Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 12. Übungsblatt

Aufgabe 1. Diese Aufgabe wurde inzwischen in der Vorlesung gelöst: Denn $L = \mathbb{Q}(\mu_3)$ ist der dritte Kreisteilungskörper, und dieser ist galoissch über $\mathbb{Q}$ mit Galoisgruppe isomorph zu $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$, wobei der nichttriviale Automorphismus gegeben ist durch $\zeta_3 \mapsto \zeta_3^2 = \zeta_3^{-1}$.
Ich skizziere trotzdem noch einen Beweis von Hand: Da ζ_3, ζ_3^2 und $\zeta_3^3 = 1$ die Nullstellen von $X^3 - 1$ sind, ist L Zerfällungskörper dieses Polynoms und damit galoissch über $\mathbb{Q}$. Das Minimalpolynom von ζ_3 ist $(X^3 - 1)/(X - 1) = X^2 + X + 1$, und dessen Nullstellen sind ζ_3 und ζ_3^{-1}. Also sind die Automorphismen genau gegeben durch $\zeta_3 \mapsto \zeta_3$ oder ζ_3^{-1}.

Aufgabe 2. In der Vorlesung wurde die Galoisgruppe bereits berechnet; ich wiederhole die Berechnung noch einmal: Zunächst ist $L = \mathbb{Q}(\sqrt[4]{3}, i)$ und $[L : \mathbb{Q}] = 8$. Ein Automorphismus $\varphi : L \to L$ ist durch $\varphi(i)$ und $\varphi(\sqrt[4]{3})$ eindeutig bestimmt. Es muß aber $\varphi(i) \in \{i, -i\}$ und $\varphi(\sqrt{4}3) \in \left\{\pm\sqrt[4]{3}, i \pm \sqrt[4]{3}\right\}$ sein (denn das sind die Nullstellenmengen der jeweiligen Minimalpolynome); das macht insgesamt 8 Möglichkeiten, und wegen $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 8$ werden alle diese Kombinationen tatsächlich durch einen Automorphismus realisiert.
Sei nun τ der Automorphismus, der $\sqrt[4]{3}$ fixiert und i auf $-i$ abbildet. Ebenso sei σ der Automorphismus, der i fixiert und $\sqrt[4]{3}$ auf $i\sqrt[4]{3}$ abbildet. Dann sieht man schnell $\mathrm{ord}\,\sigma = 4$, $\mathrm{ord}\,\tau = 2$. Außerdem ist $\tau\sigma\tau = \sigma^3$, d.h. $\tau\sigma = \sigma^3\tau$, und mit dieser Vertauschungsregel kann man jedes noch so lange Produkt von τ's und σ's umsortieren zu $\tau^i\sigma^j$ mit $0 \leqslant i \leqslant 1$ und $0 \leqslant j \leqslant 3$. Diese 8 Automorphismen sind außerdem alle verschieden, also folgt

$$G := \mathrm{Gal}(L/\mathbb{Q}) = \left\{\tau^i\sigma^j \mid 0 \leqslant i \leqslant 1, 0 \leqslant j \leqslant 3\right\}.$$

(Mit etwas mehr Begriffen aus der Gruppentheorie kann man später sehen, daß G ein „semidirektes Produkt“ von $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ ist, aber so etwas wird wohl erst in der „Höheren Algebra“ thematisiert werden.)
Für die Suche nach Zwischenkörpern schreiben wir zuerst einmal die einfachsten Zwischenkörper hin, die man sofort sehen kann, nämlich $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt[4]{3}), L$. (Daß diese alle verschieden sind, sieht man durch Vergleich der Grade.)
Die Zwischenkörper entsprechen eineindeutig den Untergruppen der Galoisgruppe. Die Untergruppen zu $\mathbb{Q}$ und L sind G und $\{\mathrm{id}\}$. Die Untergruppe zu $\mathbb{Q}(i)$ ist die vierelementige Gruppe $\mathrm{Gal}(L/\mathbb{Q}(i))$, und da diese Gruppe sicher alle σ^j, $0 \leqslant j \leqslant 3$ enthält, folgt $\mathrm{Gal}(L/\mathbb{Q}(i)) = \langle\sigma\rangle$. Ebenso sieht man $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[4]{3})) = \langle\tau\rangle$.
Jetzt beißen wir in den sauren Apfel und suchen systematisch alle Untergruppen von G. (Das ist mühsam, aber immerhin in begrenzter Zeit zu bewältigen, anders als ein wahlloses Hinschreiben immer neuer Zwischenkörper: die ganze Galoistheorie besteht ja in der Reduktion von Fragen über komplizierte Objekte (Körper) auf überschaubarere Objekte (endliche Gruppen).) Wegen $|G| = 8$ gibt es nur interessante Untergruppen mit 2 oder 4 Elementen.

