Satz 7.3.8 *(Smith-Normalform) Sei R ein euklidischer Ring und sei $H \in R^{m\times n}$. Dann existieren $P \in GL(m,R)$ und $Q \in GL(n,R)$ sowie ein $1 \leq \ell \leq \min\{m,n\}$ mit*

$$PHQ = S = \begin{pmatrix} s_1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & s_2 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \\ 0 & 0 & \dots & s_{\ell-1} & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & s_\ell & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \in R^{m\times n}$$

in Diagonalgestalt, wobei $s_1, \dots, s_\ell \in R \setminus \{0\}$ und $s_i \mid s_{i+1}$ für alle $1 \leq i \leq \ell - 1$.
Die Matrix S wird als in **Smith-Normalform** *bezeichnet, die Ringelemente $s_1, \dots s_\ell$ heißen die* **Elementarteiler** *von H und sind bis auf Assoziiertheit eindeutig bestimmt.*

In dem obigen Satz ist P das Produkt von Elementarmatrizen, die zu elementaren Zeilenumformungen gehören, und Q das Produkt von Elementarmatrizen, die zu elementaren Spaltenumformungen gehören.

Die Idee der Berechnung greift die Gedanken auf, die bereits bei der Berechnung der Zeilenstufenform für Matrizen über Ringen verwendet wurden: Schritte des Gauß-Algorithmus wirken mit solchen des euklidischen Algorithmus zusammen.

Ein naiver, nicht effizienter Algorithmus zur Berechnung der Smith-Normalform ist in Algorithmus 4 wiedergegeben. Zur besseren Lesbarkeit des Algorithmus 4 wird dabei der bereits aus Algorithmus 2 bekannte Block mit dem euklischen Algorithmus als eigene Methode Algorithmus 3 ausgekoppelt.

Auf einen bis ins letzte Detail ausgeführten formalen Beweis der Korrektheit und Terminierung der beiden Algorithmen verzichten wir hier. Dennoch diskutieren wir eingehend alle für den Beweis notwendigen Argumente. Noch eine letzte warnende Bemerkung: Im Deutschen ist sowohl die Zeile einer Matrix (englisch: row) eine Zeile als auch die Zeile eines Algorithmus (englisch: line). Darauf sollten Sie beim Lesen der folgenden Erläuterungen achten.

Algorithm 3 `SpalteAusräumen`

Input: $A \in R^{m\times n}$ über euklid. Ring R, j Spaltenindex
Output: $\tilde{A} = P \cdot A \in R^{m\times n}$, mit geeignetem $P \in Gl(m, R)$, so dass in Spalte j nur Eintrag a_{jj} nicht Null ist

1: **while** $\#\{i \mid a_{ij} \neq 0\} > 1$ **do**
2: wähle $i, s \in \{1, \ldots, m\}$ mit $a_{ij} \neq 0$, $a_{sj} \neq 0$ geeignet[2]
3: **while** $a_{ij} \neq 0$ AND $a_{sj} \neq 0$ **do**
4: $A = Q_{is}(-(a_{ij} \operatorname{div} a_{sj}) \cdot A$
5: **if** $a_{ij} \neq 0$ **then**
6: $A = Q_{si}(-(a_{sj} \operatorname{div} a_{ij}) \cdot A$
7: $\ell =$ Zeilenindex des einzigen Nicht-Null-Eintrag in Spalte j
8: $A = P_{j\ell} \cdot A$
9: **return** A

Betrachten wir zuerst Algorithmus 3: Die Schritte des Algorithmus haben wir bereits bei der Zeilenstufenform verwendet. Dort waren sie auf die führende Nicht-Null-Spalte angewandt worden und konnten daher weiter links in der Matrix keinen Schaden anrichten. In der hier gewählten Formulierung ist das jedoch nicht mehr der Fall. Insbesondere wird am Ende auch noch der einzige von Null verschiedene Eintrag, der in der Spalte j verblieben ist, auf die Position (j, j) gesetzt. Es können tatsächlich alle Einträge außerhalb der Spalte j durch die verwendeten Zeilenoperationen verändert worden sein. Dass dies nicht zu einer erneuten Verschlechterung der Matrix führt muss also im aufrufenden Algorithmus sichergestellt werden.
Die Terminierung des Algorithmus beruht inhaltlich darauf, dass die innere `WHILE`-Schleife in Zeile 3 bis 6 einen euklidischen Algorithmus auf den Einträgen a_{ij} und a_{sj} ausführt und dabei jeweils den Rest der Zeile mitschleppt. Der euklidische Algorithmus terminiert, wie wir aus Abschnitt 2.7 wissen. Da bei jedem Verlassen dieser inneren `WHILE`-Schleife ein weiterer Eintrag der Spalte den Wert 0 erhalten hat, kann die in Zeile 1 beginnende äußere `WHILE`-Schleife höchstens $m - 1$ Durchläufe benötigen, ehe keine 2 von Null verschiedene Einträge mehr vorhanden sind, und die Terminierung des Algorithmus 3 ist damit gezeigt.

