Prof. Dr. Salma Kuhlmann
Laura Wirth

Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2025

---

**Übungen zur Vorlesung *Algebraische Zahlentheorie***

## Blatt 6 – Lösung

**Aufgabe 6.1.**

Sei $p \in \mathbb{N}$ eine Primzahl.

(a) Sei $p \neq 2$.

(i) Beweisen Sie die Existenz geeigneter ganzer Zahlen $m$ und $n$ mit

$$m^2 + n^2 + 1 \equiv 0 \mod p.$$

(ii) Fixieren Sie $m, n \in \mathbb{Z}$ gemäß (i) und betrachten Sie die Menge

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

Zeigen Sie, dass $\Gamma$ ein vollständiges Gitter in $\mathbb{R}^4$ ist.

(iii) Sei $T_\Gamma$ ein fundamentales Parallelotop von $\Gamma$ mit Volumen $v(T_\Gamma) = p^2$. Beweisen Sie unter Verwendung von *Satz 21.8 (Minkowski)* die Existenz geeigneter ganzer Zahlen $a, b, c$ und $d$ mit

$$p = a^2 + b^2 + c^2 + d^2.$$

(b) Folgern Sie, dass jede natürliche Zahl eine Summe aus vier Quadraten ganzer Zahlen ist.

**Lösung:**

(a) (i) Modulo $p$ kann eine beliebige ganze Zahl $m \in \mathbb{Z}$ genau $p$ verschiedene Werte annehmen, nämlich $\overline{0}, \ldots, \overline{p-1} \in \mathbb{F}_p$. Da $p$ nach Voraussetzung eine Primzahl ist, existieren demnach exakt $\frac{p+1}{2}$ mögliche Quadrate $\overline{m^2}$ in $\mathbb{F}_p$. Selbiges gilt für eine beliebige ganze Zahl $n \in \mathbb{Z}$ und der Summe $\overline{-1-n^2}$. Falls $\overline{m^2} \neq \overline{-1-n^2}$ für alle $m, n \in \mathbb{Z}$ gilt, so liefert dies $\frac{p+1}{2} + \frac{p+1}{2} = \frac{2(p+1)}{2} = p+1$ paarweise verschiedene Elemente im Körper $\mathbb{F}_p$, der aus $p$ Elementen besteht. Dies ist unmöglich. Folglich gilt für mindestens eine Belegung von $m$ und $n$ schon $\overline{m^2} = \overline{-1-n}$ bzw. $m^2 + n^2 + 1 \equiv 0 \mod p$. □

(ii) Offensichtlich ist $\Gamma$ eine additive Untergruppe von $\mathbb{Z}^4$. In der Tat liegt $(0,0,0,0)$ offensichtlich in $\Gamma$, sodass $\Gamma$ nicht-leer ist. Seien nun $(a,b,c,d), (a',b',c',d') \in \Gamma$ beliebig aber fest, so gilt für $(a,b,c,d) - (a',b',c',d') = (a-a', b-b', c-c', d-d')$ bereits

$$c - c' \equiv (ma + nb) - (ma' - nb') \equiv m(a-a') + n(b-b') \mod p$$

sowie

$$(d - d') \equiv (mb - na) - (mb' - na') \equiv m(b-b') - n(a-a') \mod p.$$

Es folgt $(a,b,c,d)-(a',b',c',d')=(a-a',b-b',c-c',d-d')\in\Gamma$ per Definition von $\Gamma$. Zudem ist $\Gamma$ als Untermenge von $\mathbb{Z}^4$ offensichtlich diskret. Gemäß Satz 21.2 ist $\Gamma$ somit ein Gitter. Darüber hinaus liegen die Vektoren $(p,0,0,0),(0,p,0,0),(0,0,p,0),(0,0,0,p)$ offensichtlicht in $\Gamma$ und diese vier Vektoren sind (maximal) linear unabhängig in $\mathbb{R}^4$. Folglich ist $\Gamma$ vollständig. □

