Übungsblatt 3: Ringe und Polynome

1. Integritätsringe

V 1.1. Zeigen Sie, dass jeder endliche Integritätsring ein Körper ist.

Lösungshinweise: — *Man betrachte die Linksmultiplikation $\lambda_a(x) = ax$ für ein $a \in R\backslash\{0\}$, wobei R ein endlicher Integritätsring ist. Aus $ax = ay$ folgt $a(x-y) = 0$. Da R nullteilerfrei ist, folgt $x = y$. Also ist λ_a injektiv. Da R endlich ist, ist λ_a auch surjektiv und damit existiert ein $b \in R$ mit $ab = 1$. Also ist R ein Divisionsring, und wegen der Kommutativität ein Körper.* —

S 1.2. (4 Punkte) Sei R ein Ring und $K \subset R$ ein Teilkörper. Zeigen Sie:

(a) Der Ring R ist auf natürliche Weise ein Vektorraum über K.

(b) Wir nehmen zusätzlich an, dass R ein Integritätsring mit $\dim_K R < \infty$ ist. Dann ist R ein Körper. *Zusatz:* Gilt das auch noch für $\dim_K R = \infty$?

Lösungshinweise: —

(a) *R ist nach Definition eine abelsche Gruppe bezüglich Addition, es gilt $1 \cdot r = r$ für $r \in R$ und die Assoziativ- und Distributivgesetze des Vektorraums folgen ebenso aus den Ringaxiomen. (Die Skalarmultiplikation ist natürlich gegeben durch die Linksmultiplikation $K \times R \to R : (k,r) \mapsto kr$.)*

(b) *Wenn die Dimension endlich ist, lässt sich die Linksmultiplikation mit $a \in R$ durch eine Matrix mit Einträgen in K darstellen. Wir haben schon in Aufgabe 1.1 gesehen, dass λ_a injektiv ist, wenn R ein Integritätsring ist. Aus der linearen Algebra wissen wir, dass die Abbildung dann auch surjektiv ist. Damit gibt es also ein $b \in R$ mit $ab = 1$. Da R nach Voraussetzung kommutativ ist, folgt, dass R ein Körper ist.*
Eine alternative Lösung ist die Folgende. Sei $a \in R^*$. Wir betrachten die Potenzen $1, a, a^2, \dots, a^n$ mit $n = \dim_K R$. Dies sind $n+1$ Elemente in einem n-dim. Vektorraum, also linear abhängig. Es gibt also $\mu_0, \dots, \mu_n$ mit $\mu_0 1 + \mu_1 a + \dots + \mu_n a^n = 0$. Sei k der kleinste Index, so dass $\mu_k \neq 0$. Dann gilt $a^k(\mu_k + \mu_{k+1}a^1 + \dots + \mu_n a^{n-k}) = 0$. Da R ein Integritätsring ist und $a \neq 0$, folgt $\mu_k + \mu_{k+1}a + \dots + \mu_n a^{n-k} = 0$. Nun kann man aber direkt zu $1 = a \cdot \frac{-1}{\mu_k}(\mu_{k+1} + \dots + \mu_n a^{n-k-1})$ auflösen, was die Invertierbarkeit von a beweist.
Als Gegenbsp. im Fall $\dim_K R = \infty$ betrachte man den Polynomring $K[X]$ über einem Körper K.

—

2. Lokalisation

Sei R ein kommutativer Ring und S ein Untermonoid von $(R,\cdot)$, also eine multiplikativ abgeschlossene Teilmenge von R, die die 1 enthält. Wir betrachten auf $R \times S$ die Relation

$$(r,s) \sim (r',s') \quad \Leftrightarrow \quad \exists\, \overline{s} \in S :\ \overline{s}(rs' - r's) = 0$$

V 2.1. (a) Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist und die Verknüpfungen

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \quad \text{und} \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

wohldefiniert sind, wenn wir mit $\frac{r}{s}$ die Äquivalenzklasse des Elements (r,s) bezüglich der Relation $\sim$ bezeichnen.

(b) Folgern Sie, dass die Menge $S^{-1}R$ der Äquivalenzklassen damit zu einem kommutativen Ring wird. Warum ist dies eine Verallgemeinerung der Konstruktion des Bruchkörpers aus der Vorlesung?

