Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 10. Übungsblatt

Aufgabe 1.

i) Eine K-Basis von L ist beispielsweise $1, \sqrt{d}$. Wir müssen die K-lineare Abbildung $f : L \to L$ betrachten mit $f(x) = (a + b\sqrt{d})x$. Es ist $f(1) = a + b\sqrt{d}$ und $f(\sqrt{d}) = bd + a\sqrt{d}$, also erhalten wir bezüglich der angegebenen Basis die darstellende Matrix

$$A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

und nach Definition ist $\mathrm{Tr}_{L/K}(a + b\sqrt{d}) = \mathrm{Tr}\, A = 2a$ und $N_{L/K}(a + b\sqrt{d}) = \det A = a^2 - b^2 d$.

ii) Ich schreibe $\varepsilon := \sqrt[3]{e}$. Eine K-Basis von F ist $1, \varepsilon, \varepsilon^2$, und wir betrachten $g : F \to F$ mit $g(x) = (a + b\varepsilon + c\varepsilon^2)x$. Es ist $g(1) = a + b\varepsilon + c\varepsilon^2$, $g(\varepsilon) = ce + a\varepsilon + b\varepsilon^2$, $g(\varepsilon^2) = be + ce\varepsilon + a\varepsilon^2$. Als darstellende Matrix ergibt sich also

$$B = \begin{pmatrix} a & ce & be \\ b & a & ce \\ c & b & a \end{pmatrix},$$

also $\mathrm{Tr}_{F/K}(a+b\varepsilon+c\varepsilon^2) = \mathrm{Tr}\, B = 3a$ und $N_{F/K}(a+b\varepsilon+c\varepsilon^2) = \det B = a^3+(b^2-3ac)be+c^3e^2$.

Aufgabe 2.

i) Da das Polynom Grad 3 hat, genügt es zu zeigen, daß es keine rationale Nullstelle hat. Als Nullstellen kommen aber nur ± 1 in Frage, und die sind beide keine. (Hier wurde die folgende, sehr nützliche Tatsache verwendet: ist $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ mit $a_0, a_n \neq 0$, so hat jede rationale Nullstelle von f die Form a/b mit $a \mid a_0$ und $b \mid a_n$. Wer diesen Satz noch nicht kennt, beweise ihn bitte, am besten gleich in einer verallgemeinerten Fassung für beliebige faktorielle Ringe.)

ii) Das geht genau wie in Aufgabe 1: Nach Vorlesung bilden $1, x, x^2$ eine $\mathbb{Q}$-Basis von L. Mit $\varphi(a) := (1 + x^2)a$ haben wir $\varphi(1) = 1 + x^2$, $\varphi(x) = x + x^3 = -1$, $\varphi(x^2) = -x$ und damit die darstellende Matrix

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0, \end{pmatrix}$$

wodurch sich die Spur 1 und die Norm 1 ergeben.

Aufgabe 3. Es sei $L \subset M$ eine Körpererweiterung und $a \in M$ algebraisch über L. Nach Voraussetzung ist a separabel über K, aber das impliziert Separabilität über L (denn das Minimalpolynom über L ist ein Teiler des Minimalpolynoms über K, vgl. Lösung zu Aufgabe 3 von Blatt 9). Also ist L vollkommen.

Aufgabe 4. Beide Polynome haben Grad m und sind normiert, also genügt es zu zeigen, daß f ein Vielfaches von $g := \prod_{i=0}^{m-1}(T - a^{p^i})$ ist. Nun ist aber $f(T^p) = f(T)^p$ nach dem Satz vom Frobeniushomomorphismus (und da die Koeffizienten von f im Primkörper liegen, also beim Frobenius unverändert bleiben), d.h. mit a sind auch a^p, $(a^p)^p = a^{p^2}$ usw. Nullstellen von f. Wir sind also fertig, wenn wir zeigen, daß $a, a^p, \ldots, a^{p^{d-1}}$ paarweise verschieden sind. Wäre aber $a^{p^i} = a^{p^j}$ für $0 \leqslant i < j < m$, so hätten wir wegen $a^{p^i} = (a^{p^{j-i}})^{p^i}$ und der Injektivität des Frobenius die Beziehung $a = a^{p^{j-i}}$. Damit wäre nun a eine Nullstelle von $X^{p^{j-i}} - X$ und hätte damit Grad $\leqslant j - i$ über P, aber das Minimalpolynom von a ist f vom Grad $m > j - i$, Widerspruch.

