Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 13

Jendrik Stelzner

Letzte Änderung: 2. Februar 2018

Aufgabe 1

(a)

Durch Reduzieren bezüglich der Primzahl $p = 2$ erhalten wir das Polynom

$$\overline{f}(t) = t^3 + t + 1 \in \mathbb{F}_2[t]\,.$$

Dies ist ein Polynom von Grad 3 über dem Körper $\mathbb{F}_2$, dass keine Nullstellen (in $\mathbb{F}_2$) hat. Folglich ist $\overline{f}(t)$ irreduzibel. Damit ist nach dem Reduktionskriterium auch $f(t)$ irreduzibel, da $f(t)$ primitiv ist (und somit normiert).

Der Körper $\mathbb{Q}(t)$ ist perfekt, da $\operatorname{char}(\mathbb{Q}) = 0$ gilt. Das irreduzible Polynom $f(t) \in \mathbb{Q}[t]$ ist deshalb separabel, d.h. $f(t)$ hat keine mehrfache Nullstelle in L.

Bemerkung 1. Mit etwas mit Hintergrundswissen, als aus der Vorlesung bekannt ist, ließe sich auch wie folgt argumentieren:

Da $\mathbb{Q}$ ein Körper ist, genügt es auch zu zeigen, dass $f(t)$ keine rationale Nullstelle besitzt.

Da $f(t)$ ein normiertes Polynom mit ganzzahligen Koeffizienten ist, lässt sich zeigen, dass jede rationale Nullstelle von $f(t)$ bereits ganzzahlig ist (dies ist eine nicht-triviale Aussage, die *nicht* aus der Vorlesung bekannt ist). Damit genügt es dann zu zeigen, dass $f(t)$ keine ganzzahlige Nullstelle hat. Jede konstante Nullstelle von $f(t)$ muss den konstanten Koeffizienten von $f(t)$ teilen, also ein Teiler von -1 sein. Somit sind 1 und -1 die einzigen beiden möglichen rationalen Nullstellen von $f(t)$.

Da aber $f(1) = -3$ und $f(-1) = 1$ gelten, hat $f(t)$ somit keine rationale Nullstelle, ist also irreduzibel.

(b)

Es seien $x_1, x_2, x_3 \in L$ die drei paarweise verschiedenen Nullstellen von $f(t)$ in L.

Die Galoisgruppe $\operatorname{Gal}(L/\mathbb{Q})$ wirkt auf der Menge der Wurzeln $\{x_1, x_2, x_3\}$, und diese Wirkung entspricht einem Gruppenhomomorphismus $\alpha\colon \operatorname{Gal}(L/\mathbb{Q}) \to S(\{x_1, x_2, x_3\})$. Indem wir eine Bijektion zwischen den Mengen $\{x_1, \dots, x_n\}$ und $\{1, 2, 3\}$ wählen (etwa vermöge der Abbildung $x_i \mapsto i$) erhalten wir einen induzierten Gruppenisomorphismus $\varphi\colon S(\{x_1, x_2, x_3\}) \to S_3$. Damit erhalten wir insgesamt einen Grupenhomomorphismus $\beta \coloneqq \varphi \circ \alpha\colon \operatorname{Gal}(L/\mathbb{Q}) \to S_3$.

Die Wirkung der Galoisgruppe $\operatorname{Gal}(L/\mathbb{Q})$ auf der Menge der Nullstellen $\{x_1, x_2, x_3\}$ ist treu, der Gruppenhomomorphismus α also injektiv. Also ist auch β injektiv. Außerdem ist die Wirkung von $\operatorname{Gal}(L/\mathbb{Q})$ auf $\{x_1, x_2, x_3\}$ transitiv, da $f(t)$ irreduzibel ist; deshalb ist auch die Wirkung von $\operatorname{im}\beta$ auf der Menge $\{1, 2, 3\}$ transitiv.

Lemma 2. *Die Untergruppen der symmetrischen Gruppe S_3 sind die triviale Gruppe 1, die zweielementigen Gruppen $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$, sowie die beiden Gruppen A_3 und S_3.*

Beweis. Ist $H < G$ eine echte Untergruppe, so muss $\operatorname{ord}(H)$ ein echter Teiler von $\operatorname{ord}(S_3) = 6$ sein, also $\operatorname{ord}(H) \in \{1, 2, 3\}$ gelten. Inbesondere muss H zyklisch sein. Damit ergeben sich die echten Untergruppen $\langle 1\rangle = 1$, $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$ und $\langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle = A_3$. □

Die einzigen Untergruppen von S_3, die transitiv auf $\{1, 2, 3\}$ wirken, sind also A_3 und S_3. Somit gilt $\operatorname{im}\beta = A_3$ oder $\operatorname{im}\beta = S_3$.

