

## 9. Polynom- und Potenzreihenringe

Bevor wir mit der allgemeinen Untersuchung von Ringen fortfahren, wollen wir in diesem Kapitel kurz zwei sehr wichtige weitere Beispiele von Ringen einführen, deren Objekte ihr sicher in der einen oder anderen Form schon in den Grundlagen der Mathematik oder auch schon in der Schule gesehen habt: die *Polynome*, also Ausdrücke der Form

$$a_0 + a_1t + a_2t^2 + \cdots + a_nt^n \quad (1)$$

(mit  $n \in \mathbb{N}$  und gegebenen Koeffizienten  $a_n$  in einem Ring  $R$ , z. B. im Ring  $\mathbb{R}$  der reellen Zahlen), und als „unendliche Variante“ davon die *Potenzreihen*, also nicht notwendig abbrechende Summen der Form

$$a_0 + a_1t + a_2t^2 + \cdots \quad (2)$$

Vermutlich werdet ihr diese Ausdrücke dabei bisher stets als Funktionen aufgefasst haben, die einer (z. B. reellen) Zahl  $t$  die Zahl zuordnen, die eben durch die Formel (1) bzw. (2) gegeben ist. Bei den Potenzreihen muss man dazu natürlich vorher noch überprüfen, dass die Reihe für die eingesetzten Werte von  $t$  auch konvergiert.

In der Algebra ist die Herangehensweise an Polynome und Potenzreihen etwas anders. Das muss auch so sein, denn in einem allgemeinen Ring  $R$  haben wir ja überhaupt keinen Konvergenzbegriff und damit keinerlei Möglichkeit, eine unendliche Summe wie in (2) als Funktion aufzufassen: Wenn wir dort für  $t$  ein Ringelement einsetzen würden, ergäbe sich lediglich eine (undefinierte) Summe unendlich vieler Elemente aus  $R$ .

Wir wollen eine Potenzreihe wie in (2) daher in einem beliebigen Ring  $R$  als rein *formale Summe* auffassen, in die wir zunächst einmal keine Werte für  $t$  einsetzen können. Der entscheidende Punkt hierbei ist, dass wir solche Potenzreihen trotzdem addieren und multiplizieren können: Betrachten wir z. B. die formalen Potenzreihen

$$f = 1 + t + t^2 + t^3 + t^4 + t^5 + \cdots \quad \text{und} \quad g = 1 - t + t^2 - t^3 + t^4 - t^5 \pm \cdots,$$

so erscheint es sicher in einem beliebigen Ring sinnvoll, die Summe dieser beiden Reihen einfach formal koeffizientenweise als

$$f + g = 2 + 2t^2 + 2t^4 + \cdots$$

zu *definieren*, selbst wenn man für  $t$  eigentlich keine Werte einsetzen und  $f$  und  $g$  damit nicht als Funktionen ansehen kann. Analog werden wir auch eine Multiplikation von Potenzreihen durch „formales Ausmultiplizieren“ definieren und die Menge dieser formalen Potenzreihen damit zu einem Ring machen.

Bei Polynomen scheint die Situation zunächst etwas anders zu sein, denn in der *endlichen* Summe (1) könnten wir natürlich in einem beliebigen Ring  $R$  Werte für  $t$  einsetzen und das Polynom somit tatsächlich als Funktion von  $R$  nach  $R$  auffassen. Wir werden jedoch z. B. in Bemerkung 9.16 (b) sehen, dass es algebraisch viel schöner ist, Polynome dennoch *nicht* als solche Funktionen, sondern (wie schon bei den Potenzreihen) als formale Ausdrücke der Form (1) zu definieren. In der Tat macht dies in manchen Ringen einen Unterschied: Betrachten wir z. B. das Polynom  $t^2 + t$  über dem Ring  $\mathbb{Z}_2$ , so stellt dieses zwar die Nullfunktion dar (denn es ist  $\bar{0}^2 + \bar{0} = \bar{1}^2 + \bar{1} = \bar{0}$ , d. h. jedes Element von  $\mathbb{Z}_2$  wird unter der Funktion  $t \mapsto t^2 + t$  auf die Null abgebildet), es ist aber als formaler Ausdruck trotzdem nicht das Nullpolynom. Wir wollen die Polynome  $t^2 + t$  und  $\bar{0}$  über  $\mathbb{Z}_2$  daher als *verschieden* ansehen, auch wenn sie beim Einsetzen von Werten dieselbe Funktion beschreiben.

