Algebra I

Musterlösung 10

maximale Ideale, Polynomringe, endliche Körper

Das sogenannte Teichmüllerprinzip ist eine Aussage, welche äquivalent zum Auswahlaxiom ist, und welche sich besonders für Anwendungen in der Algebra eignet. Für die Formulierung des Teichmüllerprinzips müssen wir folgenden Begriff einführen:

Eine Menge M hat **endlichen Charakter**, wenn gilt:

$$X \text{ ist in } M \iff \text{jede endliche Teilmenge von } X \text{ ist in } M.$$

TEICHMÜLLERPRINZIP: Ist M eine Menge mit endlichem Charakter, so hat M bezüglich der Inklusion $\subseteq$ ein maximales Element.

63. Sei R ein Ring.

(a) Zeige, dass die Menge $M := \big\{S \subseteq R : 1_R \notin (S)\big\}$ endlichen Charakter hat.

(b) Zeige, dass R ein maximales Ideal besitzt.

(c) Zeige, dass jedes Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{a} \neq R$ zu einem maximalen Ideal erweitert werden kann.

Lösung: (a) Ist $S \in M$, so gilt für jede endliche Teilmenge $S' \subseteq S$ wegen $(S') \subseteq (S)$ offensichtlich $1_R \notin (S')$. Sei andererseits $S \subseteq R$ mit der Eigenschaft, dass für jede endliche Teilmenge $S' \subseteq S$ gilt, dass $1_R \notin (S')$ ist. Sei $s \in (S)$. Dann exisiteren $r_1, \ldots, r_n \in R$ und $s_1, \ldots, s_n \in S$ mit $s = \sum_{i=1}^{n} r_i s_i$. Somit ist $s \in (\{s_1, \ldots, s_n\})$ und es folgt $s \neq 1$. Also ist $1_R \notin (S)$.

(b) Sei $M := \big\{S \subseteq R : 1_R \notin (S)\big\}$. Dann ist $\{0\} \in M$, also $M \neq \emptyset$. Mit (a) hat M ein bezüglich Inklusion maximales Element $S_{\max}$. Für alle $r \in R$ gilt nun entweder $r \in (S_{\max})$ oder $(S_{\max} \cup \{r\}) = R$, und somit ist $(S_{\max})$ ein maximales Ideal in R.

(c) Sei $M_{\mathfrak{a}} := \big\{S \subseteq R : 1_R \notin (S \cup \mathfrak{a})\big\}$. Dann ist $\{0\} \in M_{\mathfrak{a}}$, also $M_{\mathfrak{a}} \neq \emptyset$. Mit (a) hat $M_{\mathfrak{a}}$ ein bezüglich Inklusion maximales Element $S_{\max}$. Wie in (b) folgt dann, dass $(S_{\max} \cup \mathfrak{a})$ ein maximales Ideal in R ist, welches $\mathfrak{a}$ enthält.

64. Sei R ein kommutativer Ring. Sei $R[X][Y]$ der Polynomring über $R[X]$ in der Unbestimmten Y und sei $R[Y][X]$ der Polynomring über $R[Y]$ in der Unbestimmten X.

(a) Zeige: $R[X][Y] \simeq R[Y][X]$.
Bemerkung: Für $R[X][Y]$ schreiben wir auch $R[X, Y]$. Mehr dazu in der nächsten Aufgabe.

(b) Zeige, dass das Ideal (X, Y) kein Hauptideal ist.

Lösung: (a) Sei $R \to R[Y][X]$ die offensichtliche Inklusion. Mit der universellen Eigenschaft des Polynomrings kann diese eindeutig zu einem Ringhomomorphismus $R[X] \to R[Y][X]$, der X auf X abbildet, erweitert werden. Wieder mit der universellen Eigenschaft

des Polynomrings kann dieser Homomorphismus eindeutig zu einem Ringhomomorphismus $\varphi\colon R[X][Y] \to R[Y][X]$, der Y auf X abbildet, erweitert werden. Auf dieselbe Art bekommen wir einen Ringhomomorphismus $\psi\colon R[Y][X] \to R[X][Y]$. Die Verknüpfung $\psi \circ \varphi|_{R[X]}\colon R[X] \to R[X][Y]$ ist eine Fortsetzung der Identitätsfunktion, die X auf X abbildet. Da jede solche Fortsetzung eindeutig sein muss, ist $\psi \circ \varphi|_{R[X]}$ die Identität. Dasselbe Argument wiederholt ergibt, dass $\psi \circ \varphi$ und $\varphi \circ \varphi$ die Identität sind. Somit ist φ ein Isomorphismus.

