M. Künzer

Galoistheorie, WS 08/09

Lösung 10

Aufgabe 33

(1) Nach dem Korollar in §2.5.4. existiert (bis auf Isomorphie genau) ein Körper mit p^k Elementen, genannt $\mathbf{F}_{p^k}$.

Nach Aufgabe 27.(5) gibt es in $\mathbf{F}_{p^k}^\times$ ein Element y mit $\mathrm{o}(y) = p^k - 1$. Mit Aufgabe 11.(1.b) ist $|\langle y\rangle| = \mathrm{o}(y)$, und folglich

$$\mathbf{F}_{p^k}^\times \;=\; \langle y\rangle \;.$$

In der Lösung zu Aufgabe 11.(1.b) haben wir gesehen, daß

$$\langle y\rangle \;=\; \{y^i \;:\; i \in \mathbf{Z}\} \;=\; \{y^i \;:\; i \in [0, \mathrm{o}(y)-1]\} \;=\; \{y^i \;:\; i \in [0, p^k-2]\} \;.$$

Insgesamt ist also

$$\mathbf{F}_{p^k}^\times \;=\; \{y^i \;:\; i \in [0, p^k-2]\}$$

Insbesondere ist

$$\mathbf{F}_{p^k} \;=\; \mathbf{F}_p(y) \;=\; \{f(y) \;:\; f(X) \in \mathbf{F}_p[X]\} \;,$$

da in letzterer Menge das Element y^i für alle $i \geqslant 0$ und das Element 0 auftreten.

Mit Satz 2.(2) (Minimalpolynom) ist

$$\deg \mu_{y,\mathbf{F}_p} \;=\; [\mathbf{F}_p(y) : \mathbf{F}_p] \;=\; [\mathbf{F}_{p^k} : \mathbf{F}_p] \;=\; k \;.$$

Mit Satz 2.(3) ist $\mu_{y,\mathbf{F}_p}(X)$ irreduzibel.

(2) Sei $K := \mathbf{F}_p[T]/f(T)\mathbf{F}_p[T]$. Sei $y := T + f(T)\mathbf{F}_p[T] \in K^\times$. Es ist $\mathrm{o}(y)$ ein Teiler von $|K^\times| = p^k - 1$. Also ist $y^{p^k} = y \cdot y^{p^k-1} = y$.

Da y somit eine Nullstelle von $X^{p^k} - X$ ist ist mit Satz 2.(2) das Minimalpolynom $\mu_{y,\mathbf{F}_p}(X)$ ein Teiler von $X^{p^k} - X$ in $\mathbf{F}_p[X]$. Nun ist aber $\mu_{y,\mathbf{F}_p}(X) = f(X)$, e.g. da dies ein normiertes irreduzibles Polynom mit Nullstelle y ist.

Sei $z \in K^\times$. Genauso wie für y folgt auch, daß z eine Nullstelle von $X^{p^k} - X$ ist. Ferner ist 0 eine Nullstelle dieses Polynoms. Also hat dieses Polynom sämtliche Elemente von K als Nullstelle. Sukzessives Abdividieren und Gradvergleich liefert

$$X^{p^k} - X \;=\; \prod_{z \in K} (X - z) \;\in\; K[X] \;.$$

Da nun $f(X)$ auch in $K[X]$ ein Teiler von $X^{p^k} - X$ ist, folgt, daß $f(X)$ in $K[X]$ in Linearfaktoren zerfällt (von denen keiner mit Exponent $\geqslant 2$ auftritt).

Da in der Zerlegung von $X^{p^k} - X$ in $K[X]$ kein Linearfaktor mit Exponent $\geqslant 2$ auftritt, kann $f(X)^2$ das Polynom $X^{p^k} - X$ in $K[X]$ und daher auch in $\mathbf{F}_p[X]$ nicht teilen. (Es folgt auch noch, daß in der Zerlegung von $f(X)$ in $K[X]$ kein Linearfaktor mit Exponent $\geqslant 2$ auftritt.)

Aufgabe 34

(1) Sei $\mathbf{Q}(a,b)|\mathbf{Q}$ mit $a^3 + a + 1 = 0$ und $b^2 + ab + (a^2+1) = 0$. Dann wird

$$X^3 + X + 1 \;=\; (X-a)(X-b)(X+a+b) \;\in\; \mathbf{Q}(a,b)[X]$$

Da auch $\mathbf{Q}(a,b,-a-b) = \mathbf{Q}(a,b)$, ist $\mathbf{Q}(a,b)$ der Zerfällungskörper von $X^3 + X + 1 \in \mathbf{Q}[X]$.

