M. Künzer

Galoistheorie, WS 08/09

Lösung 9

Aufgabe 29

(1) Es ist $X^4 + X + 1$ irreduzibel in $\mathbf{Q}[X]$.

Magma:

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + X + 1);
```

(2) Es ist

$$X^5 + X + 1 \;=\; (X^2 + X + 1)(X^3 - X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{Q}[X]$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^5 + X + 1);
```

(3) Schreibe $\gamma := \mathrm{i}\sqrt{3}$. Es ist

$$X^5 + X + 1 \;=\; (X + \frac{1-\gamma}{2})(X + \frac{1+\gamma}{2})(X^3 - X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{Q}(\gamma)[X]$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
KK<ga> := ext<Q | X^2 + 3>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^5 + XX + 1);
```

(4) Es ist

$$X^8 - X \;=\; X(X+1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_2[X]$.

```
F := GF(2);
R<X> := PolynomialRing(F);
Factorisation(X^8 - X);
```

(5) Es ist

$$X^8 - X \;=\; X(X+1)(X+\beta)(X+\beta^2)(X+\beta^3)(X+\beta^4)(X+\beta^5)(X+\beta^6)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_8[X]$ (was man auch ohne Magma erkennt, da jedes Element von $\mathbf{F}_8$ eine Nullstelle von $X^8 - X$ ist).

```
F := GF(2);
R<X> := PolynomialRing(F);
FF<b> := ext<F | X^3 + X + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^8 - XX);
```

(6) Es ist

$$X^{15} - X + 1 =$$
$$(X + \iota + 1)(X - \iota + 1)(X^2 + X + \iota - 1)(X^2 + X - \iota - 1)(X^9 - X^8 - X^7 - X^4 - X^3 + X^2 - X + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_9[X]$.

```
F := GF(3);
R<X> := PolynomialRing(F);
FF<i> := ext<F | X^2 + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^15 - XX + 1);
```

Aufgabe 30

(1) Es ist $X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}[X]$. Sei $\mathbf{Q}(a)|\mathbf{Q}$ mit $a^2 + a + 1 = 0$.

Es ist $X^4 + X^2 + 1 = (X + a)(X - a)(X + a + 1)(X - a - 1)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a)[X]$.

Mit $L = \mathbf{Q}(a)$ und $K = \mathbf{Q}$ ist $[L : K] = 2$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + X^2 + 1);
KK<a> := ext<Q | X^2 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + XX^2 + 1);
```

(2) Es ist $X^6 + X^2 + 1$ irreduzibel in $\mathbf{Q}[X]$. Sei $\mathbf{Q}(a)|\mathbf{Q}$ mit $a^6 + a^2 + 1 = 0$.

Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X^4 + a^2X^2 + (a^4 + 1))$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a)[X]$. Sei $\mathbf{Q}(a, b)|\mathbf{Q}(a)$ mit $b^4 + a^2b^2 + (a^4 + 1) = 0$.

Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X + b)(X - b)(X^2 + (a^2 + b^2))$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a, b)[X]$. Sei $\mathbf{Q}(a, b, c)|\mathbf{Q}(a, b)$ mit $c^2 + (a^2 + b^2) = 0$.

Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X + b)(X - b)(X + c)(X - c)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a, b, c)[X]$.

Mit $L = \mathbf{Q}(a)$ und $K = \mathbf{Q}$ ist

$$[L : K] \;=\; [\mathbf{Q}(a, b, c) : \mathbf{Q}(a, b)][\mathbf{Q}(a, b) : \mathbf{Q}(a)][\mathbf{Q}(a) : \mathbf{Q}] \;=\; 6 \cdot 4 \cdot 2 \;=\; 48\,,$$

wie man den Graden der jeweiligen Minimalpolynome entnimmt.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 + X^2 + 1);
KK<a> := ext<Q | X^6 + X^2 + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 + XX^2 + 1);
KKK<b> := ext<KK | XX^4 + a^2*XX^2 + a^4 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 + XXX^2 + 1);
KKKK<c> := ext<KKK | XXX^2 + b^2 + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 + XXXX^2 + 1);
```

(3) Es ist $X^4 + X + 1 = (X^2 + X + \alpha)(X^2 + X + \alpha^2)$ die Zerlegung in irreduzible Polynome in $\mathbf{F}_4[X]$. Sei $\mathbf{F}_4(b)|\mathbf{F}_4$ mit $b^2 + b + \alpha = 0$.

Es ist $X^4 + X + 1 = (X + b)(X + b + \alpha)(X + b + 1)(X + b + \alpha + 1)$ die Zerlegung in irreduzible Polynome in $\mathbf{F}_4(b)[X]$.

Mit $L = \mathbf{F}_4(b)$ und $K = \mathbf{F}_4$ ist $[L : K] = 2$ (und insbesondere $|\mathbf{F}_4(b)| = 16$.).

