M. Künzer

Galoistheorie, WS 08/09

Lösung 13

Aufgabe 44

(1) Schreibe $Z := \{z \in L\ :\ z^n = 1\}$. Es ist $1 \in Z$. Sind $z,\ \tilde{z}\ \in\ Z$, so ist auch $(z\tilde{z}^{-1})^n = z^n(\tilde{z}^n)^{-1} = 1$, also $z\tilde{z}^{-1} \in Z$. Also ist $Z \leqslant L^\times$.

Es zerfällt $X^n - 1$ in $L[X]$ in Linearfaktoren. Da nun

$$\mathrm{ggT}(X^n - 1, (X^n - 1)') \;=\; \mathrm{ggT}(X^n - 1,\, nX^{n-1}) \;=\; 1 \qquad (^1)\,,$$

enthält diese Produktzerlegung von $X^n - 1$ auch n verschiedene Linearfaktoren; vgl. Aufgabe 25.(2). Da aber Z gerade die Nullstellenmenge von $X^n - 1$ in L ist, folgt $|Z| = n$.

Wir verwenden die Argumente für Aufgabe 27.(5). Sei ζ_n ein Element von Z maximaler Ordnung. Es ist $\mathrm{o}(\zeta_n)$ ein Teiler von $|Z| = n$.

Mit Aufgabe 27.(4) ist $\mathrm{o}(z)$ ein Teiler von $\mathrm{o}(\zeta_n)$ für alle $z \in Z$. Also ist z eine Nullstelle von $X^{\mathrm{o}(\zeta_n)} - 1$ in L. Da letzteres Polynom mithin n verschiedene Nullstellen in L hat, folgt $n \leqslant \deg(X^{\mathrm{o}(\zeta_n)} - 1) = \mathrm{o}(\zeta_n)$.

Zusammen ist $\mathrm{o}(\zeta_n) = n$. Aber dies impliziert $|\langle\zeta_n\rangle| = \mathrm{o}(\zeta_n) = n = |Z|$, und somit $\langle\zeta_n\rangle = Z$; vgl. Aufgabe 11.(1.b).

Da $L = K(z : z \in Z)$ als Zerfällungskörper von $X^n - 1 \in K[X]$, und da $Z = \{\zeta_n^i\ :\ i \in [0, n-1]\}$, ist $L = K(\zeta_n)$.

(2) Zunächst einmal halten wir fest, daß $\mathrm{ggT}(k, n) = \mathrm{ggT}(k + zn,\, n)$ für $z \in \mathbf{Z}$, und also das Auswahlkriterium für $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, es sei $\mathrm{ggT}(k, n) = 1$, unabhängig vom betrachteten Repräsentanten k ist.

Wir haben zu zeigen, daß das Produkt zweier Elemente von $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ wieder in dieser Menge liegt, daß eine Eins in $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ liegt, und daß zu jedem Element von $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ein multiplikativ Inverses in $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ vorhanden ist. Dann ist $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ mit der Multiplikation eine Gruppe; abelsch, da $\mathbf{Z}/n\mathbf{Z}$ ein kommutativer Ring ist.

Seien $k + n\mathbf{Z},\ \tilde{k} + n\mathbf{Z}\ \in\ \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Dann ist $\mathrm{ggT}(k, n) = 1$ und $\mathrm{ggT}(\tilde{k}, n) = 1$, und somit auch $\mathrm{ggT}(k\tilde{k}, n) = 1$, i.e. $(k + n\mathbf{Z})(\tilde{k} + n\mathbf{Z}) \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$.

Es ist $1 + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ein Einselement.