[2]Mindestens ist folgende Regel bei der Auswahl zu beachten: Ist a_{ij} der einzige von Null verschiedene Eintrag in der Zeile i und teilt a_{ij} alle anderen von Null verschiedenen a_{sj}, so sollten diese durch Abziehen geeigneter Vielfacher de Zeile i zu Null reduziert werden.

Algorithm 4 `SNF (über euklidischen Ringen)`

Input: $A \in R^{m\times n}$ über euklid. Ring R
Output: $S \in R^{m\times n}$ in SNF mit $\exists P \in Gl(m,R), Q \in Gl(n,R) : P \cdot A \cdot Q = S$

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: $A = A \cdot P_{1j}$
5: **while** $\#(\{(i,1) \mid a_{i1} \neq 0\} \cup \{(1,\ell) \mid a_{1\ell} \neq 0\}) > 1)$ **do**
6: $A = \texttt{SpalteAusräumen}(A, 1)$
7: $A = (\texttt{SpalteAusräumen}(A^T, 1))^T$
8: **if** $(n == 1$ oder $m == 1)$ **then**
9: **return** A
10: $B = \begin{pmatrix} a_{22} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{m2} & \dots & a_{mn} \end{pmatrix}$
11: $A = \left(\begin{array}{c|c} a_{11} & 0_{1(n-1)} \\ \hline 0_{(m-1)1} & SNF(B) \end{array}\right)$
12: **for** $1 \leq i < \min\{m,n\}$ **do**
13: **if** $a_{ii} \nmid a_{(i+1)(i+1)}$ **then**
14: $A = A \cdot Q_{(i+1)i}(1)$
15: $A = \texttt{SpalteAusräumen}(A, i)$
16: $A = (\texttt{SpalteAusräumen}(A^T, i))^T$
17: **return** A

Wenden wir uns nun zuerst der Terminierung von Algorithmus 4 zu. Dabei gibt es zwei mögliche Problempunkte: einerseits die Rekursionstiefe der Rekursion in Zeile 11 und andererseits das Terminieren der `WHILE`-Schleife in Zeilen 5 bis 7. Da in der Rekursion in Zeile 11 aber die Matrix B stets eine Zeile weniger besitzt als die Matrix A, kann die Rekursionstiefe die Zeilenzahl m der ursprünglichen Matrix nicht übersteigen. Es bleibt also die `WHILE`-Schleife zu betrachten. In Zeile 6 wird ein größter gemeinsamer Teiler der Einträge der Spalte 1 gebildet und auf die Position $(1,1)$ gesetzt, was natürlich die Einträge der ersten Zeile verändert. In Zeile 7 geschieht dann dasselbe mit der ersten Zeile, wobei wiederum Nicht-Null-Einträge in der ersten Spalte zustande kommen können. Da aber der Eintrag a_{11} den größten gemeinsamen Teiler des vorigen Schritts enthält, fallen in jedem Schritt in

Zeile 6 bzw. Zeile 7 höchstens Faktoren des zuletzt berechneten ggT weg. Fällt in einem Durchlauf in Zeile 6 kein Faktor mehr weg, so war a_{11} bereits Teiler aller Einträge der ersten Spalte und Algorithmus 3 führt daher keine von Null verschiedenen Einträge in ersten Zeile der Matrix mehr ein. Der Eintrag a_{11} ist damit der einzige von Null verschiedene in der ersten Zeile und Spalte und die Schleife endet. Dasselbe Argument gilt entsprechend transponiert auch für Zeile 7 von Algorithmus 4. Damit ist die Terminierung von Algorithmus 4 geklärt.

