M. Künzer

Galoistheorie, WS 08/09

Lösung 6

Aufgabe 17

(1) Wir erhalten

$(+)$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

und

$(\cdot)$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

(2) Es wird

$$(\alpha^2+1)^3 \;=\; \alpha^3 \;=\; 1\,.$$

Es wird

$$(\beta^2+1)(\beta^6+1)+\beta^2 \;=\; (\beta^2+1)((\beta+1)^2+1)+\beta^2 \;=\; (\beta^2+1)\beta^2+\beta^2 \;=\; \beta^2+\beta+\beta^2+\beta^2 \;=\; \beta^2+\beta\,.$$

Es wird

$$(\iota+1)^4-\iota \;=\; ((\iota+1)^2)^2-\iota \;=\; (\iota^2+2\iota+1)^2-\iota \;=\; (-\iota)^2-\iota = -\iota-1\,.$$

(3) Es ist $X(X+1)+(X^2+X+1)\cdot 1 = 1$ in $\mathbf{F}_2[X]$, und somit $\alpha^{-1} = \alpha+1$. Man kann auch die Verknüpfungstafel aus (1) heranziehen.

Es ist $(X^2+X+1)X^2+(X^3+X+1)(X+1) = 1$ in $\mathbf{F}_2[X]$, und somit $(\beta^2+\beta+1)^{-1} = \beta^2$.

Es ist $(X+1)(X-1)+(X^2+1)\cdot(-1) = 1$ in $\mathbf{F}_3[X]$, und somit $(\iota+1)^{-1} = (\iota-1)$.

Man kann auch die Potenztabellen aus untenstehender Lösung zur Aufgabe 18 zur Inversion verwenden.

Aufgabe 18

(1) Es wird z.B.

$$\begin{array}{rcl} \alpha^0 &=& 1 \\ \alpha^1 &=& \alpha \\ \alpha^2 &=& \alpha+1\,, \end{array}$$

und also $\langle\alpha\rangle = \mathbf{F}_4^\times$.

(2) Es wird z.B.

$$\begin{array}{rcl} \beta^0 &=& 1 \\ \beta^1 &=& \beta \\ \beta^2 &=& \beta^2 \\ \beta^3 &=& \beta+1 \\ \beta^4 &=& \beta^2+\beta \\ \beta^5 &=& \beta^2+\beta+1 \\ \beta^6 &=& \beta^2+1\,, \end{array}$$

und also $\langle\beta\rangle = \mathbf{F}_8^\times$.

(3) Es wird z.B.

$$\begin{aligned}
(\iota+1)^0 &= 1\\
(\iota+1)^1 &= \iota+1\\
(\iota+1)^2 &= -\iota\\
(\iota+1)^3 &= -\iota+1\\
(\iota+1)^4 &= -1\\
(\iota+1)^5 &= -\iota-1\\
(\iota+1)^6 &= \iota\\
(\iota+1)^7 &= \iota-1
\end{aligned}$$

und also $\langle \iota+1\rangle = \mathbf{F}_9^\times$.

Beachte, daß $\langle\iota\rangle \subsetneq \mathbf{F}_9^\times$.

Aufgabe 19
Bestimme alle normierten irreduziblen Polynome in $\mathbf{F}_q$ von Grad n.

(1) Da $n \leqslant 3$, suchen wir gerade die normierten Polynome in $\mathbf{F}_4[X]$ von Grad 2 ohne Nullstelle in $\mathbf{F}_4$. Wir listen alle normierten Polynome in $\mathbf{F}_4[X]$ von Grad 2 mit nichtverschwindendem konstanten Term auf, daneben ihre Nullstellen in $\mathbf{F}_4$.