i) Eine Untergruppe mit 2 Elementen besteht genau aus id und einem Element der Ordnung 2. Die einzigen Elemente in G der Ordnung 2 sind aber τ, σ^2, $\tau\sigma$, $\tau\sigma^2$ und $\tau\sigma^3$; da wir die Untergruppe $\langle\tau\rangle$ schon verarbeitet haben (ihr Fixkörper ist $\mathbb{Q}(\sqrt[4]{3})$, bleiben uns die Untergruppen $H_1 := \{\mathrm{id}, \sigma^2\}$, $H_2 := \{\mathrm{id}, \tau\sigma\}$, $H_3 := \{\mathrm{id}, \tau\sigma^2\}$, $H_4 := \{\mathrm{id}, \tau\sigma^3\}$.

ii) Eine Untergruppe mit 4 Elementen ist abelsch und isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im ersten Fall ist sie erzeugt von einem Element der Ordnung 4; im zweiten Fall von zwei miteinander kommutierenden Elementen der Ordnung 2.

(a) Die einzigen Elemente der Ordnung 4 sind σ und σ^3; sie erzeugen beide die Untergruppe $\langle\sigma\rangle$, die wir schon verarztet haben (ihr Fixkörper ist $\mathbb{Q}(i)$). (Realitätscheck: Wir haben fünf Elemente der Ordnung 2 und zwei Elemente der Ordnung 4 gefunden; zusammen mit dem neutralen Element macht das acht Elemente, d.h. wir haben nichts übersehen.)

(b) Welche der Elemente der Ordnung zwei vertauschen miteinander? Man rechnet nach, daß τ und σ^2 kommutieren; die erzeugte Untergruppe ist $I_1 = \{\mathrm{id}, \tau, \sigma^2, \tau\sigma^2\}$. Ebenso kommutieren σ^2 und $\tau\sigma^3$, die erzeugte Untergruppe ist $I_2 = \{\mathrm{id}, \sigma^2, \tau\sigma^3, \tau\sigma\}$. Weitere Kombinationen findet man nicht.

Nun berechnen wir die zugehörigen Fixkörper, wobei ich relativ wahllos die verschiedenen Methoden von meiner Auflistung der Verfahren zur Berechnung von Fixkörpern ausprobiere:

i) Die vierelementigen Untergruppen gehören zu Fixkörpern vom Grad 2, für die es also genügt, ein einziges in ihnen enthaltenes Element anzugeben (Methode „Sammeln und Gradvergleich“). Für $I_1 = \langle\tau, \sigma^2\rangle$ bemerken wir $\sigma^2(\sqrt[4]{3}) = -\sqrt[4]{3}$; ein Element, das von σ^2 und gleichzeitig auch von τ fixiert wird, ist also $(\sqrt[4]{3})^2 = \sqrt{3}$. Also folgt $L^{I_1} = \mathbb{Q}(\sqrt{3})$.

ii) Für $I_2 = \{\mathrm{id}, \sigma^2, \tau\sigma^3, \tau\sigma\}$ nehmen wir die gleiche Methode: Wir brauchen ein Element vom Grad 2 über $\mathbb{Q}$, das von $\sigma^2 : \sqrt[4]{3} \mapsto -\sqrt[4]{3}$ und gleichzeitig von $\tau\sigma$ fixiert wird, und ein solches ist $i\sqrt{3}$. Also folgt $L^{I_2} = \mathbb{Q}(i\sqrt{3})$.

iii) Für die kleinen Untergruppen mit nur zwei Elementen sind Spurmethode und die Methode des primitiven Elements besonders geeignet. Für $H_1 = \{\mathrm{id}, \sigma^2\}$ nehmen wir die Spurmethode: eine $\mathbb{Q}$-Basis von L ist

$$1, \sqrt[4]{3}, \sqrt{3}, \sqrt[4]{3}^3, i, i\sqrt[4]{3}, i\sqrt{3}, i\sqrt[4]{3}^3.$$

