gnau dann zyklisch, wenn alle G_i zyklisch sind. Eine Gruppe G_i ist genau dann zyklisch, wenn gilt

$$\sharp\left\{\, g \in G_i \,\middle|\, g^p = 1 \,\right\} \;=\; 1$$

□

Folgerung 11.13 *Sei $p \in \mathbb{N}$ eine Primzahl, dann ist die Einheitengruppe $\mathbb{F}_p^*$ des endlichen Körpers $\mathbb{F}_p$ zyklisch.*

Beweis. Sei $l \in \mathbb{N}$ eine Primzahl, die $p-1 = \sharp\,\mathbb{F}_p^*$ teilt, dann gilt

$$\sharp\big\{\, x \in \mathbb{F}_p^* \;\big|\; x^l - 1 = 0 \,\big\} \;=\; l$$

Denn dann gibt es ein $\alpha \in \mathbb{F}_p^*$ mit $\mathrm{Ord}(\alpha) = l$, also sind $\alpha, \alpha^2, \ldots, \alpha^l$ die verschiedenen Nullstellen von $f = X^l - 1$ und f hat wegen $\deg(f) = l$ höchstens l verschiedene Nullstellen. □

Folgerung 11.14 *Sei $p \in \mathbb{N}_{>2}$ eine Primzahl, dann gilt: $a \in \mathbb{F}_p^*$ ist genau dann ein Quadrat, wenn $a^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p$ ist.*

Beweis. Für $a \in \mathbb{F}_p^*$ gilt

$$\left(a^{\frac{p-1}{2}}\right)^2 \;=\; a^{p-1} \;=\; 1$$

Also ist $a^{\frac{p-1}{2}} \in \{\pm 1\}$. Wir betrachten die Abbildung

$$\begin{array}{rcl} \chi : \mathbb{F}_p^* & \to & \{\pm 1\} \\ a & \mapsto & a^{\frac{p-1}{2}} \end{array}$$

Die Abbildung χ ist surjektiv, denn andernfalls wäre $a^{\frac{p-1}{2}} = 1$ für alle $a \in \mathbb{F}_p^*$. Dann teilte $\sharp\,\mathbb{F}_p^*$ aber $\frac{p-1}{2}$, denn $\mathbb{F}_p^*$ ist nach vorangegangener Folgerung zyklisch. Dies kann aber nicht sein. Weiter gilt

$$\sharp\,\mathrm{Ker}(\chi) \;=\; \frac{p-1}{2}$$

Betrachte nun die Abbildung

$$q : \mathbb{F}_p^* \ni x \mapsto x^2 \in FF_p^*$$

Dann ist offensichtlich $\mathrm{Ker}(q) = \{\pm 1\}$ also folgt

$$\sharp\,\mathrm{Im}(q) \;=\; \frac{\sharp\,\mathbb{F}_p^*}{\sharp\,\mathrm{Ker}(q)} \;=\; \frac{p-1}{2}$$

Weiter gilt $\chi \circ q(a) = a^{p-1} = 1$, also ist

$$\mathrm{Im}(q) \;\subseteq\; \mathrm{Ker}(\chi)$$

Wegen der Anzahl der Elemente in beiden Mengen gilt dann

$$\mathrm{Im}(q) \;=\; \mathrm{Ker}(\chi)$$

und damit folgt

$$a^{\frac{p-1}{2}} = 1 \quad\Leftrightarrow\quad a = b^2 \quad \text{für ein } b \in \mathbb{F}_p^*$$

□

12 Verhalten von Primidealen in Galoiserweiterungen

Auch in diesem Abschnitt haben wir wieder ein paar Bezeichnungen, die wir über den ganzen Abschnitt beibehalten wollen:

> A bezeichne in diesem Abschnitt wieder einen Dedekindring und $K := \mathrm{Quot}(A)$ seinen Quotientenkörper. Weiter sei L/K diesmal eine endliche Galoiserweiterung und $B := \overline{A}$ bezeichne den ganzen Abschluss von A in L. Schließlich bezeichne noch $G := \mathrm{Gal}(L/K)$.

In diesem Abschnitt knüpfen wir an die Ergebnisse aus Abschnitt 10 an. Da wir nun eine Galoiserweiterung voraussetzen können wir mit erheblich mehr Mitteln die Primideale von B und A untersuchen. Die Erkenntnisse aus Abschnitt 10 können wir hier ebenfalls benutzen, den Galoiserweiterungen sind insbesondere separabel. Wir wollen die oben eingeführte Konstellation nun zunächst wieder auf grundlegende Eigenschaften untersuchen:

Sei $\alpha \in L$. Genau dann gilt $\alpha \in B$, wenn das Minimalpolynom f_α von α über K bereits in $A[X]$ liegt. Wegen dieser Eigenschaft ist $\sigma(B) \subseteq B$ für alle $\sigma \in G$, also ist insbesondere auch $\sigma^{-1}(B) \subseteq B$ für alle $\sigma \in G$. Insgesamt gilt also

$$\sigma(B) \;=\; B \quad \text{für alle } \sigma \in G$$

Aus dem Hauptsatz der Galois-Theorie wissen wir $K = L^G$. Mit der obigen Eigenschaft erhalten wir hieraus

$$B^G \;=\; B \cap K \;=\; A$$

Seien $\mathfrak{p} \in \mathrm{Spm}(A)$ und $\mathfrak{P} \in \mathrm{Spm}(B)$ Primideale mit $\mathfrak{p} = \mathfrak{P} \cap A$, dann folgt weiter

$$\mathfrak{P}^G \;=\; \mathfrak{P} \cap K \;=\; \mathfrak{p}$$

Weiter ist für $\sigma \in G$ die folgende Menge

$$\sigma(\mathfrak{P}) \;:=\; \left\{\, \sigma(p) \,\middle|\, p \in \mathfrak{P} \,\right\}$$

ist ein Ideal von B, denn sei $b \in B$ und $p \in \mathfrak{P}$, dann gilt

$$b \cdot \sigma(p) \;=\; \sigma\big(\sigma^{-1}(b) \cdot p\big) \;\in \sigma(\mathfrak{P})$$

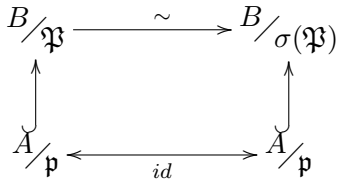
Die Abbildung

$$\begin{array}{rcl} \sigma^* : {}^{B}\!/_{\mathfrak{P}} & \to & {}^{B}\!/_{\sigma(\mathfrak{P})} \\ b + \mathfrak{P} & \mapsto & \sigma(b) + \sigma(\mathfrak{P}) \end{array}$$

ist ein Isomorphismuss, dessen Umkehrabbildung duch σ^{-1} gegeben ist. Dann ist aber insbesondere auch $\sigma(\mathfrak{P})$ ein maximales Ideal in B, da der Quotient ein Körper ist. Wei A im Fixkörper von L unter G enthalten ist, gilt weiter

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

also liegt auch $\sigma(\mathfrak{P})$ über $\mathfrak{p}$ und wir erhalten das Diagramm



Wir können ablesen, dass dann

$$f(\mathfrak{P}\,/\,\mathfrak{p}) \;=\; \left[{}^{B}\!/_{\mathfrak{P}} \,:\, {}^{A}\!/_{\mathfrak{p}}\right] \;=\; \left[{}^{B}\!/_{\sigma(\mathfrak{P})} \,:\, {}^{A}\!/_{\mathfrak{p}}\right] \;=\; f(\sigma(\mathfrak{P})/\,\mathfrak{p})$$

gelten muss. Sei nun $\mathfrak{p}\,B \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p}$ in paarweise verschiedene Primideale in B. Dann ist wegen $\sigma(\mathfrak{p}\,B) \;=\; \mathfrak{p}\,B$ auch $\mathfrak{p}\,B \;=\; \sigma(\mathfrak{p}\,B) \;=\; \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r}$ eine Zerlegung von $\mathfrak{p}\,B$ in maximale Ideale. Die Faktorisierung in Maximalideale ist aber eindeutig, also folgt

$$e(\mathfrak{P}\,/\,\mathfrak{p}) \;=\; e(\sigma(\mathfrak{p})/\,\mathfrak{p}) \qquad \text{für alle } \mathfrak{P} \in \mathrm{Spm}(B) \text{ die über } \mathfrak{p} \text{ liegen.}$$

Als nächstes wollen wir nun den Satz 11.6 beweisen, den wir im vorangegangenen Abschnitt ohne Beweis angegeben hatten.

Satz 11.6 *G operiert transitiv auf der Menge $\left\{\; \mathfrak{P} \in \mathrm{Spm}(B) \;\middle|\; \mathfrak{P} \cap A = \mathfrak{p} \;\right\}$.*

Beweis. Angenommen des Satz wäre falsch, dann gäbe es $\mathfrak{P}_1, \mathfrak{P}_2 \in \mathrm{Spm}(B)$ mit

$$\mathfrak{P}_1 \cap A \;=\; \mathfrak{p} \;=\; \mathfrak{P}_2 \cap A \qquad \text{und} \qquad \mathfrak{P}_1 \neq \sigma(\mathfrak{P}_2) \;\text{ für alle } \sigma \in G$$

Nach dem chinesischen Restsatz gäbe es dann ein $x \in B$ mit

$$\begin{aligned} x \;&\equiv\; 0 \;\text{ modulo } \mathfrak{P}_1 \\ x \;&\equiv\; 1 \;\text{ modulo } \sigma(\mathfrak{P}_2) \;\text{ für alle } \sigma \in G \end{aligned}$$

Für alle $\sigma \in G$ ist genau dann $x \equiv 1$ modulo $\sigma(\mathfrak{P}_2)$, wenn $\sigma^{-1}(x) \equiv 1$ modulo $\mathfrak{P}_2$ ist. Demnach folgte

$$N \;:=\; N_K^L(x) \;=\; \prod_{\sigma \in G} \sigma(x) \;\equiv\; 1 \;\text{ modulo } \mathfrak{P}_2$$

Also wäre insbesondere $N - 1 \in \mathfrak{P}_2 \cap K = \mathfrak{p}$. Weil auch $\mathfrak{P}_1$ über $\mathfrak{p}$ liegt, wäre dann aber auch

$$N \;\equiv\; 1 \;\text{ modulo } \mathfrak{P}_1$$

Wei aber N in B von x geteilt würde, gülte ebenfalls

$$N \;\equiv\; 0 \;\text{ modulo } \mathfrak{P}_1$$

Und dies hieße $1 \equiv 0$ modulo $\mathfrak{P}_1$, was ein Widerspruch ist. □

Folgerung 12.1 *Sei $\mathfrak{p}\,B \;=\; \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Primfaktorzerlegung von $\mathfrak{p}$ in B in paarweise verschiedene Maximalideale. Setze $f_i \;:=\; f(\mathfrak{P}_i\,/\,\mathfrak{p})$ dann gelten*

$$e_1 = \ldots = e_r \;=:\; e_{\mathfrak{p}} \qquad \text{und} \qquad f_1 = \ldots = f_r \;=:\; f_{\mathfrak{p}}$$

Beweis. Für alle $j = 1, \ldots, r$ gibt es ein $\sigma \in G$ mit $\sigma(\mathfrak{P}_1) = \sigma_j$. Damit folgen sofort

$$f(\mathfrak{P}_j \,/\, \mathfrak{p}) \;=\; f(\mathfrak{P}_1 \,/\, \mathfrak{p}) \qquad \text{und} \qquad e(\mathfrak{P}_j \,/\, \mathfrak{p}) \;=\; e(\mathfrak{P}_1 \,/\, \mathfrak{p})$$

für alle $j = 1, \ldots, r$. □

Folgerung 12.2 *In der Situation von Folgerung 12.1 gilt*

$$[L : K] \;=\; r \cdot e_{\mathfrak{p}} \cdot f_{\mathfrak{p}} \;=\; \sum_{i=1}^{r} f_i \cdot e_i$$

□

Definition 12.3 *(Zerlegungsgruppe, Zerlegungskörper)*
Seien $\mathfrak{p} \in \mathrm{Spm}(A)$ und $\mathfrak{P} \in \mathrm{Spm}(B)$ Primideale mit $\mathfrak{p} = \mathfrak{P} \cap A$, dann nennen wir die Untergruppe

$$G_{\mathfrak{P}} \;:=\; \left\{ \sigma \in G \,\middle|\, \sigma(\mathfrak{P}) \;=\; \mathfrak{P} \right\} \;\leq\; \mathrm{Gal}(L/K)$$

die Zerlegungsgruppe von $\mathfrak{P}$. Und den Fixkörper von L unter dieser Gruppe, also

$$Z_{\mathfrak{P}} \;:=\; L^{G_{\mathfrak{P}}}$$

nennen wir den Zerlegungskörper von $\mathfrak{P}$.

