Algebraische Zahlentheorie

gehalten von Prof. Dr. Brandhorst im SS '20

UNIVERSITÄT
DES
SAARLANDES

Hinweise zu Schreibfehlern an s9fhguen@stud.uni-saarland.de.

Inhaltsverzeichnis

Kapitel I.

Einführung und Ausblick

Ist m eine ganze Zahl, dann gibt es nach dem Fundamentalsatz der Aritmetik eine natürliche Zahl n und Primzahlen $p_1, \ldots, p_n$ sodass $m = \pm \prod_{i=1}^{n} p_i$.

Ist allgemeiner A ein Integritätsbereich und $a \in A$, dann heißt a eine *Einheit*, falls es ein inverses Element $b \in A$ bezüglich der Multiplikation besitzt, d. h. $ab = 1$. Wir schreiben $A^\times$ für die Einheitengruppe von A. Ein Element $\pi \in A$ heißt *Primelement*, falls gilt: „Sind $a, b \in A$, dann gilt: Ist $\pi \mid ab$, so ist $\pi \mid a$ oder $\pi \mid b$“.

Ist A ein Hauptidealring, so ist jedes $a \in A$ ein Produkt $a = u\pi_1 \cdots \pi_n$ mit $u \in A^\times$ und Primelementen $\pi_1, \ldots, \pi_n \in A$. Die Faktorisierung ist eindeutig bis auf Reihenfolge und Ersetzen von π_i durch $v\pi_i$, wobei $v \in A^\times$.

Wir wollen uns zunächst mit der Frage beschäftigen, inwieweit wir eine Primfaktorzerlegung in einem Zahlkörper K haben. Dabei stoßen wir auf folgende Probleme:

(i) Ein Faktorisierungsbegriff für Körper ergibt nur Sinn in Teilringen, z. B. $\mathbb{Z} \subseteq \mathbb{Q}$. Wir brauchen also ein Analogon $\mathcal{O}_K$ für den Ring der ganzen Zahlen.

(ii) Da die eindeutige Primfaktorzerlegung im Allgemeinen nicht gilt, brauchen wir ein Maß inwieweit sie fehlt. Das wird auf den Begriff der „Klassengruppe“ führen.

(iii) Die Faktorisierung ist nur bis auf Einheiten eindeutig. Für ein vollständiges Verständnis der Arithmetik unseres Zahlkörpers K brauchen wir die Struktur der Einheitengruppe $\mathcal{O}_K^\times$.

1. Der Ring der ganzen Zahlen eines Zahlkörpers

Sei K ein algebraischer Zahlkörper, d. h. eine endliche Körpererweiterung von $\mathbb{Q}$. Jedes Element $\alpha \in K$ erfüllt eine Gleichung $0 = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$ mit rationalen Zahlen $a_0, \ldots, a_{n-1}$. Eine Zahl α heißt *ganzalgebraisch*, falls die Koeffizienten $a_0, \ldots, a_{n-1}$ ganze Zahlen sind.

Beispiel I.1: Es sei $K = \mathbb{Q}(\sqrt{d})$, wobei d eine quadratfreie ganze Zahl sei. Dann ist jedes Element $\alpha \in K$ von der Form $\alpha = a + b\sqrt{d}$. Ist $\alpha = a + b\sqrt{d}$ mit $b \neq 0$, dann ist

$$p_\alpha = X^2 - 2aX + (a^2 - db^2).$$

Es ist $\alpha \in \mathcal{O}_K$ genau dann, wenn $2a \in \mathbb{Z}$ und $a^2 - db^2 \in \mathbb{Z}$. Damit ist

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

Beispiel I.2: Seien d eine ganze Zahl und $\zeta_d = \exp(2\pi\mathrm{i}/d)$. Ist $k = \mathbb{Q}[\zeta_d]$, dann ist $\mathcal{O}_K = \mathbb{Z}[\zeta_d]$. Details später.

2. Faktorisierung

Sei A ein Integritätsbereich. Ein Element $a \in A$ heißt *irreduzibel*, falls gilt: „Sind $b, c \in A$ und ist $a = bc$, dann ist $b \in A^\times$ oder $c \in A^\times$“. Nun ist A *faktoriell*, falls jedes Element eine eindeutige Zerlegung in irreduzible Elemente besitzt. Ist $\mathcal{O}_K$ faktoriell? Im Allgemeinen nicht.

Beispiel I.3: Wir betrachten den Ring $R = \mathbb{Z}[\sqrt{-5}]$. Dann sind

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

Faktorisierungen in irreduzible Elemente. Die Elemente $2, 3, 1 \pm \sqrt{-5}$ sind irreduzibel und paarweise nicht assoziiert. Um das einzusehen, benutzen wir die *Normabbildung*

$$N\colon \mathbb{Q}[\sqrt{-5}] \longrightarrow \mathbb{Q}, \qquad a + b\sqrt{-5} \longmapsto a^2 + 5b^2$$

Die Normabbildung ist multiplikativ. Ein Element $\alpha \in R$ ist eine Einheit genau dann, wenn $N(\alpha) = 1$, d. h. $R^\times = \{\pm 1\}$.

Angenommen $1 + \sqrt{-5} = \alpha\beta$, dann ist $N(1+\sqrt{-5}) = 6 = N(\alpha)N(\beta)$. Damit muss $N(\alpha) \in \{1, 2, 3, 6\}$ gelten. Die Zahlen 2 und 3 sind nicht in der Form $a^2 + 5b^2$ mit ganzen Zahlen a und b darstellbar. Ist $N(\alpha) = 1$, dann ist α

eine Einheit und ist $N(\alpha) = 6$, dann ist β eine Einheit. Folglich ist $1 + \sqrt{-5}$ irreduzibel. Völlig analog geht man die Elemente $2, 3, 1 - \sqrt{-5}$ durch.

Zwei Elemente a, b aus R sind assoziiert, wenn es $u \in R^\times$ mit $au = b$ gibt. Damit ist $N(au) = N(a)N(u) = N(b)$ und wegen $N(u) \in \{\pm 1\}$ sind insbesondere $1 \pm \sqrt{-5}$ nicht assoziiert zu 2 oder 3 und $1 + \sqrt{-5}$ ist nicht assoziiert zu $1 - \sqrt{-5}$.

Wir lesen aus $R^\times = \{\pm 1\}$ außerdem ab: Ein Element $\alpha \in R$ ist genau zu α und $-\alpha$ assoziiert.

Was geht in diesem Beispiel schief? In R sind nicht alle irreduziblen Elemente auch prim. Im Beispiel teilt $1 + \sqrt{-5}$ zwar $6 = 2 \cdot 3$, aber $1 + \sqrt{-5} \nmid 2, 3$.

Was können wir retten? Betrachte $210 = 6 \cdot 35 = 10 \cdot 21$. Naiv gesprochen ist die Faktorisierung nicht eindeutig in $\mathbb{Z}$. Tatsächlich ist

$$210 = (2 \cdot 3) \cdot (5 \cdot 7) = (2 \cdot 5) \cdot (3 \cdot 7).$$

Der Mathematiker Kummer hatte dazu die Idee, dass mehr Primzahlen erforderlich sind. Im Beispiel $6 = (p_1 \cdot p_2) \cdot (p_3 \cdot p_4) = (p_1 \cdot p_3) \cdot (p_2 \cdot p_4)$. Diese p_i hat Kummer „ideale Primfaktoren“ genannt. Was soll ein „idealer Faktor“ $\mathfrak{a}$ sein?

(i) $\mathfrak{a}$ soll durch die ganzalgebraischen Zahlen, die es teilt, bestimmt sein.

(ii) Teilbarkeit soll wie gewohnt funktionieren, d. h. $\mathfrak{a} \mid 0$, „Sind $a, b \in \mathcal{O}_K$ und gilt $\mathfrak{a} \mid a$ und $\mathfrak{a} \mid b$, dann gilt $\mathfrak{a} \mid a \pm b$“ und „Sind $a, b \in \mathcal{O}_K$ und gilt $\mathfrak{a} \mid a$, dann gilt für alle $b \in \mathcal{O}_K$ auch $\mathfrak{a} \mid ab$“.

(iii) $\mathfrak{a}$ soll prim sein, falls gilt: „Sind $a, b \in \mathcal{O}_K$ und gilt $\mathfrak{a} \mid ab$, dann gilt $\mathfrak{a} \mid a$ oder $\mathfrak{a} \mid b$“.

Dedekinds Vorschlag für ideale Faktoren war: Definiere $\mathfrak{a}$ als Teilmenge von $\mathcal{O}_K$ und setze $\mathfrak{a} \mid b$ genau dann, wenn $b \in \mathfrak{a}$. Heutzutage nennen wir „ideale Faktoren“ schlicht Ideale. Ideale Primfaktoren heißen heutzutage Primideale.

Sind $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ Ideale, dann heißt

$$\mathfrak{ab} := \left\{ \sum_i a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

das *Produkt der Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$. Sind $\mathfrak{a} = (a_1, \ldots, a_n)$ und $\mathfrak{b} = (b_1, \ldots, b_m)$, dann ist

$$\mathfrak{ab} = (a_1 b_1, \ldots, a_i b_j, \ldots, a_n b_m).$$

Mit der neuen Definition retten wir die eindeutige Faktorisierung: Das von α erzeugte Hauptideal (α) ist das Produkt $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ für Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq \mathcal{O}_K$.

Im Beispiel ist

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) =: \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

Genauer sind $\mathfrak{p}_1\mathfrak{p}_2 = (2)$, $\mathfrak{p}_3\mathfrak{p}_4 = (3)$, $\mathfrak{p}_1\mathfrak{p}_3 = (1 + \sqrt{-5})$ und $\mathfrak{p}_2\mathfrak{p}_4 = (1 - \sqrt{-5})$. Wir rechnen zum Beispiel nach, dass

$$(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (4, 2 - 2\sqrt{-5}, 2 + 2\sqrt{-5}, 6) \subseteq (2),$$

da jeder Erzeuger von 2 geteilt wird.

Umgekehrt ist $2 = 6 - 4 \in (4, 2 - 2\sqrt{-5}, 2 + 2\sqrt{-5}, 6)$, was die andere Inklusion zeigt.

Die Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ sind prim. Zum Beispiel da

$$\mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-5}]/(3, 1 - \sqrt{-5})$$

surjektiv ist und den Kern (3) hat, gilt $\mathbb{Z}[\sqrt{-5}]/(3, 1 - \sqrt{-5}) \cong \mathbb{Z}/(3)$. Weiter ist $\mathbb{Z}/(3)$ ein Integritätsbereich, also ist $\mathfrak{p}_2$ prim. Da $\mathbb{Z}/(3)$ sogar ein Körper ist, ist $(3, 1 - \sqrt{-5})$ tatsächlich ein *maximales Ideal*.

Wie weit haben wir uns von dem entfernt, was wir eigentlich wollten; nämlich der Primfaktorzerlegung von Elementen? In anderen Worten. Wie viele „ideale Zahlen“ haben wir den „echten Zahlen“ hinzugefügt? In gewissem Sinne nur endlich viele: Es gibt eine endliche Menge S von Idealen, sodass jedes Ideal von der Form $\mathfrak{a}(a)$ für $\mathfrak{a} \in S$ und $a \in \mathcal{O}_K$ ist. Noch besser: Wir konstruieren eine Gruppe $\mathfrak{I}$ von „gebrochenen Idealen“, in der die gebrochenen Hauptideale $(a) = a\mathcal{O}_K$ für $a \in K^\times$ eine Untergruppe P von endlichem Index bilden.

Der Index von $[\mathfrak{I} : P]$ heißt die *Klassenzahl* h_K von K. Wir werden sehen, dass $h_K = 1$ genau dann gilt, wenn $\mathcal{O}_K$ ein Hauptidealring ist und dass $h_K = 1$ genau dann gilt, wenn $\mathcal{O}_K$ faktoriell ist.

3. Einheiten

Anders als der Ring der ganzen Zahlen $\mathbb{Z}$ kann $\mathcal{O}_K$ unendlich viele Einheiten haben. Zum Beispiel ist $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ eine Einheit $[(1 + \sqrt{2})(-1 + \sqrt{2}) = 1]$, und $1 + \sqrt{2}$ hat unendliche Ordnung, denn $(1 + \sqrt{2})^m \neq 1$ für alle $m \in \mathbb{Z} - \{0\}$.

Genauer haben wir den folgenden Fakt: $\mathbb{Z}[\sqrt{2}] = \{\pm(1 + \sqrt{2})^m \mid m \in \mathbb{Z}\}$.

Bezeichnet $P(K)$ die Gruppe der Einheitswurzeln von k, dann haben wir als abelsche Gruppen die Isomorphie $\mathcal{O}_K^\times \cong P(k) \times \mathbb{Z}^r$.

Einige Anwendungen der Theorie sind:

(i) Mit algebraischer Zahlentheorie lässt sich ein Algorithmus zur Bestimmt und Galoisgruppen für beliebige algebraische Körper formulieren.

(ii) Fermats letzter Satz (1637): Für eine ganze Zahl $m \geq 3$ hat die Gleichung $x^m + y^m = z^m$ keine Lösung $(x, y, z) \in \mathbb{Z}^3$ mit $xyz \neq 0$.

Der Versuch, Fermats letzten Satz zu beweisen, war eine Motivation zur Entwicklung der Algebraischen Zahlentheorie. Der Beweis von Andrew Wiles (1994) geht über die Methoden der Algebraischen Zahlentheorie hinaus.

Satz I.4 (Fermat für $n = 3$): *Die Gleichung $x^3 + y^3 + z^3 = 0$ hat keine ganzzahligen nicht-trivialen Lösungen, d. h. $xyz \neq 0$.*

Der Beweis dieses Satzes erfordert einiges an Vorbereitung. Im Folgenden bezeichne $\omega = (-1 + \sqrt{3})/2 = \exp(2\pi\mathrm{i}/3)$ eine dritte Einheitswurzel, d. h. $\omega^2 + \omega + 1 = 0$. Setzen wir $\alpha = -x/y$, dann können wir die Lösungen der Gleichung $\alpha^3 - 1$ mit ω direkt angeben, es ist nämlich

$$\alpha^3 - 1 = (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2).$$

Damit schreiben wir die Gleichung aus Satz I.4 um zu

$$-z^3 = (x + y)(x + \omega y)(x + \omega^2 y).$$

Der Ring $\mathbb{Z}[\omega]$ ist ein euklidischer Ring, insbesondere also ein Hauptidealring und damit gibt es in $\mathbb{Z}[\omega]$ eine eindeutige Primfaktorzerlegung. Die zugehörige Normfunktion ist

$$N(a + b\omega) = a^2 - ab + b^2 = |a + b\omega|^2.$$

Die Einheiten in $\mathbb{Z}[\omega]$ sind $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$. Setzen wir $\lambda := 1 - \omega$, dann ist $N(\lambda) = 3$, d. h. λ muss ein Primelement in $\mathbb{Z}[\omega]$ sein. Wir haben $\mathbb{Z}[\omega]/(\lambda) = \{[-1], [0], [1]\}$.

Lemma I.5: *Sei $x \in \mathbb{Z}[\omega]$ mit $x \nmid \lambda$. Dann ist $x^3 \equiv \pm 1 \pmod{\lambda^4}$.*

Beweis: Es genügt den Fall $x \equiv 1 \pmod{\lambda}$ zu zeigen. Andernfalls ersetze x durch $-x$. Schreibe also $x = 1 + b\lambda$ mit $b \in \mathbb{Z}[\omega]$. Dann ist

$$\begin{aligned} x^3 - 1 &= (1 + b\lambda - 1)(1 + b\lambda - \omega)(1 + b\lambda - \omega^2) \\ &= b\lambda(\lambda + b\lambda)(-\omega^2\lambda + b\lambda) \\ &= \lambda^3 b(1 + b)(b - \omega^2) \end{aligned}$$

Nun sind b, $1+b$, $b-\omega^2$ modulo λ paarweise verschieden, also ist $[b][1+b][b-\omega^2] = [0]$. Das erzwingt aber $x^3 - 1 \equiv 0 \pmod{\lambda^4}$. □

Gilt $\lambda \nmid xyz$, so ist

$$x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \equiv \pm 1 \text{ oder } \pm 3 \not\equiv 0 \pmod{\lambda^3}.$$

Ist also $x^3 + y^3 + z^3 = 0$ mit $xyz \neq 0$, so folgt dass λ eines der x, y, z teilt. Ohne Beschränkung der Allgemeinheit teile λ unser z, also $z = \lambda^n \hat{z}$ mit $\lambda \nmid \hat{z}$ und $n \geq 1$.

Lemma I.6: *Sind $x, y, \hat{z} \in \mathbb{Z}[\omega]$ mit $xyz \neq 0$ eine Lösung von*

$$x^3 + y^3 + \varepsilon\lambda^{3n}\hat{z}^3 = 0,$$

wobei $\varepsilon \in \mathbb{Z}[\omega]^\times$, $\lambda \nmid \hat{z}$, $n \geq 1$ und $\mathrm{ggT}(x, y) = 1$, so folgt $n \geq 2$.

Beweis: Seien $x, y, \hat{z}$ und ε wie im Lemma. Dann ist

$$-\varepsilon\lambda^{3n}\hat{z}^3 \equiv x^3 + y^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}.$$

Da ± 2 nicht durch λ teilbar ist, folgt $-\varepsilon\lambda^{3n}\hat{z}^3 \equiv 0 \pmod{\lambda^4}$ und damit ist $n \geq 2$. □

Lemma I.7: *Seien $x, y, \hat{z} \in \mathbb{Z}[\omega]$ sodass $\lambda \nmid xy\hat{z}$ paarweise teilerfremde Lösungen von $x^3 + y^3 + \varepsilon\lambda^{3n}\hat{z}^3 = 0$ für $n \geq 2$ und $\varepsilon \in \mathbb{Z}[\omega]^\times$. Dann gibt es $x', y', \hat{z}' \in \mathbb{Z}$ paarweise teilerfremd mit $\lambda \nmid x'y'\hat{z}'$ und $\varepsilon' \in \mathbb{Z}[\omega]^\times$, sodass $x'^3 + y'^3 + \varepsilon'\lambda^{3(n-1)}\hat{z}'^3 = 0$ gilt.*

Beweis: Seien $x, y, \hat{z}$ und ε wie im Lemma. Aus $1 \equiv \omega \equiv \omega^2 \pmod{\lambda}$ folgt $x + y \equiv x + \omega y \equiv x + \omega^2 y \pmod{\lambda}$. Also ist

$$-\varepsilon\lambda^{3n}\hat{z}^3 \equiv (x + y)(x + \omega y)(x + \omega^2 y).$$

Da die linke Seite kongruent zu Null modulo λ ist, ist wenigstens einer der Faktoren auf der rechten Seite ein Vielfaches von λ. Nach Voraussetzug ist jeder Faktor damit ein Vielfaches von λ.

Die Quotienten $(x + y)/\lambda$, $(x + \omega y)/\lambda$ und $(x + \omega^2 y)/\lambda$ sind paarweise teilerfremd, denn

$$x + y - (x + \omega y) = \lambda y, \qquad \omega(x + y) - (x + \omega y) = -\lambda x,$$

und damit ist $\mathrm{ggT}((x + y)/\lambda, (x + \omega y)/\lambda) \mid \mathrm{ggT}(x, y) = 1$. Für die anderen Paare verfährt man analog.

In der Faktorisierung

$$-\varepsilon\lambda^{3(n-1)}\hat{z}^3 = \left(\frac{x + y}{\lambda}\right)\left(\frac{x + \omega y}{\lambda}\right)\left(\frac{x + \omega^2 y}{\lambda}\right)$$

ist genau ein Faktor durch $\lambda^{3(n-1)}$ teilbar. Wir nehmen an, dies ist $(x+y)/\lambda$. Andernfalls ersetzen wir y durch ωy oder $\omega^2 y$. Jetzt sind

$$x+y=\varepsilon_1\lambda^{3(n-2)}a^3, \quad x+\omega y=\varepsilon_2\lambda b^3, \quad x+\omega^2 y=\varepsilon_3\lambda c^3$$

mit Einheiten $\varepsilon_1,\varepsilon_2,\varepsilon_3\in\mathbb{Z}[\omega]^\times$ und paarweise teilerfremden Eisensteinzahlen $a,b,c\in\mathbb{Z}[\omega]$, sodass $\lambda\nmid abc$. Daraus erhalten wir

$$0=x+y+\omega(x+\omega y)+\omega^2(x+\omega^2 y)=\varepsilon_1\lambda^{3n-2}a^3+\varepsilon_2\omega\lambda b^3+\varepsilon_3\omega^2\lambda c^3.$$

Also folgt $0=c^3+\varepsilon_4 b^3+\varepsilon_5\lambda^{3n-1}a^3$ mit $\lambda\nmid a,b,c$ und $\varepsilon_4,\varepsilon_5\in\mathbb{Z}[\omega]^\times$. Modulo λ^2 ergibt sich

$$0\equiv c^3+\varepsilon_4 b^3\equiv\pm1\pm\varepsilon_4 \pmod{\lambda^2}.$$

Einsetzen von $\varepsilon_4\in\{\pm1,\pm\omega,\pm\omega^2\}$ liefert $\varepsilon_4=\pm1$. Mit $x'=c$, $y'=\varepsilon_4 b$ und $\hat{z}'=a$ erhalten wir $x'^3+y'^3+\varepsilon_5\lambda^{3(n-1)}\hat{z}'^3=0$. □

Beweis (Satz I.4): Wir zeigen allgemeiner: Die Gleichung $x^3+y^3+\varepsilon z^3=0$ hat keine Lösung $x,y,z\in\mathbb{Z}[\omega]$ und $\varepsilon\in\mathbb{Z}[\omega]^\times$ mit $xyz\neq0$. Nach den vorherigen Überlegungen wissen wir, dass wir ohne Beschränkung der Allgemeinheit annehmen können, dass $z=\lambda^{3n}\hat{z}$ mit $n\geq2$. Wir erhalten eine Lösung von

$$x^3+y^3+\varepsilon\lambda^{3n}\hat{z}^3=0. \tag{I.1}$$

Sei nun n minimal, sodass Gl. (I.1) eine Lösung $x,y,\hat{z}\in\mathbb{Z}[\omega]$, sodass $x,y,\hat{z}$ paarweise teilerfremd und alle verschieden von Null sind und mit $\varepsilon\in\mathbb{Z}[\omega]^\times$. Nach Lemma I.7 hat nun Gl. (I.1) auch für $n-1$ eine Lösung im Widerspruch zur Minimalität von n. □

4. Kettenbrüche und Pellsche Gleichung

Das Leitproblem dieses Abschnitts ist, alle ganzzahligen Lösungen der Pellschen Gleichung $x^2-dy^2=1$ für ganzzahlige d zu finden.

Bemerkung I.8: Ist c eine ganze Zahl und $d=c^2$, dann hat die Gleichung $x^2-dy^2=(x-cy)(x+cy)=1$ genau die Lösungen $(x,y)=(\pm1,0)$.

Wir beschränken uns also im Folgenden auf den Fall, dass d kein Quadrat ist. Der Zusammenhang zwischen der Pellschen Gleichung

$$x^2-dy^2=(x+\sqrt{d}y)(x-\sqrt{d}y)=1$$

und dem Ganzheitsring O_K, wobei $K = \mathbb{Q}[\sqrt{d}]$, erschließt sich in der Faktorisierung: Die Lösungen dieser Gleichung geschrieben als $x + \sqrt{d}y$ sind genau die Einheiten von $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$ der Norm 1. Die Lösungen der Pellschen Gleichung bilden als Kern eines Gruppenhomomorphismus also eine Untergruppe von $\mathbb{Z}[\sqrt{d}]^\times$.

Definition I.9 (Kettenbrüche): Der endliche Kettenbruch $[a_0, \ldots, a_n]$ mit Teilnennern $a_i \in \mathbb{R}$, $a_i > 0$ für $i \geq 1$, ist rekursiv definiert durch

$$[a_0] := a_0, \quad [a_0, \ldots, a_{n+1}] = [a_0, \ldots, a_n + 1/a_{n+1}] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}.$$

Algorithmus I.10 (Kettenbruchalgorithmus): Sei α eine irrationale Zahl. Schreibe $\lfloor \alpha \rfloor := \max\{z \in \mathbb{Z} \mid z \leq \alpha\}$ für die Gaußklammer und $\{\alpha\} - \alpha - \lfloor \alpha \rfloor$ für den nichtganzen Anteil von $\alpha =: \beta_0$.

(i) Setze $a_0 := \lfloor \alpha \rfloor$, $\beta_1 = 1/(\alpha - a_0) = 1/\{\alpha\}$. Es gilt $\alpha = [a_0, \beta_1]$;

(ii) Für $n \geq 1$ setze $a_n := \lfloor \beta_{n+1} \rfloor$, $\beta_n := 1/(\beta_n - \lfloor \beta_n \rfloor) = 1/\{\beta_n\}$. Es gilt $\alpha = [a_0, \ldots, a_n, \beta_{n+1}]$.

Beispiel I.11: Sei $\alpha = \sqrt{2} \approx 1{,}414\,2\ldots$ Dann sind

- $a_0 = 1$, $\beta_1 = \sqrt{2} + 1$,
- $a_1 = \lfloor \beta_1 \rfloor = 2$, $\beta_2 = \sqrt{2} + 1$,
- $a_2 = 2$, $\beta_3 = \sqrt{2} + 1$,

und so weiter. Die Kettenbruchentwicklung von $\sqrt{2}$ ist also $[1, 2, 2, \ldots] = [1, \overline{2}]$.

Satz I.12: *Seien $a_1, \ldots, a_n$ reelle Zahlen und seien $a_i > 0$ für $i \geq 1$. Setze $p_{-2} = 0$, $q_{-2} = 1$, $p_{-1} = 1$ und $q_{-1} = 0$. Definiere induktiv*

$$\begin{pmatrix} p_{i+1} & p_i \\ q_{i+1} & q_i \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} \begin{pmatrix} a_{i+1} & 1 \\ 1 & 0 \end{pmatrix} = \prod_{j=0}^{i+1} \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix}.$$

Dann gilt $[a_0, \ldots, a_n] = p_n/q_n$.

Beweis: Ausgeschrieben sind $p_{i+1} = a_{i+1}p_i + p_{i-1}$ und $q_{i+1} = a_{i+1}q_i + q_{i-1}$. Wir zeigen die Behauptung via Induktion nach i.

Für $i = 0$ haben wir $[a_0] = \frac{a_0 1 + 0}{0 + 1} = \frac{p_0}{q_0}$. Für $i = 1$ haben wir

$$\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1 0 + a_1} = a_0 + \frac{1}{a_1} = [a_0, a_1].$$

Sei die Behauptung wahr für alle Kettenbrüche der Länge kleinergleich i. Dann ist

$$\begin{aligned}[a_0,\dots,a_{i+1}] &= [a_0,\dots,a_i+\frac{1}{a_{i+1}}]\\ &= [a_0',\dots,a_i']\\ &= \frac{p_i'}{q_i'} = \frac{a_i'p_{i-1}'-p_{i-2}'}{a_i'q_{i-1}'+q_{i-2}'} = \frac{(a_i+\frac{1}{a_{i+1}})p_{i-1}+p_{i-2}}{(a_i+\frac{1}{a_{i+1}})q_{i-1}+q_{i-2}} = \frac{p_{i+1}}{q_{i+1}}. \qquad \square\end{aligned}$$

Wir bemerken, dass die Folge der Nenner q_i monoton steigt.

Bemerkung I.13: Ist $\alpha = p/q$ mit ganzen, teilerfremden Zahlen p und q, wobei $q > 0$, so bricht der Kettenbruchalgorithmus nach endlich vielen Schritten mit $p/q = [a_0,\dots,a_n]$ ab.

Um das zu sehen, schreiben wir $p = qd + r$ mit $d, r \in \mathbb{Z}$ und $0 \le r < q$ nach Division mit Rest. Dann sind $a_0 = \lfloor\alpha\rfloor = \lfloor p/q\rfloor = \lfloor d + (r/q)\rfloor = d$, $\{\alpha\} = r/q$ und $\beta_1 = q/r$. Dies ist wieder ein gekürzter Bruch, d. h. Zähler und Nenner reproduzieren den euklidischen Algorithmus.

Satz I.14: *Für $\alpha \in \mathbb{R} - \mathbb{Q}$ konvergiert die Folge der n-ten Konvergenten gegen α.*

Beweis: Sei n eine natürliche Zahl. Dann haben wir

$$\begin{aligned}|\alpha - [a_0,\dots,a_n]| &= |[a_0,\dots,a_n,\beta_{n+1}] - [a_0,\dots,a_n]|\\ &= \left|\frac{p_n\beta_{n+1}+p_{n-1}}{q_n\beta_{n+1}+q_{n-1}} - \frac{p_n}{q_n}\right|\\ &= \left|\frac{q_np_{n-1}-p_nq_{n-1}}{q_n(q_n\beta_{n+1}+q_{n-1})}\right|\\ &= \frac{1}{q_n(q_n\beta_{n+1}+q_{n-1})} \le \frac{1}{q_n(q_na_{n+1}+q_{n-1})} < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}\end{aligned}$$

denn $q_np_{n-1} - p_nq_{n-1} = \det\left(\begin{smallmatrix} p_n & p_{n-1}\\ q_n & q_{n-1}\end{smallmatrix}\right) = (-1)^n$ und $\beta_{n+1} > \lfloor\beta_{n+1}\rfloor = a_{n+1}$. $\square$

Bemerkung I.15: Wir entnehmen dem Beweis von Satz I.14 außerdem, dass $|\alpha - (p_n/q_n)| < q_n^{-2}$. Gemessen an der Größe des Nenners erhalten wir eine quadratische Approximation von α.

Die Kettenbruchentwicklung von π ist $\pi = [3, 7, 15, 1, 292, 11, 1, 2, \dots]$, d. h. die ersten Näherungsbrüche sind 3, 22/7, 333/108, 355/113 und die vierte Konvergente $355/113 = 3{,}141\,592\,92\dots$ ist bereits eine recht gute Approximation von π.

Satz I.16 (Thue-Siegel-Rot): *Sind $\alpha \in \mathbb{R}$ algebraisch und $\varepsilon > 0$, so gibt es für jedes $c > 0$ nur endlich viele teilerfremde ganze p und q, wobei $q > 0$, mit*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^{2+\varepsilon}}.$$

Dieser Satz bescherte Rot 1958 eine Fields-Medaille.

Satz I.17: *Seien $\alpha \in \mathbb{R} - \mathbb{Q}$ und $p, q \in \mathbb{Z}$, $q > 0$, teilerfremd mit*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Dann ist p/q eine Konvergente der Kettenbruchentwicklung von α.

Beweis: Sei $p/q = [a_0, \ldots, a_n]$ die Kettenbruchentwicklung von p/q. Wir haben die Wahl

$$\frac{p}{q} = [a_0, \ldots, a_n] = \begin{cases} [a_0, \ldots, a_n - 1, 1], & \text{falls } a_n \geq 2, \\ [a_0, \ldots, a_{n-1} + 1], & \text{falls } a_n = 1, \end{cases}$$

zu schreiben, sodass wir die Parität von n so wählen können, dass es ein $0 \leq \delta < 1$ gibt mit

$$\alpha - \frac{p}{q} = (-1)^n \frac{\delta}{2q^2}.$$

Schreibe nun

$$\alpha = [a_0, \ldots, a_n, \gamma] = \frac{p_n\gamma + p_{n-1}}{q_n\gamma + q_{n-1}},$$

wobei $\gamma = \frac{\alpha q_{n-1} - p_{n-1}}{-\alpha q_n + p_n} \in \mathbb{R}$. Aus

$$(-1)^n \frac{\delta}{2q^2} = \alpha - \frac{p}{q} = \frac{p_n\gamma + p_{n-1}}{q_n\gamma + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_{n-1}p_n - p_{n-1}q_n}{q_n(\gamma q_n + q_{n-1})} = \frac{(-1)^n}{q(\gamma q + q_{n-1})},$$

was äquivalent ist zu $\delta(\gamma q + q_{n-1}) = 2q$, erhalten wir $\gamma = 2/\delta - q_{n-1}/q > 2 - 1$.

Mit $\gamma_i = [a_{i+1}, \ldots, a_n, \gamma]$ erhalten wir $\gamma_i > a_{i+1} \geq 1$ und

$$x = [a_0, \ldots, a_n, \gamma] = [a_0, \ldots, a_i, [a_{i+1}, \ldots, a_n, \gamma]] = [a_0, \ldots, a_i, \gamma_{i+1}].$$

Also ist der ganze Anteil von γ_i genau a_i. Dies gibt den Anfang der Kettenbruchentwicklung von x. □

Zurück zur Pellschen Gleichung: Sei $a, b > 0$ eine Lösung der Pellschen Gleichung. Dann gilt

$$\left|\frac{a}{b} - \sqrt{d}\right| = \left|\frac{a - b\sqrt{d}}{b}\right| = \frac{1}{b(a + b\sqrt{d})} < \frac{1}{2b^2}$$

genau dann, wenn $2b < a + b\sqrt{d}$ ist. Das ist äquivalent zu $2 - 2\sqrt{d} < (a/b) - \sqrt{d}$, was wahr ist, wegen $2 - 2\sqrt{d} < 0$ und $(a/b) - \sqrt{d} > 0$. Das heißt aus Lösungen der Pellschen Gleichung erhalten wir gute Approximationen von $\sqrt{d}$. Diese sind Konvergenten der Kettenbruchentwicklung von $\sqrt{d}$.

Beispiel I.18: Ist $\alpha = \sqrt{3}$, dann sind

$$a_0 = 1, \quad \beta_1 = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2},$$
$$a_1 = 1, \quad \beta_2 = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \frac{2}{\sqrt{3} - 1} = \sqrt{3} + 1,$$
$$a_2 = 2, \quad \beta_3 = \frac{1}{\sqrt{3} - 1} = \beta_1,$$

also ist $\sqrt{3} = [1, \overline{1, 2}]$. Wir haben das Schema

x	a_n	p_n	q_n	$p_n^2 - 3q_n^3$
-2	—	0	1	-3
-1	—	1	0	1
0	1	1	1	-2
1	1	2	1	1
2	2	5	2	-2
3	1	7	4	1
4	2	19	11	-2

Beobachtung I.19: Die Kettenbruchentwicklung von $\sqrt{3}$ ist periodisch und liefert Lösungen der Pellschen Gleichung. Wie verhält sich das für allgemeines $\sqrt{d}$?

