Algebraische Zahlentheorie

gehalten von Prof. Dr. Weitze-Schmithüsen im Sommer 23

UNIVERSITÄT
DES
SAARLANDES

Inhaltsverzeichnis

Allgemeine Informationen

Dieser Vorlesungsmitschrieb wird von einem Studenten erstellt und es handelt sich um einen nicht autorisierten Aufschrieb. Textsatz ist keine Garantie für Fehlerfreiheit. Wenn Sie Fehler in diesem Aufschrieb finden, schreiben Sie gerne eine E-Mail (zum Beispiel unter Angabe von Nummer des Abschnittes und Fehlerbeschreibung oder mit einem handschriftlich markiertem pdf) an:

s9fhguen@stud.uni-saarland.de

Kapitel 1

Einleitung

Die Hauptdarsteller der algebraischen Zahlentheorie sind *algebraische Zahlkörper*, also endliche Körpererweiterungen des Körpers der rationalen Zahlen $\mathbb{Q}$.

Klassische Beispiele für algebraische Zahlkörper bilden die *quadratische Zahlkörper*, d. h. Körpererweiterungen der rationalen Zahlen vom Grad 2. Diese sind immer von der Form $\mathbb{Q}(\sqrt{d})$ für eine ganze Zahl d. Quadratische Zahlkörper zerfallen in die reellquadratischen Zahlkörper, bei denen $d > 0$, und die imaginärquadratischen Zahlkörper, bei denen $d < 0$.

Je ein Beispiel für ein imaginärquadratischen Zahlkörper beziehungsweise reellquadratischen Zahlkörper wären $\mathbb{Q}(\mathrm{i}) = \mathrm{Lin}_{\mathbb{Q}}(1, \mathrm{i})$ beziehungsweise $\mathbb{Q}(\sqrt{-5}) = \mathrm{Lin}_{\mathbb{Q}}(1, \sqrt{-5})$.

Weitere klassische Beispiele für algebraische Zahlkörper sind die *zyklotomischen Körper*, d. h. Körper der Gestalt $\mathbb{Q}(\zeta_n)$ für eine primitive n-te Einheitswurzel ζ_n.

Den Ausgangspunkt für diese Vorlesung bilden die ganzen Zahlen $\mathbb{Z}$, die im Körper der rationalen Zahlen eingebettet sind. Genauer ist $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$. Für die ganzen Zahlen gibt es den wohlbekannten Fundamentalsatz der Arithmetik, der besagt, dass jede ganze Zahle eine eindeutige Primfaktorzerlegung besitzt.

Ein Ziel dieser Vorlesung wird sein, Konzepte für die rationalen Zahlen auf algebraische Zahlkörper zu verallgemeinern. Als erste Frage werden wir nach dem korrekten Analogon der ganzen Zahlen in einem algebraischen Zahlkörper K fragen. Das wird auf das Konzept des *Ganzheitsring* $\mathcal{O}_K$ führen. Diesen Ganzheitsring werden wir im Folgenden untersuchen. Insbesondere werden wir die Einheiten und Primelemente dieses Rings versuchen zu verstehen. Schließlich werden wir über eindeutige Primfaktorzerlegungen in Ganzheitsringen nachdenken und passende Verallgemeinerungen dieses Begriffs besprechen: Kummers Theorie idealer Zahlen. Als Maß dafür, wie weit ein Ganzheitsring davon entfernt ist, faktoriell zu sein, werden wir seine *Klassengruppe* $\mathrm{C}\ell_K$ einführen

und studieren. Ist die Klassengruppe trivial, dann haben wir eine eindeutige Primfaktorzerlegung.

Schließlich wollen wir geometrische Methoden, nämlich *Minkowski-Theorie*, verwenden, um die Struktur algebraischer Zahlen zu untersuchen. Dazu betrachten wir algebraische Zahlen als Punkte des $\mathbb{R}^n$, zeigen, dass $\#\,\mathrm{C}\ell$ endlich ist und berechnen die Einheitengruppe $\mathcal{O}_K^\times$. Zugehörig zu dieser Frage ist der *Dirichletsche Einheitensatz*.

Befruchtend für das Gebiet der algebraischen Zahlentheorie ist der legendäre letzte Satz von Fermat, der sagt, dass es für eine natürliche Zahl $n \geq 3$ keine paarweise verschiedenen ganzen Zahlen x, y und z gibt, sodass $x^n + y^n = z^n$ gilt. Dieser wurde 1637 von Fermat formuliert und erst 1994 von Andrew Wiles abschließend bewiesen.

Damit ist das Interesse für algebraische Zahlentheorie aber nicht abgestorben. Eine bis heute offene Frage ist, ob es unendlich viele algebraische Zahlkörper mit trivialer Klassengruppe gibt.

Kapitel 2

Algebraische ganze Zahlen

1 Ganzheitsringe

Eine komplexe Zahl z heißt ganzzahlig, falls es ein ganzzahliges normiertes Polynom $f = X^n + \sum_{i=0}^{n-1} a_i X^i$ gibt, sodass $f(z) = 0$ ist. Dieses Ganzheitskonzept soll uns für diesen Abschnitt leiten.

Als Generalvoraussetzung gehen wir im Folgenden stets davon aus, dass die Ringe, mit denen wir zu tun haben, kommutativ sind und eine Eins besitzen.

Definition II.1.1 (Ganzheit für Ringerweiterungen): Seien A ein Ring und B eine Ringerweiterung von A. Ist b ein Element von B und gibt es ein normiertes Polynom $f = X^n + \sum_{i=0}^{n-1} a_i X^i$ mit $n \geq 1$ und Koeffizienten aus A, sodass $f(b) = 0$, dann heißt b *ganz über* A.

Die Menge $\mathrm{Int}_B(A) = \{b \in B \text{ ganz über } A\}$, oder einfach nur $\mathrm{Int}(A)$, falls der Ring B aus dem Kontext klar ist, heißt *ganzer Abschluss von* A *in* B. Ist $B = \mathrm{Int}(A)$, dann heißt B *ganz über* A.

Unser erstes Ziel wird es sein zu zeigen, dass $\mathrm{Int}(A)$ in der oben beschriebenen Situation ein Ring ist.

Proposition II.1.2 (Ganzheitskriterien): *Seien A ein Ring, B eine Ringerweiterung von A und $b_1, \ldots, b_n$ Elemente von B. Genau dann sind $b_1, \ldots, b_n$ ganz über A, wenn $A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt ist.*

In der oben beschriebenen Situation ist $A[b_1, \ldots, b_n]$ die kleinste in B enthaltene A-Algebra, der $b_1, \ldots, b_n$ enthält. Diese A-Algebra kann man explizit angeben als

$$A[b_1, \ldots, b_n] = \Big\{ \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} a_{(k_1,\ldots,k_n)} b_1^{k_1} \cdots b_n^{k_n} : a_{(k_1,\ldots,k_n)} \in A \Big\}.$$

Korollar II.1.3 (Grundlegende Fakten über ganze Ringerweiterungen): *Seien A ein Ring und B eine Ringerweiterung von A.*

(i) *Der ganze Abschluss $\mathrm{Int}_B(A)$ von A in B ist selbst ein Ring.*

(ii) *Ist C eine Ringerweiterung von B und sind B ganz über A sowie C ganz über B, dann ist auch C ganz über A.*

Beweis: (i) Seien b_1 und b_2 Elemente von $\mathrm{Int}(A)$. Es bezeichne b die Differenz $b_1 - b_2$ oder das Produkt $b_1 b_2$. Nach Proposition II.1.2 ist $A[b_1, b_2, b] = A[b_1, b_2]$ ein endlich erzeugter A-Modul. Wiederum wegen Proposition II.1.2 sind dann b_1, b_2 und b ganz über A.

(ii) Sei c ein Element von C. Nach Voraussetzung gibt es Elemente $b_0, \ldots, b_{n-1}$ von B, sodass $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$. Der Ring $R = A[b_0, \ldots, b_{n-1}]$ ist nach Proposition II.1.2 ein endlich erzeugter A-Modul, und auch $R[c]$ ist ein endlich erzeugter R-Modul, der wegen der obigen Gleichung von 1, c, $\ldots$, c^{n-1} über R erzeugt wird. Erneute Anwendung von Proposition II.1.2 liefert schließlich, dass c ganz über A ist. □

Bevor wir Proposition II.1.2 beweisen können, wollen wir an ein paar Konzepte aus der linearen Algebra erinnern.

Erinnerung II.1.4: Seien R ein Ring und A in $R^{r\times r}$ eine Matrix. Für i, j in $\{1, \ldots, r\}$ bezeichne $A_{i,j}$ die $(r-1) \times (r-1)$-Matrix, die durch Streichung der i-ten Zeile und j-ten Spalte von A entsteht. Die Matrix $A^* = (a^*_{i,j})$ mit Einträgen

$$a^*_{i,j} = (-1)^{i+j} \det(A_{i,j}), \qquad 1 \leq i, j \leq r$$

heißt *Adjunkte von A*. Es gilt $A^*A = AA^* = (\det A)I_r$. Ferner gilt für jedes x in R^r mit $Ax = 0$, dass $(\det A)x = 0$.

Beweis (Proposition II.1.2): „$\Longrightarrow$“: Wir zeigen: Ist b in B ganz über A, dann ist $A[b]$ endlich erzeugt als A-Modul. Die Behauptung folgt dann durch Induktion.

Sei also b ganz über A. Dann gibt es ein Polynom f in $A[X]$, sodass $f(b) = 0$. Ist c ein Element von $A[b]$, dann gibt es ein Polynom g in $A[X]$, sodass $c = g(b)$ gilt. Weil f normiert ist, gibt es Polynome r und q in $A[X]$, sodass $g = qf + r$ und $\deg(r) < \deg(f)$. Es ist also $c = g(b) = r(b) = a_0 + a_1 b + a_{n-1}b^{n-1}$ für geeignete Elemente $a_0, \ldots, a_{n-1}$ von A. Als A-Modul wird $A[b]$ deshalb erzeugt von $1, b, \ldots, b^{n-1}$.

„$\Longleftarrow$“: Sei $A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul, sagen wir erzeugt von $w_1, \ldots, w_r$. Ferner sei b ein Element von $A[b_1, \ldots, b_n]$. Für jedes i in $\{1, \ldots, r\}$

liegt bw_i in $A[b_1, \ldots, b_n]$, insbesondere gibt es Elemente $a_{j,i}$ von A, sodass $bw_i = a_{1,i}w_1 + \cdots + a_{1,r}w_r$. Es gibt also eine Matrix $C = (a_{i,j})$ in $A^{r\times r}$, sodass

$$b\begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = C\begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix}.$$

Entsprechend gilt $(bI_r - C)(w_1, \ldots, w_r)^t = 0$ und nach der vorangegangenen Erinnerung gilt des Weiteren, dass $\det(bI_r - C)(w_1, \ldots, w_r)^t = 0$. Wir können 1 ausdrücken als Linearkombination $1 = \alpha_1 w_1 + \cdots + \alpha_r w_r$ mit geeigneten Elementen $\alpha_1, \ldots, \alpha_r$ von A und erhalten so, dass

$$\begin{aligned}\det(bI_r - C) &= \det(bI_r - C)1 \\ &= \alpha_1 \det(bI_r - C)w_1 + \cdots + \alpha_r \det(bI_r - C)w_r = 0.\end{aligned}$$

Setzen wir $f = \det(XI_r - C)$, dann ist f normiert und wir haben $f(b) = 0$, womit b ganz über A ist. □

Ein Ring A, der nullteilerfrei ist, heißt *Integritätsbereich* oder *Integritätsring*. Ist A ein Integritätsbereich, dann gibt es den Quotientenkörper

$$\mathrm{Quot}(A) = \left\{ \frac{a_1}{a_2} : a_1, a_2 \in A, a_2 \neq 0 \right\}_{/\sim}$$

wobei wir „$a_1/a_2 \sim b_1/b_2$“ schreiben, wenn $a_1b_2 = b_1a_2$. Diese Konstruktion liefert in der Tat einen Körper und dieser heißt *Quotientenkörper von A*. Die Abbildung $A \to \mathrm{Quot}(A)$, $a \mapsto a/1$ ist eine Einbettung von Ringen.

Definition II.1.5 (Normalisierung von Integritätsbereichen): Seien A ein Integritätsbereich und $K = \mathrm{Quot}(A)$ der zugehörige Quotientenkörper.

(i) Der ganze Abschluss $\mathrm{Int}_K(A)$ heißt *Normalisierung von A*.

(ii) Ist $\mathrm{Int}(A) = A$, dann heißt A *ganzabgeschlossen*.

Wir erinnern an weitere bekannte Konzepte aus der (linearen) Algebra. Seien dazu R ein Integritätsbereich, m ein Element von $R - (R^\times \cup \{0\})$.

(i) Falls für alle a und b in R mit $m = ab$ gilt, dass a oder b eine Einheit ist, dann heißt m *irreduzibel*.

(ii) Gilt für alle a und b in R mit $m \mid ab$, dass $m \mid a$ oder $m \mid b$, dann heißt m *prim*.

(iii) Kann jedes Element x von $R-\{0\}$ (bis auf Veränderung der Reihenfolge und bis auf Assoziiertheit) in eindeutiger Art und Weise als Produkt $x = up_1 \cdots p_n$ einer Einheit u und irreduziblen Elementen $p_1, \ldots, p_n$ schreiben, dann heißt R *faktoriell*.

In der linearen Algebra zeigt man, dass Irreduzibelität aus Primalität folgt. Außerdem zeigt man in der Algebra, dass in faktoriellen Ringen Primalität und Irreduzibelität zusammenfallen.

Bemerkung II.1.6: Sei A ein faktorieller Ring. Dann ist A ganzabgeschlossen.

Beweis: Sei $\alpha = a/a'$ ein Element von $\mathrm{Quot}(A)$, d. h. a und a' liegen in A und a' ist von Null verschieden. Wir dürfen annehmen, dass 1 der größte gemeinsame Teiler von a und a' ist. Angenommen, α wäre ganz über A. Dann gäbe es Elemente $\lambda_0, \ldots, \lambda_{n-1}$ von A, sodass $\alpha^n + \lambda_{n-1}\alpha^{n-1} + \cdots + \lambda_0 = 0$. Durchmultiplizieren mit a'^n lieferte dann, dass

$$a^n + \lambda_{n-1}a'a^{n-1} + \cdots + \lambda_0 a'^n = 0,$$

d. h. $a^n = -a'(\lambda_{n-1}a^{n-1} + \cdots + \lambda_0 a'^{n-1})$, weshalb a' ein Teiler von a^n sein müsste. Wäre π ein Primelement von A, das a' teilen würde, dann würde π auch a teilen, was unserer Voraussetzung an a und a' widerspräche. Darum muss a' eine Einheit sein und α bereits zu A gehören. □

Proposition II.1.7 (Ganzer Abschluss in Erweiterungskörpern): *Seien A ein Integritätsbereich, K der Quotientenkörper von A und A ganzabgeschlossen. Ist L eine endliche Körpererweiterung von K und B der ganze Abschluss von A in L. Dann gilt:*

(i) *B ist ganzabgeschlossen in L.*

(ii) $L = \{\beta = b/a \mid b \in B, a \in A - \{0\}\} = \mathrm{Quot}(B)$.

(iii) $B = \{\beta \in L \mid$ *Das normierte Minimalpolynom f_β von β liegt in $A[X]$*$\}$.

Insbesondere ist B ein ganzabgeschlossener Ring.

Beweis: (i) Sei C der ganze Abschluss von B in L. Dann ist B ganz über A und C ganz über B, sodass Korollar II.1.3 bereits liefert, dass C ganz über A ist, weshalb C in B enthalten sein muss, also gleich B ist.

(ii) Sei β ein Element von L. Da L eine endliche Körpererweiterung über K ist, gibt es ein Polynom f_β in $K[X]$ mit $f_\beta(\beta) = 0$, d. h. es gibt $a'_0, \ldots, a'_n$ in K mit $a'_n\beta^n + a'_{n-1}\beta^{n-1} + \cdots + a'_0 = 0$. Durchmultiplizieren mit dem Produkt der

Nenner liefert $a_0, \ldots, a_n$ aus A, sodass $a_n\beta^n + \cdots + a_0\beta = 0$, und multiplizieren dieser Gleichung mit a_n^{n-1} gibt

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + a_{n-2}a_n(a_n\beta)^{n-2} + \cdots + a_0a_n^{n-1} = 0.$$

Das heißt, dass $b = a_n\beta$ ganz über A ist und damit in B liegt, und $\beta = b/a_n$ ist von der behaupteten Gestalt.

(iii) Die Inklusion „$\supseteq$“ folgt per Definition. Bleibt „$\subseteq$“ zu zeigen. Sei also β ganz über A. Das heißt es gibt ein normiertes Polynom g aus $A[X]$, sodass $g(\beta) = 0$. Sei f_β in $K[X]$ das normierte Minimalpolynom von β. Dann wird g von f_β geteilt. Im algebraischen Abschluss $\overline{K}$ von K können wir f_β schreiben als Produkt von Linearfaktoren $f_\beta = (X - \gamma_1)\cdots(X - \gamma_n)$ für geeignete Elemente $\gamma_1, \ldots, \gamma_n$ von $\overline{K}$. Da g von f_β geteilt wird, sind $\gamma_1, \ldots, \gamma_n$ Nullstellen von g, weshalb sie ganz über A sind. Darum sind die Koeffizienten von f_β ebenfalls ganz über A, außerdem liegen sie in K und aus diesem Grund ist f_β sogar in $A[X]$. □

Definition II.1.8 (Ganzheitsringe von Zahlkörpern): Sei K ein Zahlkörper. Der Ring

$$\begin{aligned}\mathcal{O}_K &= \mathrm{Int}_K(\mathbb{Z}) \\ &= \{\alpha \in K \mid \text{Normiertes Minimalpolynom } f_\alpha \text{ von } \alpha \text{ liegt in } \mathbb{Z}[X]\}\end{aligned}$$

heißt *Ganzheitsring von K*.

Die Charakterisierung $K = \mathrm{Quot}(\mathcal{O}_K) = \{b/a \mid b \in \mathcal{O}_K, a \in \mathbb{Z} - \{0\}\}$ folgt direkt aus Proposition II.1.7, und außerdem erhalten wir aus dieser Proposition, dass $\mathcal{O}_K$ ganzabgeschlossen ist.

Beispiel II.1.9 (Erste Ganzheitsringe): (i) Ist K der Körper der rationalen Zahlen, dann ist der Ganzheitsring

$$\mathcal{O}_K = \{\alpha \in \mathbb{Q} \mid \text{Normiertes Minimalpolynom } f_\alpha \text{ liegt in } \mathbb{Z}[X]\} = \mathbb{Z},$$

denn für eine rationale Zahl α ist $f_\alpha = X - \alpha$ das zugehörige Minimalpolynom.

(ii) Seien K der Körper $\mathbb{Q}(\mathrm{i})$ und $\alpha = a + b\mathrm{i}$ ein Element von $\mathbb{Q}(\mathrm{i})$ ist $\alpha^2 = a^2 + 2ab\mathrm{i} - b^2 = 2a\alpha - (a^2 + b^2)$, sodass $f_\alpha = X^2 - 2aX + (a^2 + b^2)$ das Minimalpolynom von α ist.

Ist a eine ganze Zahl, dann auch b.

Ist $a = k/2$ für eine ungerade ganze Zahl k, dann schreiben wir $b = b_1/b_2$ für ganze Zahlen b_1 und b_2 mit $\mathrm{ggT}(b_1, b_2) = 1$. Die Zahl $\ell = a^2 + b^2 = k^2/4 + (b_1/b_2)^2$

ist dann eine ganze Zahl, und $4b_2^2\ell = b_2^2k^2 + 4b_1^2$, sodass b_2 in $\{1, 2\}$ liegen muss. Wäre $b_2 = 2$, dann hätten wir $16\ell = 4k^2 + 4b_1^2$, sodass $4\ell = k^2 + b_1^2$ mit ungeradem k und b_1 sein müsste. Das widerspräche aber $k^2 \equiv 1 \equiv b_1^2$.

Als Ergebnis halten wir fest: Der Ganzheitsring von $K = \mathbb{Q}(\mathrm{i})$ ist genau der Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$.

(iii) Sei K der Körper $\mathbb{Q}(\zeta_n)$ für eine primitive n-te Einheitswurzel ζ_n. In der Algebra zeigt man üblicherweise, dass der Grad dieser Körpererweiterung gerade $[K : \mathbb{Q}] = \varphi(n)$ ist. Hierbei bezeichnet φ die Euler'sche Phi-Funktion. Entsprechend ist $\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$ eine Basis von K über $\mathbb{Q}$. Wir werden später zeigen, dass der Ganzheitsring dieses Zahlkörpers der Ring $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ ist. Dafür werden wir Diskriminanten verwenden müssen.

(iv) Sei K der Zahlkörper $\mathbb{Q}(\sqrt{5})$ und $\alpha = \frac{1}{2}(1+\sqrt{5})$. Dann ist $(2\alpha-1)^2 = 5$, sodass $4\alpha^2 - 4\alpha + 1 = 5$, also $\alpha^2 - \alpha - 1 = 0$. Das Minimalpolynom von α ist deshalb $f_\alpha = X^2 - X - 1$ und α ganz. Entsprechend ist $\mathcal{O}_K$ *nicht* der Ring $\mathbb{Z}[\sqrt{5}]$.

2 Ganzheitsbasen und Diskriminanten von Körpererweiterungen

Erinnerung II.2.1 (Spur und Norm): Seien K ein Körper und L ein Erweiterungskörper von K mit $[L : K] = n$. Ist α ein Element von L, dann erhalten wir eine K-lineare Abbildung $T_\alpha \colon L \to L$, $\beta \mapsto \alpha\beta$. Man nennt $\mathrm{Tr}(\alpha) = \mathrm{Tr}_{L|K}(\alpha) = \mathrm{Tr}(T_\alpha)$ die *Spur von* α und $N(\alpha) = N_{L|K}(\alpha) = \det T_\alpha$ die *Norm von* α.

Wegen der Eigenschaften von Spur und Determinante haben wir für α_1 und α_2 aus L, dass

$$\mathrm{Tr}_{L|K}(\alpha_1 + \alpha_2) = \mathrm{Tr}_{L|K}(\alpha_1) + \mathrm{Tr}_{L|K}(\alpha_2), \quad N_{L|K}(\alpha_1\alpha_2) = N_{L|K}(\alpha_1)N_{L|K}(\alpha_2).$$

Anders formuliert sind $\mathrm{Tr}_{L|K} \colon (L, +) \to (K, +)$ und $N_{L|K} \colon L^\times \to K^\times$ Gruppenhomomorphismen.

Ist $L = K(\alpha_0)$ eine einfache Körpererweiterung und $f_{\alpha_0} = X^n + \sum_{i=0}^{n-1} a_i X^i$ das Minimalpolynom von α_0, dann ist $\mathrm{Tr}_{L|K}(\alpha_0) = -a_{n-1}$ und $N_{L|K}(\alpha_0) = (-1)^n a_0$.

Ist $L|K$ eine separable Körpererweiterung, ist $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$, ist α ein Element von L und ist f_α das zugehörige charakteristische Polynom, dann ist

$$f_\alpha = \prod_{i=1}^{n} \big(X - \sigma_i(\alpha)\big).$$

Entsprechend gilt $\mathrm{Tr}_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$ und $N_{L|K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

Schließlich sind Spur und Norm transitiv. Sind genauer $K \subseteq L$ und $L \subseteq M$ Körpererweiterungen, dann sind

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

Beispiel II.2.2 (Spur und Norm für quadratische Zahlkörper): (i) Seien L der Körper $\mathbb{Q}(\mathrm{i})$ und $\alpha = a + b\mathrm{i}$ ein Element von L. Für die $\mathbb{Q}$-Basis $B = \{1, \mathrm{i}\}$ von L erhalten wir

$$D_{BB}(T_\alpha) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \qquad \mathrm{Tr}(\alpha) = 2\alpha, \qquad N(\alpha) = a^2 + b^2.$$

Ferner haben wir letztes Mal bereits das Minimalpolynom von α berechnet, dieses ist $f_\alpha = X^2 - 2aX + a^2 + b^2$.

(ii) Seien allgemeiner d eine quadratfreie ganze Zahl d und L der Zahlkörper $\mathbb{Q}(\sqrt{d})$. Dann ist $B = \{1, \sqrt{d}\}$ eine $\mathbb{Q}$-Basis von L. Für das Element $\alpha = a + b\sqrt{d}$ können wir Norm und Spur wie oben direkt bestimmen:

$$D_{BB}(T_\alpha) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \qquad \mathrm{Tr}(\alpha) = 2a, \qquad N(\alpha) = a^2 - b^2 d.$$

Das Minimalpolynom von α ist $f_\alpha = X^2 - 2aX + a^2 - b^2 d$.

Definition II.2.3 (Diskriminante): Seien A ein Integritätsring, $K = \mathrm{Quot}(A)$, $L|K$ eine separable Körpererweiterung vom Grad n und $\mathrm{Hom}(L, \overline{K})$ sei die Menge $\{\sigma_1, \ldots, \sigma_n\}$. Es seien $B = \{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L und

$$A_B = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

Die Determinante $\det(A_B^2) = (\det A_B)^2 = (\det A)(\det A^t)$ heißt *Diskriminante von L über K bezüglich* $\{\alpha_1, \ldots, \alpha_n\}$ und wird mit $d(\alpha_1, \ldots, \alpha_n)$ bezeichnet.

Beispiel II.2.4 (Diskriminanten für quadratische Zahlkörper): Seien d eine quadratfreie ganze Zahl, L der Zahlkörper $\mathbb{Q}(\sqrt{d})$ und K der Körper der rationalen Zahlen. Dann ist

$$\mathrm{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}}) = \{\sigma_1 = \mathrm{id}, \sigma_2 \colon a + b\sqrt{d} \mapsto a - b\sqrt{d}\}.$$

Wir rechnen zunächst bezüglich der $\mathbb{Q}$-Basis $B_1 = \{1, \sqrt{d}\}$:

$$A_{B_1} = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}, \qquad \det(A_{B_1}) = -2\sqrt{d}, \qquad d(1, \sqrt{d}) = 4d.$$

Rechnen wir mit der $\mathbb{Q}$-Basis $B_2 = \{1 + \sqrt{d}, 1 - \sqrt{d}\}$, dann liefert das

$$A_{B_2} = \begin{pmatrix} 1+\sqrt{d} & 1-\sqrt{d} \\ 1-\sqrt{d} & 1+\sqrt{d} \end{pmatrix}, \qquad \det(A_{B_2}) = (1+\sqrt{d})^2 - (1-\sqrt{d})^2 = 4\sqrt{d}$$

und für die Diskriminante bezüglich B_2 ergibt sich $d(1 + \sqrt{d}, 1 - \sqrt{d}) = 16d$.

Proposition II.2.5 (Berechnungsmöglichkeiten für die Diskriminante): *Seien A ein Integritätsring, $K = \mathrm{Quot}(A)$, $L|K$ eine separable Körpererweiterung vom Grad n und $B = \{\alpha_1, \ldots, \alpha_n\}$ eine Basis von $L|K$.*

(i) *Es bezeichne C_B die Matrix $(\mathrm{Tr}(\alpha_i\alpha_j))_{1\le i,j\le n}$. Dann ist $\det C_B$ die Diskriminante $d(\alpha_1, \ldots, \alpha_n)$. Insbesondere gehört sie zu K.*

(ii) *Sei θ aus L ein primitives Element für L über K, d. h. $L = K(\theta)$, und es sei B die K-Basis $\{1, \theta, \ldots, \theta^{n-1}\}$ von L. Mit der Schreibweise $\theta_i = \sigma_i(\theta)$ gilt $d(1, \theta, \ldots, \theta^{n-1}) = \prod_{1\le i<j\le n}(\theta_i - \theta_j)$.*

Beweis: (i) Aus der linearen Algebra ist bekannt, dass $\det(A_B)^2 = \det(A_B^t A_B)$ und es gilt

$$\begin{aligned} A_B^t A_B &= (\sigma_j(\alpha_i))_{i,j}(\sigma_k(\alpha_\ell))_{k,\ell} \\ &= \Big(\sum_{j=1}^{n} \sigma_j(\alpha_i)\sigma_j(\alpha_\ell)\Big)_{i,\ell} = \Big(\sum_{j=1}^{n} \sigma_j(\alpha_i\alpha_\ell)\Big)_{i,\ell} = (\mathrm{Tr}_{L|K}(\alpha_i\alpha_\ell))_{i,\ell} = C_B. \end{aligned}$$

(ii) Zur vorgegebenen Matrix B ist

$$\det A_B = \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix} = V_n(\theta_1, \ldots, \theta_n)$$

die Vandermonde-Matrix zu den Einträgen $\theta_1, \ldots, \theta_n$. Aus der linearen Algebra ist bekannt, dass man für die Determinante der Vandermonde-Matrix durch Induktion die Formel $\det V_n(\theta_1, \ldots, \theta_n) = \prod_{1\le i<j\le n}(\theta_i - \theta_j)$ erhält. □

Proposition II.2.6 (Diskiminante ungleich Null): *Seien A ein Integritätsring, $K = \mathrm{Quot}(A)$, $L|K$ eine separable Körpererweiterung vom Grad n und B der ganze Abschluss $\mathrm{Int}_L(A)$.*

(i) *Die bilineare Abbildung*

$$h\colon L \times L \longrightarrow K, \qquad (x, y) \longmapsto \mathrm{Tr}(xy)$$

ist nicht degeneriert, d. h. für kein y in $L - \{0\}$ ist die lineare Abbildung $h_y\colon L \to K$, $x \mapsto \mathrm{Tr}(xy)$ die Nullabbildung.

(ii) *Für jede Basis $\{\alpha_1, \ldots, \alpha_n\}$ der Körpererweiterung $L|K$ ist die Diskriminante $d(\alpha_1, \ldots, \alpha_n)$ von Null verschieden.*

Beweis: (i) Da $L|K$ separabel ist, gibt es ein primitives Element θ und eine zugehörige Basis $\{1, \theta, \ldots, \theta^{n-1}\}$ von L über K. Die Gramsche Matrix von h bezüglich der Basis B ist $G = (\mathrm{Tr}(\theta^{i-1}\theta^{j-1}))_{i,j}$. Nach Proposition II.2.5(i) haben wir $\det G = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \le i < j \le n}(\theta_j - \theta_i)^2 \neq 0$, wobei θ_i wie zuvor für $\sigma_i(\theta)$ steht. Damit ist h nicht degeneriert.

(ii) Nach Proposition II.2.5(i) ist $d(\alpha_1, \ldots, \alpha_n) = \det C$ für $C = (\mathrm{Tr}(\alpha_i\alpha_j))_{i,j}$, wobei C die Fundamentalmatrix von h bezüglich der Basis $\{\alpha_1, \ldots, \alpha_n\}$ ist. Weil h nach (i) nicht degeneriert ist, ist auch diese Determinante von Null verschieden. □

Notation II.2.7: Seien R ein Ring und S ein Erweiterungsring von R. Dann schreiben wir $\mathrm{Int}_S(R)$ für den *ganzen Abschluss von R in S*.

Im Folgenden wollen wir annehmen, dass A ganzabgeschlossen ist, d. h. für $K = \mathrm{Quot}(A)$ wollen wir annehmen, dass $A = \mathrm{Int}_K(A)$. Für eine Körpererweiterung L von K schreiben wir B für den ganzen Abschluss $\mathrm{Int}_L(A)$.

Proposition II.2.8 (Spur und Norm erhält Ganzheit): *Seien $L|K$ eine separable Körpererweiterung vom Grad n, $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ mit $\sigma_1 = \mathrm{id}$ und x ein Element von B.*

(i) *Für jedes σ in $\mathrm{Hom}_K(L, \overline{K})$ ist auch $\sigma(x)$ ganz über A.*

(ii) *Es sind $\mathrm{Tr}_{L|K}(x)$ und $N_{L|K}(x)$ ganz über A.*

(iii) *Genau dann ist x eine Einheit in B, wenn $N_{L|K}(x)$ in $A^\times$ liegt.*

Beweis: (i) Da x zu B gehört, liefert Bemerkung I.1.7, dass das normierte Minimalpolynom f_x von x über K in $A[X]$ liegt. Dann ist auch $\sigma(x)$ eine Nullstelle von f_x, weshalb $\sigma(x)$ ganz über A ist.

(ii) Da x in B liegt, wissen wir, dass $\mathrm{Tr}_{L|K}(x) = \sum_{i=1}^{n} \sigma_i(x)$ gilt. Nach (i) ist $\mathrm{Tr}(x)$ ganz über A und lebt in K, sodass $\mathrm{Tr}(x)$ auch zu A gehört.

(iii) Die Implikation „$\Longrightarrow$“ folgt aus (ii) in Verbindung mit der Multiplikativität der Norm.

Zu „$\Longleftarrow$“: Ist $N_{L|K}(x)$ eine Einheit in A, dann gibt es ein Element a von A, sodass $1 = aN_{L|K}(x) = a\prod_{i=1}^{n} \sigma_i(x) = (a\prod_{i=2}^{n} \sigma_i(x))x$, was gerade bedeutet, dass x eine Einheit in B ist. □

Korollar II.2.9 (Ganzzahligkeit der Diskriminiante): *Seien $L|K$ eine separable Körpererweiterung von Grad n und $\alpha_1, \ldots, \alpha_n$ Elemente von B, die eine K-Basis von L bilden. Dann ist $d(\alpha_1, \ldots, \alpha_n)$ in A enthalten.*

Beweis: Proposition I.2.4(i) und Proposition I.2.8(ii). □

Satz 1 (Basen von ganzen Elementen): *Seien $L|K$ eine separable Körpererweiterung vom Grad n, $\alpha_1, \ldots, \alpha_n$ Elemente von B derart, dass $\{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L bildet und $d = d(\alpha_1, \ldots, \alpha_n)$ die Diskriminante von L über K bezüglich $\alpha_1, \ldots, \alpha_n$, die in A liegt. Dann ist dB in $A\alpha_1 + \cdots + A\alpha_n$ enthalten.*

Beweis: Sei α ein Element von B. Dann gibt es geeignete Elemente $c_1, \ldots, c_n$ von K, sodass $\alpha = \sum_{i=1}^{n} c_i\alpha_i$. Für jedes i in $\{1, \ldots, n\}$ ist $\alpha_i\alpha = \sum_{j=1}^{n} \alpha_i c_j \alpha_j$ ein Element von B. Für die Spur dieser Elemente erhalten wir

$$\mathrm{Tr}_{L|K}(\alpha_i\alpha) = c_1 \mathrm{Tr}(\alpha_i\alpha_1) + \cdots + c_n \mathrm{Tr}(\alpha_i\alpha_n),$$

d. h. der Vektor $x = (c_1, \ldots, c_n)^t$ des K^n ist Lösung eines linearen Gleichungssystems $Mx = y$ für $y = (\mathrm{Tr}(\alpha_1\alpha), \ldots, \mathrm{Tr}(\alpha_n\alpha))^t$ in A^n und $M = (\mathrm{Tr}(\alpha_i\alpha_j))$ in $A^{n\times n}$. Mit der Erinnerung zur Adjunkten sehen wir ein, dass einerseits $(\det M)x = M^{\#}Mx = M^{\#}y$ gilt und dass andererseits $M^{\#}y$ auch in A^n liegt. Das liefert uns, dass für jedes i das Element dc_i zu A gehört. Aus der ursprünglichen Gleichung für α folgt, dass $d\alpha = dc_1\alpha_1 + \cdots + dc_n\alpha_n$ in $A\alpha_1 + \cdots + A\alpha_n$ enthalten ist. □

Definition II.2.10 (Ganzheitsbasis): Seien A ein Integritätsbereich, K der Quotientenkörper von A, $L|K$ eine separable Körpererweiterung von Grad n, $B = \mathrm{Int}_L(A)$ der ganze Abschluss von A in L und $\alpha_1, \ldots, \alpha_n$ Elemente von B. Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von B als A-Modul, d. h. für jedes α in B gibt es eindeutige Elemente $c_1, \ldots, c_n$ in A mit $\alpha = \sum_{i=1}^{n} c_i\alpha_i$, dann heißt $\{\alpha_1, \ldots, \alpha_n\}$ eine *Ganzheitsbasis von B über A.*

Bemerkung II.2.11 (Ganzzahlige vs. Ganzheitsbasis): (i) Wir haben bereits gesehen, dass in der beschriebenen Situation für L die Charakterisierung $L = \{b/a \mid b \in B, a \in A - \{0\}\}$ gilt. Eine K-Basis $\{\alpha_1 = b_1/a_1, \ldots, \alpha_n = b_n/a_n\}$ von L liefert deshalb eine ganzzahlige Basis $\{\alpha'_1, \ldots, \alpha'_n\}$ durch Ausräumen der Nenner, zum Beispiel durch Multiplikation jedes α_i mit $a_1 \cdots a_n$. Insbesondere gibt es immer ganzzahlige Basen.

(ii) Im Allgemeinen sind ganzzahlige Basen keine Ganzheitsheitsbasen. In Beispiel I.1.9 haben wir schon $L = \mathbb{Q}(\sqrt{5})$, $K = \mathbb{Q}$, $A = \mathbb{Z}$ und $\alpha = 1/2(1+\sqrt{5})$ betrachtet und gesehen, dass α ganz über $\mathbb{Z}$ ist, weshalb $\{1, \sqrt{5}\}$ zwar eine ganzzahlige $\mathbb{Q}$-Basis, aber keine Ganzheitsbasis ist.

Korollar II.2.12 (aus Satz 1): *Sei L ein Zahlkörper vom Grad n mit Ganzheitsring $\mathcal{O}_L$. Dann besitzt $\mathcal{O}_L$ eine Ganzheitsbasis. Insbesondere gilt $\mathcal{O}_L \cong \mathbb{Z}^n$.*

Beweis: Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine ganzzahlige $\mathbb{Q}$-Basis von L. Nach Satz 1 ist $d\mathcal{O}_L$ enthalten in $\bigoplus_{i=1}^n \mathbb{Z}\alpha_i$, beziehungsweise $\mathcal{O}_L$ enthalten in $\bigoplus_{i=1}^n \mathbb{Z}\frac{\alpha_i}{d}$. Deshalb ist $\mathcal{O}_L$ Untermodul eines freien $\mathbb{Z}$-Moduls und damit selbst frei. Ferner ist $\operatorname{Rang} \mathcal{O}_L$ höchstens n. Andererseits haben wir $\bigoplus_{i=1}^n \mathbb{Z}\alpha_i \subseteq \mathcal{O}_L$, weshalb $\operatorname{Rang} \mathcal{O}_L$ wenigstens n sein muss. Darum folgt $\operatorname{Rang} \mathcal{O}_L = n$ und $\mathcal{O}_L \cong \mathbb{Z}^n$. □

Bemerkung II.2.13 (Diskriminante von Ganzheitsbasen in Zahlkörpern): Wie wir zuvor gezeigt haben, ist $d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(\operatorname{Tr}(\alpha_i\alpha_j))_{i,j}$ und $(\operatorname{Tr}(\alpha_i\alpha_j))$ ist die Fundamentalmatrix der Bilinearform $h\colon (x, y) \mapsto \operatorname{Tr}(xy)$ bezüglich der Basis $\{\alpha_1, \ldots, \alpha_n\}$.

