Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein  Dipl.-Math. Jochen Schröder

# Einführung in Algebra und Zahlentheorie – Übungsblatt 8

**Aufgabe 1** (4 Punkte)

Sei $R$ ein kommutativer Ring. Die Elemente von $R[[X]] = \{\sum_{i=0}^{\infty} a_i X^i : a_i \in R\}$ heißen *formale Potenzreihen*. Glaube[1], dass $R[[X]]$ mit den folgenden Verknüpfungen[2] zu einem Ring wird:

$$\begin{aligned} \sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i &= \sum_{i=0}^{\infty} c_i X^i \quad \text{mit } c_i = a_i + b_i, \\ \sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{\infty} b_i X^i &= \sum_{i=0}^{\infty} c_i X^i \quad \text{mit } c_i = \sum_{j=0}^{i} a_j b_{i-j}. \end{aligned}$$

Zeige, dass $\sum_{i=0}^{\infty} a_i X^i$ genau dann invertierbar ist, wenn $a_0$ in $R$ invertierbar ist.
Gib für $a_0 \in R^\times, a_1 \in R$ eine allgemeine Formel für das multiplikativ Inverse zu $a_0 + a_1 X$ an und wende sie an, um $(1-X)^{-1}$ zu berechnen.

**Lösung Aufgabe 1**

Sei $\sum_{i=0}^{\infty} a_i X^i$ invertierbar mit $\sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{\infty} b_i X^i = 1 = 1X^0 + 0X^1 + 0X^2 + ....$ Die Faltungsformel und Koeffizientenvergleich zeigt $a_0 b_0 = 1$, also ist $a_0$ invertierbar in $R$. Dies zeigt „⇒“.

„⇐“ Sei nun $\sum_{i=0}^{\infty} a_i X^i$ mit $a_0 \in R^\times$ gegeben. Gesucht ist $\sum_{i=0}^{\infty} b_i X^i$, so dass $c_i = \sum_{j=0}^{i} a_j b_{i-j} \overset{(!)}{=} \begin{cases} 1 & \text{für } i = 0 \\ 0 & \text{sonst} \end{cases}$ $(*)$.

Setze $b_0 = a_0^{-1}$. Dann ist die Bedingung $(*)$ erfüllt für $i = 0$.
Seien nun für $n \in \mathbb{N}$ alle Koeffizienten $b_0, ..., b_{n-1}$ bestimmt, so dass die Bedingung $(*)$ erfüllt ist für alle $i = 0, ..., n-1$. (Dies ist möglich, da zur Berechnung dieser $c_i$ nur die Koeffizienten $b_0$, ..., $b_{n-1}$ benötigt werden.) Die Forderung $0 \overset{(!)}{=} \sum_{j=0}^{n} a_j b_{n-j}$ ist äquivalent zu $a_0 b_n = -\sum_{j=1}^{n} a_j b_{n-j}$ und wegen $a_0 \in R^\times$ können wir $b_n = -a_0^{-1} \sum_{j=1}^{n} a_j b_{n-j}$ setzen.
Für diese $b_0, ..., b_n$ gilt die Bedingung $(*)$ für alle $i = 0, ..., n$ und wir können induktiv das Inverse zu $\sum_{i=0}^{\infty} a_i X^i$ konstruieren.

Wir berechnen das Inverse zu $a_0 + a_1 X$ mit obiger Formel. Wir setzen $b_0 = a_0^{-1}$. Da $a_i = 0$ für $i \geq 2$ ist, wird die allgemeine Formel für die Koeffizienten einfacher: Für $n \geq 1$ setzen wir $b_n = -a_0^{-1} \sum_{j=1}^{n} a_j b_{n-j} = -a_0^{-1} a_1 b_{n-1} = (-a_0^{-1} a_1) b_{n-1}$. Induktiv erhalten wir $b_n = (-a_0^{-1} a_1)^n \cdot b_0 = (-1)^n \cdot a_0^{-n-1} \cdot a_1^n$.
Also ist $(a_0 + a_1 X)^{-1} = \sum_{i=0}^{\infty} (-1)^i \cdot a_0^{-i-1} \cdot a_1^i X^i$.

