Euclidean Rings

We would like to extend the result about matrices over integers to other rings. Why? We will see some applications later on. However, in Mathematics, it is common to take a result which has been proved for a particular object and ask if it can be "generalised"; in fact, generalisation is one of the basic tasks in mathematics.

So we can ask if, given a matrix A with entries in R, there is a sequence of row and column operations which bring it into the form where the only non-zero entries are along the diagonal and if these entries are d_1, d_2, $\ldots$, d_r in some order, then d_{k+1} lies in the ideal generated by d_k for all k from 1 to $(r-1)$. (Note that the statement in terms of ideals is the translation to general rings of the statement of divisibility in integers.) This diagonal form is called the "Smith" normal form of the matrix.

Exercise: (Starred) Show that for *any* non-zero 2×2 matrix A, the two-sided ideal generated by A in the ring $M_2(\mathbb{Q})$ of 2×2 matrices with rational entries, is the whole ring.

Thus, our intuition about integers is unlikely to work with non-commutative rings for the problem of finding a Smith normal form of a matrix. So we will restrict our attention to commutative rings R for this topic.

Division

The key step of our matrix reduction algorithm was the division of a larger integer by a smaller one. In order to make this work we need a function d from non-zero elements elements of R to the set $\mathbb{N} \cup \{0\}$ of non-negative integers that measures the size of an element. This function should have the properties:

1. Given two elements a and b of R, we have $d(a \cdot b) = d(a)d(b)$.
2. Given two elements a and b of R with $a \neq 0$. If $d(b) \leq d(a)$, then then either $a + b = 0$ or $d(a + b) \leq d(a)$.
3. Given $d(b) \leq d(a)$, there is are element q and r in R so that $a = b \cdot q + r$ with either $r = 0$ or $0 \leq d(r) < d(b)$.

A ring with such a function is called a Euclidean ring to indicate that the Euclidean division algorithm can be carried out such a ring to calculate the greatest common divisor of a pair of elements. This is a special case of the matrix reduction algorithm below.

The algorithm below will assume that the entries of A in the i-th row for $i \leq t$ are 0 except possibly for the entry at (i, i); similarly for the j-th column for $j \leq t$. Let us called this condition (C_t). We start the algorithm with $t = 0$.

Step 1

Examine the values $d(A_{i,j})$ for $i > t$ and $j > t$ where $A_{i,j} \neq 0$. If there are no such values then go to Step 4.

If there are such values, then choose an (i, j) for which this is the smallest.

Step 2 for rows

If there are no non-zero entries in the j-th column of A other than $A_{i,j}$, then go to step 2 for columns.

For an $m > t$ and $m \neq i$ with $A_{m,j} \neq 0$, we write $A_{m,j} = q_m A_{i,j} + r_m$ using (3) above. We then subtract q_m times the i-th row of A from the m-th row of A. We note that does not change the structure of the columns of A upto the t-th.

The resulting *new* matrix A has $A_{m,j} = r_m$ and $d(r_m) < d(A_{i,j})$.

Now go back to step 1.

Step 2 for columns

If there are no non-zero entries in the i-th row of A other than $A_{i,j}$, then go to step 3.

For an $m > t$ and $m \neq j$ with $A_{i,m} \neq 0$, we write $A_{i,m} = p_m A_{i,j} + s_m$ using (3) above. We then subtract p_m times the j-th column of A from the m-th column of A. We note that does not change the structure of the rows of A upto the t-th.

The resulting *new* matrix A has $A_{i,m} = s_m$ and $d(s_m) < d(A_{i,j})$.

Now go back to step 1.

Step 3

When we come here the only non-zero entry of A in the i-th row of A is $A_{i,j}$; similarly for entries in the j-column of A.

We now increase t and replace it with $t + 1$.

We now swap the i-row of A with the t-th row and the j-th column of A with the t-th column. It follows that our matrix satisfies the condition C_t (for the new larger value of t).

We now go back to step 1.

Step 4

When we reach this step, the only non-zero values of A are along the diagonal.

We swap rows and columns until these diagonal values are in increasing order of value of d, except that the 0 rows and columns go to the end.

Now consider the first two successive non-zero entries along the diagonal that do not satisfy the condition that d_k divides d_{k+1}. Note that, by the above interchanges, we have $d(d_k) \leq d(d_{k+1})$, so we can use (3) to write $d_{k+1} = qd_k + r$.

We now add the k-th row to the $k+1$-th row and subtract q times the k-th column from the $k+1$-th column. The entry $A_{k+1,k+1}$ then becomes r. As a result of (3), we have $d(r) < d(d_k)$, so we can go back to step 1 with $t = (k-1)$ and repeat the above Steps as required.

If there is no such pair, then the matrix is in Smith normal form and we can stop.

Example

In order to give an example of the above process, we first need to give an example of a ring R that has a size function d such as the one above. One important example of this is the ring $R = \mathbb{Q}[T]$, ring of polynomials with rational coefficients. The function d is given by taking the degree of a polynomial. (Note that the degree of the zero polynomial is not defined.) The method of "long division" for polynomials that we learned in high-school ensures that it satisfies (3) given above.

Since the above steps always involve two rows or two columns, we can illustrate the method for a 2×2 matrix with entries in R. So let use use the matrix

$$A = \begin{pmatrix} 2 - T^2 & 1 + T \\ 1 - T & 1 + T^2 \end{pmatrix}$$

We see that the entry $A_{1,2}$ is of the smallest degree. We can use this to divide the entry $A_{2,2}$:

$$1 + T^2 = (1 + T) \cdot (-1 + T) + 2$$

So we subtract $-1 + T$ times the first row from the second row to get the matrix

$$A = \begin{pmatrix} 2 - T^2 & 1 + T \\ 3 - 3T - T^2 + T^3 & 2 \end{pmatrix}$$

Now the new smallest entry is $A_{2,2} = 2$. So we subtract $(1/2)(1 + T)$ times row 2 from row 1 to get the matrix

$$A = \begin{pmatrix} (1/2) + T - T^4/4 & 0 \\ 3 - 3T - T^2 + T^3 & 2 \end{pmatrix}$$

Now the entries in the same column as $A_{2,2}$ are 0. So we work with columns. We subtract $(1/2)(3 - 3T - T^2 + T^3)$ times the column 2 from column 1 to get the matrix

$$A = \begin{pmatrix} (1/2) + T - T^4/4 & 0 \\ 0 & 2 \end{pmatrix}$$

So now we interchange the columns and the rows to get the matrix

$$A = \begin{pmatrix} 2 & 0 \\ 0 & (1/2) + T - T^4/4 \end{pmatrix}$$

This matrix is in normal form.

Exercise: Take any 3×3 matrix B with rational coefficients and consider the matrix $A = B - T \cdot 1$ where 1 denotes the identity matrix. Calculate the normal form of this matrix A.

The significance of this kind of normal form will become evident by and by.

Fields

A commutative ring F with the additional property that every non-zero element has a multiplicative inverse is called a *field*. Our typical example is the field $\mathbb{Q}$ of rational numbers. Other examples are the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers.

Exercise: Check that $\mathbb{Z}/p$ is a field if and only if p is a prime number.

Using long division, one can check that the ring $R = F[T]$ of polynomials satisfies the above condition with respect to the function d that assigns the degree of a polynomial to it. Hence, the above procedure of matrix reduction works over such rings as well.