Es ist $[\mathbf{Q}(a,b) : \mathbf{Q}] = [\mathbf{Q}(a,b) : \mathbf{Q}(a)][\mathbf{Q}(a) : \mathbf{Q}] = 2 \cdot 3 = 6$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^3 + X + 1);
KK<a> := ext<Q | X^3 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^3 + XX + 1);
KKK<b> := ext<KK | XX^2 + a*XX + a^2 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^3 + XXX + 1);
```

(2) Sei $\mathbf{Q}(a,b)|\mathbf{Q}$ mit $a^4+4a^2+4a+8=0$ und $b^3+ab^2+(a^2+4)b+(a^3+4a+8)=0$. In $\mathbf{Q}(a,b)[X]$ wird

$$\begin{aligned} & X^4+4X^2+8X+8 \\ = \; & (X-a)\cdot(X-b)\cdot \\ & \cdot\big(X+\tfrac{1}{28}(-2a^3+3a^2-2a-6)b^2+\tfrac{1}{14}(3a^3-a^2+10a+16)b+\tfrac{1}{14}(-2a^3+3a^2-2a-20)\big)\cdot \\ & \cdot\big(X+\tfrac{1}{28}(2a^3-3a^2+2a+6)b^2+\tfrac{1}{14}(-3a^3+a^2-10a-2)b+\tfrac{1}{14}(2a^3-3a^2+16a+20)\big)\ . \end{aligned}$$

Da $\mathbf{Q}(a,b)$ von den Nullstellen dieses Polynoms erzeugt wird, ist $\mathbf{Q}(a,b)$ der Zerfällungskörper von $X^4+4X^2+8X+8\in\mathbf{Q}[X]$.

Es ist $[\mathbf{Q}(a,b):\mathbf{Q}]=[\mathbf{Q}(a,b):\mathbf{Q}(a)][\mathbf{Q}(a):\mathbf{Q}]=3\cdot 4=12$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + 4*X^2 + 8*X + 8);
KK<a> := ext<Q | X^4 + 4*X^2 + 8*X + 8>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + 4*XX^2 + 8*XX + 8);
KKK<b> := ext<KK | XX^3 + a*XX^2 + (a^2 + 4)*XX + a^3 + 4*a + 8>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^4 + 4*XXX^2 + 8*XXX + 8);
```

(3) Sei $\mathbf{Q}(a,b,c)|\mathbf{Q}$ mit $a^6-a^3+2=0$, $b^3+(a^3-1)=0$ und $c^2+ac+a^2=0$. In $\mathbf{Q}(a,b,c)[X]$ wird

$$X^6-X^3+2 \;=\; (X-a)(X-b)(X-c)(X+c+a)\big(X-\tfrac{1}{2}(a^5-a^2)bc+b\big)\big(X+\tfrac{1}{2}(a^5-a^2)bc\big)\ .$$

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 - X^3 + 2);
KK<a> := ext<Q | X^6 - X^3 + 2>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 - XX^3 + 2);
KKK<b> := ext<KK | XX^3 + a^3 - 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 - XXX^3 + 2);
KKKK<c> := ext<KKK | XXX^2 + a*XXX + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 - XXXX^3 + 2);
```

Da $\mathbf{Q}(a,b,c)$ von den Nullstellen dieses Polynoms erzeugt wird, ist $\mathbf{Q}(a,b,c)$ der Zerfällungskörper von $X^6-X^3+2\in\mathbf{Q}[X]$.

Es ist $[\mathbf{Q}(a,b,c):\mathbf{Q}]=[\mathbf{Q}(a,b,c):\mathbf{Q}(a,b)][\mathbf{Q}(a,b):\mathbf{Q}(a)][\mathbf{Q}(a):\mathbf{Q}]=2\cdot 3\cdot 6=36$.

(4) In $\mathbf{Q}(\sqrt{2},\mathrm{i})$ wird

$$X^2+1 \;=\; (X+\mathrm{i})(X-\mathrm{i})\ .$$

Somit ist $\mathbf{Q}(\sqrt{2},\mathrm{i})$ der Zerfällungskörper von X^2+1 über $\mathbf{Q}(\sqrt{2})$.

Es wird $[\mathbf{Q}(\sqrt{2},\mathrm{i}) : \mathbf{Q}(\sqrt{})] = 2$, da X^2+1 in $\mathbf{Q}(\sqrt{2})[X]$ irreduzibel ist, da es ja sogar in $\mathbf{R}[X]$ irreduzibel ist.

Magma ist nicht unbedingt erforderlich. Will man es anwenden, sieht das z.B. wie folgt aus.

