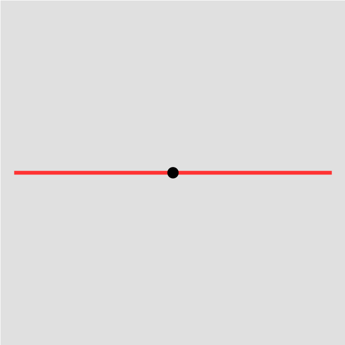
Computing orthogonal complements on finite tori

David Wilding

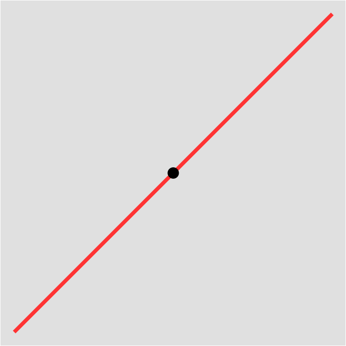
MRSC 2012

Many of us would be able to sketch the row space of a (sufficiently small!) real matrix, but what about the row space of a matrix whose entries are congruence classes of integers? As you'll see in the talk, it's possible, and actually quite fun, to draw such spaces and their orthogonal complements on the surface of a torus. I'll explain what an orthogonal complement is in this context, although you might well be able to guess, and I'll describe a nice way to compute such things.

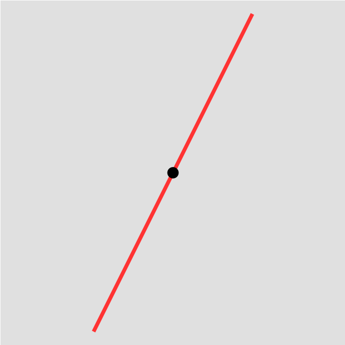
$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$



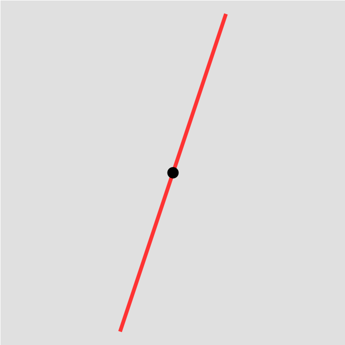
$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

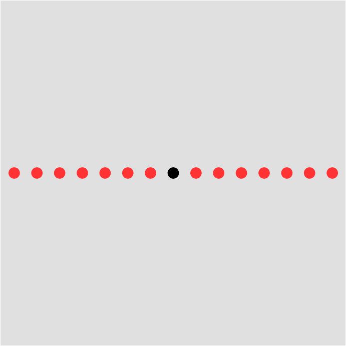


$$\begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix}$$

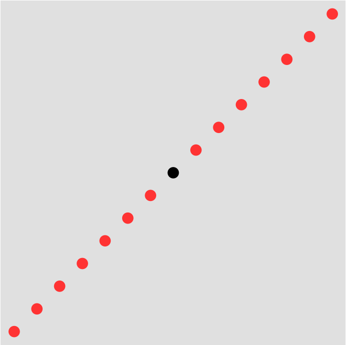


These first four slides show the row spaces of various matrices in the real plane $\mathbf{R}^2$*. The origin is the black dot in the middle and as we increase the top right entry in the matrix the row space (which is a line because the matrix only has one non-zero row) increases in steepness.*

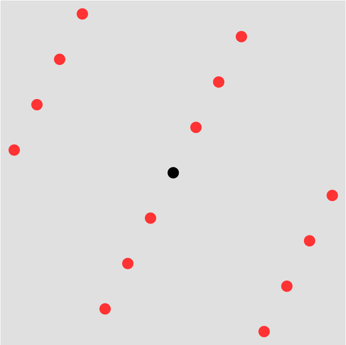
$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$



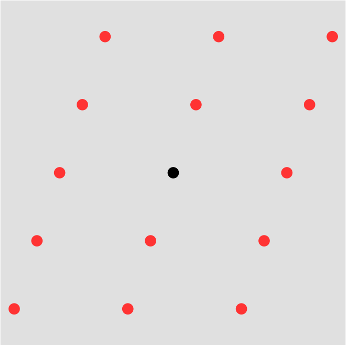
$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$