(c) Betrachten Sie $R = \mathbb{Z}/6$ mit $S_1 = \{\overline{1}, \overline{3}\}$, $S_2 = R^\times$ und $S_3 = R$. Wieviele Elemente hat $S_i^{-1}R$ für $i \in \{1,2,3\}$? Gibt es noch andere multiplikativ abgeschlossene Mengen in $\mathbb{Z}/6$?

Lösungshinweise: —

(a) *Die Reflexivität und Symmetrie sind klar. Zur Transitivität betrachte $(r,s) \sim (r',s')$ und $(r',s') \sim (r'',s'')$. Daraus folgt, dass $\bar{s}, \hat{s} \in S$ existieren, so dass $\bar{s}(rs' - r's) = 0$ und $\hat{s}(r's'' - r''s') = 0$ gilt. Es gilt nun $\bar{s}\hat{s}s'(rs'' - r''s) = \bar{s}\hat{s}(s''(rs' - r's) + s(r's'' - r''s')) = 0$. Also gilt $(r,s) \sim (r'',s'')$, weil $\bar{s}\hat{s}s \in S$.*
Zur Wohldefiniertheit der Addition betrachte $(r_1,s_1) \sim (r_2,s_2)$ (mit $\bar{s}$) und $(r_1',s_1') \sim (r_2',s_2')$ (mit $\hat{s}$). Zu zeigen ist, dass $(r_1s_1' + r_1's_1, s_1s_1') \sim (r_2s_2' + r_2's_2, s_2s_2')$. Es gilt $\bar{s}\hat{s}((r_1s_1' + r_1's_1)s_2s_2' - (r_2s_2' + r_2's_2)s_1s_1') = \bar{s}\hat{s}s_1's_2'(r_1s_2 - r_2s_1) + \bar{s}\hat{s}s_1s_2(r_1's_2' - r_2's_1') = 0$, was zu zeigen war.
Für die Wohldefiniertheit der Multiplikation müssen wir $(r_1r_1', s_1s_1') \sim (r_2r_2', s_2s_2')$ zeigen. Es gilt hier $\bar{s}\hat{s}(r_1r_1's_2s_2' - r_2r_2's_1s_1') = \bar{s}\hat{s}(r_1s_2 - r_2s_1)r_1's_2' + \bar{s}\hat{s}(r_1's_2' - r_2's_1')r_2s_1 = 0$. Damit ist alles gezeigt.

(b) *Hier muss man die Ringaxiome nachrechnen. Die Assoziativität, Kommutativität und Distributivität rechnet man direkt nach. Das Nullelement ist $\frac{0}{1}$ und die Eins ist gegeben durch $\frac{1}{1}$.*
Wählt man $S = R^*$ in einem Integritätsring R, so ergibt sich die Konstruktion des Bruchkörpers, da man dann das $\bar{s}$ in der Definition von $\sim$ kürzen kann.

(c) *Im Fall S_3 können wir stets $\bar{s} = 0$ wählen, so dass alle Brüche zueinander äquivalent sind. Damit wird $S_3^{-1}R$ der Nullring. Im Fall $S_2 = \{1,-1\}$ kann man jeden Bruch in die Form $\frac{r}{1}$ bringen, indem man gegebenenfalls mit -1 erweitert. Aus den Aufgaben 2.2 und 2.3 folgt dann $R \cong S_2^{-1}R$. Der interessanteste Fall ist $S_1 = \{1,3\}$. Wir bekommen also zuerst 12 Brüche der Form $\frac{r}{1}$ und $\frac{r}{3}$. Manche davon sind aber zueinander äquivalent. Man rechnet direkt nach, dass alle Brüche, die einen geraden Zähler haben zur 0 äquivalent sind. Ebenso prüft man nach, dass alle Brüche, deren Zähler sich um eine gerade Zahl unterscheiden, äquivalent sind. Damit hat $S_1^{-1}R$ höchstens zwei Elemente. Aber $(0,1)$ ist nicht äquivalent zu $(1,1)$, also sind es genau zwei Elemente.*
Andere multiplikativ abgeschlossene Teilmengen von $\mathbb{Z}/6$ sind $\{1,2,-2\}, \{1\}, \{0,1\}, \{1,-2\}, \{1,3,-2,0\}, \{1,2,3,-2,0\}, \{1,-1,2,-2\}, \{1,2,3,-2,0\}, \ldots$ usw.

