AN ELEMENTARY PROOF OF THE JORDAN CANONICAL FORM

Enzo R. Gentile

Let $V$ be a finite dimensional vector space over a field $K$. Let $t$ be an endomorphism of $V$. Then, as it is well known, $V$ can be written as a direct sum of cyclic subspaces. If $m_t(X) \in K[X]$ denotes the minimal polynomial of $t$, in studying the structure of $t$ one is reduced to consider the case where $m_t(X) = p(X)^a$, with $p(X)$ an irreducible polynomial in $K[X]$ and where $a$ is a natural number.

A cyclic subspace of $V$ admits the following matrix representation:

\[
\begin{pmatrix}
P & N \\
P & N \\
\vdots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
P & N \\
P
\end{pmatrix}
\]

where $P$ is a block consisting of the companion matrix of $p(X)$ and where $N$ is the block

\[
\begin{pmatrix}
0 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots \\
0 & 0 & \cdots & 0 & 1 \\
1 & 0 & \cdots & 0 & 0
\end{pmatrix}
\]

of the same size as $P$.

The rational canonical form of $t$ consists of the matrix obtained by assembling blocks of the type $(C)$. If $p(X) = X - k$, $k \in K$ (for instance if $K$ is algebraically closed) then $(C)$ becomes a Jordan block, and the canonical form is called the Jordan canonical form. The proof of the Jordan canonical form depends essentially on the canonical form of a nilpotent endomorphism, fact tediously proven in most books in linear algebra.
In this Note we intend to give a direct proof of the Jordan canonical form. Nevertheless the ideas in the proof permit to prove the structure theorem of finitely generated torsion modules over a principal domain, which shall be done elsewhere.

To start with, we set some terminology. Throughout this Note, subspace means subspace invariant (or stable) under \( t \). Furthermore morphism means morphism commuting with \( t \). Recall that a subspace \( W \) of \( V \) is a direct summand of \( V \) if and only if there is a morphism \( f: V \rightarrow W \) whose restriction \( f|_{W} \) to \( W \) coincides with \( \text{Id}_{W} \).

Let \( v \in V \). With \( \langle v \rangle \) we denote the cyclic subspace of \( V \) generated by \( v \). Any element of \( \langle v \rangle \) can be written as \( a(t)v \) for some \( a(X) \in K[X] \).

From now on assume that \( t \) is a nilpotent morphism. For any \( v \in V, v \neq 0 \) we define the order of \( v \) as the highest positive integer \( o(v) \) satisfying

\[ t^{o(v)}v = 0, \quad t^{o(v)-1}v \neq 0. \]

Notice the following property of \( o(v) \): for any \( a(X) \in K[X] \),

\[ a(t)v = 0 \text{ implies that } X^{o(v)} \text{ divides } a(X). \]

In fact, this follows from the property of being \( K[X] \) a principal domain and standard arguments on polynomials.

Let \( v \in V \) be an element of order \( s \). We consider in \( \langle v \rangle \) the following sequences of subspaces:

\[ 0 \subset \langle t^{s-1}v \rangle \subset \ldots \subset \langle t^{i}v \rangle \subset \ldots \subset \langle tv \rangle \subset \langle v \rangle \]

We claim that if \( x \in \langle v \rangle \) then

\[ t^{i}x = 0 \text{ iff } x \in \langle t^{s-1}v \rangle \]

In fact, part "if" is trivial. On the other hand, let \( t^{i}x = 0 \).

Write \( x = a(t)v \). Then \( 0 = t^{i}x = t^{i}a(t)v \) and therefore \( X^{s} \) divides \( X^{i}a(X) \), which implies that \( a(X) \) is divisible by \( X^{s-i} \),

\[ a(X) = X^{s-i}r(X). \]

Finally \( x = t^{s-i}r(t)v \in \langle t^{s-i}v \rangle \) as we wanted to prove.

Next we start to prove that \( V \) is a direct sum of cyclic subspaces. Let \( v \in V \) be an element of highest order in \( V \). This implies that

\[ t^{s}z = 0 \text{ for any } z \text{ in } V. \]

Let \( \langle v \rangle \) be the cyclic subspace of \( V \) generated by \( v \). We shall define a projection of \( V \) onto \( \langle v \rangle \).

For this, let \( W \) be a subspace of \( V \) satisfying the following properties
i) \( \langle v \rangle \subset W \)

ii) There is a morphism \( f: W \to \langle v \rangle \) such that \( f(\langle v \rangle) = \text{Id}(\langle v \rangle) \)

iii) \( W \) is maximal with properties i) and ii).

Obviously if \( W = V \) nothing has to be proved. Assume then \( V \neq W \).

Choose \( u \in V - W \) and consider the subspace

\[ W' = W + \langle u \rangle. \]

\( W' \) contains \( \langle v \rangle \) and we shall extend \( f \) to \( W' \).

Let \( J \) be the ideal of all polynomials \( a(X) \) in \( K[x] \) satisfying

\[ a(t)u \in W. \]

\( J \) is generated by a monic polynomial \( g(X) \). Since \( t^s u = 0 \in W \) it follows that \( X^s \in J \), therefore \( g(X) \) divides \( X^s \), so \( g(X) = X^d \)

for some \( d \leq s \). Notice that \( t^d u \in W \) therefore \( f(t^d u) \in \langle v \rangle \).

But since \( t^{s-d} f(t^d) = f(t^s u) = 0 \), by an earlier remark we get that \( f(t^d u) \in \langle t^d v \rangle \), that is

\[ f(t^d u) = t^d x \]

for some \( x \in \langle v \rangle \).

We set

\[ f': W + \langle u \rangle \to \langle v \rangle \]

\[ f': w + a(t)u \mapsto f(w) + a(t)x \]

and we claim that \( f' \) is a well defined morphism of \( W' \) onto \( \langle v \rangle \).

Let \( w, w' \in W, a(X), a'(X) \in K[x] \) satisfy

\[ w + a(t)u = w' + a'(t)u. \]

Hence

\[ (a'(t) - a(t))u = w - w' \in W \]

implies that

\[ a'(X) - a(X) \in J \), that is \( a'(X) - a(X) = b(X)x^d \]

Therefore

\[ f(w) - f(w') = f(b(t)t^d u) = b(t)t^d x = (a'(t) - a(t))x \]
\[ f(w) + a(t)x = f(w') + a'(t)x \]

which says that \( f' \) is well defined. Clearly \( f' \) is a morphism of \( W' \) onto \( \langle v \rangle \) that extends \( f \). Since \( W \) is properly contained in \( W' \), we have a contradiction. Therefore \( f \) is a projection of \( V \) onto \( \langle v \rangle \) and we can write

\[ V = \langle v \rangle \oplus V' \]

But by an inductive argument, \( V' \) is a direct sum of cyclic subspaces, so \( V \) is a direct sum of cyclic subspaces and this was our claim.

REMARK. Notice that the present proof holds for any endomorphism \( t \) whose minimal polynomial is \( m_t(X) = p(X)^a \), with \( p(X) \) irreducible in \( K[X] \). As we remarked at the beginning the general situation \( m_t(X) = \Pi p_i(X)^{a_i} \) of different irreducible factors reduces trivially to the case above.