LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Sommersemester 2019
8. Juli 2019

Höhere Algebra – Lösungsskizzen zu Übungsblatt 9

Aufgabe 1 (6 Punkte).
Sei $S_\mathfrak{p}(0) := \ker(A \to A_\mathfrak{p})$.

a) Wir wollen zeigen, dass gilt $S_\mathfrak{p}(0) \subseteq \mathfrak{p}$. Dazu sehen wir zuerst, dass $a \in S_\mathfrak{p}(0)$ gilt, genau dann wenn $ua = 0$ für ein $u \in A \setminus \mathfrak{p}$ gilt. Sei nun $a \in S_\mathfrak{p}(0)$. Mit der obigen Äquivalenz gilt, also $ua \in \mathfrak{p}$ und somit $a \in \mathfrak{p}$, was zu zeigen war.

b) Wir zeigen zuerst $\sqrt{S_\mathfrak{p}(0)} = \mathfrak{p} \Rightarrow \mathfrak{p}$ ist minimales Primideal. Angenommen es gibt ein Primideal $\mathfrak{p}_1 \subsetneq \mathfrak{p}$. Sei $a \in \mathfrak{p} \setminus \mathfrak{p}_1$. Dann folgt $a^n \in S_\mathfrak{p}(0)$ für ein $n \in \mathbb{N}$ und somit auch $ua^n = 0$ für ein $u \in A \setminus \mathfrak{p}$. Daraus folgt wiederum, dass $ua^n \in \mathfrak{p}_1$ und wegen $a^n \notin \mathfrak{p}_1$ folgt $u \in \mathfrak{p}_1 \subset \mathfrak{p}$, was ein Widerspruch zur Annahme ist. Also ist $\mathfrak{p}$ ein minimales Primideal.
Nun wollen wir zeigen, dass aus '$\mathfrak{p}$ minimales Primideal' folgt, dass $\sqrt{S_\mathfrak{p}(0)} = \mathfrak{p}$ gilt. Wir wenden nun einen Satz aus der Vorlesung auf $M' = 0$ und $M = A$ an, was möglich ist, da wir A als noethersch vorausgesetzt haben. Sei also

$$(0) = \bigcap_{i=1}^{n} \mathfrak{q}_i,\ \sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$$

eine minimale Zerlegung. Da $\mathfrak{p}$ minimal ist, gibt es ein $\mathfrak{q}_i$ mit $\mathfrak{p} = \mathfrak{p}_i$. Satz 6.2.5 besagt jetzt: $\mathfrak{q}_i = \ker(A \to A_\mathfrak{p}) = S_\mathfrak{p}(0)$. Also $\sqrt{S_\mathfrak{p}(0)} = \mathfrak{p}$.

c) Sei $\mathfrak{p} \supseteq \mathfrak{p}'$. Wir wollen zeigen: $S_\mathfrak{p}(0) \subseteq S_{\mathfrak{p}'}(0)$. Es gilt $\mathfrak{p} \supseteq \mathfrak{p}' \Leftrightarrow A \setminus \mathfrak{p} \subseteq A \setminus \mathfrak{p}'$. Wir sehen ein:

$$\begin{aligned} A \to A_\mathfrak{p} \to A_{\mathfrak{p}'},\\ a \mapsto \frac{a}{1};\ \frac{a}{u} \mapsto \frac{a}{u} \end{aligned}$$

ist dieselbe Abbildung wie $A \to A_{\mathfrak{p}'}, a \mapsto \frac{a}{1}$.
Also ist $S_\mathfrak{p}(0) = \ker(A \to A_\mathfrak{p}) \subseteq \ker(A \to A_{\mathfrak{p}'}) = S_{\mathfrak{p}'}(0)$, was zu zeigen war.

Aufgabe 2 (6 Punkte).
i)⇒ii): Da b ganz über A ist gibt es eine Gleichung der Form $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, $a_i \in A$. Ist $k \geq 0$, so folgt $b^{n+k} = -(a_1 b^{n+k-1} + \cdots + a_n b^k)$ und Induktion liefert, dass alle Potenzen von b in dem von $\{1, b, b^2, \ldots, b^{n-1}\}$ erzeugten A-Untermodul von $A[b]$ liegen, d.h. der A-Modul $A[b]$ wird von $\{1, b, \ldots, b^{n-1}\}$ erzeugt.

ii)⇒ iii): Setze $C = A[b]$. Offensichtlich ist C ein Ring mit $A \subseteq A[b] \subseteq B$; nach Annahme ist $A[b]$ ein endlicher erzeugter A-Modul.

iii)⇒ iv): Setze $M = C$; M ist offensichtlich ein $A[b]$-Modul und nach Annahme endlich

erzeugter A-Modul. Sei $a' \in A[b]$ mit $a' \cdot C = 0$. Dann ist insbesondere $a' \cdot 1 = 0$, also $a' = 0$ und damit $\mathrm{Ann}_{A[b]}(M) = 0$.

iv)$\Rightarrow$ i): Ist M der $A[b]$-Modul mit den Eigenschaften aus iv), so betrachte die Abbildung $\phi : M \to M,\ m \mapsto bm$. Da M ein $A[b]$-Modul ist, gilt $bM \subseteq M$. Nach Cayley-Hamilton (angewandt mit Ideal A) gibt es ein normiertes Polynom $p(X) \in A[X]$ mit $p(\phi) = 0$, sodass $p(b)M = 0$. Wegen $\mathrm{Ann}_{A[b]}(M) = 0$ folgt $p(b) = 0$, d.h. b ist ganz über A.