Sei $k + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Da $\mathrm{ggT}(k, n) = 1$, gibt es $s,\ t\ \in\ \mathbf{Z}$ mit $sk + tn = 1$; vgl. Aufgabe 2. Es ist $\mathrm{ggT}(s, n) = 1$, da ein gemeinsamer Faktor von s und n auch in $sk + tn = 1$ auftreten würde. Also ist $s + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Ferner ist

$$(s + n\mathbf{Z})(k + n\mathbf{Z}) \;=\; sk + n\mathbf{Z} \;=\; (sk + tn) + n\mathbf{Z} \;=\; 1 + n\mathbf{Z}\,.$$

Die Elementordnungen in $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$ ergeben sich wie folgt. Wir verwenden die Konvention, z für $z + 12\mathbf{Z}$ zu schreiben.

$$\begin{array}{lcl} \mathrm{o}(1) & = & 1 \\ \mathrm{o}(5) & = & 2 \\ \mathrm{o}(-5) & = & 2 \\ \mathrm{o}(-1) & = & 2 \end{array}$$

Folglich ist $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$ nicht von einem Element erzeugt, denn dieses müßte Ordnung 4 haben; vgl. Aufgabe 11.(1.b).

Ist jedoch p prim, so ist $\mathrm{U}(\mathbf{Z}/p\mathbf{Z}) = \mathbf{F}_p^\times$ von einem Element erzeugt, vgl. Aufgabe 27.(5).

[1] Wofür man char $K = 0$ benötigt.

(3) Zeigen wir, daß eine wohldefinierte Abbildung $\mathrm{Gal}(L|K) \longrightarrow \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, $\sigma \longmapsto i_\sigma$ vorliegt.

Zum einen ist zu zeigen, daß aus $\zeta_n^i = \zeta_n^j$ folgt, daß $i + n\mathbf{Z} = j + n\mathbf{Z}$; daß also das Element ζ_n^i die Restklasse des Exponenten i modulo n bestimmt. Nun ist aber $\mathrm{o}(\zeta_n) = n$ in $L^\times$ nach (1). Aus $\zeta_n^i = \zeta_n^j$, d.h. aus $\zeta_n^{j-i} = 1$ folgt also, daß $n = \mathrm{o}(\zeta_n)$ den Exponenten $j - i$ teilt, d.h. daß $j \equiv_n i$.

Zum anderen ist zu zeigen, daß $\mathrm{ggT}(i_\sigma, n) = 1$ für $\sigma \in \mathrm{Gal}(L|K)$. Nun ist aber

$$\zeta_n \;=\; \sigma^{-1}(\sigma(\zeta_n)) \;=\; \sigma^{-1}(\zeta_n^{i_\sigma}) \;=\; \sigma^{-1}(\zeta_n)^{i_\sigma} \;=\; \zeta_n^{i_{\sigma^{-1}}\cdot i_\sigma}$$

Folglich ist $i_{\sigma^{-1}} \cdot i_\sigma \equiv_n 1$, i.e. es gibt ein $t \in \mathbf{Z}$ mit $i_{\sigma^{-1}} \cdot i_\sigma + nt = 1$. Somit können i_σ und n keinen nichttrivialen gemeinsamen Faktor haben, da dieser auch in 1 aufgehen würde.

Zeigen wir, daß ein Gruppenmorphismus vorliegt. Seien $\sigma,\ \rho \in \mathrm{Gal}(L|K)$. Es wird

$$\zeta_n^{i_{\rho\circ\sigma}} \;=\; (\rho\circ\sigma)(\zeta_n) = \rho(\zeta_n^{i_\sigma}) \;=\; \rho(\zeta_n)^{i_\sigma} \;=\; (\zeta_n^{i_\rho})^{i_\sigma} \;=\; \zeta_n^{i_\rho\cdot i_\sigma}\ ,$$

also $i_{\rho\circ\sigma} + n\mathbf{Z} = (i_\rho + n\mathbf{Z})\cdot(i_\sigma + n\mathbf{Z})$.

