

## Übungen zur Vorlesung Elementare Zahlentheorie (SS 18)

PD Dr. Jürgen Müller, Dr. Martin Bender

---

### (5.1) Aufgabe: Quadratische Zahlringe für $4 \mid (d-1)$ .

Es seien  $d \in \mathbb{Z} \setminus \{0, 1\}$  quadratfrei mit  $4 \mid (d-1)$ , und

$$R_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] := \left\{a + b\frac{1+\sqrt{d}}{2} \in \mathbb{C}; a, b \in \mathbb{Z}\right\}.$$

Man zeige:

a)  $R_d$  ist ein kommutativer Ring, und es gilt

$$R_d = \left\{\frac{1}{2}(a + b\sqrt{d}) \in \mathbb{C}; a, b \in \mathbb{Z}, 2 \mid (a-b)\right\}.$$

Außerdem wird durch  $N: R_d \rightarrow \mathbb{Z}: z \mapsto z \cdot \kappa(z)$ , wobei  $\kappa$  die Konjugation sei, eine multiplikative Abbildung mit Werten in  $\mathbb{Z}$  definiert.

b) Es gilt  $R_d^* = \{z \in R_d; |N(z)| = 1\}$ . Daraus folgere man: Ist  $d < 0$ , so ist  $R_d^*$  endlich. Genauer gilt  $R_d^* = \{\pm 1\}$  für  $d \leq -7$ , und  $R_{-3}^* = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ .

c) Für  $d \in \{-11, -7, -3, 5, 13\}$  ist  $R_d$  Euklidisch bezüglich der Gradabbildung  $R_d \setminus \{0\} \rightarrow \mathbb{N}_0: z \mapsto |N(z)|$ .

### (5.2) Aufgabe: Quadratische Zahlringe als faktorielle Ringe.

Es seien  $d \in \mathbb{Z} \setminus \{0, 1\}$  quadratfrei, sowie  $\mathcal{O}_d := \mathbb{Z}[\sqrt{d}]$  falls  $4 \nmid (d-1)$ , und  $\mathcal{O}_d := \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$  falls  $4 \mid (d-1)$ . Durch Betrachtung geeigneter Faktorisierungen zeige man für möglichst viele der folgenden Fälle (das sind alle mit  $|d| \leq 30$ ), daß  $\mathcal{O}_d$  *nicht* faktoriell ist:

a)  $d \in \{-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30\}$ .

b)  $d \in \{10, 15, 26, 30\}$ .

### (5.3) Aufgabe: Diophantische Gleichungen.

Man zeige, daß die Gleichung  $X^3 = Y^2 + 1$  nur die ganzzahligen Lösungen  $x = 1$  und  $y = 0$  hat.

**Hinweis.** Man benutze den Ring  $\mathbb{Z}[i]$  der Gaußschen Zahlen.

### (5.4) Aufgabe: Quadratzahlen.

Man zeige, daß sich unter den Summen  $1 + 2 + \dots + n$ , für  $n \in \mathbb{N}$ , unendliche viele Quadratzahlen befinden.

**Hinweis.** Man benutze die Einheitengruppe  $\mathbb{Z}[\sqrt{2}]^*$ .

---

**Abgabe:** 17.05.2018 (Donnerstag), bis 10:00 Uhr.