Mit $a_0 = 1, a_1 = -1$ ergibt sich $(1-X)^{-1} = \sum_{i=0}^{\infty} X^i$, was man durch Ausmultiplizieren leicht verifiziert.

**Aufgabe 2** (4 Punkte)

Gegeben sei der Monoidring $\mathbb{Z}[M]$, wobei $M = (\mathbb{Z}/2\mathbb{Z}, \cdot)$.

[1] Das heißt, dass du es nicht beweisen musst. Es dir klarzumachen oder deinen Tutor zu fragen, kann aber nicht schaden.
[2] Die Verknüpfungen sehen aus wie im Monoidring. Mache dir klar, was der Unterschied zwischen dem Monoidring $R[X] \cong R[\mathbb{N}_0]$ und $R[[X]]$ ist und welche Eigenschaft von $\mathbb{N}_0$ wir benötigen, damit die Verknüpfungen dennoch funktionieren!

a) Sammle einen halben Punkt, indem du ein allgemeines Element aus $\mathbb{Z}[M]$, das Ergebnis des Produktes zweier solcher Elemente sowie die beiden Neutralelemente explizit angibst.

b) Bestimme nun die Einheitengruppe $\mathbb{Z}[M]^\times$.

c) Bestimme alle Nullteiler. Gib weiterhin für jeden Nullteiler $x \in \mathbb{Z}[M]$ die Menge $N_x = \{y \in \mathbb{Z}[M] : xy = 0\}$ an.

**Lösung Aufgabe 2**

a) Ein allgemeines Element hat die Form $a \cdot \overline{0} + b \cdot \overline{1}$ mit $a, b \in \mathbb{Z}$. Länger kann man auch $\delta_{\overline{0}}$ anstatt $\overline{0}$ und $\delta_{\overline{1}}$ anstatt $\overline{1}$ schreiben.
Für allgemeine Elemente $a \cdot \overline{0} + b \cdot \overline{1}$, $c \cdot \overline{0} + d \cdot \overline{1}$ gilt $(a \cdot \overline{0} + b \cdot \overline{1}) \cdot (c \cdot \overline{0} + d \cdot \overline{1}) = (ac + ad + bc) \cdot \overline{0} + bd \cdot \overline{1}$.
Das additive Neutralelement ist $0 \cdot \overline{0} + 0 \cdot \overline{1}$, das multiplikative Neutralelement $0 \cdot \overline{0} + 1 \cdot \overline{1}$.

b) Ein Element $a \cdot \overline{0} + b \cdot \overline{1}$ ist dann invertierbar, wenn es $c \cdot \overline{0} + d \cdot \overline{1}$ gibt, so dass $(a \cdot \overline{0} + b \cdot \overline{1})(c \cdot \overline{0} + d \cdot \overline{1}) \stackrel{!}{=} 0 \cdot \overline{0} + 1 \cdot \overline{1}$ ist.
Mit der Multiplikationsformel aus Aufgabenteil a) gibt dies folgende Bedingung:
Es gibt $c, d \in \mathbb{Z}$, so dass $ac + ad + bc = 0, bd = 1$.
Letztere sagt $b = d \in \{\pm 1\}$. Dabei reicht es den Fall, $b = d = 1$ zu betrachten, denn diejenigen Einheiten mit $b = d = -1$ stehen mit denen mit $b = d = 1$ in Bijektion, indem wir das Vorzeichen umkehren (Multiplikation mit $-1$).
Mit $b = d = 1$ ist die zweite Bedingung erfüllt, die erste wird zu $ac + a + c = 0$, was wir umformen zu $0 = ac + a + c = (c + 1)a + c = (c + 1)a + c + 1 - 1 = (c + 1)(a + 1) - 1 \Rightarrow (a + 1)(c + 1) = 1$.
Ein solches $c$ existiert offensichtlich genau dann, wenn $a + 1 \in \{\pm 1\}$ liegt, was zwei Einheiten gibt: $-2 \cdot \overline{0} + 1 \cdot \overline{1}$ und $0 \cdot \overline{0} + 1 \cdot \overline{1} = 1$.
Insgesamt erhalten wir durch Multiplikation mit $-1$ die Einheitengruppe $\{-2 \cdot \overline{0} + 1 \cdot \overline{1}, 0 \cdot \overline{0} + 1 \cdot \overline{1}, 2 \cdot \overline{0} - 1 \cdot \overline{1}, 0 \cdot \overline{0} - 1 \cdot \overline{1}\}$.