Aufgabe 5.

i) Ich biete zwei Argumente an, eines konkret und eines abstrakter.

   (a) Durch Induktion nach k (mit einem geeigneten Induktionsanfang, wobei ich persönlich den Extremfall $k = 0$ bevorzuge) reduziert man auf den Fall $k = 2$, der da lautet: Sind $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd, so ist $\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$. In dieser Gleichung ist „$\leqslant$“ (sogar „$|$“) ohne jede Voraussetzung an die Ordnungen von a und b korrekt. Ist aber $(ab)^e = 1$, so folgt insbesondere $a^e = b^{-e}$; da ganz allgemein ist die Ordnung einer Potenz eines Elementes ein Teiler der Ordnung des Elementes selbst ist, muß die Ordnung von $a^e = b^{-e}$ also ein gemeinsamer Teiler von $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ und damit 1 sein. Also folgt $a^e = b^{-e} = 1$, d.h. e ist durch $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ und damit durch $\mathrm{ord}(a) \cdot \mathrm{ord}(b)$ teilbar, womit die noch fehlende Ungleichung gezeigt ist.

   (b) Es sei $n_i := \mathrm{ord}(a_i)$ und $n := \prod_{i=1}^k n_i$. Es gibt genau einen Gruppenhomomorphismus $\varphi : \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z} \to G$ mit $(e_1, \ldots, e_k) \mapsto \prod_{i=1}^k a_i^{e_i}$. Das Bild von φ enthält alle a_i, muß also eine durch alle n_i und damit durch n teilbare Ordnung haben; also hat es genau n Elemente, d.h. φ ist injektiv. Aber es ist $\varphi(\overline{1}, \ldots, \overline{1}) = \prod_{i=1}^k a_i$, und $(\overline{1}, \ldots, \overline{1})$ hat die Ordnung n nach dem chinesischen Restsatz (denn es ist das Bild von $\overline{1}$ unter dem Isomorphismus $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$). Das zeigt die Behauptung.

ii) Ist a_i ein Element der Ordnung $p_i^{n_i}$ für alle i, so hat $a := \prod_{i=1}^r a_i$ nach Teil i) die Ordnung n, ist also ein Erzeuger von G, d.h. G ist zyklisch. – Alternativ könnte man mit den Sylowschen Sätzen argumentieren: Da G abelsch ist, gibt es zu jedem Primteiler von $|G|$ nur eine einzige Sylowsche Untergruppe, und daraus folgt mit etwas Arbeit, daß G direktes Produkt seiner Sylow-Untergruppen ist. Nach Voraussetzung sind diese aber zyklisch, und nach dem chinesischen Restsatz folgt, daß auch G zyklisch ist.

Aufgabe 6. Das geht wie Aufgabe 2 von Blatt 9. Um zu zeigen, daß K ein Körper ist, muß man zeigen, daß d irreduzibel in $\mathbb{Z}[i]$ ist (was im Fall, daß d eine Primzahl in $\mathbb{Z}$ ist, äquivalent dazu ist, daß -1 kein Quadrat in $\mathbb{Z}/d\mathbb{Z}$ ist). Um das zu tun, verwenden wir wieder die „Norm“ $N(a + bi) = a^2 + b^2$ (das ist tatsächlich die Norm $N_{\mathbb{C}/\mathbb{R}}(a + bi)$ oder $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi)$), von der wir schon wissen: $z = a + bi \in \mathbb{Z}[\sqrt{-1}]$ ist genau dann invertierbar, wenn $N(z) = 1$ ist; vgl. die Lösungen zu Aufgaben 3 und 4 von Blatt 5.)

