M. Künzer

Galoistheorie, WS 08/09

Lösung 5

Aufgabe 13

(1) Da $\mathbf{Z}$ ein Hauptidealbereich ist, und da $a\mathbf{Z} \cap b\mathbf{Z} \neq \{0\}$ (da z.B. ab enthalten ist), gibt es genau ein $x \in \mathbf{Z}_{\geqslant 1}$ mit $a\mathbf{Z} \cap b\mathbf{Z} = x\mathbf{Z}$.

Wir behaupten, daß $x = \mathrm{kgV}(a, b)$ ist.

Zum einen ist $x \in a\mathbf{Z}$, also x Vielfaches von a, und $x \in b\mathbf{Z}$, also x Vielfaches von b.

Ist umgekehrt $y \in \mathbf{Z}_{\geqslant 1}$ gegeben mit y Vielfaches von a und y Vielfaches von b, dann ist $y \in a\mathbf{Z} \cap b\mathbf{Z} = x\mathbf{Z}$, und folglich y Vielfaches von x, insbesondere also $y \geqslant x$.

Also ist x das kleinste gemeinsame Vielfache von a und b, i.e. $x = \mathrm{kgV}(a, b)$.

Vgl. auch Aufgabe 6.(3); dort wurde der Spezialfall $\mathrm{ggT}(a, b) = 1$ und also $\mathrm{kgV}(a, b) = ab$ gebraucht.

(2) Wir verwenden $a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{kgV}(a, b)\mathbf{Z}$ nach (1) und $a\mathbf{Z} + b\mathbf{Z} = \mathrm{ggT}(a, b)\mathbf{Z}$ nach §1.7.2, wobei $a, b \in \mathbf{Z}$. Es wird

$$\begin{array}{rcl} (12\mathbf{Z} + 30\mathbf{Z}) \cap 21\mathbf{Z} & = & \mathrm{ggT}(12, 30)\mathbf{Z} \cap 21\mathbf{Z} \\ & = & 6\mathbf{Z} \cap 21\mathbf{Z} \\ & = & \mathrm{kgV}(6, 21)\mathbf{Z} \\ & = & 42\mathbf{Z}\,. \end{array}$$

Also ist $x = 42$.

(3) Wir verwenden Aufgabe 8. Zunächst wird mit Euklid

$$(X^4 + 1)\mathbf{F}_2[X] + (X^4 + X^3 + 1)\mathbf{F}_2[X] \;=\; (X^2 + 1)\mathbf{F}_2[X]\,.$$

Dann gibt Euklid

$$(X^2 + 1)\mathbf{F}_2[X] + (X^3 + 1)\mathbf{F}_2[X] \;=\; (X + 1)\mathbf{F}_2[X]$$

Insgesamt also

$$\begin{array}{rl} & \big((X^4 + 1)\mathbf{F}_2[X] + (X^4 + X^3 + X + 1)\mathbf{F}_2[X]\big) + (X^3 + 1)\mathbf{F}_2[X] \\ = & (X^2 + 1)\mathbf{F}_2[X] + (X^3 + 1)\mathbf{F}_2[X] \\ = & (X + 1)\mathbf{F}_2[X]\,. \end{array}$$

Also ist $f(X) = X + 1$.

Vgl. auch die Definition des ggT von Polynomen im Beispiel in §1.7.3.

Aufgabe 14

Wende die Bemerkung aus §1.6.2 an auf die Situation, in den dortigen Bezeichnungen, $n = 1$, $R = \mathbf{F}_2$, $S = \mathbf{F}_2[X]$, $a = c$ die Einbettung von $\mathbf{F}_2$ nach $\mathbf{F}_2[X]$, und $s_1 = u(X)$ für ein noch zu spezifizierendes Polynom $u(X) \in \mathbf{F}_2[X]$.

Dann wird $f(X) \in \mathbf{F}_2[X]$ abgebildet auf $f(u(X)) \in \mathbf{F}_2[X]$.

(Für $u(X) = X$ z.B. erhalten wir so die Identität auf $\mathbf{F}_2[X]$. Für $u(X) = X^2$ erhalten wir einen injektiven, aber nicht surjektiven Ringmorphismus – es liegt etwa das Polynom X nicht im Bild. Etc.)

Für $u(X) = X + 1$ erhalten wir einen Ringmorphismus φ von $\mathbf{F}_2[X]$ nach $\mathbf{F}_2[X]$, der nicht gleich der Identität ist. Es schickt φ das Polynom $f(X) \in \mathbf{F}_2[X]$ auf das Polynom $f(X + 1) \in \mathbf{F}_2[X]$.

Wir *behaupten,* daß φ ein Isomorphismus ist, der $\varphi^2 = \mathrm{id}_{\mathbf{F}_2[X]}$ erfüllt. Dazu genügt es zu zeigen, daß letzteres gilt - eine Abbildung, die quadriert die Identität ist, ist insbesondere bijektiv.

Für $f(X) \in \mathbf{F}_2[X]$ wird in der Tat

$$\begin{array}{rcl} \varphi^2\big(f(X)\big) & = & \varphi\big(\varphi\big(f(X)\big)\big) \\ & = & \varphi\big(f(X+1)\big) \\ & = & f((X+1)+1) \\ & = & f(X)\ . \end{array}$$

Aufgabe 15

(1) Schreibe $R = \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$. Es wird

$$\begin{array}{ccccc} \mathbf{Z} & \xrightarrow{\varepsilon_R} & \mathbf{Z}/8\mathbf{Z} & \times & \mathbf{Z}/12\mathbf{Z} \\ z & \longmapsto & (z+8\mathbf{Z} & \times & z+12\mathbf{Z})\ , \end{array}$$

da dies ein Ringmorphismus von $\mathbf{Z}$ nach R ist und es nur einen solchen gibt, namentlich ε_R; vgl. §1.7.3.

