LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2018/19
7. Januar 2019

# Algebra – Lösungsskizzen zu Übungsblatt 7

**Aufgabe 1 (8 Punkte).**

a) Es gilt offensichtlich $0 \in T_p(M)$. Für $m_1, m_2 \in T_p(M)$ existieren $n_1, n_2 \in \mathbb{N}_0$ mit $p^{n_1}m_1 = 0$ und $p^{n_2}m_2 = 0$ und somit gilt $p^{n_1+n_2}(m_1 - m_2) = 0$, also $m_1 - m_2 \in T_p(M)$. Folglich ist $T_p(M)$ eine Untergruppe von $M$.

b) Da $\mathbb{Z}$ selbst torsionsfrei ist und verschiedene Primzahlen natürlich teilerfremd sind, folgt aus dem Isomorphismus aus der Angabe sofort die Behauptung.

c) Da $\mathbb{F}_p := \mathbb{Z}\,/\,p\,\mathbb{Z}$, ist $T/pT$ ein $\mathbb{F}_p$-Vektorraum und es gilt $\dim_{\mathbb{F}_p}(T/pT)$ ist gleich der Anzahl der $e_i > 0$. Als nächstes betrachten wir den $\mathbb{F}_p$-Vektorraum $pT/p^2T$ und sehen ein, dass gilt: $\dim_{\mathbb{F}_p}(pT/p^2T)$ ist gleich der Anzahl der $e_i > 1$. Diese Argumentation kann man verallgemeinern und erhält somit

$$\dim_{\mathbb{F}_p}(p^nT/p^{n+1}T) = \#\{e_i \mid e_i > n\}.$$

d) Es reicht zu zeigen, dass $p_j^{e_{1j}}, \dots, p_j^{e_{sj}}$ mit $e_{1j} \geq e_{2j} \geq \dots \geq e_{sj}$ eindeutig durch $T_{p_j}(M)$ bestimmt sind. Ohne Einschränkung fixieren wir wie oben ein $p := p_j$. Mit Teilaufgabe c) erhält man für die Anzahl der $e_{ij}$ mit $e_{ij} = 1$ den Ausdruck

$$\dim_{\mathbb{F}_p}(T/pT) - \dim_{\mathbb{F}_p}(pT/p^2T)$$

was nur vom Isomorphietyp von $T$ abhängt. Sukzessive zeigt man auf diese Weise, dass

$$\#\{e_{ij} \text{ mit } e_{ij} = n\} = \dim_{\mathbb{F}_p}(p^{n-1}T/p^nT) - \dim_{\mathbb{F}_p}(p^nT/p^{n+1}T).$$

Da die rechte Seite nur vom Isomorphietyp von $T_p(M)$ abhängt und dieser eindeutig vom Isomorphietyp von $M$ bestimmt ist, haben wir die Eindeutigkeit der $e_{ij}$ gezeigt.

**Aufgabe 2 (7 Punkte).**

a) Wir benötigen einen Ring $R \subseteq \mathbb{R}$ mit den Eigenschaften $\mathbb{Q} \subseteq R$ und $\sqrt{2} \in R$. Damit müssen auch alle ($\mathbb{Q}$-)Vielfachen von $\sqrt{2}$ in $R$ liegen; außerdem gilt $\sqrt{2}^2 \in \mathbb{Q}$. Betrachen wir als Kandidaten für $R$ also die Menge

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}\,.$$

Die Verknüpfungen $+$ und $\cdot$ werden von $\mathbb{R}$ auf $\mathbb{Q}(\sqrt{2})$ eingeschränkt. Wir überprüfen nun, dass dies ein Unterring von $\mathbb{R}$ ist. Beispielsweise folgt die Abgeschlossenheit bzgl. $\cdot$ für $a, b, c, d \in \mathbb{Q}$ aus

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

die Abgeschlossenheit bzgl. $+$ erhält man vollkommen analog. Das Neutralelement für die Addition ist $0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ und für $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ist $-a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ das additive Inverse. Offensichtlich ist $\mathbb{Q}(\sqrt{2})$ auch ein Monoid bzgl. $\cdot$.

Wir zeigen noch, dass $\mathbb{Q}(\sqrt{2})$ der kleinste solche Unterring von $\mathbb{R}$ ist. Dazu betrachten wir die Menge aller Unterringe von $\mathbb{R}$ mit den gewünschten Eigenschaften. Bilden wir den Schnitt über alle diese Ringe, erhalten wir wieder einen Ring $U$ (nachprüfen!). Damit ist klar, dass es zum einen nur einen kleinsten solchen Teilring geben kann und dass zum anderen $U \subseteq \mathbb{Q}(\sqrt{2})$ gelten muss. Da aber $\mathbb{Q} \subseteq U$ und $\sqrt{2} \in U$ und $U$ ein Ring, also abgeschlossen bzgl. Multiplikation und Addition ist, muss für $a, b \in \mathbb{Q}$ auch $a + b\sqrt{2} \in U$ gelten. Insbesondere folgt $\mathbb{Q}(\sqrt{2}) \subseteq U$ und damit Gleichheit.

b) Wir müssen zeigen, dass jedes $a \neq 0$ aus $R$ ein multiplikatives Inverses besitzt. Betrachten wir dazu die Abbildung „Multiplikation mit $a$“:

$$\pi_a : R \to R, r \mapsto ra$$

Diese Abbildung ist injektiv, denn für $r, r' \in R$ mit $\pi_a(r) = \pi_a(r')$ gilt $ra = r'a$ gdw. $ra - r'a = 0$ gdw. $(r - r')a = 0$. Da $R$ ein Integritätsbereich und $a \neq 0$ ist, kann die letzte Gleichung nur für $r - r' = 0$, also $r = r'$ erfüllt sein.