Lemma I.20: *Seien $d \in \mathbb{N}$ kein Quadrat und $\alpha := \sqrt{d} = [a_0, \ldots, a_{n-1}, \beta_n]$. Dann gilt*

$$\beta_k = \frac{P_k + \sqrt{d}}{Q_k}$$

mit P_k und Q_k in $\mathbb{Z}$ definiert wie folgt:

$$P_0 = 0, \quad P_{k+1} = a_k Q_k - P_k, \qquad Q_0 = 1, \quad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}.$$

Beweis: Wir zeigen die Aussage per Induktion. Der Induktionsanfang $k = 0$ ist klar. Gilt die Behauptung für ein k, dann haben wir

$$\begin{aligned}\beta_{k+1} &= \frac{1}{\beta_k - a_k} \\ &= \frac{1}{\frac{P_k+\sqrt{d}}{Q_k} - a_k} = \frac{Q_k}{\sqrt{d} + P_k - a_k Q_k} = \frac{Q_k(\sqrt{d}+P_{k+1})}{d - P_{k+1}^2} = \frac{\sqrt{d}+P_{k+1}}{Q_{k+1}}\end{aligned}$$

und der Induktionsschritt ist vollzogen. Bleibt zu zeigen, dass die P_k, Q_k tatsächlich ganze Zahlen sind. Es ist $Q_k Q_{k-1} = d - P_k^2$, also $Q_k \mid d - P_k^2$. Damit ist Q_k auch ein Teiler von

$$d - P_{k+1}^2 = d - (P_k - Q_k a_k)^2 = d - P_k^2 - Q_k(2a_k + Q_k a_k)$$

und $Q_{k+1} \in \mathbb{Z}$. □

Lemma I.21: *Es gilt $P_1 = P_{k+1}$ und $Q_1 = Q_{k+1}$ genau dann, wenn $Q_k = 1$.*

Beweis: Ist $Q_k = 1$, dann ist $\beta_k = P_k + \sqrt{d}$, d. h. $a_k = \lfloor \beta_k \rfloor = P_k + a_0$. Also ist

$$P_{k+1} = a_k Q_k - P_k = a_0 = a_0 Q_0 - P_0 = P_1$$

und $Q_{k+1} = (d - P_{k+1}^2)/Q_k = (d - P_1^2)/Q_0 = Q_1$. Seien umgekehrt $P_{k+1} = P_1$ und $Q_{k+1} = Q_1$. Dann ist

$$\frac{d - P_1^2}{Q_0} = Q_1 = Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k},$$

d. h. $Q_0 = Q_k = 1$, was wir zeigen wollten. □

Lemma I.22: *Für $k \in \mathbb{N}$ gilt $P_k^2 - d q_k^2 = (-1)^{k+1} Q_{k+1}$.*

Beweis: Wir schreiben

$$\sqrt{d} = \alpha = [a_0, \ldots, a_k, \beta_{k+1}] = \frac{p_k \beta_{k+1} + p_{k-1}}{q_k \beta_{k+1} + q_{k+1}}.$$

Umformen von $\beta_{k+1} = \frac{P_{k+1}+\sqrt{d}}{Q_{k+1}}$ und Einsetzen ergibt

$$d q_k + P_{k+1} p_k - Q_{k+1} p_{k-1} = (p_k - P_{k+1} q_k - Q_{k+1} q_{k-1})\sqrt{d}.$$

Da die linke Seite eine ganze Zahl ist und der Vorfaktor von $\sqrt{d}$ auch eine ganze Zahl ist, aber $\sqrt{d}$ irrational ist, muss die ganze Gleichung Null sein. Also ist

$$\begin{aligned}0 &= p_k(p_k - P_{k+1} q_k - Q_{k+1} q_{k-1}) - q_k(d q_k - P_{k+1} p_k - Q_{k+1} p_{k-1}) \\ &= p_k^2 - d q_k^2 + Q_{k+1}(q_k p_{k-1} - p_k q_{k-1}) = p_k^2 - d q_k^2 + (-1)^k Q_{k+1}.\end{aligned}$$ □

Ist $Q_{k+1} = 1$, so erhalten wir also tatsächlich $p_k^2 - dq_k^2 = (-1)^{k+1}$, d. h. eine Lösung der Pellschen Gleichung. Für Lösungen der Pellschen Gleichung müssen wir also noch die Periodizität der Kettenbruchentwicklung von $\sqrt{d}$ zeigen.

Lemma I.23: *Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d}))$ mit $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$, wobei $a, b \in \mathbb{Q}$. Für $k \geq 1$ gilt $\beta_k > 1$ und $-1 < \sigma(\beta_k) < 0$.*

Beweis: Per Definition ist $\beta_{k+1} = \{\beta_k\}^{-1} > 1$. Die zweite Ungleichung zeigen wir per Induktion nach k. Für $k = 1$ ist

$$\sigma(\beta_1) = \sigma([\sqrt{d} - \lfloor\sqrt{d}\rfloor]^{-1}) = \frac{-1}{\sqrt{d} + \lfloor\sqrt{d}\rfloor}$$

und $\sqrt{d} + \lfloor\sqrt{d}\rfloor > 1$. Gilt die Induktionsbehauptung für ein k, dann haben wir $-1 < \sigma(\beta_{k+1}) = [\sigma(\beta_k) - \lfloor\beta_k\rfloor]^{-1} < 0$, da $\sigma(\beta_k) \in (-1, 0)$. □

Lemma I.24: *Für $k \geq 1$ gilt $0 < P_k < \sqrt{d}$ und $0 < Q_k < 2\sqrt{d}$.*

Beweis: Angenommen Q_k wäre negativ. Dann hätten wir

$$\frac{P_k - \sqrt{d}}{Q_k} = \sigma(\beta_k) < 0 < 1 < \beta_k = \frac{P_k + \sqrt{d}}{Q_k},$$

was zur Folge hätte dass $P_k - \sqrt{d} > P_k + \sqrt{d}$, was absurd ist. Damit ist $Q_k > 0$. Wegen

$$\frac{\sqrt{d} - P_k}{Q_k} = -\sigma(\beta_k) < 1 < \beta_k = \frac{P_k + \sqrt{d}}{Q_k},$$

ist $0 < (\sqrt{d} + P_k)/Q_k - (\sqrt{d} - P_k)/Q_k = 2P_k/Q_k$ und damit $0 < P_k$.

Da $\sigma(\beta_k) = (P_k - \sqrt{d})/Q_k < 0$ ist $P_k < \sqrt{d}$. Schließlich lesen wir aus $\beta_k = (P_k + \sqrt{d})/Q_k > 1$ ab, dass $Q_k < P_k + \sqrt{d} < 2\sqrt{d}$. □

Insbesondere gibt es nur endlich viele Möglichkeiten für die P_k, Q_k, also auch für die β_k. Es gibt deshalb $k, r > 1$ sodass $\beta_r = \beta_{k+r}$. Mit Blick auf Lemma I.4.14 brauchen wir $r = 1$. Das liefert uns den folgenden Satz:

Satz I.25: *Es gibt $s \geq 0$, sodass $\sqrt{d} + \lfloor\sqrt{d}\rfloor = [\overline{2a_0, \ldots, a_n}]$. Insbesondere ist*

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_s, 2a_0}] \quad \textit{und} \quad \beta_{s+2} = \beta_1.$$

Beweis: Wir setzen

$$y_k := \begin{cases} \frac{1}{\sqrt{d}-\lfloor\sqrt{d}\rfloor} = \beta_1 > 1, & \text{falls } k = 0, \\ \frac{Q_k}{\sqrt{d}-P_k} = \frac{-1}{\sigma(\beta_k)} > 1, & \text{falls } k \geq 1. \end{cases}$$

Es gelten nun die Rekursionen

$$\begin{aligned} y_1 &= \frac{Q_1}{\sqrt{d}-P_1} = \frac{d-a_0^2}{\sqrt{d}-a_0} = \sqrt{d}+a_0 = \sqrt{d}+\lfloor\sqrt{d}\rfloor = 2a_0 + \frac{1}{y_0}, \\ y_{k+1} &= \frac{Q_{k+1}}{\sqrt{d}-P_{k+1}} = \frac{\frac{d-P_{k+1}^2}{Q_k}}{\sqrt{d}-P_{k+1}} = \frac{\sqrt{d}+P_{k+1}}{Q_k} \\ &= \frac{\sqrt{d}+a_kQ_k-P_k}{Q_k} = \frac{\sqrt{d}-P_k}{Q_k} + a_k = a_k + \frac{1}{y_k}. \end{aligned}$$

Daraus folgt

$$\lfloor y_{k+1}\rfloor = \begin{cases} 2a_0, & \text{falls } k = 0, \\ a_k, & \text{falls } k \geq 1. \end{cases}$$

Nun sei $1 \leq r \in \mathbb{N}$ minimal, sodass $t \geq 1$ existiert mit $y_{r+t} = y_r$. Angenommen, $r > 1$. Dann wäre

$$y_{r-1} = \frac{1}{y_r - a_{r-1}} = \frac{1}{y_r - \lfloor y_r\rfloor} = \frac{1}{y_{r+t} - \lfloor y_{r+t}\rfloor} = y_{r-1+t},$$

und r doch nicht minimal. Damit ist $r = 1$ und $y_{1+t} = y_1$. Mit $s := t-1$ erhalten wir $y_{s+2} = y_1$, insbesondere $\beta_1 = \beta_{s+2}$. Dies liefert den Startpunkt der Periodizität der Kettenbruchentwicklung von $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_{s+1}}]$. Weiter gilt $a_{s+1} = \lfloor y_{s+2}\rfloor = \lfloor y_1\rfloor = 2a_0$, so dass wir das gewünschte Ergebnis $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_s, 2a_0}]$ erhalten. □

Korollar I.26: *Die Pellsche Gleichung $x^2 - dy^2 = 1$ hat eine nicht-triviale Lösung.*

Satz I.27: *Sei $n \in \mathbb{N}$ minimal mit $(-1)^{n+1}Q_{n+1} = 1$. Dann sind alle Lösungen der Pellschen Gleichung $x^2 - dy^2 = 1$ gegeben durch*

$$x + \sqrt{d}y = \pm(p_n + q_n\sqrt{d})^\ell \qquad (\ell \in \mathbb{Z}).$$

Beweis: Sei $\varepsilon = p_n + q_n\sqrt{d} > 1$. Da $\pm(x+y\sqrt{d})^{-1} = \pm(x-y\sqrt{d})$ dürfen wir $x + y\sqrt{d} > 1$ annehmen. Wir zeigen, dass es $m \in \mathbb{N}$ mit $x + y\sqrt{d} = \varepsilon^m$ gibt. Es gibt $m \in \mathbb{N}$ mit $\varepsilon^m < x + \sqrt{d}y < \varepsilon^{m+1}$, also auch $1 \leq x + y\sqrt{d}) < \varepsilon$. Wir setzen $x_0 + y_0\sqrt{d} := \varepsilon^{-m}(x + y\sqrt{d})$. Weiter ist $1 = x_0^2 - dy_0^2 = (x_0 + \sqrt{d}y_0)(x_0 - \sqrt{d}y_0)$.

Angenommen $x_0 + y_0\sqrt{d} > 1$. Dann wäre $0 < \varepsilon^{-1} < x_0 - y_0\sqrt{d} < 1$, d. h. wir hätten

$$2x_0 = (x_0 + y_0\sqrt{d}) + (x_0 - y_0\sqrt{d}) > 1 + \varepsilon^{-1}$$

und analog $2y_0\sqrt{d} = (x_0 + y_0\sqrt{d}) - (x_0 - y_0\sqrt{d}) > 1 - 1 = 0$. Wir erhielten also $x_0^2 + dy_0^2 \leq 1$, $x_0 > 0$ und $y_0 > 0$ sowie $1 < x_0 + y_0\sqrt{d} < \varepsilon = p_n + q_n\sqrt{d}$. Weil $x_0 = (1 + dy_0^2)^{1/2}$ streng monoton wachsend in y_0 ist, impliziert dies $y_0 < q_n$ und $x_0 < p_n$.

Als nicht-triviale Lösung der Pellschen Gleichung ist x_0/y_0 eine Konvergente von $\sqrt{d}$ mit kleinerem Nenner als p_n/q_n. Da die Nenner monoton mit n wachsen, liegt dies im Widerspruch zur Minimalität von n.

Somit ist $1 > x_0 + \sqrt{d}y_0 = \varepsilon^{-m}(x + \sqrt{d}y)$. □

Kapitel II.

Ganzheit

Im Folgenden sind alle Ringe kommutativ und unital.

Definition II.1: Sei $A \subseteq B$ eine Ringerweiterung. Das Element $\beta \in B$ heißt *ganz über* A, falls es $a_0, \ldots, a_{n-1} \in A$, $n \geq 1$, gibt, sodass

$$\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_0 = 0.$$

Ist jedes $\beta \in B$ ganz über A, so heißt B *ganz über* A.

Satz II.2: *Sei $A \subseteq B$ eine Ringerweiterung. Die Elemente $\beta_1, \ldots, \beta_n$ sind genau dann allesamt ganz über A, wenn der Ring $A[\beta_1, \ldots, \beta_n]$ ein endlich erzeugter A-Modul ist.*

Beweis: Sei $\beta \in B$ ganz über A und $f \in A[X]$ ein normiertes Polynom mit $f(\beta) = 0$ und $\deg(f) \geq 1$. Jedes Polynom $g \in A[X]$ lässt sich nun als $g = qf + r$ mit Polynomen q und r aus $A[X]$ und $\deg(r) < \deg(f) =: m$ schreiben. Somit ist $g(\beta) = q(\beta)f(\beta) + r(\beta) = r(\beta) = r_{m-1}\beta^{m-1} + \cdots + \beta r_1 + r_0$. Also wird der A-Modul $A[\beta]$ von $\beta^{m-1}, \ldots, 1$ erzeugt.

Den allgemeinen Fall mit $\beta_1, \ldots, \beta_n \in B$ zeigt man via Induktion nach n. Ist β_n ganz über A, so auch über $R = A[\beta_1, \ldots, \beta_{n-1}]$. Nach dem eben gezeigten ist dann $R[\beta_n] = A[\beta_1, \ldots, \beta_n]$ ein endlich erzeugter R-Modul. Ist nun $R = A[\beta_1, \ldots, \beta_{n-1}]$ endlich erzeugter A-Modul durch $r_1, \ldots, r_k \in R$ und $R[\beta_n]$ erzeugt über R durch $\omega_1, \ldots, \omega_s$, so erzeugen $\{r_i\omega_j \mid 1 \leq i \leq k, 1 \leq j \leq s\}$ den Ring $R[\beta_n] = A[\beta_1, \ldots, \beta_n]$ über A.

Sei nun umgekehrt der A-Modul $A[\beta_1, \ldots, \beta_n]$ erzeugt von $\omega_1, \ldots, \omega_r$. Sei $\beta \in A[\beta_1, \ldots, \beta_n]$. Mit geeigneten $a_{ij} \in A$ können wir für $1 \leq i \leq r$ schreiben

$$\beta\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j$$

Die Matrix $M = [\beta E - (a_{ij})]$ erfüllt also $M.(\omega_1, \ldots, \omega_r)^t = 0$. Es gibt $c_1, \ldots, c_r$ in A, sodass $1 = c_1\omega_1 + \cdots + c_r\omega_r$. Mit der adjunkten Matrix M^* erhalten wir

$$0 = (c_1, \ldots, c_r)M^*M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \det M(c_1, \ldots, c_r) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = (\det M)1 = \det M.$$

Mit $0 = \det M = \det(\beta E - a_{ij})$ erhalten wir eine normierte Gleichung für β mit Koeffizienten in A. Damit ist β ganz über A. □

Korollar II.3: *Mit $\beta_1, \ldots, \beta_n \in B$ ist auch jedes weitere $\beta \in A[\beta_1, \ldots, \beta_n]$ ganz über A. Insbesondere auch $\beta_1 + \beta_2$ und $\beta_1\beta_2$.*

Beweis: $A[\beta_1, \ldots, \beta_n] = A[\beta_1, \ldots, \beta_n, \beta]$. □

Satz II.4: *Seien $A \subseteq B \subseteq C$ Teilringe. Ist nun C ganz über B und B ganz über A, dann ist C ganz über A.*

Beweis: Sei $c \in C$. Da C ganz über B ist, gibt es $b_0, \ldots, b_{n-1} \in B$, wobei $n \geq 1$, mit $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$. Nach Satz II.2 ist nun $R = A[b_0, \ldots, b_{n-1}]$ ein endlich erzeugter A-Modul und $R[c]$ ist ein endlich erzeugter R-Modul. Folglich ist $R[c]$ sogar endlich erzeugt über A, also nach Satz II.2 ganz über A. □

Definition II.5: Sei $A \subseteq B$ ein Teilring. Die Menge

$$\bar{A}^B = \{b \in B \mid b \text{ ist ganz über } A\}$$

heißt der *ganze Abschluss von A in B*. Nach Korollar II.3 bildet $\bar{A}^B$ einen Teilring von B. Ist $A = \bar{A}^B$, so nennen wir A *ganzabgeschlossen in B*. Wir schreiben auch $\bar{A}$ für $\bar{A}^B$, falls der Ring B aus dem Kontext klar ist.

Definition II.6: Sei A ein Integritätsring mit Quotientenkörper K. Der ganze Abschluss $\bar{A}^K$ von A in K heißt auch die *Normalisierung von A*. Gilt $A = \bar{A}^K$, so heißt A *ganzabgeschlossen*.

Satz II.7: *Ist A ein faktorieller Ring, dann ist A ganzabgeschlossen.*

Beweis: Sei dazu b/c in $\bar{A}^K$. Es gibt also $a_0, \ldots, a_{n-1} \in A$, sodass

$$\left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_0 = 0.$$

Es folgt $b^n + b^{n-1}ca_{n-1} + \cdots + a_0c^n = 0$. Ist nun $\pi \in A$ ein Primelement mit $\pi \mid c$, so folgt $\pi \mid b^n$, also $\pi \mid b$. Wir dürfen den Bruch gekürzt, also $\mathrm{ggT}(b, c) = 1$, annehmen. Folglich kann c keine Primteiler haben und ist somit eine Einheit in A. Insgesamt ist nun $b/c \in A$. □

Definition II.8: Sei L ein algebraischer Zahlkörper, also eine endliche Erweiterung von $\mathbb{Q}$. Der ganze Abschluss von $\mathbb{Z}$ in L heißt der *Ring der ganzen Zahlen von L*. Wir schreiben hierfür $\mathcal{O}_L$.

Satz II.9: *Sei K der Quotientenkörper von A und $K \subseteq L$ eine Körpererweiterung. Ist $\alpha \in L$ algebraisch über K, so gibt es ein $d \in A$ sodass $d\alpha$ ganz über A ist.*

Beweis: Nach Annahme gibt es $a_0, \ldots, a_{m-1} \in K$, wobei $m \geq 1$, sodass

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0.$$

Sei $d \in A$ so, dass die da_i für $0 \leq i \leq m-1$ alle zu A gehören. Dann ist $(\alpha d)^m + a_{m-1}d(\alpha d)^{m-1} + \cdots + a_0 d^m = 0$, was die Ganzheit von αd über A liefert. □

Korollar II.10: *Sei A ein Integritätsbereich mit Quotientenkörper K. Ferner sei $K \subseteq L$ eine Körpererweiterung und B der ganze Abschluss von A in L. Ist $L|K$ algebraisch, so ist L der Quotientenkörper von B.*

Beweis: Nach Satz II.9 ist jedes Element $\alpha \in L$ von der Form β/d mit $\beta \in B$ und $d \in A$. □

Satz II.11: *Es seien A ein Integritätsbereich mit Quotientenkörper K und $L|K$ eine Körpererweiterung von endlichem Grad. Ist A ganzabgeschlossen, so ist $\alpha \in L$ ganz über A genau dann, wenn sein Minimalpolynom μ_α über K Koeffizienten in A hat.*

Beweis: Sei $\alpha \in L$ ganz über A und $g = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ ein Polynom aus $A[X]$ mit $g(\alpha) = 0$. Folglich ist μ_α ein Teiler von g und alle Nullstellen von μ_α in einem algebraischen Abschluss von L sind ganz über A. Die Koeffizienten von μ_α sind symmetrische Polynome in den Nullstellen und so nach Korollar II.3 ganz über A. Da A nach Voraussetzung ganzabgeschlossen (in K) ist, liegt μ_α bereits in $A[X]$. □

Bemerkung II.12: Dies erlaubt es uns, einige Ganzheitsringe zu bestimmen. So ist ein Element $\alpha \in \mathbb{Q}[\sqrt{d}]$ ganz genau dann, wenn Spur und Norm ganz sind.

Definition II.13: Sei $L|K$ eine endliche Körpererweiterung und $\alpha \in L$. Wir erhalten die K-lineare Abbildung $\ell_\alpha \colon L \to L$, $x \mapsto \alpha x$. Die *Spur von α* ist $\mathrm{Tr}_{L|K}(\alpha) = \mathrm{Tr}(\ell_\alpha)$. Die *Norm von α* ist $N_{L|K}(\alpha) = \det(\ell_\alpha)$. Für das charakteristische Polynom $\chi_\alpha = \det(t\,\mathrm{id} - \ell_\alpha) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ gilt $a_{n-1} = -\mathrm{Tr}_{L|K}(\alpha)$ und $a_0 = (-1)^n N_{L|K}(\alpha)$, wobei $n = [L : K]$.

Im Folgenden sei stets Ω ein algebraischer Abschluss des Körpers K.

Satz II.14: *Seien $L|K$ endlich und separabel mit $n = [L : K]$. Dann gilt für $\beta \in L$ und $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \Omega)$:*

(i) $\chi_\beta = \prod_{i=1}^n (X - \sigma_i(\beta))$,

(ii) $\mathrm{Tr}_{L|K}(\beta) = \sum_{i=1}^n \sigma_i(\beta)$,

(iii) $N_{L|K}(\beta) = \prod_{i=1}^n \sigma_i(\beta)$.

Beweis: Es gilt $\chi_\beta = \mu_\beta^d$ mit $d = [L : K(\beta)]$, ist nämlich $1, \beta, \ldots, \beta^{m-1}$ eine Basis von $K(\beta)|K$ und $\alpha_1, \ldots, \alpha_d$ eine Basis von $L|K(\beta)$, dann ist

$$\{\alpha_1, \beta\alpha_1, \ldots, \beta^{m-1}\alpha_1, \alpha_2, \ldots, \beta^{m-1}\alpha_d\}$$

eine Basis von $L|K$ und die Darstellungsmatrix von ℓ_β ist eine Blockdiagonalmatrix mit d Blöcken der Gestalt

$$C = \begin{pmatrix} 0 & & & & -c_0 \\ 1 & \ddots & & & -c_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & -c_{n-2} \\ & & & 1 & -c_{n-1} \end{pmatrix}$$

wobei $\mu_\beta = X^m + c_{m-1}X^{m-1} + \cdots + c_0$. Es ist $\chi_C = \mu_\beta$, sodass $\chi_\beta = \mu_\beta^d$ wie gewünscht. Da $L|K$ separabel ist, zerfällt $\mathrm{Hom}_K(L, \Omega)$ unter der Äquivalenzrelation

$$\sigma \sim \tau \iff \sigma|_{K(\beta)} = \tau|_{K(\beta)}$$

in m Äquivalenzklassen der Mächtigkeit d.

Sei $\tau_1, \ldots, \tau_m$ ein Repräsentantensystem, dann ist

$$\mu_\beta = \prod_{i=1}^m (X - \tau_i\beta), \qquad \chi_\beta = \prod_{i=1}^m (X - \tau_i\beta)^d = \prod_{i=1}^m \prod_{\sigma \sim \tau_i} (X - \sigma\beta) = \prod_{j=1}^r (X - \sigma_j\beta),$$

und wir haben (i) bewiesen. Aussagen (ii) und (iii) folgen aus (i). □

In der Situation von (Satz II.11) sind also auch Norm und Spur ganzer Elemente ganz.

Im Folgenden sei stets Ω ein algebraischer Abschluss von K.

Korollar II.15: *Ist $K \subseteq L \subseteq M$ ein Turm endlicher Körpererweiterungen, so gilt*

$$\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}, \qquad N_{L|K} \circ N_{M|L} = N_{M|K}.$$

Beweis: Wir führen den Beweis nur im separablen Fall. Sei also $M|K$ separabel. Dann zerfällt $\mathrm{Hom}_K(M,\Omega)$ unter der Relation „$\sigma \sim \tau$, falls $\sigma|_L = \tau|_L$“ in $m = [L:K]$ Äquivalenzklassen der Ordnung $[M:L]$. Sei $\{\sigma_1,\dots,\sigma_m\}$ ein Repräsentantensystem, also insbesondere $\{\sigma_1|_L,\dots,\sigma_m|_L\} = \mathrm{Hom}_K(L,\Omega)$. Für die Äquivalenzklassen gilt

$$\{\sigma \mid \sigma \sim \sigma_i\} = \{\tau \circ \sigma_i \mid \tau \in \mathrm{Hom}_{\sigma_i(L)}(\sigma_i M, \Omega)\}.$$

Wir erhalten für $\gamma \in M$, dass

$$\begin{aligned}\mathrm{Tr}_{M|K}(\gamma) &= \sum_{i=1}^{m} \sum_{\sigma\sim\sigma_i} \sigma\gamma \\ &= \sum_{i=1}^{m} \mathrm{Tr}_{\sigma_i(M)|\sigma_i(L)}(\sigma_i(\gamma)) = \sum_{i=1}^{m} \sigma_i(\mathrm{Tr}_{M|L}(\gamma)) = \mathrm{Tr}_{L|K}(\mathrm{Tr}_{M|L}(\gamma)).\end{aligned}$$

Hierbei erklärt sich die dritte Gleichheit wie folgt: Ist $\omega_1,\dots,\omega_n$ eine L-Basis von M, so ist $\sigma_i\omega_1,\dots,\sigma_i\omega_n$ eine $\sigma_i(L)$-Basis von $\sigma_i(M)$. Ist nun $(c_{jk}) \in L^{n\times n}$ die Darstellungsmatrix von $\ell_\gamma\colon M \to M$ bezüglich $\omega_1,\dots,\omega_n$, so ist $(\sigma_i(c_{jk}))$ die Darstellungsmatrix von $\ell_{\sigma_i(\gamma)}\colon \sigma_i(M) \to \sigma_i(M)$. Entsprechend ist $\mathrm{Tr}(\ell_{\sigma_i(\gamma)}) = \sigma_i(\mathrm{Tr}(\ell_\gamma)) = \sigma_i \mathrm{Tr}_{M|K}(\gamma)$. □

Definition II.16: Sei $L|K$ eine endliche Körpererweiterung. Die K-bilineare Abbildung

$$(\cdot,\cdot)\colon L \times L \longrightarrow K, \qquad (a,b) \longmapsto \mathrm{Tr}(ab)$$

heiß *Spurform von* $L|K$.

Ist $(\beta_1,\dots,\beta_n)$ eine Basis von $L|K$, so heißt $d(\beta_1,\dots,\beta_n) := \det \mathrm{Tr}(\beta_i\beta_j)$ ihre *Diskriminante*.

Bemerkung II.17: Für eine weitere Basis $\gamma_i = \sum_{j=1}^n c_{ij}\beta_j$ und ihre Diskriminante gilt $d(\gamma_1,\dots,\gamma_n) = \det(c_{ij})^2 d(\beta_1,\dots,\beta_n)$.

Satz II.18: *Sei $L|K$ eine endliche separable Körpererweiterung vom Grad n und $\{\sigma_1,\dots,\sigma_n\} = \mathrm{Hom}_K(L,\Omega)$. Dann gilt für eine Basis*

$$d(\beta_1,\dots,\beta_n) = \det([\sigma_i(\beta_j)])^2.$$

Beweis: Wir rechnen nach:

$$\begin{aligned}d(\beta_1,\dots,\beta_n) &= \det \mathrm{Tr}(\beta_i\beta_j) \\ &= \det \sum_k \sigma_k(\beta_i\beta_j) \\ &= \det \sum_k \sigma_k(\beta_i)\sigma_k(\beta_j) = \det \sigma_k(\beta_i) \det \sigma_k(\beta_j) = \det \sigma_k(\beta_i)^2. \ \square\end{aligned}$$

Definition II.19: Sei K ein Körper und $f \in K[X]$. Die Diskriminante von $f = \prod_{i=1}^{n}(X - \theta_i)$, wobei $\theta_i \in \Omega$, ist

$$\mathrm{Disk}(f) = \prod_{i<j}(\theta_i - \theta_j)^2 \in K.$$

Lemma II.20: *Für eine Basis von $L|K$ der Form $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ gilt*

$$d(1, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 = \mathrm{Disk}\,\mu_\theta,$$

wobei $\theta_i = \sigma_i(\theta)$.

Beweis: Nach (Satz II.18) haben wir mit der Vandermonde-Determinante

$$\begin{aligned} d(1, \ldots, \theta^{n-1}) &= \det \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix}^2 \\ &= \det \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \vdots & \theta_2 - \theta_1 & \cdots & \cdots & (\theta_2 - \theta_1)\theta_2^{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \theta_n - \theta_1 & \cdots & \cdots & (\theta_n - \theta_1)\theta_n^{n-2} \end{pmatrix}^2 \\ &= \prod_{j=2}^{n}(\theta_j - \theta_i)^2 \det \begin{pmatrix} 1 & \theta_2 & \cdots & \theta_2^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \theta_n & \ldots & \theta_n^{n-2} \end{pmatrix}^2 = \cdots = \prod_{i<j}(\theta_j - \theta_i)^2 \square \end{aligned}$$

Satz II.21: *Sei $L|K$ eine endliche separable Körpererweiterung. Dann ist die Spurform nicht ausgeartet (d. h. ist $(\alpha, \beta) = 0$ für alle $\beta \in L$, dann ist $\alpha = 0$). Insbesondere ist $d(\beta_1, \ldots, \beta_n) \neq 0$ für jede Basis von $L|K$.*

Beweis: Da $L|K$ separabel ist, findet sich ein primitives Element $\theta \in L$ mit $K(\theta) = L$. Also ist $(1, \theta, \ldots \theta^{n-1})$ eine Basis von $L|K$. Dann ist

$$d(1, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0,$$

denn es gilt $\sigma_i = \sigma_j$ genau dann, wenn $\theta_i = \sigma_i(\theta) = \sigma_j(\theta) = \theta_j$ ist. Ist $\beta_i = \sum_{j=1}^{n} c_{ij}\theta^{j-1}$ eine weitere Basis, so ist $\det(c_{ij}) \neq 0$, also

$$d(\beta_1, \ldots, \beta_n) = \det(c_{ij})^2 d(1, \ldots, \theta^{n-1}) \neq 0. \qquad \square$$

Im Folgenden sei wieder A ein ganzabgeschlossenere Integritätsbereich, K sein Quotientenkörper und B sein ganzer Abschluss in der endlichen Körpererweiterung $L|K$.

Lemma II.22: *Sei $\beta_1, \ldots, \beta_n \in B$ eine Basis von $L|K$. Für die Diskriminante $d = d(\beta_1, \ldots, \beta_n)$ gilt $dB \subseteq \beta_1 A + \cdots + \beta_n A \subseteq B$.*

Beweis: Vermöge der Basis $(\beta_1, \ldots, \beta_n)$ identifizieren wir L mit K^n. Weiter sei $G = \mathrm{Tr}(\beta_i\beta_j)_{i,j} \in K^{n\times n}$ die Gramsche Matrix der Spurform. Für ein Element $\beta = \sum_{j=1}^n c_j\beta_j$ von B gilt $\mathrm{Tr}(\beta_i\beta) = b_i \in A$. Also ist $Gc = b$ in A^n und folglich

$$d \cdot \beta = d \cdot (\beta_1, \ldots, \beta_n)c = (\beta_1, \ldots, \beta_n)G^*b \in A\beta_1 + \ldots A\beta_n$$

wie gewünscht. □

Satz II.23: *Ist $L|K$ separabel und ist A ein Hauptidealring, so ist jeder endlich erzeugte B-Untermodul $0 \neq M \subseteq L$ ein freier A-Modul vom Rang $[L : K]$.*

Beweis: Sei $0 \neq M$ ein endlich erzeugter B-Modul. Ist $(\beta_1, \ldots, \beta_n)$ eine Basis von $L|K$, so liegt sie nach Multiplikation mit einem gemeinsamen Nenner bereits in B. Nach (II.22) ist nun $dB \subseteq A\beta_1 + \cdots + A\beta_n =: M_0 \subseteq B$. Genau so finden wir für ein Erzeugendensystem $\mu_1, \ldots, \mu_r$ des B-Moduls M ein $a \in A$ mit allen $a\mu_i \in B$ und damit $aM \subseteq B$. Nach dem Hauptsatz über Moduln über Hauptidealringen sind M und M_0 freie A-Moduln und

$$\mathrm{Rang}_A M = \mathrm{Rang}_A adM \leq \mathrm{Rang}_A dB \leq \mathrm{Rang}_A M_0.$$

Als B-Modul ist für $0 \neq m \in M$ schon $mB \subseteq M$, also ist

$$\mathrm{Rang}\, M_0 \leq \mathrm{Rang}\, B = \mathrm{Rang}\, mB \leq \mathrm{Rang}\, M.$$

Insgesamt ist $\mathrm{Rang}\, M = \mathrm{Rang}\, M_0 = [L : K]$. □

Satz II.24: *Ist K ein Zahlkörper, dann ist $\mathcal{O}_K$ der größte Unterring, der als $\mathbb{Z}$-Modul endlich erzeugt ist.*

Beweis: Nach (II.21) ist $\mathcal{O}_K$ endlich erzeugt. Ist B ein weiterer Unterring, der als $\mathbb{Z}$-Modul endlich erzeugt ist, so ist für $b \in B$ der Ring $\mathbb{Z}[b] \subseteq B$ auch endlich erzeugt, also ist b ganz über $\mathbb{Z}$ und damit bereits in $\mathcal{O}_K$. Damit ist $B \subseteq \mathcal{O}_K$ und die Maximalität ist gezeigt. □

Definition II.25: Für einen Zahlkörper K heißt eine Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul eine *Ganzheitsbasis von K*.

