1 Matrices over Rings

Let R be a ring (commutative with 1). The "multiplicative group" of R is the group of invertible elements

$$R^\times = \{a \in R \mid ab = 1 \text{ for some } b \in R\} = \{a \in R \mid a \text{ divides } 1\}.$$

In the same way the (non-commutative) R-algebra $M_{qq}(R)$ of $q \times q$-matrices over R has a group of invertible elements ("general linear group")

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

The determinant defines a multiplicative map

$$\operatorname{Det}\colon M_{qq}(R) \longrightarrow R,$$

and

$$A \in GL_q(R) \Longrightarrow AB = \mathbf{1}_q \text{ for some } B \Longrightarrow \operatorname{Det} A \cdot \operatorname{Det} B = \operatorname{Det} \mathbf{1}_q = 1$$

$$\Longrightarrow \operatorname{Det} A \in R^\times.$$

The converse implication is also true. For a proof we consider the adjoint matrix $\tilde{A} = (\tilde{a}_{ij})$ where

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

Using this we can prove:

Proposition 1 *For $A \in M_{qq}(R)$ the following holds:*
(i) $A\tilde{A} = \operatorname{Det} A \cdot \mathbf{1}_q$.
(ii) $A \in GL_q(R) \Longleftrightarrow \operatorname{Det} A \in R^\times$*; if this is true, then*

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

Proof. (i) is the expansion rule for determinants.
(ii) immediately follows from (i). $\diamond$

In particular Det induces a group homomorphism $GL_q(R) \longrightarrow R^\times$.

Example For $R = \mathbb{Z}/n\mathbb{Z}$ the statement (ii) of Proposition 1 can be rewritten as:

$$A \in M_{qq}(\mathbb{Z}) \text{ is invertible } \mod n \iff \operatorname{Det} A \text{ is coprime with } n.$$

Remarks

1. The expenses for calculating the inverse matrix A^{-1} are, if statement (ii) is naively evaluated:
   - one $q \times q$-determinant with $q!$ summands, each with q factors,
   - q^2 determinants of size $(q-1) \times (q-1)$.

   This is extremely inefficient—it is exponential in q.
2. Using GAUSSian elimination the expenses drop to $\mathrm{O}(q^3)$. But this is not quite true: Exact calculation produces rational numbers with *huge* numerators and denominators that require additional resources.

There is a modification of the elimination algorithm that uses only integers and is much more efficient, see the next section. However also this procedure produces large intermediate results.

An alternative algorithm uses the Chinese Remainder Theorem: Each ring homomorphism $\varphi\colon R \longrightarrow R'$ induces a homomorphism of R-algebras

$$\varphi_q\colon M_{qq}(R) \longrightarrow M_{qq}(R')$$

by componentwise evaluation. If $A \in M_{qq}$ is invertible, then

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

Hence also $\varphi_q(A)$ is invertible. Furthermore $\operatorname{Det}\varphi_q(A) = \varphi(\operatorname{Det} A)$, so we have a commutative diagram

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

Applying this to $R = \mathbb{Z}$ we use the residue class homomorphisms $\mathbb{Z} \longrightarrow \mathbb{F}_p$ (p prime) for sufficiently many primes p such that the product of these primes is $> \operatorname{Det} A$. Then we calculate

- $\operatorname{Det} A \bmod p$ in all the fields $\mathbb{F}_p$ (avoiding huge numbers, since all intermediate results may be represented as numbers between 0 and $p-1$),
- $\operatorname{Det} A \in \mathbb{Z}$ using the Chinese Remainder Theorem.