LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT
Prof. Dr. Werner Bley
Sommersemester 2018

Algebraische Zahlentheorie
Lösungsvorschläge zu Übungsblatt 1

Aufgabe 1
Sei $\alpha := \frac{3+2\sqrt{6}}{1-\sqrt{6}}$ und $K := \mathbb{Q}(\sqrt{6})$. Dann gilt: $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -6$ und $\mathrm{N}_{L/K}(\alpha) = 3$. Also ist α eine ganze Zahl in K. Das Minimalpolynom ist gegeben durch $x^2 + 6x + 3$.

Aufgabe 2
Sei $K := \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z} \setminus \{0, 1\}$, quadratfrei.
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 $a = \alpha + \beta\sqrt{d} \in \mathcal{O}_K$, 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 $\mu_a = T^2 - 2\alpha T + \alpha^2 - d\beta^2$, 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 $\mathcal{O}_K \subseteq A_d$ 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 $\mathcal{O}_K \supseteq A_d$. 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!

Aufgabe 3
Unter Verwendung von $u \in \mathcal{O}_K^\times \iff N(u) = 1$ findet man

$$\begin{cases} \{\pm 1\}, & \text{falls } d \neq -1, -3, \\ \{\pm 1, \pm\sqrt{-1}\}, & \text{falls } d = -1, \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}, & \text{falls } d = -3. \end{cases}$$

Aufgabe 4
(a) Sei $K = \mathrm{Quot}(B)$ und Z der Zerfällungskörper von $fg \in K[t]$. Es gibt somit Elemente α_i und $\beta_j \in Z$, sodass

$$fg = \prod_i (t - \alpha_i) \prod_j (t - \beta_i),$$

und die α_i bzw. β_j sind die Nullstellen von f bzw. g in Z. Da diese Elemente insbesondere Nullstellen des normierten Polynoms $fg \in C[t]$ sind, sind sie ganz über C in Z, und da C ganz über A ist, sind sie ganz über A. Da Summen und Produkte von ganzen Elementen ganz sind, sind alle Koeffizienten von f und g ganz über A. Wegen $f, g \in B[t]$ liegen die Koeffizienten aber in B und somit im ganzen Abschluss von A in B, ðin C. Dies ist aber genau die Behauptung.
(b) Wir bezeichnen den ganzen Abschluss von $A[t]$ in $B[t]$ mit D und wollen somit die Gleichheit $D = C[t]$ zeigen. Da C und t ganz über $A[t]$ sind, folgt $D \supseteq C[t]$. Für die umgekehrte Inklusion sei $f \in B[t]$ ganz über $A[t]$, d.h. es existieren Polynome $g_i \in A[t]$, sodass

$$f^m + g_1 f^{m-1} + \cdots + g_m = 0.$$

Wähle nun $r \in \mathbb{N}$ größer als m und als das Maximum der Grade der g_i, und setze $f_1 = f - t^r \in B[t]$. Aufgrund der Wahl von r ist $-f_1$ normiert. Ersetzen wir f durch $f_1 + t^r$ in der Ganzheitsgleichung oben, erhalten wir

$$(f_1 + t^r)^m + g_1 (f_1 + t^r)^{m-1} + \cdots + g_m = 0$$

und mit geeigneter Wahl von Polynomen $h_i \in B[t]$ gilt

$$f_1^m + h_1 f_1^{m-1} + \cdots + h_m = 0.$$

Insbesondere ergibt sich sich $h_m = (t^r)^m + g_1 \cdot (t_r)^{m-1} + \cdots + g_m \in A[t]$, und h_m ist normiert. Umstellen liefert

$$h_m = -f_1 \cdot \left(f_1^{m-1} + h_1 \cdot f_1^{m-2} + \cdots + h_{m-1} \right).$$

Da h_m und $-f_1$ wie bereits bemerkt normiert sind, ist Teilaufgabe (a) auf dieses Produkt anwendbar und wir erhalten $f \in C[t]$. Da $f \in D$ beliebig gewählt wurde, folgt $D \subseteq C[t]$.
(c) Es gilt $\mathrm{Quot}(A[t]) = K(t)$. Nach Teilaufgabe (b) ist $A[t]$ ganz abgeschlossen in $K[t]$, und $K[t]$ ist als faktorieller Ring wiederum abgeschlossen in seinem Quotientenkörper $K(t)$. Somit ist auch $A[t]$ ganz abgeschlossen in $K(t)$.

Aufgabe 5
Falls b ganz über A ist, so ist der Modul $M := A[b]$ endlich erzeugt. Genauer: $1, b, \ldots, b^{n-1}$ erzeugen M, falls b einer Ganzheitsgleichung $f \in A[X], f$ normiert, vom Grad n genügt.
Sei umgekehrt $m_1, \ldots, m_s$ ein A-Erzeugendensystem von M. Dann gilt wegen $bM \subseteq M$

$$b(m_1, \ldots, m_s)^t = T(m_1, \ldots, m_s)^t$$

mit einer Matrix $T \in M_s(A)$. Also gilt:

$$(bE - T)(m_1, \ldots, m_s)^t = 0. \tag{1}$$

Für eine beliebige Matrix $S \in M_s(A)$ bezeichne A' die adjungierte Matrix. Es gilt dann: $AA' = A'A = \det(A)E$.
Wir multiplizieren (1) mit der adjugierten Matrix von $(bE - T)$ und erhalten

$$\det(bE - T)(m_1, \ldots, m_s)^t = (bE - T)'(bE - T)(m_1, \ldots, m_s)^t = (0 \ldots 0)^t.$$

Also annulliert $\det(bE - T)$ den Modul M. Aufgrund der zweiten Voraussetzung ist also $\det(bE - T) = 0$ bzw. b ist Nullstelle des normierten Polynoms $\det(XE - T)$. Also ist b ganz über A.