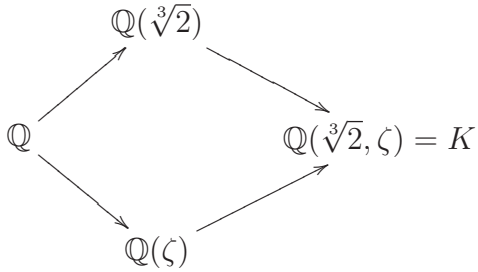
Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 9. Übungsblatt

Aufgabe 1.

i) Zunächst hat $\sqrt[3]{2}$ sicher das Minimalpolynom $X^3 - 2$ über $\mathbb{Q}$ (die Irreduzibilität sieht man etwa mit Eisenstein). Die dritte Einheitswurzel $\zeta := e^{\frac{2}{3}\pi i}$ ist Nullstelle von $X^3-1 = (X-1)(X^2+X+1)$, und wegen $\zeta \neq 1$ damit Nullstelle des (etwa durch Reduktion modulo 2 als irreduzibel zu enttarnenden) Polynoms $X^2 + X + 1$. Der Gesamtgrad von $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \zeta) = K$ ist dann nach dem Gradsatz entweder 6 oder 3, je nachdem, ob die zweite Erweiterung noch Grad 2 oder nur noch Grad 1 hat. Letzteres kann aber nicht sein, denn $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, aber $K = \mathbb{Q}(\sqrt[3]{2}, \zeta) \not\subset \mathbb{R}$.
Eine andere Art, das einzusehen, ist der folgende Trick: Im Diagramm von Inklusionen



haben die beiden linken Inklusionen Grad 3 bzw. 2, so daß der Gesamtgrad nach dem Gradsatz sowohl durch 3 als auch durch 2 teilbar sein muß. (Das geht allgemein, wenn man zwei Elemente von teilerfremdem Grad adjungiert.)

ii) Die Nullstellen von $X^3 - 2$ sind $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$. Diese liegen sicherlich alle in K; andererseits wird K wegen $\zeta = (\zeta\sqrt[3]{2})/\sqrt[3]{2}$ auch von ihnen erzeugt, d.h. K ist Zerfällungskörper des Polynoms.

iii) Das ist eine (sogar äquivalente) Umformulierung der Tatsache, daß $K/\mathbb{Q}$ (als Zerfällungskörper) normal ist: zunächst gilt nämlich $\varphi(K) \subset K$, denn jedes $a \in K$ mit Minimalpolynom f über $\mathbb{Q}$ wird durch φ auf eine Nullstelle von f abgebildet, aber die liegen alle in K. Aus $\varphi(K) \subset K$ folgt aber dann $\varphi(K) = K$, denn φ ist als Körperhomomorphismus injektiv, und injektive Endomorphismen eines endlichdimensionalen Vektorraums sind bijektiv.

Aufgabe 2. Eine Bemerkung vorweg: Es ist $\mathbb{Z}[\sqrt{-1}] \cong \mathbb{Z}[X]/(X^2 + 1)$. Damit kann man folgende Isomorphie zeigen:

$$K = \mathbb{Z}[\sqrt{-1}]/(7) \cong (\mathbb{Z}/7\mathbb{Z})[X]/(X^2 + 1).$$

Es ist also egal, ob man zuerst zu $\mathbb{Z}$ eine Wurzel aus -1 hinzufügt und danach 7 ausdividiert, oder ob man zuerst zum Körper $\mathbb{Z}/7\mathbb{Z}$ übergeht und dann eine Wurzel aus -1 hinzufügt. Das ist zwar nicht wirklich essentiell für die Lösung der Aufgabe, aber für die intuitive Vorstellung hilfreich.

i) Da $\mathbb{Z}[\sqrt{-1}]$ ein Hauptidealring ist, genügt es zu zeigen, daß 7 in diesem Ring irreduzibel ist. Eine nichttriviale Faktorisierung $7 = (a+bi)(c+di)$ liefert durch Bildung der Norm $49 = (a^2+b^2)(c^2+d^2)$, und wegen des Wörtchens „nichttrivial“ (d.h. keiner der Faktoren ist invertierbar) muß dann

$a^2 + b^2 = c^2 + d^2 = 7$ sein. Diese Gleichung hat aber keine ganzzahligen Lösungen, denn 7 ist keine Summe zweier Quadratzahlen.[1]

ii) Wegen $\overline{7} = \overline{0}$ in K (nach Konstruktion) ist der Primkörper K_0 isomorph zu $\mathbb{Z}/7\mathbb{Z}$.

iii) Spätestens jetzt sollte man sich überlegen, daß $K = (K_0)(a)$ ist, wobei $a = \overline{\sqrt{-1}}$ ist mit $a^2 + 1 = 0$, und dieses Polynom ist irreduzibel, da sonst -1 ein Quadrat in $\mathbb{Z}/7\mathbb{Z}$ wäre. Also ist $[K : K_0] = 2$.

iv) Ja, denn K ist sogar Zerfällungskörper von $X^2 + 1$ über K_0 (die Nullstellen sind a und $-a$).

