Direct sum of A-invariant subspaces

(based on two talks by Prof. S. Kumaresan at RKMVERI)

Shameek Paul

Definition 1. Let V be an $\mathbb{F}$-vector space and let $A \in L(V)$. A subspace W is called an A-invariant subspace if for every $v \in W$ we have $Av \in W$.

Observation 2. Let $\mathcal{C}$ be a collection of A-invariant subspaces of a vector space V, and let $W = \bigcap \mathcal{C}$. Then W is an A-invariant subspace of V.

Remark 3. Let V be a vector space and let $S \subseteq V$. Suppose $W_S = \bigcap \mathcal{C}_S$ where $\mathcal{C}_S$ is the collection

$$\mathcal{C}_S = \Big\{ W : W \text{ is an } A\text{-invariant subspace of } V \text{ which contains } S \Big\}.$$

From Observation 2 it follows that W_S is an A-invariant subspace of V which contains S. Given any A-invariant subspace W of V which contains S, we see that $W \in \mathcal{C}_S$ and hence it follows that $W_S \subseteq W$.

Definition 4. Let V be a vector space and let $S \subseteq V$. We say that W_S is the *smallest* A-invariant subspace of V which contains S.

Lemma 5. *Let V be an $\mathbb{F}$-vector space, let $v \in V$, and let $S = \{v\}$. Then $W_S = W$ where*

$$W = \Big\langle A^k v : k \in \mathbb{Z} \text{ with } k \geq 0 \Big\rangle.$$

Proof. Since W_S is an A-invariant subspace of V which contains S, we see that $A^k v \in W_S$ for every $k \in \mathbb{Z}$ with $k \geq 0$. Thus, we see that $W \subseteq W_S$. Since W is an A-invariant subspace of V which contains S, by Remark 3 we see that $W_S \subseteq W$. Hence, it follows that $W_S = W$. $\square$

Definition 6. Let V be an $\mathbb{F}$-vector space and let $A \in L(V)$. Suppose $p(X) = c_0 + c_1 X + \cdots + c_r X^r \in \mathbb{F}[X]$. We define $p(A)$ to be the operator $c_0 I + c_1 A + \cdots + c_r A^r \in L(V)$.

Observation 7. Let V be an $\mathbb{F}$-vector space, let $v \in V$, and let $S = \{v\}$. By Lemma 5 we see that

$$W_S = \Big\{ p(A)\, v : p(X) \in \mathbb{F}[X] \Big\}.$$

Remark 8. Let V be a vector space, let $A \in L(V)$, and let $S \subseteq V$. The smallest A-invariant subspace of V which contains S will not be used in the rest of this note.

Observation 9. Let V be an $\mathbb{F}$-vector space and let $A \in L(V)$. Suppose $V = W_1 \oplus \cdots \oplus W_k$ where the W_i's are A-invariant subspaces. Let

$$\mathfrak{B} = \coprod_{i=1}^{n} \mathfrak{B}_i$$

where $\mathfrak{B}_i$ is a basis of W_i for every i. Then $\mathfrak{B}$ is a basis of V. If V is finite dimensional, the matrix of A with respect to $\mathfrak{B}$ is a block diagonal matrix.

In Lemma 5, we have seen a way to construct A-invariant subspaces. The next result gives us another approach to find A-invariant subspaces. We will see that this method is more suitable for expressing V as a direct sum of A-invariant subspaces.

Lemma 10. *Let V be an $\mathbb{F}$-vector space and let $A, B \in L(V)$ such that $AB = BA$. Suppose $W = \ker B$. Then W is an A-invariant subspace.*

Proof. Let $v \in W$. Then we see that $Bv = 0$. Since $AB = BA$, we see that $BAv = ABv = 0$. Thus, we see that $Av \in \ker B$. Hence, it follows that W is an A-invariant subspace. $\square$

Observation 11. If V is an $\mathbb{F}$-vector space, then $L(V)$ is also an $\mathbb{F}$-vector space. Let $A \in L(V)$ and let $\mathcal{C}_A = \big\{B \in L(V) : AB = BA\big\}$. Then we see that $\mathcal{C}_A$ is a subspace of $L(V)$.

Remark 12. Let $A \in L(V)$. Then for every $k \geq 0$ we see that $A^k \in \mathcal{C}_A$. Thus, by Observation 11 we see that $p(A) \in \mathcal{C}_A$ for every $p(X) \in \mathbb{F}[X]$. So by Lemma 10 we see that $\ker p(A)$ is an A-invariant subspace for every $p(X) \in \mathbb{F}[X]$.

