G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 8

Aufgabe 31.

(1) Wir betrachten hierzu den surjektiven Ringmorphismus

$$\begin{array}{ccccccccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \times & \mathbf{Z}/3\mathbf{Z} & \times & \mathbf{Z}/7\mathbf{Z} & \times & \mathbf{Z}/11\mathbf{Z} \\ z & \longmapsto & (z & , & z & , & z & , & z)\,, \end{array}$$

der uns nach dem chinesischen Restsatz gegeben ist (wir unterschlagen die Restklassen-Querstriche).

Ferner ist sein Kern ist gegeben durch $2 \cdot 3 \cdot 7 \cdot 11\mathbf{Z} = 462\mathbf{Z}$. Finden wir also *ein* Urbild x_0 von (a, b, c, d), so erhalten wir die Menge $x_0 + 462\mathbf{Z}$ aller Urbilder.

Wir suchen Urbilder von $(1, 0, 0, 0)$, von $(0, 1, 0, 0)$, von $(0, 0, 1, 0)$ und von $(0, 0, 0, 1)$.

Ad $(1, 0, 0, 0)$. Der Euklidsche Algorithmus liefert $1 \cdot 231 - 115 \cdot 2 = 1$, und damit $231 \longmapsto (1, 0, 0, 0)$.

Ad $(0, 1, 0, 0)$. Der Euklidsche Algorithmus liefert $1 \cdot 154 - 51 \cdot 3 = 1$, und damit $154 \longmapsto (0, 1, 0, 0)$.

Ad $(0, 0, 1, 0)$. Der Euklidsche Algorithmus liefert $(-2) \cdot 66 + 19 \cdot 7 = 1$, und damit $-132 \longmapsto (0, 0, 1, 0)$.

Ad $(0, 0, 0, 1)$. Der Euklidsche Algorithmus liefert $5 \cdot 42 - 19 \cdot 11 = 1$, und damit $210 \longmapsto (0, 0, 0, 1)$.

Es ist also

$$\{x \in \mathbf{Z} \mid x \equiv_2 a,\ x \equiv_3 b,\ x \equiv_7 c,\ x \equiv_{11} d\} \;=\; 231a + 154b - 132c + 210d + 462\mathbf{Z}\,.$$

(2) Vorüberlegung. Es ist $x \equiv_6 c$ wegen $\mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ äquivalent zu $x \equiv_2 c$ und $x \equiv_3 c$. Da aber auch $x \equiv_2 a$ gelten muß, ist $a \equiv_2 c$ notwendige Voraussetzung, um ein x wie gewünscht zu erhalten.

In anderen Worten, **falls $a \not\equiv_2 c$,** dann ist

$$\{x \in \mathbf{Z} \mid x \equiv_4 a,\ x \equiv_7 b,\ x \equiv_6 c\} \;=\; \emptyset\,.$$

Falls hingegen $a \equiv_2 c$, so folgt aus $x \equiv_4 a$, daß $x \equiv_2 c$. Letztere Bedingung ist mithin redundant. In anderen Worten, es ist dann

$$\{x \in \mathbf{Z} \mid x \equiv_4 a,\ x \equiv_7 b,\ x \equiv_6 c\} \;=\; \{x \in \mathbf{Z} \mid x \equiv_4 a,\ x \equiv_7 b,\ x \equiv_3 c\}\,.$$

Wir betrachten den surjektiven Ringmorphismus

$$\begin{array}{ccccccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/4\mathbf{Z} & \times & \mathbf{Z}/7\mathbf{Z} & \times & \mathbf{Z}/3\mathbf{Z} \\ z & \longmapsto & (z & , & z & , & z) \end{array}$$

mit Kern $84\mathbf{Z}$.

Wir suchen Urbilder von $(1, 0, 0)$, von $(0, 1, 0)$ und von $(0, 0, 1)$.

Ad $(1, 0, 0)$. Der Euklidsche Algorithmus liefert $1 \cdot 21 - 5 \cdot 4 = 1$, und damit $21 \longmapsto (1, 0, 0)$.

Ad $(0, 1, 0)$. Der Euklidsche Algorithmus liefert $3 \cdot 12 - 5 \cdot 7 = 1$, und damit $36 \longmapsto (0, 1, 0)$.

Ad $(0, 0, 1)$. Der Euklidsche Algorithmus liefert $1 \cdot 28 - 9 \cdot 3 = 1$, und damit $28 \longmapsto (0, 0, 1)$.

Also wird in diesem Fall

$$\{x \in \mathbf{Z} \mid x \equiv_4 a,\ x \equiv_7 b,\ x \equiv_6 c\} \;=\; 21a + 36b + 28c + 84\mathbf{Z}\,.$$

Aufgabe 32.

