11.C Some Decomposition Theorems

For investigation of an operator $f: V \longrightarrow V$ on a K-vector space V, it is important to decompose V into simplest possible f-invariant subspaces. The decomposition theorem 11.C.2 is very useful. We first prove the following lemma:

11.C.1 Lemma Let $f: V \longrightarrow V$ and $g: V \longrightarrow V$ be commuting operators on the K-vector space V. For every polynomial $F \in K[X]$, the subspaces $\operatorname{Ker} F(f)$ and $\operatorname{Im} F(f)$ are g-invariant.

Proof Since $fg = gf$, g also commute with $F(f)$, i.e. $F(f)g = gF(f)$. Therefore, it follows that: if $x \in \operatorname{Ker} F(f)$, i.e. $F(f)(x) = 0$, then $F(f)(g(x)) = g(F(f)(x)) = 0$, i.e. $g(x) \in \operatorname{Ker} F(f)$. Further, if $x \in \operatorname{Im} F(f)$, i.e. $x = F(f)(y)$ with $y \in V$ and hence $g(x) = g(F(f)(y)) = F(f)(g(y))$, i.e. $g(x) \in \operatorname{Im} F(f)$.

11.C.2 Theorem Let $f: V \longrightarrow V$ be an operator on the K-vector space V. Further, let $F(f) = 0$ for some polynomial $F \in K[X]$, $F \neq 0$, with factorisation $F = F_1 \cdots F_r$ into pairwise relatively prime factors, i.e. $\gcd(F_i, F_j) = 1$ for $1 \leq i, j \leq r$, $i \neq j$. Let $G_i = F/F_i$, $i = 1, \ldots, r$ and

$$1 = S_1 G_1 + \cdots + S_r G_r \quad \text{with } S_1, \ldots, S_r \in K[X].$$

Then $V = \sum_{i=1}^{r} {}^{\oplus} \operatorname{Ker} F_i(f)$ and the family of projections p_i, $i = 1, \dots, r$, corresponding to this direct sum is

$$p_i = (S_i G_i)(f) = S_i(f) \circ G_i(f), \; i = 1, \dots, r.$$

In particular, $\operatorname{Ker} F_i(f) = \operatorname{Im} p_i$ and the projections p_i commute with f for every $i = 1, \dots, r$

Proof Since the polynomials $G_1, \dots, G_r$ are relatively prime in $K[X]$, by Bezout's Lemma there exist $S_1, \dots, S_r \in K[X]$ such that

$$1 = S_1 G_1 + \cdots + S_r G_r.$$

It is enough to show that the operators $p_i = (S_i G_i)(f)$ satisfy the conditions:

$$p_1 + \cdots + p_r = \mathrm{id}_V, \quad p_i p_j = 0 \text{ for } 1 \le i, j \le r, \; i \ne j$$

and $\operatorname{Im} p_i = \operatorname{Ker} F_i(f)$ for all $i = 1, \dots, r$.

The equation $\overbrace{p_1 + \cdots + p_r}^{= \mathrm{id}_V}$ is clear from $S_1 G_1 + \cdots + S_r G_r = 1$ by substituting f for the indeterminate X.

For $i \ne j$, F divides $(S_i G_i)(S_j G_j)$ and hence $p_i p_j = (S_i G_i)(f) \circ (S_j G_j(f)) = 0$, since $F(f) = 0$.

Further, it follows that $p_i = p_i \, \mathrm{id}_V = p_i \sum_{j=1}^{r} p_j = p_i^2$ for all $i = 1, \dots, r$. Finally, suppose that $x \in \operatorname{Ker} F_i(f)$, i.e. $F_i(f)(x) = 0$ and hence

$$x = \sum_{j=1}^{r} (S_j G_j)(f)(x) = (S_i G_i)(f)(x) = p_i(x),$$

i.e. $\operatorname{Ker} F_i(f) \subseteq \operatorname{Im} p_i$. Conversely, $F_i(f)\, p_i = F_i(f)(S_i G_i)(f) = (F_i S_i G_i)(f) = S_i(f) F(f) = 0$ for and hence $\operatorname{Im} p_i \subseteq \operatorname{Ker} F_i(f)$ for all $i=1,\dots,r$.

