Friedrich-Schiller-Universität Jena
Mathematisches Institut
M.Sc.Mikael Johansson

Übungen zu Algebra 2

Sommersemester 2006 Lösungen zu Übungsblatt 5

Eine ganze algebraische Zahl ist eine algebraische Zahl, die über $\mathbb{Z}$ ganz ist.

Aufgabe 1: (2 P.) Seien S_1, S_2 zwei kommutative Erweiterungsringe des Rings R, und sei $f\colon S_1 \to S_2$ ein Homomorphismus von R-Algebren. Zeigen Sie: ist $\alpha \in S_1$ ganz über R, dann ist auch $f(\alpha)$ ganz über R.

Lösung: α ganz über R heißt es gibt ein Polynom $\tau = X^r + \sum_i a_i X^i \in R[X]$ mit $\tau(\alpha) = 0$. Dann aber ist

$$\begin{aligned}\tau(f(\alpha)) &= f(\alpha)^r + \sum_i a_i f(\alpha)^i \\ &= f(\alpha^r) + \sum_i f(a_i \alpha^i) \\ &= f(\alpha^r + \sum_i a_i \alpha^i) = f(0) = 0\end{aligned}$$

und daher ist τ auch ein entsprechendes Polynom für $f(\alpha)$. Daher ist auch $f(\alpha)$ ganz über R.

* * *

Aufgabe 2: (4 P.) Sei $A \in M_n(\mathbb{C})$ eine Matrix mit $A^m = E_n$ für ein $m \geq 1$. Zeigen Sie, dass A diagonalisierbar ist. Zeigen Sie ferner, dass die Determinante und sogar die Spur von A ganze algebraische Zahlen sind.

Lösung: Da $A^m = E_n$ ist $A^m - 1 = 0$, und so erfüllt A die Gleichung $X^m - 1 = 0$. Daher teilt das minimalpolynom $m_A | X^m - 1$. Da dieses keine wiederholte Wurzel besitzt, gilt das auch für m_A. Daher ist jedes Block im Jordansche Normalform der größe 1×1, also ist die Jordansche Normalform diagonal.

Da $1 = \det E_n = \det A^m = (\det A)^m$ ist $\det A$ ein Wurzel von $X^m - 1$, und daher ist $\det A$ ganz. Auf die Diagonale vom Diagonalisierung von A liegen die Eigenwerte, die alle m:te Einheitswurzeln sein mussen. Nun ist ein Einheitswurzel ganz über $\mathbb{Z}$ und die Summe ganze Zahlen ist auch ganz. Daher ist $\mathrm{Spur}(A) = \mathrm{Spur}(D(A)) = \sum \lambda_i$.

* * *

Aufgabe 3:

a) (2 P.) Zeigen Sie: ist $a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ eine ganze algebraische Zahl, so liegt das Polynom $X^2 - 2aX + (a^2 - nb^2)$ in $\mathbb{Z}[X]$.

Lösung: Ist $x = a + b\sqrt{n}$ ganz, dann können wir das Minimalpolynom finden in dem wir aus diese Gleichung eine Polynomgleichung in x und ohne vorkommen von Quadratwurzel herleiten:

$$\begin{aligned} x &= a + b\sqrt{n} \\ x - a &= b\sqrt{n} \\ (x-a)^2 &= b^2 n \\ x^2 - 2ax + a^2 - b^2 n &= 0 \end{aligned}$$

Nun sind, damit dieses Polynom auch ein ganzes Zahl bestimmt, alle Koeffizienten aus $\mathbb{Z}$, das heißt die Bedingung aus der Aufgabenstellung.

* * *

b) (2 P.) Bestimmen Sie die ganzen algebraischen Zahlen in $\mathbb{Q}(\sqrt{7})$.

Lösung: Für ein ganzes algebraisches Zahl $a+b\sqrt{7}$ in $\mathbb{Q}(\sqrt{7})$ gilt dass $-2a, a^2-7b^2 \in \mathbb{Z}$. Ist $-2a \in \mathbb{Z}$, dann ist entweder $a \in \mathbb{Z}$ oder $a - \frac{1}{2} \in \mathbb{Z}$. Ist $a - \frac{1}{2} \in \mathbb{Z}$, dann ist $2a = 1 \pmod 2$. Lass daher $\hat{a} = 2a$. Dann ist $a^2 - 7b^2 = \frac{\hat{a}^2}{4} - 7b^2$. Sei nun $\hat{b} = 2b$, so dass $a^2 - 7b^2 = \frac{\hat{a}^2 - 7\hat{b}^2}{4}$. Dann ist $a^2 - 7b^2 \in \mathbb{Z}$ äquivalent dazu, dass $\hat{a}^2 - 7\hat{b}^2 = 0 \pmod 4$. Nun ist aber $\hat{a} = 1 \pmod 2$, und daher ist $\hat{a}^2 = 1 \pmod 4$, und $7 = -1 \pmod 4$. Also muss $b^2 = -1 \pmod 4$, damit $\hat{a}^2 - 7\hat{b}^2 = 1 + \hat{b}^2 = 0 \pmod 4$. Die Quadrate mod 4, aber, sind genau 0 und 1. Also können wir keine solche $\hat{b}$ finden, und daher sind die ganze algebraische Zahlen in $\mathbb{Q}(\sqrt{7})$ genau $\mathbb{Z}[\sqrt{7}]$.

* * *

c) (2 P.) Bestimmen Sie die ganzen algebraischen Zahlen in $\mathbb{Q}(\sqrt{5})$.