Bemerkung II.26: Ist $(\alpha_1, \ldots, \alpha_n)$ eine Basis von $K|\mathbb{Q}$ und ist

$$N = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$$

für $\beta_1, \ldots, \beta_n \in K$, so ist $\beta_i = \sum_{j=1}^n a_{ij}\alpha_j$ mit $(a_{ij}) \in \mathrm{Gl}_n(\mathbb{Z})$. Insbesondere ist

$$d(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 d(\beta_1, \ldots, \beta_n) = d(\beta_1, \ldots, \beta_n).$$

Also ergibt $d(N) := d(\alpha_1, \ldots, \alpha_n)$ Sinn. Für $N = \mathcal{O}_K$ ist dies die Diskriminante $d_K = d(\mathcal{O}_K)$ des Zahlkörpers K.

Satz II.27: *Sind $N \subseteq M \subseteq K$ zwei $\mathbb{Z}$-Moduln vom Rang $n = [K : \mathbb{Q}]$, dann gilt $d(N) = [M : N]^2 d(M)$, wobei $[M : N] = \#(M/N)$.*

Beweis: Sei $(\alpha_1, \ldots, \alpha_n)$ eine $\mathbb{Z}$-Basis von N und $(\beta_1, \ldots, \beta_n)$ eine $\mathbb{Z}$-Basis von M. Dann ist $\alpha_i = \sum_{j=1}^n a_{ij}\beta_j$ mit $A = (a_{ij}) \in \mathbb{Z}^{n\times n}$. Nach dem Satz über die Smith-Normalform gibt es $U, V \in \mathrm{Gl}_n(\mathbb{Z})$ mit $UAV = \mathrm{diag}(d_1, \ldots, d_n)$. Dann gilt $M/N \cong \bigoplus_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$, also

$$[M : N] = \#(M/N) = \prod_{i=1}^n d_i = \det UAV = |\det A|,$$

was den Beweis beschließt. □

Zunächst als Nachtrag zu (Lemma II.20): Sind $L = K[\theta]$ und ist μ_θ gegeben durch $\mu_\theta = \prod_{i=1}^n (X - \theta_i)$, dann ist

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 = (-1)^{n(n-1)/2} N_{L|K}(\mu'_\theta(\theta)).$$

Von der ersten Gleichheit haben wir uns bereits überzeugt, die zweite Gleichheit sieht man so ein:

$$\begin{aligned}\prod_{i<j} (\theta_i - \theta_j)^2 &= (-1)^{n(n-1)/2} \prod_{i=1}^n \prod_{i\neq j} (\theta_i - \theta_j) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^n \mu'_\theta(\theta_i) = (-1)^{n(n-1)/2} N(\mu'_\theta(\theta)),\end{aligned}$$

denn $\mu'_\theta = \sum_{i=1}^n \prod_{j\neq i} (X - \theta_j)$.

Im Folgenden sei stets K ein Körper der Charakteristik Null. Wir wollen den Ring der ganzen Zahlen in ein paar Beispielen bestimmen.

Beispiel II.28: Wir berechnen die Diskriminante von $f = X^n + aX + b$, wobei $a, b \in K$, unter der Annahme es sei irreduzibel. Sei β eine Nullstelle von f und sei $\gamma = f'(\beta) = n\beta^{n-1} + a$. Wir berechnen nun $N_{K[\beta]|K}(\gamma)$. Aus $\beta^n + a\beta + b = 0$, was äquivalent ist zu $n\beta^{n-1} + an + nb\beta^{-1} = 0$, also $n\beta^{n-1} = -an - nb\beta^{-1}$, erhalten wir

$$\begin{aligned}\gamma = n\beta^{n-1} + a = a(1-n) - nb\beta^{-1} &\iff \gamma - a(1-n) = -nb\beta^{-1} \\ &\iff \beta = \frac{-nb}{\gamma - a(1-n)}.\end{aligned}$$

Folglich ist $K[\gamma] = K[\beta]$ und $\deg \mu_\gamma = n$. Schreibe mit geeigneten $P, Q \in K[X]$

$$f\left(\frac{-nb}{X - a(1-n)}\right) = \frac{P(X)}{Q(X)}.$$

Dann gilt $P(\gamma)/Q(\gamma) = f(\beta) = 0$, also ist $P(\gamma) = 0$. Nun ist

$$P = [(-1)^n n^n b^n + a(-nb)(x - (1-n)a)^{n-1} + b(x - (1-n)a)^n]/b$$

normiert und vom Grad n, also ist P das Minimalpolynom von γ. Damit ist

$$\begin{aligned}N(\gamma) = (-1)^n P(0) &= n^n b^{n-1} + n(1-n)^{n-1}a^n + (1-n)^n a^n \\ &= n^n b^{n-1} + n(1-n)^{n-1}a^n + (1-n)^{n-1}a^n - n(n-1)^{n-1}a^n \\ &= n^n b^{n-1} + (1-n)^{n-1}a^n = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.\end{aligned}$$

Schlussendlich erhalten wir

$$\mathrm{Disk}(f) = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

Zum Beispiel sind

- $\mathrm{Disk}(x^2 + ax + b) = a^2 - 4b$,
- $\mathrm{Disk}(x^3 + ax + b) = -27b^2 - 4a^3$,
- $\mathrm{Disk}(x^4 + ax + b) = 256b^3 - 27a^4$.

Für alles kompliziertere benutzt man einen Computer.

Die Strategie zur Bestimmung von $\mathcal{O}_K$ wird sein:

- Schreibe $K = \mathbb{Q}[\alpha]$ mit $\alpha \in \mathcal{O}_K$,
- Berechne $d = d(1, \alpha, \ldots, \alpha^{n-1})$,

- Ist d quadratfrei, so ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Ganzheitsbasis, denn
$$d(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Disk}(K)[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$
impliziert $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$.
- Ist d nicht quadratfrei, so braucht $\{1, \alpha, \ldots, \alpha^{n-1}\}$ keine Ganzheitsbasis zu sein. Suche dann nach ganzen Zahlen, die nicht in $\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ enthalten sind.

Beispiel II.29: (i) Es sei $f = X^3 - X - 1 \in \mathbb{Q}[X]$. Das Polynom f ist irreduzibel, denn andernfalls hätte f eine Nullstelle in $\mathbb{Q}$. Diese wäre aber eine ganze Zahl, die 1 teilt, aber ± 1 sind keine Nullstellen von f.

Sei α eine Nullstelle von f. Dann ist $d(1, \alpha, \alpha^2) = \mathrm{Disk}(f) = -27 + 4 = -23$ quadratfrei. Folglich ist $\{1, \alpha, \alpha^2\}$ eine Ganzheitsbasis von $\mathbb{Q}[\alpha]$.

(ii) Es sei $f = X^3 + X + 1 \in \mathbb{Q}[X]$. Dann ist $\mathrm{Disk}(f) = -31$. Ist α eine Nullstelle, dann ist $\{1, \alpha, \alpha^2\}$ eine Ganzheitsbasis von $K = \mathbb{Q}[\alpha]$ und
$$\mathcal{O}_K = \mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(X^3 + X + 1).$$

Beispiel II.30 (Dedekind): Es seien $f = X^3 + X^2 - 2X + 8 \in \mathbb{Q}[X]$ und α eine Nullstelle von f. Dann ist $\mathrm{Disk}(f) = -2012 = -4 \cdot 503$. Das Element $\frac{1}{2}(\alpha + \alpha^2)$ ist ganz, und $d(1, \alpha, \frac{1}{2}(\alpha + \alpha^2)) = -503$ ist quadratfrei, also ist $(1, \alpha, \frac{1}{2}(\alpha + \alpha^2))$ eine Ganzheitsbasis. Dedekind hat gezeigt: Es gibt kein $\theta \in \mathcal{O}_K$ mit $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Beispiel II.31: Das Polynom $f = X^5 - X - 1$ ist irreduzibel in $\mathbb{F}_3[X]$, also auch in $\mathbb{Q}[X]$. Die Diskriminante von f ist $\mathrm{Disk}(f) = 2869 = 19 \cdot 151$, also auch quadratfrei. Damit ist $\mathcal{O}_K = \mathbb{Z}[\alpha]$, wobei α eine Nullstelle von f ist und $K = \mathbb{Q}[\alpha]$ gilt.

Satz II.32: *Sei K ein algebraischer Zahlkörper.*

(i) *Das Vorzeichen der Diskriminante von K ist $(-1)^s$, wobei $2s$ die Anzahl der Einbettungen $K \hookrightarrow \mathbb{C}$, deren Bild nicht in $\mathbb{R}$ enthalten ist, beschreibt.*

(ii) *Es gilt* $\mathrm{Disk}(K) \equiv 0, 1 \pmod 4$[1]

Beweis: (i) Sei $K = \mathbb{Q}[\alpha]$ und seien $\alpha_1 = \alpha, \ldots, \alpha_r$ die reellen Konjugierten von α und $\alpha_{r+1}, \bar{\alpha}_{r+1}, \ldots, \alpha_{r+s}, \bar{\alpha}_{r+s}$ die komplexen Konjugierten. Es gilt
$$\mathrm{sign}(d(1, \alpha, \ldots, \alpha^{n-1})) = \mathrm{sign}\left(\prod_{i=1}^{s} (\alpha_{r+i} - \bar{\alpha}_{r+i})^2\right) = (-1)^s,$$
da alle anderen Faktoren entweder Quadrate reeller Zahlen sind oder in komplex konjugierten Paaren auftreten.

[1] Diese Aussage ist bekannt als Stickelbergers Satz.

(ii) Sei $\alpha_1, \dots, \alpha_n$ eine Ganzheitsbasis von K und $\mathrm{Hom}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$. Es gilt $\mathrm{Disk}(K) = \det(\sigma_i \alpha_j)^2$. Mit der Leibniz-Formel für die Determinante haben wir

$$\begin{aligned}\mathrm{Disk}(K) &= \Big(\sum_{\tau \in S_n} \mathrm{sgn}(\tau) \prod_{i=1}^{n} \sigma_{\tau(i)} \alpha_j \Big)^2 \\ &= \Big(\sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma_{\tau(i)} \alpha_j - \sum_{\tau \in S_n - A_n} \prod_{i=1}^{n} \sigma_{\tau(i)} \alpha_j \Big)^2 = (P - N)^2 = (P + N)^2 - 4PN.\end{aligned}$$

Sei ρ ein Element der Galois-Gruppe der normalen Hülle von K in Ω. Dann ist $\rho(P) = P$ und $\rho(N) = N$ oder es ist $\rho(P) = N$ und $\rho(N) = P$: Es ist nämlich $\rho \circ \sigma_i = \sigma_j$, definiere also $\hat{\rho}\colon \{1, \dots, n\} \to \{1, \dots, n\}$ durch $\hat{\rho}(i) := j$. Jetzt ist

$$\rho\Big(\sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma_{\tau(i)} \alpha_j \Big) = \sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma_{\hat{\rho} \circ \tau(i)} \alpha_j = \begin{cases} P, & \text{falls } \hat{\rho} \in A_n, \\ N, & \text{falls } \hat{\rho} \notin A_n. \end{cases}$$

In jedem Fall sind $P + N$ und PN invariant unter ρ. Somit sind sie rationale Zahlen. Da sie auch ganz über $\mathbb{Z}$ sind, sind sie bereits ganze Zahlen. Es folgt

$$\mathrm{Disk}(K) \equiv (P + N)^2 \equiv 0, 1 \pmod 4. \qquad \square$$

Beispiel II.33: Für eine ganze quadratfreie Zahl m betrachte $\mathbb{Q}[\sqrt{m}]$. Es ist $\mathrm{Disk}(X^2 - m) = 4m$.

(i) Ist $m \equiv 2, 3 \pmod 4$, dann sagt der Satz von Stickelberger, dass $\mathrm{Disk}(K)$ nicht m ist. Bleibt nur $\mathrm{Disk}(K) = 4m$, denn m ist quadratfrei. Damit ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

(ii) Ist $m \equiv 1 \pmod 4$, dann ist $\theta = \frac{1}{2}(1 + \sqrt{m})$ ganz, denn

$$\mu_\theta = X^2 - X + \frac{1}{4}(1 - m) \in \mathbb{Z}[X].$$

Da $d(1, \theta) = m$ quadratfrei ist, ist $(1, \theta)$ eine Ganzheitsbasis und $\mathbb{Z}[\theta] = \mathcal{O}_K$.

Bemerkung II.34: Sind K und K' isomorph, so haben sie denselben Grad und die selbe Diskriminante. Die Umkehrung dieser Aussage ist falsch.

Aus Lemma II.0.22 erhalten wir für $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, mit $d = d(\alpha_1, \dots, \alpha_n)$, dass

$$d\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\frac{\alpha_1}{d} + \cdots + \mathbb{Z}\frac{\alpha_n}{d}.$$

Sei nun $\alpha + M$ eine Nebenklasse in $(\frac{1}{d}M)/M$. Dann ist entweder jeder Repräsentant aus der Nebenklasse ganz oder keiner. Um eine Ganzheitsbasis von $\mathcal{O}_K$ zu bestimmen genügt es also, Vetreter der d^n-Nebenklassen auf Ganzheit zu prüfen. Das Problem hierbei ist, dass d^n riesig wird.

Zum Beispiel ist $d = \mathrm{Disk}(x^5 + 17x^4 + 3x^3 + 2x^2 + x + 1) = 285\,401\,001$. Schon $285\,401\,001^5$ ist hoffnungslos zu groß für Computer.

Als erste Verbesserung könnten wir die einzelnen Primteiler p mit $p^2 \mid d$ untersuchen und dann in $\frac{1}{p}M$ nach ganzen Elementen suchen. Es geht aber noch besser!

Mit Algorithmus meinen wir eine Prozedur, die theoretisch ein Computer durchführen könnte und die nach endlich vielen Schritten zum richtigen Ergebnis kommt. Besteht die Eingabe des Algorithmus aus N Bits, so heißt der Algorithmus *gut*, falls es ein $C > 0$ gibt, sodass seine Laufzeit durch N^C beschränkt ist.

Ein *praktikabler* Algorithmus ist einer, der implementiert wurde und der nützlich ist.

Pohst und Zassenhaus entwickelten dern Round-2-Algorithmus zur Berechnung einer Ganzheitsbasiss für kleine Diskriminanten und kleinen Grad. Der ersten Schritt des Algorithmus ist das Finden der Quadratteiler von d. Dies ist auch der schwierigste Schritt im Algorithmus. Die Laufzeit eine N-stellige Zahl zu faktorisieren ist exponentiell in der Zahl der Stelle N. Gegeben die Primfaktorzerlegung von d ist der Algorithmus gut im obigen Sinne.

Kapitel III.

Ideale

Erinnerung III.1: Sei R ein Ring. Dann heißt R Noethersch, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) Jedes Ideal von R ist endlich erzeugt.

(ii) Jede aufsteigende Kette von Idealen wird stationär.

(iii) Jede nichtleere Menge von Idealen besitzt ein maximales Element.

Ohne Beweis verwenden wir im Folgenden die Aussage: „Ist A ein Noetherscher Ring, dann ist jeder endlich erzeugte A-Modul Noethersch“.

Beispiel III.2: Ist K ein Körper, so ist $K[X_1, \ldots, X_n]$ Noethersch. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist Noethersch. Ist K ein Körper, so ist $K[X_1, X_2, X_3, \ldots]$ nicht Noethersch.

Satz III.3: *Sei K ein Zahlkörper. Der Ring $\mathcal{O}_K$ ist Noethersch, ganzabgeschlossen und von Dimension 1 (d. h. jedes Primideal $\mathfrak{p} \neq 0$ ist maximal).*

Beweis: Als Untermodul des endlich erzeugten $\mathbb{Z}$-Moduls $\mathcal{O}_K \cong \mathbb{Z}^n$ ist jedes Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ ein endlich erzeugter $\mathbb{Z}$-Modul. Damit ist $\mathfrak{a}$ erst recht endlich erzeugt über $\mathcal{O}_K$. Als ganzer Abschluss von $\mathbb{Z}$ ist $\mathcal{O}_K$ auch ganzabgeschlossen.

Bleibt zu zeigen, dass $\dim \mathcal{O}_K = 1$. Sei dazu $0 \neq \mathfrak{p}$ ein Primideal von $\mathcal{O}_K$. Nun ist $\mathfrak{p} \cap \mathbb{Z} = (p)$ ein Primideal. Sei $0 \neq y \in \mathfrak{p}$ und seien $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, sodass

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0,$$

d. h. $a_0 = -y^n - a_{n-1}y^{n-1} - \cdots - a_1 y \in \mathfrak{p}$. Entsprechend gilt $0 \neq a_0 \in \mathfrak{p} \cap \mathbb{Z}$, und damit $(p) \neq 0$. Wir haben die exakte Sequenz

$$\mathfrak{p} \cap \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_K/\mathfrak{p}.$$

Also ist $\mathbb{Z}/(\mathfrak{p}) \subseteq \mathcal{O}_K/\mathfrak{p}$ und weiter ist $\mathcal{O}_K = \mathbb{Z}[a_0, \ldots, a_{n-1}]$, weswegen gilt dass $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/(p)[\bar{a}_0, \ldots, \bar{a}_{n-1}]$. Der Integritätsbereich $\mathcal{O}_K/\mathfrak{p}$ entsteht also aus dem Körper $\mathbb{Z}/(p)$ durch Adjunktion endlich vieler algebraischer Elemente. Folglich ist er ein Körper und $\mathfrak{p}$ maximal.

Alternativ haben wir das Diagramm

$$\mathcal{O}_K/\mathfrak{p} \twoheadleftarrow \mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\cong} \mathbb{Z}^n/p\mathbb{Z}^n,$$

d. h. $\#\mathcal{O}_K/\mathfrak{p} \leq p^n$. Als endlicher Integritätsbereich muss $\mathcal{O}_K/\mathfrak{p}$ bereits ein Körper sein. □

Definition III.4: Ein Noetherscher, ganzabgeschlossener Ring der Dimension 1 heißt *Dedekindring*.

Beispiel III.5: Der Koordinatenring $K[C]$ einer glatten Kurve C ist ein Dedekindring.

Im Folgenden sei stets $\mathcal{O}$ ein Dedekindring.

Lemma III.6: *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$ gibt es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

Beweis: Sei M die Menge der Ideale von $\mathcal{O}$, für die die Aussage des Lemmas nicht gilt. Angenommen, M wäre nicht leer. Da $\mathcal{O}$ Noethersch ist, hätte M ein maximales Element $\mathfrak{a}$ Da $\mathfrak{a}$ kein Primideal wäre, gäbe es $b_1, b_2 \in \mathcal{O}$ sodass $b_1 b_2 \in \mathfrak{a}$, aber $b_1, b_2 \notin \mathfrak{a}$. Für $\mathfrak{a}_1 := (b_1)+\mathfrak{a}$ und $\mathfrak{a}_2 := (b_2)+\mathfrak{a}$ gälte $\mathfrak{a} \subseteq \mathfrak{a}_1$, $\mathfrak{a} \subseteq \mathfrak{a}_2$ und $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. Aufgrund der Maximalität von $\mathfrak{a}$ wären $\mathfrak{a}_1$ und $\mathfrak{a}_2$ keine Elemente von M, d. h. es gäbe Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1$, $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{a}_2$. Wir hätten also $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{a}$ im Widerspruch zur Wahl von $\mathfrak{a}$. □

Lemma III.7: *Ist $\mathfrak{p}$ ein Primidal und $\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}$, so ist*

$$\mathfrak{a}\mathfrak{p}^{-1} = \left\{ \sum_i \alpha_i \beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{p}^{-1} \right\} \neq \mathfrak{a}$$

für jedes Ideal $\mathfrak{a} \neq 0$.

Beweis: Sei $a \in \mathfrak{p} - \{0\}$ und $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r. Nun ist eines der Primideale $\mathfrak{p}_i$ enthalten in $\mathfrak{p}$, denn sonst gäbe es für jedes i ein $a_i \in \mathfrak{p}_i - \mathfrak{p}$ mit $a_1 \cdots a_r \in \mathfrak{p}$. Ohne Beschränkung der Allgemeinheit ist $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Aufgrund der Maximalität von $\mathfrak{p}_1$ folgt $\mathfrak{p} = \mathfrak{p}_1$. Wegen der Minimaltität von r

ist $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$. Also gibt es ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ mit $b \notin \mathfrak{a}\mathcal{O}$ und somit $a^{-1}b \notin \mathcal{O}$. Andererseits ist aber $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$ und somit per Definition $a^{-1}b \in \mathfrak{p}^{-1}$. Damit ist $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Sei nun $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem. Angenommen, $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Für jedes $x \in \mathfrak{p}^{-1}$ hätten wir dann $x\alpha_i = \sum_j a_{ij}\alpha_j$, wobei a_{ij} geeignete Elemente von $\mathcal{O}$ wären. Für die Matrix $(x\delta_{ij} - a_{ij})$ wäre damit $A(\alpha_1, \ldots, \alpha_n)^t = 0$ und es wäre $A^*A(\alpha_1, \ldots, \alpha_n)^t = 0$, also erhielten wir schließlich $\det A(\alpha_1, \ldots, \alpha_n)^t = 0$ und somit $\det A = 0$. Daher wäre x als Nullstelle des normierten Polynoms $\det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$ ganz. Da aber $\mathcal{O}$ ganzabgeschlossen ist, wäre schon $x \in \mathcal{O}$, also $\mathfrak{p}^{-1} = \mathcal{O}$ im Widerspruch zum soeben gezeigten. □

Satz III.8: *Jedes von* (0) *und* (1) *verschiedene Ideal* $\mathfrak{a} \subseteq \mathcal{O}$ *besitzt eine bis auf Reihenfolge eindeutige Zerlegung in* $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ *in Primideale* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$.

Beweis: Zunächst zeigen wir die Existenz. Wir arbeiten per schlechte Menge: Setze

$$\mathfrak{M} := \{\mathfrak{a} \trianglelefteq \mathcal{O} \mid \mathfrak{a} \neq (0), (1),\ \mathfrak{a} \text{ hat keine Zerlegung in Primideale}\}$$

Angenommen, $\mathfrak{M}$ wäre nicht leer. Da $\mathcal{O}$ Noethersch ist, hätte M ein maximales Element $\mathfrak{a}$. Es gäbe ein maximales Ideal $\mathfrak{p} \subseteq \mathcal{O}$, sodass $\mathfrak{a}$ in $\mathfrak{p}$ enthalten wäre. Nach dem vorangegangenen Lemma hätten wir

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}.$$

Weiter wäre mit (Lemma IV.7) $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ und folglich $\mathfrak{p}\mathfrak{p}^{-1}$. Da $\mathfrak{a}$ maximal in $\mathfrak{M}$ wäre, könnte $\mathfrak{a}\mathfrak{p}^{-1}$ kein Element von $\mathfrak{M}$ sein. Außerdem könnte $\mathfrak{a}$ nicht gleich $\mathfrak{p}$ sein, d. h. es müssten $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{p}\mathfrak{p}^{-1} = (1)$. Damit müsste $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ mit geeigneten Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Dann wäre aber auch

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$$

im Widerspruch zur Voraussetzung. Foglich muss $\mathfrak{M}$ leer sein und wir sind fertig.

Zur Eindeutigkeit: Für ein Primideal $\mathfrak{p}$ gilt: Ist $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, dann ist schon $\mathfrak{a}$ ist enthalten in $\mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$. Das heißt wenn $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$, dann gilt schon $\mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$. Weiter ist $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Seien nun $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ und $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ zwei Zerlegungen mit Primidealen $\mathfrak{p}_i, \mathfrak{q}_j$ in $\mathcal{O}$. Dann teilt $\mathfrak{p}_1$ eines der $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, etwa $\mathfrak{q}_1$. Dann hätten wir $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$ und damit wegen der Maximalität $\mathfrak{p}_1$ schon $\mathfrak{p}_1 = \mathfrak{q}_1$. Wir können $\mathfrak{p}_1 = \mathfrak{q}_1$ fallen lassen und erhalten

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

Induktiv erhalten wir $r = s$ und nach Umordnung $\mathfrak{p}_i = \mathfrak{q}_i$ für $1 \leq i \leq r$. □

Definition III.9: Ein *gebrochenes Ideal von K* ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K. Die Ideale von $\mathcal{O}$ nennen wir *ganze Ideale*

Beispiel III.10: Für $a \in K^\times$ ist $a\mathcal{O}$ ein gebrochenes Hauptideal. Zum Beispiel $(1/2)\mathbb{Z} \subseteq \mathbb{Q}$.

Lemma III.11: *Die gebrochenen Ideale von K sind genau die $\mathcal{O}$-Moduln $\mathfrak{a} \neq 0$ für die ein $0 \neq c \in \mathcal{O}$ exisitert mit $c\mathfrak{a} \subseteq \mathcal{O}$.*

Beweis: Ist $\mathfrak{a} = a_1\mathcal{O} + \cdots + a_n\mathcal{O}$, so tut es ein $0 \neq c \in \mathcal{O}$ mit $ca_1 \cdots a_n \in \mathcal{O}$.

Ist umgekehrt $c\mathfrak{a} \subseteq \mathcal{O}$, dann ist, da $\mathcal{O}$ Noethersch ist, $c\mathfrak{a} = \alpha_1\mathcal{O} + \cdots + \alpha_n\mathcal{O}$ mit $\alpha_i \in \mathcal{O}$ und somit $\mathfrak{a} = \alpha_1/c\mathcal{O} + \cdots + \alpha_n/c\mathcal{O}$. □

Satz III.12: *Die Menge der gebrochenen Ideal bildet eine abelsche Gruppe, die Idealgruppe $\mathfrak{J}_K$ von K. Das neutrale Element ist $\mathcal{O}$ und das Inverse zu $\mathfrak{a} \in \mathfrak{J}_K$ ist*

$$(\mathcal{O} : \mathfrak{a}) = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\} =: \mathfrak{a}^{-1}.$$

Beweis: Die Assoziativität und Kommutativität sind klar, ferner ist $\mathfrak{a}\mathcal{O} = \mathfrak{a}$ klar. Für ein Primideal $\mathfrak{p} \subseteq \mathcal{O}$ ist $\mathfrak{p} \subseteq (\mathcal{O} : \mathfrak{p})\mathfrak{p} \subseteq \mathcal{O}$. Da $\mathfrak{p}$ maximal ist, ist $(\mathcal{O} : \mathfrak{p})\mathfrak{p} = \mathcal{O}$ und damit $(\mathcal{O} : \mathfrak{p}^{-1}) = \mathfrak{p}^{-1}$.

Das Inverse zu $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathcal{O}$ ist also $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} = \mathfrak{b}$.

Ist nun $\mathfrak{a}$ ein gebrochenes Ideal und $c \in \mathcal{O}$ mit $c\mathfrak{a} \leq \mathcal{O}$, dann ist $(c)(c\mathfrak{a})^{-1}$ ein Inverses von $\mathfrak{a}$. Insgesamt ist $\mathfrak{J}_K$ eine abelsche Gruppe.

Es bleibt zu zeigen, dass $\mathfrak{b} = (\mathcal{O} : \mathfrak{a})$. Aus $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ folgt $\mathfrak{b} \subseteq (\mathcal{O} : \mathfrak{a})$. Umgekehrt folgt aus $x \in (\mathcal{O} : \mathfrak{a})$, d. h. $x\mathfrak{a} \subseteq \mathcal{O}$, dass $x\mathfrak{a}\mathfrak{b} = (x) \subseteq \mathfrak{b}$, also ist $x \in \mathfrak{b}$ und somit ist $(\mathcal{O} : \mathfrak{a}) = \mathfrak{b} = \mathfrak{a}^{-1}$. □

Korollar III.13: *Jedes Ideal $\mathfrak{a} \in \mathfrak{J}_K$ ist von der Form $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$ mit $\nu_\mathfrak{p} \in \mathbb{Z}$ und $\nu_\mathfrak{p} = 0$ für fast alle Primideale $\mathfrak{p}$.*

In anderen Worten: $\mathfrak{J}_K$ ist die freie abelsche Gruppe, die von den Primidealen $\mathfrak{p} \neq 0$ erzeugt wird.

Definition III.14: Sei $P_K := \{a\mathcal{O} \mid a \in K^\times\}$. Die *Klassengruppe* oder *Idealklassengruppe* Cl_K von K ist der Quotient $\mathfrak{J}_K/\mathfrak{P}_K$.

Betrachte die folgende exakte Sequenz:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^\times & \longrightarrow & K^\times & \longrightarrow & \mathfrak{J}_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 1 \\ & & & & a & \longmapsto & a\mathcal{O} & & & & \end{array}$$

Die Einheitengruppe $\mathcal{O}^\times$ beschreibt den Verlust, den wir beim Übergang von Zahlen zu Idealen erleiden und die Klassengruppe die Größe der Ausdehnung.

Beispiel III.15: (i) Die Ringe $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$ und $\mathbb{Z}[\omega]$, wobei ω eine dritte Einheitswurzel ist, sind Hauptidealbereiche. Damit ist $\mathrm{Cl}_K = \{1\}$ in diesem Fall.

(ii) Wir betrachten die affine elliptische Kurve $E := y^2 = x^3 + ax + b\mathrm{i}$. Diese hat die Diskriminante $\Delta = -4a^3 - 27b^2 \neq 0$ und $\mathbb{C}[E] = \mathbb{C}[x, y]/y^2 - x^3 - ax - b$ ist der Ring der regulären Funktionen. $\mathbb{C}[E]$ ist ein Dedekindring und die Klassengruppe ist überabzählbar – es ist nämlich

$$\mathrm{Cl}(\mathbb{C}[E]) \cong \mathrm{Pic}^0(\bar{E}) \cong \bar{E}(\mathbb{C}) \cong \mathbb{C}/\Lambda$$

für ein Gitter $\Lambda \subseteq \mathbb{C}$ und $\bar{E} \subseteq \mathbb{P}^3$ den projektiven Abschluss.

Wir wollen uns im Folgenden mit der Klassengruppe von ganzalgebraischen Erweiterungen beschäftigen. Wir wollen zeigen, dass $\#\,\mathrm{Cl}_K < \infty$ und dass $\mathcal{O}_K^\times \cong \mu_k \times \mathbb{Z}^r$.

Kapitel IV.

Gitter

Definition IV.1: Es sei V ein n-dimensionaler Vektorraum über dem Körper $\mathbb{R}$. Ein Gitter in V ist eine Untergruppe der Form $\Gamma = \mathbb{Z}_1 v_1 + \cdots + \mathbb{Z} v_m$ mit Vektoren $v_1, \ldots, v_m \in V$ sodass $\{v_1, \ldots, v_m\}$ linear unabhängig ist.

Ist $n = m$, so heißt das Gitter *voll* oder *vollständig*. $(v_1, \ldots, v_m)$ ist eine Basis von Γ und $\Phi = \{x^t v \mid x \in [0,1)^m\}$ die Grundmasche von Γ.

Beispiel IV.2: Hier fehlt eine Skizze.

Kein Gitter in $\mathbb{R}$ oder $\mathbb{C}$ ist zum Beispiel $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z} \subseteq \mathbb{R}$, da $\{2, \sqrt{2}\}$ $\mathbb{R}$-linear abhängig ist.

Bemerkung IV.3: Die Grundmasche Φ ist ein Fundamentalbereich der Wirkung von Γ auf V. Insbesondere ist Φ ein Repräsentantensystem von V/Γ.

Satz IV.4: *Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis: Ohne Beschränkung der Allgmeinheit sei $\mathbb{R}\Gamma = V$ – ersetze sonst V durch $\mathbb{R}\Gamma$. Sei $\Gamma \subseteq V$ ein Gitter mit Basis $v_1, \ldots, v_n$. Für $\gamma = \sum_i a_i v_i \in \Gamma$ ist $U = \{\sum_i x_i v_i \mid |x_i - a_i| < 1|\}$ eine offene Umgebung mit $\Gamma \cap U = \{\gamma\}$. Also ist Γ diskret.

Sei umgekehrt $\Gamma \subseteq V$ eine diskrete Untergruppe. Da $\mathbb{R}\Gamma = V$ finden wir eine in Γ gelegene Basiss $\{v_1, \ldots, v_n\} \subseteq \Gamma$ von V. Sei

$$\Gamma_0 = \mathbb{Z} v_1 + \cdots + \mathbb{Z} v_n$$

das zugehörige Gitter und Φ_0 seine Grundmasche. Nun ist $\Gamma \cap \Phi_0$ ein Repräsentantensystem von $\Gamma/\Gamma_0 \subseteq V/\Gamma_0$. Da Φ_0 beschränkt und Γ diskret ist, ist $\Gamma \cap \Phi_0 = [\mathbb{T} : \Gamma_0]q$ endlich. Es gilt also $q\Gamma \subseteq \Gamma_0$ und damit $\Gamma_0 \subseteq \Gamma \subseteq 1/q\Gamma_0$.

