Übungsblatt 4

Durchweg sei R ein kommutativer Ring mit 1.

Aufgabe 1. Zeigen Sie:

1. Ist R ein Integritätsbereich, so auch der Polynomring $R[X]$.
2. In diesem Fall ist die Einheitengruppe $R[X]^*$ von $R[X]$ isomorph zu R^*.

Beweis. 1. Seien $f, g \in R[\![X]\!] \setminus \{0\}$ mit $f(X) = \sum_{i=0}^{n} a_i X^i$, $g(X) = \sum_{i=0}^{m} b_i X^i$, $m, n \in \mathbb{N}_0$, $a_n \neq 0 \neq b_m$ und $fg = 0$, so gilt

$$0 = f(X)g(X) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k,$$

wobei $a_i = b_j = 0$ für $i > n, j > m$. Insbesondere gilt

$$0 = \sum_{i=0}^{n+m} a_i b_{n+m-i} = \left(\sum_{i=0}^{n-1} a_i \underbrace{b_{n+m-i}}_{=0} \right) + a_n b_m + \left(\sum_{i=n+1}^{k} \underbrace{a_i}_{=0} b_{n+m-i} \right) = a_n b_m.$$

Da R ein Integritätsbereich ist und $a_n \neq 0 \neq b_m$ gilt, folgt $a_n b_m \neq 0$, ein Widerspruch.

2.

Lemma 0.1. *Seien $f, g \in R[X]$, so gilt $deg(fg) = deg(f) + deg(g)$.*

Beweis. Seien $f, g \in R[\![X]\!]$ mit $f(X) = \sum_{i=0}^{n} a_i X^i$, $g(X) = \sum_{i=0}^{m} b_i X^i$ und $m, n \in \mathbb{N}_0$. Für $f = 0$ oder $g = 0$ ist die Aussage offensichtlich korrekt. Seien also $f \neq 0 \neq g$ und $a_n \neq 0 \neq b_m$, so gilt

$$\begin{aligned} f(X)g(X) &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k \\ &= \left(\sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k \right) + \left(\sum_{k=n+m+1}^{\infty} \left(\sum_{i=0}^{k} \underbrace{a_i b_{k-i}}_{=0} \right) X^k \right) \\ &= \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k. \end{aligned}$$

Es gilt also $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Sei $f \in R[X]^*$, so existiert ein eindeutiges $g \in R[X]$ mit $fg = 1$. Somit folgt mit dem obigen Lemma

$$0 = \deg(fg) = \deg(f) + \deg(g),$$

d.h. $\deg(f) = 0 = \deg(g)$. Somit können wir f eindeutig einem Element aus R^* identifizieren. Sei andersherum $f \in R^*$, so fasse f als (konstantes) Polynom auf, welches offensichtlich invertierbar in $R[X]$ ist. Diese beiden Identifikationen sind zueinander inverse Ringhomomorphismen, sodass insbesondere gilt $R^* \cong R[X]^*$.

□

Aufgabe 2. Setze $L = \left\{ \sum_{i=0}^{\infty} a_i X^i \in R[X] \mid a_1 = 0 \right\}$.

1. Zeigen Sie, dass L ein Unterring von $R[X]$ ist, jedoch nicht ein Ideal in $R[X]$.
2. Zeigen Sie, dass L isomorph ist zum Faktorring $R[X][Y]/(X^2 - Y^3)$.

Beweis. 1. Offensichtlich ist L eine additive Untergruppe von $R[X]$. Es bleibt also nur noch die Abgeschlossenheit bezüglich der Multiplikation zu zeigen. Seien hierfür $f, g \in L$ mit $f(X) = \sum_{i=0}^{n} a_i X^i$, $g(X) = \sum_{i=0}^{m} b_i X^i$, so gilt

$$f(X)g(X) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k.$$

Da $f, g \in L$ folgt mit $k = 1$

$$\sum_{i=0}^{1} a_i b_{1-i} = a_0 b_1 + a_1 b_0 = 0,$$

d.h. $fg \in L$.
Die Menge L ist kein Ideal, denn mit $1 \in L$ und $X \notin L$ gilt $1 \cdot X = X \notin L$.