Lösung: Ähnlich wie für $\mathbb{Q}(\sqrt{7})$ können wir feststellen, dass für ein ganzes $a+b\sqrt{5} \notin \mathbb{Z}[\sqrt{5}]$ muss $1 - 5\hat{b}^2 = 0 \pmod 4$. Jedoch ist nun $5 = 1 \pmod 4$, und daher muss $\hat{b}^2 = 1 \pmod 4$. Dies ist einfach lösbar, dadurch dass $\hat{b} = 1 \pmod 2$ gesetzt wird. Daher sind die ganze algebraische Zahlen in $\mathbb{Q}(\sqrt{5})$ genau $\mathbb{Z}[\sqrt{5}] + \mathbb{Z}\frac{1+\sqrt{5}}{2}$.

* * *

Aufgabe 4: Sei G eine endliche Gruppe, und sei R das Zentrum der Gruppenalgebra $\mathbb{C}G$. Für $g \in G$ bezeichnen wir mit c_g das Element aus $\mathbb{C}G$, das die Summe aller Elemente der Konjugationsklasse von g ist. Das heißt,

$$c_g = \sum \{g' \in G \mid \exists h \in G \; g' = hgh^{-1}\}\,.$$

a) (2 P.) Jedes c_g liegt in R, und die Elemente c_g stellen sogar eine Basis des $\mathbb{C}$-Vektorraums R dar.

Lösung: Ist $a = \sum_{g \in G} \lambda_g g \in R$, dann ist $hah^{-1} = a$ für alle $h \in G$. Das passiert genau dann, wenn für alle g' in die Konjugationsklasse von g: $\lambda_{g'} = \lambda_g$, denn sonst könnten wir h so wählen, dass $hgh^{-1} = g'$ ist, und dann wäre durch ein Koeffizientenvergleich $\lambda_{g'} \neq \lambda_g$ die gebrauchte Widerspruch zu $hah^{-1} = a$. Daher können wir $a = \sum_g \lambda_g \sum_h h$ schreiben, mit g die Repräsentanten der Konjugationsklassen und h die Mitglieder der jeweiligen Konjugationsklasse. Von dieses Ausdruck ist es klar, dass die $c_g = \sum_h h$ eine Basis für R aufbaut.

*　　*　　*

b) (2 P.) Für $h_1, h_2 \in G$ ist $c_{h_1} c_{h_2}$ eine $\mathbb{Z}$-lineare Kombination von den Elementen c_g.

Lösung: Produkte zentrale Elemente sind auch zentral, und daher sind sie $\mathbb{C}$-lineare Kombinationen der c_gs. Die Koeffizient von c_g ist dabei genau die Koeffizient von g in $c_{h_1} c_{h_2}$; dies wiederum ist genau die Anzahl von Paare (k_1, k_2) solche dass k_i in die Konjugationsklasse von h_i liegt, und $k_1 k_2 = g$. Dieses Anzahl ist offensichtlich ein ganzes Zahl.

*　　*　　*

c) Jedes c_g ist ganz über $\mathbb{Z}$.

Lösung: Die Teilmodul $\mathbb{Z}[c_g]_{g \in G}$ ist endlich als $\mathbb{Z}$-Algebra, da die c_g laut b eine Modulbasis ausmachen. Daher ist jedes Element in dieser Teilmodul ganz über $\mathbb{Z}$.

*　　*　　*

Aufgabe 5: Sei R ein noetherscher Ring. Zeigen Sie, dass der Potenzreihen-Ring $R[[X]]$ auch noethersch ist. *Hinweis*: Der Grad einer Potenzreihe $\sum_{n \geq 0} a_n X^n$ ist $\min\{n \mid a_n \neq 0\}$. Versucht man den Beweis des Basissatzes entsprechend anzupassen, so hört die Rekursion nie auf. Warum ist das aber kein Problem?

Lösung: Sei $0 \neq I \trianglelefteq R[\![X]\!]$. Für ein $f = \sum_i a_i x^i \in R[\![X]\!]$ setzen wir $\operatorname{grad} f = \min\{i : a_i \neq 0\}$, und $\mathrm{LC}(f) = a_{\operatorname{grad} f}$.

$\mathrm{LC}(I)$ ist ein Ideal in R, denn für $a, b \in \mathrm{LC}(I)$ gibt es $f, g \in R[\![X]\!]$ mit $a = \mathrm{LC}(f)$ und $b = \mathrm{LC}(g)$. Daher ist $a + b = \mathrm{LC}(f + g)$ für $a \neq -b$. Für den Fall $a = -b$ können wir feststellen dass $0 = \mathrm{LC}(0)$, und daher ist auch $a - a \in \mathrm{LC}(I)$. Weiterhin ist $ra = \mathrm{LC}(rf)$, und so ist $ra \in \mathrm{LC}(I)$.

Da nun R noethersch ist, ist $LC(I) = \langle LC(f_i) \rangle_{i=1}^m$ für irgendwelche f_i. Wir nehmen ein N mit $N \geq \operatorname{grad} f_i$ für alle f_i. Dann gilt für alle f mit $\operatorname{grad} f \geq N$: $f = \sum_i \alpha_i f_i$.

Für jedes $j \in [N]$ lassen wir nun $L_j = \mathrm{LC}(f : \operatorname{grad} f \leq j)$. Dies ist auch ein Ideal für jedes j, und so gibt es $f_{ij} \in I$ deren führende Koeffizienten L_j erzeugen.

Nun können wir für ein f sukzessiv die führende Koeffizient vernichten mit Kombinationen der f_{ij} bis dahin, das die Grad von f N übersteigt. In diese Prozess werden wir letztendlich unendlich viele von den f_i, f_{ij} benutzen – jedoch wird in jeder Grad nur eine endliche Kombination benutzt, und so wird die gesamte benutzte Glieder eine Potenzreihe ausmachen. Daher liegt die benutzte Vernichtungen in $R[\![X]\!]$ bleiben.

*　　*　　*