i) Wäre 3 nicht irreduzibel, so gäbe es nicht-invertierbare $z, w \in \mathbb{Z}[i]$ mit $zw = 3$ mit folgt $9 = N(z)N(w)$, also $N(z) = N(w) = 3$. Aber die Gleichung $a^2 + b^2 = 3$ hat keine ganzzahligen Lösungen, Widerspruch. Also ist 3 irreduzibel, d.h. K ist ein Körper. – Die Charakteristik von K ist die eindeutig bestimmte Primzahl, die in K zu null wird, und 3 wird sicher zu null. Also ist der Primkörper $P = \mathbb{Z}/3\mathbb{Z}$. Außerdem zeigt man wie in Aufgabe 2 von Blatt 9, daß K aus P durch Adjunktion einer Wurzel aus $-\overline{1}$ entsteht, und damit folgt $[K : P] = 2$.

ii) Dieser Fall ist sogar einfacher, denn $N(1+i) = 2$ ist prim, so daß aus $zw = 1+i$, also $N(z)N(w) = 2$ sofort $N(z) = 1$ oder $N(w) = 1$ folgt. – Außerdem ist $2 = (1+i)(1-i)$ ein Vielfaches von $d = 1+i$, wird also null, d.h. der Primkörper ist $P = \mathbb{Z}/2\mathbb{Z}$. Außerdem behaupte ich $P = K$: denn jedes Element von K hat die Form $z = \overline{a+bi}$ mit $a, b \in \mathbb{Z}$, aber wegen $\overline{i} = -\overline{1}$ folgt $z = \overline{a-b} \in P$. Insbesondere ist also $[K : P] = 1$.

iii) Der Fall geht genau wie der letzte, und als Primkörper bekommt man $\mathbb{Z}/5\mathbb{Z}$ und wieder $[K : P] = 1$ (wegen $\overline{i} = -\overline{2}$).

Aufgabe 7. Jetzt kommen leider die abstrakteren Geschichten.

i) Ich zeige zuerst eine nützliche allgemeine Tatsache: Ist L/K eine normale Erweiterung und $\overline{K}$ ein algebraischer Abschluß von K, so ist jeder K-Homomorphismus $\varphi : L \to \overline{K}$ in Wirklichkeit ein Automorphismus von L über K; insbesondere gibt es von beiden Arten von Abbildungen genau gleich viele. Aber für jedes $a \in L$ ist $\varphi(a) \in L$ (denn $\varphi(a)$ muß eine Nullstelle des Minimalpolynoms von a sein, und die liegen alle in L), also ist φ schon einmal ein K-Homomorphismus $L \to L$. Ist $[L : K]$ endlich, und das ist der für uns wichtige Fall, so folgt daraus schon die Bijektivität, und wir sind fertig.[1]
Um jetzt $|\mathrm{Aut}(L/K)|$ zu bestimmen, muß man also nur die K-Homomorphismen $L \to \overline{K}$ zählen. Das ist zum einen schon in der Vorlesung gemacht – es gibt genau $d = [L : K]$ Stück, wie behauptet –, aber man kann es sich mit dem Satz vom primitiven Element auch noch einmal überlegen: Nach diesem gibt es ein $a \in L$ mit $L = K(a)$, und das Minimalpolynom von a hat genau d verschiedene Nullstellen in $\overline{K}$. Aber die K-Homomorphismen $L \to \overline{K}$ sind genau dadurch bestimmt, daß a auf eine dieser Nullstellen von f abgebildet wird, also gibt es d solche Homomorphismen.