(b) Sei P ein Polynom mit $(P) = (X, Y)$. Die Elemente aus (X, Y) sind genau die Polynome, deren konstanter Koeffizient gleich 0 ist. Daher muss der konstante Koeffizient von P gleich 0 sein. Ausserdem muss P sowohl X als auch Y teilen. Sei $Q \in R[X, Y]$ mit $X = PQ$. Seien a_X der Koeffizient von X in P und a_Y der Koeffizient von Y in P. Sei weiter b_0 der konstante Koeffizient in Q. Aus $X = PQ$ folgt $1 = a_X b_0$ und $0 = a_Y b_0$. Also sind a_X und b_0 Einheiten und es folgt $a_Y = 0$. Mit demselben Argument für Y können wir aber schliessen, dass a_Y eine Einheit und $a_X = 0$ sein muss. Das ist ein Widerspruch.

Sei Λ eine Indexmenge und sei $\mathscr{X} := \{X_\lambda : \lambda \in \Lambda\}$ eine Menge von Symbolen. Sei R ein kommutativer Ring. Ziel der nächsten Aufgabe ist es, den Polynomring $R[\mathscr{X}]$ zu definieren.

Eine *gerichtete Menge* ist eine Menge I mit einer binären Relation, die folgende Eigenschaften erfüllt:

- Reflexivität: $\forall i \in I\colon i \preceq i$
- Transitivität: $\forall i, j, k \in I\colon (i \preceq j) \wedge (j \preceq k) \Rightarrow (i \preceq k)$
- Existenz einer oberen Schranke: $\forall i, j \in I\, \exists k \in I\colon i, j \preceq k$.

Ein *induktives System von Ringen* besteht aus einer gerichteten Menge $(I, \preceq)$, einer Menge von Ringen $\{R_i : i \in I\}$ und für alle $i, j \in I$ mit $i \preceq j$ einem Ringhomomorphismus $f_{ij}\colon R_i \to R_j$, der die folgenden Eigenschaften erfüllt:

- $\forall i \in I\colon f_{ii} = id_{R_i}$
- $\forall i, j, k \in I,\, i \preceq j \preceq k\colon f_{ik} = f_{jk} \circ f_{ij}$.

Der *Kolimes* des induktiven Systems ist dann wie folgt definiert. Auf der disjunkten Vereinigung $\dot{\bigcup}_{i\in I} R_i$ definieren wir eine Äquivalenzrelation. Seien $x \in R_i$ und $y \in R_j$. Dann gilt

$$x \sim y \quad \Leftrightarrow \quad \exists k \in I\colon (i, j \preceq k) \wedge (f_{ik}(x) = f_{jk}(y)).$$

Die unterliegende Menge des Rings $\operatorname{colim}_{i\in I} R_i$ ist nun definiert als die Menge aller Äquivalenzklassen dieser Äquivalenzrelation.

65. (a) Definiere Addition und Multiplikation auf $\operatorname{colim}_{i\in I} R_i$. Zeige, dass diese Operationen wohldefiniert sind und $\operatorname{colim}_{i\in I} R_i$ zu einem Ring machen.

(b) Sei $\operatorname{fin}(\mathscr{X})$ die Menge aller *endlichen* Teilmengen von $\mathscr{X}$. Für $S \in \operatorname{fin}(\mathscr{X})$ sei $\operatorname{Numm}(S)$ die Menge aller Bijektionen $\{1, \ldots, |S|\} \to S$.

Sei

$$I := \bigcup_{S\in\operatorname{fin}(\mathscr{X})} \{S\} \times \operatorname{Numm}(S)\,.$$

Die Elemente von I sind geordnete Paare $\langle S, f\rangle$ mit $S \in \operatorname{fin}(\mathscr{X})$ und $f \in \operatorname{Numm}(S)$. Zeige, dass I mit der Relation

$$\langle S, f\rangle \preceq \langle S', f'\rangle \quad \Leftrightarrow \quad S \subseteq S'$$

eine gerichtete Menge ist.

(c) Definiere ein gerichtetes System mit dieser gerichteten Menge mit

$$R_{S,f} := R[f(1)][f(2)]...[f(|S|)].$$

Dessen Kolimes ist der Polynomring $R[\mathscr{X}]$.

(d) Verallgemeinere die universelle Eigenschaft von $R[X]$ auf $R[\mathscr{X}]$.

