M. Künzer

Galoistheorie, WS 08/09

Lösung 14

Aufgabe 48

(1) Zunächst zeigen wir, daß für $a \in \mathbf{Z}$ genau dann $g^a = 1$ ist, wenn $\mathrm{o}(g) = n$ ein Teiler von a ist. Ist $a \equiv_n 0$, so ist $g^a = 1$. Ist umgekehrt $g^a = 1$, so schreibe $a = nq + r$ mit $q \in \mathbf{Z}$ und $r \in [0, n-1]$. Dann folgt $g^r = g^{nq} g^r = g^a = 1$, und also, wegen der Minimalität von $\mathrm{o}(g)$, $r = 0$; vgl. Aufgabe 11.

Sei $U \leqslant G$. Sei $e := |G|/|U| = n/|U|$; vgl. Aufgabe 38.(1.c). Wir wollen zeigen, daß $U = \langle g^e \rangle$.

Ist $g^i \in U$, so ist $(g^i)^{|U|} = 1$ mit Aufgabe 11.(1.c), und also $i|U|$ ein Vielfaches von $n = e|U|$. Somit ist i Vielfaches von e, und also $g^i \in \langle g^e \rangle$. Insgesamt ist $U \leqslant \langle g^e \rangle$.

Ferner ist $\mathrm{o}(g^e) = |U|$; vgl. Aufgabe 27.(2). Also ist $|U| = |\langle g^e \rangle|$; vgl. Aufgabe 11.(1.b). Es folgt $U = \langle g^e \rangle$.

(2) Schreibe $\mathrm{Frob} := \mathrm{Frob}_{\mathbf{F}_{p^s}}$. Es ist $\mathrm{Gal}(\mathbf{F}_{p^s} | \mathbf{F}_p) = \langle \mathrm{Frob} \rangle$ von Ordnung s; vgl. §3.6.

Sei d ein Teiler von s. Sei $K := \mathrm{Fix}_{\langle \mathrm{Frob}^d \rangle} \mathbf{F}_{p^s}$. Es ist $\mathrm{Gal}(\mathbf{F}_{p^s} | K) = \langle \mathrm{Frob}^d \rangle$ von Ordnung s/d; vgl. Satz 8.(2) aus §3.5.1.3 und Aufgabe 27.(2). Also ist $[K : \mathbf{F}_p] = d$, insbesondere also $K \simeq \mathbf{F}_{p^d}$.

Auf diese Weise erhält man alle Zwischenkörper, da jede Untergruppe von $\langle \mathrm{Frob} \rangle$ nach (1) von der Form $\langle \mathrm{Frob}^d \rangle$ ist für einen Teiler d von s, und da nach Satz 9 (Hauptsatz der Galoistheorie) aus §3.5.2 jeder Körper zwischen $\mathbf{F}_{p^s}$ und $\mathbf{F}_p$ Fixkörper einer Untergruppe von $\langle \mathrm{Frob} \rangle$ in $\mathbf{F}_{p^s}$ ist.

(3) Es ist $X^6 + X + 1 \in \mathbf{F}_2[X]$ irreduzibel. Also können wir $\mathbf{F}_{64} = \mathbf{F}_2(\varepsilon)$ mit $\varepsilon^6 = \varepsilon + 1$ konstruieren.

Dies kann z.B. mittels

```
F := GF(2);
R<X> := PolynomialRing(F);
Factorisation(X^6 + X + 1);
FF<e> := ext<F | X^6 + X + 1>;
```

in Magma geschehen.

Es ist $\mathrm{Gal}(\mathbf{F}_{64} | \mathbf{F}_2) = \langle \mathrm{Frob}_{\mathbf{F}_{64}} \rangle$ von Ordnung 6. Schreibe kurz $\mathrm{Frob} := \mathrm{Frob}_{\mathbf{F}_{64}}$.