Seien L ein Zahlkörper und $B = \{\alpha_1, \ldots, \alpha_n\}$, $B' = \{\alpha'_1, \ldots, \alpha'_n\}$ Ganzheitsbasen von L. Dann ist $\mathcal{O}_L = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i = \bigoplus_{i=1}^n \mathbb{Z}\alpha'_i$. Die Basiswechselmatrix $T = D_{BB'}$ ist in diesem Fall enthalten in $\mathrm{Gl}_n(\mathbb{Z})$, hat also Determinante ± 1, und für die Fundamentalmatrizen $(\operatorname{Tr}(\alpha_i\alpha_j))_{i,j}$, $(\operatorname{Tr}(\alpha'_i\alpha'_j))_{i,j}$ gilt

$$\begin{aligned} d(\alpha'_1, \ldots, \alpha'_n) &= \det(\operatorname{Tr}(\alpha'_i\alpha'_j))_{i,j} \\ &= \det T^2 \det(\operatorname{Tr}(\alpha_i\alpha_j))_{i,j} = d(\alpha_1, \ldots, \alpha_n), \end{aligned}$$

sodass alle Diskriminanten von Zahlkörpern bezüglich Ganzheitsbasen gleich sind.

Definition II.2.14 (Diskriminante eines Zahlkörpers): Sei K ein Zahlkörper. Die Diskriminante von K über $\mathbb{Q}$ bezüglich einer (und damit jeder) Ganzheitsbasis wird *Diskriminante von K* genannt und mit d_K notiert.

Satz 2 (B-Moduln in L sind freie A-Moduln): *Seien A ein Hauptidealring, $K = \operatorname{Quot}(A)$, $L|K$ eine separable Körpererweiterung vom Grad n und $0 \neq M$ ein endlich erzeugter B-Untermodul von L. Dann ist M ein freier A-Modul von Rang $n = [L : K]$.*

Erinnerung II.2.15 (Struktursatz): Seien A ein Hauptidealring und M_0 ein freier A-Modul. Dann gilt:

(i) Jeder Untermodul M von M_0 hat eine Basis, ist also frei.

(ii) Der Rang von M ist höchstens der Rang von M_0.

Beweis (von Satz 2): Seien $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von L über K bestehend aus Elementen von B, $d = d(\alpha_1, \ldots, \alpha_n)$ die Diskriminante und $\{\mu_1, \ldots, \mu_r\}$ ein Erzeugendensystem von M als B-Modul. Unter Verwendung der Charakterisierung $L = \{b/a \mid b \in B, a \in A - \{0\}\}$ sehen wir ein, dass es a in A gibt, sodass $\{a\mu_1, \ldots, a\mu_r\}$ enthalten ist in B. Damit ist adM enthalten in dB, was wiederum in $\bigoplus_{i=1}^n A\alpha_i$ liegt. Nach Erinnerung II.2.15 ist adM selbst ein freier A-Modul von Rang höchstens n. Andererseits ist A^n isomorph zu $\bigoplus_{i=1}^n A\alpha_i\mu_i$, was in M enthalten ist, sodass der Rang von M mindestens n ist. Insgesamt ist $\operatorname{Rang} M = n$. □

Beispiel II.2.16 (Ganzheitsbasen für quadratische Zahlkörper): Seien D eine quadratfreie, von Null und Eins verschiedene ganze Zahl, L der Zahlkörper $\mathbb{Q}(\sqrt{D})$ und K der Körper der rationalen Zahlen. In Beispiel I.1.19 haben wir das normierte Minimalpolynom von $\alpha = a + b\sqrt{D}$ aus L bestimmt; das war nämlich $f_\alpha = X^2 - 2aX + a^2 - b^2D$. Genau dann ist also α ein Element des Ganzheitsrings, wenn $\operatorname{Tr}(\alpha) = 2a$ und $N(\alpha) = a^2 - b^2D$ ganze Zahlen sind.

(i) Wir zeigen für $\alpha = a + b\sqrt{D}$ in $\mathcal{O}_L$, dass $2b$ eine ganze Zahl ist. Dazu schreiben wir b als p/q mit geeigneten teilerfremden ganzen Zahlen p und q. Da α im Ganzheitsring liegt, ist $a^2 + b^2D = z$ eine ganze Zahl, sodass

$$\begin{aligned}(2a)^2 - 4b^2D = 4z &\Longrightarrow q^2(2a)^2 - 4p^2D = 4q^2z \\ &\Longrightarrow 4p^2D = q^2((2a)^2 - 4z)\end{aligned}$$

weshalb q entweder 1 oder 2 sein muss.

(ii) Wir zeigen, dass im Fall $q = 2$ gelten muss: $D \equiv 1 \pmod 4$. Wegen der letzten Gleichung in (i) ist

$$p^2D = (2a)^2 - 4z \equiv (2a)^2 \pmod 4.$$

Da p und q nach Voraussetzung teilerfremd sind, muss p ungerade sein. Damit gilt für die rationale Zahl a, dass $2a$ ungerade ist, da D als quadratfrei angenommen ist. Entsprechend gilt $p^2 \equiv 1 \equiv (2a)^2 \pmod 4$, womit $D \equiv 1 \pmod 4$. Zusammenfassend gesagt gilt im Fall $D \not\equiv 1 \pmod 4$, dass $\mathcal{O}_L = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{D}]$.

(iii) Wir zeigen, dass im Fall $D \equiv 1 \pmod 4$ gilt: a und b sind ganz oder $2a$ und $2b$ sind ungerade.

Ist in (i) $q = 1$, dann zeigt die letzte Gleichung in (i), dass a eine ganze Zahl ist. Wegen $q = 1$ ist dann auch b eine ganze Zahl.

Gilt $q = 2$ in (i), dann folgt in (ii) dass $2a$ und $p = 2b$ ungerade sind.

Zusammenfassend erhalten wir im Fall $D \equiv 1 \pmod 4$ für den Ganzheitsring

$$\mathcal{O}_L = \left\{ \frac{a'}{2} + \frac{b'}{2}\sqrt{D} : a', b' \in \mathbb{Z} \right\} \cup \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} = \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{D}\right].$$

Als Fazit halten wir für die Ganzheitsringe quadratischer Zahlkörper fest:

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{falls } D \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{D}], & \text{falls } D \equiv 1 \pmod 4. \end{cases}$$

Insbesondere ist im ersten Fall $\{1, \sqrt{D}\}$ und im zweiten Fall $\{1, \frac{1}{2}(1+\sqrt{D})\}$ eine Ganzheitsbasis. In Beispiel II.2.3 haben wir bereits die zugehörige Diskriminante berechnet, nämlich$d_L = d(1, \sqrt{D}) = 4\sqrt{D}$ und für die andere Ganzheitsbasis erhalten wir

$$d_L = d\left(1, \frac{1}{2} + \frac{1}{2}\sqrt{D}\right) = \det \begin{pmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{D} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{D} \end{pmatrix}^2 = (-\sqrt{D})^2 = D.$$

Aus Beispiel II.2.3 und Bemerkung II.2.13 folgt insbesondere, dass die Menge $\{1 + \sqrt{D}, 1 - \sqrt{D}\}$ für $D \equiv 2, 3 \pmod 4$ keine Ganzheitsbasis von $\mathbb{Z}[\sqrt{D}]$ ist.

Proposition II.2.17 (Diskriminanten von Komposita): *Gegeben seien ein Körper K und Galoiserweiterungen $L|K$ und $L'|K$ vom Grad n beziehungsweise m, sodass $K = L \cap L'$. Ferner sei A ein Teilring von K, sodass $K = \mathrm{Quot}(A)$ gilt, und es bezeichne $B = \mathrm{Int}_L(A)$ sowie $B' = \mathrm{Int}_{L'}(A)$. Des Weiteren seien $\{w_1, \ldots, w_n\}$ respektive $\{w'_1, \ldots, w'_m\}$ Ganzheitsbasen der Körpererweiterungen $L|K$ respektive $L'|K$ bezüglich A mit Diskriminanten $d = d(w_1, \ldots, w_n)$ und $d' = d(w'_1, \ldots, w'_m)$. Sind d und d' koprim, d. h., gibt es x und x' in A, sodass $1 = xd + x'd'$, dann ist $\{w_i w'_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$ eine Ganzheitsbasis des Kompositum LL' über K bezüglich A und die Diskriminante dieser Erweiterung ist $d^m d'^n$.*

Beweis: Aus der Algebra ist bekannt, dass LL' in der Situation eine Galoiserweiterung von K ist, dass für den Grad $[LL' : K] = nm$ gilt, und dass $\{w_i w'_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$ eine K-Basis von LL' ist. Über die

Galoisgruppen $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$ und $\mathrm{Gal}(L'|K) = \{\sigma'_1, \ldots, \sigma'_m\}$ wissen wir, dass sich jedes σ_i eindeutig zu einem $\hat{\sigma}_i$ beziehungsweise jedes σ'_j eindeutig zu einem $\hat{\sigma}'_j$ in $\mathrm{Gal}(LL'|L')$ respektive $\mathrm{Gal}(LL'|L)$ fortsetzen lässt, und dass $\mathrm{Gal}(LL'|K) = \{\hat{\sigma}_i \circ \hat{\sigma}'_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$ ist. Seien $B' = \mathrm{Int}_{LL'}(A)$ und α ein Element von B'. Dann gibt es eindeutig bestimmte Elemente $\alpha_{i,j}$ in K, sodass

$$\alpha = \sum_{i,j} \alpha_{i,j} w_i w'_j = \sum_{j=1}^{m} \beta_j w'_j$$

mit $\beta_j = \sum_i \alpha_{i,j} w_i$. Für jedes $1 \leq i \leq m$ wissen wir, dass $\hat{\sigma}'_i(\alpha) = \sum_{j=1}^{m} \beta_j \hat{\sigma}'_i(w'_j)$, da $\hat{\sigma}'_j$ zur Galoisgruppe $\mathrm{Gal}(LL'|L)$ gehört. Das bedeutet, dass $b = (\beta_1, \ldots, \beta_m) \in L^m$ Lösung des Gleichungssystems $a = Tb$ mit $a = (\hat{\sigma}'_1(\alpha), \ldots, \hat{\sigma}'_m(\alpha))^t$ aus B'^m und $T = (\sigma'_i(w'_j))$ aus $B'^{m \times m}$ ist. Für die Matrix T haben wir $\det T^2 = d(w'_1, \ldots, w'_m) = d'$, sodass

$$d'b = \det T^2 \; b = \det(T) T^{\#} T b = (\det T) T^{\#} a$$

zu B' gehört. Deshalb ist jedes der $d'\beta_j$ ein Element von B' und da β_j in L lebt, liegt $d'\beta_j$ sogar in B. Aber $d'\beta_j = \sum_{i=1}^{n} d'\alpha_{i,j} w_i$, sodass die $d'\alpha_{i,j}$ in A liegen müssen, da $\{w_1, \ldots, w_n\}$ eine Ganzheitsbasis ist. Analog erhält man, dass alle $d\alpha_{i,j}$ in A liegen. Wegen der Teilerfremdheit von d und d' können wir schreiben $\alpha_{i,j} = (x'd' + xd)\alpha_{i,j}$, und die rechte Seite gehört nach dem oben Gezeigten zu A. Darum ist $\{w_i w_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$ eine Ganzheitsbasis von LL' über K.

Nun zur Bestimmung von $d(\{w_i, w'_j\})$. Seien $M = (\hat{\sigma}_k \hat{\sigma}'_\ell(w_i w'_j))_{((k,\ell),(i,j))}$, $Q = (\hat{\sigma}_k(w_i))$ und $Q' = (\hat{\sigma}'_\ell(w'_j))$. Dann ist

$$M = \begin{pmatrix} Q & & \\ & \ddots & \\ & & Q \end{pmatrix} \begin{pmatrix} I\hat{\sigma}'_1(w'_1) & \cdots & I\hat{\sigma}'_m(w'_1) \\ \vdots & \ddots & \vdots \\ I\hat{\sigma}'_i(w'_m) & \cdots & I\hat{\sigma}'_m(w'_m) \end{pmatrix} = CD.$$

Wir halten fest, dass $(\det Q)^2 = d$ und $(\det Q')^2)d'$. Damit erhalten wir $(\det C)^2 = (\det Q)^{2m}$ und $(\det D)^2 = (\det Q')^{2n}$, was die Behauptung liefert. □

3 Ideale

Seien K stets ein Zahlkörper vom Grad $n = [K : \mathbb{Q}]$ und $\mathcal{O}_K$ der zugehörige Ganzheitsring. Ferner seien $N = N_{K|\mathbb{Q}} \colon K \to \mathbb{Q}$ und $\mathrm{Tr} = \mathrm{Tr}_{K|\mathbb{Q}} \colon K \to \mathbb{Q}$ die zugehörige Norm beziehungsweise Spur.

Aus Proposition II.2.8 wissen wir, dass Elemente des Ganzheitsring $\mathcal{O}_K$ auch ganze Norm beziehungsweise Spur haben, und dass ein Element des Ganzheitsring genau dann eine Einheit ist, wenn die Norm eine Einheit im Ring $\mathbb{Z}$ ist.

Bemerkung II.3.1: Jedes von Null verschiedene Element α von $\mathcal{O}_K$ lässt sich als Produkt einer Einheit und irreduziblen Elementen von $\mathcal{O}_K$ schreiben.

Beweis: Sei α ein Element von $\mathcal{O}_K - \{0\}$. Ohne Einschränkung dürfen wir annehmen, dass α weder irreduzibel noch eine Einheit ist, denn dann sind wir bereits fertig. Es gibt also β und γ aus $\mathcal{O}_K - \mathcal{O}_K^\times$, sodass $\alpha = \beta\gamma$. Wegen $|N(\alpha)| = |N(\beta)||N(\gamma)|$ und da alle Normen ganzen Zahlen sind, liefert Proposition II.2.8 die Ungleichungskette

$$1 < |N(\beta)|, |N(\gamma)| < |N(\alpha)|.$$

Nun folgt die Behauptung per Induktion. □

Bemerkung II.3.2 (Uneindeutigkeit): Sei K der Zahlkörper $\mathbb{Q}(\sqrt{-5})$. Aus Beispiel II.2.16 kennen wir seinen Ganzheitsring, der ist nämlich $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In $\mathcal{O}_K$ haben wir die Gleichheit $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Unter Verwendung von Normargumenten, es ist ja in diesem Fall $N(a+b\sqrt{D}) = a^2 - Db^2 = a^2+5b^2$, sieht man ein, dass 2, 3, $1+\sqrt{-5}$ und $1-\sqrt{-5}$ irreduzibel sind. Aus der obigen Gleichung zu den Zerlegungen von 6 folgt allerdings auch, dass keines dieser irreduziblen Elemente prim ist. Deshalb sind die Hauptideale (2), (3), ... keine Primideale.

Erinnerung II.3.3 (Grundbegriffe zu Idealen): Sei R (wie immer) ein kommutativer Ring mit Eins und es sei I ein Ideal von R.

(i) Falls I ein echtes Ideal von R ist, und falls für alle a, b in R mit ab in I gilt, dass a oder b zu I gehört, dann heißt I ein *Primideal*. Genau dann ist I ein Primideal, wenn R/I ein Integritätsring ist.

(ii) Falls I ein echtes Ideal von R ist und falls für jedes Ideal J von R mit $I \subseteq J \subseteq R$ gilt, dass $I = J$ oder $J = R$, dann heißt I ein *maximales Ideal*. Genau dann ist I maximal, wenn R/I ein Körper ist. Insbesondere sind maximale Ideale Primideale.

(iii) Falls jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq \ldots$ von Idealen in R stationär wird, dann heißt R ein *noetherscher Ring*. Genau dann ist der Ring R noethersch, wenn jedes Ideal von R endlich erzeugt ist.

Proposition II.3.4 (Struktur der Ideale im Ganzheitsring):

(i) *Der Ganzheitsring $\mathcal{O}_K$ ist noethersch.*

(ii) *Ist $I \neq (0)$ ein Ideal von R, dann ist I als $\mathbb{Z}$-Modul isomorph zu $\mathbb{Z}^n$.*

Beweis: Sei I ein von (0) verschiedenes Ideal von $\mathcal{O}_K$. Nach Korollar II.2.12 ist $\mathcal{O}_K$ isomorph zu $\mathbb{Z}^n$.

Zu Aussage (ii): Als Ideal in $\mathcal{O}_K$ ist I insbesondere ein $\mathcal{O}_K$-Modul und so erst recht ein $\mathbb{Z}$-Untermodul von $\mathcal{O}_K$. Für ein Element x von I liegt $x\mathcal{O}_K$ ganz in I, was seinerseits in $\mathcal{O}_K$ enthalten ist, und der Ganzheitsring ist isomorph zu $\mathbb{Z}^n$. Da auch $x\mathcal{O}_K$ isomorph zu $\mathbb{Z}^n$ ist, ist I freier $\mathbb{Z}$-Modul vom Rang n.

Insbesondere folgt (i), da jedes Ideal nach dem oben Gezeigten endlich erzeugt ist. □

Beispiel II.3.5 (Gitter in den Gaußschen Zahlen): Für den Zahlkörper $\mathbb{Q}(\mathrm{i})$ ist der Ring der Gauß'schen Zahlen der zugehörige Ganzheitsring. Sei I das Ideal $(2+\mathrm{i})$. Dann haben wir

$$\begin{aligned} I &= \{(a+b\mathrm{i})(2+\mathrm{i}) \mid a,b \in \mathbb{Z}\} \\ &= \{2a-b+(a+2b)\mathrm{i} \mid a,b \in \mathbb{Z}\} = \mathbb{Z}(2+\mathrm{i}) \oplus \mathbb{Z}(-1+2\mathrm{i}) \cong \left\langle \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\rangle_{\mathbb{Z}}, \end{aligned}$$

wobei der Modul am Ende für das von den angegebenen Vektoren erzeugte Gitter in $\mathbb{R}^2$ stehen soll. Die Elemente von I bilden also ebenfalls ein Gitter in $\mathbb{Z}[\mathrm{i}]$.

Proposition II.3.6: *Sei $\mathfrak{p}$ ein nichttriviales Primideal in $\mathcal{O}_K$. Dann ist $\mathfrak{p}$ maximal.*

Beweis: Da $\mathfrak{p}$ per Voraussetzung nicht das Nullideal ist, liefert Proposition II.3.4, dass $\mathbb{Z}^n \cong \mathfrak{p} \subseteq \mathcal{O}_K \subseteq \mathbb{Z}^n$. Nach dem Elementarteilersatz ist $\mathcal{O}_K/\mathfrak{p}$ ein endlicher Integritätsring. Aber da endliche Integritätsringe Körper sind, ist $\mathfrak{p}$ ein maximales Ideal. □

Definition II.3.7 (Dedekindring): Sei R ein kommutativer Ring mit Eins. Ist R darüber hinaus ein noetherscher Integritätsbereich, der ganzabgeschlossen ist und in dem von Null verschiedene Primideale maximal sind, dann heißt R ein *Dedekindring*.

Insbesondere sind Ganzheitsringe algebraischer Zahlkörper Dedekindringe.

Satz 3 (Eindeutige Primfaktorzerlegung für Ideale): *Seien R ein Dedekindring und I ein von Null verschiedenes Ideal. Dann hat I eine bis auf Reihenfolge der Faktoren eindeutige Zerlegung $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Wir lassen $r = 0$ zu und decken so $I = R$ ab.*

Moralisch gesprochen gelingt uns die eindeutige Primfaktorzerlegung durch Hinzunahme „ideeller Zahlen“. Es sei allerdings vor folgender Fehleinschätzung gewarnt: Weder sind faktorielle Ringe Dedekindringe (beispielsweise Polynomringe in mehreren Veränderlichen), noch sind Dedekindringe faktorielle Ringe (beispielsweise $\mathbb{Z}[\sqrt{-5}]$).

Erinnerung II.3.8 (Grundrechenarten für Ideale): Seien R ein kommutativer unitärer Ring und I, J Ideale in R.

(i) Die Menge $I + J = \{a + b \mid a \in I, b \in J\}$ heißt *Summe von I und J*.

(ii) Die Menge $IJ = \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}_0, a_i \in I, b_i \in J\}$ heißt *Produkt von I und J*.

(iii) Falls $I + J = R$ ist, dann heißen die Ideale *koprim*. Das ist genau dann der fall, wenn es a in I und b in J gibt, sodass $a + b = 1$.

Wir halten fest, dass I und J in $I + J$ enthalten sind, wohingegen IJ sowohl in I als auch in J enthalten ist. Summen und Produkte von Idealen sind kommutativ und assoziativ; (0) ist neutrales Element für „+“, und R ist neutrales Element für „$\cdot$“. Die Menge der Ideale von R wird mit „+“ beziehungsweise „$\cdot$“ jeweils zu einem kommutativen Monoid.

Erinnerung II.3.9 (Koprime Ideale): Seien R ein kommutativer unitärer Ring und $I_1, \ldots, I_n$ koprime Ideale in R. Dann gilt:

(i) Schnitt und Produkt der Ideale stimmen überein, d. h. $\prod_{j=1}^{k} I_j = \bigcap_{j=1}^{k} I_j$.

(ii) Auch I_1 und $\prod_{j=2}^{k} I_j$ sind koprim.

(iii) Sind I und J koprime Ideale von R, dann gibt es ein x in R, sodass $x \equiv 1 \pmod{I}$ und $x \equiv 0 \pmod{J}$.

(iv) Für $I = I_1 \cap \cdots \cap I_k$ gilt dann $R/I \cong R/I_1 \oplus \cdots \oplus R/I_k$.

Lemma II.3.10 (Erste Etappe für Satz 3): *Seien R ein noetherscher Ring und I ein von Null verschiedenes Ideal von R. Dann gibt es nicht-triviale Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von R, sodass $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I$.*

Beweis: Wir verwenden das Lemma von Zorn. Sei

$$M = \{I \lhd R \mid I \neq (0) \text{ und es gibt keine Primideale wie beschrieben.}\}.$$

Angenommen, M wäre nicht leer. Wir betrachten M mit „$\subseteq$“ als Ordnungsrelation.

Da R ein noetherscher Ring ist, wird jede aufsteigende Kette stationär und hat deshalb eine obere Schranke. Nach dem Lemma von Zorn enthält M ein maximales Element I_0. Insbesondere kann I_0 also kein Primideal sein. Deshalb gibt es a und b aus R, sodass zwar ab zu I gehört, aber weder a noch b. Wir erhalten so echt größere Ideale $I_1 = I_0 + (a)$ und $I_2 = I_0 + (b)$, die beide nicht zu M gehören können; I_0 war ja maximal. Entsprechend gibt es nichttriviale Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ in R, sodass $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I_1$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subseteq I_2$. Nach der vorangegangenen Erinnerung haben wir

$$I_0 \supseteq I_1 I_2 = (I_0 + (a))(I_0 + (b)) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

im Widerspruch zur Behauptung. Die Annahme war also falsch und M muss leer sein. □

Proposition II.3.11: *Seien R ein Dedekindring, $\mathfrak{p}$ ein von Null verschiedenes Primideal, und*

$$\mathfrak{p}^{-1} = \{x \in K = \mathrm{Quot}(R) \mid x\mathfrak{p} \subseteq R\}.$$

Dann gilt:

(i) *Der Ring R ist eine echte Teilmenge von $\mathfrak{p}^{-1}$.*

(ii) *Für jedes von Null verschiedene Ideal I von R ist $I \neq I\mathfrak{p}^{-1}$.*

(iii) *$\mathfrak{p}^{-1}\mathfrak{p} = R$, d. h. $\mathfrak{p}$ ist invertierbar.*

Später definieren wir gebrochene Ideale und sehen dann, dass $\mathfrak{p}^{-1}$ ein gebrochenes Ideal ist.

Beweis: (i) Aus der Definition von $\mathfrak{p}^{-1}$ folgt, dass R in $\mathfrak{p}^{-1}$ enthalten ist. Bleibt zu zeigen, dass $R \neq \mathfrak{p}^{-1}$ ist. Wir wählen dazu $a \in \mathfrak{p} - \{0\}$. Zu diesem a wollen wir ein b in R konstruieren, sodass zwar b/a in $\mathfrak{p}^{-1}$ liegt, aber nicht zu R gehört.

Nach Lemma II.3.10 gibt es von Null verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ in R, sodass $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq (a) \subseteq \mathfrak{p}$. Wir wählen k minimal.

Als Erstes zeigen wir, dass es $1 \leq j \leq k$ gibt, sodass $\mathfrak{p}_j = \mathfrak{p}$. Angenommen, keines der $\mathfrak{p}_i$ wäre gleich $\mathfrak{p}$, d. h. $\mathfrak{p}_i \not\subseteq \mathfrak{p}$ für $1 \leq i \leq k$, weil von Null verschiedene Primideale in Dedekindringen maximal sind. Für jedes $1 \leq i \leq k$ gibt es also ein

b_i in $\mathfrak{p}_i$, sodass b_i nicht zu $\mathfrak{p}$ gehört. Dann wäre $b = b_1 \cdots b_k \in \mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{p}$, was bedeuten müsste, dass eines der b_i zu $\mathfrak{p}$ gehört. Das steht aber im Widerspruch zur Annahme. Wir dürfen deshalb ohne Einschränkung annehmen, dass $\mathfrak{p}_1 = \mathfrak{p}$ gilt.

Als Zweites konstruieren wir das gewünschte b. Weil k minimal gewählt war, ist $\mathfrak{p}_2 \cdots \mathfrak{p}_k \not\subseteq (a)$, sodass es ein b in $\mathfrak{p}_2 \ \cdots \mathfrak{p}_k$ gibt, das nicht zu (a) gehört. Damit ist b/a kein Element von R, aber $b\mathfrak{p} \subseteq \mathfrak{p}_2 \ \cdots \mathfrak{p}_k\mathfrak{p}_1 \subseteq (a)$, weshalb $b/a\mathfrak{p}$ in R enthalten ist, und so ist b/a ein Element von $\mathfrak{p}^{-1}$.

(ii) Sei I ein nicht-triviales Ideal von R. Angenommen, $I\mathfrak{p}^{-1}$ wäre gleich I. Wir wählen x in $\mathfrak{p}^{-1} - R$ (was nach (i) nichtleer ist), und ein Erzeugendensystem $\{a_1, \ldots, a_n\}$ von I. Für jedes $1 \leq i \leq k$ ist xa_i von der Form $\sum_{j=1}^{k} \alpha_{i,j} a_j$ mit geeigneten $\alpha_{i,j}$ aus R. Die Matrix $A = (\alpha_{i,j})$ gehört zu $R^{k\times k}$ und $B = xI - A$ gehört zu $K^{k\times k}$. Per Konstruktion ist $B(a_1, \ldots, a_n)^t = 0$, sodass $\det B = 0$ sein muss.

Da das charakteristische Polynom von A, $f = \chi_A = \det(XI_k - A)$, in $R[X]$ liegt, normiert ist, und x zur Nullstelle hat, muss x ganz über R sein. Weil R ein Dedekindring ist, ist R ganzabgeschlossen, und so muss x zu R gehören. Das widerspricht der Wahl von x, sodass „$I = I\mathfrak{p}^{-1}$“ in der beschriebenen Situation nicht eintreten kann.

(iii) Die Inklusion „$\subseteq$“ gilt per Definition von $\mathfrak{p}^{-1}$. Zur Inklusion „$\supseteq$“: Natürlich ist $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$. Weil R ein Dedekindring ist, ist $\mathfrak{p}$ maximal. Außerdem sieht man anhand der Definition, dass $\mathfrak{p}\mathfrak{p}^{-1}$ ein Ideal von R ist. Aus (ii) erhalten wir direkt, dass $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$, sodass $\mathfrak{p}\mathfrak{p}^{-1} = R$ sein muss. □

Beweis (von Satz 3): Zur Existenz der Zerlegung: Sei

$$M = \{I \lhd R \mid (0) \neq I \subsetneq R, I \text{ ist kein Produkt von Primidealen}\}.$$

Wir nehmen an, dass M nicht die leere Menge ist. Wie in Lemma II.3.10 erhalten wir dann ein maximales Element I_0 in M. Wir wählen ein maximales Ideal $\mathfrak{p}$, das I_0 enthält. Da I_0 zu M gehört, muss $I_0 \neq \mathfrak{p}$ gelten. Aus Proposition II.3.11 folgt, dass I_0 echt in $I_0\mathfrak{p}^{-1}$ enthalten ist, und dass $I_0\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$ gilt.

Weil I_0 von $\mathfrak{p}$ verschieden ist, folgt, dass $I_0\mathfrak{p}^{-1}$ nicht R sein kann. Denn sonst wäre $I_0 = I_0R = I_0\mathfrak{p}\mathfrak{p}^{-1} = R\mathfrak{p} = \mathfrak{p}$. Insgesamt haben wir also, dass $I_0\mathfrak{p}^{-1}$ ein echtes Ideal von R ist, das I_0 echt enthält. Weil I_0 per Voraussetzung maximal in M ist, liegt $I_0\mathfrak{p}^{-1}$ nicht in M, weshalb es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von R gibt, sodass $I_0\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. Aber dann ist $I_0 = I_0\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_k\mathfrak{p}$ im Widerspruch zu den Eigenschaften der Elemente von M. Die Menge M muss also leer sein und die Behauptung folgt.

Für die Eindeutigkeit der Zerlegung verwenden wir, dass $\mathfrak{p}$ ein Primideal ist genau dann, wenn für alle Ideale I und J mit $IJ \subseteq \mathfrak{p}$ gilt, dass $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$.

Sei also I ein von Null verschiedenes Ideal von R mit Zerlegungen $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ für Primideale $\mathfrak{p}_i, \mathfrak{q}_j$ von R. Insbesondere ist $\mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ enthalten in $\mathfrak{p}_1$. Ohne Einschränkung dürfen wir annehmen, dass $\mathfrak{q}_1$ in $\mathfrak{p}_1$ enthalten ist, und dann folgt $\mathfrak{p}_1 = \mathfrak{q}_1$, da R ein Dedekindring ist. Wir haben deshalb

$$\mathfrak{p}_2 \cdots \mathfrak{p}_k = \mathfrak{p}_1^{-1}\mathfrak{p}_1\mathfrak{p}_2 \ \cdots \mathfrak{p}_k = \mathfrak{q}_1^{-1}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_\ell.$$

Per Induktion folgt nun die Behauptung. □

Wir haben uns bereits überlegt, dass die Menge der Ideale eines Integritätsbereichs mit „$\cdot$“ einen kommutativen Monoid mit neutralem Element R bilden. Durch Hinzunahme von gebrochenen Idealen möchten wir für passende Ringe aus diesem Monoid eine Gruppe machen. Die Eigenschaft, noethersch zu sein, wird dafür entscheidend benötigt werden.

Definition II.3.12 (Gebrochene Ideale): Seien R ein noetherscher Integritätsbereich und $K = \mathrm{Quot}(R)$ der zugehörige Quotientenkörper. Ein von Null verschiedener endlich erzeugter R-Untermodul J von K heißt *gebrochenes Ideal zu R.*

Beispiel II.3.13 (Erste gebrochene Ideale): (i) Gewöhnliche von Null verschiedene Ideale von R sind bereits gebrochene Ideale zu R.

(ii) Sei R der Ring der ganzen Zahlen. Dann ist $\mathbb{Z}\frac{2}{3} \subseteq \mathbb{Q}$ ein gebrochenes Ideal zu $\mathbb{Z}$. Achtung, $\mathbb{Z}\frac{2}{3}$ ist nicht dasselbe Ideal wie $\mathbb{Z}\frac{1}{3}$. Als anderes Beispiel betrachten wir $\mathbb{Z}\frac{2}{3} + \mathbb{Z}\frac{4}{5}$. Dafür haben wir

$$\mathbb{Z}\frac{2}{3} + \mathbb{Z}\frac{4}{5} = \mathbb{Z}\frac{10}{15} + \mathbb{Z}\frac{12}{15} = \mathbb{Z}\frac{2}{15},$$

weil $\mathrm{ggT}(10, 12) = 2$ ist.

Proposition II.3.14 (Äquivalente Beschreibung gebrochener Ideale): *Seien R ein noetherscher Integritätsring und $K = \mathrm{Quot}(R)$ der zugehörige Quotientenkörper. Ein R-Untermodul J von K ist genau dann ein gebrochenes Ideal zu R, wenn es ein d in $R - \{0\}$ gibt, sodass dJ in R enthalten ist.*

Beweis: „$\Longrightarrow$“: Da J endlich erzeugt ist, gibt es endlich viele Elemente $x_1, \ldots, x_k$ in K, sodass $J = Rx_1 + \cdots + Rx_k$. Wir schreiben $x_i = a_i/b_i$ mit geeigneten a_i und b_i aus R, $b_i \neq 0$. Dann leistet $d = \prod_{i=1}^n b_i$ das Gewünschte.

„$\Longleftarrow$“: Sei d ein von Null verschiedenes Element von R, sodass dJ in R enthalten ist. Da J ein R-Modul ist, ist dJ ein Ideal in R. Weil R ein noetherscher Ring ist, gibt es $a_1, \ldots, a_k$ in R mit $dJ = Ra_1 + \cdots + Ra_k$. Das bedeutet, dass $J = R\frac{a_1}{d} + \cdots + R\frac{a_k}{d}$ endlich erzeugt, und damit ein gebrochenes Ideal ist. □

Definition II.3.15 (Monoid der gebrochenen Ideale): Seien R ein noetherscher Integritätsbereich und $K = \mathrm{Quot}(R)$ der zugehörige Quotientenkörper. Für zwei gebrochene Ideale J_1, J_2 zu R heißt

$$J_1 J_2 = \left\{ \sum_{i=1}^{k} a_i b_i : k \in \mathbb{N}, a_1, \ldots, a_k \in J_1, b_1, \ldots, b_k \in J_2 \right\}$$

das *Produkt von* J_1 *und* J_2. Auch $J_1 J_2$ ist ein gebrochenes Ideal. Ist J ein gebrochenes Ideal zu R, dann ist $JR = J$.

Es bezeichne $I(R) = \{J \subseteq K$ gebrochenes Ideal zu $R\}$. Dann ist $I(R)$ mit der Multiplikation gebrochener Ideale ein kommutatives Monoid, d. h. das Produkt gebrochener Ideale ist kommutativ, assoziativ, und es gibt ein neutrales Element.

Definition II.3.16 (Invertierbarkeit gebrochener Ideale): Seien R ein noetherscher Integritätsbereich und $K = \mathrm{Quot}(R)$ der Quotientenkörper. Ist J_1 ein gebrochenes Ideal zu R und gibt es ein gebrochenes Ideal J_2 zu R, sodass $J_1 J_2 = R$, dann heißt J_1 *invertierbar*.

Für ein gebrochenes Ideal J schreiben wir $J^{-1} = \{x \in K \mid xJ \subseteq R\}$. Dieses ist wieder ein gebrochenes Ideal und JJ^{-1} ist in R enthalten.

Sind J_1 und J_2 gebrochene Ideale, sodass $J_1 J_2 = R$, dann ist $J_2 = J_1^{-1}$.

Ist J ein gebrochenes Ideal zu R, dann gibt es Ideale I_1 und I_2 von R, sodass $I_2 J = I_1$ gilt.

Beweis: Zum zweiten Teil der Definition: Es ist zum Ersten klar, dass J^{-1} ein R-Modul ist. Zum Zweiten gilt für a aus $J - \{0\}$, dass aJ^{-1} in R enthalten ist. Aber das heißt genau, dass J^{-1} ein gebrochenes Ideal ist.

Zum dritten Teil der Definition: „$\subseteq$“: Sei x ein Element von J_2. Dann ist xJ_1 enthalten in $J_2 J_1 = J_1 J_2 = R$, sodass x zu J_1^{-1} gehört.

„$\supseteq$“: Ist x ein Element von J_1^{-1}, dann liegt xJ_1 in R, d. h. $xJ_1 J_2$ ist in $RJ_2 = J_2$ enthalten. Insbesondere ist $x = x1$ in J_2 enthalten und wir sind fertig.

Zum vierten Teil der Definition: Setzen wir $I_2 = \{x \in R \mid xJ \subseteq R\}$ und $I_1 = I_2 J$, dann ist I_1 ein gebrochenes Ideal, das in R enthalten ist, also ein echtes Ideal von R. □

Beispiel II.3.17: (i) Seien k ein Körper und $k[X,Y]$ der Polynomring über k in zwei Veränderlichen. Wir betrachten das Ideal $J = (X,Y)$. Dann ist

$$J^{-1} = \left\{ \frac{f}{g} \in k(X,Y) : \frac{f}{g} J \subseteq k[X,Y] \right\} = k[X,Y].$$

(ii) Aus Proposition II.3.11 wissen wir über Primideale $\mathfrak{p}$ eines Dedekindrings, dass $\mathfrak{p}^{-1}\mathfrak{p} = R$ gilt.

Satz 4 (Gruppe der gebrochenen Ideale): *Sei R ein Dedekindring. Dann wird die Menge der gebrochenen Ideale $I(R)$ von R zusammen mit der Multiplikation gebrochener Ideale zu einer freien abelschen Gruppe, die von den nicht-trivialen Primideale in R frei erzeugt wird. Insbesondere gilt: Jedes gebrochene Ideal J in $I(R)$ lässt sich eindeutig schreiben als*

$$J = \prod_{(0) \neq \mathfrak{p} \lhd R \text{ } prim} \mathfrak{p}^{\nu_\mathfrak{p}}$$

für geeignete Exponenten $\nu_\mathfrak{p}$ aus $\mathbb{Z}$, wobei $\nu_\mathfrak{p}$ für fast alle $\mathfrak{p}$ Null ist. Hierbei steht $\mathfrak{p}^k$ für $\prod_{i=1}^{k} \mathfrak{p}$ für natürliche k, $\mathfrak{p}^0 = R$ und $\mathfrak{p}^{-k} = (\mathfrak{p}^{-1})^k$ für negative ganze Zahlen k.