Aufgabe 3 (4 Punkte).

a) Sei $d \in D$. Da $B \subseteq D$ ganz ist, gibt es eine Gleichung der Form $d^n + b_1 d^{n-1} + \cdots + b_n = 0,\ b_i \in B$. Da $A \subseteq B$ ganz ist, ist mit (Aufgabe 2 + Induktion) $B' = A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul. Weiter ist d ganz über B', so dass nach Aufgabe 2 $B'[d]$ ein endlich erzeugter B'-Modul ist. Also ist $B'[d]$ ein endlich erzeugter A-Modul, und wegen $A[d] \subseteq B'[d]$ ist nach Aufgabe 1, iii) d ganz über A.

b) Ist $b \in B$ ganz über C, so ist nach a) b ganz über A, also $b \in C$.

Aufgabe 4 (6 Punkte).

a) Sei $\alpha \in \mathcal{O}_K$, d.h. es existiert ein $f(x) \in \mathbb{Z}[x]$ normiert mit $f(\alpha) = 0$. Sei außerdem $g(x) \in \mathbb{Q}[x]$ das Minimalpolynom von α. Dann gilt $g(x) \mid f(x)$. Aus der Algebra wissen wir aber, dass für ein normiertes $f(x) \in \mathbb{Z}[x]$ gilt: Ist $f(x) = g(x)h(x)$ mit $g(x), h(x) \in \mathbb{Q}[x]$ normiert, dann gilt schon $g(x), h(x) \in \mathbb{Z}[x]$. Daraus folgt sofort die Behauptung.
Die Rückrichtung folgt direkt aus den Definitionen.

b) Zur Vereinfachung der Notation definieren wir $\mathcal{O}_d := \mathcal{O}_{\mathbb{Q}(\sqrt{d}),\mathbb{Z}}$. Da d quadratfrei ist, ist ganz offensichtlich $\sqrt{d} \notin \mathbb{Q}$; gleichzeitig ist $T^2 - d \in \mathbb{Q}[T]$ ein Polynom mit Nullstelle $\sqrt{d}$. Damit ist $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ galoissch vom Grad 2 mit nicht-trivialem Automorphismus σ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Ist $a = \alpha + \beta\sqrt{d} \in \mathcal{O}_d$, so ist auch $\sigma(a)$ ganz über $\mathbb{Z}$, und damit sind die Koeffizienten des Minimalpolynoms $\mu_a = (T - a)(T - \sigma(a))$ gleichzeitig rational und ganz über $\mathbb{Z}$, also ganze Zahlen. Konkret ist $\mu_a = T^2 - 2\alpha T + \alpha^2 - n\beta^2$, und damit müssen $A := 2\alpha$ und $\alpha^2 - d\beta^2$ ganze Zahlen sein. Insbesondere ist dann mit $B := 2\beta$ auch dB^2 eine ganze Zahl. Schreibt man nun 2β als vollständig gekürzten Bruch $\frac{r}{s}$, so $d\frac{r^2}{s^2} = k$, also $dr^2 = ks^2$ für ein $k \in \mathbb{Z}$; ist nun p ein Primfaktor von s, so teilt das Quadrat p^2 das Produkt dr^2. $\frac{r}{s}$ ist aber vollständig gekürzt, also teilt p^2 den Faktor d. Aus der Quadratfreiheit von d folgt nun, dass s keine solchen Primfaktoren enthalten kann, es gilt also $B \in \mathbb{Z}$. Aber damit $\alpha^2 - d\beta^2 = \frac{1}{4}(A^2 - dB^2)$ eine ganze Zahl sein kann, muss $A^2 \equiv dB^2 \mod (4)$ gelten.

Die einzigen Quadrate modulo 4 sind aber 0 und 1. Aus der Quadratfreiheit von d folgt offensichtlich $d \not\equiv 0 \mod (4)$ und es gilt zwei Fälle zu unterscheiden: Ist $d \equiv 2, 3$, so muss $B^2 \equiv 0$ sein, also auch $A^2 \equiv 0$, und damit sind A, B gerade und α, β ganze Zahlen, d.h. $a \in \mathbb{Z}[\sqrt{d}]$.

Im Fall $d \equiv 1$ folgt $A^2 \equiv B^2$, was bedeutet, dass A und B entweder beide gerade oder beide ungerade sind.

In beiden Fällen ist also $\mathcal{O}_d \subseteq A_d$ mit

$$A_d := \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d \equiv 1 \bmod 4. \end{cases}$$

Zeigen wir nun $\mathcal{O}_d \supseteq A_d$. Das ist im Fall $d \equiv 2,3$ einfach, denn $\sqrt{d}$ ist ganz über $\mathbb{Z}$ mit Ganzheitsgleichung $T^2 - d$. Im Fall $d \equiv 1$ sehen wir zuerst ein, dass $(1+\sqrt{d})/2$ offensichtlich Nullstelle des Polynoms $(2T-1)^2 - d$, aber dieses nicht normiert ist. Normieren wir es mit Gewalt, so erhalten wir das Polynom

$$\frac{1}{4}[(2T-1)^2 - d] = T^2 - T + \frac{1-d}{4},$$

und dieses hat tatsächlich ganzzahlige Koeffizienten!