M. Künzer

Galoistheorie, WS 08/09

Lösung 11

Aufgabe 37

(1) Zum einen ist $1_H = f(1_G) \in f(U)$. Seien zum anderen $x,\, y \in f(U)$ gegeben. Schreibe $x = f(u)$ und $y = f(v)$ mit $u,\, v \in U$. Es wird

$$xy^{-1} \;=\; f(u)f(v)^{-1} \;=\; f(uv^{-1}) \;\in\; f(U)\;.$$

(2) Da $G \leqslant G$, können wir (1) anwenden und erhalten $\operatorname{Im} f = f(G) \leqslant H$.

(3) Mit (2) ist $\operatorname{Im} f \leqslant G$, und insbesondere $\operatorname{Im} f$ eine Gruppe, mit von H vererbter Multiplikation. Da f ein Gruppenmorphismus ist, gilt dies auch für $f|^{\operatorname{Im} f}$. Da nun nach Voraussetzung f injektiv ist, ist $f|^{\operatorname{Im} f}$ bijektiv. Insgesamt ist $f|^{\operatorname{Im} f}$ also ein Gruppenisomorphismus.

(4) Zeigen wir zunächst, daß aus $N \leqslant H$ folgt, daß $f^{-1}(N) \leqslant G$. Zum einen ist $f(1_G) = 1_H \in N$, also $1_G \in f^{-1}(N)$. Seien zum anderen $x,\, y \in f^{-1}(N)$, d.h. $f(x),\, f(y) \in N$. Dann ist

$$f(xy^{-1}) \;=\; f(x)f(y)^{-1} \;\in\; N\;,$$

also $xy^{-1} \in f^{-1}(N)$.

Zeigen wir nun, daß aus $N \trianglelefteq H$ noch folgt, daß $f^{-1}(N) \trianglelefteq G$.

Sei $g \in G$. Wir *behaupten,* daß ${}^{g}f^{-1}(N) \subseteq f^{-1}(N)$. Sei hierzu $x \in f^{-1}(N)$, d.h. $f(x) \in N$. Dann wird

$$f({}^{g}x) \;=\; f(gxg^{-1}) \;=\; f(g)f(x)f(g)^{-1} \;=\; {}^{f(g)}f(x) \;\in\; N\;,$$

da $N \trianglelefteq H$, also ${}^{g}x \in f^{-1}(N)$. Dies zeigt die *Behaupptung.*

Diese Behauptung auf g^{-1} statt g angewandt liefert ${}^{g^{-1}}f^{-1}(N) \subseteq f^{-1}(N)$. Diese Inklusionsbeziehung auf beiden Seiten von links mit g konjugiert gibt

$$f^{-1}(N) \;=\; {}^{g}({}^{g^{-1}}f^{-1}(N)) \;\subseteq\; {}^{g}f^{-1}(N)\;.$$

Insgesamt also ${}^{g}f^{-1}(N) = f^{-1}(N)$.

(5) Da $\{1_H\} \trianglelefteq H$, können wir (4) anwenden und erhalten $\operatorname{Kern} f = \{g \in G \,:\, f(g) = 1_H\} = f^{-1}(\{1_H\}) \trianglelefteq G$.

Aufgabe 38 (Satz von Lagrange in (1.c))

(1) Sei $U \leqslant G$. Die Voraussetzung $|G|$ endlich werden wir erst im Teil (c) brauchen.

  (a) Seien $b,\, b' \in G$. Sei $bU \cap b'U \neq \emptyset$. Zu zeigen ist, daß $bU = b'U$. Durch Rollenvertauschung von b und b' genügt es zu zeigen, daß $bU \subseteq b'U$. Sei also $x \in bU \cap b'U$. Schreibe $x = bu = b'v$ mit $u,\, v \in U$. Sei $y \in bU$. Wir haben zu zeigen, daß $y \in b'U$. Schreibe $y = bw$ mit $w \in U$. In der Tat wird

$$y \;=\; bw \;=\; b'\underbrace{vu^{-1}w}_{\in U} \;\in\; b'U\;.$$

  (b) Die Abbildungen $U \longrightarrow bU,\ u \longmapsto bu$ und $bU \longrightarrow U,\ x \longmapsto b^{-1}x$ invertieren sich wechselseitig, da

$$u \;\longmapsto\; bu \;\longmapsto\; b^{-1}bu \;=\; u$$

und

$$x \;\longmapsto\; b^{-1}x \;\longmapsto\; bb^{-1}x \;=\; x\;.$$

  Insbesondere ist $U \longrightarrow bU,\ u \longmapsto bu$ eine Bijektion.