Anwenden der H_1-Spur $\mathrm{id} + \sigma^2$ auf diese Elemente liefert der Reihe nach

$$2, 0, 2\sqrt{3}, 0, 2i, \ldots$$

und hier kann man schon aufhören, denn $\mathbb{Q}(\sqrt{3}, i)$ hat bereits Grad 4 über $\mathbb{Q}$ und muß damit L^{H_1} sein.

iv) Für $H_2 = \{\mathrm{id}, \tau\sigma\}$ nehme ich noch einmal die Spurmethode. Anwenden von $\mathrm{id} + \tau\sigma$ auf die Basiselemente liefert

$$2, (1-i)\sqrt[4]{3}, 0, (1+i)\sqrt[4]{3}^3, 0, (i-1)\sqrt[4]{3}, 2i\sqrt{3}, (i+1)\sqrt[4]{3}^3.$$

Also wird L^{H_2} über $\mathbb{Q}$ erzeugt von $(1-i)\sqrt[4]{3}$ und $(1+i)\sqrt[4]{3}^3$. Man kann sogar zeigen, daß $L^{H_2} = \mathbb{Q}((1-i)\sqrt[4]{3})$ ist, denn die G-Bahn dieses Elementes enthält (mindestens) vier verschiedene Elemente, d.h. es erzeugt eine Erweiterung vom Grad $\geqslant 4$, also bereits L^{H_2}.

v) Für $H_3 = \{\mathrm{id}, \tau\sigma^2\}$ nehme ich die Methode des primitiven Elements: Es ist $L = \mathbb{Q}(i + \sqrt[4]{3})$ (denn dieses Element wird durch die G-Operation auf 8 verschiedene Bilder geschickt, muß also primitives Element sein). L^{H_3} wird also erzeugt von den Koeffizienten des Polynoms

$$(X - i - \sqrt[4]{3})(X - \tau\sigma^2(i + \sqrt[4]{3})) = (X - i - \sqrt[4]{3})(X + i + \sqrt[4]{3}) = X^2 - (i + \sqrt[4]{3})^2.$$

Aber wegen $(i + \sqrt[4]{3})^2 = -1 + 2i\sqrt[4]{3} + \sqrt{3}$ ist $L^{H_3} = \mathbb{Q}(\sqrt{3} + 2i\sqrt[4]{3})$.

vi) Für $H_4 = \{\mathrm{id}, \tau\sigma^3\}$ bemühe ich ein weiteres mal die Methode des primitiven Elements. Als Polynom ergibt sich

$$\begin{aligned}(X - i - \sqrt[4]{3})(X - \tau\sigma^3(i + \sqrt[4]{3})) &= (X - i - \sqrt[4]{3})(X - i\sqrt[4]{3} + i) \\ &= X^2 - (1+i)\sqrt[4]{3}X + 1 + i\sqrt{3} - (1+i)\sqrt[4]{3}.\end{aligned}$$

Also wird L^{H_4} erzeugt von $(1+i)\sqrt[4]{3}$ und $1 + i\sqrt{3} - (1+i)\sqrt[4]{3}$, d.h. $L^{H_4} = \mathbb{Q}((1+i)\sqrt[4]{3}, i\sqrt{3})$.

