2.5 Ringe und noch mehr Ringe

In der Linearen Algebra sind Ihnen schon einige Ringe begegnet. Diese und weitere werden wir in dem Abschnitt nennen und einige besonders wichtige nochmals allgemeiner oder strenger einführen.

$\mathbb{Z}$ und $\mathbb{Z}_m$

Zusätzlich zum wohlbekannten Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot)$, mit dem Ihnen der Umgang bereits aus der Schule bekannt ist, wurde in der linearen Algebra noch ein weiterer, damit eng verwandter Ring eingeführt:

$$\mathbb{Z}_m = \{0, \ldots, m-1\} \quad \text{(Vorlesung SS2019)}$$

mit Addition und Multiplikation

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (a, b) &\longmapsto (a + b) \bmod m \\ \cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (a, b) &\longmapsto (a \cdot b) \bmod m, \end{aligned}$$

bzw.

$$(\mathbb{Z}/m\mathbb{Z}, +, \cdot) \quad \text{(Vorlesung WS2019/20)}$$

mit Addition und Multiplikation

$$\begin{aligned} + : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ ([a]_m, [b]_m) &\longmapsto [a + b]_m \\ \cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ ([a]_m, [b]_m) &\longmapsto [a \cdot b]_m. \end{aligned}$$

Diese beiden Ringe sind tatsächlich isomorph, aber mittels zweier verschiedener Zugänge eingeführt, wobei der im zweiten Fall gewählte Zugang einer allgemeinen Konstruktion entspricht, die wir in ein paar Wochen kennenlernen werden. Wenn hier im Moment eine Schreibweise verwendet wird und Sie in Ihrer Vorlesung die andere kennengelernt haben, dann dürfen Sie gefahrlos in der Ihnen bekannten weiterdenken, bis alle die allgemeine Konstruktion kennengelernt haben.

Bemerkung 2.5.1 *Der Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist, wie wir in der Linearen Algebra bereits gesehen haben, genau dann ein Körper, wenn m prim ist. Als Nullteiler hatten wir andererseits genau die Klassen $[a]_m$ mit $\mathrm{ggT}(a, m) \neq 1$ bestimmt und hatten festgestellt, dass jedes Element außer $[0]_m$ in $\mathbb{Z}/m\mathbb{Z}$ Nullteiler oder Einheit ist.*

Matrizenring und Vektorraumhomomorphismen

Ein ganz zentrales Objekt in der Linearen Algebra war der nicht-kommutative Ring mit 1 $(\mathrm{Mat}(n; K), +, \cdot)$ der $n \times n$-Matrizen mit Einträgen in einem Körper K und der Matrixaddition und Matrixmultiplikation als Verknüpfungen. Da in diesen Definitionen und im Verifizieren der Ringeigenschaften in der Linearen Algebra nirgends die Existenz eines multiplikativen Inversen in K verwendet wurde, läßt sich in gleicher Weise auch der Ring der $n \times n$ Matrizen $(\mathrm{Mat}(n; R), +, \cdot)$ über einem kommutativen Ring R mit 1 definieren.
Das Einselement im Ring $(\mathrm{Mat}(n; R), +, \cdot)$ ist die Diagnoalmatrix, deren Diagonaleinträge alle 1_R sind und die wir wieder als Einheitsmatrix bezeichnen. Wir schreiben dafür wie in der Linearen Algebra E_n.

Sei nun ein K-Vektorraum V über einem Körper K mit Basis $\mathcal{B}$ gegeben. Ein zentrales Ergebnis der Linearen Algebra waren die K-Vektorraum- und Ringisomorphismen

$$\begin{aligned} \Phi : End_K(V) &\longrightarrow Mat(n; K) \\ F &\longmapsto M_{\mathcal{B}}^{\mathcal{B}}(F) \\ \text{und} & \\ \Phi\,|_{Aut_K(V)} \colon Aut_K(V) &\longrightarrow GL(n; K) \\ F &\longmapsto M_{\mathcal{B}}^{\mathcal{B}}(F), \end{aligned}$$

wobei auf der Seite der Vektorraumendomorphismen die Ringoperationen gerade festgelegt sind als:

$$\begin{aligned} \forall x \in V : (f +_{End_K(V)} g)(x) &:= f(x) +_V g(x) \\ (f \cdot_{End_K(V)} g)(x) &:= (f \circ g)(x) \end{aligned}$$