ii) Nach dem, was wir in (i) bemerkt haben, genügt es, die Formeln

$$N_{L/K}(x) = \prod_{\sigma : L \to \overline{K}} \sigma(x) \quad \text{und} \quad \mathrm{Tr}_{L/K}(x) = \sum_{\sigma : L \to \overline{K}} \sigma(x)$$

zu beweisen, und diese sind sogar für beliebige endliche separable Erweiterungen richtig. Für die Spur wurde das in der Vorlesung gezeigt, und der gleiche Beweis funktioniert auch für die Norm; ich führe ihn trotzdem noch einmal vor – doppelt (und vielleicht auch: leicht unterschiedlich!) erklärt lernt sich besser.
Die Idee ist, die Körpererweiterung zu zerlegen in $K \subset K(x) \subset L$. Nach der Transitivitätsformel für die Norm gilt

$$N_{L/K}(x) = N_{K(x)/K} \circ N_{L/K(x)}(x) \overset{(*)}{=} N_{K(x)/K}(x^e) = \big(N_{K(x)/K}(x)\big)^e$$

mit $e = [L : K(x)]$, wobei wir in $(*)$ die Formel für die Norm eines Elements des Grundkörpers verwendet haben.
Nun gilt ja $N_{K(x)/K}(x) = \prod_{\sigma : K(x) \to \overline{K}} \sigma(x)$ nach Vorlesung.[2] Wir sind also fertig, wenn wir zeigen: Jeder K-Homomorphismus $K(x) \to \overline{K}$ ist Einschränkung von genau e verschiedenen K-Homomorphismen $L \to \overline{K}$. Das ist aber (fast) genau Satz III.4.9 der Vorlesung.

[1] Interessiert einen der allgemeine Fall, so muß man ein anderes Argument bemühen, zum Beispiel dieses: Sei $a \in L$ mit Minimalpolynom f über K, und es sei $X \subset L$ die Nullstellenmenge von f. Dann induziert φ eine Abbildung $X \to X$, die (wie φ selbst) injektiv ist. Aber X ist endlich, also ist diese Abbildung auch surjektiv, d.h. es gibt ein $x \in X$ mit $\varphi(x) = a$. Das zeigt die Surjektivität von $\varphi : L \to L$.

[2] Denn die rechte Seite ist das Produkt aller Nullstellen, also $\pm$ der konstante Term des Minimalpolynoms f von x über K. Daß dieser mit der Norm auf der linken Seite übereinstimmt, wurde in der Vorlesung durch Angabe einer konkreten darstellenden Matrix bewiesen; ein abstrakterer Beweis ist der folgende: $N_{K(x)/K}(x)$ ist die Determinante, also $\pm$ der konstante Term des charakteristischen Polynoms g der Abbildung $\varphi_x : K(x) \to K(x)$, $a \mapsto xa$. Nun ist aber nach Cayley–Hamilton $0 = g(\varphi_x) = \varphi_{g(x)}$, woraus $g(x) = 0$ folgt, und damit ist g ein Vielfaches von f. Vergleich der Grade zeigt $g = f$, also folgt die Behauptung. (Vgl. zu dieser Technik auch den Lösungsvorschlag zur Zusatzaufgabe von Blatt 7.)

Aufgabe 8.

i) Körperhomomorphismen sind injektiv, also kann man die Frage umformulieren: kann es in einer separablen Erweiterung $K \subset L$ einen Zwischenkörper F geben, der inseparabel über K ist? Nein, nach einer Aufgabe vom letzten Übungsblatt, oder direkt: Separabilität ist eine Aussage über alle Elemente von L, die deshalb auch für Zwischenkörper gilt.

ii) Ja, beispielsweise könnte ja L einfach der separable Abschluß von K in F sein.

iii) In i) ändert sich nichts. In ii) dagegen sehr wohl: jedes Element von $M \setminus K$ ist inseparabel über K, also muß ein Homomorphismus $L \to M$ Bild in K haben, und das geht nur, wenn $K = L$ ist.