(1) Zeigen wir zunächst, daß das angegebene Tupel $K[X]/(f(X))$ als Vektorraum erzeugt. Sei $g(X) \in K[X]$. Division mit Rest liefert $g(X) = f(X)s(X) + r(X)$, mit entweder $r(X) \neq 0$ und $\deg r \in [0, (\deg f) - 1]$ oder $r(X) = 0$. Jedenfalls ist

$$\overline{h(X)} \;=\; \overline{r(X)} \;\in\; \langle \bar{X}^0, \bar{X}^1 \ldots, \bar{X}^n \rangle \,.$$

Zeigen wir nun, daß das angegebene Tupel linear unabhängig ist. Seien $\lambda_i \in K$ mit

$$\sum_{i \in [0,n-1]} \lambda_i \bar{X}^i \;=\; 0$$

gegeben. Sei $h(X) := \sum_{i\in[0,n-1]} \lambda_i X^i$. Jedes Element von $(f(X))$ ist von Grad $\geq n$ oder gleich 0. Dahingegen ist $h(X)$ von Grad $\leq n-1$ oder gleich 0. Da nach Voraussetzung $\overline{h(X)} = 0$ sein soll, i.e. $h(X) \in (f(X))$, bleibt nur die Möglichkeit $h(X) = 0$, i.e. $\lambda_i = 0$ für alle $i \in [0, n-1]$.

(2) Mit (1) ist $R = \{0, 1, \bar{X}, \bar{X}+1\}$.

Ein Ringmorphismus $R \longrightarrow R$ ist durch das Bild ξ von X gegeben, falls dieses Bild die Gleichung $\xi^2 + \xi + 1 = 0$ erfüllt. Diese hat nun in R die beiden Nullstellen $\bar{X}$ und $\bar{X}+1$. Also gibt es die beiden Ringmorphismen

$$\begin{array}{ccc} R & \xrightarrow{\mathrm{id}} & R \\ \bar{X} & \longmapsto & \bar{X} \end{array} \qquad\qquad \begin{array}{ccc} R & \xrightarrow{\varphi} & R \\ \bar{X} & \longmapsto & \bar{X}+1\,. \end{array}$$

Die Identität ist ein Automorphismus. Da $\bar{X}+1$ ein Ringerzeuger (äquivalent, $\mathbf{F}_2$-Algebrenerzeuger) von R ist, i.e. $R = \mathbf{F}_2[\bar{X}+1]$, ist auch φ surjektiv, und damit wegen R endlich ein Automorphismus.

Da $X^2 + X + 1 \in \mathbf{F}_2[X]$ von Grad ≤ 3 ist und in $\mathbf{F}_2$ keine Nullstelle aufweist, ist es irreduzibel. Wegen 35 (1) ist nun R ein Körper.

(3) Ein Ringmorphismus von S nach T ist gegeben durch ein Bildelement $\xi \in T$, welches $\xi^4 - 1 = 0$ erfüllt. Die Nullstellenmenge dieses Polynoms in T ist nun gegeben durch $\{1, -1, \bar{X}, -\bar{X}\}$.

Somit gibt es die 4 Ringmorphismen

$$\begin{array}{ccc} S & \xrightarrow{\varphi_1} & T \\ \bar{X} & \longmapsto & 1 \end{array} \qquad \begin{array}{ccc} S & \xrightarrow{\varphi_{-1}} & T \\ \bar{X} & \longmapsto & -1 \end{array} \qquad \begin{array}{ccc} S & \xrightarrow{\varphi_{\bar{X}}} & T \\ \bar{X} & \longmapsto & \bar{X} \end{array} \qquad \begin{array}{ccc} S & \xrightarrow{\varphi_{-\bar{X}}} & T \\ \bar{X} & \longmapsto & -\bar{X}\,. \end{array}$$

Es sind 1 und -1 keine Ringerzeuger (äquivalent, $\mathbf{F}_3$-Algebrenerzeuger) von T, da jeweils $\bar{X}$ nicht im Erzeugnis liegt. Also sind φ_1 und φ_{-1} nicht surjektiv.

Dahingegen sind $\bar{X}$ und $-\bar{X}$ Ringerzeuger von T. Also sind $\varphi_{\bar{X}}$ und $\varphi_{-\bar{X}}$ surjektiv.

Injektiv kann überhaupt keine Abbildung von S nach T sein, da $|S| = 3^4 > 3^2 = |T|$.

