

## Matrizen über Ringen<sup>1</sup>

Sei  $R$  ein Ring (kommutativ mit 1). Die „multiplikative Gruppe“ von  $R$  ist die Gruppe der invertierbaren Elemente, also

$$R^\times = \{a \in R \mid ab = 1 \text{ für ein } b \in R\} = \{a \in R \mid a|1\}.$$

Ebenso betrachtet man in der (nichtkommutativen)  $R$ -Algebra  $M_{qq}(R)$  der  $q \times q$ -Matrizen über  $R$  die Gruppe der invertierbaren Elemente

$$GL_q(R) = \{A \in M_{qq}(R) \mid AB = \mathbf{1}_q \text{ für ein } B \in M_{qq}(R)\}.$$

Die Determinante definiert eine multiplikative Abbildung

$$\text{Det}: M_{qq}(R) \longrightarrow R.$$

Klar ist:

$$\begin{aligned} A \in GL_q(R) \implies AB = \mathbf{1}_q \text{ für ein } B \implies \text{Det } A \cdot \text{Det } B &= \text{Det } \mathbf{1}_q = 1 \\ \implies \text{Det } A \in R^\times. \end{aligned}$$

Zum Beweis der Umkehrung betrachtet man die adjungierte Matrix  $\tilde{A} = (\tilde{a}_{ij})$  mit

$$\tilde{a}_{ij} = A_{ji} = \text{Det} \begin{pmatrix} a_{11} & \dots & a_{1,i-1} & a_{1,i+1} & \dots & a_{1q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{j-1,1} & \dots & a_{j-1,i-1} & a_{j-1,i+1} & \dots & a_{j-1,q} \\ a_{j+1,1} & \dots & a_{j+1,i-1} & a_{j+1,i+1} & \dots & a_{j+1,q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{q1} & \dots & a_{q,i-1} & a_{q,i+1} & \dots & a_{qq} \end{pmatrix}$$

Damit kann man zeigen:

**Satz 1** Für  $A \in M_{qq}(R)$  gilt

- (i)  $A\tilde{A} = \text{Det } A \cdot \mathbf{1}_q$ .
- (ii)  $A \in GL_q(R) \iff \text{Det } A \in R^\times$ ; ist dies der Fall, so

$$A^{-1} = \frac{1}{\text{Det } A} \tilde{A}.$$

*Beweis.* (i) ist der Determinanten-Entwicklungssatz.

(ii) folgt sofort aus (i).  $\diamond$

**Beispiel.** Im Falle  $R = \mathbb{Z}/n\mathbb{Z}$  kann man das so formulieren:

$$A \in M_{qq} \text{ ist invertierbar mod } n \iff \text{Det } A \text{ ist zu } n \text{ teilerfremd.}$$

---

<sup>1</sup>Klaus Pommerening, Kryptologie; 21. Juni 2002, letzte Änderung: 1. Juli 2002

## Bemerkungen

1. Der Rechenaufwand zur Berechnung der inversen Matrix  $A^{-1}$  beträgt bei naiver Anwendung von (ii):

- Eine  $q \times q$ -Determinante aus  $q!$  Summanden zu je  $q$  Faktoren,
- $q^2$  Stück  $(q-1) \times (q-1)$ -Determinanten.

Das ist sehr ineffizient – nämlich exponentiell in  $q$ .

2. Mit GAUSSscher Elimination sinkt der Aufwand auf  $O(q^3)$ . Der Haken dabei ist, dass beim exakten Rechnen rationale Zahlen mit *riesigen* Zählern und Nennern auftreten.

3. Ein modifiziertes rein ganzzahliges Eliminationsverfahren ist effizienter, siehe im nächsten Abschnitt, kann aber immer noch recht große Zwischenergebnisse liefern.

4. Ein Ringhomomorphismus  $\varphi: R \rightarrow R'$  induziert einen  $R$ -Algebra-Homomorphismus  $\varphi_q: M_{qq}(R) \rightarrow M_{qq}(R')$ . Ist  $A \in M_{qq}$  invertierbar, so

$$\varphi_q(A)\varphi_q(A^{-1}) = \varphi_q(AA^{-1}) = \varphi_q(\mathbf{1}_q) = \mathbf{1}_q,$$

also ist auch  $\varphi(A)$  invertierbar.

Allgemeiner gilt  $\text{Det } \varphi_q(A) = \varphi(\text{Det } A)$ , d.h., das Diagramm

$$\begin{array}{ccc} M_{qq}(R) & \xrightarrow{\varphi_q} & M_{qq}(R') \\ \text{Det} \downarrow & & \downarrow \text{Det} \\ R & \xrightarrow{\varphi} & R' \end{array}$$

ist kommutativ.

Im Fall  $R = \mathbb{Z}$  kann man die Restklassen-Homomorphismen  $\mathbb{Z} \rightarrow \mathbb{F}_p$  ( $p$  prim) für genügend viele Primzahlen  $p$  ausnützen – so dass deren Produkt garantiert  $> \text{Det } A$  ist –, indem man:

- alle  $\text{Det } A \bmod p$  berechnet (ohne riesige Zwischenergebnisse!),
- $\text{Det } A$  daraus mit dem chinesischen Restsatz bestimmt. [Siehe nächstes Kapitel der Vorlesung.]