7.2 Matrizen und Elementare Umformungen

Grundlegende Objekte in den Überlegungen der Linearen Algebra waren nicht nur Körper und Vektorräume über diesen Körpern, sondern gerade für explizite Rechnungen auch Matrizen. In direkter Analogie zu den früheren Definitionen und Konstruktionen erhalten wir, sobald wir statt Körpern auch Ringe zulassen, den Begriff einer Matrix mit Einträgen aus einem Ring, worauf aufbauend genau die gleichen Operationen Addition, Skalarmultiplikation und Matrixmultiplikation definiert werden wie auf der Menge der Matrizen mit Einträgen aus einem Körper.

Analog zu dem in der Linearen Algebra betrachteten Spezialfall von Matrizen über Körpern, erhalten wir hier über einem Integritätsring R den R-Modul $R^{m\times n}$ von $m \times n$ Matrizen mit Einträgen in R sowie den Ring $R^{n\times n}$ der $n \times n$ Matrizen mit Einträgen in R. Auch der Begriff der Determinante läßt sich ohne Schwierigkeiten in diesen allgemeineren Kontext übertragen, indem man die Leibnizformel als Definition verwendet und dann die Eigenschaften nachweisst. Einzig die Tatsache, dass es Elemente in R gibt, die weder Null noch Einheit sind, benötigt hier einen weiteren Gedanken: Eine quadratische Matrix mit Einträgen aus R ist genau dann invertierbar, wenn ihre Determinante dies ist. (Man denke an die Formel für die Inverse mittels der Adjunkten.)

Definition 7.2.1 *Sei R ein Integritätsring und sei $n \in \mathbb{N}$. Dann bezeichnet $Gl(n, R)$ die Einheitengruppe des Matrizenringes $R^{n\times n}$, d.h.*

$$Gl(n, R) = \{A \in R^{n\times n} \mid A \text{ invertierbar}\} = \{A \in R^{n\times n} \mid \det(A) \in R^*\}.$$

Die Elemente von $Gl(n, R)$ bezeichnet man als **unimodulare** *Matrizen.*

Sie erinnern sich sicher aus der Linearen Algebra daran, dass uns die Matrizen in $Gl(n, K)$ Basiswechsel des K^n geliefert haben und uns so zum Begriff äquivalenter Matrizen führten. Das ist hier nicht anders.

Definition 7.2.2 *Sei R ein Integritätsring und seien $m, n \in \mathbb{N}$. Dann heissen zwei Matrizen $A, B \in R^{m\times n}$* **äquivalent**, *falls*

$$\exists P \in Gl(m, R),\ \exists Q \in Gl(n, R) : \quad B = PAQ.$$

Schon in der Linearen Algebra spielten die elementaren Zeilenoperationen und die Elementarmatrizen eine wichtige Rolle. Jede invertierbare Matrix

ließ sich aus solchen Matrizen durch Matrixmultiplikation zusammenbauen. Auch das werden wir hier wiedersehen, aber in diesem allgemeineren Kontext müssen wir wieder auf Ringelemente achten, die weder Null noch Einheit sind.

Erinnerung 7.2.3 *In der Linearen Algebra hatten wir drei verschiedene Formen von elementaren Zeilenumformungen für Matrizen $M \in K^{n\times n}$ kennengelernt, die wir jeweils mit Matrixmultiplikation mit einer geeigneten invertierbaren Matrix von links identifiziert hatten:*

$S_k(\lambda)$ *Multiplizieren der k-ten Zeile von M mit dem Faktor $\lambda \in K \setminus \{0\}$:* $S_k(\lambda) \cdot M$

$Q_{k,\ell}(\mu)$ *Addieren des μ-fachen der ℓ-ten Zeile von M zur k-ten Zeile von M ($k \neq \ell$), wobei $\mu \in K$:* $Q_{k,\ell}(\mu) \cdot M$

$P_{k,\ell}$ *Vertauschen der k-ten und ℓ-ten Zeile von M:* $P_{k,\ell} \cdot M$

Die Matrizen $S_k(\lambda)$, $Q_{k,\ell}(\mu)$ und $P_{k,\ell}$ wurden dabei aus der Einheitsmatrix durch Anwendung der entsprechenden elementaren Zeilenumformung erzeugt.