Zeigen wir, daß dieser Gruppenmorphismus $\mathrm{Gal}(L|K) \longrightarrow \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, $\sigma \longmapsto i_\sigma + n\mathbf{Z}$ injektiv ist. Ist $i_\sigma \equiv_n 1$, so ist

$$\sigma(\zeta_n) \;=\; \zeta_n^{i_\sigma} \;=\; \zeta_n \;=\; \mathrm{id}(\zeta_n)\ ,$$

da $\mathrm{o}(\zeta_n) = n$. Da $L = K(\zeta_n)$, folgt $\sigma = \mathrm{id}_L$; vgl. dritte Bemerkung aus §3.4.1.

Da also $\mathrm{Gal}(L|K)$ isomorph zu einer Untergruppe der abelschen Gruppe $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ist, ist $\mathrm{Gal}(L|K)$ insbesondere abelsch.

Aufgabe 45

(1) Ist $\mathrm{char}\,K = 0$, so ist $\mathrm{char}\,L = 0$ und somit L perfekt.

Ist $\mathrm{char}\,K = p > 0$, so ist $\mathrm{Frob}_K : K \xrightarrow{\sim} K$. Wir haben zu zeigen, daß $\mathrm{Frob}_L : L \longrightarrow L$ surjektiv ist.

Es ist L ein K-Vektorraum wie üblich.

Ferner wird L zu einem K-Vektorraum vermöge der Addition auf L und der skalaren Multiplikation $x * y := x^p y$ für $x \in K$ und $y \in L$. Schreibe diesen $L^{(p)}$. In der Tat ist für $y,\ y' \in L$ und $x,\ x' \in K$

$$\begin{array}{lllllll} 1 * y & = & 1^p \cdot y & = & 1 \cdot y & = & y \\ x * (y + y') & = & x^p(y + y') & = & x^p y + x^p y' & = & x * y + x * y' \\ (x + x') * y & = & (x + x')^p y & = & x^p y + x'^p y & = & x * y + x' * y \\ (xx') * y & = & (xx')^p y & = & x^p x'^p y & = & x * (x' * y)\ . \end{array}$$

Sei $(y_1, \ldots, y_n)$ eine K-Basis von L. Dann ist $(y_1, \ldots, y_n)$ auch eine K-Basis von $L^{(p)}$, wie man wie folgt einsieht.

Lineare Unabhängigkeit. Aus

$$x_1 * y_1 + \cdots + x_n * y_n \;=\; 0$$

für $x_i \in K$ folgt, daß $x_1^p y_1 + \cdots + x_n^p y_n = 0$, woraus $x_i^p = 0$ stets, woraus, wegen Injektivität von Frob_K, $x_i = 0$ stets.

Erzeugendensystem. Es gibt für ein gegebenes y Elemente $x_i \in K$ mit

$$y = x_1 y_1 + \cdots + x_n y_n\ .$$

Sei $\tilde{x}_i^p = x_i$ stets, was wegen Frob_K surjektiv möglich ist. Also wird

$$y = \tilde{x}_1^p y_1 + \cdots + \tilde{x}_n^p y_n \;=\; \tilde{x}_1 * y_1 + \cdots + \tilde{x}_n * y_n\ .$$

Da nun $(y_1, \ldots, y_n)$ als K-Basis von $L^{(p)}$ nachgewiesen ist, folgt $\dim_K L^{(p)} = n = \dim_K L$.

Nun ist Frob_L sicher injektiv. Aufgefaßt als Abbildung von L nach $L^{(p)}$ ist nun Frob_L auch K-linear, da

$$\mathrm{Frob}_L(xy) \;=\; x^p y^p \;=\; x * \mathrm{Frob}_L(y)$$

für $x \in K$ und $y \in L$. Als injektive Abbildung zwischen gleichdimensionalen Vektorräumen L und $L^{(p)}$ ist Frob_L also auch surjektiv.

Somit ist L perfekt.

(2) Es genügt zu zeigen, daß M Zerfällungskörper eines Polynoms in $K[X]$ ist, welches in ein Produkt verschiedener irreduzibler Polynome zerfällt.