—

S 2.2. (2 Punkte) Zeigen Sie, dass die Abbildung $R \to S^{-1}R : r \mapsto \frac{r}{1}$ genau dann injektiv ist, wenn $S \subset R^*$ keine Nullteiler von R enthält.

Lösungshinweise: — *Wenn S einen Nullteiler s_1 enthält, so dass $s_1r_1 = 0$ für ein $r_1 \in R^*$, dann ist $\frac{r_1}{1} \sim \frac{0}{1}$ und die Abbildung damit nicht injektiv. Enthält S keine Nullteiler, so folgt aus $\bar{s}(r1 - r'1) = 0$, dass $r - r' = 0$, die Abbildung ist also injektiv.* —

V 2.3. Zeigen Sie, dass die Abbildung $R \to S^{-1}R : r \mapsto \frac{r}{1}$ surjektiv ist, wenn $S \subset R^\times$.

Lösungshinweise: — *Sei $\frac{r}{s} \in S^{-1}R$. Dann gibt es wegen $S \subset R^\times$ ein Inverses $s^{-1} \in R$. Dann sind aber $\frac{r}{s}$ und $\frac{rs^{-1}}{1}$ äquivalent, wie man sofort nachrechnet. Also liegt $\frac{r}{s}$ im Bild der betrachteten Abbildung.* —

3. Polynomringe

V 3.1. $P \in \mathbb{Z}[X]$ hat keine Nullstellen in $\mathbb{Z}$ wenn $P(0)$ und $P(1)$ ungerade sind.

Lösungshinweise: — *Wenn ein Polynom $p \in \mathbb{Z}[X]$ eine Nullstelle in $\mathbb{Z}$ hat, dann auch eine in $\mathbb{Z}/2$, da die Abbildung $\mathbb{Z}[X] \to \mathbb{Z}/2[X] : p \mapsto p$ ein Ringhomomorphismus ist. Nach Voraussetzung hat p keine Nullstelle in $\mathbb{Z}/2$, also damit auch keine in $\mathbb{Z}$.* —

V 3.2. Man bestimme die Gruppe $\mathbb{Z}/4[X]^\times$ der invertierbaren Elemente in $\mathbb{Z}/4[X]$.

Lösungshinweise: — *Wir betrachten den Ringhomomorphismus $\varphi : \mathbb{Z}/4[X] \to \mathbb{Z}/2[X] : p \mapsto p$. Einheiten werden von einem Ringhomomorphismus auf Einheiten abgebildet. Da $\mathbb{Z}/2$ ein Körper ist, sind die Einheiten in $\mathbb{Z}/2[X]$ nur die invertierbaren Körperelemente, also $\mathbb{Z}/2[X]^\times = \{1\}$. Damit ist die Menge $\mathbb{Z}/4[X]^\times$ in der Menge $\varphi^{-1}(1) = \{p = \pm 1 + 2u : u \in \mathbb{Z}/4[X]\}$ enthalten. Andererseits sieht man direkt, dass alle Elemente in der obigen Menge selbstinvers und damit invertierbar sind.* —

S 3.3. (3 Punkte) Sei $\mathbb{F}_4 := (\mathbb{Z}/2[X])/(X^2+X+1)$.

(a) Bestimmen Sie die Anzahl der Elemente von $\mathbb{F}_4$ und zählen sie diese auf.

(b) Erstellen Sie die Additions- und Multiplikationstafeln von $\mathbb{F}_4$.

(c) Ist der Quotientenring $\mathbb{F}_4$ ein Körper?

Lösungshinweise: —

(a) *In $\mathbb{F}_4$ gilt die Gleichung $X^2 = X+1$. Damit kann jedes Polynom auf ein lineares Polynom reduziert werden. Es bleiben also die Restklassen der Elemente $0, 1, X$ und $X+1$. Diese sind alle verschieden, denn aus der Gleicheit von zwei dieser Elemente würde folgen, dass ein Vielfaches von X^2+X+1 gleich einem linearen Polynom in $\mathbb{Z}/2[X]$ ist, was nach Definition des Polynomringes nicht der Fall ist. (Benutze z.B. die Gradfunkton).*

(b) *Die Tabellen:*

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

·	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

(c) *Man muss nur nachprüfen, ob jedes Element ungleich 0 ein multiplikatives Inverses besitzt. Dies sieht man aber sofort aus der Verknüpfungtafel.*

—

4. Polynomielle Abbildungen

Sei $K[X]$ der Polynomring über dem Körper K.