(c) Sei nun $|G|$ endlich. Mit (a) ist G eine disjunkte Vereinigung von Teilmengen der Form bU für gewisse $b \in G$. Mit (b) haben alle Teilnehmer dieser disjunkten Vereinigung die Kardinalität $|U|$. Also ist $|U|$ ein Teiler von $|G|$.

(2) Es ist $(1,3) \circ (1,3,4) = (3,4)$. Es ist $(1,6,3) \circ (2,4,3,5) \circ (2,4) = (1,6,3,5,2)$.

(3) Nichtnormale Untergruppen:

$$\langle (1,2) \rangle,\ \langle (1,3) \rangle,\ \langle (2,3) \rangle \ \leqslant\ \mathcal{S}_3\ .$$

Normale Untergruppen:

$$\{\mathrm{id}\},\ \langle (1,2,3) \rangle,\ \mathcal{S}_3\ \trianglelefteqslant\ \mathcal{S}_3\ .$$

Man erhält die komplette Liste durch sukzessives Hinzufügen von Erzeugenden. Auf diese Weise kann man die Untergruppen erhalten, die minimal über einer gegebenen Untergruppe liegen, d.h. so, daß echt dazwischen keine weitere liegt.

So z.B. erkennt man (von Hand oder via Magma), daß für jedes Element $x \in \mathcal{S}_3 \smallsetminus \{(1,2)\}$ gilt, daß bereits $\langle (1,2),\, x \rangle = \mathcal{S}_3$. Also kann es echt zwischen $\langle (1,2) \rangle$ und $\mathcal{S}_3$ keine weiteren Untergruppen mehr geben.

Schließlich prüft man die erhaltene Liste von Untergruppen auf Normalität durch.

(4) Mittels `Order(sub<SymmetricGroup(12) | (1,2,3,4,5,6,7,8,9,10,11,12), (1,3)>);` erhalten wir die Ordnung der angegebenen Untergruppe

$$|\langle (1,2,3,4,5,6,7,8,9,10,11,12), (1,3) \rangle| \ =\ 1036800\ .$$

Ferner ist

$$|\mathcal{S}_{12}| \ =\ 12!\ =\ 479001600$$

Und in der Tat ist $479001600/1036800 = 462$.

Aufgabe 39

(1) In Aufgabe 34.(2) wurde der Zerfällungskörper $\mathbf{Q}(a,b)$ konstruiert, mit

$$\begin{array}{rcl} \mu_{a,\mathbf{Q}}(X) & = & X^4 + 4X^2 + 4X + 8 \\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^3 + aX^2 + (a^2+4)X + (a^3 + 4a + 8)\ . \end{array}$$

Insbesondere war $[\mathbf{Q}(a,b) : \mathbf{Q}] = 12$ festgestellt worden. Es zerfiel

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

An den für all dies notwendig gewesenen Magma-Quelltext hängen wir noch die Definitionen

$$\begin{array}{rcl} \gamma_1 & := & a \\ \gamma_2 & := & b \\ \gamma_3 & := & \frac{1}{28}(2a^3 - 3a^2 + 2a + 6)b^2 + \frac{1}{14}(-3a^3 + a^2 - 10a - 16)b + \frac{1}{14}(2a^3 - 3a^2 + 2a + 20) \\ \gamma_4 & := & \frac{1}{28}(-2a^3 + 3a^2 - 2a - 6)b^2 + \frac{1}{14}(3a^3 - a^2 + 10a + 2)b + \frac{1}{14}(-2a^3 + 3a^2 - 16a - 20) \end{array}$$

an.

```
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);
ga1 := a;
ga2 := b;
ga3 := 1/28*(2*a^3 - 3*a^2 + 2*a + 6)*b^2 + 1/14*(-3*a^3 + a^2 - 10*a - 16)*b
       + 1/14*(2*a^3 - 3*a^2 + 2*a + 20);
ga4 := 1/28*(-2*a^3 + 3*a^2 - 2*a - 6)*b^2 + 1/14*(3*a^3 - a^2 + 10*a + 2)*b
       + 1/14*(-2*a^3 + 3*a^2 - 16*a - 20);
```

Es ist $m = 2$ und $n = 4$. Bestimmen wir das Bild von $\mathrm{Gal}(X^4 + 4X^2 + 8X + 8)$ in $\mathcal{S}_4$.