We remark here that the polynomials $S_1,\dots,S_r$ in 11.C.2 can be explicitly found by using the Euclidean algorithm (if the factors $F_1,\dots,F_r$ are given). From 11.C.5 we can also deduce the implication (3) $\Rightarrow$ (1) in 11.B.5. More precisely:

11.C.3 Theorem Let $f : V \longrightarrow V$ be an operator on the K-vector space V. Suppose that $F \in K[X]$ splits into simple linear factors in $K[X]$, i.e. $F = (X-\lambda_1)\cdots(X-\lambda_r)$, $\lambda_i, \lambda_j \in K$, $\lambda_i \neq \lambda_j$, $i \neq j$, and that $F(f)=0$. Then

$$V = V_f(\lambda_1) \oplus \cdots \oplus V_f(\lambda_r)$$

In particular, if f is diagonalisable. The projections $p_f(\lambda)$, $\lambda \in K$, the spectral decomposition

$$f = \sum_{\lambda \in K} \lambda\, p_f(\lambda),$$ are polynomials in f.

Proof Since $V_f(\lambda_i) = \operatorname{Ker}(f - \lambda_i \operatorname{id}_V)$, $i=1,\dots,r$, the assertion directly follows from 11.C.2.

11.C.4 Theorem Let $f : V \longrightarrow V$ be an operator on the K-vector space V. Let $F \in K[X]$, $F \neq 0$, with factorisation $F = F_1 \cdots F_r$ into product of pairwise relatively prime factors, i.e. $\gcd(F_i, F_j) = 1$ for all $1 \leq i, j \leq r$, $i \neq j$. Then

$$\operatorname{Ker} F(f) = \sum_{i=1}^{r}{}^{\oplus} \operatorname{Ker} F_i(f)$$

Proof Let $U = \operatorname{Ker} F(f)$. Then U is an f-invariant subspace and $F(f|U) = F(f)/U = 0$. Since $\operatorname{Ker} F_i(f) \subseteq U$, $\operatorname{Ker} F_i(f) = \operatorname{Ker} F_i(f|U)$ $i=1,\dots,r$. The assertion now follows from 11.C.2.

11.C.5 Primary Decomposition Theorem Let $f: V \to V$ be an operator on the finite dimensional K-vector space V with the characteristic polynomial $\chi_f = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and the minimal polynomial $\mu_f = p_1^{\beta_1} \cdots p_r^{\beta_r}$, where $p_1, \dots, p_r$ are distinct monic prime factors of χ_f (resp. μ_f). Then $1 \le \beta_i \le \alpha_i$, $i=1,\dots,r$ and

$$V = V_1 \oplus \cdots \oplus V_r \quad \text{with } V_i := \operatorname{Ker} P_i^{\alpha_i}(f) = \operatorname{Ker} P_i^{\beta_i}(f)$$

Further, $\chi_{f|V_i} = P_i^{\alpha_i}$, $\operatorname{Dim} V_i = \alpha_i \deg P_i$ and $\mu_{f|V_i} = P_i^{\beta_i}$, $i=1,\dots,r$. Moreover, the projections corresponding to the above direct sum decomposition $V = V_1 \oplus \cdots \oplus V_r$ are polynomials in f.

Proof By 11.A.14 χ_f and μ_f have the same prime factors and by the Cayley-Hamilton theorem $\mu_f \mid \chi_f$. This proves that $1 \le \beta_i \le \alpha_i$, $i=1,\dots,r$.

Let $V_i := \operatorname{Ker} P_i^{\alpha_i}(f)$. Since $P_i^{\alpha_i}$ are pairwise relatively prime it follows that $V = V_1 \oplus \cdots \oplus V_r$

by 11.C.2, since $\chi_f(f)=0$. Since $\mu_f(f)=0$, we have $V = V_1' \oplus \cdots \oplus V_r'$ with $V_i' = \operatorname{Ker} P_i^{\beta_i}(f)$, $i=1,\dots,r$. Now, since $V_i' \subseteq V_i$ for every $i=1,\dots,r$, it follows that $V_i' = V_i$ for all $i=1,\dots,r$.
Further, since $P_i^{\beta_i}(f/V_i)=0$ and $\mu_{f/V_i} \mid P_i^{\beta_i}$,

we have $\mu_f \mid \mu_{f/V_1} \cdots \mu_{f/V_r}$ and so $\mu_{f/V_i} = P_i^{\beta_i}$

Therefore χ_{f/V_i} is a power of P_i, since χ_{f/V_i} and μ_{f/V_i} have the same prime factors. From $\chi_f = \chi_{f/V_1} \cdots \chi_{f/V_r}$ it follows that $\chi_{f/V_i} = P_i^{\alpha_i}$, $i=1,\dots,r$.

The subspaces $V_1,\dots,V_r$ in 11.C.5 are called the <u>primary components of V with respect to f</u>.

