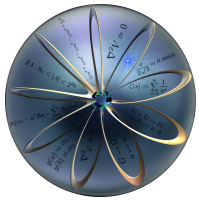

planetmath.org

Math for the people, by the people.

proof of theorem about cyclic subspaces

Canonical name	ProofOfTheoremAboutCyclicSubspaces
Date of creation	2013-03-22 17:32:53
Last modified on	2013-03-22 17:32:53
Owner	FunctorSalad (18100)
Last modified by	FunctorSalad (18100)
Numerical id	7
Author	FunctorSalad (18100)
Entry type	Proof
Classification	msc 15A04

We first prove the case $r = 2$. The $\subseteq$ inclusion is clear, since the right side is a T-invariant subspace that contains $v_1 + v_2$.

For the other inclusion, it is sufficient to show that $v_1, v_2 \in Z(v_1 + v_2, T)$. The idea is that the action of T on $v_1 + v_2$ can "isolate" the two summands if their annihilator polynomials are coprime. Let's write m_i for m_{v_i}.

Since $(m_1, m_2) = 1$, there exist polynomials p and q such that

$$pm_1 + qm_2 = 1 \tag{1}$$

this is Bzout's lemma (or the Euclidean algorithm, or the fact that $k[X]$ is a principal ideal domain).

Now $pm_1(T)$ is the projection from $Z(v_1, T) \oplus Z(v_2, T)$ to $Z(v_2, T)$:

$$(pm_1)(T)v_1 = p(T)m_1(T)v_1 = p(T)0 = 0 \tag{2}$$

(by assumption that m_1 is the annihilator polynomial of v_1) and

$$(pm_1)(T) = 1 - (qm_2)(T) \tag{3}$$

(by choice of p and q), so

$$(pm_1)(T)v_2 = v_2 - q(T)m_2(T)v_2 = v_2 - q(T)0 = v_2 \tag{4}$$

Any subspace that is invariant under T is also invariant under polynomials of T. Therefore, the preceding equations show that $v_2 = (pm_1)(T)(v_1 + v_2) \in Z(v_1 + v_2, T)$. By symmetry, we also get that $v_1 \in Z(v_1 + v_2, T)$.

For the last claim, we note that the annihilator polynomial m of $Z(v_1, T) \oplus Z(v_2, T)$ is the least common multiple of m_1 and m_2 (that m is a multiple of m_1 follows from the fact that m must annihilate v_1, and the set of polynomials that annihilate v_1 is the ideal generated by m_1). Since m_1 and m_2 are coprime, the lcm is just their product.

That concludes the proof for $r = 2$. If r is arbitrary, we can simply apply the $r = 2$ case inductively. We only have to check that the coprimality condition is preserved under applying the $r = 2$ case to $i = 1, 2$. But it is well-known that if p, q, r (in $k[X]$ or in any principal ideal domain) are pairwise coprime, then pq and r are also coprime.