proof of cyclic vector theorem

Canonical name	ProofOfCyclicVectorTheorem
Date of creation	2013-03-22 14:14:42
Last modified on	2013-03-22 14:14:42
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	12
Author	CWoo (3771)
Entry type	Proof
Classification	msc 15A04

First, let's assume f has a cyclic vector v. Then $B = \{v, f(v), ..., f^{n-1}(v)\}$ is a basis for V. Suppose g is a linear transformation which commutes with f. Consider the coordinates $(\alpha_0, ..., \alpha_{n-1})$ of $g(v)$ in B, that is

$$g(v) = \sum_{i=0}^{n-1} \alpha_i f^i(v).$$

Let

$$P = \sum_{i=0}^{n-1} \alpha_i X^i \in k[X].$$

We show that $g = P(f)$. For $w \in V$, write

$$w = \sum_{j=0}^{n-1} \beta_j f^j(v),$$

then

$$\begin{aligned} g(w) &= \sum_{j=0}^{n-1} \beta_j g(f^j(v)) = \sum_{j=0}^{n-1} \beta_j f^j(g(v)) \\ &= \sum_{j=0}^{n-1} \beta_j f^j(\sum_{i=0}^{n-1} \alpha_i f^i(v)) = \sum_{j=0}^{n-1} \beta_j \sum_{i=0}^{n-1} \alpha_i f^{j+i}(v) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \beta_j \alpha_i f^{j+i}(v) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \beta_j \alpha_i f^{j+i}(v) = \sum_{i=0}^{n-1} \alpha_i f^i(\sum_{j=0}^{n-1} \beta_j f^j(v)) = \sum_{i=0}^{n-1} \alpha_i f^i(w) \end{aligned}$$

Now, to finish the proof, suppose f doesn't have a cyclic vector (we want to see that there is a linear transformation g which commutes with f but is not a polynomial evaluated in f). As f doesn't have a cyclic vector, then due to the cyclic decomposition theorem V has a basis of the form

$$B = \{v_1, f(v_1), ..., f^{j_1}(v_1), v_2, f(v_2), ..., f^{j_2}(v_2), ..., v_r, f(v_r), ..., f^{j_r}(v_r)\}.$$

Let g be the linear transformation defined in B as follows:

$$g(f^k(v_1)) = \begin{cases} 0 & \text{for every } k = 0, \ldots, j_1 \\ f^{k_i}(v_i) & \text{for every } i = 2, \ldots, r \text{ and } k_i = 0, \ldots, j_i. \end{cases}$$

The fact that f and g commute is a consequence of g being defined as zero on one f-invariant subspace and as the identity on its complementary f-invariant subspace. Observe that it's enough to see that g and f commute in the basis B (this fact is trivial). We see that, if $k = 0, ..., j_1 - 1$, then

$$(gf)(f^k(v_1)) = g(f^{k+1}(v_1)) = 0 \quad \text{and} \quad (fg)(f^k(v_1)) = f(g(f^k(v_1)) = f(0) = 0.$$

If $k = j_1$, we know there are $\lambda_0, ..., \lambda_{j_1}$ such that

$$f^{j_1+1}(v_1) = \sum_{k=0}^{j_1} \lambda_k f^k(v_1),$$

so

$$(gf)(f^{j_1}(v_1)) = \sum_{k=0}^{j_1} \lambda_k g(f^k(v_1)) = 0 \quad \text{and} \quad (fg)(f^{j_1}(v_1)) = f(0) = 0.$$

Now, let $i = 2, ..., r$ and $k_i = 0, ..., j_i - 1$, then

$$(gf)(f^{k_i}(v_i)) = g(f^{k_i+1}(v_i)) = f^{k_i+1}(v_i) \quad \text{and} \quad (fg)(f^{k_i}(v_i)) = f(g(f^{k_i}(v_i)) = f^{k_i+1}(v_i).$$

In the case $k_i = j_i$, we know there are $\lambda_{0,i}, ..., \lambda_{j_i,i}$ such that

$$f^{j_i+1}(v_i) = \sum_{k=0}^{j_i} \lambda_{k,i} f^k(v_i)$$

then

$$(gf)(f^{j_i}(v_i)) = g(f^{j_i+1}(v_i)) = \sum_{k=0}^{j_i} \lambda_{k,i} g(f^k(v_i)) = \sum_{k=0}^{j_i} \lambda_{k,i} f^k(v_i) = f^{j_i+1}(v_i),$$

and

$$(fg)(f^{j_i}(v_i)) = f(g(f^{j_i}(v_i)) = f(f^{j_i}(v_i)) = f^{j_i+1}(v_i).$$

This proves that g and f commute in B. Suppose now that g is a polynomial evaluated in f. So there is a

$$P = \sum_{k=0}^{h} c_k X^k \in K[X]$$

such that $g = P(f)$. Then, $0 = g(v_1) = P(f)(v_1)$, and so the annihilator polynomial m_{v_1} of v_1 divides P. But then, as the annihilator m_{v_2} of v_2 divides m_{v_1} (see the cyclic decomposition theorem), we have that m_{v_2} divides P, and then $0 = P(f)(v_2) = g(v_2) = v_2$ which is absurd because v_2 is a vector of the basis B. This finishes the proof.