LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
7. Februar 2019

Algebra – Lösungsskizzen zu Übungsblatt 13

Aufgabe 1

a) Man überzeugt sich schnell davon, dass $L = \mathbb{Q}(\sqrt{2}, i)$ gilt, und mit dem Gradlemma berechnet man $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$; es folgt $|G(L/\mathbb{Q})| = 4$. Wir wollen die Galoisgruppe explizit angeben. Dazu erkennen wir, dass es auf $\mathbb{Q}(\sqrt{2})$ die zwei Isomorphismen $\phi_1, \phi_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ gibt, die durch $\phi(\sqrt{2}) = \sqrt{2}$ und $\phi_2(\sqrt{2}) = -\sqrt{2}$ eindeutig bestimmt sind. Dass dies die einzigen Isomorphismen sind, folgt aus der Tatsache, dass jeder Isomorphismus die Nullstellen des Minimalpolynoms $f = X^2 - 2$ von $\sqrt{2}$ auf Nullstellen von f abbilden muss und dass jeder Isomorphismus durch das Bild von $\sqrt{2}$ eindeutig festgelegt ist. Mit den gleichen Argumenten findet man nun die vier möglichen Isomorphismen von L:

$$\begin{array}{cccc} \phi_{1,1} : L \to L & \phi_{1,2} : L \to L & \phi_{2,1} : L \to L & \phi_{2,2} : L \to L \\ \sqrt{2} \mapsto \sqrt{2} & \sqrt{2} \mapsto \sqrt{2} & \sqrt{2} \mapsto -\sqrt{2} & \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i & i \mapsto -i & i \mapsto i & i \mapsto -i \end{array}$$

Damit ist die Galoisgruppe bestimmt und es gilt $G(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wir finden die Untergruppen $\{id\}, \langle\phi_{1,2}\rangle, \langle\phi_{2,1}\rangle, \langle\phi_{2,2}\rangle, G(L/\mathbb{Q})$.
Zu den Fixkörpern: Man sieht schnell ein, dass $L^{\{id\}} = L$, $L^{G(L/\mathbb{Q})} = \mathbb{Q}$, $L^{\langle\phi_{1,2}\rangle} = \mathbb{Q}(\sqrt{2})$ und $L^{\langle\phi_{2,1}\rangle} = \mathbb{Q}(i)$ gilt. Zur Untergruppe $\langle\phi_{2,2}\rangle$ korrespondiert nach dem Hauptsatz der Galoistheorie ein Körper von Grad 2 über $\mathbb{Q}$. Offensichtlich gilt auch $\phi_{2,2}(i\sqrt{2}) = i\sqrt{2}$ und $\mathbb{Q}(i\sqrt{2}) = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset L$ ist eine Körpererweiterung von $\mathbb{Q}$ von Grad 2, die in $L^{\langle\phi_{2,2}\rangle}$ enthalten ist. Insgesamt folgt also bereits die Gleichheit.

b) Die Nullstellen von g sind schnell gefunden, sie lauten: $\sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}$ und $-i\sqrt[4]{5}$. Wegen $\sqrt[4]{5}, i\sqrt[4]{5} \in M$ folgt ebenso schnell, dass $\sqrt[4]{5}, i \in M$ gilt; insbesondere sehen wir somit $M = \mathbb{Q}(\sqrt[4]{5}, i)$ ein. Jetzt erkennt man noch, dass $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ eine Erweiterung von Grad 4 ist (Minimalpolynom!) und dass $\mathbb{Q}(\sqrt[4]{5}, i)/\mathbb{Q}(\sqrt[4]{5})$ eine Erweiterung von Grad 2 ist (Der kleinere Körper ist Teilmengen von $\mathbb{R}$, der große nicht, also ist der Grad größer gleich 2. Außerdem ist $X^2 + 1 \in \mathbb{Q}(\sqrt[4]{5})[X]$ und damit ist der Grad kleiner gleich 2). Damit hat nach dem Gradsatz $M/\mathbb{Q}$ den Grad 8. Zu galoissch: Separabel ist klar als algebraische Erweiterung des perfekten Körpers $\mathbb{Q}$ und normal ist ebenso klar als Zerfällungskörper von f.

Zur Galoisgruppe: Jedes Element $\rho \in G(M/\mathbb{Q})$ permutiert die Nullstellen der Minimalpolynome von Elementen in M, insbesondere die Nullstellen von $X^2 + 1$ und

$g = X^4 - 5$. Insbesondere finden wir die Elemente σ, τ in $G(M/\mathbb{Q})$, die durch folgende Bedingungen eindeutig definiert sind:

$$\begin{aligned} \sigma : M &\to M & \qquad \tau : M &\to M \\ i &\mapsto -i & \qquad i &\mapsto i \\ \sqrt[4]{5} &\mapsto \sqrt[4]{5} & \qquad \sqrt[4]{5} &\mapsto i\sqrt[4]{5} \end{aligned}$$

Jetzt zeigt schnelles Nachrechnen $\sigma(\tau(i\sqrt[4]{5})) = -\sqrt[4]{5} \neq \sqrt[4]{5} = \tau(\sigma(i\sqrt[4]{5}))$, also ist $G(M/\mathbb{Q})$ nicht abelsch[1].

