Next, let us suppose that we have a bunch of vectors $X_1 = \binom{x_1}{y_1}, \ldots, X_k = \binom{x_k}{y_k}$, arranged as the columns of a $2 \times k$–matrix. Then we define the matrix product

$$AX = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 & \ldots & x_k \\ y_1 & \ldots & y_k \end{pmatrix} =_{def} \begin{pmatrix} ax_1 + by_1 & \ldots & ax_k + by_k \\ cx_1 + dy_1 & \ldots & cx_k + dy_k \end{pmatrix},$$

i.e., we simply apply the matrix A to each column vector in order, obtaining new column vectors. For example, the product of two 2×2–matrices is:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Similar facts hold for 3×3–matrices, which can be applied to 3-dimensional column-vectors, and so on. However, the formulas for the determinant and inverse matrix are more complicated. This concludes our brief review of linear algebra over the real numbers.

Linear algebra modulo N. In §1, when we were dealing with single characters and enciphering maps of $\mathbf{Z}/N\mathbf{Z}$, we found that two easy types of maps to work with were:

(a) "linear" maps $C = aP$, where a is invertible in $\mathbf{Z}/N\mathbf{Z}$;

(b) "affine" maps $C = aP + b$, where a is invertible in $\mathbf{Z}/N\mathbf{Z}$.

We have a similar situation when our message units are digraph-vectors. We first consider linear maps. The difference when we work with $(\mathbf{Z}/N\mathbf{Z})^2$ rather than $\mathbf{Z}/N\mathbf{Z}$ is that now instead of an integer a we need a 2×2–matrix, which we shall denote A. We start by giving a systematic explanation of the type of matrices we need.

Let R be any commutative ring, i.e., a set with multiplication and addition satisfying the same rules as in a field, except that we do *not* require that any nonzero element have a multiplicative inverse. For example, $\mathbf{Z}/N\mathbf{Z}$ is always a ring, but it is not a field unless N is prime. We let R^* denote the subset of invertible elements of R. For example, $(\mathbf{Z}/N\mathbf{Z})^* = \{0 < j < N \mid g.c.d.(j, N) = 1\}$.

If R is a commutative ring, we let $M_2(R)$ denote the set of all 2×2–matrices with entries in R, with addition and multiplication defined in the usual way for matrices. We call $M_2(R)$ a "matrix ring over R"; $M_2(R)$ itself is a ring, but it is *not* a commutative ring, i.e., in matrix multiplication the order of the factors makes a difference.

Earlier in this section, the matrices considered were the case when $R = \mathbf{R}$ is the ring (actually, field) of real numbers. Recall that a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with real numbers a, b, c, d has a multiplicative inverse if and only if the determinant $D = ad - bc$ is nonzero, and in that case the inverse matrix is