Gemäß (1) sind die Untergruppen von $\langle \mathrm{Frob} \rangle$ gegeben durch

$$
\begin{tikzcd}
 & \{\mathrm{id}_{\mathbf{F}_{64}}\} \arrow[dl, dash] \arrow[dr, dash] & \\
\langle \mathrm{Frob}^2 \rangle \arrow[dr, dash] & & \langle \mathrm{Frob}^3 \rangle \arrow[dl, dash] \\
 & \langle \mathrm{Frob} \rangle &
\end{tikzcd}
$$

wobei $|\langle \mathrm{Frob}^2 \rangle| = 3$ und $\langle \mathrm{Frob}^3 \rangle| = 2$.

Sicher ist $\mathrm{Fix}_{\{\mathrm{id}_{\mathbf{F}_{64}}\}} \mathbf{F}_{64} = \mathbf{F}_{64} = \mathbf{F}_2(\varepsilon)$ und $\mathrm{Fix}_{\langle \mathrm{Frob} \rangle} \mathbf{F}_{64} = \mathbf{F}_2$; vgl. erste Bemerkung in §3.5.1.4.

Wir berechnen $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64}$. Eine $\mathbf{F}_2$-Basis von $\mathbf{F}_{64}$ ist gegeben durch $(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)$. Da $\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}$ eine surjektive $\mathbf{F}_2$-lineare Abbildung von $\mathbf{F}_{64}$ nach $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64}$ ist, wird unter dieser Abbildung diese Basis auf ein $\mathbf{F}_2$-Erzeugendensystem abgebildet; vgl. §3.5.1.2.

Allgemein ist $\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(x) = x + x^4 + x^{16}$ für $x \in \mathbf{F}_{64}$.

Somit wird

$$
\begin{array}{rl}
 & \big(\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(1),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^2),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^3),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^4)),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^5)\big) \\
= & \big(1+1+1,\ \varepsilon + \varepsilon^4 + \varepsilon^{16},\ \varepsilon^2 + \varepsilon^8 + \varepsilon^{32},\ \varepsilon^3 + \varepsilon^{12} + \varepsilon^{48},\ \varepsilon^4 + \varepsilon^{16} + \varepsilon,\ \varepsilon^5 + \varepsilon^{20} + \varepsilon^{17}\big) \\
= & \big(1,\ 1,\ 1,\ 0,\ 1,\ \varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5\big)
\end{array}
$$

Also ist eine $\mathbf{F}_2$-Basis von $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle}\, \mathbf{F}_{64}$ gegeben durch $(1,\ \varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5)$. Somit ist

$$\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle}\, \mathbf{F}_{64} \ = \ \mathbf{F}_2(\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5)\ .$$

In der Tat ist $\mu_{\varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5,\mathbf{F}_2}(X) = X^2 + X + 1$, womit wir mit Satz 3 (Morphismen induziert von Nullstellen) einen Isomorphismus

$$\begin{array}{rcl} \mathbf{F}_4 & \xrightarrow{\sim} & \mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle}\, \mathbf{F}_{64} \\ \alpha & \longmapsto & \varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 \end{array}$$

bekommen, unter Verwendung unserer Standardnotation.

Wir berechnen $\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle}\, \mathbf{F}_{64}$. Eine $\mathbf{F}_2$-Basis von $\mathbf{F}_{64}$ ist gegeben durch $(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)$.

Allgemein ist $\mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(x) = x + x^8$ für $x \in \mathbf{F}_{64}$.

Somit wird

$$\begin{array}{rl} & \big(\mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(1),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^2),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^3),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^4)),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^5)\big) \\ = & \big(1+1,\ \varepsilon + \varepsilon^8,\ \varepsilon^2 + \varepsilon^{16},\ \varepsilon^3 + \varepsilon^{24},\ \varepsilon^4 + \varepsilon^{32},\ \varepsilon^5 + \varepsilon^{40}\big) \\ = & \big(0,\ \varepsilon + \varepsilon^2 + \varepsilon^3,\ 1 + \varepsilon + \varepsilon^2 + \varepsilon^4,\ 1 + \varepsilon^3 + \varepsilon^4,\ 1 + \varepsilon^3 + \varepsilon^4,\ 1 + \varepsilon + \varepsilon^2 + \varepsilon^3\big) \end{array}$$