Lösung: (a) Für ein $x \in \dot{\bigcup}_{i\in I} R_i$ bezeichnen wir die Äquivalenzklasse von x mit $[x]$. Seien nun $x \in R_i$ und $y \in R_j$. Sei $k \in I$ mit $i, j \preceq k$. Wegen $f_{ii}(x) = x$ gilt $[x] = [f_{ik}(x)]$ und $[y] = [f_{jk}(y)]$ und wir definieren

$$\begin{aligned}[x] + [y] &:= [f_{ik}(x) + f_{jk}(y)]\\ [x] \cdot [y] &:= [f_{ik}(x) \cdot f_{jk}(y)].\end{aligned}$$

Wir müssen zeigen, dass $[f_{ik}(x) + f_{jk}(y)]$ und $[f_{ik}(x) \cdot f_{jk}(y)]$ unabhängig von der Wahl von x, y und k sind. Wir beschränken uns auf den Fall der Addition, die Multiplikation funktionier genau gleich. Seien also $x' \in R_{i'}$ und $y \in R_{j'}$ mit $[x] = [x']$ und $[y] = [y']$. Dann existieren ein $i'', j'' \in I$ mit $i, i' \preceq i''$ und $j, j' \preceq j''$ für die $f_{ii''}(x) = f_{i'i''}(x')$ und $f_{jj''}(y) = f_{j'j''}(y')$ gilt. Es existiert $k'' \in I$ mit $i'', j'' \preceq k''$. Wir müssen zeigen, dass $[f_{ik}(x) + f_{jk}(y)] = [f_{i'k''}(x') + f_{j'k''}(y')]$ ist. Sei $l \in I$ mit $k, k'' \preceq l$. Dann ist

$$\begin{aligned}[f_{ik}(x) + f_{jk}(y)] &= [f_{kl}(f_{ik}(x) + f_{jk}(y))]\\ &= [f_{kl}(f_{ik}(x)) + f_{kl}(f_{jk}(y))]\\ &= [f_{il}(x) + f_{jl}(y)]\\ &= [f_{i'l}(x') + f_{j'l}(y')]\\ &= [f_{k''l}(f_{i'k''}(x')) + f_{k''l}(f_{j'k''}(y'))]\\ &= [f_{k''l}(f_{i'k''}(x') + f_{j'k''}(y'))]\\ &= [f_{i'k''}(x') + f_{j'k''}(y')].\end{aligned}$$

Somit ist die Addition, und genau gleich die Multiplikation, wohldefiniert. Da alle für alle $i, j \in I$ die Abbildung f_{ij} ein Ringhomomorphismus ist, ist $f_{ij}(0_{R_i}) = 0_{R_j}$ und es gilt $[0_{R_i}] = [0_{R_j}]$. Wegen

$$[x] + [0_{R_i}] = [x + 0_{R_i}] = [x]$$

existiert somit ein neutrales Element der Addition. Analog existiert ein neutrales Element der Multiplikation. Für Assoziativität seien $x \in R_i, y \in R_j, z \in R_k$. Sei $l \in R$ mit $i, j, k \preceq l$. Dann gilt

$$\begin{aligned}([x] + [y]) + [z] &= [f_{il}(x) + f_{jl}(y)] + [f_{kl}(z)]\\ &= [(f_{il}(x) + f_{jl}(y)) + f_{kl}(z)]\\ &= [f_{il}(x) + (f_{jl}(y) + f_{kl}(z))]\\ &= [f_{il}(x)] + [f_{jl}(y) + f_{kl}(z)]\\ &= [x] + ([y] + [z]).\end{aligned}$$

Genau auf dieselbe Weise lassen sich Assoziativität der Multiplikation, Kommutativität und die Distribuitivitätsregeln auf die Ringaxiome in einem R_l zurückführen.

(b) Sei $\langle S, f\rangle \in I$. Wegen $S \subseteq S$ ist die Reflexivität erfüllt. Seien weiter $\langle S', f'\rangle, \langle S'', f''\rangle \in I$ mit $\langle S, f\rangle \preceq \langle S', f'\rangle$ und $\langle S', f'\rangle \preceq \langle S'', f''\rangle$. Das bedeutet $S \subseteq S'$ und $S' \subseteq S''$. Dann gilt aber auch $S \subseteq S''$ und somit $\langle S, f\rangle \preceq \langle S'', f''\rangle$. Also ist Transitivität erfüllt. Für die Existenz einer oberen Schranke seien $\langle S, f\rangle, \langle S', f'\rangle \in I$. Dann gilt für jedes Element $\langle S'', f''\rangle$ in der

nichtleeren Menge $\{S \cup S'\} \times \mathrm{Numm}\langle S \cup S'' \rangle$, dass $\langle S, f\rangle \preceq \langle S'', f''\rangle$ und $\langle S', f'\rangle \preceq \langle S'', f''\rangle$ ist. Somit ist $(I, \preceq)$ eine gerichtete Menge.