Bemerkung 7.2.4 *Sei R ein Integritätsring. Dann gibt es drei verschiedene Formen von elementaren Zeilenumformungen, die jeweils wieder mit der Matrixmultiplikation von links mit den folgenden Matrizen identifiziert werden können:*

$S_k(\lambda)$ *Multiplizieren der k-ten Zeile von M mit dem Faktor $\lambda \in R^*$:* $S_k(\lambda) \cdot M$

$Q_{k,\ell}(\mu)$ *Addieren des μ-fachen der ℓ-ten Zeile von M zur k-ten Zeile von M ($k \neq \ell$), wobei $\mu \in R$:* $Q_{k,\ell}(\mu) \cdot M$

$P_{k,\ell}$ *Vertauschen der k-ten und ℓ-ten Zeile von M:* $P_{k,\ell} \cdot M$

Die Matrizen $S_k(\lambda)$, $Q_{k,\ell}(\mu)$ und $P_{k,\ell}$ wurden dabei aus der Einheitsmatrix durch Anwendung der entsprechenden elementaren Zeilenumformung erzeugt.

Sehen Sie den einzigen Unterschied zur davor abgedruckten Erinnerung? Statt $\lambda \in K \setminus \{0\}$ ist nun $\lambda \in R^*$ gefordert, was aber wegen $K^* = K \setminus \{0\}$ doch keine grundlegende Änderung darstellt. Natürlich gelten auch weiterhin die strukturellen Eigenschaften der Elementarmatrizen, wie man direkt nachrechnen kann:

Lemma 7.2.5 *Sei R Integritätsring, seien $k, \ell \in \mathbb{N}$ mit $k \neq \ell$ und seien $\lambda \in R^*$ und $\mu \in R$. Dann gilt*

a) $S_k(\lambda)^T = S_k(\lambda)$

b) $Q_{k,\ell}(\mu)^T = Q_{\ell,k}(\mu)$

c) $P_{k,\ell}^T = P_{k,\ell}$

d) $S_k(\lambda)^{-1} = S_k(\lambda^{-1})$

e) $Q_{k,\ell}(\mu)^{-1} = Q_{k,\ell}(-\mu)$

f) $P_{k,\ell}^{-1} = P_{k,\ell}$

Wie im Vektorraumfall können wir auch hier Spaltenoperationen auf eine Matrix anwenden, indem wir die Transponierten der entsprechenden Elementarmatrizen (der passenden Zeilenoperation) von rechts an die Matrix multiplizieren. Insbesondere gilt folgende Aussage auch für freie R-Moduln:

Satz 7.2.6 *Sei R ein Integriätsring, seien $m, n \in \mathbb{N}$ und sei $A \in R^{m\times n}$. Die $m \times n$-Matrix B entstehe aus A durch elementare Zeilen- und Spaltenoperationen. Dann existieren $P \in Gl(m, R)$ und $Q \in Gl(n, R)$ mit*

$$B = PAQ.$$

Dabei ist P gerade das Produkt der zu den Zeilenumformungen gehörigen Elementarmatrizen und Q das der zu den Spaltenumformungen gehörigen.

Wie sieht es in diesem allgemeinere Kontext mit dem Gauß-Algorithmus und der Zeilenstufenform aus? Überträgt sich auch diese Theorie? Können wir eine Zeilenstufenform wie bei Vektorräumen durch elementare Zeilenumformungen der Form $Q_{k,\ell}(\mu)$ und $P_{k,\ell}$ erreichen? Läßt die Zeilenstufenform eine Lösbarkeitsentscheidung zu? Hier verläßt uns unser Glück, wie wir an den folgenden Bemerkungen direkt erkennen können:

Bemerkung 7.2.7 *Selbst eine einzige lineare Gleichung in 2 Unbekannten über einem Ring ist nicht immer lösbar. Man denke etwa an die folgende lineare Gleichung in zwei Unbekannten über $\mathbb{Z}$:*

$$4x + 6y = 3,$$

die nicht lösbar ist, da $\mathrm{ggT}(4, 6) = 2 \nmid 3$. Damit ist eine rein strukturelle Lösbarkeitsentscheidung etwa auf Basis einer Zeilenstufenform nicht möglich.