Es ist S kein Körper, da darin $(\bar{X}^2+1)(\bar{X}^2-1) = 0$ ist, ohne daß einer der beiden Faktoren verschwindet.

Es ist T mit 35 (1) ein Körper, da $X^2 + 1 \in \mathbf{F}_3[X]$ irreduzibel ist, da es keine Nullstelle und Grad ≤ 3 hat.

Aufgabe 33.

(1) Es ist

$$\begin{array}{rcl} R/(2) & \simeq & \mathbf{Z}[X]/(X^4-5, 2) \\ & \simeq & \mathbf{F}_2[X]/(X^4-5) \\ & = & \mathbf{F}_2[X]/((X+1)^4)\,. \end{array}$$

In letzterem Ring ist die Restklasse von $X+1$ nilpotent, aber ungleich Null. Also ist auch sein isomorphes Bild in $R/(2)$, dort ebenfalls die Restklasse von $X+1$, nilpotent und ungleich Null.

(2) Mit dem Chinesischen Restsatz wird

$$\begin{array}{rcl} R/(11) & \simeq & \mathbf{Z}[X]/(X^4-5, 11) \\ & \simeq & \mathbf{F}_{11}[X]/(X^4-5) \\ & = & \mathbf{F}_{11}[X]/((X-2)(X+2)(X^2+4)) \\ & \simeq & \mathbf{F}_{11}[X]/(X-2) \times \mathbf{F}_{11}[X]/(X+2) \times \mathbf{F}_{11}[X]/(X^2+4) \\ & \simeq & \mathbf{F}_{11} \times \mathbf{F}_{11} \times \mathbf{F}_{11}[X]/(X^2+4)\,. \end{array}$$

Es ist $X^2+4 \in \mathbf{F}_{11}[X]$ irreduzibel, und also mit 35 (1) der Quotient $\mathbf{F}_{11}[X]/(X^2+4)$ ein Körper. Da mithin keiner der ringdirekten Faktoren ein nilpotentes Element ungleich 0 enthält, gilt dies auch für $R/(11)$.

Aufgabe 34.

(1) Mit dem Chinesischen Restsatz wird

$$\begin{array}{rcccc} \mathbf{R}[X]/(X^2-3) & \xrightarrow[\sim]{\varphi} & \mathbf{R}[X]/(X-\sqrt{3}) & \times & \mathbf{R}[X]/(X+\sqrt{3}) \\ a\bar{X}+b & \longmapsto & (a\bar{X}+b & , & a\bar{X}+b) \end{array}$$

Ferner haben wir Isomorphismen

$$\begin{array}{rcl} \mathbf{R}[X]/(X-\sqrt{3}) & \xrightarrow[\sim]{\psi_1} & \mathbf{R} \\ \bar{X} & \longmapsto & \sqrt{3} \end{array} \qquad \begin{array}{rcl} \mathbf{R}[X]/(X+\sqrt{3}) & \xrightarrow[\sim]{\psi_2} & \mathbf{R} \\ \bar{X} & \longmapsto & -\sqrt{3}\,. \end{array}$$

Der zusammengesetzte Isomorphismus $(\psi_1 \times \psi_2) \circ \varphi$ von $\mathbf{R}[X]/(X^2-3)$ nach $\mathbf{R} \times \mathbf{R}$ schickt also in der Tat $a\bar{X}+b$ auf $(a\sqrt{3}+b, -a\sqrt{3}+b)$.

(2) Es wird $(\bar{X}-b)^2 = \bar{X}^2 - 2b\bar{X} + b^2 = -2b\bar{X} + b^2 + 3$, und die behauptete Gleichung folgt.

(3) Es wird

$$\begin{array}{rcl} |\sqrt{3}-x_{n+1}| & = & |\pi_1(\bar{X}-x_{n+1})| \\ & = & |\pi_1(\bar{X}-\frac{x_n^2+3}{2x_n})| \\ & \overset{(2)}{=} & |\pi_1((-2x_n)^{-1}(\bar{X}-x_n)^2)| \\ & \overset{\pi_1 \text{ Ringmorphismus}}{=} & |\pi_1((-2x_n)^{-1})(\pi_1(\bar{X}-x_n))^2| \\ & = & |2x_n|^{-1}|\pi_1(\bar{X}-x_n)|^2 \\ & = & |2x_n|^{-1}|\sqrt{3}-x_n|^2\,. \end{array}$$

Für alle $b \in \mathbf{R} \smallsetminus \{0\}$ ist $\frac{b^2+3}{2b} \geq 1$, da $b^2+3 \geq 2b$, da $(b^2+3)-2b = (b-1)^2+2 \geq 0$. Also ist $x_n \geq 1$ für alle $n \geq 1$.