By Remark 12 and Observation 9 we see that we need to find polynomials $p_1(X), \ldots, p_r(X) \in \mathbb{F}[X]$ such that $V = \ker p_1(A) \oplus \cdots \oplus \ker p_r(A)$. We will use some results from algebra.

Lemma 13. *Let $p_1(X), \ldots, p_r(X) \in \mathbb{F}[X]$ be pairwise relatively prime and let $p(X) = p_1(X) \cdots p_r(X)$. For every $i \in \{1, \ldots, r\}$ let $q_i(X) = \dfrac{p(X)}{p_i(X)}$. Then the* gcd *of $q_1(X), \ldots, q_r(X)$ is* 1.

Proof. Suppose there exists an irreducible polynomial $f(X) \in \mathbb{F}[X]$ such that $f(X) \mid q_i(X)$ for every $i \in \{1, \ldots, r\}$. Since $f(X)$ is a prime polynomial which divides $q_1(X) = p_2(X) \cdots p_r(X)$, there exists $j \in \{2, \ldots, r\}$ such that $f(X) \mid p_j(X)$.

Again, since $f(X)$ divides $q_j(X) = p_1(X) \cdots \widehat{p_j(X)} \cdots p_r(X)$, there exists $k \in \{1, \ldots, r\} \setminus \{j\}$ such that $f(X) \mid p_k(X)$. This contradicts our assumption that $p_j(X)$ and $p_k(X)$ are relatively prime. It follows that the gcd of $q_1(X), \ldots, q_r(X)$ is 1. $\square$

Lemma 14. *Let R be a PID and let $x_1, \ldots, x_r \in R$. Suppose $a \in R$ is the gcd of $x_1, \ldots, x_r$. Then $\langle x_1, \ldots, x_r \rangle = \langle a \rangle$.*

Proof. Since R is a PID, there exists $b \in R$ such that $\langle x_1, \ldots, x_r \rangle = \langle b \rangle$. Since for every $i \in \{1, \ldots, r\}$ we have $a \mid x_i$ we see that $x_1, \ldots, x_r \in \langle a \rangle$ and hence $\langle x_1, \ldots, x_r \rangle \subseteq \langle a \rangle$. Thus, we see that $\langle b \rangle \subseteq \langle a \rangle$. For every $i \in \{1, \ldots, r\}$ we have $x_i \in \langle b \rangle$ and hence $b \mid x_i$. Since a is the gcd of the x_i's, we see that $b \mid a$ and hence $\langle a \rangle \subseteq \langle b \rangle$. It follows that $\langle a \rangle = \langle b \rangle$. ☐

Theorem 15 (Primary decomposition theorem)**.** *Let $A \in L(V)$. Suppose there exist $p_1(X), \ldots, p_r(X) \in \mathbb{F}[X]$ which are pairwise relatively prime. Let $p(X) = p_1(X) \cdots p_r(X)$. Then*

$$\ker p(A) = \ker p_1(A) \oplus \cdots \oplus \ker p_r(A).$$

Proof. For every $i \in \{1, \ldots, r\}$ let $q_i(X) = p(X)/p_i(X)$. By Lemmas 13 and 14 we see that $1 \in \big\langle q_1(X), \ldots, q_r(X) \big\rangle$. So there exist $f_1(X), \ldots, f_r(X) \in \mathbb{F}[X]$ such that $f_1(X)q_1(X) + \cdots + f_r(X)q_r(X) = 1$. It follows that

$$f_1(A)q_1(A) + \cdots + f_r(A)q_r(A) = I. \tag{1}$$

Let $v \in V$. From (1), it follows that $v = v_1 + \cdots + v_r$ where $v_i = f_i(A)q_i(A)v$ for every $i \in \{1, \ldots, r\}$. Suppose $v \in \ker p(A)$. Then for every $i \in \{1, \ldots, r\}$ we see that

$$p_i(A)v_i = p_i(A)f_i(A)q_i(A)v = f_i(A)p(A)v = 0$$

and hence $v_i \in \ker p_i(A)$. It follows that

$$\ker p(A) \subseteq \ker p_1(A) + \cdots + \ker p_r(A).$$

Let $i \in \{1, \ldots, r\}$. Since $p_i(X)q_i(X) = p(X)$, we see that $p_i(A)q_i(A) = p(A)$. Let $v \in V$. If $p_i(A)v$, then $p(A)v = 0$. It follows that $\ker p_i(A) \subseteq \ker p(A)$. Thus, we see that