Zumindest über euklidischen Ringen kann durch Operationen der Form $Q_{k,\ell}(\mu)$ und $P_{k,\ell}$ tatsächlich eine Zeilenstufenform erreicht werden. Jedoch ist es deutlich aufwendiger als über einem Körper. Erinnern wir uns in Algorithmus 1 zuerst an den Algorithmus über einem Körper, den wir in der Linearen Algebra kennengelernt haben.

Algorithm 1 `ZSF (über Körpern)`

Input: $A \in K^{m\times n}$ über einem Körper K
Output: $Q \cdot A = \tilde{A} \in K^{m\times n}$ in ZSF mit Q Produkt elem. Zeilenoperationen

1: **if** $A == O_{mn}$ **then**
2: **return** A
3: $j = \min\{\ell \in \{1,\dots,n\} | \exists i \in \{1,\dots,m\} : a_{i\ell} \neq 0\}$
4: wähle $i \in \{1,\dots,m\}$ mit $a_{ij} \neq 0$
5: $A = P_{1i} \cdot A$
6: **for** $2 \leq k \leq m$ **do**
7: $A = Q_{k1}(-\frac{a_{kj}}{a_{1j}}) \cdot A$
8: $A_1 = (a_{11} \dots a_{1n})$, $B = (a_{(i+1)j})_{1\leq i\leq m-1, 1\leq j\leq n}$
9: **return** $\begin{pmatrix} A_1 \\ \hline \\ ZSF(B) \end{pmatrix}$

Schritt 7 von Algorithmus 1 ist über Ringen so offensichtlich nicht ausführbar, da die Invertierbarkeit von a_{1j} nicht gegeben ist. In euklidischen Ringen (und auch etwas allgemeiner in Hauptidealringen) läßt sich das jedoch geeignet ersetzen. Wir betrachten hier der Einfachheit halber nur euklidische Ringe, wo wir Schritt 7 von Algorithmus 1 in Algorithmus 2 durch eine Folge von Divisionen mit Rest ersetzen.

Haben Sie es in Algorithmus 2 erkannt? In Zeilen 6 bis 9 wird hier der euklidische Algorithmus für a_{ij} und a_{sj} in der inneren Schleife ausgeführt wird. Es wird also jeweils in der ersten von Null verschiedenen Spalte der größte gemeinsame Teiler aller Einträge gebildet und dieser dann an die Pivot-Position gesetzt. Auch hierbei treten nur Zeilenoperationen der Formen P_{kl} und $Q_{kl}(\mu)$ auf.

Algorithm 2 `ZSF (über euklidischen Ringen)`

Input: $A \in R^{m\times n}$ über euklid. Ring R
Output: $Q \cdot A = \tilde{A} \in R^{m\times n}$ in ZSF mit Q Produkt elem. Zeilenoperationen

1: **if** $A == O_{mn}$ **then**
2: **return** A
3: $j = \min\{k \in \{1,\dots,n\} | \exists i \in \{1,\dots,m\} : a_{ik} \neq 0\}$
4: **while** $\#\{i \mid a_{ij} \neq 0\} > 1$ **do**
5: wähle $i, s \in \{1,\dots,m\}$ mit $a_{ij} \neq 0$, $a_{sj} \neq 0$
6: **while** $a_{ij} \neq 0$ AND $a_{sj} \neq 0$ **do**
7: $A = Q_{is}(-(a_{ij} \operatorname{div} a_{sj}) \cdot A$
8: **if** $a_{ij} \neq 0$ **then**
9: $A = Q_{si}(-(a_{sj} \operatorname{div} a_{ij}) \cdot A$
10: $r =$ verbleibender Index mit $a_{ir} \neq 0$
11: $A = P_{1r} \cdot A$
12: $A_1 = (a_{11} \dots a_{1n})$, $B = (a_{(i+1)j})_{1\leq i\leq m-1, 1\leq j\leq n}$
13: **return** $\left(\begin{array}{c} A_1 \\ \hline \\ ZSF(B) \end{array}\right)$

Im Fall von quadratischen Matrizen impliziert das außerdem, dass sich die Determinante bei den verwendeten Operationen höchstens im Vorzeichen verändert. Eine reduzierte Gaußsche Normalform ist über Ringen allerdings im Allgemeinen nicht erreichbar, da dazu jedes Pivot-Element die Einträge darüber teilen müsste, wozu aber kein Grund besteht. Wir werden später einige Möglichkeiten kennenlernen, wie Matrizen über Ringen auf Normalform gebracht werden können.