Also ist eine $\mathbf{F}_2$-Basis von $\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle}\, \mathbf{F}_{64}$ gegeben durch $(1,\ \varepsilon + \varepsilon^2 + \varepsilon^3,\ \varepsilon^3 + \varepsilon^4,\ )$. Beachte, daß

$$(\varepsilon + \varepsilon^2 + \varepsilon^3)^2 \ = \ 1 + (\varepsilon + \varepsilon^2 + \varepsilon^3) + (\varepsilon^3 + \varepsilon^4)\ .$$

Somit ist

$$\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle}\, \mathbf{F}_{64} \ = \ \mathbf{F}_2(\varepsilon + \varepsilon^2 + \varepsilon^3)\ .$$

In der Tat ist $\mu_{\varepsilon+\varepsilon^2+\varepsilon^3,\mathbf{F}_2}(X) = X^3 + X + 1$, womit wir mit Satz 3 (Morphismen induziert von Nullstellen) einen Isomorphismus

$$\begin{array}{rcl} \mathbf{F}_8 & \xrightarrow{\sim} & \mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle}\, \mathbf{F}_{64} \\ \beta & \longmapsto & \varepsilon + \varepsilon^2 + \varepsilon^3 \end{array}$$

bekommen, unter Verwendung unserer Standardnotation.

Alle Zwischenkörper in ein dem obigen Untergruppendiagramm entsprechendes Diagramm eingetragen, erhalten wir also folgendes.

$$\begin{tikzcd}[column sep=tiny] & \mathbf{F}_{64} = \mathbf{F}_2(\varepsilon) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbf{F}_4 \simeq \mathbf{F}_2(\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5) \arrow[dr, dash] & & \mathbf{F}_2(\varepsilon + \varepsilon^2 + \varepsilon^3) \simeq \mathbf{F}_8 \arrow[dl, dash] \\ & \mathbf{F}_2 & \end{tikzcd}$$

Aufgabe 49

(1) Es sind $\mathcal{S}_1 = \{\mathrm{id}\}$ und $\mathcal{S}_2 = \langle (1,2) \rangle$ abelsch und somit auflösbar.

Die Auflösbarkeit von $\mathcal{S}_3$ wurde im ersten Beispiel in §4.1 eingesehen.

Wir zeigen die Auflösbarkeit von $\mathcal{S}_4$. Es ist $N := \langle (1,2)(3,4),\ (1,3)(2,4) \rangle$ ein abelscher Normalteiler von $\mathcal{S}_4$, vgl. Bemerkung zur Vorsicht in §4.1.

Sei $A := \langle (1,2)(3,4),\ (1,3)(2,4),\ (1,2,3) \rangle$ ([1]). Laut Magma ist $|A| = 12$.

Sei allgemein G eine endliche Gruppe, und sei $H \leqslant G$ mit $2|H| = |G|$. Wir *behaupten,* daß $H \trianglelefteq G$.

Sei $g \in G$. Zu zeigen ist, daß ${}^gH = gHg^{-1} \overset{!}{=} H$, i.e. daß $gH \overset{!}{=} Hg$.

[1] Es ist $A = \mathcal{A}_4$ der Kern der Signumsabbildung $\mathcal{S}_4 \longrightarrow \{\pm 1\}$.

Wir bemerken, daß $G = H \sqcup xH = H \sqcup Hx$ für jedes $x \in G \setminus H$; vgl. Aufgabe 38.(1). Insbesondere ist $xH = G \setminus H = Hx$.

Ist nun $g \in H$, so ist $gH = H = Hg$. Ist $g \notin H$, so ist $gH = G \setminus H = Hg$ mit der eben gemachten Bemerkung. Dies zeigt die *Behauptung.*

Insbesondere ist $A \trianglelefteqslant \mathcal{S}_4$. Da $N \trianglelefteqslant \mathcal{S}_4$, ist auch $N \trianglelefteqslant A$. Insgesamt also

$$\{\mathrm{id}\} \ \trianglelefteqslant\ N \ \trianglelefteqslant\ A \ \trianglelefteqslant\ \mathcal{S}_4 \ .$$

Wie schon festgestellt, ist $N/\{\mathrm{id}\} \simeq N$ abelsch.

