# LÖSUNGSHINWEISE BLATT 14
# ALGEBRAISCHE ZAHLENTHEORIE

## Aufgabe 14.1

*Zeigen Sie, daß die Gleichung $a^2 - 47b^2 = \pm 19$ unendlich viele Lösungen in den ganzen Zahlen hat.*

Die Grundidee für die Diskussion dieser Gleichung ist: Die Existenz einer Lösung ist äquivalent zur Existenz eines Elements mit Norm 19, welche aus der Trivialität der Klassengruppe folgt. Die Existenz unendlich vieler Elemente folgt dann aus dem Einheitensatz. Dazu betrachtet man den Zahlkörper $K = \mathbb{Q}(\sqrt{47})$.

(a) $K$ ist reell, also ist $r_1 = 2$, $r_2 = 0$, $n = 2$. Die Diskriminante ist $d = 4 \cdot 47$. Damit ist die Minkowski-Schranke $\sqrt{47}$. In jeder Idealklasse liegt also ein ganzes Ideal mit Norm $\leq \sqrt{47} \sim 6.85$. Es müssen also alle Ideale bestimmt werden, die Norm $\leq 6$ haben.

Es gilt $47 \equiv 3 \mod 4$, also ist $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - 47)$. Wir faktorisieren die Primzahlen 2, 3 und 5.

Für die Primzahl 2 haben wir

$$\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 - 1) \cong \mathbb{F}_2[X]/(X + 1)^2,$$

also ist 2 verzweigt. Es gibt ein Primideal von $\mathcal{O}_K$, das über 2 liegt, nämlich $(2, \sqrt{47} + 1)$.

Für die Primzahl 3 haben wir

$$\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^2 - 2) \cong \mathbb{F}_9,$$

also ist 3 träge.

Für die Primzahl 5 haben wir

$$\mathcal{O}_K/(5) \cong \mathbb{F}_5[X]/(X^2 - 2),$$

also ist auch 5 träge.

Es gibt also nur zwei Ideale mit Norm $\leq 6$, nämlich $(2, \sqrt{47} + 1)$ mit Norm 2 und $(2)$ mit Norm 4.

(b) Wir müssen nur noch zeigen, daß das Ideal $(2, \sqrt{47} + 1)$ ein Hauptideal ist – wir suchen also ein Element mit Norm 2. Das Element $7 + \sqrt{47}$ hat Norm 2, also ist $(2, \sqrt{47} + 1) = (7 + \sqrt{47})$. Analog zum Beweis von Satz 8.13 folgt damit, daß die Klassenzahl von $\mathbb{Q}(\sqrt{47})$ gleich 1 ist.

(c) Wir faktorisieren das Ideal $(19)$ in $\mathcal{O}_K$. Es gilt

$$\mathcal{O}_K/(19) \cong \mathbb{F}_{19}[X]/(X^2 - 9) \cong \mathbb{F}_{19}[X]/(X + 3) \times \mathbb{F}_{19}[X]/(X - 3).$$

Es gibt also zwei Primideale, die über $(19)$ liegen, nämlich $(19, \sqrt{47} + 3)$ und $(19, \sqrt{47} - 3)$.

(d) Aus (b) folgt, daß die beiden Primideale $(19, \sqrt{47} + 3)$ und $(19, \sqrt{47} - 3)$ Hauptideale sein müssen. Es gibt also Elemente $x_1 = a_1 + \sqrt{47}b_1$ und $x_2 = a_2 + \sqrt{47}b_2$ mit $(x_1) = (19, \sqrt{47} + 3)$ und $(x_2) = (19, \sqrt{47} - 3)$.

Diese beiden Elemente haben Norm $\pm 19$, also gilt $a_1^2 - 47b_1^2 = \pm 19$ und $a_2^2 - 47b_2^2 = \pm 19$. Wir haben also zwei Lösungen $(a_1, b_1)$ und $(a_2, b_2)$.

(e) Da die Norm von Elementen multiplikativ ist, sind für alle Einheiten $y \in \mathcal{O}_K^*$ auch $yx_1$ und $yx_2$ wieder Elemente mit Norm $\pm 19$. Durch Multiplikation mit Einheiten erhält man aus den gegebenen Lösungen also neue Lösungen. Es reicht damit zu zeigen, daß es in $\mathcal{O}_K$ unendlich viele Einheiten gibt. Dies folgt aus dem Einheitensatz. Der Körper $\mathbb{Q}(\sqrt{47})$ ist reell, also ist $r = 2$, und es gilt

$$\mathcal{O}_K^* \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Es gibt also unendlich viele Lösungen der Ausgangsgleichung.

(f) Es ist $N(13+2\sqrt{47}) = -19$, mit $(13+2\sqrt{47})(7-\sqrt{47})$ ist dieses Element ein Erzeuger von $(19, \sqrt{47} - 3)$. Analog ist $13 - 2\sqrt{47}$ ein Erzeuger von $(19, \sqrt{47} + 3)$, und $N(13 - 2\sqrt{47}) = -19$.