Polynom	Nullstellenmenge
X^2+1	$\{1\}$
$X^2+\alpha$	$\{\alpha^2\}$
$X^2+\alpha^2$	$\{\alpha\}$
X^2+X+1	$\{\alpha,\ \alpha^2\}$
$X^2+X+\alpha$	$\emptyset$
$X^2+X+\alpha^2$	$\emptyset$
$X^2+\alpha X+1$	$\emptyset$
$X^2+\alpha X+\alpha$	$\emptyset$
$X^2+\alpha X+\alpha^2$	$\{1,\alpha^2\}$
$X^2+\alpha^2 X+1$	$\emptyset$
$X^2+\alpha^2 X+\alpha$	$\{1,\alpha\}$
$X^2+\alpha^2 X+\alpha^2$	$\emptyset$

Somit sind die normierten irreduziblen Polynome von Grad 2 in $\mathbf{F}_4[X]$ gegeben durch

$$X^2+X+\alpha,\ X^2+X+\alpha^2,\ X^2+\alpha X+1,\ X^2+\alpha X+\alpha,\ X^2+\alpha^2X+1,\ X^2+\alpha^2X+\alpha^2\ .$$

(2) Da $n \leqslant 3$, suchen wir gerade die normierten Polynome in $\mathbf{F}_3[X]$ von Grad 3 ohne Nullstelle in $\mathbf{F}_3$. Wir listen alle normierten Polynome in $\mathbf{F}_3[X]$ von Grad 3 mit nichtverschwindendem konstanten

Term auf, daneben ihre Nullstellen in $\mathbf{F}_3$.

Polynom	Nullstellenmenge
X^3+1	$\{-1\}$
X^3-1	$\{1\}$
X^3+X+1	$\{1\}$
X^3+X-1	$\{-1\}$
X^3-X+1	$\emptyset$
X^3-X-1	$\emptyset$
X^3+X^2+1	$\{1\}$
X^3+X^2-1	$\emptyset$
X^3+X^2+X+1	$\{-1\}$
X^3+X^2+X-1	$\emptyset$
X^3+X^2-X+1	$\emptyset$
X^3+X^2-X-1	$\{1,-1\}$
X^3-X^2+1	$\emptyset$
X^3-X^2-1	$\{-1\}$
X^3-X^2+X+1	$\emptyset$
X^3-X^2+X-1	$\{1\}$
X^3-X^2-X+1	$\{1,-1\}$
X^3-X^2-X-1	$\emptyset$

Somit sind die normierten irreduziblen Polynome von Grad 3 in $\mathbf{F}_3[X]$ gegeben durch

$$\begin{array}{l} X^3-X+1,\ X^3-X-1,\ X^3+X^2-1,\ X^3+X^2+X-1, \\ X^3+X^2-X+1,\ X^3-X^2+1,\ X^3-X^2+X+1,\ X^3-X^2-X-1\,. \end{array}$$

(3) Vorweg bemerken wir, daß X^2+X+1 das einzige (normierte) irreduzible Polynom von Grad 2 in $\mathbf{F}_2[X]$ ist.

Die (normierten) Polynome vierten Grades in $\mathbf{F}_2[X]$ ohne Nullstelle in $\mathbf{F}_2$ sind

$$X^4+X+1,\ X^4+X^2+1,\ X^4+X^3+1\,.$$

Wenn unter diesen eines nichttrivial in zwei Faktoren zerfllt, muß dieser Faktor von Grad 2 und irreduzibel sein – bei einem reduziblen Faktor von Grad 2 würde ja auch noch ein Faktor von Grad 1 abspalten, d.h. eine Nullstelle auftreten.

In der Tat ist $X^4+X^2+1=(X^2+X+1)^2$. Ferner sind weder X^4+X+1 noch X^4+X^3+1 durch X^2+X+1 teilbar (e.g. weil $\alpha^4+\alpha+1=1\neq 0$ und $\alpha^4+\alpha^3+1=\alpha\neq 0$). Also sind die irreduziblen Polynome von Grad 4 in $\mathbf{F}_2[X]$ gegeben durch

$$X^4+X+1,\ X^4+X^3+1\,.$$

Aufgabe 20

Es gibt keinen Isomorphismus $\mathbf{Z}/9\mathbf{Z}\xrightarrow{\sim}\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$, denn die Charakteristik von $\mathbf{Z}/9\mathbf{Z}$ ist 9, die Charakteristik von $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ aber 3.

