Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 7. Übungsblatt

Aufgabe 1.

i) Zunächst ist $\sqrt{a}$ sicherlich eine Nullstelle von $X^2 - a$, und das ist genau dann irreduzibel über $\mathbb{Q}$, wenn es keine rationale Nullstelle besitzt, d.h. wenn $\sqrt{a} \notin \mathbb{Q}$ gilt. Andernfalls ist das Minimalpolynom $X - \sqrt{a}$.
Ebenso ist $\sqrt[3]{a}$ eine Nullstelle von $X^3 - a$. Gibt es kein $b \in \mathbb{Q}$ mit $b^3 = a$, so ist das Polynom irreduzibel und damit das gesuchte Minimalpolynom. Andernfalls folgt $b = \sqrt[3]{a}$ (deswegen, weil wir uns darauf verständigt haben, die unter letzterem Ausdruck die *reelle* dritte Wurzel zu verstehen!), und wir erhalten das Minimalpolynom $X - \sqrt[3]{a}$.

ii) Es ist $\zeta_3^3 = 1$, also ist ζ_3 Nullstelle von $X^3 - 1$. Dieses Polynom ist nicht irreduzibel, denn es hat nach der geometrischen Summenformel die Faktorisierung $(X-1)(X^2+X+1)$. Nun ist ζ_3 sicher keine Nullstelle des ersten Faktors und muß dafür Nullstelle von $F := X^2 + X + 1$ sein. Dieses Polynom ist außerdem irreduzibel, wie man etwa durch Reduktion modulo 2 sieht (das einzige normierte irreduzible Polynom vom Grad 2 modulo 2 ist gerade $X^2 + X + 1$).

Bemerkung: Was wäre passiert, wenn wir in i) statt der *reellen* dritten Wurzel von a eine der *komplexen* dritten Wurzeln genommen hätten? Falls a keine dritte Potenz in $\mathbb{Q}$ ist, hätte sich nichts geändert, da dann immer noch $X^3 - a$ irreduzibel ist. Im anderen Fall passiert nun etwas: Ist $a = b^3$ mit $b \in \mathbb{Q}$, so ist $X^3 - a = X^3 - b^3 = (X-b)(X^2+bX+b^2)$ nach der geometrischen Summenformel. Eine nicht-reelle dritte Wurzel von a ist keine Nullstelle des ersten Faktors, muß also eine Nullstelle des zweiten Faktors $X^2 + bX + b^2$ sein. Da dieser irreduzibel ist (mangels rationaler Nullstellen), ist er dann das gesuchte Minimalpolynom.

Aufgabe 2.

i) Es sei $\varphi : K \to L$ ein Ringhomomorphismus, wobei K und L Körper sind. Der Kern von φ ist ein Ideal in K und kann damit nur 0 oder K selbst sein. Der zweite Fall würde aber $\varphi = 0$ bedeuten, was nicht sein kann, denn $\varphi(1_K) = 1_L \neq 0_L$. Also hat φ trivialen Kern und ist damit injektiv.
Alternativ könnte man den Kern auch zu Fuß ausrechnen: Ist $0 \neq a \in K$, so ist $\varphi(a) \cdot \varphi(a^{-1}) = \varphi(1_K) = 1_L$, d.h. $\varphi(a) \neq 0$, und damit ist $\ker \varphi = 0$.

ii) Sei $a \in L$ beliebig. Da L ein endlichdimensionaler K-Vektorraum ist, können die unendlich vielen Elemente $1, a, a^2, a^3, \dots$ nicht K-linear unabhängig sein. Es gibt also eine nichttriviale Gleichung der Form $\sum_{i=0}^n r_i a^i = 0$ mit $r_i \in K$, und das zeigt, daß a Nullstelle des nichttrivialen Polynoms $\sum_{i=0}^n r_i X^i \in K[X]$ ist. Also ist a algebraisch.

Aufgabe 3. Die Idee ist, aus einer K-Basis von L und einer L-Basis von M eine K-Basis von M zu konstruieren. Sei also $a_1, \dots, a_n \in L$ eine K-Basis und $b_1, \dots, b_m \in M$ eine L-Basis, wobei nach Definition $n = [L : K]$ und $m = [M : L]$ gilt. Ich behaupte, daß die paarweisen Produkte $a_i b_j$ eine K-Basis von M bilden (und bin dann fertig, denn von ihnen gibt es $n \cdot m = [L : K] \cdot [M : L]$ Stück). Seien also $r_{ij} \in K$ mit

$$\sum_{i,j} r_{ij} a_i b_j = 0.$$

Durch Umsortieren der Summe erhalten wir

$$0 = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} r_{ij} a_i \right) b_j.$$

Die inneren Summen liegen alle in L, und da die b_j linear unabhängig über L sind, folgt $\sum_{i=1}^{n} r_{ij} a_i = 0$ für alle j. Aber da die a_i wiederum linear unabhängig über K sind, folgt damit $r_{ij} = 0$ für alle i und alle j, und das war zu beweisen.

