

## 8.7 Ganzzahlige Elimination

Wie löst man lineare Gleichungssysteme über dem Ring  $\mathbb{Z}$  der ganzen Zahlen? Wie berechnet man Determinanten? Wie findet man eine inverse Matrix? Wie in der bekannten linearen Algebra über Körpern ist auch in der allgemeineren Situation über Ringen die *Trigonalisation* von Matrizen der Schlüssel zu effizienten Algorithmen.

Einen etwas hinreichend allgemeinen Rahmen liefern folgende drei Klassen von Ringen (kommutativ, nullteilerfrei, mit 1):

- **faktorielle Ringe** = ZPE-Ringe: Alle Elemente haben eine Primzerlegung, insbesondere gibt es zu je zwei Elementen einen größten gemeinsamen Teiler ggT.
- **Hauptidealringe**: Jedes Ideal ist Hauptideal. Hauptidealringe sind faktoriell, und jeder ggT zweier Elemente lässt sich linear aus diesen kombinieren.
- **Euklidische Ringe**: Es gibt eine Division mit Rest. Euklidische Ringe sind Hauptidealringe; ein ggT zweier Elemente lässt sich samt seiner linearen Darstellung effizient mit dem erweiterten euklidischen Algorithmus bestimmen.

Die Menge der invertierbaren Matrizen mit Determinante 1 wird als  $SL_n(R) \subseteq GL_n(R)$  bezeichnet.

**Hilfssatz 4** Sei  $R$  ein Hauptidealring,  $a_1, \dots, a_n \in R$ ,  $d$  ein ggT( $a_1, \dots, a_n$ ). Dann gibt es eine invertierbare Matrix  $U \in SL_n(R)$  mit

$$U \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

*Beweis.* Sind alle  $a_i = 0$ , ist die Behauptung trivial. Ansonsten kann man (nach einer eventuellen Permutation) o. B. d. A.  $a_1 \neq 0$  annehmen. Da der Fall  $n = 1$  ebenfalls trivial ist, kann man auch  $n \geq 2$  annehmen.

Sei  $d_2 := \text{ggT}(a_1, a_2)$  (gemeint ist ein ggT) – dann ist  $d_2 \neq 0$  – und allgemeiner  $d_i = \text{ggT}(a_1, \dots, a_i) = \text{ggT}(d_{i-1}, a_i)$  für  $i = 3, \dots, n$ . Nun ist  $d_2 = c_1 a_1 + c_2 a_2$  Linearkombination. Damit gilt die Gleichung

$$\begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 a_1 + c_2 a_2 \\ -\frac{a_2 a_1}{d_2} + \frac{a_1 a_2}{d_2} \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix}$$

mit der invertierbaren Koeffizientenmatrix

$$C = \begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \quad \text{mit } \text{Det } C = \frac{c_1 a_1}{d_2} + \frac{c_2 a_2}{d_2} = 1.$$

Dann geht es mit vollständiger Induktion weiter: Im allgemeinen Schritt sei schon

$$U' \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \\ a_i \\ \vdots \\ a_n \end{pmatrix} \quad \text{mit } a_i \neq 0$$

erreicht. Dann formt man genauso wie eben zwei Koordinaten um:

$$\begin{pmatrix} d' \\ a_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} d'' \\ 0 \end{pmatrix};$$

damit wird sukzessive die Matrix  $U$  aufgebaut.  $\diamond$

**Bemerkung.** Die Inverse der Matrix  $C$  im Beweis ist

$$C^{-1} = \begin{pmatrix} \frac{a_1}{d_2} & -c_2 \\ \frac{a_2}{d_2} & c_1 \end{pmatrix}$$

Daraus folgt, dass  $U$  und  $U^{-1}$  zusammen durch höchstens  $n - 1$ -fache Anwendung des euklidischen Algorithmus bestimmbar sind, dazu  $n - 1$  Multiplikationen von  $n \times n$ -Matrizen.