$$\ker p_1(A) + \cdots + \ker p_r(A) \subseteq \ker p(A)$$

and hence

$$\ker p(A) = \ker p_i(A) + \cdots + \ker p_r(A).$$

Suppose for every $i \in \{1, \ldots, r\}$ there exists $v_i \in \ker p_i(A)$ such that $v_1 + \cdots + v_r = 0$. Let $j \in \{1, \ldots, r\}$. Since $p_j(X)$ and $q_j(X)$ are relatively prime, by Lemma 14 we see that there exist $f(X), g(X) \in \mathbb{F}[X]$ such that $f(X)p_j(X) + g(X)q_j(X) = 1$ and hence $f(A)p_j(A) + g(A)q_j(A) = I$. Thus,

$$v_j = f(A)p_j(A)v_j + g(A)q_j(A)v_j = g(A)q_j(A)v_j. \tag{2}$$

Since $v_j = -v_1 - \cdots - \widehat{v_j} - \cdots v_r$, we see that $p_1(A) \cdots \widehat{p_j(A)} \cdots p_r(A)v_j = 0$. Thus, we see that $q_j(A)v_j = 0$. So from (2) we see that $v_j = 0$. Thus, for every $j \in \{1, \ldots, r\}$ we have $v_j = 0$. Hence, we are done. ☐

Observation 16. Let $A \in L(V)$ and let $J_A = \big\{p(X) \in \mathbb{F}[X] : p(A) = 0\big\}$. Then J_A is an ideal in $\mathbb{F}[X]$. Suppose V is finite dimensional. Then $L(V)$ is finite dimensional. Since $\big\{A^k : k \geq 0\big\}$ is a subset of $L(V)$, it must be linearly dependent. Thus, it follows that $J_A \neq \{0\}$.
(The ideal J_A may be non-zero even when V is not finite dimensional.)

Definition 17. Let $A \in L(V)$. Suppose $J_A \neq \{0\}$. Since $\mathbb{F}[X]$ is a PID, the ideal J_A is a principal ideal. So there exists a unique monic polynomial $m_A(X) \in \mathbb{F}[X]$ such that $J_A = \big\langle m_A(X)\big\rangle$. We call the polynomial $m_A(X)$ the *minimal polynomial of* A. We sometimes denote $m_A(X)$ by $m(X)$.

Corollary 18. *Let $A \in L(V)$ such that $m_A(X) = (X - \lambda_1)^{k_1} \cdots (X - \lambda_r)^{k_r}$ where $\lambda_1, \dots, \lambda_r$ are distinct elements of $\mathbb{F}$, i.e., $m_A(X)$ splits in $\mathbb{F}[X]$. Then*

$$V = \ker(A - \lambda_1 I)^{k_1} \oplus \cdots \oplus \ker(A - \lambda_r I)^{k_r}.$$

Proof. Let $m(X) = m_A(X)$. Since $m(A) = 0$, we see that $\ker m(A) = V$. Also, since the λ_i's are distinct, the polynomials $(X - \lambda_1)^{k_1}, \dots, (X - \lambda_r)^{k_r}$ are pairwise relatively prime. Hence, the result follows from Theorem 15. $\square$

Observation 19. Let $A \in L(V)$ such that $m(X) = (X-\lambda_1)^{k_1} \cdots (X-\lambda_r)^{k_r}$ where $\lambda_1, \dots, \lambda_r$ are distinct elements of $\mathbb{F}$. Let $W = \ker(A - \lambda_1 I)^{k_1}$. We observe that $(A - \lambda_1 I)^{k_1} = 0$ on W. If $(A - \lambda_1 I)^{k_1 - 1} = 0$, then this contradicts the fact that $m(X)$ is the minimal polynomial of A. It follows that $(A - \lambda_1 I)^{k_1 - 1} \neq 0$.