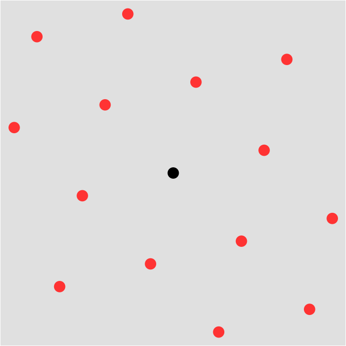
$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix}$$

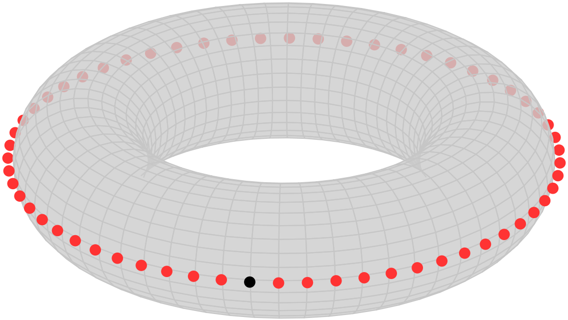


$$\begin{bmatrix} 1 & 4 \\ 0 & 0 \end{bmatrix}$$

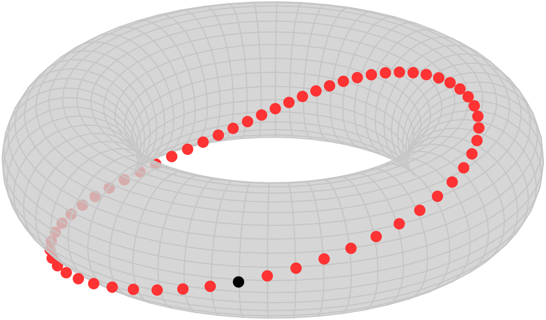


These five slides show the row spaces of the same matrices (plus one more) in the plane $\mathbf{Z}_{15}^2$, *which has* $15^2 = 225$ *points in total. All operations here are carried out modulo* 15, *so the left and right edges of the plane should be identified. Similarly the bottom and top edges should be identified, forming a torus.*

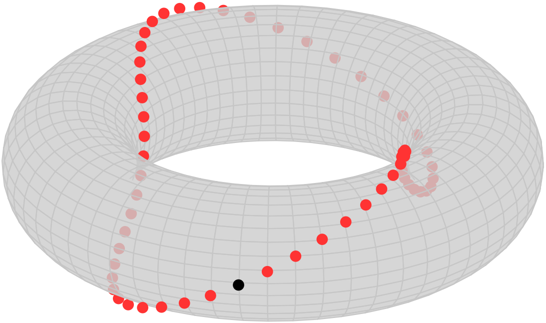
$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$



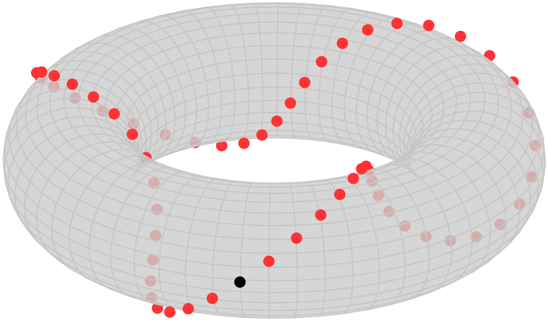
$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$



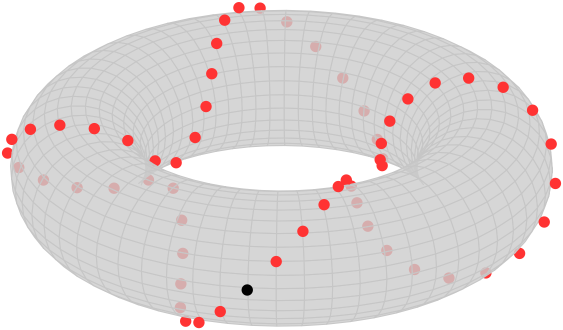
$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 4 \\ 0 & 0 \end{bmatrix}$$