Für $p = \sum_{k=0}^{n} a_k X^k$ sei die Abbildung $f_p : K \to K$ durch $x \mapsto p(x) = \sum_{k=0}^{n} a_k x^k$ gegeben.

4.1. Die Abbildung $\varphi : K[X] \to K^K : p \mapsto f_p$ ist ein Ringhomorphismus.

Lösungshinweise: — *Man muss prüfen, dass $f_{p+q} = f_p + f_q, f_{pq} = f_p f_q$ und $f_1 = 1$ gilt. Diese folgen aber direkt aus den Definitionen der Addition und Multiplikation von Abbildungen. Z.B. $f_{pq}(x) = (pq)(x) = p(x)q(x) = f_p(x)f_q(x) = (f_p f_q)(x)$.* —

V 4.2. Wenn K unendlich viele Elemente hat, dann ist φ injektiv, aber nicht surjektiv.

Lösungshinweise: — *Um die Injekivität zu zeigen, reicht es den Kern der Abbildung zu betrachten. Sei also $f_p = 0$ für ein $p \in K[X]$. Das bedeutet aber, dass p unendlich viele Nullstellen besitzt. Dies kann aber über einem Körper K nur dann sein, wenn $p = 0$.*

Um zu zeigen, dass nicht jede Abbildung in K^K eine polynomielle Abbildung ist, betrachtet man die Abbildung δ, die bei 0 den Wert 1 annimmt und sonst 0 ist. Diese ist nicht durch ein Polynom darstellbar, da sie unendlich viele Nullstellen hat, aber nicht die Nullfunktion ist.

Eine andere Beaobachtung ist, dass die Menge $K[X]$ die Kardinalität $|K|$ besitzt, während die Kardinalität $|K^K|$ mindestens die der Potenzmenge $2^{|K|}$ ist. Damit kann es keine Surjektion geben.

—

V 4.3. Wenn K endlich ist, dann ist φ surjektiv, aber nicht injektiv.

Lösungshinweise: — *Dass die Abbildung nicht injektiv ist, sieht man schon daran, dass K^K endlich ist und $K[X]$ unendlich viele Elemente besitzt. Man kann aber auch konkret das Polynom $p = \prod_{k\in K}(X-k)$ als Beispiel für ein Polynom im Kern benutzen.*
Um die Surjektivität zu sehen, zeigen wir, dass wir eine Basis von K^K erhalten können. Eine solche ist gegeben durch die Menge der Abbildungen $\{\delta_a : a \in K\}$. Dabei ist δ_a definiert als die Abbildung, die bei a den Wert 1 annimmt und sonst 0 ist. Wir betrachten dazu zuerst $p_a = \prod_{k\in K\setminus a}(X-k)$. Die zugehörige Abbidung ist 0 außerhalb von a und es gilt $p_a(a) \neq 0$, da K ein Körper ist. Damit wird dann $\delta_a = \frac{p_a}{p_a(a)}$, also durch ein Polynom darstellbar. —

5. Charakterisierung des Polynomrings über einem Körper

5.1. Ist $R = K[X]$ der Polynomring über einem Körper K, dann definiert der Grad eine surjektive Abbildung $\nu\colon R \to \mathbb{N}\cup\{-\infty\}$, die folgende Eigenschaften erfüllt:
(1) Für $a,b \in R$ mit $b \neq 0$ existieren $c,d \in R$ so dass $a = bc+d$ mit $\nu(d) < \nu(b)$.
(2) Für alle $a,b \in R$ gilt $\nu(ab) = \nu(a)+\nu(b)$ und $\nu(a+b) \leq \sup\{\nu(a),\nu(b)\}$ mit Gleichheit wenn $\nu(a) \neq \nu(b)$.

