M. Künzer

Galoistheorie, WS 08/09

Lösung 7

Aufgabe 23

Addition und Multiplikation sind ersichtlich kommutativ. Die Multiplikation ist ersichtlich assoziativ. Das Element $\frac{1}{1}$ ist ersichtlich neutral bezüglich der Multiplikation.

Die nun noch fehlenden Eigenschaften wollen wir nachweisen. Seien $\frac{r}{s}$, $\frac{r'}{s'}$, $\frac{r''}{s''} \in \operatorname{frac} R$.

Es wird $\frac{r}{s} + \frac{0}{1} = \frac{r\cdot 1 + s\cdot 0}{s\cdot 1} = \frac{r}{s}$.

Es wird $\frac{r}{s} + \frac{(-r)}{s} = \frac{rs+(-r)s}{s^2} = \frac{0}{s^2} = \frac{0}{1}$.

Es wird

$$\begin{aligned}
(\tfrac{r}{s} + \tfrac{r'}{s'}) + \tfrac{r''}{s''} &= \tfrac{rs'+r's}{ss'} + \tfrac{r''}{s''} \\
&= \tfrac{(rs'+r's)s''+r''ss'}{ss's''} \\
&= \tfrac{rs's''+r'ss''+r''ss'}{ss's''} \\
&= \tfrac{rs's''+s(r's''+r''s')}{ss's''} \\
&= \tfrac{r}{s} + \tfrac{r's''+r''s'}{s's''} \\
&= \tfrac{r}{s} + (\tfrac{r'}{s'} + \tfrac{r''}{s''})\ .
\end{aligned}$$

Es wird

$$\begin{aligned}
(\tfrac{r}{s} + \tfrac{r'}{s'})\tfrac{r''}{s''} &= \tfrac{rs'+r's}{ss'}\,\tfrac{r''}{s''} \\
&= \tfrac{(rs'+r's)r''}{ss's''} \\
&= \tfrac{(rs'+r's)r''s''}{ss's''^2} \\
&= \tfrac{rr''s's''+r'r''ss''}{ss''s's''} \\
&= \tfrac{rr''}{ss''} + \tfrac{r'r''}{s's''}\ .
\end{aligned}$$

Es ist $\frac{r}{s} = \frac{0}{1}$ genau dann, wenn $r\cdot 1 = s \cdot 0$; i.e. genau dann, wenn $r = 0$. Sei also $r \neq 0$. Es wird $\frac{r}{s}\frac{s}{r} = \frac{rs}{sr} = \frac{1}{1}$.

Aufgabe 24

(1) Es ist $\operatorname{Frob}_K(1) = 1^p = 1$. Es ist $\operatorname{Frob}_K(xy) = (xy)^p = x^p y^p$ für $x,\ y \in K$. Für die Verträglichkeit mit der Addition merken wir an, daß der Binomialkoeffizient $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ für $i \in [1, p-1]$ im Zähler einen Faktor p enthält, nicht aber im Nenner. Also ist diesenfalls $\binom{p}{i}$ ein Vielfaches von p. Es folgt

$$\operatorname{Frob}_K(x{+}y) \;=\; (x{+}y)^p \;=\; x^p{+}\tbinom{p}{1}\,x^{p-1}y^1{+}\cdots{+}\tbinom{p}{p-1}\,x^1y^{p-1}{+}y^p \;=\; x^p{+}y^p \;=\; \operatorname{Frob}_K(x){+}\operatorname{Frob}_K(y)\ ,$$

da in K gilt, daß $p = 0$.

Als Morphismus von Körpern ist Frob_K injektiv; vgl. Aufgabe 7.(1).

Ist K ein endlicher Körper, so ist Frob_K als injektive Selbstabbildung einer endlichen Menge auch bijektiv, und mithin ein Automorphismus.

Allgemein ist das aber nicht der Fall. So z.B. ist $\operatorname{Frob}_{\mathbf{F}_p(X)}$ nicht surjektiv, da $X \in \mathbf{F}_p(X)$ nicht in $\operatorname{Frob}_K(\mathbf{F}_p(X))$ liegt. Denn *wäre* $X = \left(\frac{f(X)}{g(X)}\right)^p$ für gewisse $f(X) \in \mathbf{F}_p[X]$ und $g(X) \in \mathbf{F}_p[X] \smallsetminus \{0\}$, dann wäre $Xg(X)^p = f(X)^p$, und also

$$1 \;\equiv_p\; 1 + p\deg g \;=\; \deg(Xg(X)^p) \;=\; \deg(f(X)^p) \;=\; p\deg f \;\equiv_p\; 0\ ,$$

Widerspruch.