```
F := GF(2);
R<X> := PolynomialRing(F);
FF<a> := ext<F | X^2 + X + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^4 + XX + 1);
FFF<b> := ext<FF | XX^2 + XX + a>;
RRR<XXX> := PolynomialRing(FFF);
Factorisation(XXX^4 + XXX + 1);
```

…plus eine Umformung der entstandenen Koeffizienten von Hand.

Aufgabe 31

(1) Zunächst stellen wir mittels Magma fest, daß $X^2 - 2 \in \mathbf{Q}[X]$ und $X^2 - 3 \in \mathbf{Q}(\sqrt{2})[X]$ irreduzibel sind. Folglich ist

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}] \;=\; [\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] \;=\; 2\cdot 2 \;=\; 4\,.$$

Eine Basis von $\mathbf{Q}(\sqrt{2},\sqrt{3})$ über $\mathbf{Q}$ ist gegeben durch

$$(1,\,\sqrt{2},\,\sqrt{3},\,\sqrt{6})\;,$$

wofür wir $\sqrt{2}\sqrt{3} = \sqrt{6}$ vereinfacht haben.

Wir verwenden die Charakterisierung von $\mu_{\sqrt{2}+\sqrt{3},\mathbf{Q}}(X)$ als normiertes Polynom minimalen Grades in $\mathbf{Q}[X]$ mit Nullstelle $\sqrt{2}+\sqrt{3}$.

Wir berechnen also einmal die Potenzen von $\sqrt{2}+\sqrt{3}$, ausgedrückt in der vorstehenden Basis.

$$\begin{array}{rcrcrcrcr}
(\sqrt{2}+\sqrt{3})^0 & = & 1\cdot 1 & + & 0\cdot\sqrt{2} & + & 0\cdot\sqrt{3} & + & 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^1 & = & 0\cdot 1 & + & 1\cdot\sqrt{2} & + & 1\cdot\sqrt{3} & + & 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^2 & = & 5\cdot 1 & + & 0\cdot\sqrt{2} & + & 0\cdot\sqrt{3} & + & 2\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^3 & = & 0\cdot 1 & + & 11\cdot\sqrt{2} & + & 9\cdot\sqrt{3} & + & 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^4 & = & 49\cdot 1 & + & 0\cdot\sqrt{2} & + & 0\cdot\sqrt{3} & + & 20\cdot\sqrt{6}
\end{array}$$

Es stellt sich mittels Linearer Algebra heraus, daß

$$\Big((\sqrt{2}+\sqrt{3})^0,\,(\sqrt{2}+\sqrt{3})^1,\,(\sqrt{2}+\sqrt{3})^2,\,(\sqrt{2}+\sqrt{3})^3\Big)$$

linear unabhängig ist.

Ferner stellt sich mittels Linearer Algebra heraus, daß

$$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + (\sqrt{2}+\sqrt{3})^0 \;=\; 0\,.$$

Dies, zusammen mit der vorher festgestellen linearen Unabhängigkeit, zeigt, daß $X^4 - 10X^2 + 1$ das normierte Polynom kleinsten Grades mit Nullstelle $\sqrt{2}+\sqrt{3}$ ist. In anderen Worten, wir haben

$$\mu_{\sqrt{2}+\sqrt{3},\mathbf{Q}}(X) \;=\; X^4 - 10X^2 + 1\,.$$

Insbesondere ist $[\mathbf{Q}(\sqrt{2}+\sqrt{3}) : \mathbf{Q}] = 4$. Aus Dimensionsgründen folgt, daß $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$.

(2) Zunächst ist natürlich

$$\begin{array}{rcl}
\mu_{0,\mathbf{F}_2}(X) & = & X\\
\mu_{1,\mathbf{F}_2}(X) & = & X+1\,.
\end{array}$$

Es hat das irreduzible Polynom $X^3 + X + 1 \in \mathbf{F}_2[X]$ die Nullstelle β, und also auch die Nullstellen β^2 und β^4, wie eine Anwendung des Frobenius liefert; vgl. Bemerkung in §2.3.4. Also

$$\begin{array}{rcl}
\mu_{\beta,\mathbf{F}_2}(X) & = & X^3 + X + 1\\
\mu_{\beta^2,\mathbf{F}_2}(X) & = & X^3 + X + 1\\
\mu_{\beta^4,\mathbf{F}_2}(X) & = & X^3 + X + 1\,.
\end{array}$$