Hier konnten wir die Verknüpfung $+_{End_K(V)}$ auf $End_K(V)$ einfach von der Verknüpfung $+_V$ im Wertebereich der Abbildung erben. Dabei ist es

kein Zufall, dass dann nicht nur die Operation selbst, sondern auch Assoziativität, neutrales und inverses Element sich direkt auf diejenigen von $(V, +)$ zurückführen lassen, wie wir bereits in der Linearen Algebra am Rande bemerkt hatten. Das werden wir im folgenden ausnutzen, um noch weitere Beispiele von Ringen kennenzulernen.

Ringe von Abbildungen und von Folgen

Legen wir zuerst ein wenig Notation fest, damit das folgende klar herausgearbeitet werden kann.

Die Menge der Abbildungen von einer nicht-leeren Menge A in eine nicht-leere Menge B bezeichnen wir mit

$$B^A = Abb(A, B) = \{f : A \longrightarrow B \mid f Abbildung\}.$$

Zwei Abbildungen $f, g \in Abb(A, B)$ sind gleich, wenn $f(a) = g(a)$ für alle $a \in A$.

Ist in dieser Notation nun B ein kommutativer Ring R mit 1, so ist auch $R^A = Abb(A, R)$ ein kommutativer Ring mit 1 mit Hilfe der ererbten Verknüpfungen

$$\begin{aligned} (f +_{Abb(A,R)} g)(x) &:= f(x) +_R g(x) \quad \forall x \in A \\ (f \cdot_{Abb(A,R)} g)(x) &:= f(x) \cdot_R g(x) \quad \forall x \in A. \end{aligned}$$

Betrachten wir nun zwei wichtige Spezialfälle:

- Ist $A = \{1, \ldots, n\} \subseteq \mathbb{N}$, so ist

$$\begin{aligned} R^A &= \{f : \{1, \ldots, n\} \longrightarrow R \mid f \text{ Abbildung}\} \\ &\cong \{(f(1), \ldots, f(n)) \mid f(i) \in R \ \forall 1 \leq i \leq n\} \\ &= \{(a_1, \ldots, a_n) \mid a_i \in R \ \forall 1 \leq i \leq n\} \\ &= R^n. \end{aligned}$$

  In diesem Fall ist R^A also gerade isomorph zur Menge aller n-Tupel von Einträgen aus R verknüpft mit kompomentenweiser Addition und Multiplikation.

- Ist $A = \mathbb{N}_0$, so erhalten wir

$$\begin{aligned} R^{\mathbb{N}_0} &= \{f : \mathbb{N}_0 \longrightarrow R \mid f \text{ Abbildung}\} \\ &\cong \{(a_i)_{i\in\mathbb{N}_0} \mid a_i \in R \ \ \forall i \in \mathbb{N}_0\} \\ &= \text{Menge aller Folgen mit Gliedern in } R, \end{aligned}$$

  wobei hier die gliedweise Addition und Multiplikation die Verknüpfungen sind.

Wir sehen also, dass es kein Zufall ist, dass die Menge aller R-Folgen einen kommutativen Ring bildet mit der konstanten Folge $(1)_{i\in\mathbb{N}_0}$ als neutralem Element der Multiplikation. Der Vollständigkeit halber sei explizit erwähnt, dass die Folge $(0)_{i\in\mathbb{N}_0}$ hier das neutrale Element der Addition ist.

Betrachten wir nun zum Abschluss noch eine unter gliedweiser Addition und gliedweiser Multiplikation abgeschlossene Teilmenge von $R^{\mathbb{N}_0}$, die allerdings keinen Ring mit 1 bildet und damit kein Unterring von $R^{\mathbb{N}_0}$ ist. Überlegen Sie, wo das Problem liegt.