Da $L|K$ galoisch ist, ist L Zerfällungskörper eines Polynoms $g(X) \in K[X]$, welches in ein Produkt verschiedener irreduzibler Polynome zerfällt; vgl. zweites Lemma in §3.5.1.4.

Sei $h(X) := \mathrm{kgV}(f(X), g(X)) \in K[X]$. Mit loc. cit. genügt es zu zeigen, daß M der Zerfällungskörper von $h(X)$ ist.

Sei $\{\gamma_1, \ldots, \gamma_k\}$ die Nullstellenmenge von $g(X)$ in M. Da $g(X)$ bereits in $L[X]$ in Linearfaktoren zerfällt, ist $\{\gamma_1, \ldots, \gamma_k\} \subseteq L$.

Sei $\{\varphi_1, \ldots, \varphi_\ell\}$ die Nullstellenmenge von $f(X)$ in M. Die Situation stellt sich so dar.

$$\begin{array}{ccl} M & = & L(\varphi_1, \ldots, \varphi_\ell) \\ | & & \\ L & = & K(\gamma_1, \ldots, \gamma_k) \\ | & & \\ K & & \end{array}$$

Es ist $\{\gamma_1, \ldots, \gamma_k\} \cup \{\varphi_1, \ldots, \varphi_\ell\}$ die Nullstellenmenge von $h(X)$. Es ist $M = L(\varphi_1, \ldots, \varphi_\ell) = K(\gamma_1, \ldots, \gamma_k, \varphi_1, \ldots, \varphi_\ell)$. Da sich dieses Erzeugnis durch Weglassen von doppelt aufgeführten Erzeugern nicht ändert, erzeugen die Nullstellen von $h(X)$ in M den Körper M über K.

Um zu zeigen, daß $h(X) \in M[X]$ in ein Produkt von Linearfaktoren zerfällt, genügt es zu zeigen, daß jeder normierte irreduzible Faktor $u(X)$ von $h(X)$ in $K[X]$ im größeren Polynomring $M[X]$ in ein Produkt von Linearfaktoren zerfällt.

Wir betrachten also solch ein $u(X)$. Es ist $u(X)$ ein Teiler von $f(X)$ oder von $g(X)$ in $K[X]$ (möglicherweise von beiden).

Teilt $u(X)$ das Polynom $f(X)$, dann zerfällt daher $u(X)$ bereits in $L[X]$ in Linearfaktoren, also auch in $M[X]$.

Teilt $u(X)$ das Polynom $g(X)$, dann zerfällt daher $u(X)$ in $M[X]$ in Linearfaktoren.

Aufgabe 46

(1) Es ergibt sich der Zerfällungskörper von $X^6 + 3X + 3 \in \mathbf{Q}[X]$ zu $\mathbf{Q}(a, b, c, d)$ mit

$$\begin{array}{rcl} 0 & = & a^6 + 3a + 3 \\ 0 & = & b^3 + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)b^2 \\ & & +\frac{1}{17}(-3a^5 + 7a^4 - 5a^3 + 6a^2 + 3a - 33)b + \frac{1}{17}(3a^5 - 7a^4 + 5a^3 - 6a^2 - 3a - 18) \\ 0 & = & c^2 + \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 + 11a + 15)c + \frac{1}{17}(-11a^5 + 3a^4 - 7a^3 + 5a^2 - 6a - 36) \\ 0 & = & d^2 + \big(b + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)\big)d \\ & & +\big(b^2 + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)b + \frac{1}{17}(-3a^5 + 7a^4 - 5a^3 + 6a^2 + 3a - 33)\big)\ . \end{array}$$

Insbesondere ist $|\operatorname{Gal}(X^6 + 3X + 3)| = [\mathbf{Q}(a, b, c, d) : \mathbf{Q}] = 2 \cdot 2 \cdot 3 \cdot 6 = 72$.

