LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer, Thomas Jahn

Sommersemester 2015
4. Mai 2015

Lineare Algebra 2 – Lösungsskizzen zu Übungsblatt 1

Aufgabe 1 (6 Punkte).
Angenommen, es gäbe ein $f \in \mathbb{Z}[x]$ mit $(x,2) = (f)$. Dann wäre $2 = fg$ mit einem geeigneten $g \in \mathbb{Z}[x]$, und weil sich Grade von Polynomen (über nullteilerfreien Ringen) beim Multiplizieren addieren, folgt $\deg f = 0$. Also ist $f = a \in \mathbb{Z}$ eine ganze Zahl. Andererseits ist $x = f \cdot h = ah$ für ein $h \in \mathbb{Z}[x]$; ist $h = \sum_{i=0}^{n} r_i x^i$, so folgt $1 = ar_1$, also ist a in $\mathbb{Z}$ invertierbar, und das bedeutet $a = \pm 1$. Dann folgt also $(x,2) = (f) = (a) = (\pm 1) = \mathbb{Z}[x]$.

Aber das ist nicht wahr, denn es ist $1 \notin (x,2)$: Gäbe es nämlich $p, q \in \mathbb{Z}[x]$ mit $1 = xp + 2q$, so wäre (durch Einsetzen von $x = 0$) $1 = 2q(0)$, und das ist nicht möglich wegen $q(0) \in \mathbb{Z}$.

Aufgabe 2 (6 Punkte).

a) Es ist schon bekannt, dass $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ein Unterkörper von $\mathbb{C}$ ist. Zunächst behaupten wir, dass das Bild des Einsetzungshomomorphismus $\alpha : \mathbb{Q}[x] \to \mathbb{C}$ genau $\mathbb{Q}(\sqrt{2})$ ist. Dass ganz $\mathbb{Q}(\sqrt{2})$ getroffen wird, ist klar, denn $\alpha(a + bx) = a + b\sqrt{2}$. Aber jedes Element im Bild von α ist eine Summe von Produkten von rationalen Zahlen und $\sqrt{2}$, und diese Elemente liegen alle im Ring $\mathbb{Q}(\sqrt{2})$. Also induziert α einen surjektiven Homomorphismus von $\mathbb{Q}$-Algebren $\mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$, den wir wieder α nennen.

   Wir müssen also zeigen, dass $\ker(\alpha) = (x^2 - 2)$ gilt. Es gilt aber $\ker(\alpha) \supseteq (x^2 - 2)$, da jedes $g(x) \in (x^2 - 2)$ die Form hat: $g(x) = f(x) \cdot [x^2 - 2]$ für ein passendes $f(x) \in \mathbb{Q}[x]$ und aus dieser Darstellung folgt sofort $g(\sqrt{2}) = 0$, d.h. $g(x) \in \ker(\alpha)$.
   Wir wollen nun $\ker(\alpha) \subseteq (x^2 - 2)$ zeigen. Sei $g(x) \in \ker(\alpha)$. Da $\mathbb{Q}[x]$ ein euklidscher Ring ist, gibt es ein $q(x), r(x) \in \mathbb{Q}[x]$ mit $g(x) = [x^2 - 2] \cdot q(x) + r(x)$, so dass $\deg(r(x)) < \deg(x^2 - 2) = 2$ gilt. Somit erhalten wir $0 = g(\sqrt{2}) = r(\sqrt{2})$. Da aber $\sqrt{2} \notin \mathbb{Q}$ ist das nur möglich wenn $r(x) = 0$, d.h. aber dass gilt $g(x) = [x^2 - 2] \cdot q(x)$ für ein $q(x) \in \mathbb{Q}[x]$. Also folgt $g(x) \in (x^2 - 2)$.

b) Das folgt aus a), denn der Ring ist zu einem Körper isomorph und damit selbst ein Körper.

c) Wir wissen aus der Linearen Algebra 1, dass $\{1, \sqrt{2}\}$ eine $\mathbb{Q}$-Basis des Vektorraums $\mathbb{Q}(\sqrt{2})$ ist. Da wir in a) und b) gezeigt haben, dass $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(f)$ gilt, folgt: $\dim_{\mathbb{Q}}(\mathbb{Q}[x]/(f)) = 2$, wenn man $\mathbb{Q}[x]/(f)$ als Vektorraum über $\mathbb{Q}$ auffasst.