Wir bezeichnen mit $R^{(\mathbb{N}_0)}$ die Menge derjenigen Folgen mit Gliedern in R, die nur endlich viele von 0_R verschiedene Glieder haben, d.h.

$$R^{(\mathbb{N}_0)} = \{(a_i)_{i\in\mathbb{N}_0} \mid a_i \in R \ \ \forall i \in \mathbb{N}_0 \text{ und } a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}.$$

$R^{(\mathbb{N}_0)}$ bildet eine abelsche Gruppe unter der gliedweisen Addition und ist ein Untergruppe von $R^{\mathbb{N}_0}$.

Bemerkung 2.5.2 *Der Vergleich von Elementen in $R^{\mathbb{N}_0}$ und in $R^{(\mathbb{N}_0)}$ ist ein Vergleich von Abbildungen, wobei zwei Abbildungen gleich sind, wenn sie auf allen Elementen der Urbildmenge jeweils dasselbe Bild haben. Für die hier betrachteten Mengen von Folgen ist das genau der gliedweise Vergleich.*

Polynomring und Potenzreihenring

Polynome sind Ihnen bereits in der Schule begegnet, wo allerdings oft kein bewusster Unterschied zwischen Polynomen und Polynomabbildung gemacht wurde. In der Linearen Algebra jedoch haben wir diesen Unterschied bereits gemacht, indem wir Polynome als Elemente des Polynomringes betrachteten

und Polynomabbildungen mittels eines Polynoms und des Einsetzungshomomorphismus erzeugten. Dieser Unterschied wird sich auch in der nun folgenden strengen Einführung von Polynomringen über kommutativen Ringen widerspiegeln.

Der Einstieg ist dabei sehr formal und greift auf das eben Dargestellte zurück: Wir führen Potenzreihen und Polynome als Folgen ihrer Koeffizienten ein, d.h. wir bewegen uns weiter in den Mengen $R^{\mathbb{N}_0}$ bzw. $R^{(\mathbb{N}_0)}$. Dabei behalten wir aber nur die gliedweise Addition bei und definieren eine andere Multiplikation, was natürlich auch zu einem anderen neutralen Element der Multiplikation führt. wobei wir aber nicht die vorher betrachtete ererbte gliedweise Multiplikation verwenden, sondern diese Verknüpfung in anderer Weise festlegen. Das bedingt dann auch ein anderes neutrales Element

Satz 2.5.3 *Sei R ein kommutativer Ring mit 1 und seien $(R^{\mathbb{N}_0}, +)$ und $(R^{(\mathbb{N}_0)}, +)$ die eben eingeführten abelschen Gruppen. Mit der Multiplikation*

$$\begin{array}{rcl} \cdot : R^{\mathbb{N}_0} \times R^{\mathbb{N}_0} & \longrightarrow & R^{\mathbb{N}_0} \\ ((a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0}) & \longmapsto & (\sum\limits_{k+m=i} a_k b_m)_{i\in\mathbb{N}_0} \end{array}$$

ist $(R^{\mathbb{N}_0}, +, \cdot)$ ein kommutativer Ring mit Einselement $(e_i)_{i\in\mathbb{N}_0} = (1, 0, \dots)$. Mit dieser Multiplikation ist $(R^{(\mathbb{N}_0)}, +, \cdot)$ ein Unterring von $(R^{\mathbb{N}_0}, +, \cdot)$.

Beweis: Zu zeigen ist hier zuerst die Assozitativität (AG) sowie das neutrale Element (NE) für den größeren Ring.