Bemerkung 12.4 *Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ und $\mathfrak{p}\, B \;=\; \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$ mit $e := e_{\mathfrak{p}}$ die Primfaktorzerlegung von $\mathfrak{p}$ in B in paarweise verschiedene Maximalideale. Dann ist für alle $i = 1, \ldots, r$ die Abbildung*

$$\begin{array}{rcl} {}^{G}\!/_{G_{\mathfrak{P}_i}} & \to & \left\{ \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r \right\} \\ \sigma & \mapsto & \sigma(\mathfrak{P}_i) \end{array}$$

eine Bijektion. Also gelten

$$[G : G_{\mathfrak{P}_i}] \;=\; r \qquad \text{und} \qquad \sharp G_{\mathfrak{P}_i} \;=\; e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$$

für alle $i = 1, \ldots, r$. Wir erhalten die beiden nützlichen Äquivalenzen

- *Die Gruppen $G_{\mathfrak{P}_i}$ bestehen genau dann aus je einem Element, wenn $\mathfrak{p}$ voll verzweigt ist.*
- *Genau dann ist $G_{\mathfrak{P}} = G$ für ein $\mathfrak{P}$ über $\mathfrak{p}$, wenn $\mathfrak{P}$ das einzige Primideal in B ist, das über $\mathfrak{p}$ liegt.*

Weiter gilt

$$G_{\sigma(\mathfrak{P}_i)} \;=\; \sigma \circ G_{\mathfrak{P}_i} \circ \sigma^{-1} \qquad \text{für alle } i = 1, \ldots, r$$

Ist G insbesondere abelsch, so gilt ausserdem $G_{\mathfrak{P}_i} = G_{\mathfrak{P}_j}$ für alle $i, j = 1, \ldots, r$.

Satz 12.5 *Seien* $\mathfrak{p} \in \mathrm{Spm}(A)$ *und* $\mathfrak{P} \in \mathrm{Spm}(B)$ *Primideale mit* $\mathfrak{p} = \mathfrak{P} \cap A$. *Setze* $\mathfrak{P}_z := \mathfrak{P} \cap Z_{\mathfrak{P}}$, *dann gelten*

(i) $\mathfrak{P}_z$ *ist unzerlegt in* L.

(ii) $e(\mathfrak{P} \,/\, \mathfrak{P}_z) = e_{\mathfrak{p}}$ *und* $f(\mathfrak{P} \,/\, \mathfrak{P}_z) = f_{\mathfrak{p}}$.

(iii) $e(\mathfrak{P}_z \,/\, \mathfrak{p}) = 1 = f(\mathfrak{P}_z \,/\, \mathfrak{p})$.

Beweis. Wir zeigen zunächst Teil **(i)**. Nach Konstruktion des Zerlegungskörpers gilt

$$\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$$

und $\mathfrak{P}$ liegt offensichtlich über $\mathfrak{P}_z$. Nach Satz 11.6 operiert G transitiv auf der Menge der Primideale, die über $\mathfrak{P}_z$ liegen, also folgt aus $\sigma(\mathfrak{P}) = \mathfrak{P}$, dass $\mathfrak{P}$ das einzige Ideal von B über $\mathfrak{P}_z$ ist.
Die Teile **(ii)** und **(iii)** zeigen wir auf einmal. Sei dazu $\mathfrak{p}\, B = \mathfrak{P}_1^{e_{\mathfrak{p}}} \cdots \mathfrak{P}_r^{e_{\mathfrak{p}}}$ die Primfaktorzerlegung von $\mathfrak{p}$ in B in paarweise verschiedene Maximalideale. Nach Folgerung 12.2 gilt

$$[L : K] = r \cdot e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$$

In der vorangegangenen Bemerkung haben wir gezeigt, dass $[G : G_{\mathfrak{P}}] = r$ ist, also gilt

$$[L : Z_{\mathfrak{P}}] = \sharp G_{\mathfrak{P}} = e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$$

Setze nun $e' := e(\mathfrak{P} \,/\, \mathfrak{P}_z)$ und $f' = f(\mathfrak{P} \,/\, \mathfrak{P}_z)$, dann wird $e_{\mathfrak{p}}$ von e' und $f_{\mathfrak{p}}$ von f' geteilt und es gilt

$$e' \cdot f' = [L : Z_{\mathfrak{P}}] = e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$$

Also folgt Teil **(ii)**. Weiter sind dann

$$f(\mathfrak{P}_z \,/\, \mathfrak{p}) = \frac{f_{\mathfrak{p}}}{f'} = 1\, \frac{e_{\mathfrak{p}}}{e'} = e(\mathfrak{P}_z \,/\, \mathfrak{p})$$

□

Satz 12.6 *Seien* $\mathfrak{p} \in \mathrm{Spm}(A)$ *und* $\mathfrak{P} \in \mathrm{Spm}(B)$ *Primideale mit* $\mathfrak{p} = \mathfrak{P} \cap A$, *dann haben wir für alle* $\sigma \in G$ *die Abbildung*

$$\begin{array}{rcl} \overline{\sigma} : {}^{B}\!/_{\mathfrak{P}} & \to & {}^{B}\!/_{\mathfrak{P}} \\ b + \mathfrak{P} & \mapsto & \sigma(b) + \mathfrak{P} \end{array}$$

Mit den Kurznotationen $\kappa(\mathfrak{P}) := {}^{B}\!/_{\mathfrak{P}}$ *und* $\kappa(\mathfrak{p}) := {}^{A}\!/_{\mathfrak{p}}$ *induziert diese Abbildung einen Gruppenhomomorphismus*

$$\varphi : G_{\mathfrak{P}} \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{p})}\left(\kappa(\mathfrak{P})\right)$$

Es gilt: Die Körpererweiterung l/k *ist normal und der oben genannte Gruppenhomomorphismus ist surjektiv.*

Beweis. Nach Satz 12.5 ist $f(\mathfrak{P}_z \,/\, \mathfrak{p}) = 1$ für $\mathfrak{P}_z := \mathfrak{P} \cap Z_{\mathfrak{P}}$. Das heißt aber nichts anderes als

$$[Z_{\mathfrak{P}} : \kappa(\mathfrak{p})] \;=\; 1 \quad \Leftrightarrow \quad Z_{\mathfrak{P}} \;=\; \kappa(\mathfrak{p})$$

Wir befinden uns also ohne Einschränkung in der Situation $\kappa(\mathfrak{p}) = Z_{\mathfrak{P}}$ und $G_{\mathfrak{P}} = G$. Sei nun $\overline{\theta} \in K$ und hierzu $\overline{g} \in \kappa(\mathfrak{p})[X]$ das Minimalpolynom von $\overline{\theta}$ über $\kappa(\mathfrak{p})$. Wähle nun ein $\theta \in B \subset L$, so dass $\overline{\theta} = \theta + \mathfrak{P}$ gilt, und sei $f \in A[X]$ das Minimalpolynom von θ über K. Da L/K galoisch ist, ist L/K insbesondere normal. Also zerfällt f über B in Linearfaktoren

$$f \;=\; (X - \theta_1) \cdots (X - \theta_m) \;\in B[X]$$

Hierbei seien θ_i die Nullstellen von f in B. Betrachte nun f unter der Projektion nach $\kappa(\mathfrak{P})$, dann gilt

$$\overline{f} \;=\; (X - \overline{\theta}_1) \cdots (X - \overline{\theta}_m) \;\in \kappa(\mathfrak{P})[X]$$

also ist insbesondere auch $\overline{\theta}$ eine Nullstelle von $\overline{f}$. Wir können f auch unter der Projektion nach $\kappa(\mathfrak{p})$ betrachten und $\overline{\theta}$ ist immernoch eine Nullstelle von $\overline{f}$ aber $\overline{g}$ war das Minimalpolynom von $\overline{\theta}$ in $\kappa(\mathfrak{p})[X]$, also wird $\overline{f}$ von $\overline{g}$ in $\kappa(\mathfrak{p})[X]$ geteilt. Dann zerfällt $\overline{g}$ aber über $\kappa(\mathfrak{P})$ in Linearfaktoren und wir haben den ersten Teil des Satzes gezeigt.
Sei nun κ der maximal separable Zwischenkörper $\kappa(\mathfrak{p}) \subseteq \kappa \subseteq \kappa(\mathfrak{P})$ dann ist die Erweiterung $\kappa/\kappa(\mathfrak{p})$ galoisch und es gilt

$$\mathrm{Aut}_{\kappa(\mathfrak{p})}\left(\kappa(\mathfrak{P})\right) \;\cong\; \mathrm{Gal}\left(\kappa/\kappa(\mathfrak{p})\right)$$

Nach dem Satz vom primitiven Element gibt es ein $\overline{\theta} \in \kappa$ mit

$$\kappa \;=\; \kappa(\mathfrak{p})(\overline{\theta})$$

Seien nun $\theta, \overline{g}, f$ wie eben, dann gibt es ein $\theta' \in B$ mit $f(\theta') \;=\; 0$ und $\theta' + \mathfrak{P} \;=\; \sigma(\overline{\theta})$ für ein $\sigma \in \mathrm{Gal}\left(\kappa/\kappa(\mathfrak{p})\right)$. Da L/K galoisch ist, gibt es ein $\tilde{\sigma} \in \mathrm{Gal}(L/K)$ mit $\tilde{\sigma}(\theta) \;=\; \theta'$ und damit ist die Abbildung

$$\begin{array}{rcl} G = \mathrm{Gal}(L/K) & \to & \mathrm{Gal}\left(\kappa/\kappa(\mathfrak{p})\right) \\ \tilde{\sigma} & \mapsto & \sigma \end{array}$$

surjektiv. □

Definition 12.7 *(Trägheitsgruppe, - körper)*
Seien $\mathfrak{p} \in \mathrm{Spm}(A)$ und $\mathfrak{P} \in \mathrm{Spm}(B)$ Primideale mit $\mathfrak{p} = \mathfrak{P} \cap A$. Mit dem surjektiven Gruppenhomomorphismus

$$\varphi : G_{\mathfrak{P}} \;\longrightarrow\; \mathrm{Aut}_{\kappa(\mathfrak{p})}\left(\kappa(\mathfrak{P})\right)$$

sowie den Kurznotationen $\kappa(\mathfrak{P}) := {}^{B}\!/_{\mathfrak{P}}$ und $\kappa(\mathfrak{p}) := {}^{A}\!/_{\mathfrak{p}}$ definieren wir die Trägheitsgruppe von $\mathfrak{P}$ als

$$I_{\mathfrak{P}} \;:=\; \mathrm{Ker}(\varphi) \;\leq\; G_{\mathfrak{P}}$$

und den Trägheitskörper $T_{\mathfrak{P}}$ von $\mathfrak{P}$ wieder als Fixkörper von L unter der Trägheitsgruppe, das heißt

$$T_{\mathfrak{P}} \;=\; L^{I_{\mathfrak{P}}}$$

Satz 12.8 *Seien* $\mathfrak{p} \in \operatorname{Spm}(A)$ *und* $\mathfrak{P} \in \operatorname{Spm}(B)$ *Primideale mit* $\mathfrak{p} = \mathfrak{P} \cap A$*. Dann gelten*

- *Die Körpererweiterung* $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ *ist normal und separabel (also galoisch)*
- $\operatorname{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \operatorname{Aut}_{\kappa(\mathfrak{p})}\big(\kappa(\mathfrak{P})\big)$
- $\operatorname{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$

Ist zusätzlich auch $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ *separabel, dann gelten weiter*

(i) $e(\mathfrak{P} \,/\, \mathfrak{P}_T) = e_{\mathfrak{p}}$ *und* $f(\mathfrak{P} \,/\, \mathfrak{P}_T) = 1$

(ii) $e(\mathfrak{P}_T \,/\, \mathfrak{P}) = 1$ *und* $f(\mathfrak{P}_T \,/\, \mathfrak{P}) = f_{\mathfrak{p}}$

mit $\mathfrak{P}_T := \mathfrak{P} \cap T_{\mathfrak{P}}$

Beweis. Die ersten drei Punkte sind offensichtliche Folgerungen aus dem Hauptsatz der Galois-Theorie. Setzen wir voraus, dass $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel ist, dann gilt

$$\sharp \operatorname{Aut}_{\kappa(\mathfrak{p})}\big(\kappa(\mathfrak{P})\big) \;=\; \big[\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})\big] \;=\; f_{\mathfrak{p}} \;=:\; f$$

Wie wir wissen gilt $\sharp G_{\mathfrak{P}} = f_{\mathfrak{p}} \cdot e_{\mathfrak{p}}$ dann muss $\sharp I_{\mathfrak{P}} = e_{\mathfrak{p}} =: e$ gelten. Betrachte die Diagramme

$$\begin{array}{ccccc} I_{\mathfrak{P}} & \longrightarrow & G_{\mathfrak{P}} & \longrightarrow & \operatorname{Gal}\big(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\big) \\ & \searrow^{1} & & \nearrow & \end{array}$$

$$\begin{array}{ccccc} I_{\mathfrak{P}} & = & \operatorname{Gal}(L/T_{\mathfrak{P}}) & \twoheadrightarrow & \operatorname{Gal}\big(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)\big) \\ & & & \searrow^{1} & \downarrow \\ & & & & \operatorname{Gal}\big(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\big) \end{array}$$

Also gilt $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$. Aus dieser Gleichung folgt sofort $f(\mathfrak{P}(\mathfrak{P}_T) = 1$ und damit

$$e(\mathfrak{P} \,/\, \mathfrak{P}_T) \;=\; e(\mathfrak{P} \,/\, \mathfrak{P}_T) f(\mathfrak{P} \,/\, \mathfrak{P}_T) \;=\; [L : T_{\mathfrak{P}}] \;=\; \sharp I_{\mathfrak{P}} \;=\; e_{\mathfrak{p}}$$