Aufgabe 4.

i) Nach Aufgabe 3 genügt es, sich zu überlegen, daß die Erweiterungen $K \subset K(a)$ und $K(a) \subset K(a,b) = K(a)(b)$ beide endlich sind. Aber nach Vorlesung erzeugt ein einzelnes algebraisches Element stets eine endliche Erweiterung. Daß a algebraisch über K ist, steht in der Angabe; daß b algebraisch über $K(a)$ ist, ist sogar eine schwächere Aussage als die, daß b algebraisch über K ist.

ii) Natürlich sind $0, 1 \in L$ algebraisch über K (sogar ganz K ist algebraisch über K). Sind aber nun $a, b \in L$ algebraisch über K, so ist zu zeigen, daß $a + b, ab, a^{-1}, -a$ ebenfalls algebraisch über K sind. Aber diese Elemente liegen alle in $K(a,b)$, und das ist nach i) eine endliche Erweiterung von K, deren Elemente also nach Aufgabe 2 ii) alle algebraisch über K sind.

iii) Es sei $L_{\mathrm{alg}} \subset L$ die Menge der über K algebraischen Elemente; nach ii) ist L_{alg} ein Körper, der K enthält. Nach Voraussetzung gilt $S \subset L_{\mathrm{alg}}$, und nach Definition von $K(S)$ als kleinster Unterkörper, der K und S enthält, folgt $K(S) \subset L_{\mathrm{alg}}$, d.h. alle Elemente von $K(S)$ sind algebraisch über K.

Zusatzaufgabe. Schreiben wir $a := \sqrt{2} + \sqrt{3}$. Man muß sich erst einmal ein Polynom $F \in \mathbb{Q}[X]$ von möglichst kleinem Grad verschaffen mit $F(a) = 0$. Das geht auf mehrere Arten:

i) Mit roher Gewalt: Ausmultiplizieren liefert $a^2 = 5 + 2\sqrt{6}$, also $(a^2 - 5)^2 = 24$. Also ist a Nullstelle von $F = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1$.

ii) Mit linearer Algebra: Für ein verwandtes Problem gibt's ein fertiges Rezept aus den ersten paar Semestern, nämlich: ist $\varphi : V \to V$ ein linearer Endomorphismus eines endlichdimensionalen K-Vektorraumes, wie findet man dann ein nichttriviales Polynom, in das man φ einsetzen kann, um die Nullabbildung zu erhalten? Der Satz von Cayley-Hamilton sagt, daß man das charakteristische Polynom von φ nehmen kann.
Was hat das mit unserer Situation zu tun? Nun, a liegt in $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$, und das ist ein endlichdimensionaler K-Vektorraum. Nun ist die Abbildung $\varphi_a : L \to L$, $x \mapsto ax$, sicher $\mathbb{Q}$-linear, und für jedes Polynom $F \in \mathbb{Q}[X]$ gilt $F(\varphi_a) = \varphi_{F(a)}$. Insbesondere folgt aus $F(\varphi_a) = 0$ auch $\varphi_{F(a)} = 0$, also insbesondere $0 = \varphi_{F(a)}(1) = F(a)$. Man kann also für F einfach das charakteristische Polynom von φ_a nehmen.
Der Beweis der Gradformel zeigt (zusammen mit der Beobachtung $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$), daß $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine $\mathbb{Q}$-Basis von L ist. Die darstellende Matrix von φ_a bezüglich dieser Basis ist

$$\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

und als charakteristisches Polynom ergibt sich mit etwas Geduld dasselbe F wie in i).
Bemerkung: Dieses (in dieser Situation unnötig umständliche) Argument ist in der Theorie sehr wichtig, weil es – sieht man genau hin – gar keinen Grundkörper benötigt, sondern im Wesentlichen mit

einem Grund*ring* auskommt. Mehr darüber findet sich in Büchern über Kommutative Algebra unter dem Schlagwort „Ganze Ringerweiterungen".

Um zu zeigen, daß $F = X^4 - 10X^2 + 1$ tatsächlich das Minimalpolynom von a ist, genügt es, die Irreduzibliltät von F über $\mathbb{Q}$ zu beweisen. Zunächst hat F keine rationalen Nullstellen (substituiere dazu $Y = X^2$) und folglich keine Faktoren vom Grad 1 oder 3. Um Faktoren vom Grad 2 auszuschließen, machen wir den Ansatz

$$X^4 - 10X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a+c)X^3 + (ac+b+d)X^2 + (ad+bc)X + bd,$$

aus dem sich durch Koeffizientenvergleich ergibt:

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= -10 \\ ad + bc &= 0 \\ bd &= 1. \end{aligned}$$

Daraus bekommt man zunächst $c = -a$, und weiter $a(d - b) = 0$. Verschwindet der zweite Faktor, folgt wegen $bd = 1$ zwingend $b = d = \pm 1$, aber die zweite Gleichung liefert dann $\pm 2 = 10 + a^2$ im Widerspruch zu $a \in \mathbb{Q}$. Also muß $a = 0$ sein, und es folgt $bd = 1$, $b + d = -10$. Zusammen bedeutet das aber $b^2 + 10b + 1 = 0$, und das ist für $b \in \mathbb{Q}$ nicht möglich.
(Später, mit Galoistheorie, geht es leichter: Da kann man anderweitig begründen, daß das Minimalpolynom von a den Grad 4 haben muß, und wegen der Eindeutigkeit des Minimalpolynoms muß es damit unser F sein (das folglich irreduzibel ist).)