Bemerkung 3. Eine Untergruppe $H \leq S_n$, die transitiv auf der Menge $\{1, \dots, n\}$ wirkt (bezüglich der Einschränkung der kanonischen Wirkung von S_n auf $\{1, \dots, n\}$) ist eine *transitive Untergruppe*.

(c)

Wir geben mehrere mögliche Vorgehensweisen an:

- Zunächst rechnen wir nach, dass $a^2 - a - 2$ nd $2 - a^2$ Nullstellen von $f(t)$ sind.
  - Hierfür setzen wir beide Werte in das Polynom $f(t)$ ein und Vereinfachen anschließend dei Ergebnisse mithilfe der Identität $a^3 = 3a + 1$ (die eine Umformulierung der Annahme $0 = f(a) = a^3 - 3a + 1$ ist): Es gilt

$$\begin{aligned}
&f(a^2 - a - 2) \\
&= (a^2 - a - 2)^3 - 3(a^2 - a - 2) - 1 \\
&= a^6 - 3a^5 - 3a^4 + 11a^3 + 3a^2 - 9a - 3 \\
&= a^3(3a + 1) - 3a^2(3a + 1) - 3a(3a + 1) + 11(3a + 1) + 3a^2 - 9a - 3 \\
&= 3a^4 - 8a^3 - 9a^2 + 21a + 8 \\
&= 3a(3a + 1) - 8(3a + 1) - 9a^2 + 21a + 8 = 0\,,
\end{aligned}$$

und es gilt

$$
\begin{aligned}
f(2-a^2) &= (2-a^2)^3 - 3(2-a^2) - 1 = -a^6 + 6a^4 - 9a^2 + 1 \\
&= -a^3(3a+1) + 6a^1(3a+1) - 9a^2 + 1 = -3a^4 - a^3 + 9a^2 + 6a + 1 \\
&= -3a(3a+1) - (3a+1) + 9a^2 + 6a + 1 = 0\,.
\end{aligned}
$$

- Mithilfe von Polynomdivison erhalten wir, dass

$$
\begin{aligned}
f(a^2-a-2) &= a^6 - 3a^5 - 3a^4 + 11a^3 + 3a^2 - 9a - 3 \\
&= (a^3 - 3a^2 + 3)\underbrace{(a^3 - 3a - 1)}_{=0} = 0\,,
\end{aligned}
$$

und dass

$$
f(a^2-a-2) = -a^6 + 6a^4 - 9a^2 + 1 = (-a^3 + 3a - 1)\underbrace{(a^3 - 3a - 1)}_{=0} = 0\,.
$$

Es bleibt zu zeigen, dass die Nullstellen a, a^2-a-2 und $2-a^2$ paarweise verschieden sind, dass es sich also tatsächlich um alle drei Nullstellen von a handelt. Dies ergibt sich daraus, dass $f(t)$ das Minimalpolynom von a ist (denn $f(t)$ ist irreduzibel mit $f(a) = 0$), und somit die Potenzen $1, a, a^2$ linear unabhängig über $\mathbb{Q}$ sind.

- Es gilt

$$
\begin{aligned}
&(t-a)(t-(a^2-a-2))(t-(2-a^2)) \\
=\,& t^3 + (-a^4 + a^3 + 3a^2 - 2a - 4)t + (a^5 - a^4 - 4a^3 + 2a^2 + 4a)
\end{aligned}
$$

Analog zu den obigen Rechnungen lassen sich die Koeffizienten vereinfachen, wodurch sich das Polynom $f(t)$ ergibt.

Wir erhalten nun, dass die einfache Körpererweiterung $\mathbb{Q}(a)$ bereits alle Nullstellen des Polynoms $p(t)$ erhalten. Somit ist $\mathbb{Q}(a)$ bereits ein Zerfälllungskörper von $f(t)$, weshalb bereits $L = \mathbb{Q}(a)$ gilt.

Die Körpererweiterung $L/\mathbb{Q}$ ist galoissch, da L ein Zerfällungskörper des separablen Polynoms $f(t) \in \mathbb{Q}[t]$ ist. Damit erhalten wir, dass

$$
|\mathrm{Gal}\,(L/\mathbb{Q})| = [L:\mathbb{Q}] = [\mathbb{Q}(a):\mathbb{Q}] = \deg m_a(t) = \deg f(t) = 3\,.
$$

Damit erhalten wir, dass es sich bei $\mathrm{Gal}\,(L/\mathbb{Q})$ nicht um S_3 handelt, sondern um A_3.