2. Betrachte die Zuordnung

$$\phi : R[X][Y] \to L; \sum_{(i,j) \in I} a_{ij} X^i Y^j \mapsto \sum_{(i,j) \in I} a_{ij} X^{3i+2j},$$

wobei $I \subseteq \mathbb{N}_0^2$ endlich ist. Wir zeigen im Folgenden, dass ϕ ein Ringepimorphismus mit $\ker(\phi) = (X^2 - Y^3)$ ist.
Zunächst stellen wir fest, dass $\{3i + 2j \mid i, j \in N_0\} = \mathbb{N}_0 \setminus \{1\}$ gilt.
Aus vorherigem folgt wegen $1 \notin \{3i + 2j \mid i, j \in N_0\}$ die Wohldefiniertheit von ϕ, denn sei $p(X, Y) = \sum_{(i,j) \in I} a_{ij} X^i Y^j \in R[X][Y]$, so gilt

$$\phi(p)(X) = \sum_{(i,j) \in I} a_{ij} X^{3i+2j}$$

und somit ist $\phi(p) \in L$. Da ϕ die R–lineare Fortsetzung der Zuordnung $X^i Y^j \mapsto X^{3i+2j}$ ist, ist ϕ ein Gruppenhomomorphismus von $(R[X][Y], +)$ nach $(L, +)$. Seien $f, g \in R[X][Y]$ mit $f(X, Y) = \sum_{(i,j) \in I} a_{ij} X^i Y^j$, $g(X, Y) = X^k Y^l$, so gilt

$$\begin{aligned}
\phi(fg)(X) &= \phi\left(\sum_{(i,j) \in I} a_{ij} X^{i+k} Y^{j+l} \right) \\
&= \sum_{(i,j) \in I} a_{ij} X^{3(i+k)+2(j+l)} \\
&= \left(\sum_{(i,j) \in I} a_{ij} X^{3i+2j} \right) X^{3k+2l} \\
&= \phi(f)\phi(g)(X).
\end{aligned}$$

Wegen der R–Linearität von ϕ gilt die obige Gleichung auch für beliebige $g \in R[X][Y]$. Insgesamt erhalten wir, dass ϕ ein Ringhomomorphismus ist.
Um die Surjektivität zu beweisen, reicht es wegen der R–Linearität von ϕ aus zu zeigen, dass

$$\left\{ X^k \mid k \in \mathbb{N}_0 \setminus \{1\} \right\} \subseteq \mathrm{Im}(\phi)$$

gilt. Dies folgt aus der Tatsache $\{3i + 2j \mid i,j \in N_0\} = \mathbb{N}_0 \setminus \{1\}$, denn sei $k \in \mathbb{N}_0 \setminus \{1\}$, so existieren $i,j \in \mathbb{N}_0$ mit $3i + 2j = k$ und somit $\phi(X^i Y^j) = X^{3i+2j} = X^k \in \operatorname{Im}(\phi)$.
Als nächstes berechnen wir den Kern von ϕ. Zunächst gilt offensichtlich, dass $\phi(X^2 - Y^3) = X^6 - X^6 = 0$, d.h. $\left(X^2 - Y^3\right) \subseteq \ker(\phi)$. (Ein kürzerer Beweis der folgenden Tatsache wird unten in der Bemerkung gegeben.)
Sei nun $p \in R[X][Y]$ mit $p(X,Y) = \sum_{(i,j)\in I} a_{ij} X^i Y^j$ und $\phi(p) = 0$. So gilt $\phi(p)(X) = \sum_{(i,j)\in I} a_{ij} X^{3i+2j} = 0$.Wir sortieren die Summe um und fassen Summanden zusammen, indem wir die folgende Partition von I einführen. Sei $I = \dot{\bigcup}_{k\in\mathbb{N}_0} I_k$ mit $I_k := \{(i,j) \in I \mid 3i + 2j = k\}$, so gilt

$$0 = \phi(p)(X) = \sum_{k\in\mathbb{N}_0} \left(\sum_{(i,j)\in I_k} a_{ij} \right) X^k$$

und damit

$$\sum_{(i,j)\in I_k} a_{ij} = 0$$

für alle $k \in \mathbb{N}_0$. Wir werden zeigen, dass $\sum_{(i,j)\in I_k} a_{ij} X^i Y^j \in (X^2 - Y^3)$ für alle $k \in \mathbb{N}_0$ und damit gilt auch $p \in (X^2 - Y^3)$. Fixiere also ein $k \in \mathbb{N}_0$ mit $|I_k| =: n \in \mathbb{N}$, denn für $n = 0$ gilt $\sum_{(i,j)\in I_k} a_{ij} X^i Y^j = 0 \in (X^2 - Y^3)$. Wegen