$$\begin{tikzcd}
\mathbf{Q}(a,b) \arrow[r, "\sigma_2", "\sim"'] & \mathbf{Q}(\gamma_1',\gamma_2') \\
\mathbf{Q}(a) \arrow[u] \arrow[r, "\sigma_1", "\sim"'] & \mathbf{Q}(\gamma_1') \arrow[u] \\
\mathbf{Q} \arrow[u] \arrow[r, equal] & \mathbf{Q} \arrow[u]
\end{tikzcd}$$

Nullstellen bedeute im folgenden stets Nullstellen in $\mathbf{Q}(a,b)$.

Die Nullstellen von
$$\mu_{a,\mathbf{Q}}(X) \;=\; X^4 + 4X^2 + 8X + 8$$
sind γ_1, γ_2, γ_3 und γ_4 ([1]). Unter diesen haben wir ein γ_1' auszuwählen.

Fall $\gamma_1' = \gamma_1$. Es ist
$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^3 + \gamma_1 X^2 + (\gamma_1^2 + 4)X + (\gamma_1^3 + 4\gamma_1 + 8)\;,$$
welches die Nullstellen γ_2, γ_3 und γ_4 hat ([2]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_2$. Wir erhalten das zulässige Tupel (γ_1, γ_2). Es werden

$$\begin{array}{rcl}
\sigma_2(\gamma_3) & = & \frac{1}{28}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 6)\gamma_2^2 + \frac{1}{14}(-3\gamma_1^3 + \gamma_1^2 - 10\gamma_1 - 16)\gamma_2 + \frac{1}{14}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 20) \\
& = & \gamma_3 \\
\sigma_2(\gamma_4) & = & \frac{1}{28}(-2\gamma_1^3 + 3\gamma_1^2 - 2\gamma_1 - 6)\gamma_2^2 + \frac{1}{14}(3\gamma_1^3 - \gamma_1^2 + 10\gamma_1 + 2)\gamma_2 + \frac{1}{14}(-2\gamma_1^3 + 3\gamma_1^2 - 16\gamma_1 - 20) \\
& = & \gamma_4
\end{array}$$

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right) = \mathrm{id}$. Das war klar, denn schickt man γ_1 auf γ_1 und γ_2 auf γ_2, so erhält man die Identität. Der Systematik halber haben wir es vollständig angeführt.

Zwischenstand : $|\langle \mathrm{id}\rangle| = 1 < 12$.

Subfall $\gamma_2' = \gamma_3$. Wir erhalten das zulässige Tupel (γ_1, γ_3). Es werden

$$\begin{array}{rcl}
\sigma_2(\gamma_3) & = & \frac{1}{28}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 6)\gamma_3^2 + \frac{1}{14}(-3\gamma_1^3 + \gamma_1^2 - 10\gamma_1 - 16)\gamma_3 + \frac{1}{14}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 20) \\
& = & \gamma_4 \\
\sigma_2(\gamma_4) & = & \frac{1}{28}(-2\gamma_1^3 + 3\gamma_1^2 - 2\gamma_1 - 6)\gamma_3^2 + \frac{1}{14}(3\gamma_1^3 - \gamma_1^2 + 10\gamma_1 + 2)\gamma_3 + \frac{1}{14}(-2\gamma_1^3 + 3\gamma_1^2 - 16\gamma_1 - 20) \\
& = & \gamma_2\;,
\end{array}$$

wobei Magma für den letzten Schritt hilft ([3]).

---

[1] `Factorisation(XXX^4 + 4*XXX^2 + 8*XXX + 8);`

[2] `Factorisation(XXX^3 + ga1*XXX^2 + (ga1^2 + 4)*XXX + (ga1^3 + 4*ga1 + 8));`

[3] Man kann wie folgt vorgehen.

```
R2<Ga1,Ga2> := PolynomialRing(KKK,2);
Ga3 := 1/28*(2*Ga1^3 - 3*Ga1^2 + 2*Ga1 + 6)*Ga2^2 + 1/14*(-3*Ga1^3 + Ga1^2 - 10*Ga1 - 16)*Ga2
       + 1/14*(2*Ga1^3 - 3*Ga1^2 + 2*Ga1 + 20);
Ga4 := 1/28*(-2*Ga1^3 + 3*Ga1^2 - 2*Ga1 - 6)*Ga2^2 + 1/14*(3*Ga1^3 - Ga1^2 + 10*Ga1 + 2)*Ga2
       + 1/14*(-2*Ga1^3 + 3*Ga1^2 - 16*Ga1 - 20);
Evaluate(Ga3,[ga1,ga3]);
Evaluate(Ga4,[ga1,ga3]);
Evaluate(Ga3,[ga1,ga3]) eq ga4;
```

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right) = (2,3,4)$.

