Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 10 zur Zahlentheorie

Aufgabe 1.

(a) Sei $0 \neq \alpha \in I$. Dann gibt es eine kanonische Surjektion $R/(\alpha) \longrightarrow R/I$. Aus Aufgabe 1 auf Blatt 9 erhält man $|R/I| \leq |R/\alpha| = N_{K|\mathbb{Q}}(\alpha) < \infty$.

(b) Zunächst bemerkt man, dass $\mathfrak{p}^{k-1}/\mathfrak{p}^k$ ein $R/\mathfrak{p}$–Vektorraum ist. Denn ist $\overline{x} \in \mathfrak{p}^{k-1}/\mathfrak{p}^k$ und sind $\alpha, \beta \in R$ mit $\alpha - \beta \in \mathfrak{p}$. So ist $\alpha x - \beta x \in \mathfrak{p}^k$ und daher ist $\alpha x \equiv \beta x \mod \mathfrak{p}^k$. Sei weiter $x \in \mathfrak{p}^{k-1} \setminus \mathfrak{p}^k$ (aufgrund der eindeutigen Primidealzerlegung existiert solch ein x). Aufgrund der Wahl von x gilt $\mathfrak{p}^k \subsetneq \mathfrak{p}^k + (x) \subseteq \mathfrak{p}^{k-1}$ und daher $(x) + \mathfrak{p}^k = \mathfrak{p}^{k-1}$. Insbesondere ist dann $(R/\mathfrak{p})\overline{x} = \mathfrak{p}^{k-1}/\mathfrak{p}^k$, was zeigt, dass $\mathfrak{p}^{k-1}/\mathfrak{p}^k$ als $R/\mathfrak{p}$–Vektorraum von $\overline{x} \neq 0$ erzeugt wird und daher eindimensional ist

(c) Zunächst bemerkt man, dass $R/\mathfrak{p}^n$ ein $R/\mathfrak{p}$–Vektorraum ist. Wir haben folgende Kompositionsreihe von $R/\mathfrak{p}^n$ als $R/\mathfrak{p}$–Modul

$$0 = \mathfrak{p}^n/\mathfrak{p}^n \subsetneq \mathfrak{p}^{n-1}/\mathfrak{p}^n \subsetneq \cdots \subsetneq \mathfrak{p}^0/\mathfrak{p}^n = R/\mathfrak{p}^n.$$

Nach dem Isomorphiesatz sind alle Kompositionsfaktoren isomorph zu $R/\mathfrak{p}$. Daher ist die Dimension von $R/\mathfrak{p}^n$ als $R/\mathfrak{p}$–Vektorraum gerade n und es folgt $\#(R/\mathfrak{p}^n) = (\#(R/\mathfrak{p}))^n$.

(d) Sei die Primidealzerlegung von I und J gegeben durch $I = \mathfrak{p}^{e_1} \cdots \mathfrak{p}^{e_r}$ und $J = \mathfrak{p}^{f_1} \cdots \mathfrak{p}^{f_r}$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und $e_i, f_i \in \mathbb{N}_0$. Unter Anwendung des chinesischen Restsatzes und der vorherigen Teilaufgaben erhalten wir

$$\begin{aligned}
\#(R/(IJ)) &= \#\left(R/\mathfrak{p}_1^{e_1+f_1} \times \cdots \times R/\mathfrak{p}_r^{e_r+f_r}\right) \\
&= (\#(R/\mathfrak{p}_1^{e_1+f_1})) \cdots (\#(R/\mathfrak{p}_r^{e_r+f_r})) \\
&= (\#(R/\mathfrak{p}_1))^{e_1+f_1} \cdots (\#(R/\mathfrak{p}_r))^{e_r+f_r} \\
&= (\#(R/\mathfrak{p}_1))^{e_1} \cdots (\#(R/\mathfrak{p}_r))^{e_r} (\#(R/\mathfrak{p}_1))^{f_1} \cdots (\#(R/\mathfrak{p}_r))^{f_r} \\
&= (\#(R/I))(\#(R/J)).
\end{aligned}$$

Aufgabe 2.

(a) Sei $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ die Zerlegung von (p) in Potenzen paarweiser verschiedener Primideale $\mathfrak{p}_1, \ldots \mathfrak{p}_r$. Nach Aufgabe 1 ist

$$p^2 = N_{k|\mathbb{Q}}(p) = (\#(R/\mathfrak{p}_1))^{e_1} \cdots (\#(R\mathfrak{p}_r))^{e_r}.$$

Da p eine Primzahl ist, gibt es nur die folgenden drei Zerlegungsmöglichkeiten:

(a) Es ist $e_i = 2$ für ein $i \in \{1, \ldots, r\}$ und $e_j = 0$ für $j \neq i$. In diesem Fall ist (p) die zweite Potenz eines Primideals.