Mit Induktion folgt nun, daß $|\sqrt{3}-x_n| \leq |\sqrt{3}-x_1|^{2^{n-1}} = |\sqrt{3}-1|^{2^{n-1}}$ für $n \geq 1$. Da $1 < 3 < 4$, ist $1 < \sqrt{3} < 2$, und somit geht $|\sqrt{3}-1|^{2^{n-1}} \to 0$. Also geht $x_n \to \sqrt{3}$.

Zahlenwerte: $x_1 = 1$, $x_2 = 2$, $x_3 = 7/4$, $x_4 = 97/56 \approx 1.73214$. Zum Vergleich, $\sqrt{3} \approx 1.73205$

Aufgabe 35.

(1) Die Aussage ist richtig.

Erster Lösungweg. Wir zeigen, daß $(f(X))$ ein maximales Ideal in $K[X]$ ist. Ohne Einschränkung ist $f(X)$ normiert.

Sei $(f(X)) \subseteq I \subset K[X]$ ein Ideal. Wir haben $I = (f(X))$ zu zeigen.

Sei $g(X)$ normiert minimalen Grades in I. Sei $h(X) \in I$ beliebig. Division mit Rest gibt $h(X) = g(X)s(X)+r(X)$ mit entweder $r(X) \neq 0$ und $\deg r \in [0, (\deg g)-1]$ oder $r(X) = 0$. Da $r(X) \in I$, gibt die Minimalität des Grades von $g(X)$, daß $r(X) = 0$ zu sein hat. Also ist $g(X)$ ein Teiler von $h(X)$. Es folgt $I = (g(X))$.

Insbesondere teilt $g(X)$ das Polynom $f(X)$. Da $f(X)$ irreduzibel ist, und $f(X)$ und $g(X)$ normiert sind, ist $g(X) = f(X)$ oder $g(X) = 1$. Letzterenfalls wäre aber $I = K[X]$. Also ist $g(X) = f(X)$. Es folgt $I = (f(X))$.

Zweiter Lösungsweg. Wir invertieren jedes Element in $K[X]/(f(X))$ außer der Null. Sei $g(X) \in K[X] \smallsetminus (f(X))$ ein Repräsentant eines solchen Elements. Da $f(X)$ irreduzibel ist, sind $f(X)$ und $g(X)$ teilerfremd. Somit gibt es mit dem Euklidschen Algorithmus Polynome $s(X)$, $t(X) \in K[X]$ mit

$$s(X)f(X) + t(X)g(X) = 1\,.$$

Es folgt $t(X)g(X) \equiv_{f(X)} s(X)f(X) + t(X)g(X) = 1$, i.e. $\overline{t(X)}\,\overline{g(X)} = 1$, wie zu zeigen.

(2) Die Aussage ist richtig. Sei $x \in R \smallsetminus \{0\}$. Wir suchen ein $y \in R$ mit $yx = 1$. Da unter den Idealen (x^n) mit $n \geq 0$ nur endlich viele verschieden sein können, gibt es $0 \leq k < l$ mit $(x^k) = (x^l)$. Insbesondere gibt es ein $z \in R$ mit $zx^l = x^k$. Setzen wir $y = zx^{l-k-1}$, so wird $yx \cdot x^k = (zx^{l-k-1})x \cdot x^k = zx^l = 1 \cdot x^k$. Kürzen von x^k, was in einem Integritätsbereich gestattet ist, gibt $yx = 1$.

(3) Die Aussage ist richtig. Denn der Kern von $K \longrightarrow R$ kann nur 0 oder K sein. Wäre er gleich K, so gälte im Bild des Morphismus, und damit auch in R, die Gleichheit $1 = 0$. Daraus folgte $R = 0$, was aber ausgeschlossen war. Also ist der Kern gleich 0 und der Morphismus injektiv.

(4) Die Aussage ist richtig. Sei $x \in R \smallsetminus \{0\}$. Wir müssen zeigen, daß es ein $y \in R$ gibt, für welches $yx = 1$. Dazu genügt es zu zeigen, daß die Abbildung

$$\begin{array}{ccc} R & \xrightarrow{(-)x} & R \\ r & \longmapsto & rx \end{array}$$

surjektiv ist, denn dann enthält ihr Bild insbesondere die 1. Da R ein Integritätsbereich ist, ist sie injektiv.

Diese Abbildung ist nun eine K-linearer Endomorphismus des endlichdimensionalen K-Vektorraums R. Aus ihrer Injektivität folgt also ihre Surjektivität.