Das negative Vorzeichen kommt also vor. Wenn das positive Vorzeichen vorkommt, dann gibt es ein Element mit Norm $-1$, also eine ganzzahlige Lösung von $a^2 - 47b^2 = -1$. Wir betrachten diese Gleichung modulo 47. Eine Lösung existiert, wenn $a^2 \equiv -1 \mod 47$ ist. Man kann aber (z.B. mit dem Legendre-Symbol) nachprüfen, daß $-1$ keine Quadratzahl modulo 47 ist. Es gibt also keine Elemente mit Norm $-1$. Damit gibt es auch keine Lösungen von $a^2 - 47b^2 = 1$.

## Aufgabe 14.2

Zuerst brauchen wir eine Kompatibilitätsaussage für Körpererweiterungen. Wir betrachten einen Turm von Erweiterungen $L_2/L_1/K$. Dann gilt

$$N_{L_2/K}(\alpha) = N_{L_1/K}(N_{L_2/L_1}(\alpha)).$$

Dies sind Formeln für die Determinante von Endomorphismen von Vektorräumen, sie werden wie im Beweis von Lemma 2.11 bewiesen. Man sieht dann direkt, daß die behauptete Aussage für die Körpererweiterung $L_2/K$ gilt, wenn sie sowohl für $L_2/L_1$ als auch für $L_1/K$ gilt.

Wir beweisen die Aussage erst einmal für eine Erweiterung von lokalen Körpern. Wenn $L/K$ unverzweigt ist, dann haben wir

$$|N_{L/K}(x)|_v = |N_{L/K}(u\pi^n)|_v = |N_{L/K}(u)|_v |N_{L/K}(\pi^n)|_v =$$

$$= |\pi^n|_v^{[L:K]} = |\pi^n|_w = |x|_w.$$

Der erste Schritt ist einfach, daß jedes $x$ als $u\pi^n$ geschrieben werden kann, wobei $u \in \mathcal{O}_L^*$ und $\pi$ ein Erzeuger des maximalen Ideals von $\mathcal{O}_L$ ist. Der zweite Schritt ist die Multiplikativität von Norm und Betrag. Der dritte Schritt nutzt, daß die Norm einer Einheit wieder eine Einheit ist, und deren Betrag also 1 ist. Außerdem kann man $\pi$ von vornherein so wählen, daß $\pi \in K$. Der vierte Schritt ist die Normierung des $w$-Betrages.

Analog zeigen wir für eine total verzweigte Erweiterung

$$|N_{L/K}(x)|_v = |N_{L/K}(u\pi^n)|_v = |N_{L/K}(\pi^n)|_v.$$

Nun kann $\pi$ nicht mehr so gewählt werden, daß es in $K$ liegt. Aber es gilt (bis auf eine Einheit), daß $\pi^e$ ein Erzeuger des maximalen Ideals von $\mathcal{O}_K$

ist, wobei $e$ den Verzweigungsgrad von $L/K$ bezeichnet. Damit ist

$$|N_{L/K}(\pi^n)|_v^e = |N_{L/K}(\pi^{ne})|_v = |\pi^{ne}|_v^{[L:K]} = |\pi^n|_w^e = |x|_w^e.$$

Da die Beträge Werte in den positiven reellen Zahlen annehmen, folgt auch $|N_{L/K}(\pi^n)|_v = |x|_w$.

Da sich jede Erweiterung von lokalen Körpern in einen unverzweigten und einen verzweigten Teil zerlegen läßt, haben wir die Behauptung für lokale Körper gezeigt.

Wir betrachten nun eine Erweiterung von globalen Körpern. Wir können uns auf den Fall einschränken, daß die Erweiterung $L/K$ separabel ist: Andernfalls faktorisieren wir $L/K$ in $L/K_s/K$, wobei $K_s/K$ separabel und $L/K_s$ rein inseparabel ist. Für eine rein inseparable Erweiterung $L/K_s$ haben wir für $\alpha \in L$ immer das Minimalpolynom $X^{p^n} - \alpha^{p^n}$. Damit ist $N_{L/K_s}(\alpha) = \alpha^{p^n}$. Die Erweiterung $L/K_s$ ist in jeder Primzahl rein verzweigt, diesen Fall haben wir bereits erledigt.

Nun müßen wir noch die lokalen Aussagen zusammensetzen. Wir haben ein kommutatives Diagramm von Körpereinbettungen

$$\begin{array}{ccc} L & \longrightarrow & \prod_{w_i|v} L_{w_i} \\ \uparrow & & \uparrow \\ K & \longrightarrow & K_v \end{array}$$

Multiplikation mit $x$ ist ein Endomorphismus des $K$-Vektorraums $L$ sowie des $K_v$-Vektorraums $\prod_{w_i|v} L_{w_i}$. Eine $K$-Basis in $L$ liefert eine Basis in $\prod_{w_i|v} L_{w_i}$, da die Gradformel besagt, daß die entsprechenden Dimensionen gleich sind. Für die Norm als Determinante des Endomorphismus folgt dann

$$N_{L/K}(x) = \prod_{w_i|v} N_{L_{w_i}/K_v}.$$

Wir schließen

$$|N_{L/K}(x)|_v = \prod_{w_i|v} |N_{L_{w_i}/K_v}(x)|_v = \prod_{w_i|v} |x|_{w_i}.$$