Aufgabe 3. Die Nullstellen von X^3-2 sind $a := \sqrt[3]{2}$, $\zeta_3 a$ und $\zeta_3^2 a$. Damit erhalten wir $L = \mathbb{Q}(a, \zeta_3 a, \zeta_3^2 a) = \mathbb{Q}(a, \zeta_3)$. Betrachten des Körperturms $\mathbb{Q} \subset \mathbb{Q}(a) \subset L$ zeigt außerdem $[L : \mathbb{Q}] = 6$ (die erste Erweiterung hat sicher Grad 3, die zweite Grad $\leqslant 2$, aber Grad 1 kann nicht sein, da $\mathbb{Q}(a)$ sich in $\mathbb{R}$ einbetten läßt, L aber nicht: es gibt immer nur eine einzige reelle dritte Wurzel einer Zahl).
Jetzt geht es wie in Aufgabe 2: Ein Automorphismus $\sigma : L \to L$ ist durch $\varphi(a)$ und $\varphi(\zeta_3)$ vollständig bestimmt. Aber da $\varphi(a) \in \{a, \zeta_3 a, \zeta_3^2 a\}$ und $\sigma(\zeta_3) \in \{\zeta_3, \zeta_3^2\}$ sein muß, gibt es insgesamt 6 Möglichkeiten, und wegen $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$ gelten muß, kommen alle vor.
Ist σ der Automorphismus, der ζ_3 fixiert und a auf $\zeta_3 a$ abbildet, und τ der Automorphismus, der a fixiert und ζ_3 auf $\zeta_3^2 = \zeta_3^{-1}$ abbildet, so rechnet man nach, daß $\mathrm{ord}\,\sigma = 3$ und $\mathrm{ord}\,tau = 2$ ist. Also wird $G := \mathrm{Gal}(L/\mathbb{Q})$ von σ und τ erzeugt (denn die von σ, τ erzeugte Untergruppe muß eine durch 2 und 3, also durch 6 teilbare Ordnung haben). Da außerdem $\tau\sigma\tau = \sigma^2$, also $\tau\sigma = \sigma^2\tau$ ist (insbesondere ist G nicht abelsch, und evtl. weiß man schon, daß die einzige nichtabelsche Gruppe mit sechs Elementen die S_3 ist), erhält man wie in Aufgabe 2

$$G = \left\{\sigma^i\tau^j \,|\, 0 \leqslant i \leqslant 2, 0 \leqslant \tau \leqslant 1\right\}.$$

Für die Suche nach Zwischenkörpern schreiben wir zuerst einmal vier Zwischenkörper hin, die man sofort sehen kann, nämlich $\mathbb{Q}, \mathbb{Q}(\zeta_3), \mathbb{Q}(a), L$. (Diese sind auch alle verschieden, denn sie haben Grade $1, 2, 3, 4$). Die noch fehlenden suchen wir mit dem Hauptsatz der Galoistheorie mittels Untersuchung von G: Die trivialen Untergruppen $\{id\}$ und G entsprechen den trivialen Zwischenkörpern L und $\mathbb{Q}$, die haben wir schon. Jede andere Untergruppe hat nach Lagrange Ordnung 2 oder 3. Nach Sylowtheorie gibt es nur eine Untergruppe der Ordnung 3, also nur einen Zwischenkörper vom Grad 2, und den haben wir schon (nämlich $\mathbb{Q}(\zeta_3)$). Außerdem gibt es eine oder drei Untergruppen der Ordnung 2, aber es müssen drei sein, denn nicht nur τ, sondern auch $\sigma\tau$ und $\sigma^2\tau$ haben die Ordnung 2. Diese Untergruppen sind also $H_1 = \{\mathrm{id}, \tau\}$, $H_2 = \{\mathrm{id}, \sigma\tau\}$, $H_3 = \{\mathrm{id}, \sigma^2\tau\}$.
Um die zugehörigen Fixkörper auszurechnen, probieren wir wieder die verschiedenen Verfahren aus. Dabei kann man aber wieder einen Trick anwenden: die Fixkörper L^{H_i} haben Grad 3, also keine echten Unterkörper mehr außer $\mathbb{Q}$. Wir müssen also jeweils nur ein Element von L^{H_i} finden, das nicht in $\mathbb{Q}$ liegt.

i) Einen Zwischenkörper zu einer Untergruppe der Ordnung 2, d.h. einen Zwischenkörper vom Grad 3, haben wir schon, nämlich $\mathbb{Q}(a)$. Da a offenbar von τ fixiert wird, ist $\mathbb{Q}(a) = L^{H_1}$.
ii) Für H_2 nehmen wir die Spurmethode: eine $\mathbb{Q}$-Basis von L ist

$$1, a, a^2, \zeta_3, \zeta_3 a, \zeta_3 a^2.$$

Die H_2-Spur ist $\mathrm{id} + \sigma\tau$, und ihre Anwendung auf die Basiselemente liefert

$$2, (1 + \zeta_3)a, \ldots.$$

Nach der Bemerkung oben können wir schon aufhören, und es folgt $L^{H_2} = \mathbb{Q}(1 + \zeta_3)a$.
iii) Für H_3 machen wir das gleiche mit der H_3-Spur $\mathrm{id} + \sigma^2\tau$. Ihre Anwendung liefert

$$2, (1 + \zeta_3^2)a, \ldots.$$

Also ist $L^{H_3} = \mathbb{Q}((1 + \zeta_3^2)a)$.