Wir erhalten die Nullstellen

$$\begin{array}{rcl} \gamma_1 & := & a \\ \gamma_2 & := & b \\ \gamma_3 & := & c \\ \gamma_4 & := & d \\ \gamma_5 & := & -c - \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 + 11a + 15) \\ \gamma_6 & := & -d - b + \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 - 6a + 15) \end{array}$$

von $X^6 + 3X + 3 \in \mathbf{Q}(a, b, c, d)[X]$.

Wir gehen diesesmal nun nicht systematisch durch die Fälle, Subfälle etc., sondern suchen per Zufallsprinzip Erzeuger der Galoisgruppe, in der Hoffnung, daß das schneller geht.

Folgender Magma-Quelltext liefert das Resultat.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 + 3*X + 3);
KK<a> := ext<Q | X^6 + 3*X + 3>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 + 3*XX + 3);
KKK<b> := ext<KK | XX^3 + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15)*XX^2
          + 1/17*(-3*a^5 + 7*a^4 - 5*a^3 + 6*a^2 + 3*a - 33)*XX
          + 1/17*(3*a^5 - 7*a^4 + 5*a^3 - 6*a^2 - 3*a - 18)>;
RRR<XXX> := PolynomialRing(KKK);
KKKK<c> := ext<KKK | XXX^2 + 1/17*(6*a^5 - 14*a^4 + 10*a^3 - 12*a^2 + 11*a + 15)*XXX
           + 1/17*(-11*a^5 + 3*a^4 - 7*a^3 + 5*a^2 - 6*a - 36)>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 + 3*XXXX + 3);
KKKKK<d> := ext<KKKK | XXXX^2 + (b
            + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15))*XXXX
            + b^2 + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15)*b
            + 1/17*(-3*a^5 + 7*a^4 - 5*a^3 + 6*a^2 + 3*a - 33)>;
RRRRR<XXXXX> := PolynomialRing(KKKKK);
Factorisation(XXXXX^6 + 3*XXXXX + 3);
RBIG<Ga1,Ga2,Ga3,Ga4,Y> := PolynomialRing(Q,5);
Ga5 := -Ga3 - 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 + 11*Ga1 + 15);
Ga6 := -Ga4 - Ga2 + 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 - 6*Ga1 + 15);
ga1 := a;
ga2 := b;
ga3 := c;
ga4 := d;
ga5 := Evaluate(Ga5,[ga1,ga2,ga3,ga4,0]);
ga6 := Evaluate(Ga6,[ga1,ga2,ga3,ga4,0]);
(XXXXX-ga1)*(XXXXX-ga2)*(XXXXX-ga3)*(XXXXX-ga4)*(XXXXX-ga5)*(XXXXX-ga6); // zur Probe
muga1 := Y^6 + 3*Y + 3;
muga2 := Y^3 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15)*Y^2
         + 1/17*(-3*Ga1^5 + 7*Ga1^4 - 5*Ga1^3 + 6*Ga1^2 + 3*Ga1 - 33)*Y
         + 1/17*(3*Ga1^5 - 7*Ga1^4 + 5*Ga1^3 - 6*Ga1^2 - 3*Ga1 - 18);
muga3 := Y^2 + 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 + 11*Ga1 + 15)*Y
         + 1/17*(-11*Ga1^5 + 3*Ga1^4 - 7*Ga1^3 + 5*Ga1^2 - 6*Ga1 - 36);
muga4 := Y^2 + (Ga2 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15))*Y
         + Ga2^2 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15)*Ga2
         + 1/17*(-3*Ga1^5 + 7*Ga1^4 - 5*Ga1^3 + 6*Ga1^2 + 3*Ga1 - 33);

muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga1,0,0,0,XXXXX]);
Factorisation(muga2s); // 246 (resultierende Nullstellennummern)
muga3s:= Evaluate(muga3,[ga1,ga2,0,0,XXXXX]);
Factorisation(muga3s); // 35
muga4s:= Evaluate(muga4,[ga1,ga2,ga5,0,XXXXX]);
Factorisation(muga4s); // 46
Evaluate(Ga5,[ga1,ga2,ga5,ga4,0]); // 3
Evaluate(Ga6,[ga1,ga2,ga5,ga4,0]); // 6 // (3,5)
Order(sub<SymmetricGroup(6) | (3,5)>);
// *** Zwischenstand: Ordnung = 2 ***
Evaluate(Ga5,[ga1,ga2,ga5,ga6,0]); // 3
```