Zur Korrektheit von Algorithmus 4 gehen wir induktiv nach der Zahl der Zeilen von A vor, was zum rekursiven Aufbau des Algorithmus passt. Besitzt A nur eine Zeile, so wird A bis Zeile 6 nicht verändert und in Zeile 7 wird die erste Zeile auf die Form $(\mathrm{ggT}(a_{11}, \ldots, a_{1n}), 0, \ldots, 0)$ gebracht, womit auch die Schleife verlassen wird. Die Bedingung in Zeile 8 ist erfüllt und der Algorithmus in Zeile 9 verlassen, wobei A in trivialer Weise die Bedingungen an eine Smith-Normal-Form erfüllt.
Im Induktionsschritt betrachten wir nun eine Matrix A mit m Zeilen, die nicht die Nullmatrix ist. Zeile 4 des Algorithmus sorgt dann dafür, dass die erste Spalte keine Nullspalte ist. Nach der Schleife in den Zeilen 5 bis 7 hat dann die Matrix A, wie oben schon besprochen, die Struktur

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

Wobei die rechte untere $(m-1) \times (n-1)$-Matrix gerade durch Zeile 11 des Algorithmus auf Smith-Normal-Form gebracht wird. Insbesondere sind nur die ersten k Diagonalelemente von $SNF(B)$ (für ein geeignetes $0 \leq k \leq \min(m, n) - 1$) von Null verschieden und sie erfüllen die Teilbarkeitsbedingung der Smith-Normalform. Zu diesem Zeitpunkt kann also nur noch eine Teilbarkeitsbedingung $a_{11} \mid a_{ii}$ verletzt sein für ein $i > 1$; wegen der bereits erreichten Smith-Normal-Form des rechten unteren Blocks muss damit aber auch gelten $a_{11} \nmid a_{22}$. Der erste Durchlauf der `FOR`-Schleife in Zeilen 12 bis 16 addiert somit in Zeile 14 die zweite Spalte der Matrix auf die erste, so dass in Zeile 15 $\mathrm{ggT}(a_{11}, a_{22})$ nach a_{11} geschrieben wird, wobei wegen der Struktur der Matrix an Position $(1, 2)$ ein Vielfaches von a_{22} neu zustande kommt, das aber wegen Teilbarkeit dann in Zeile 16 des Algorithmus ohne Folgen für

die erste Spalte gelöscht werden kann. Zu diesem Zeitpunkt ist sichergestellt, dass das neue a_{11} das neue a_{22} und auch alle weiteren a_{ii} teilt. (Überlegen Sie, warum.) Ungeschickterweise kann das neue a_{22} nun weitere Faktoren erhalten haben, so dass die Teilbarkeitsbedingung $a_{22} \mid a_{33}$ verletzt sein kann, die dann aber im folgenden Schleifendurchlauf repariert wird. Unter Iteration dieses Vorgehens ist schließlich nach spätestens $\min(m,n)-1$ Durchläufen der Schleife auch die Teilbarkeitsbedingung an die Smith-Normal-Form erfüllt.

Bemerkung 7.3.9 *Zu einer gegebenen Matrix $H \in R^{m\times n}$ über einem euklidischen Ring R lassen sich Ideale betrachten, die von allen Determinanten von Untermatrizen von H einer festen Größe erzeugt werden. Ist die Größe der Untermatrizen $k \times k$, so bezeichnet man dieses Ideal als das Ideal der* **k-Minoren** *von H. Minorenideale bleiben unter elementaren Zeilenoperationen vom Typ P_{ij} und $Q_{ij}(\mu)$ angewandt auf H unverändert*[3]*. Dies läßt direkt einsehen, wenn man in einer Fallunterscheidung für jede der Operationen die Fälle untersucht, in denen 0 bzw. 1 bzw. 2 Zeilen einer Untermatrix durch die elementare Zeilenoperation verändert wurden und sich klarmacht, warum sich insgesamt am Ideal nichts geändert hat.*
Die in Satz 7.3.8 eingeführten und in Algorithmus 4 berechneten Elementarteiler $s_1, \ldots, s_\ell$ der Matrix H stehen zu den Minorenidealen von H in engem Zusammenhang: Für $1 \leq k \leq \ell = \mathrm{rk}(H)$ ist das Ideal der k-Minoren von H erzeugt durch das Element $(\prod_{i=1}^{k} s_i)$. Damit wissen wir, dass die Elementarteiler einer Matrix bis auf Assoziiertheit eindeutig bestimmt sind. Ganz nebenbei eröffnet diese andere Interpretation der Elementarteiler auch einen alternativen Weg zu ihrer Berechnung mittels Minorenidealen und Euklidischem Algorithmus. Dieser Weg ist zwar ebenfalls nicht effizient, jedoch bisweilen hilfreich.

