**Universität Konstanz**
**Fachbereich Mathematik und Statistik**
**Sommersemester 2011**

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

# Lösungsblatt 9 zur Zahlentheorie

**Aufgabe 1.**
Sei $[K : \mathbb{Q}] = n$. Dann ist $R \cong \mathbb{Z}^n$ als abelsche Gruppe. Sei

$$\mu\colon R \longrightarrow R,$$
$$\alpha \longmapsto x\alpha.$$

Offenbar ist dann $R/(x) = R/(\operatorname{im}(\mu))$. Ist $M$ eine Darstellungsmatrix der Abbildung $\mu$ bezüglich einer gewählten $\mathbb{Z}$–Basis von $R$, so ist $R/(x) \cong \mathbb{Z}^n / \operatorname{im}(M)$ als abelsche Gruppe. Wegen $0 \neq x$ ist $0 \neq N_{K|\mathbb{Q}}(x) = \det(M)$. Daher ist die Smithsche Normalform der Matrix $M$ eine Diagonalmatrix mit von null verschiedenen Einträgen $q_1, \ldots ,q_n$ und es gilt $\det(M) = q_1 \cdots q_n$. Wir haben daher

$$R/(x) \cong \mathbb{Z}^n/(\operatorname{im} M) \cong \mathbb{Z}/(q_1) \times \cdots \times \mathbb{Z}/(q_n)$$

als abelsche Gruppe. Insbesondere gilt daher

$$|R/(x)| = q_1 \ldots q_n = \det(M) = N_{K|\mathbb{Q}}(x).$$

**Aufgabe 2.**

(a) Die Ideale von $R/\mathfrak{p}^n$ stehen in (inklusionserhaltender) Bijektion zu den Idealen von $R$, die $\mathfrak{p}^n$ enthalten. Sei $\mathfrak{p}^n \subseteq I \subseteq R$ solch ein Ideal. Wir schreiben $I = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ für die Primidealzerlegung von $I$. Dabei seien $\mathfrak{p}_i \subset R$ für $i = 1, \ldots ,r$ paarweise verschiedene Primideale und $e_1, \ldots ,e_r \in \mathbb{N}_0$. Für alle $1 \leq i \leq r$ gilt nach Voraussetzung

$$\mathfrak{p}^n \subseteq \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq \mathfrak{p}_i.$$

Da $\mathfrak{p}$ prim und maximal ist gilt daher $\mathfrak{p} = \mathfrak{p}_i$. Also hat $I$ die Form $\mathfrak{p}^k$ für ein $k \in \mathbb{N}_0$. Wegen $\mathfrak{p}^n \subseteq I = \mathfrak{p}^k$ und der Eindeutigkeit der Primidealzerlegung ist $k \leq n$. Daher ist

$$\left\{\mathfrak{p}^k/\mathfrak{p}^n \mid 0 \leq k \leq n\right\}$$

genau die Menge der Ideale von $R/\mathfrak{p}^n$. Insbesondere hat $R/\mathfrak{p}^n$ nur endlich viele Ideale. Bleibt noch zu zeigen, dass ein jedes solche ein Hauptideal ist. Sei dazu $k \in \{0, \ldots ,n\}$ fixiert und $x \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$. Dann ist $(x)/\mathfrak{p}^n$ ein Ideal von $R/\mathfrak{p}^n$ und daher von der Form $\mathfrak{p}^l/\mathfrak{p}^n$ für ein $n$. Wegen $x \in \mathfrak{p}^k$ ist $l \geq k$. Wegen $x \notin \mathfrak{p}^{k+1}$ ist $l \leq k$ und daher ist $(x)/\mathfrak{p}^n = \mathfrak{p}^k$.

(b) Sei nun $0 \neq I \subseteq R$ ein beliebiges Ideal und $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ die Primidealzerlegung mit paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots ,\mathfrak{p}_r$. Dann gilt nach chinesischem Restsatz

$$R/I \cong R/\mathfrak{p}_1^{e_1} \times \cdots \times R/\mathfrak{p}_r^{e_r}.$$

Die Behauptung folgt aus Teilaufgabe (a), wenn man zeigt, dass die Ideale eines direkten Produkts von Ringen $A := R_1 \times \ldots R_r$ mit Ringen $R_i$ genau die $I_1 \times \cdots \times I_r$ sind, wobei die $I_i$ jeweils Ideale von $R_i$ sind. Offensichtlich ist $I_1 \times \cdots \times I_r$ ein Ideal von $A$, es ist daher nur noch zu zeigen, dass jedes Ideal von $A$ von dieser Form ist. Sei $I \subseteq A$ ein Ideal und sei $s_i \in A$ mit

$$s_i = (\delta_{i1}, \ldots, \delta_{ir}),$$

also das Element aus $A$, das an der $i$–ten Position den Eintrag 1 und an den übrigen Positionen den Eintrag Null hat. Dann ist

$$I = 1 \cdot I = (s_1 + \cdots + s_r)I = s_1 I + \cdots + s_r I = I_1 \times \cdots \times I_r$$

wobei $I_i := s_i I$ ein Ideal in $R_i$ ist.