Lösungshinweise: — *Die Gradabbildung ist surjektiv, weil* $\deg(0) = -\infty$ *und* $\deg(X^n) = n$ *nach Definition. Die Eigenschaft (1) wird im Skript bewiesen und die Eigenschaft (2) folgt aus der Definition der Gradfunktion zusammen mit Rechenregeln für Polynomaddition und -multiplikation.* —

V 5.2. Sei R ein kommutativer Ring mit einer surjektiven Abbildung $\nu\colon R \to \mathbb{N}\cup\{-\infty\}$, die obige Eigenschaften (1) und (2) erfüllt.
(a) Man zeige $\nu(a) = -\infty \Leftrightarrow a = 0$ und $\nu(a) = 0 \Leftrightarrow a \in R^\times$.
(b) Man zeige, dass $K = \{\, a \in R \mid \nu(a) \leq 0 \,\}$ ein Unterkörper von R ist.
(c) Für $X \in R$ mit $\nu(X) = 1$ ist $R = K[X]$ der Polynomring in X und $\nu = \deg$.

Lösungshinweise: —

(a) *Wegen der Surjektivität gibt es ein $b \in R$ mit $\nu(b) = 1$. Dann gilt aber $\nu(0) = \nu(0b) = \nu(0)+\nu(b) = \nu(0)+1$. Dies geht nur, falls $\nu(a) = -\infty$. Ist andererseits $a \neq 0$, dann kann man b durch a mit Rest teilen und erhält $b = ac+d$ mit $\nu(d) < \nu(a)$. Damit ist $\nu(a) \neq -\infty$.*
Wenn $\nu(a) = 0$ gilt, so folgt $a \neq 0$ aus dem Obigen und man teile die 1 durch a mit Rest. Es ergibt sich $1 = ac+d$ mit $\nu(d) < \nu(a) = 0$, also $d = 0$. Damit ist aber a invertierbar.
Als nächstes bestimmen wir $\nu(1)$. Es gilt $\nu(b) = \nu(1b) = \nu(1)+\nu(b)$ für alle $b \in R$. Wählt man ein b mit $\nu(b) \neq -\infty$, so folgt $\nu(1) = 0$.
Ist nun a invertierbar, so gilt $0 = \nu(1) = \nu(ba) = \nu(b)+\nu(a)$ für ein $b \in R$. Diese Gleichung kann aber nur für $\nu(b) = \nu(a) = 0$ erfüllt sein.

(b) *Nach Teil (a) gilt $K = R^\times \cup \{0\}$. Damit ist die Menge multiplikativ abgeschlossen und die Nichtnullelemente besitzen multiplikative Inverse in K. Die Assoziativ-, Kommutativ und Distributivgesetze vererben sich von R. Aus der Gleichung $\nu(a+b) \leq \sup\{\nu(a),\nu(b)\}$ folgt sofort, dass Summen von Elementen aus K wieder in K enthalten sind. Negative Einheiten sind auch Einheiten und $-0 = 0$. Damit ist alles gezeigt.*

(c) *Sei ein $X \in R$ mit $\nu(X) = 1$ gegeben. Dann folgt mit Induktion aus $\nu(ab) = \nu(a)+\nu(b)$ die Gleichung $\nu(X^n) = n$ und aus $\nu(a+b) \leq \sup\{\nu(a),\nu(b)\}$ bekommen wir $\nu(p) \leq n$ für $p = \sum_{k=0}^n a_k X^k$ für $a_k \in K$. Wenn $a_n \neq 0$ ist, so folgt $\nu(p) = n$, da wir das Polynom zuerst mit a_n^{-1} multiplizieren können ohne den Grad zu verändern. Sei also o.B.d.A. $p = X^n+q$ mit $\nu(q) \leq n-1$. Dann gilt $n = \nu(p-q) \leq \sup\{\nu(p),\nu(-q)\} \leq n$. Also $\nu(p) = n$. Die ν-Funktion entspricht also auf $K[X]$ der Gradfunktion* deg. *Aber ist $K[X]$ überhaupt ein Polynomring und gilt $R \subset K[X]$? Dazu müssen wir zeigen, dass die Darstellung $p = \sum_{k=0}^n a_k X^k$ von Elementen aus $K[X]$ eindeutig ist und jeder Element $r \in R$ sich auch so darstellen lässt.*
Sei also $p = \sum_{k=0}^n a_k X^k = \sum_{k=0}^n b_k X^k$, bzw. $\sum_{k=0}^n (a_k - b_k)X^k = 0$. Wähle k maximal, so dass $a_k - b_k \neq 0$. Dann ist $-\infty = \nu(0) = k$, ein Widerspruch. Die Darstellung ist also eindeutig. Sei nun