Berechnen wir das Minimalpolynom von β^3. Die Potenzen von β^3, ausgedrückt in der Standardbasis $(\beta^0, \beta^1, \beta^2)$, sind gegeben durch

$$\begin{array}{rcrcrcr} (\beta^3)^0 & = & 1\cdot\beta^0 & + & 0\cdot\beta^1 & + & 0\cdot\beta^2 \\ (\beta^3)^1 & = & 1\cdot\beta^0 & + & 1\cdot\beta^1 & + & 0\cdot\beta^2 \\ (\beta^3)^2 & = & 1\cdot\beta^0 & + & 0\cdot\beta^1 & + & 1\cdot\beta^2 \\ (\beta^3)^3 & = & 0\cdot\beta^0 & + & 0\cdot\beta^1 & + & 1\cdot\beta^2\,. \end{array}$$

Wir sehen, daß

$$\big((\beta^3)^0,\, (\beta^3)^1,\, (\beta^3)^2\big)$$

linear unabhängig über $\mathbf{F}_2$ ist. Ferner ist

$$(\beta^3)^3 + (\beta^3)^2 + (\beta^3)^0 \;=\; 0\,.$$

Beides zusammen gibt X^3+X^2+1 als normiertes Polynom minimalen Grades mit Nullstelle β^3, in anderen Worten, $\mu_{\beta^3,\mathbf{F}_2}(X) = X^3 + X^2 + 1 \in \mathbf{F}_2[X]$. Anwendung des Frobenius liefert die weiteren Nullstellen β^6 und $\beta^{12} = \beta^5$; vgl. Bemerkung in §2.3.4. Also

$$\begin{array}{rcl} \mu_{\beta^3,\mathbf{F}_2}(X) & = & X^3+X^2+1 \\ \mu_{\beta^5,\mathbf{F}_2}(X) & = & X^3+X^2+1 \\ \mu_{\beta^6,\mathbf{F}_2}(X) & = & X^3+X^2+1\,. \end{array}$$

Ein Automorphismus von $\mathbf{F}_8 = \mathbf{F}_2(\beta)$ schränkt nach der ersten Bemerkung in §2.1 identisch auf $\mathbf{F}_2$ ein und muß mit der Bemerkung in §2.3.4 folglich das Element β auf eine Nullstelle seines Minimalpolynoms $X^3 + X + 1$ über $\mathbf{F}_2$ schicken, als da wären β, β^2 und β^4.

Nun schickt aber $\mathrm{Frob}^0_{\mathbf{F}_8}$ bereits β nach β, $\mathrm{Frob}^1_{\mathbf{F}_8}$ schickt β nach β^2 und $\mathrm{Frob}^2_{\mathbf{F}_8}$ schickt β nach β^4.

Da ein Körpermorphismus von $\mathbf{F}_8 = \mathbf{F}_2(\beta)$ in einen anderen Körper bereits durch das Bild von β festliegt, gibt es also außer den Potenzen des Frobenius keine weiteren Automorphismen von $\mathbf{F}_8$.

Aufgabe 32

Es ist $K(y)|K(y^2)|K$. Um zu zeigen, daß $\deg \mu_{y^2,K} = \deg \mu_{y,K}$ ist, genügt es zu zeigen, daß $K(y^2) = K(y)$; vgl. Satz 2.(2) (Minimalpolynom).

Nun ist $K(y) = K(y^2)(y)$ ebenfalls eine endliche monogene Erweiterung. Es ist y eine Nullstelle von $X^2 - y^2 \in K(y^2)[X]$. Also ist $\mu_{y,K(y^2)}(X)$ ein Teiler von $X^2 - y^2$, und insbesondere von Grad 1 oder von Grad 2. Dies zieht $[K(y) : K(y^2)] \in \{1, 2\}$ nach sich.

Mit dem Gradsatz ist nun $[K(y) : K] = [K(y) : K(y^2)][K(y^2) : K]$. Da $[K(y) : K]$ ungerade ist, folgt $[K(y) : K(y^2)] = 1$, und mithin $K(y) = K(y^2)$.

Zur Frage, ob $\mu_{y,K}(X) = \mu_{y^2,K}(X)$ ist. Dies ist im allgemeinen nicht der Fall. Sei z.B. $K = \mathbf{Q}$ und $y = \sqrt[3]{2}$. Es ist

$$\mu_{\sqrt[3]{2},\mathbf{Q}}(X) \;=\; X^3 - 2\,,$$

wohingegen sich

$$\mu_{(\sqrt[3]{2})^2,\mathbf{Q}}(X) \;=\; X^3 - 4$$

ergibt. Denn beide Polynome sind laut Magma irreduzibel und haben das jeweilig angegebene Element als Nullstelle.

Ferner liefert der Grad des ersten Minimalpolynoms, daß in der Tat $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ ungerade ist.