Nach dem Hauptsatz über endliche abelsche Gruppen besitzt Γ nun eine $\mathbb{Z}$-Basis $(u_1, \ldots, u_n)$. Da diese den Raum V aufspannt, ist sie auch $\mathbb{R}$-linear unabhängig und somit M ein Gitter. □

Lemma IV.5: *Ein Gitter Γ in V ist genau dann vollständig, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt mit $\bigcup_{\gamma\in\Gamma}(\gamma + M) = V$.*

Beweis: Für ein vollständiges Gitter tut es die Grundmasche $M = \Phi$. Sei umgekehrt $M \leq V$ beschränkt mit $V = \bigcup_\gamma \gamma + M$ und $v \in V$ beliebig. Zu einer natürlichen Zahl i finden wir nun $m_i \in M$ und $\gamma_i \in M$ mit $iv = \gamma_i + m_i$. Da M beschränkt ist, ist m/i eine Nullfolge und

$$v = \lim_{i\to\infty} \frac{\gamma_i + m_i}{i} = \lim_{i\to\infty} \frac{\gamma_i}{i} \in \mathrm{cl}(\mathbb{Q}\Gamma) = \mathbb{R}\Gamma.$$

Somit ist $V = \mathbb{R}\Gamma$ und Γ voll. □

Im Folgenden sei V ein euklidischer Vektorraum, d. h. $\dim V = n < \infty$ und V trägt ein Skalarprodukt $\langle\cdot,\cdot\rangle$. Für eine Orthonormalbasis $(e_1, \ldots, e_n)$ erhalten wir $V \cong \mathbb{R}^n$ und damit ein Maß μ auf V. Der von $(e_1, \ldots, e_n)$ aufgespannte Würfel erhält das Volumen 1. Ist $(v_1, \ldots, v_n)$ eine Basis eines Gitter $\Gamma \subseteq V$ und $v_i = \sum_j a_{ij}e_j$, so ist bekanntlich das Volumen des von $(v_1, \ldots, v_n)$ aufgespannten Spats Φ gegeben durch $\mathrm{vol}(\Phi) = |\det A|$, wobei $A = (a_{ij})$. Nun ist

$$\det(\langle v_i, v_j\rangle)_{ij} = \det\Big(\sum_{k=1}^n\sum_{\ell=1}^n a_{ik}a_{j\ell}\langle e_k, e_\ell\rangle\Big)_{ij} = \det\Big(\sum_{k=1}^n a_{ik}a_{jk}\Big)_{ij} = (\det A)^2.$$

Definition IV.6: Sei Γ ein Gitter. Das Volumen von Γ ist das Volumen der Grundmasche Φ von Γ, also

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = \sqrt{|\det(\langle v_i, v_j\rangle)_{ij}|},$$

wobei $(v_1, \ldots, v_n)$ eine Basis des Gitters ist.

Beispiel IV.7: (i) Es ist $\mathrm{vol}(\mathbb{Z}^n) = 1$.

(ii) Ist ω eine dritte Einheitswurzel, dann ist

$$\mathrm{vol}(\mathbb{Z}[\omega]) = \left|\begin{pmatrix} 1 & \cos 2\pi/6 \\ 0 & \sin 2\pi/6 \end{pmatrix}\right| = \sqrt{3}/2.$$

Definition IV.8: Sei V ein n-dimensionaler euklidischer Vektorraum. Eine Teilmenge $X \subseteq V$ heißt *zentralsymmetrisch*, falls $X = -X$. X heißt *konvex*, falls für $x, y \in X$ auch die Menge $\{tx + (1-t)y \mid t \in [0,1]\}$ (die Linie von x nach y) in X enthalten ist.

Beispiel IV.9: Skizzen zu Konvex, nicht konvex und zentralsymmetrisch.

Satz IV.10 (Mikowskischer Gitterpunktsatz): *Seien $\Gamma \subseteq V$ ein volles Gitter, $n = \dim V$ und $X \subseteq V$ zentralsymmetrisch und konvex. Ist $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$, so gibt es ein $0 \neq x \in \Gamma \cap X$.*

Beweis: Zunächst überlegen wir uns, dass es genügt, zwei verschiedene Gitterpunkte $\gamma_1, \gamma_2 \in \Gamma$ zu finden, sodass $(1/2X + \gamma_1) \cap (1/2X + \gamma_2) \neq \varnothing$.

Sei dazu $1/2x_1 + \gamma_1 = 1/2x_2 + \gamma_2$, wobei $x_1, x_2 \in X$, ein Punkt aus dem Durchschnitt. Dann ist $\gamma := \gamma_1 - \gamma_2 = 1/2(x_1 - x_2)$ der Mittelpunkt der Strecke von x_2 nach $-x_1$, der zu X gehört.

Nehmen wir also an, die Mengen $1/2X + \gamma$, wobei $\gamma \in \Gamma$, seien paarweise disjunkt. Dann wäre

$$\begin{aligned}\mathrm{vol}(\Phi) &\geq \mathrm{vol}\left(\bigcup_{\gamma\in\Gamma}\dot{}\,(1/2X+\gamma)\cap\Phi\right)\\ &= \sum_{\gamma\in\Gamma}\mathrm{vol}[(1/2X+\gamma)\cap\Phi]\\ &= \sum_{\gamma\in\Gamma}\mathrm{vol}[1/2X\cap(\Phi-\gamma)] = \mathrm{vol}(1/2X) = 2^{-n}\,\mathrm{vol}(X) > \mathrm{vol}(\Phi),\end{aligned}$$

was nicht sein kann. □

Als Übungsaufgabe beleibt dem Leser überlassen zu zeigen, dass für kompakte X bereits $\mathrm{vol}(X) \geq 2^n \mathrm{vol}(\Gamma)$ gilt.

Satz IV.11 (Lagranges Vier-Quadrate-Satz): *Jede natürliche Zahl ist die Summe von vier Quadratzahlen.*

Beweis: Von Euler, der den Satz selbst nicht beweisen konnte, stammt der Beitrag

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)\\ &\quad= (aA-bB-cC-dD)^2+(aB+bA+cD+dC)^2\\ &\qquad+(aC-bC-cA+dB)^2+(aD+bC-cB+dA)^2\end{aligned}$$

Eine Erklärung dieser Identität findet sich mit den sogenannten *Quaternionen* $\mathbb{H} = \mathbb{R}\langle i,j,k\rangle/(i^2 = j^2 = k^2 = -1, ijk = -1)$ und der Identität $|x|^2|y|^2 = |xy|^2$ für $x = a + bi + cj + dk$ und $y = A + Bi + Cj + Dk$.

Wegen des Beitrags von Euler genügt es also zu zeigen, dass jede Primzahl p eine Summe von vier Quadratzahlen ist. Zunächst ist $1^2 + 1^2 + 0^2 + 0^2 = 2$. Wir können also $p > 2$ annehmen. Die Gleichung $m^2 + n^2 + 1 \equiv 0 \pmod{p}$ hat

eine Lösung in den ganzen Zahlen, denn andernsfalls wären die je $(p+1)/2$ Elemente im Bild der Abbildungen

$$\mathbb{F}_p \longrightarrow \mathbb{F}_p, \qquad m \longmapsto m^2 \quad \text{und} \quad n \longmapsto -n^2 - 1$$

disjunkt.

Seien nun $n, m \in \mathbb{Z}$ eine Lösung der Kongruenz. Wir betrachten das Gitter

$$\Lambda = \{(a,b,c,d) \in \mathbb{Z}^4 \mid c \equiv ma + nb \pmod{p},\ d \equiv mb - na \pmod{p}\}.$$

Nun ist $\mathbb{Z}^4 \supseteq \Lambda \supseteq p\mathbb{Z}^4$ und $\Lambda/p\mathbb{Z}^4$ ist ein zweidimensionaler Untervektorraum von $\mathbb{F}_p^4$. Also hat Λ den Index p^2 in $\mathbb{Z}^4$ und das Volumen seiner Grundmasche ist p^2.

Sei T der Ball von Radius r um den Ursprung. Mit $\mathrm{vol}(T) = \pi^2 r^4/2$ und einem r mit $2p > r^2 > 1{,}9p$ erhalten wir $16\,\mathrm{vol}(\Gamma) < \mathrm{vol}(T)$. Nach Satz IV.10 erhalten wir ein $0 \neq (a,b,c,d) \in \Lambda \cap T$. Wegen $(a,b,c,d) \in \Lambda$ ist

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ma+nb)^2 + (na-mb)^2 \\ &\equiv a^2(m^2+n^2+1) + b^2(n^2+m^2+1) \equiv 0 \pmod{p} \end{aligned}$$

und weil $(a,b,c,d) \in T$ ist $0 < x = a^2 + b^2 + c^2 + d^2 < r^2 < 2p$. Diese beiden Bedingungen erfüllt nur $x = p$. □

Wir wollen nun den Ring $\mathcal{O}_K$ der ganzen Zahlen eines Zahlkörpers K als Gitter in einem euklidischen Vektorraum auffassen. Wie schon das Beispiel $\mathbb{Z}[\sqrt{2}]$ zeigt, brauchen wir zunächst einen geeigneten Vektorraum. Dies sind die Räume $K \otimes_{\mathbb{Q}} \mathbb{R}$ und $K \otimes_{\mathbb{Q}} \mathbb{C}$.

Explizit ist

$$K \otimes_{\mathbb{Q}} \mathbb{C} \longrightarrow \prod_{\tau \in \mathrm{Hom}(K,\mathbb{C})} \mathbb{C} = \mathbb{C}^{\mathrm{Hom}(K,\mathbb{C})} =: K_{\mathbb{C}}, \qquad a \otimes x \longmapsto (\tau(a)x)_{\tau \in \mathrm{Hom}(K,\mathbb{C})}$$

ein Isomorphismus. Auf der rechten Seite können wir nun das übliche Skalarprodukt $\langle (x_\tau), (y_\tau) \rangle = \sum_\tau x_\tau \bar{y}_\tau$ definieren.

Die komplexe Konjugation $F(a \otimes x) = a \otimes \bar{x}$ geht über zu $F(z)_\tau = \bar{\tau}_{\bar{t}}$, wobei $z \in \mathbb{K}_{\mathbb{C}}$, denn $F(\tau(a)x)_\tau = \tau(a)\bar{x} = \overline{\bar{\tau}(a)x}_\tau$. Die Inklusion $K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{C}$ liefert uns, dass $K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \mid F(z) = z\}$ und durch die Einschränkung das kanonische Skalarprodukt $\langle \cdot, \cdot \rangle \colon K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ und das zugehörige kanonische Volumen. Sei $j \colon K \to K_{\mathbb{R}}$, $a \mapsto (\tau a)_\tau$ die Inklusion.

Satz IV.12: *Für ein Ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ ist $\Gamma := j\mathfrak{a}$ ein vollständiges Gitter in $K_{\mathbb{R}}$ mit* $\mathrm{vol}(\Gamma) = |d_K|^{1/2}[\mathcal{O}_K : \mathfrak{a}]$.

Beweis: Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von Γ und $\mathrm{Hom}(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\}$. Einerseits ist nun

$$\det(\tau_\ell \alpha_j)^2 = d(\alpha_1, \ldots, \alpha_r) = d(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2 d_K$$

und andererseits ist

$$\begin{aligned} \mathrm{vol}(\Gamma)^2 &= |\det\langle j\alpha_i, j\alpha_k\rangle_{i,k}| \\ &= \det(\sum_{\ell=1}^{n} \tau_\ell \alpha_i \bar{\tau}_\ell \alpha_k)_{ik} = \det(\tau_\ell \alpha_i)\det(\bar{\tau}_\ell \alpha_k) = |\det \tau_\ell \alpha_i|^2. \end{aligned}$$ □

Seien $\rho_1, \ldots, \rho_r \colon K \to \mathbb{R}$ die reellen und $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s \colon K \to \mathbb{C}$ die komplexen Einbettungen von K, sodass $n = r + 2s$. Wir erhalten so

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} = \prod_{\tau} \mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_\sigma\}.$$

Satz IV.13: *Für den Isomorphismus*

$$f \colon K_{\mathbb{R}} \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s}, \qquad (z_\tau) \longmapsto (z_{s_1}, \ldots, z_{s_r}, z_{\sigma_1}, \ldots, z_{\sigma_s})$$

ist $\langle a_\tau, b_\tau\rangle = \sum_{i=1}^{r} a_{s_i} b_{s_i} + 2\sum_{i=1}^{s} a_{\sigma_i}\bar{b}_{\sigma_i}$. *Insbesondere gilt für Borel-messbares* $X \subseteq K_{\mathbb{R}}$, *dass* $\mathrm{vol}_{\mathrm{kan}}(X) = 2^s \mathrm{vol}_{\mathrm{Leb}}(f(X))$.

Beweis: Wegen der Polarisierungsidentität genügt es, $a_\tau = b_\tau \in K_{\mathbb{R}}$ zu betrachten. Dafür finden wir

$$\langle a_\tau, a_\tau\rangle = \sum_{i=1}^{r} a_{s_i}^2 + \sum_{i=1}^{s} |a_{\sigma_i}|^2 + \sum_{i=1}^{s} |a_{\bar{\sigma}_i}^2 = \sum_{i=1}^{r} a_{s_i}^2 + 2\sum_{i=1}^{s} |a_{\sigma_i}|^2,$$

was wir zeigen wollten. □

Lemma IV.14: *Für* $X_t = \{(z_\tau) \in \mathbb{K}_R \mid \sum_\tau |z_\tau| \le t\}$ *gilt* $\mathrm{vol}_{\mathrm{kan}}(x_t) = 2^r \pi^s t^n / n!$.

Beweis: Wir rechnen in Koordinaten.

$$f(X_t) = \Big\{x \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i=1}^{r} |x_i| + 2\sum_{j=1}^{s} |z_{r+j}|^2 \le t\Big\}.$$

Aus der Symmetrie in den r reellen Koordinaten erhalten wir:

$$2^s \mathrm{vol}_{\mathrm{kan}}(X_t) = 2^s \mathrm{vol}_{\mathrm{Leb}}(f(X_t)) = 2^{r+s} \mathrm{vol}_{\mathrm{Leb}}(Y_t),$$

wobei $Y_t = \{x \in f(X_t) \mid x_1, \dots, x_r \geq 0\}$. Drücken wir die komplexen Koordinaten in Polarkoordinaten aus, also $z_j = \rho_j/2(\cos\theta_j + \mathrm{i}\sin\theta_j)$, dann erhalten wir

$$2^s \operatorname{vol}_{\mathrm{kan}}(X_t) = 2^{r+s}\frac{(2\pi)^3}{4^s}\int_{Z_t} \rho_1 \cdots \rho_s \, dx_1 \cdots dx_r \, d\rho_1 \cdots d\rho_s = 2^r\pi^s t^n/n!,$$

wobei $Z_t = \{(x_1, \dots, x_r; \rho_1, \dots, \rho_s) \in \mathbb{R}^{r+s} \mid 0 \leq x_i, \rho_i,\ \sum_i x_i + \sum_i \rho_i \leq t\}$. Für die letzte Gleichheit verweisen wir auf eine Übungsaufgabe. □

Wir erinnern uns der Ungleichung des geometrischen und arithmetischen Mittels. Für reelle Zahlen $a_1, \dots, a_n \in [0, \infty)$ gilt $(\prod_i a_i)^{1/n)} \leq 1/n \sum_i a_i$ beziehungsweise äquivalent $\prod_i a_i \leq \frac{1}{n^n}(\sum_i a_i)^n$.

Definition IV.15: Die Absolutnorm eines Ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ ist $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$.

Als Übungsaufgabe kann man zeigen, dass $N(a\mathcal{O}_K) = |N_{K|\mathbb{Q}}(a)|$.

Satz IV.16: *Jedes Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ enthält ein Element $\alpha \neq 0$ mit Norm*

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_k|}N(\mathfrak{a}).$$

Hierbei heißt $(4/\pi)^s n!/n^n\sqrt{|d_k|}$ die Minkowski-Schranke.

Beweis: Die Menge X_t ist kompakt, konvex und zentralsymmetrisch. Ist nun t ausreichend groß, dass $\operatorname{vol}(X_t) \geq 2^n \operatorname{vol}(j\mathfrak{a})$, dann erhalten wir aus Satz IV.10 ein $0 \neq j\alpha \in j\mathfrak{a}$. Für dieses $\alpha \in \mathfrak{a}$ gilt

$$|N_{K|\mathbb{Q}}(\alpha)| = \prod_\tau |\tau\alpha| \leq \frac{1}{n^n}\Big(\sum_\tau |\tau\alpha|\Big)^n \leq \frac{t^n}{n^n}. \tag{IV.1}$$

Für unsere Ungleichung brauchen wir $2^r\pi^s t^n/n! \geq 2^n\sqrt{|d_k|}N(\mathfrak{a})$, also genügt

$$t^n \geq 2^{n-r}\pi^{-s}n!\sqrt{|d_k|}N(\mathfrak{a}).$$

Einsetzen in Gl. (IV.1) liefert jetzt die Behauptung. □

Satz IV.17: *Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ die Primzerlegung von $0 \neq \mathfrak{a} \leq \mathcal{O}_K$, so ist*

$$N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{\nu_i}.$$

Beweis: Da die $\mathfrak{p}_i$ teilerfremd sind, gilt $\bigcap_{i=1}^r \mathfrak{p}_i^{\nu_i} = \prod_{i=1}^r \mathfrak{p}_i^{\nu_i}$. Nach dem chinesischen Restsatz ist $\mathcal{O}_K/\mathfrak{a} \cong \bigoplus_{i=1}^r \mathcal{O}_K/\mathfrak{p}_i^{\nu_i}$, sodass es genügt, den Fall einer Primpotenz $\mathfrak{p}^\nu$ zu betrachten. In der Kette $\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$ ist $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ein $\mathcal{O}_K/\mathfrak{p}$-Vektorraum der Dimension 1.

In der Tat: Ist $a \in \mathfrak{p}^i - \mathfrak{p}^{i+1}$, so ist $p^{i+1} \subsetneq \mathfrak{b} := (a) + \mathfrak{p}_{i+1} = \mathfrak{p}^i$, denn andernfalls wäre $\mathfrak{b}\mathfrak{p}^{-i}$ ein echter Teiler von $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$. Folglich ist $\bar{a} = a + \mathfrak{p}$ eine Basis von $\mathfrak{p}^{i+1}/\mathfrak{p}^i \cong \mathcal{O}_K/\mathfrak{p}$. Es gilt damit

$$[\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K : \mathfrak{p}] \cdot [\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}] = N(\mathfrak{p}^\nu),$$

was wir zeigen wollten. □

Satz IV.18: *Seien $K|\mathbb{Q}$ eine Körpererweiterung vom Grad n, d_K die Diskriminante von K und $2s$ die Anzahl der echt komplexen Einbettungen von K. Dann gibt es ein Repräsentantensystem der Klassengruppe Cl_K aus Idealen $\mathfrak{a} \subseteq \mathcal{O}_K$ mit*

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |d|^{1/2} =: M_K.$$

Beweis: Sei $\mathfrak{c} \in \mathfrak{J}_K$ ein gebrochenes Ideal. Dann gibt es ein $d \in K^\times$, sodass $\mathfrak{b} = d\mathfrak{c}^{-1}$ ein Ideal in $\mathcal{O}_K$ ist. Es gibt nun ein $\beta \in \mathfrak{b}$ mit $|N_{K|\mathbb{Q}}(\beta)| \leq M_K N(\mathfrak{b})$.

Mit $\beta\mathcal{O}_K \subseteq \mathfrak{b}$ folgt $\beta\mathcal{O}_K = \mathfrak{a}\mathfrak{b}$ für ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ mit $\mathfrak{a} \sim \mathfrak{b}^{-1} \sim \mathfrak{c}$. Hier schreiben wir $\mathfrak{a} \sim \mathfrak{b}^{-1}$, falls es $c \in K^\times$ mit $(c)\mathfrak{a} = \mathfrak{b}$ gibt, d. h. falls $[\mathfrak{a}] = [\mathfrak{b}]$ in Cl_K. Wir schließen den Beweis mit $N(\mathfrak{a})N(\mathfrak{b}) = |N_{K|\mathbb{Q}}(\beta)| \leq M_K N(\mathfrak{b})$, also $N(\mathfrak{a}) \leq M_K$. □

Satz IV.19: *Die Klassenzahl Cl_K von K ist endlich.*

Beweis: Es genügt zu zeigen, dass es nur endlich viele Ideale $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq M_K$ gibt. Ist $0 \neq \mathfrak{p}$ ein Primideal in $\mathcal{O}_K$ und $(p) = \mathfrak{p} \cap \mathbb{Z}$, so ist $\mathcal{O}_K/\mathfrak{p}|\mathbb{Z}/p\mathbb{Z}$ eine endliche Körpererweiterung von einem Grad $f \geq 1$. Also ist $N(\mathfrak{p}) = p^f$. Für festes $p \in \mathbb{Z}$ gibt es nur endlich viele Primideale $\mathfrak{p} \subseteq \mathcal{O}_K$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$, da dies $\mathfrak{p} \mid p\mathcal{O}_K$ impliziert. Es gibt also nur endlich viele Primideale mit beschränkter Absolutnorm. Nach Satz IV.17 gibt es dann überhaupt nur endlich viele Ideale mit beschränkter Absolutnorm. □

Beispiel IV.20: (i) Es sei $K = \mathbb{Q}[\mathrm{i}]$. In diesem Fall sind $r = 0$ und $s = 1$, d. h. nach Satz IV.18 gilt für den Erzeuger $\mathfrak{a}$ von Cl_k, dass

$$N(\mathfrak{a}) \leq M_K = \frac{2!}{2^2}\frac{4}{\pi} \cdot 2 < 1{,}27.$$

Es folgt $N(\mathfrak{a}) = 1$ und damit $\mathfrak{a} = (1)$. Also ist $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealring. Euklidisch ist stärker! Zum Beispiel ist $\mathbb{Z}[\sqrt{15}]$ ein Hauptidealring, aber nicht euklidisch.

(ii) Sei $K = \mathbb{Q}(\sqrt{-5})$. Dann ist $N(\mathfrak{a}) \leq M_K \leq 3$. Also teilt $\mathfrak{a}$ das Hauptideal (2). Auf Übungsblatt 6 wird gezeigt, dass $\mathfrak{a} = (2, 1 + \sqrt{-5})$ und $\mathfrak{a}^2$, also ist $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$.

(iii) Sei K ein kubischer Körper mit $d_K < 0$. Das Vorzeichen von d_K ist $(-1)^s$ und $3 = n = r + 2s$. Also ist $r = s = 1$ und

$$M_K < 0.283|d_K|^{1/2}.$$

Für $|d_K|y49$ ist nun $M_K < 2$ und folglich $\mathrm{Cl}_K = 1$. Dies gilt zum Beispiel für die kubischen Körper mit Diskriminante -23 und -31 aus vorangegangen Beispielen.

(iv) Für den Stammkörper K von $x^3+10x+1$ ist $d_K \leq -4027$ und $M_K < 18$. Man kann zeigen, dass $\mathrm{Cl}_K \cong \mathbb{Z}/6\mathbb{Z}$.

Kapitel V.

Einheiten

Ziel dieses Kapitels ist einzusehen, dass $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r$. Das Hauptwerkzeug zum Erreichen dieses Ziels wird der Minkowskische Gitterpunktsatz sein.

Im Folgenden sei K weiterhin ein Zahlkörper. Weiter sei

$$K_{\mathbb{R}}^\times = \{(x_z) \in K_{\mathbb{R}} \mid x_\tau \neq 0 \text{ für alle } \tau \in \mathrm{Hom}(K, \mathbb{C})\}.$$

Wir erhalten Homomorphismen

$$\begin{array}{ccccc} & & \overset{\lambda}{\curvearrowright} & & \\ K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \longrightarrow & \mathbb{R}^{r+s} \\ \alpha & \longmapsto & (\tau(\alpha))_\tau & & \\ & & (z_\tau)_\tau & \longmapsto & (\log|z_{\tau_1}|, \ldots, \log|z_{s_r}|, 2\log|z_{\sigma_1}|, \ldots 2\log|z_{\sigma_s}|) \end{array}$$

Ferner seien $\mu(K) = \{\alpha \in K \mid \exists\, n : \alpha^n = 1\}$ und $\Gamma = \lambda(\mathcal{O}_K^*)$.

Satz V.1: *Die Sequenz*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \longrightarrow \{0\}$$

ist exakt.

Beweis: Es ist zu zeigen, dass $\mu(K) = \ker\lambda$. Ist $\alpha \in \mu(K)$, so ist $\alpha^n = 1$, also auch $\tau(\alpha)^n = 1$ für $\tau \in \mathrm{Hom}(K, \mathbb{C})$. Folglich ist $\lambda(\alpha) = (\varepsilon_\tau \log|\tau\alpha|)_\tau = (\varepsilon_\tau \log 1)_\tau = 0$.

Andererseits ist $\ker\lambda$ enthalten in der kompakten Menge $\{(x_\tau) \in K_{\mathbb{R}} \mid |x_\tau| = 1\}$ und dem Gitter $j\mathcal{O}_K$. Also ist $\ker\lambda$ endlich. Damit hat jedes Element der endlichen Gruppe $\ker\lambda$ endliche Ordnung, ist also eine Einheitswurzel. $\square$

Lemma V.2: *Zu gegebener Norm $a \in \mathbb{Z}$ gibt es bis aus assoziierte nur endlich viele $\alpha \in \mathcal{O}_K$ mit $N_{K|\mathbb{Q}}(\alpha) = \alpha$.*

Beweis: Wegen $|N_{K|\mathbb{Q}}(\alpha)| = N((\alpha))$ ist dies äquivalent dazu, dass es nur endlich viele Hauptideale mit vorgegebener Norm gibt. Dies haben wir bereits gesehen. □

Satz V.3: $\Gamma = \lambda(\mathcal{O}_K^\times)$ *ist ein Gitter in* $\mathbb{R}^{r+s}$.

Beweis: Wir zeigen, dass Γ eine diskrete Untergruppe des $\mathbb{R}^{r+s}$ ist. Dazu genügt es zu zeigen, dass die beschränkte Menge

$$B_C = \{x \in \mathbb{R}^{r+s} \mid |x_i| < \exp(C), 1 \le i \le r; |x_{r+j}| < \exp(2C), 1 \le j \le s\}$$

für jedes C nur endlich viele Punkte von Γ enthält.

Es ist nun aber $\exp^{-1}(B_C) = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < C\}$ beschränkt, also der Durchschnitt $j\mathcal{O}_K^\times \cap \exp^{-1}(B_C) \subseteq \exp^{-1}(B_C) \cap j\mathcal{O}_K$ endlich. Und ebenso sein Bild $B_C \cap \Gamma$. □

Lemma V.4: *Es ist* $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\alpha) = \pm 1\}$.

Beweis: Sind $\alpha, \beta \in \mathcal{O}_K$ mit $\alpha\beta = 1$, so ist $1 = N(1) = N(\alpha\beta) \le N(\alpha)N(\beta)$, also $N(\alpha) \in \{\pm 1\}$.

Sei nun umgekehrt $N(\alpha) = \pm 1$. Betrachte K als Teilmenge von $\mathbb{C}$ vermöge einer Einbettung. Dann haben wir

$$1 = N(\alpha) = \prod_\tau \tau\alpha = \alpha \prod_{\tau \neq \mathrm{id}} \tau\alpha = \alpha \pm \beta,$$

also ist $\beta = 1/\alpha \in K$ und weiter β als Produkt ganzer Elemente ganz, also $\beta \in \mathcal{O}_K$. □

Das Bild der Norm 1 Fläche $N = \{(z_\tau)_\tau \in K_\mathbb{R} \mid \prod_\tau z_\tau = 1\}$ unter exp ist wegen

$$\begin{aligned}\log|\prod_\tau z_\tau| &= \sum_{i=1}^r \log|z_{\rho_i}| + \sum_{j=1}^s |z_{\sigma_j}| + \sum_{j=1}^s \log|z_{\bar{\sigma}_j}| \\ &= \sum_{i=1}^r \log|z_{\rho_i}| + 2\sum_{j=1}^s |z_{\sigma_j}|\end{aligned}$$

die Spur 0 Hyperebene $S = \{x \in \mathbb{R}^{r+s} \mid \sum_i x_i = 0\}$.

Satz V.5: *Das Gitter* Γ *ist voll in* S*. Insbesondere ist* $\Gamma \cong \mathbb{Z}^{r+s-1}$*.*

Beweis: Wir zeigen, dass Γ voll ist, indem wir eine beschränkte Menge $M \subseteq S$ mit $\bigcup_{\gamma \in M} M + \gamma = S$ angeben. Genauso gut können wir ihr Urbild $T = \exp^{-1}(M)$ angeben und zeigen, dass $\bigcup_{\varepsilon \in \mathcal{O}_K^\times} T\varepsilon = N$ gilt. Wir bemerken dazu, dass wenn T kompakt ist, auch $M = \exp(T)$ kompakt, insbesondere beschränkt ist.

Zu $c_\tau \in [0, \infty)$ mit $c_\tau = c_{\bar{\tau}}$, wobei $\tau \in \mathrm{Hom}(K, \mathbb{C})$, und $c = \prod_\tau c_\tau$ setze $Z = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| \leq c_\tau\}$. Seien weiter $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K - \{0\}$ derart, dass jedes $\alpha \in \mathcal{O}_K - \{0\}$ mit $|N_{K|\mathbb{Q}}(\alpha)| \leq c$ zu einander assoziiert sind. Setze nun $T = \bigcup_{i=1}^k z_j \alpha_i^{-1} \cap N$. Die Menge T ist kompakt, da Z kompakt und N abgeschlossen ist, und damit sind auch die $Z_j \alpha_i^{-1} \cap N$ kompakt.

Nun ist $N = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} Tj\varepsilon$. Das sieht man so ein: Sei C so groß, dass $\mathrm{vol}(Z) > 2^n \mathrm{vol}(j\mathcal{O}_K)$. Sei $(y_\tau) \in N$. Da $N(y) := \prod_\tau y_\tau = 1$, ist $\mathrm{vol}(Z) = \mathrm{vol}(Zy^{-1})$. Wir finden mit dem Satz von Minkowski ein $j\alpha \in \mathcal{O}_K \cap Zy^{-1}$, d. h. es gibt $z \in \mathbb{Z}$ mit $j\alpha = zy^{-1}$. Weiter ist $|N_{K|\mathbb{Q}}(\alpha)| = |N(j\alpha)| \leq CN(y^{-1}) = C$. Also finden wir ein $\varepsilon \in \mathcal{O}_K^\times$ mit $\alpha_i = \varepsilon\alpha$. Insgesamt ist $y = zj\alpha^{-1} = zj\alpha_i^{-1} j\varepsilon \in Zj\alpha_i^{-1} j\varepsilon \in Tj\varepsilon$. □

Satz V.6 (Dirichletscher Einheitensatz): *Sei* K *ein algebraischer Zahlkörper mit* r *reellen und* $2s$ *komplexen Einbettungen. Dann ist* $\mathcal{O}_K^\times \cong \mu(k) \times \mathbb{Z}^{r+s-1}$*.*

Beweis: Die exakte Sequenz

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \longrightarrow \Gamma \longrightarrow 0$$

zeigt, dass $\mathcal{O}_K^\times$ eine endlich erzeugte abelsche Gruppe ist. Nun ist $\mu(K)$ genau der Torsionsanteil und $\mathcal{O}_K^\times / \mu(K) \cong \Gamma \cong \mathbb{Z}^{r+s-1}$ der freie Anteil. □

Der Satz besagt, dass es sogenannte „Grundeinheiten“ $\varepsilon_1, \ldots, \varepsilon_t \in \mathcal{O}_K^\times$ gibt, sodass jedes $\varepsilon \in \mathcal{O}_K^\times$ eine eindeutige Darstellung $\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_{r+s-1}^{\nu_{r+s-1}}$ besitzt, wobei $\nu_i \in \mathbb{Z}$ und $\zeta \in \mu(K)$.

Satz V.7: *Der Regulator* R_K *des Körpers* K *ist definiert als die Determinante eines beliebigen Minors vom Rang* $t = r+s-1$ *von* $(\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)) \in \mathbb{R}^{(t+1)\times t}$*. Es gilt* $\mathrm{vol}(j\mathcal{O}_K^\times) = \sqrt{r+s} R$*.*

Beweis: Der Vektor $\lambda_0 := (r+s)^{-2}(1, \ldots, 1)^t \in \mathbb{R}^{r+s}$ steht orthogonal auf der Spur 0 Hyperebene und hat Länge 1. Folglich ist das $t+1$-dimensionale Volumen des von $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ aufgespannten Spats gleich dem t-dimensionalen Volumen des von $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ aufgespannten Spats, d. h. gleich $\mathrm{vol}(j\mathcal{O}_K^\times)$. Also ist $\mathrm{vol}(j\mathcal{O}_K^\times) = |\det(\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t))|$. Die Summe der Zeilen ist nun $((r+s)^{-2}, 0, \ldots, 0)$. Addieren wir also alle Zeilen zu einer festen Zeile, so können wir nach dieser entwicklen und erhalten den Satz. □

Beispiel V.8: Sei K ein kubischer Zahlkörper mit $d_K < 0$. Dann ist $r = s = 1$. Vermöge der reellen Einbettung sehen wir K als Teilmenge von $\mathbb{R}$ und damit ist $\mu(K) = \{\pm 1\}$. Es ist also $\mathcal{O}_K^\times = \{\pm\varepsilon^n\}$ für eine Grundeinheit $\varepsilon \in K$. Mit ε sind auch $-\varepsilon$, ε^{-1} und $-\varepsilon^{-1}$ Grundeinheiten, wir können also $\varepsilon > 1$ annehmen.