Nach diesen Vorbemerkungen können wir nun damit beginnen, Potenzreihen über einem beliebigen Ring exakt zu definieren. Wie gerade erläutert ist eine solche formale Potenzreihe der Form (2) einfach dadurch gegeben, dass man ihre Koeffizienten  $a_0, a_1, a_2, \dots$  angibt. Dabei gibt es für die

Wahl dieser Koeffizienten keinerlei Einschränkungen. Eine Potenzreihe „ist“ also letztlich einfach diese Folge  $a_0, a_1, a_2, \dots$  in  $R$ , d. h. eine Abbildung von  $\mathbb{N}$  nach  $R$ .

**Definition 9.1** (Potenzreihen). Es sei  $R$  ein Ring.

- (a) Eine (**formale**) **Potenzreihe** über  $R$  ist eine Abbildung  $\mathbb{N} \rightarrow R$ ,  $n \mapsto a_n$ . Wir werden eine solche Potenzreihe jedoch *nie* als derartige Abbildung, sondern *immer* in der Form

$$\sum_{k=0}^{\infty} a_k t^k \quad \text{oder} \quad a_0 + a_1 t + a_2 t^2 + \dots$$

schreiben (wobei wir für  $k$  natürlich auch einen anderen Buchstaben wählen können). Beachte, dass es sich dabei aber nur um eine *formale Schreibweise* für die obige Abbildung  $\mathbb{N} \rightarrow R$  und *nicht* um eine wirkliche „unendliche Summe“ in  $R$  handelt!

Die Menge aller Potenzreihen über  $R$  wird mit  $R[[t]]$  bezeichnet.

- (b) Sind  $f = \sum_{k=0}^{\infty} a_k t^k$  und  $g = \sum_{k=0}^{\infty} b_k t^k$  zwei Potenzreihen über  $R$ , so definieren wir ihre Summe  $f + g$  und ihr Produkt  $f \cdot g$  als die Potenzreihen

$$f + g := \sum_{k=0}^{\infty} (a_k + b_k) t^k$$

und

$$f \cdot g := \sum_{n=0}^{\infty} \left( \underbrace{\sum_{k+l=n} a_k b_l}_{(*)} \right) t^n.$$

Beachte dabei, dass die Summe  $(*)$  eine „echte“ (endliche) Summe in  $R$  ist, während die beiden anderen Summenzeichen die „formalen unendlichen Summen“ aus (a) sind.

**Bemerkung 9.2.**

- (a) In der Schreibweise von Definition 9.1 können wir  $t$  als *formale Variable* auffassen. Natürlich könnte man auch hier einen anderen Buchstaben als formale Variable wählen und die Notation  $R[[t]]$  entsprechend abändern. Wir werden die formale Variable einer Potenzreihe in diesem Skript jedoch immer mit dem Buchstaben  $t$  bezeichnen.
- (b) Beachte, dass die Multiplikation von Potenzreihen in Definition 9.1 (b) genau so eingeführt wurde, wie man es erwarten würde, wenn man diese formalen unendlichen Summen naiv ausmultiplizieren könnte: Dann wäre nämlich

$$\begin{aligned} \left( \sum_{k=0}^{\infty} a_k t^k \right) \cdot \left( \sum_{l=0}^{\infty} b_l t^l \right) &= (a_0 + a_1 t + a_2 t^2 + \dots) \cdot (b_0 + b_1 t + b_2 t^2 + \dots) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) t + (a_0 b_2 + a_1 b_1 + a_2 b_0) t^2 + \dots \\ &= \sum_{n=0}^{\infty} \left( \sum_{k+l=n} a_k b_l \right) t^n, \end{aligned}$$