Zu den gesuchten Zwischenkörpern: τ hat Ordnung 4, also hat $\langle\tau\rangle$ Index 2 in $G(M/\mathbb{Q})$ und ist insbesondere Normalteiler. Der Hauptsatz der Galoistheorie sagt uns nun, dass $E = M^{\langle\tau\rangle}$ galoissch über $\mathbb{Q}$ ist.

Dann rechnen wir noch nach, dass $\left(\tau\sigma\tau^{-1}\right)(\sqrt[4]{5}) = -\sqrt[4]{5}$ gilt, also insbesondere auch $\tau\sigma\tau^{-1} \neq \sigma, id$. Damit ist $\langle\sigma\rangle$ kein Normalteiler in $G(M/\mathbb{Q})$ und $E' = M^{\langle\sigma\rangle}$ ist keine galoissche Erweiterung von $\mathbb{Q}$.

Aufgabe 2

Sei E/K galoissch mit $G(E/K) \cong S_n$, $n \geq 5$.

a) Wir wollen zeigen, dass es genau einen Zwischenkörper F von E/K mit $[F : K] = 2$ gibt. Mit dem Hauptsatz der Galoistheorie, gibt es genau dann einen solchen Zwischenkörper, wenn es genau eine Untergruppe von S_n gibt mit Index 2. Dies gilt aber, denn jede Untergruppe von Index 2 ist ein Normalteiler. Sei also $H \cong A_n$ mit $H \leq G(E/K)$, dann ist $F := E^H$ der gesuchte Körper.

b) Da nach Satz 1.7.7 des Protokolls gilt $A_n \lhd S_n$, gilt natürlich auch $G(E/F) \lhd G(E/K)$ und nach dem Hauptsatz der Galoistheorie, dass $G(F/K)$ galoissch ist.

c) Die Bemerkung nach Folgerung 1.7.9 des Protokolls sagt, dass A_n für $n \geq 5$ einfach ist, d.h. die Normalteilerreihe von S_n mit $n \geq 5$ ist: $\{1\} \lhd A_n \lhd S_n$.
Wir wollen nun zeigen, dass es keinen Zwischenkörper L von E/F gibt mit L/F galoissch. Um das zu zeigen, nehmen wir an, dass einen nicht-trivialen Zwischenkörper L gibt, so dass L/F galoissch ist. Mit dem Hauptsatz der Galoistheorie folgt dann, dass $G(E/L) \lhd G(E/F)$ gilt. Per Voraussetzung gilt aber $G(E/F) \cong A_n$. Da der Zwischenkörper nicht trivial sein soll (also nicht E oder F), gibt es einen nicht-trivialen Normalteiler der A_n. Dies ist aber ein Widerspruch zu A_n einfach. Wir können also folgern, dass es keinen Zwischenkörper L mit der gewünschten Eigenschaft geben kann.

d) Nach Satz 5.1.3 des Protokolls gilt, dass eine Erweiterung L/F genau dann galoissch ist, wenn L/F normal und separabel ist.
Wir wissen bereits, dass E/F galoissch ist, also ist E/F mit dem obigen Satz 5.1.3 separabel.
Wir nehmen nun an, dass es gibt einen Zwischenkörper L von E/F, so dass L/F normal ist. Zudem wissen wir bereits, dass L/F separabel ist, da E/F separabel ist (mit Satz 4.5.12). Dann muss mit Satz 5.1.3 L/F auch galoissch sein. Widerspruch zu Teilaufgabe c). Also gibt es keinen Zwischenkörper L mit der gewünschten Eigenschaft.

[1] Wer sich etwas mehr Mühe macht, kann zeigen, dass $G(M/\mathbb{Q})$ isomorph zu D_4, also zur Symmetriegruppe eines regelmäßigen Vierecks, ist. Jede solche Symmetriegruppe D_n eines regelmäßigen n-Ecks ist von einer Drehung und einer Spiegelung erzeugt. In unserem Falle entspricht dabei σ der Spiegelung und τ der Drehung, was man durch eine kleine Skizze sofort nachvollziehen kann.

e) Gelte nun $G(E/K) \cong S_p$ für eine Primzahl $p \geq 5$. Wir wissen, dass gilt $|S_p| = p!$ und somit die p-Sylowuntergruppen die Ordnung p haben. Außerdem kann man zeigen, dass es $(p-2)!$ verschiedene p-Sylowuntergruppen gibt. Sei nun $\{M_i : 1 \leq i \leq (p-2)!\}$ die Menge der Untergruppen von $G(E/K)$ die isomorph zu diesen p-Sylowuntergruppen der S_p sind. Dann gibt es nach dem Hauptsatz der Galoistheorie genau $(p-2)!$ Zwischenkörper $N_i := E^{M_i}$. Für diese Zwischenkörper N_i gilt: $[N_i : K] = (p-1)!$, da $p! = [E : K] = [E : N_i] \cdot [N_i : K]$ und $[E : N_i] = |M_i| = p$.