Zwischenstand : $|\langle (2,3,4)\rangle| = 3 < 12$.

Subfall $\gamma_2' = \gamma_4$. Wir erhalten das zulässige Tupel (γ_1, γ_4). Es werden

$$\begin{array}{rcl}\sigma_2(\gamma_3) & = & \frac{1}{28}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 6)\gamma_4^2 + \frac{1}{14}(-3\gamma_1^3 + \gamma_1^2 - 10\gamma_1 - 16)\gamma_4 + \frac{1}{14}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 20) \\ & = & \gamma_2 \\ \sigma_2(\gamma_4) & = & \frac{1}{28}(-2\gamma_1^3 + 3\gamma_1^2 - 2\gamma_1 - 6)\gamma_4^2 + \frac{1}{14}(3\gamma_1^3 - \gamma_1^2 + 10\gamma_1 + 2)\gamma_4 + \frac{1}{14}(-2\gamma_1^3 + 3\gamma_1^2 - 16\gamma_1 - 20) \\ & = & \gamma_3\end{array}$$

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right) = (2,4,3)$.

Zwischenstand : $|\langle (2,3,4),\ (2,4,3)\rangle| = 3 < 12$. Es kann $(2,4,3)$ weiters wieder entfallen.

Fall $\gamma_1' = \gamma_2$. Es ist

$$\mu_{b,\mathbf{Q}(a)}^{\sigma_2}(X) \;=\; X^3 + \gamma_2 X^2 + (\gamma_2^2 + 4)X + (\gamma_2^3 + 4\gamma_2 + 8)\ ,$$

welches die Nullstellen γ_1, γ_3 und γ_4 hat ([4]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Wir erhalten das zulässige Tupel (γ_2, γ_1). Es werden

$$\begin{array}{rcl}\sigma_2(\gamma_3) & = & \frac{1}{28}(2\gamma_2^3 - 3\gamma_2^2 + 2\gamma_2 + 6)\gamma_1^2 + \frac{1}{14}(-3\gamma_2^3 + \gamma_2^2 - 10\gamma_2 - 16)\gamma_1 + \frac{1}{14}(2\gamma_2^3 - 3\gamma_2^2 + 2\gamma_2 + 20) \\ & = & \gamma_4 \\ \sigma_2(\gamma_4) & = & \frac{1}{28}(-2\gamma_2^3 + 3\gamma_2^2 - 2\gamma_2 - 6)\gamma_1^2 + \frac{1}{14}(3\gamma_2^3 - \gamma_2^2 + 10\gamma_2 + 2)\gamma_1 + \frac{1}{14}(-2\gamma_2^3 + 3\gamma_2^2 - 16\gamma_2 - 20) \\ & = & \gamma_3\end{array}$$

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right) = (1,2)(3,4)$.

Zwischenstand : $|\langle (2,3,4),\ (1,2)(3,4)\rangle| = 12$ ([5]).

Abbruch der Fallunterscheidungen, da fertig!

Als Ergebnis erhalten wir das isomorphe Bild von $\mathrm{Gal}(X^4 + 4X^2 + 8X + 8)$ in $\mathcal{S}_4$

$$\langle (2,3,4),\ (1,2)(3,4)\rangle\ .$$

Die Liste ihrer Elemente erhält man via `{u : u in sub<SymmetricGroup(4) | (2,3,4), (1,2)(3,4)>};`, sie war nicht verlang, sieht hier aber noch ganz hübsch aus:

$$\begin{array}{l}\langle (2,3,4),\ (1,2)(3,4)\rangle \;= \\ \{\mathrm{id},\ (1,2,3),\ (1,2,4),\ (1,3,2),\ (1,3,4),\ (1,4,2),\ (1,4,3),\ (2,3,4),\ (2,4,3),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}\ .\end{array}$$

(2) In Aufgabe 30.(2) wurde der Zerfällungskörper $\mathbf{Q}(a,b,c)$ konstruiert, mit

$$\begin{array}{rcl}\mu_{a,\mathbf{Q}}(X) & = & X^6 + X^2 + 1 \\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^4 + a^2X^2 + (a^4 + 1) \\ \mu_{c,\mathbf{Q}(a,b,c)}(X) & = & X^2 + (a^2 + b^2)\ .\end{array}$$