c) $a \cdot \overline{0} + b \cdot \overline{1}$ ist ein Nullteiler, wenn es $c, d$ gibt, die nicht beide 0 sind, so dass $(a \cdot \overline{0} + b \cdot \overline{1})(c \cdot \overline{0} + d \cdot \overline{1}) \stackrel{!}{=} 0 \cdot \overline{0} + 0 \cdot \overline{1}$ ist.
Dies gibt die Bedingungen $bd = 0, ac + ad + bc = 0$.
**Fall 0:** $a = b = 0$ ist langweilig. 0 ist ein Nullteiler und $N_0$ ist der ganze Monoidring.
**Fall 1:** $b \neq 0$. Dann muss $d = 0$ sein, genau dann ist die erste Bedingung erfüllt.
Damit wird die zweite Bedingung zu $0 = ac + bc = (a + b)c$. Da es $(c, d) \neq (0, 0)$ geben soll, muss hier $a = -b$ $(\neq 0)$ sein. Für diese Belegung existieren passende $c, d$, nämlich $d = 0$ (siehe oben), $c$ beliebig.
Also ist für jedes $a \in \mathbb{Z} \setminus \{0\}$ $x = a \cdot \overline{0} - a \cdot \overline{1}$ ein Nullteiler mit $N_x = \{c \cdot \overline{0} + 0 \cdot \overline{1} : c \in \mathbb{Z}\}$.
**Fall 2:** $b = 0$, die erste Bedingung ist dann automatisch erfüllt. Es gilt $a \neq 0$.
Die zweite Bedingung wird zu $0 = ac + ad = a(c + d) \stackrel{a \neq 0}{\Rightarrow} c + d = 0$ und genau diese $c, d$ erfüllen dann die zweite Bedingung.
Insgesamt ist jedes $x = a \cdot \overline{0} + 0 \cdot \overline{1}$ $(a \neq 0)$ ein Nullteiler mit $N_x = \{c \cdot \overline{0} - c \cdot \overline{1} : c \in \mathbb{Z}\}$.

**Aufgabe 3** (4 Punkte)
Zeige, dass $\mathbb{R}[X]/(X^2 - X)$ und $\mathbb{R}[(\mathbb{Z}/2\mathbb{Z}, \cdot)]$ als $\mathbb{R}$-Algebren isomorph sind.
(Es versteht sich von selbst, dass hierbei zunächst verstanden werden sollte, wie die $\mathbb{R}$-Algebren-Struktur jeweils aussieht!)

**Lösung Aufgabe 3**
Zur Erinnerung: Eine $\mathbb{R}$-Algebra ist ein Ring mit $\mathbb{R}$-Modul-Struktur (äquivalent dazu ist es ein Ring mit Ringhomomorphismus von $\mathbb{R}$ in diesen Ring). Ein $\mathbb{R}$-Algebren-Homomorphismus ist dann ein Ringhomomorphismus, der gleichzeitig eine $\mathbb{R}$-lineare Abbildung ist.