Wir behaupten jetzt, dass $|d_K| < 4\varepsilon^3 + 24$. Das sieht man so: Weil ε keine rationale Zahl ist, muss bereits – wegen $[K : \mathbb{Q}] = 3$ – gelten, dass $\mathbb{Q}(\varepsilon) = K$. Die weiteren Konjugierten $\varepsilon_1, \varepsilon_2 \in \mathbb{C}$ von ε sind damit komplex konjugiert, d. h. $\varepsilon_1 = \bar{\varepsilon}_2$. Somit ist das Produkt $\varepsilon\varepsilon_1\varepsilon_2 = 1$ (und nicht -1). Setze $\varepsilon = u^2$ für $1 < u \in \mathbb{R}$. Dann ist $\varepsilon_1 = u^{-1}\exp(\mathrm{i}\theta)$ und $\varepsilon_2 = u^{-1}\exp(\mathrm{i}\theta)$, wobei $\theta \in [0, \pi]$. Es gilt

$$\begin{aligned}
d'^{1/2} &= d(1, \varepsilon, \varepsilon^2)^{1/2} \\
&= (u^2 - u^{-1}\exp(\mathrm{i}\theta))(u^2 - u^{-1}\exp(-\mathrm{i}\theta))(u^{-1}\exp(\mathrm{i}\theta - u^{-1}\exp(-\mathrm{i}\theta)) \\
&= |u^2 - u^{-1}\exp(\mathrm{i}\theta)|^2 a\mathrm{i}u^{-1}\sin\theta \\
&= |u^2 - u^{-1}\cos(\theta) - u^{-1}\mathrm{i}\sin\theta|^2 2\mathrm{i}u^{-1}\sin\theta \\
&= |u^4 - u\cos\theta + u^{-2}(\cos^2\theta + \sin^2\theta)|2\mathrm{i}u^{-1}\sin\theta \\
&= |u^3 + u^{-3} - 2\cos\theta|2\mathrm{i}\sin\theta.
\end{aligned}$$

Mit der Bezeichnung $2\xi := u^3 - u^{-3}$ sehen wir, dass $|d'|^{1/2} = 4(\xi - \cos\theta)\sin\theta$. Für festes u hat $|d'|^{1/2}$ sein Maximum bei

$$0 = \xi\cos\theta - \cos^2\theta + \sin^2\theta = \xi\cos\theta - 2\cos^2\theta + 1 = \xi x - 2x^2 + 1 =: -g(x),$$

mit $x = \cos\theta \in [-1, 1]$. Es ist nun $g(1) = 1 - \xi = 1 - \frac{1}{2}(u^3 + u^{-3}) < 0$ und weiter ist $g(-1/(2u^3)) = \frac{3}{4}(u^{-6} - 1) < 0$. Da g ein Polynom zweiten Grades ist, hat g eine Nullstelle größer als 1 und eine Nullstelle x_0 mit $-1 < x_0 < -(2u^3)^{-1}$, da $g(-1) = 1 + \xi > 0$. Diese Nullstelle x_0 liefert das Maximum von $|d'|^{1/2}$ mit festem u. Für später halten wir fest:

$$x_0^2 > \frac{1}{4u^6} \implies 0 > \frac{1}{u^6} - 4x_0^2 > \frac{1}{u^6} - 4x_0^2 - 4x_0^4. \tag{V.1}$$

Wir können damit abschätzen

$$\begin{aligned}
|d_k| \le |d'| &= 16(\xi^2 - 2\xi\cos\theta + \cos^2\theta)(1 - \cos^2\theta) \\
&\le 16(\xi^2 - 2x_0\xi + x_0^2)(1 - x_0^2) \\
&= 16(\xi^2 - 2(2x_0^2 - 1) + x_0^2)(1 - x_0^2) \\
&= 16(\xi^2 - 3x_0^2 + 2)(1 - x_0^2) \\
&= 16(\xi^2 - x_0^2 + 1 - x_0^4) \\
&= 4u^6 + 8 + 4u^{-6} - 16x_0^2 - 16x_0^4 + 16 \\
&= 4u^6 + 24 + 4(u^{-6} - 4x_0^2 - 4x_0^4) < 4u^6 + 24 = 4\varepsilon^3 + 24.
\end{aligned}$$

Für den Zahlkörper $K = \mathbb{Q}[\alpha]$ mit $\alpha \in \mathbb{R}$ und $\alpha^3 + 10\alpha + 1 = 0$ können wir das gezeigte jetzt anwenden: Die Diskrimimante d_K haben wir bereits zu $d_K = -4027$ bestimmt, sodass die Grundeinheit die Ungleichung

$$\varepsilon > \sqrt[3]{\frac{4027 - 24}{4}} > 10$$

erfüllt. Da $N(\alpha) = -1$ ist $\alpha \in \mathcal{O}_K^\times$. Weiter ist $\alpha = -0{,}099\,900\,3\ldots$ und so ist $\beta = -\alpha^{-1} = 10{,}009\,98\ldots$. Da β außerdem eine Potenz von ε ist, muss $\beta = \varepsilon$ gelten.

Bemerkung V.9: Der Regulator spielt die selbe Rolle für $\mathcal{O}_K^\times$ wie die Diskriminante für $\mathcal{O}_K$. Für jede Menge $\{\varepsilon_1, \ldots, \varepsilon_t\} \subseteq \mathcal{O}_K^\times$ unabhängiger Einheiten lässt sich der Regulator $R(\varepsilon_1, \ldots, \varepsilon_t)$ definieren. Sei U die von ε_i und $\mu(K)$ erzeugte Untergruppe. Der Index dieser Untergruppe ist

$$[\mathcal{O}_K^\times : U] = \frac{\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_t)}{R_K}.$$

Ähnlich wie im Beispiel gibt es allgemein untere Schranken für den Regulator.

Kapitel VI.

Lokalisierung

Erinnerung VI.1: Seien A ein Integritätsbereich, $S \subseteq A - \{0\}$ eine multiplikativ abgeschlossene Menge und $K = \mathrm{Quot}(A)$. Dann gelten:

(i) $S^{-1}A = \{a/s \in K \mid a \in A, s \in S\}$ ist die Lokalisierung von A an S.

(ii) $A_{\mathfrak{p}} = S^{-1}A$ für $S = A - \mathfrak{p}$, wobei $\mathfrak{p} \subseteq A$ ein Primideal ist.

(iii) Es gibt die Bijektion

$$\begin{aligned} \{\mathfrak{q} \subseteq S^{-1}A \text{ prim}\} &\longleftrightarrow \{\mathfrak{p} \subseteq A \text{ prim}, \mathfrak{p} \cap S \neq \varnothing\} \\ \mathfrak{q} &\longmapsto \mathfrak{q} \cap A \\ \mathfrak{p}S^{-1}A &\longmapsfrom \mathfrak{p}. \end{aligned}$$

Satz VI.2: *Ist A ein Dedekindring, so ist es auch $S^{-1}A$.*

Beweis: Jedes Ideal von $S^{-1}A$ ist von der Form $\mathfrak{a}S^{-1}A$ für ein Ideal $\mathfrak{a} \subseteq A$. Mit $\mathfrak{a}$ ist auch $\mathfrak{a}S^{-1}A$ endlich erzeugt. Folglich ist $S^{-1}A$ Noethersch.

Sind $0 \neq \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq S^{-1}A$ Primideale, so auch $0 \neq \mathfrak{q}_1 \cap A \subseteq \mathfrak{q}_2 \cap A \subseteq A$. Da $\mathfrak{q}_1 \cap A$ maximal ist, folgt $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$ und damit $\mathfrak{q}_1 = \mathfrak{q}_2$ nach der vorangegangenen Erinnerung. Folglich ist jedes Primideal $0 \neq \mathfrak{q}_1 \subseteq S^{-1}A$ maximal.

Ist schließlich $x \in K$ ganz über A, d. h.

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0}$$

mit $a_0, \ldots, a_{n-1} \in A$ und $s_0, \ldots, s_{n-1} \in S$, so liefert Multiplikation mit s^n, wobei $s = s_0 \cdots s_{n-1}$, dass sx ganz über A ist. Da A ganzabgeschlossen ist, ist nun $sx \in A$, d. h. $x \in S^{-1}A$. □

Definition VI.3: Ein Hauptidealbereich mit genau einem Primideal $0 \neq \mathfrak{p}$ heißt *diskreter Bewertungsring.*

Satz VI.4: *Sei A ein Noetherscher Integritätsbereich. Es ist A ein Dedekindring genau dann, wenn alle Lokalisierungen $A_\mathfrak{p}$ an Primidealen $0 \neq \mathfrak{p} \subseteq A$ diskrete Bewertungsringe sind.*

Beweis: „⇒“: Sei A ein Dedekindring. Dann ist es auch $A_\mathfrak{p}$. Das maximale Ideal $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$ ist das einzige nicht-triviale Primideal. Ist nun $\pi \in \mathfrak{m} - \mathfrak{m}^2$, so ist aufgrund der eindeutigen Faktorisierung von Idealen in $A_\mathfrak{p}$ das Hauptideal (π) eine Potenz des maximalen Ideals, sagen wir $(\pi) = \mathfrak{m}^n$. Jetzt muss aber $n = 1$ gelten. Die anderen von Null verschiedenen Ideale sind genau die Hauptideale $(\pi^k) = \mathfrak{m}^k$. Also ist $A_\mathfrak{p}$ ein Hauptidealring und somit auch ein diskreter Bewertungsring.

„⇐“: Wir behaupten $A = \bigcap\{A_\mathfrak{p} \mid \mathfrak{p} \subseteq A \text{ prim}\} \subseteq K$. Sei dazu $a/b \in \bigcap_\mathfrak{p} A_\mathfrak{p}$ und $\mathfrak{a} = \{x \in A \mid xa \in bA\} \subseteq A$. Ist nun $\mathfrak{p} \subseteq A$ ein Primideal, so gibt es ein $c \in A$ und ein $s \notin \mathfrak{p}$ mit $a/b = c/s \in A_p$. Also ist $as = cb$, d. h. $s \in \mathfrak{a}$ und $s \notin \mathfrak{p}$. Folglich ist $\mathfrak{a} \not\subset \mathfrak{p}$. Nur das Ideal (1) ist in keinem maximalen Ideal enthalten. Folglich ist $\mathfrak{a} = (1)$ und weiter $1 \in \mathfrak{a}$, d. h. $1a \in bA$, also $a/b \in A$. Dies zeigt die Behauptung.

Ist nun $x \in K$ ganz über A, so ist es auch ganz über $A_\mathfrak{p}$ für alle $\mathfrak{p}$ und damit $x \in \bigcap_\mathfrak{p} A_\mathfrak{p} = A$.

Sind $0 \neq \mathfrak{p} \subseteq \mathfrak{q} \subseteq A$ prim, so ist $\mathfrak{p}A_\mathfrak{q} \subseteq \mathfrak{q}A_\mathfrak{q}$. Da $\mathfrak{p}A_\mathfrak{q}$ maximal ist, folgt $\mathfrak{p}A_\mathfrak{q} = \mathfrak{q}A_\mathfrak{q}$ und damit $\mathfrak{p} = \mathfrak{q}$.

Schließlich ist A nach Voraussetzung Noethersch, womit wir insgesamt erhalten, dass A ein Dedekindring ist. □

Definition VI.5: Eine *diskrete Exponentialbewetung* oder kurz *disrekte Bewertung* ist eine Funktion $\nu\colon K \to \mathbb{Z} \cup \{\infty\}$, die für alle $a, b \in K$ erfüllt, dass

(i) $\nu(ab) = \nu(a) + \nu(b)$,

(ii) $\nu(a) = \infty$ genau dann, wenn $a = 0$,

(iii) $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$.

Sie heißt *normiert*, falls ν surjektiv ist.

Beispiel VI.6: (i) Seien A ein Hauptidealbereich, K der Quotientenkörper von A und $\pi \in A$ ein Primelement. Jedes $c \in K$ ist von der Form $\pi^m \frac{a}{b}$ mit $\pi \nmid ab$ und $m \in \mathbb{Z}$. Setze $\nu(c) = m$.

(ii) Seien A ein Dedekindring, $\mathfrak{p} \subseteq A$ ein Primideal. Für $c \in K^\times$ sei $\mathfrak{p}^{\nu(c)}$ die Potenz von $\mathfrak{p}$ in der Primidealzerlegung von (c).

(iii) Die Pol- beziehungsweise Nullstellenordnung in einem Punkt einer meromorphen Funktion auf einem Gebiet $U \subseteq \mathbb{C}$.

(iv) Primdivisoren auf normalen Varietäten entsprechen diskreten Bewertungen auf dem rationalen Funktionenkörper.

Satz VI.7: *Sei ν eine diskrete Bewertung von K. Dann ist*

$$A := \{a \in K \mid \nu(a) \geq 0\}$$

ein direkter Bewertungsring mit maximalem Ideal $\mathfrak{m} = \{a \in K \mid \nu(a) > 0\}$.

Kapitel VII.

Faktorisierungen

Im Folgenden seien stets A ein Dedekindring, $K = Q(A)$ sein Quotientenkörper, $L|K$ eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L.

Satz VII.1: *B ist ein Dedekindring.*

Beweis: Da $L|K$ separabel ist, ist B ein endlich erzeugter A-Modul. Ist $d = d(\alpha_1, \ldots, \alpha_n)$, dann ist B enthalten in der Summe $(\alpha_1/d)A + \cdots + (\alpha_n/d)A$. Damit ist jedes Ideal von B als Untermodul eines Noetherschen A-Moduls ein endlich erzeugter A-Modul, deshalb insbesondere ein endlich erzeugter B-Modul. Der Rest folgt wie für $K = \mathbb{Q}$. □

Bemerkung VII.2: Ist A ein Dedekindring und $L|K$ nur eine endliche Körpererweiterung, dann ist $\bar{A}^L$ weiterhin ein Dedekindring.

Definition VII.3: Sei $0 \neq \mathfrak{q} \subseteq A$ prim. Dann ist $\mathfrak{q}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, wobei die $e_i \geq 0$ und die $\mathfrak{p}_i$ Primideale sind. Ist eines der $e_i > 1$, so heißt $\mathfrak{q}$ *verzweigt in* B. Die Zahl e_i ist der Verzweigungsindex von $\mathfrak{p}_i$ über $\mathfrak{q}$. Der Körpergrad

$$[B/\mathfrak{p}_i : A/\mathfrak{q}] =: f_i$$

heißt *Trägheitsgrad von* $\mathfrak{p}_i$. Das Ideal $\mathfrak{q}$ heißt *träge in* L, falls $\mathfrak{q}B$ prim ist und voll zerlegt, d. h. falls $e_i = f_i = 1$ für alle i gilt. Wir schreiben für $\mathfrak{p} \mid \mathfrak{q}B$ auch $\mathfrak{p} \mid \mathfrak{q}$.

Beispiel VII.4: Seien $A = \mathbb{Z}$ und $B = \mathbb{Z}[\mathrm{i}]$. Das Primideal $2 = (1 + \mathrm{i})^2$ ist verzweigt mit Index 2. Das Primideal (3) ist träge in $\mathbb{Q}[\mathrm{i}]$ und $\mathbb{Z}[\mathrm{i}]/(3) \cong \mathbb{F}_9$. Das Primideal $(5) = (2 + \mathrm{i})(2 - \mathrm{i})$ ist voll erzeugt.

Satz VII.5: *Seien nun $B = A[\alpha]$ und $\mu = \mu_\alpha \in A[X]$ das Minimalpolynom von α. Ferner seien $\mathfrak{q} \subseteq A$ prim und $\mu_1, \ldots, \mu_g \in A[X]$ normiert und derart gewählt, dass $\mu \equiv \prod_{i=1}^g \mu_i^{e_i} \pmod{\mathfrak{p}}$ die Primfaktorzerlegung in $(A/\mathfrak{q})[X]$ ist. Dann ist $\mathfrak{q}B = \prod_{i=1}^g (\mathfrak{q}, \mu_i(\alpha))^{e_i}$ die Primfaktorzerlegung von $\mathfrak{q}B$. Weiter gilt*

$$B/(\mathfrak{q}, \mu_i(\alpha)) \cong (A/\mathfrak{q})[X]/(\bar{\mu}_i),$$

und so ist $\operatorname{grad} f_i = \deg \mu_i$.

Beweis: Aus der Voraussetzung $B = A[\alpha]$ erhalten wir den Isomorphismus $A[X]/(\mu) \to B$, $x \mapsto \alpha$. Mit der Bezeichnung $k := A/\mathfrak{q}$ erhalten wir daraus den Isomorphismus

$$k[X]/(\bar{\mu}) \longrightarrow B \otimes_A A/\mathfrak{q} = B/\mathfrak{q}B, \qquad x \mapsto \alpha + \mathfrak{q}B.$$

Im Ring $k[X]/(\bar{\mu}) \cong \prod_{i=1}^g k[X]/(\bar{\mu}_i)$ sind $(\bar{\mu}_1), \ldots, (\bar{\mu}_g)$ genau die maximalen Ideale und die e_i sind minimal mit der Eigenschaft dass $\prod_{i=1}^g \bar{\mu}_i^{e_i} = 0$. Das Ideal $(\bar{\mu}_i)$ entspricht dem Ideal $(\mu_i(\alpha) + \mathfrak{q}B)$ in $B/\mathfrak{q}B$ und dieses gibt als Urbild das Primideal $\mathfrak{p}_i := (\mu_i(\alpha), \mathfrak{q})$ in B. Also sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ alle Primideale in B, die $\mathfrak{q}$ enthalten, und damit genau die Primteiler von $\mathfrak{q}$. Die Exponenten e_i' in $\mathfrak{q}B = \prod_{i=1}^g \mathfrak{p}_i^{e_i'}$ sind dadurch charakterisiert, dass sie minimal mit $\mathfrak{q}B \supseteq \prod_{i=1}^g \mathfrak{p}_i^{e_i'}$ sind. Es folgt $e_i' = e_i$. □

Beispiel VII.6: Sei $L = \mathbb{Q}[\alpha]$ und α eine Nullstelle von $\mu = X^3 + 10X + 1$. Die Diskriminante $\operatorname{Disk}(\mu) = -4027$ ist prim, sodass $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

$\mathfrak{q}$	$\mu \pmod{q}$	(q)
2	$(1+X)(1+X+X^2)$	$(2, 1+\alpha)(2, 1+\alpha+\alpha^2)$
3	$(2+X)(2+X+X^2)$	$(3, 2+\alpha)(3, 2+\alpha+\alpha^2)$
5	$(1+X)(1+4X+X^2)$	$(5, 1+\alpha)(5, 1+4\alpha+\alpha^2)$
17	$(1+10X+X^3)$	(17)
4027	$(2215+X)^2(3624+X)$	$(4027, 2215+\alpha)^2(3624+\alpha)$

Für $\mu = X^2 - 8X + 15$ gilt $\operatorname{Disk}(\mu) = -4027$. Aber

$$(17) = (17, 4+\beta)(1716+\beta)(17, 7+\beta)$$

ist zerlegt. Damit ist $\mathbb{Q}(\alpha) \ncong \mathbb{Q}(\beta)$. Ist $\operatorname{Sp}(K)$ die Menge der spaltenden Primzahlen und sind $K|\mathbb{Q}$, $K'|\mathbb{Q}$ Galoissch, dann kann man zeigen, dass $K \cong K'$ genau dann gilt, wenn $\operatorname{Sp}(K) = \operatorname{Sp}(K')$.

Bemerkung VII.7: Unter der Voraussetzung $B = A[\alpha]$ finden wir

(i) $[L:K] = \deg \mu_\alpha = \deg \prod_{i=1}^g \mu_i^{e_i} = \sum_{i=1}^g e_i \deg \mu_i = \sum_{i=1}^g e_i f_i$.

(ii) Das Primideal $\mathfrak{q}$ ist genau dann verzweigt, wenn $\bar{\mu}$ eine doppelte Nullstelle hat. Die Restklasse $\bar{\mu}$ hat genau dann eine doppelte Nullstelle, wenn $\mathrm{Disk}(\bar{\mu}) = 0 \in A/\mathfrak{q}$ ist, was genau dann gilt, wenn $\mathfrak{q} \mid \mathrm{Disk}(\mu)$.

Diese Erkenntnisse wollen wir jetzt für $B = \bar{A}^L$ verallgemeinern.

Lemma VII.8: *Für $0 \neq \mathfrak{q} \subseteq A$ und ein Primideal $\mathfrak{p} \subseteq B$ gilt $\mathfrak{p} \mid \mathfrak{q}$ genau dann, wenn $\mathfrak{q} = \mathfrak{p} \cap K$.*

Beweis: „⇒“: Es gilt $\mathfrak{p} \mid \mathfrak{q}$ genau dann, wenn $\mathfrak{q}B \subseteq \mathfrak{p}$, d. h. $\mathfrak{q} \subseteq \mathfrak{p} \cap K = \mathfrak{p} \cap A$. Weil $\mathfrak{q}$ nicht-trivial und maximal ist, also $\mathfrak{q} = \mathfrak{p} \cap K$.

„⇐“: Gilt $\mathfrak{q} = \mathfrak{p} \cap K$, dann ist auch $\mathfrak{q} \subseteq \mathfrak{p}$, d. h. $\mathfrak{q}B \subseteq \mathfrak{p}$, was per Definition gerade $\mathfrak{p} \mid \mathfrak{q}$ heißt. □

Satz VII.9: *Seien weiterhin $L|K$ separabel, $n = [L:K]$ und $\mathfrak{p}_1, \ldots, \mathfrak{p}_g \subseteq B$ die Primteiler von $\mathfrak{q} \subseteq A$. Dann gilt:*

(i) $n = \sum_{i=1}^g e_i f_i$, *(Fundamentale Gleichung)*

(ii) *Ist $L|K$ Galoissch, so sind jeweils alle Trägheitsgrade f_i und alle Verzweigungsindizes e_i gleich. Es gilt somit $n = efg$.*

Beweis: (i) Wir zeigen, dass beide Seiten der Gleichung der Dimension von $B/\mathfrak{q}B$ als $A/\mathfrak{q}$-Vektorraum entsprechen. Nach dem Chinesischen Restsatz gilt für die rechte Seite

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

d. h. es genügt $[B/\mathfrak{p}^{e_i} : A/\mathfrak{q}] = e_i f_i$ zu zeigen. Wie zuvor ist

$$B \supseteq \mathfrak{p}_i \supseteq \mathfrak{p}_i^2 \supseteq \cdots \supseteq \mathfrak{p}_i^{e_i}$$

eine Kette von $B/\mathfrak{p}_i$-Vektorräumen mit Quotienten $\mathfrak{p}_i^k/\mathfrak{p}_i^{k+1} \cong B/\mathfrak{p}_i$ von Dimension $f_i = [B/\mathfrak{p} : A/\mathfrak{q}]$, sodass die Dimension von $B/\mathfrak{p}_i$ genau $e_i f_i$ ist.

Für die linke Seite nehmen wir zunächst an, A wäre ein Hauptidealring. Dann wäre $B \cong A^m$ ein freier A-Modul und $L = B \otimes_A K \cong K^m$, d. h. es wäre $m = [L:K] = n$. Mit

$$B/\mathfrak{q}B \cong B \otimes_A A/\mathfrak{q} \cong A^n \otimes_A A/\mathfrak{q} \cong (A/\mathfrak{q})^n$$

erhielten wir $[B/\mathfrak{q}B : A/\mathfrak{q}] = n$.

Ist A kein Hauptidealring, dann können wir mit $S = A - \mathfrak{q}$, $A' = S^{-1}A$ und $B' = S^{-1}B$ fortfahren. Es gilt $\mathfrak{q}B' = \prod_{i=1}^g (\mathfrak{p}_i B')^{e_i}$, $A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}$ sowie $B'/\mathfrak{p}_i B' \cong B/\mathfrak{p}_i$ und diesmal ist $A' = A_\mathfrak{q}$ ein Hauptidealring.

(ii) Sei $L|K$ Galoissch. Jedes $\sigma \in \mathrm{Gal}(L|K)$ induziert einen Automorphismus von $B = \bar{A}^L$. Insbesondere ist mit $\mathfrak{p}$ auch $\sigma\mathfrak{p}$ prim. Aus „$\mathfrak{p}|\mathfrak{q}$ genau dann, wenn $\mathfrak{q} = \mathfrak{p} \cap K$“ folgt, dass mit $\mathfrak{p}|\mathfrak{q}$ auch $\sigma\mathfrak{p} \mid \mathfrak{q}$ gilt. Weiter ist $e(\mathfrak{p} \mid \mathfrak{q}) = e(\sigma\mathfrak{p}|\mathfrak{q})$ und $f(\mathfrak{p}|\mathfrak{q}) = f(\sigma\mathfrak{p}|\mathfrak{q})$. Es genügt also zu zeigen, dass σ transitiv auf den Primfaktoren von $\mathfrak{q}B$ operiert. Seien dazu $\mathfrak{P}$ und $\mathfrak{Q}$ Primteiler von $\mathfrak{q}B$.

Wären $\mathfrak{P}$ und $\mathfrak{Q}$ nicht konjugiert, dann gäbes es nach dem Chinesischen Restsatz ein $\beta \in \mathfrak{Q} - \bigcup_\sigma \sigma\mathfrak{P}$ (z. B. mit $\beta \equiv 0 \pmod{\mathfrak{Q}}$ und $\beta \equiv 1 \pmod{\mathfrak{P}}$). Nun ist aber einerseits

$$b = N_{L|K}(\beta) = \prod_\sigma \sigma\beta \in A \cap \mathfrak{Q} = \mathfrak{q}$$

und andererseits ist für jedes $\sigma \in \mathrm{Gal}(L|K)$ schon $\beta \notin \sigma^{-1}\mathfrak{P}$ und so $\sigma\beta \notin \mathfrak{P}$. Das Produkt $\prod_\sigma \sigma\beta = b$, dessen sämtliche Faktoren nicht in $\mathfrak{P}$ liegen, wäre in $\mathfrak{q} \subseteq \mathfrak{P}$ enthalten, was einem Primideal nicht passieren kann. □

Definition VII.10: Sei B eine A-Algebra, die als A-Modul isomorph ist zu A^n. Dann können wir wie gehabt Spur und Norm eines Elements von B als Spur und Determinante der Linksmultiplikation definieren. Die Diskriminante ist

$$d(B/A) = d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{B|A}(\alpha_i\alpha_j))_{i,j} \in A/(A^\times)^2$$

wobei $\alpha_1, \ldots, \alpha_n$ eine Basis des A-Moduls B ist.

Beispiel VII.11: Ist A der Ring der ganzen Zahlen $\mathbb{Z}$ und $B = \mathcal{O}_L \cong \mathbb{Z}^n$, dann ist $d(\mathcal{O}_K/\mathbb{Z}) = d_{K_0} \in \mathbb{Z}/(\mathbb{Z}^\times)^2 \cong \mathbb{Z}$.

Satz VII.12: *Sei K ein Zahlkörper, $L|K$ eine endliche Körpererweiterung, $A \subseteq K$ ein Dedekindring und $B = \bar{A}^L$. Ist B ein freier A-Modul und $\mathfrak{q} \subseteq A$ prim, so gilt: Das Primideal $\mathfrak{q}$ ist verzweigt in L genau dann, wenn $\mathfrak{q} \mid d(B/A)$. Insbesondere gibt es nur endlich viele verzweigte Primideale.*

Lemma VII.13: *Seien A ein Ring und $B_1, \ldots, B_g$ Ringerweiterungen von A, die freie A-Moduln sind. Dann ist*

$$d\Big(\prod_{i=1}^g B_i/A\Big) = \prod_{i=1}^g d(B_i/A).$$

Beweis: Die Mengen $E_1, \ldots, E_n$ seien A-Basen der B_i. Dann berechnen wir $d(\prod_{i=1}^g B_i/A)$ vermöge der Basis $\bigcup_{i=1}^d E_i$ von $\prod_{i=1}^d B_i$. □

Erinnerung: Seien R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann heißt

$$\mathrm{rad}(\mathfrak{a}) = \{x \in R \mid \exists\, n \in \mathbb{N} : x^n \in \mathfrak{a}\}$$

das *Radikal von* $\mathfrak{a}$. Man kann zeigen, dass gilt:

$$\bigcap\{\mathfrak{p} \mid \mathfrak{p} \subseteq R \text{ prim}\} = \mathrm{rad}(0) \iff R \text{ ist reduziert}$$
$$\iff 0 \text{ ist das einzige nilpotente Element von } R.$$

Lemma VII.14: *Sei k ein perfekter Körper und B eine endlichdimensionale kommutative k-Algebra. Dann ist B reduziert genau dann, wenn $d(B/k) \neq 0$.*

Beweis: Ist $0 \neq \beta \in B$ nilpotent, so können wir β zu einer Basis $(\beta = e_1, \ldots, e_n)$ von B fortsetzen. Es ist nun für jedes i auch βe_i nilpotent und so auch die lineare Abbildung $B \to B$, $x \mapsto (\beta e_i) \cdot x$ und ihre Darstellungsmatrix M. Es gilt $\mu_M = x^r$ und so $\mathrm{Tr}_{B|k}(\beta) = \mathrm{Tr}(M) = 0$. Folglich ist die erste Zeile von $\mathrm{Tr}(e_i e_j)_{ij}$ gleich Null, also $d(B|k) = 0$.

Sei umgekehrt B reduziert, d. h. $0 = \mathrm{rad}(0) = \cap(\mathfrak{p} \mid \mathfrak{p} \subseteq R \text{ prim})$. Ist $\mathfrak{p} \subseteq B$ prim, so ist $B/\mathfrak{p}$ ein algebraischer Integritätsbereich über k, also ein Körper, d. h. $\mathfrak{p}$ ist maximal. Sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ Primideale, so sind sie paarweise prim (d. h. für $i \neq j$ ist $\mathfrak{p}_i + \mathfrak{p}_j = R$), da sie maximal sind. Der Chinesische Restsatz liefert

$$B/\bigcap_{i=1}^{r} \mathfrak{p}_i = \prod_{i=1}^{r} B/\mathfrak{p}_i.$$

Es gilt also $\infty > [B : k] \geq [B/\bigcap_{i=1}^{r} \mathfrak{p}_i : k] = \sum_{i=1}^{r} [B/\mathfrak{p}_i : k] \geq r$. Folglich hat B nur endlich viele Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$. Wir haben also

$$B \cong B/(0) \cong B/\bigcap_{i=1}^{g} \mathfrak{p}_i = \prod_{i=1}^{g} B/\mathfrak{p}_i,$$

entsprechend ist $d(B|k) = \prod_{i=1}^{g} d(B/\mathfrak{p}_i|k)$. Da k perfekt ist, ist die Körpererweiterung $B/\mathfrak{p}_i|k$ separabel und so folgt $d(B/\mathfrak{p}_i|k) \neq 0$. Also ist $d(B) = \prod_i d(B/\mathfrak{p}_i|A) \neq 0$. □

Beweis (Satz VIII.12): Sei $0 \neq \mathfrak{q} \subseteq A$ prim und $(e_1, \ldots, e_n)$ eine A-Basis von B. Dann ist $(\bar{e}_1, \ldots, \bar{e}_n)$ eine $A/\mathfrak{q}$-Basis von $B \otimes_A A/\mathfrak{q} \cong B/\mathfrak{q}B$. Aus der Definition der Diskriminante folgt

$$d(B|A) \pmod{\mathfrak{q}} = d(B/\mathfrak{q}B|A/\mathfrak{q}).$$

Aus dem vorherigen Lemma erhalten wir mit $\mathfrak{q}B = \prod_i \mathfrak{p}_i^{e_i}$, dass

$$\begin{aligned} d(B/\mathfrak{q}B|A/\mathfrak{q}) \neq 0 &\iff B/\mathfrak{q}B \text{ ist reduziert} \\ &\iff B/\mathfrak{q}B \cong \prod B/\mathfrak{p}_i^{e_i} \\ &\iff \text{Jedes } B/\mathfrak{p}_i^{e_i} \text{ ist reduziert} \\ &\iff \text{Jedes } e_i \text{ ist 1.} \end{aligned}$$

□

Bemerkung VII.15: Ist $A = \mathcal{O}_K$ und $B = \mathcal{O}_L$ nicht notwendig frei über A, so ist für $S = A - \mathfrak{q}$, $S^{-1}A = A_\mathfrak{q}$ ein Hauptidealbereich, also ist $S^{-1}B$ frei und $d(S^{-1}B|S^{-1}A) = (\mathfrak{q}A_\mathfrak{q})^{m(\mathfrak{q})}$. Setze

$$d(B|A) = \prod_{\mathfrak{q} \subseteq A \text{ prim}} \mathfrak{q}^{m(\mathfrak{q})}.$$

Da fast alle $m(\mathfrak{q}) = 0$ sind, definiert dieses ein Ideal und es gilt $\mathfrak{q} \mid d(B|A)$ genau dann, wenn $\mathfrak{q}$ verzweigt in B ist.

Kapitel VIII.

Hilbertsche Verzweigungstheorie

Im Folgenden sei $L|K$ eine Galoissche Körpererweiterung. Wir hatten bereits gesehen, dass $\mathrm{Gal}(L|K) =: G$ transitiv auf der Menge der Primteiler eines Primideals $\mathfrak{p}_K \subseteq \mathcal{O}_K$ operiert.

Definition VIII.1: Sei $\mathfrak{P} \subseteq \mathcal{O}_L$ prim. Dann heißt $G_\mathfrak{P} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ die *Zerlegungsgruppe von* $\mathfrak{P}$ und $Z_\mathfrak{P} = L^{G_\mathfrak{P}} = \{x \in L \mid \sigma x = x \text{ für alle } \sigma \in G_\mathfrak{P}\}$ der *Zerlegungskörper*. Es gilt für $\mathfrak{P}_K = \mathfrak{P} \cap K$, dass

$$\mathfrak{P}_K\mathcal{O}_L = \prod_{\sigma \in G/G_\mathfrak{P}} \sigma\mathfrak{p}^e.$$

Die Anzahl der Primteiler von $\mathfrak{P}_K$ in L ist also $g = [G : G_\mathfrak{P}]$ und weiter sind $f = [\mathcal{O}_L/\sigma\mathfrak{P} : \mathcal{O}_K/\mathfrak{P}_K]$ und $n = [L : K] = efg$.

Für $\mathfrak{P} \subseteq \mathcal{O}$ schreibe $\kappa(\mathfrak{P}) := \mathcal{O}/\mathfrak{P}$ für den Restkörper.

Satz VIII.2: *Für* $\mathfrak{P}_Z := \mathfrak{P} \cap Z_\mathfrak{P}$ *ist:*

(i) $\mathfrak{P}_Z\mathcal{O}_L = \mathfrak{P}^e$,

(ii) $[\kappa(\mathfrak{P}) : \kappa(\mathfrak{P}_Z)] = f$,

(iii) $e(\mathfrak{P}_Z|\mathfrak{P}_K) = f(\mathfrak{P}_Z|\mathfrak{P}_K) = 1$.