(iii) Betrachte die Kugel $B_r(0)$ mit Radius $r$ und Mittelpunkt $0$ in $\mathbb{R}^4$. Diese ist offensichtlich eine beschränkte, symmetrische, konvexe und Lebesgue-messbare Untermenge von $\mathbb{R}^4$. Sei nun $r$ geeignet gewählt, sodass $(1.9)p < r^2 < 2p$ erfüllt ist. Das Volumen einer Kugel beträgt allgemein $\frac{\pi^2 r^4}{2}$ . In dieser Belegung folgt somit

$$v(B_r(0))=\frac{\pi^2 r^4}{2}>16p^2=16v(T_\Gamma)=2^4 v(T_\Gamma).$$

Gemäß Satz 21.8 (Minkowski) existiert somit ein $\gamma\neq 0$ in $\Gamma\cap B_r(0)$. Fixiere ein solches. Da $\gamma$ insbesondere in $\Gamma$ liegt, ist $\gamma$ daher von der Form $\gamma=(a,b,c,d)\in\mathbb{Z}^4$ mit $c\equiv ma+nb \mod p$ und $d\equiv mb-na \mod p$. Folglich gilt

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

unter Einbezug von Aufgabenteil (i). Somit ist $a^2+b^2+c^2+d^2$ ein Vielfaches von $p$. Ferner gilt jedoch auch $\gamma\in B_r(0)$, weshalb $a^2+b^2+c^2+d^2\in]0,2p[_{\mathbb{Z}}$ ebenfalls erfüllt sein muss. Insgesamt erhält man $a^2+b^2+c^2+d^2=p$. □

(b) Offensichtlich gilt $2=1^2+1^2+0^2+0^2$ und folglich ist unter Einbezug von Aufgabenteil (a) jede Primzahl eine Summe von vier Quadraten ganzer Zahlen. Seien nun $a,b,c,d,A,B,C,D\in\mathbb{Z}$ beliebig aber fest, so gilt

$$\begin{aligned}
& (a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)\\
=\ & (\underbrace{aA-bB-cC-dD}_{=:a_0\in\mathbb{Z}})^2+(\underbrace{aB+bA+cD+dC}_{=:b_0\in\mathbb{Z}})^2\\
& +(\underbrace{aC-bD+cA+dB}_{=:c_0\in\mathbb{Z}})^2+(\underbrace{aD+bC-cB+dA}_{=:d_0\in\mathbb{Z}})^2\\
=\ & a_0^2+b_0^2+c_0^2+d_0^2.
\end{aligned}$$

Iterativ folgt daher für eine beliebige natürliche Zahl aus der Primfaktorisierung die Behauptung. □

**Aufgabe 6.2.**

Bestimmen Sie die Klassengruppe von $\mathbb{Z}[\sqrt{10}]$.

**Lösung:**

In Anlehnung an die Notation aus der Vorlesung setze $K := \mathbb{Q}(\sqrt{10})$, dann ist $D_K = 40$ und $c_K = \frac{\sqrt{40}}{2} = \sqrt{10} < 4$. Es werden nun zunächst die Primfaktorisierungen von $\langle 2\rangle$ und $\langle 3\rangle$ bestimmt. Seien für die Betrachtung von $\langle 2\rangle$ zunächst $a, b \in \mathbb{Z}$ beliebig aber fest und man bemerke, dass $a + b\sqrt{10} \in \langle 2, \sqrt{10}\rangle$ genau dann erfüllt ist, wenn $a$ gerade ist. Folglich gilt $|\mathcal{O}_K/\langle 2, \sqrt{10}\rangle| = 2$. Somit ist $\langle 2, \sqrt{10}\rangle$ ein Primideal, das insbesondere die 2 enthält. Ferner gilt

$$\langle 2, \sqrt{10}\rangle\langle 2, \sqrt{10}\rangle = \langle 4, 2\sqrt{10}, 10\rangle = \langle 2, 2\sqrt{10}\rangle = \langle 2\rangle$$

und somit ist $\langle 2, \sqrt{10}\rangle$ der einzige Primfaktor von $\langle 2\rangle$. Jedoch ist $\langle 2, \sqrt{10}\rangle$ kein Hauptideal:

> Angenommen $a + b\sqrt{10}$ mit geeigneten $a, b \in \mathbb{Z}$ ist erzeugend für $\langle 2, \sqrt{10}\rangle$. Dann gilt
>
> $$|N(a + b\sqrt{10})| = N(\langle a + b\sqrt{10}\rangle) = N(\langle 2, \sqrt{10}\rangle) = 2$$
>
> bzw. $a^2 - 10b^2 = \pm 2$. Folglich gilt $a^2 \equiv \pm 2 \mod 5$. Dies ist jedoch nicht möglich, da 2 und $-2$ keine Quadrate modulo 5 sind. Die Annahme war also falsch. ◇