Mit Lemma 11.2 und Satz 12.5 gilt aber auch

$$e_{\mathfrak{p}} \;=\; e(\mathfrak{P} \,/\, \mathfrak{P}_z) \;=\; e(\mathfrak{P} \,/\, \mathfrak{P}_T) \cdot e(\mathfrak{P}_T \,/\, \mathfrak{P}_z)$$

Also muss $e(\mathfrak{P}_T \,/\, \mathfrak{P}_z) = 1$ sein. Damit erhalten wir aber auch sofort

$$f(\mathfrak{P}_T \,/\, \mathfrak{P}_z) \;=\; e(\mathfrak{P}_T \,/\, \mathfrak{P}_z) \cdot f(\mathfrak{P}_T \,/\, \mathfrak{P}_z) \;=\; [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] \;=\; [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] \;=\; f_{\mathfrak{p}}$$

□

Bemerkung 12.9 *Wir können die Situation von Satz 12.8 grafisch aufarbeiten, es gilt*

				Grad	Verzw. Ind.	Trägh. Grad
$\{1\}$	–	–	L			
	$\big\vert$	$\big\vert$		$\big\vert\ e_{\mathfrak{p}}$	$\big\vert\ e_{\mathfrak{p}}$	$\big\vert\ 1$
$I_{\mathfrak{P}}$	–	–	$T_{\mathfrak{P}}$			
	$\big\vert$	$\big\vert$		$\big\vert\ f_{\mathfrak{p}}$	$\big\vert\ 1$	$\big\vert\ f_{\mathfrak{P}}$
$G_{\mathfrak{P}}$	–	–	$Z_{\mathfrak{P}}$			
	$\big\vert$	$\big\vert$		$\big\vert\ r$	$\big\vert\ 1$	$\big\vert\ 1$
G	–	–	K			

13 Verzweigtheit von Primidealen

Sei wieder A ein Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(A)$. Sei weiter L/K eine endliche separable Körpererweiterung mit $[L : K] = n$, dann bezeichne B den ganzen Abschluss von A in L. Zur Erinnerung: Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein maximales Ideal, und sei

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

die Primfaktorzerlegung des von $\mathfrak{p}$ in B erzeugten Ideals in paarweise verschiedene Primfaktoren. Dann nennen wir $\mathfrak{P}$ in L (bzw. B) verzweigt, wenn ein $\mathfrak{P}_i \,/\, \mathfrak{p}$ verzweigt ist. Das heißt, wenn für ein $i \in \{1, \ldots, r\}$ gilt

$$e(\mathfrak{P}_i \,/\, \mathfrak{p}) \;>\; 1 \qquad \text{oder} \qquad {}^{B}\!/_{\mathfrak{P}_i}/{}^{A}\!/_{\mathfrak{p}} \text{ ist nicht separabel.}$$

In Folgerung 10.10 erarbeiteten wir ein Kriterium dafür, wann ein Ideal unverzweigt ist, allerdings mussten wir dafür ein Hilfsideal $\mathcal{F}$ konstruieren und wir konnten keine Aussage über Ideale treffen, die dieses $\mathcal{F}$ geteilt haben. In diesem Abschnitt wollen wir ein sehr präzises Kriterum dafür angeben, wann ein Ideal (un-)verzweigt ist.

Definition 13.1 *(Diskriminante des ganzen Abschlusses)*
Wir bezeichnen das Ideal von A, welches von den Diskriminanten aller K-Basen $\{\omega_1, \ldots, \omega_n\} \subset B$ von L erzeugt wird, als die Diskriminante von B über A. In Formeln

$$D_{B/A} \;:=\; \big(D(\omega_1, \ldots, \omega_n) \,\big|\, \{\omega_1, \ldots, \omega_n\} \subset B \text{ ist eine } K\text{-Basis von } L \big) \;\lhd\; A$$

Lemma 13.2 *Ist B ein freier A-Modul mit Basis $\{\omega_1, \ldots, \omega_n\}$, dann ist $D_{B/A} \lhd A$ ein Hauptideal mit*

$$D_{B/A} \;=\; \big(D(\omega_1, \ldots, \omega_n) \big)$$

Beweis. Nach Voraussetzung ist

$$B \;=\; A\omega_1 \oplus \ldots \oplus A\omega_n$$

Sei nun $\{u_1, \ldots, u_n\}$ eine beliebige K-Basis von L mit $u_i \in B$ für alle $i = 1 \ldots n$, dann gibt es Koeffizienten $M_{i,j} \in A$ mit

$$u_i \;=\; \sum_{j=1}^{n} M_{i,j} \cdots \omega_j$$

Bezeichne die von den $M_{i,j}$ gegebene Koeffizientenmatrix mit $M \in \mathrm{Mat}_{n\times n}(A)$, dann ist

$$D(u_1, \ldots, u_n) \;=\; \det\Big(\big(Tr_K^L(u_i, u_j)\big)_{i,j=1,\ldots,n} \Big) \;=\; \big(\det(M)\big)^2 \cdot D(\omega_1, \ldots, \omega_n)$$

□

Anmerkung Im Allgemeinen ist B kein freier Modul über A.

Wir sind nun soweit den Satz, den wir in diesem Abschnitt beweisen wollen, zu formulieren:

Satz 13.3 *Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein maximales Ideal. Dann ist $\mathfrak{p}$ genau dann verzweigt in L, wenn die Diskriminante von A über B von $\mathfrak{p}$ geteilt wird, das heißt, wenn $\mathfrak{p} \supseteq D_{A/B}$.*

Bevor wir diesen Satz jedoch beweisen können müssen wir noch etwas über die Diskriminante von A über B und noch allgemeiner etwas über Algebren über Körpern lernen.

Lemma 13.4 *Sei $S \subseteq A\backslash\{0\}$ ein multiplikatives System, dann gilt*

$$D_{S^{-1}B/S^{-1}A} \;=\; S^{-1}D_{B/A}$$

Beweis. Sei $\{\omega_1, \ldots, \omega_n\} \subset B$ eine K-Basis von L, dann ist auch $\{\frac{\omega_1}{1}, \ldots, \frac{\omega_n}{1}\} \subset S^{-1}B$ eine K-Basis von L. Dies gibt uns sofort die erste Inklusion

$$D_{S^{-1}B/S^{-1}A} \;\supseteq\; S^{-1}D_{B/A}$$

Sei nun $\{\omega'_1, \ldots, \omega'_n\} \subset S^{-1}B$ eine K-Basis von L, dann gibt es ein $s \in S$, sodass $s\omega_i \in B$ für alle $i = 1 \ldots n$ gilt. Per Definition ist $0 \notin S$, also ist insbesondere $s \neq 0$. Daher ist auch die Menge $\{s\omega'_1, \ldots, s\omega'_n\} \subset B$ eine K-Basis von L und es gilt

$$D(s\omega'_1, \ldots, s\omega'_n) \;=\; s^n \cdot D(\omega'_1, \ldots, \omega'_n) \;\in D_{B/A}$$

und damit folgt die andere Inklusion. □

Bemerkung 13.5 *Es gelten*

1. *Falls es ein primitives Element $\alpha \in B$ mit $B = A[\alpha]$ gibt, dann ist B frei über A mit Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Sei weiter $f \in A[X]$ das Minimalpolynom von α, dann gilt*

$$D_{B/A} \;=\; \big(D(1, \alpha, \ldots, \alpha^{n-1})\big) \;=\; \big(\, N_K^L\big((f'(\alpha)\big)\,\big)$$

2. *Ist $\mathfrak{p} \in \mathrm{Spm}(A)$ maximal, dann ist $A_\mathfrak{p}$ ein Hauptidealbereich. und $B_\mathfrak{p} := (A\backslash\mathfrak{p})^{-1}B$ ist ein freier Modul von endlichem Rang n. Es folgt*

$$D_{B_\mathfrak{p}/A_\mathfrak{p}} \;=\; \big(\, D(\omega_1, \ldots, \omega_n)\,\big) \quad \text{für eine } A_\mathfrak{p}\text{-Basis } \{\omega_1, \ldots, \omega_n\} \text{ von } B_\mathfrak{p}$$

   Wir erhalten

$$D_{B/A}A_\mathfrak{p} \;=\; D_{B_\mathfrak{p}/A_\mathfrak{p}} \qquad (*)$$

3. *Die Diskriminante $D_{B/A}$ lässt sich durch die Gleichung $(*)$ lokal ausrechnen. Betrachte die Primidealfaktorisierung*

$$D_{B/A} \;=\; \prod_{\mathfrak{p}\in\mathrm{Spm}(A)} \mathfrak{p}^{v_\mathfrak{p}(D_{B/A])}}$$

   von $D_{B/A}$ in A. Betrachten wir nun das von $D_{A/B}$ in $A_\mathfrak{p}$ erzeugte Ideal, dann vereinfacht sich die Primidealfaktorisierung zu

$$D_{B/A}A_\mathfrak{p} \;=\; (\mathfrak{p}\,A_\mathfrak{p})^{v_\mathfrak{p}(D_{B/A})}$$

   Mit Gleichung $(*)$ können wir diese Faktorisierung erweitern zu

$$\big(\, D(\omega_1, \ldots, \omega_n)\,\big) \;=\; D_{B_\mathfrak{p}/A_\mathfrak{p}} \;=\; D_{B/A}A_\mathfrak{p} \;=\; (\mathfrak{p}\,A_\mathfrak{p})^{v_\mathfrak{p}(D_{B/A})}$$

   für eine geeignete $A_\mathfrak{p}$-Basis $\{\omega_1, \ldots, \omega_n\}$ von $B_\mathfrak{p}$. Insbesondere erhalten wir auch

$$v_\mathfrak{p}(D_{B/A}) \;=\; v_{\mathfrak{p}\,A_\mathfrak{p}}(D_{B_\mathfrak{p}/A_\mathfrak{p}})$$

Mit dem nächsten Lemma wollen wir den folgenden Einschub über k-Algebren motivieren:

Lemma 13.6 *Sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein maximales Ideal, dann gilt: $\mathfrak{p}$ ist genau dann unverzweigt in L, wenn der Ring ${}^{B}\!/_{\mathfrak{p}\,B}$ ein endliches Produkt von endlichen und separablen Körpererweiterungen von ${}^{A}\!/_{\mathfrak{p}}$ ist.*

Beweis. Sei $\mathfrak{p}\,B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ die Primidealfaktorisierung von $\mathfrak{p}\,B$ in paarweise verschiedene Primideale $\mathfrak{P}_i \in \mathrm{Spm}(B)$, dann gilt mit dem chinesischen Restsatz

$$ {}^{B}\!/_{\mathfrak{p}\,B} \;=\; {}^{B}\!/_{\mathfrak{P}_1^{e_1}} \times \ldots \times {}^{B}\!/_{\mathfrak{P}_r^{e_r}} $$

Per Definition ist $\mathfrak{p}$ genau dann unverzweigt, wenn alle $e_i = 1$ und alle Erweiterungen ${}^{B}\!/_{\mathfrak{P}_i}/{}^{A}\!/_{\mathfrak{p}}$ separabel sind. □

Wir können den Ring ${}^{B}\!/_{\mathfrak{p}\,B}$ als eine Algebra über dem Körper ${}^{A}\!/_{\mathfrak{p}}$ auffassen. Diese Situation wollen wir nun noch allgemeiner untersuchen. Sei im Folgenden also stets k ein Körper und $\mathfrak{a}$ eine k-Algebra mit $\dim_k(\mathfrak{a}) = n < \infty$.

Lemma 13.7 *$\mathfrak{a}$ hat nur endlich viele maximale Ideale $\{\mathfrak{m}_1, \dots, \mathfrak{m}_s\} = \mathrm{Spm}(\mathfrak{a})$ und es gibt ein $N \in \mathbb{N}$ mit*

$$ \bigcap_{i=1}^{s} \mathfrak{m}_s \;=\; \left\{\, a \in \mathfrak{a} \;\middle|\; a^N = 0 \,\right\} $$

Beweis. Seien $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ die maximalen Ideale von $\mathfrak{a}$, dann gilt $\mathfrak{m}_i + \mathfrak{m}_j = \mathfrak{a}$ für $i \neq j$. Nach dem chinesischen Restsatz ist die Abbildung

$$ \mathfrak{a} \;\twoheadrightarrow\; {}^{\mathfrak{a}}\!/_{\mathfrak{m}_1} \times \ldots \times {}^{\mathfrak{a}}\!/_{\mathfrak{m}_r} $$

für alle $r \in \mathbb{N}$ surjektiv. Da die Dimension von $\mathfrak{a}$ über k aber endlich ist, kann es nicht unendlich viele maximalideale geben. Für die Aussage über den Schnitt der Ideale sei $a \in \mathfrak{a}$ ein nilpotentes Element mit $a^N = 0$ für ein $N \in \mathbb{N}$ Für jedes $\mathfrak{m} \in \mathrm{Spm}(\mathfrak{a})$ haben wir die Abbildung

$$ \begin{aligned} \pi_{\mathfrak{m}} : \mathfrak{a} &\;\to\; {}^{\mathfrak{a}}\!/_{\mathfrak{m}} \\ a &\;\mapsto\; \overline{a} \end{aligned} $$

Es gilt $\overline{a}^{\,N} = 0$ also ist a^N in allen maximalen idealen $\mathfrak{m}$ von $\mathfrak{a}$. Diese Ideale sind insbesondere prim, also gilt $a \in \mathfrak{m}$ für alle $\mathfrak{m} \in \mathrm{Spm}(\mathfrak{a})$ und damit liegt a im Schnitt.
Für die andere Inklusion sei nun $a \in \mathfrak{m}$ für alle $\mathfrak{m} \in \mathrm{Spm}(\mathfrak{a})$.