und das ist ja gerade unsere Definition. In der Analysis ist es ein *Satz* (den ihr in den Grundlagen der Mathematik vielleicht schon bewiesen habt), dass dieses „unendliche Ausmultiplizieren“ — das sogenannte *Cauchy-Produkt von Reihen* — bei bestimmten konvergenten reellen oder komplexen Reihen erlaubt ist [G, Satz 7.33]. Bei uns in der Algebra dagegen ist dies einfach nur die *Definition* der Multiplikation von formalen Potenzreihen.

**Beispiel 9.3.** In einem Ring  $R$  betrachten wir die Potenzreihe

$$f = 1 + t + t^2 + t^3 + \dots = \sum_{k=0}^{\infty} t^k \in R[[t]].$$

Dann ist das Produkt von  $f$  mit sich selbst nach Definition 9.1 (b)

$$f^2 = \sum_{n=0}^{\infty} \left( \sum_{k+l=n} 1 \cdot 1 \right) t^n = \sum_{n=0}^{\infty} (n+1) t^n,$$

da die Summe über  $k$  und  $l$  aus  $n + 1$  Summanden (nämlich  $(k, l) = (0, n), (1, n - 1), \dots, (n, 0)$ ) besteht.

**Lemma 9.4.** Für jeden Ring  $R$  ist die Menge  $R[[t]]$  aller Potenzreihen über  $R$  mit den Verknüpfungen aus Definition 9.1 (b) ein Ring. Er wird der (**formale**) **Potenzreihenring** über  $R$  genannt.

*Beweis.* Die Überprüfung der Ringaxiome aus Definition 7.1 ergibt sich durch einfaches Nachrechnen. Wir zeigen hier exemplarisch den Beweis der Distributivität (R3): Für

$$f = \sum_{k=0}^{\infty} a_k t^k, \quad g = \sum_{k=0}^{\infty} b_k t^k \quad \text{und} \quad h = \sum_{l=0}^{\infty} c_l t^l$$

ist

$$\begin{aligned} (f + g) \cdot h &= \left( \sum_{k=0}^{\infty} (a_k + b_k) t^k \right) \cdot \left( \sum_{l=0}^{\infty} c_l t^l \right) \\ &= \sum_{n=0}^{\infty} \left( \sum_{k+l=n} (a_k + b_k) c_l \right) t^n \\ &\stackrel{(*)}{=} \sum_{n=0}^{\infty} \left( \sum_{k+l=n} a_k c_l + \sum_{k+l=n} b_k c_l \right) t^n \\ &= \sum_{n=0}^{\infty} \left( \sum_{k+l=n} a_k c_l \right) t^n + \sum_{n=0}^{\infty} \left( \sum_{k+l=n} b_k c_l \right) t^n \\ &= f \cdot h + g \cdot h, \end{aligned}$$

wobei (\*) die Distributivität in  $R$  ist (beachte, dass die Summen über  $k$  und  $l$  „echte“ endliche Summen in  $R$  sind) und alle anderen Gleichungen aus der Definition 9.1 (b) der Addition und Multiplikation in  $R[[t]]$  folgen.

Die Null in  $R[[t]]$  ist natürlich die Potenzreihe, bei der alle Koeffizienten gleich 0 sind; die Eins diejenige, bei der nur der konstante Koeffizient gleich 1 und alle anderen gleich 0 sind.  $\square$

**Notation 9.5.** Aus naheliegenden Gründen schreibt man die Potenzreihe

$$a_0 + 0 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 + \dots \in R[[t]]$$

