1. A short proof of Jordan normal form

Let $T : V \to V$ be a linear transformation of a finite dimensional complex vector space. We shall outline a proof that there is basis of V in which T is represented by a matrix in *Jordan normal form*

$$\begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_r \end{pmatrix}$$

where each A_i is a *Jordan block matrix* $J_t(\lambda)$ for some $t \in \mathbb{N}$ and $\lambda \in \mathbb{C}$:

$$J_t(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}_{t \times t.}$$

1.1. **Reduction to nilpotent maps.**

The first step is to reduce to the case where $T^q = 0$ for some $q \geq 1$; that is, T is nilpotent. We need the following lemma.

Lemma 1. *If $f(X) \in \mathbb{C}[X]$ and $g(X) \in \mathbb{C}[X]$ are coprime polynomials such that $f(T)g(T) = 0$ then $V = \operatorname{im} f(T) \oplus \operatorname{im} g(T)$. Moreover the subspaces in this decomposition are T-invariant and the minimal polynomial of T restricted to $\operatorname{im} g(T)$ divides $f(T)$.*

Proof. If $v = f(T)w$ then $Tv = f(T)Tw$ so the subspaces are T-invariant. By Euclid's algorithm there exist two further polynomials $a(X)$ and $b(X)$ such that $a(X)f(X) + b(X)g(X) = 1$. Hence for any $v \in V$,

$$f(T)(a(T)v) + g(T)(b(T)v) = v.$$

This shows that $f(T)a(T)$ is a projection onto $\operatorname{im} f(T)$ and that $V = f(T)V + g(T)V$. If $v \in \operatorname{im} g(T)$, with say $v = g(T)w$, then $f(T)v = f(T)h(T)w = 0$ so the minimal polynomial of T on $\operatorname{im} g(T)$ divides $f(T)$. Finally, if $v \in \operatorname{im} f(T) \cap \operatorname{im} g(T)$ then $v = a(T)(f(T)v) + b(T)(g(T)v) = 0 + 0 = 0$. □

Suppose that the minimal polynomial of T factorises as

$$(X - \lambda_1)^{a_1} \dots (X - \lambda_r)^{a_r}$$

where the λ_i are distinct and each $a_i \geq 1$. By applying the lemma with $f(X) = (X - \lambda_i)^{a_i}$ and $g(X)$ the product of the remaining factors, we can split up V into subspaces $V_1 \dots V_r$ such that $T : V_i \to V_i$ has minimal polynomial dividing $(X - \lambda_i)^{a_i}$. (This result is sometimes known as the 'Primary Decomposition Theorem'.) By considering the maps $T - \lambda_i 1_V$ we may then reduce to the case where T acts nilpotently. We give two ways to deal with this case.

1.2. **Jordan normal form for nilpotent maps (the quick way).** We work by induction on $\dim V$. As T is nilpotent, $\dim \operatorname{im} T < \dim T$. If $\operatorname{im} T = 0$ then $T = 0$ and the result is trivial, so we may assume that $\operatorname{im} T \neq 0$. By induction we may find $u_1, \ldots, u_k \in \operatorname{im} T$ so that

$$u_1, Tu_1, \ldots, T^{a_1-1}u_1, \ldots, u_k, Tu_k, \ldots, T^{a_k-1}u_k$$

is a basis for $\operatorname{im} T$. (In this basis $T : \operatorname{im} T \to \operatorname{im} T$ is in Jordan normal form.)

For $1 \leq i \leq k$ choose $v_i \in V$ such that $u_i = Tv_i$. Clearly $\ker T \supseteq \langle T^{a_1-1}u_1, \ldots, T^{a_k-1}u_k \rangle$. Extend this basis to a basis of $\ker T$, by $w_1, \ldots, w_l$ say. We claim that the vectors

$$v_1, Tv_1, \ldots, T^{a_1}u_1, \ldots, v_k, Tv_k, \ldots, T^{a_k}v_k, w_1, \ldots, w_l$$

form a basis for V. Linear independence may readily be checked by applying T to any given linear relation between the vectors. To show that they span V, we use dimensional counting. We know that $\dim \ker T = k + l$ and $\dim \operatorname{im} T = a_1 + \ldots + a_k$. Hence

$$\dim T = (a_1 + 1) + \ldots + (a_k + 1) + l,$$

which is the number of vectors above. Therefore we have constructed a basis for V in which $T : V \to V$ is in Jordan normal form.

1.3. **Jordan normal form for nilpotent maps (the slow way).** Suppose that $T^q = 0$ and $T^{q-1} \neq 0$. Let $v \in V$ be any vector such that $T^{q-1}v \neq 0$. One can check that the vectors $v, Tv, \ldots, T^{q-1}v$ are linearly independent. Their span, U say, is an T-invariant subspace of V. With respect to the given basis of U, the matrix of $T : U \to U$ is the Jordan block $J_q(0)$. Therefore, if we could find a T-invariant complement for U, an easy induction on $\dim V$ would complete the proof.