Behauptung *Für alle $b \in \mathfrak{a}$ gibt es ein $\lambda \in k\backslash\{0\}$ mit $ab + \lambda \in \mathfrak{a}^\times$.*

Beweis. Betrachte wieder die Abbildung $\pi_{\mathfrak{m}}$ dann gilt $\pi_{\mathfrak{m}}(ab + \lambda) = \lambda$, denn $ab \in \mathfrak{m}$ da a im Schnitt aller $\mathfrak{m}$ liegt. Da nach Voraussetzung $\lambda \neq 0$ ist, ist $ab + \lambda$ in keinem maximalen Ideal enthalten, also ist $ab + \lambda$ eine Einheit von $\mathfrak{a}$. ◇

Weil n die Dimension von $\mathfrak{a}$ über k ist, ist die Menge $\{a^n, \dots, a^0\}$ linear abhängig über k, das heißt es gibt $\lambda_{n-1}, \dots, \lambda_0 \in k$ mit

$$ a^n + \lambda_{n-1}a^{n-1} + \ldots + a\lambda_1 + \lambda_0 \;=\; 0 $$

Falls $\lambda_{n-1} = \ldots = \lambda_0 = 0$ gilt, so folgt $a^n = 0$ und a ist nilpotent. Gibt es hingegen ein $0 \leq l \leq n-1$ mit $\lambda_l \neq 0$ und $\lambda_0 = \ldots = \lambda_{l-1} = 0$ dann gilt

$$a^l \cdot (a^{n-l} + \lambda_{n-1}a^{n-l-1} + \ldots + \lambda_l) \;=\; 0$$

Aber der Klammerausdruch ist nach der Behauptung eine Einheit, also ist a auch in diesem Fall nilpotent. □

Definition und Folgerung 13.8 *(Reduziert)*
Sei $\mathfrak{a}$ eine endlich dimensionale k-Algebra. Es sind äquivalent:

1. *$\mathfrak{a}$ ist reduziert, das heißt für alle $a \in \mathfrak{a}$, für die es ein $n \in \mathbb{N}$ mit $a^n = 0$ gibt, gilt $a = 0$. In Worten: Wir sagen $\mathfrak{a}$ ist reduziert, wenn Null das einzige nilpotente Element von $\mathfrak{a}$ ist.*
2. *$\mathfrak{a}$ ist ein endliches Produkt von endlichen Erweiterungskörpern über k, das heißt*

$$\mathfrak{a} \;\cong\; k_1 \times \ldots \times k_r \qquad \text{mit } k_i/k \text{ ist endlich für alle } i = 1, \ldots, r$$

Beweis. Die erste Aussage ist nach dem vorangegangenen Lemma äquivalent dazu, dass der Durchschnitt über alle Maximalideale $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ von $\mathfrak{a}$ nur das Nullideal ist. Genau dann ist aber

$$\begin{array}{rcl} \mathfrak{a} & \to & \displaystyle\prod_{i=1}^{s} \mathfrak{a}/\mathfrak{m}_i \\ a & \mapsto & (a + \mathfrak{m}_i)_{i=1\ldots s} \end{array}$$

ein Isomorphismus. □

Definition 13.9 *(Spur und Spurform)*
Sei $a \in \mathfrak{a}$ ein Element, dann definieren wir die Spur von a in $\mathfrak{a}$ als die Spur der k-linearen Abbildung

$$\begin{array}{rcl} a\cdot : \mathfrak{a} & \to & \mathfrak{a} \\ x & \mapsto & ax \end{array}$$

Also $Tr_k^{\mathfrak{a}}(a) := Spur(a\cdot)$. Damit definieren wir die Spurform wie üblich als

$$\begin{array}{rcl} Tr^{\mathfrak{a}} : \mathfrak{a} \times \mathfrak{a} & \to & k \\ (a, b) & \mapsto & Tr_k^{\mathfrak{a}}(ab) \end{array}$$

Bemerkung 13.10 *Ist $\{a_1, \ldots, a_n\}$ eine k-Basis von $\mathfrak{a}$, dann ist*

$$D(a_1, \ldots, a_n) \;:=\; \det\left(Tr^{\mathfrak{a}}(a_i, a_j)_{i,j=1\ldots n}\right) \;\in k$$

Die in der vorangegangen Definition eingeführte Spurform ist eine nicht ausgeartete Bilinearform über k, das heißt die Abbildung

$$\begin{array}{rcl} \mathfrak{a} & \mapsto & \mathrm{Hom}_k(\mathfrak{a}, k) \\ a & \mapsto & \left[\, b \mapsto Tr_k^{\mathfrak{a}}(ab) \,\right] \end{array}$$

ist ein Isomorphismus. Genau dann gibt es aber eine k-Basis $\{a_1, \ldots, a_n\}$ von $\mathfrak{a}$ für deren Diskriminante $D(a_1, \ldots, a_n) \neq 0$ gilt. Da die Diskriminante die Determinante einer Matrix und damit unabhängig von der Basis ist, ist sie dann für alle k-Basen ungleich Null.

Lemma 13.11 *Sei $\mathfrak{a}$ das Produkt von zwei k-Algebren $\mathfrak{a}_1, \mathfrak{a}_2$, das heißt $\mathfrak{a} = \mathfrak{a}_1 \times \mathfrak{a}_2$. Es gelten*

1. $(\mathfrak{a}, Tr^{\mathfrak{a}}) \cong (\mathfrak{a}_1, Tr^{\mathfrak{a}_1}) \times (\mathfrak{a}_2, Tr^{\mathfrak{a}_2})$
   Das heißt die Spurform ist mit der Trennung verträglich.

2. *Die Spurform auf $\mathfrak{a}$ ist genau dann nicht ausgeartet, wenn sowohl die Spurform auf $\mathfrak{a}_1$ als auch die Spurform auf $\mathfrak{a}_2$ nicht ausgeartet ist.*

Beweis. Wähle k-Basen $\mathcal{B}_1 := \{a_1, \dots a_r\}$ von $\mathfrak{a}_1$ und $\mathcal{B}_2 := \{b_1, \dots, b_s\}$ von $\mathfrak{a}_2$, dann ist

$$\mathcal{B} := \big\{(a_1, 0), \dots, (a_r, 0), (0, b_1), \dots, (0, b_s)\big\}$$

eine k-Basis von $\mathfrak{a}_1 \times \mathfrak{a}_2$ 0 $\mathfrak{a}$. Seien nun $a \in \mathfrak{a}_1$ und $b \in \mathfrak{a}_2$. Seien weiter M_1 die Matrix zu

$$a\cdot : \mathfrak{a}_1 \ni x \mapsto ax \in \mathfrak{a}_1$$

bezüglich $\mathcal{B}_1$ und M_2 die Matrix zu

$$b\cdot : \mathfrak{a}_2 \ni x \mapsto bx \in \mathfrak{a}_2$$

bezüglich $\mathcal{B}_2$, dann ist

$$M := \begin{pmatrix} M_1 & \\ & M_2 \end{pmatrix}$$

die Matrix zu

$$ab\cdot : \mathfrak{a} \ni x \mapsto abx \in \mathfrak{a}$$

bezüglich $\mathcal{B}$. Damit gilt

$$Tr_k^{\mathfrak{a}}(ab) = Tr^{\mathfrak{a}}\big((a, b)\big) = Tr_k^{\mathfrak{a}_1}(a) + Tr_k^{\mathfrak{a}_2}(b)$$

Für den Nachweis des zweiten Teils seien die Elemente aus $\mathcal{B}$ mit v_i bezeichnet. In Produkträumen gilt $(a, 0) \cdot (0, b) = (0, 0) = 0$. Damit folgt also

$$\big(Tr^{\mathfrak{a}}(v_i, v_j)\big)_{i,j=1,\dots,r+s} = \begin{pmatrix} \big(Tr^{\mathfrak{a}_1}(a_i, a_j)\big)_{i,j=1,\dots,r} & \\ & \big(Tr^{\mathfrak{a}_2}(b_i, b_j)\big)_{i,j=1,\dots,s} \end{pmatrix}$$

Damit erhalten wir die Gleichung

$$D_{\mathfrak{a}}(v_1, \dots, v_{r+s}) = D_{\mathfrak{a}_1}(a_1, \dots, a_r) \cdot D_{\mathfrak{a}_2}(b_1, \dots, b_s)$$

und damit folgt die Behauptung aus der vorangegangen Bemerkung. □

Satz 13.12 *Sei $\mathfrak{a}$ eine k-Algebra endlicher Dimension, dann sind die folgenden Aussagen äquivalent:*

(1) *Die Spurform $Tr^{\mathfrak{a}}$ auf $\mathfrak{a}$ ist nicht ausgeartet.*

(2) *$\mathfrak{a}$ ist ein endliches Produkt von endlichen separablen Erweiterungskörpern über k, das heißt*

$$\mathfrak{a} \cong k_1 \times \ldots \times k_r \qquad \text{mit } k_i/k \text{ ist endlich und separabel für alle } i = 1, \dots, r$$

Beweis. Wir zeigen zunächst die leichtere Richtung „(1) $\Rightarrow$ (2)“. Nach Voraussetzung sind alle Körpererweiterungen k_i/k endlich und separabel. Nach Satz 4.9 ist dann die Spurform $Tr_k^{k_i}$ von k_i über k nicht ausgeartet. Mit dem Vorangegangenen Lemma folgt dann die behauptete Implikation.
Die andere Richtung „(2) $\Rightarrow$ (1)“ beweisen wir nur für den Fall, dass k ein vollkommener Körper ist, das heißt für den Fall, das jede Körpererweiterung über k separabel ist.

Behauptung *Wenn die Spurform auf $\mathfrak{a}$ nicht ausgeartet ist, dann ist $\mathfrak{a}$ reduziert.*

Beweis. Sei a ein nilpotentes Element von $\mathfrak{a}$, etwa mit $a^N = 0$ für ein $N \in \mathbb{N}$, dann gilt $(ab)^N = 0$ für alle $b \in \mathfrak{a}$, also ist auch ab für alle $b \in \mathfrak{a}$ nilpotent. Dann ist aber $f = X^n \in k[X]$ mit $n = \dim_k(\mathfrak{a})$ das charakteristische Polynom von ab für alle $b \in \mathfrak{a}$. Nach Bemerkung 4.2 Teil 4 ist die Spur eines Elements genau der zweithöchste Koeffizient des charakteristischen Polynoms. Also in unserem Fall $Tr^{\mathfrak{a}}(ab) = 0$ für alle $b \in \mathfrak{a}$. Wei die Spurform nach Voraussetzung nicht ausgeartet ist, muss dann $ab = 0$ sein und dies natürlich für alle $b \in \mathfrak{a}$. Also muss a bereits das Nullelement gewesen sein. $\diamond$

Nach Folgerung 13.8 ist $\mathfrak{a}$ genau dann reduziert, wenn $\mathfrak{a}$ ein endliches Produkt von endlichen Erweiterungskörpern über k ist. $\square$

Anmerkung Obwohl wir die zweite Implikation nur für vollkommene Körper gezeigt haben, gilt sie so wie wir sie behauptet haben. Zu zeigen bleibt dann noch, dass aus der Annahme, k_i/k sei nicht separabel, folgt, dass die zugehörige Spurform $Tr_k^{k_i}$ ausgeartet ist.