$$\begin{aligned} 0 &= \sum_{(i,j)\in I_k} a_{ij} \\ \Leftrightarrow a_{l,m} &= -\sum_{(i,j)\in I_k \setminus \{(l,m)\}} a_{ij} \end{aligned}$$

für ein fixiertes $(l,m) \in I_k \neq \varnothing$ erhalten wir

$$\sum_{(i,j)\in I_k} a_{ij} X^i Y^j = \sum_{(i,j)\in I_k \setminus \{(l,m)\}} \left(a_{ij} X^i Y^j - a_{ij} X^l Y^m \right).$$

Betrachte die Summanden $a_{ij} X^i Y^j - a_{ij} X^l Y^m$. Wegen $3i + 2j = 3l + 2m$ gilt $i = l$ genau dann, wenn $j = m$. Ist $i = l$, so gilt $a_{ij} X^i Y^j - a_{ij} X^l Y^m = 0 \in (X^2 - Y^3)$. Nehme also o.E. an, dass $i > l$, so gilt auch $m > j$. Somit erhalten wir

$$a_{ij} X^i Y^j - a_{ij} X^l Y^m = a_{ij} X^l Y^j \left(X^{i-l} - Y^{m-j} \right).$$

Da $3(i - l) + 2(j - m) = 0$ nur die ganzzahligen Lösungen der Form $i - l = 2\alpha$ und $j - m = -3\alpha$ mit $\alpha \in \mathbb{Z}$ besitzt, wobei wir hier nur positive α betrachten, gilt

$$a_{ij} X^i Y^j - a_{ij} X^l Y^m = a_{ij} X^l Y^j \left((X^2)^\alpha - (Y^3)^\alpha \right).$$

Wegen $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$ für beliebige $a, b \in R$ erhalten wir

$$\begin{aligned} a_{ij} X^i Y^j - a_{ij} X^l Y^m &= a_{ij} X^l Y^j \left((X^2)^\alpha - (Y^3)^\alpha \right) \\ &= a_{ij} X^l Y^j (X^2 - Y^3) \cdot \\ &\quad (X^{2(\alpha-1)} + X^{2(\alpha-2)} Y^3 + \ldots + + X^2 Y^{3(\alpha-2)} + Y^{3(\alpha-1)}) \in (X^2 - Y^3). \end{aligned}$$

Insgesamt gilt also $p \in (X^2 - Y^3)$.
Da ϕ ein surjektiver Ringhomomorphismus mit $\ker(\phi) = \left(X^2 - Y^3\right)$ ist, liefert der Homomorphiesatz $R[X][Y]/\left(X^2 - Y^3\right) \cong L$.

□

Bemerkung 0.2. *Alternativ und insbesondere eleganter kann man die Aussage* $\ker(\phi) \subseteq (X^2 - Y^3)$ *wie folgt zeigen.*
Zunächst stellen wir fest, dass $X^m Y^n = (X^2 - Y^3) X^{m-2} Y^n + X^{m-2} Y^{n+3}$ *für* $n, m \in \mathbb{N}_0$ *mit* $m \geq 2$ *gilt. Sei* $f \in R[X][Y]$*, so existieren also nach vorherigem* $f_0, f_1 \in R[Y]$ *und* $g \in R[X,Y]$ *mit*

$$f(X,Y) = f_0(Y) + f_1(Y)X + (X^2 - Y^3) g(X,Y).$$

Insgesamt erhalten wir also für $f \in ker(\phi)$

$$\begin{aligned} 0 &= \phi(f)(X) \\ &= f(X^3, X^2) \\ &= f_0(X^2) + f_1(X^2)X^3 + (X^6 - X^6)g(X^3, X^2) \\ &= f_0(X^2) + f_1(X^2)X^3. \end{aligned}$$

Da $deg(f_0(X^2)) = deg(f_0(X^2)X^3)$ gilt, muss $f_0 = f_1 = 0$ gelten.