(2) Es ist $\mathrm{Frob}_{\mathbf{F}_p}$ ein Automorphismus von $\mathbf{F}_p$.

Nach der ersten Bemerkung in §2.1 operiert aber jeder Automorphismus eines Körpers K von Charakteristik p identisch auf dem Primkörper, d.h. auf den Elementen im Bild von ε_K.

Im Falle $K = \mathbf{F}_p$ ist nun $\varepsilon_{\mathbf{F}_p}$ surjektiv, i.e. es ist $\mathbf{F}_p$ sein eigener Primkörper. Es folgt $\mathrm{Frob}_{\mathbf{F}_p} = \mathrm{id}_{\mathbf{F}_p}$. Elementweise geschrieben heißt dies, daß $x^p = \mathrm{Frob}_{\mathbf{F}_p}(x) = x$ für alle $x \in \mathbf{F}_p$. In anderen Worten, es ist $z^p \equiv_p z$ für alle $z \in \mathbf{Z}$, und dies ist die Aussage des Kleinen Fermatschen Satzes.

(3) Z.B. ist $X^3 - X + 1 \in \mathbf{F}_3[X]$ mangels Nullstelle irreduzibel. Sei

$$\mathbf{F}_{27} \ := \ \mathbf{F}_3[X]/(X^3 - X + 1)\mathbf{F}_3[X] \,.$$

Schreibe $\gamma := X + (X^3 - X + 1)\mathbf{F}_3[X]$. Dann ist $\gamma^3 = \gamma - 1$ und $3 = 0$ in $\mathbf{F}_{27}$. Eine Basis von $\mathbf{F}_{27}$ über $\mathbf{F}_3$ ist gegeben durch $(\gamma^0, \gamma^1, \gamma^2)$, und insbesondere ist $|\mathbf{F}_{27}| = 3^3 = 27$ wie gewünscht.

Sei $x = \lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0 \in \mathbf{F}_{27}$, wobei $\lambda_i \in \mathbf{F}_3$ für $i \in [0, 2]$. Es wird

$$\begin{array}{rcl}
\mathrm{Frob}_{\mathbf{F}_{27}}(x) - x & = & (\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0)^3 - (\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0) \\
& = & (\lambda_2^3\gamma^6 + \lambda_1^3\gamma^3 + \lambda_0^3\gamma^0) - (\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0) \\
& = & (\lambda_2\gamma^6 + \lambda_1\gamma^3 + \lambda_0\gamma^0) - (\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0) \\
& = & \lambda_2\gamma^6 + \lambda_1\gamma^3 - \lambda_2\gamma^2 - \lambda_1\gamma^1 \\
& = & \lambda_2(\gamma - 1)^2 + \lambda_1(\gamma - 1) - \lambda_2\gamma^2 - \lambda_1\gamma^1 \\
& = & \lambda_2\gamma^1 + (\lambda_1 + \lambda_2)\gamma^0 \,.
\end{array}$$

Dies ist wegen der linearen Unabhängigkeit von $(\gamma^0, \gamma^1, \gamma^2)$ über $\mathbf{F}_3$ genau dann gleich 0, wenn $\lambda_2 = 0$ und $\lambda_1 = 0$. Also ist

$$\{x \in \mathbf{F}_{27} \ : \ \mathrm{Frob}_{\mathbf{F}_{27}}(x) = x\} \ = \ \{\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0 \ : \ \lambda_i \in \mathbf{F}_3, \ \lambda_1 = \lambda_2 = 0\} \ = \ \mathbf{F}_3 \,.$$

Alternativ kann man hierfür anführen, daß $\mathrm{Frob}_{\mathbf{F}_{27}}(x) = x$ gilt für alle Elemente des Primkörpers $\mathbf{F}_3$, daß das Polynom $X^3 - X$ höchstens 3 Nullstellen in $\mathbf{F}_{27}$ haben kann und daß somit genau diese drei Elemente von $\mathbf{F}_3$ Nullstellen davon sind.

