Primary Decomposition Theorem*

Graeme Taylor

April 17, 2004

When working with a linear map, it is often convenient to make use of the isomorphism between such an operator and its matrix representation. However, any given vector space will have many bases, and in general a change of basis alters the matrix version of a given operator. Hence, it is useful to examine both invariants of a map (properties which do not change regardless of the basis, such as the determinant or trace) and to come up with canonical forms for representing a map by a matrix. The best-case (i.e., simplest) scenario is when a linear map is diagonalisable; that is, we can find a basis with respect to which the matrix only has entries on the lead diagonal. Unfortunately, such a decomposition is not always possible- it is a special case of the more general jordan canonical form (with 1×1 Jordan blocks).

The most we can do is decompose a linear operator into a smaller, simpler collection of operators which tell us how the linear operator works. More formally, for $\alpha : V \to V$, where V is a finite dimensional vector space over any field, the aim is to decompose V as a direct sum of α-invariant subspaces. (a subspace W is α-invariant if for any $w \in W$, $\alpha(w) \in W$.)

The primary decomposition theorem states that this decomposition is determined by the minimal polynomial of α :

Let $\alpha : V \to V$ be a linear operator whose minimal polynomial factorises into monic, coprime polynomials-

$$m_\alpha(t) = p_1(t)p_2(t)$$

Then,

$$V = W_1 \oplus W_2$$

Where the W_i are α-invariant subspaces such that p_i is the minimum polynomial of $a|_{W_i}$.

*First appeared on Everything2, at *http://www.everything2.com/index.pl?node_id=1532181*

Repeated application of this result (i.e., fully factorising ma into pairwise coprime factors) gives a more general version: if $m_\alpha(t) = p_1(t) \dots p_k(t)$ as described, then

$$V = W_1 \oplus \dots \oplus W_k$$

With α-invariant W_i with corresponding minimal polynomal p_i.

It may now be apparent that diagonalisation is a special case in which each W_i has a minimal polynomial which consists of a single factor, $(t - \lambda_i)$; i.e. if $m_\alpha = (t - \lambda_1) \dots (t - \lambda_k)$ for distinct λ_i then α is diagonalisable with the λ_i as the diagonal entries.

Proof of the Primary Decomposition Theorem

The theorem makes two assertions; that we can construct α-invariant subspaces W_i based on the p_i; and that the direct sum of these W_i constructs V.

For the first, a result about invariant subspaces is needed:
Lemma: if $\alpha, \beta : V \to V$ are linear maps such that $\alpha\beta = \beta\alpha$, then Ker β is α-invariant.
Proof: Take $w \in$ Kerβ - we need to show that $\alpha(w)$ is also in Ker β. Now $\beta(\alpha(w)) = \alpha(\beta(w))$ by assumption, so $\beta(\alpha(w)) = \alpha(0)$ since $w \in$ Ker β , $= 0$ since α is a linear map. But if $\beta(\alpha(w)) = 0$ then $\alpha(w) \in$ Kerβ, hence Ker β is α-invariant. ■

Given this result, we now take the W_i as Ker $p_i(\alpha)$. Then since $p_i(\alpha)\alpha = \alpha p_i(\alpha)$, it follows that Ker $p_i = W_i$ is α-invariant.

We now seek to show that

(i) $V = W_1 + W_2$

(ii) $W_1 \cap W_2 = \{\mathbf{0}\}$ (that is, V decomposes as a direct sum of the W_i's.)

Using Euclid's Algorithm for polynomials, since the p_i are coprime there are polynomials q_i such that $p_1(t)q_1(t)+p_2(t)q_2(t) = 1$. So for any $v \in V$, consider $w_1 = p_2(\alpha)q_2(\alpha)v$ and $w_2 = p_1(\alpha)q_1(\alpha)v$. Then $v = w_1 + w_2$ by the above identity. We can confirm that

$$w_1 \in W_1 : p_1(\alpha)w_1 = m_\alpha(\alpha)q_2(\alpha)v = 0$$

Similarly, $w_2 \in W_2$. So we have (i).

For (ii), let $v \in W_1 \cap W_2$. Then

$$v = id(v) = q_1(\alpha)p_1(\alpha)v + q_2(\alpha)p_2(\alpha)v = \mathbf{0}$$

So $W_1 \cap W_2 = \{\mathbf{0}\}$.

Finally, for the claimed minimum polynomials. Let m_i be the min.poly. of $\alpha|_{W_i}$. We have that $p_i(\alpha|_{W_i}) = 0$, so the degree of p_i is at least that of m_i. This holds for each i. However,

$$p_1(t)p_2(t) = m_\alpha(t) = lcm\{m_1(t), m_2(t)\}$$

so we obtain

$$\deg p_1 + \deg p_2 = \deg m_\alpha = \deg m_1 + \deg m_2$$

It follows that $\deg p_i = \deg m_i$ for each i, and given monic p_i it must be that $m_i = p_i$. ■