Beweis: Wir zeigen zunächst, dass jedes gebrochene Ideal J invertierbar ist. Ist J ein Primideal $\mathfrak{p} \neq 0$, dann folgt die Behauptung aus Proposition II.3.11.

Ist J ein Ideal in R, dann liefert Satz 3 eine Zerlegung $J = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in nicht-triviale Primideale von R. Das Ideal $\mathfrak{p}_r^{-1} \cdots \mathfrak{p}_1^{-1}$ gilt das Gewünschte.

Sei nun J irgendein gebrochenes Ideal zu R. Dann gibt es ein Element d von R, sodass $I_1 = dJ$ ein Ideal von R ist. Das bedeutet, dass wir die folgende Gleichungskette haben: $J(dI_1^{-1}) = (\frac{1}{d} I_1)(dI_1^{-1}) = \frac{1}{d} dI_1 I_1^{-1} = R$. Das Ideal dI_1^{-1} ist ein gebrochenes Ideal und also invers.

Bleibt zu zeigen, dass $I(R)$ frei von den nicht-trivialen Primidealen von R erzeugt wird. Nach Definition II.3.15 gibt es Ideale I_1 und I_2 von R, sodass $J = I_2^{-1} I_1 = I_1 / I_2$. Aus Satz 3 erhalten wir die gewünschte Beschreibung als Produkt in der Aussage des Satzes. Die Eindeutigkeitsaussage in Satz 3 liefert uns auch in dieser Situation die Eindeutigkeit. □

Bemerkung II.3.18: Seien R ein Dedekindring, $K = \mathrm{Quot}(R)$ der Quotientenkörper und $\mathcal{H} = \{(a) = Ra \mid a \in K^\times\}$ die *Menge der gebrochenen Hauptideale.* Dann ist $\mathcal{H}$ ein Normalteiler in $I(R)$ und wir erhalten folgende exakte Sequenz von Gruppen:

$$1 \longrightarrow R^\times \xhookrightarrow{f_1} K^\times \xrightarrow{f_2} I(R) \xrightarrow{f_3} I(R)/\mathcal{H} \longrightarrow 1$$

mit den Abbildungen $f_1\colon R^\times \to K^\times$, $x \mapsto x$, $f_3\colon K^\times \to I(R)$, $x \mapsto Rx$ und $f_3\colon I(R) \to I(R)/\mathcal{H}$, $x \mapsto [x]$.

Beweis: Seien a und b von Null verschiedene Elemente von K und J ein gebrochenes Ideal zu R. Dann gilt $(Ra)(Rb) = (Rab)$ und $(Ra)^{-1} = Ra^{-1}$, und $J(Ra)J^{-1} = JRJ^{-1}a = JJ^{-1}a = Ra$.

Die angegebene Sequenz ist exakt, weil $R = Ra$ genau dann gilt, wenn a eine Einheit in R ist. □

Definition II.3.19 (Idealklassengruppe): Sei K ein algebraischer Zahlkörper mit Ganzheitsring $\mathcal{O}_K$. Mit den Bezeichnungen von oben heißt $\mathrm{C}\ell_K = I(\mathcal{O}_K)/\mathcal{H}$ die *Idealklassengruppe zu* K.

Beispiel II.3.20: (i) Ist $K = \mathbb{Q}$, dann ist $\mathrm{C}\ell_{\mathbb{Q}} = \{0\}$.

(ii) Allgemeiner gilt: Genau dann ist $\mathrm{C}\ell_K = \{0\}$, wenn der Ganzheitsring $\mathcal{O}_K$ ein Hauptidealring ist.

Insbesondere messen $\mathrm{C}\ell_K$ und $\mathcal{O}_K$ den „Fehler“, den wir machen, wenn wir von Zahlen zu „ideellen Zahlen“ übergehen. $\mathrm{C}\ell_K$ misst „Expansion“, und $\mathcal{O}_K$ die „Kontraktion“.

Bemerkung II.3.21: Sei R ein Dedekindring. Genau dann ist R faktoriell, wenn R ein Hauptidealring ist.

Beweis: „$\Longleftarrow$“ ist klar – wir wissen schon lange, dass Hauptidealringe faktoriell sind.

„$\Longrightarrow$“: Wegen Satz 3 genügt es zu zeigen, dass jedes Primideal ein Hauptideal ist. Sei also $\mathfrak{p}$ ein nicht-triviales Primideal von R und a ein von Null verschiedenes Element von $\mathfrak{p}$. Dann gibt es eine Zerlegung von a in von Null verschiedene Primelemente $a = x_1 \cdots x_r$, da R per Voraussetzung faktoriell ist. Wir haben also $(a) = (x_1) \cdots (x_r) \subseteq \mathfrak{p}$ und es gibt $1 \leq i \leq r$, sodass $(x_i) \subseteq \mathfrak{p}$. Da beide Ideale nicht-triviale Primideale und damit maximal sind, muss $\mathfrak{p} = (x_i)$ gelten.□

Wir wollen im Folgenden zeigen, dass die Klassengruppe eines algebraischen Zahlkörpers endlich ist. Dazu betrachten wir Minkowski'sche Gittertheorie.

4 Gitter

Wir haben bereits gesehen, dass $\mathbb{Z}[\mathrm{i}]$, der Ganzheitsring des algebraischen Zahlkörpers $\mathbb{Q}[\mathrm{i}]$, als Gitter im $\mathbb{R}^2$ aufgefasst werden kann. Diesen Ansatz möchten wir auf allgemeine Ganzheitsringe ausweiten.

Definition II.4.1: Sei V ein endlichdimensionaler reeller Vektorraum der Dimension n.

(i) Sei Γ eine Untergruppe von $(V,+)$. Gibt es eine $\mathbb{R}$-linear unabhängige Menge $\{v_1,\ldots,v_m\}$ von V, sodass $\Gamma = \mathrm{Lin}_{\mathbb{Z}}(v_1,\ldots,v_m) = \bigoplus_{i=1}^m \mathbb{Z}v_i$, dann heißt Γ ein *Gitter in* V. In diesem Fall heißt $(v_1,\ldots,v_n)$ eine *Gitterbasis von* Γ und die Menge

$$F = \Big\{ \sum_{i=1}^m x_i v_i : x_i \in [0,1) \Big\}$$

heißt *Fundamentalmasche von* Γ *bezüglich der Gitterbasis* $(v_1,\ldots,v_m)$.

(ii) Sei Γ ein Gitter in V. Ist eine Gitterbasis von Γ ebenfalls eine Basis von V, dann heißt Γ *vollständig*.

Häufig wird von einem „Gitter“ bereits verlangt, vollständig zu sein.

Bemerkung II.4.2: (i) Gitter sind endlich erzeugte Untergruppen von V und damit isomorph zu $\mathbb{Z}^m$. Die Umkehrung gilt allerdings nicht. Zwar ist $\Gamma = \mathrm{Lin}_{\mathbb{Z}}((1,0)^t,(\sqrt{2},0)^t)$ isomorph zu $\mathbb{Z}^2$, aber $((1,0)^t,(\sqrt{2},0)^t)$ ist nicht $\mathbb{R}$-linear unabhängig und damit keine Gitterbasis.

(ii) Sei Γ in der Situation von Definition II.4.1 ein vollständiges Gitter in V. Dann gilt $V = \bigcup_{\gamma\in\Gamma} F + \gamma$.

Seien X ein topologischer Raum und M eine Teilmenge von X. Gibt es für jedes m in M eine offene Menge U in X, sodass $U \cap M = \{m\}$ gilt, dann heißt M *diskret in* X. Das ist äquivalent dazu, dass die Spurtopologie auf M die diskrete Topologie ist, d. h. die Potenzmenge von M, weil ja alle Einpunktmengen in M offen sind.

Wir statten den $\mathbb{R}^n$ im Folgenden mit der Standardtopologie aus, die beispielsweise vom euklidischen Skalarprodukt induziert wird.

Bemerkung II.4.3: Sei $\Gamma = \bigoplus_{i=1}^m \mathbb{Z}v_i$ ein Gitter im $\mathbb{R}^n$ mit Gitterbasis $(v_1,\ldots,v_m)$. Dann ist Γ eine diskrete Teilmenge.

Beweis: Sei γ ein Element des Gitters, d. h. $\gamma = \sum_{i=1}^m a_i v_i$ mit geeigneten ganzzahligen Koeffizienten $a_1,\ldots,a_m$. Die Menge

$$U = \{\sum_{i=1}^m x_i v_i \mid x_i \in \mathbb{R}, |a_i - x_i| < 1\}$$

ist eine offene Teilmenge des $\mathbb{R}^n$ und es gilt $U \cap \Gamma = \{\gamma\}$. □

Proposition II.4.4: *Sei Γ eine additive Untergruppe des $\mathbb{R}^n$. Genau dann ist Γ ein Gitter, wenn Γ diskret ist.*

Für den Beweis dieser Aussage schieben wir das folgende Hilfslemma ein:

Lemma II.4.5 (Differenzumgebung): *Sei U eine Umgebung von Null in $\mathbb{R}^n$. Dann gibt es eine offene Umgebung U' von Null, die in U enthalten ist, sodass gilt: Für Punkte x und y in U' ist $x - y$ in U enthalten.*

Beweis: Ohne Einschränkung dürfen wir annehmen, dass U von der Form $B(0, r)$ ist. Die offene Teilmenge $U' = B(0, r/2)$ leistet dann das Gewünschte.□

Beweis (von Proposition II.4.4): „$\Longrightarrow$“ haben wir bereits in Bemerkung II.4.3 gezeigt.

„$\Longleftarrow$“: Sei Γ eine diskrete additive Untergruppe des $\mathbb{R}^n$. Wir gehen in Schritten vor.

Als Erstes zeigen wir, dass Γ abgeschlossen ist. Angenommen, Γ wäre nicht abgeschlossen. Dann gäbe es ein x in $\mathrm{cl}(\Gamma) - \Gamma$. Sei nun U eine Umgebung der Null in $\mathbb{R}^n$. Nach Lemma II.4.5 finden wir eine offene Nullumgebung U' in U, sodass für y_1 und y_2 in U' die Differenz $y_1 - y_2$ in U liegen.

Weil x in $\mathrm{cl}(\Gamma) - \Gamma$ liegt, gibt es verschiedene Elemente γ_1, γ_2 von Γ in $x + U'$. Es sind deshalb auch $\gamma_i - x$ paarweise verschieden und in U' enthalten. Nach Voraussetzung liegt ihre Differenz $\gamma_1 - \gamma_2$, die von Null verschieden und in Γ enthalten ist, in U. Darum ist Null ein Häufungspunkt von Γ, aber das widerspricht unserer Annahme an Γ.

Sei nun $V_0 = \mathrm{Lin}_{\mathbb{R}}(\Gamma)$ der von Γ erzeugte, m-dimensionale Untervektorraum von V. Für diesen Vektorraum finden wir eine Basis $(u_1, \ldots, u_m)$ als $\mathbb{R}$-Vektorraum, sodass $u_1, \ldots, u_m$ zu Γ gehören, und wir definieren ein neues Gitter $\Gamma_0 = \bigoplus_{i=1}^{m} \mathbb{Z}u_i \subseteq \Gamma$.

Als Zweites zeigen wir, dass $[\Gamma : \Gamma_0]$ endlich ist. Es bezeichne $\mathcal{R}$ ein Nebenklassenvertretersystem von Γ_0 in Γ. Dieses Nebenklassenvertretersystem können wir schreiben als $\mathcal{R} = \{\gamma_i \mid i \in I\}$ für eine geeignete Indexmenge I. Per Konstruktion ist Γ_0 ein vollständiges Gitter im Vektorraum V_0, d. h. $V = \bigcup_{\gamma \in \Gamma_0} F_0 + \gamma$, wobei F_0 die Fundamentalmasche von Γ_0 bezeichnet.

Ohne Einschränkung dürfen wir annehmen, dass γ_i in F_0 liegt, denn γ_i liegt in Γ, was natürlich in $\mathrm{Lin}_{\mathbb{R}}(\Gamma) = V$ enthalten ist. Es gibt also ein γ_i' aus F_0 und γ_i'', sodass $\gamma_i = \gamma_i' + \gamma_i''$. Da wir uns nur für die Nebenklasse interessieren, dürfen wir γ_i durch γ_i' ersetzen.

Weil aber F beschränkt und Γ diskret ist, kann $\{\gamma_i \mid i \in I\}$ nicht unendlich sein und die Behauptung folgt.

Als Drittes zeigen wir, dass es eine $\mathbb{R}$-linear unabhängige Menge $\{v_1, \ldots, v_m\}$ von $\mathbb{R}^n$ gibt, sodass $\Gamma = \bigoplus_{i=1}^m \mathbb{Z}v_i$ ist.

Sei q der Index von Γ_0 in Γ. Dann ist $q\Gamma_0$ in Γ enthalten, denn für jedes $\overline{a}$ in Γ/Γ_0 ist $\mathrm{ord}(\overline{a})$ ein Teiler von q, sodass für jedes a in Γ gilt, dass qa zu Γ_0 gehört. Wir haben deshalb

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) \oplus \cdots \oplus \mathbb{Z}\left(\frac{1}{q}u_m\right) \subseteq V_0.$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es eine Basis $v_1', \ldots, v_n'$ von $1/q\Gamma_0$ und natürliche Zahlen $\alpha_1, \ldots, \alpha_r$, $r \leq m$, sodass $\Gamma = \bigoplus_{i=1}^r \mathbb{Z}\alpha_i v_i'$. Da $\mathrm{Lin}_{\mathbb{R}}(\Gamma) = V_0$ ist, muss bereits $r = m$ gelten. Insbesondere ist Γ ein Gitter. □

Proposition II.4.6 (Vollständige Gitter): *Sei Γ ein Gitter im $\mathbb{R}^n$. Genau dann ist Γ vollständig, wenn es eine beschränkte Teilmenge M von V gibt, sodass $\bigcup_{\gamma\in\Gamma} \gamma + M = \mathbb{R}^n$ ist.*

Beweis: Wir können Γ schreiben als $\Gamma = \bigoplus_{i=1}^m \mathbb{Z}v_i$ mit geeigneten $v_1, \ldots, v_m$, sodass $(v_1, \ldots, v_m)$ linear unanhängig ist.

„$\Longrightarrow$“: Ist $m = n = \dim \mathbb{R}^n$, dann leistet die Fundamentalmasche das Gewünschte.

„$\Longleftarrow$“: Sei $V_0 = \mathrm{Lin}_{\mathbb{R}}(\Gamma)$. Wir wollen zeigen, dass $V = V_0$. Sei dazu v ein Element von V. Wir betrachten die Vielfachen $v_n = nv$ für n aus den natürlichen Zahlen. Per Voraussetzung ist jedes $v_n = nv$ von der Form $\gamma_n + w_n$ für geeignete γ_n aus Γ und w_n aus M. Damit ist $v = (1/n)v_n = (1/n)\gamma_n + (1/n)w_n$. Da M beschränkt ist, geht die Folge $((1/n)w_n)_{n\in\mathbb{N}}$ gegen Null, d. h. $(1/n)\gamma_n$ konvergiert gegen v. Weil V_0 abgeschlossen ist, muss dann auch v zu V_0 gehören. □

Ab jetzt statten wir unseren n-dimensionalen $\mathbb{R}$-Vektorraum V mit einem Skalarprodukt $\langle\cdot,\cdot\rangle$ aus. Auf dem $\mathbb{R}^n$ ist das Lebesgue-Maß das eindeutige Maß auf der Borelschen σ-Algebra, sodass für eine Orthogonalbasis $\{v_1, \ldots, v_n\}$ gilt: Für $H(v_1, \ldots, v_n) = H = \{\sum_{i=1}^n x_i v_i \mid x_i \in [0,1]\}$ ist $\mathrm{vol}(H) = \|v_1\| \cdots \|v_n\|$.

Wir erhalten so auf V ein eindeutiges Maß μ, sodass für jede Orthogonalbasis $(w_1, \ldots, w_n)$ und $H(w_1, \ldots, w_n) = \mu(H) = \|v_1\| \cdots \|w_n\|$. Im Folgenden schreiben wir $\mathrm{vol}(A) = \mu(A)$ für das Volumen einer messbaren Menge A.

Wir halten fest, dass μ translationsinvariant ist, d. h. für jede messbare Menge A in V und jedes x in V gilt $\mathrm{vol}(x + A) = \mathrm{vol}(A)$.

Sind ferner $v_1, \ldots, v_n$ linear unabhängig in V, dann gilt für $H(v_1, \ldots, v_n)$, dass $\mathrm{vol}(H) = \det A$ für die Basiswechselmatrix $A = D_{E,B}(\mathrm{id})$ von $B = \{v_1, \ldots, v_n\}$ zu einer Orthonormalbasis E. Wir erinnern daran, dass für die Matrix A gilt: $A^t A = (\langle v_i, v_j\rangle)_{i,j}$.

Satz 5 (Minkowskischer Gitterpunktsatz): *Seien Γ ein vollständiges Gitter im euklidischen Vektorraum V mit Skalarprodukt $\langle \cdot, \cdot \rangle$ und X eine zentralsymmetrische konvexe Teilmenge von V. Ist* $\mathrm{vol}(X) > 2^{\dim V} \mathrm{vol}(\Gamma)$*, dann enthält X ein von Null verschiedenes Element γ von Γ. Hierbei ist* $\mathrm{vol}(\Gamma) = \mathrm{vol}(F)$ *das Volumen der Fundamentalmasche von Γ.*

Bemerkung II.4.7: Sei Γ ein Gitter in V. Dann ist $\mathrm{vol}(\Gamma)$ unabhängig von der gewählten Gitterbasis $v_1, \ldots, v_n$ von Γ, denn Basiswechsel in $\mathbb{Z}^n$ haben Determinante ± 1.

Beweis: Statt X betrachten wir die Menge $(1/2)X = \{(1/2)x \in V \mid x \in X\}$. Dann haben wir $\mathrm{vol}((1/2)X) = 2^{-n} \mathrm{vol}(X)$.

Angenommen, kein von Null verschiedenes γ aus Γ läge in X.

Als Erstes können wir dann für alle verschiedenen γ_1, γ_2 in Γ folgern, dass $(\gamma_1 + (1/2)X) \cap (\gamma_2 + (1/2)X) = \varnothing$. Es gäbe sonst ja x_1, x_2 aus X und verschiedene γ_1, γ_2 aus Γ, sodass $\gamma_1 + x_1/2 = \gamma_2 + x_2/2$, d. h. $0 \neq \gamma_1 - \gamma_2 = 1/2(x_2 - x_1)$ läge in X, da X zentralsymmetrisch und konvex ist.

Als Zweites sei F die Fundamentalmasche von Γ. Dann erhalten wir

$$\begin{aligned} \mathrm{vol}(\Gamma) = \mathrm{vol}(F) &\geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(F \cap \left(\frac{1}{2}X + \gamma\right)\right) \\ &= \sum_{\gamma \in \Gamma} \mathrm{vol}\left((F - \gamma) \cap \left(\frac{1}{2}X\right)\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n} \mathrm{vol}(X). \ \square \end{aligned}$$

5 Minkowski-Theorie

In diesem Abschnitt wollen wir untersuchen, wie man den Ganzheitsring $\mathcal{O}_K$ eines algebraischen Zahlkörpers als Gitter in einem geeigneten euklidischen Vektorraum $(V, \langle \cdot, \cdot \rangle)$ auffassen können. Einen solchen euklidischen Vektorraum wollen wir konstruktiv bestimmen. In dieser Situation werden Ideale $\mathfrak{a}$ des Ganzheitsrings $\mathcal{O}_K$ zu Teilgittern.

Es wird sich als zielführend herausstellen, Elemente a von Idealen zu bestimmen, deren Norm möglichst klein ist.

Mithilfe dieser Methoden wird es uns später gelingen zu zeigen, dass die Idealklassengruppe eines algebraischen Zahlkörpers endlich ist.

Im Folgenden seien stets K ein algebraischer Zahlkörper vom Grad n über $\mathbb{Q}$, $\mathcal{O}_K$ der zugehörige Ganzheitsring und $\mathcal{H} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\}$.

Definition II.5.1: Wir schreiben $K_{\mathbb{C}} = \prod_{tau \in \mathcal{H}} \mathbb{C} = \mathbb{C}_{\tau_1} \times \cdots \times \mathbb{C}_{\tau_n}$. Dieser $\mathbb{C}$-Vektorraum ausgetattet mit dem Standardskalarprodukt, d. h. für Elemente $x = (x_\tau)$ und $y = (y_\tau)$ von $K_{\mathbb{C}}$ ist $\langle x, y\rangle = \sum_{\tau \in \mathcal{H}} x_\tau \overline{y}_\tau$. In diesen n-dimensionalen hermiteschen Vektorraum gibt es die $\mathbb{Q}$-lineare Einbettung $j\colon K \to K_{\mathbb{C}}$, die durch $c \mapsto \prod_{\tau \in \mathcal{H}} = (\tau_1(c), \ldots, \tau_n(c))$ definiert ist.

Auf dem Körper der komplexen Zahlen $\mathbb{C}$ haben wir den Körperautomorphismus $F\colon \mathbb{C} \to \mathbb{C}$ der komplexen Konjugation, d. h. $z \mapsto \overline{z}$. Genauer gesagt ist $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, F\}$.

Die Galoisgruppe $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ operiert auf $\mathcal{H} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ durch $F \circ \tau = \overline{\tau}$. Wir schreiben auch $F(\tau)$ für $F \circ \tau$.

Bemerkung II.5.2 (Komplexe Konjugation): (i) Auf dem Vektorraum $K_{\mathbb{C}}$ haben wir die Abbildung $F\colon K_{\mathbb{C}} \to K_{\mathbb{C}}$, $z = (z_\tau)_\tau \mapsto (\overline{z}_{\overline{\tau}})_\tau$. Diese ist ein Homomorphismus reeller Vektorräume und eine Involution, d. h. $F \circ F = \mathrm{id}$. So wie für die komplexen Zahlen wird uns F dabei helfen, ein passendes reelles Analogon von $K_{\mathbb{C}}$ zu finden.

(ii) Das Standardskalarprodukt $\langle \cdot, \cdot \rangle\colon K_{\mathbb{C}} \times K_{\mathbb{C}} \to \mathbb{C}$ ist F-äquivariant, d. h. für x und y haben wir $\langle F(x), F(y)\rangle = F(\langle x, y\rangle)$. Man beachte die missbräuchliche Verwendung von F für die Abbildung von oben sowie die komplexe Konjugation auf $\mathbb{C}$.

(iii) Die $\mathbb{C}$-lineare Abbildung $\mathrm{Tr}\colon K_{\mathbb{C}} \to \mathbb{C}$, $z = (z_\tau) \mapsto \sum_{i=1}^n z_{\tau_i}$ ist F-äquivariant und

$$\mathrm{Tr} \circ j\colon K \xhookrightarrow{j} K_{\mathbb{C}} \xrightarrow{\mathrm{Tr}} \mathbb{C}$$

liefert die übliche Spur $\mathrm{Tr}_{K|\mathbb{Q}}$.

Beweis: Die erste Aussage ist klar.

Zu (ii): Für x und y aus $K_{\mathbb{C}}$ gilt

$$\langle F(x), F(y)\rangle = \sum_{i=1}^n \overline{x}_{\overline{\tau}_i} y_{\overline{\tau}_i} = \overline{\sum_{i=1}^n x_{\overline{\tau}_i} \overline{y}_{\overline{\tau}_i}} = \overline{\langle x, y\rangle} = F(\langle x, y\rangle).$$

Zu (iii): Die $\mathbb{C}$-Linearität der Abbildung ist klar, F-Äquivarianz zeigt man wie in (ii). Schließlich haben wir

$$c \xmapsto{j} (\tau_1(c), \ldots, \tau_n(c)) \xmapsto{\mathrm{Tr}} \sum_{i=1}^n \tau_i(c) = \mathrm{Tr}_{K|\mathbb{Q}}(c).$$

□

Bemerkung II.5.3: Für den reellen Vektorraum $K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \mid F(z) = z\}$, also die Menge von Vektoren $z = (z_{\tau_1}, \ldots, z_{\tau_n})$ aus $K_{\mathbb{C}}$ mit $z_{\overline{\tau}_i} = \overline{z_{\tau_i}}$, gilt:

(i) $\langle \cdot, \cdot \rangle|_{K_{\mathbb{R}} \times K_{\mathbb{R}}}$ ist ein reelles Skalarprodukt auf $K_{\mathbb{R}}$.

(ii) Die Einbettung von K in $K_{\mathbb{C}}$ ist tatsächlich $K_{\mathbb{R}}$.

(iii) Die Spur Tr nimmt auf $K_{\mathbb{R}}$ nur reelle Werte an.

Ein Wort zur Warnung: Wir halten fest, dass es sich bei $K_{\mathbb{R}}$ um keinen $\mathbb{C}$-Unterraum von $K_{\mathbb{C}}$ handelt.

Beweis: (i) Sind x und y in $K_{\mathbb{R}}$, dann ist $F(\langle x, y \rangle) = \langle F(x), F(y) \rangle = \langle x, y \rangle$, d. h. $\langle x, y \rangle$ ist eine reelle Zahl.

(ii) Für c aus K ist $F(j(c)) = F(\tau_1(c), \ldots, \tau_n(c)) = (\overline{\tau_1(c)}, \ldots, \overline{\tau_n(c)}) = j(c)$, sodass $j(c)$ zu $K_{\mathbb{R}}$ gehört. □

Im Folgenden unterscheiden wir in der Notation nicht mehr zwischen $\langle \cdot, \cdot \rangle$ und $\langle \cdot, \cdot \rangle|_{K_{\mathbb{R}}} \times K_{\mathbb{R}}$.

Definition II.5.4: Wir nennen $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle)$ *Minkowski-Raum*, das Skalarprodukt $\langle \cdot, \cdot \rangle$ auf $K_{\mathbb{R}}$ bezeichnen wir als die *kanonische Metrik*, und das von $\langle \cdot, \cdot \rangle$ definierte Maß nennen wir das *kanonische Maß*.

Der Minkowski-Raum ist ausgestattet mit der Einbettung $j \colon K \to K_{\mathbb{R}}$ und der Spurabbildung $\mathrm{Tr} \colon K_{\mathbb{R}} \to K$, wobei $\mathrm{Tr} \circ j = \mathrm{Tr}_{K|\mathbb{Q}}$.

Wir verwenden den Standardisomorphismus $\mathbb{C} \to \mathbb{R}^2$, $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$.

Proposition II.5.5 (Explizite Beschreibung des Minkowski-Raum): *Es seien $\rho_1, \ldots, \rho_r$ diejenigen Einbettungen aus $\mathcal{H}$, deren Wertebereich in den reellen Zahlen liegt (auch reelle Einbettungen genannt) und $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$ die komplexen Einbettungen, d. h. $n = r + 2s$. Dann erhalten wir den Isomorphismus $f \colon K_{\mathbb{R}} \to \prod_{\tau \in \mathcal{H}} \mathbb{R}$, wobei (z_τ) geschickt wird auf (x_τ) mit*

$$x_\tau = \begin{cases} x_{\rho_i} = z_{\rho_i}, & \text{falls } i \in \{1, \ldots, r\}, \\ x_{\sigma_j} = \mathrm{Re}(z_{\sigma_j}), x_{\overline{\sigma}_j} = \mathrm{Im}(z_{\sigma_j}), & \text{falls } j \in \{1, \ldots, s\}. \end{cases}$$

Der Isomorphismus f überträgt das Skalarprodukt $\langle \cdot, \cdot \rangle$ auf das Skalarprodukt $(\cdot, \cdot)$, das durch $(x, y) = \sum_{\tau \in \mathcal{H}} \alpha_\tau x_\tau y_\tau$ definiert ist, wobei

$$\alpha_\tau = \begin{cases} 1, & \text{falls } \tau \in \{\rho_1, \ldots, \rho_r\}, \\ 2, & \text{falls } \tau \in \{\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s\}. \end{cases}$$

Für den Beweis werden folgende elementare Identitäten nützlich. Für eine komplexe Zahl w gilt $w + \overline{w} = 2\,\mathrm{Re}(w)$ und für komplexe Zahlen a und b gilt die Identität $\mathrm{Re}(ab) = \mathrm{Re}(a)\,\mathrm{Re}(b) - \mathrm{Im}(a)\,\mathrm{Im}(b)$.

Beweis: Sei (z_τ) in $K_{\mathbb{C}}$. Genau dann gehört (z_τ) zu $K_{\mathbb{R}}$, wenn $z_{\rho_1}, \ldots, z_{\rho_r}$ reell sind und $z_{\overline{\sigma}_i} = \overline{z_{\sigma_i}}$. Das heißt f ist ein Isomorphismus.

Wir schreiben $z = (z_\tau) = (x_\tau + \mathrm{i}y_\tau)$ mit geeigneten reellen Zahlen x_τ, y_τ, und analog $z' = (z'_\tau) = (x'_\tau + \mathrm{i}y'_\tau)$. Dann ist

$$\begin{aligned}(f(z), f(z')) &= \langle z, z' \rangle \\ &= \sum_{\tau \in \mathcal{H}} z_\tau \overline{z'_\tau} = \sum_{i=1}^{r} x_{\rho_i} x_{\rho'_i} + \sum_{j=1}^{s} z_{\sigma_j} \overline{z'_{\sigma_j}} + \sum_{j=1}^{s} z_{\overline{\sigma}_j} \overline{z'_{\overline{\sigma}_j}}.\end{aligned}$$

Unter Verwendung von $z_{\overline{\sigma}_j} = \overline{z_{\sigma_j}}$ sowie $z'_{\overline{\sigma}_j} = \overline{z'_{\sigma_j}}$ können wir aus der obigen Gleichung herauslesen, dass

$$\begin{aligned}(f(z), f(z') &= \sum_{i=1}^{r} x_{\rho_i} x'_{\rho_i} + 2 \sum_{j=1}^{s} \mathrm{Re}(z_{\sigma_j} \overline{z'_{\sigma_j}}) \\ &= \sum_{i=1}^{r} x_{\rho_i} x'_{\rho_i} + 2 \sum_{j=1}^{s} x_{\sigma_j} x'_{\sigma_j} + y_{\sigma_j} y'_{\sigma_j} \\ &= \sum_{i=1}^{r} f(z)_{\rho_i} f(z')_{\rho_i} + 2 \sum_{j=1}^{s} f(z)_{\sigma_j} f(z')_{\sigma_j} + f(z)_{\overline{\sigma}_j} f(z')_{\overline{\sigma}_j},\end{aligned}$$

was wir zeigen wollten. □

Bemerkung II.5.6 (Kanonisches Maß und Lebesgue-Maß): Sei X eine bezüglich des kanonischen Maßes messbare Teilmenge des $K_{\mathbb{R}}$. Für die Volumina bezüglich der beiden Maße gilt dann $\mathrm{vol}_{\mathrm{kan}}(X) = 2^s \,\mathrm{vol}_{\mathrm{Leb}}\, f(X)$, da in der Definition der induzierten Norm die Wurzel auftaucht.

Proposition II.5.7 (Ideale als Gitter): *Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal des Ganzheitsrings $\mathcal{O}_K$. Dann ist $\Gamma = j(\mathfrak{a})$ ein vollständiges Gitter in $K_{\mathbb{R}}$ und $\mathrm{vol}(\Gamma) = [\mathcal{O}_K : \mathfrak{a}]|d_K|^{1/2}$, wobei d_K die Diskriminante der Körpererweiterung $\mathbb{Q} \subseteq K$ ist.*

Bemerkung II.5.8 (Diskriminante von Idealen): Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in $\mathcal{O}_K$. Nach Satz 2 ist $\mathfrak{a}$ isomorph zu $\mathbb{Z}^n$ für $n = [K : \mathbb{Q}]$; es gibt also Elemente $\alpha_1, \ldots, \alpha_n$ von $\mathcal{O}_K$, sodass $\mathfrak{a} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. Für diese Basis ist $d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = \det(\tau_i(\alpha_j)_{i,j})^2$ die Diskriminante von $\mathfrak{a}$. Genau wie für den Ganzheitsring zeigt man, dass die Diskriminante eines Ideals nicht von der gewählten Basis $\alpha_1, \ldots, \alpha_n$ abhängt, da Basiswechsel über $\mathbb{Z}$ Determinante ± 1 haben. Sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Ideale in $\mathcal{O}_K$ mit $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$, dann gilt $d(\alpha_1) = [\mathfrak{a}_2 : \mathfrak{a}_1]^2 d(\mathfrak{a}_2)$.

Wir zeigen die zweite Aussage der obigen Bemerkung. Nach Satz 2 ist $n = \mathrm{Rang}(\mathcal{O}_K) = \mathrm{Rang}(\mathfrak{a}_1) = \mathrm{Rang}(\mathfrak{a}_2)$. Nach dem Hauptsatz für endlich erzeugte $\mathbb{Z}$-Moduln gibt es eine Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}_2$ und Elementarteiler $k_1, \ldots, k_n$ aus den natürlichen Zahlen, sodass $k_1\alpha_1, \ldots, k_n\alpha_n$ eine Basis von $\mathfrak{a}_1$ ist. Für den Index von $\mathfrak{a}_1$ in $\mathfrak{a}_2$ erhalten wir deshalb $[\mathfrak{a}_2 : \mathfrak{a}_1] = k_1 \cdots k_n$. Außerdem haben wir

$$\begin{aligned} d(\mathfrak{a}_1) &= d(k_1\alpha_1, \ldots, k_n\alpha_n) \\ &= \det(\tau_i(k_j\alpha_j)_{i,j})^2 = k_1^2 \cdots k_n^2 \det(\tau_i(\alpha_j)_{i,j}) = k_1^2 \cdots k_n^2 d(\mathfrak{a}_2) \end{aligned}$$

Insbesondere folgt aus dem oben gezeigten, dass jedes Ideal in $\mathcal{O}_K$ endlichen Index hat. Für $\mathfrak{a}_2 = \mathcal{O}_K$ und $\mathfrak{a}_1$ irgendein Ideal haben wir ja die Gleichung $d(\mathfrak{a}_1) = [\mathcal{O}_K : \mathfrak{a}_1]^2 d_K$, und die Diskriminanten sind irgendwelche ganzen Zahlen.

Beweis (von Proposition II.5.7): Wir wählen die $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}$, d. h. $\mathfrak{a} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$.

Die Menge $\Gamma = j(\mathfrak{a}) = \bigoplus_{i=1}^n \mathbb{Z} j(\alpha_i)$ ist offensichtlich ein Gitter in $K_\mathbb{R}$. Für sein Volumen gilt $\mathrm{vol}(\Gamma) = |\det(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k}|^{1/2}$ und mithilfe der Matrix

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n) \end{pmatrix}.$$

können wir schreiben $(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k} = (\sum_{\ell=1}^n \tau_\ell(\alpha_i)\overline{\tau_\ell(\alpha_k)})_{i,k} = AA^t$. Aber das bedeutet $\mathrm{vol}(\Gamma) = |\det(A)\det\big(\overline{A}^t\big)|^{1/2} = |\det(A)|$. Wegen

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = \det(A)^2 \quad \text{und} \quad d(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]^2 d_K$$

folgt daraus die Behauptung. □

Proposition II.5.9 (Kleine Idealelemente): *Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal des Ganzheitsrings $\mathcal{O}_K$ und für jedes τ aus $\mathrm{Hom}(K, \mathbb{C})$ sei eine positive reelle Zahl c_τ gegeben, sodass $c_{\overline{\tau}} = c_\tau$. Ist $\prod_{\tau\in\mathcal{H}} c_\tau > (2/\pi)^s |d_K|^{1/2}$, dann gibt es ein von Null verschiedenes Element a von $\mathfrak{a}$, sodass für jedes τ in $\mathrm{Hom}(K, \mathbb{C})$ gilt: $|\tau(\alpha)| < c_\tau$.*

Beweis: Wir wollen natürlich den Minkowskischen Gitterpunktsatz verwenden. Transportieren wir $\mathfrak{a}$ per j nach $K_\mathbb{R}$ wie zuvor und nennen das Bild Γ, dann haben wir $\mathrm{vol}(\Gamma) = |d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}]$. Im Minkowskiraum $K_\mathbb{R}$ wählen wir die Menge $X = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ und verwenden den Isomorphismus

$$f\colon K_\mathbb{R} \longrightarrow \prod_{\tau\in\mathcal{H}} \mathbb{R}_\tau, \qquad (z_\tau) \longmapsto (x_\tau) \quad \text{mit} \quad x_\tau = \begin{cases} x_{\rho_i} = z_{\rho_i}, \\ x_{\sigma_i} = \mathrm{Re}\, z_{\sigma_i}, \\ x_{\overline{\sigma}_i} = \mathrm{Im}\, z_{\sigma_i}. \end{cases}$$

Dann ist

$$f(X) = \left\{(x_\tau) \in \prod_{\tau\in\mathcal{H}} \mathbb{R}_\tau : |x_{\rho_i}| < c_{\rho_i}, 1 \le i \le r, x_{\sigma_i}^2 + x_{\overline{\sigma_j}}^2 < c_{\sigma_j}^2, 1 \le j \le s\right\}$$

und $\mathrm{vol}_{\mathrm{can}}(X) = 2^s \,\mathrm{vol}_{\mathrm{Leb}}(f(X)) = 2^s \prod_{i=1}^r 2c_{\rho_i} \prod_{j=1}^s \pi c_{\sigma_j}^2 = 2^{r+s}\pi^s \prod_{\tau\in\mathcal{H}} c_\tau$. Nach Voraussetzung ist dieses Volumen größer als $2^n|d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}] = 2^n \,\mathrm{vol}(\Gamma)$ und die Behauptung folgt aus dem Gitterpunktsatz. □

6 Die Klassenzahl

Wie immer seien K ein algberaischer Zahlkörper vom Grad n über $\mathbb{Q}$ mit Ganzheitsring $\mathcal{O}_K$. In diesem Abschnitt wollen wir zeigen, dass die Klassengruppe $\mathrm{C}\ell_K$ endlich ist.

Die grobe Beweisidee wird sein, zu zeigen, dass jedes gebrochene Ideal J ein Element x enthält, dessen Norm $N_{K|\mathbb{Q}}(x)$ „klein“ ist. Denn dann ist $(x)J^{-1}$ ganz und ebenfalls „klein“. Im zweiten Schritt werden wir dann zeigen, dass es nur endlich viele „kleine“ ganze Ideale gibt.

Definition II.6.1 („Größe“ eines Ideals): Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal in $\mathcal{O}_K$. Wir nennen $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|$ die *Norm von* $\mathfrak{a}$.