Wir sind nun endlich so weit unseren Ausflug zu endlich dimensionalen Algebren über Körpern zu beenden und den weiter oben postulierten Satz zu beweisen:

Satz 13.3 *Sei A ein Dedekindring mit Quotientenkörper $K := \mathrm{Quot}(A)$ und sei L/K eine endliche separable Körpererweiterung vom Grad n. Bezeichne B den ganzen Abschluss von A in L und sei $\mathfrak{p} \in \mathrm{Spm}(A)$ ein maximales Ideal. Dann ist $\mathfrak{p}$ genau dann verzweigt in L, wenn die Diskriminante von A über B von $\mathfrak{p}$ geteilt wird, das heißt, wenn $\mathfrak{p} \supseteq D_{A/B}$.*

Beweis. Setzen wir $\mathfrak{a} := {}^{B}\!/_{\mathfrak{p}\,B}$ und $k := \kappa(\mathfrak{p}) = {}^{A}\!/_{\mathfrak{p}}$, dann gilt nach Satz 13.12: $\mathfrak{p}$ ist genau dann unverzweigt in L, wenn die Spurform $Tr^{\mathfrak{a}}$ nicht ausgeartet ist. Weiter wissen wir, dass die Lokalisierung $A_{\mathfrak{p}}$ von A in $\mathfrak{p}$ ein Hauptidealbereich ist, also ist $B_{\mathfrak{p}}$ ein freier $A_{\mathfrak{p}}$ Modul, das heißt es gibt Elemente $\omega_1, \ldots, \omega_n \in B_{\mathfrak{p}}$ mit

$$B_{\mathfrak{p}} \;=\; A_{\mathfrak{p}}\omega_1 \oplus \ldots \oplus A_{\mathfrak{p}}\omega_n$$

Seien nun $\overline{\omega}_1, \ldots, \overline{\omega}_n$ die Bilder von $\omega_1, \ldots, \omega_n$ unter der natürlichen Projektion nach

$${}^{B_{\mathfrak{p}}}\!/_{\mathfrak{p}\,B_{\mathfrak{p}}} \;\cong\; {}^{B}\!/_{\mathfrak{p}\,B} \;=\; \mathfrak{a}$$

Weil $\{\omega_1, \ldots, \omega_n\}$ eine $A_{\mathfrak{p}}$-Basis von $B_{\mathfrak{p}}$ ist, ist $\{\overline{\omega}_1, \ldots, \overline{\omega}_n\}$ eine $\kappa(\mathfrak{p})$-Basis von $\mathfrak{a}$. Sei nun $b \in B_{\mathfrak{p}}$, dann gibt es Elemente $M_{i,j} \in A_{\mathfrak{p}}$ mit

$$b\omega_i \;=\; \sum_{j=1}^{n} M_{i,j}\omega_j \qquad \text{und} \qquad Tr_{A_{\mathfrak{p}}}^{B_{\mathfrak{p}}}(b) \;=\; \sum_{i=1}^{n} M_{i,i}$$

Betrachte nun $\overline{b} = b + \mathfrak{p}\,B$, dann gibt es Elemente $\overline{M}_{i,j} \in \kappa(\mathfrak{p})$ mit

$$\overline{b}\overline{\omega}_i \;=\; \sum_{j=1}^{n} \overline{M}_{i,j}\overline{\omega}_j \qquad \text{und} \qquad Tr^{\mathfrak{a}}(\overline{b}) \;=\; \sum_{i=1}^{n} \overline{M}_{i,i}$$

und die $\overline{M}_{i,j}$ sind die Bilder der $M_{i,j}$. Damit gilt aber für alle $b_1, b_2 \in B_\mathfrak{p}$

$$Tr^\mathfrak{a}(\overline{b}_1\overline{b}_2) \;\equiv\; Tr_{A_\mathfrak{p}}^{B_\mathfrak{p}}(b_1 b_2) \text{ modulo } \mathfrak{p}\, B_\mathfrak{p}$$

Dann folgt aber für die Diskriminante

$$D(\overline{\omega}_1, \ldots, \overline{\omega}_n) \;\equiv\; D(\omega_1, \ldots, \omega_n) \text{ modulo } \mathfrak{p}\, B_\mathfrak{p}$$

und weiter

$$D(\omega_1, \ldots, \omega_n) \;\equiv\; D_{B_\mathfrak{p}/A_\mathfrak{p}} \text{ modulo } \mathfrak{p}\, A_\mathfrak{p}$$

Damit erhalten wir die Äquivalenz, dass $Tr^\mathfrak{a}$ genau dann nicht ausgeartet ist, wenn $D(\overline{\omega}_1, \ldots, \overline{\omega}_n)$ nicht Null ist, das heißt genau dann wenn $D_{B_\mathfrak{p}/A_\mathfrak{p}}$ nicht von $\mathfrak{p}\, A_\mathfrak{p}$ geteilt wird. Also genau dann, wenn $D_{B/A}$ nicht von $\mathfrak{p}$ geteilt wird. □

Folgerung 13.13 *Sei $K/\mathbb{Q}$ ein endlicher Zahlkörper, dann gibt es eine Primzahl $p \in \mathbb{N}$, so dass (p) verzweigt ist in K.*

Beweis. Aus der Minkowski-Theorie folgt

$$D_{\mathcal{O}_K/\mathbb{Z}} \;>\; 1$$

also gibt es eine Primzahl, die die Diskriminante von $\mathcal{O}_K$ über $\mathbb{Z}$ teilt. □

Kapitel V

Analytische Methoden

14 Dedekindsche Zeta-Funktion

Im Abschnitt über die Gaußschen Zahlen haben wir einige komplexe Reihen in Definition 1.13 gesetzt. Wir erinnern uns insbesondere an die Riemannsche ζ-Funktion: Für $s \in \mathbb{C}$ mit $\Re(s) > 1$ setzten wir

$$\zeta(s) \quad := \quad \sum_{n=1}^{\infty} \frac{1}{n^s}$$

In diesem Abschnitt wollen wir eine dieser Reihe nicht unähnliche Funktion definieren und somit einen analytischen Zugang für die Untersuchung von Zahlkörpern über $\mathbb{Q}$ schaffen.

Definition 14.1 *(Verallgemeinerter Kegel)*
Sei $n \in \mathbb{N}$ und $X \subset \mathbb{R}^n$ eine Teilmenge, dann nennen wir X einen verallgemeinerten Kegel in $\mathbb{R}^n$, wenn gelten:

1. $0 \notin X$
2. *Für alle $x \in X$ und alle $\lambda \in \mathbb{R}_+$ ist auch $\lambda x \in X$*

Bemerkung 14.2 *Sei $n \in \mathbb{N}$ und $X \subset \mathbb{R}^n$ ein verallgemeinerter Kegel in $\mathbb{R}^n$, dann ist eine Funktion*

$$F : X \quad \to \quad \mathbb{R}_+$$

mit

1. *Für alle $x \in X$ und alle $\lambda \in \mathbb{R}_+$ gilt $f(\lambda x) \; = \; \lambda^n F(x)$*
2. *Die Menge*
$$T \quad := \quad \left\{ x \in X \,\middle|\, F(X) \leq 1 \right\}$$
ist beschränkt in $\mathbb{R}^n$ und $vol(T) =: v$ existiert und ist nicht Null.

Dann ist F auf ganz X eindeutig durch die Elemente der Menge $\{ x \in X \mid F(x) = 1 \}$ bestimmt.

Satz 14.3 *Seien $n \in \mathbb{N}$ und $\Lambda \in \mathbb{R}^n$ ein Gitter. Setze*

$$\Delta \;:=\; vol\left(\mathbb{R}^n/\Lambda\right)$$

für das Maß der Grundmasche. Sei weiter $X \subset \mathbb{R}^n$ ein verallgemeinerte Kegel und F eine Funktion wie in Bemerkung 14.2. Dann konvergiert die Reihe

$$\overline{\zeta}(s) \;:=\; \sum_{x \in X \cap \Lambda} \frac{1}{F(x)^s}$$

für alle $s \in \mathbb{R}_{>1}$ und es gilt

$$\lim_{s \searrow 1} (s-1) \cdot \overline{\zeta}(s) \;=\; \frac{v}{\Delta}$$

mit $v = vol(T)$. Hierbei sei „$s \searrow 1$“ die Kurzschreibweise für $s \to 1$ und $s > 1$.

Bevor wir diesen Satz zeigen ziehen wir den Spezialfall für $n = 1$ in einem Lemma heraus.

Lemma 14.4 *Betrachte den Spezialfall $n = 1$, $X = (0, \infty)$, $F(1) := 1$ und $\Lambda = \mathbb{Z} \subset \mathbb{R}$ in Satz 14.3, dann sind*

$$\overline{\zeta}(s) \;=\; \sum_{m \in \mathbb{N}} \frac{1}{m^s} \qquad \text{und} \qquad \lim_{s \searrow 1} (s-1) \cdot \overline{\zeta}(s) \;=\; 1 \;=\; \frac{v}{\Delta}$$

Beweis. Jedes Intervall der Form $[a, \infty) \subset \mathbb{R}$ mit $a > 0$ ist ein verallgemeinerter Kegel in $\mathbb{R}$ und $F(a+1) := 1$ ist eine sinnvolle Setzung der Funktion nach Bemerkung 14.2. $\mathbb{Z}$ ist ein Gitter in $\mathbb{R}$. In diesem Spezialfall ist die Konvergenz ein aus der Funktionentheorie bekanntes Ergebniss über die Riemannsche ζ-Funktion. □

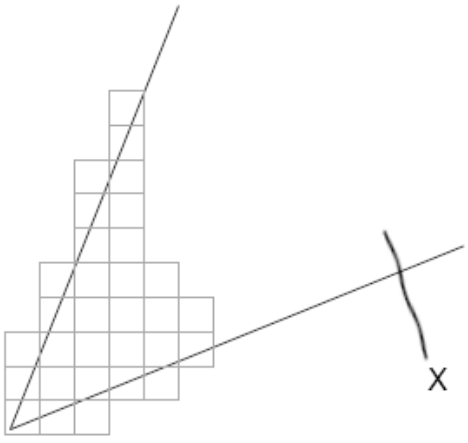
Beweis des Satzes. Wir wollen den verallgemeinerten Kegel mit immer kleineren Gittern überdecken (Betrachte die vereinfachte zwei-dimensionale Darstellung rechts). Für $r \in \mathbb{R}_+$ setze

$$\Lambda_r \;:=\; \left\{ \frac{1}{r} \cdot x \,\middle|\, x \in \Lambda \right\}$$

dann ist das Volumen der Grundmasche entsprechend kleiner. Es gilt

$$vol\left(\mathbb{R}^n/\Lambda_r\right) \;=\; \frac{\Delta}{r^n}$$

Setze weiter $N(r) \;:=\; \sharp\big(T \cap \Lambda_r\big)$ dann erhalten wir



$$v \;=\; vol(T) \;=\; \lim_{r \to \infty} N(r) \frac{\Delta}{r^n} \;=\; \Delta \cdot \lim_{r \to \infty} \frac{N(r)}{r^n}$$

Setze nun $rT := \{\, rt \,|\, t \in T \,\} = \{\, x \in X \,|\, F(x) \le r^n \,\}$. Dann gilt

$$N(r) \;=\; \sharp(rT \cap \Lambda) \;=\; \sharp\big\{\, x \in X \cap \Lambda \,\big|\, F(x) \le r^n \,\big\}$$

Insbesondere ist $\Lambda \cap X$ also abzählbar. Numeriere die nun Elemente so, dass gilt

$$0 \;<\; F(x_1) \;\le\; F(x_2) \;\le\; F(x_3) \;\le\; \ldots \qquad \text{für alle } x_i \in X \cap \Lambda$$

Setze $r_k := \sqrt[n]{F(x_k)}$, dann gelten

$$\{x_1, \ldots, x_k\} \subseteq r_k T \quad \text{und} \quad x_k \notin (r_k - \varepsilon)T \text{ für alle } \varepsilon > 0$$

Wir erhalten also für alle $\varepsilon > 0$ die Abschätzung $N(r_k - \varepsilon) < k \leq N(r_k)$, Multipliziere diese Abschätzung mit $\frac{1}{r_k^n}$ durch und erhalte weiter

$$\frac{v}{\Delta} \overset{k\to\infty}{\longleftarrow} \frac{N(r_k-\varepsilon)}{(r_k-\varepsilon)^n} \cdot \frac{(r_k-\varepsilon)^n}{r_k^n} \leq \tfrac{k}{r_k^n} < \frac{N(r_k)}{r_k^n} \overset{k\to\infty}{\longrightarrow} \frac{v}{\Delta}$$

Mit dem Quetschlemma folgt dann auch

$$\lim_{k\to\infty} \frac{k}{r_k^n} = \lim_{k\to\infty} \frac{k}{F(x_k)} = \frac{v}{\Delta}$$

Damit wissen wir: Für alle $\varepsilon > 0$ gibt es ein $k_0 \in \mathbb{N}$ so dass für alle $k > 0$ und alle $s > 1$ gilt

$$\frac{\left(\frac{v}{\Delta} - \varepsilon\right)^s}{k^s} < \frac{1}{F(x_k)} < \frac{\left(\frac{v}{\Delta} + \varepsilon\right)^s}{k^s}$$

Für $a_k \geq 0$ ist die Folge der Partialsummen der Reihe $\sum \frac{1}{a_k}$ monoton wachsend. Für alle $k > 0$ und alle $s > 1$ ist $\frac{1}{F(x_k)^s} > 0$. Damit ist die Folge der Partialsummen von

$$\sum_{k=1}^{\infty} \frac{1}{F(x_k)^s}$$

monoton wachsend. Nach der vorangegangenen Überlegung ist diese Folge aber nach oben durch

$$\left(\frac{v}{\Delta} + \varepsilon\right)^s \cdot \left(\sum_{k=k_0}^{\infty} \frac{1}{k^s} + \sum_{k=1}^{k_0} \frac{1}{F(x_k)^s}\right) < \infty$$

beschränkt. Also ist die Reihe konvergent. Betrachte nun die Abschätzung

$$\lim_{s\searrow 1} \left(\frac{v}{\Delta} - \varepsilon\right)^s \cdot (s-1) \cdot \zeta(s) \leq \lim_{s\searrow 1} (s-1) \cdot \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} \leq \lim_{s\searrow 1} \left(\frac{v}{\Delta} + \varepsilon\right)^s \cdot (s-1) \cdot \zeta(s)$$

Wobei ζ hier die Riemannsche ζ-Funktion bezeichne. Nach dem Lemma 14.4 gilt dann aber

$$\left(\frac{v}{\Delta} - \varepsilon\right) \leq \lim_{s\searrow 1} (s-1) \cdot \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} \leq \left(\frac{v}{\Delta} + \varepsilon\right)$$

Also sind $\limsup$ und $\liminf$ durch die Ausdrücke $\frac{v}{\Delta} \pm \varepsilon$ beschränkt. Da diese Ungleichungen aber für alle $\varepsilon > 0$ gelten, stimmen $\limsup$ und $\liminf$ überein, daher existiert der Grenzwert und nimmt den den behaupteten Wert an. □

Anmerkung Anstelle von $s \in \mathbb{R}$ mit $s > 1$ können wir auch $s \in \mathbb{C}$ betrachten. Dann folgt aus unserem Beweis mit leichten abwandlungen auch die gleichmäßg absolute Konvergenz von $\overline{\zeta}(s)$ auf der Menge $\{ s \in \mathbb{C} \mid \Re(s) > 1 \}$. Der Weierstraßsche M-Test liefert dann auch die Holomorphie von $\overline{\zeta}$ auf eben jener Menge.