Aufgabe 3.
i) $\Longrightarrow$ ii). Ist M/K separabel (d.h. jedes Element von M hat separables Minimalpolynom über K), so sicherlich („a fortiori") auch L/K. Etwas mehr argumentieren muß man für die Separabilität von M/L: Sei dazu $a \in M$ mit Minimalpolynomen f über K und g über L. Dann muß aber $g \mid f$ in $L[X]$ gelten (denn $f \in L[X]$ mit $f(a) = 0$), und nach Voraussetzung hat f nur einfache Nullstellen. Damit hat aber auch g nur einfache Nullstellen, d.h. a ist separabel über L. (Allgemeiner haben wir gezeigt: Ist ein Element separabel über K, so auch über jedem größeren Körper. Das werden wir im Folgenden auch öfters implizit verwenden.)
ii) $\Longrightarrow$ i). Ganz allgemein gilt: Ist $K \subset L = K(a_1, \ldots, a_n)$ algebraisch, und ist jedes a_i separabel über $K(a_1, \ldots, a_{i-1})$, so ist $K \subset L$ separabel. Das wurde in der Vorlesung zwar nicht formuliert, aber bewiesen, nämlich als Folgerung (i) zu Satz III.4.5. (Dort wird zwar verlangt, daß jedes a_i separabel über K sei, aber nur, um sofort daraus zu folgern, daß es insbesondere separabel über $K(a_1, \ldots, a_{i-1})$ ist).
Seien nun L/K und M/L separabel und $a \in M$ beliebig. Dann hat a separables Minimalpolynom f über L; seien $a_1, \ldots, a_n \in L$ dessen Koeffizienten. Dann ist a auch separabel über $K(a_1, \ldots, a_n)$ (denn das Minimalpolynom ist auch hier f), und nach dem oben Gesagten ist damit die Erweiterung $K \subset K(a_1, \ldots, a_n, a)$ separabel, d.h. a ist separabel über K.

Aufgabe 4. Es sei L ein Körper, über dem f zerfällt (beispielsweise ein Zerfällungskörper von f). Dann kann man $f = \prod_{i=1}^{n}(X - a_i)$ mit $a_i \in L$ schreiben, und damit gibt es zu jedem i genau einen K-Homomorphismus $\varphi_i : K(a) \to L$ mit $\varphi_i(a) = a_i$: denn es ist $K(a) \cong K[X]/(f)$, und der eindeutig bestimmte Homomorphismus $K[X] \to L$ mit $X \mapsto a_i$ faktorisiert über $K[X]/(f)$, da $f(a_i) = 0$ ist. – Das zeigt die Behauptung, und da f separabel ist, sind die a_i und damit auch die φ_i sogar paarweise verschieden.

Aufgabe 5. Es sei $F : L \to L$ der Frobeniushomomorphismus $x \mapsto x^p$.

i) Für jedes n ist $K^{p^{-n}} := \{x \in L \mid x^{p^n} \in K\} = (F^n)^{-1}(K) \supset K$ ein Unterkörper (als Urbild eines Unterkörpers unter einem Körperhomomorphismus), und $K^{p^{-\infty}} = \bigcup_{n \geqslant 1} K^{p^{-n}}$ ist die Verinigung einer aufsteigenden (!) Kette von Unterkörpern, also wieder ein Unterkörper. – Natürlich kann man auch einfach zu Fuß (unter Verwendung von F) nachrechnen, daß $K^{p^{-\infty}}$ abgeschlossen unter den Körperoperationen ist und K enthält.

ii) Es sei $a \in L$; wir müssen zeigen, daß a separabel über $K^{p^{-\infty}}$ ist. Sei dazu f das Minimalpolynom von a über K. Dann kann man f schreiben als $f(X) = f_0(X^q)$ mit $q = p^\ell$ für ein $\ell \geqslant 0$, wobei f_0 irreduzibel *und separabel* ist. Da L/K normal ist, zerfällt f über L; es seien also $a_1, \ldots, a_r \in L$ die *verschiedenen* Nullstellen von f (von mir aus $a_1 = a$). Dann sind die a_i^q die (verschiedenen, denn der Frobenius ist injektiv) Nullstellen von f_0, also $f_0 = \prod_{i=1}^{r}(X - a_i^q)$ und damit $f = \prod_{i=1}^{r}(X^q - a_i^q) =$

