Principal Rings

As mentioned in the section on Euclidean rings, one can use Euclid's division algorithm in such rings to calculate the greatest common divisor of two elements in such rings. This can be taken a step further.

Exactly as in the case of integers one can show that every ideal consists of all multiples of a single element as follows. If the ideal is $\{0\}$ then it consists of all multiples of 0. On the other hand, if there is a non-zero element in I, then take a non-zero element a in I which has the smallest size using the d function. (For example, if R is the collection of polynomials over a field, then take the non-zero element of I of least degree). Given any other element b of I, we can divide b by a and write $b = q \cdot a + r$ where r has smaller size than a. However, it is clear that $r = b - q \cdot a$ lies in I, hence by assumption on the size of a, we must have $r = 0$. Thus, we see that every element of I is in $R \cdot a$.

Thus, Euclidean rings are examples of *principal ideal rings*; these are commutative rings R so that *every* ideal I in R is of the form $a \cdot R$; in other words, the ideal I consists of all multiples of a fixed element a of it.

In the spirit of generalisation, we can ask whether the reduction of matrices can be generalised to such rings. Indeed we can as we shall show below.

A *domain* is a ring in which 0 is the only zero-divisor. We note that the ring of integers and the ring of polynomials with coefficients in a field are domains.

A P.I.D. or a principal ideal domain is a ring which is both, a domain and a principal ideal ring.

Exercise: Show that $\mathbb{Z}/n$ (for any n) is a principal ideal ring.

Exercise: Show that $\mathbb{Z}/n$ is a domain only if n is a prime.

Matrix Reduction over a PID

We would like to show that matrices over a PID R can also be reduced to normal form as with the ring of integers and more generally, with Euclidean rings.

One difficulty that we have is that we can't use row/column reduction since we no longer have a method for division.

We note that a row operation involves left multiplication by a matrix whose determinant is 1. Similarly, column reduction involves right multiplication by a matrix whose determinant is 1. Thus, we can try to show that given a matrix A over a PID, there are matrices S and T, each of determinant 1 so that $S \cdot A \cdot T$ is in normal form. Since matrices of determinant 1 are units in $M_k(R)$, we can also allow more general invertible matrices in matrix rings to play the roles of S and T.

Recalling the method used earlier, we had a row (or column) of *two* entries a and b and we had to find a way to replace one of them by the greatest common divisor using multiplication by a matrix of determinant 1.

Since $a \cdot R + b \cdot R$ is a principal ideal (since R is a PID), we know that this is of the form $c \cdot R$ for a suitable c. We assume that a is not 0 so that c too is not 0. We have a relation of the form $a \cdot x + b \cdot y = c$. Moreover, we also have $a = c \cdot m$ and $b = c \cdot n$. It follows that

$$c \cdot (m \cdot x + n \cdot y) = c \text{ or equivalently } c \cdot (m \cdot x + n \cdot y - 1) = 0$$

Now, since $c \neq 0$ it is not a zero-divisor on R, so we must have $m \cdot x + n \cdot y = 1$. We also note that $n \cdot a = m \cdot b$. This gives us the identity

$$\begin{pmatrix} x & y \\ -n & m \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ 0 \end{pmatrix}$$

This is the *key* step in reducing matrices to normal form as it replaces a pair of entries a and b in a particular column to the greatest common divisor c (of a and b) and 0 via left multiplication by a suitable matrix of determinant 1. A similar approach leads to a suitable matrix for right multiplication when one has a matrix with a pair of entries in a particular row.

The algorithm for matrix reduction similar to the one described for the Euclidean case can now be followed to perform matrix reduction.

However, there is one further catch. In the case of Euclidean rings, we can be sure that our algorithm terminates (even with Step 4) since any new entries being created are of smaller size. Since we no longer have a size function, this way of proving termination is not available to us. Instead we need the following result.

Noetherian-ness of PIDs: Given an sequence of ideals I_i, with $I_i \subset I_{i+1}$ in a PID, there is a k so that $I_k = I_{k+r}$ for all $r \geq 1$.

Using this result, the infinite descent argument can be applied again to argue that the ideals generated by the matrix entries cannot keep getting bigger. It follows easily that the algorithm terminates.

To prove the Noetherian property, we put I to be the union of the ideals I_i. Given a and b in I, there is an i so that I_i contains a and there is a j so that I_j contains b. If k is the maximum of i and j, then both a and b lie in I_k. It follows that $a + b$ lies in I_k since the latter is an ideal. Thus I is closed under addition. Moreover if c is any element of R, the $a \cdot c$ lies in I_k since the latter is an ideal. Thus I is closed under multiplication by elements of R. In other words, I is an ideal.

Since R is a PID, the ideal I must be of the form $a \cdot R$ for some a in R. In that case a lies in I and hence lies in I_k for some k. Then it follows that $I_k = I = I_{k+r}$ for all $r \geq 1$.

We have thus completed the proof of that a matrix over a PID can be reduced to normal form. Note that the proof is abstract in the sense that it does not give us a way to *construct* the greatest common divisor of two elements.