These five slides show the row spaces of the same matrices again, but this time in the plane $\mathbf{Z}_{60}^2$ *drawn as a torus. The first coordinate direction goes right from the origin (the black dot) round the torus, and the second coordinate direction goes up from the origin over the torus. All operations here (and for the rest of the talk) are carried out modulo* 60*.*

Orthogonality

$$\begin{bmatrix} a & b \end{bmatrix} \cdot \begin{bmatrix} x & y \end{bmatrix} = ax + by = 0$$

Orthogonality

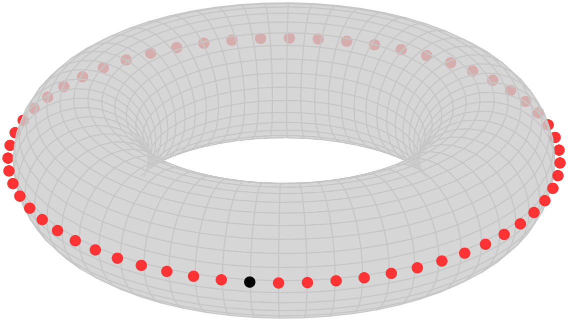
$$\begin{bmatrix} a & b \end{bmatrix} \cdot \begin{bmatrix} x & y \end{bmatrix} = ax + by = 0$$

For example

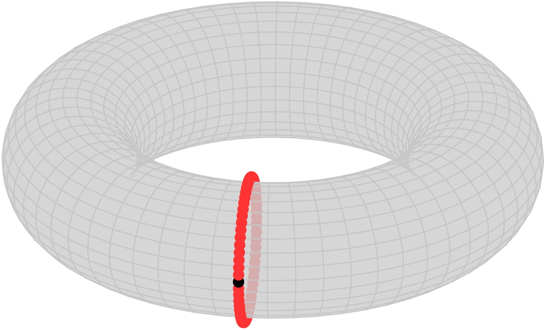
- $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \end{bmatrix}$ are orthogonal
- so are $\begin{bmatrix} 1 & 2 \end{bmatrix}$ and $\begin{bmatrix} 56 & 2 \end{bmatrix}$

Two vectors are orthogonal if their dot product is zero (modulo 60). This allows more vectors to be orthogonal than we would usually expect. The orthogonal complement of a set X of vectors is the set of vectors y with $x \cdot y = 0$ for all $x \in X$. The purpose of this talk is to show you how to, given a matrix A, find a matrix B whose row space is the orthogonal complement of the row space of A.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

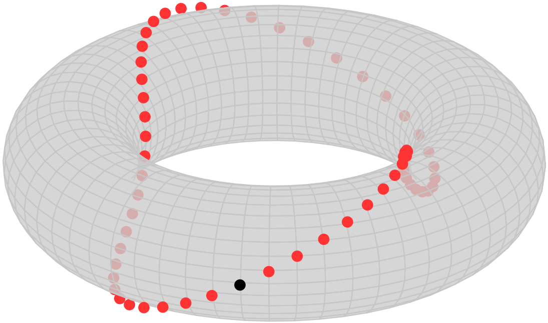


$$\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$$

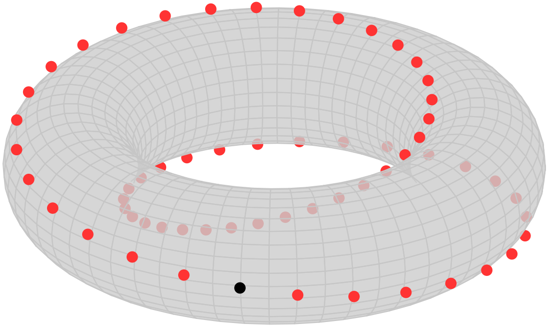


These two slides show a simple row space followed by its orthogonal complement. I use a squiggly arrow for the procedure "find a matrix whose row space is the orthogonal complement" described above.