Eine Gruppe von Primzahlordnung p ist zyklisch, und also auch abelsch. Denn ein Element darin hat Ordnung 1 oder p; vgl. Aufgabe 11.(1.c). Also hat jedes Element $\neq 1$ darin Ordnung p, und erzeugt daher die Gruppe; vgl. Aufgabe 11.(1.b).

Somit ist A/N zyklisch wegen $|A/N| = |A|/|N| = 3$ prim; vgl. Lösung zu Aufgabe 38.(1).

Ferner ist $\mathcal{S}_4/A$ zyklisch wegen $|\mathcal{S}_4/A| = |\mathcal{S}_4|/|A| = 2$ prim; vgl. Lösung zu Aufgabe 38.(1).

Insgesamt ist $\mathcal{S}_4$ als auflösbar nachgewiesen.

(2) Sei, dem Hinweis folgend, $M \trianglelefteqslant N \leqslant \mathcal{S}_n$ mit N/M abelsch gegeben. Wir *behaupten,* daß wenn N alle Zykel der Länge 3 enthält, so auch M.

Seien $x,\ y \in N$. Da N/M abelsch ist, wird

$$\begin{aligned}(xyx^{-1}y^{-1})M &= (xM)(yM)(xM)^{-1}(yM)^{-1}\\ &= (xM)(xM)^{-1}(yM)(yM)^{-1}\\ &= ((xx^{-1})M)((yy^{-1})M)\\ &= 1\cdot M\ ,\end{aligned}$$

und also $xyx^{-1}y^{-1} \in M$.

Sei (a,b,c) ein beliebiger Zykel von Länge 3 aus $\mathcal{S}_n$. Sei $\{a,b,c,d,e\} \subseteq [1,n]$ mit $|\{a,b,c,d,e\}| = 5$. Dies ist möglich, da $n \geqslant 5$.

Nach Voraussetzung sind (a,b,d) und (a,c,e) in N. Mit der eben gemachten Bemerkung wird

$$M \ \ni\ (a,b,d)\circ(a,c,e)\circ(a,b,d)^{-1}\circ(a,c,e)^{-1} \ =\ (a,b,c)\ .$$

Somit enthält auch M jeden Zykel von Länge 3 aus $\mathcal{S}_n$.

Sei nun *angenommen,* es ist $\mathcal{S}_n$ auflösbar. Sei

$$\{\mathrm{id}\} \ =\ G_0 \ \trianglelefteqslant\ G_1 \ \trianglelefteqslant\ \cdots \ \trianglelefteqslant\ G_k \ =\ \mathcal{S}_n$$

eine Subnormalreihe mit allen Subfaktoren abelsch. Es enthält G_k alle Zykel der Länge 3 aus $\mathcal{S}_n$. Da nun mit G_i auch G_{i-1} jeweils alle Zykel der Länge 3 aus $\mathcal{S}_n$ enthält, folgt mit absteigender Induktion, daß dies auch für $G_0 = \{\mathrm{id}\}$ zutrifft. Dies ist ein *Widerspruch.*

Also existiert in $\mathcal{S}_n$ keine Subnormalreihe mit allen Subfaktoren abelsch. D.h. $\mathcal{S}_n$ ist nicht auflösbar.

Aufgabe 50

Sei $\hat{f}(X) \in K[X]$ das Produkt über die Menge der irreduziblen normierten Faktoren von $f(X) \in K[X]$. Es ist L auch ein Zerfällungskörper von $\hat{f}(X)$ über K, da mit $f(X)$ auch sein Teiler $\hat{f}(X)$ in $L[X]$ in Linearfaktoren zerfällt, und da jede Nullstelle von $f(X)$ in L auch eine Nullstelle von $\hat{f}(X)$ ist, und somit die Nullstellen des letzteren ebenfalls L über K erzeugen.