Für die Betrachtung von $\langle 3\rangle$ bemerke nun stattdessen, dass $a+b\sqrt{10} \in \langle 3, 1-\sqrt{10}\rangle$ genau dann erfüllt ist, wenn $a \equiv -b \mod 3$ gilt. Dies impliziert somit $|\mathcal{O}_K/\langle 3, 1 - \sqrt{10}\rangle| = 3$. Damit ist $\langle 3, 1 - \sqrt{10}\rangle$ ein Primideal. Gleichermaßen gilt auch $a + b\sqrt{10} \in \langle 3, 1 + \sqrt{10}\rangle$ genau dann, wenn $a \equiv b \mod 3$ erfüllt ist. Dies impliziert $|\mathcal{O}_K/\langle 3, 1 + \sqrt{10}\rangle| = 3$ und folglich ist auch $\langle 3, 1 - \sqrt{10}\rangle$ ein Primideal. Jedoch ist weder $\langle 3, 1 - \sqrt{10}\rangle$ noch $\langle 3, 1 + \sqrt{10}\rangle$ ein Hauptideal:

> Angenommen man kann $a, b \in \mathbb{Z}$ geeignet wählen, sodass $a + b\sqrt{10}$ das Ideal $\langle 3, 1 - \sqrt{10}\rangle$ bzw. $\langle 3, 1 + \sqrt{10}\rangle$ erzeugt. Dann gilt $|N(a + b\sqrt{10})| = N(\langle a + b\sqrt{10}\rangle) = N(\langle 3, 1 - \sqrt{10}\rangle) = N(\langle 3, 1 + \sqrt{10}\rangle) = 3$ bzw. $a^2 - 10b^2 = \pm 3$. In anderen Worten also $a^2 \equiv \pm 3 \mod 5$. Da jedoch weder 3 noch $-3$ ein Quadrat modulo 5 ist, liefert dies einen Widerspruch. ◇

Ferner gilt $\langle 3, 1 + \sqrt{10}\rangle\langle 3, 1 - \sqrt{10}\rangle = \langle 3\rangle$ und damit sind $\langle 3, 1 - \sqrt{10}\rangle$ und $\langle 3, 1 + \sqrt{10}\rangle$ die einzigen Primfaktoren von $\langle 3\rangle$. Da $\mathbb{Z}[\sqrt{10}]$ kein Hauptidealbereich ist, enthält die Klassengruppe von $\mathbb{Z}[\sqrt{10}]$ mindestens zwei Elemente und nach obiger Beobachtung darüber hinaus maximal vier Elemente. Damit ist die Klassengruppe von $\mathbb{Z}[\sqrt{10}]$ isomorph zu $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ oder zu $\mathbb{Z}_4$. Bemerke nun ferner, dass $-2 + \sqrt{10} \in \langle 3, 1 + \sqrt{10}\rangle \cap \langle 2, \sqrt{10}\rangle$ gilt und folglich existiert ein $I \triangleleft \mathcal{O}_K$ mit $I\langle 3, 1 + \sqrt{10}\rangle\langle 2, \sqrt{10}\rangle = \langle -2 + \sqrt{10}\rangle$. Eine einfache Normberechnung offenbart nun

$$N(I) \cdot 3 \cdot 2 = N(I)N(\langle 3, 1 + \sqrt{10}\rangle)N(\langle 2, \sqrt{10}\rangle) = |N(-2 + \sqrt{10})| = 6$$

und folglich tritt $N(I) = 1$ ein. In anderen Worten gilt also $I = \mathcal{O}_K$ sowie

$$\langle 3, 1 + \sqrt{10}\rangle\langle 2, \sqrt{10}\rangle = \langle -2 + \sqrt{10}\rangle.$$

Folglich besteht die Klassengruppe von $\mathbb{Z}[\sqrt{10}]$ aus zwei Elementen, der Idealklassengruppe von $\mathcal{O}_K$ und jener von $\langle 2, \sqrt{10}\rangle$. □

**Aufgabe 6.3.**

Sei $0 < d \in \mathbb{Z}$ quadratfrei.

(a) Sei $d \equiv 2, 3 \mod 4$. Beweisen Sie, dass die Gleichung $x^2 - dy^2 = 1$ unendlich viele Lösungen besitzt.