Injektive Abbildungen auf endlichen, gleich großen Mengen sind aber auch surjektiv. Insbesondere gibt es ein $b \in R$ mit $\pi_a(b) = 1 = ba$, also ein multiplikatives Inverses von $a$.

**Aufgabe 3 (6 Punkte).**

a) Es ist klar, dass eine Einheit in $R$ auch eine Einheit in $R[X]$ ist. Nun nehmen wir an $f \in R[X]^\times$. Also gibt es ein $g \in R[X]$ mit $fg = 1$. Wir erhalten

$$0 = \deg(1) = \deg(fg) \geq \deg(f) + \deg(g)$$

und somit müssen beide Polynome Grad 0 haben, was sofort die Aussage zeigt.

b) Eine Richtung ist klar. Für die andere Richtung nehmen wir an, $f, g \in R[X]$ sind nicht das Nullpolynom. Sei $f = \sum_{i=0}^{k} a_i X^i \quad g = \sum_{i=0}^{l} b_i X^i$ wobei $a_k$ und $b_l$ die höchsten nicht-verschwindenden Koeffizienten sind. Der Koeffizient von $X^{k+l}$ im Produkt $f \cdot g$ ist nun aber $a_k b_l$. Da $R$ nullteilerfrei ist, ist $a_k b_l \neq 0$ also ist $fg$ nicht das Nullpolynom.

**Aufgabe 4 (6 Punkte).**

a) Ist $\sum_{i=0}^{\infty} a_i X^i$ eine Einheit mit Inversem $\sum_{i=0}^{\infty} b_i X^i$, dann ist $\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{i=0}^{\infty} c_i X^i = 1$, also insbesondere $c_0 = 1 = a_0 b_0$ und damit $a_0$ eine Einheit.

Sei $f = \sum_{i=0}^{\infty} a_i X^i \in R[\![X]\!]$ und $a_0$ eine Einheit. Wir suchen ein Inverses $g = \sum_{i=0}^{\infty} b_i X^i$. Ihr Produkt bezeichnen wir wie zuvor mit $h = \sum_{i=0}^{\infty} c_i X^i$, wobei $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ gilt. Damit $g$ ein Inverses von $f$ ist, muss $h = 1$ erfüllt sein, also $c_0 = 1$ und $c_i = 0$ für $i > 0$. Dazu setzen wir $b_0 = a_0^{-1}$. Wir zeigen nun induktiv, dass es für $i > 0$ Elemente $b_1, \ldots, b_i$ gibt, sodass $c_i = \sum_{k=0}^{i} a_i b_{i-k} = 0$ gilt. Zuerst sehen wir, dass $0 = c_1 = a_0 b_1 + a_1 b_0$ nach $b_1$ aufgelöst werden kann, da $a_0$ eine Einheit ist, und wir somit $b_1$ bestimmen können. Seien nun $b_0, \ldots, b_i$ so bestimmt, dass $c_0, \ldots, c_i = 0$ gilt. Damit können wir auch die Gleichung $0 = c_{i+1} = \sum_{k=0}^{i+1} a_k b_{i+1-k}$ nach $b_{i+1}$ auflösen, was die Behauptung zeigt.

b) Betrachten wir nun den Homomorphismus

$$\varphi : K[\![X]\!] \to K, \quad \sum_{i=0}^{\infty} a_i X^i \mapsto a_0$$

Offensichtlich ist $\varphi$ surjektiv mit $\ker(\varphi) = (X)$. Mit dem Homomorphiesatz folgt

$$K[\![X]\!]/(X) \cong K.$$

Sei nun $(0) \neq \mathfrak{a} \subsetneq K[\![X]\!]$ ein echtes Ideal und

$$n := \min\{k \in \mathbb{N} \;\mid\; \text{es gibt ein } \sum_{i=0}^{\infty} a_i X^i \in \mathfrak{a} \text{ mit } a_k \neq 0 \text{ und } a_j = 0 \text{ für } j < k\}.$$

Da $\mathfrak{a}$ ein echtes Ideal ist und somit keine Einheit enthält, folgt mit Teil a), dass $n \geq 1$ gilt. Ist nun $f \in \mathfrak{a}$ mit $f = \sum_{i=n}^{\infty} a_i X^i$ und $a_n \neq 0$, so folgt offenbar $f = X^n \cdot g$ mit $g = \sum_{i=n}^{\infty} a_i X^{i-n} \in K[\![X]\!]$, also insbesondere $f \in (X^n)$ und nach der Wahl von $n$ somit $\mathfrak{a} \subset (X^n)$. Es ist aber $g$ eine Einheit in $K[\![X]\!]$ und somit gilt $X^n = g^{-1} f \in \mathfrak{a}$, woraus wir $(X^n) \subset \mathfrak{a}$ schließen. Insgesamt folgt somit $\mathfrak{a} = (X^n)$.

Insgesamt haben wir somit gezeigt, dass es neben den trivialen Idealen $(0)$ und $K[\![X]\!]$ nur die Ideale der Form $(X^n)$ für $n \in \mathbb{N}$ gibt.

Dies zeigt auch, dass $K[\![X]\!]$ ein Hauptidealring und $(X)$ das einzige maximale Ideal ist.