Es folgt $(\deg f)! = n! = [L : K] \leqslant (\deg \hat{f})! \leqslant (\deg f)!$, also $(\deg \hat{f})! = (\deg f)!$, also $\deg \hat{f} = \deg f$ und also $\hat{f}(X) = f(X)$; vgl. Satz 4 aus §2.5.2.

In anderen Worten, $f(X) \in K[X]$ zerfällt in ein Produkt verschiedener normierter irreduzibler Faktoren.

Somit können wir die letzte Folgerung aus §3.4.1 anwenden, und stellen fest, daß $\mathrm{Gal}(f(X)) \xrightarrow{\sim} \mathcal{S}_n$. In anderen Worten, für jede Permutation der Nullstellen von $f(X)$ in L gibt es einen Automorphismus von $L|K$, der zu dieser Permutation einschränkt.

Sei nun *angenommen,* es ist $f(X) = u(X)v(X)$ mit $u(X), v(X) \in K[X]$ normiert und mit $\deg u, \deg v \geqslant 1$. Dann gibt es ein $y \in L$ mit $u(y) = 0$ und ein $z \in L$ mit $v(z) = 0$. Da y und z insbesondere beides Nullstellen von $f(X)$ in L sind, gibt es nach dem eben Gesagten ein $\sigma \in \mathrm{Aut}(L|K)$ mit $\sigma(y) = z$. Also ist $u(z) = u(\sigma(y)) = \sigma(u(y)) = \sigma(0) = 0$ und $v(z) = 0$. Somit ist $\mu_{z,K}(X)$ ein Teiler von $u(X)$ und von $v(X)$; vgl. Satz 2 aus §2.3.2. Also ist $\mu_{z,K}(X)^2$ ein Teiler von $f(X)$, und wir haben einen *Widerspruch.*

Ein alternatives Argument. Die Konstruktion des Zerfällungskörpers liefert nur dann eine Erweiterung von Grad $n!$, wenn im i-ten Schritt eine Erweiterung von Grad $n - i + 1$ vorgenommen wird, wobei $i \in [1, n]$, denn ansonsten resultiert ein echt kleinerer Grad. Zerfällt nun $f(X)$ in zwei Faktoren von Grad $\geqslant 1$, so ist schon im ersten Schritt keine Erweiterung um Grad n mehr möglich.

Aufgabe 51

(1) Der Zerfällungskörper von $X^5 + 5X^2 + 3 \in \mathbf{Q}[X]$ ergibt sich mittels Magma zu $\mathbf{Q}(a, b)$ mit

$$\begin{array}{rcl} 0 & = & a^5 + 5a^2 + 3 \\ 0 & = & b^2 - \frac{1}{3}(a^4 + a^3 + a^2 + 3a + 3)b - (a - 1)\ . \end{array}$$

Insbesondere ist $[\mathbf{Q}(a, b) : \mathbf{Q}] = 10$, und somit auch $|\,\mathrm{Gal}(X^5 + 5X^2 + 3)| = 10$.

Wir berechnen $\mathrm{Gal}(X^5 + 5X^2 + 3) = \langle (2, 3)(4, 5), (1, 2, 4, 5, 3)\rangle$. Der zugehörige Magma-Quelltext:

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^5 + 5*X^2 + 3);
KK<a> := ext<Q | X^5 + 5*X^2 + 3>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^5 + 5*XX^2 + 3);
KKK<b> := ext<KK | XX^2 + 1/3*(-a^4 - a^3 - a^2 - 3*a - 3)*XX - a + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^5 + 5*XXX^2 + 3);
RBIG<Ga1,Ga2,Y> := PolynomialRing(Q,3);
Ga3 := -Ga2 + 1/3*(Ga1^4 + Ga1^3 + Ga1^2 + 3*Ga1 + 3);
Ga4 := 1/3*(Ga1^4 + 5*Ga1)*Ga2 - 1/3*(Ga1^4 + 5*Ga1);
Ga5 := -1/3*(Ga1^4 + 5*Ga1)*Ga2 - 1/3*(Ga1^3 + Ga1^2 + Ga1 + 3);
ga1 := a;
ga2 := b;
ga3 := Evaluate(Ga3,[ga1,ga2,0]);;
ga4 := Evaluate(Ga4,[ga1,ga2,0]);;
ga5 := Evaluate(Ga5,[ga1,ga2,0]);;
(XXX-ga1)*(XXX-ga2)*(XXX-ga3)*(XXX-ga4)*(XXX-ga5); // zur Probe
muga1 := Y^5 + 5*Y^2 + 3;
muga2 := Y^2 - 1/3*(Ga1^4 + Ga1^3 + Ga1^2 + 3*Ga1 + 3)*Y - (Ga1 - 1);

