Jordan Canonical Form

An endomorphism A of a (finite dimensional) vector space M over $\mathbb{Q}$ (or more generally a field) can be identified with a square matrix by fixing a basis of M over $\mathbb{Q}$. When we change the basis of M, the matrix A is replaced by $S \cdot A \cdot S^{-1}$ for a suitable invertible matrix S.

In a previous section we showed that there is a basis in which the matrix takes a block form with blocks along the diagonal of the form $C_{P_1}, C_{P_2}, \ldots, C_{P_k}$, where C_P denotes the "companion" matrix of a polynomial P, and we have $P_1|P_2|\cdots|P_k$ where P_i are polynomials in $\mathbb{Q}[T]$.

To further study M, we must therefore study the matrix C_P. Recall that this is the matrix by which T operates on the vector space $\mathbb{Q}[T]/P(T)$ in terms of the basis $1, T, \ldots, T^{d-1}$ of this vector space of dimension $d = \deg(P)$. We have

$$C_P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-1} \end{pmatrix}$$

where $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_0$.

In order to understand this further, we will apply the theorem on factorisation of elements of a PID to the polynomial ring $\mathbb{Q}[T]$ (or more generally $F[T]$ for a field F).

Chinese Remainder Theorem

Given a and b elements in a commutative ring R such that $a \cdot R + b \cdot R = R$; this means that there are elements x and y in R such that $a \cdot x + b \cdot y = 1$. Consider the natural homomorphism $R/(a \cdot b) \to R/a \times R/b$ given by $c \mapsto (c, c)$.

If the image (c, c) of c is $(0, 0)$, then $c = a \cdot m$ and $c = b \cdot n$ for some elements m and n in R. It follows that

$$c = c \cdot (a \cdot x + b \cdot y) = b \cdot n \cdot a \cdot x + a \cdot m \cdot b \cdot y = (a \cdot b) \cdot (n \cdot x + m \cdot y)$$

Hence, c is itself 0 in $R/(a \cdot b)$. Thus, the map is one-to-one.

Conversely, given (d, e) in $R/a \times R/b$, we take

$$c = d \cdot (1 - a \cdot x) + e \cdot (1 - b \cdot y)$$

We then check that

$$c - d = -d \cdot a \cdot x + e \cdot a \cdot x = a \cdot (e \cdot x - d \cdot x)$$

We similarly check that $c - e$ is divisible by b. Hence c maps to (d, e) in $R/a \times R/b$.

In other words, we have checked that the above map is an isomorphism. This is known as the Chinese Remainder Theorem.

Jordan Blocks

Given a polynomial $P(T)$ over $\mathbb{Q}[T]$, we factor it as

$$P(T) = u \cdot P_1(T)^{n_1} \cdots P_k(T)^{n_k}$$

where the n_i are positive integers and $P_i(T)$ are irreducible polynomials. By an application of the Chinese Remainder Theorem it follows that

$$\mathbb{Q}[T]/P(T) = \mathbb{Q}[T]/(P_1(T)^{n_1}) \times \cdots \times \mathbb{Q}[T]/(P_k(T)^{n_k})$$

Thus, the study of C_P (which is the matrix of multiplication by T on the above vector space in the basis $1, T, \ldots, T^{n-1}$, can be reduced to a block matrix with diagonal blocks of the form C_Q for Q a power of an irreducible polynomial.

We can also do this over *any* field F.

In particular, let us consider the case where the irreducible polynomial is of the form $(T - a)$ for some element a. In that case, we want to understand the action of T on the space $F[T]/((T - a)^n)$. Let us study this in the basis $1, (T - a), \ldots, (T - a)^{n-1}$. We note that

$$T \cdot (T - a)^k = a \cdot (T - a)^k + (T - a)^{k+1}$$

It follows that the matrix of multiplication by T in this basis has the form

$$J_{a,k} = \begin{pmatrix} a & 1 & 0 & \ldots & 0 \\ 0 & a & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & a \end{pmatrix}$$

(In other words, we have a's on the diagonal and 1's above the diagonal.) This is a Jordan block.

Combining the results of the previous sections we see that *if* the *minimal* polynomial $P(T)$ of a matrix splits up as

$$P(T) = u \cdot (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}$$

wth distinct values a_i, then the matrix can be written in block form with each block as a Jordan block $J_{a_i,m}$ for $m \leq n_i$. (We may need smaller m for the other factors P_i that divide the minimal polynomial and are principal factors of the characteristic polynomial as before.)

In particular, if $n_i = 1$ for all i, which is to say that the minimal polynomial $P(T)$ has distinct roots, then the matrix can be written in diagonal form.

Conversely, if a matrix is D in diagonal form with $a_1, \dots, a_r$ as the *distinct* entries along the diagonal, then it is quite easy to see that the matrix satisfies the polynomial $Q(T) = (T - a_1) \dots (T - a_r)$. By the definition of the minimal polynomial, the minimal polynomial of D divides $Q(T)$, hence it has distinct roots.

Exercise: Show that $Q(T)$ *is* the minimal polynomial for a diagonal matrix whose diagonal entries are from the set of distinct elements $\{a_1, \dots, a_r\}$.

To apply the above steps, we need to write the polynomial $P(T)$ as a product of factors of degree 1. This can always be done over the field of complex numbers.

Fundamental Theorem of Algebra: A polynomial in $\mathbb{C}[T]$ is irreducible if and only if it is of degree 1.

Thus, a matrix can be diagonalised over the field of complex numbers if and only if its minimal polynomial has distinct roots.

In general, any matrix can be put in Jordan Block form over the field of complex numbers.

The proof of the fundamental theorem of algebra is not an algebraic proof! In fact, it depends on topological properties of the field of real numbers or the theory of analytic functions on the field of complex numbers. Thus, a proof of this theorem can only be found in a book on complex analysis or some book where the ordered field of real numbers is studied in detail. In particular, we will not prove it here.

Exercise: Given a and b distinct rational numbers, find a matrix S (in terms of a and b) so that

$$S \cdot \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \cdot S^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Exercise: Given a and $b \neq 0$ rational numbers, find a matrix S (in terms of a and b) so that

$$S \cdot \begin{pmatrix} a - b & b \\ -b & a + b \end{pmatrix} \cdot S^{-1} = \begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix}$$