(b) Es ist $e_i = 1$ und $e_j = 1$ für verschiedene $i,j \in \{1,\dots,n\}$ und $e_k = 0$ für $k \neq i,j$. In diesem Fall ist (p) das Produkt zweier verschiedener Primideale.

(c) Es ist $e_1 = 1$ für ein $i \in \{1,\dots,r\}$ und $e_j = 0$ für $j \neq i$. In diesem Fall ist (p) selbst ein Primideal.

In allen Fällen folgt die Behauptung.

(b) Ist $\mathfrak{p}_1$ ein Hauptideal, so gilt in C_R die Gleichung $\overline{0} = \overline{\mathfrak{p}_2} + \overline{0}$, woraus folgt, dass $\mathfrak{p}_2$ ein Hauptideal ist. Vertauschung von $\mathfrak{p}_1$ und $\mathfrak{p}_2$ ergibt die Umkehrung. Ist $(p) = \mathfrak{p}_1\mathfrak{p}_2$ ein Produkt von zwei Primhauptidealen, so gibt es $\alpha \in \mathfrak{p}_1$ und $\beta \in \mathfrak{p}_2$ mit $\alpha\beta = p$. Inbesondere ist

$$p^2 = N_{K|\mathbb{Q}}(\alpha\beta) = N_{K|\mathbb{Q}}(\alpha)N_{K|\mathbb{Q}}(\beta).$$

Da weder α noch β eine Einheit ist, folgt daher $N_{K|\mathbb{Q}}(\alpha) = \pm p$. Gibt es umgekehrt ein $x \in R$ mit $N_{K|\mathbb{Q}}(x) = \pm p$, so ist $(xx^*) = (p)$. Also $(x)(x^*) = (p)$. Aufgrund der eindeutigen Primidealzerlegung müssen die Hauptideal (x) und (x^*) Primideale sein.

(c) Angenommen p ist ein Primideal. Dann ist (p) maximal und $R/(p)$ ein Körper. Weiter ist $|R/(p)| = N_{K|\mathbb{Q}}(p) = p^2$, was zeigt, dass $R/(p) = \mathbb{F}_{p^2}$ ist.

Aufgabe 3.
Sei zunächst $\alpha(\mathfrak{p}) \geq 0$ für alle $\mathfrak{p} \in M$. Wir wählen für alle $\mathfrak{p} \in M$ ein $x_\mathfrak{p} \in \mathfrak{p}^{\alpha(\mathfrak{p})} \setminus \mathfrak{p}^{\alpha(\mathfrak{p})+1}$. Setze $I = \prod_{\mathfrak{p}\in M} \mathfrak{p}^{\alpha(\mathfrak{p})+1}$. Da M endlich ist, folgt aus dem chinesischem Restsatz, dass

$$R/I \cong \prod_{\mathfrak{p}\in M} R/\mathfrak{p}^{\alpha(\mathfrak{p})+1}.$$

Insbesondere lässt sich ein $x \in R$ wählen mit $x \equiv_{\mathfrak{p}^{\alpha(p)+1}} x_\mathfrak{p}$ für alle $\mathfrak{p} \in M$. Behauptung: Es gilt $v_\mathfrak{p}(x) = \alpha(\mathfrak{p})$ für alle $\mathfrak{p} \in M$.
Wegen $x \equiv_{\mathfrak{p}^{\alpha(p)+1}} x_\mathfrak{p}$ ist $x \in \mathfrak{p}^{\alpha(p)} \setminus \mathfrak{p}^{\alpha(\mathfrak{p})+1}$, woraus die Behauptung folgt. Ist nun α beliebig, schreibe $\alpha = \alpha_+ - \alpha_-$ mit $\alpha_+,\alpha_- \in \mathbb{N}_0^M$. Dann lässt sich jeweils x_+ und x_- finden mit $v_\mathfrak{p}(x_+) = \alpha_+(\mathfrak{p})$ und $v_\mathfrak{p}(x_-) = \alpha_-(\mathfrak{p})$ für alle $\mathfrak{p} \in M$. Damit gilt dann $v_\mathfrak{p}(\frac{x_+}{x_-}) = \alpha_+(\mathfrak{p}) - \alpha_-(\mathfrak{p}) = \alpha(\mathfrak{p})$ für alle $\mathfrak{p} \in M$.

Angenommen R habe nur endlich viele paarweise verschiedene Primideale $\mathfrak{p}_1,\dots,\mathfrak{p}_r$. Sei $I = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ ein Ideal von R. Dann gibt es $x \in R$ mit $v_{\mathfrak{p}_i}(x) = e_i$ für $i = 1,\dots,r$. Daher ist $(x) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ ein Hauptideal, was zeigt, dass jedes Ideal in R ein Hauptideal ist.