Zunächst verstehen wir die $\mathbb{R}$-Algebren-Strukturen. Dies ist nicht sehr schwer.

Jedes $\overline{f} \in \mathbb{R}[X]/(X^2 - X)$ besitzt einen eindeutigen Vertreter $aX + b \in \mathbb{R}[X]$. Die Addition ist komponentenweise gegeben, die Multiplikation durch $X^2 = X$ wie folgt: $(aX + b)(cX + d) = (ac + ad + bc)X + bd$.
$\mathbb{R}$ ist Teilring von $\mathbb{R}[X]/(X^2 - X)$ durch $r \mapsto r$ $(= \overline{r})$, was die $\mathbb{R}$-Algebren-Struktur festlegt. Die skalare

Multiplikation ist also durch koeffizientenweise skalare Multiplikation gegeben.

Der Monoidring $\mathbb{R}[(\mathbb{Z}/2\mathbb{Z}, \cdot)]$ (mit Elementen der Form $c \cdot \overline{0} + d \cdot \overline{1}$) ist $\mathbb{R}$-Algebra wie wir dies in der Vorlesung gesehen haben: Die Ringstruktur ist klar, die Addition wird komponentenweise berechnet, die Multiplikation durch eine Faltungsformel, wie wir sie in Aufgabe 2 bereits gesehen haben - dort mit anderem Skalarbereich.
Die Einbettung von $\mathbb{R}$ geschieht durch $r \mapsto r \cdot \overline{1}$, denn $\overline{1}$ ist das Neutralelement des Monoids und in der Vorlesung haben wir gesehen, dass dies eine $\mathbb{R}$-Algebren-Struktur definiert, die wieder durch skalare Multiplikation der einzelnen Koeffizienten gegeben ist.

Schließlich müssen wir nur noch alles zusammenbringen, was wir gesehen haben und die richtige Bijektion finden:
Die Zuordnung $\varphi : aX + b \mapsto a \cdot \overline{0} + b \cdot \overline{1}$ ist offensichtlich eine bijektive Zuordnung von $\mathbb{R}[X]/(X^2 - X)$ nach $\mathbb{R}[(\mathbb{Z}/2\mathbb{Z}, \cdot)]$ und es reicht zu zeigen, dass dies ein Algebren-Homomorphismus ist.
Für beliebige $aX + b, cX + d \in \mathbb{R}[X]/(X^2 - X)$ gilt:
$\varphi((aX + b) + (cX + d)) = \varphi((a + c)X + (b + d)) = (a + c) \cdot \overline{0} + (b + d) \cdot \overline{1} = (a \cdot \overline{0} + b \cdot \overline{1}) + (c \cdot \overline{0} + d \cdot \overline{1}) = \varphi(aX + b) + \varphi(cX + d)$.
$\varphi((aX + b) \cdot (cX + d)) = \varphi((ac + ad + bc)X + bd) = (ac + ad + bc) \cdot \overline{0} + bd \cdot \overline{1} = (a \cdot \overline{0} + b \cdot \overline{1})(c \cdot \overline{0} + d \cdot \overline{1}) = \varphi(aX + b) \cdot \varphi(cX + d)$.
$\varphi(1) = \varphi(0X + 1) = 0 \cdot \overline{0} + 1 \cdot \overline{1} = 1$.
Also ist $\varphi$ ein Ringhomomorphismus und für alle $r \in R, aX + b \in \mathbb{R}[X]/(X^2 - X)$ gilt:
$\varphi(r \cdot (aX + b)) = \varphi(raX + rb) = ra \cdot \overline{0} + rb \cdot \overline{1} = r(a \cdot \overline{0} + b \cdot \overline{1}) = r\varphi(aX + b)$.