$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

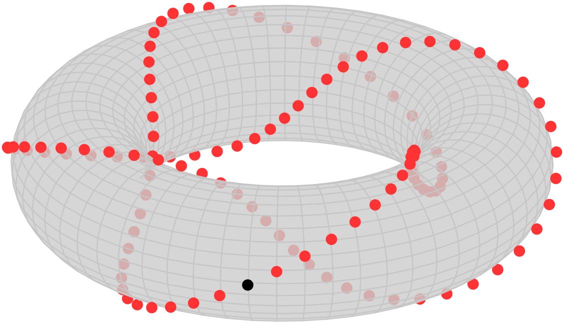


$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 0 \\ 58 & 1 \end{bmatrix}$$

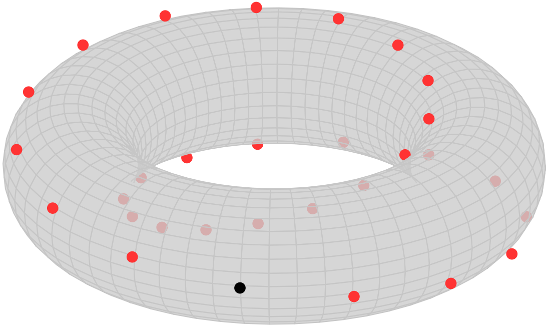


A more complicated row space has, perhaps unsurprisingly, a more complicated orthogonal complement.

$$\begin{bmatrix} 1 & 2 \\ 0 & 30 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 2 \\ 0 & 30 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 0 \\ 56 & 2 \end{bmatrix}$$



By giving the matrix another non-zero row I can double the number of points in the row space. I then get the same kind of orthogonal complement, but this time with half as many points. This is a general result: the product of the size of a row space and the size of its orthogonal complement is the size of the whole space. In this example $120 \cdot 30 = 60^2$.

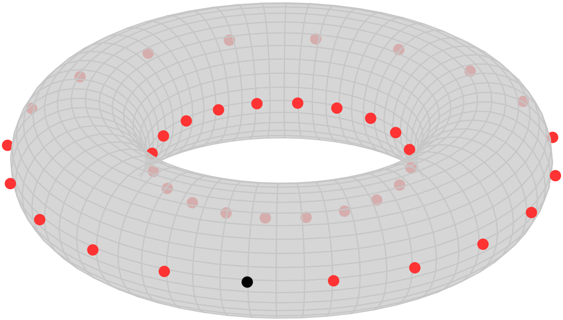
$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \qquad \rightsquigarrow \qquad \begin{bmatrix} 60/a & 0 \\ 0 & 60/b \end{bmatrix}$$

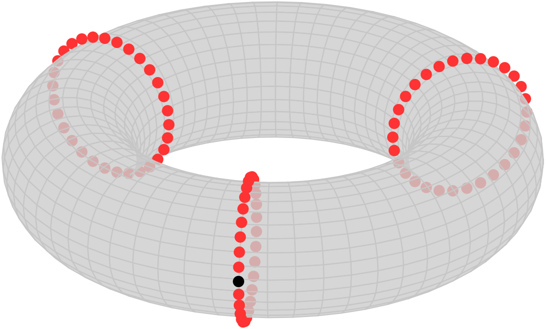
$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 60/a & 0 \\ 0 & 60/b \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

Finding an orthogonal complement matrix for a diagonal matrix is easy: just divide 60 *by the diagonal entries. Doing this a second time produces the original matrix again, which suggests that the double orthogonal complement of a row space is (for diagonal matrices at least) the same as the row space itself. In fact this result is true for arbitrary matrices.*

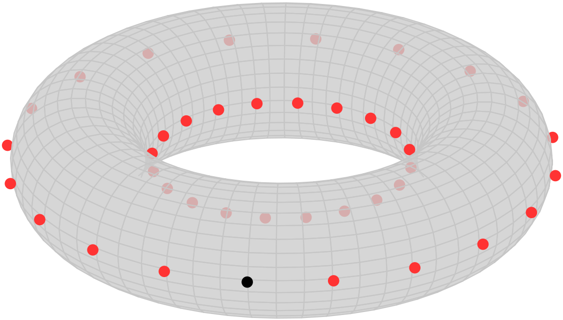
$$\begin{bmatrix} 3 & 0 \\ 0 & 30 \end{bmatrix}$$



$$\begin{bmatrix} 3 & 0 \\ 0 & 30 \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 20 & 0 \\ 0 & 2 \end{bmatrix}$$



$$\begin{bmatrix} 3 & 0 \\ 0 & 30 \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 20 & 0 \\ 0 & 2 \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 3 & 0 \\ 0 & 30 \end{bmatrix}$$