Der Kern von ε_R berechnet sich zu $8\mathbf{Z} \cap 12\mathbf{Z} = \mathrm{kgV}(8,12)\mathbf{Z} = 24\mathbf{Z}$; vgl. Aufgabe 13.(1). Also ist $\mathrm{char}(\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}) = 24$.

(2) Betrachte folgendes Dreieck von Ringmorphismen.

$$\begin{tikzcd} \mathbf{Z} \arrow[r, "\varepsilon_L"] \arrow[d, "\varepsilon_K"'] & L \\ K \arrow[ur, "f"'] & \end{tikzcd}$$

Dieses Dreieck kommutiert, i.e. $f \circ \varepsilon_K = \varepsilon_L$, da es nur einen Ringmorphismus von $\mathbf{Z}$ nach L gibt, namentlich ε_L; vgl. §1.7.3.

Um $\mathrm{char}\, K \overset{!}{=} \mathrm{char}\, L$ zu zeigen, haben wir zu zeigen, daß

$$(\mathrm{char}\, K)\mathbf{Z} \ = \ \mathrm{Kern}\, \varepsilon_K \overset{!}{=} \mathrm{Kern}\, \varepsilon_L \ = \ (\mathrm{char}\, L)\mathbf{Z}\ ;$$

vgl. §1.7.3.

Beachte, daß f injektiv ist; vgl. Aufgabe 7. Also ist $f(x) = 0$ genau dann, wenn $x = 0$, wobei $x \in K$.

Also wird

$$\begin{array}{rcl} \mathrm{Kern}\, \varepsilon_L & = & \{z \in \mathbf{Z}\ :\ \varepsilon_L(z) = 0\} \\ & = & \{z \in \mathbf{Z}\ :\ f(\varepsilon_K(z)) = 0\} \\ & = & \{z \in \mathbf{Z}\ :\ \varepsilon_K(z) = 0\} \\ & = & \mathrm{Kern}\, \varepsilon_K\ . \end{array}$$

Aufgabe 16

(1) Sei etwa $n = ab$ mit $a,\, b \in [2, n-1]$. Dann sind $a \not\equiv_n 0$ und $b \not\equiv_n 0$, i.e. $a + n\mathbf{Z} \neq 0 + n\mathbf{Z}$ und $b + n\mathbf{Z} \neq 0 + n\mathbf{Z}$. Wohl aber ist

$$(a+n\mathbf{Z})(b+n\mathbf{Z}) \ = \ (ab+n\mathbf{Z}) \ = \ n+n\mathbf{Z} \ = \ 0+n\mathbf{Z}\ .$$

Also ist $\mathbf{Z}/n\mathbf{Z}$ kein Integritätsbereich; vgl. §1.5.

(2) Euklid liefert

$$1 \ = \ (X^7+1)(-X^3+X^2-X-1) + (X^4+1)(X^6-X^5+X^4+X^3-X^2+X-1)\ .$$

Also ist

$$(X^4+1)(X^6-X^5+X^4+X^3-X^2+X-1) \;\equiv_{X^7+1}\; 1\;,$$

mit anderen Worten,

$$\big(X^4+1+(X^7+1)\mathbf{F}_3[X]\big)^{-1} \;=\; X^6-X^5+X^4-X^3-X^2+X-1+(X^7+1)\mathbf{F}_3[X]\;.$$

Vgl. Aufgabe 8, Aufgabe 4.(1).

(3) Es ist $\dim_{\mathbf{F}_2} R = \deg(X^3+X^2+X+1) = 3$; vgl. Lemma aus §1.7.5. Also ist $|R| = 2^{\dim_{\mathbf{F}_2} R} = 2^3 = 8$.
Schreibe $\bar{X} := X + (X^3+X^2+X+1)\mathbf{F}_2[X]$.
Es ist z.B. $\bar{X}\cdot(\bar{X}^2+\bar{X}+1) = 1 + (\bar{X}^3+\bar{X}^2+\bar{X}+1) = 1$. Also ist $\bar{X}$ invertierbar. Ferner ist $\bar{X}\neq 1$, wie man etwa mit der in loc. cit. gegebenen Basis $(\bar{X}^0,\bar{X}^1,\bar{X}^2)$ erkennt, oder aber direkt dank $X\not\equiv_{X^4-1} 1$. Vgl. (4).
Da wir aber in $\mathbf{F}_2[X]$

$$X^3+X^2+X+1 \;=\; (X+1)(X^2+1) \;=\; (X+1)^3$$

haben, folgt nun, daß zwar $\bar{X}+1\neq 0$ und $\bar{X}^2+1\neq 0$ (wie man z.B. mit der eben genannten Basis erkennt), aber

$$(\bar{X}+1)(\bar{X}^2+1) \;=\; 0\;.$$

Also ist R kein Integritätsbereich.

(4) Schreibe $\bar{X} := X + f(X)K[X]$. Sei $n := \deg f$.
Es ist

$$0 \;=\; f(X)+f(X)K[X] \;=\; f(\bar{X}) \;=\; f_n\bar{X}^n + f_{n-1}\bar{X}^{n-1}+\cdots+f_1\bar{X}+f_0\;.$$

Also wird

$$1 \;=\; -f_0^{-1}(f_n\bar{X}^{n-1}+f_{n-1}\bar{X}^{n-2}+\cdots+f_1)\cdot\bar{X}.$$

Es folgt

$$(X+f(X)K[X])^{-1} \;=\; \bar{X}^{-1} \;=\; -f_0^{-1}(f_n\bar{X}^{n-1}+f_{n-1}\bar{X}^{n-2}+\cdots+f_1)\;.$$