Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2014/2015

Christoph Hanselka
Markus Schweighofer

Einführung in die Algebra, Übungsblatt 7, Lösungsvorschlag

Aufgabe 1. Sei R ein faktorieller Ring mit Quotientenkörper K und sei $\mathbb{P}_R$ wie in der Vorlesung ein Vertretersystem der Primelemente ungleich 0 modulo Assoziiertheit.

(a) Zeige, dass $\Phi\colon R^\times \times \mathbb{Z}^{(\mathbb{P}_R)} \to K^\times : (c,\alpha) \mapsto c\mathbb{P}_R^\alpha$ ein Gruppenisomorphismus ist.

(b) Zu $a \in K^\times$ sei $\Phi^{-1}(a) = (c_a, \alpha_a)$. Zeige, dass für $p \in \mathbb{P}_R$ die Abbildung

$$v_p\colon K \to \mathbb{Z} \cup \{\infty\}$$
$$a \mapsto \begin{cases} \alpha_a(p), & \text{falls } a \neq 0 \\ \infty, & \text{falls } a = 0 \end{cases}$$

eine diskrete Bewertung auf K ist, genannt *p-Bewertung* oder *p-adische Bewertung*.

(c) Verwende (b) um zu zeigen, dass $\sqrt{2}$ nicht rational ist.

Lösungsvorschlag. (a) Seien $(c,\alpha), (d,\beta) \in R^\times\mathbb{Z}^{(\mathbb{P}_R)}$. Dann ist

$$\begin{aligned}
\Phi((c,\alpha)(d,\beta)) = \Phi(cd, \alpha+\beta) = cd\mathbb{P}_R^{\alpha+\beta} &= cd \prod_{p\in\operatorname{supp}(\alpha+\beta)} p^{(\alpha+\beta)(p)} \\
&\overset{(1)}{=} cd \prod_{p\in\operatorname{supp}(\alpha)\cup\operatorname{supp}(\beta)} p^{\alpha(p)+\beta(p)} \\
&= c\left(\prod_{p\in\operatorname{supp}(\alpha)\cup\operatorname{supp}(\beta)} p^{\alpha(p)}\right) d\left(\prod_{p\in\operatorname{supp}(\alpha)\cup\operatorname{supp}(\beta)} p^{\beta(p)}\right) \\
&\overset{(2)}{=} c\left(\prod_{p\in\operatorname{supp}(\alpha)} p^{\alpha(p)}\right) d\left(\prod_{p\in\operatorname{supp}(\beta)} p^{\beta(p)}\right) \\
&= \Phi(c,\alpha)\Phi(d,\beta).
\end{aligned}$$

Φ ist also ein Gruppenhomomorphismus. Beachte dabei in (1), dass $\operatorname{supp}(\alpha+\beta) \subseteq \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$, im Allgemeinen hier aber keine Gleichheit herrscht, jedoch sich das Produkt nicht ändert, da als zusätzliche Faktoren nur weitere Einsen hinzukommen. Ähnliches gilt für (2).

Nach Definition eines faktoriellen Ringes ist $R \setminus \{0\}$ im Bild von Φ. Letzteres ist aber eine Untergruppe von $K^\times$, enthält also auch $\{\, \frac{a}{b} \mid a,b \in R\setminus\{0\} \,\} = K^\times$. Also ist Φ surjektiv.

Um die Injektivität zu zeigen, sei $(c, \alpha) \in \ker \Phi$. Zu zeigen ist $c = 1$ und $\alpha = 0$. Wir können α zerlegen in einen nichtnegativen Teil und einen nichtpositiven Teil, also $\alpha = \alpha_+ - \alpha_-$ mit $\alpha_+, \alpha_- \in \mathbb{N}_0^{(\mathbb{P}_R)}$. Da $1 = \Phi(c, \alpha) = \Phi(c, \alpha_+) \left(\Phi(1, \alpha_-)\right)^{-1}$ bekommen wir also

$$c\mathbb{P}_R^{\alpha_+} = \Phi(c, \alpha_+) = \Phi(1, \alpha_-) = 1\mathbb{P}_R^{\alpha_-}$$

Nun verwenden wir die Eindeutigkeit der Primfaktorzerlegung in R, um zu bekommen, dass $c = 1$ und $\alpha_+ = \alpha_-$ und damit auch $\alpha = 0$.

(b) Sei $p \in \mathbb{P}_R$. Per Definition ist $v_p(0) = \infty$. Es ist $v_p|_{K^\times} = \mathrm{ev}_p \circ \pi_2 \circ \Phi^{-1}$, wobei $\pi_2 \colon R^\times \times \mathbb{Z}^{(\mathbb{P}_R)} \to \mathbb{Z}^{(\mathbb{P}_R)}$ die Projektion auf die zweite Komponente und $\mathrm{ev}_p \colon \mathbb{Z}^{(\mathbb{P}_R)} \to \mathbb{Z}$ die Auswertung in p ist. Sowohl π_2, als auch ev_p sind nach Definition der jeweiligen Gruppenstrukturen Homomorphismen, damit auch die Verkettung $v_p|_{K^\times}$.

Zu zeigen bleibt noch die ultrametrische Dreiecksungleichung, also $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ für alle $a, b \in K$. Seien also $a, b \in K$, ohne Einschränkung beide ungleich Null. Schreibe $a = \frac{x}{h}$ und $b = \frac{y}{h}$ für $x, y, h \in R \setminus \{0\}$, wobei wir durch Erweiterung annehmen können, dass a und b einen gemeinsamen Nenner haben. Sei außerdem $x = p^k \widetilde{x}$ sowie $y = p^\ell \widetilde{y}$, wobei $\widetilde{x}$ und $\widetilde{y}$ nicht von p geteilt werden. Also $k = v_p(x)$ und $\ell = v_p(y)$. Sei $n = \min\{k, \ell\}$. Dann gilt offensichtlich, dass $p^n | (x+y)$ in R, also $v_p(x+y) \geq n$ und damit

$$\begin{aligned} v_p(a+b) = v_p\left(\frac{x+y}{h}\right) &= v_p(x+y) - v_p(h) \geq n - v_p(h) = \min\{k, \ell\} - v_p(h) \\ &= \min\{v_p(x), v_p(y)\} - v_p(h) = \min\{v_p(x) - v_p(h), v_p(y) - v_p(h)\} \\ &= \min\{v_p(a), v_p(b)\} \end{aligned}$$

(c) Nehme $R := \mathbb{Z}$, $K := \mathbb{Q}$ und $\mathbb{P}_\mathbb{R} := \mathbb{P}$. Wäre $\sqrt{2} \in \mathbb{Q}$, so $2v_2(\sqrt{2}) = v_2((\sqrt{2})^2) = v_2(2) = 1$, was hieße, dass 1 eine gerade Zahl wäre.