über einem Ring  $R$  einfach kurz als  $a_0$ , und die Potenzreihe

$$0 + 1 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 + \dots \in R[[t]]$$

einfach als  $t$ . Da die Addition und Multiplikation in  $R[[t]]$  ja gerade so definiert sind, wie man es durch formales Addieren und Ausmultiplizieren von Potenzreihen erwarten würde, können wir dann jede „abbrechende Potenzreihe“

$$a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n + 0 \cdot t^{n+1} + 0 \cdot t^{n+2} + \dots,$$

also jede Potenzreihe  $\sum_{k=0}^{\infty} a_k t^k$ , für die es ein  $n \in \mathbb{N}$  gibt mit  $a_k = 0$  für alle  $k > n$ , offensichtlich einfach als

$$a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n,$$

schreiben, wobei dies nun *keine* formale Summe mehr ist, sondern eine „echte“ Verknüpfung der Potenzreihen  $a_0, \dots, a_n, t \in R[[t]]$  mit der Addition und Multiplikation wie in Definition 9.1 (b). Diese „abbrechenden Potenzreihen“ sind jetzt genau die Polynome, die wir bereits am Anfang dieses Kapitels erwähnt hatten.

**Definition 9.6** (Polynome). Es sei  $R$  ein Ring.

- (a) Ein **Polynom** über  $R$  ist eine Potenzreihe der Form  $a_0 + a_1 t + \dots + a_n t^n$ , also eine Potenzreihe, bei der nur endlich viele Koeffizienten ungleich Null sind. Die Menge aller Polynome über  $R$  wird mit  $R[t]$  bezeichnet.

- (b) Ist  $f \in R[t]$  ein Polynom mit  $f \neq 0$ , so können wir  $f$  offensichtlich eindeutig als

$$f = a_0 + a_1 t + \cdots + a_n t^n$$

mit  $n \in \mathbb{N}$  und  $a_n \neq 0$  schreiben. Die Zahl  $n$ , also der höchste in  $f$  auftretende Exponent von  $t$ , wird der **Grad** von  $f$  genannt und als  $\deg f$  geschrieben (die Bezeichnung kommt vom englischen Wort „degree“). Der höchste Koeffizient  $a_n \in R$  heißt **Leitkoeffizient** von  $f$ . Man nennt  $f$  **normiert**, wenn dieser Leitkoeffizient gleich 1 ist.

Den Grad des Nullpolynoms definiert man formal als  $\deg 0 = -\infty$  (auf diese Art bleiben z. B. die Formeln aus Lemma 9.7 (a) und 9.9 (a) auch in diesem Fall richtig).

- (c) Ein Polynom vom Grad  $-\infty$  oder 0 heißt **konstantes Polynom**, eines vom Grad 1 **lineares Polynom**.

**Lemma 9.7.** *Es sei wieder  $R$  ein Ring.*

- (a) Sind  $f, g \in R[t]$  Polynome über  $R$ , so sind auch  $f + g$  und  $f \cdot g$  Polynome über  $R$ , und es gilt

$$\deg(f + g) \leq \max\{\deg f, \deg g\} \quad \text{und} \quad \deg(f \cdot g) \leq \deg f + \deg g.$$

- (b) Es gilt  $R \leq R[t] \leq R[[t]]$ , wobei  $R$  wie in Notation 9.5 als Teilmenge von  $R[t]$  bzw.  $R[[t]]$  angesehen wird, indem man ein  $a_0 \in R$  als konstantes Polynom auffasst.

Insbesondere ist  $R[t]$  also ein Ring; er wird der **Polynomring** über  $R$  genannt.

*Beweis.*

- (a) Für  $f = 0$  oder  $g = 0$  sind die Aussagen aufgrund der Definition  $\deg 0 = -\infty$  richtig. Da  $f$  und  $g$  ansonsten nur Terme  $t^k$  mit  $k \leq \deg f$  bzw.  $k \leq \deg g$  enthält, ist natürlich aufgrund von Definition 9.1 (b) klar, dass  $f + g$  und  $f \cdot g$  nur Terme  $t^k$  mit  $k \leq \max\{\deg f, \deg g\}$  bzw.  $k \leq \deg f + \deg g$  enthalten kann.
- (b) Beide Aussagen folgen mit (a) direkt aus dem Unterringkriterium von Lemma 7.23.  $\square$