```
Evaluate(Ga6,[ga1,ga2,ga5,ga6,0]); // 4 // (3,5)(4,6)
Order(sub<SymmetricGroup(6) | (3,5), (3,5)(4,6)>);
// Erzeugnis auch = <(3,5), (4,6)>
// *** Zwischenstand: Ordnung = 4 ***
muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456
muga2s:= Evaluate(muga2,[ga1,0,0,0,XXXXX]);
Factorisation(muga2s); // 246
muga3s:= Evaluate(muga3,[ga1,ga4,0,0,XXXXX]);
Factorisation(muga3s); // 35
muga4s:= Evaluate(muga4,[ga1,ga4,ga5,0,XXXXX]);
Factorisation(muga4s); // 26
Evaluate(Ga5,[ga1,ga4,ga5,ga2,0]); // 3
Evaluate(Ga6,[ga1,ga4,ga5,ga2,0]); // 6 // (2,4)(3,5)
Order(sub<SymmetricGroup(6) | (3,5), (4,6), (2,4)(3,5)>);
// Erzeugnis auch = <(3,5),(4,6),(2,4)>
// *** Zwischenstand: Ordnung = 12 ***
muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga2,0,0,0,XXXXX]);
Factorisation(muga2s); // 135
muga3s:= Evaluate(muga3,[ga2,ga1,0,0,XXXXX]);
Factorisation(muga3s); // 46
muga4s:= Evaluate(muga4,[ga2,ga1,ga4,0,XXXXX]);
Factorisation(muga4s); // 35
Evaluate(Ga5,[ga2,ga1,ga4,ga3,0]); // 6
Evaluate(Ga6,[ga2,ga1,ga4,ga3,0]); // 5 // (1,2)(3,4)(5,6)
Order(sub<SymmetricGroup(6) | (3,5), (4,6), (2,4), (1,2)(3,4)(5,6)>);
// Erzeugnis auch = <(4,6), (2,4), (1,2)(3,4)(5,6)>
// *** Zwischenstand: Ordnung = 72 ***
```

Es ergibt sich $\mathrm{Gal}(X^6 + 3X + 3) \xrightarrow{\sim} \langle (4,6), (2,4), (1,2)(3,4)(5,6) \rangle$;

(2) Was bislang geschah.

Gemäß Aufgabe 34.(1) ist der Zerfällungskörper von $X^3 + X + 1 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a,b)$ mit $a^3 + a + 1 = 0$ und $b^2 + ab + a^2 + 1 = 0$. Insbesondere ist $[\mathbf{Q}(a,b) : \mathbf{Q}] = 6$, und $\mathbf{Q}(a,b)|\mathbf{Q}$ galoisch; cf. zweites Lemma in §3.5.1.4.

Seien $\gamma_1 := a$, $\gamma_2 = b$ und $\gamma_3 := -a - b$ die Nullstellen von $X^3 + X + 1$ in $\mathbf{Q}(a,b)$.

Nach §3.4.2.1 (resp. zweiter Folgerung in §3.4.1) ist $\mathrm{Gal}(X^3 + X + 1) \xrightarrow{\sim} \mathcal{S}_3$. Wir identifizieren entlang diesem Isomorphismus.

Nach Satz 9 (Hauptsatz) entsprechen die gesuchten Zwischenkörper zwischen $\mathbf{Q}$ und $\mathbf{Q}(a,b)$ den Untergruppen von $\mathrm{Gal}(X^3 + X + 1) = \mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q}) = \mathcal{S}_3$.