(c) Sei $0 \neq a \in I$. Dann ist nach Teilaufgabe (b) das Ideal $I/(a)$ von $R/(a)$ ein Hauptideal, etwa erzeugt von $\bar{b}$. Somit ist $I = (a,b)$.

**Aufgabe 3.**

(a) Sei $p \in \mathbb{N}$ eine Primzahl. Angenommen es gibt $x,y \in \mathbb{Z}$ mit $x^2 + 5y^2 = p$. Dann ist $(x+\pi y)(x-\pi y) = x^2 + 5y^2 = p$. Weiter ist $N(x + \pi y) = x^2 + 5y^2 = N(x - \pi y) = p \notin \mathbb{Z}^\times$, was zeigt, dass weder $(x+\pi y)$ noch $(x-\pi y)$ eine Einheit ist. Daher ist $p$ reduzibel. Sei umgekehrt $p$ reduzibel. Dann gibt es $\alpha,\beta \in R$ mit Norm verschieden von $\pm 1$, so dass $\alpha\beta = p$. Dann muss $N(\alpha) = \pm p$ sein. Da die Norm in $K$ stets nichtnegativ ist muss sogar $N(\alpha) = p$ sein. Ist $\alpha = x + \pi y$ mit $x,y \in \mathbb{Z}$, so ist $N(\alpha) = x^2 + 5y^2 = p$.

(b) Zunächst hat weder $x^2 + 5y^2 = 3$ noch $x^2 + 5y^2 = 7$ eine Lösung in $\mathbb{Z}$. Daher sind sowohl 3 als auch 7 irreduzibel in $R$. Weiter ist

$$21 = 3 \cdot 7 = (4 + \pi)(4 - \pi).$$

Allerdings ist teilt weder 3 noch 7 einen der beiden Faktoren auf der rechten Seite. Also ist weder 3 noch 7 prim.

(c) Als abelsche Gruppe ist $R = \mathbb{Z} \oplus \mathbb{Z}\pi$. Also ist

$$R/(3) = (\mathbb{Z} \oplus \mathbb{Z}\pi)/(3\mathbb{Z} \oplus 3\mathbb{Z}\pi) = \mathbb{Z}/(3) \oplus \mathbb{Z}/(3)\pi$$

als abelsche Gruppe.

(d) Wir betrachten zunächst die 3. Wir schreiben $\mathfrak{p}_1 := (3,1 + 2\pi)$, $\mathfrak{p}_2 := (3,1 - 2\pi)$. Es ist

$$\mathfrak{p}_1\mathfrak{p}_2 = (9,3 - 6\pi,3 + 6\pi, -9) \subseteq (3).$$

Anderseits ist $9 - ((3 - 6\pi) + (3 + 6\pi)) = 3$, woraus die Idealgleichung

$$\mathfrak{p}_1\mathfrak{p}_2 = (3)$$

folgt. Bleibt noch zu zeigen, dass $\mathfrak{p}_1$ und $\mathfrak{p}_2$ Primideale sind. Wir zeigen, dass sie maximal sind. Es ist offenbar $(3) \subset \mathfrak{p}_1,\mathfrak{p}_2$ aber $(3) \neq \mathfrak{p}_1,\mathfrak{p}_2$. Daher ist $R/\mathfrak{p}_i$ ein Quotient von $R/(3)$ nach einem echten Ideal. Es ist $|R/(3)| = 9$. Daher muss $|R/\mathfrak{p}_i| = 3$ sein. Dann muss aber $R/\mathfrak{p}_i \cong \mathbb{Z}/(3)$ ein Körper sein, woraus folgt, dass $\mathfrak{p}_1,\mathfrak{p}_2$ maximale Ideale sind.

Nun finden wir eine Primidealzerlegung von (7). Nach Aufgabe 1 ist $|R/(7)| = N_{K|\mathbb{Q}}(7) = 49$. Ist $I \neq R$ ein echtes Oberideal von 7, so muss daher $|R/I| = 7$ sein, was sofort zeigt, dass $I$ maximal ist (denn $R/I = \mathbb{Z}/(7)$ ist ein Körper). Weiter erkennt man aus dem Klassifikationssatz für abelsche Gruppen, dass als abelsche Gruppe $R/(7) = \mathbb{Z}/(49)$ oder $R/(7) = \mathbb{Z}/(7) \oplus \mathbb{Z}/(7)$

ist. Es gibt daher höchstens zwei Untergruppen mit Index 7, daher kann es höchstens zwei Primoberideale von (7) geben. Weiter lassen sich beide Ideale mit 7 und einem weiteren Element erzeugen (Aufgabe 2.(c)). Wir machen daher den Ansatz

$$(7) = (7,\alpha)(7,\beta)$$

für geeignete $\alpha,\beta \in R$. In Analogie zu oben raten wir $\alpha = 2 + 3\pi$ und $\beta = 2 - 3\pi$. Wegen $\alpha\beta = 49$ ist obiges Produkt in (7) enthalten. Analog zu oben rechnet man nach, dass 49 und 28 im Produkt dieser Ideale liegen und somit auch $7 = 2 \cdot 28 - 49$. Damit haben wir eine Zerlegung von (7) in Primideale gefunden.