Lemma 20. *Let $A \in L(V)$ and let $\lambda \in \mathbb{F}$. Suppose there exists $k \in \mathbb{N}$ such that $(A - \lambda I)^k = 0$ and $(A - \lambda I)^{k-1} \neq 0$. Then there exist $v_1, \dots, v_k \in V$ such that $v_1 \neq 0$, $Av_1 = \lambda v_1$, and $Av_i = \lambda v_i + v_{i-1}$ for every $i \in \{2, \dots, k\}$.*

Proof. As $(A - \lambda I)^{k-1} \neq 0$, there exists $u \in V$ such that $(A - \lambda I)^{k-1} u \neq 0$. For every $i \in \{1, \dots, k\}$ let $v_i = (A - \lambda I)^{k-i} u$. So we see that

$$v_1 = (A - \lambda I)^{k-1} u, \; v_2 = (A - \lambda I)^{k-2} u, \; \dots\dots, \; v_{k-1} = (A - \lambda I) u, \; v_k = u.$$

Since $(A - \lambda I) v_1 = (A - \lambda I)^k u = 0u = 0$, we see that $Av_1 = \lambda v_1$. For every $i \in \{2, \dots, k\}$ we see that $(A - \lambda I) v_i = v_{i-1}$ and so $Av_i = \lambda v_i + v_{i-1}$. $\square$

Lemma 21. *Let $A \in L(V)$ and let $\lambda \in \mathbb{F}$. Suppose there exist $v_1, \dots, v_k \in V$ such that $v_1 \neq 0$, $Av_1 = \lambda v_1$, and $Av_i = \lambda v_i + v_{i-1}$ for every $i \in \{2, \dots, k\}$. Then the set $\mathfrak{B} = \{v_1, \dots, v_k\}$ is linearly independent.*

Proof. Suppose there exists a non-zero tuple $(a_1, \dots, a_k) \in \mathbb{F}^k$ such that $a_1 v_1 + \cdots + a_k v_k = 0$. Let $m = \max\{i : a_i \neq 0\}$. Then $a_m \neq 0$. Since for every $i \in \{1, \dots, k\}$ we have $(A - \lambda I)^i v_i = 0$, we see that $(A - \lambda I)^{m-1} v_i = 0$ for every $i \in \{1, \dots, m-1\}$. Also, we see that $(A - \lambda I)^{m-1} v_m = v_1$. Thus,

$$0 = (A - \lambda I)^{m-1} 0 = (A - \lambda I)^{m-1} (a_1 v_1 + \cdots + a_{m-1} v_{m-1} + a_m v_m) = a_m v_1.$$

Since $v_1 \neq 0$, we get the contradiction that $a_m = 0$. Hence, it follows that the set $\mathfrak{B}$ is linearly independent. $\square$

Definition 22. Let $A \in L(V)$ and let $\lambda \in \mathbb{F}$. A set of vectors $\{v_1, \ldots, v_k\}$ is called a *Jordan string for* (A, λ) if $v_1 \neq 0$, $Av_1 = \lambda v_1$, and $Av_i = \lambda v_i + v_{i-1}$ for every $i \in \{2, \ldots, k\}$.

Remark 23. Let $A \in L(V)$ and let $\lambda \in \mathbb{F}$. By Lemma 21 we see that a Jordan string for (A, λ) is an independent set. If there exists a Jordan string for (A, λ), then we see that λ is an eigenvalue of A. Every Jordan string for (A, λ) contains a unique eigenvector for A with eigenvalue λ.

Remark 24. Let $B \in L(V)$ be a nilpotent operator. Then 0 is the unique eigenvalue of B. Suppose there exists $\lambda \in \mathbb{F}$ such that there exists a Jordan string for (B, λ). Then by Remark 23 we see that $\lambda = 0$.

Definition 25. Let $A \in L(V)$. A basis $\mathfrak{B}$ of V is called a *Jordan basis for* A if there exist $\lambda_1, \ldots, \lambda_m \in \mathbb{F}$ (not necessarily distinct) such that

$$\mathfrak{B} = \coprod_{i=1}^{m} \mathfrak{B}_i$$

where $\mathfrak{B}_i$ is a Jordan string for (A, λ_i) for every $i \in \{1, \ldots, m\}$.