Beweis: Die über $\mathfrak{P}_Z$ liegenden Primideale von $\mathcal{O}_L$ sind von der Form $\sigma\mathfrak{P}$ mit $\sigma \in \mathrm{Gal}(L|Z_\mathfrak{P}) = G_\mathfrak{P}$, also ist $\sigma\mathfrak{P} = \mathfrak{P}$. Es ist $[L : K] = \#(G) = efg$ mit

$$g = [G : G_\mathfrak{P}] = [Z_\mathfrak{P} : K]$$

folgt $[L : Z_\mathfrak{P}] = ef$. Ist $\mathfrak{P}^{e'} = \mathfrak{P}_Z\mathcal{O}_L$ und $\mathfrak{P}_Z^{e''} = \mathfrak{P}_K\mathcal{O}_{Z_\mathfrak{P}}$, so folgt

$$\mathfrak{P}_K\mathcal{O}_L = (\mathfrak{P}_Z\mathcal{O}_L)^{e''} = (\mathfrak{P}^{e'})^{e''} = \mathfrak{P}^{e' \cdot e''},$$

also ist $e = e' \cdot e''$. Für die Trägheitsgrade gilt analog $f = f' \cdot f''$.

Für die Zerlegung von $\mathfrak{P}_Z$ in L gilt $ef = [L : Z_\mathfrak{P}] = e' \cdot f' \cdot g' = e' \cdot f'$. Es folgt $e' = e$, $f' = f$ und $e'' = f'' = 1$. □

Da per Definition $\sigma\mathfrak{P} = \mathfrak{P}$ für $\sigma \in G_\mathfrak{P}$, wirkt $G_\mathfrak{P}$ auf $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$.

Satz VIII.3: *Die Körpererweiterung $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)$ ist normal und der Homomorphismus*

$$G_\mathfrak{P} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K))$$

ist surjektiv.

Beweis: Da der Trägheitsgrad $f(\mathfrak{P}_Z|\mathfrak{P}_K) = 1$ ist nach dem vorherigen Satz, folgt dass $\kappa(\mathfrak{P}_Z) = \kappa(\mathfrak{P}_K)$. Ohne Beschränkung der Allgemeinheit können wir also annehmen, dass $Z_\mathfrak{P} = K$ und $G_\mathfrak{P} = G$.

Sei $\theta \in \mathcal{O}_L$ Repräsentant eines beliebigen $\bar{\theta} \in \mathcal{O}_L/\mathfrak{P} = \kappa(\mathfrak{P})$. Für die Minimalpolynome gilt $\mu_{\bar{\theta}} \mid \bar{\mu}_\theta$. Da $L|K$ als Galoissche Körpererweiterung normal ist, zerfällt μ_θ in $\mathcal{O}_L$ in Linearfaktoren. Damit zerfällt auch $\bar{\mu}_\theta$ in $\kappa(\mathfrak{P})$ und somit auch sein Teiler $\mu_{\bar{\theta}}$. Da $\bar{\theta}$ beliebig war, ist $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)$ normal.

Sei $\bar{\theta}$ jetzt ein primitives Element der separablen Hülle von $\kappa(\mathfrak{P}_K)$ in $\kappa(\mathfrak{P})$. Ist nun

$$\varphi \in \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)) = \mathrm{Gal}(\kappa(\mathfrak{P}_K)(\bar{\theta})|\kappa(\mathfrak{P}_K))$$

so ist $\varphi(\bar{\theta})$ eine Nullstelle von $\mu_{\bar{\theta}}$, also auch von $\bar{\mu}_\theta$. Es gibt also eine Nullstelle $\theta' \in L$ von μ_θ mit $\varphi(\bar{\theta}) = \bar{\theta}'$. Diese ist via einem $\sigma \in \mathrm{Gal}(L|K)$ zu θ konjugiert, also ist $\sigma\theta = \theta' \equiv \varphi\bar{\theta} \pmod{\mathfrak{P}}$. Es ist also $\bar{\sigma} = \varphi$ und der Homomorphismus ist surjektiv. □

Definition VIII.4: Die *Trägheitsgruppe* $I_\mathfrak{P}$ ist der Kern des Homomorphismus $G_\mathfrak{P} \to \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K))$. Der Fixkörper $L^{I_\mathfrak{P}} =: T_\mathfrak{P}$ heißt *Trägheitskörper*.

Satz VIII.5:

(i) *$T_\mathfrak{P}|Z_\mathfrak{P}$ ist normal.*

(ii) $\mathrm{Gal}(T_\mathfrak{P}|Z_\mathfrak{P}) \cong \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K))$.

Ist $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)$ separabel, so ist einerseits $\#(I_\mathfrak{P}) = [L : T_\mathfrak{P}] = e$ und andererseits $[G_\mathfrak{P} : I_\mathfrak{P}] = [T_\mathfrak{P} : Z_\mathfrak{P}] = f$. In diesem Fall ist $e \leq e(\mathfrak{P}|\mathfrak{P}_T)$ und $1 = e(\mathfrak{P}_T|\mathfrak{P}_Z)$ sowie $1 = f(\mathfrak{P}|\mathfrak{P}_T)$ und $f = f(\mathfrak{P}_T|\mathfrak{P}_Z)$.

Beweis: $L|Z_\mathfrak{P}$ ist Galoissch mit Galoisgruppe $\mathrm{Gal}(L|Z_\mathfrak{P}) = G_\mathfrak{P}$. Da $I_\mathfrak{P}$ normal in $G_\mathfrak{P}$ liegt, ist der Zwischenkörper $T_\mathfrak{P}|Z_\mathfrak{P}$ normal und $G(T_\mathfrak{P}|Z_\mathfrak{P}) \cong G_\mathfrak{P}/I_\mathfrak{P}$. Das zeigt (i). Aus der Sequenz

$$1 \longrightarrow I_\mathfrak{P} \longrightarrow G_\mathfrak{P} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)) \longrightarrow 1$$

folgt (ii).

Es ist nun $I_{\mathfrak{P}} = \mathrm{Gal}(L|I_{\mathfrak{P}})$ die Zerlegungsgruppe von $\mathfrak{P}$ über $T_{\mathfrak{P}}$, sodass nach (VIII.3) die Abbildung $I_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T))$ surjektiv ist.

Andererseits liegt $I_{\mathfrak{P}}$ sogar im Kern von

$$G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)) \supseteq \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)).$$

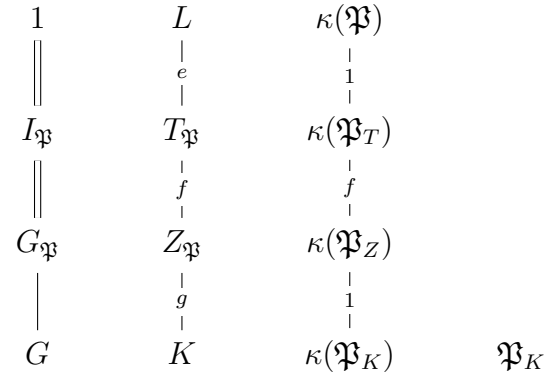
und somit ist letztere trivial. Nach Separabilität von $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)$ ist

$$f(\mathfrak{P}|\mathfrak{P}_T) := [\kappa(\mathfrak{P}) : \kappa(\mathfrak{P}_T)] = \#(\mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)) = 1.$$

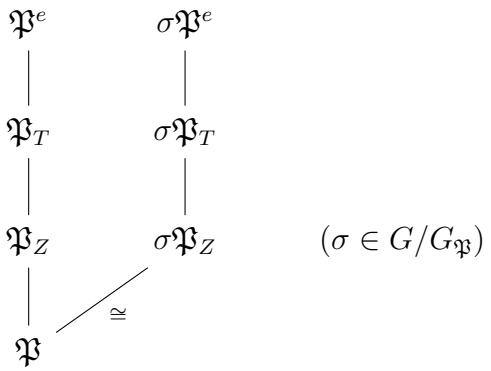
Also ist $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$ und $f := f(\mathfrak{P}|\mathfrak{P}_K) = f(\mathfrak{P}|\mathfrak{P}_T) \cdot f(\mathfrak{P}_T|\mathfrak{P}_Z)$. Aus (ii) folgt $f = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}]$ und so ist $f = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = e(\mathfrak{P}_T|\mathfrak{P}_Z) \cdot f(\mathfrak{P}_T|\mathfrak{P}_Z) \cdot g'$, also ist $e(\mathfrak{P}_T|\mathfrak{P}_Z) = g' = 1$.

Aus $\#(G_{\mathfrak{P}}) = [L : Z_{\mathfrak{P}}] = ef$ gewinnen wir nun, dass $e(\mathfrak{P}|\mathfrak{P}_T) = e$ und $f(\mathfrak{P}|\mathfrak{P}_T) = 1$. □

Zusammenfassend erhalten wir für den Fall, dass $\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_K)$ separabel ist, das Bild



Ist $G_{\mathfrak{P}}$ sogar nomal in G, d. h. ist $Z_{\mathfrak{P}}|K$ Galoisch, so gilt



Andernfalls können wir lediglich $\mathfrak{P}_K \cdot \mathcal{O}_{Z_{\mathfrak{P}}} = \mathfrak{P}_Z \cdot I$ mit $\mathfrak{P}_Z \nmid I$ schließen.

Kapitel IX.

Kreisteilungskörper

Im Folgenden sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel, d. h. $\zeta = \exp(2\pi \mathrm{i} m/n)$ mit $m \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Erinnerung: Das Minimalpolynom von ζ ist $\Phi_n = \prod((x-\zeta^m) \mid m \in (\mathbb{Z}/n\mathbb{Z})^\times)$. Der Körper $\mathbb{Q}(\zeta)$ heißt n-ter Kreisteilungskörper und sein Grad ist

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] = \deg \Phi_n = \#\mathbb{Z}/n\mathbb{Z}^\times =: \varphi(n),$$

wobei φ die Eulersche-φ-Funktion bezeichnet. Die Abbildung

$$\mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \sigma \longmapsto \bar{m}$$

wobei $\sigma(\zeta) = \zeta^m$, ist ein Isomorphismus von Gruppen.

Im Folgenden bezeichne $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\zeta)}$.

Lemma IX.1: *Sei $n = p^\nu$ eine Primpotenz und $\lambda := 1 - \zeta$. Dann ist die Primidealzerlegung von $p\mathcal{O}$ genau $p\mathcal{O} = (\lambda)^{\varphi(p^\nu)}$. Weiter ist* $\mathrm{Disk}(\Phi_{p^\nu}) = \pm p^s$ *mit $s = p^{\nu-1}(\nu p - \nu - 1)$.*

Beweis: Setzen wir $t := x^{p^{\nu-1}}$, so können wir schreiben

$$\Phi_{p^\nu} = \frac{X^{p^\nu} - 1}{X^{p^{\nu-1}} - 1} = \frac{t^p - 1}{t - 1} = t^{p-1} + \cdots + t + 1,$$

d. h. $p = \Phi_{p^\nu}(1) = \prod((1 - \zeta^m) | m \in (\mathbb{Z}/n\mathbb{Z})^\times)$. Es ist

$$\frac{1 - \zeta^m}{1 - \zeta} = \zeta^{m-1} + \cdots + 1 \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}$$

und genauso erhalten wir für $\zeta' = \zeta^m$ sowie $\zeta = \zeta'^{m'}$, dass

$$\frac{1 - \zeta}{1 - \zeta^m} = \frac{1 - \zeta'^{m'}}{1 - \zeta'} \in \mathbb{Z}[\zeta'] = \mathbb{Z}[\zeta] \subseteq \mathcal{O}.$$

Also ist $(1-\zeta^m)/(1-\zeta)$ eine Einheit in $\mathcal{O}$, wir haben

$$p = \prod_m (1-\zeta^m) = \prod_m \frac{1-\zeta^m}{1-\zeta}(1-\zeta)^{\varphi(p^\nu)}$$

und es ist $p\mathcal{O} = (1-\zeta)^{\varphi(p^\nu)}\mathcal{O}$. Da $\varphi(p^\nu) = [\mathbb{Q}[\zeta] : \mathbb{Q}]$ zeigt die fundamentale Gleichung, dass $(1-\zeta)$ ein Primideal vom Trägheitsgrad 1 ist. Schließlich haben wir $\pm\operatorname{Disk}(\Phi_{p^\nu}) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi'_n(\zeta))$ und

$$\frac{d\Phi_{p^\nu}}{dx}(x^{p^{\nu-1}}-1)\Phi_{p^\nu}\bigg|_{x=\zeta} = x^{p^{\nu-1}}-1 = (\zeta^{p^{\nu-1}}-1)\Phi'_{p^\nu}(\zeta) = p^\nu\zeta^{p^{\nu-1}}.$$

Setze $\xi := \zeta^{p^{\nu-1}}$. Dieses ξ ist eine p-te Einheitswurzel. Insgesamt ist

$$\pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi'_{p^\nu}(\zeta)) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\frac{p^\nu\zeta^{p^{\nu-1}}}{\xi-1}\right) = \frac{(p^\nu)^{\varphi(p^\nu)}}{N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1))^{p^{\nu-1}}} = \frac{p^{\nu p^{\nu-1}(p-1)}}{p^{p^{\nu-1}}},$$

was wir zeigen wollten. □

Lemma IX.2: *Sei $n = p^\nu$ und $\zeta = \zeta_{p^\nu}$ eine primitive p^ν-te Einheitswurzel. Dann ist $\mathcal{O} = \mathbb{Z}[\zeta]$.*

Beweis: Aus dem vorherigen Lemma erhalten wir $p^s = d(1,\zeta,\ldots,\zeta^{\varphi(n)})$ und so ist $p^s\mathcal{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}$. Mit $\lambda := 1-\zeta$ ist $\mathcal{O}/(\lambda) \cong \mathbb{F}_p$. Also ist $\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O}$ und erst recht $\mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O}$. Wir erhalten $\lambda\mathcal{O} = \lambda\mathbb{Z}[\zeta] + \lambda^2\mathcal{O}$. Einsetzen liefert, dass

$$\mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^2\mathcal{O}.$$

Induktiv erhalten wir $\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^t\mathcal{O}$ für jedes $t \geq 1$. Für $t = s\cdot\varphi(n)$ ist $(\lambda)^t = (\lambda)^{\varphi(n)\cdot s} = (p)^s$. Mit $p^s\mathcal{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}$ sehen wir, dass

$$\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^t\mathcal{O} = \mathbb{Z}[\zeta] + p^s\mathcal{O} = \mathbb{Z}[\zeta]$$

und wir sind fertig. □

Lemma IX.3: *Seien L und L' Zahlkörper. Gilt für die Körpergrade $[L:\mathbb{Q}][L':\mathbb{Q}] = [LL':\mathbb{Q}]$, dann ist für $g = \operatorname{ggT}(d_L, d_{L'})$ die folgende Gleichung erfüllt:*

$$\mathcal{O}_{LL'} \subseteq \frac{1}{g}\mathcal{O}_L \cdot \mathcal{O}_{L'}.$$

Für $g = 1$ gilt $d_{LL'} = d_{L'}^{[L':\mathbb{Q}]} \cdot d_L^{[L:\mathbb{Q}]}$.

Beweis: Wir zeigen äquivalent, dass $g\mathcal{O}_{LL'} \subseteq \mathcal{O}_L\mathcal{O}_{L'}$. Seien $\omega_1, \ldots, \omega_n$ und $\omega'_1, \ldots, \omega'_n$ Ganzheitsbasen von $\mathcal{O}_L$ respektive $\mathcal{O}_{L'}$. Wegen der Gleichung für die Körpergrade ist $\omega_i\omega'_j$ eine Basis des Kompositums, sodass wir jedes $\alpha \in \mathcal{O}_{LL'}$ eindeutig schreiben können als $\alpha = \sum_{ij} a_{ij} w'_i w_j$ mit geeigneten rationalen Zahlen a_{ij}. Es ist zu zeigen, dass $g\alpha \in \mathcal{O}_L\mathcal{O}_{L'}$, d. h. $ga_{ij} \in \mathbb{Z}$.

Ohne Beschränkung der Allgemeinheit können wir L und L' als Teilkörper der komplexen Zahlen auffassen. Jede Einbettung $i\colon L \hookrightarrow \mathbb{C}$ setzt sich fort zu einer Einbettung $\sigma\colon LL' \hookrightarrow \mathbb{C}$, die L' fest lässt, d. h. $\sigma \in \mathrm{Hom}_{L'}(LL', \mathbb{C})$.

Um dies zu sehen, schreibe $L = \mathbb{Q}(\omega)$. Dann ist $LL' = L'(\omega)$. Nach der Gleichung über die Körpergrade ändert sich der Grad des Minimalpolynoms von ω nicht, wenn wir es statt über $\mathbb{Q}$ über L' nehmen. Folglich ist $\sigma\colon L'(\omega) \to \mathbb{C}$ eindeutig bestimmt durch $\sigma(\omega) = i(\omega)$.

Wir erhalten

$$\sigma(\alpha) = \sum_{ij} a_{ij}\omega_{i'}\sigma(\omega_j) = \sum_j \sigma(w_j) \cdot \sum_i a_{ij}\omega'_i.$$

Für $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{L'}(LL', \mathbb{C}) \cong \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ rechnen wir nach, dass

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{pmatrix} \cdot \begin{pmatrix} \sum_i a_{i1}\omega'_i \\ \vdots \\ \sum_i a_{in}\omega'_n \end{pmatrix}.$$

Wir bezeichnen die Matrix in der obigen Gleichung mit T, den Vektor auf der rechten Seite mit b und den Vektor auf der linken Seite mit a.

Es ist $(\det T)^2 = d_L$ und $(\det T)b = T^*a$. Nun sind die Einträge von T und a allesamt ganz über $\mathbb{Z}$, und somit auch die von $d_L b = \det(T) \cdot T^*a$ – d. h. $\det(T) \cdot T^*a \in \mathcal{O}_{L'}^n$.

Da $(d_L b)_j = \sum_i (d_L a_{ij})\omega'_i \in \mathcal{O}_L = \bigoplus_{i=1}^n \mathbb{Z}\omega'_i$ gilt, liegen die Koeffizienten $d_L a_{ij}$ allesamt in $\mathbb{Z}$.

Vertauschen der Rollen von ω_i und ω'_j liefert mit den selben Argumenten, dass ebenfalls $d_{L'}a_{ij} \in \mathbb{Z}$. Schreibe nun mit dem Lemma von Bézout $g = xd_L + x'd_{L'}$. Dann ist $ga_{ij} = xd_L a_{ij} + x'd_L a_{ij}$ eine ganze Zahl.

Ist nun $g = 1$, so ist $\mathcal{O}_{LL'} = \mathcal{O}_L\mathcal{O}_{L'} = \bigoplus_{ij} \mathbb{Z}(\omega_i\omega'_j)$. Wegen der Gleichung für die Körpergrade ist

$$\mathrm{Hom}(LL', \mathbb{C}) = \{\sigma_i\sigma'_j \mid \sigma \in \mathrm{Hom}_{L'}(LL', \mathbb{C}), \sigma'_j \in \mathrm{Hom}_L(LL', \mathbb{C})\}.$$

Wir berechnen die Determinante von $(\sigma_i\sigma'_j)(\omega_k\omega'_\ell) = \sigma_i(\omega_k)\sigma'_j(\omega'_\ell) \in \mathbb{C}^{nn' \times nn'}$. Diese Matrix ist (bis auf Umordnung) genau das Kronecker-Produkt

$$(\sigma_i(\omega_k)_{ik} \otimes (\sigma'_j(\omega_\ell)'))_{j\ell} = T \otimes T'$$

und so $d_{LL'} = \det(T \otimes T')^2 = (\det T)^{2n'} \cdot (\det T')^{2n} = d_L^{n'} \cdot d_{L'}^n$. Dies beschließt den Beweis. Wir bemerken, dass wegen der Gleichung der Körpergrade gilt, dass $LL' \cong L \otimes_{\mathbb{Q}} L'$ und $\mathrm{Hom}(LL', \mathbb{C}) \cong \mathrm{Hom}(L, \mathbb{C}) \times \mathrm{Hom}(L', \mathbb{C})$. □

Satz IX.4: *Seien n eine natürliche Zahl und ζ eine primitive n-te Einheitswurzel. Dann ist $\mathcal{O} = \mathbb{Z}[\zeta]$.*

Beweis: Für $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ ist $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{p_1^{\nu_1}}) \cdots \mathbb{Q}(\zeta_{p_t^{\nu_t}})$ das Kompositum und

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \prod_{i=1}^{t} \varphi(p_i^{\nu_i} = \prod_{i=1}^{t} [\mathbb{Q}(\zeta_{p_i^{\nu_i}}) : \mathbb{Q}].$$

Weiter sind auch die Diskriminanten der $\mathbb{Q}(\zeta_{p_i^{\nu_i}})$ teilerfremd, sodass wir das eben bewiesene Lemma auf die Ganzheitsbasis $\{1, \zeta_{p_i}, \ldots, \zeta_{p_i}^{d_i - 1}\}$ mit $d_i = \varphi(p_i^{\nu_i})$ sukzessive anwenden können. Es ist also

$$\zeta_{p_1^{\nu_1}}^{j_1} \cdots \zeta_{p_t^{\nu_t}}^{j_t}, \qquad 0 \le j_i \le d_i - 1$$

eine Ganzheitsbasis von $\mathbb{Q}(\zeta)$. Jedes dieser Elemente ist aber eine Potenz von ζ und folglich $\mathbb{Z}[\zeta] = \mathcal{O}$. □

Satz IX.5: *Seien n eine natürliche Zahl und $n = \prod_p p^{\nu_p}$ die zugehörige Primfaktorzerlegung. Sei f_p die Ordnung von $\bar{p} \in (\mathbb{Z}/(n/p^{\nu_p})\mathbb{Z})^\times$. Dann ist*

$$p\mathbb{Z}[\zeta] = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{e_p} \quad \textit{mit} \quad e_p = \varphi(p^{\nu_p})$$

die Primidealzerlegung von (p) und die $\mathfrak{p}_i$ sind vom Trägheitsgrad f_p. Es gilt $\varphi(n) = e_p f_p g_p$.

Beweis: Wegen $\mathcal{O} = \mathbb{Z}[\zeta]$ genügt es nach (Bemerkung VII.5), die Primfaktorzerlegung von $\Phi_n \pmod p$ zu bestimmen. Es ist also zu zeigen, dass

$$\Phi_n \equiv (p_1 \cdots p_{g_p})^{e_p} \pmod p$$

mit $p_i \in \mathbb{F}_p[X]$ irreduzibel und vom Grad f_p. Für $n = p^{\nu_p} \cdot m$, $\xi = \zeta^{p^{\nu_p}}$, $\eta = \zeta^m$ sind die Produkte $\xi^i \eta^j$, wobei $i \in (\mathbb{Z}/m\mathbb{Z})^\times$ und $j \in (\mathbb{Z}/p^{\nu_p}\mathbb{Z})^\times$ genau die primitiven n-ten Einheitswurzeln. Es ist somit

$$\Phi_n = \prod_{i,j} (X - \xi^i \eta^j).$$

Aus $0 = (\eta^j)^{p^{\nu_p}} - 1 \equiv (\eta^j - 1)^{p^{\nu_p}} \pmod{p\mathbb{Z}[\zeta]}$ erhalten wir $\eta^j \equiv 1 \pmod{p\mathbb{Z}[\zeta]}$. Somit ist

$$\Phi_n \equiv \prod_{i,j}(X - \xi^i\eta^j) = \prod_i (X - \xi^i)^{\varphi(p^{\nu_p})} = \Phi_m^{\varphi(p^{\nu_p})} \pmod{p\mathbb{Z}[\zeta]}$$

und sogar $\Phi_n \equiv (\Phi_m)^{\varphi(p^{\nu_p})} \pmod{p\mathbb{Z}}$, da $p\mathbb{Z} = p\mathbb{Z}[\zeta] \cap \mathbb{Z}$. Als Teiler von $X^m - 1$ ist $\bar{\Phi}_m \in \mathbb{F}_p[X]$ separabel, hat also nur einfache Nullstellen. Folglich ist $e_p = \varphi(p^{\nu_p})$ gezeigt.

Sei nun $\mathfrak{p} \mid (p)$ ein Primteiler. Es bleibt zu zeigen, dass $[\mathcal{O}/\mathfrak{p} : \mathbb{F}_p] = f_p$, wobei f_p die Ordnung von $\bar{p}$ in der Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ bezeichnet. Da $\bar{X}^m - 1$ separabel ist, induziert $\mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{p}$ eine Bijektion der m-ten Einheitswurzeln $\mu_m(\mathbb{Q}(\zeta)) \to \mu_m(\mathcal{O}/\mathfrak{p})$. Weiter ist $\mathcal{O}/\mathfrak{p}$ auch erzeugt von $\zeta_m \pmod{p}$ und somit ist $\mathcal{O}/\mathfrak{p}$ genau der Zerfällungskörper von $\bar{\Phi}_m \in \mathbb{F}_p[X]$. d. h. die kleinste Erweiterung $\mathbb{F}_q$ von $\mathbb{F}_p$, die eine primitive m-te Einheitswurzel enthält. Die Gruppe $\mathbb{F}_q^\times$ ist zyklisch als Einheitengruppe eines endlichen Körpers und von der Ordnung $q - 1$. Sie enthält genau dann ein Element der Ordnung m, falls $m \mid q - 1$, d. h. $q \equiv 1 \pmod{m}$. Nun ist $q = p^f$ für ein $f \geq 1$ und für $f = f_p$ ist q minimal mit $q = p^f \equiv 1 \pmod{m}$. □

Korollar IX.6: *Sei p eine Primzahl. Dann ist p genau dann verzweigt, wenn $n \equiv 0 \pmod{p}$, es sei denn $p = 2 = \mathrm{ggT}(4, n)$. Ist weiter $p \neq 2$, so ist sie voll zerlegt in $\mathbb{Q}(\zeta)$ genau dann, wenn $p \equiv 1 \pmod{n}$.*

Kapitel X.

Quadratische Reste

Definition X.1: Sei p eine Primzahl.

(i) Eine Restklasse $\bar{a} \in \mathbb{F}_p$ heißt *quadratischer Rest modulo* p, falls es eine ganze Zahl b mit $\bar{a} = \bar{b}^2$ gibt.

(ii) Sei $p \neq 2$ eine Primzahl. Das Legendre-Symbol ist

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}, \qquad \bar{a} \longmapsto \begin{cases} 1, & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{sonst.} \end{cases}$$

Für eine ganze Zahl a setzen wir

$$\left(\frac{a}{p}\right) := \begin{cases} \left(\frac{\bar{a}}{p}\right), & \text{falls } p \nmid a, \\ 0, & \text{falls } p \mid a. \end{cases}$$

Satz X.2: *Es gilt das* quadratische Rezirozitätsgesetz*:*

(i) *Seien $q, p > 2$ verschiedene Primzahlen. Dann gilt*

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

(ii) *Erster Ergänzungssatz:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{falls } p \equiv 1 \pmod 4, \\ -1, & \textit{falls } p \equiv 3 \pmod 4. \end{cases}$$

(iii) *Zweiter Ergänzungssatz:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{falls } p \equiv 1, 7 \pmod 8, \\ -1, & \textit{falls } p \equiv 3, 5 \pmod 8. \end{cases}$$

Beispiel X.3: Seien $p = 1889$ und $q = 67$. Hat $x^2 \equiv 67 \pmod{1889}$ eine Lösung $x \in \mathbb{Z}$? Zur Beantwortung dieser Frage können wir einfach das entsprechende Legendre-Symbol ausrechnen:

$$\left(\frac{67}{1889}\right) = \left(\frac{1889}{67}\right) = \left(\frac{13}{67}\right) = \left(\frac{67}{13}\right) = \left(\frac{2}{13}\right) = -1,$$

damit ist die Antwort: „Nein, so eine ganze Zahl x gibt es nicht“.

Lemma X.4 (Euler):

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Lemma X.5: *Es sei $p > 2$ eine Primzahl. Dann gelten:*

(i) $\mathbb{F}_p^\times \to \{\pm 1\}$, $a \mapsto (\frac{a}{p})$ *ist ein Epimorphismus.*

(ii) *Für $a, b \in \mathbb{Z}$ gilt $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.*

Beweis: Die Einheitengruppe $\mathbb{F}_p^\times$ ist zyklisch, d. h. $(\mathbb{F}_p^\times) \cong (\mathbb{Z}/(p-1), +)$. Also ist

$$\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong (\mathbb{Z}/(p-1)\mathbb{Z}/2(\mathbb{Z}/(p-1)\mathbb{Z})) \cong \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}.$$

Das Legendre-Symbol stimmt also mit dem Epimorphismus $\mathbb{F}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$ überein. Die zweite Aussage folgt aus der ersten. □

Beispiel X.6: Gibt es irgendeine ganze Zahl x mit $x^2 \equiv 2012 \pmod{30167}$? Wegen $30167 = 97 \cdot 311$ sagt uns der Chinesische Restsatz, dass es genau so eine Lösung x gibt, falls die Kongruenzen

$$\begin{aligned} x^2 &\equiv 2012 \pmod{97}, \\ x^2 &\equiv 2012 \pmod{311}. \end{aligned}$$

lösbar sind. Wegen $2012 \equiv 72 \pmod{97}$ und $2012 \equiv 146 \pmod{311}$ berechnen wir die Legendre-Symbole $(\frac{72}{97})$ und $(\frac{146}{311})$. Zunächst ist

$$\left(\frac{72}{97}\right) = \left(\frac{2 \cdot 6^2}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{6}{97}\right)^2 = \left(\frac{2}{97}\right) = 1,$$

außerdem haben wir

$$\begin{aligned} \left(\frac{146}{311}\right) &= \left(\frac{2 \cdot 73}{311}\right) \\ &= \left(\frac{2}{311}\right)\left(\frac{73}{311}\right) = \left(\frac{73}{311}\right) = \left(\frac{311}{73}\right) = \left(\frac{19}{73}\right) = \left(\frac{73}{19}\right) = \left(\frac{16}{19}\right) = 1. \end{aligned}$$

Die Gleichung hat also in der Tat eine ganzzahlige Lösung. Per Computer kann man ausrechnen, dass $7553^2 - 2012 = 1891 \cdot 30\,167$.

Bemerkung X.7: Seien a eine quadratfreie ganze Zahl und $p > 2$ prim. Es ist $(\frac{a}{p}) = 1$ genau dann, wenn es eine ganze Zahl b mit $x^2 - a \equiv (x+b)(x-b) \pmod{p}$ gibt. Teilt p nicht $d(1, \sqrt{a})$, dann bedeutet das, dass $(P) = (P, \sqrt{a}+b)(p, \sqrt{a}-b)$ voll zerlegt in $\mathbb{Q}(\sqrt{a})$ ist.

Idee X.8: Wir haben die Isomorphie $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist zyklisch und von der Ordnung $p-1$. Es gibt also genau eine Untergruppe vom Index 2, d. h. genau einen Zwischenkörper K mit $[K : \mathbb{Q}] = 2$ und $[\mathbb{Q}(\zeta_p) : K] = (p-1)/2$. Es ist $K = \mathbb{Q}(\sqrt{d})$ für irgendeine ganze Zahl d. Ist $p \equiv 1 \pmod{4}$, so ist p die einzige in $\mathbb{Q}(\sqrt{p})$ verzweigte Primzahl und $\mathbb{Q}(\sqrt{p})$ ist der einzige quadratische Zahlkörper mit dieser Eigenschaft.

Für $p \equiv 3 \pmod{4}$ ist $-p \equiv 1 \pmod{4}$ und wieder ist p die einzige in $\mathbb{Q}(\sqrt{-p})$ verzweigte Primzahl. Also ist $d = (-1)^{(p-1)/2}p =: p^*$. Man kann d auch explizit ohne Galois-Theorie finden. Für

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) \xi^a$$

ist $\tau^2 = p^*$.

Lemma X.9: *Es seien ℓ und p ungerade Primzahlen, $\ell^* := (-1)^{(\ell-1)/2}\ell$ und ζ eine primitive ℓ-te Einheitswurzel. Dann ist p voll zerlegt in $\mathbb{Q}(\sqrt{\ell^*})$ genau dann, wenn p in $\mathbb{Q}(\zeta)$ in eine gerade Anzahl von Primidealen zerfällt.*

Beweis: Ist $(p) = \mathfrak{p}_1\mathfrak{p}_2$ voll zerlegt in $\mathbb{Q}(\sqrt{d^*})$ und $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ mit $\sigma\mathfrak{p}_1 = \mathfrak{p}_2$, so bildet σ über $\mathfrak{p}_1$ liegende Primideale von $\mathbb{Z}[\zeta]$ bijektiv auf die über $\mathfrak{p}_2 = \sigma\mathfrak{p}_1$ liegenden ab. Die Zahl der über (p) liegenden Primideale von $\mathbb{Z}[\zeta]$ ist also gerade.

Zerfällt umgekehrt p in $\mathbb{Q}(\zeta)$ in eine gerade Anzahl g von Primidealen, dann ist $g = [G : G_\mathfrak{p}]$ für die Zerlegungsgruppe $G_\mathfrak{p}$ eines Primideals $\mathfrak{p}$, das p teilt. Da nun der Zerlegungskörper $Z_\mathfrak{p}$ den geraden Grad $g = [Z_\mathfrak{p} : \mathbb{Q}]$ hat, muss er $\mathbb{Q}(\sqrt{\ell^*})$ enthalten. Der Trägheitsgrad von $\mathfrak{p}_Z = Z_\mathfrak{p} \cap \mathfrak{P}$ ist eins und genau so sein Verzweigungsindex. Selbiges muss also auch für $\mathfrak{p}_K = \mathfrak{p} \cap \mathbb{Q}(\sqrt{\ell^*})$ gelten, d. h. (p) ist voll zerlegt in $\mathbb{Q}(\sqrt{\ell^*})$. □

Beweis (des quadratischen Reziprozitätsgesetzes): Zu (i): Seien ℓ und p ungerade Primzahlen. Es ist $(\frac{\ell^*}{p}) = 1$ genau dann, wenn p voll zerlegt ist in $\mathbb{Q}(\sqrt{\ell^*})$. Nach dem vorherigen Lemma ist das äquivalent dazu, dass p in $\mathbb{Q}(\zeta_\ell)$ in eine gerade Anzahl g von Primidealen zerfällt. Wegen $efg = \varphi(\ell) = \ell - 1$ ist das genau dann der Fall, wenn

$$g = \frac{\ell-1}{p} = \frac{\ell-1}{ef} = \frac{\ell-1}{f}$$

gerade ist, wobei f die Ordnung von $\bar{p}$ in $\mathbb{F}_\ell^\times$ beschreibt. Jetzt ist $(\ell-1)/f$ gerade genau dann, wenn f ein Teiler von $(\ell-1)/2$ ist, was genau dann der Fall ist, wenn $1 \equiv p^{(\ell-1)/2} \pmod{\ell}$. Nach dem Satz von Euler gelangen wir also zu

$$1 \equiv p^{\frac{\ell-1}{2}} \equiv \left(\frac{p}{\ell}\right) \pmod{\ell},$$

und wir erhalten

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

Zu (ii): Das ist eine direkte Konsequenz des Lemmas von Euler.