7.3 Darstellende Matrizen und Smith-Normal-Form

Im vorigen Abschnitt haben wir gesehen, dass der Umgang mit Matrizen über Ringen sich nur in wenigen Punkten von den bekannten Tatsachen aus der Linearen Algebra unterscheidet. Eine besonders wichtige Verwendung von Matrizen bestand in der Linearen Algebra in der Beschreibung von Vektorraumhomomorphismen nach Wahl von Basen. Auch dies werden wir nun auf Homomorphismen freier Moduln über einem Integritätsring verallgemeinern.

Definition 7.3.1 *Sei R Integritätsring und sei $\varphi : M \longrightarrow N$ ein Homomorphismus von freien R-Moduln. Sei $\mathcal{B} = (x_1, \ldots, x_n)$ eine Basis von M und $\mathcal{C} = (y_1, \ldots, y_m)$ eine Basis von N. Dann heißt die Matrix $H = (h_{ij}) \in R^{m\times n}$ mit*

$$\varphi(x_j) = \sum_{i=1}^{m} h_{ij} y_i$$

die **darstellende Matrix** *von φ bzgl. $\mathcal{B}$ und $\mathcal{C}$, kurz $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$.*

Bemerkung 7.3.2 *Analog zur Linearen Algebra läßt sich direkt zeigen, dass ein R-Modul-Homomorphismus bereits durch Angabe der Bilder der Basiselemente festgelegt ist. Das Bild eines beliebigen Elements ergibt sich dann durch lineare Fortsetzung:*

$$\varphi(a) = \varphi(\sum_{j=1}^{n} \alpha_j x_j) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} h_{ij}\alpha_j \right) y_i.$$

Wie schon in der Linearen Aglebra bezeichnet man Matrizen $M_{\mathcal{C}}^{\mathcal{B}}(Id_M) \in R^{n\times n}$ als auch als **Transformationsmatrizen** *bzgl. der Basen $\mathcal{B}$ und $\mathcal{C}$ von M.*

Verwenden wir die Koordinatenisomorphismen $I_{\mathcal{B}}$ und $I_{\mathcal{C}}$ gemäß Satz 7.1.19 und definieren wir mittels der Matrix H aus Definition 7.3.1 einen R-Modulhomomorphismus

$$\begin{array}{rccc} F_H : R^{n\times 1} & \longrightarrow & R^{m\times 1} \\ a & \longmapsto & Ha, \end{array}$$

so sehen wir das bereits aus der Linearen Algebra bekannte kommutative Diagramm wieder:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ I_{\mathcal{B}} \downarrow & & \downarrow I_{\mathcal{C}} \\ R^{n\times 1} & \xrightarrow{F_H} & R^{m\times 1} \end{array}$$

Mit denselben Überlegungen wie im Fall der Vektorräume gilt:

Satz 7.3.3 *(Komposition von R-Modulhomomorphismen) Sei R ein Integritätsring und seien M_1, M_2 und M_3 endlich-erzeugte freie R-Moduln vom Rang m_1, m_2 bzw. m_3 mit Basen $\mathcal{B}_1$, $\mathcal{B}_2$ bzw. $\mathcal{B}_3$. Seien ausserdem $\varphi_1 : M_1 \longrightarrow M_2$ und $\varphi_2 : M_2 \longrightarrow M_3$ R-Modulhomomorphismen. Dann gilt*

$$M_{\mathcal{B}_3}^{\mathcal{B}_1}(\varphi_2 \circ \varphi_1) = M_{\mathcal{B}_3}^{\mathcal{B}_2}(\varphi_2) \cdot M_{\mathcal{B}_2}^{\mathcal{B}_1}(\varphi_1)$$

An dieser Stelle ist es beim Nacharbeiten sehr instruktiv, sich das zugehörige kommutative Diagramm, das aus der linearen Algebra bekannt ist, nochmals aufzuzeichnen. Machen Sie sich dabei die verschiedenen Wege durch das kommutative Diagramm bewusst.