Proposition II.6.2 (Normeigenschaften): *Für die Norm von Idealen gilt:*

(i) $N(\mathcal{O}_K) = 1$.

(ii) *Für Ideale* $\mathfrak{a}, \mathfrak{b}$ *in* $\mathcal{O}_K$ *ist* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

(iii) *Ist* α *in* $\mathcal{O}_K$*, dann ist* $N((\alpha)) = N_{K|\mathbb{Q}}(\alpha)$.

Insbesondere lässt sich die Norm fortsetzen zu einem Gruppenhomomorphismus $N\colon I(\mathcal{O}_K) \to \mathbb{Q}_{>0}^\times$*, der* $\prod_{i=1}^k \mathfrak{p}_i^{\alpha_i}$ *auf* $\prod_{i=1}^k N(\mathfrak{p}_i)^{\alpha_i})$ *schickt.*

Mit dem Beweis von Proposition II.2.6 machen wir später weiter.

Lemma II.6.3 (Teilbarkeit von Idealen in Dedekindringen): *Seien* $\mathfrak{a}$ *und* $\mathfrak{b}$ *Ideale in einem Dedekindring* R*. Genau dann ist* $\mathfrak{a}$ *in* $\mathfrak{b}$ *enthalten, wenn* $\mathfrak{b}$ *ein Teiler von* $\mathfrak{a}$ *ist, d. h. wenn es ein Ideal* $\mathfrak{b}'$ *in* R *gibt, sodass* $\mathfrak{a} = \mathfrak{b}\mathfrak{b}'$.

Beweis: „$\Longleftarrow$“ ist klar.

„$\Longrightarrow$“: Falls $\mathfrak{b} = (0)$ ist, dann ist die Aussage klar. Sonst definieren wir $\mathfrak{b}' = \mathfrak{b}^{-1}\mathfrak{a}$. Dieses liegt in R, da $\mathfrak{a}$ in $\mathfrak{b}$ enthalten ist, und $\mathfrak{b}^{-1}\mathfrak{b} = R$ gilt. □

Beweis (von Proposition II.6.2): (i) Die erste Aussage folgt direkt aus der Definition der Norm.

(ii) Zunächst nehmen wir, dass die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ koprim sind. Nach dem Chinesischen Restsatz gilt dann $\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$, weshalb

$$N(\mathfrak{ab}) = [\mathcal{O}_K : \mathfrak{ab}] = |\mathcal{O}_K/\mathfrak{ab}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{b}| = N(\mathfrak{a})N(\mathfrak{b})$$

Es bleibt zu zeigen, dass für von Null verschiedene Primideale $\mathfrak{p}$ in $\mathcal{O}_K$ gilt: $N(\mathfrak{p}^k) = N(\mathfrak{p})^k$. Wir wissen bereits, dass wir eine absteigende Kette von Idealen $\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^k$ erhalten. Wegen der eindeutigen Primfaktorzerlegung ist diese Kette sogar strikt absteigend.

Des Weiteren ist $F = \mathcal{O}_K/\mathfrak{p}$ ein Körper, da $\mathcal{O}_K$ ein Dedekindring ist, und so Primideale in $\mathcal{O}_K$ maximal sind.

Schließlich sind die Quotienten $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ Vektorräume über F.

Wir behaupten, dass $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ein eindimensionaler Vektorraum über F ist. Ist nämlich a in $\mathfrak{p}^i - \mathfrak{p}^{i+1}$, dann haben wir $\mathfrak{p}^i \supseteq (a) + \mathfrak{p}^{i+1} \supseteq \mathfrak{p}^{i+1}$. Aber dann muss wegen der eindeutigen Primfaktorzerlegung und dem vorangegangenen Lemma bereits $(a) + \mathfrak{p}^{i+1} = \mathfrak{p}^i$ gelten, weshalb $\overline{a}$ in $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ als F-Vektorraum erzeugt.

Wir erhalten nun $|\mathfrak{p}^i/\mathfrak{p}^{i+1}| = |F| = |\mathcal{O}_K/\mathfrak{p}| = [\mathcal{O}_K : \mathfrak{p}] = N(\mathfrak{p})$, sodass

$$N(\mathfrak{p}^k) = [\mathcal{O}_K : \mathfrak{p}^k] = [\mathcal{O}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{k-1} : \mathfrak{p}^k] = |F|^k = N(\mathfrak{p})^k.$$

Nun folgt die Behauptung aus der eindeutigen Primfaktorzerlegung in Verbindung mit der Tatsache, dass für verschiedene Primideale $\mathfrak{p}$, $\mathfrak{q}$ und natürliche Zahlen a und b die Ideale $\mathfrak{p}^a$ und $\mathfrak{q}^b$ koprim sind.

(iii) Sei $\mathfrak{a}$ das Hauptideal (a). Wegen des Elementarteilersatzes und Satz 2 gibt es eine Basis $B = \{x_1, \ldots, x_n\}$ von $\mathcal{O}_K$ und natürliche Zahlen $k_1, \ldots, k_n$, sodass $C = \{k_1x_1, \ldots, k_nx_n\}$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ ist. Außerdem haben wir uns bereits klargemacht, dass $[\mathcal{O}_K : \mathfrak{a}] = k_1 \cdots k_n = \det(D_{BC})$ für die Basiswechselmatrix von B nach C gilt.

Wir erhalten aber auch eine $\mathbb{Z}$-Basis C' von $\mathfrak{a}$ mit $\{ax_1, \ldots, ax_n\}$, und die Basiswechselmatrix $D_{CC'}$ hat Determinante ± 1.

Wir erinnern uns daran, dass $N_{K|\mathbb{Q}}(a) = \det(x \mapsto ax) = \det(D_{BB}(x \mapsto ax))$ die Norm des Elements a ist. Die Darstellungsmatrix $D_{BB}(x \mapsto ax)$ ist aber genau die Matrix $D_{BC'} = D_{BC}D_{CC'}$. Insgesamt können wir deshalb zusammenfassen, dass $N_{K|\mathbb{Q}}(a) = \pm \det D_{BC} = \pm[\mathcal{O}_K : \mathfrak{a}]$ und $N(\mathfrak{a}) > 0$. Daraus folgt die Behauptung. □

Lemma II.6.4 (Kleine Elemente in Idealen): *In jedem von Null verschiedenen Ideal $\mathfrak{a}$ von $\mathcal{O}_K$ gibt es ein von Null verschiedenes Element a, für dessen Norm gilt: $|N_{K|\mathbb{Q}}(a)| \leq (2/\pi)^s |d_K|^{1/2} N(\mathfrak{a})$.*

Beweis: Wegen Proposition 5.9 gibt es für jedes gegebene Tupel $(c_\tau)_{\tau\in\mathcal{H}}$ mit $c_{\overline{\tau}} = c_\tau$ und $\prod_{\tau\in\mathcal{H}} c_\tau > (2/\pi)^s |d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}]$ gibt es ein Element a in $\mathfrak{a} - \{0\}$, sodass für jede Einbettung τ aus $\mathcal{H}$ gilt: $|\tau(a)| < c_\tau$.

Für jedes $\varepsilon > 0$ erhalten wir also ein von Null verschiedenes a, sodass

$$|N_{K|\mathbb{Q}}(a)| = |\prod_{\tau\in\mathcal{H}} \tau(a)| = \prod_{\tau\in\mathcal{H}} |\tau(a)| < \prod_{\tau\in\mathcal{H}} c_\tau < \left(\frac{2}{\pi}\right)^s |d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}] + \varepsilon.$$

Weiterhin wissen wir, dass $|N_{K|\mathbb{Q}}(a)|$ eine natürliche Zahl ist, weil a ein ganzes Element ist. Darum erhalten wir ein Element a aus $\mathfrak{a} - \{0\}$, für dessen Norm $|N_{K|\mathbb{Q}}(a)| \leq (2/\pi)^s |d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}]$ gilt. □

Satz 6 (von Kronecker): *Die Idealklassengruppe* $\mathrm{C}\ell_K = I(\mathcal{O}_K)/\mathcal{H}$ *ist eine endliche Gruppe.*

Beweis: Sei $\mathfrak{p}$ ein von Null verschiedenes echtes Ideal unseres Dedekindrings $\mathcal{O}_K$. Dann ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Körpererweiterung von $\mathbb{F}_p$ für die Primzahl p mit $\mathbb{Z}p = \mathfrak{p} \cap \mathbb{Z}$. Man überlegt sich, dass das Ideal $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal ist. Nach Proposition II.3.6 ist $\mathcal{O}/\mathfrak{p}$ ist ein endlicher Körper, weshalb $\mathfrak{p} \cap \mathbb{Z}$ nicht das Nullideal sein kann. Es gibt deshalb eine Primzahl p mit $\mathbb{Z}p = \mathfrak{p} \cap \mathbb{Z}$. In der beschriebenen Situation erhalten wir eine Einbettung $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$.

Sei $M > 0$ vorgegeben. Wir zeigen im Folgenden, dass es nur endlich viele Primideale $\mathfrak{p}$ in $\mathcal{O}_K$ gibt, sodass $N(\mathfrak{p}) \leq M$. Nach unseren ersten Überlegungen ist $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z}p$ und $N(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}] = p^f$ für $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$. Wegen $N(\mathfrak{p}) \leq M$ gibt es nur endlich viele Möglichkeiten für p und f. Für ein gegebenes p gilt aber: Liegt p in $\mathfrak{p}$, dann ist $\mathcal{O}_K p$ in $\mathfrak{p}$ enthalten und $\mathfrak{p}$ ist ein Teiler von $\mathcal{O}_K p$. Wegen der Eindeutigkeit der Primfaktorzerlegung gibt es nur endlich viele solche $\mathfrak{p}$.

Schließlich verwenden wir die eindeutige Primfaktorzerlegung, um die Aussage für allgemeine Ideale zu erhalten. Sei also $M > 0$ vorgegeben. Jedes von Null verschiedene Ideal $\mathfrak{a}$ von $\mathcal{O}_K$ lässt sich schreiben als $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ für Primideale $\mathfrak{p}_i$ und natürliche Zahlen ν_i. Es gilt

$$M \geq N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdots N(\mathfrak{p}_r)^{\nu_r}$$

und die Behauptung folgt aus dem zweiten Schritt.

Zu guter Letzt zeigen wir, dass jede Klasse $[\mathfrak{a}]$ in $\mathrm{C}\ell_K$ ein ganzahliges Ideal $\mathfrak{a}_1 \subseteq \mathcal{O}_K$ enthält, sodass $N(\mathfrak{a}_1) \leq M^{\min} = (2/\pi)^a |d_K|^{1/2}$.

Ist $\mathfrak{a}$ ein gebrochenes Ideal, dann auch $\mathfrak{a}^{-1}$. Nach Proposition II.3.14 gibt es ein Element d in $\mathcal{O}_K - \{0\}$, sodass $d\mathfrak{a}^{-1}$ ganz in $\mathcal{O}_K$ enthalten ist. Wir setzen $\mathfrak{b} = d\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ und erhalten das Ideal $\mathfrak{b}^{-1} = d^{-1}\mathfrak{a}$, das in $[\mathfrak{a}]$ liegt.

Nach Lemma II.6.4 gibt es ein von Null verschiedenes Element b von $\mathfrak{b}$, sodass $|N_{K|\mathbb{Q}}(b)| \leq M^{\min} N(\mathfrak{b})$, weshalb

$$N((b)\mathfrak{b}^{-1}) = N((b))N(\mathfrak{b}^{-1}) = N_{K|\mathbb{Q}}(b)N(\mathfrak{b}^{-1}) \leq M^{\min}.$$

Wir setzen $\mathfrak{a}_1 = (b)\mathfrak{b}^{-1}$. Weil b zu $\mathfrak{b}$ gehört, ist $\mathfrak{a}_1$ in $\mathcal{O}_K$ enthalten; per Konstruktion haben wir $N(\mathfrak{a}_1) \leq M^{\min}$ und es ist $[\mathfrak{a}_1] = [\mathfrak{b}^{-1}] = [\mathfrak{a}]$. Die letzten beiden Schritte liefern nun, dass es nur endlich viele Idealklassen gibt. □

Korollar II.6.5 (Endlich viele Ideale von beschränkter Norm): *Sei $M > 0$ vorgegeben. Dann gibt es in $\mathcal{O}_K$ nur endlich viele Ideale, deren Index höchstens M ist.*

Das haben wir im Beweis von Satz 6 gezeigt.

Bemerkung II.6.6 (Minkowski-Schranke): Die Schranke $M^{\min} = (2/\pi)^s |d_K|^{1/2}$ heißt Minkowski-Schranke und kann verwendet werden, um die Klassengruppe zu bestimmen.

Definition II.6.7 (Klassenzahl): Sei K ein algebraischer Zahlkörper. Dann heißt $h_K = |\mathrm{C}\ell_K| = [I(\mathcal{O}_K) : \mathcal{H}]$ die *Klassenzahl von K*.

Genau dann ist die Klassenzahl $h_K = 1$, wenn die Klassengruppe $\mathrm{C}\ell_K$ die triviale Gruppe $\{0\}$ ist. Das tritt genau dann ein, wenn $\mathcal{O}_K$ ein Hauptidealring ist, oder äquivalent ein faktorieller Ring.

Beispiel II.6.8: Sei K der imaginärquadratische Zahlkörper $\mathbb{Q}(\sqrt{-14})$. Es ist $D = -14 \equiv 2 \pmod 4$, sodass $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ ist. Die Einbettungen von K ist die Menge $\mathcal{H} = \{\sigma_1 = \mathrm{id}, \sigma_2 \colon a + b\sqrt{-14} \mapsto a - b\sqrt{-14}\}$ und die Diskriminante von K ist $d_K = 4D = -56$.

Für die Minkowski-Schranke $M^{\min}$ aus Satz 6 finden wir

$$M^{\min} = \left(\frac{2}{\pi}\right)\sqrt{56} \approx 4,764.$$

Sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}_K$, dessen Norm $N(\mathfrak{P})$ höchstens M ist. Wir erinnern uns, dass dann $\mathfrak{P} \cap \mathbb{Z} = (p)$ ein Primideal und $\mathcal{O}/\mathfrak{P}$ eine Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist.

Die Möglichkeiten für $N(\mathfrak{P})$ sind $N(\mathfrak{P}) = p^f \leq M$, sodass p in $\{2, 3\}$ enthalten sein muss. Ferner ist $\mathfrak{P}$ ein Teiler von $\mathcal{O}_K p$.

Wir behaupten, dass $(2) = (\sqrt{-14}, 2)(\sqrt{-14}, 2) = (-14, 2\sqrt{-14}, 4)$ die Primfaktorzerlegung von (2) in $\mathcal{O}_K$ ist.

Das Ideal $\mathfrak{P}_1 = (\sqrt{-14}, 2)$ ist ein Primideal, denn $\varphi\colon \mathbb{Z}[\sqrt{-14}] \to \mathbb{Z}/2\mathbb{Z}$, die $a + b\sqrt{-14}$ auf $a \pmod 2$ schickt, ist ein Ringhomomorhismus:

$$\begin{aligned}\varphi\Big((a_1 + b_1\sqrt{-14})(a_2 + b_2\sqrt{-14})\Big) &= \varphi(a_1a_2 - 14b_1b_2 + (\dots)\sqrt{-14}) \\ &= a_1a_2 - 14b_1b_2 \pmod 2 = a_1a_2 \pmod 2.\end{aligned}$$

Der Kern dieses surjektiven Ringhomomorphismus φ ist das Ideal $\mathfrak{P}_1$, weshalb $\mathbb{Z}[\sqrt{-14}]/\mathfrak{P}_1 \cong \mathbb{Z}/2\mathbb{Z}$ ist, und $N(\mathfrak{P}_1) = [\mathbb{Z}[\sqrt{-14}] : \mathfrak{P}_1] = 2$.

Analog zeigt man, dass $(3) = (1 + \sqrt{-14}, 3)(1 - \sqrt{-14}, 3) = \mathfrak{P}_2\mathfrak{P}_3$ eine Primfaktorzerlegung in $\mathcal{O}_K$ ist. Dazu verwendet man den Ringhomomorphismus $\psi\colon \mathbb{Z}[\sqrt{-14}] \to \mathbb{Z}/3\mathbb{Z}$, der $a + b\sqrt{-14}$ schickt auf $a - b \pmod 3$.

Nun versuchen wir zu entscheiden, ob $\mathcal{O}_K$ ein Hauptidealring ist. Wir wissen bereits, dass in einem Hauptidealring die Norm eines Ideals mit der Norm der Körpererweiterung des Erzeugers übereinstimmt. Die Ideale $\mathfrak{P}_1, \mathfrak{P}_2$ und $\mathfrak{P}_3$ sind allesamt keine Hauptideale. Wäre nämlich $\mathfrak{P}_i = (\alpha)$ für ein Element $\alpha = a + b\sqrt{-14}$, dann wäre $N(\mathfrak{P}_i) = N_{K|\mathbb{Q}}(\alpha) = a^2 + 14b^2$. Wegen $N(\mathfrak{P}_i) = 2, 3$ kann das aber nicht passieren.

Weiterhin ist $[\mathfrak{P}_1]^2 = [1]$, weil wir oben gesehen haben, dass $\mathfrak{P}_1^2$ ein Hauptideal ist, und ebenfalls wegen der vorherigen Überlegungen haben wir $[1] = [\mathfrak{P}_2][\mathfrak{P}_3]$.

Wir suchen nun weitere Relationen für die Elemente in $\mathrm{C}\ell_K$, um sie vollständig zu bestimmen. Das wollen wir mit „Elementen mit kleiner Norm“ tun. Beispielsweise ist $N_{K|\mathbb{Q}}(2 + \sqrt{-14}) = 4 + 14 = 18 = 9 \cdot 2$, sodass $(2 + \sqrt{-14}) = \mathfrak{P}_1\mathfrak{P}_2^2$ oder $(2 + \sqrt{-14}) = \mathfrak{P}_1\mathfrak{P}_3^2$. Diesen Faktorisierungen entsprechen die Relationen $[\mathfrak{P}_1] = [\mathfrak{P}_2]^2$ oder $[\mathfrak{P}_1] = [\mathfrak{P}_3]^2$. Per Fallunterscheidung sieht man nun ein, dass $[\mathfrak{P}_1] = [\mathfrak{P}_2]^2 = [\mathfrak{P}_3]^2$, und darum gilt $\mathrm{C}\ell_K = \mathbb{Z}/4\mathbb{Z}$. Entsprechend ist $h_K = 4$.

Definition II.6.9 (Reguläre Primzahl): Seien K ein zyklotomischer Körper $\mathbb{Q}(\zeta_p)$ für eine primitive p-te Einheitswurzel und h_p die zugehörige Klassenzahl. Wenn h_p nicht von p geteilt wird, dann heißt die Primzahl p *regulär*; sonst *irregulär*.

Als Ausblick halten wir ein paar wichtige Aussagen fest. Das ist beispielsweise der Satz von Heegner: Ist $K = \mathbb{Q}[\sqrt{-D}]$ ein imaginärquadratischer Zahlkörper für eine quadratfreie natürliche Zahl D, dann ist die Klassenzahl 1 genau dann, wenn D zur Menge $\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ gehört. Diese Menge heißt Menge der *Heegnerzahlen*.

Beispielsweise der reellquadratische Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$ hat Klassenzahl 1 für D aus $\{2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, \dots\}$. Man vermutet, dass es unendlich viele quadratfreie natürliche Zahlen D gibt, sodass die Klassengruppe von $\mathbb{Q}[\sqrt{D}]$ trivial ist, aber man weiß es nicht.

Man weiß allgemeiner ebenfalls nicht, ob es unendlich viele Zahlkörper mit Klassenzahl 1 gibt. Diese Frage steht in Zusammenhang mit Fermats letztem Satz, der aussagt, dass es für paarweise verschiedene ganze Zahlen x, y, z und eine natürliche Zahl $p \geq 3$ keine Beziehung der Form $x^p + y^p = z^p$ geben kann. Dieser Zusammenhang wird hergestellt durch

$$y^p = z^p - x^p = (z - x)(z - \zeta_p x) \cdots (z - \zeta_p^{p-1} x)$$

als Gleichung in $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}[\zeta_p]}$. Wär der Ganzheitsring $\mathbb{Z}[\zeta_p]$ faktoriell, dann würde eine nichttriviale Lösung zu einem Widerspruch führen. Die Tatsache „Die Klasenzahl von $\mathbb{Q}[\zeta_p]$ ist 1“ würde also bedeuten, dass $x^p + y^p = z^p$ keine nichttrivialen Lösungen besitzt.

Kummer hat erkannt, dass dieses Argument auch funktionieren würde, wenn p kein Teiler der Klassenzahl h_p ist. Daher stammt die Definition der Regularität einer Primzahl. Irreguläre Primzahlen sind übrigens sehr selten!

Der Beweis des letzten Satzes von Fermat wurde später mit anderen Methoden, nämlich mithilfe elliptischer Kurven, von Andrew Wiles gegeben.

7 Multiplikative Minkowski-Theorie

Im Folgenden seien wieder stets K ein algebraischer Zahlkörper von Grad n, $\mathcal{H} = \mathrm{Hom}(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\} = \{\rho_1, \ldots, \rho_r, \sigma_1, \overline{\sigma}_1, \ldots, \sigma_r, \overline{\sigma}_r\}$. Wie bereits eingeführt, betrachten wir wieder den (komplexen) Minkowski-Raum

$$K \longrightarrow K_{\mathbb{C}} = \prod_{\tau \in \mathcal{H}} \mathbb{C}, \qquad c \longmapsto (\tau_1(c), \ldots, \tau_n(c))$$

und den reellen Minkowski-Raum

$$j \colon K_{\mathbb{R}} = \mathrm{Fix}_{K_{\mathbb{C}}}(F) = \{(x_\tau)_{\tau \in \mathcal{H}} \mid x_\rho \in \mathbb{R}, \text{ falls } \rho \text{ reell }, \overline{x}_\sigma = x_{\overline{\sigma}}, \text{ falls } \sigma \text{ komplex}\}.$$

Bemerkung II.7.1: Wir betrachten den Minkowski-Raum $K_{\mathbb{C}}$ nun als $\mathbb{C}$-Algebra.

(i) Genau dann ist c invertierbar in $K^\times$, wenn $j(c)$ zu $K_{\mathbb{C}}^\times$ gehört.

(ii) Für die Abbildung $N \colon K_{\mathbb{C}}^\times \to \mathbb{C}^\times$, $(x_\tau) \mapsto \prod_{\tau \in \mathcal{H}} x_\tau$ gilt

$$(N \circ j)_{K_{\mathbb{C}}^\times} \colon K^\times \xrightarrow{\ j\ } K_{\mathbb{C}}^\times \xrightarrow{\qquad N \qquad} \mathbb{C}^\times$$

$$c \longmapsto (\tau_1(c), \ldots, \tau_n(c)) \longmapsto \prod_{i=1}^n \tau_i(c) = N_{K|\mathbb{Q}}(c)$$

(iii) Mit der Logarithmusabbildung $\ell\colon \mathbb{C}^\times \to \mathbb{R}$, $z \mapsto \log|z|$ erhalten wir eine Abbildung

$$\widehat{\ell}\colon K_{\mathbb{C}}^\times \longrightarrow \prod_{\tau\in\mathcal{H}} \mathbb{R}, \qquad (x_\tau)_{\tau\in\mathcal{H}} \longmapsto (\log|x_\tau|)_{\tau\in\mathcal{H}}.$$

Proposition II.7.2: *Das folgende Diagramm von Gruppen ist kommutativ:*

$$\begin{array}{ccccc} K^\times & \xrightarrow{\ j\ } & K_{\mathbb{C}}^\times & \xrightarrow{\ \widehat{\ell}\ } & \prod_{\tau\in\mathcal{H}} \mathbb{R} \\ {\scriptstyle N_{K|\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \xrightarrow[\ \ell\ ]{} & \mathbb{R} \end{array}$$

Dieses Diagramm ist F-äquivariant für die jeweilige Aktion von F auf allen Gruppen des Diagramms.

Beweis: Das linke Quadrat des Diagramms kommutiert nach Bemerkung II.7.1. Wir betrachten das rechte Quadrat. Sei dazu $(x_\tau)_{\tau\in\mathcal{H}}$ ein Element von $K_{\mathbb{C}}^\times$. Die Norm $N\colon K_{\mathbb{C}}^\times \to \mathbb{C}^\times$ schickt $(x_\tau)_{\tau\in\mathcal{H}}$ auf das Produkt $\prod_{\tau\in\mathcal{H}} x_\tau$ und $\widehat{\ell}$ schickt $(x_\tau)_{\tau\in\mathcal{H}}$ auf $(\log|x_\tau|)_{\tau\in\mathcal{H}}$. Beispielsweise aus der Analysis ist bekannt, dass $\log|\prod_{\tau\in\mathcal{H}}| = \sum_{\tau\in\mathcal{H}} \log|x_\tau|$.

Zu den verschiedenen Aktionen von F auf den teilnehmenden Gruppen: Auf $K^\times$ und $\mathbb{Q}^\times$ operiert F trivial, auf $K_{\mathbb{C}}^\times$ operiert (das Analogon zur komplexen Konjugation) F durch $(x_\tau)_{\tau\in\mathcal{H}} \mapsto (\overline{x}_{\overline{\tau}})_{\tau\in\mathcal{H}}$, und auf $\mathbb{C}^\times$ operiert F durch komplexe Konjugation. Auf $\prod_{\tau\in\mathcal{H}} \mathbb{R}$ operiert F durch $(x_\tau)_{\tau\in\mathcal{H}} \mapsto (x_{\overline{\tau}})_{\tau\in\mathcal{H}}$ und auf $\mathbb{R}$ trivial.

Nun zur F-Äquivarianz des Diagramms: Für jedes c in $F^\times$ ist

$$F \circ j(c) = F(\tau(c)_t) = F(\overline{\tau(c)}_\tau) = (\tau(c))_\tau = j(c),$$

für jede Familie $(x_\tau)_\tau$ in $K_{\mathbb{C}}^\times$ haben wir

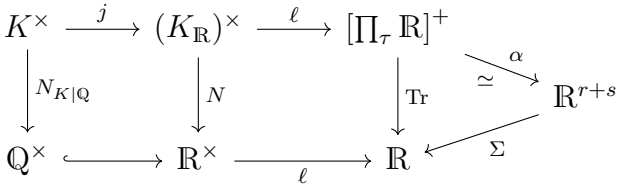
$$F(\ell(x_\tau)) = F(\log(x_\tau)_\tau) = (\log(x_{\overline{\tau}})_\tau) = (\log(\overline{x}_{\overline{\tau}})_\tau) = \ell((\overline{x}_{\overline{\tau}})_\tau) = \ell(F(x_\tau))$$

und für jede Familie $(x_\tau)_\tau$ in $K_{\mathbb{C}}^\times$ gilt

$$N(F(x_\tau)_\tau) = N(\overline{x}_{\overline{\tau}})_\tau = \prod_\tau \overline{x}_{\overline{\tau}} = \prod_\tau \overline{x}_\tau = \overline{\prod_\tau x_\tau} = F(N(x_\tau)_\tau).$$

Damit ist alles gezeigt. □

Bemerkung II.7.3: Ersetzen wir im Diagramm aus Proposition II.7.2 jede Gruppe durch die jeweilige Untergruppe der Fixelemente von F, dann erhalten wir das Diagramm



Hierbei ist $K_\mathbb{R}$ der reelle Minkowski-Raum aus Abschnitt 5, Σ bezeichnet die Funktion $\mathbb{R}^{r+s} \to \mathbb{R}$, $(x_1, \ldots, x_{r+s}) \mapsto \sum_{i=1}^{r+s} x_i$ und

$$\Big[\prod_\tau \mathbb{R}\Big]^+ = \Big\{(x_{\rho_1}, \ldots, x_{\rho_r}, x_{\sigma_1}, x_{\overline{\sigma}_1}, \ldots, x_{\sigma_s}, x_{\overline{\sigma}_s} \in \prod_{\tau \in \mathcal{H}} \mathbb{R} : x_{\sigma_i} = x_{\overline{\sigma}_i}\Big\}.$$

Der Isomorphismus α aus dem obigen Diagramm ist die Abbildung

$$\alpha\colon \Big[\prod_\tau \mathbb{R}\Big]^+ \longrightarrow \mathbb{R}^{r+s}, \qquad (x_{\rho_1}, \ldots, x_{\sigma_s}) \longmapsto (x_{\rho_1}, \ldots x_{\rho_r}, 2x_{\sigma_1}, \ldots, 2x_{\sigma_s}).$$

Das angehängte Dreieck auf der rechten Seite kommutiert ebenfalls, denn $\alpha \circ \ell$ ist die Abbildung

$$\alpha \circ \ell\colon (K_\mathbb{R})^\times \longrightarrow \mathbb{R}^{r+s},$$
$$(x_{\rho_1}, \ldots, x_{\rho_r}, x_{\overline{\sigma}_1}, \ldots, x_{\sigma_s}, x_{\overline{\sigma}_s}) \longmapsto (\log|x_{\rho_1}|, \ldots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \ldots, \log|x_{\sigma_2}|^2).$$

8 Dirichletscher Einheitensatz

Das Ziel dieses Abschnittes wird die Bestimmung der Einheitengruppe $\mathcal{O}_K^\times$ der Ganzheitsringes $\mathcal{O}_K$ eine algebraischen Zahlkörpers K von Grad n über $\mathbb{Q}$. Wir haben bereits gesehen, dass wir die Einheitengruppe folgendermaßen charakterisieren können:

$$\mathcal{O}_K^\times = \{\varepsilon \in \mathcal{O}_K \text{ ist invertierbar}\} = \{\varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) \in \{\pm 1\}\}.$$

Siehe dazu Proposition I.2.8. Ferner sitzt in $\mathcal{O}_K^\times$ die endliche Untergruppe der endlichen Einheitswurzeln

$$\mu(K) = \{x \in \mathcal{O}_K \mid \text{Es gibt } k \text{ in } \mathbb{N} \text{ mit } x^k = 1\}.$$

Diese Gruppe ist endlich, weil aus $x^k = 1$ folgt, dass $\mathbb{Q}(x)$ in K sitzt, was eine Erweiterung des Grades $\varphi(k)$ ist. In Wahrheit kommen in $\mu(K)$ deshalb nur diejenigen Einheitswurzeln vor, deren Ordnung ein Teiler des Grades n ist.

Mithilfe multiplikativer Minkowski-Theorie werden wir im Folgenden die Gruppen

$$\begin{aligned} \mathcal{O}_K^\times &= \{\varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) \in \{\pm 1\}\}, \\ S &= \{(x) \in K_\mathbb{R}^\times \mid N(x) = \pm 1\}, \\ H &= \{z \in [\prod_\tau \mathbb{R}]^+ \mid \mathrm{Tr}(x) = 0\} \end{aligned}$$

studieren. Die Menge S interpretieren wir als die Hyperfläche der Elemente in $K_\mathbb{R}^\times$, deren Norm 1 beträgt, und H interpretieren wir als die Hyperebene der Elemente mit Spur 0. $(S, \cdot)$ ist eine Untergruppe von $K_\mathbb{R}^\times$ und H ist ein $\mathbb{R}$-Untervektorraum von $[\prod_\tau \mathbb{R}]^+$.

Zu den Mengen S und H halten wir folgendes fest: Ist $x^k = 1$, dann ist $|x| = 1$. Ferner gilt für x mit $x^k = 1$, dass $\tau(x)^k = 1$, sodass x zu $\mu(K)$ gehört. Das bedeutet, dass $\ell(j(x)) = 0$ ist, sodass $\mu(K)$ in $\ker(\ell \circ j)$ enthalten ist.

Als Einschränkung der Morphismen aus dem Diagramm in Bemerkung II.7.3 erhalten wir

$$(\mathcal{O}_K^\times, \cdot) \xrightarrow{j} (S, \cdot) \xrightarrow{\ell} (H, +)$$

als Morphismen von Gruppen. Wir bezeichnen das Bild von $\mathcal{O}_K^\times$ unter $\ell \circ j$ mit Γ. Im Folgenden werden wir sehen, dass Γ ein vollständiges Gitter in H, und damit isomorph zu $\mathbb{Z}^{r+s-1}$, ist.

Proposition II.8.1 (Charakterisierung der Einheitengruppe): *Die Sequenz*

$$1 \longrightarrow \mu(K) \hookrightarrow \mathcal{O}_K^\times \xrightarrow{\ell \circ j} \Gamma \longrightarrow 1$$

ist eine kurze exakte Sequenz.

Beweis: Wir haben die Namen so gewählt, dass nur zu zeigen ist, dass $\mu(K) = \ker(\log|\cdot|)$. Sei also ε eine Einheit von K. Genau dann liegt ε in $\ker(\log|\cdot|)$, wenn für jedes τ aus $\mathcal{H}$ gilt, dass $\log|\tau(\varepsilon)| = 0$, was genau dann eintritt, wenn für jedes τ aus $\mathcal{H}$ gilt: $|\tau(\varepsilon)| = 1$.

„$\subseteq$“: Liegt ε in $\mu(K)$, dann gibt es eine natürliche Zahl k, sodass $\varepsilon^k = 1$, d. h. für alle τ aus $\mathcal{H}$ ist $\tau(\varepsilon)^k = 1$, woraus bereits folgt, dass $|\tau(\varepsilon)| = 1$.

„$\supseteq$“: Gehört ε zu $\ker(\log|\cdot|)$, dann gilt für alle τ aus $\mathcal{H}$, dass $|\tau(\varepsilon)| = 1$. Damit liegt $j(\varepsilon) = (\tau(\varepsilon))_{\tau \in \mathcal{H}}$ in einem beschränkten Bereich in $K_\mathbb{R}$ und ist Gitterpunkt des Gitters $j(\mathcal{O}_K) \subseteq K_\mathbb{R}$. Es gibt deshalb nur endlich viele solcher Punkte, was $\ker(\log|\cdot|)$ endlich macht. Also hat ε endliche Ordnung, und ε gehört zu $\mu(K)$. □

Lemma II.8.2 (Elemente vorgegebener Norm): *Für die natürliche Zahl a setzen wir $M_a = \{a \in \mathcal{O}_K \mid |N_{K|\mathbb{Q}}(\alpha)| = a\}$. Es gilt*

$$|M_a/\!\sim| \leq [\mathcal{O}_K : a\mathcal{O}_K] = N((a)),$$

wobei „$\sim$“ die Assoziiertheitsrelation ist, die durch „$\alpha_1 \sim \alpha_2$ genau dann, wenn es h in $\mathcal{O}_K^\times$ gibt, sodass $\alpha_2 = h\alpha_1$“ erklärt ist. Insbesondere ist $M_a/\!\sim$ endlich.

Beweis: Wir wissen bereits, dass $|\mathcal{O}_K/a\mathcal{O}_K| = [\mathcal{O}_K : a\mathcal{O}_K] = N(a\mathcal{O}_K) < \infty$. Ferner sind in jeder Nebenklasse die Elemente, deren Norm Betrag a hat, assoziiert zueinander.

Gehören nämlich α_1 und α_2 zur selben Nebenklasse, und gilt für ihre Normen $|N_{K|\mathbb{Q}}(\alpha_1)| = |N_{K|\mathbb{Q}}(\alpha_2)| = a$, dann gibt es γ in $\mathcal{O}_K$, sodass $\alpha_2 - \alpha_1 = a\gamma$, und deshalb gilt $\alpha_2/\alpha_1 = 1 + (a/\alpha_1)\gamma = 1 \pm (N(\alpha_1)/\alpha_1)\gamma$.

Das Element $N(\alpha_1)/\alpha_1$ können wir schreiben als $N(\alpha_1)/\alpha_1 = \prod_{\tau\in\mathcal{H}-\{\mathrm{id}\}} \tau(\alpha_1)$, und da alle Faktoren ganz sind, gehört das Produkt sogar zu $\mathcal{O}_K$. Deshalb liegt α_2/α_1 in $\mathcal{O}_K$; genau so behandelt man α_1/α_2. Damit sind α_1 und α_2 assoziiert. Insgesamt folgt die Behauptung. □

Satz 7 (Dirichletscher Einheitensatz): *Die Gruppe Γ aus Proposition II.8.1 ist ein vollständiges Gitter in H. Insbesondere ist H isomorph zu $\mathbb{Z}^{r+s-1}$.*

Beweis: Als erstes zeigen wir, dass Γ ein Gitter ist. Das tun wir, indem wir zeigen, dass Γ eine diskrete Untergruppe in H ist. Für die positive reelle Zahl c setzen wir

$$Q_c = \Big\{(x_\tau)_\tau \in \prod_{\tau\in\mathcal{H}} \mathbb{R} : \text{Für jedes } \tau \text{ in } \mathcal{H} \text{ ist } |x_\tau| \leq c\Big\}.$$

Das Urbild von Q_c unter ℓ ist die Menge

$$\ell^{-1}(Q_c) = \Big\{(z_\tau)_\tau \in \prod_{\tau\in\mathcal{H}} \mathbb{C}^\times : \text{Für alle } \tau \text{ in } \mathcal{H} \text{ ist } |z_\tau| \leq e^c\Big\}$$

und $\ell^{-1}(Q_c) \cap j(\mathcal{O}_K^\times)$ ist endlich, da $j(\mathcal{O}_K^\times)$ ein Gitter ist. Damit ist auch $|Q_c \cap \Gamma|$ endlich.

Als zweiten Schritt wollen wir mithilfe von Proposition II.4.6 zeigen, dass das Gitter Γ vollständig ist. Diese Proposition hat ausgesagt, dass Γ genau dann vollständig ist, wenn es eine beschränkte Teilmenge M von H gibt, sodass $H = \bigcup_{\gamma\in\Gamma} \gamma + M$.

Wir versuchen im Folgenden eine beschränkte Teilmenge T von S zu konstruieren, sodass $S = \bigcup_{\varepsilon\in\mathcal{O}_K^\times} Tj(\varepsilon)$. Haben wir das geschafft, dann setzen wir

$M = \ell(T)$ und erhalten einerseits, dass $H = \bigcup_{\varepsilon\in\mathcal{O}_K^\times} M + \ell(j(\varepsilon)) = \bigcup_{\gamma\in\Gamma} M + \gamma$, da $\ell\colon S \to H$ surjektiv ist, und andererseits, dass M beschränkt ist.

Die Beschränktheit von M sieht man so: Da T beschränkt ist, gibt es eine Konstante $C > 0$, sodass für alle x in T und alle τ in $\mathcal{H}$ gilt, dass $|x_\tau| < C$. Wegen $\prod_{\tau\in\mathcal{H}} |x_\tau| = 1$ gibt es ein $c > 0$, sodass für alle x in T und τ in $\mathcal{H}$ gilt: $|x_\tau| > c$. Aber dann ist $M = \log(T)$ beschränkt in H.