(AG) Seien $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0}, (c_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$. Dann gilt

$$\begin{aligned} ((a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0}) \cdot (c_i)_{i\in\mathbb{N}_0} &= \left(\sum_{r+m=i} \left(\sum_{j+k=r} a_j b_k \right) c_m \right)_{i\in\mathbb{N}_0} \\ &= \left(\sum_{j+k+m=i} a_j b_k c_m \right)_{i\in\mathbb{N}_0} \\ &= \left(\sum_{j+r=i} a_j \left(\sum_{k+m=r} b_k c_m \right) \right)_{i\in\mathbb{N}_0} \\ &= (a_i)_{i\in\mathbb{N}_0} \cdot ((b_i)_{i\in\mathbb{N}_0} \cdot (c_i)_{i\in\mathbb{N}_0}). \end{aligned}$$

(NE) Sei $(a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$. Dann gilt

$$\begin{aligned}(e_i)_{i\in\mathbb{N}_0}\cdot(a_i)_{i\in\mathbb{N}_0} &= \left(\sum_{j+k=i} e_j a_k\right)_{i\in\mathbb{N}_0}\\ &= (a_i)_{i\in\mathbb{N}_0}\\ &= \left(\sum_{j+k=i} a_j e_k\right)_{i\in\mathbb{N}_0}\\ &= (a_i)_{i\in\mathbb{N}_0}\cdot(e_i)_{i\in\mathbb{N}_0}\end{aligned}$$

Da wir wissen, dass der kleinere Ring eine abelsche Untergruppe des größeren Rings bzgl. der Addition ist und da $(e_i)_{i\in\mathbb{N}_0}$ offensichtlich im kleineren Ring enthalten ist, bleibt nur noch die Abgeschlossenheit der Multiplikation für die Anwendung des Unterringkriteriums übrig. Seien dazu $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in R^{(\mathbb{N}_0)}$. Dann gibt es $i_0, j_0 \in \mathbb{N}_0$, so dass $a_i = 0$ und $b_j = 0$ für alle $i \geq i_0$ bzw. $j \geq j_0$. Damit ist

$$\sum_{i+j=m} a_i b_j = 0 \quad \text{für alle } m \geq i_0 + j_0,$$

was die Abgeschlossenheit unter Multiplikation zeigt.

□

Bemerkung 2.5.4 *Die Abbildung*

$$\begin{aligned}\varphi : R &\longrightarrow R^{(\mathbb{N}_0)}\\ a &\longmapsto (a, 0, \dots)\end{aligned}$$

ist ein injektiver Ringhomomorphismus, wie man direkt nachprüfen kann. Damit läßt sich R auffassen als Unterring von $R^{(\mathbb{N}_0)}$ und damit auch von $R^{\mathbb{N}_0}$.

Die gerade eingeführte Multiplikation erscheint auf den ersten Blick unnatürlich. Die Philosophie dahinter ist, dass zu dem m-ten Folgenglied des Produkts die Produkte all derjenigen Folgenglieder der Faktoren beitragen, deren Indizes in Summe gerade m ergeben. Wir können ein neues Symbol t wählen und den i-ten Eintrag einer Folge mit t^i markieren. Dann tragen zum

m-ten Glied des Produkts der Folgen $(a_i t^i)$ und $(b_j t^j)$ genau die Glieder bei, bei denen $t^i \cdot t^j = t^m$. Das erinnert doch schon sehr an das Produkt zweier Summen, wie wir es aus der Schule und den vorigen Semestern kennen. Deshalb kann man die folgen aus $R^{\mathbb{N}_0}$ und $R^{(\mathbb{N}_0)}$ auch mit Hilfe des neuen Symbols t als formale Summen schreiben und die oben definierte Multiplikation als Produkt der Summen auffassen.

Definition 2.5.5 *Sei R ein kommutativer Ring mit 1. Ein Element von $R^{\mathbb{N}_0}$ heißt* **formale Potenzreihe** *über R, ein Element von $R^{(\mathbb{N}_0)}$ heißt* **Polynom** *über R. Das i-te Folgenglied einer Potenzreihe oder eines Polynoms wird als i-ter* **Koeffizient** *bezeichnet. Das neutrale Element der Addition als das* **Nullpolynom**.
Für den Ring der formalen Potenzreihen über R schreiben wir

$$R[[t]] = \{f = \sum_{i=0}^{\infty} a_i t^i \mid (a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}\}$$

mit einem neuen Symbol t und sagen der Ring der formalen Potenzreihen über R in der Variablen t, für den Ring der Polynome über R schreiben wir analog

$$R[t] = \{f = \sum_{i=0}^{\infty} a_i t^i \mid (a_i)_{i\in\mathbb{N}_0} \in R^{(\mathbb{N}_0)}\}.$$