muga1s:= Evaluate(muga1,[0,0,XXX]);
Factorisation(muga1s); // 12345 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga1,0,XXX]);
Factorisation(muga2s); // 23 (resultierende Nullstellennummern)
Evaluate(Ga3,[ga1,ga3,0]); // 2
Evaluate(Ga4,[ga1,ga3,0]); // 5
Evaluate(Ga5,[ga1,ga3,0]); // 4 // (2,3)(4,5)
Order(sub<SymmetricGroup(5) | (2,3)(4,5)>);
// *** Zwischenstand: Ordnung = 2 ***
muga1s:= Evaluate(muga1,[0,0,XXX]);
Factorisation(muga1s); // 12345 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga2,0,XXX]);
Factorisation(muga2s); // 14 (resultierende Nullstellennummern)
Evaluate(Ga3,[ga2,ga4,0]); // 1
```

```
Evaluate(Ga4,[ga2,ga4,0]); // 5
Evaluate(Ga5,[ga2,ga4,0]); // 3 // (1,2,4,5,3)
Order(sub<SymmetricGroup(5) | (2,3)(4,5), (1,2,4,5,3)>);
// *** Zwischenstand: Ordnung = 10 ***
```

Sei $G := \mathrm{Gal}(X^5 + 5X^2 + 3) = \langle (2,3)(4,5), (1,2,4,5,3) \rangle$. Sei $N := \langle (1,2,4,5,3) \rangle \leqslant G$.

Da $|G| = 2|N|$, ist $N \trianglelefteq G$; vgl. Argument in der Lösung zu Aufgabe 49.(1). Betrachte die Subnormalreihe

$$\{\mathrm{id}\} \;\trianglelefteq\; N \;\trianglelefteq\; G\,.$$

Da die Subfaktoren beide von primer Ordnung sind, namentlich 5 und 2, sind beide Subfaktoren zyklisch, insbesondere abelsch; vgl. Argument in der Lösung zu Aufgabe 49.(1)

Somit ist G auflösbar. Mit dem Satz von Galois aus §4.4.2 ist mithin $X^5+5X^2+3 \in \mathbf{Q}[X]$ auflösbar.

(2) Der Zerfällungskörper von $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ ergibt sich mittels Magma in der üblichen Weise zu $\mathbf{Q}(a, b, c, d)$ mit

$$\begin{array}{rcl}
0 & = & a^5 + 5a^2 + 2 \\
0 & = & b^4 + ab^3 + a^2b^2 + (a^3 + 5)b + (a^4 + 5a) \\
0 & = & c^3 + (b + a)c^2 + (b^2 + ab + a^2)c + (b^3 + ab^2 + a^2b + (a^3 + 5)) \\
0 & = & d^2 + (c + (b + a))d + (c^2 + (b + a)c + (b^2 + ab + a^2))\,.
\end{array}$$

Insbesondere ist $[\mathbf{Q}(a, b, c, d) : \mathbf{Q}] = 5 \cdot 4 \cdot 3 \cdot 2 = 5!$, und somit $\mathrm{Gal}(X^5 + 5X^2 + 2) = \mathcal{S}_5$; vgl. letzte Folgerung in §3.4.1.

Ferner hat sich im Verlauf dieser Rechnung $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ als irreduzibel herausgestellt, was auch mit Aufgabe 50 im nachhinein nochmals bestätigt wird.

Dank Aufgabe 49.(2) ist $\mathcal{S}_5$ nicht auflösbar. Mit dem Satz von Galois aus §4.4.2 ist mithin $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ nicht auflösbar.