Nun zur Konstruktion von T. Wir wählen einen hinreichend großen vollständigen Quader in $K_\mathbb{R}$, d. h. wir wählen Konstanten $c_\tau > 0$, sodass $c_{\overline{\tau}} = c_\tau$ und $C = \prod_{\tau\in\mathcal{H}} c_\tau > M^{\min}$ und definieren $X = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$.

Wählen wir $y = (y_\tau)_\tau$ in S, dann ist Xy ebenfalls ein Quader, denn $Xy = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_c| < c_\tau|y|\}$ und $\prod_{\tau\in\mathcal{H}} |y_\tau| = |N(y)| = 1$. Insbesondere ist $\prod_{\tau\in\mathcal{H}} c'_\tau = C$.

Nun wählen wir endlich viele $\alpha_1, \ldots, \alpha_N$ in $\mathcal{O}_K$, sodass jedes α in $\mathcal{O}_K - \{0\}$ mit $|N_{K|\mathbb{Q}}(\alpha)| \leq C$ zu einem der α_i assoziiert ist – das können wir nach Lemma II.7.2 tun – und setzen $T = S \cap \bigcup_{i=1}^N Xj|\alpha_i|^{-1}$.

Dass dieses T unseren Wünschen genügt, weisen wir nun nach.

Da X beschränkt ist, ist $Xj|\alpha_i|^{-1}$ beschränkt, und so auch die endliche Vereinigung T dieser Mengen.

Zur Mengengleichheit $S = \bigcup_{\varepsilon\in\mathcal{O}_K^\times} Tj(\varepsilon)$. Sei y in S. Wegen $\prod_{\tau\in\mathcal{H}} c'_\tau = C$ und Proposition II.5.9 gibt es ein α in $\mathcal{O}_K$, sodass $j(\alpha)$ in $Xy^{-1} = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| < c'_\tau\}$ liegt. Das heißt $j(\alpha) = xy^{-1}$ für ein x aus X.

Ferner gilt $|N_{K|\mathbb{Q}}(\alpha)| = |N(xy^{-1})| = |N(x)| < \prod_{\tau\in\mathcal{H}} c_\tau = C$, weshalb α zu einem der α_i assoziiert ist. Es gibt also ein ε in $\mathcal{O}_K^\times$, sodass $\alpha = \varepsilon\alpha_i$ und $y = xj(\alpha)^{-1} = xj(\alpha_i)^{-1}j(\varepsilon)$.

Bleibt zu zeigen, dass $xj(\alpha_i)^{-1}$ zu T gehört. Einerseits liegt $xj(\alpha_i)^{-1}$ in $Xj(\alpha_i)^{-1}$, andererseits folgt, da y und $j(\varepsilon)$ zu S gehören, dass $xj(\alpha_i)^{-1}$ in S liegt. Weil $xj(\alpha_i)^{-1}$ zu T gehört, liegt $y = xj(\alpha_i)^{-1}j(\varepsilon)$ in $Tj(\varepsilon)$. Damit ist alles gezeigt. □

Korollar II.8.3 (Satz von Dirichlet): *Bezeichnen r die Anzahl der reellen- und s die Anzahl der komplexen Einbettungen des algebraischen Zahlkörpers K, dann ist $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \times \mu(K)$.*

Beweis: Zum Beweis des Satzes von Dirichlet verwenden wir die kurze exakte Sequenz

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda=\ell\circ j} \Gamma \cong \mathbb{Z}^{r+s-1} \longrightarrow 1.$$

Wir wählen eine Basis $v_1, \ldots, v_m$ von Γ, $m = r + s - 1$, und Urbilder $\varepsilon_1, \ldots, \varepsilon_m$ in $\mathcal{O}_K^\times$. Bezeichnet $A = \langle\varepsilon_1, \ldots, \varepsilon_m\rangle_\mathbb{Z} \subseteq \mathcal{O}_K^\times$, dann ist $\lambda|_A$ ein Isomorphismus,

es gilt $A \cap \mu(K) = \{1\}$, da $\mu(K) = \ker \lambda$ und die Abbildung

$$A \times \mu(K) \longrightarrow \mathcal{O}_K^\times, \qquad (a, \xi) \longmapsto a\xi$$

ist ein Isomorphismus. Dabei folgt die Injektivität der obigen Abbildung aus der vorangegangenen Bemerkung zum Kern von λ, und die Surjektivität aus Satz 7. □

Beispiel II.8.4 (Quadratische Zahlkörper): (i) Sei K der algebraische Zahlkörper $\mathbb{Q}[\sqrt{7}]$. Mit den Bezeichnungen der vergangenen Abschnitte sind dann $r = 2$ und $s = 0$, sodass $r+s-1 = 1$ und $\Gamma \cong \mathbb{Z}$ gelten. Ferner ist $\mu(K) = \{\pm 1\}$, da ± 1 die einzigen reellen Einheitswurzeln sind, d. h. $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Analog zeigt man: Der Ganzheitsring jedes reell-quadratischen Zahlkörpers hat die Einheitengruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

(ii) Sei K der algebraische Zahlkörper $\mathbb{Q}[\sqrt{-3}]$. Dann sind $r = 0$ und $s = 1$, d. h. $r + s - 1 = 0$. Folglich ist $\Gamma \cong \{0\}$. Außerdem erfüllt eine nicht-reelle dritte Einheitswurzel ξ_3 die Relation $\xi_3^2 + \xi_3 + 1 = 0$, woraus folgt, dass $\xi_3 = -1/2(1 + \sqrt{-3})$, was in K enthalten ist. Damit ist $\mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\xi_3]$ und $\mu(K) = \{\pm 1, \pm\xi_3, \pm\xi_3^2\} \cong \mathbb{Z}/6\mathbb{Z}$. Insgesamt folgt $\mathcal{O}_K^\times \cong \mathbb{Z}/6\mathbb{Z}$.

Wir wollen versuchen, die Ergebnisse des vorherigen Beispiels etwas zu verallgemeinern. Ist D eine quadratfreie natürliche Zahl und ist ξ_k eine k-te Einheitswurzel, die in $\mathbb{Q}[\sqrt{-D}]$ liegt, dann ist $\varphi(k) = 2$, sodass $k = 3, 4$ oder $k = 1, 2$.

Das Argument dafür ist die Euler'sche Phi-Funktion, an deren Werte auf Primzahlpotenzen wir kurz erinnern: Ist p prim, dann ist $\varphi(p) = p - 1$ und $\varphi(p^\ell) = p^\ell - p^{\ell-1} = p^{\ell-1}(p - 1)$. Sind $p \neq q$ prim, dann ist $\varphi(p^a q^b) = \varphi(p^a) - \varphi(p^b)$.

Mit diesen Tatsachen sieht man ein, dass für ξ_3 in $\mathbb{Q}[\sqrt{-D}]$ schon folgen muss, dass $\mathbb{Q}[\xi_3] = \mathbb{Q}[\sqrt{-D}]$; falls i zu $\mathbb{Q}[\sqrt{-D}]$ gehört, folgt bereits $\mathbb{Q}[\mathrm{i}] = \mathbb{Q}[\sqrt{-D}]$.

Bemerkung II.8.5 (Imaginär-quadratische Zahlkörper):

(i) Ist $K = \mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\xi_3]$, dann ist $\mathcal{O}_K^\times \cong \mathbb{Z}/6\mathbb{Z}$.

(ii) Ist $K = \mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[\mathrm{i}]$, dann ist $\mathcal{O}_K^\times \cong \mathbb{Z}/4\mathbb{Z}$.

(iii) Für alle anderen imaginär-quadratischen Zahlkörper gilt $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z}$.

9 Primideale in Ganzheitsringen

Unser Ziel für diesen Abschnitt ist die Beschreibung der Primideale $\widehat{\mathfrak{p}}$ im Ring $\widehat{\mathcal{O}} = \mathcal{O}_K$. Dabei wollen wir intensiv ausnutzen, dass $\widehat{\mathfrak{p}} \cap \mathbb{Z}$ ein Primideal (p) in

$\mathbb{Z}$ ist. Das Erzeugis $\widehat{\mathcal{O}}p$ besitzt eine Primidealzerlegung $\widehat{\mathcal{O}}p = \widehat{\mathfrak{p}}_1^{e_1} \cdots \widehat{\mathfrak{p}}_r^{e_r}$ und wir werden sehen, dass für jedes Primideal $\widehat{\mathfrak{p}}_i$ gilt, dass $\widehat{\mathfrak{p}}_i \cap \mathbb{Z} = (p)$.

Zunächst möchten wir eine etwas allgemeinere Situation betrachten als nur Ganzheitsringe algebraischer Zahlkörper.

Proposition II.9.1: *Seien $\mathcal{O}$ ein Dedekindring, $K = \mathrm{Quot}(\mathcal{O})$ der zugehörige Quotientenkörper, L eine endliche separable Körpererweiterung von K und es bezeichne $\widehat{\mathcal{O}} = \mathrm{Int}_L(\mathcal{O})$ den ganzen Abschluss von $\mathcal{O}$ in L. Dann ist $\widehat{\mathcal{O}}$ selbst ein Dedekindring.*

Beweis: Wir haben uns bereits überlegt, dass L der Quotientenkörper von $\widehat{\mathcal{O}}$ ist, was uns bereits liefert, dass $\widehat{\mathcal{O}}$ ganzabgeschlossen ist.

Nun zu von Null verschiedenen Primidealen in $\widehat{\mathcal{O}}$. Sei $\widehat{\mathfrak{p}}$ ein Primideal von $\widehat{\mathcal{O}}$ und $\mathfrak{p}$ bezeichne $\widehat{\mathfrak{p}} \cap \mathcal{O}$. Weil $\widehat{\mathfrak{p}}$ von Null verschieden war, gibt es ein $x \neq 0$ in $\widehat{\mathfrak{p}}$. Dieses x ist ganz über $\mathcal{O}$, weshalb es Elemente $a_0, \ldots, a_{n-1}$ in $\mathcal{O}$ gibt, sodass $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Ohne Einschränkung dürfen wir annehmen, dass $a_0 \neq 0$ ist, weshalb wir schreiben können $a_0 = -x^n - a_{n-1}x^{n-1} - \cdots - a_1 x$, was in $\widehat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}$ liegt. Das zeigt, dass $\mathfrak{p}$ nicht trivial ist. Da $\mathcal{O}$ ein Dedekindring ist, ist $\mathfrak{p}$ maximal in $\mathcal{O}$. Folglich ist $\mathcal{O}/\mathfrak{p}$ ein Körper und $\mathcal{O}/\mathfrak{p} \hookrightarrow \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ ist eine endliche Erweiterung von $\mathcal{O}/\mathfrak{p}$. Das zeigt, dass $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ ein Körper ist, sodass $\widehat{\mathfrak{p}}$ ein maximales Ideal ist.

Schließlich bleibt zu zeigen, dass $\widehat{\mathcal{O}}$ noethersch ist. Dazu wählen wir eine K-Basis $\{\alpha_1, \ldots, \alpha_n\}$ der Körpererweiterung $L|K$. Da wir Nenner ausräumen können dürfen wir annehmen, dass $\alpha_1, \ldots, \alpha_n$ in $\widehat{\mathcal{O}}$ liegen. Wir bezeichnen mit $d = d(\alpha_1, \ldots, \alpha_n)$ die Diskriminante der Körpererweiterung bezüglich der gewählten Basis. Wegen Proposition II.2.6 ist diese von Null verschieden und nach Korollar II.2.9 ist d ein Element von $\mathcal{O}$.

Satz 1 sagt uns, dass $d\widehat{\mathcal{O}}$ in $\bigoplus_{i=1}^n \mathcal{O}\alpha_i$ enthalten ist. Mit anderen Worten ist $\widehat{\mathcal{O}}$ enthalten in $M = \bigoplus_{i=1}^n \mathcal{O}\frac{\alpha_i}{d}$. Jedes Ideal in $\widehat{\mathcal{O}}$ ist Untermodul eines endlich erzeugten $\mathcal{O}$-Moduls M und da $\mathcal{O}$ noethersch ist, ist M als $\mathcal{O}$-Modul noethersch, sodass I endlich erzeugt ist. Insgesamt folgt, dass $\widehat{\mathcal{O}}$ noethersch ist. □

Im Folgenden setzen wir die Sitation von Propisition II.9.1 voraus.

Definition II.9.2 (Lage von Primidealen): Ist $\widehat{\mathfrak{p}}$ ein nichttriviales Primideal in $\widehat{\mathcal{O}}$, dann ist $\mathfrak{p} = \widehat{\mathfrak{p}} \cap \mathcal{O}$ ein nichttriviales Primideal in $\mathcal{O}$. Wir sagen, $\widehat{\mathfrak{p}}$ *liege über* $\mathfrak{p}$.

Proposition II.9.3 (Die Primideale über einem gegebenen Ideal): *Sei $\mathfrak{p}$ ein von Null verschiedenes Primideal von $\mathcal{O}$. Für das von $\mathfrak{p}$ erzeugte $\mathfrak{p}\widehat{\mathcal{O}}$ in $\widehat{\mathcal{O}}$ gilt:*

(i) $\mathfrak{p}\widehat{\mathcal{O}} \neq \widehat{\mathcal{O}}$.

(ii) *Es gibt endlich viele Primideale* $\widehat{\mathfrak{p}}_1, \ldots, \widehat{\mathfrak{p}}_r$ *und Exponenten* $e_1, \ldots, e_r$, *sodass* $\mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}_1^{e_1} \cdots \widehat{\mathfrak{p}}_r^{e_r}$.

(iii) *Genau dann liegt das Primideal* $\widehat{\mathfrak{p}}$ *in* $\widehat{\mathcal{O}}$ *über* $\mathfrak{p}$, *wenn* $\widehat{\mathfrak{p}} \in \{\widehat{\mathfrak{p}}_1, \ldots, \widehat{\mathfrak{p}}_r\}$.

Beweis: (i) Sei π ein Element von $\mathfrak{p} - \mathfrak{p}^2$. Wegen des Satzes über die eindeutige Primidealzerlegung können wir $\pi\mathcal{O}$ schreiben als $\pi\mathcal{O} = \mathfrak{p}\mathfrak{a}$ für ein Primideal $\mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, da π nicht in $\mathfrak{p}^2$ liegt. Das bedeutet, dass $\mathcal{O} = \mathfrak{p} + \mathfrak{a}$ ist; es gibt also Elemente b von $\mathfrak{p}$ und s in $\mathfrak{a}$, sodass $1 = b + s$. Es ist zu beachten, dass s nicht in $\mathfrak{p}$ liegt, aber $s\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p} = \pi\mathcal{O}$.

Angenommen, $\mathfrak{p}\widehat{\mathcal{O}}$ wäre gleich $\widehat{\mathcal{O}}$. Dann wäre $s\widehat{\mathcal{O}} = s\mathfrak{p}\widehat{\mathcal{O}} \subseteq \pi\widehat{\mathcal{O}}$, sodass $s = \pi x$ für ein x aus $\widehat{\mathcal{O}}$. Da aber s und π in K lägen, müsste auch x in $\widehat{\mathcal{O}} \cap K = \mathcal{O}$ liegen, weshalb s in $\pi\mathcal{O} \subseteq \mathfrak{p}$ folgen müsste, was nicht sein kann.

(ii) Das folgt aus dem Satz über die eindeutige Primidealzerlegung in Dedekindringen.

(iii) „$\Longleftarrow$“: Wir zeigen, dass $\widehat{\mathfrak{p}}_i \cap \mathcal{O} = \mathfrak{p}$.

Per Definition ist $\mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}_1^{e_1} \cdots \widehat{\mathfrak{p}}_r^{e_r} \subseteq \widehat{\mathfrak{p}}_i$, weshalb $\mathfrak{p}$ in $\widehat{\mathfrak{p}}_i \cap \mathcal{O}$ liegt. Weil 1 nicht zu $\widehat{\mathfrak{p}}_i$, und deshalb erst recht nicht zu $\widehat{\mathfrak{p}}_i \cap \mathcal{O}$ gehört, ist $\mathfrak{p} = \widehat{\mathfrak{p}}_i \cap \mathcal{O}$ ein maximales Ideal in $\mathcal{O}$.

„$\Longrightarrow$“: Ist $\widehat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}$, dann ist $\mathfrak{p}\widehat{\mathcal{O}} \subseteq \widehat{\mathfrak{p}}$. Nach II.6.3 wird deshalb $\mathfrak{p}\widehat{\mathcal{O}}$ von $\widehat{\mathfrak{p}}$ geteilt. □

Definition II.9.4: Sei $\mathfrak{p}$ ein von Null verschiedenes Primideal von $\mathcal{O}$ und es sei $\mathfrak{p}\widehat{\mathcal{O}} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ die Primidealzerlegung von $\mathfrak{p}\widehat{\mathcal{O}}$. Für jedes $1 \leq i \leq n$ ist $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i$ eine Körpererweiterung von $\mathcal{O}/\mathfrak{p}$.

(i) Der Exponent e_i heißt *Verzweigungsindex von* $\widehat{\mathfrak{p}}_i$. Ist $e_i = 1$, dann heißt das Ideal $\widehat{\mathfrak{p}}_i$ *unverzweigt*. Ist $e_1 = \cdots = e_r = 1$, und sind die Körpererweiterungen $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i$ von $\mathcal{O}/\mathfrak{p}$ separabel, dann heißt das Ideal $\mathfrak{p}$ *unverzweigt*.

(ii) Der Grad $f_i = [\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i : \mathcal{O}/\mathfrak{p}]$ heißt *Trägheitsgrad* von $\widehat{\mathfrak{p}}_i$.

(iii) Ist $\mathfrak{p}$ unverzweigt und $r = 1$ dann heißt $\mathfrak{p}$ *träge*. Das ist genau dann der Fall, wenn $\mathfrak{p}\widehat{\mathcal{O}}$ ein Primideal ist.

(iv) Ist $r = n = [L : K]$, dann heißt $\mathfrak{p}$ *vollzerlegt*.

(v) Ist $r = 1$, dann heißt $\mathfrak{p}$ *unzerlegt*.

Ist $\widehat{\mathcal{O}}$ ein Ganzheitsring eines Zahlkörpers, dann sind die Separabilitätsforderungen in (i) immer erfüllt, da dann $\mathcal{O}/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ und endliche Körper perfekt sind.

Satz 8 (Verzweigungsformel): *In der Situation von Definition II.9.4 gilt für die Verzweigungsindizes und Trägheitsgrade die Formel* $\sum_{i=1}^{r} e_i f_i = n = [L : K]$.

Beweis: Um die Formel zu zeigen, zeigen wir die Gleichheit $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}} = \bigoplus_{i=1}^{r} \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i^{e_i}$ von $k = \mathcal{O}/\mathfrak{p}$-Vektorräumen.

Wenn wir das gezeigt haben, liefern die Aussagen „$\dim_k \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}} = n$“ und „$\dim_k \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i^{e_i} = e_i f_i$“ die Behauptung.

Zur ersten Behauptung: Wir wählen eine k-Basis $\overline{w}_1, \ldots, \overline{w}_m$ von $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ zusammen mit Urbildern $w_1, \ldots, w_m$ in $\widehat{\mathcal{O}}$. Im Folgenden zeigen wir, dass $w_1, \ldots, w_m$ eine K-Basis von L ist, woraus die Behauptung folgt.

Zuerst zeigen wir die K-lineare Unabhängigkeit. Seien dazu $\alpha_1, \ldots, \alpha_m$ Elemente von K, sodass $\sum_{i=1}^{m} \alpha_i w_i = 0$. Ohne Einschränkung dürfen wir annehmen, dass $\alpha_1, \ldots, \alpha_m$ in $\mathcal{O}$ liegen, da $K = \mathrm{Quot}(\mathcal{O})$ ist. Angenommen, nicht alle α_i wären Null. Dann ist $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ nicht das Nullideal, und wir können das gebrochene Ideal $\mathfrak{a}^{-1}$ in $K = \mathrm{Quot}(\mathcal{O})$ betrachten. Weil $\mathfrak{p}$ ein echtes Ideal von $\mathcal{O}$ ist, ist $\mathfrak{a}^{-1}\mathfrak{p}$ echt enthalten in $\mathfrak{a}^{-1}\mathcal{O} = \mathfrak{a}^{-1}$. Wir finden also c in $\mathfrak{a}^{-1} - \mathfrak{a}^{-1}\mathfrak{p}$, d. h. $c\mathfrak{a} \not\subseteq \mathfrak{p}$. Durchmultiplizieren der Gleichung $\sum_{i=1}^{m} \alpha_i w_i = 0$ liefert $\sum_{i=1}^{m} c\alpha_i w_i = 0$. Per Wahl von c liegt $c\alpha_i$ für $1 \leq i \leq n$ in $\mathcal{O}$, sodass $\sum_{i=1}^{m} \overline{c\alpha_i}\,\overline{w}_i = \overline{0}$ in $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$, wobei die $\overline{c\alpha_i}$ zu $\mathcal{O}/\mathfrak{p} = k$ gehören.

Das heißt wir haben $\overline{c\alpha_1} = \cdots = \overline{c\alpha_m} = \overline{0}$ in $\mathcal{O}/\mathfrak{p}$, da $\overline{w}_1, \ldots, \overline{w}_m$ eine Basis von $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ bilden. Das heißt gerade, dass $c\alpha_1, \ldots, c\alpha_m$ in $\mathfrak{p}$ liegen, d. h. $c\mathfrak{a} = (c\alpha_1, \ldots, c\alpha_m)$ ist in $\mathfrak{p}$ enthalten. Das widerspricht der Wahl von c.

Nun zeigen wir, dass L von $\{w_1, \ldots, w_m\}$ als K-Vektorraum erzeugt wird. Wir definieren $M = \mathcal{O}w_1 + \cdots + \mathcal{O}w_m \subseteq \widehat{\mathcal{O}}$, wobei wir M als $\mathcal{O}$-Modul verstehen.

Wegen $k\overline{w}_1 + \cdots + k\overline{w}_m = \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ ist $\widehat{\mathcal{O}} = M + \mathfrak{p}\widehat{\mathcal{O}}$. Wir schreiben $N = \widehat{\mathcal{O}}/M$ und lesen aus der vorherigen Gleichung ab, dass $N = \mathfrak{p}N$.

Im Beweis von Proposition II.9.1 haben wir mitbewiesen, dass $\widehat{\mathcal{O}}$ ein endlich erzeugter $\mathcal{O}$-Modul ist; damit ist auch N ein endlich erzeugter $\mathcal{O}$-Modul. Wir finden also Elemente $\alpha_1, \ldots, \alpha_s$ in $\mathcal{O}$, sodass $N = \bigoplus_{i=1}^{s} \mathcal{O}\overline{\alpha}_i$. Wegen $N = \mathfrak{p}N$ gibt es für jedes $\overline{\alpha}_i$ Koeffizienten $\alpha_{i,1}, \ldots, \alpha_{i,s}$ in $\mathfrak{p}$, sodass $\overline{\alpha}_i = \sum_j \alpha_{i,j}\overline{\alpha}_j$. Das liefert uns die Matrix $A = (\alpha_{i,j})$ aus $\mathfrak{p}^{s\times s}$ und $A' = A - I$. Dann ist $A'(\overline{\alpha}_1, \ldots, \overline{\alpha}_s)^t = 0$. Wir halten fest, dass $\det A' \equiv \det(-I) = (-1)^s \pmod{p}$, sodass insbesondere $\det A' \neq 0$ gilt. Wir dürfen also mit der Adjunkten arbeiten, d. h.

$$0 = A'^{\#} A' \begin{pmatrix} \overline{\alpha}_1 \\ \vdots \\ \overline{\alpha}_s \end{pmatrix} = d \begin{pmatrix} \overline{\alpha}_1 \\ \vdots \\ \overline{\alpha}_s \end{pmatrix}.$$

Damit ist $dN = 0$, also ist $d\widehat{\mathcal{O}} \subseteq M = \bigoplus_{i=1}^{m} \mathcal{O}w_i$ und $\{w_1, \ldots, w_m\}$ bilden eine K-Basis von L, was wir zeigen wollten. Damit ist die erste Gleichung etabliert.

Nun zeigen wir, dass $\dim_k \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i^{e_i} = e_i f_i$. Dazu betrachten wir die Kette

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i^{e_i} \supseteq \widehat{\mathfrak{p}}_i/\widehat{\mathfrak{p}}_i^{e_i} \supseteq \widehat{\mathfrak{p}}_i^2/\widehat{\mathfrak{p}}_i^{e_i} \supseteq \cdots \supseteq \widehat{\mathfrak{p}}_i^{e_i-1}/\widehat{\mathfrak{p}}_i^{e_i} \supseteq \{0\}$$

von k-Vektorräumen. Wie wir bereits an anderer Stelle gezeigt haben, ist $\widehat{\mathfrak{p}}_i^j/\widehat{\mathfrak{p}}_i^{j+1} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i$. Wegen der eindeutigen Primidealzerlegung finden wir α in $\widehat{\mathfrak{p}}_i^j - \widehat{\mathfrak{p}}_i^{j+1}$ und erhalten den Homomorphismus $\widehat{\mathcal{O}} \to \widehat{\mathfrak{p}}_i^j/\widehat{\mathfrak{p}}_i^{j+1}$, $a \mapsto [\alpha a]$. Dieser ist surjektiv, denn wir haben $\widehat{\mathfrak{p}}_i^{j+1} \subsetneq \widehat{\mathfrak{p}}_i^{j+1} + \widehat{\mathcal{O}}\alpha \subseteq \widehat{\mathfrak{p}}_i^j$, sodass $\widehat{\mathfrak{p}}_j^{j+1} + \widehat{\mathcal{O}}\alpha = \widehat{\mathfrak{p}}_i^j$. Ferner ist der Kern dieses Homomorphismus gerade $\widehat{\mathfrak{p}}^i$, d. h. wir haben mit einem Isomorphismus zu tun. Damit erhalten wir

$$\dim_k \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_k \widehat{\mathfrak{p}}_i^j/\widehat{\mathfrak{p}}_i^{j+1} = e_i \dim_k \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i = e_i f_i.$$

□

10 Primideale in den Gauß'schen Zahlen

Sei K der algebraische Zahlkörper $\mathbb{Q}[\mathrm{i}]$. Wie wir bereits gezeigt haben, ist sein Ganzheitsring $\mathcal{O}_K = \mathbb{Z}[\mathrm{i}]$ der Ring der Gauß'schen Zahlen. Im Folgenden wollen wir die Primideale $\widehat{\mathfrak{p}}$ in $\mathbb{Z}[\mathrm{i}]$ untersuchen.

Ein Primideal im Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptideal, das von einem Primelement p erzeugt wird. Das Ideal $p\mathbb{Z}[\mathrm{i}]$ lässt sich wie wir wissen zerlegen in ein Produkt von Primidealen $p\mathbb{Z}[\mathrm{i}] = \widehat{\mathfrak{p}}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, wobei $2 = \sum_{i=1}^r e_i f_i$ nach Satz 8.

Bemerkung II.10.1 (Mögliche Verzweigungsverhalten): Sei $\widehat{\mathfrak{p}}$ ein Primideal in $\mathbb{Z}[\mathrm{i}]$ und $(p) = \widehat{\mathfrak{p}} \cap \mathbb{Z}$ das Ideal, über dem $\widehat{\mathfrak{p}}$ liegt. Das Ideal $p\mathbb{Z}[\mathrm{i}]$ hat eine Primidealzerlegung $p\mathbb{Z}[\mathrm{i}] = \widehat{\mathfrak{p}}_1^{e_1} \cdots \widehat{\mathfrak{p}}_r^{e_r}$ und nach Satz 8 gilt $\sum_{i=1}^r e_i f_i = 2$, wobei $f_i = [\mathbb{Z}[\mathrm{i}]/\widehat{\mathfrak{p}}_i : \mathbb{Z}/p\mathbb{Z}]$. Dadurch, dass 2 sehr klein ist, gibt es nur wenige mögliche Summen zu unterscheiden, nämlich $1 \cdot 1 + 1 \cdot 1$, $1 \cdot 2$ und $2 \cdot 1$.

Die drei möglichen Fälle sind also

(i) $r = 2$, $e_1 = f_1 = 1$ und $e_2 = f_2 = 1$, sodass $p\mathbb{Z}[\mathrm{i}] = \widehat{\mathfrak{p}}_1\widehat{\mathfrak{p}}_2$ ein vollverzweigtes Ideal ist.

(ii) $r = 1$, $e_1 = 1$ und $f_1 = 2$, sodass $p\mathbb{Z}[\mathrm{i}]$ selbst ein Primideal in $\mathbb{Z}[\mathrm{i}]$ ist; d. h. (p) ist träge.

(iii) $r = 1$, $e_1 = 2$ und $f_1 = 1$, sodass $p\mathbb{Z}[\mathrm{i}] = \widehat{\mathfrak{p}}_1^2$.

Bemerkung II.10.2 (Besonderheiten in $\mathbb{Z}[\mathrm{i}]$): (i) Der Ring der Gauß'schen Zahlen ist ein euklidischer Ring, und damit insbesondere ein Hauptidealring. Insbesondere können wir ein Primideal $\mathfrak{p}$ schreiben als $\mathfrak{p} = (\pi)$ für ein Primelement von $\mathbb{Z}[\mathrm{i}]$.

(ii) Primalität und Irreduzibelität sind in $\mathbb{Z}[\mathrm{i}]$ dasselbe Konzept.

(iii) $\mathrm{Gal}(\mathbb{Q}[\mathrm{i}]|\mathbb{Q}) = \{\mathrm{id}, \sigma\colon a + b\mathrm{i} \mapsto a - b\mathrm{i}\}$.

(iv) Auf $\mathbb{Z}[\mathrm{i}]$ haben wir die Norm $N\colon a + b\mathrm{i} \mapsto a^2 + b^2$, sodass

$$\mathbb{Z}[\mathrm{i}]^\times = \{\alpha \in \mathbb{Z}[\mathrm{i}] \mid N(\alpha) = 1\} = \{\pm 1, \pm \mathrm{i}\}.$$

Insbesondere können wir Gleichheit von Hauptidealen sehr einfach beschreiben. Ein Element $\alpha = a + b\mathrm{i}$ von $\mathbb{Z}[\mathrm{i}]$ ist assoziiert genau zu den Elementen $a + b\mathrm{i}$, $-a - b\mathrm{i}$, $a\mathrm{i} - b$, $-a\mathrm{i} + b$.

Proposition II.10.3 (Träge Primideale): *Sei p eine prime natürliche Zahl. Genau dann ist p prim in $\mathbb{Z}[\mathrm{i}]$, wenn (p) ein träges Ideal in $\mathbb{Z}$ ist. Das ist der Fall genau dann, wenn $p \equiv 3 \pmod 4$ ist.*

Beweis: „$\Longrightarrow$“: Angenommen, $p \not\equiv 3 \pmod 4$. Dann haben wir zwei Fälle zu unterscheiden, nämlich $p = 2$ oder $p \equiv 1 \pmod 4$.

Für $p = 2$ haben wir $(2) = (1 + \mathrm{i})(1 - \mathrm{i})$ und $N(1 + \mathrm{i}) = N(1 - \mathrm{i}) = 2$. Insbesondere sind $1 + \mathrm{i}$ und $1 - \mathrm{i}$ keine Einheiten, weshalb p in diesem Fall nicht prim ist.

Für $p \equiv 1 \pmod 4$ ist p von der Form $p = 1+4n$ für eine geeignete natürliche Zahl n. Nach dem Satz von Wilson gilt für $x = (2n)!$, dass $x^2 \equiv -1 \pmod p$ (was wir später in Proposition II.10.4 zeigen werden). Das bedeutet, dass $p \mid x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$ in $\mathbb{Z}[\mathrm{i}]$ gilt. Aber $p^{-1}(x \pm \mathrm{i}) = x/p \pm \mathrm{i}/p$, was nicht in $\mathbb{Z}[\mathrm{i}]$ liegt, sodass p nicht prim sein kann.

„$\Longleftarrow$“: Angenommen, p wäre nicht prim in $\mathbb{Z}[\mathrm{i}]$. Wir müssen zeigen, dass in diesem Fall $p \not\equiv 3 \pmod 4$ ist.

Da p in $\mathbb{Z}[\mathrm{i}]$ nicht prim ist, können wir p schreiben als $p = (a_1 + b_1\mathrm{i})(a_2 + b_2\mathrm{i})$, wobei $N(a_i + b_i\mathrm{i})$ von 1 verschieden sind. Wegen der Multiplikativität der Norm ist dann $p^2 = N(p) = N(a_1 + b_1\mathrm{i})N(a_2 + b_2\mathrm{i})$, weshalb $N(a_i + b_i\mathrm{i}) = p$ sein muss. Nun ist aber $p = N(a_i + b_i\mathrm{i}) = a_i^2 + b_i^2$. Weil jetzt $a_1^2 + b_1^2 \equiv 0, 1 \pmod 4$ sein muss, kann nur $p \not\equiv 3 \pmod 4$ sein. □

Proposition II.10.4 (Satz von Wilson): *Sei p eine prime natürliche Zahl.*

(i) $(p - 1)! \equiv -1 \pmod p$.

(ii) *Ist p von der Form $p = 1 + 4n$ für eine natürliche Zahl n, dann ist* $(2n)!^2 \equiv -1 \pmod p$.

Beweis: (i) Für $p = 2$ ist alles klar. Wir dürfen deshalb annehmen, dass p eine ungerade Primzahl ist. Wir betrachten das Polynom $X^{p-1} - 1$ in $\mathbb{Z}/p\mathbb{Z}[X]$.

Da $\overline{0}$ keine Nullstelle von $X^{p-1}-1$ ist, aber $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit $p-1$ Einheiten ist, sind alle Klassen $\overline{1},\dots,\overline{p-1}$ Nullstellen von $X^{p-1}-1$, d. h. es gilt

$$X^{p-1}-1=(X-\overline{1})\cdots(X-\overline{p-1}).$$

Der Koeffizient von X^0 ist $-1\equiv(-1)^{p-1}(p-1)!\equiv(p-1)!\pmod p$.

(ii) Aus (i) folgt:

$$\begin{aligned}-1&\equiv(p-1)!\\&\equiv(4n)!\\&\equiv 1\cdots 2n\cdot(p-1)(p-2)\cdots(p-2n)\equiv(-1)^{2n}((2n)!)^2 \pmod p\end{aligned}$$

was wir zeigen wollten. □

Bemerkung II.10.5 (Nicht-träge Primzahlen): (i) Ist $p=2$, dann können wir $2=(1+\mathrm{i})(1-\mathrm{i})$ in $\mathbb{Z}[\mathrm{i}]$ schreiben, d. h. $(2)_{\mathbb{Z}[\mathrm{i}]}=(1+\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}(1-\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}=(1+\mathrm{i})^2_{\mathbb{Z}[\mathrm{i}]}$. Wir haben also $r=1$, $e_1=2$, $f_1=1$.

(ii) Ist $p\equiv 1 \pmod 4$, dann ist p nach Proposition II.10.3 reduzibel. Wir können also schreiben $p=\alpha_1\alpha_2$ für $\alpha_i=a_i+b_i\mathrm{i}$ aus $\mathbb{Z}[\mathrm{i}]$, die keine Einheiten sind. Dann gilt $p^2=N(p)=N(\alpha_1)N(\alpha_2)$, sodass

$$N(\alpha_1)=p=N(\alpha_2)=a_1^2+b_1^2=(a_1+b_1\mathrm{i})(a_1-b_1\mathrm{i}).$$

Nach Bemerkung II.10.2 sind $a_1+b_1\mathrm{i}$ und $a_2+b_2\mathrm{i}$ nicht assoziiert, weshalb $(p)_{\mathbb{Z}[\mathrm{i}]}=(a_1+b_1\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}(a_1-b_1\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}$. Deshalb ist $r=2$, $e_1=f_1=1$, $e_2=f_2=1$ und das Ideal $p\mathbb{Z}[\mathrm{i}]$ ist vollverzweigt.

Ohne Einschränkung dürfen wir annehmen, dass $a_1>|b_1|>0$, denn das können wir durch Multiplikation mit einer Einheit erreichen.

Proposition II.10.6 (Charakterisierung der Primideale in $\mathbb{Z}[\mathrm{i}]$): *Der Ring der Gauß'schen Zahlen $\mathbb{Z}[\mathrm{i}]$ hat genau die folgenden nichttrivialen Primideale:*

(i) *Über $(p)=(2)$ liegt $(1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$. Hierbei sind $(2)_{\mathbb{Z}[\mathrm{i}]}=(1+\mathrm{i})^2_{\mathbb{Z}[\mathrm{i}]}$, $r=1$, $e_1=2$, $f_1=1$. Wir haben $\mathbb{Z}/2\mathbb{Z}\cong\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})\mathbb{Z}[\mathrm{i}]$.*

(ii) *Über (p) mit $p\equiv 1 \pmod 4$ liegen Ideale $(a+b\mathrm{i})\mathbb{Z}[\mathrm{i}]$ und $(a-b\mathrm{i})\mathbb{Z}[\mathrm{i}]$ mit a^2+b^2p und $a>|b|>0$. Hierbei ist $(p)_{\mathbb{Z}[\mathrm{i}]}=(a+b\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}(a-b\mathrm{i})_{\mathbb{Z}[\mathrm{i}]}$, $r=2$, $e_1=e_2=f_1=f_2=1$; $(p)_{\mathbb{Z}[\mathrm{i}]}$ ist vollzerlegt und $\mathbb{Z}/p\mathbb{Z}\cong\mathbb{Z}[\mathrm{i}]/(a+b\mathrm{i})\mathbb{Z}[\mathrm{i}]$.*

(iii) *Über (p) mit $p\equiv 3 \pmod 4$ liegt $(p)\mathbb{Z}[\mathrm{i}]$, d. h. es sind $r=1$, $e_1=1$ und $f_1=2$, (p) ist träge, und $\mathbb{Z}/p\mathbb{Z}\hookrightarrow\mathbb{Z}[\mathrm{i}]/p\mathbb{Z}[\mathrm{i}]$ ist eine Grad-2-Erweiterung, sodass $\mathbb{Z}[\mathrm{i}]/p\mathbb{Z}[\mathrm{i}]\cong\mathbb{F}_{p^2}$.*

Erinnerung II.10.7 (Spektrum eines Rings): Sei R ein kommutativer unitärer Ring. Dann heißt

$$\operatorname{Spec} R = \{\mathfrak{p} \text{ Primideal in } R\}$$

das *Spektrum von R.*

Beispiel II.10.8: (i) Ist R der Ring der ganzen Zahlen $\mathbb{Z}$, dann ist $\operatorname{Spec} R = \{(p) \mid p \text{ ist natürliche Primzahl}\} \cup \{0\}$.