Bemerkung 7.3.4 *Betrachtet man die Aussage des obigen Satzes im Falle eines Isomorphismus, der mit seiner Inversen verknüpft wird, so ergibt sich (bei Benennung der Basen mit $\mathcal{B}$ und $\mathcal{C}$ in der offensichtlichen Weise):*

$$E_n = M_{\mathcal{B}}^{\mathcal{B}}(\varphi^{-1} \circ \varphi) = M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1}) \cdot M_{\mathcal{C}}^{\mathcal{B}}(\varphi),$$

womit direkt klar ist, dass

$$M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1}) = (M_{\mathcal{C}}^{\mathcal{B}}(\varphi))^{-1}.$$

Auch das kommutative Diagramm für den Basiswechsel, das wir im Vektorraumfall in der Linearen Algebra ausführlich besprochen haben, sehen wir hier wieder. Auch hier ist nur der Satz aufgeführt, das Erstellen des Diagramms bleibt den Studierenden beim Nacharbeiten überlassen.

Satz 7.3.5 *(Basiswechsel) Sei R ein Integritätsring und seien M, N freie R-Moduln vom Rang m bzw. n. Seien weiterhin $\mathcal{B}$ und $\mathcal{B}'$ Basen von M*

und $\mathcal{C}$ und $\mathcal{C}'$ Basen von N. Sei schließlich $\varphi : M \longrightarrow N$ ein R-Modul-Homomorphismus. Dann gilt:

$$M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) = M_{\mathcal{C}'}^{\mathcal{C}}(Id_N) \cdot M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \cdot M_{\mathcal{B}}^{\mathcal{B}'}(Id_M),$$

wobei $M_{\mathcal{C}'}^{\mathcal{C}}(Id_N) \in Gl(n,R)$ und $M_{\mathcal{B}}^{\mathcal{B}'}(Id_M) \in Gl(m,R)$. Insbesondere sind darstellende Matrizen der selben Abbildung zu unterschiedlichen Basen zueinander äquivalente Matrizen.
Ist umgekehrt eine Matrix H darstellende Matrix eines R-Modul-Homomorphismus zwischen freien Moduln bzgl. fester Basen und ist H' eine dazu äquivalente Matrix, so ist H' darstellende Matrix derselben Abbildung bzgl. anderer geeigneter Basen.

In der Linearen Algebra hatte sich der Begriff der Äquivalenz von Matrizen als relativ unspektakulär herausgestellt, wie der folgende Satz (5.5.1 in der Linearen Algebra) zeigte:

Erinnerung 7.3.6 *Seien V, W K-Vektorräume der Dimensionen $\dim_K(V) = n$ und $\dim_K(W) = m$. Sei $\varphi : V \longrightarrow W$ ein K-Vektorraum-Homomorphismus mit Rang $rk(\varphi) = r$. Dann existieren Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W mit*

$$M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \left(\begin{array}{c|c} E_r & 0_{r,n-r} \\ \hline 0_{m-r,r} & 0_{m-r,n-r} \end{array}\right).$$

Das folgende Beispiel zeigt jedoch, dass die Aussage im Fall von Moduln nicht mehr so langweilig sein wird:

Beispiel 7.3.7 *Sei $R = \mathbb{Z}$, $M = N = R^1$ mit Basis (e_M) bzw. (e_N). Sei ferner $\varphi : M \longrightarrow N$ der Homomorphismus, der durch $\varphi(e_M) = 3 \cdot e_N$ eindeutig festgelegt wird. Dann ist die darstellende Matrix gerade*

$$A = \begin{pmatrix} 3 \end{pmatrix}.$$

Es gibt aber keine Basen von M und N, als $\mathbb{Z}$-Moduln bzgl. derer die darstellende Matrix die 1×1-Einheitsmatrix wäre. Einerseits ist $(3 \cdot 1_N)$ kein Erzeugendensystem und damit keine Basis von N, andererseits läßt sich $\frac{1}{3} \cdot 1_M$ nicht in M bilden.

Die Erweiterung von Erinnerung 7.3.6 auf den Fall von Moduln ist die Smith-Normalform, die man für Moduln über Hauptidealringen stets erreichen kann. Wir werden sie hier aus praktischen Gründen nur für euklidische Ringe formulieren und in diesem Fall auch einen Algorithmus zu ihrer Berechnung angeben.