10

**Beispiel 9.8.** Sowohl für den Grad von  $f + g$  als auch für den von  $f \cdot g$  kann in Lemma 9.7 (a) eine echte Ungleichung stehen: Für  $R = \mathbb{Z}_4$  und das Polynom  $f = g = \bar{2}t + \bar{1}$  vom Grad 1 ist

$$\deg(f + g) = \deg(\bar{4}t + \bar{2}) = \deg(\bar{2}) = 0 < 1 = \max\{\deg f, \deg g\}$$

und

$$\deg(f \cdot g) = \deg((\bar{2}t + \bar{1})^2) = \deg(\bar{4}t^2 + \bar{4}t + \bar{1}) = \deg(\bar{1}) = 0 < 2 = \deg f + \deg g.$$

Ist  $R$  ein Integritätsring, so steht bei der Formel für  $\deg(f \cdot g)$  jedoch immer die Gleichheit:

**Lemma 9.9.** *Für jeden Integritätsring  $R$  gilt:*

- (a) (**Gradformel**) Für alle  $f, g \in R[t]$  gilt  $\deg(f \cdot g) = \deg f + \deg g$ .
- (b)  $R[t]$  ist ein Integritätsring.
- (c) Die Einheitsgruppe des Polynomrings über  $R$  ist  $R[t]^* = R^*$ , besteht also genau aus den konstanten Polynomen mit Wert in  $R^*$ .

*Beweis.*

- (a) Für  $f = 0$  oder  $g = 0$  ist die Formel wegen  $\deg 0 = -\infty$  trivialerweise richtig. Ist ansonsten  $n = \deg f$  und  $m = \deg g$ , so können wir  $f$  und  $g$  als

$$f = a_n t^n + \cdots + a_1 t + a_0 \quad \text{und} \quad g = b_m t^m + \cdots + b_1 t + b_0$$

mit  $a_n, b_m \neq 0$  schreiben. Damit ist

$$f \cdot g = a_n b_m t^{n+m} + (\text{Terme mit niedrigeren Potenzen von } t).$$

Da  $R$  ein Integritätsring ist, folgt nun  $a_n b_m \neq 0$  und damit  $\deg(f \cdot g) = n + m = \deg f + \deg g$ .

- (b) Sind  $f, g \neq 0$ , also  $\deg f, \deg g \geq 0$ , so ist nach (a) auch  $\deg(f \cdot g) \geq 0$  und damit  $f \cdot g \neq 0$ .

- (c) Offensichtlich ist jede Einheit von  $R$  auch eine von  $R[t]$ . Ist umgekehrt  $f \in R[t]^*$ , so gibt es ein  $g \in R[t]$  mit  $f \cdot g = 1$ . Aus der Gradformel (a) folgt daraus  $\deg f + \deg g = 0$ , also  $\deg f = \deg g = 0$ . Damit liegen  $f = a_0$  und  $g = b_0$  in  $R$ , und wegen  $f \cdot g = a_0 \cdot b_0 = 1$  muss sogar  $f = a_0 \in R^*$  gelten.  $\square$

**Aufgabe 9.10.** Für eine Potenzreihe  $f = \sum_{n=0}^{\infty} a_n t^n$  über einem Ring  $R$  definieren wir die (formale) Ableitung als  $f' := \sum_{n=1}^{\infty} n a_n t^{n-1}$ .

- (a) Man zeige: Für alle  $f, g \in R[[t]]$  gilt  $(f + g)' = f' + g'$  und  $(fg)' = f'g + fg'$ .  
 (b) Bestimme in den beiden Fällen  $R = \mathbb{R}$  und  $R = \mathbb{Z}_7$  alle Potenzreihen mit Ableitung  $0 \in R[[t]]$ .

**Aufgabe 9.11.** Es seien  $R$  ein Ring und  $a \in R$ . Zeige, dass die Potenzreihe  $1 - at \in R[[t]]$  invertierbar ist, und berechne  $(1 - at)^{-1} \in R[[t]]$ .