$r \in R$ gegeben. Wenn $r \notin K$ (sonst sind wir fertig), teile r durch X mit Rest: $r = cX + d$ und $\nu(d) < \nu(X) = 1$. Damit ist also $d \in K$. Es folgt, dass $n = \nu(r) = \nu(cX+d) \leq \sup\{\nu(cX), \nu(d)\} = \sup\{\nu(c)+1, 0\} = \nu(c)+1$, da $c \neq 0$ (sonst wäre $r \in K$ gewesen). Ebenso ist $\nu(c)+1 = \nu(cX) = \nu(r-d) \leq \sup\{\nu(r), \nu(-d)\} \leq n$. Damit ist also $\nu(c) = n-1$ und man kann induktiv verfahren. Wenn c als Polynom in $K[X]$ darstellbar ist, dann auch $r = cX + d$.

—

6. GRUPPENRINGE

S 6.1. (2 Punkte) Sei R ein Integritätsring und G eine Gruppe. Wenn es ein Element $g \in G$ endlicher Ordnung gibt, also $g \neq 1$ aber $g^n = 1$ für ein $n \geq 1$, dann hat der Gruppenring $R[G]$ Nullteiler. *Hinweis:* endliche geometrische Reihe.

Eine berühmte Vermutung von Kaplansky fragt nach der Umkehrung: Wenn eine Gruppe G keine Elemente endlicher Ordnung hat, dann hat der Gruppenring $R[G]$ keine Nullteiler. Diese Vermutung ist bis heute offen.

Lösungshinweise: — *Die Gleichung $g^n = 1$ kann im Gruppenring zu $g^n - 1 = 0$ umgeschrieben werden. Dies zerfällt in $(g-1)(g^{n-1} + \ldots + g + 1)$. Daraus folgt sofort, dass $g-1$ ein Nullteiler in $R[G]$ ist, wenn wir zeigen können, dass die beiden auftretenden Faktoren nicht 0 sind. Dies ist nicht von vornherein klar, denn $g^5 + g^4 + g^3 + g^2 + g + 1$ ist 0 für $R = \mathbb{Z}/_2$ und $g^3 = 1$ (also auch $g^6 = 1$).*
Da $g \neq 1$ vorausgesetzt war, wissen wir zumindest, dass $g - 1 \neq 0$. Das Element $f := g^{n-1} + \ldots + g + 1$ ist aber nur dann ungleich 0, wenn wir am Anfang unser n minimal wählen. Dann wissen wir, dass die auftretenden Summanden g^i $(0 \leq i < n)$ alle verschieden sind (aus $g^i = g^j$ folgt $g^{j-i} = 1$ und aus der Minimalität von n dann $i = j$) und f nach Definition von $R[G]$ nicht 0 sein kann. —

7. POTENZREIHENRINGE

Wir sagen in einem Monoid $(M, \cdot)$ gilt *endliche Zerlegbarkeit* wenn zu jedem $m \in M$ nur endlich viele Paare $(a,b) \in M \times M$ existieren, die $ab = m$ erfüllen Dies gilt zum Beispiel für $(\mathbb{N}, +)$ und $(\mathbb{N}^d, +)$, nicht aber für $(\mathbb{Z}, +)$ und $(\mathbb{Q}_{\geq 0}, +)$.

V 7.1. Sei R ein kommutativer Ring und M ein Monoid, in dem endliche Zerlegbarkeit gilt. Auf der Menge $S = R^M$ aller Abbildungen definieren wir Summe und Produkt wie im Skript angegeben. Man weise nach, dass $(S, +, \cdot)$ ein Ring ist. Der Ring S ist genau dann kommutativ wenn das Monoid M kommutativ ist.

Lösungshinweise: — *Die Lösung dieser Aufgabe erfordert Ausdauer und Sicherheit im Umgang mit den Definitionen. Sonst ist es aber nichts weiter als eine längere Rechnung. (Man beachte, dass die Ringgesetze im Zusammenhang mit der Addition erfüllt sind, da wir die Addition wie immer definieren. Nur die Multiplikation ist als Faltungsprodukt nicht trivialerweise assoziativ, distributiv und hat ein Einselement.) Durch die endliche Zerlegbarkeit bekommt man bei der Faltung keine Probleme mit unendlichen Summen. Man vergleiche auch mit entsprechenden Rechnungen im Skript.* —

Für das Monoid $(\mathbb{N}, +)$ betrachten wir Abbildungen $f\colon \mathbb{N} \to R$. Wir stellen uns f vor als eine unendliche Summe $\sum_{k=0}^{\infty} f_k X^k$. Hier hat das Summenzeichen $\sum$ nur einen symbolischen Sinn: algebraisch können wir nur Summen für endlich viele Terme definieren.

