for each i, $a_{ij} = 0$ for all j. So, S_2 is linearly independent.

We now show that K_ϕ has a basis consisting of a union of T-cycles.

<u>Lemma 7.3.10</u> Let W be a T-invariant subspace of K_ϕ and let β be a basis for W. Then the following statements are true:

(a) Suppose that $x \in N(\phi(T))$, but $x \notin W$. Then $\beta \cup \beta_x$ is linearly independent

(b) For some $w_1, w_2, \ldots, w_s$ in $N(\phi(T))$, β can be extended to the linearly independent set

$$\beta' = \beta \cup \beta_{w_1} \cup \beta_{w_2} \cdots \cup \beta_{w_s},$$ whose span contains $N(\phi(T))$

Proof: (a) Let $\beta = \{v_1, v_2, \ldots, v_k\}$ and suppose that

$$\sum_{i=1}^{k} a_i v_i + z = \theta \quad \text{and} \quad z = \sum_{j=0}^{d-1} b_j T^j(x),$$ where d is the degree of $\phi(t)$. Then $z \in C_x \cap W$ and hence $C_z \subseteq C_x \cap W$. Suppose that $z \neq \theta$. Then z has $\phi(t)$ as its T-annihilator, and therefore

$d = \dim(C_z) \leq \dim(C_x \cap W) \leq \dim(C_x) = d$. It follows that $C_x = C_x \cap W$. Consequently $x \in W$, contrary to the hypothesis that $x \notin W$. Therefore $z = \theta$, from which it follows that $b_j = \theta$ for all j. Since β is linearly independent, it follows that $a_i = 0$ for all i. Thus $\beta \cup \beta_x$ is linearly independent.

(b) Suppose that W does not contain $N(\phi(T))$. choose a vector $w_1 \in N(\phi(T))$ that is not in W. By (a) $\beta_1 = \beta \cup \beta_{w_1}$ is linearly independent. Let $W_1 = \text{span}(\beta_1)$. If W does not contain $N(\phi(T))$, choose a vector w_2 in $N(\phi(T))$, but not in W_1, so that $\beta_2 = \beta_1 \cup \beta_{w_2} = \beta \cup \beta_{w_1} \cup \beta_{w_2}$ is linearly independent. Continuing this process, we eventually obtain vectors $w_1, w_2, \ldots, w_s$ in $N(\phi(T))$ such that the union $\beta' = \beta \cup \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_s}$ is a linearly independent set whose span contains $N(\phi(T))$.

<u>Theorem 7.3.11</u> If the minimal polynomial of T is of the form $p(t) = (\phi(t))^m$, then there exists a rational canonical basis for T.

Proof: The proof is mathematical induction on m. Suppose that $m=1$, apply (b) of lemma 7.3.10 to $W = \{0\}$ to obtain a linearly independent subset of V of the form

$\beta_{v_1} \cup \beta_{v_2} \cup \cdots \cup \beta_{v_k}$, whose spans contains $N(\phi(T))$,

Since $V \supseteq N(\phi(T))$, this set is a rational Canonical basis for V.

Now suppose that, for some integer $m > 1$, the result is valid whenever the minimal polynomial of T is of the form $(\phi(t))^k$, where $k < m$ and assume that the minimal polynomial of T is $p(t) = (\phi(t))^m$. Let $r = \text{rank}\{\phi(T)\}$. Then $R(\phi(T))$ is a T-invariant subspace of V and the restriction of T to this subspace has $(\phi(t))^{m-1}$ as its minimal polynomial. Therefore we may apply the induction hypothesis to obtain a rational canonical basis for the restriction of T

to $R(\phi(T))$. Suppose that $v_1, v_2, \ldots, v_k$ are the generating vectors of the T-cyclic bases that constitutes this rational canonical basis. For each i, choose w_i in V such that $v_i = \phi(T)(w_i)$. By Theorem 7.3.9, the union β of the sets β_{w_i} is linearly independent. Let $W = span(\beta)$. Then W contains $R(\phi(T))$. Apply (b) of lemma 7.3.10 and adjoin additional T-cyclic bases $\beta_{w_{k+1}}, \beta_{w_{k+2}}, \ldots, \beta_{w_s}$ to β if necessary, where w_i is in $N(\phi(T))$ for $i \geq k$, to obtain a linearly independent set $\beta' = \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_s}$ whose span W' contain both W and $N(\phi(T))$. We show that $W' = V$. Let U denote the restriction of $\phi(T)$ to W' which is $\phi(T)$-invariant. By the way in which W' was obtained from $R(\phi(T))$, it follows that $R(U) = R(\phi(T))$ and $N(U) = N(\phi(T))$.

Therefore,

$$\dim(W') = \text{rank}(U) + \text{nullity}(U)$$
$$= \text{rank}(\phi(T)) + \text{nullity}(\phi(T))$$
$$= \dim V$$

Thus $W' = V$ and β' is a rational canonical basis for T.

<u>Corollary 7.3.12</u> K_ϕ has a basis consisting of the union of T-cyclic bases.

Proof: Apply Theorem 7.3.11 to the restriction of T to K_ϕ.

We are now ready to study the general case.

Theorem 7.3.13 Every linear operator on a finite dimensional vector space has a rational canonical basis and, hence, a rational canonical form.

Proof: Let T be a linear operator on a finite dimensional vector space V and let $p(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2}\cdots(\phi_k(t))^{m_k}$ be the minimal polynomial of T, where $\phi_i(t)$'s are the distinct irreducible monic factors of $p(t)$ and m_i's are positive integer for all i. The proof is by mathematical induction on k. The case k=1 is proved in Theorem 7.3.11.

Suppose that the result is valid when the minimal polynomial contains fewer than k distinct irreducible factors for some k>1 and suppose that $p(t)$ contains k distinct factors. Let U be the restriction of T to the T-invariant subspace $W = R((\phi_k(T))^{m_k})$ and let $q(t)$ be the minimal polynomial of U. Then $q(t)$ divides $p(t)$. Furthermore $\phi_k(t)$ does not divide $q(t)$. For otherwise, there would exists a non-zero vector $x \in W$ such that $\phi_k(U)(x) = \theta$ and a vector $y \in V$ such that $x = (\phi_k(T))^{m_k}(y)$. It follows that $(\phi_k(T))^{m_k+1}(y) = \theta$, and hence $y \in K_{\phi_k}$ and $x = (\phi_k(T))^{m_k}(y) = \theta$ by Theorem 7.3.6(e), a contradiction.

Then $q(t)$ contains fewer than k distinct irreducible divisors. So by induction hypothesis U