**Aufgabe 4**
Sei $R = \mathbb{Z}/2\mathbb{Z}[X]$. Finde alle Polynome $f \in R \setminus R^\times$ vom Grad $\leq 4$, die die folgende Eigenschaft erfüllen: Ist $f = gh$ das Produkt zweier Polynome $g, h \in R$, so ist $g \in R^\times$ oder $h \in R^\times$.[3]

**Lösung Aufgabe 4**
Die einzige Einheit im Polynomring ist $\overline{1}$, diese ist ausgeschlossen. Das Nullpolynom erfüllt die Bedingung nicht, lässt sich zum Beispiel als $\overline{0} = \overline{0} \cdot \overline{0}$ in Nicht-Einheiten zerlegen.
Ein Polynom vom Grad 1 muss unzerlegbar sein, denn einer der Faktoren einer Zerlegung muss Grad 1 haben. $X, X + \overline{1}$ sind unzerlegbar vom Grad 1.
Ein Polynom vom Grad 2 oder Grad 3 ist genau dann zerlegbar, wenn es eine Nullstelle hat, denn eine Zerlegung in Nichteinheiten muss ein Polynom vom Grad 1 enthalten:
Ein Polynom vom Grad 2 hat die Form $X^2 + aX + b$ und ist unzerlegbar, wenn es keine Nullstelle hat. Dies impliziert $b = \overline{1}$ (sonst wäre $\overline{0}$ eine Nullstelle) und dann $a = \overline{1}$ (sonst wäre $\overline{1}$ eine Nullstelle). Es gibt also genau ein unzerlegbares Polynom vom Grad 2: $X^2 + X + \overline{1}$.
Ein Polynom vom Grad 3 hat die Form $X^3 + aX^2 + bX + c$ und ist unzerlegbar, wenn es keine Nullstelle hat. Wieder muss $c = \overline{1}$ sein, damit $\overline{0}$ keine Nullstelle ist, und damit $\overline{1}$ keine Nullstelle ist, muss $a + b + c = \overline{0} \Rightarrow a + b = \overline{1}$ sein. Wir erhalten zwei unzerlegbare Polynome vom Grad 3: $X^3 + X^2 + \overline{1}$, $X^3 + X + \overline{1}$.

Schließlich suchen wir alle unzerlegbaren Polynome von Grad 4. Wieder ist sicher jedes Polynom zerlegbar, das eine Nullstelle hat. Desweiteren sind diejenigen Polynome zerlegbar, die in zwei Polynome vom Grad 2 zerfallen, wobei wir nur diejenigen betrachten müssen, die keine Nullstelle haben, denn die anderen haben wir ja bereits abgedeckt. Dass ein Polynom in zwei Polynome vom Grad 2 zerfällt, aber keine Nullstelle hat, bedeutet dabei gerade, dass die beiden Faktoren selbst unzerlegbar sind.
Ein Polynom $X^4 + aX^3 + bX^2 + cX + d$ hat keine Nullstelle, wenn $d = \overline{1}$ und zusätzlich $a + b + c = \overline{1}$ gelten. Davon gibt es 4 Stück. Vorher haben wir gesehen, dass es genau ein unzerlegbares Polynom vom Grad 2 gibt, also auch nur ein Polynom vom Grad 4, das in zwei unzerlegbare Polynome vom Grad 2 zerfällt: $X^2 + X + \overline{1}$ und dessen Produkt mit sich selbst ist $X^4 + X^2 + \overline{1}$.
Dieses Polynom müssen wir aus der Liste der Polynome ohne Nullstelle streichen und erhalten die drei unzerlegbaren Polynome $X^4 + X^3 + X^2 + X + \overline{1}, X^4 + X^3 + \overline{1}, X^4 + X + \overline{1}$.

[3] Wir suchen also Polynome, die sich nicht als Produkt von zwei Nichteinheiten schreiben lassen. Wir nennen solche Polynome *irreduzibel* oder *unzerlegbar* und werden in nächster Zeit einiges über diesen Begriff in beliebigen Ringen lernen. Im Fall von Polynomen lässt sich das aber gut ohne Vorwissen durchrechnen.