Insbesondere war $[\mathbf{Q}(a,b,c) : \mathbf{Q}] = 48$ festgestellt worden. Es zerfiel

$$X^6 + X^2 + 1 \;=\; (X-a)(X-b)(X-c)(X+a)(X+b)(X+c)\ .$$

[4] `Factorisation(XXX^3 + ga2*XXX^2 + (ga2^2 + 4)*XXX + (ga2^3 + 4*ga2 + 8));`

[5] `Order(sub<SymmetricGroup(4) | (2,3,4), (1,2)(3,4)>);`

An den damaligen Magma-Quelltext hängen wir noch die Definitionen

$$
\begin{array}{rcl}
\gamma_1 & = & a \\
\gamma_2 & = & b \\
\gamma_3 & = & c \\
\gamma_4 & = & -a \\
\gamma_5 & = & -b \\
\gamma_6 & = & -c
\end{array}
$$

an.

```
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);
ga1 := a;
ga2 := b;
ga3 := c;
ga4 := -a;
ga5 := -b;
ga6 := -c;
```

Es ist $m = 3$ und $n = 6$. Bestimmen wir das Bild von $\mathrm{Gal}(X^6 + X^2 + 1)$ in $\mathcal{S}_6$.

$$
\begin{tikzcd}
\mathbf{Q}(a,b,c) \arrow[r, "\sigma_3", "\sim"'] & \mathbf{Q}(\gamma_1', \gamma_2', \gamma_3') \\
\mathbf{Q}(a,b) \arrow[r, "\sigma_2", "\sim"'] \arrow[u] & \mathbf{Q}(\gamma_1', \gamma_2') \arrow[u] \\
\mathbf{Q}(a) \arrow[r, "\sigma_1", "\sim"'] \arrow[u] & \mathbf{Q}(\gamma_1') \arrow[u] \\
\mathbf{Q} \arrow[r, equal] \arrow[u] & \mathbf{Q} \arrow[u]
\end{tikzcd}
$$

Nullstellen bedeute im folgenden stets Nullstellen in $\mathbf{Q}(a,b,c)$.
Die Nullstellen von

$$\mu_{a,\mathbf{Q}}(X) \;=\; X^6 + X^2 + 1$$

sind γ_1, γ_2, γ_3, γ_4, γ_5 und γ_6 ([6]). Unter diesen haben wir ein γ_1' auszuwählen.
Fall $\gamma_1' = \gamma_1$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^4 + \gamma_1^2 X^2 + (\gamma_1^4 + 1)\;,$$

welches die Nullstellen γ_2, γ_3, γ_5 und γ_6 hat ([7]). Unter diesen haben wir ein γ_2' auszuwählen.

[6] `Factorisation(XXXX^6 + XXXX^2 + 1);`
[7] `Factorisation(XXXX^4 + ga1^2 * XXXX^2 + (ga1^4 + 1));`

Subfall $\gamma_2' = \gamma_2$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_2^2)\;,$$

welches die Nullstellen γ_3 und γ_6 hat ([8]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_3)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&2&3&4&5&6 \end{smallmatrix}\right) = \mathrm{id}$.

Zwischenstand : $|\langle \mathrm{id}\rangle| = 1 < 48$.

Subsubfall $\gamma_3' = \gamma_6$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_6)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\gamma_6 & = & \gamma_3\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&2&6&4&5&3 \end{smallmatrix}\right) = (3,6)$.

Zwischenstand : $|\langle (3,6)\rangle| = 2$.

Subfall $\gamma_2' = \gamma_3$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_3^2)\;,$$

welches die Nullstellen γ_2 und γ_5 hat ([9]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_2$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_3, \gamma_2)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_3 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\gamma_2 & = & \gamma_5\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&3&2&4&6&5 \end{smallmatrix}\right) = (2,3)(5,6)$.

Zwischenstand : $|\langle (3,6),\, (2,3)(5,6)\rangle| = 8 < 48$ ([10]).

Subsubfall $\gamma_3' = \gamma_5$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_3, \gamma_5)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_3 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\gamma_5 & = & \gamma_2\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&3&5&4&6&2 \end{smallmatrix}\right) = (2,3,5,6)$.