(ii) Ist R der Polynomring $\mathbb{C}[X]$, dann ist $\operatorname{Spec} R = \{(X-a) \mid a \in \mathbb{C}\} \cup \{(0)\}$, da $\mathbb{C}$ algebraisch abgeschlossen sind und da in Hauptidealringen Primalität und Irreduzibelität übereinstimmen.

(iii) Ist R der Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$, dann ist

$$\begin{aligned}\operatorname{Spec} R = \{&(1+\mathrm{i})\} \\ &\cup \{(a+b\mathrm{i}) \mid a^2+b^2 \equiv 1 \pmod 4, a > |b| > 0\} \\ &\cup \{(a-b\mathrm{i}) \mid a^2+b^2 \equiv 1 \pmod 4, a > |b| > 0\} \\ &\cup \{(p) \mid p \in \mathbb{N} \text{ prim}, p \equiv 3 \pmod 4\}\end{aligned}$$

wie wir gerade gezeigt haben.

Korollar II.10.9 (Zwei-Quadrate-Satz):

(i) *Sei p aus $\mathbb{N}$ eine Primzahl. Genau dann gibt es zwei ganze Zahlen a und b, sodass $p = a^2 + b^2$, wenn $p \not\equiv 3 \pmod 4$.*

(ii) *Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{\nu_{p_1}(n)} \cdots p_r^{\nu_r(n)}$ für nichtnegative Exponenten $\nu_{p_i}(n)$. Genau dann gibt es ganze Zahlen a und b mit $n = a^2 + b^2$, wenn die $\nu_p(n)$ für all diejenigen p mit $p \equiv 3 \pmod 4$ gerade sind.*

Beweis: (i) „$\Longrightarrow$“: Ist $p = a^2+b^2$, dann ist $p = (a+b\mathrm{i})(a-b\mathrm{i}) = \pi_1\pi_2$, wobei $N(\pi_1) = a^2+b^2 = p = N(\pi_2)$. Das bedeutet, dass p in $\mathbb{Z}[\mathrm{i}]$ nicht prim ist. Nach Proposition II.10.6 muss deshalb $p \not\equiv 3 \pmod 4$ gelten.

Alternativ kann man darüber argumentieren, dass $a^2 + b^2 \equiv 0, 1 \pmod 4$. „$\Longleftarrow$“: Wie in Bemerkung II.10.5.

(ii) „$\Longleftarrow$“: Um die Notation zu vereinfachen schreiben wir $k_i = \nu_{p_i(n)}$. Ohne Einschränkung können wir annehmen, dass $p_1, \ldots, p_s \not\equiv 3 \pmod 4$ und dass $p_{s+1}, \ldots, p_r \equiv 3 \pmod 4$. Das bedeutet wir dürfen annehmen, dass $k_{s+j} = 2k'_{s+j}$ für $1 \le j \le \ell$. Deshalb ist $n = p_1^{k_1} \cdots p_s^{k_s} p_{s+1}^{2k'_{s+1}} \cdots p_r^{2k'_r}$.

Für $1 \leq j \leq s$ können wir $p_j = (a_j + b_j\mathrm{i})(a_j - bj\mathrm{i})$ schreiben. Sei α die Gaußsche Zahl $\prod_{j=1}^{s}(a_j + b_j\mathrm{i}) \prod_{j=1}^{r-s} p_{s+j}^{k'_{s+j}}$. Für $1 \leq j \leq s$ ist $N(a_j + b_j\mathrm{i}) = p_j$ und für $s+1 \leq j \leq r$ ist $N(p_j^{k'_j}) = (p_j^{k'_j})^2 = p_j^{k_j}$ und da die Norm multiplikativ ist, haben wir $N(\alpha) = p_1^{k_1} \cdots p_r^{k_r} = n$. Weil α zu $\mathbb{Z}[\mathrm{i}]$ gehört, gibt es ganze Zahlen a und b, sodass $\alpha = a + b\mathrm{i}$, d. h. $N(\alpha) = a^2 + b^2$.

„$\Longrightarrow$“: Seien $n = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i})$ und p eine natürliche Zahl, sodass $p \equiv 3 \pmod 4$. Dann ist p auch in $\mathbb{Z}[\mathrm{i}]$ prim. In $\mathbb{Z}[\mathrm{i}]$ gibt es eine Primfaktorzerlegung von n und für den nichttrivialen Automorphismus σ in $\mathrm{Gal}(\mathbb{Z}[\mathrm{i}])$ gilt $\sigma(a + b\mathrm{i}) = a - b\mathrm{i}$ sowie $\sigma(p) = p$. Wird also $a + b\mathrm{i}$ von p^k geteilt, dann auch $a - b\mathrm{i}$ und wir sind fertig. □

11 Affiner Koordinatenring

In diesem Abschnitt möchten wir ein anderes Beispiel für das Setting in Abschnitt 9 sehen.

Proposition II.11.1 (Polynomring als Dedekindring): *Sei k ein Körper. Dann ist $k[X]$ ein Dedekindring.*

Beweis: Es bezeichne R den Ring $k[X]$. Weil R ein Hauptidealring ist, ist natürlich jedes Ideal endlich erzeugt. Dass R ein Integritätsring ist, ist klar. Sei nun $(a) = \mathfrak{p}$ ein nichttriviales Primideal, das in einem Primideal $\mathfrak{q} = (b)$ enthalten ist. Weil $k[X]$ ein Hauptidealring ist, ist a zum Einen irreduzibel und zum Anderen wegen der Inklusion ein Vielfaches $a = rb$ für irgendein r aus $k[X]$, d. h. r ist eine Einheit und $\mathfrak{p} = \mathfrak{q}$. Insbesondere ist jedes nichttriviale Primideal maximal. Schließlich sagt uns Bemerkung II.1.6, dass $k[X]$ als faktorieller Ring ganzabgeschlossen ist. □

Bemerkung II.11.2: Allgemeiner sind Hauptidealringe genau die faktoriellen Dedekindringe. Die Richtung „$\Longrightarrow$“ ist genau der obige Beweis, die Richtung „$\Longleftarrow$“ ist Bemerkung II.3.21.

Bemerkung II.11.3: Der Quotientenkörper der Polynomrings $k[X]$ ist der sogenannte Körper der rationalen Funktionen

$$\mathbb{C}(X) = \mathrm{Quot}(k[X]) = \left\{ \frac{f}{g} : f, g \in K[X], q \neq 0 \right\}.$$

Im Folgenden nehmen wir an, dass k der Körper der komplexen Zahlen $\mathbb{C}$ ist.

Bemerkung II.11.4: Wir betrachten die Polynomringe $\mathbb{C}[Y]$, $\mathbb{C}[Z]$ und den Ringhomomorphismus $\varphi\colon \mathbb{C}[Y] \to \mathbb{C}[Z]$, $Y \mapsto Z^3$. Dieser ist injektiv, weshalb wir $\mathcal{O} = \mathbb{C}[Y]$ vermöge φ als Teilring von $\widehat{\mathcal{O}} = \mathbb{C}[Z]$ auffassen können.

Ferner induziert der Ringhomomorphismus φ einen Körperhomomorphismsu der Quotientenkörper $\widehat{\varphi}\colon K = \mathbb{C}(X) \to L = \mathbb{C}(Z)$. Das erlaubt uns, L als Körpererweiterung von K aufzufassen. L hat Grad 3 über K, genauer ist $L = K(\alpha)$ für $\alpha = Z$ und das Minimalpolynom f_α von α ist $f_\alpha = X^3 - Y$, was wir mithilfe einer primitiven dritte Einheitswurzel ζ_3 schreiben können als $(X - Z)(X - \zeta_3 Z)(X - \zeta_3^2 Z)$.

Insbesondere gilt in unserem Setting $\widehat{\mathcal{O}} = \mathbb{C}[Z] = \mathrm{Int}_L(\mathcal{O})$.

Setting II.11.5: In diesem Abschnitt betrachten wir das folgende Setting:

$$\begin{array}{ccc} \widehat{\mathcal{O}} = \mathrm{Int}_L(\mathcal{O}) = \mathbb{C}[Z] & \hookrightarrow & \mathrm{Quot}(\widehat{\mathcal{O}}) = \mathbb{C}(Z) = L \\ \uparrow & & \uparrow 3 \\ \mathcal{O} = \mathbb{C}[Y] & \hookrightarrow & \mathrm{Quot}(\mathcal{O}) = \mathbb{C}(Y) = K \end{array}$$

Wir fragen uns, welche Primideale $\widehat{\mathfrak{p}}$ in $\widehat{\mathcal{O}}$ über dem Primideal $\mathfrak{p} = (X - c)$ in $\mathcal{O}$ liegen.

Bemerkung II.11.6: In Setting II.11.5 gilt: Über $\mathfrak{p} = (Y - c) = (Z^3 - c)$ liegen, falls $c \neq 0$ ist, die Primideale $(Z - \sqrt[3]{c})$, $(Z - \zeta_3\sqrt{3}[c])$ und $(Z - \zeta_3^2\sqrt[3]{c})$. In diesem Fall gilt für die Verzweigungs- und Trägheitsindizes $e_i = 1 = f_i$.

Ist $c = 0$, dann ist $\mathfrak{p} = (Y) = (Z)^3$, und darüber liegt nur das Primideal $\widehat{\mathfrak{p}} = (Z)$, wobei $e_1 = 3$ und $f_1 = 1$.

Beispiel II.11.7 (Grad-3-Morphismus auf affiner Gerade): Sei p die Polynomfunkktion $p\colon \mathbb{C} \to \mathbb{C}$, $x \mapsto x^3$. Ist $c \neq 0$, dann hat c die drei Urbilder $\sqrt[3]{c}$, $\sqrt[3]{c}\zeta_3$ und $\sqrt[3]{c}\zeta_3^2$, wobei $\sqrt[3]{c}$ irgendeine Lösung der Gleichung $X^3 - c = 0$ meint. Nur $c = 0$ hat das einzige Urbild 0.

Für $c \neq 0$ gibt es eine Umgebung V von c, sodass $p^{-1}(V)$ aus drei Zusammenhangskomponenten U_1, U_2 und U_3 besteht, die jeweils vermöge p homöomorph zu V sind. Das bedeutet, dass p auf $\mathbb{C} - \{0\}$ (topologisch) unverzweigt ist.

Für $c = 0$ gibt es eine Umgebung V von p, sodass $p|_{p^{-1}(V)}\colon p^{-1}(V) \to V$ eine 3:1-Abbildung ist.

Bemerkung II.11.8: Beispiel II.11.7 kann algebraisch so interpretiert werden: $\mathbb{C}[Z] = \{p\colon \mathbb{C} \to \mathbb{C}$ Polynomfunktion$\}$ ist die $\mathbb{C}$-Algebra der sogenannten *regulären Funktionen*. Für die Varietät $V = \mathbb{C}$ schreibt man die zugehörige Algebra der regulären Funktionen ab und an auch als $\mathbb{C}[V]$.

Man nennt $\mathrm{Spec}^{\max}(\mathbb{C}[Z]) = \{m \trianglelefteq \mathbb{C}[Z] \text{ maximal}\} = \{(X-c) \mid c \in \mathbb{C}\}$ das maximale Spektrum von $\mathbb{C}[Z]$. Die maximalen Ideale des Koordinatenrings entsprechen bijektiv den Punkten der Varietät.

Der surjektive Morphismus $p\colon V_1 = \mathbb{C} \to V_2 = \mathbb{C}$, $z \mapsto z^3$ induziert einen injektiven Ringhomomorphismus $p^*\colon \mathbb{C}[V_2] = \mathbb{C}[Y] \to \mathbb{C}[V_1] = \mathbb{C}[Z]$, $f \mapsto f \circ p$, den *Pullback längs p*. Wir haben gerade $p^*(Y) = Z^3$, es handelt sich bei diesem Pullback also um unsere ursprüngliche Einbettung.

Der Pullback p^* induziert die Abbildung $\mathrm{Spec}^{\max}\mathbb{C}[V_1] \to \mathrm{Spec}^{\max}\mathbb{C}[V_2]$, $\mathfrak{m} \mapsto (p^*)^{-1}(\mathfrak{m})$ auf den maximalen Idealen der beteiligten Ringe. Im Allgemeinen wird man keine Abbildung auf maximalen Idealen Idealen erhalten; hier geht entscheidend ein, dass wir mit Dedekindringen zutun haben.

Wir halten die wichtigsten Informationen nochmal in einer Zusammenfassung fest:

- p^* ist genau unsere Einbettung aus Setting II.11.5.
- Die verschiedenen Verzweigungsbegriffe passen in dieser Situation zusammen.

Für irreduzible glatte affine Kurven über $\mathbb{C}$ ist der Koordinatenring immer ein Dedekindring und man kann analog vorgehen.

Als Vorbereitung für Abschnitt 12 möchten wir uns mit der Frage beschäftigen, was mit dem Spektrum eines Rings beim Bilden von Quotienten geschieht.

Weiterhin gilt unsere Generalvoraussetzung an Ringe, kommutativ zu sein und eine Eins zu haben.

Proposition II.11.9: *Seien R und S Ringe und $\varphi\colon R \to S$ ein Homomorphismus.*

(i) *Ist $\mathfrak{q}$ ein Primideal in S, dann ist $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ ein Primideal in R.*

(ii) *Ist φ surjektiv und ist $\mathfrak{p}$ ein Primideal in R, das den Kern von φ enthält, dann ist $\mathfrak{q} = \varphi(\mathfrak{p})$ ein Primideal in S.*

Beweis: (i) Urbilder von Idealen sind Ideale. Bleibt zu zeigen, dass $\mathfrak{p}$ prim ist, d. h. es bleibt zu zeigen, dass für ein Produkt ab, das in $\mathfrak{p}$ liegt, folgen muss, dass a oder b in $\mathfrak{p}$ enthalten ist. Ist ab in $\mathfrak{p}$, dann liegt $\varphi(ab)$ in $\mathfrak{q}$. Wegen der Primalität von $\mathfrak{q}$ dürfen wir ohne Einschränkung annehmen, dass $\varphi(a)$ in $\mathfrak{q}$ liegt, d. h. a ist in $\mathfrak{p}$ enthalten.

(ii) Wir wissen bereits: Ist φ surjektiv, dann sind auch Bilder von Idealen Ideale. Seien also nun s_1, s_2 Elemente von S, sodass ab in $\mathfrak{q}$ enthalten ist. Weil φ surjektiv ist, gibt es r_1, r_2 in R, sodass $\varphi(r_i) = s_i$. Damit gilt $\varphi(r_1 r_2) = \varphi(s_1 s_2)$. Deshalb liegt $r_1 r_2$ in $\varphi^{-1}(\varphi(\mathfrak{p}))$ und da $\ker\varphi$ in $\mathfrak{p}$ enthalten ist, gilt sogar $\varphi^{-1}(\varphi(\mathfrak{p})) = \mathfrak{p}$. Ohne Einschränkung liegt a in $\mathfrak{p}$ und damit $\varphi(a)$ in $\mathfrak{q}$. □

Beispiel II.11.10 (Gegenanzeige): (i) Seien $R = \mathbb{Z}$, $S = \mathbb{Q}$ und $\iota\colon \mathbb{Z} \to \mathbb{Q}$, $z \mapsto z/1$ die kanonische Einbettung. Dann ist $\varphi(\mathbb{Z})$ kein Ideal in $\mathbb{Q}$. Allgemeiner ist $\iota(a\mathbb{Z})$ kein Ideal von $\mathbb{Q}$, wenn a eine von Null verschiedene ganze Zahl ist.

(ii) Ist $R = \mathbb{Z}$, $S = \mathbb{Z}/4\mathbb{Z}$ und $\varphi\colon \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ die kanonische Projektion. Dann ist $\mathfrak{p} = 3\mathbb{Z}$ ein Primdideal in $\mathbb{Z}$, aber $\varphi(\mathfrak{p}) = \mathbb{Z}/4\mathbb{Z}$ ist kein Primideal.

Korollar II.11.11 (Induzierte Abbildung auf Spektren): *In der Situation von Proposition II.11.9 gilt: Schreiben wir*

$$\mathrm{Spec}_S(R) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \ker\varphi \subseteq \mathfrak{p}\},$$

dann induziert der Ringhomomorphismus $\varphi\colon R \to S$ die Abbildung (von Mengen) $\varphi^*\colon \mathrm{Spec}(S) \to \mathrm{Spec}_S(R)$, $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$. Ist φ surjektiv, dann ist φ^* eine Bijektion. In diesem Fall ist $\varphi_*\colon \mathfrak{p} \mapsto \varphi(\mathfrak{p})$ die Umkehrabbildung.

12 Primideale für einfache Körpererweiterungen

In diesem Abschnitt möchten wir das folgende Setting untersuchen und Primideale berechnen.

Setting II.12.1: Seien $\mathcal{O}$ ein Dedekindring, K der Quotientenkörper von $\mathcal{O}$, L eine separable Körpererweiterung von K vom Grad n und θ ein primitives Element für die Erweiterung, das in $\widehat{\mathcal{O}} = \mathrm{Int}_L(\mathcal{O})$ liegt, d. h. $L = K(\theta)$. Schließlich bezeichne $\widehat{\mathcal{O}}' = \mathcal{O}[\theta] \subseteq \widehat{\mathcal{O}}$.

Unser Ziel ist es also, Primideale in $\widehat{\mathcal{O}}$ unter Verwendung von $\widehat{\mathcal{O}}'$ zu bestimmen. Dazu ist es zielführend, das größte Ideal $\mathfrak{F}$ in $\widehat{\mathcal{O}}$ zu betrachten, das in $\widehat{\mathcal{O}}'$ liegt.

Definition II.12.2 (Konduktor/Führer): In der beschriebenen Situation bezeichne $\mathfrak{F} = \{\alpha \in \widehat{\mathcal{O}} \mid \alpha\widehat{\mathcal{O}} \subseteq \widehat{\mathcal{O}}'\}$. Dabei handelt es sich um ein nichttriviales Ideal von $\widehat{\mathcal{O}}$, das *Konduktor* oder *Führer* von $\widehat{\mathcal{O}}'$ in $\widehat{\mathcal{O}}$ genannt wird.

Achtung, der Konduktor hängt ab vom gewählten primitiven Element.

Bemerkung II.12.3: Dass $\mathfrak{F}$ tatsächlich ein Ideal ist, wird als Übungsaufgabe zu zeigen sein; genau so, dass es sich bei $\mathfrak{F}$ um das größte Ideal von $\widehat{\mathcal{O}}$ handelt, das im Unterring $\widehat{\mathcal{O}}'$ liegt. Ist $\widehat{\mathcal{O}} = \widehat{\mathcal{O}}'$, dann ist $\mathfrak{F} = \widehat{\mathcal{O}}' = \widehat{\mathcal{O}}$.

Satz 9 (Beschreibung der Primideale in $\widehat{\mathcal{O}}$): *In Setting II.12.1 seien g in $\mathcal{O}[X]$ das Minimalpolynom des primitiven Elements θ, $\mathfrak{p}$ ein Primideal in $\mathcal{O}$ und $k = \mathcal{O}/\mathfrak{p}$, sowie $\overline{g}$ das Bild von g in $k[X]$ unter der kanonischen Projektion*

$\mathcal{O}[X] \to k[X]$. *Sei* $\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$ *die Primfaktorzerlegung von* $\overline{g}$ *in* $k[X]$ *und seien* g_i *normierte Urbilder der* $\overline{g}_i$. *Ist* $\mathfrak{p}$ *koprim zu* $\mathfrak{F} \cap \mathcal{O}$, *was bedeutet, dass* $\mathfrak{p} + (\mathfrak{F} \cap \mathcal{O}) = \mathcal{O}$, *dann erhalten wir die Primideale* $\widehat{\mathfrak{p}}_i$ *über* $\mathfrak{p}$ *durch*

$$\widehat{\mathfrak{p}}_i = \mathfrak{p}\widehat{\mathcal{O}} + g_i(\theta)\widehat{\mathcal{O}} \qquad (1 \le i \le r)$$

Dabei sind $f_i = \deg(\overline{g}_i)$ *die Trägheitsgrade und die* e_i *die Verzweigungsindizes.*

Beispiel II.12.4: Seien $\mathcal{O} = \mathbb{Z}$, $\widehat{\mathcal{O}} = \mathbb{Z}[\mathrm{i}]$ und $\theta = \mathrm{i}$. Dann ist $g = g_i = X^2 + 1$ und $\widehat{\mathcal{O}} = \widehat{\mathcal{O}}' = \mathfrak{F} = \mathbb{Z}[\mathrm{i}]$, d. h. jedes Primideal $\mathfrak{p}$ ist koprim zu $\mathfrak{F} \cap \mathcal{O}$ und die Voraussetzungen von Satz 9 damit erfüllt.

Seien p eine natürliche Primzahl und $\overline{g} = X^2 + 1$ das Bild von g in $\mathbb{Z}/p\mathbb{Z}[X]$. Dann gilt:

(i) Ist $p = 2$, dann ist $\overline{g} = X^2 + 1 = (X-1)^2$, d. h. $r = 1$ und $g_1 = X - 1$. Nach Satz 9 liegt $\widehat{\mathfrak{p}}_1 = 2\mathbb{Z}[\mathrm{i}] + (\mathrm{i}-1)\mathbb{Z}[\mathrm{i}] = (\mathrm{i}-1)\mathbb{Z}[\mathrm{i}]$ über 2 mit Trägheitsgrad $f_1 = 1$ und $e_1 = 2$.

(ii) Ist $p \equiv 1 \pmod 4$, dann ist p von der Form $4k + 1$ für eine natürliche Zahl k. Nach dem Satz von Wilson hat $\overline{g} = X^2 + 1$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$; nämlich $\overline{a} = \overline{(2k)!}$. Deshalb gilt $\overline{g} = X^2 + 1 = (X - \overline{a})(X + \overline{a})$. Nach Satz 9 liegen über $\mathfrak{p}$ die zwei Primideale

$$\widehat{\mathfrak{p}}_1 = p\mathbb{Z}[\mathrm{i}] + (\mathrm{i} - a)\mathbb{Z}[\mathrm{i}], \qquad \widehat{\mathfrak{p}}_2 = p\mathbb{Z}[\mathrm{i}] + (\mathrm{i} + a)\mathbb{Z}[\mathrm{i}]$$

(iii) Ist $p \equiv 3 \pmod 4$, dann hat $\overline{g} = X^2 + 1$ keine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$. Damit ist $\overline{g}$ persönlich prim in $\mathbb{Z}/p\mathbb{Z}[X]$. Aus Satz 9 folgt wieder: Über $\mathfrak{p}$ liegt das Primideal $\widehat{\mathfrak{p}}_1 = p\mathbb{Z}[\mathrm{i}] + \mathcal{O}\mathbb{Z}[\mathrm{i}] = p\mathbb{Z}[\mathrm{i}]$. In diesem Fall sind $f_1 = 2$ und $e_1 = 1$.

Diese Ergebnisse passen mit den Ergebnissen aus Abschnitt 10 zusammen.

Beweis: Wir möchten die Primideale $\widehat{\mathfrak{p}}$ bestimmen, die in $\widehat{\mathcal{O}}_i$ über $\mathfrak{p}$ liegen. Nach Korollar II.11.11 angewendet auf den surjektiven Homomorphismus $\pi\colon \widehat{\mathcal{O}} \to \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ steht $\operatorname{Spec}\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ in 1 : 1-Beziehung zu denjenigen Primidealen $\widehat{\mathfrak{p}}$ aus $\operatorname{Spec}\mathcal{O}$, für die $\mathfrak{p}\widehat{\mathcal{O}} \subseteq \widehat{\mathfrak{p}}$, was genau die Menge der $\widehat{\mathfrak{p}}$ aus $\operatorname{Spec}(\widehat{\mathcal{O}})$ sind, für die $\widehat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}$.

Wir zeigen im Folgenden die Isomorphien $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}} \cong \widehat{\mathcal{O}}'/\mathfrak{p}\widehat{\mathcal{O}}' \cong k[X]/(\overline{g})$ von k-Algebren.

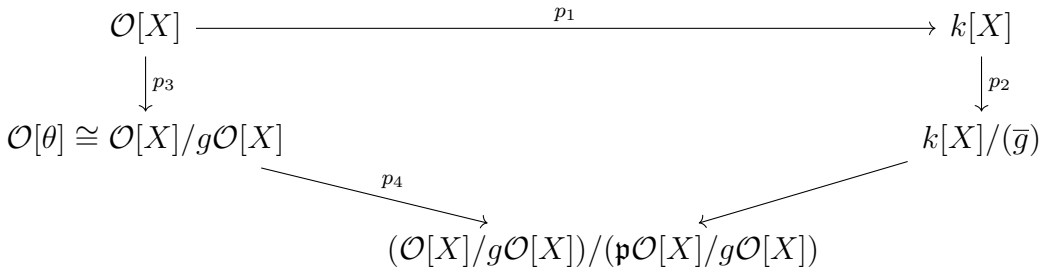
Zuerst zeigen wir $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}} \cong \widehat{\mathcal{O}}'/\mathfrak{p}\widehat{\mathcal{O}}'$. Die Einbettung $\widehat{\mathcal{O}}' \hookrightarrow \widehat{\mathcal{O}}$ induziert den Homomorphismus $\varphi\colon \mathcal{O}[\theta] = \widehat{\mathcal{O}}' \to \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$.

Weil $\mathfrak{F} \cap \mathcal{O}$ und $\mathfrak{p}$ koprim sind, gibt es a aus $\mathfrak{F} \cap \mathcal{O}$ und p aus $\mathfrak{p}$, sodass $1 = a + p$. Insbesondere ist $\mathfrak{p}\widehat{\mathcal{O}} + \mathfrak{F} = \widehat{\mathcal{O}}$. Wegen $\mathfrak{F} \subseteq \widehat{\mathcal{O}}'$ haben wir sogar $\mathfrak{p}\widehat{\mathcal{O}} + \widehat{\mathcal{O}}' = \widehat{\mathcal{O}}$. Das bedeutet, dass φ surjektiv ist.

Nun zur Injektivität: Dass $\mathfrak{p}\widehat{\mathcal{O}}$ in $\ker\varphi$ enthalten ist, ist klar.

Andererseits ist $\ker\varphi = \widehat{\mathcal{O}}' \cap \mathfrak{p}\widehat{\mathcal{O}}$. Da $\mathfrak{F} \cap \mathcal{O}$ und $\mathfrak{p}$ koprim sind, finden wir wieder p in $\mathfrak{p}$ und a in $\mathfrak{F} \cap \mathcal{O}$, sodass $1 = p + a$. Für ein x aus $\ker\varphi = \widehat{\mathcal{O}}' \cap \mathfrak{p}\widehat{\mathcal{O}}$ haben wir $x = 1x = px + ax$, wobei px in $\mathfrak{p}\widehat{\mathcal{O}}'$. Außerdem liegt auch ax in $\mathfrak{p}\widehat{\mathcal{O}}'$ in $\mathfrak{p}\widehat{\mathcal{O}}'$ wegen der Eigenschaft des Führers. Damit ist φ auch injektiv und die erste Isomorphie ist etabliert.

Als zweites zeigen wir $\widehat{\mathcal{O}}'/\mathfrak{p}\widehat{\mathcal{O}}' \cong k[X]/(\overline{g})$. Wir erinnern daran, wie wir die Namen gewählt haben; es waren nämlich $\widehat{\mathcal{O}}' = \mathcal{O}[\theta]$ und $k = \mathcal{O}/\mathfrak{p}$. Wir sind in der Situation



und wir haben $\ker p_2 \circ p_1 = (g, \mathfrak{p})$ sowie $\ker(p_4 \circ p_3) = (g, \mathfrak{p})$. Nach dem zweiten Isomorphiesatz gilt $(\mathcal{O}[X]/g\mathcal{O}[X])/(\mathfrak{p}\mathcal{O}[X]/g\mathcal{O}[X]) \cong \mathcal{O}[\theta]/\mathfrak{p}\mathcal{O}[\theta] = \widehat{\mathcal{O}}'/\mathfrak{p}\widehat{\mathcal{O}}'$. Die beiden etablierten Isomorphismen zeigen nun, dass

$$k[X]/(\overline{g}) \longrightarrow \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}, \qquad [\overline{h}] \longmapsto [h(\theta)]$$

ein Isomorphismus ist.

Als Nächstes möchten wir das Spektrum des Rings $R_1 = k[X]/(\overline{g})$ bestimmen. Im Hauptidealring $k[X]$ hat $\overline{g}$ per Voraussetzung die Primfaktorzerlegung $\overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$. Wir haben die surjektive kanonische Projektion $k[X] \to k[X]/(\overline{g})$. Nach Korollar II.11.11 haben wir erstens

$$\operatorname{Spec} R_1 \longleftrightarrow \{\mathfrak{p} \in \operatorname{Spec}(k[X]) \mid \overline{g} \in \mathfrak{p}\} = \{(\overline{g}_1), \ldots, (\overline{g}_r)\},$$

sodass $\operatorname{Spec} R_1 = \{([\overline{g}_1]), \ldots, ([\overline{g}_r])\}$. Zweitens ist

$$R_1/([\overline{g}_i]) = k[X]/(\overline{g})/[\overline{g}_i]k[X]/(\overline{g}) = k[X]/\overline{g}_i k[X]$$

ein k-Vektorraum der Dimension $\deg \overline{g}_i$. Insgesamt ist $R_1/([\overline{g}_i])$ eine Körpererweiterung vom Grad $\deg(\overline{g}_i)$. Drittens gilt in R_1, dass

$$\bigcap_{i=1}^{r} ([\overline{g}_i])^{\ell_i} = (\overline{g}) = (0).$$

Nun bestimmen wir das Spektrum des Rings $R_2 = \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$. Dazu verwenden wir den Isomorphismus $k[X]/(\overline{g}) \to \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$, der durch $[\overline{g}] \mapsto [g(\theta)]$ definiert ist. Nach den vorherigen Überlegungen ist

$$\operatorname{Spec} R_2 = \{[g_i(\theta)] = \mathfrak{p}_i \mid 1 \le i \le r\},$$

$[(\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}})/\mathfrak{p}_i : k] = \deg(\overline{g}_i)$ und $\bigcap_{i=1}^r \mathfrak{p}_i^{e_i} = (0)$.

Schließlich erhalten wir die Behauptung des Satzes wie folgt: Die Primideale in $\widehat{\mathcal{O}}$ über $\mathfrak{p}$ erhalten wir nach Vorüberlegung und dem vorangegangenen Schritt als die Urbilder $\widehat{\mathfrak{p}}_i$ der Primideale $\mathfrak{p}_i$ in $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}'$, sodass $\widehat{\mathfrak{p}}_i = g_i(\theta)\widehat{\mathcal{O}} + \mathfrak{p}\widehat{\mathcal{O}}$.

Außerdem erhalten wir über die Grade über k aus dem vorangegangenen Schritt, dass $f_i = [\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i : k] = \deg(\overline{g}_i)$ die zugehörigen Trägheitsgrade sind.

Und da $\bigcap_{i=1}^r \widehat{\mathfrak{p}}_i^{e_i}$ in $\mathfrak{p}\widehat{\mathcal{O}}$ enthalten ist, wird $\prod_{i=1}^r \widehat{\mathfrak{p}}_i^{e_i}$ von $\mathfrak{p}\widehat{\mathcal{O}}$ geteilt. Deshalb gibt es geeignete $e_i' \le e_i$, sodass

$$\mathfrak{p}\widehat{\mathcal{O}} = \prod_{i=1}^r \widehat{\mathfrak{p}}_i^{e_i'}$$

Weil aber $n = [L : K] = \deg g = \sum_{i=1}^r e_i \deg(g_i)$ gilt, sagt uns Satz 8, dass auch $n = \sum_{i=1}^r e_i' f_i$, was $e_i = e_i'$ impliziert. □

Korollar II.12.5 (Endlichkeit verzweigter Stellen): *Seien θ ein Element von $\widehat{\mathcal{O}}$, $L = K[\theta]$ und $\operatorname{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Es bezeichne*

$$d_\theta = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\theta) - \sigma_j(\theta))$$

die Diskriminante der Basis $\{1, \theta, \ldots, \theta^{n-1}\}$ von L über K.

(i) *Sei $\mathfrak{p}$ ein zu $\mathfrak{F} \cap \mathcal{O}$ und $d_\theta\mathcal{O}$ koprimes Ideal von θ. Dann ist $\mathfrak{p}$ unverzweigt.*

(ii) *Es gibt nur endlich viele verzweigte Primideale in $\mathcal{O}$.*

Beweis: (i) Da $\mathfrak{p}$ koprim zu $\mathfrak{F} \cap \mathcal{O}$ ist, können wir Satz 9 anwenden. Das Minimalpolynom g_θ von θ lebt dann in $\mathcal{O}[X]$, dessen Bild in $\mathcal{O}/\mathfrak{p}[X] = k[X]$ wir wieder mit $\overline{g}$ bezeichnen wollen, und das in $k[X]$ wieder die Primfaktorzerlegung $\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$ haben soll. Schließlich bezeichne $\overline{d}_\theta$ das Bild der Diskriminante d_θ unter der kanonischen Projektion auf $k[X]$. Da $\mathfrak{p}$ koprim zu $d_\theta\mathcal{O}$ vorausgesetzt ist, ist $\overline{d}_\theta$ von Null verschieden. Wir wollen zeigen, dass $e_1 = \cdots = e_r = 1$ und dass die Körpererweiterung $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i$ von $\mathcal{O}/\mathfrak{p}$ für alle $\widehat{\mathfrak{p}}_i$ über $\mathfrak{p}$ separabel ist. Das wollen wir tun, indem wir zeigen, dass $\overline{g}_\theta$ keine mehrfachen Nullstellen im algebraischen Abschluss $\overline{k}$ von k besitzt.

Die Nullstellen von g_θ sind $\theta_1 = \sigma_1(\theta), \ldots, \theta_n = \sigma_n(\theta)$ und bezeichnet L^{NH} die normale Hülle von L, dann liegen die Nullstellen im ganzen Abschluss $\mathcal{O}' = \mathrm{Int}_{L^{\mathrm{NH}}}(\mathcal{O}) \subseteq L^{\mathrm{NH}}$. Insbesondere können wir g_θ in $\mathcal{O}'[X]$ schreiben als $g_\theta = \prod_{i=1}^n (X - \theta_i)$.

Die Situation, die wir geschaffen haben, ist im folgenden Diagramm festgehalten:

$$\begin{array}{ccccc} \mathfrak{p}' & \subseteq & \mathcal{O}' & \subseteq & L^{\mathrm{NH}} \\ \uparrow & & \uparrow & & \uparrow \\ \widehat{\mathfrak{p}} & \subseteq & \widehat{\mathcal{O}} & \subseteq & L \\ \uparrow & & \uparrow & & \uparrow \\ \mathfrak{p} & \subseteq & \mathcal{O} & \subseteq & K \end{array}$$

Ist $\mathfrak{p}'$ ein Primideal über $\widehat{\mathfrak{p}}$ in $\mathcal{O}'$, dann erhalten wir eine Körperkette

$$\mathcal{O}'/\mathfrak{p}' \supseteq \widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \supseteq \mathcal{O}/\mathfrak{p} = k.$$

Bezeichnet θ_i' das Bild von θ_i in $\mathcal{O}'/\mathfrak{p}'$, dann ist $g_\theta = (X - \theta_1') \cdots (X - \theta_n')$ in $\mathcal{O}'/\mathfrak{p}'[X]$ und außerdem ist $d_\theta' = \prod_{1 \le i < j \le n} (\theta_i' - \theta_j')$ von Null verschieden. Deshalb sind die θ_i' im Erweiterungskörper $\mathcal{O}'/\mathfrak{p}'$ von k paarweise verschieden und g_θ zerfällt in paarweise verschiedene Linearfaktoren. Mit anderen Worten: $e_1 = \cdots = e_n = 1$ und $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ ist separabel; genauer ist $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} = k(\widehat{\theta})$ für das Bild $\widehat{\theta}$ von θ in $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$. □

13 Quadratische Körpererweiterungen und quadratisches Reziprozitätsgesetz

Im ganzen Abschnitt seien $L = \mathbb{Q}[\sqrt{D}]$ für eine quadratfreie natürliche Zahl D, $\widehat{\mathcal{O}} = \mathcal{O}_L = \mathrm{Int}_L(\mathbb{Z})$, $K = \mathbb{Q}$ und $\mathcal{O} = \mathbb{Z}$. Zur Einfachheit schreiben wir $\theta = \sqrt{D}$. Weiterhin sei p stets eine natürliche Primzahl.

Aus Beispiel II.2.13 wissen wir: Ist $D \equiv 2, 3 \pmod 4$, dann ist $\widehat{\mathcal{O}} = \mathbb{Z}[\sqrt{D}]$ mit Ganzheitsbasis $\{1, \sqrt{D}\}$ und Diskriminante $4D = d$.

Ist $D \equiv 1 \pmod 4$, dann hat K den Ganzheitsring $\widehat{\mathcal{O}} = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{D})]$ mit Ganzheitsbasis $\{1, \frac{1}{2}(1 + \sqrt{D})\}$ und Diskriminante $D = d$.

Aufgabe 2 von Blatt 9 sagt uns außerdem: Da $[\widehat{\mathcal{O}} : \mathbb{Z}[\sqrt{D}]]\mathbb{Z} = 2\mathbb{Z}$ nicht von $\mathfrak{p}$ geteilt wird, lässt sich Satz 9 auf $\mathfrak{p}$ anwenden. Das Minimalpolynom von $\theta = \sqrt{D}$ ist $g_\theta = X^2 - D$, welches für $p \neq 2$ auf $\overline{g}_\theta = X^2 - \overline{D}$ in $\mathbb{F}_p[X]$ projiziert wird. Nun gibt es drei mögliche Fälle:

(i) Ist $\overline{D} = 0$, dann ist $\overline{g}_\theta = X^2$ und Satz 9 liefert uns, dass $\mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}_1^2$. In diesem Fall ist $\mathfrak{p}$ totalverzweigt.

(ii) Ist $\overline{D} \neq 0$ und hat $X^2 = \overline{D}$ eine Lösung in $\mathbb{F}_p$, dann liefert Satz 9, dass $\mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}_1\widehat{\mathfrak{p}}_2$, d. h. $\mathfrak{p}$ ist vollzerlegt.