Aufgabe 4.

i) L ist Zerfällungskörper eines separablen Polynoms über K (nimm beliebige Erzeuger von L über K und multipliziere ihre Minimalpolynome, Dopplungen vermeidend). Nach Konstruktion ist LL' dann Zerfällungskörper desselben Polynoms über L'. Also ist LL'/L' normal, endlich und wieder separabel, also galoissch.

ii) Sei $\sigma \in \mathrm{Gal}(LL'/L')$. Um zu zeigen, daß man durch Einschränkung ein Element von $\mathrm{Gal}(L/L \cap L')$ erhält, müssen wir zeigen, daß σ auf $L \cap L'$ nichts tut und $\sigma(L) = L$ ist. Ersteres ist klar wegen $L \cap L' \subset L'$, zweiteres sieht man so: Es ist $\sigma(L) \subset L$, denn jedes $a \in L$ wird durch σ auf eine Nullstelle seines Minimalpolynoms über L' abgebildet, und das ist insbesondere eine Nullstelle seines Minimalpolynoms über K; aber L ist normal über K, d.h. alle diese Nullstellen liegen in L. Aus $\sigma(L) \subset L$ folgt nun $\sigma(L) = L$, da σ injektiv ist und $L/L \cap L'$ endlich ist (oder durch Betrachten von σ^{-1}). Also ist ρ eine wohldefinierte Abbildung und sicherlich ein Gruppenhomomorphismus (Einschränken vertauscht mit Komposition).
Weiter ist ρ injektiv, denn da LL' von L und L' erzeugt wird, ist ein Automorphismus von LL' eindeutig festgelegt durch seine Einschränkungen auf L' (die trivial sein muß für Elemente von $\mathrm{Gal}(LL'/L')$) und L. Für die Surjektivität von ρ sei $H \subset \mathrm{Gal}(L/L \cap L')$ das Bild von ρ. Nach dem Hauptsatz genügt es zu zeigen, daß $L^H = L \cap L'$ ist (denn dann folgt $H = \mathrm{Gal}(L/L \cap L')$, denn $L/L \cap L'$ ist ja galoissch)). Natürlich wird jedes Element von $L \cap L'$ von ganz H fixiert, liegt also in L^H. Ist aber $x \in L^H$, so wird x nach Definition von allen Elementen von $\mathrm{Gal}(LL'/L')$ fixiert, liegt also in L' und damit in $L \cap L'$, wie behauptet.

Zusatzaufgabe. Die Aussage folgt durch Kombination zweier Tatsachen:

i) Ist $K \subset L$ eine endliche Galoiserweiterung und $a \in L$ beliebig, so kann man das Minimalpolynom f von a über K folgendermaßen berechnen: Schreibe $\{\sigma(a) \mid \sigma \in \mathrm{Gal}(L/K)\} = \{a_1, \ldots, a_r\}$ mit $a_i \neq a_j$ für $i \neq j$. Dann ist $f = \prod_{i=1}^{r}(X - a_i)$.
Der Grund ist: Das Polynom $g := \prod_{i=1}^{r}(X - a_i)$ ist nach Konstruktion invariant unter der Operation von $\mathrm{Gal}(L/K)$, hat also nach Galoistheorie Koeffizienten in K. Andererseits muß jedes Polynom über K mit Nullstelle a alle a_i als Nullstelle haben, d.h. $g \mid f$. Zusammen folgt $g = f$.

ii) Ist $K \subset L = K(a)$ eine einfache endliche Erweiterung, M ein Zwischenkörper und g das Minimalpolynom von a über M, so wird M über K erzeugt von den Koeffizienten von g.
Der Grund ist: Sei M' der von den Koeffizienten von g erzeugte Zwischenkörper; dann ist $M' \subset M$. Andererseits ist g das Minimalpolynom von a auch über M', d.h. $L = K(a) = M(a) = M'(a)$ hat den gleichen Grad über M wie über M', und nach dem Gradsatz folgt $[M : M'] = 1$, d.h. $M = M'$.

In der Aufgabe nun ist $K \subset L = K(a)$ Galoissch, also auch $L^H \subset L = L^H(a)$ mit Galoisgruppe H. Das Minimalpolynom von a über L^H ist also $\prod_{\sigma \in H}(X - \sigma(a))$, denn die $\sigma(a)$ sind paarweise verschieden, da a primitives Element ist. Nach ii) folgt dann die Behauptung.