**Aufgabe 9.12.** Zeige, dass eine Potenzreihe  $\sum_{n=0}^{\infty} a_n t^n$  über einem Ring  $R$  genau dann in  $R[[t]]$  invertierbar ist, wenn  $a_0 \in R^*$ .

**Aufgabe 9.13.** In dieser Aufgabe wollen wir mit Hilfe von Potenzreihen eine explizite Formel für die durch

$$a_0 = a_1 = 1 \quad \text{und} \quad a_{n+2} = a_{n+1} + a_n \quad \text{für } n \in \mathbb{N}$$

rekursiv definierte *Fibonacci-Folge*  $1, 1, 2, 3, 5, 8, 13, \dots$  herleiten.

- (a) Nach Aufgabe 9.12 ist  $1 - t - t^2$  in  $\mathbb{R}[[t]]$  invertierbar. Zeige, dass sich das Inverse dieser Potenzreihe als  $\frac{1}{1-t-t^2} = \frac{b_1}{1-c_1 t} + \frac{b_2}{1-c_2 t}$  für gewisse  $b_1, b_2, c_1, c_2 \in \mathbb{R}$  schreiben lässt, und bestimme diese Koeffizienten.  
 (b) Zeige, dass die Fibonacci-Zahlen genau die Koeffizienten der Potenzreihe  $\frac{1}{1-t-t^2}$  sind, d. h. dass

$$\frac{1}{1-t-t^2} = \sum_{n=0}^{\infty} a_n t^n$$

gilt, und folgere daraus für  $n \in \mathbb{N}$  die nicht-rekursive Formel

$$a_n = \frac{1}{\sqrt{5}} \cdot \left( \left( \frac{1+\sqrt{5}}{2} \right)^{n+1} - \left( \frac{1-\sqrt{5}}{2} \right)^{n+1} \right).$$

**Aufgabe 9.14.** Ist der Potenzreihenring  $R[[t]]$  über einem Integritätsring  $R$  ebenfalls wieder ein Integritätsring?

Wie schon am Anfang dieses Kapitels erwähnt bestimmt ein Polynom über  $R$  eine Funktion von  $R$  nach  $R$ :

**Definition 9.15** (Polynomfunktionen). Ist  $f = a_0 + a_1 t + \dots + a_n t^n$  ein Polynom über einem Ring  $R$  und  $x \in R$ , so heißt das Ringelement

$$f(x) := a_0 + a_1 x + \dots + a_n x^n \in R$$

der **Wert** von  $f$  in  $x$ . Die zugehörige Funktion  $R \rightarrow R$ ,  $x \mapsto f(x)$  wird eine **Polynomfunktion** genannt. Ist  $f(x) = 0 \in R$ , so heißt  $x$  eine **Nullstelle** von  $f$ .

**Bemerkung 9.16.**

- (a) Beachte, dass wir für Potenzreihen  $f \in R[[t]]$  keinen Wert  $f(x)$  in einem Punkt  $x \in R$  definieren können, da wir in der Algebra (also ohne Konvergenzbegriff) keine unendlichen Summen in  $R$  bilden können.  
 (b) Nach Definition 9.15 bestimmt jedes Polynom  $f$  über einem Ring  $R$  eine Polynomfunktion  $R \rightarrow R$ ,  $x \mapsto f(x)$ . Wie wir schon in der Einleitung dieses Kapitels gesehen haben, können aber zwei verschiedene Polynome dieselbe Polynomfunktion bestimmen: Das Polynom  $t^2 + t$  über  $\mathbb{Z}_2$  hat z. B. in jedem Element von  $\mathbb{Z}_2$  den Wert Null. Während die beiden Polynome  $t^2 + t$  und  $\bar{0}$  verschieden sind, sind die beiden zugehörigen *Polynomfunktionen*  $t \mapsto t^2 + t$

und  $t \mapsto \bar{0}$  hier also gleich. Beachte, dass dies u. a. auch bedeutet, dass man einer *Polynomfunktion* in der Regel keinen wohldefinierten Grad zuordnen kann — hier verhalten sich Polynome aus algebraischer Sicht also deutlich schöner als Polynomfunktionen.