$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 60/a & 0 \\ 0 & 60/b \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

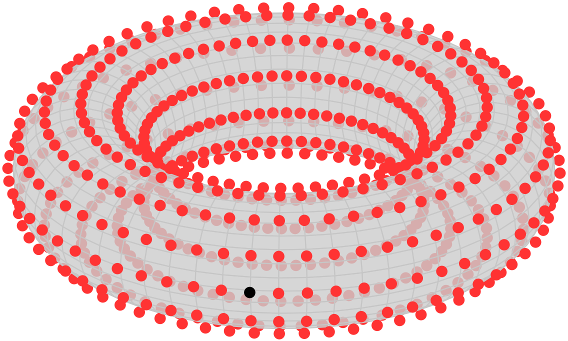
Hang on ...

The procedure for finding an orthogonal complement matrix for a diagonal matrix is not quite as simple as I suggested because the diagonal entries might not divide 60*.*

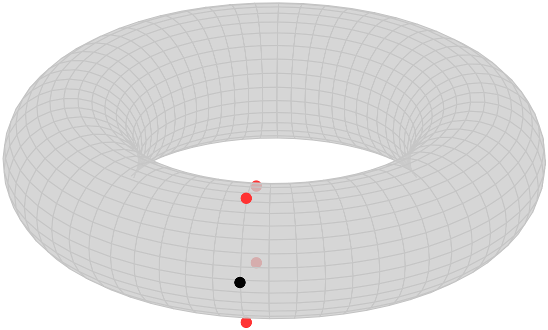
$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \gcd(a, 60) & 0 \\ 0 & \gcd(b, 60) \end{bmatrix} \quad \text{are equivalent}$$

Replacing the diagonal entries by their greatest common divisors with 60 *produces (without changing the row space) a matrix whose diagonal entries do divide* 60*. These new entries can then be divided into* 60 *to produce an orthogonal complement matrix.*

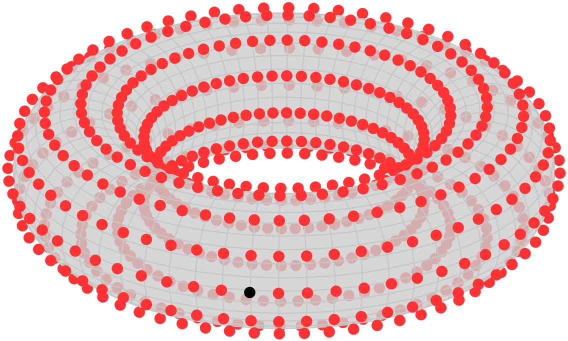
$$\begin{bmatrix} 53 & 0 \\ 0 & 25 \end{bmatrix}$$



$$\begin{bmatrix} 53 & 0 \\ 0 & 25 \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 0 & 0 \\ 0 & 12 \end{bmatrix}$$



$$\begin{bmatrix} 53 & 0 \\ 0 & 25 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 0 \\ 0 & 12 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix}$$



The greatest common divisor of 53 *and* 60 *is* 1*, so* 53 *is replaced by* $60/1$*, which is zero (modulo 60). Similarly the greatest common divisor of* 25 *and* 60 *is* 5*, so* 25 *is replaced by* $60/5 = 12$*. Applying this procedure again does not give the original matrix, but at least it gives one with the original row space.*

Arbitrary A

Arbitrary	A
Diagonal	MAN

Arbitrary	A		
Diagonal	MAN	$\rightsquigarrow$	B

Arbitrary	A	$\rightsquigarrow$	BN^{t}
Diagonal	MAN	$\rightsquigarrow$	B

To find an orthogonal complement matrix for an arbitrary matrix A, first make it diagonal by multiplying it on the left and on the right by invertible matrices M and N (this can always be done), then find an orthogonal complement matrix B for this diagonal matrix. Finally multiply B on the right by the transpose of the invertible matrix N.