Aufgabe 3

a) Zuerst wollen wir festhalten, dass mit Lemma 5.1.7 E'/K eine Galoiserweiterung mit Galoisgruppe $G := G(E'/K)$ ist. Per Definition enthält E' alle Nullstellen von $f(X)$. Sei $\beta \in N$ und $\tau \in G$. Dann gilt also $f(\beta) = 0$ nach Voraussetzung und da τ Elemente aus K festhält bekommen wir $f(\tau(\beta)) = \tau(f(\beta)) = 0$, also auch $\tau(\beta) \in N$. Offensichtlich gilt auch für $\beta \in N$ und $\mathrm{id} \in G$, $\mathrm{id}(\beta) = \beta$ und für $\tau_1, \tau_2 \in G$: $(\tau_1 \circ \tau_2)(\beta) = \tau_1(\tau_2(\beta))$.

b) Aus Lemma 1.8.2 folgt, dass uns die Linkstranslation T_g von $G(E'/K)$ nach $S(N)$ ein Gruppenhomomorphismus ist. Der Zerfällungskörper enthält per Definition von allen Elemente aus N (über K) erzeugt. Ein Automorphismus von E'/K nach E'/K der alle Erzeuger festhält, muss aber schon die Identität sein. Also ist der Kern der Abbildung trivial und der Homomorphismus injektiv.

c) Sei $n \leq 4$, nicht wie in der Angabe angeführt $n \leq 5$, da ist mir leider ein Tippfehler passiert. Mit Teilaufgabe b) können wir G als Untergruppe der S_n auffassen. Wir wissen für diese S_n, dass sie auflösbar sind, also ist G als Untergruppe einer auflösbaren Gruppe auflösbar. Satz 1.6.5 der Vorlesung sagt uns aber, dass für endliche und auflösbare Gruppen eine Normalreihe mit zyklischen Faktoren exisitiert. Sei diese $\{1\} \triangleleft G_1 \triangleleft G_2 \cdots \triangleleft G_m = G$. Wir setzen nun $K_{m-1} := K_m^{G_1}$. Da G_1 nun zyklisch ist, folgt aus dem Hauptsatz der Galoistheorie, dass K_m/K_{m-1} eine zyklische Galoiserweiterung ist. Nun definieren wir $K_{m-2} := K_m^{G_2}$. Also bekommen wir mit dem Hauptsatz der Galoistheorie, dass K_m/K_{m-2} eine Galoiserweiterung mit Galoisgruppe G_2 ist. Da aber (wegen Normalreihe) auch $G_1 \triangleleft G_2$ gilt, ist wiederum mit dem Hauptsatz, K_{m-1}/K_{m-2} eine Galoiserweiterung mit einer Galoisgruppe isomorph zu G_2/G_1. Da die Faktoren der Normalreihe aber zyklisch sind, haben wir auch hier die gewünschte Eigenschaft gezeigt. Man sieht jetzt, dass man dieses Vorgehen iterieren kann bis $K_0 = K_m^{G_m}$ und somit ist die Teilaufgabe gezeigt.

Aufgabe 4

a) Sei $G(E/K)$ abelsch, ist $G(E/F)$ ein Normalteiler und somit ist F/K nach Satz 5.1.9 galoissch und somit auch normal.

b) Sei E/K galoissch und $G(E/K)$ eine p-Gruppe, i.e. $|G(E/K)| = p^m$ für ein $m \in \mathbb{N}$. Wir wollen nun einen Zwischenkörper F von E/K finden für den gilt: $[E : F] = p$ und F/K galoissch. Der Hauptsatz der Galoistheorie sagt uns einerseits, dass es für i) reicht, eine Untergruppe $H \leq G(E/K)$ zu finden mit $|H| = p$, denn dann gilt für $F := E^H$ $[E : F] = |H| = p$, andererseits sollte dann für ii) $G(E/F) \triangleleft G(E/K)$ erfüllt sein, denn dann gilt: F/K ist galoissch.
Wir haben somit die Lösung dieser körpertheoretischen Aufgabe reduziert auf ein

Problem der Gruppentheorie, nämlich: Finde für eine p-Gruppe $G := G(E/K)$ einen Normalteiler der Ordnung p.
Nach Satz 1.6.4 aus dem Protokoll, wissen wir nun, dass G ein nicht-triviales Zentrum hat. Das Zentrum ist natürlich abelsch und ein Normalteiler von G. Als Untergruppe einer p-Gruppe ist das Zentrum wiederum eine p-Gruppe. Nun können wir Lemma 1.9.3 aus dem Protokoll anwenden, dass unter der Voraussetzung, dass eine Primzahl p die Gruppenordnung einer endlichen abelschen Gruppe teilt, garantiert, dass eine Untergruppe der Ordnung p gibt. Wir nennen diese Untergruppe von $Z(G)$ nun H. Zusätzlich stellen wir fest, dass H als Untergruppe des Zentrums auch ein Normalteiler von G ist. Also haben wir ingesamt gezeigt, dass ein $H \lhd G$ existiert mit $|H| = p$ und somit die gesamte Aussage gezeigt.