Wir werden in Folgerung 11.16 allerdings noch sehen, dass Polynome und Polynomfunktionen über Körpern mit unendlich vielen Elementen (also z. B.  $\mathbb{R}$  oder  $\mathbb{C}$ ) übereinstimmen, so dass es in diesem wohl wichtigsten Fall keinen Unterschied macht, ob wir bei Polynomen an Funktionen oder an die formalen Ausdrücke aus Definition 9.6 denken.

**Aufgabe 9.17.** Man zeige:

- (a) Sind  $R \leq S$  Ringe und  $x \in S$ , so ist die „Auswerteabbildung“

$$\varphi: R[t] \rightarrow S, f = \sum_{k=0}^n a_k t^k \mapsto f(x) := \sum_{k=0}^n a_k x^k$$

ein Ringhomomorphismus.

- (b) Jedes Element des Ringes  $\mathbb{R}[t]/\langle t^2 + 1 \rangle$  lässt sich in der Form  $\overline{x + yt}$  mit  $x, y \in \mathbb{R}$  schreiben.

- (c) Die Abbildung  $\mathbb{R}[t]/\langle t^2 + 1 \rangle \rightarrow \mathbb{C}, \bar{f} \mapsto f(i)$  ist ein Ringisomorphismus.

(Man kann  $\mathbb{C}$  also algebraisch sehr elegant als  $\mathbb{R}[t]/\langle t^2 + 1 \rangle$  definieren — dies definiert dann gleichzeitig schon die Addition und Multiplikation auf  $\mathbb{C}$  und zeigt dafür ohne weitere Rechnung alle Ringaxiome. In der Tat werden wir in Beispiel 11.21 (b) noch sehen, dass sich sogar alle Körperaxiome schon automatisch ergeben.)

**Bemerkung 9.18** (Die Notation  $R[\cdot]$ ). Um Verwirrungen zu vermeiden, ist es wichtig zu verstehen, dass die Notation  $R[\cdot]$  für einen Ring  $R$  zwei verschiedene Dinge bedeuten kann:

- (a) Steht in den Klammern eine (vorher unbekannte) formale Variable, so wie in  $R[t]$  in Definition 9.6, so ist der dort eingeführte Polynomring gemeint.
- (b) Steht in den Klammern ein Element  $a$  eines größeren bereits bekannten Ringes  $S \geq R$ , so wie z. B. in  $\mathbb{Z}[\sqrt{5}i]$  mit  $a = \sqrt{5}i \in \mathbb{C}$  in Aufgabe 7.24, so ist der *Ring aller Werte von Polynomausdrücken* in diesem Element mit Koeffizienten in  $R$  gemeint, also der Unterring

$$R[a] := \{c_0 + c_1 a + \cdots + c_n a^n : n \in \mathbb{N}; c_0, \dots, c_n \in R\}$$

von  $S$ . Liegt  $a^2$  bereits wieder in  $R$ , so können wir uns dabei natürlich auf lineare Polynomausdrücke beschränken und erhalten z. B.

$$\mathbb{Z}[\sqrt{5}i] = \{c_0 + c_1 \sqrt{5}i : c_0, c_1 \in \mathbb{Z}\} \leq \mathbb{C}$$

wie in Aufgabe 7.24.

Die in der Literatur übliche gleiche Notation für diese beiden Konzepte kommt daher, dass in beiden Fällen Polynomausdrücke in dem in Klammern genannten Element betrachtet werden. Auch die Sprechweise ist daher oft in beiden Fällen gleich: Man sagt, dass  $R[\cdot]$  aus  $R$  durch *Adjunktion* des in Klammern stehenden Elements entsteht und spricht die Fälle (a) und (b) oben demzufolge auch als „ $R$  adjungiert  $t$ “ bzw. „ $R$  adjungiert  $a$ “. Die formale Konstruktion dieser Ringe ist in (a) und (b) jedoch unterschiedlich.