Zu (iii): Es sei $\zeta = \zeta_8$ eine achte Einheitswurzel. Dann ist $\mathrm{i} = \zeta^2$ und

$$x^4 + 1 = (x^2 - \mathrm{i})(x + \mathrm{i}) = (x^2 - \zeta^2)(x^2 - \zeta^{-2}).$$

Durch Ausmultiplizieren der rechten Seite erhalten wir $(\zeta+\zeta^{-1})^2 = 2$. Schreiben wir $a := \zeta + \zeta^{-1}$, liest sich die Gleichung $a^2 = 2$. Ist nun $p \equiv \pm 1 \pmod 8$, so ist

$$a^p \equiv \zeta^p + \zeta^{-p} = \zeta + \zeta^{-1} = a \pmod{p\mathbb{Z}[\zeta]}.$$

Es folgt $a^{p-1} \equiv 1 \pmod{p\mathbb{Z}[\zeta]}$, also $(\frac{2}{p}) = 2^{(p-1)/2} \equiv 1 \pmod p$.

Für $p \equiv \pm 5 \pmod 8$ ist $a^p \equiv \zeta^p + \zeta^{-p} = \zeta^5 + \zeta^{-5} = -(\zeta^1 + \zeta^{-1}) \equiv -a \pmod{p\mathbb{Z}[\zeta]}$. Und so ist $-1 = a^{p-1} = 2^{(p-1)/2} \equiv (\frac{2}{p}) \pmod p$. □

Bemerkung X.10: Euler hat das Quadratische Reziprozitätsgesetz bereits vermutet, jedoch erst Gauß hat es 1796 per Induktion bewiesen. Später fand er mindestens 8 weitere Beweise für das Quadratische Reziprozitätsgesetz. Auf der Homepage von Franz Lemmermeyer finden sich über 240 weitere Beweise in mindestens 30 Beweisfamilien. Keiner ist offensichtlich.

Bemerkung X.11: Bevor wir $(\frac{a}{p})$ im quadratischen Reziprozitätsgesetz umdrehen konnten, brauchten wir die Primfaktorzerlegung von a. Dies ist algorithmisch teuer.

Definition X.12: Sei n eine ungerade natürliche Zahl mit Primfaktorzerlegung $n = \prod_{i=1}^r p_i^{e_i}$. Dann ist das Jacobi-Symbol

$$\left(\frac{a}{n}\right) = \prod_{i=1}^n \left(\frac{a}{p_i}\right)^{e_i} \in \{0, \pm 1\}$$

mit $(\frac{a}{1}) = 1$, falls $a \neq 0$ und Null sonst, eine Fortsetzung des Legendre-Symbols.

Bemerkung X.13: Ist a ein quadratischer Rest modulo n, so auch für alle Primfaktoren p_i aus der Primfaktorzerlegung von n und $(\frac{a}{n}) = 1$.

Die Umkehrung dieser Aussage ist falsch. Es ist nämlich

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1,$$

aber 2 ist kein Quadrat modulo 15.

Die Abbildung

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \qquad a \longmapsto \left(\frac{a}{n}\right)$$

ist ein Homomorphismus (wegen des Chinesischen Restsatzes).

Satz X.14: *Seien n und m teilerfremde ganze Zahlen. Dann gelten:*

(i) $(\frac{n}{m})(\frac{m}{n}) = (-1)^{(n-1)/2(m-1)/2}$,

(ii) $(\frac{-1}{n}) = (-1)^{(n-1)/2}$,

(iii) $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$.

Beweis: Zu (ii) Sind a und b ungerade, dann haben wir die Äquivalenzen

$$\begin{aligned}\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2 &\iff a-1+b-1 \equiv ab-1 \pmod 4\\ &\iff (a-1)(b-1) \equiv 0 \pmod 4\end{aligned}$$

wobei die letzte Aussage wahr ist, da a und b ungerade sind. Also ist $n \mapsto (-1)^{(n-1)/2}$ multiplikativ für n ungerade und genauso $(\frac{-1}{n})$, sie stimmen für alle Primzahlen überein, sind also gleich.

Der Beweis von (iii) funktioniert genau wie der von (ii).

Zu (i): Die linke und rechte Seite sind multiplikativ in m und n. Damit reicht es, $n = p \neq q = m$ zu betrachten, wobei p und q ungerade Primzahlen sind. Aber in diesem Fall greift das quadratische Reziprozitätsgesetz. □

Beispiel X.15: Wir haben

$$\begin{aligned}\left(\frac{101}{167}\right) &= \left(\frac{167}{101}\right)\\ &= \left(\frac{66}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{33}{101}\right) = (-1)\left(\frac{33}{101}\right) = -\left(\frac{101}{33}\right) = -\left(\frac{2}{33}\right) = -1.\end{aligned}$$

Die Strategie zum Berechnen des Jacobi-Symbols ist:

- Faktoren 2 und -1 im „Zähler“ abspalten,
- Das Jabobisymbol $(\frac{m}{n})$ mit dem Reziprozitätsgesetz unter Beachtung des Vorzeichens bearbeiten und anschließend m modulo n reduzieren,
- Wiederholen.

Die Strategie ist ähnlich zum euklidischen Algorithmus und hat auch eine ähnliche Laufzeit.

Kapitel XI.

Die p-adischen Zahlen

Jede natürliche Zahl f hat ein eindeutige p-adische Darstellung

$$f = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n,$$

wobei $a_i \in \{0, \ldots, p-1\}$ und n eine natürliche Zahl sind. Wir erhalten sie wie folgt: Setze $f_0 := f$, $a_i \equiv f_i \pmod{p}$ und $f_{i+1} = \frac{f_i - a_i}{p}$.

Beispiel XI.1: Seien $f = 216$ und $p = 5$.

(i) Es ist $216 \equiv 1 \pmod{5}$ also $a_0 = 1$ und $f_1 = \frac{216-1}{5} = 43$.

(ii) Es ist $43 \equiv 3 \pmod{5}$, also $a_1 = 3$ und $f_2 = \frac{43-3}{5} = 8$.

(iii) Es ist $8 \equiv 3 \pmod{5}$, also $a_2 = 3$ und $f_3 = \frac{8-3}{5} = 1$.

(iv) Es ist $1 \equiv 1 \pmod{5}$, also $a_3 = 1$ und $f_4 = 0$.

Wir haben für f damit die Darstellung $f = 216 = 1 + 3 \cdot 5 + 3 \cdot 25 + 1 \cdot 125$ gefunden. Wir schreiben dafür $216 = 1{,}331_5$.

Versuchen wir das Verfahren mit $f = -1$, dann ist $f_0 = -1 \equiv p - 1 \pmod{p}$ und $a_0 = p - 1$, $f_1 = -1$. Für alle i haben wir also $a_i = p - 1$ und $f_i = -1$. Wir erhalten „$-1 = p - 1 + (p-1) \cdot p + (p-1) \cdot p^2 + \ldots$“. Diesem Ausdruck wollen wir einen Sinn verleihen.

Dazu sehen wir die formale Reihe $\sum_{\nu=0}^{\infty} a_\nu p^\nu$ als Folge ihrer Partialsummen $s_n = \sum_{\nu=0}^{n} a_\nu p^\nu$. Jede Partialsumme ist auch eindeutig durch ihre Restklasse $\bar{s}_n = s_n \pmod{p^n}$ bestimmt.

Definition XI.2: Die Menge der ganzen p-adischen Zahlen ist

$$\mathbb{Z}_p := \Big\{ \sum_{\nu=0}^{\infty} a_\nu p^\nu : a_\nu \in \{0, \ldots, p-1\} \Big\}.$$

Wir erhalten eine Einbettung

$$\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p, \qquad f \longmapsto (s_n)_{n\in\mathbb{N}},$$

wobei $f \equiv s_n = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \pmod{p^n\mathbb{Z}_{(p)}}$. Das Bild von f heißt p-adische Entwicklung von f.

Definition XI.3: Die Menge der p-adischen Zahlen ist

$$\mathbb{Q}_p := \Big\{ \sum_{\nu=-m}^{\infty} a_\nu p^\nu : a_\nu \in \{0,\dots,p-1\}, m \in \mathbb{N}\Big\}.$$

Schreiben wir $f \in \mathbb{Q}$ als $g/h \cdot p^{-m}$ mit $g, h \in \mathbb{Z}$, wobei $p \nmid gh$, so ordnen wir ihr die Entwicklung $\sum_{\nu=0}^{\infty} a_\nu p^{\nu-m}$ zu, wobei $\sum_{\nu=0}^{\infty} a_\nu p^\nu$ die p-adische Entwicklung von g/h in $\mathbb{Z}_{(p)}$ ist. Wir erhalten die Einbettung $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Beispiel XI.4: Es ist $1/(1-p) = 1 + p + p^2 + \dots$, denn

$$1 = (1 + p + p^2 + \cdots + p^{n-1})(1-p) + p^n,$$

also ist $1/(1-p) \equiv 1 + p + \cdots + p^{n-1}$ modulo $p^n\mathbb{Z}_{(p)}$.

Wir wollen nun $\mathbb{Z}_p$ die Struktur eines Rings geben. Dazu betrachten wir $f = \sum_{\nu=0}^{\infty} a_\nu p^\nu$ nicht als Folge der Partialsummen s_n in $\mathbb{Z}$, sondern als Familie von Restklassen $\bar{s}_n = s_n + p^n\mathbb{Z} \in \mathbb{Z}/p^n\mathbb{Z}$. Wir erhalten Abbildungen

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \qquad \dots$$

mit $\lambda_n(\bar{s}_{n+1}) = \bar{s}_n$. Die Familie $(\bar{s}_n)_{n\in\mathbb{N}}$ liegt also im *projektiven Limes*

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \Big\{(x_n)_{n\in\mathbb{N}} \in \prod_{i=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \forall\, n : \lambda_n(x_{n+1}) = x_n\Big\}.$$

Satz XI.5: *Wir erhalten eine bijektive Abbildung*

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, \qquad \sum_{\nu=0}^{\infty} a_\nu p^\nu \longmapsto (\bar{s}_n)_{n\in\mathbb{N}} = \Big(\sum_{\nu=0}^{n-1} a_\nu p^\nu \pmod{p^n}\Big)_{n\in\mathbb{N}}.$$

Der Beweis bleibt dem Leser überlassen. Das Bild dieser Abbildung ist ein Teilring des Produktes, sodass $\mathbb{Z}_p$ die Struktur eines Rings erhält. Weiter ist $\mathbb{Q}_p = Q(\mathbb{Z}_p)$ der Quotientenkörper. Vermöge dieser Bijektion identifizieren wir $\mathbb{Z}_p$ und $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Die Einbettung $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ hat nun die Gestalt

$$a \longmapsto (a \pmod{p}, a \pmod{p^2}, a \pmod{p^3}, \dots)$$

Anwendung: Gibt es zu einem Polynom $F \in \mathbb{Z}[x_1, \ldots, x_n]$ eine ganzzahlige Lösung $F(x_1, \ldots, x_n) = 0$? Im Allgemeinen ist das eine sehr schwierige Frage. Üblicherweise wird man das Problem abschwächen: Man fragt, ob

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

lösbar für alle ganzen Zahlen m ist. Nach dem Chinesischen Restsatz ist das äquivalent zur Frage, ob $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ für alle Primzahlen p und $\nu \in \mathbb{N}$ lösbar ist.

Satz XI.6: *Seien $F \in \mathbb{Z}[X_1, \ldots, X_n]$ und p eine Primzahl. Dann ist die diophantische Gleichung $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ für alle $\nu \in \mathbb{N}$ lösbar genau dann, wenn $F(x_1, \ldots, x_n) = 0$ in $\mathbb{Z}_p$ lösbar ist.*

Beweis: Wir fassen $\mathbb{Z}_p$ hierfür als den projektiven Limes auf. Über dem Produktring $\prod_{\nu=1}^{\infty} \mathbb{Z}/p^\nu\mathbb{Z}$ zerfällt die Gleichung $F(x_1, \ldots, x_n) = 0$ in ihre Komponenten $F^{(\nu)}(x_1, \ldots, x_n) = 0 \pmod{p^\nu}$. Ist $(a_1, \ldots, a_n) = ({a_1}^{(\nu)}, \ldots, {a_n}^{(\nu)})_{\nu\in\mathbb{Z}}$ in $\mathbb{Z}_p^n$ eine p-adische Lösung, dann gilt für alle natürlichen Zahlen ν, dass

$$F({a_1}^{(\nu)}, \ldots, {a_n}^{(\nu)}) \equiv 0 \pmod{p^\nu}.$$

Sei umgekehrt $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}$ für jedes ν lösbar, d. h. $F = 0$ ist lösbar im Produktring. Sei $(a_\nu)_{\nu\in\mathbb{N}} \in \prod_{\nu=1}^{\infty} \mathbb{Z}/p^\nu\mathbb{Z}$ eine Lösung von $F = 0$. Diese braucht aber nicht in $\varprojlim_\nu \mathbb{Z}/p^\nu\mathbb{Z}$ zu liegen. Für eine einfachere Notation nehmen wir $n = 1$ und schreiben $a_\nu = {a_1}^{(\nu)}$. Der allgemeine Fall geht genau so.

Wir sehen $(a_\nu)_{\nu\in\mathbb{N}}$ nun als Folge in $\mathbb{Z}$. Nach dem Schubfachprinzip sind unendlich viele Folgenglieder kongruent modulo p, sagen wir zu $y_1 \in \mathbb{Z}/p\mathbb{Z}$. Wir finden also eine Teilfolge $({a_\nu}^{(1)})_{\nu\in\mathbb{N}}$ mit ${a_\nu}^{(1)} \equiv y_1 \pmod{p}$ für alle ν. Wieder gibt es ein $y_2 \in \mathbb{Z}/p^2\mathbb{Z}$, sodass unendlich viele Folgenglieder ${a_\nu}^{(1)}$ kongruent sind zu y_2 modulo p^2. Wir finden also eine Teilfolge ${a_\nu}^{(2)}$ von ${a_\nu}^{(2)}$ mit ${a_\nu}^{(2)} \equiv y_2 \pmod{p^2}$ für alle $\nu \in \mathbb{N}$. Weiter ist $y_2 \equiv y_1 \pmod{p}$, weil $({a_\nu}^{(2)})$ eine Teilfolge ist.

Fahren wir induktiv so fort, erhalten wir für jede natürliche Zahl k eine Teilfolge $({a_\nu}^{(k+1)})_{\nu\in\mathbb{N}}$ von $({a_\nu}^{(k)})_{\nu\in\mathbb{N}}$ und ein $y_{k+1} \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ mit $y_{k+1} \equiv y_k \pmod{p^k}$. Die y_k definieren also eine p-adische Zahl $y = (y_k)_{k\in\mathbb{N}} \in \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ mit $F(y) = 0$. □

Definition XI.7: Wir definieren den p-adischen Absolutbetrag per

$$\begin{aligned} |\cdot|_p \colon \mathbb{Q} \longrightarrow \mathbb{R}, \qquad & a \longmapsto |a|_p := p^{-\nu_p}(a) \\ & 0 \longmapsto 0 = p^{-\infty}. \end{aligned}$$

Beispiel XI.8: Es sind $|3|_2 = 1$, $|2|_2 = 1/2$, $|12|_2 = 1/4$ und $|5/4|_2 = 4$.

Lemma XI.9: *Für alle rationalen Zahlen a und b gelten:*

(i) $|a|_p = 0$ *genau dann, wenn* $a = 0$,

(ii) $|ab|_p = |a|_p|b|_p$,

(iii) $|a + b|_p \leq \max\{|a|_p, |b|_p\}$

Insbesondere ist $|\cdot|_p$ ein Betrag auf $\mathbb{Q}$.

Wir werden später sehen, dass die Beträge auf $\mathbb{Q}$ im Wesentlichen $|\cdot|_p$ und $|\cdot|_\infty := |\cdot|$ sind. Das heißt: Jeder weitere Betrag ist eine Potenz $|\cdot|_p^s$ oder $|\cdot|_\infty^s$ mit $s > 0$.

Satz XI.10 (Geschlossenheitsrelation): *Sei $0 \neq a$ eine rationale Zahl. Dann ist*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |a|_p = 1.$$

Beweis: Durch Umformung von $a = (\pm 1) \cdot \prod_{p \in \mathbb{P}} p^{\nu_p} = (a/|a|_\infty) \prod_{p \in \mathbb{P}} |a|_p^{-1}$ folgt die Behauptung. □

Sei R_∞ die Menge der Cauchyfolgen in $\mathbb{Q}$ bezüglich $|\cdot|_\infty$ und $\mathfrak{m}_\infty$ die Menge der Nullfolgen. R_∞ ist ein Ring und $\mathfrak{m}_\infty$ ist ein maximales Ideal. Wir setzen $\mathbb{R} := R_\infty/\mathfrak{m}_\infty$.

Analog sei R_p der Ring der Cauchyfolgen in $\mathbb{Q}$ bezüglich $|\cdot|_p$ und $\mathfrak{m}_p$ die Menge der Nullfolgen. Wie für $\mathbb{R}$ zeigen man, dass $\mathfrak{m}_p$ ein maximales Ideal ist. Es ist $\mathbb{Q}_p = R_p/\mathfrak{m}_p$.

Der Betrag $|\cdot|_p$ und die Bewertung ν_p setzen sich stetig auf $\mathbb{Q}_p$ fort. Es gilt weiterhin für $a \in \mathbb{Q}_p$, dass $|a|_p = p^{-\nu_p(a)}$.

Satz XI.11: *Die Menge $\mathbb{Q}_p$ ist bezüglich $|\cdot|_p$ vollständig, d. h. jede Cauchyfolge in $\mathbb{Q}_p$ konvergiert.*

Der Beweis geht genau wie für die reellen Zahlen durch.

Beispiel XI.12: Jede formale Reihe $\sum_{\nu=0}^{\infty} a_\nu p^\nu$ liefert als Folge ihrer Partialsummen $s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu$ eine Cauchyfolge in $\mathbb{Q}_p$, denn

$$|s_n - s_m| = \left| \sum_{\nu=m}^{n-1} a_\nu p^\nu \right|_p \leq \max\{|a_\nu p^\nu|_p \mid m \leq \nu \leq n-1\} \leq p^{-m}.$$

Insbesondere konvergiert jede formale Reihe in $\mathbb{Q}_p$.

Die Norm $|\cdot|_p$ induziert die Metrik $d_p(x,y) := |x-y|_p$ und so auch eine Topologie. Diese ist allerdings nicht so schön wie die von $\mathbb{R}$. So ist $\mathbb{Q}_p$ total unzusammenhängend.

Satz XI.13: *Der topologische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$ ist der Teilring*

$$\mathbb{Z}_p = \{x \in \mathbb{Q} \mid |x|_p \leq 1\}.$$

Beweis: Dass es sich bei $\mathbb{Z}_p$ um einen Teilring von $\mathbb{Q}_p$ handelt, folgt direkt aus $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ und $|x|_p|y|_p = |xy|_p$.

Per Definition ist $\mathbb{Z}_p$ abgeschlossen, da $|\cdot|_p$ stetig ist. Weiter ist $\mathbb{Z}$ enthalten in $\mathbb{Z}_p$, ist nämlich $a \in \mathbb{Z}$, dann ist $|a|_p = p^{-\nu_p} \leq 1$, und damit ist $\mathrm{cl}(\mathbb{Z}) \subseteq \mathbb{Z}_p$.

Sei umgekehrt $x \in \mathbb{Z}_p$. Es gebe eine Cauchyfolge $(x_n)_{n\in\mathbb{N}}$ in $(\mathbb{Q}, |\cdot|_p)$. Der einzige Häufungspunkt von $|\cdot|_p$ ist die Null. Folglich ist $|x|_p = 0$ oder es gibt dann eine Cauchyfolge $(x_n)_{n\in\mathbb{N}}$ in $(\mathbb{Q}, |\cdot|_p)$ mit $\lim_{n\to\infty} x_n = x$ und $|x| = |x_n| = |x_m|$ für ein geeignetes $n \in \mathbb{N}$ und jedes $m \geq n$. In jedem Fall ist $|x_m|_p \leq 1$ für alle $m \geq n$. Das heißt, dass $x_m \in \mathbb{Z}_{(p)}$ für $m \geq n$. Wir finden dann ein $y_n \in \mathbb{Z}$ mit $y_n \equiv x_n \pmod{p^n\mathbb{Z}_{(p)}}$. Damit ist $|x_n - y_n|_p \leq p^{-n}$ und so ist $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = x$. Damit gilt $x \in \mathrm{cl}(\mathbb{Z})$. □

Satz XI.14:

(i) *Es ist $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$.*

(ii) *Jedes Element $x \in \mathbb{Q}_p^\times$ hat eine eindeutige Darstellung $x = up^m$ mit $m = \nu_p(x)$ und $u \in \mathbb{Z}_p^\times$.*

Beweis: Aussage (i) bleibt dem Leser als Übung überlassen. Zu Aussage (ii): Es ist $m = \nu_p(x)$ eine ganze Zahl. Setzen wir $u := x \cdot p^{-m}$, dann ist

$$|u|_p = |x|_p \cdot |p^{-m}|_p = p^{-\nu_p(x)} \cdot p^m = 1.$$ □

Satz XI.15: *Die Ideale von $\mathbb{Z}_p$ sind genau die Hauptideale (0) und*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \nu_p(x) \geq n\}$$

für $n \geq 0$ und es ist $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Beweis: Sei $(0) \neq \mathfrak{a} \subseteq \mathbb{Z}_p$ ein Ideal und sei $x \in \mathfrak{a}$ derart, dass $\nu_p(x) = m$ mit m minimal ist. Ist nun $y \in \mathfrak{a}$, dann ist $\nu_p(y/x) = \nu_p(y) - \nu_p(x) \geq 0$ wegen der Minimalität von m. Damit ist $y/x \in \mathbb{Z}_p$. Damit ist $y = (y/x)x \in (x)$, d. h. $(x) = \mathfrak{a}$. Nach Satz XI.14(ii) ist $x = up^m$ mit $u \in \mathbb{Z}_p^\times$, also $\mathfrak{a} = (p^m)$.

Der Homomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$$

ist surjektiv. Ist nämlich $x \in \mathbb{Z}_p$ so gibt es, da $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ liegt, eine ganze Zahl a mit $|a - x|_p < 1/p^n$, d. h. $\nu_p(x - a) \geq n$ und damit gilt $x - a \in p^n\mathbb{Z}_p$ und $x \equiv a \pmod{p^n\mathbb{Z}_p}$. Weiter ist der Kern des Homomorphismus $p^n\mathbb{Z}$, sodass wir mit dem Homomorphiesatz $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ schließen können. □

Die Familie von Homomorphismen $\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z} \cong \mathbb{Z}/p^n\mathbb{Z}$ liefert einen Homomorphismus

$$\iota\colon \mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, \qquad x \longmapsto (x \pmod{p}, x \pmod{p^2}, \dots).$$

Tatsächlich ist ι sogar eine Isomorphie.

Satz XI.16: *Wir haben den Isomorphismus $\iota\colon \mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.*

Beweis: Es ist $x \in \ker \iota$ genau dann, wenn für alle $n \geq 0$ gilt, dass $x \in p^n\mathbb{Z}_p$. Das ist genau dann der Fall, wenn für alle $n \geq 0$ gilt, dass $\nu_p(x) \geq n$, was äquivalent ist zu $|x|_p \leq p^{-n}$. Das tritt genau dann ein, wenn $|x|_p = 0$, also wegen der Eigenschaften des Betrags genau dann, wenn $x = 0$.

Ein Element $y \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ ist eine Folge von Partialsummen $s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu$. Diese ist eine Cauchyfolge und konvergiert somit gegen $x = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$. Es ist

$$x - s_n = \sum_{\nu=n}^{\infty} a_\nu p^\nu \equiv 0 \pmod{p^n\mathbb{Z}_p},$$

d. h. $\iota(x) = (s_n)_{n\in\mathbb{N}} = y \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, was wir zeigen wollten. □

Bemerkung XI.17: Sei $\mathbb{Z}[[X]]$ der Ring der formalen Potenzreihen mit ganzen Koeffizienten. Es ist $\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X - P)$.

Kapitel XII.

Bewertungen

Definition XII.1: Eine *Bewertung eines Körpers* K ist eine Funktion $|\cdot|\colon K \to \mathbb{R}$ mit

(i) $|x| \geq 0$,

(ii) $|x| = 0$ genau dann, wenn $x = 0$,

(iii) $|xy| = |x||y|$,

(iv) $|x + y| \leq |x| + |y|$.

Sie liefert die Metrik $d := d_{|.|}$ mit $d_{|.|}(x, y) = |x-y|$ und macht so unseren Körper K zu einem metrischen Raum. Insbesondere ist K damit ein topologischer Raum.

Beispiel XII.2: (i) Seien K ein Zahlkörper und $\sigma\colon K \hookrightarrow \mathbb{C}$ eine Einbettung. Definieren wir $|x| := |\sigma(x)|$, dann liefert das eine Bewertung von K.

(ii) Seien $\mathcal{O}$ ein Dedekindring und $K = Q(\mathcal{O})$. Sind $\mathfrak{p} \subseteq \mathcal{O}_K$ prim und $q > 1$, dann definiert $|a|_{\mathfrak{p}} = q^{-\operatorname{ord}_{\mathfrak{p}}(a)}$ eine Bewertung auf K.

Ist K ein Zahlkörper und $\mathfrak{p} \subseteq \mathcal{O}_K$ prim, dann liefert $|a|_{\mathfrak{p}} = N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(a)}$ eine Bewertung auf K.

(iii) Sei K ein Körper. Dann heißt

$$|x| = \begin{cases} 0, & \text{falls } x = 0, \\ 1, & \text{sonst,} \end{cases}$$

die *triviale Bewertung von* K. Sie ist die einzige Bewertzung eines endlichen Körpers, da jedes von Null verschiedene Element eines endlichen Körpers eine Einheitswurzel ist.

Definition XII.3: Zwei Bewertungen $|\cdot|_1$, $|\cdot|_2$ des Körpers K heißen *äquivalent*, in Zeichen $|\cdot|_1 \sim |\cdot|_2$, falls sie die gleiche Topologie induzieren.

Satz XII.4: *Seien K ein Körper und $|\cdot|_1$, $|\cdot|_2$ Bewertungen auf K. Die Bewertungen sind äquivalent genau dann, wenn es ein $s > 0$ mit $|\cdot|_1 = |\cdot|_2^s$ gibt.*

Beweis: Die Implikation „$\Leftarrow$“ bleibt dem Leser zur Übung überlassen.

Für „$\Rightarrow$“: Seien $x \in K$ und $|\cdot|$ eine beliebige Bewertung. Es ist $\lim_{n\to\infty} x^n = 0$ genau dann, wenn $|x| < 1$. Also folgt aus $|\cdot|_1 \sim |\cdot|_2$, dass wenn $|x|_1 < 1$ auch $|x|_2 < 1$.

Gilt umgekehrt für $x \in K$ mit $|x|_1 < 1$ auch $|x_2| < 1$, dann ist $|\cdot|_1 \sim |\cdot|_2$. Sei dazu $y \in K$ fest mit $|y|_1 > 1$ und $x \in K^\times$. Es ist $|y|_1^\alpha = |x|_1$ für ein geeignetes $0 < \alpha \in \mathbb{R}$. Sei nun (n_i/m_i) mit $0 < m_i, n_i \in \mathbb{Z}$ eine rationale Folge, die von oben gegen α konvergieren. Dann ist

$$|x|_1 < |y|_1^\alpha < |y|_1^{m_i/n_i},$$

d. h. wir haben

$$1 > \frac{|x|_1}{|y|_1^{n_i/m_i}} \implies 1 > \frac{|x|_1^{m_i}}{|y|_1^{n_i}} = \left|\frac{x^{m_i}}{y^{n_i}}\right|_1 \implies 1 > \left|\frac{x^{m_i}}{y^{m_i}}\right| > \left|\frac{x^{m_i}}{y^{n_i}}\right|_2,$$

woraus wir $|y|_2^{n_i/m_i} > |x|_2$ gewinnen. Für $i \to \infty$ erhalten wir damit $|y|_2^\alpha \geq |x|_2$. Konvergiert n_i/m_i von unten gegen α, so erhalten wir mit den selben Argumenten $|y|_2^\alpha \leq |x|_2$. Insgesamt also $|y|_2^\alpha = |x|_2$.

Für alle $x \in K^\times$ haben wir damit

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\alpha_x \log|y|_1}{\alpha_x \log|y|_2} = \frac{\log|y|_1}{\log|y|_2} =: s,$$

d. h. $|x|_1 = |x|_2^s$. Aus $|y|_1 > 1$ folgt $|y|_2 > 1$, also $s > 0$. □

Satz XII.5 (Approximationssatz): *Seien K ein Körper, $|\cdot|_1, \ldots, |\cdot|_n$ paarweise nichtäquivalente Bewertungen von K und $a_1, \ldots, a_n \in K$ gegeben. Es gibt dann für alle $\varepsilon > 0$ ein $x \in K$, sodass $|x - a_i|_i < \varepsilon$ für $1 \leq i \leq n$.*

Lemma XII.6: *In der Situation des Approximationssatzes gibt es ein $z \in K$ mit $|z|_1 > 1$ und $|z|_j < 1$ für $2 \leq j \leq n$.*

Beweis: Wir zeigen die Aussage per Induktion nach n. Wir haben im Beweis von Satz XII.4 gesehen, dass $|\cdot|_1$ genau dann äquivalent zu $|\cdot|_2$ ist, wenn für alle $x \in K$ gilt: Ist $|x|_1$, so auch $|x|_2 < 1$.

Da $|\cdot|_1$ per Voraussetzung nicht äquivalent zu $|\cdot|_2$ ist, gibt es also $\alpha \in K$ mit $|\alpha|_1 < 1$ und $|\alpha| \geq 1$. Genauso gibt es $\beta \in K$ mit $|\beta|_1 \geq 1$ und $|\beta|_2 < 1$. Für $z := \beta/\alpha$ gilt

$$|z|_1 = \frac{|\beta|_1}{|\alpha|_1} > 1, \qquad |z|_2 = \frac{|\beta|_2}{|\alpha|_2} < 1,$$

das heißt wir haben unseren Kandidaten z gefunden.

Die Behauptung gelte jetzt bereits für $n-1$ Bewertungen. Nach Induktionsvoraussetzungen finden wir $y \in K$ mit $|y|_1 > 1$ und $|y|_j < 1$ für $2 \leq j \leq n-1$.

Ist $|y|_n < 1$, dann sind wir mit $z = y$ fertig.

Ist $|y|_n = 1$, so finden wir nach Induktionsvoraussetzung ein $w \in K$ mit $|w|_1 > 1$ und $|w|_n \leq 1$. Nun leistet $z := y^\ell w$ für ℓ ausreichend groß das Gewünschte.

Ist $|y|_n$ schließlich strikt größer als 1, so betrachten wir $t_m = y^m/(1+y^m)$. Es gilt

$$\lim_{m\to\infty} |t_m|_j = \begin{cases} 1, & \text{falls } j \in \{1, n\}, \\ 0, & \text{falls } 2 \leq j \leq n-1. \end{cases}$$

Für m groß genug und w wie im zweiten Fall ergibt sich damit

$$|wt_m|_j = |w|_j |t_m|_j = \begin{cases} > 1, & \text{falls } j = 1, \\ < 1, & \text{sonst}, \end{cases}$$

das heißt $z = wt_m$ genügt. □

Beweis (von Satz XII.5): Nach dem soeben bewiesenen Lemma finden wir für jedes i ein z_i, das beliebig nahe bei Eins liegt bezüglich $|\cdot|_i$ und sonst sehr nahe bei Null. Nun erfüllt $x = \sum_{i=1}^n a_i z_i$ die Bedingungen des Satzes. □

Definition XII.7: Seien K ein Körper und $|\cdot|$ eine Bewertung auf K. Die Bewertung $|\cdot|$ heißt *archimedisch*, falls $\{|n \cdot 1| \mid n \in \mathbb{N}\}$ unbeschränkt ist.

Satz XII.8: *Seien K ein Körper und $|\cdot|$ eine Bewertung auf K. Die Bewertung ist nicht archimedisch genau dann, wenn die verschärfte Dreiecksungleichung $|x+y| \leq \max\{|x|, |y|\}$ gilt.*

Beweis: „⇐“: Es gilt $|n| = |1 + \cdots + 1| \leq \max\{|1|\} = 1$.

„⇒“: Sei umgekehrt $|n| \leq N \in \mathbb{N}$ für alle $n \in \mathbb{N}$. Seien $x, y \in K$ mit $|x| \geq |y|$. Dann ist $|x|^\nu |y|^{\ell-\nu} \leq |x|^\ell$ für $0 \leq \nu \leq \ell$. Damit schätzen wir ab

$$|x+y|^\ell = |(x+y)^\ell| \leq \sum_{\nu=0}^{\ell} \left|\binom{\ell}{\nu}\right| |x^\nu y^{\ell-\nu}| \leq \sum_{\nu=0}^{\ell} \left|\binom{\ell}{\nu}\right| |x|^\ell \leq (\ell+1)N|x|^\ell.$$

Wegen der Monotonie der ℓ-ten Wurzel erhalten wir

$$|x+y| \leq (\ell+1)^{1/\ell} N^{1/\ell} |x| \overset{\ell\to\infty}{\longrightarrow} |x|,$$

womit wir $|x+y| \leq \max\{|x|,|y|\}$ gezeigt haben. □

Satz XII.9: *Jede nicht-triviale Bewertung auf $\mathbb{Q}$ ist äquivalent zu $|\cdot|_\infty$ oder $|\cdot|_p$ für $p \in \mathbb{P}$.*

Beweis: Sei $\|\cdot\|$ eine nicht archimedische Bewertung von $\mathbb{Q}$. Für jede natürliche Zahl n gilt $\|n\| = \|\sum_{i=1}^{n} 1\| \leq \|1\| = 1$. Es muss nun eine Primzahl p geben mit $\|p\| < 1$, da andernfalls für jede Primzahl p gelten würde, dass $\|p\| = 1$. Aber dann wäre $\|x\| \leq 1$ für alle $x \in \mathbb{Q}^\times$, und so wäre $\|\cdot\|$ trivial im Widerspruch zur Annahme. Für dieses p haben wir

$$p\mathbb{Z} \subseteq \mathfrak{a} = \{a \in \mathbb{Z} \mid \|a\| < 1\} \subsetneq \mathbb{Z},$$

und weil p maximal ist, ist $p\mathbb{Z} = \mathfrak{a}$.