In Aufgabe 38.(3) wurden die Untergruppen von $\mathcal{S}_3$ ermittelt wie im folgenden Diagramm angegeben. Hierbei sind Linien von oben nach unten als Inklusion zu lesen.

$$\begin{tikzcd}
& & \{\mathrm{id}\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[ddr, dash] & \\
\langle(1,2)\rangle \arrow[ddrr, dash] & \langle(1,3)\rangle \arrow[ddr, dash] & \langle(2,3)\rangle \arrow[dd, dash] & \\
& & & \langle(1,2,3)\rangle \arrow[dl, dash] \\
& & \mathcal{S}_3 &
\end{tikzcd}$$

Die Korrespondenz weist nun einer Untergruppe U den Zwischenkörper $\mathrm{Fix}_U\, \mathbf{Q}(a,b)$ zu.

Es sind $\mathrm{Fix}_{\{\mathrm{id}\}}\, \mathbf{Q}(a,b) = \mathbf{Q}(a,b)$ und $\mathrm{Fix}_{\mathcal{S}_3}\, \mathbf{Q}(a,b) = \mathbf{Q}$; vgl. erste Bemerkung in §3.5.1.4.

In Aufgabe 41.(1) wurde eine $\mathbf{Q}$-Basis von $\mathrm{Fix}_{\langle(1,3)\rangle}\, \mathbf{Q}(a,b)$ zu $(1,\, b,\, a^2 + ba + 1)$ bestimmt. Da $-b^2 = ba + a^2 + 1$, folgt $\mathrm{Fix}_{\langle(1,3)\rangle}\, \mathbf{Q}(a,b) = \mathbf{Q}(b)$.

In Aufgabe 41.(2) wurde eine $\mathbf{Q}$-Basis von $\mathrm{Fix}_{\langle(1,2,3)\rangle}\, \mathbf{Q}(a,b)$ zu $(1,\, -a + b + 3a^2 b)$ bestimmt. Es folgt $\mathrm{Fix}_{\langle(1,2,3)\rangle}\, \mathbf{Q}(a,b) = \mathbf{Q}(-a + b + 3a^2 b)$.

Wir setzen diese Berechnung nun fort.

Für $\langle(1,2)\rangle = \{\mathrm{id},\, (1,2)\}$ schicken die zugehörigen Automorphismen

$$\begin{array}{ccccccc} a & \stackrel{\mathrm{id}}{\longmapsto} & a & \quad & a & \stackrel{(1,2)}{\longmapsto} & b \\ b & \longmapsto & b & \quad & b & \longmapsto & a\,. \end{array}$$

Wir erhalten folgendes $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(1,2)\rangle}\, \mathbf{Q}(a,b)$.

$$\begin{array}{rl} & \big(\,\mathrm{Tr}_{\langle(1,2)\rangle}(1),\ \mathrm{Tr}_{\langle(1,2)\rangle}(a),\ \mathrm{Tr}_{\langle(1,2)\rangle}(a^2),\ \mathrm{Tr}_{\langle(1,2)\rangle}(b),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba^2)\big) \\ = & \big(1+1,\ a+b,\ a^2+b^2,\ b+a,\ ba+ab,\ ba^2+ab^2\big) \\ = & \big(2,\ a+b,\ -ba-1,\ a+b,\ 2ba,\ 1\big)\ . \end{array}$$

Dies reduziert sich z.B. zur $\mathbf{Q}$-Basis

$$\big(1,\ a+b,\ -ba-1\big)\ .$$

Da nun $(a+b)^2 = -ba - 1$, wird $\mathrm{Fix}_{\langle(1,2)\rangle}\, \mathbf{Q}(a,b) = \mathbf{Q}(a+b)$.