Observation 26. Let $A \in L(V)$. Suppose there exists an *ordered* Jordan basis $\mathfrak{B}$ of V for the operator A. The matrix of A with respect to $\mathfrak{B}$ is a block diagonal matrix. Each block corresponds to a Jordan string in $\mathfrak{B}$. A block which corresponds to a Jordan string for (A, λ) is of the form

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & \lambda \end{pmatrix}.$$

Definition 27. Let $A \in L(V)$. Suppose there exists an ordered Jordan basis $\mathfrak{B}$ of V for the operator A. The matrix of A with respect to $\mathfrak{B}$ is said to be in *Jordan canonical form.*

Observation 28. Let $A \in L(V)$, let $\lambda \in \mathbb{F}$, and let $B = A - \lambda I$. Let $\mathfrak{B}$ be a basis of V. Since $A = B + \lambda I$, the matrix of A with respect to $\mathfrak{B}$ is obtained by adding the matrix λI to the matrix of B with respect to $\mathfrak{B}$. If $\mathfrak{B}$ is a Jordan string for $(B, 0)$, then $\mathfrak{B}$ is a Jordan string for (A, λ). Since if we have $v_{i-1}, v_i \in V$ such that $Bv_i = v_{i-1}$, then we see that $Av_i = \lambda v_i + v_{i-1}$.

Theorem 29. *Let* $\dim V = n$ *and let* $A \in L(V)$. *Suppose there exists* $\lambda \in F$ *and* $k \in \mathbb{N}$ *such that* $(A - \lambda I)^k = 0$. *Then* V *has a Jordan basis* $\mathfrak{B}$ *for* A.

Proof. Let $B = A - \lambda I$. By Observation 28, it is enough to show that V has a Jordan basis $\mathfrak{B}$ for B. If $B = 0$, then any basis of V is a Jordan basis for B. So we may assume that $B \neq 0$. Since $B^k = 0$, by Remark 24 we see that 0 is an eigenvalue of B. So there exists $u \in V \setminus \{0\}$ such that $Bu = 0$ and hence $\ker B \neq \{0\}$.

We will show that V has a Jordan basis $\mathfrak{B}$ for B by induction on $\dim V$. When $n = 1$, we see that $B = \{u\}$ is a Jordan basis. Let $n \geq 2$ and let W denote the image of B. Since $B \neq 0$, by the rank-nullity theorem, we see that $1 \leq \dim W \leq n - 1$. Since W is a B-invariant subspace, we see that $B_{|W} \in L(W)$. Since $B^k = 0$, we see that $\left(B_{|W}\right)^k = 0$.

Thus, by the induction hypothesis, we see that W has a Jordan basis $\mathfrak{B}'$ for the operator $B_{|W}$. Using Remark 24 we see that

$$\mathfrak{B}' = \coprod_{i=1}^{m} \mathfrak{B}'_i$$

where $\mathfrak{B}'_i$ is a Jordan string for $\left(B_{|W}, 0\right)$ for every $i \in \{1, \ldots, m\}$. For every $i \in \{1, \ldots, m\}$ let

$$\mathfrak{B}'_i = \left\{v_1^{(i)}, v_2^{(i)}, \ldots, v_{k_i}^{(i)}\right\}.$$

Then $Bv_1^{(i)} = 0$ and for every $j \in \{2, \ldots, k_i\}$ we see that $Bv_j^{(i)} = v_{j-1}^{(i)}$.

Let $\mathfrak{B}'_0 = \left\{v_1^{(1)}, \ldots, v_1^{(m)}\right\}$. Since $\mathfrak{B}'_0 \subseteq \mathfrak{B}$, we see that $\mathfrak{B}'_0$ is a linearly independent subset of $\ker B$. So there exists $r \in \mathbb{N} \cup \{0\}$ such that $\ker B$ has dimension $m + r$. There exist $z_1, \ldots, z_r \in V$ such that

$$\mathfrak{B}_0 = \left\{v_1^{(1)}, \ldots, v_1^{(m)}\right\} \bigcup \left\{z_1, \ldots, z_r\right\}$$

be a basis of $\ker B$. Since $\mathfrak{B}'$ is a basis of W, by the rank-nullity theorem, it follows that

$$n = k_1 + \cdots + k_m + m + r. \tag{3}$$

For every $i \in \{1, \ldots, m\}$ there exists $v_i \in V$ such that $Bv_i = v_{k_i}^{(i)}$. For every $i \in \{1, \ldots, m\}$ we let

$$\mathfrak{B}_i = \left\{v_1^{(i)}, v_2^{(i)}, \ldots, v_{k_i}^{(i)}, v_i\right\}$$

and for every $i \in \{m + 1, \ldots, m + r\}$ we let $\mathfrak{B}_i = \{z_i\}$. We observe that $\mathfrak{B}_i$ is a Jordan string for $(B, 0)$ for every $i \in \{1, 2, \ldots, m + r\}$. Let