Wir betrachten im Folgenden wieder einen endlichen Zahlkörper $K/\mathbb{Q}$ vom Grad $[K : \mathbb{Q}] = n$. Ausserdem verwenden wir wieder

$$\begin{aligned} r &:= \sharp\{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) \,|\, \sigma \text{ ist reell }\} \\ 2s &:= \sharp\{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) \,|\, \tau \neq \overline{\tau}\} \end{aligned}$$

Das heißt r ist die Anzahl der reellen Einbettungen von K in $\mathbb{C}$ und s die Anzahl der Paare von komplexen Einbettungen von K nach $\mathbb{C}$.

Definition und Satz 14.5 *(Dedekindsche ζ-Funktion)*
Die durch die Reihe

$$\zeta_K(t) := \sum_{\substack{\mathfrak{a} \lhd \mathcal{O}_K \\ \mathfrak{a} \neq (0)}} \frac{1}{\big(\mathbb{N}(\mathfrak{a})\big)^t}$$

definierte Dedekindsche ζ-Funktion konvergiert für alle $s > 1$ und es gilt

$$\lim_{t \searrow 1} (t-1) \cdot \zeta_K(t) = h_K \cdot \frac{2^{r+s} \cdot \pi^s \cdot R_K}{\omega \cdot \sqrt{|D_K|}}$$

wobei h_K die Klassenzahl nach Definition 6.2, R_K den Regulator nach Definition 8.14 und D_K die Diskriminante nach Definition 4.10 bezeichne. Weiter sei $\omega := \sharp\mu(K)$ die Anzahl der in K liegenden Einheitswurzeln und r, s wie oben angegeben.

Beweis. Für alle $c \in \mathcal{C}\ell(K)$ setzen wir

$$\zeta_K(t,c) := \sum_{\substack{\mathfrak{a} \lhd \mathcal{O}_K \\ \mathfrak{a} \in c}} \frac{1}{\mathbb{N}(\mathfrak{a})^t}$$

Dann erhalten wir die Dedekindsche ζ-Funktion als

$$\zeta_K(t) = \sum_{c \in \mathcal{C}\ell(K)} \zeta_K(t,c)$$

Der Satz folgt mit dieser Eigenschaft dann sofort aus der folgenden

Behauptung 1 *Die Reihe $\zeta_K(t,c)$ konvergiert für $t > 1$ mit*

$$\lim_{t \searrow 1} (t-1) \cdot \zeta_k(t,c) = \frac{2^{r+s} \cdot \pi^s \cdot R_K}{\omega \cdot \sqrt{|D_K|}}$$

Beweis. Fixiere ein $\mathfrak{a}' \in \mathcal{O}_K$ mit $\mathfrak{a}' \in c^{-1}$ dem zu c inversen Gruppenelement aus $\mathcal{C}\ell(K)$, also mit $c \cdot c^{-1} = 1_{\mathcal{C}\ell(K)}$. Dann gibt es eine Bijektion

$$\begin{array}{ccc} \{\, \mathfrak{a} \lhd \mathcal{O}_K \mid \mathfrak{a} \in c \,\} & \overset{1:1}{\longleftrightarrow} & \{\, (\alpha) \,|\, \alpha \in \mathfrak{a}' \,\} \\ \mathfrak{a} & \mapsto & \mathfrak{a} \cdot \mathfrak{a}' = (\alpha) \\ (\alpha)(\mathfrak{a}')^{-1} & \leftarrow\!\shortmid & (\alpha) \end{array}$$

Und wir erhalten für alle $\alpha \in \mathfrak{a}'$ die Gleichung

$$\big|N_{\mathbb{Q}}^K(\alpha)\big| = \mathbb{N}\big((\alpha)\big) = \mathbb{N}(\mathfrak{a}) \cdot \mathbb{N}(\mathfrak{a}') \qquad \Leftrightarrow \qquad \mathbb{N}(\mathfrak{a}) = \frac{\big|N_{\mathbb{Q}}^K(\alpha)\big|}{\mathbb{N}(\mathfrak{a}')}$$

Damit können wir die Reihe schreiben als

$$\zeta_K(t,c) \;=\; \big(\mathbb{N}(\mathfrak{a}')\big)^t \cdot \sum_{(\mathfrak{a}) \subseteq \mathfrak{a}'} \frac{1}{\big|\, N_{\mathbb{Q}}^K(\alpha)\big|^t}$$

Wir betrachten nun wieder die Einbettungen von K nach $\mathbb{C}$ und numerieren

$$\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) \;=\; \big\{\sigma_1,\ldots,\sigma_r,\tau_1,\overline{\tau}_1,\ldots,\tau_s,\overline{\tau}_s\big\}$$

Dann erhalten wir insgesamt ein kommutatives Diagramm

$$\begin{array}{ccc} K & \xhookrightarrow{\;\iota\;} & K \otimes_{\mathbb{Q}} \mathbb{R} \;\cong\; \mathbb{R}^r \times \mathbb{C}^s \\ {\scriptstyle N_{\mathbb{Q}}^K}\big\downarrow & & \big\downarrow{\scriptstyle N} \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} \end{array}$$

Mit den Abbildungen

$$\iota(\alpha) \;:=\; \big(\sigma_1(\alpha),\ldots,\sigma_r(\alpha),\tau_1(\alpha),\ldots,\tau_s(\alpha)\big)$$

und

$$\begin{array}{rccl} N: & \mathbb{R}^r \times \mathbb{C}^s & \to & \mathbb{R} \\ & (x_1,\ldots,x_r,z_1,\ldots,z_s) & \mapsto & |x_1|\cdots|x_r|\cdot|z_1|^2\cdots|z_s|^2 \end{array}$$

Aus der kommutativität folgt also $N_{\mathbb{Q}}^K(\alpha) \;=\; N\big(\iota(\alpha)\big)$. Weiter ist

$$\mathbb{R}^r \times \mathbb{C}^s \;\cong\; \mathbb{R}^r \times \mathbb{R}^{2s} \;\cong\; \mathbb{R}^n \qquad \text{mit } n = [K:\mathbb{Q}]$$

In Satz 7.18 haben wir gezeigt, dass $\iota(\mathfrak{a}')$ ein Gitter in $\mathbb{R}^n$ ist mit

$$vol\left(\mathbb{R}^n\big/_{\iota(\mathfrak{a}')}\right) \;=\; \mathbb{N}(\mathfrak{a}') \cdot \sqrt{|D_K|}$$

Wir wollen nun den vorangegangenen Satz 14.3 anwenden. Dazu benötigen wir einen verallgemeinerten Kegel $X \subseteq \mathbb{R}^n \cong K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ der die Eigenschaft: Für alle $\alpha \in \mathcal{O}_K$ gibt es genau ein $\beta \in \iota(\mathcal{O}_K) \cap X$ mit $\alpha = \beta \cdot u$ für ein $u \in \mathcal{O}_K^\times$, erfüllt. Denn dann gilt

$$\zeta_K(t,c) \;=\; \mathbb{N}(\mathfrak{a}')^t \cdot \left(\sum_{\alpha \,\in\, \iota(\mathfrak{a}') \cap X} \frac{1}{N\big(\iota(\mathfrak{a})\big)^t} \right)$$

Wenden wir dann Satz 14.3 mit $F := N$ an, dann konvergiert $\zeta_K(t,c)$ für alle $t > 1$ mit

$$\lim_{t \searrow 1} (t-1) \cdot \zeta_K(t,c) \;=\; \mathbb{N}(\mathfrak{a}') \cdot \frac{vol\big(\big\{\, x \in X \,\big|\, N(x) \le 1 \,\big\}\big)}{\mathbb{N}(\mathfrak{a}') \cdot \sqrt{|D_K|}}$$

Es gilt

$$\big\{\, y \in K_{\mathbb{R}} \,\big|\, N(y) \neq 0 \,\big\} \;\cong\; (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \;\cong\; K_{\mathbb{R}}^\times$$

Zu Beginn von Abschnitt 8 haben wir die Abbildung

$$\begin{array}{rccl} l: (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \cong K_{\mathbb{R}}^\times & \to & \mathbb{R}^{r+s} \\ (x_1,\ldots,x_r,z_1,\ldots,z_s) & \mapsto & \big(\log|x_1|,\ldots,\log|x_r|,\log|z_1|^2,\ldots,\log|z_s|^2\big) \end{array}$$

definiert. Damit können wir das kommutative Diagramm von zuvor erweitern zu

$$\begin{array}{ccccc} K^\times & \overset{\iota}{\hookrightarrow} & (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s & \overset{l}{\longrightarrow} & \mathbb{R}^{r+s} \\ \downarrow{\scriptstyle N_{\mathbb{Q}}^K} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow[\log|\cdot|]{} & \mathbb{R} \end{array}$$

mit

$$Tr : \mathbb{R}^{r+s} \ni (x_i)_{i=1,\dots,r+s} \mapsto \sum_{i=1}^{r+s} x_i \in \mathbb{R}$$

Wir haben ebenfalls in Abschnitt 8 gezeigt, dass $l \circ \iota(\mathcal{O}_K^\times)$ ein Gitter in der Menge

$$\{ y \in \mathbb{R}^{r+s} \mid Tr(y) = \}$$

ist. Mit dem Dirichletschen Einheitssatz 8.5 gibt es dann $\varepsilon_1, \dots, \varepsilon_m \in \mathcal{O}_K^\times$ mit $m = r + s - 1$ Fundamentaleinheiten von $\mathcal{O}_K^\times$ mit

$$l\big(\iota(\mathcal{O}_K^\times)\big) = \mathbb{Z}\, l(\varepsilon_1) \otimes \dots \otimes \mathbb{Z}\, l(\varepsilon_m)$$

Wir definieren nun die Schreibweisen

$$l^* := \big(\underbrace{1, \dots, 1}_{r \text{ - mal}}, \underbrace{2, \dots, 2}_{s \text{ - mal}}\big) \in \mathbb{R}^{r+s}$$

$$l(\underline{x}) := l(x_1, \dots, x_r, z_1, \dots, z_s) =: \big(l_1(\underline{x}), \dots, l_{r+s}(\underline{x})\big)$$

dann ist $Tr(l^*) = r + 2s = n$ und die Menge $\{l^*, l(\varepsilon_1), \dots, l(\varepsilon_m)\}$ ist eine Basis von $\mathbb{R}^{r+s}$. Es gilt

$$Tr\big(l(\underline{x})\big) = \xi Tr(l^*) + \xi_1 Tr\big(l(\varepsilon_1)\big) + \dots + \xi_m Tr\big(l(\varepsilon_m)\big) = \xi n$$

Wei das obenstehende Diagramm Kommutiert gilt aber auch

$$Tr\big(l(\underline{x})\big) = \log\big(N(\underline{x})\big)$$

Damit erhalten wir $\xi = \frac{\log\left(N(\underline{x})\right)}{n}$. Betrachte nun die Einschränkung von l auf $(\mathbb{R}^\times)^r$, dann gilt

$$l\big((x_1, \dots, x_r)\big) = \frac{l^*}{n} \cdot \log\big(N(x_1, \dots, x_r)\big) + \sum_{i=1}^{m} \xi_i \cdot l(\varepsilon_i)$$

mit $\xi_i \in \mathbb{R}$. Dies bringt uns auf die Idee die folgende Menge zu definieren:
Für $x \in K_{\mathbb{R}}$ gilt genau dann $x \in X$, wenn gelten

1. $N(x) \neq 0$ und $l(x) = \xi l^* + \xi_1 \cdot l(\varepsilon_1) + \dots + \xi_m \cdot l(\varepsilon_m)$
2. Für alle $i = 1, \dots, m$ gilt $0 \leq \xi_i < 1$ und
3. $0 \leq \arg(x_1) < \frac{2\pi}{\omega}$

Zur Bedingung 1. ist fest zu halten, dass wegen $N(x) \neq 0$ der Ausdruck $l(x)$ wohldefiniert ist. Zur 3. Bedingung beachte: Das Argument einer reellen Zahl ist entweder 0, wenn die reelle Zahl positiv ist, oder π, wenn die reelle Zahl negativ ist. Da ω die Anzahl der Einheitswurzeln in K bezeichnet, und $\pm 1 \in \mathbb{Q}$ sind, gilt $\omega \geq 2$ für alle K, damit schließt die 3. Bedingung also negative Werte für x_1 aus, wenn $r \geq 1$. (Bei $r = 0$ ist $x_1 \in \mathbb{C}$)
Wir zeigen zunächst eine wichtige Eigenschaft der so definierten Menge X:

Lemma 14.6 *Für alle $\underline{y} \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ gibt es genau ein $\underline{x} \in X$ mit $y = x \cdot \iota(u)$ für ein $u \in \mathcal{O}_K^\times$*

Beweis des Lemmas. Wir zeigen zunächst die Eindeutigkeit. Dazu sei $\underline{y} \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$, dann nehmen wir an es gäbe $\underline{x}, \underline{x}' \in X$ mit $\underline{x} \cdot \iota(v) = \underline{y} = \underline{x}' \cdot \iota(v')$ mit $v, v' \in \mathcal{O}_K^\times$ Dies können wir umformen zu

$$\underline{x}' \;=\; \underline{x} \cdot \iota(u) \quad \text{ für ein } u \in \mathcal{O}_K^\times$$

Wir müssen für den Nachweis der Eindeutigkeit $u = 1$ zeigen. Nach dem Dirichletschen Einheitssatz 8.5 gilt

$$u \;=\; \zeta \cdot \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} \quad \text{ mit } n_i \in \mathbb{Z} \text{ und } \zeta \in \mu(K)$$

Nach der Vorüberlegung, die wir im Beweis des Satzes bereits angestellt haben, gibt es reelle Zahlen $\xi, \xi', \xi_1, \xi_1', \ldots, \xi_m, \xi_m' \in [0,1)$ so dass

$$\begin{aligned} l(\underline{x}') &= \xi' \, l^* + \xi_1' \, l(\varepsilon_1) + \ldots + \xi_m' \, l(\varepsilon_m) \\ l(\underline{x}) + l(u) &= \xi \, l^* + \xi_1 \, l(\varepsilon_1) + \ldots + \xi_m \, l(\varepsilon_m) + n_1 \, l(\varepsilon_1) + \ldots + n_m \, l(\varepsilon_m) \end{aligned}$$

Nach unserer Annahme gilt aber $l(\underline{x}') = l(\underline{x}) + l(u)$, also muss $n_i = 0$ für alle $i = 1, \ldots, m$ sein. Es gilt

$$\underline{x}' \;=:\; (x_1', \ldots, x_r', z_1', \ldots, z_s') \;=\; \big(\sigma_1(\zeta)\, x_1, \ldots, \sigma_r(\zeta)\, x_r, \tau_1(\zeta)\, z_1, \ldots, \tau_s(\zeta)\, z_s\big)$$

Nach der dritten Bedingung gelten

$$0 \;\leq\; arg(x_1'), arg(x_1) \;<\; \frac{2\pi}{\omega}$$

Da $\zeta \in \mu(K)$ eine Einheitswurzel ist, gilt weiter

$$\sigma_i(\zeta), \tau_j(\zeta) \;\in\; \left\{ \exp\left(\frac{2\pi k}{\omega}\right) \,\middle|\, 0 \leq\; k \;< \omega \right\} \qquad \text{für alle } i = 1, \ldots, r \text{ und } j = 1, \ldots, s$$

Also muss $\zeta = 1$ gelten und insgesamt folgt

$$u \;=\; 1 \cdot \varepsilon_1^0 \cdots \varepsilon_m^0 \;=\; 1$$

Für die Existenz sei $\underline{y} \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ mit

$$l(\underline{y}) \;=\; \xi \, l^* + \xi_1 \, l(\varepsilon_1) + \ldots + \xi_m \, l(\varepsilon_m)$$

Finde nun $n_i \in \mathbb{Z}$ so dass $0 \leq \xi_i - n_i < 1$ für alle $1 = 1, \ldots, m$ gilt, dann ist

$$l\big(\underline{y} \cdot \iota(\varepsilon_1^{-n_1} \cdots \varepsilon_m^{-n_m})\big) \;=\; \xi \, l^* + (\xi_1 - n_1) \cdot l(\varepsilon_1) + \ldots + (\xi_m - n_m) \cdot l(\varepsilon_m)$$

Damit haben wir eine Einheit $v^{-1} := \varepsilon_1^{-n_1} \cdots \varepsilon_m^{-n_m} \in \mathcal{O}_K^\times$ gefunden, so dass die zweite Bedingung für $\underline{y} \cdot \iota(v^{-1})$ erfüllt ist. Wähle nun ein $\zeta \in \mu(K)$ so dass $\sigma_1(\zeta) = \exp\left(\frac{2\pi i}{\omega}\right)$ gilt. Dann gibt es ein $k \in \{0, 1, \ldots, \omega\}$ mit

$$\frac{2\pi k}{\omega} \;\leq\; arg\big(y_1 \cdot [\iota(v^{-1})]_1\big) \;<\; \frac{2\pi(k+1)}{\omega}$$

Setze dann $u := \zeta^k \cdot \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m}$ dann ist $\underline{y} \cdot \iota(u)^{-1} \in X$ das gesuchte Element. □

Damit haben wir für ein fixiertes $c \in \mathcal{C}\ell(K)$ und ein hierzu gewähltes $\mathfrak{a}' \in c^{-1}$ gezeigt, dass

$$\begin{aligned}\zeta(t,c) &= \sum_{\substack{\mathfrak{a} \lhd \mathcal{O}_K \\ \mathfrak{a} \in c}} \frac{1}{\big(\mathbb{N}(\mathfrak{a})\big)^t} = \big(\mathbb{N}(\mathfrak{a}')\big)^t \cdot \sum_{(\alpha) \subseteq \mathfrak{a}'} \frac{1}{\big(N_{\mathbb{Q}}^K(\alpha)\big)^t} \\ &= \big(\mathbb{N}(\mathfrak{a})\big)^t \cdot \sum_{\alpha \in \iota(\mathfrak{a}') \cap X} \frac{1}{\big(\mathbb{N}(\alpha)\big)^t}\end{aligned}$$

Damit wir aber wie gewünscht den Satz 14.3 anwenden dürfen müssen wir noch zeigen, dass X ein verallgemeinerter Kegel ist. Dies ist die Aussage des folgenden Lemmas.

Lemma 14.7 *X ist ein verallgemeinerter Kegel, das heißt:*
Für alle $\lambda \in \mathbb{R}_+$ und alle $\underline{x} \in X$ gilt $\lambda \cdot \underline{x} \in X$

Beweis des Lemmas. Sei $\lambda \in \mathbb{R}_+$ und $\underline{x} =: (x_1, \ldots, x_r, z_1, \ldots, z_s) \in X$ Dann erfüllt $\underline{x}$ die Bedingungen

1. $N(\underline{x}) \neq 0$ und $l(\underline{x}) = \xi l^* + \xi_1 \cdot l(\varepsilon_1) + \ldots + \xi_m \cdot l(\varepsilon_m)$
2. Für alle $i = 1, \ldots, m$ gilt $0 \leq \xi_i < 1$ und
3. $0 \leq \arg(x_1) < \frac{2\pi}{\omega}$

Betrachte nun

$$N(\lambda\underline{x}) = |\lambda x_1| \cdot |\lambda x_r| \cdot |\lambda z_1|^2 \cdots |\lambda z_s|^2 = \lambda^n N(\underline{x})$$

also ist, wegen $\lambda > 0$ und $N(\underline{x}) \neq 0$, die Bedingung $N(\lambda\underline{x}) \neq 0$ erfüllt. Ebenso gilt

$$\begin{aligned}l(\lambda\underline{x}) &= \big(\log|\lambda x_1|, \ldots, \log|\lambda x_r|, \log|\lambda z_1|^2, \ldots, \log|\lambda z_s|^2\big) \\ &= \big(\underbrace{\log|\lambda|, \ldots, \log|\lambda|}_{r \text{ - mal}}, \underbrace{2\log|\lambda|, \ldots, 2\log|\lambda|}_{s \text{ - mal}}\big) + l(\underline{x}) = \log(\lambda) \cdot l^* + l(\underline{x})\end{aligned}$$

Da die Bedingung zwei für $\underline{x}$ erfült ist, ist sie also auch für $\lambda\underline{x}$ erfüllt. Zum Schluss gilt $arg(\lambda) = 0$ wegen $\lambda > 0$, also ist $arg(x_1) = arg(\lambda x_1)$ und damit ist auch die dritte Bedingung für $\lambda\underline{x}$ erfüllt. □

Setze nun

$$T := \big\{\, x \in X \,\big|\, 0 < N(x) \leq 1 \,\big\}$$

Falls $vol(T)$ existiert und größer Null ist, liefert Satz 14.3 die Aussage von **Behauptung 1**. Es gilt der folgende

Satz 14.8 *Sei vol ein Maß auf $K_{\mathbb{R}}$, dass so normiert ist, dass $vol(\mathcal{O}_K) = \sqrt{|D_K|}$ gilt. Dann ist*

$$vol(T) = \frac{2^{r+s} \cdot \pi^s \cdot R_K}{\omega}$$

Wir wollen dieses Satz beweisen, indem wir das Lebesgue-Integral der konstanten Funktion 1 über T ausrechnen. Dass wir das Lebesque-Maß dazu verwenden dürfen zeigt die nächste Bemerkung.

Bemerkung 14.9 *Es gilt*

$$K_{\mathbb{R}} \;:=\; K \otimes_{\mathbb{Q}} \mathbb{R} \;\cong\; \mathbb{R}^r \times \mathbb{C}^s \;\cong\; \mathbb{R}^{r+2s} \;=\; \mathbb{R}^n$$

Die Positiv definite Bilinearform auf $K_{\mathbb{R}}$, auf der das Maß, das die Bedingung $vol(\mathcal{O}_K) = \sqrt{|D_K|}$ erfüllt, basiert, haben wir gesetzt als

$$\begin{aligned}\big\langle (\underline{x},\underline{z}), (\underline{x}*,\underline{z}') \big\rangle \;&:=\; (x_1,\ldots,x_r,z_1,\ldots,z_s)\cdot(x_1',\ldots,x_r',z_1',\ldots,z_s') \\ &=\; x_1x_1' + \ldots + x_rx_r' + 2z_1\overline{z'}_1 + \ldots + 2z_s\overline{z'}_s\end{aligned}$$

Das Lebesgue-Maß λ auf $\mathbb{R}^n$ basiert auf dem Standart-Skalarprodukt des $\mathbb{R}^n$. Für alle messbaren Mengen $\Omega \subset K_{\mathbb{R}} \cong \mathbb{R}^n$ gilt

$$vol(\Omega) \;=\; 2^s \cdot \lambda(\Omega)$$

Für den Nacheis von Satz 14.8 genügt es nun also zu zeigen, dass gilt

$$\lambda(T) \;=\; \frac{2^r \cdot \pi^s \cdot R_K}{\omega}$$

Wie schon erwähnt wollen wir dafür das Lebesgue-Integral

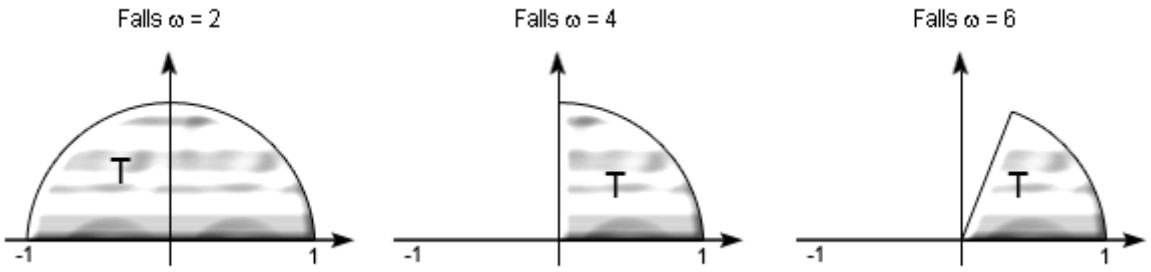
$$\lambda(T) \;=\; \int_T 1\, d\lambda$$

berechnen. Dazu wollen wir uns zunächst eine geometrische Vorstellung von T machen:

Beispiel 31 *(Geometrische Vorstellung der Grundfläche T)*

1. *Sei $K = \mathbb{Q}$, dann ist $X = \mathbb{R}_+$ und $N(x) = |x| = x$ für $x \in X$. Die Grundfläche ist $T = (0,1]$ ein Intervall und es gilt $\lambda_1(T) \;=\; 1$.*
2. *Wir betrachten den zweidimensionalen Fall: $K = \mathbb{Q}(\sqrt{d})$ mit $d < 0$ in $\mathbb{Z}$ quadratfrei. Es gilt*

$$\mu(K) \;=\; \mu\big(\mathbb{Q}(\sqrt{d})\big) \;=\; \begin{cases} \{\pm 1,\, \pm i\,\} & \text{falls } d = -1 \\ \{\pm 1,\, \pm\zeta,\, \pm\zeta^2\,\} & \text{falls } d = -3 \text{ mit } \zeta = e^{\frac{2\pi i}{3}} \\ \{\pm 1\,\} & \text{sonst} \end{cases}$$



Insgesamt gilt also $\lambda_2(T) \;=\; \frac{\pi}{\omega}$.