Für $\langle(2,3)\rangle = \{\mathrm{id},\, (2,3)\}$ schicken die zugehörigen Automorphismen

$$\begin{array}{ccccccc} a & \stackrel{\mathrm{id}}{\longmapsto} & a & \quad & a & \stackrel{(2,3)}{\longmapsto} & a \\ b & \longmapsto & b & \quad & b & \longmapsto & -a-b\,. \end{array}$$

Wir erhalten folgendes $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(2,3)\rangle}\, \mathbf{Q}(a,b)$.

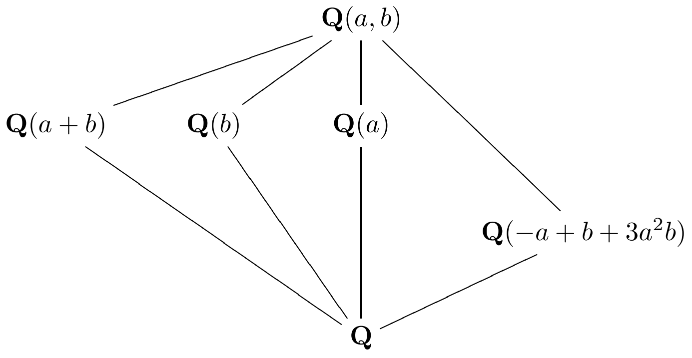
$$\begin{array}{rl} & \big(\,\mathrm{Tr}_{\langle(2,3)\rangle}(1),\ \mathrm{Tr}_{\langle(2,3)\rangle}(a),\ \mathrm{Tr}_{\langle(2,3)\rangle}(a^2),\ \mathrm{Tr}_{\langle(2,3)\rangle}(b),\ \mathrm{Tr}_{\langle(2,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(2,3)\rangle}(ba^2)\big) \\ = & \big(1+1,\ a+a,\ a^2+a^2,\ b+(-a-b),\ ba+(-a-b)a,\ ba^2+(-a-b)a^2\big) \\ = & \big(2,\ 2a,\ 2a^2,\ -a,\ -a^2,\ a+1\big) \end{array}$$

Dies reduziert sich z.B. zur $\mathbf{Q}$-Basis

$$\big(1,\ a,\ a^2\big)\ .$$

Also wird $\mathrm{Fix}_{\langle(2,3)\rangle}\, \mathbf{Q}(a,b) = \mathbf{Q}(a)$.

Wir tragen in das den Untergruppen entsprechende Körperdiagramm die Fixkörper ein. Hierbei sind Linien von unten nach oben als Inklusion zu lesen.



Aufgabe 47

(1) Mit dem zweiten Lemma aus §3.5.1.4 ist E der Zerfällungskörper eines normierten Polynoms $g(X) \in K[X]$, das dort in verschiedene normierte irreduzible Faktoren zerfällt. In $E[X]$ zerfällt $g(X)$ in verschiedene Linearfaktoren; vgl. die zweite Bemerkung in §3.4.1. Also zerfällt $g(X)$ auch in $L[X]$ in verschiedene normierte irreduzible Faktoren. Nun ist E auch Zerfällungskörper von $g(X)$ über L; vgl. zweite Bemerkung aus §2.5.1. Also ist $E|L$ galoisch; vgl. Aufgabe 45.(1) und zweites Lemma aus §3.5.1.4.

(2) Sei $q = p^r$ für p prim und $r \geqslant 1$. Nach dem Lemma aus §2.5.4 ist $\mathbf{F}_{q^s}$ Zerfällungskörper von $X^{q^s} - X$ über $\mathbf{F}_p$. Im Beweis zu loc. cit., Teil (1), wurde auch gezeigt, daß $X^{q^s} - X$ in $\mathbf{F}_{q^s}[X]$ in verschiedene Linearfaktoren zerfällt. Also zerfällt $X^{q^s} - X$ in $\mathbf{F}_q[X]$ in verschiedene irreduzible Faktoren. Nun ist $\mathbf{F}_{q^s}$ auch Zerfällungskörper von $X^{q^s} - X$ über $\mathbf{F}_q$; vgl. zweite Bemerkung aus §2.5.1. Also ist $\mathbf{F}_{q^s}|\mathbf{F}_q$ galoisch.