$$\mathfrak{B} = \coprod_{i=1}^{m+r} \mathfrak{B}_i\,.$$

We claim that $\mathfrak{B}$ is a Jordan basis of V for the operator B. From (3) we see that $\mathfrak{B}$ has size n. So it is enough to show that $\mathfrak{B}$ is linearly independent. Suppose there exist there exist $a_1, \ldots, a_r \in \mathbb{F}$ and for every $i \in \{1, \ldots, m\}$ there exist $c_1^{(i)}, \ldots, c_{k_i}^{(i)}, b_i \in \mathbb{F}$ such that

$$a_1 z_1 + \cdots + a_r z_r + \sum_{i=1}^{m} \left(c_1^{(i)} v_1^{(i)} + c_2^{(i)} v_2^{(i)} + \cdots + c_{k_i}^{(i)} v_{k_i}^{(i)} + b_i v_i\right) = 0. \tag{4}$$

Applying the operator B we see that

$$\sum_{i=1}^{m}\left(c_2^{(i)}v_1^{(i)}+\cdots+c_{k_i}^{(i)}v_{k_i-1}^{(i)}+b_iv_{k_i}^{(i)}\right)=0.$$

This is a linear combination of the elements of $\mathfrak{B}'$ which is a basis of W. So we see that it must be the trivial linear combination. From (4) we see that

$$a_1z_1+\cdots+a_rz_r+c_1^{(1)}v_1^{(1)}+\cdots+c_1^{(m)}v_1^{(m)}=0.$$

This is a linear combination of the elements of $\mathfrak{B}_0$ which is a basis of $\ker B$. So we see that it must be the trivial linear combination. Thus, we see that the linear combination in (4) is the trivial linear combination. Hence, our claim is true and so we are done.

Since $\mathfrak{B}$ has size n, another way to show that $\mathfrak{B}$ is a Jordan basis of V for the operator B is to show that $\mathfrak{B}$ spans V.

Let $v \in V$. Since $\mathfrak{B}'$ is a basis of W for every $i \in \{1,\dots,m\}$ there exist $a_1^{(i)},\dots,a_{k_i}^{(i)} \in \mathbb{F}$ such that

$$Bv=\sum_{i=1}^{m}\left(a_1^{(i)}v_1^{(i)}+\cdots\cdots+a_{k_i-1}^{(i)}v_{k_i-1}^{(i)}+a_{k_i}^{(i)}v_{k_i}^{(i)}\right).$$

So we see that

$$Bv=B\left(\sum_{i=1}^{m}\left(a_1^{(i)}v_2^{(i)}+\cdots\cdots+a_{k_i-1}^{(i)}v_{k_i}^{(i)}+a_{k_i}^{(i)}v_i\right)\right).$$

Thus, we see that

$$v-\sum_{i=1}^{m}\left(a_1^{(i)}v_2^{(i)}+\cdots\cdots+a_{k_i-1}^{(i)}v_{k_i}^{(i)}+a_{k_i}^{(i)}v_i\right)\in\ker B.$$

Since $\mathfrak{B}_0$ is a basis of $\ker B$, there exist $b_1,\dots,b_m,c_1,\dots,c_r \in \mathbb{F}$ such that

$$v-\sum_{i=1}^{m}\left(a_1^{(i)}v_2^{(i)}+\cdots+a_{k_i-1}^{(i)}v_{k_i}^{(i)}+a_{k_i}^{(i)}v_i\right)$$

$$=b_1v_1^{(1)}+\cdots+b_mv_1^{(m)}+c_1z_1+\cdots+c_rz_r.$$

Hence, it follows that $\mathfrak{B}$ spans V. So we are done. ☐

Remark 30. Let $A \in L(V)$ and let $\lambda \in \mathbb{F}$. Suppose there exists $k \in \mathbb{N}$ such that $(A-\lambda I)^k = 0$. By Theorem 29, we see that V has a Jordan basis $\mathfrak{B}$ for A. We can check that $(A-\lambda I)^{k-1} \neq 0$ if and only if $\mathfrak{B}$ has a Jordan string for (A,λ) of size k.

Corollary 31. *Let V be a finite dimensional vector space over $\mathbb{F}$ and let $A \in L(V)$. If $m_A(X)$ splits in $\mathbb{F}[X]$, then V has a Jordan basis for A.*

Proof. This follows from Observation 9, Corollary 18, Observation 19, and Theorem 29. ☐