To show that a suitable complement exists, we work by induction on q. If $q = 1$, then $T = 0$ and any vector space complement to U will do. Now suppose we can find complements when $T^{q-1} = 0$.

Consider $\operatorname{im} T \subseteq V$. On $\operatorname{im} T$, T acts as a nilpotent linear map such that $T^{q-1} = 0$ and $T^{q-2}(Tv) \neq 0$, so by induction on q we get

$$\operatorname{im} T = \langle Tv, \ldots, T^{q-1}v \rangle \oplus W$$

for some T-invariant subspace W. Note that $U \cap W = 0$. Our task is to extend W to a suitable T-invariant complement for U in V.

Suppose first that $W = 0$. In this case, $\operatorname{im} T = \langle Tv, \ldots, T^{q-1}v \rangle$ and $\ker T \cap \operatorname{im} T = \langle T^{q-1}v \rangle$. Extend $T^{q-1}v$ to a basis of $\ker T$, say by $v_1, \ldots, v_s$. By the rank-nullity formula

$$v, Tv \ldots, T^{q-1}v, v_1, \ldots, v_s$$

is a basis of V. The subspace spanned by $v_1, \ldots, v_s$ is an T-invariant complement to U.

Now suppose that $W \neq 0$. Then T induces a linear transformation, $\bar{T}$ say, on V/W. Let $\bar{v} = v + W$. Since $\operatorname{im} \bar{T} = \langle \bar{T}\bar{v}, \ldots, \bar{T}^{q-1}\bar{v} \rangle$, the first case implies that there is an $\bar{T}$-invariant complement in V/W to $\langle \bar{v}, \bar{T}\bar{v}, \ldots \bar{T}^{q-1}\bar{v} \rangle$. The preimage of this complement in V is a suitable complement to U

2. The structure theorem for finite abelian groups

The idea used in the 'slow proof' above can also be used to prove the structure theorem for finite abelian groups. By induction on the order of the group it will suffice to show that if $H = \langle x \rangle$ is a maximal cyclic subgroup of a finite abelian group G then H has a complementary subgroup.

We work by induction on the order of H. If $|H| = 1$ then necessarily $|G| = 1$, so we may suppose that $|H| > 1$. Let p be a prime factor of $|H|$. Provided that pH is non-zero, one can check that pH is a maximal cyclic subgroup of pG, so by induction, pH has a complement in pG. On the other hand, if $pH = 0$ then we can just take pG as the complement. Let $pG = pH \oplus K$. If $K \neq 0$ then G/K has order strictly less than $|G|$, so by a further induction we have

$$G/K = \langle x + K \rangle \oplus L/K$$

for some complement L. As before, L provides a suitable complement to H in G.

We are left with the case $pG = pH$. We may regard G/pG as a vector space over the field with p-elements. Take any vector space complement to $\bar{x} = x + pG$, say $\langle \bar{y}_1, \ldots, \bar{y}_s \rangle$. We would like to have $py_j = 0$ but all we have at the moment is $py_j \in pG = \langle px \rangle$. However this is easily corrected: if $py_j = mpx$ then we replace y_j with $y'_j = y_i - mx$. So G is a direct sum of H with s cyclic groups of order p:

$$G = \langle x \rangle \oplus \langle y'_1 \rangle \ldots \oplus \langle y'_s \rangle . \quad \square$$

To classify finitely generated abelian groups we need a further splitting theorem, namely that if G is a finitely generated abelian group and $T \leq G$ is its torsion subgroup, that is, the set of elements of finite order, then there is a free abelian subgroup $K \leq G$ such that $G = T \oplus K$. As a free generating set for G/T will lift to a free generating set for a complement of T in G, it suffices to show that G/T is a free abelian group. This follows at once from the following lemma:

Lemma 2. *A finitely generated torsion free abelian group is free.*

Proof. Suppose that G is a finitely generated torsion free abelian group that is not free. Then any set of generators for G satisfies a non-trivial relation. Choose, from all possible generating sets for the group and all the non-trivial relations satisfied by these generating sets, a relation

$$a_1 g_1 + \ldots + a_n g_n$$

where $|a_1| + \ldots + |a_n|$ is as small as possible. We may reorder and change the sign of the generators so that $a_1 = \max |a_i|$ and $a_2 > 0$. Consider the new generating set $g_1, g_1 + g_2, \ldots, g_n$. This satisfies the new relation

$$(a_1 - a_2)g_1 + a_2(g_1 + g_2) + \ldots + a_n g_n = 0$$

in contradiction to our original choice. $\square$

Mark Wildon, January 2005
wildon@maths.ox.ac.uk