Bemerkung 2.5.6 *Sei R ein kommutativer Ring mit 1 und sei $f = \sum_{i=0}^{\infty} a_i t^i \in R[t]$. Dann sind nur endlich viele Koeffizienten von f nicht Null und es existiert ein maximales $i \in \mathbb{N}_0$ mit $a_i \neq 0$.*

Definition 2.5.7 *Sei R ein kommutativer Ring mit 1. Die Abbildung*

$$\begin{aligned} \deg : R[t] \setminus \{0\} &\longrightarrow \mathbb{N}_0 \\ \sum_{i=0}^{\infty} a_i t^i &\longmapsto \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\} \end{aligned}$$

heißt die **Gradabbildung**. *Für $f = \sum_{i=0}^{\infty} a_i t^i \in R[t]$ wird $\deg(f)$ als der* **Grad** *von f bezeichnet, $a_{\deg(f)}$ heißt der* **Leitkoeffizient** *von f, kurz $LC(f)$, $a_{\deg(f)} t^{\deg(f)}$ der* **Leitterm** *von f, kurz $LT(f)$.*
Wir setzen $\deg(0) := -\infty$.

Ist $\deg(f) = n$, so schreiben wir auch $\sum_{i=0}^{n} a_i t^i$ statt $\sum_{i=0}^{\infty} a_i t^i$.

Beobachtung 2.5.8

- *Ist R ein Körper, so ist $R[t]$ ein unendlich-dimensionaler Vektorraum mit Basis $(1, t, t^2, \dots)$.*
- *Seien $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i \in R[t]$ mit $a_n \neq 0 \neq b_m$. Dann gilt*

$$\deg(f+g) \leq \max\{n, m\}$$

da für alle $j > \max\{n, m\}$ gilt: $a_j = 0 = b_j$ und damit auch $a_j + b_j = 0$. Gleichheit gilt in der Ungleichung offensichtlich, falls $n \neq m$ gilt oder bei $n = m$ dann $a_n \neq -b_n$.

- *Seien f und g wie zuvor. Dann gilt*

$$\deg(f \cdot g) \leq n + m,$$

da für jedes $j > n + m$ gilt, dass $k + r = j$ nur gelten kann, wenn mindestens eine der beiden Ungleichungen $k > n$ und $r > m$ erfüllt ist. (Beachten Sie, dass $-\infty + m = -\infty = n - \infty$.)

Lemma 2.5.9 *Sei R kommutativer Ring mit 1 und seien $f, g \in R[t]$. Dann gilt:*

a) Sind die Leitkoeffizienten von f und g keine Nullteiler in R , so gilt

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

b) $R[t]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist.

c) Ist R Integritätsring, so gilt

$$(R[t])^* = \varphi(R^*)$$

mit dem injektiven Ringhomomorphismus aus Bemerkung 2.5.4.

Beweis: Seien $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i$ mit $a_n \neq 0 \neq b_m$. Sind a_n und b_m nicht Nullteiler in R, dann gilt $a_n \cdot b_m \neq 0$ und damit $\deg(f \cdot g) = n + m$, was Behauptung a) beweist.
Besitzt R Nullteiler, so sind diese mittels des injektiven Ringhomomorphismus φ aus Bemerkung 2.5.4 auch Nullteiler in $R[t]$. Besitzt andererseits $R[t]$ Nullteiler $f = \sum_{i=1}^{n} a_i t^i$ und $g = \sum_{i=1}^{m} b_i t^i$ mit $a_n \neq 0 \neq b_m$ und $f \cdot g = 0$, so muss der $n + m$-te Koeffizient von $f \cdot g$, also $a_n \cdot b_m$, ebenfalls Null sein, was