Beweis von Satz 14.8. Wir werden im ersten Schritt die zu berechnende Menge Isometrisch umformen um die Berechnung zu vereinfachen. Im zweiten Schritt wollen wir geschickt substituieren. Setze Hilfsmengen für $0 \leq k < \omega$

$$T_k \;:=\; \left\{ \underline{x} \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \underline{x} \text{ erfüllt die Bedingungen 1., 2. und 3'.} \right\}$$

1. $0 < N(\underline{x}) \leq 1$

2. $l(\underline{x}) = \xi\, l^* + \xi_1\, l(\varepsilon_1) + \ldots + \xi_m l(\varepsilon_m)$ mit $0 \leq \xi_i < 1$ für alle i

3'. $\frac{2\pi k}{\omega} \leq arg(x_1) \leq \frac{2\pi(k+1)}{\omega}$

Es ist also $T_0 = T$. Wähle nun eine Einheitswurzel $\zeta \in \mu(K)$ mit $\sigma_1(\zeta) = \exp(\frac{2\pi i}{\omega})$ dann ist

$$T_k \;=\; \iota(\zeta)^k \cdot T_0$$

Die Multiplikationsabbildung

$$\begin{aligned} \iota(\zeta)\cdot \,:\, \mathbb{R}^n &\;\to\; \breve{}R^n \\ x &\;\mapsto\; \iota(\zeta)\cdot x \end{aligned}$$

Ist ein $\mathbb{R}$-Vektorraumhomomorphismus mit Determinante $\det\left(\iota(\zeta)\cdot\right) \;=\; |N_{\mathbb{Q}}^K(\zeta)| \;=\; 1$. Damit ist $\lambda(T_k) \;=\; \lambda(T)$. Es gilt

$$\bigcup_{k=0}^{\omega-1} T_k \;=\; \left\{ \underline{x} \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; 0 \leq N\underline{x} < 1 \text{ und } 0 \leq \xi_i < 1 \right\}$$

Das heißt in der Gesamtvereinigung fällt also die Bedingung 3'. weg. Weil die Mengen T_k für alle T disjungt sind gilt

$$\lambda\left(\bigcup_{k=0}^{\omega-1} T_k\right) \;=\; \omega \cdot \lambda(T_0) \;=\; \omega \cdot \lambda(T)$$

Wir füren eine Weitere Menge ein. Setze

$$\overline{T} \;:=\; \left\{ \underline{x} \in \bigcup_{k=0}^{\omega-1} T_k \;\middle|\; x_1, \ldots, x_r \in \mathbb{R}_+ \right\}$$

Weiter sei G eine Gruppe, deren Elemente von der Form $g \;=\; (a_1, \ldots, a_r, 1, \ldots, 1) \;\in\; \mathbb{Z}^{r+s}$ mit $a_i \in \{\pm 1\}$ sind, das heißt

$$G \;:=\; \{\, (\underbrace{\pm 1, \ldots, \pm 1}_{r \text{ - mal}}, \underbrace{1, \ldots, 1}_{s \text{ - mal}}) \,\}$$

Dann gilt

$$\bigcup_{k=0}^{\omega-1} T_k \;=\; \bigcup_{g \in G} g\overline{T}$$

Damit können wir das Lebesgue-Maß von $\overline{T}$ in Abhängigkeit des Maßes der Vereinigun der T_k bestimmen. Es gilt

$$\lambda(\overline{T}) \;=\; \frac{1}{2^r} \cdot \lambda\left(\bigcup_{k=0}^{\omega-1} T_k\right) \qquad \Rightarrow \qquad \lambda(T) \;=\; \frac{2^r}{\omega} \cdot \lambda(\overline{T})$$

Wir können nun die Substitution angeben. Bisher haben wir

$$\lambda(\overline{T}) \;=\; \int_{(\overline{T})} \cdots \int \; 1 \; dx_1 \; \ldots \; dx_r \; d\Re(z_1) \; d\Im(z_1) \; \ldots \; d\Re(z_s) \; d\Im(z_s)$$

Setze nun für den reellen Anteil $\rho_j := x_j$ für $j = 1, \ldots, r$. für den komplexen Anteil setze

$$\rho_{j+r}^{\exp(i\cdot\theta_{j+r})} \;:=\; z_j \quad \text{das heißt } \rho_{j+r} = |z_j| \quad \text{ für } j = 1, \ldots, s$$

Wir erhalten die Substitution

$$\int_{(\overline{T})} \cdots \int \; 1 \; dx_1 \; \ldots \; dx_r \; d\Re(z_1) \; d\Im(z_1) \; \ldots \; d\Re(z_s) \; d\Im(z_s)$$

$$= \; \int_{(\overline{T})} \cdots \int \; \rho_{r+1} \cdots \rho_{r+s} \; d\rho_1 \; \ldots \; d\rho_r \; d\theta_{r+1} \; \ldots \; d\theta_{r+s}$$

Weiter erhalten wir eine neue Beschreibung der Menge $\overline{T}$ bezüglich der neuen Variablen:

$$\overline{T} \;=\; \Big\{ (\rho_1, \ldots, \rho_{s+r}) \,\Big|\, \rho_1, \ldots, \rho_{s+r} \in \mathbb{R}_+ \;\text{ und }\; \prod_{j=1}^{r+s} \rho_j^{l_j^*} \;\leq\; 1 \Big\}$$

Für alle $j = 1, \ldots, r+s$ gilt

$$\log\left(\rho_j^{l_j^*}\right) \;=\; \frac{l_j^*}{n} \cdot \log\Big(\prod_{j=1}^{r+s} \rho_j^{l_j^*} \Big) \;+\; \sum_{k=1}^{m} \xi_k \cdot l_j(\varepsilon_k) \qquad \text{mit } 0 \leq \xi_k < 1$$

Damit erhalten wir für $\underline{x} \in \overline{T}$

$$l(\underline{x}) \;=\; \big(\log(\rho_1^{l_1^*}), \ldots, \log(\rho_{r+s}^{l_{r+s}^*}) \big) \;=:\; \big(l_1(\underline{x}), \ldots, l_{r+s}(\underline{x}) \big)$$

Insbesondere ist dann $N(\underline{x}) = \prod_{j=1}^{r+s} \rho_j^{l_j^*} \leq 1$. Setze

$$M \;:=\; \begin{pmatrix} l_1^* & l_1(\varepsilon_1) & \cdots & l_1(\varepsilon_m) \\ l_2^* & l_2(\varepsilon_1) & \cdots & l_2(\varepsilon_m) \\ \vdots & \vdots & & \vdots \\ l_{r+s}^* & l_{r+s}(\varepsilon_1) & \cdots & l_{r+s}(\varepsilon_m) \end{pmatrix} \;\in \mathrm{Mat}_{r+s \times r+s}(\mathbb{R})$$

Für die Berechnung der Determinante von M dürfen wir Vielfache einer Zeile zu einer anderen hinzuaddieren, ohne das sich die Determinante ändert. Addiere also die Zeilen 2 bis $r+s$ einmal zur ersten Zeile, dann gilt

$$\det(M) \;=\; \det \begin{pmatrix} n & 0 & \cdots & 0 \\ l_2^* & l_2(\varepsilon_1) & \cdots & l_2(\varepsilon_m) \\ \vdots & \vdots & & \vdots \\ l_{r+s}^* & l_{r+s}(\varepsilon_1) & \cdots & l_{r+s}(\varepsilon_m) \end{pmatrix} \;=\; n \cdot R_K \;\neq 0$$

Setze nun $\xi := \rho_1^{l_1^*} \cdots \rho_{r+s}^{l_{r+s}^*}$, dann gilt für alle $j = 1, \ldots, r+s$

$$\log\left(\rho_j^{l_j^*}\right) \;=\; \frac{l_j^*}{n} \cdot \log(\xi) \;+\; \sum_{k=1}^{m} \xi_k \cdot l_j(\varepsilon_k) \qquad \text{mit } 0 \le \xi_k < 1 \tag{14.1}$$

Dann können wir $\overline{T}$ noch besser beschreiben durch

$$\overline{T} \;:=\; \left\{ \left(\log(\rho_j^{l_j^*})\right)_{0 \le j \le r+s} \,\middle|\, \log(\rho_j^{l_j^*}) \;=\; \frac{l_j^*}{n} \cdot \log(\xi) \;+\; \sum_{k=1}^{m} \xi_k \cdot l_j(\varepsilon_k) \qquad \text{mit } 0 \le \xi, \xi_k < 1 \right\}$$

Damit wir diese zweite Substitution aber für die Berechnung des Integrals nutzen können müssen wir noch die Jacobi-Matrix aufstellen. Es gelten

$$\frac{\partial \rho_i}{\partial \xi} \;=\; \frac{\rho_j}{n\xi} \qquad \text{und} \qquad \frac{\partial \rho_i}{\partial \xi_k} \;=\; \frac{\rho_j}{l_j^*} \cdot l_j(\varepsilon_k)$$

Damit erhalten wir die Jacobi-Matrix als

$$J \;=\; \begin{pmatrix} \frac{l_1^*}{n\xi} & \frac{\rho_1}{l_1^*} l_1(\varepsilon_1) & \cdots & \frac{\rho_1}{l_1^*} l_1(\varepsilon_m) \\ \vdots & \vdots & & \vdots \\ \frac{l_{r+s}^*}{n\xi} & \frac{\rho_{r+s}}{l_{r+s}^*} l_{r+s}(\varepsilon_1) & \cdots & \frac{\rho_{r+s}}{l_{r+s}^*} l_{r+s}(\varepsilon_m) \end{pmatrix} \;=\; \frac{\rho_1 \cdots \rho_{r+s}}{n \cdot \xi \cdot 2^s} \cdot M$$

Damit kennen wir die Determinante der Jacobi-Matrix bereits, denn es gilt

$$\det(J) \;=\; \frac{\rho_1 \cdots \rho_{r+s}}{\xi \cdot 2^s} \cdot R_K \;=\; \frac{R_K}{2^s \cdot \rho_{r+1} \cdot \rho_{r+s}}$$

Damit gilt bei der Substitution

$$\begin{aligned} dx_1 \,\ldots\, dx_r \; d\Re(z_1) \; d\Im(z_1) \,\ldots\, d\Re(z_s) \; d\Im(z_s) & \\ &= \; \rho_{r+1} \cdots \rho_{r+s} \;\; d\rho_1 \,\ldots\, d\rho_r \;\, d\theta_{r+1} \,\ldots\, d\theta_{r+s} \\ &= \; \det(J) \cdot \rho_{r+1} \cdots \rho_{r+s} \;\; d\xi \;\, d\xi_1 \,\ldots\, d\xi_m \;\, d\theta_{r+1} \,\ldots\, d\theta_{r+s} \end{aligned}$$

Wir erhalten also insgesamt

$$\begin{aligned} \lambda(\overline{T}) \;&=\; \int_{(\overline{T})} \cdots \int \; 1 \;\, dx_1 \,\ldots\, dx_r \; d\Re(z_1) \; d\Im(z_1) \,\ldots\, d\Re(z_s) \; d\Im(z_s) \\ &=\; \int_{(\overline{T})} \cdots \int \det(J) \cdot \rho_{r+1} \cdots \rho_{r+s} \;\; d\rho_1 \,\ldots\, d\rho_r \;\, d\theta_{r+1} \,\ldots\, d\theta_{r+s} \\ &=\; \int_{(\overline{T})} \cdots \int \frac{R_K}{2^s} \;\; d\rho_1 \,\ldots\, d\rho_r \;\, d\theta_{r+1} \,\ldots\, d\theta_{r+s} \\ &=\; \frac{R_K}{2^s} \cdot \int_0^{2\pi} \; d\theta_{r+1} \cdots \int_0^{2\pi} \; d\theta_{r+s} \cdot \int_0^1 \; d\xi \cdot \int_0^1 \; d\xi_1 \cdots \int_0^1 \; d\xi_m \\ &=\; \pi^s \cdot R_K \end{aligned}$$

Wir erhalten also insgesamt

$$\lambda(T) \;=\; \frac{2^r}{\omega} \cdot \lambda(\overline{T}) \;=\; \frac{2^r \cdot \pi^s \cdot R_K}{\omega}$$

Damit folgt der Satz aus Bemerkung 14.9. □

Mit Satz 14.8 ist **Behauptung 1** bewiesen. Erinnerung:

Behauptung 1 *Die Reihe $\zeta_K(t,c)$ konvergiert für $t > 1$ mit*

$$\lim_{t \searrow 1} (t-1) \cdot \zeta_k(t,c) \;=\; \frac{2^{r+s} \cdot \pi^s \cdot R_K}{\omega \cdot \sqrt{|D_K|}}$$

Und damit folgt auch sofort der Satz über die Dedekindsche ζ-Funktion 14.5. □

Kapitel VI

Anhang

i Literaturverzeichnis

[L1] **J. Neukirch**, Algebraische Zahlentheorie
[L2] **S. Lang**, Algebraic Numbertheory
[L3] **G. Wiese**, Vorlesungsskript Algebra II (uni.johoelken.de)
[L4] **G. Wiese**, Vorlesungsskript Algebra I (uni.johoelken.de)

ii Danksagungen

An dieser Stelle möchte ich mich bei allen Leser_innen bedanken, die mich auf (Tipp-)Fehler in meiner Mitschrift aufmerksam gemacht haben. Insbesondere möchte ich Jann Behrend und Kathrin Hövelmanns für das gewissenhafte Durchlesen danken.
Weiterhin danke ich Andrea Heßler für das Bereitstellen Ihrer Mitschrift der Vorlesung über die Gauß'schen Zahlen und Claudius Zibrowius für seine Mitschrift der Vorlesung über Lokalisierung (9.1 bis 9.13).

iii Lizenz

Stichwortverzeichnis