Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 7 zur Zahlentheorie

Aufgabe 1.

(a) Der Ring $\mathbb{Z}[X]$ ist faktoriell und daher ganz abgeschlossen in $\mathbb{Q}(x)$.

(b) Sei $A = \mathbb{Z}[X]/(X^2+4)$. Setze $p := \overline{X}/\overline{2}$. Dann ist $p \in Q(A)$, denn $\overline{2}$ ist kein Nullteiler in A (sonst wäre $2 \mid X^2+4$ in $\mathbb{Z}[X]$). Auf der anderen Seite ist $p \notin A$, denn sonst wäre $\overline{X} = \overline{2q}$ für ein $q \in \mathbb{Z}[X]$, also

$$(X-2q) \mid (X^2+4).$$

Da X^2+4 irreduzibel in $\mathbb{Z}[X]$ ist, müsste $(X-2q) = (X^2+4)$ oder $(X-2) = \pm 1$ sein, was nicht möglich ist. Jedoch ist p ganz über A. Denn es ist

$$\overline{p^2+1} = \overline{\frac{X^2}{4}+1} = \frac{1}{4}\overline{(X^2+4)} = 0.$$

(Man beachte dazu, dass 2 und somit 4 kein Nullteiler in A ist.)

(c) Es ist $X^2-3X+2 = (X-2)(X-1)$ reduzibel. Es ist $(X-2)+(X-1) = (1)$, was zeigt, dass die Ideale $(X-2)$ und $(X-1)$ koprim sind. Nach dem chinesischen Restsatz gilt daher

$$\mathbb{Z}[X]/(X^2-3X+2) \cong \mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/(X-2) \cong \mathbb{Z} \times \mathbb{Z}.$$

Es genügt also zu untersuchen, ob $B := \mathbb{Z} \times \mathbb{Z}$ ganz abgeschlossen ist. Man beachte, dass B kein Integritätsring ist. Die Nullteiler in B sind gerade die Elemente der Form $(0,a)$ bzw. $(a,0)$ mit $a \in \mathbb{Z}$. Daher ist

$$Q(B) = \left\{ \frac{(a,b)}{(c,d)} \middle| a,b,c,d \in \mathbb{Z},\ c,d \neq 0 \right\} = \mathbb{Q} \times \mathbb{Q}.$$

Sei nun $x = (\frac{a}{c}, \frac{b}{d}) \in Q(B)$. Ist x ganz über B, so gibt es eine Ganzheitsgleichung von x mit Koeffizienten aus B. Liest man diese komponentenweise, so erhält man Ganzheitsgleichungen für $\frac{a}{c}$ und $\frac{b}{d}$ über $\mathbb{Z}$. Da $\mathbb{Z}$ ganz abgeschlossen ist, folgt $\frac{a}{c}, \frac{b}{d} \in \mathbb{Z}$. Daher ist $x \in B$, was zeigt, dass B ganz abgeschlossen ist.

Aufgabe 2.
Da R ein Dedekindring ist, sind die Ideale $\mathfrak{p}$ und $\mathfrak{q}$ jeweils maximal. Wegen $\mathfrak{p} \neq \mathfrak{q}$ gibt es also $x \in \mathfrak{p}$ und $y \in \mathfrak{q}$ mit $x+y=1$. Insbesondere ist

$$1 = 1^{n+m} = \sum_{i=0}^{n+m} x^{n+m-i} y^i.$$

Für $0 \leq i \leq m$ ist $x^{n+m-i}y^i \in \mathfrak{p}^n$ und für $m \leq i \leq n+m$ ist $x^{n+m-i}y^i \in \mathfrak{q}^m$. Daher ist $1 \in \mathfrak{p}^n + \mathfrak{q}^m$, was zu zeigen war. Sei nun M ein zyklischer Modul mit Erzeuger $z \in M$. Dann hat man einen surjektiven R–Modulhomomorphismus

$$\begin{aligned} f\colon R &\longrightarrow M, \\ r &\longmapsto rz. \end{aligned}$$

Sei $I := \ker(f) \subseteq R$. Dann gibt es paarweise verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ und $e_1, \dots, e_r \in \mathbb{N}$ mit $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Da je zwei dieser Idealpotenzen koprim sind, folgt die Behauptung nach dem chinesischen Restsatz.

Aufgabe 3.

(a) Diese Behauptung ist falsch. Sei dazu $R := \mathbb{Z}[X]$, sowie $I = (2,X)$. Dann ist

$$(R : I) = \{p \in \mathbb{Q}(X) \mid 2p \in \mathbb{Z}[X], Xp \in \mathbb{Z}[X]\}.$$

Dann ist $(R : I) = R$, denn $2p \in \mathbb{Z}[X]$ impliziert $p \in \mathbb{Q}[X]$ und $Xp \in \mathbb{Z}[X]$ impliziert $p \in \mathbb{Z}(x)$. Zusammen ergibt dies $p \in \mathbb{Q}[X] \cap \mathbb{Z}(X) = \mathbb{Z}[X]$. Dann ist jedoch $(R : I) \cdot I = I \neq R$.

(b) Diese Behauptung ist richtig. Es ist

$$\begin{aligned} x \in ((I : J) : K) &\Leftrightarrow xK \subseteq (I : J) \\ &\Leftrightarrow (xK)J \subseteq I \\ &\Leftrightarrow x(KJ) \subseteq I \\ &\Leftrightarrow x \in (I : KJ) = (I : JK). \end{aligned}$$

(c) Diese Behauptung ist richtig. Es ist

$$\begin{aligned} x \in \left(\bigcap_{i=1}^r I_i : J\right) &\Leftrightarrow xJ \subset \bigcap_{i=1}^r I_i \\ &\Leftrightarrow xJ \subseteq I_i \text{ für alle } i = 1, \dots, r \\ &\Leftrightarrow x \in (I_i : J) \text{ für alle } i = 1, \dots, r \\ &\Leftrightarrow x \in \bigcap_{i=1}^r (I_i : J). \end{aligned}$$

(d) Diese Behauptung ist falsch. Sei dazu $R = \mathbb{Z}$, $I_1 = (2)$, $I_2 = (3)$ und $J = (6)$. Es ist $(6 : 2) = (3)$ und $(6 : 3) = (2)$. Allerdings ist $(6 : (2,3)) = (6 : \mathbb{Z}) = (6) \neq (2) + (3) = \mathbb{Z}$.