Aufgabe 3. Der Ring $R[\![X]\!]$ der formalen Potenzreihen mit Koeffizienten in R ist definiert wie folgt. Als Menge ist

$$R[\![X]\!] = R^{\mathbb{N}_0} = \{(a_0, a_1, \dots) \mid a_i \in R \text{ für } i \in \mathbb{N}_0\}.$$

Addition und Multiplikation sind definiert wie im Polynomring $R[X]$.

1. Zeigen Sie, dass $R[\![X]\!]^* = \left\{\sum_{i=0}^{\infty} a_i X^i \in R[X] \mid a_0 \in R^*\right\}$ gilt.

2. Sei R ein Körper. Bestimmen Sie alle Ideal von $R[\![X]\!]$.

Beweis. 1. Seien $f, g \in R[\![X]\!]$ mit $f(X) = \sum_{i=0}^{\infty} a_i X^i$ und $g(X) = \sum_{i=0}^{\infty} b_i X^i$, so gilt nach Definition

$$f(X)g(X) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k.$$

Also gilt genau dann $fg = 1$, wenn $a_0 b_0 = 1$ und $\sum_{i=0}^{k} a_i b_{k-i} = 0$ für alle $k \geq 1$.

Ist nun $f \in R[\![X]\!]^*$, so gilt $a_0 \in R^*$, d.h. $f \in \left\{\sum_{i=0}^{\infty} a_i X^i \in R[X] \mid a_0 \in R^*\right\}$. Ist andersherum $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \left\{\sum_{i=0}^{\infty} a_i X^i \in R[X] \mid a_0 \in R^*\right\}$, so betrachten wir $g(X) = \sum_{i=0}^{\infty} b_i X^i$ mit $b_0 = a_0^{-1}$ und $b_n = -a_0^{-1} \sum_{j=0}^{n-1} a_{n-j} b_j$. Es gilt $a_0 b_0 = a_0 a_0^{-1} = 1$ und für $k \geq 1$

$$\begin{aligned} \sum_{i=0}^{k} a_i b_{k-i} &= \sum_{i=0}^{k} a_{k-i} b_i \\ &= \left(\sum_{i=0}^{k-1} a_{k-i} b_i\right) + a_0 b_k \\ &= \left(\sum_{i=0}^{k-1} a_{k-i} b_i\right) + a_0 \left(-a_0^{-1} \sum_{j=0}^{k-1} a_{k-j} b_j\right) \\ &= \left(\sum_{i=0}^{k-1} a_{k-i} b_i\right) - \left(\sum_{j=0}^{k-1} a_{k-j} b_j\right) \\ &= 0. \end{aligned}$$

Somit ist f eine Einheit in $R[\![X]\!]$.

2. Wir zeigen im Folgenden, dass die Ideale von $R[\![X]\!]$ der Form $\{0\}$ und (X^n) mit $n \in \mathbb{N}_0$ sind. Dazu stellen wir zunächst fest, dass für ein beliebiges $f \in R[\![X]\!] \setminus \{0\}$ ein $u \in R[\![X]\!]^*$ und $n \in \mathbb{N}_0$ existieren, sodass $f(X) = X^n u(X)$. Sei also $f(X) = \sum_{i=0}^{\infty} a_i X^i \in R[\![X]\!] \setminus \{0\}$ mit

$n \in \mathbb{N}_0$ minimal, sodass $a_n \neq 0$ (d.h. $a_n \in R^*$), so gilt $f(X) = X^n \left(\sum_{i=n}^{\infty} a_i X^{i-n}\right)$. Nach Teil (1) ist $u(X) := \sum_{i=n}^{\infty} a_i X^{i-n}$ eine Einheit.

Sei nun $I \lhd R[\![X]\!]$ ein von $\{0\}$ verschiedenes Ideal, so können wir ein Element $f \in I$ mit $f(X) = X^n u(X)$ wählen, sodass $n \in \mathbb{N}_0$ minimal und $u \in R[\![X]\!]^*$ ist. Es ist $I = (X^n)$, denn offensichtlich gilt wegen $X^n = f(X) \cdot u(X)^{-1}$

$$(X^n) \subseteq I$$

und andersherum mit $g \in I \setminus \{0\}$ mit $g(X) = X^m v(X)$, $m \in \mathbb{N}_0$ und $R[\![X]\!]^*$ gilt nach Definition $m \geq n$ und somit

$$g(X) = X^n X^{m-n} v(c) \in (X^n),$$

d.h. $I \subseteq (X^n)$.