(iii) Ist $\overline{D} \neq 0$ und hat $X^2 = \overline{D}$ keine Lösung in $\mathbb{F}_p$, dann ist $\mathfrak{p}\widehat{\mathcal{O}}$ bereits selbst prim und $\mathfrak{p}$ ist träge.

Definition II.13.1 (Legendre-Symbol): Seien p eine natürliche Primzahl und a ein Element von $\mathbb{F}_p^\times$. Die durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } X^2 = a \text{ in } \mathbb{F}_p \text{ eine Lösung hat,} \\ -1, & \text{falls } X^2 = a \text{ keine Lösung in } \mathbb{F}_p \text{ hat,} \end{cases}$$

definierte Funktion heißt *Legendre-Symbol*. Ist $(\frac{a}{p}) = 1$, dann heißt a ein *quadratischer Rest*.

Proposition II.13.2 (Verzweigtheit in quadratischen Zahlkörpern): *Sei p eine ungerade Primzahl. Genau dann wird D von p geteilt, wenn $\mathfrak{p}$ totalverzweigt ist. Wird D nicht von p geteilt und ist $(\frac{\overline{D}}{p}) = 1$, dann ist $\mathfrak{p}$ vollzerlegt. Wird D nicht von p geteilt und ist $(\frac{\overline{D}}{p}) = -1$, dann ist $\mathfrak{p}$ träge.*

Die Behauptung der obigen Proposition folgt aus der vorausgegangenen Vorüberlegung.

Bemerkung II.13.3 (Legendre-Symbol als Gruppenhomomorphismus): (i) Für eine Einheit a aus $\mathbb{F}_p$ gilt $\overline{(\frac{a}{p})} = a^{(p-1)/2}$.

(ii) Sind a und b Einheiten aus $\mathbb{F}_p$, dann gilt $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$, d. h. die Abbildung $(\frac{=}{=})\colon \mathbb{F}_p^\times \to \{\pm 1, \cdot\}$, $a \mapsto (\frac{a}{p})$ ist ein Gruppenhomomorpismus.

(iii) Der zugehörige Homomorphismus ist surjektiv, d. h. es gibt Einheiten in $\mathbb{F}_p$, die keine Wurzel besitzen.

(iv) $(\mathbb{F}_p^\times)^2 = \{a^2 \mid a \in \mathbb{F}_p^\times\}$ ist eine Untergruppe von $\mathbb{F}_p^\times$. Genauer gesagt hat diese Untergruppe Index 2 in $\mathbb{F}_p^\times$. Insbesondere gibt es genau so viele quadratische Reste in $\mathbb{F}_p^\times$ wie Einheiten, die keine quadratischen Reste sind.

(v) Aus (iv) folgt sofort: $\sum_{c \in \mathbb{F}_p^\times} (\frac{c}{p}) = 0$.

Wir zeigen Aussagen (iv) und (i). Aus diesen folgen dann alle anderen Behauptungen. Sei $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ die durch $a \mapsto a^2$ definierte Abbildung. Diese ist ein Gruppenhomomorphismus und $(\mathbb{F}_p^\times)^2 = \operatorname{im}\varphi$ ist eine Untergruppe

von $\mathbb{F}_p^\times$. Den Index können wir nun bestimmen, indem wir den Kern von φ bestimmen, aber dieser ist gerade $\ker\varphi = \{\pm 1\}$.

Wir wissen, dass Einheitengruppen endlicher Körpern zyklisch sind. Genauer ist $\mathbb{F}_p^\times$ von Ordnung $p-1$. Ist c ein Erzeuger der Einheitengruppe, dann ist $c^{p-1} = 1$ und $c^{(p-1)/2} = -1$. Für $a = c^k$ ist dann

$$a^{\frac{p-1}{2}} = c^{\frac{p-1}{2}k} = \begin{cases} 1, & \text{genau dann, wenn } k \text{ gerade ist,} \\ -1, & \text{genau dann, wenn } k \text{ ungerade ist.} \end{cases}$$

Außerdem folgt für k gerade, dass $(\frac{a}{p}) = 1$ und ist k ungerade, dann ist $(\frac{a}{p}) = -1$; zum Beispiel wegen Aussage (iv).

Behauptung (ii) folgt wegen (i) aus den Potenzgesetzen, und (iii) folgt direkt aus (iv). Schließlich ist (v) auch klar wegen (iv).

Satz 10 (Gaußsches Reziprozitätsgesetz): *Sind ℓ und p verschiedene ungerade Primzahlen, dann ist*

$$\left(\frac{\overline{\ell}}{p}\right)\left(\frac{\overline{p}}{q}\right) = (-1)^{(\ell-1)(p-1)/4}.$$

Ferner gelten

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beweis: Dass $(\frac{-1}{p})$ den angegebenen Wert hat, zeigt Bemerkung II.13.3(i).

Für $(\frac{2}{p})$ rechnen wir in $\mathbb{Z}[\mathrm{i}]$. Dazu verwenden wir die Gleichungen $(1+\mathrm{i})^2 = 2\mathrm{i}$ und $(1+\mathrm{i})^p \equiv 1 + \mathrm{i}^p \pmod p$. Mithilfe dieser können wir schreiben

$$(1+\mathrm{i})^p = (1+\mathrm{i})((1+\mathrm{i})^2)^{\frac{p-1}{2}} = (1+\mathrm{i})(2\mathrm{i})^{\frac{p-1}{2}} = (1+\mathrm{i})\mathrm{i}^{\frac{p-1}{2}}2^{\frac{p-1}{2}},$$

sodass $(1+\mathrm{i})i^{\frac{p-1}{2}}(\frac{2}{p}) \equiv 1 + i(-1)^{\frac{p-1}{2}} \pmod p$. Nun unterscheiden wir Fälle.

Ist $\frac{p-1}{2}$ gerade, dann ist $(1+\mathrm{i})(-1)^{\frac{p-1}{4}}(\frac{2}{p}) \equiv 1+\mathrm{i} \pmod p$, d. h. $(\frac{2}{p}) = (-1)^{\frac{p-1}{4}} \pmod p$.

Ist $\frac{p-1}{2}$ ungerade, dann haben wir $(1+\mathrm{i})\mathrm{i}(-1)^{\frac{p-3}{4}}(\frac{2}{p}) \equiv 1 - \mathrm{i} \pmod p$ und erhalten daraus $(\frac{2}{p}) \equiv (-1)^{\frac{p+1}{4}} \pmod p$.

Um beide Fälle zusammenzuführen verwenden wir, dass $\frac{p^2-1}{8} = \frac{p-1}{4}\frac{p+1}{2} = \frac{p+1}{4}\frac{p-1}{2}$. Damit erhalten wir im ersten Fall

$$(-1)^{\frac{p^2-1}{8}} = \left((-1)^{\frac{p-1}{4}}\right)^{\frac{p+1}{2}} = (-1)^{\frac{p-1}{4}} \equiv \left(\frac{2}{p}\right) \pmod p.$$

Weil auf beiden Seiten 1 oder -1 steht, ist das sogar eine ehrliche Gleichheit. Im zweiten Fall verfahren wir genau so und erhalten

$$(-1)^{\frac{p^2-1}{8}} = \left((-1)^{\frac{p+1}{4}}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{4}} = \left(\frac{2}{p}\right).$$

Nun zum allgemeinen Fall, d. h. $(\frac{\ell}{p})(\frac{p}{\ell}) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$. Dazu betrachten wir eine eine primitive ℓ-te Einheitswurzel ζ und rechnen in $\mathbb{Z}[\zeta]$. Sei $\tau = \sum_{a\in\mathbb{F}_p^\times}(\frac{a}{\ell})\zeta^a$.

Als erstes zeigen wir, dass $\tau^2 = (\frac{-1}{\ell})\ell$. Um das zu tun verwenden wir die Identitäten $(\frac{b}{\ell}) = (\frac{b^{-1}}{\ell})$, und $(\frac{c}{\ell}) = (\frac{-c}{\ell})$ genau dann, wenn $(\frac{-1}{\ell}) = 1$. Es gilt

$$\begin{aligned}
\left(\frac{-1}{\ell}\right)\tau^2 &= \left(\frac{-1}{\ell}\right)\sum_{a,b\in\mathbb{F}_\ell^\times}\left(\frac{a}{\ell}\right)\left(\frac{b}{\ell}\right)\zeta^{a+b}\\
&= \sum_{a,b\in\mathbb{F}_\ell^\times}\left(\frac{-ab}{\ell}\right)\zeta^{a+b}\\
&= \sum_{a,b\in\mathbb{F}_\ell^\times}\left(\frac{ab^{-1}}{\ell}\right)\zeta^{a-b}\\
&= \sum_{b,c\in\mathbb{F}_\ell^\times}\left(\frac{c}{\ell}\right)\zeta^{bc-b}\\
&= \sum_{c\in\mathbb{F}_\ell^\times-\{1\}}\left(\frac{c}{\ell}\right)\sum_{b\in\mathbb{F}_\ell^\times}\zeta^{b(c-1)} + \sum_{b\in\mathbb{F}_\ell^\times}\left(\frac{1}{\ell}\right).
\end{aligned}$$

Unter Verwendung von $\zeta = \zeta^{c-1}$ erhalten wir $\sum_{b\in\mathbb{F}_\ell^\times}\zeta^{b(c-1)} = \sum_{b\in\mathbb{F}_\ell^\times}\zeta^b = -1$, sodass

$$\left(\frac{-1}{\ell}\right)\tau^2 = (-1)(-1) + \ell - 1 = \ell,$$

was wir zeigen wollten.

Als zweites setzen wir die eben bestimmte Gleichheit ein. Mithilfe von $(\frac{\ell}{p}) = \ell^{\frac{p-1}{2}} \pmod p$ und $(\frac{-1}{\ell}) = (-1)^{\frac{p-1}{2}}$ folgt

$$\tau^p = \tau(\tau^2)^{\frac{p-1}{2}} = \tau\left((-1)^{\frac{\ell-1}{2}}\right)^{\frac{p-1}{2}}\left(\frac{\ell}{p}\right) \pmod p. \tag{2.1}$$

Andererseits gilt aber auch

$$\tau^p \equiv \sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{a}{\ell}\right)\zeta^{ap} \equiv \left(\frac{p}{\ell}\right)^2\sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{a}{\ell}\right)\zeta^{ap} \equiv \left(\frac{p}{\ell}\right)\sum_{a\in\mathbb{F}_\ell^\times}\left(\frac{ap}{\ell}\right)\zeta^{ap} \equiv \left(\frac{p}{\ell}\right)\tau \pmod p \tag{2.2}$$

Die Gl. (2.1) and (2.2) ergeben deshalb, dass

$$\tau\left(\frac{p}{\ell}\right) = \tau(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\left(\frac{\ell}{p}\right) \pmod{p}.$$

Damit ist $\tau^2(\frac{p}{\ell}) = \tau^2(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}(\frac{\ell}{p}) \pmod{p}$, weshalb $(\frac{p}{\ell})(\frac{\ell}{p}) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$ wie gewünscht. □

14 Hilbertsche Verzweigungstheorie

In diesem Abschnitt möchten wir Verzweigungstheorie für Dedekindringerweiterungen, falls die entsprechende Körpererweiterung normal ist, studieren. In diesem Abschnitt folgen wir Setting II.12.1, wobei wir zusätzlich fordern, dass L eine galoissche Körpererweiterung von K ist. Es bezeichne G die Galoisgruppe $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$ und θ in $\widehat{\mathcal{O}}$ sei ein primitives Element für die Körpererweiterung L, d. h. $L = K(\theta)$.

Erinnerung: Genau dann ist die Körpererweiterung $L|K$ normal, wenn L Zerfällungskörper von K ist. Das ist äquivalent dazu, dass das Minimalpolynom f_α in $K[X]$ für jedes α aus L über L in Linearfaktoren zerfällt, weshalb $\mathrm{Hom}_K(L, \overline{L}) \cong \mathrm{Aut}(L|K)$.

Genau dann ist die Körpererweiterung $L|K$ galoissch, wenn sie separabel und normal ist. Das tritt genau dann ein, wenn $|\mathrm{Aut}(L|K)| = [L : K] = n$ und in diesem Fall schreiben wir $\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K)$.

Proposition II.14.1 (Galois-Aktion auf Primidealen): *Seien $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathcal{O}}$ und $\mathfrak{p} = \widehat{\mathfrak{p}} \cap \mathcal{O}$.*

(i) *Für jedes σ aus $\mathrm{Aut}(L|K)$ ist $\sigma(\widehat{\mathfrak{p}})$ ein Primideal, das über $\mathfrak{p}$ liegt.*

(ii) *Die Gruppe $\mathrm{Gal}(L|K)$ operiert transitiv auf der Menge der Primideale in $\widehat{\mathcal{O}}$, die über $\mathfrak{p}$ liegen.*

Beweis: (i) Es gilt $\sigma(\widehat{\mathcal{O}}) = \widehat{\mathcal{O}}$, da $\widehat{\mathcal{O}}$ ganzabgeschlossen ist. Man rechnet direkt nach, dass $\sigma(\widehat{\mathfrak{p}})$ ein Primideal in $\widehat{\mathcal{O}}$ ist. Weil $\sigma|_K = \mathrm{id}_K$ ist, ist erst recht $\sigma|_{\mathcal{O}} = \mathrm{id}_{\mathcal{O}}$ und $\sigma(\widehat{\mathfrak{p}}) \cap \mathcal{O} = \sigma(\widehat{\mathfrak{p}} \cap \mathcal{O}) = \mathfrak{p}$.

(ii) Aus (i) folgt, dass $\mathrm{Gal}(L|K)$ auf der Menge der Primideale operiert. Bleibt zu zeigen, dass diese Aktion tatsächlich transitiv ist, d. h. dass die Aktion nur eine Bahn hat. Seien dazu $\widehat{\mathfrak{p}}$ und $\widehat{\mathfrak{q}}$ Primideale in $\widehat{\mathcal{O}}$, die über $\mathfrak{p}$ liegen. Per Definition ist $\widehat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p} = \widehat{\mathfrak{q}} \cap \mathcal{O}$. Angenommen, $\widehat{\mathfrak{p}}$ und $\widehat{\mathfrak{q}}$ lägen nicht

in derselben G-Bahn. Dann wäre $\widehat{\mathfrak{q}}$ koprim zu $\sigma_1(\widehat{\mathfrak{p}}), \ldots, \sigma_n(\widehat{\mathfrak{p}})$. Per chinesischem Restsatz gäbe es dann ein x in $\widehat{\mathcal{O}}$, sodass

$$x \equiv 0 \pmod{\widehat{\mathfrak{q}}}, \quad x \equiv 1 \pmod{\sigma_1(\widehat{\mathfrak{p}})}, \quad \ldots \quad x \equiv 1 \pmod{\sigma_n(\widehat{\mathfrak{p}})}$$

und für dieses x wäre einerseits $N_{L|K}(x) = \prod_{i=1}^{n} \sigma_i(x)$ enthalten in $\widehat{\mathfrak{q}}$, weil x im Produkt auftaucht, aber da die Norm ganz ist andererseits auch in $\mathcal{O}$, d. h. in $\mathfrak{p}$.

Weil x für jedes σ aus G in keinem der $\sigma_i(\widehat{\mathfrak{p}})$ enthalten wäre, wären auch die $\sigma_1(x), \ldots, \sigma_n(x)$ nicht in $\widehat{\mathfrak{p}}$ enthalten. Da $\widehat{\mathfrak{p}}$ prim ist, könnte $N_{L|K}(x)$ nicht in $\widehat{\mathfrak{p}}$ enthalten sein, und so könnte $N_{L|K}(x)$ nicht in $\mathfrak{p}$ liegen. Unsere Annahme war also falsch und die Aktion ist transitiv. □

Definition II.14.2 (Invarianten der Aktion): Sei $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathcal{O}}$.

(i) Wir schreiben $G_{\widehat{\mathfrak{p}}}$ für den Stabilisiator $\mathrm{Stab}_G(\widehat{\mathfrak{p}})$ und nennen $G_{\widehat{\mathfrak{p}}}$ die *Zerlegungsgruppe von* $\widehat{\mathfrak{p}}$.

(ii) Wir schreiben $Z_{\widehat{\mathfrak{p}}} = \{x \in L \mid \forall\, \sigma \in G_{\widehat{\mathfrak{p}}} : \sigma(x) = x\} = L^{G_{\widehat{\mathfrak{p}}}}$ und nennen das den *Zerlegungskörper von* $\widehat{\mathfrak{p}}$.

Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(L|Z_{\widehat{\mathfrak{p}}}) = G_{\widehat{\mathfrak{p}}}$.

Bemerkung II.14.3 (Bedeutung der Zerlegungsgruppe): Seien $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathcal{O}}$ und $\mathfrak{p}$ ein Primideal in $\mathcal{O}$, sodass $\widehat{\mathfrak{p}}$ über $\mathfrak{p}$ liegt. Nach der Bahnformel gilt

$$G/G_{\widehat{\mathfrak{p}}} \longleftrightarrow G\widehat{\mathfrak{p}} = \{\mathfrak{q} \text{ Primideal über } \mathfrak{p}\}.$$

Insbesondere ist $[G : G_{\widehat{\mathfrak{p}}}]$ die Anzahl der Primideale über $\mathfrak{p}$, welche wir wie früher mit r bezeichnen.

Genau dann ist $G_{\widehat{\mathfrak{p}}} = \{1\}$, wenn $r = [G : G_{\widehat{\mathfrak{p}}}] = |G| = n$, also genau dann, wenn $\mathfrak{p}$ vollzerlegt ist.

Genau dann ist $G_{\widehat{\mathfrak{p}}} = G$, wenn $\mathfrak{p}$ unzerlegt ist, d. h. wenn $r = [G : G_{\widehat{\mathfrak{p}}}] = 1$.

Für einen Automorphismus σ aus G ist $G_{\sigma(\widehat{\mathfrak{p}})} = \sigma^{-1} \circ G_{\widehat{\mathfrak{p}}} \circ \sigma$.

All diese Behauptungen sind direkte Konsequenzen aus Proposition I.14.1 und den Definitionen.

Bemerkung II.14.4 (Bei Normalität gleiche Verzweigungsdaten pro Faser): Sei $mathfrakp\mathcal{O} = \widehat{\mathfrak{p}}_1^{e_1} \cdots \widehat{\mathfrak{p}}_r^{e_r}$ die Primidealzerlegung und $f_i = [\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i : \mathcal{O}/\mathfrak{p}]$ die zugehörigen Trägheitsgrade. Aus der Normalität der Körpererweiterung folgt dann $e_1 = \cdots = e_r$ und $f_1 = \cdots = f_r$.

Beweis: Nach Proposition II.14.1 gibt es ein σ_i in G, sodass $\sigma_i(\widehat{\mathfrak{p}}_1) = \widehat{\mathfrak{p}}_i$, d. h. σ_i induziert einen Isomorphismus $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_1 \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}_i$. Beides sind Vektorräume über $k = \mathcal{O}/\mathfrak{p}$, weshalb $f_1 = f_i$.

Genau dann wird $\mathfrak{p}\widehat{\mathcal{O}}$ von $\widehat{\mathfrak{p}}_1^k$ geteilt, wenn $\mathfrak{p}\mathcal{O}$ in $\widehat{\mathfrak{p}}_1^k$ enthalten ist, was wiederum äquivalent ist dazu, dass $\mathfrak{p}\widehat{\mathcal{O}}$ in $(\sigma(\widehat{\mathfrak{p}}_1))^k = \widehat{\mathfrak{p}}_i^k$ enthalten ist. Damit gilt $e_1 = e_i$. □

Insbesondere gilt also $\mathfrak{p}\widehat{\mathcal{O}} = \prod_{i=1}^{r} \sigma_i(\widehat{\mathfrak{p}})^e$, wenn $\sigma_1, \ldots, \sigma_r$ ein Nebenklassenvertretersystem von $G_{\widehat{\mathfrak{p}}_1}$ in G ist.

Wir betrachten die Kette von Körpererweiterungen $K \subseteq Z_{\widehat{\mathfrak{p}}} \subseteq L$. In diesem Fall gilt $\widehat{\mathcal{O}} \cap Z_{\widehat{\mathfrak{p}}} = \mathrm{Int}_{Z_{\mathfrak{p}}}(\mathcal{O}) = \widehat{\mathcal{O}}_Z$ und die Situation stellt sich dar wie in folgendem Diagramm abgebildet:

$$\begin{array}{ccccc}
\widehat{\mathfrak{p}} & \subset & \widehat{\mathcal{O}} & \subseteq & L \\
{\scriptstyle e',f'}\uparrow & & \uparrow & & \uparrow \\
\widehat{\mathfrak{p}} \cap \widehat{\mathcal{O}}_Z = \widehat{\mathfrak{p}}_Z & \subset & \widehat{\mathcal{O}}_Z & \subset & Z_{\widehat{\mathfrak{p}}} = L^{G_{\widehat{\mathfrak{p}}}} \\
{\scriptstyle e'',f''}\uparrow & & \uparrow & & \uparrow \\
\mathfrak{p} & \subset & \mathcal{O} & \subseteq & K
\end{array}$$

Hierbei ist $\widehat{\mathfrak{p}}_Z$ vollzerlegt und $\widehat{\mathfrak{p}}$ unverzweigt, wie wir in der nächsten Proposition festhalten wollen.

Proposition II.14.5: *Sei $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathcal{O}}$ über dem Primideal $\mathfrak{p}$ in $\mathcal{O}$. Ferner bezeichne $\widehat{\mathfrak{p}}_Z = \widehat{\mathfrak{p}} \cap \widehat{\mathcal{O}}_Z$ das dazwischenliegende Primideal. Seien e der Verzweigungsindex, f der Trägheitsgrad und k die Anzahl der Primideale in $\widehat{\mathcal{O}}$, die über $\mathfrak{p}$ liegen. Dann gilt:*

(i) *$\widehat{\mathfrak{p}}_Z$ ist unzerlegt in $L|Z_{\widehat{\mathfrak{p}}}$, d. h. $\widehat{\mathfrak{p}}$ ist das einzige Primideal in $\widehat{\mathcal{O}}$ über $\mathfrak{p}$.*

(ii) *$\widehat{\mathfrak{p}}$ hat über $\widehat{\mathfrak{p}}_Z$ den Verzweigungsindex e und den Trägheitsgrad f, d. h. $\widehat{\mathfrak{p}}_Z\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}^e$ und $[\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} : \widehat{\mathcal{O}}_Z/\widehat{\mathfrak{p}}_Z] = f$.*

(iii) *$\widehat{\mathfrak{p}}_Z$ über $\mathfrak{p}$ ist vollzerlegt, d. h. Verzweigungsindex 1 und Trägheitsgrad 1.*

Beweis: Zu (i): Per Definition ist $Z_{\widehat{\mathfrak{p}}} = L^{G_{\widehat{\mathfrak{p}}}}$, weshalb $\mathrm{Gal}(L|Z_{\widehat{\mathfrak{p}}}) = G_{\widehat{\mathfrak{p}}}$. Nach Bemerkung II.14.3 ist $\widehat{\mathfrak{p}}_Z$ unzerlegt.

Zu (ii) und (iii): Es bezeichne e' den Verzweigungsindex von $\widehat{\mathfrak{p}}$ über $\widehat{\mathfrak{p}}_Z$ und e'' den Verzweigungsindex von $\widehat{\mathfrak{p}}_Z$ über $\widehat{\mathfrak{p}}$. Analog notieren wir f' und f'' für die Trägheitsgrade. Wir haben also Zerlegungen $\widehat{\mathfrak{p}}_Z\widehat{\mathcal{O}} = \widehat{\mathfrak{p}}^{e'} \cdots$ und $\mathfrak{p}\widehat{\mathcal{O}}_Z = \mathfrak{p}_Z^{e''}$, sodass $\mathfrak{p}\widehat{\mathcal{O}} = (\mathfrak{p}\widehat{\mathcal{O}}_Z)\widehat{\mathcal{O}} = (\widehat{\mathfrak{p}}_Z^{e'})^{e''} \cdots$ und $e'e'' = e$.

Zweitens haben wir die Kette von Körpererweiterungen $\mathcal{O}/\mathfrak{p} \subseteq \widehat{\mathcal{O}}_Z/\widehat{\mathfrak{p}}_Z \subseteq \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$, deren Grade f'' respektive f' sind; sodass $f = f'f''$.

Nach Satz 8 gilt für die Körpererweiterung $L|K$, dass $n = [L : K] = efr$, wobei $r = [G : G_{\widehat{\mathfrak{p}}}]$, und genauso haben wir für $L|Z_{\widehat{\mathfrak{p}}}$, dass $[L : Z_{\widehat{\mathfrak{p}}}] = e'f'1$ sowie $[L : Z_{\widehat{\mathfrak{p}}}] = |G_{\widehat{\mathfrak{p}}}| = |G|/[G : G_{\widehat{\mathfrak{p}}}] = n/r = ef$, d. h. es gilt $ef = e'f'$. Wegen $e = e'e''$ und $f = f'f''$ erhalten wir damit $e''f'' = 1$, sodass $e'' = f'' = 1$; genau so für e' und f'. □

Definition II.14.6 (Restklassenkörper): Sei $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathfrak{O}}$. Dann heißt $\kappa(\widehat{\mathfrak{p}}) = \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ der *Restklassenkörper von* $\widehat{\mathfrak{p}}$.

Bemerkung II.14.7 (Restklassenkörper für $\widehat{\mathfrak{p}}_Z$): Für die Primstellen $\widehat{\mathfrak{p}}_Z$ im Zerlegungskörper über $\mathfrak{p}$ gilt nach Proposition II.14.5, dass $[\kappa(\widehat{\mathfrak{p}}_Z) : \kappa(\mathfrak{p})] = f'' = 1$. Deshalb ist $\kappa(\widehat{\mathfrak{p}}) \cong \kappa(\mathfrak{p}) \cong \mathcal{O}/\mathfrak{p}$, und für diesen Körper schreiben wir k wie sonst.

Proposition II.14.8 (Normalität steigt ab): *Sei $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathfrak{O}}$. Ist L normal über K, dann ist $\kappa(\widehat{\mathfrak{p}})$ normal über $\kappa(\mathfrak{p})$.*

Beweis: Wir schreiben $k = \kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$ wie gewohnt. Seien $\overline{\alpha}$ ein Element von k, $\overline{g}$ in $k[X]$ das zugehörige Minimalpolynom und α ein Urbild von $\overline{\alpha}$ in $\widehat{\mathcal{O}} \subset L$. Schließlich bezeichne f das Minimalpolynom von α.

Zunächst gilt $f(\alpha) = 0$, weshalb $\overline{f}(\overline{\alpha}) = 0$ ist, und $\overline{g}$ von $\overline{f}$ geteilt wird.

Weiter ist $L|K$ eine normale Erweiterung, d. h. $f = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{L})}(X - \sigma(\alpha))$, wobei $\sigma(\alpha$ in L liegen, und sogar ganz sind. Also zerfällt $\overline{f}$ über $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}) = \kappa(\widehat{\mathfrak{p}})$ in Linearfaktoren. Damit auch $\overline{g}$ und $\kappa(\widehat{\mathfrak{p}})$ ist normal über k. □

Wir halten fest: Ist $\widehat{\mathfrak{p}}$ das einzige Primideal über $\mathfrak{p}$, dann gilt für jedes σ aus $\mathrm{Gal}(L|K)$, dass $\sigma(\widehat{\mathfrak{p}}) = \widehat{\mathfrak{p}}$. Die Aktion von G auf $\widehat{\mathcal{O}}$ steigt also ab zu einer Aktion auf $\kappa(\widehat{\mathfrak{p}})$.

Lemma II.14.9 (Abstieg der Galois-Aktion): *Seien $\widehat{\mathfrak{p}}$ ein unzerlegtes Primideal über $\mathfrak{p}$ und $k = \mathcal{O}/\mathfrak{p}$. Dann ist der folgende Gruppenhomomorphismus surjektiv:*

$$\varphi\colon G = \mathrm{Gal}(L|K) \longrightarrow \mathrm{Aut}_k(\kappa(\widehat{\mathfrak{p}})), \qquad \sigma \longmapsto (a + \widehat{\mathfrak{p}} \mapsto \sigma(a) + \widehat{\mathfrak{p}})$$

Beweis: Sei $\overline{\sigma}$ in $\mathrm{Aut}_k(\kappa(\widehat{\mathfrak{p}}))$. Wir suchen ein σ aus $\mathrm{Gal}(L|K)$, sodass $\varphi(\sigma) = \overline{\sigma}$. Bezeichnet E den separablen Abschluss von k in $\kappa(\mathfrak{p}) = \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$. Dann ist $E = k(\overline{\theta})$ für ein geeignetes $\overline{\theta}$ aus $E \subseteq \kappa(\widehat{\mathfrak{p}}) = \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$.

Seien nun $\overline{g}$ das Minimalpolynom von θ in $k[X]$, θ ein Urbild von $\overline{\theta}$ in $\widehat{\mathcal{O}}$ und f das Minimalpolynom von θ in $\mathcal{O}[X]$. Dann ist $\overline{f}$ das Bild von f in $k[X]$. Nach der vorangegangenen Proposition zerfallen f, $\overline{f}$ und g in Linearfaktoren und $\overline{f}$ wird von $\overline{g}$ geteilt.

Ist $\overline{\sigma}(\overline{\theta})$ eine Nullstelle von $\overline{g}$, dann ist $(X - \overline{\sigma}(\overline{\theta}))$ ein Linearfaktor von $\overline{g}$ und damit von $\overline{f}$. Das heißt es gibt ein Urbild θ' in $\widehat{\mathcal{O}}$, sodass $\overline{\sigma}(\overline{\theta})$ in $\kappa(\widehat{\mathfrak{p}})$ liegt und θ' eine Nullstelle von f ist, da f über $\widehat{\mathcal{O}}$ in Linearfaktoren zerfällt. Es gibt also ein σ in $\mathrm{Gal}(L|K)$, sodass $\sigma(\theta) = \theta'$.

Ist $\varphi(\sigma)(\overline{\theta}) = \sigma(\overline{\theta})$, dann ist $\varphi(\sigma)|_E = \sigma|_E$, weshalb $\overline{\sigma}^{-1} \circ \varphi(\sigma)$ in $\mathrm{Aut}(\kappa(\mathfrak{p})|E)$ liegt. Aber es gilt $\mathrm{Aut}(\kappa(\mathfrak{p})|E) = \{\mathrm{id}\}$, da die Erweiterung $\kappa(\mathfrak{p})$ von E rein separabel ist, und damit ist $\overline{\sigma} = \varphi(\sigma)$. □

Proposition II.14.10 (Aktion der Zerlegungsgruppe auf $\kappa(\widehat{\mathfrak{p}})$): *Die Aktion der Galois-Gruppe* $\mathrm{Gal}(L|K)$ *induziert den folgenden surjektiven Gruppenhomomorphismus:*

$$\varphi\colon G_{\widehat{\mathfrak{p}}} \longrightarrow \mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p})), \qquad \sigma \longmapsto (a + \widehat{\mathfrak{p}} \mapsto \sigma(a) + \widehat{\mathfrak{p}})$$

Weil Primideale in L unzerlegt über Primidealen in $Z_{\widehat{\mathfrak{p}}}$ liegen und $G_{\widehat{\mathfrak{p}}} = \mathrm{Gal}(L|Z_{\widehat{\mathfrak{p}}})$ ist, folgt die Behauptung aus Lemma II.14.9 und Bemerkung II.14.7.

Definition II.14.11 (Trägheitsgruppe und Trägheitskörper): Sei $\varphi\colon G_{\widehat{\mathfrak{p}}} \to \mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p}))$ der Gruppenhomomorphismus aus Proposition II.14.10. Die Menge

$$I_{\widehat{\mathfrak{p}}} = \ker\varphi = \{\sigma \in \mathrm{Gal}(L|K) \mid \forall\, a \in \widehat{\mathcal{O}} : \sigma(a) \equiv a \pmod{\widehat{\mathfrak{p}}}\}$$

heißt *Trägheitsgruppe zu* $\widehat{\mathfrak{p}}$, und

$$T_{\widehat{\mathfrak{p}}} = L^{I_{\widehat{\mathfrak{p}}}} = \{x \in L \mid \forall\, \sigma \in I_{\widehat{\mathfrak{p}}} : \sigma(x) = x\}$$

heißt *Trägheitskörper zu* $\widehat{\mathfrak{p}}$.

Die Bezeichnung $I_{\widehat{\mathfrak{p}}}$ rührt vom englischen Wort *inertia* für Trägheit her. Über den Hauptsatz der Galois-Theorie haben wir die Korrespondenz

$$\begin{array}{rcl}
\{\mathrm{id}\} & & L \\
\big\downarrow & & \big| \\
\ker\varphi = I_{\widehat{\mathfrak{p}}} & & T_{\widehat{\mathfrak{p}}} \\
\big\downarrow & \longleftrightarrow & \big| \\
\mathrm{Fix}_G(\widehat{\mathfrak{p}}) = G_{\widehat{\mathfrak{p}}} & & Z_{\widehat{\mathfrak{p}}} \\
\big\downarrow & & \big| \\
\mathrm{Gal}(L|K) = G & & K
\end{array}$$

Bemerkung II.14.12 (Kurze exakte Trägheitssequenz): Wir haben die kurze exakte Sequenz:

$$\{\mathrm{id}\} \longrightarrow I_{\widehat{\mathfrak{p}}} \longrightarrow G_{\widehat{\mathfrak{p}}} \longrightarrow \mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p})) \longrightarrow \{1\}$$

Proposition II.14.13: *Für jedes Primideal $\widehat{\mathfrak{p}}$ in $\widehat{\mathcal{O}}$ gilt:*

(i) *Die Erweiterung $T_{\widehat{\mathfrak{p}}}|Z_{\widehat{\mathfrak{p}}}$ ist normal und dazu gehören die Galois-Gruppen* $\mathrm{Gal}(T_{\widehat{\mathfrak{p}}}|Z_{\widehat{\mathfrak{p}}}) \cong \mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p}))$ *sowie* $\mathrm{Gal}(L|T_{\widehat{\mathfrak{p}}}) \cong I_{\widehat{\mathfrak{p}}}$.

(ii) *Ist $\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p})$ separabel, dann ist $|I_{\widehat{\mathfrak{p}}}| = [L : T_{\widehat{\mathfrak{p}}}] = e$ und $[G_{\widehat{\mathfrak{p}}} : I_{\widehat{\mathfrak{p}}}] = [T_{\widehat{\mathfrak{p}}} : Z_{\widehat{\mathfrak{p}}}] = f$.*

(iii) *Ist $\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p})$ separabel und bezeichnet $\widehat{\mathfrak{p}}_T = \widehat{\mathfrak{p}} \cap T_{\widehat{\mathfrak{p}}}$, dann ist der Verzweigungsindex von $\widehat{\mathfrak{p}}$ über $\widehat{\mathfrak{p}}_T$ gleich e und der Trägheitsgrad ist 1. Ferner ist der Verzweigungsindex von $\widehat{\mathfrak{p}}_T$ über $\widehat{\mathfrak{p}}_Z$ eins und der Trägheitsgrad ist f.*

Beweis: (i) Die Trägheitsgruppe $I_{\widehat{\mathfrak{p}}}$ ist normal in $G_{\widehat{\mathfrak{p}}}$. Der Hauptsatz der Galois-Theorie schlägt also zu und sagt uns, dass $\mathrm{Gal}(T_{\widehat{\mathfrak{p}}}|Z_{\widehat{\mathfrak{p}}}) = G_{\widehat{\mathfrak{p}}}/I_{\widehat{\mathfrak{p}}}$. Die Trägheitsgruppe haben wir so gebaut, dass dieser Quotient gerade isomorph zu $\mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p}))$ ist. Ferner ist $T_{\widehat{\mathfrak{p}}}$ per Konstruktion der Fixkörper der Trägheitsgruppe.

(ii) Ist der Körpererweiterung $\kappa(\widehat{\mathfrak{p}})|\kappa(\mathfrak{p})$ separabel, dann haben wir die Gleichung

$$\frac{ef}{|I_{\widehat{\mathfrak{p}}}|} = \frac{|G_{\widehat{\mathfrak{p}}}|}{|I_{\widehat{\mathfrak{p}}}|} = |\mathrm{Aut}(\kappa(\widehat{\mathfrak{p}})|\kappa(\widehat{\mathfrak{p}}))| = [\kappa(\widehat{\mathfrak{p}}) : \kappa(\mathfrak{p})] = f.$$

(iii) Können wir zeigen, dass $\kappa(\widehat{\mathfrak{p}}_T) = \kappa(\widehat{\mathfrak{p}})$, dann folgt, dass der Trägheitsgrad von $\widehat{\mathfrak{p}}$ über $\widehat{\mathfrak{p}}_T$ eins ist. Dann muss der Verzweigungsindex von $\widehat{\mathfrak{p}}$ über $\widehat{\mathfrak{p}}_T$ gleich e sein, was für den Verzweigungsindex von $\widehat{\mathfrak{p}}_T$ über $\widehat{\mathfrak{p}}$ liefert, dass dieser gleich $ef/e = f$ sein muss. Die Verzweigungsindizes zwingen dann den Trägheitsgrad von $\widehat{\mathfrak{p}}_T$ über $\widehat{\mathfrak{p}}$ eins zu sein. Die fehlende, eingangs erwähnte Gleichheit zeigen wir in der folgenden Bemerkung. □

Bemerkung II.14.14: Es gilt $\kappa(\widehat{\mathfrak{p}}_T) = \kappa(\widehat{\mathfrak{p}})$. Seien nämlich $L' = T_{\widehat{\mathfrak{p}}}$ und $K' = Z_{\widehat{\mathfrak{p}}}$. Dann erhalten wir aus Lemma II.4.9 einen surjektiven Gruppenhomomorphismus

$$\mathrm{Gal}(T_{\widehat{\mathfrak{p}}}|Z_{\widehat{\mathfrak{p}}}) \twoheadrightarrow \mathrm{Aut}_{\kappa(\widehat{\mathfrak{p}}_Z)}(\kappa(\widehat{\mathfrak{p}}_T)).$$

15 Zyklotomische Körper

In diesem Abschnitt möchten wir die sogenannten zyklotomischen Körper untersuchen. Das sind Körpererweiterungen des Körpers der rationalen Zahlen um primitive n-te Einheitswurzeln. Einerseits möchten wir einsehen, dass $\mathcal{O}_K = \mathbb{Z}[\zeta]$ wenn ζ eine n-te primitive Einheitswurzel und $K = \mathbb{Q}[\zeta]$ ist, andererseits möchten wir die Primideale in diesem Ganzheitsring bestimmen.

In diesem Abschnitt seien stets ℓ eine positive Primzahl und $\zeta_n = \zeta$ eine primitive n-te Einheitswurzel.