(4) Z.B. ist $X^4 + X + 1 \in \mathbf{F}_2[X]$ irreduzibel; vgl. Aufgabe 19.(3). Sei

$$\mathbf{F}_{16} \ := \ \mathbf{F}_2[X]/(X^4 + X + 1)\mathbf{F}_2[X] \,.$$

Schreibe $\delta := X + (X^4 + X + 1)\mathbf{F}_2[X]$. Dann ist $\delta^4 = \delta + 1$ und $2 = 0$ in $\mathbf{F}_{16}$. Eine Basis von $\mathbf{F}_{16}$ über $\mathbf{F}_2$ ist gegeben durch $(\delta^0, \delta^1, \delta^2, \delta^3)$, und insbesondere ist $|\mathbf{F}_{16}| = 2^4 = 16$ wie gewünscht.

Sei $x = \lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0 \in \mathbf{F}_{16}$, wobei $\lambda_i \in \mathbf{F}_2$ für $i \in [0, 3]$. Es wird

$$\begin{array}{rcl}
\mathrm{Frob}^2_{\mathbf{F}_{16}}(x) - x & = & (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0)^4 - (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0) \\
& = & (\lambda_3\delta^{12} + \lambda_2\delta^8 + \lambda_1\delta^4 + \lambda_0\delta^0) + (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0) \\
& = & (\lambda_3(\delta + 1)^3 + \lambda_2(\delta + 1)^2 + \lambda_1(\delta + 1)) + (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1) \\
& = & \lambda_3(\delta^2 + \delta + 1) + \lambda_2 + \lambda_1 \,.
\end{array}$$

Wegen der linearen Unabhängigkeit von $(\delta^0, \delta^1, \delta^2, \delta^3)$ über $\mathbf{F}_2$ ist dies genau dann gleich 0, wenn $\lambda_3 = 0$ und $\lambda_1 = \lambda_2$. Also ist

$$K := \{x \in \mathbf{F}_{16} \ : \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) = x\} \ = \ \{\lambda_1(\delta^2 + \delta) + \lambda_0 \ : \ \lambda_0, \, \lambda_1 \, \in \mathbf{F}_2\} \,.$$

Es ist K ein Teilkörper, da $\mathrm{Frob}^2_{\mathbf{F}_{16}}(1) = 1$, und da aus $x, y \in \mathbf{F}_{16}$ mit $\mathrm{Frob}^2_{\mathbf{F}_{16}}(x) = x$ und $\mathrm{Frob}^2_{\mathbf{F}_{16}}(y) = y$ folgt, daß

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(x - y) \ = \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) - \mathrm{Frob}^2_{\mathbf{F}_{16}}(y) \ = \ x - y \,,$$

daß

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(xy) \ = \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x)\,\mathrm{Frob}^2_{\mathbf{F}_{16}}(y) \ = \ xy$$

und daß, falls $x \neq 0$,

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(x^{-1}) \;=\; \mathrm{Frob}^2_{\mathbf{F}_{16}}(x)^{-1} \;=\; x^{-1}\;.$$

Also ist K ein Teilring abgeschlossen unter Inversion von nichtverschwindenden Elementen, und somit ein Teilkörper. (Festgestellt zu haben, daß ein Teilring eines endlichen Körpers vorliegt, hätte auch gereicht, da ein endlicher Integritätsbereich notwendig ein Körper ist.)

Nun ist

$$(\delta^2+\delta)^2 + (\delta^2+\delta) + 1 \;=\; \delta^4+\delta^2+\delta^2+\delta+1 \;=\; 0\;.$$

Also faktorisiert der Ringmorphismus

$$\begin{array}{rcl} \mathbf{F}_2[X] & \longrightarrow & \mathbf{F}_{16} \\ X & \longmapsto & \delta^2+\delta \end{array}$$

über den Ringmorphismus

$$\begin{array}{rcl} \mathbf{F}_2[X]/(X^2+X+1)\mathbf{F}_2[X] & \longrightarrow & \mathbf{F}_{16} \\ X + (X^2+X+1)\mathbf{F}_2[X] & \longmapsto & \delta^2+\delta\;. \end{array}$$

In der Tat schickt ersterer das Polynom X^2+X+1 auf $(\delta^2+\delta)^2+(\delta^2+\delta)+1 = 0_{\mathbf{F}_{16}}$, und also das Ideal $(X^2+X+1)\mathbf{F}_2[X]$ auf $\{0_{\mathbf{F}_{16}}\}$.