Ist a eine ganze Zahl, dann gibt es $b \in \mathbb{Z}$ mit $\mathrm{ggT}(b,p) = 1$ und $a = bp^m$. Es ist $b \notin p\mathbb{Z} = \mathfrak{a}$, also ist $\|b\| = 1$ und $\|a\| = \|p\|^m = |p|^s$ mit $s = -\log\|p\|/\log p$, d. h. $\|\cdot\|$ ist äquivalent zu einer p-adischen Bewertung.

Seien nun $\|\cdot\|$ eine archimedische Bewertung und n, m positive natürliche Zahlen. Es ist $m = a_0 + a_1 n + \ldots a_r n^r$ mit $a_i \in \{0, \ldots, n-1\}$ und $n^r \leq m$, sodass

$$\|m\| \leq \sum_{i=0}^{r} \|a_i\| \|m\|^i \leq \sum_{i=0}^{r} \|a_i\| \|n\|^r \leq (r+1) n \|n\|^r \leq \left(1 + \frac{\log m}{\log n}\right) n \|n\|^{\log m/\log n}$$

wegen $r \leq \log m/\log n$. Ersetzen wir m durch m^k, dann erhalten wir

$$\|m^k\| \leq \left(1 + k\frac{\log m}{\log n}\right) n \|n\|^{k\cdot(\log m/\log n)}.$$

Wegen der Monotonie der k-ten Wurzel liefert das

$$\|x\| \leq (1 + k(\log m/\log n))^{1/k} n^{1/k} \|n\|^{\log m/\log n}.$$

Für $k \to \infty$ ergibt sich damit $\|m\| \leq \|n\|^{\log m/\log n}$, d. h.

$$\|m\|^{\frac{1}{\log m}} \leq \|n\|^{\frac{1}{\log n}}.$$

Vertauschen der Rollen von m und n liefert $\|m\|^{1/\log m} = \|n\|^{1/\log n}$. Also ist $\|n\|^{1/\log n} = c \in \mathbb{R}$ konstant für alle $n \in \mathbb{N}$. Mit $s = \log c$ gilt für alle $n \in \mathbb{N}$, dass $\|n\| = c^{\log n} = (\exp(s))^{\log n} = n^s$. Es gilt also für alle $z = a/b \in \mathbb{Q}$, dass $\|z\| = \|a/b\| = |a/b|_\infty^s = |z|_\infty^s$. Damit ist $\|\cdot\|$ äquivalent zum gewöhnlichen Betrag. □

Definition XII.10: Sei $|\cdot|$ eine nicht archimedische Bewertung des Körpers K. Die zu $|\cdot|$ gehörende Exponentialbewertung von K ist

$$r\colon K \longrightarrow \mathbb{R} \cup \{\infty\}, \qquad \nu(x) = \begin{cases} -\log|x|, & \text{falls } x \neq 0, \\ \infty, & \text{falls } x = 0. \end{cases}.$$

Es gelten

(i) $\nu(x) = \infty$ genau dann, wenn $x = 0$,

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

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

wobei wir für $a \in \mathbb{R}$ definieren, dass $a + \infty = \infty$ und außerdem $\infty + \infty = \infty$. Aus (iii) folgt: Sind x und y Elemente von K mit $|x| \neq |y|$, dann ist $|x + y| = \max\{|x|, |y|\}$. Ist umgekehrt ν eine Exponentialbewertung und ist $q > 1$, dann ist $|x| = q^{-\nu(x)}$ eine gewöhnliche Bewertung.

Zwei Exponentialbewertungen ν_1, ν_2 sind äquivalent genau dann, wenn $\nu_1 = s\nu_2$ mit $s \in \mathbb{R}$.

Beispiel XII.11: Sei $K = \mathbb{F}_q(t)$, wobei $q = p^n$ mit p prim und n natürliche Zahl. Zu einem irreduziblen Polynom $f \in \mathbb{F}_q[t]$ erhalten wir die Exponentialbewertung

$$\nu_f(g) = \nu, \quad \text{falls } g = f^\nu \frac{h_1}{h_2} \quad \text{mit } h_1, h_2 \in \mathbb{F}_q[t] \text{ und } f \nmid h_1 h_2.$$

Dies ist die uns vertraute Bewertung $\nu_{(f)}$ des Dedekindrings $\mathbb{F}_q[t]$. Die zugehörige Betragsbewertung ist

$$|g|_f = g^{d_f^{\nu_f(g)}},$$

wobei $d_f = \deg f = [\mathbb{F}_q[t]/(f) : \mathbb{F}_q]$. Für $f = t - a$ gibt ν_f genau die Nullstellen- beziehungsweise Polordnung der eingesetzten Funktion in a zurück.

Eine weitere Bewertung liefert

$$\nu_\infty\colon \mathbb{F}_q(t) \longrightarrow \mathbb{Z} \cup \{\infty\}, \qquad \nu_\infty\left(\frac{g}{h}\right) = \deg(g) - \deg(h).$$

Die zugehörige Betragsbewertung ist $|f|_\infty = q^{-\nu_\infty(f)}$. Dies ist die zum Ideal $(1/t)$ des Ringes $\mathbb{F}_q[1/t] \subseteq \mathbb{F}_q(t)$ gehörige Bewertung. Es gilt

$$\prod_{\mathfrak{p}} |f|_{\mathfrak{p}} = 1,$$

wobei $\mathfrak{p}$ die Primideale von $\mathbb{F}_q[t]$ und das Symbol ∞ durchläuft.

Satz XII.12: *Sei $(K, |\cdot|)$ ein bewerteter Körper. Es ist*

$$\mathcal{O} = \{x \in K \mid \nu(x) \geq 0\} = \{x \in K \mid |x| \leq 1\}$$

ein Ring mit $\mathcal{O}^\times = \{x \in K \mid \nu(x) = 0\} = \{x \in K \mid |x| = 1\}$. Dieser Ring hat das maximale Ideal $\mathfrak{p} = \{x \in K \mid \nu(x) > 0\} = \{x \in K \mid |x| < 1\}$.

Der Beweis ist Routine.

Satz XII.13: *Sei $(K, |\cdot|)$ ein diskret bewerteter Körper. Dann ist $\mathcal{O}$ ein Hauptidealbereich, also ein diskreter Bewertungsring. Ist ν außerdem normiert, so sind $\mathfrak{p}^n = \{x \in K \mid \nu(x) \geq n\} = \pi^n\mathcal{O}$ mit $n \geq 0$ und $\pi \in \mathcal{O}$ prim, d. h. $\nu(\pi) = 1$, genau die Ideale von $\mathcal{O}$. Es ist weiter $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.*

Beweis: Ohne Beschränkung der Allgemeinheit dürfen wir ν als normiert annehmen. Sei $\pi \in \mathcal{O}$ mit $\nu(\pi) = 1$. Ist nun $a \in \mathcal{O}$, so ist $\nu(a\pi^{-\nu(\pi)}) = 0$; das Element $u := a\pi^{-\nu(\pi)}$ ist also eine Einheit und $a = u\pi^m$ für $m := \nu(\pi)$.

Ist jetzt $\mathfrak{a}$ ein Ideal von $\mathcal{O}$ und $a \in \mathfrak{a}$ ein Element mit minimaler Bewertung, so ist jedes $b \in \mathfrak{a}$ von der Form $(b/a)a \in (\pi^m)$, denn $b/a \in \mathcal{O}$. Also ist $\mathfrak{a} = (\pi^m)$. Die Wahl von π liefert den Isomorphismus

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{p}, \qquad u \cdot \pi^n + \mathfrak{p}^{n+1} \longmapsto u \pmod{\mathfrak{p}}. \qquad \square$$

In einem diskret bewerteten Körper ist $\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \ldots$ eine Umgebungsbasis von $0 \in K$, d. h. jede offene Umgebung U der Null enthält ein $\mathfrak{p}^n$ für ausreichend großes n. Entsprechend ist $\mathcal{O}^\times \supseteq 1 + \mathfrak{p} \supseteq 1 + \mathfrak{p}^2 \supseteq \ldots$ eine Umgebungsbasis der 1 bestehend aus den Untergruppen $1 + \mathfrak{p}^n$ von $\mathcal{O}^\times$. Sind nämlich $x, y \in \mathfrak{p}^n$, so ist

$$(1 + x)(1 + y) = 1 + x + y + xy \in 1 + \mathfrak{p}^n$$

und

$$\frac{1}{1 - x} \equiv 1 + x + \cdots + x^{n-1} \pmod{\mathfrak{p}^n},$$

d. h. $(1 - x)^{-1} \in 1 + (x + \cdots + x^{n-1}) + \mathfrak{p}^n \subseteq 1 + \mathfrak{p}^n$.

Satz XII.14:

(i) $\mathcal{O}^\times/(1 + \mathfrak{p}^n) \cong (\mathcal{O}/\mathfrak{p}^n)^\times$,

(ii) $1 + \mathfrak{p}^n/1 + \mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ *für* $n \geq 1$.

Beweis: (i) Wir betrachten den Homomorphismus

$$\mathcal{O}^\times \longrightarrow (\mathcal{O}/\mathfrak{p}^n)^\times, \qquad u \longmapsto u + \mathfrak{p}^n.$$

Er ist surjektiv, da $u + \mathfrak{p}^n$ genau dann eine Einheit ist, wenn u nicht in $\mathfrak{p}$ enthalten ist, d. h. $u \in \mathcal{O}^\times = \mathcal{O} - \mathfrak{p}$. Sein Kern ist $1 + \mathfrak{p}^n$.

(ii) Die Aussage ergibt sich nach Wahl eines Primelementes $\pi \in \mathcal{O}$ durch den Homomorphiesatz und den surjektiven Homomorphismus

$$1 + \pi^n\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}, \qquad 1 + \pi^n a \longmapsto a + \mathfrak{p},$$

dessen Kern $1 + \mathfrak{p}^{n+1}$ ist. □

Kapitel XIII.

Komplettierungen

Definition XIII.1: Ein bewerteter Körper $(K, |\cdot|)$ heißt *vollständig*, falls jede Cauchyfolge in K konvergiert.

Definition XIII.2: Seien $(K, |\cdot|)$ ein bewerteter Körper, R der Ring der Cauchyfolgen und $\mathfrak{m}$ das maximale Ideal der Nullfolgen. Dann heißt $(\hat{K}, |\cdot|)$ mit $\hat{K} := R/\mathfrak{m}$ und $|\cdot|$ stetig fortgesetzt die *Komplettierung von* $(K, |\cdot|)$.

Satz XIII.3: *Sei $(K, |\cdot|)$ ein bewerteter Körper. Dann gilt:*

(i) *$(\hat{K}, |\cdot|)$ ist vollständig,*

(ii) *Die Komplettierung ist eindeutig.*

Beweis: Aussage (i) zeigt man wie für $(\mathbb{Q}, |\cdot|_\infty)$.

Zu Aussage (ii): Ist $(\hat{K}', |\cdot|')$ ein weiterer vollständiger Körper, der $(K, |\cdot|)$ als dichten Teilkörper enthält, so definieren wir $\sigma\colon \hat{K} \to \hat{K}'$ wie folgt: Schreibe $a \in \hat{K}$ als Grenzwert einer Cauchyfolge $(a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$. Da $|\cdot|'$ und $|\cdot|$ auf K übereinstimmen, ist $(a_n)_{n\in\mathbb{N}}$ auch eine Cauchy-Folge bezüglich $|\cdot|'$ und $\sigma(a) \in K'$ definiert als der Grenzwert von a_n bezüglich $|\cdot|'$. Es gilt

$$|a| = \lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |a_n|' = |\sigma(a)|. \qquad \square$$

Satz XIII.4: *Sei $(K, |\cdot|)$ ein vollständiger Körper. Ist $|\cdot|$ archimedisch, so gibt es einen Isomorphismus σ von K nach $\mathbb{R}$ oder $\mathbb{C}$ mit $|\sigma(a)| = |a|^s$ für alle $a \in K$ mit einem festen $s > 0$.*

Beweis: Nach Satz XII.8 ist $|\cdot||_{\mathbb{Q}}$ äquivalent zum gewöhnlichen Betrag $|\cdot|_\infty$. Ohne Beschränkung der Allgemeinheit sei $|\cdot||_{\mathbb{Q}} = |\cdot|_\infty$. Sei $\hat{\mathbb{Q}}$ der Abschluss von $\mathbb{Q}$ in K. Dann ist $(\hat{\mathbb{Q}}, |\cdot|)$ eine Komplettierung von $(\mathbb{Q}, |\cdot|_\infty)$. Diese ist eindeutig

nach dem eben gezeigten, d. h. es gibt einen Isomorphismus $\sigma\colon \hat{\mathbb{Q}} \to \mathbb{R}$ mit $|\sigma(a)| = |a|_\infty$. Ohne Beschränkung der Allgemeinheit können wir also annehmen, dass $(\mathbb{R}, |\cdot|) \subseteq (K, |\cdot|)$.

Zum Beweis, dass $K = \mathbb{R}$ oder $K = \mathbb{C}$ zeigen wir, dass jedes $\beta \in K$ einer quadratischen Gleichung genügt. Betrachte dazu die Abbildung

$$f\colon \mathbb{C} \longrightarrow \mathbb{R}, \qquad z \longmapsto |\beta^2 - (z + \bar{z})\beta + z\bar{z}|.$$

Aus $\lim_{z\to\infty} f(z) = \infty$ folgt, dass f ein Minimum m auf $\mathbb{C}$ annimmt und $M = \{z \in \mathbb{C} \mid f(z) = m\} \neq \varnothing$ beschränkt und abgeschlossen ist. Es gibt also $z_0 \in M$ mit $|z_0| \geq |z|$ für jedes $z \in M$. Es genügt nun $m = 0$ zu zeigen, da sogleich $\beta^2 - (z_0 + \bar{z}_0)\beta + z_0\bar{z}_0 = 0$ folgt.

Angenommen es wäre $m > 0$. Dann fänden wir $0 < \varepsilon < m$, wir könnten die Funktion g erklärt durch

$$g(x) = x^2 + (z_0 + \bar{z}_0)x + z_0\bar{z}_0 + \varepsilon = (x - z_1)(x - \bar{z}_1) = x^2 - (z_1 + \bar{z}_1) + z_1\bar{z}_1$$

betrachten und fänden $|z_0| + \varepsilon = |z_1|$, d. h. $|z_0| < |z_1|$ und damit $z_1 \notin M$. Insgesamt hätten wir dann $f(z_1) > m$. Seien nun n eine natürliche Zahl und G erklärt durch

$$G(x) = (g(x) - \varepsilon)^n - (-\varepsilon)^n = \prod_{i=1}^{2n}(x - \alpha_i) = \prod_{i=1}^{2n}(x - \bar{\alpha}_i)$$

mit geeigneten $\alpha_i \in \mathbb{C}$. Also ist

$$G(z_1) = (g(z_1) - \varepsilon)^n - (-\varepsilon)^n = (-\varepsilon)^n - (-\varepsilon)^n = 0.$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $z_1 = \alpha_1$. Dann ist

$$|G(x)|^2 = \Big|\prod_{i=1}^{2n}(x - \alpha_i)\prod_{i=1}^{2n}(x - \bar{\alpha}_i)\Big| = \prod_{i=1}^{2n}|x^2 - (\alpha_i + \bar{\alpha}_i)x + \alpha_i\bar{\alpha}_i|$$

Jetzt haben wir wegen $\alpha_1 = z_1$ und $m = \min\{f(z) \mid z \in \mathbb{C}\}$, dass

$$|G(\beta)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(z_1)m^{2n-1}$$

und wir haben die Abschätzung

$$|G(\beta)| \leq |\beta^2 + (z_0 + \bar{z}_0)\beta + z_0\bar{z}_0| + |\varepsilon|^n = f(z_0)^n + |\varepsilon|^n = m^n + \varepsilon^n,$$

d. h. wir haben insgesamt $f(z_1)m^{2n-1} \leq |G(\beta)|^2 \leq (m^n + \varepsilon^n)^2$. Das formen wir um und erhalten

$$\frac{f(z_1)}{m} \leq \left(1 + \left|\frac{\varepsilon}{m}\right|^2\right) \overset{n\to\infty}{\longrightarrow} 1,$$

d. h. $f(z_1) \leq m$ im Widerspruch dazu, dass $f(z_1)$ kein Minimum ist. □

Ist ν eine zu $|\cdot|$ gehörige Exponentialbewertung, so setzt sich ν stetig zu $\hat{\nu}$ auf $\hat{K}$ fort. Ist $a = \lim_{n\to\infty} a_n$, so ist $\hat{\nu}(a - a_n) > \nu(a)$ für ausreichend große n. Damit folgt, dass $\nu(a_n) = \hat{\nu}(a_n - a + a) = \min\{\hat{\nu}(a_n - a), \hat{\nu}(a)\} = \hat{\nu}(a)$ für ausreichend große n. Die Folge $(\nu(a_n))_{n\in\mathbb{N}}$ wird also stationär und es folgt $\hat{\nu}(\hat{K}) = \nu(K)$. Die Fortsetzung $\hat{\nu}$ ist genau dann normiert und diskret, wenn ν normiert und diskret ist.

Korollar XIII.5: *Sind $\mathcal{O}$ und $\hat{\mathcal{O}}$ die zugehörigen Bewertungsringe mit maximalen Idealen $\mathfrak{p}$ beziehungsweise $\hat{\mathfrak{p}}$, so gilt*

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}.$$

Ist weiter ν diskret, so gilt $\hat{\mathcal{O}}/\hat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n$.

Beweis: Wir zeigen die Aussage auf dieselbe Weise wie wir gezeigt haben, dass $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Wir betrachten

$$\varphi\colon \mathcal{O} \longrightarrow \hat{\mathcal{O}}/\hat{\mathfrak{p}}, \qquad x \longmapsto x + \hat{\mathfrak{p}}.$$

Es ist $x \in \ker\varphi$ genau dann, wenn $x \in \hat{\mathfrak{p}}$. Das ist äquivalent zu $\hat{\nu}(x) > 0$, was genau dann eintritt, wenn $\nu(x) > 0$, also genau dann, wenn $x \in \mathfrak{p}$.

Weiter ist φ surjektiv, da $\mathcal{O}$ dicht in $\hat{\mathcal{O}}$ liegt, es also zu $x \in \hat{\mathcal{O}}$ ein $a \in \mathcal{O}$ gibt mit $|x - a| < 1$, also $\nu(x - a) > 0$. Nun ist $x = a + (x - a) \equiv a \pmod{\mathfrak{p}}$.

Der Beweis der zweiten Aussage bleibt dem Leser als Übungsaufgabe überlassen. □

Satz XIII.6: *Seien $R \subseteq \mathcal{O}$ ein Repräsentantensystem für $K = \mathcal{O}/\mathfrak{p}$, $0 \in R$ und $\pi \in \mathcal{O}$ ein Primelement. Dann lässt sich jedes $x \in \hat{K}^\times$ eindeutig als konvergente Laurentreihe in π schreiben, d. h. $x = \sum_{n=m}^{\infty} a_n\pi^n$ mit $a_i \in R$, $a_m \neq 0$ und $m \in \mathbb{Z}$.*

Beweis: Schreibe $x = \pi^m u$ mit $u \in \mathcal{O}^\times$. Wegen $\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$ hat $u \pmod{\hat{\mathfrak{p}}}$ einen eindeutigen Repräsentanten $a_0 \in R - \{0\}$. Damit ist $u = a_0 + \pi b_1$ mit $b_1 \in \hat{\mathcal{O}}$. Sind $a_0, \ldots, a_{n-1} \in R$ mit $u = a_0 + a_1\pi + \ldots a_{n-1}\pi^{n-1} + \pi^n b_n$, wobei $\pi^n b_n \in \hat{\mathcal{O}}$, bereits gefunden und eindeutig, so ist auch $a_n \in R$ durch $a_n \equiv b_n$

(mod $\pi\hat{\mathcal{O}}$) eindeutig bestimmt, da $\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$. Es ist also $b_n = a_n + \pi b_{n+1}$ und so

$$u = a_0 + \cdots + a_n\pi^n + b_{n+1}\pi^{n+1}.$$

Induktiv finden wir eine eindeutig bestimmte Reihe $\sum_{\nu=0}^{\infty} a_\nu \pi^\nu$. Sie konvergiert gegen u, da das Restglied $\pi^{n+1}b_{n+1}$ gegen Null konvergiert. □

Beispiel XIII.7: (i) Für $(\hat{K}, |\cdot|) = (\mathbb{Q}_p, |\cdot|_p)$ und $R = \{0, \ldots, p-1\}$ erhalten wir die uns vertraute p-adische Entwicklung.

(ii) Für $(\hat{K}, |\cdot|) = (\hat{K}(t), |\cdot|_{(t)})$ können wir $R = K$ wählen und erhalten eine Darstellung $\sum_{i=m}^{\infty} a_i t^i$, wobei $a_i \in K$ und $m \in \mathbb{Z}$, als formale Laurentreihe.

Definition XIII.8: Sei $(K, |\cdot|)$ ein diskret bewerteter Körper mit Bewertungsring $\mathcal{O}$. Der projektive Limes ist

$$\varprojlim_{n\to\infty} \mathcal{O}/\mathfrak{p}^n = \Big\{(x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n : x_{n+1} \equiv x_n \pmod{\mathfrak{p}^n}\Big\}.$$

Satz XIII.9: *Sei $(K, |\cdot|)$ ein vollständig diskret bewerteter Körper. Dann ist*

$$\mathcal{O} \cong \varprojlim_{n\to\infty} \mathcal{O}/\mathfrak{p}^n \quad \textit{vermöge} \quad x \longmapsto (x \pmod{\mathfrak{p}^n})_n.$$

Beweis: Der Kern der Abbildung ist $\bigcap_{n\geq 1} \mathfrak{p}^n = (0)$, also ist die Abbildung injektiv. Für die Surjektivität seien $\mathfrak{p} = \pi\mathcal{O}$ und R ein Repräsentantensystem von $\mathcal{O}/\mathfrak{p}$. Wir haben gesehen, dass jedes Element $\mathcal{O}/\mathfrak{p}^n$ durch $a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \pmod{\mathfrak{p}^n}$ mit geeigneten $a_i \in R$ eindeutig dargestellt ist. Jedes Element $s \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ ist somit durch eine Folge von Summen $s_n = \sum_{i=0}^{n-1} a_i\pi^i$ mit gleichbleibenden Koeffizienten a_i aus R geegeben. Es ist das Bild des Elementes

$$x = \lim_{n\to\infty} s_n = \sum_{\nu=0}^{\infty} a_\nu \pi^\nu \in \mathcal{O}.$$

□

Bemerkung XIII.10: Wir verstehen $\mathcal{O}/\mathfrak{p}^n$ mit der diskreten Topologie und $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ mit der Produkttopologie.

Eine Basis der Produkttopologie auf $\prod_{i\in I} X_i$ ist durch die Mengen der Bauart $\prod_{i\in I} U_i$ mit $U_i \subseteq X_i$ offen und $U_i \neq X_i$ nur für endlich viele i gegeben.

Der projektive Limes wird so zu einer abgeschlossenen Teilmenge des Produktes und mit der Teilraumtopologie zu einem topologischen Ring (d. h. die Ringverknüpfungen sind stetig bezüglich der Teilraumtopologie). Weiter wird $\mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ ein Homöomorphismus.

Lemma XIII.11: *Sei $|\cdot|$ eine nicht-archimedische Bewertung eines Körpers K. Ist $|x| \neq |y|$, dann ist $|x+y| = \max\{|x|, |y|\}$.*

Beweis: Die verschärfte Dreiecksungleichung sagt $|x+y| \leq \max\{|x|, |y|\}$. Wir nehmen an $|x| > |y|$. Dann haben wir

$$|x| = |x+y-y| \leq \max\{|x+y|, |y|\} \leq |x|;$$

also ist $|x| = \max\{|x+y|, |y|\}$ und wegen $|x| > |y|$ folgt $|x| = |x+y|$. □

Im Folgenden sei $(K, |\cdot|)$ ein nicht-archimedisch bewerteter Körper.

Lemma XIII.12: *Die Bewertung $|\cdot|$ lässt sich durch*

$$\Big|\sum_{i=0}^{n} a_i X^i\Big| = \max\{|a_i| \mid 0 \leq i \leq n\}$$

mit $a_i \in K$ zu einer Bewertung auf $K[X]$ fortsetzen.

Beweis: Sei $f \in K[X]$. Dass f genau dann das Nullpolynom ist, wenn $|f| = 0$ und $|f+g| \leq \max\{|f|, |g|\}$, ist klar. Für $|fg| = |f||g|$ folgen wir dem Beweis des Gauß-Lemmas für Polynome mit ganzen Koeffizienten und erinnern uns an Lemma XIII.11. Seien also $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$. Dann ist

$$fg = \sum_{k=0}^{n+m} c_k X^k \quad \text{wobei} \quad c_k = \sum_{\ell=0}^{k} a_\ell b_{k-\ell}.$$

Offenbar ist $|c_k| \leq |f||g|$, d. h. $|fg| \leq |f||g|$.

Für die andere Ungleichung seien i, j minimal mit $|a_i| = |f|$ und $|b_j| = |g|$. Dann ist $c_{i+j} = \sum_{\ell=0}^{i+j} a_\ell b_{(i+j)-\ell}$ mit $|a_\ell| < |a_i|$ für $\ell < i$ und $|b_{(i+j)-\ell}| < |b_j|$ für $\ell > i$ erhalten wir

$$|a_\ell b_{(i+j)-\ell}| = \begin{cases} |a_i b_j| - \varepsilon, & \text{falls } \ell \neq i, \\ |a_i b_j| = |f||g|, & \text{für } \ell = i \end{cases}$$

mit geeignetem $\varepsilon > 0$. Also ist $|c_{i+j}| = |f||g|$ und es folgt $|f||g| \leq |fg|$. □

Definition XIII.13: Seien $\mathcal{O}$ der Bewertungsring von K, $\mathfrak{p}$ sein maximales Ideal und $K = \mathcal{O}/\mathfrak{p}$. Ein Polynom $f \in \mathcal{O}[X]$ heißt *primitiv*, falls $|f| = 1$. Äquivalent: $f \not\equiv 0 \pmod{\mathfrak{p}}$.

Lemma XIII.14 (Hensels Lemma): *Seien $(K, |\cdot|)$ vollständig und $|\cdot|$ nicht archimedisch. Sei weiterhin $f \in \mathcal{O}[X]$ primitiv. Lässt sich f schreiben als $f \equiv \bar{g}\bar{h} \pmod{\mathfrak{p}}$ mit $\bar{g}, \bar{h} \in K[X]$ teilerfremd, dann gibt es $g, h \in \mathcal{O}[X]$ mit $\deg g = \deg \bar{g}$, $g \equiv \bar{g} \pmod{\mathfrak{p}}$, $h \equiv \bar{h} \pmod{\mathfrak{p}}$ und $f = gh$.*

Beweis: Wir setzen $d := \deg f$ und $m := \deg \bar{g}$. Damit haben wir die Abschätzung $\deg \bar{h} = \deg \bar{f} - \deg g \leq d - m$ für den Grad von $\bar{h}$. Seien $g_0, h_0 \in \mathcal{O}[X]$ mit $g_0 \equiv \bar{g} \pmod{\mathfrak{p}}$, $h_0 \equiv \bar{h} \pmod{\mathfrak{p}}$ mit $m = \deg g_0$ und $\deg h_0 \leq d - m$. Da $\bar{g}$ und $\bar{h}$ teilerfremd sind, gibt es Polynome $a, b \in \mathcal{O}[X]$ mit $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$. Unter den Koeffizienten von $f - gh$, $ag_0 + bh_0 - 1 \in \mathfrak{p}[X]$ wähle einen mit kleinstem Betrag und nenne ihn π.

Wir setzen an, dass $g = g_0 + \pi p_1 + \pi^2 p_2 + \dots$ und $h = h_0 + \pi q_1 + \pi^2 q_2 + \dots$ mit geeigneten Polynomen $p_i, q_i \in \mathcal{O}[X]$, die $\deg p_i < n$ und $\deg q_i \leq d - m$ leisten.

Angenommen, wir haben

$$g_{m-1} = g_0 + \pi p_1 + \pi^2 p_2 + \dots + \pi^{n-1} p_{n-1}, \qquad h_{n-1} = h_0 + \pi q_1 + \pi^2 q_2 + \dots + \pi^{n-1} q_{n-1}$$

mit $f \equiv g_{n-1} h_{n-1} \pmod{\pi^n}$ bereits gefunden. Per Ansatz ist $g_n = g_{n-1} + p_n \pi^n$ und $h_n = h_{n-1} + q_n \pi^n$. Einsetzen dieser Gleichungen in $f \equiv g_n h_n$ liefert

$$\begin{aligned} f \equiv g_n h_n &= g_{n-1} h_{n-1} + (g_{n-1} q_n + h_{n-1} p_n)\pi^n + \pi^{2n}(p_n \cdot q_n) \\ &\equiv g_{n-1} h_{n-1} + (g_{n-1} q_n + h_{n-1} p_n)\pi^n \pmod{\pi^{n+1}} \end{aligned}$$

was äquivalent ist zu

$$\pi^{-n}(f - g_{n-1} h_{n-1}) \equiv g_{n-1} q_n + h_{n-1} p_n \equiv g_0 q_n + h_0 p_n \pmod{\pi}.$$

Setze jetzt $f_n := f - g_{n-1} h_{n-1}$. Es gilt $f_n \in \mathcal{O}[X]$. Wir suchen nach der obigen Gleichung also p_n und q_n in $\mathcal{O}[X]$ mit

$$f_n \equiv g_0 q_n + h_0 p_n \equiv \pi,$$

sodass weiterhin die Bedinungen an die Grade von p_n, q_n erfüllt ist. Es ist

$$f_n = 1 f_n \equiv (g_0 a + h_0 b) f_n \equiv g_0 (a f_n) + h_0 (b f_n) \pmod{\pi}.$$

Nach Division mit Rest finden wir $b f_n = q g_0 + r$ mit $\deg r < \deg g_0 = m$. Wegen $g_0 \equiv \bar{g} \pmod{\mathfrak{p}}$ und $\deg g_0 = \deg \bar{g}$ ist der höchste Koeffizient von g_0 nicht in $\mathfrak{p}$, also ist er in $\mathcal{O}^\times$. Es folgt $q \in \mathcal{O}[X]$. Setzen wir $r := p_n$, dann finden wir

$$f_n \equiv g_0 a f_n + h_0 (q g_0 + p_n) \equiv g_0 (a f_n + h_0 q) + h_0 p_n \pmod{\pi}.$$

Streichen wir aus $af_n + h_0 q$ alle durch π teilbaren Koeffizienten heraus, dann erhalten wir ein Polynom $q_n \equiv af_n + qh_0 \pmod{\pi}$ mit

$$f_n \equiv g_0 q_n + h_0 p_n \pmod{\pi}.$$

Es ist $\deg g_0 q_n = \deg(f_n - h_0 p_n) \leq d$, also ist $\deg q_n \leq d - m$ wie gefordert. Wir schließen mit $g = \lim_{n\to\infty} g_n$, $h = \lim_{n\to\infty} h_n$. □

Beispiel XIII.15: Wir betrachten $X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Dieses Polynom zerfällt in $\mathbb{F}_p$ in verschiedene Linearfaktoren, was es uns erlaubt, das Henselsche Lemma anzuwenden. Damit zerfällt $X^{p-1} - 1$ auch in $\mathbb{Z}_p[X]$ in Linearfaktoren. Der Ring $\mathbb{Z}_p$ enthält also die $(p-1)$-ten Einheitswurzeln.

Bemerkung XIII.16: Die Bedingung zur Teilerfremdheit von $\bar{g}$ und $\bar{h}$ lässt sich abschwächen zum Preis einer besseren Startapproximation. Genauer: Seien $f, g_0, h_0 \in \mathcal{O}[X]$ und f normiert. Gilt $|f - g_0 h_0| < |\mathrm{Res}(g_0, h_0)|^2$, so gibt es g und h in $\mathcal{O}[X]$ mit $gh = f$ sowie $\deg g = \deg g_0$ und $\deg h = \deg h_0$. Es genügt sogar $|f - g_0 h_0| < |\mathrm{disk}(f)|$.

Dies liefert einen Algorithmus zur Faktorisierung in $\mathbb{Q}_p[X]$: Gegeben ein Polynom f, berechne $\mathrm{disk}(f)$. Ist sie Null, so haben f und f' einen gemeinsamen Faktor. Diesen finden wir mit dem euklidischen Algorithmus. Andernfalls ist $\nu_p(\mathrm{disk}(f)) = m \geq 0$ und es genügt f im endlichen Ring $\mathbb{Z}/p^m\mathbb{Z}$ zu faktorisieren.

Dies liefert auch einen Algorithmus zur Faktorisierung in $\mathbb{Q}[X]$. Zunächst wird die (feinere) Faktorisierung in $\mathbb{Q}_p[X]$ berechnet. Im nächsten Schritt sucht man nach Faktoren, deren Produkt in $\mathbb{Q}[X]$ liegt. Diese ergeben die Primfaktorzerlegung in $\mathbb{Q}[X]$.