Für Summe und Produkt gilt in dieser Schreibweise

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) + \Big(\sum_{k=0}^{\infty} g_k X^k\Big) = \sum_{k=0}^{\infty} (f_k + g_k) X^k$$

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) \cdot \Big(\sum_{\ell=0}^{\infty} g_\ell X^\ell\Big) = \sum_{n=0}^{\infty} \Big(\sum_{k+\ell=n} f_k g_\ell\Big) X^n$$

Den so entstehenden Ring $R[[X]]$ nennt man den Ring der *Potenzreihen* über R. Zur Betonung spricht man von *formalen Potenzreihen*, denn anders als in der Analysis umgehen wir hier alle Fragen der Konvergenz: Diese Potenzreihen sind nur formale Ausdrücke und beschreiben nicht etwa Funktionen. Wichtig ist allein, dass sie einen Ring bilden.

V 7.2. Man bestimme die invertierbaren Elemente in $R[[X]]$.
Wenn R ein Integritätsring ist, ist dann auch $R[[X]]$ ein Integritätsring?
Für jedes $n \in \mathbb{N}$ ist $\mathfrak{m}^n = \{ \sum_{k=n}^{\infty} f_k X^k \mid f_k \in R\}$ ein Ideal in $R[[X]]$.
Ist R ein Körper, so sind $\mathfrak{m}^0, \mathfrak{m}^1, \mathfrak{m}^2, \ldots, \{0\}$ die einzigen Ideale des Rings $R[[X]]$.

Lösungshinweise: — *Die invertierbaren Elemente in $R[[X]]$ sind diejenigen, von der Form $a+Xu$ mit $a \in R^\times, u \in R[[X]]$. Multiplizieren wir diese mit a^{-1}, reicht es Elemente der Form $1+Xu$ zu invertieren. Man kann das Inverse aber direkt hinschreiben: $1 - Xu + X^2u^2 - X^3u^3 \pm \ldots$ (geometrische Reihe). Dies beschreibt wirklich ein Element aus $R[[X]]$, da vor den späteren Termen in der Summe immer höhere X-Potenzen stehen. Damit wird ab dem Term $X^k u^k$ der Wert der Summe an den Potenzen $X^0, \ldots, X^k$ nicht mehr verändern und "konvergiert" in diesem Sinne.*

Wenn a nicht invertierbar ist, dann ist $a+Xu$ ebenfalls nicht invertierbar. Denn ein Inverses müsste die Form $b+Xv$ besitzen und die Multiplikation der beiden Terme zeigt, dass dann $ab = 1$ sein müsste.

Wir können jedes Element in $R[[X]]^*$ in der Form $X^k(a+Xu)$ mit $a \neq 0, u \in R[[X]]$ und einem $k \in \mathbb{N}_0$ schreiben. Multiplizieren wir das mit einem anderen Element $X^l(b+Xv) \in R[[X]]^*$, so ergibt dies $X^{k+l}(ab + X(u+v) + X^2uv)$ Dies kann nur für $ab = 0$ verschwinden. Wenn R ein Integritätsring ist, ist also auch $R[[X]]$ ein Integritätsring.

Die Idealeigenschaften von $\mathfrak{m}^n$ rechnet man direkt nach.

Wir müssen also nur noch zeigen, dass im Fall eines Körpers R jedes Ideal I ungleich 0 so aussieht. Sei $X^k(a+Xu)$ ein Element in I mit minimalem k und $a \neq 0$. Das Element $a+Xu$ ist invertierbar und somit liegt auch X^k im Ideal I. Also ist $\mathfrak{m}^k \subset I$. Andererseits ist auch $I \subset \mathfrak{m}^k$, denn sei $X^l(b+Xv) \in I$ mit $b \neq 0$, so ist $l \geq k$ (wegen Minimalität) und somit ist das Element in $\mathfrak{m}^k$ enthalten. —