(c) Seien $\langle S, f\rangle, \langle S', f'\rangle \in I$ mit $\langle S, f\rangle \preceq \langle S', f'\rangle$. Sei $R \to R[f'(1)] \dots [f'(|S'|]$ die offensichtliche Einbettung. Mit der universellen Eigenschaft des Polynomrings lässt sich diese eindeutig zu einem Ringhomomorphismus $R[f(1)] \to R[f'(1)] \dots [f'(|S'|]$, der $f(1)$ auf $f(1)$ abbildet, fortsetzen. Induktiv existiert ein eindeutiger Ringhomomorphismus

$$f_{\langle S,f\rangle,\langle S',f'\rangle} \colon R[f(1)] \dots [f(|S|)] \to R[f'(1)] \dots [f'(|S'|],$$

der für alle $n = 1, \dots, |S|$ das Element $f(n)$ auf $f(n)$ abbildet.

Nach Konstruktion ist

$$f_{\langle S,f\rangle,\langle S,f\rangle} \colon R[f(1)] \dots [f(|S|)] \to R[f(1)] \dots [f(|S|]$$

der eindeutiger Ringhomomorphismus, der für alle $n = 1, \dots, |S|$ das Element $f(n)$ auf $f(n)$ abbildet. Wegen der Eindeutigkeit muss dieser die Identität sein und die erste Eigenschat eines gerichteten Systems ist erfüllt.

Sei $\langle S'', f''\rangle \in I$ mit $\langle S, f\rangle, \langle S', f'\rangle \preceq \langle S'', f''\rangle$. Die Abbildung $f_{\langle S',f'\rangle,\langle S'',f''\rangle} \circ f_{\langle S',f'\rangle,\langle S,f\rangle}$ ist auf R die offensichtliche Inklusion. Ausserdem gilt für jedes $n = 1, \dots, |S|$ nach Definition

$$f_{\langle S',f'\rangle,\langle S'',f''\rangle} \circ f_{\langle S',f'\rangle,\langle S,f\rangle}(f[n]) = f_{\langle S',f'\rangle,\langle S'',f''\rangle}(f[n]) = f[n].$$

Wegen der Eindeutigkeit gilt daher

$$f_{\langle S',f'\rangle,\langle S'',f''\rangle} \circ f_{\langle S,f\rangle,\langle S,f\rangle} = f_{\langle S,f\rangle,\langle S'',f''\rangle}$$

und wir haben alle Eingenschaften eines gerichteten Systems nachgeprüft.

(d) Sei $\varphi \colon R \to S$ ein Ringhomomorphismus. Dann existiert für jede Abbildung $\alpha \colon \Lambda \to S$ ein eindeutiger Ringhomomorphismus $\psi \colon R[\mathscr{X}] \to S$, sodass die beiden Bedingungen

- $\psi|_R = \varphi$
- $\forall \lambda \in \Lambda \colon \psi(X_\lambda) = \alpha(\Lambda)$

erfüllt sind.

66. (a) Konstruiere einen Körper mit 5^2 Elementen.
Hinweis: Suche im Ring $\mathbb{F}_5[X]$ ein Polynom p vom Grad 2, sodass (p) ein Primideal ist, und betrachte $\mathbb{F}_5[X]/(p)$.

(b) Konstruiere einen Körper mit 2^5 Elementen.

Lösung: (a) Sei $p \in \mathbb{F}_5[X]$ ein Polynom vom Grad 2. Sei q ein weiteres Polynom. Nach dem Euklidischen Algorithmus gibt es eindeutige Polynome a, r mit $\deg(r) < \deg(p)$ und $q = ap + r$. Das bedeutet $q + (p) = r + (p)$. Wegen $|\{b \in \mathbb{F}_5[X] : \deg(b) < \deg(p)\}| = 5^p$ hat $\mathbb{F}_5[X]/(p)$ Kardinalität 5^2. Als endlicher Ring ist er genau dann ein Körper, wenn er nullteilerfrei ist, also, wenn (p) ein Primideal ist. Seien $a_1, a_2 \in \mathbb{F}_5[X]$ mit $a_1 a_2 \in (p)$. Seien b_1, b_2 Polynome mit $a_i + (p) = b_i + (p)$ und $\deg(b_i) < \deg(p) = 2$. Dann muss aus Gradgründen $\deg(b_1 b_2) \leq \deg(p)$ gelten und somit folgt entweder $\deg(b_1) = \deg(b_2) = 1$ oder $b_1 b_2 = 0$. Letzteres beduetet, dass b_1 oder b_2 in (p) liegt. Falls es keine nichtkonstanten Polynome p_1, p_2 vom Grad 1 gibt mit $p = p_1 p_2$, so ist $p_1, p_2 \notin (p)$, daher ist (p) ein Primideal.