Es gibt keinen Isomorphismus $\mathbf{Z}/9\mathbf{Z}\xrightarrow{\sim}\mathbf{F}_9$, denn die Charakteristik von $\mathbf{Z}/9\mathbf{Z}$ ist 9, die Charakteristik von $\mathbf{F}_9$ aber 3.

Es gibt keinen Isomorphismus $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\xrightarrow[\sim]{f}\mathbf{F}_9$, denn es wäre sonst $f((1,0))f((0,1))=f((0,0))=0$, aber $f((1,0))\neq 0$ und $f((0,1))\neq 0$, was wegen $\mathbf{F}_9$ Körper nicht geht. Kurz, da $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ kein Integritätsbereich ist, $\mathbf{F}_9$ als Körper aber schon, geht das nicht. (Alternativ kann man anführen, daß es in $\mathbf{F}_9$ ein invertierbares Element der Ordnung 8 gibt, in $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ aber nicht.)

Aufgabe 21

Wir behaupten, daß es in $\mathbf{F}_8$ keinen Teilring aus 4 Elementen gibt.

Angenommen, doch. Sei $R \subseteq \mathbf{F}_8$ ein Teilring mit $|R| = 4$. Da R ein endlicher Integritätsbereich ist, ist R ein Teilkörper von $\mathbf{F}_8$. Es ist $R^\times := R \smallsetminus \{0\}$ eine Gruppe aus 3 Elementen. Nach Aufgabe 11.(1.c) teilt die Ordnung jedes Elements in $R^\times$ die 3. Nun haben nach loc. cit. aber alle Elemente von $\mathbf{F}_8^\times$ eine Ordnung, die 7 teilt, insbesondere auch die von $R^\times$. Da aber $\mathrm{ggT}(3,7) = 1$, müssen alle Elementordnungen von $R^\times$ die 1 teilen, i.e. gleich 1 sein. Nun hat aber nur die Eins einer Gruppe die Ordnung 1. Also $R^\times = \{1\}$. Aber $|R^\times| = 3$. Dies ist ein *Widerspruch.*

Aufgabe 22

Sei $R \xrightarrow{f} S$ ein Morphismus kommutativer Ringe. Sei $I \subseteq S$ ein Ideal.

(1) Da $f(0) = 0 \in J$, ist $0 \in f^{-1}(J)$.

Sind $x,\ y \in f^{-1}(J)$, so ist $f(x-y) = f(x) - f(y) \in J$, also $x - y \in f^{-1}(J)$.

Ist $x \in f^{-1}(J)$ und ist $r \in R$, so ist $f(rx) = f(r)f(x) \in J$, und also $rx \in f^{-1}(J)$.

Also ist $f^{-1}(J) \subseteq R$ ein Ideal.

Ist $r \in \mathrm{Kern}\, f$, so ist $f(r) = 0 \in J$, und also $r \in f^{-1}(J)$. Also ist $\mathrm{Kern}\, f \subseteq J$. (Alternativ, da $\{0\} \subseteq J$, ist auch $f^{-1}(\{0\}) \subseteq f^{-1}(J)$.)

(2) Wir haben zu zeigen, daß R/I genau 2 Ideale enthält. Wir wenden (1) an auf $R \xrightarrow{\rho} R/I$. Sei $J \subseteq R/I$ ein Ideal. Dann ist

$$I \;=\; \mathrm{Kern}\,\rho \;\subseteq\; \rho^{-1}(J) \;\subseteq\; R\,.$$

Da $I \subseteq R$ ein maximales Ideal ist, folgt $\rho^{-1}(J) = I$ oder $\rho^{-1}(J) = R$.

Ersterenfalls ist, wegen ρ surjektiv, $J = \rho(\rho^{-1}(J)) = \rho(I) = \{0_{R/I}\}$.

Zweiterenfalls ist, wegen ρ surjektiv, $J = \rho(\rho^{-1}(J)) = \rho(R) = R/I$.

Die Menge der Ideale von R/I ist somit gleich $\{\{0_{R/I}\},\ R/I\}$. Es bleibt uns anzumerken, daß $R/I \neq \{0_{R/I}\}$, da $I \subsetneq R$, daß also in der Tat auch zwei verschiedene Ideale aufgelistet sind.