Erinnerung II.15.1: Der Grad der Körpererweiterung ist $d = [\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(n)$. Die Körpererweiterung $\mathbb{Q}[\zeta]$ über $\mathbb{Q}$ ist galoissch. Genauer ist

$$\mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}) = \{\sigma_i \text{ mit } \sigma_i(\zeta) \mapsto \zeta^i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times\} \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Für jede natürliche Zahl k gilt $(X-1)(X^{k-1} + X^{k-2} + \cdots + 1) = X^k - 1$, weshalb

$$\psi_k = X^{k-1} + X^{k-2} + \cdots + 1 = \frac{X^k - 1}{X - 1} = \prod_{i=1}^{k-1}(X - \zeta_k^i).$$

Für $X = 1$ erhalten wir insbesondere, dass $n = (1-\zeta)\cdots(1-\zeta_k^{n-1})$. Ist $n = \ell^k$ eine Primzahlpotenz, dann gilt für $d = \varphi(n) = \ell^{k-1}(\ell-1)$:

$$\phi_n = \frac{\psi_{\ell^k}}{\psi_{\ell^{k-1}}} = \frac{X^{\ell^k} - 1}{X^{\ell^{k-1}} - 1} = X^{\ell^{k-1}(\ell-1)} + \cdots + X^{\ell^{k-1}} + 1.$$

Lemma II.15.2: *Ist g eine Einheit in $\mathbb{Z}/n\mathbb{Z}$, dann liegt $\varepsilon_g = (1-\zeta^g)/(1-\zeta)$ im Ganzheitsring $\mathcal{O}_K$.*

Beweis: Nach Erinnerung II.15.1 ist $\varepsilon_g = \psi_g(\zeta) = \zeta^{g-1} + \cdots + 1$ ganz. Wir wissen, dass $\varepsilon_g^{-1} = (1-\zeta)/(1-\zeta^g)$. Für g' mit $gg' \equiv 1 \pmod{n}$ erhalten wir $\zeta^{gg'} = \zeta$, und so folgt

$$\varepsilon_g^{-1} = \frac{1 - (\zeta^g)^{g'}}{1 - \zeta^g} = \phi_g(\zeta^g) = (\zeta^g)^{g'-1} + \cdots + \zeta^g + 1,$$

was ebenfalls ganz ist. □

Proposition II.15.3: *Sei n die Primzahlpotenz ℓ^k.*

(i) *Es gilt $\ell\mathcal{O} = (1-\zeta)^{\varphi(n)}$ und $(1-\zeta)$ ist ein Primideal mit Trägheitsgrad 1.*

(ii) *Ist* $s = \ell^{k-1}(kl-k-1)$*, dann gilt für die Diskriminante der Körpererweiterung bezüglich der Standardbasis, dass* $d(1,\zeta,\dots,\zeta^{\varphi(n)-1}) = \pm\ell^s$.

(iii) *Der Ganzheitsring ist* $\mathcal{O} = \mathbb{Z}[\zeta]$ *und* $\{1,\zeta,\dots,\zeta^{\varphi(n)-1}\}$ *ist eine Ganzheitsbasis.*

Beweis: (i) Nach Erinnerung II.15.1 ist $\ell = \phi_n(1) = \prod_{g\in(\mathbb{Z}/n\mathbb{Z})^\times}(1-\zeta^g)$. Wir haben die Darstellung $1-\zeta^g = \varepsilon_g(1-\zeta)$, $\varepsilon_g = (1-\zeta^g)/(1-\zeta)$, und das vorangegangene Lemma sagt uns, dass ε_g ganz ist. Das heißt $\ell = (\prod_{g\in(\mathbb{Z}/n\mathbb{Z})^\times}\varepsilon_g)(1-\zeta)^{\varphi(n)}$, und der erste Faktor dieses Produkts ist ganz. Insgesamt folgt $(\ell) = (1-\zeta)^{\varphi(n)}$.

(ii) Wir wollen zeigen, dass $d(1,\zeta,\dots,\zeta^{\varphi(n)-1}) = \pm\ell^s$ für $s = \ell^{k-1}(k\ell-k-1)$. Seien $\zeta_1,\dots,\zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln; genauer möchten wir haben, dass $\zeta_i = \sigma_i(\zeta)$. Nach Proposition I.2.5 ist

$$d(1,\zeta,\dots,\zeta^{\varphi(n)-1}) = \prod_{1\le i<j\le n}(\zeta_j-\zeta_i)^2 = \pm\prod_{i=1}^{d}\prod_{j\neq i}(\zeta_j-\zeta_i).$$

Das n-te Kreisteilungspolynom $\Phi_n = \prod_{i=1}^{\varphi(n)}(X-\zeta_i)$ hat die Ableitung $\Phi_n' = \sum_{i=1}^{\varphi(n)}\prod_{j\neq i}(X-\zeta_i)$, sodass $\Phi_n'(\zeta_i) = \prod_{j\neq i}(X-\zeta_j)$, weshalb

$$d(1,\zeta,\dots,\zeta^{\varphi(n)-1}) = \pm\prod_{i=1}^{d}\Phi_n'(\zeta_i) = \prod_{i=1}^{d}\Phi_n'(\sigma_i(\zeta)) = \pm N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\Phi_n'(\zeta)).$$

Verwenden wir nun die Formel $\Phi_n = (X^{\ell^k}-1)/(X^{\ell^{k-1}}-1)$ für $n = \ell^k$, dann erhalten wir, dass $(X^{\ell^{k-1}}-1)\Phi_n = X^{\ell^k}-1$ und so

$$\ell^k X^{\ell^k-1} = \Phi_n'(X^{\ell^{k-1}}-1) + \Phi_n(\cdots).$$

Einsetzen von ζ in diese Gleichung gibt $\ell^k\zeta^{\ell^k-1} = \Phi_n'(\zeta)(\zeta^{\ell^{k-1}}-1)$. Schreiben wir ξ für $\zeta^{\ell^{k-1}}$, dann wird diese Gleichung zu $\ell^k\zeta^{-1} = \Phi_n'(\zeta)(\xi-1)$. Wir halten fest, dass ξ selbst eine primitive ℓ-te Einheitswurzel ist. Einerseits ist

$$N_{\mathbb{Q}[\xi]|\mathbb{Q}} = \prod_{i=1}^{\ell-1}(\xi^i-1) = \pm\ell$$

nach I.15.3(iii) und andererseits ist

$$N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\xi-1) = N_{\mathbb{Q}[\xi]|\mathbb{Q}}(N_{\mathbb{Q}[\zeta]|\mathbb{Q}[\xi]}(\xi-1)) = N_{\mathbb{Q}[\xi]|\mathbb{Q}}\Big((\xi-1)^{\ell^{k-1}}\Big) = \pm\ell^{\ell^{k-1}}.$$

Schließlich ist $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\zeta^{-1}) = \pm1$, weil ζ^{-1} eine Einheit in $\mathcal{O}$ ist. Nun haben wir alles zusammen um die Diskriminante zu berechnen:

$$d(1,\zeta,\dots,\zeta^{\varphi(n)-1}) = \pm N_{\mathbb{Q}[\zeta]|\mathbb{Q}}\left(\frac{\ell^k\zeta^{-1}}{\xi-1}\right) = \pm\frac{(\ell^k)^{\varphi(n)}}{\ell^{\ell^{k-1}}} = \pm\ell^s.$$

(iii) Nach Satz 1 ist $\ell^s\mathcal{O}$ enthalten in $\mathbb{Z}[\zeta]$, und das ist enthalten in $\mathcal{O}$. Aus (i) folgt, weil der Trägheitsgrad 1 ist, dass $\mathcal{O}/(1-\zeta) \cong \mathbb{Z}/\ell\mathbb{Z}$. Schreiben wir λ für $1-\zeta$, dann ist $\mathcal{O} = \lambda\mathcal{O}+\mathbb{Z}$, weshalb erst recht $\mathcal{O} = \lambda\mathcal{O}+\mathbb{Z}[\zeta]$ gilt. Multiplizieren mit λ liefert $\lambda\mathcal{O} = \lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta]$, d. h. $\mathcal{O} = \lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta] + \mathbb{Z}[\zeta] = \lambda^2\mathcal{O} + \mathbb{Z}[\zeta]$. Induktiv erhalten wir so, dass $\mathcal{O} = \lambda^t\mathcal{O} + \mathbb{Z}[\zeta]$ für alle natürlichen Zahlen t.

Wir setzen $t = s\varphi(\ell^k)$. Nach (i) ist $\ell\mathcal{O} = \lambda^{\varphi(\ell^k)}\mathcal{O}$, sodass $\mathcal{O} = \ell^s\mathcal{O} + \mathbb{Z}[\zeta]$. Wegen Satz 1 ist $\ell^s\mathcal{O}$ enthalten in $\mathbb{Z}[\zeta]$, d. h. $\mathcal{O} = \mathbb{Z}[\zeta]$. □

Proposition II.15.4 (Ganzheitsring und Ganzheitsbasis): *Für eine natürliche Zahl n gilt ebenfalls $\mathcal{O} = \mathbb{Z}[\zeta]$ und $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ ist eine Ganzheitsbasis von $\mathcal{O}$.*

Beweis: Seien $n = \ell_1^{k_1} \cdots \ell_r^{k_r}$ die Primfaktorzerlegung und $\zeta_i = \zeta^{n/\ell_i^{k_i}}$. Dann ist ζ_i eine primitive $\ell_i^{k_i}$-te Einheitswurzel und $\varphi(\ell_i^{k_i})$ der Grad der Körpererweiterung $[\mathbb{Q}[\zeta_i] : \mathbb{Q}]$. Weil wir die ζ_i teilerfremd konstruiert haben, gilt $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta_1] \cdots \mathbb{Q}[\zeta_r]$ nach dem Chinesischen Restsatz. Induktiv können wir deshalb für $1 \leq i \leq r$ zeigen, dass

$$\{\zeta_1^{m_1} \cdots \zeta_i^{m_i} \mid m_1 \in \{0, \ldots, \varphi(\ell_1^{k_1})\}, \ldots, m_i \in \{0, \ldots, \varphi(\ell_i^{k_i})\}\}$$

eine Ganzheitsbasis von $\mathbb{Q}[\zeta_1, \ldots, \zeta_i]$ ist, und dass die Primteiler der zugehörigen Diskriminanten $\ell_1, \ldots, \ell_i$ sind. Das folgt aus Proposition II.2.17 und Proposition II.15.3. Insgesamt erhalten wir also, dass

$$\{\zeta_1^{m_1} \cdots \zeta_r^{m_r} \mid m_1 \in \{0, \ldots, \varphi(\ell_1^{k_1})\}, \ldots, m_i \in \{0, \ldots, \varphi(\ell_r^{k_r})\}\}$$

eine Ganzheitsbasis von $\mathcal{O}$ ist. Weil jedes Produkt $\zeta_1^{m_1} \cdots \zeta_r^{m_r}$ eine Potenz von ζ ist, folgt daraus die Behauptung. □

Im Folgenden schreiben wir $\widehat{\mathcal{O}}$ für den Ganzheitsring von $K = \mathbb{Q}[\zeta]$.

Lemma II.15.5: *Seien p eine Primzahl und $\widehat{\mathfrak{p}}$ ein Primideal in $\widehat{\mathcal{O}}$ über $p\mathbb{Z}$. Wir schreiben $n = p^{\nu_p}m$, wobei $\mathrm{ggT}(p, m) = 1$. Dann gilt für jede p^{ν_p}-te Einheitswurzel η_j, dass $\eta_j \equiv 1 \pmod{\widehat{\mathfrak{p}}}$.*

Beweis: Weil $\mathbb{Q}[\zeta]$ die n-ten Einheitwurzeln enthält, und p^{ν_p} ein Teiler von n ist, liegt η_j in $\widehat{\mathcal{O}}$. Um die Behauptung zu zeigen, zeigen wir, dass $\eta_j - 1$ in $\widehat{\mathfrak{p}}$ liegt. Dazu verwenden wir, dass $(X-1)^{p^{\nu_p}} \equiv X^{p^{\nu_p}} - 1 \pmod{p}$ per binomische Formel. Anders ausgedrückt ist $(X-1)^{p^{\nu_p}}$ von der Form $X^{p^{\nu_p}} - 1 + f$ für irgendein f aus $p\mathbb{Z}[X]$. Also gilt

$$(\eta_j - 1)^{p^{\nu_p}} = 0 + f(\eta_j)$$

für $f(\eta_j)$ in $p\widehat{\mathcal{O}}$. Deshalb ist $(\eta_j - 1)^{p^{\nu_p}}$ in $p\widehat{\mathcal{O}}$ enthalten, was wiederum in $\widehat{\mathfrak{p}}$ liegt. Deshalb ist $\eta_j - 1$ in $\widehat{\mathfrak{p}}$, was wir zeigen wollten. □

Satz 11 (Primideale in Kreisteilungskörpern): *Sei p eine Primzahl und es bezeichne $\nu_p = \max\{k \in \mathbb{N} \mid p^k \mid n\}$, $f_p = \min\{f \in \mathbb{N} \mid p^f \equiv 1 \pmod{n/p^{\nu_p}}\}$. Ist ζ eine n-te Einheitswurzel, dann ist*

$$p\mathcal{O}_K = (\widehat{\mathfrak{p}}_1 \cdots \widehat{\mathfrak{p}}_r)^{\varphi(p^{\nu_p})}$$

die Primidealzerlegung in $K = \mathbb{Q}[\zeta]$. Hierbei sind $\widehat{\mathfrak{p}}_1, \ldots, \widehat{\mathfrak{p}}_r$ paarweise verschiedene Primideale über $p\mathbb{Z}$ und der Trägheitsgrad ist f_p.

Zunächst stellen wir eine Vorüberlegung für den Beweis an. Für eine primitive n-te Einheitswurzel $\overline{\zeta}$ im algebraischen Abschluss von $\mathbb{F}_p$ möchten wir $[\mathbb{F}_p[\overline{\zeta}] : \mathbb{F}]$ bestimmen.

Sei dazu K ein Erweiterungskörper von $\mathbb{F}_p$ vom Grad h. Die Einheitengruppe $K^\times$ besteht aus Einheitswurzeln und ist zyklisch vom Grad $p^h - 1$. Genau dann enthält K eine primitive n-te Einheitswurzel, wenn $p^h - 1$ von n geteilt wird.

Der kleinste Körper, der $\overline{\zeta}$ enthält, hat nach unseren Überlegungen also Grad $\min\{f \mid p^f \equiv 1 \pmod{n}\}$. Weil dieser Körper $\mathbb{F}_p[\overline{\zeta}]$ ist, haben wir damit den Grad bestimmt, den wir bestimmen wollten.

Beweis: Die Strategie wird natürlich sein, Satz 9 zu verwenden, weil wir mit einer primitiven Körpererweiterung zu tun haben und das Minimalpolynom des primitiven Elements kennen. Im Folgenden schreiben wir $\widehat{\mathcal{O}} = \mathcal{O}_K$. Weil $\widehat{\mathcal{O}}_K = \mathbb{Z}[\zeta]$ ist, ist $\mathcal{F} = \widehat{\mathcal{O}}$ und Satz 9 kann auf alle Primelemente p in $\mathbb{Z}$ angewendet werden.

Sei $g = \Phi_n$ das Minimalpolynom von ζ in $\mathbb{Z}[X]$ und wie in Satz 9 bezeichne $\overline{g}$ das Bild von g in $\mathbb{F}_p[X]$. Wir wollen zeigen, dass $\overline{g}$ zerfällt als $\overline{g} = (\overline{p}_1 \cdots \overline{p}_r)^{\varphi(p^{\nu_p})}$, wobei $\overline{p}_1, \ldots, \overline{p}_r$ paarweise verschieden, irreduzibel und von Grad f_p sind.

Weil $\mathbb{Q}[\zeta]$ normal über $\mathbb{Q}$ ist, sind die Exponenten in der Primfaktorzerlegung von $\overline{g}$ alle gleich.

(i) Wir zeigen die Behauptung, falls p kein Teiler von n ist. Dann ist die Abbildung $\mu_n(\mathcal{O}_K) \to \mu_n(\mathcal{O}_K/\widehat{\mathfrak{p}})$, $a \mapsto \overline{a}$ ein Isomorphismus.

Die Abbildung ist injektiv, denn für ein a in $\mu_n(\mathcal{O}_K) - \{1\}$ ist Nullstelle von $h = X^{n-1} + X^{n-2} + \cdots + 1$. Wäre $a \equiv 1 \mod \widehat{\mathfrak{p}}$, dann wäre $O = h(a) \equiv n \pmod{\widehat{\mathfrak{p}}}$. Weil aber n nicht zu $p\mathbb{Z}$ gehört, gehört es erst recht nicht zu $\widehat{\mathfrak{p}}$.

Die Surjektivität folgt, weil alle beteiligten Gruppen endlich sind und Elemente gezählt werden können.

Insbesondere ist das Bild $\overline{\zeta}$ von ζ in $\mathcal{O}_K/\widehat{\mathfrak{p}}$ eine primitive n-te Einheitswurzel und für $\kappa(\widehat{\mathfrak{p}}) = \mathcal{O}_K/\widehat{\mathfrak{p}}$ gilt

$$\mathbb{Z}/n\mathbb{Z} \cong \mu_n(\kappa(\widehat{\mathfrak{p}})) \subseteq \kappa(\widehat{\mathfrak{p}})^\times$$

sodass $|\kappa(\widehat{\mathfrak{p}})| - 1$ von n geteilt wird. Deshalb gilt $\mathbb{F}_p \subseteq \mathbb{F}_p[\overline{\zeta}] \subseteq \kappa(\widehat{\mathfrak{p}})$, wobei $[\mathbb{F}_p[\zeta] : \mathbb{F}_p] = f_p$ per Vorüberlegung, d. h. $\mathbb{F}_p[\overline{\zeta}] \cong \mathbb{F}_{p^{f_p}}$.

Wir wollen zeigen, dass $\overline{\Phi}_n = \overline{p}_1 \cdots \overline{p}_r$ für paaarweise verschiedene irreduzible Polynome $\overline{p}_1, \ldots, \overline{p}_r$ vom Grad f_p. Dazu betrachten wir die Primfaktorzerlegung $\overline{\Phi}_n = \overline{p}_1 \cdots \overline{p}_r$ mit möglicherweise gleichen Faktoren.

Weil ζ eine Nullstelle von Φ_n ist, folgt, dass $\overline{\zeta}$ eine Nullstelle von $\overline{\Phi}_n$ ist. Deshalb ist $\overline{\zeta}$ Nullstelle eines der Primteiler $\overline{p}_i$. Weil die $\overline{p}_i$ aber irreduzibel in $\mathbb{F}_p[X]$ sind, muss dasjenige $\overline{p}_i$, das $\overline{\zeta}$ zur Nullstelle hat, das Minimalpolynom von $\overline{\zeta}$ sein. Entsprechend ist $[\mathbb{F}_p[\overline{\zeta}] : \mathbb{F}_p] = f_p$ per Vorüberlegung.

Andererseits hat $\overline{\Phi}_n$ nach der Vorüberlegung genau $\varphi(n)$ verschiedene Nullstellen, was genau der Grad von $\overline{\Phi}_n$ ist. Somit sind $\overline{p}_1, \ldots, \overline{p}_r$ verschieden.

(ii) Sei nun p ein Teiler von n und schreibe $n = p^{\nu_p} m$ mit $\mathrm{ggT}(m, p) = 1$. Weil wir in der Algebra etwas über den chinesischen Restsatz gelernt haben, wissen wir, dass $\mu_n \times \mu_{p^{\nu_p}} \to \mu_n$, $(\xi_i, \eta_j) \mapsto \xi_i \eta_j$ ein Isomorphismus von Gruppen ist. Wir können das Kreisteilungspolynom Φ_n schreiben als

$$\begin{aligned}\Phi_n &= \prod_{\substack{\xi_k \text{ primitive} \\ n\text{-te Einheitswurzel}}} (X - \xi_k) \\ &= \prod_{\substack{\xi \text{ primitiv in } \mu_m \\ \eta_j \text{ primitiv in } \mu_{p^{\nu_p}}}} (X - \xi_i \eta_j) = \prod_{\xi_i \text{ primitiv in } \mu_m} (X - \xi_i)^{\varphi(p^{\nu_p})} \pmod{\widehat{\mathfrak{p}}}.\end{aligned}$$

Hierbei ist $\widehat{\mathfrak{p}}$ eines der Primideale in $\mathcal{O}_K$ über $p\mathbb{Z}$. Die letzte Gleichheit in der obigen Gleichung kommt von Lemma II.15.5. Deshalb ist $\Phi_n \equiv \Phi_m^{\varphi(p^{\nu_p})} \pmod{p}$.

Bezeichnet $\overline{\Phi}_m$ das Bild von Φ_m in $\mathbb{F}_p[X]$, dann wissen wir aus Schritt (i), dass $\overline{\Phi}_m$ die Primfaktorzerlegung $\overline{\Phi}_m = \overline{p}_1 \cdots \overline{p}_r$ mit irreduziblen, paarweise verschiedenen Polynomen $\overline{p}_i$ von Grad f_p in $\mathbb{F}_p[X]$ hat. Damit erhalten wir die gewünschte Aussage für $\overline{\Phi}_n = (\overline{p}_1 \cdots \overline{p}_r)^{\varphi(p^{\nu_p})}$. □

Korollar II.15.6 (Verzweigtheit und Vollzerlegtheit):

(i) *Eine Primzahl p ist verzweigt in $\mathbb{Q}[\zeta_n]$ genau dann, wenn n von p geteilt wird und falls p nicht 2 oder $n \not\equiv 2 \pmod 4$ ist.*

(ii) *Sei $\mathbb{Q}[\zeta_n]$ ein echter Erweiterungskörper von $\mathbb{Q}$. Genau dann ist p vollzerlegt in $\mathbb{Q}[\zeta_n]$, wenn $p \equiv 1 \pmod n$ und $p \neq 2$.*

Beweis: (i) Für die Verzweigtheit müssen wir nichts weiter beachten, weil die Körpererweiterung $\kappa(\widehat{\mathfrak{p}})$ von $\mathbb{F}_p$ immer separabel sind. Wir müssen deshalb

nur zeigen, dass alle Verzweigungsindizes 1 sind. Es ist also p unverzweigt genau dann, wenn

$$1 = \varphi(p^{\nu_p}) = \begin{cases} p^{\nu_p - 1}(p-1), & \text{falls } \nu_p > 0, \\ 1, & \text{falls } \nu_p = 0. \end{cases}$$

Der untere Fall tritt genau dann ein, wenn p kein Teiler von n ist, und der obere Fall tritt genau dann ein, wenn $p = 2$ und $\nu_p = 1$, d. h. $n \equiv 2 \pmod 4$.

(ii) Genau dann ist p vollzerlegt, wenn p unverzweigt und $f_p = 1$ ist. Das ist äquivalent dazu, dass p unverzweigt und $p \equiv 1 \pmod{n/p^{\nu_p}}$. In (i) haben wir uns überlegt, wann p unverzweigt ist, und beide Bedingungen zusammen reduzieren sich auf $p \equiv 1 \pmod n$ oder $p = 2$ und $n = 2$. Aber $p = 2$ und $n = 2$ haben wir dadurch ausgeschlossen, dass wir eine echte Körpererweiterung haben wollen. □

Proposition II.15.7: *Seien nun $n = \ell$ prim, $\zeta = \zeta_\ell$, und $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell = (\frac{-1}{\ell})\ell$. Die Primzahl p ist vollzerlegt in $\mathbb{Q}[\sqrt{\ell^*}]$ genau dann, wenn p in $\mathbb{Q}[\zeta_\ell]$ in eine gerade Anzahl von Primidealen zerfällt.*

Beweis: Sei $\tau = \sum_{a \in \mathbb{F}_p^\times} (\frac{a}{\ell})\zeta_\ell^a$ die Gauß-Summe. Im Beweis des quadratischen Reziprozitätsgesetzes (Satz 10) haben wir uns überlegt, dass $\tau^2 = (\frac{-1}{\ell})\ell = \ell^*$. Insbesondere ist $\mathbb{Q}[\sqrt{\ell^*}] = \mathbb{Q}[\tau] \subseteq \mathbb{Q}[\zeta_\ell]$.

„$\Longrightarrow$“: Sei p vollzerlegt in $\mathbb{Q}[\tau]$, d. h. $p\mathcal{O}_{\mathbb{Q}[\tau]} = \widehat{\mathfrak{q}}_1\widehat{\mathfrak{q}}_2$ mit verschiedenen Idealen $\widehat{\mathfrak{q}}_1$, $\widehat{\mathfrak{q}}_2$. Die Gruppe $U = \mathrm{Gal}(\mathbb{Q}[\zeta_\ell]|\mathbb{Q}[\tau])$ hat Index 2 in der Galois-Gruppe $G = \mathrm{Gal}(\mathbb{Q}[\zeta_\ell] : \mathbb{Q})$. Ein σ_0 aus $G - U$ bildet die Primideale in $\mathbb{Q}[\zeta_\ell]$ über $\widehat{\mathfrak{q}}_1$ bijektiv auf die Primideale in $\mathbb{Q}[\zeta_\ell]$ über $\widehat{\mathfrak{q}}_2$ ab, weshalb die Anzahl der Primideale in $\mathbb{Q}[\zeta_\ell]$, die über p liegen, gerade ist.

„$\Longleftarrow$“: Die Anzahl sei gerade und es sei $\widehat{\mathfrak{p}}$ ein Primideal in $\mathbb{Q}[\zeta_\ell]$ über p. Die Zerlegungsgruppe $G_{\widehat{\mathfrak{p}}} = \mathrm{Stab}_G(\widehat{\mathfrak{p}})$ gehört zum Zerlegungskörper $Z_{\widehat{\mathfrak{p}}}$ und nach der Bahnformel ist $[G : G_{\widehat{\mathfrak{p}}}]$ die Länge der Bahn, also die Anzahl der Primideale über p.

Außerdem ist G zyklisch von Ordnung $\ell - 1$, worin $U = \mathrm{Gal}(\mathbb{Q}[\zeta_\ell]|\mathbb{Q}[\tau])$ mit Index 2 sitzt. Ferner ist $G_{\widehat{\mathfrak{p}}}$ eine Untergruppe von geradem Index, sodass $G_{\widehat{\mathfrak{p}}}$ in U enthalten sein muss. Nach dem Hauptsatz der Galois-Theorie ist deshalb $\mathbb{Q}[\tau]$ enthalten in $Z_{\widehat{\mathfrak{p}}}$.

Insgesamt erhalten wir den Körperturm $\mathbb{Q} \subseteq \mathbb{Q}[\tau] \subseteq Z_{\widehat{\mathfrak{p}}} \subseteq \mathbb{Q}[\zeta_\ell]$. Wir haben bereits gezeigt (Proposition II.14.5), dass p in $Z_{\widehat{\mathfrak{p}}}|\mathbb{Q}$ vollzerlegt ist. Erst recht ist p damit vollzerlegt in $\mathbb{Q}[\tau]$. □

Proposition II.15.8 (Bereinigtes Reziprozitätsgesetz): *Seien ℓ und p verschiedene ungerade Primzahlen und $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell = (\frac{-1}{\ell})\ell$. Dann gilt*

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell^*}{p}\right).$$

Beweis: Genau dann ist $(\frac{\ell^*}{p}) = 1$, wenn p in $\mathbb{Q}[\sqrt{\ell^*}]$ vollzerlegt ist. Nach Proposition II.15.7 ist das äquivalent dazu, dass p in $\mathbb{Q}[\zeta_\ell]$ in eine gerade Anzahl von Primidealen zerfällt.

Es bezeichne r die Anzahl der Primideale über p in $\mathbb{Q}[\zeta_\ell]$. In Satz 11 haben wir uns überlegt, dass $p\mathcal{O}_{\mathbb{Q}[\zeta_\ell]} = (\widehat{\mathfrak{p}}_1 \cdots \widehat{\mathfrak{p}}_r)^{\varphi(p^{\nu_p})}$, aber da p und ℓ teilerfremd sind, ist sogar $p\mathcal{O}_{\mathbb{Q}[\zeta_\ell]} = \widehat{\mathfrak{p}}_1 \cdots \widehat{\mathfrak{p}}_r$. Die Trägheitsgrad f_p von $p\mathcal{O}_{\mathbb{Q}[\zeta_\ell]}$ ist darüber hinaus gegeben durch $f_p = \min\{f \mid p^f \equiv 1 \pmod{\ell}\}$.

Nach der Verzweigungsformel ist $rf_p = [\mathbb{Q}[\zeta_\ell] : \mathbb{Q}] = \ell - 1$, was bedeutet, dass r genau dann gerade ist, wenn f_p ein Teiler von $(\ell-1)/2$ ist. Das ist erfüllt genau dann, wenn $(\frac{p}{\ell}) = p^{\frac{\ell-1}{2}} \equiv 1 \pmod{\ell}$.

Insgesamt erhalten wir so, dass $(\frac{\ell^*}{p}) = 1$ genau dann, wenn $(\frac{p}{\ell}) = 1$, und das wollten wir zeigen. □

Korollar II.15.9 (Reziprozitätsgesetz via Hilberts Verzweigungstheorie): *Aus Proposition II.15.8 lässt sich das quadratische Reziprozitätsgesetz ableiten.*

Beweis: Weil das Legendre-Symbol multiplikativ ist, liefert uns die obige Proposition die Gleichungskette

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell^*}{p}\right) = \left(\frac{(-1)}{p}\right)^{\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right).$$ □

Satz 12 (Dirichletscher Primzahlsatz): *Sei n eine natürliche Zahl. Es gibt unendlich viele Primzahlen p, sodass $p \equiv 1 \pmod{n}$.*

Bemerkung II.15.10: Sei Φ_n das n-te Kreisteilungspolynom in $\mathbb{Z}[X]$.

(i) Φ_n hat als konstanten Term ± 1.

(ii) Für jede ganze Zahl a ist $\Phi_n(a) \equiv \pm 1 \pmod{a}$.

(iii) Für jede natürliche Zahl N gibt es eine Primzahl $p \geq N$, sodass $\overline{\Phi}_n$ in $\mathbb{F}_p[X]$ eine Nullstelle besitzt.

Beweis: (i) Weil Φ_n ein Teiler von $X^n - 1$ ist, muss der konstante Term ± 1 sein.

(ii) Direkte Konsequenz von (i) durch Einsetzen von a.

(iii) Ein Primteiler p von $\phi_n(N!)$ leistet das Gewünschte. Zunächst sollten wir uns überlegen, dass $p > N$ sein muss. Wir wissen, dass $\Phi_n(N!) \equiv \pm 1 \pmod{N!}$, sodass insbesondere $\Phi_n(N!) \equiv \pm 1 \pmod{x}$ für jeden Teiler x von $N!$ mit $1 \leq x \leq N$. Deshalb kann x nicht von p geteilt werden, sodass $p > N$. Weil p ein Teiler von $\Phi_n(N!)$ ist, ist $N!$ eine Nullstelle von Φ_n. □

Beweis: Im Folgenden sei p stets eine ungerade Primzahl. Wegen Korollar II.15.6 ist $p \equiv 1 \pmod{n}$ genau dann, wenn p in $\mathbb{Q}[\zeta_n]$ vollzerlegt ist.

Es genügt deshalb zu zeigen, dass es unendlich viele Primzahlen p gibt, die in $\mathbb{Q}[\zeta_n]$ vollzerlegt sind. Dazu verwenden wir Satz 9 und betrachten $\overline{\Phi}_n$ in $\mathbb{F}_p[X]$. Wegen der Verzweigungsformel brauchen wir, dass $\overline{\Phi}_n$ zerfällt als $\overline{\Phi}_n = \overline{g}_1 \cdots \overline{g}_r$ mit $\deg(\overline{g}_1) = \cdots = \deg(\overline{g}_r)$.

Genau dann ist also p vollzerlegt, wenn $\overline{\Phi}_n$ über $\mathbb{F}_p$ in Linearfaktoren zerfällt. Dazu genügt es zu zeigen, dass $\overline{\Phi}_n$ in $\mathbb{F}_p$ eine Nullstelle hat, weil $\mathbb{Q}[\zeta_n]$ eine normale Erweiterung von $\mathbb{Q}$ ist.

Wegen Bemerkung II.15.10 gibt es unendlich viele solche Primzahlen p. □

16 Fermats Problem

Fermats Vermutung war, dass es für $n \geq 3$ keine ganzen Zahlen a, b und c geben kann, sodass $a^n + b^n = c^n$. Wir wollen sehen, wie weit die erlernten Methoden dazu reichen, gewisse Argumente zu geben.

Satz 13 (Fermat für reguläre Primzahlen): *Wir setzen voraus, dass $p \geq 5$ eine reguläre Primzahl ist, d. h. für $K = \mathbb{Q}[\zeta_p]$ wird $|\mathrm{C}\ell_K|$ nicht von p geteilt. Dann gibt es keine positiven ganzen Zahlen x, y und z, sodass $x^p + y^p = z^p$, falls xyz nicht von p geteilt wird.*

Seien x und y von Null verschieden, ζ eine p-te primitive Einheitswurzel und $\hat{y} = -y$. Dann können wir schreiben

$$\begin{aligned} x^p + y^p &= x^p - \hat{y}^p \\ &= \hat{y}^p \left(\left(\frac{x}{\hat{y}} \right)^p - 1 \right) \\ &= \hat{y}^p \left(\frac{x}{\hat{y}} - 1 \right) \cdots \left(\frac{x}{\hat{y}} - \zeta^{p-1} \right) = (x - \hat{y}) \cdots (x - \hat{y}\zeta^{p-1}) = \prod_{k=0}^{p-1} (x + y\zeta^k) \end{aligned}$$

In der Vorbereitung für den Beweis halten wir ein paar Fakten fest, die wir nun zwar aus zeitlichen Gründen nicht mehr zeigen können, aber mit den erlernten Methoden zeigen könnten.

Bemerkung II.16.1: (i) Wenn xyz nicht von p geteilt wird, dann sind die Hauptideale $(x+y)$, …, $(x+\zeta^{p-1}y)$ teilerfremd.

(ii) Seien G eine endliche Gruppe, und p eine Primzahl, die $|G|$ nicht teilt. Ist g ein Element von G und gilt $g^p = 1$, dann ist $g = 1$. Das ist eine direkte Konsequenz aus dem Satz von Lagrange.

Wird also $|\mathrm{C}\ell_K|$ nicht von p geteilt, und sind I ein Hauptideal, sowie J ein Ideal mit $J^p = I$, dann muss J bereits ein Hauptideal gewesen sein.

(iii) Ist p eine ungerade Primzahl, dann ist jede Einheit von $\mathbb{Z}[\zeta]$ von der Gestalt $\zeta^g r$ für eine reelle Zahl r und $0 \leq g \leq p-1$.

(iv) Über dem Primideal p liegt das Primideal $(1-\zeta)$ in $\mathbb{Q}[\zeta_p]$ und wegen $e = \varphi(p) = p-1$ sind $f = r = 1$ nach der Verweigungsformel.

Da $f = 1$ ist, gilt $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{F}_p$. Für jedes α in $\mathbb{Z}[\zeta]$ gibt es deshalb eine ganze Zahl k, sodass $\alpha \equiv k \pmod{1-\zeta}$. Für jedes α in $\mathbb{Z}[\zeta]$ gibt es deshalb eine ganze Zahl m mit $\alpha^p \equiv m \pmod{\mathbb{Z}[\zeta]}$.

(v) $\zeta + 1$ ist eine Einheit.

(vi) Im Beweis von Satz 13 dürfen wir ohne Einschränkung annehmen, dass $x \not\equiv y \pmod{p}$. Ist nämlich $x \equiv y \equiv -z \pmod{p}$, dann ist $z \equiv z^p \equiv x^p + y^p \equiv x + y = -2z \pmod{p}$ und $3z \equiv 0 \pmod{p}$, was der Annahme $p \geq 5$ und $p \nmid z$ widerspricht.

Beweis (Satz 13): Sei $I_k = (x+\zeta^k y) \subset \mathbb{Z}[\zeta]$. Nach der Vorüberlegung ist $(z)^p = (z^p) = (x^p + y^p) = I_0 \cdots I_{p-1}$. Wegen Bemerkung II.16.1 wissen wir, dass $I_0, \ldots, I_{p-1}$ p-te Potenze sind, d. h. $I_k = (J_k)^p$ für irgendwelche Ideale J_k.

Nach (ii) aus der Vorüberlegung ist $J_k = (\alpha_k)$ für ein $\alpha_k \in \mathbb{Z}[\zeta]$ und somit $x + \zeta^k y = \varepsilon \alpha_k^p$ für ε in $\mathbb{Z}[\zeta]^\times$. Wegen (iii) ist $x + \zeta y = \zeta^g r \alpha_1^p$ für eine reelle Zahl r. Es ist also $\zeta^{-g}(x+\zeta y) \equiv rm \pmod{p\mathbb{Z}[\zeta]}$ für eine ganze Zahl m. Komplexe Konjugation liefert jetzt, dass $\zeta^g(x+\zeta^{-1}y) \equiv rm \pmod{p\mathbb{Z}[\zeta]}$. Damit erhalten wir

$$x + \zeta y - \zeta^{2g} x - \zeta^{2g-1} y \equiv 0 \pmod{p\mathbb{Z}[\zeta_p]}.$$

Nun unterscheiden wir Fälle, um diese Linearkombination von Erzeugern zu untersuchen

(i) Ist $g = 0$, dann ist $(\zeta - \zeta^{-1})y \equiv 0 \pmod{p\mathbb{Z}[\zeta]}$. Weil $\zeta^2 - 1) = (\zeta-1)(\zeta+1)$ und $(\zeta+1)$ Einheiten sind, muss bereits $\zeta y - y = (\zeta-1)y \equiv 0 \pmod{p\mathbb{Z}[\zeta]}$ gelten, was wegen $p \nmid y$ den Voraussetzungen widerspräche.

(ii) Ist $g = 1$, dann führen ähnliche Argumente auf einen Widerspruch.

(iii) Ist $g > 1$, dann muss gelten, dass $2g - 1$ von p geteilt werden. In dem Fall ist nämlich $\zeta^{2g-1} = 1 \pmod{p\mathbb{Z}[\zeta]}$ und $(x-y)+(y-x)\zeta \equiv 0 \pmod{p\mathbb{Z}[\zeta]}$. Koeffizientenvergleich liefert dann $p \mid (x - y)$, sodass $x \equiv y \pmod{p}$; aber das haben wir ausgeschlossen, siehe (iv) aus der vorangegangenen Bemerkung. □