Aufgabe 3 (6 Punkte).

a) Jedes Element von $K[x][\epsilon]$ hat die Form $h = \sum_{i=0}^{n} \epsilon^i f_i$ mit gewissen $f_i \in K[x]$. In R ist $[\epsilon^2] = 0$, also ist dann $[h] = [f_0 + \epsilon f_1]$; das zeigt die Existenz dieser Darstellung. Für die Eindeutigkeit sei $[f + \epsilon g] = [\widetilde{f} + \epsilon \widetilde{g}]$; das bedeutet $f - \widetilde{f} + \epsilon(g - \widetilde{g}) = \epsilon^2 \cdot q$ mit $q \in K[x][\epsilon]$. Der Fall $q \neq 0$ kann aber aus Gradgründen (wobei der Grad in ϵ gemeint ist) nicht sein; also folgt $q = 0$, d.h. $f + \epsilon g = \widetilde{f} + \epsilon \widetilde{g}$, und das bedeutet $f = \widetilde{f}$ und $g = \widetilde{g}$.

b) Es genügt sicher, dies für Polynome der Form $f = x^k$ zu überprüfen (denn beide Seiten reichen Summen und Skalarmultiplikationen in f komplett durch). Es ist aber nach der binomischen Formel

$$f([x + \epsilon]) = [x + \epsilon]^k = [x^k + \epsilon k x^{k-1} + \epsilon^2 (\dots)] = [x^k + \epsilon k x^{k-1}] = [f + \epsilon f'].$$

c) Nach b) ist einerseits

$$(fg)([x + \epsilon]) = [fg + \epsilon(fg)'],$$

andererseits – Einsetzen ist ein Ringhomomorphismus! –

$$\begin{aligned}(fg)([x + \epsilon]) &= f([x + \epsilon]) \cdot g([x + \epsilon]) \\ &= [f + \epsilon f'][g + \epsilon g'] \\ &= [fg + \epsilon(fg' + f'g) + \epsilon^2 f'g'] \\ &= [fg + \epsilon(fg' + f'g)],\end{aligned}$$

und aufgrund der Eindeutigkeitsaussage in a) folgt $(fg)' = fg' + f'g$. (Dieser Beweis ist sogar noch natürlicher als derjenige "aus der Analysis", womit im Wesentlichen dieselbe Rechnung gemeint war, ausgehend von der Formel $f([x + \epsilon]) - f([x]) = [\epsilon f']$.)

Aufgabe 4 (6 Punkte).

a) Wir beschreiben in dieser Teilaufgabe noch einmal kurz das Verfahren.
Sei $a \equiv a_i \bmod n_i$ ein System von Kongruenzen mit $i \in \{1, \dots, m\}$. Wir überprüfen zuerst, ob die n_i paarweise teilerfremd sind, was z.B. in Teilaufgabe a) auch stimmt. Dann definieren wir $n_i' := n/n_i$, wobei $n := \prod_{i=1}^{m} n_i$ ist. Nun suchen wir zu jedem n_i' mit Hilfe des Euklidschen Algorithmus ein Inverses t_i von n_i' mod n_i.
Mit dem aus der Vorlesung präsentierten Verfahren wissen wir dann, dass gilt $a = \sum_{i=1}^{m} a_i t_i n_i' \bmod n$. Insbesondere haben wir also eine Lösung des gegebenen Systems gefunden. Das Einsetzen der Zahlenwerte liefert: $a = 15437$.
Diese Lösung ist nicht eindeutig, das sie mit Vielfachen von 16200 erweitert werden kann.

b) Wir sehen, dass gilt $100 = 25 \cdot 4$ and 25 und 4 sind teilerfremd. Mit dem Chinesischen Restsatz sind die Lösungen von $x \equiv 49^{2015} \bmod 100$ gleich den Lösungen des Systems von simultanen Kongruenzen:

$$\begin{aligned}x &\equiv 49^{2015} \bmod 25 \\ x &\equiv 49^{2015} \bmod 4.\end{aligned}$$

Also gilt,

$$49^{2015} \equiv (-1)^{2015} \bmod 25 \equiv -1 \bmod 25$$
$$49^{2015} \equiv 1^{2015} \bmod 4 \equiv 1 \bmod 4.$$

Mit dem in a) präsentierten Lösungsverfahren erhalten wir:

$$\begin{aligned} x &\equiv ((-1) \cdot 19 \cdot 4 + 1 \cdot 1 \cdot 25) \bmod 100 \\ &\equiv (-76 + 25) \bmod 100 \\ &\equiv -51 \bmod 100 \\ &\equiv 49 \bmod 100 \end{aligned}$$

c) Mit dem in Teilaufgabe a) beschriebenen Verfahren erhält man: $q = -x^2 + 2x + 2$. Diese Lösung ist nicht eindeutig, da sie mit Vielfachen von $(x-1)(x-2)(x-3)$ erweitert werden kann.