□

Aufgabe 4. Ein Element r heißt nilpotent, falls ein $n \in \mathbb{N}$ existiert mit $r^n = 0$. Zeigen Sie:

1. Die Menge $N(R)$ der nilpotenten Elemente in R ist ein Ideal von R.
2. Für $u \in R$ und $r \in N(R)$ gilt stets $u + r \in R^*$.

Beweis. 1. Zunächst rechnen wir nach, dass $N(R)$ eine additive Untergruppe von R ist. Offensichtlich ist $0 \in N(R)$ und für alle $r \in N(R)$ gilt auch $-r \in N(R)$. Es bleibt also die Abgeschlossenheit begüglich der Addition zu zeigen. Seien $r_1, r_2 \in N(R)$ mit $r_1^{n_1} = r_2^{n_2} = 0$, so können wir wegen der Kommutativität der Multiplikation in R und $1 \in R$ den binomischen Lehrsatz anwenden. Es gilt

$$\begin{aligned}(r_1 + r_2)^{n_1+n_2} &= \sum_{k=0}^{n_1+n_2} \binom{n_1 + n_2}{k} r_1^k r_2^{n_1+n_2-k} \\ &= \left(\sum_{k=0}^{n_1} \binom{n_1 + n_2}{k} r_1^k r_2^{n_1+n_2-k}\right) + \left(\sum_{k=n_1+1}^{n_1+n_2} \binom{n_1 + n_2}{k} r_1^k r_2^{n_1+n_2-k}\right) \\ &= 0,\end{aligned}$$

also ist $N(R)$ eine additive Untergruppe.
Seien $r \in R$ und $s \in N(R)$ mit $s^n = 0$, so gilt $(rs)^n = r^n s^n = 0$. Somit erhalten wir, dass $N(R)$ ein Ideal ist.

2. Zunächst stellen wir fest, dass $u + r$ genau dann invertierbar ist, wenn $u^{-1}(u + r) = 1 + u^{-1} r$ invertierbar ist. Sei also $u + r \in R^*$, so gilt offensichtlich $\left(u^{-1}(u + r)\right)^{-1} = (u + r)^{-1} u \in R^*$. Ist $u^{-1}(u + r)$ invertierbar, so gilt

$$\left(\left(u^{-1}(u + r)\right)^{-1} u^{-1}\right)(u + r) = \left(\left(u^{-1}(u + r)\right)^{-1} u^{-1}\right) u u^{-1}(u + r) = 1,$$

d.h. $u + r \in R^*$. Da $N(R)$ ein Ideal ist, gilt wegen des ersten Teils des Lemma $u^{-1} r \in N(R)$. Es reicht also aus die Situation für $u = 1$ zu betrachten.
Sei nun $f(X) := \frac{1}{1+X}$ und die Potenzreihenentwicklung durch folgenden Ausdruck gegeben

$$\frac{1}{1 + X} = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} X^k = \sum_{k=0}^{\infty} \frac{(-1)^k k!}{(1 + X)_{|X=0}^{k+1} k!} X^k = \sum_{k=0}^{\infty} (-1)^k X^k,$$

wobei $f^{(k)}(X) = (-1)^k \frac{k!}{(1+X)^{k+1}}$. Letzteres lässt sich einfach mittels vollständiger Induktion nach k beweisen.
Da $r \in N(R)$ gilt, lässt sich der Ausdruck $f(r)$ berechnen und es gilt

$$f(r) = \sum_{k=0}^{n} (-1)^k r^k,$$

wobei $r^n = 0$. Somit gilt

$$\begin{aligned}
(1+r)\cdot f(r) &= \left(\sum_{k=0}^{n}(-1)^k r^k\right) + \left(\sum_{k=0}^{n}(-1)^k r^{k+1}\right)\\
&= \left(\sum_{k=0}^{n}(-1)^k r^k\right) + \left(\sum_{k=1}^{n+1}(-1)^{k-1} r^k\right)\\
&= \left(\sum_{k=1}^{n}(-1)^k r^k\right) + (-1)\left(\sum_{k=1}^{n}(-1)^k r^k\right) + 1 + (-1)^n r^{n+1}\\
&= 1.
\end{aligned}$$

Insgesamt erhalten wir also

$$(1+r)^{-1} = f(r).$$

$\square$