Bemerkung 7.3.10 *Mit Hilfe der in der vorigen Bemerkung eingeführten Minorenideale läßt sich auch der Rang einer Matrix, der in der Linearen Algebra als die maximale Anzahl linear unabhängiger Zeilen (bzw. Spalten) definiert war, auf Matrizen über (geeigneten) Ringen verallgemeinern. Die Maximalzahl linear unabhängiger Zeilen kann im Vektorraumfall als das größte $k \in \mathbb{N}$ charakterisiert werden, so dass das Ideal der k-Minoren nicht das Nullideal ist. Diese Charakterisierung wird für Matrizen über Hauptidealringen als Definition verwendet und ist genau das ℓ aus der Smith-Normal-Form.*

[3] und natürlich auch unter Anwendung von elementaren Spaltenoperationen vom Typ P_{ij}^T und $Q_{ij}(\mu)^T$

Wir hatten bereits zu Beginn des Abschnitts betont, dass wir an Matrizen über einem Ring R insbesondere zur Beschreibung von Homomorphismen freier R-Moduln interessiert sind. Daher werden wir nun die Erkenntnisse über die Smith-Normal-Form einer Matrix umformulieren in den Elementarteilersatz für endlich-erzeugte, freie R-Moduln. Wie zuvor bei der Smith-Normal-Form gilt der Satz nicht nur über euklidischen Ringen, sondern auch etwas allgemeiner über Hauptidealringen.

Satz 7.3.11 *Sei R ein euklidischer Ring und seien M, N freie R-Moduln vom endlichen Rang m bzw. n. Sei weiterhin $\varphi : N \longmapsto M$ ein R-Modul-Homomorphismus. Dann existieren Basen $\mathcal{B} = (v_1, \ldots, v_n)$ von N und $\mathcal{C} = (w_1, \ldots, w_m)$ von M, ein $\ell \in \mathbb{N}_0$ mit $0 < \ell \leq \min(n, m)$ sowie $s_1, \ldots, s_\ell \in R \setminus \{0\}$, so dass $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ in Smith-Normal-Form ist mit Elementarteilern $s_1, \ldots, s_\ell$. Diese heißen auch die* **Elementarteiler** *von φ.*

Wie oben schon bemerkt, ist ℓ der Rang der Matrix bzw. des R-Modul-Homomorphismus. Die Elementarteiler eines Homomorphismus sind (wie schon vorher die einer Matrix) bis auf Assoziiertheit eindeutig bestimmt.

Beweis: Seien $\mathcal{B}'$ und $\mathcal{C}'$ beliebige Basen von N bzw. M. Dann ist $A = M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi)$ eine $m \times n$ Matrix mit Einträgen aus R und wir können Satz 7.3.8 auf A anwenden. Dabei liefern uns die invertierbaren quadratischen Matrizen $P \in Gl(m, R)$ und $Q \in Gl(n, R)$ gerade Basiswechsel in neue Basen, bzgl. derer die Matrix des Homomorphismus in Smith-Normal-Form ist, d.h.

$$S = P \cdot A \cdot Q = M_{\mathcal{C}}^{\mathcal{C}'}(id_M) \cdot M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) \cdot M_{\mathcal{B}'}^{\mathcal{B}}(id_N).$$

□

Korollar 7.3.12 *In der Notation des vorigen Satzes gilt:*

a) $(s_1 w_1, \ldots, s_\ell w_\ell)$ *ist Basis von* $\mathrm{Im}(\varphi)$

b) $(v_{\ell+1}, \ldots, v_n)$ *ist Basis von* $\ker(\varphi)$

c) $\ell = \mathrm{rk}(\mathrm{Im}(\varphi))$

d) $n - \ell = \mathrm{rk}(\ker(\varphi))$

e) $n = \mathrm{rk}(\mathrm{Im}(\varphi)) + \mathrm{rk}(\ker(\varphi))$