Zwischenstand : $|\langle (3,6),\, (2,3)(5,6),\, (2,3,5,6)\rangle| = 8 < 48$ ([11]). Es kann $(2,3,5,6)$ weiters wieder entfallen.

---

[8] `Factorisation(XXXX^2 + (ga1^2 + ga2^2));`

[9] `Factorisation(XXXX^2 + (ga1^2 + ga3^2));`

[10] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6)>);`

[11] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,3,5,6)>);`

Subfall $\gamma_2' = \gamma_5$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_5^2)\;,$$

welches die Nullstellen γ_3 und γ_6 hat ([12]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_3)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_5 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&3&4&2&6 \end{smallmatrix}\right) = (2,5)$.

Zwischenstand : $|\langle(3,6),\ (2,3)(5,6),\ (2,5)\rangle| = 8 < 48$ ([13]). Es kann $(2,5)$ weiters wieder entfallen.

Subsubfall $\gamma_3' = \gamma_6$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_6)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_5 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\gamma_6 & = & \gamma_3\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&6&4&2&3 \end{smallmatrix}\right) = (2,5)(3,6)$.

Zwischenstand : $|\langle(3,6),\ (2,3)(5,6),\ (2,5)(3,6)\rangle| = 8 < 48$ ([14]). Es kann $(2,5)(3,6)$ weiters wieder entfallen.

Subfall $\gamma_2' = \gamma_6$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_6^2)\;,$$

welches die Nullstellen γ_2 und γ_5 hat ([15]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_2$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_2)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_6 & = & \gamma_3 \\ \sigma_3(\gamma_6) & = & -\gamma_2 & = & \gamma_5\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&6&2&4&3&5 \end{smallmatrix}\right) = (2,6,5,3)$.

Zwischenstand : $|\langle(3,6),\ (2,3)(5,6),\ (2,6,5,3)\rangle| = 8 < 48$ ([16]). Es kann $(2,6,5,3)$ weiters wieder entfallen.

Subsubfall $\gamma_3' = \gamma_5$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_5)$. Es werden

$$\begin{array}{rcccl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_6 & = & \gamma_3 \\ \sigma_3(\gamma_6) & = & -\gamma_5 & = & \gamma_2\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&6&5&4&3&2 \end{smallmatrix}\right) = (2,6)(3,5)$.

Zwischenstand : $|\langle(3,6),\ (2,3)(5,6),\ (2,6)(3,5)\rangle| = 8 < 48$ ([17]). Es kann $(2,6)(3,5)$ weiters wieder entfallen.

---

[12] `Factorisation(XXXX^2 + (ga1^2 + ga5^2));`
[13] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,5)>);`
[14] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,5)(3,6)>);`
[15] `Factorisation(XXXX^2 + (ga1^2 + ga6^2));`
[16] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,6,5,3)>);`
[17] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,6)(3,5)>);`

Fall $\gamma_1' = \gamma_2$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \ = \ X^4 + \gamma_2^2 X^2 + (\gamma_2^4 + 1) \ ,$$

welches die Nullstellen γ_1, γ_3, γ_4 und γ_6 hat ([18]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \ = \ X^2 + (\gamma_2^2 + \gamma_1^2) \ ,$$

welches die Nullstellen γ_3 und γ_6 hat ([19]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_2, \gamma_1, \gamma_3)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_5) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6 \ . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&1&3&5&4&6 \end{smallmatrix}\right) = (1,2)(4,5)$.

Zwischenstand : $|\langle (3,6),\ (2,3)(5,6),\ (1,2)(4,5)\rangle| = 48$ ([20]).

Abbruch der Fallunterscheidungen, da fertig!

Als Ergebnis erhalten wir das isomorphe Bild von $\mathrm{Gal}(X^6 + X^2 + 1)$ in $\mathcal{S}_6$

$$\langle (3,6),\ (2,3)(5,6),\ (1,2)(4,5)\rangle \ .$$

Die Liste ihrer Elemente erhält man mit

```
{u : u in sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (1,2)(4,5)>};
```

Mit etwas mehr Erfahrung kann man sich auch "verdächtige Fälle" auswählen, um so ein langes Stagnieren des Erzeugnisses, wie hier geschehen, zu verhindern zu versuchen.

[18] `Factorisation(XXXX^4 + ga2^2 * XXXX^2 + (ga2^4 + 1));`
[19] `Factorisation(XXXX^2 + (ga2^2 + ga1^2));`
[20] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (1,2)(4,5)>);`