Sei $p = X^2 + 2$. Durch Ausprobieren erkennen wir, dass dieses Polynom keine Nullstelle in $\mathbb{F}_5$ hat. Das beduetet, dass es keine $p_1, p_2 \in \mathbb{F}_5[X]$ vom Grad 1 gibt mit $p = p_1 p_2$. Also wäre eine Möglichkeit für den gesuchten Körper $\mathbb{F}_5[X]/(X^2 + 2)$.

Bemerkung: Die Restklasse $X + (p)$ ist eine Nullstelle von $Y^2 + 2 \in \mathbb{F}_5[X]/(X^2 + 2)[Y]$.

(b) Wir beginnen wie in (a). Sei $p \in \mathbb{F}_2[X]$ ein Polynom vom Grad 5. Sei q ein weiteres Polynom. Nach dem Euklidischen Algorithmus gibt es eindeutige Polynome $a, r \in \mathbb{F}_2[X]$ mit $\deg(r) < \deg(p)$ und $q = ap + r$. Das bedeutet $q + (p) = r + (p)$. Wie in Teil (a) gilt nun $|\{b \in \mathbb{F}_2[X] : \deg(b) < \deg(p)\}| = 2^p$ und daher $|\mathbb{F}_2[X]/(p)| = 2^5$. Sei $b \in \mathbb{F}_2[X]$ nicht 0 mit $\deg(b) < \deg(p)$. Nimm an, dass p kein Produkt zweier nichtkonstanter Polynome ist. Dann können p und b_i keine gemeinsamen Teiler ausser 1 haben und mit dem euklidischen Algorithmus können wir 1 als Linearkombination von p und b_i darstellen. Daher ist (p) maximal und somit ist $\mathbb{F}_2[X]/(p)$ ein Körper.

Das Polynom (p) darf keine Nullstelle haben und nicht in Polynome vom Grad 2 und 3 zerfallen. Das einzige nullstellenlose Polynom vom Grad 2 ist $X^2 + X + 1$. Wenn p keine Nullstelle hat und zusätzlich nicht durch $X^2 + X + 1$ teilbar ist, sind wir fertig. Durch Ausprobieren finden wir $p = X^5 + X^4 + X^3 + X^2 + 1$.

Bemerkung: Wieder ist die Restklasse $X + (p)$ eine Nullstelle von $Y^5 + Y^4 + Y^3 + Y^2 + 1 \in \mathbb{F}_2[X]/(p)[Y]$.

67. Bestimme die Einheitengruppe des Rings $(\mathbb{Z}/4\mathbb{Z})[X]$.

Lösung: We claim that

$$(\mathbb{Z}/4\mathbb{Z})[X]^* = \big\{1 + 2f \;\big|\; f \in \mathbb{Z}/4\mathbb{Z}[X]\big\}.$$

"$\subseteq$": Consider the ring homomorphism $\varphi : (\mathbb{Z}/4\mathbb{Z})[X] \to (\mathbb{Z}/2\mathbb{Z})[X]$ obtained by extending the homomorphism $\mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})[X]$, $\bar{1} \mapsto \bar{1}$ by $X \mapsto X$. Since $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ is a field, we already know that $(\mathbb{Z}/2\mathbb{Z})[X]^* = (\mathbb{Z}/2\mathbb{Z})^* = \{1\}$. On the other hand, as a ring homomorphism φ maps units to units. Thus for all $g \in (\mathbb{Z}/4\mathbb{Z})[X]^*$ we have $\varphi(g) = 1$, and so g has the desired form.

"$\supseteq$": Let $g := 1 + 2f$ for some $f \in (\mathbb{Z}/4\mathbb{Z})[X]$. Then we have $g^2 = 1 + 4f + 4f^2 = 1$, so g is a unit in $(\mathbb{Z}/4\mathbb{Z})[X]$.