To get M

- permute rows
- negate rows
- add multiples of rows

To get M

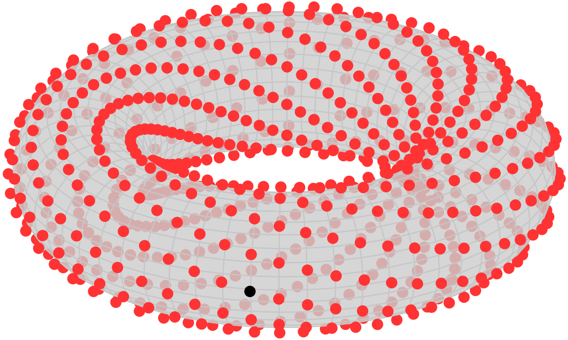
- permute rows
- negate rows
- add multiples of rows

To get N

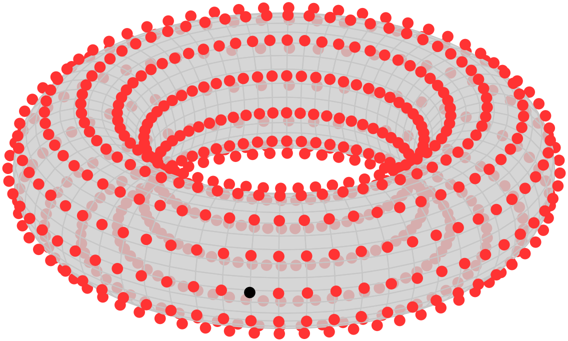
- permute columns
- negate columns
- add multiples of columns

The matrices M and N can be found using row operations and column operations, and they will be invertible because the allowed operations are invertible. For example, adding a multiple of a row to a different row can be undone by subtracting off that multiple again.

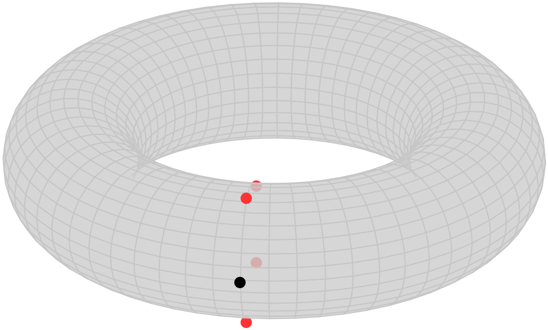
$$\begin{bmatrix} 1 & 4 \\ 10 & 5 \end{bmatrix}$$



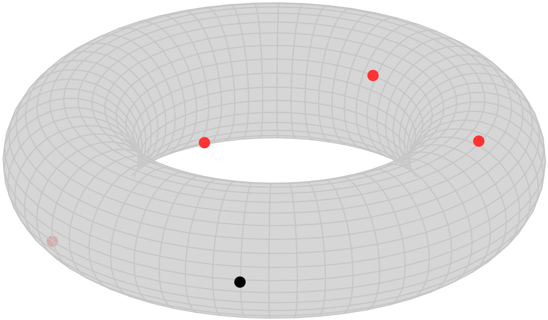
$$\begin{bmatrix} 1 & 4 \\ 10 & 5 \end{bmatrix} \begin{bmatrix} 1 & 52 \\ 58 & 17 \end{bmatrix} = \begin{bmatrix} 53 & 0 \\ 0 & 5 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 4 \\ 10 & 5 \end{bmatrix} \begin{bmatrix} 1 & 52 \\ 58 & 17 \end{bmatrix} = \begin{bmatrix} 53 & 0 \\ 0 & 5 \end{bmatrix} \qquad \rightsquigarrow \qquad \begin{bmatrix} 0 & 0 \\ 0 & 12 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 4 \\ 10 & 5 \end{bmatrix} \quad \rightsquigarrow \quad \begin{bmatrix} 0 & 0 \\ 0 & 12 \end{bmatrix} \begin{bmatrix} 1 & 58 \\ 52 & 17 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 24 & 24 \end{bmatrix}$$



These final four slides illustrate the full procedure for finding an orthogonal complement matrix for an arbitrary matrix. The row space is first untwisted by multiplying the matrix on the right by an invertible matrix (in this example no matrix M is needed). The orthogonal complement of this untwisted row space is then found and, finally, twisted using the transpose of the invertible matrix.