[1] Nach unserer Bemerkung oben hätten wir auch genausogut zeigen können, daß -1 kein Quadrat im Körper $\mathbb{Z}/7\mathbb{Z}$ ist. Ganz allgemein ergibt sich mit dieser Überlegung: eine Primzahl p ist genau dann Summe zweier Quadratzahlen, wenn -1 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Nun kann man sich relativ leicht überlegen, daß (für eine ungerade Primzahl p) -1 genau dann ein Quadrat modulo p ist, wenn $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ gilt, wenn also $(p-1)/2$ eine *gerade* Zahl ist. Damit haben wir schon fast den folgenden berühmten Satz aus der Zahlentheorie bewiesen: Eine ungerade Primzahl p ist genau dann Summe zweier Quadrate, wenn $p - 1$ durch vier teilbar ist.

g^q mit $g = \prod_{i=1}^{r}(X - a_i)$. Nun ist aber $a = a_1$ nach Konstruktion eine Nullstelle von g, aber die Koeffizienten von g liegen in $K^{p^{-\infty}}$, denn ihre q-ten Potenzen sind die Koeffizienten von f und liegen damit in K. Also ist a Nullstelle des *separablen* Polynoms g über $K^{p^{-\infty}}$, und das zeigt die Behauptung.

Aufgabe 6. Wir zeigen zunächst allgemeiner: Ist K ein Körper der Charakteristik $p > 0$, und ist $a \in K$ keine p-te Potenz, so ist $f = X^p - a \in K[X]$ inseparabel und irreduzibel. Die Inseparabilität folgt aus $f' = 0$. Für die Irreduzibilität sei $g \in K[X]$ ein (normierter) Faktor von f. In einem Zerfällungskörper K' von f besitzt f eine Nullstelle b, also $b^p = a$, und damit gilt $f = X^p - b^p = (X - b)^p$. Also muß $g = (X - b)^d$ mit $0 \leqslant d \leqslant p$ gelten. Jetzt kann man auf vielerlei Arten argumentieren, etwa so:

i) Der zweithöchste Koeffizient von g ist (bis aufs Vorzeichen) $d \cdot b \in K$; wegen $b \notin K$ nach Voraussetzung muß dann $d \cdot 1_K = 0$ sein, also $p \mid d$.
ii) Der konstante Koeffizient von g ist (bis aufs Vorzeichen) $b^d \in K$. Wegen $b^p = a \in K$ gilt für die Untergruppe $U := \{n \in \mathbb{Z} \mid b^n \in K\}$ von $\mathbb{Z}$ dann $d \in U$, $p \in U$, $1 \notin U$. Nach der Klassifikation der Untergruppen von $\mathbb{Z}$ können dann aber p und d nicht teilerfremd sein, also folgt $p \mid d$.

Jedenfalls ergibt sich $d = 0$ oder $d = p$, und das heißt, daß f irreduzibel ist.
Jetzt können wir die beiden Teilaufgaben bequem lösen:

i) Nach dem schon Bewiesenen ist nur zu zeigen, daß T keine p-te Potenz in $K(T)$ ist. Andernfalls wäre aber $T = (r/s)^p$ mit gewissen $r, s \in K[T]$, also $s^p T = r^p$, aber die rechte Seite hat durch p teilbaren Grad, die linke Seite nicht – Widerspruch.
ii) „Nur dann“. Ist K vollkommen, so ist jedes irreduzible Polynom über K separabel (denn jedes irreduzible Polynom tritt als Minimalpolynom eines geeigneten Elementes eines geeigneten Erweiterungskörpers auf). Nach dem oben allgemein Bewiesenen muß dann aber jedes $a \in K$ eine p-te Potenz sein (sonst wäre ja $X^p - a$ inseparabel und irreduzibel), also ist der Frobenius surjektiv.
„Immer dann“: Es sei $f \in K[X]$ ein irreduzibles Polynom; wir müssen zeigen, daß f separabel ist. Schreibe aber $f(X) = f_0(X^q)$ mit $q = p^\ell$ und f_0 separabel. Ist $f_0 = \sum_{i=0}^{d} a_i X^i$, so bedeutet das $f = \sum_{i=0}^{d} a_i X^{qi} = \sum_{i=0}^{d} (b_i X^i)^q = (\sum_{i=0}^{d} b_i X^i)^q$, wobei die $b_i \in K$ sind mit $b_i^q = a_i$ – solche gibt es, da der Frobenius surjektiv ist. Also ist f eine q-te Potenz in $K[X]$, aber da f ja irreduzibel ist, folgt $q = 1$, d.h. $f = f_0$, und f ist separabel.