In Standardnotation umgeschrieben liest sich letzterer nun

$$\begin{array}{rcl} \mathbf{F}_4 & \longrightarrow & \mathbf{F}_{16} \\ \alpha & \longmapsto & \delta^2+\delta\;. \end{array}$$

Als Körpermorphismus ist dieser nun injektiv; vgl. Aufgabe 7. Da $\mathbf{F}_4 = \langle 1,\alpha\rangle_{\mathbf{F}_2}$ (Vektorraumerzeugnis über $\mathbf{F}_2$), und da dieser Morphismus $\mathbf{F}_2$-linear ist, ist das Bild gegeben durch $\langle 1,\delta^2+\delta\rangle_{\mathbf{F}_2}$. Dies ist aber gerade gleich K. Somit liefert unser injektiver Körpermorphismus durch Einschränkung des Bildbereichs einen Körperisomorphismus

$$\begin{array}{rcl} \mathbf{F}_4 & \longrightarrow & K \\ \alpha & \longmapsto & \delta^2+\delta\;. \end{array}$$

Man hätte zur Konstruktion von $\mathbf{F}_{16}$ alternativ auch ein irreduzibles Polynom von Grad 2 in $\mathbf{F}_4[X]$ verwenden können; vgl. Aufgabe 19.(3).

Aufgabe 25

(1) Es ist $f'(X) = X^{s-1}(X-1)^{t-1}(tX+s(X-1))$. Um also zu zeigen, daß $\mathrm{ggT}(f(X),f'(X)) = X^{s-1}(X-1)^{t-1}$, genügt es, zu zeigen, daß $X(X-1)$ und $tX+s(X-1)$ teilerfremd sind. Und in der Tat, X teilt letzteres Polynom nicht, da X wegen $s\neq 0$ den Summanden $s(X-1)$ nicht teilt. Genauso teilt $(X-1)$ letzteres Polynom nicht, da es wegen $t\neq 0$ den Summanden tX nicht teilt.

So zu argumentieren können wir uns leisten, da wir in $K[X]$ die eindeutige Zerlegung in irreduzible Polynome kennen; vgl. §1.9.

(2) Nach Voraussetzung können wir $f(X) = \prod_{i\in[1,r]}(X-\gamma_i)^{s_i}$ für gewisse $r\geqslant 0$, $\gamma_i\in K$ und $s_i\geqslant 1$ schreiben, wobei $\gamma_i\neq\gamma_j$ falls $i\neq j$.

Beachte, daß

$$f'(X) \;=\; \sum_{k\in[1,r]} s_i(X-\gamma_i)^{s_i-1} \prod_{i\in[1,r]\smallsetminus\{k\}} (X-\gamma_i)^{s_i}\;.$$

Ist $s_i = 1$ für alle $i\in[1,r]$, so wird $f'(\gamma_j) = \prod_{i\in[1,r]\smallsetminus\{j\}}(\gamma_j-\gamma_i)\neq 0$ und somit $f'(X)$ kein Vielfaches von $(X-\gamma_j)$ für alle $j\in[1,r]$. Folglich ist $\mathrm{ggT}(f(X),f'(X)) = 1$.

Ist umgekehrt $s_j\geqslant 2$ für ein $j\in[1,r]$, so wird $f'(\gamma_j) = s_j(\gamma_i-\gamma_i)^{s_j-1}\prod_{i\in[1,r]\smallsetminus\{j\}}(\gamma_j-\gamma_i) = 0$. Also ist $(X-\gamma_j)$ ein Teiler von $f'(X)$, und also insgesamt ein Teiler von $\mathrm{ggT}(f(X),f'(X))$. Folglich ist $\mathrm{ggT}(f(X),f'(X))\neq 1$.

(3) Sei $g_K(X)$ der in $K[X]$ genommene ggT von $f(X)$ und $h(X)$.

Sei $g_L(X)$ der in $L[X]$ genommene ggT von $f(X)$ und $h(X)$.

Mit dem Euklidschen Algorithmus gibt es $s_K(X),\, t_K(X) \in K[X]$ mit

$$(*) \qquad f(X)s_K(X) + h(X)t_K(X) \;=\; g_K(X)$$

und $s_L(X),\, t_L(X) \in L[X]$ mit

$$(**) \qquad f(X)s_L(X) + h(X)t_L(X) \;=\; g_L(X)\,;$$

vgl. Aufgabe 8.

Da $g_L(X)$ ein Teiler von $f(X)$ und von $h(X)$ in $L[X]$ ist, zeigt $(*)$, daß $g_L(X)$ auch ein Teiler von $g_K(X)$ in $L[X]$ ist.

Da $g_K(X)$ ein Teiler von $f(X)$ und von $h(X)$ in $K[X]$ ist, zeigt $(**)$, daß $g_K(X)$ auch ein Teiler von $g_L(X)$ in $L[X]$ ist.

Insgesamt folgt $g_K(X) = g_L(X)$.