```
Q := Rationals();
S<T> := PolynomialRing(Q);
K<a> := ext<Q | T^2 - 2>;
R<X> := PolynomialRing(K);
Factorisation(X^2 + 1);
KK<b> := ext<K | X^2 + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^2 + 1);
```

Teilaufgabe (4) diene nur der Illustration, daß der Grundkörper auch eine Erweiterung von $\mathbf{Q}$ sein kann.

Aufgabe 35

Sei L ein Zerfällungskörper von X^p-a. Sei $b\in L$ eine Nullstelle von X^p-a, i.e. sei $b^p=a$. Dann ist $(X-b)^p = X^p-b^p = X^p-a$ in $L[X]$.

Sei *angenommen,* es hat X^p-a einen nichttrivialen normierten Faktor $f(X)\in K[X]$. Dann ist $f(X)$ in $L[X]$ von der Form $(X-b)^s$ für ein $s\in[1,p-1]$. Insbesondere ist $f_0=(-b)^s\in K$. Seien $u,\,v\in\mathbf{Z}$ so, daß $su+pv=1$. Es folgt

$$-b \;=\; (-b)^{su+pv} \;=\; \underbrace{((-b)^s)^u}_{\in K}\underbrace{(-1)^{pv}a^v}_{\in K} \;\in\; K\;,$$

und mithin $b\in K$. Also ist a die p-te Potenz des Elements b von K, im *Widerspruch* zur Voraussetzung an a.

Somit ist X^p-a als in $K[X]$ irreduzibel nachgewiesen.

Nun ist $\mu_{b,K}(X)=X^p-a$, da dies ein normiertes irreduzibles Polynom in $K[X]$ mit Nullstelle b ist. Mit Satz 2.(2) (Minimalpolynom) folgt nun, daß $[K(b):K]=p$. Da andererseits, wie oben schon festgestellt,

$$X^p-a \;=\; (X-b)^p \;\in\; K(b)[X]$$

ist, ist $K(b)$ ein Zerfällungskörper von X^p-a.

Da zwei Zerfällungskörper isomorph sind, folgt $[L:K]=[K(b):K]=p$. (Da desweiteren $K(b)\subseteq L$, folgt $K(b)=L$.)

Da der Frobenius für endliche Körper bijektiv ist, kann ein Element $a\in K$ wie in der Aufgabenstellung vorausgesetzt nur für einen unendlichen Körper K der Charakteristik p (wie z.B. $\mathbf{F}_p(T)$) existieren.

Aufgabe 36

(1) Die Aussage ist falsch. So z.B. ist in Aufgabe 34.(1) (in den Bezeichnungen der dortigen Lösung) zwar $\mu_{a,\mathbf{Q}}(X)=X^3+X+1$, aber $\mathbf{Q}(a)$ kein Zerfällungskörper von X^3+X+1, da die Zerlegung dieses Polynom in irreduzible Faktoren in $\mathbf{Q}(a)[X]$ die Gestalt

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

hat, und darin also ein Faktor von Grad $\geqslant 2$ aufgetreten ist.

(2) Die Aussage ist richtig. Denn es ist $X-y$ ein Teiler von $\mu_{y,K}(X)$ in $K(y)[X]$, da $\mu_{y,K}(y)=0$. Es ist aber mit Satz 2.(2) (Minimalpolynom) $\deg\mu_{y,K}=[K(y):K]=2$. Somit liefert Division die Zerlegung

$$\mu_{y,K}(X) \;=\; (X-y)(X-z)$$

in $K(y)[X]$. Da insbesondere $z\in K(y)$ ist, ist $K(y,z)=K(y)$ der Zerfällungskörper von $\mu_{y,K}(X)$.