Damit lassen sich Matrizen trigonalisieren. (Eine genauere Betrachtung führt zur HERMITESchen Normalform.)

**Satz 8** (i) Sei  $R$  ein Hauptidealring und  $A \in M_{pq}(R)$ . Dann gibt es eine invertierbare Matrix  $U \in SL_p(R)$  so dass  $H = UA$  die Gestalt

$$\begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ & & * \\ 0 & & \end{pmatrix} \quad \text{für } p \geq q, \quad \begin{pmatrix} * & \dots & \dots & * \\ & \ddots & \dots & \\ & & \dots & \\ 0 & & & * \end{pmatrix} \quad \text{für } p < q$$

hat.

(ii) Ist  $R$  euklidisch, so lassen sich  $U$  und  $U^{-1}$  gemeinsam mit höchstens  $\frac{p(p-1)}{2}$  Durchführungen eines erweiterten euklidischen Algorithmus bestimmen.

**Spezialfall.** Zu einer quadratischen Matrix  $A \in M_{pp}(R)$  wird  $H = UA$  bestimmt. Dann ist

$$\text{Det } A = \text{Det } H = h_{11} \cdots h_{pp}.$$

Ist  $A$  invertierbar, so ist  $A^{-1} = (U^{-1}H)^{-1} = H^{-1}U$ . Dabei ist  $H^{-1}$  für die Dreiecksmatrix  $H$  trivial zu bestimmen. Determinantenberechnung und Invertierung sind also auf die Trigonalisierung zurückgeführt.

*Beweis.* Der Beweis besteht in der Angabe eines Algorithmus. Sei  $r := \min\{p, q\}$ . Der Algorithmus wird initialisiert durch

$$H := A, \quad U := \mathbf{1}_p, \quad V := \mathbf{1}_p.$$

Es wird eine Schleife über  $j = 1, \dots, r$  durchgeführt; invariante Relationen sind dabei  $UA = H$ ,  $UV = \mathbf{1}_p$ .

- Im  $j$ -ten Durchlauf sehe  $H$  zu Beginn so aus:

$$\begin{pmatrix} * & & & & \\ & \ddots & & & * \\ & & * & & \\ & & & h_{jj} & \\ & 0 & & \vdots & \\ & & & & h_{pj} \end{pmatrix}$$

Falls  $h_{jj} = \dots = h_{pj} = 0$ , sind wir mit diesem Durchlauf fertig. Sonst wird nach dem Hilfssatz eine Matrix  $U' \in SL_{p-j+1}(R)$  zusammen mit  $(U')^{-1}$  gewonnen mit

$$U' \begin{pmatrix} h_{jj} \\ \dots \\ h_{pj} \end{pmatrix} = \begin{pmatrix} d_j \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

Es ist  $\begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} \in SL_p(R)$ . Man setzt als Ergebnis des Schleifendurchlaufs

$$U := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} U, \quad H := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} H, \quad V := V \begin{pmatrix} \mathbf{1} & 0 \\ 0 & (U')^{-1} \end{pmatrix}.$$

Nach dem letzten Schleifendurchlauf haben  $U$  und  $H$  die gewünschte Gestalt.  
 $\diamond$

Wie invertiert man nun eine Matrix  $A \in GL_q(\mathbb{Z}/n\mathbb{Z})$ ? Dazu fasst man  $A$  als ganzzahlige Matrix auf und bestimmt nach Satz 8 ein  $U \in SL_q(\mathbb{Z})$ , so dass  $H = UA$  ganzzahlige obere Dreiecksmatrix ist. Bei Reduktion mod  $n$  bleibt die Gleichung  $H = UA$  erhalten und ebenso  $A^{-1} = H^{-1}U$ ; da  $A$  mod  $n$  invertierbar ist, müssen alle Diagonalelemente von  $H$  mod  $n$  invertierbar sein.