(b) Sei $d \equiv 1 \mod 4$. Beweisen Sie, dass die Gleichung $x^2 - dy^2 = 4$ unendlich viele Lösungen besitzt.

**Lösung:**

(a) Da nach Annahme $d \equiv 2, 3 \mod 4$, gilt für $K := \mathbb{Q}(\sqrt{d})$ bereits $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Seien nun $x, y \in \mathbb{Z}$ beliebig aber fest, dann hat das Element $x + y\sqrt{d} \in \mathcal{O}_K$ genau dann die Norm $1$, wenn $x^2 - dy^2 = 1$ erfüllt ist. Es genügt dementsprechend zu beweisen, dass in $\mathcal{O}_K$ unendlich viele Elemente mit Norm $1$ existieren.

Ein Element in $\mathcal{O}_K$ besitzt genau dann die Norm $\pm 1$, wenn es eine Einheit ist. Da $K$ ein quadratischer Zahlkörper ist, existieren ferner zwei reelle Einbettungen von $K$ in $\mathbb{C}$. Folglich hat $\mathcal{O}_K^\times$ den freien Rang $1$ nach dem Dirichtletschen Einheitensatz. Somit existiert ein $u \in \mathcal{O}_K^\times$ von unendlicher Ordnung und als Einheit besitzt $u$ insbesondere Norm $\pm 1$. Aus der Multiplikativität der Norm folgt somit insbesondere, dass $w := u^2 \in \mathcal{O}_K^\times$ die Norm $1$ hat. Ferner hat auch für jedes $n \in \mathbb{N}$ das Element $w^n \in \mathcal{O}_K^\times$ die Norm $1$ (erneut aus der Multiplikativität der Norm). Letztendlich ist $w$ von unendlicher Ordnung, da bereits $u$ unendliche Ordnung besitzt und $w := u^2$ gewählt wurde. In anderen Worten impliziert für $n, m \in \mathbb{N}$ die Beziehung $w^n = w^m$ stets $n = m$. Somit beinhaltet $\mathcal{O}_K$ unendlich viele Elemente mit Norm 1. □

(b) Da nach Annahme $d \equiv 1 \mod 4$, gilt für $K := \mathbb{Q}(\sqrt{d})$ bereits $\mathcal{O}_K = \mathbb{Z}[1 + \frac{\sqrt{d}}{2}]$. Seien nun $x, y \in \mathbb{Z}$ beliebig aber fest, dann hat das Element $x + y\sqrt{d} \in \mathcal{O}_K$ genau dann die Norm $1$, wenn $x^2 + xy + \frac{1-d}{4}y^2 = 1$ bzw. $4 = 4x^2 + 4xy + (1-d)y^2 = (2x + y)^2 - dy^2$ erfüllt ist. Ferner folgt aus $a + b\frac{1+\sqrt{d}}{2} \neq e + f\frac{1+\sqrt{d}}{2}$ stets $a + 2b \neq e + 2f$ oder $b \neq f$ für beliebige ganze Zahlen $a, b, e, f$, sodass es insgesamt zu beweisen genügt, dass in $\mathcal{O}_K$ unendlich viele Elemente mit Norm $1$ existieren.

Da $K$ ein quadratischer Zahlkörper ist, existieren insbesondere zwei reelle Einbettungen von $K$ in $\mathbb{C}$. Folglich hat $\mathcal{O}_K^\times$ den freien Rang $1$ nach dem Dirichtletschen Einheitensatz. Somit existiert ein $u \in \mathcal{O}_K^\times$ von unendlicher Ordnung und als Einheit besitzt $u$ insbesondere Norm $\pm 1$. Aus der Multiplikativität der Norm, folgt somit insbesondere, dass $w := u^2 \in \mathcal{O}_K^\times$ die Norm $1$ hat. Ferner hat auch für jedes $n \in \mathbb{N}$ das Element $w^n \in \mathcal{O}_K^\times$ die Norm $1$ (erneut aus der Multiplikativität der Norm). Letztendlich ist $w$ von unendlicher Ordnung, da bereits $u$ unendliche Ordnung besitzt und $w := u^2$ gewählt wurde. In anderen Worten impliziert für $n, m \in \mathbb{N}$ die Beziehung $w^n = w^m$ stets $n = m$. Somit beinhaltet $\mathcal{O}_K$ unendlich viele Elemente mit Norm 1. □