(d)

Da die Erweiterung $L/\mathbb{Q}$ galoissch ist, entsprechen die Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}$ in bijektiver Weise den Zwischengruppen $1 \leq H \leq \mathrm{Gal}\,(L/\mathbb{Q})$, also Untergruppen von $\mathrm{Gal}\,(L/\mathbb{Q})$. Da $\mathrm{Gal}\,(L/\mathbb{Q}) \cong A_3 \cong \mathbb{Z}/3$ gilt, sind 1 und $\mathrm{Gal}\,(L/\mathbb{Q})$ die einzigen beiden Untergruppen von $\mathrm{Gal}\,(L/\mathbb{Q})$. Folglich sind $\mathbb{Q}$ und L die einzigen beiden Zwischenkörper von L.

Aufgabe 4

(a)

Die Aussage ist *wahr*:

Da jedes Element $x \in M$ separabel über K ist, gilt dies insbesondere für jedes $x \in L$. Also ist auch die Erweiterung L/K separabel.

Jedes $x \in M$ ist Nullstelle eines separablen Polynoms $f(t) \in K[t]$, da M/K separabel ist. Indem wir $f(t)$ als ein Polynom $f(t) \in L[t]$ auffassen, ist x dann auch Nullstelle eines separablen Polynoms $f(t) \in L[t]$. Also ist auch die Erweiterung M/L separabel.

(b)

Die Aussage ist *wahr*, denn die Erweiterung $\mathbb{Q}(\pi, i)/\mathbb{Q}(\pi)$ ist normal und separabel:

Da $\operatorname{char}(\mathbb{Q})(\pi) = 0$ gilt, ist der Körper $\mathbb{Q}(\pi)$ perfekt, und die Körpererweiterung $\mathbb{Q}(\pi, i)/\mathbb{Q}(\pi)$ somit separabel.

Das Polynom $t^2 + 1 \in \mathbb{Q}(\pi)$ zerfällt über der Körperweiterung $\mathbb{C}/\mathbb{Q}(\pi)$ in die Linearfaktoren $(t-i)(t+i)$, weshalb $\mathbb{Q}(\pi, i) = \mathbb{Q}(\pi)(i, -i)$ der Zerfällungskörper von t^2+1 in $\mathbb{C}/\mathbb{Q}(\pi)$ ist. Somit ist $\mathbb{Q}(\pi, i)/\mathbb{Q}(\pi)$ ein Zerfällungskörper von $t^2 + 1$, die Erweiterung also normal.

(c)

Die Aussage ist *falsch*: Man betrachte etwa die Körpererweiterung $L/\mathbb{Q}$ aus Aufgabe 1: Dort gilt $[L : \mathbb{Q}] = 3$, aber die Erweiterung $L/\mathbb{Q}$ hat nur zwei Zwischenkörper.

(d)

Die Aussage ist *falsch*:

Ist K ein beliebiger Körper, so ist die Erweiterung K/K eine endliche Galoiserweiterung, so dass es keine echten Zwischenkörper $K \subsetneq L \subsetneq K$ gibt. Aber $[K : K] = 1$ ist nicht prim.

Bemerkung 4. Schließt man den Fall $L = K$ aus, so *stimmt* die Aussage: Dann ist $G \coloneqq \operatorname{Gal}(L/\mathbb{Q})$ eine endliche Gruppe, und nach dem Hauptsatz der Galoistheorie entsprechen die Zwischenkörper $K \subseteq M \subseteq L$ bijektiv den Untergruppen der Galoisgruppe G. Die Gruppe G ist nicht-trivial, da $|G| = [L : K] > 1$ gilt, und nach Annahme besitzt G keine Untergruppen außer 1 und G.

Behauptung. *Es gilt $G \cong \mathbb{Z}/p$ mit p prim.*

Beweis. Für $g \in G$ mit $g \neq 1$ ist die Untergruppe $\langle g \rangle$ eine nicht-triviale Untergruppe von G, und somit nach Annahme $G = \langle g \rangle$. Also ist die nicht-trivale Gruppe G zyklisch, und somit gilt $G \cong \mathbb{Z}/n$ für ein $n \geq 2$. Ist n nicht prim, so besitzt $\mathbb{Z}/n$ nicht-triviale echte Untergruppen. □

Somit ist $[L : K] = |G| = p$ prim, da L/K galoissch ist.