Using Theorem 11.C.5 one can reduce the investigation of a linear operator on a finite dimensional vector space to the case when the characteristic polynomial and hence also the minimal polynomial is a power of a prime polynomial. If the primary component of f corresponding to the minimal polynomial $(X-\lambda)^\beta$ (resp. the characteristic polynomial $(X-\lambda)^\alpha$, then the restriction of f to U is trigonalizable with minimal polynomial $(X-\lambda)^\beta$ and hence there exists a basis of U such that the matrix of $f|U$

is an upper triangular matrix $\mathfrak{A} \in M_\alpha(K)$ with all diagonal elements equal to λ. This restriction is diagonalisable if and only if $\beta = 1$, i.e. the eigenvalue λ of f is a simple zero of the minimal polynomial of f. In this case we say that λ is a diagonalisable eigenvalue of f. If the characteristic polynomial χ_f of f splits (completely) into linear factors, i.e. if f is trigonalisable, then we have:

11.C.6 Theorem Let $f: V \longrightarrow V$ be an operator on the finite dimensional K-vector space V with the characteristic polynomial

$$\chi_f = (X - \lambda_1)^{\alpha_1} \cdots (X - \lambda_r)^{\alpha_r}; \quad \lambda_1, \ldots, \lambda_r \in K,$$

$\lambda_i \neq \lambda_j$, $i \neq j$. Then there exists a basis of V such that the matrix of f is a diagonal-block $\mathrm{Diag}(\mathfrak{A}_1, \ldots, \mathfrak{A}_r)$, where every block

$$\mathfrak{A}_i = \begin{pmatrix} \lambda_i & * & \cdots & * \\ 0 & \lambda_i & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_i \end{pmatrix} \in M_{\alpha_i}(K).$$

More generally the blocks $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ in 11.C.6, can be further simplified, we shall carry on this in the next section.

Now, let $f: V \longrightarrow V$ be an algebraic operator on the K-vector space V with minimal polynomial of the form

$$\mu_f = (X-\lambda_1)^{\beta_1} \cdots (X-\lambda_r)^{\beta_r}, \ \lambda_1, \dots, \lambda_r \in K,$$

$\lambda_i \neq \lambda_j$, $i \neq j$, $\beta_j \geq 1$ for $i = 1, \dots, r$. Then by 11.C.2

$$V = V_1 \oplus \cdots \oplus V_r$$

where $V_i = \operatorname{Ker}(f - \lambda_i \, id_V)^{\beta_i}$, $i = 1, \dots, r$ and the projections $p_1, \dots, p_r$ corresponding to this direct sum decompositions are polynomials in f and in particular they commute with f. The operator $d := \lambda_1 p_1 + \cdots + \lambda_r p_r$ is diagonalisable and operates on each V_i as the homothecy by λ_i. Therefore the operator $f - d$ operates on V_i as $f - \lambda_i \, id_V$ and hence nilpotent on V_i, since $(f - \lambda_i \, id_V)^{\beta_i} | V_i = 0$. Altogether the operator $n := f - d$ is nilpotent on V. This proves the existence assertion in the following theorem:

11.C.7 Theorem (Canonical decomposition) Let $f: V \longrightarrow V$ be an algebraic operator on the K-vector space V with the minimal polynomial $\mu_f \in K[X]$ which splits (completely) into linear factors in $K[X]$. Then there exist unique operators d and n on V with the following properties:

(1) $f = d + n$

(2) d and n commute, i.e. $dn = nd$.

(3) d is diagonalisable and n is nilpotent.
Further, d and n are polynomials in f.

Proof We need to show the uniqueness of d and n. Let d_1 and n_1 be operators on V satisfying the properties (1), (2), (3). Then $f = d + n = d_1 + n$ and so $h := d - d_1 = n - n_1$. The operators d_1 and n_1 commute with f and hence also with d, and n. Therefore by 11.B.15 $h = d - d_1 = n_1 - n$ is diagonalisable and nilpotent and hence must be the zero-operator, i.e. $d = d_1$ and $n = n_1$

The decomposition in 11.C.7 is called the additive canonical decomposition of f. If f is invertible, then it has the multiplicative canonical decomposition:

11.C.8 Corollary The notation and hypothesis as in 11.C.7, in addition assume that f is invertible, i.e. all eigenvalues of f are non-zero. Then there exist unique operators d and u on V with the following properties:

(1) $f = du$

(2) d and u commute, i.e. $du = ud$.

(3) d is diagonalisable and u is unipotent.

Further, d and n are polynomials in f.

Proof Let $f = d + n$ as in 11.C.7. Then d is invertible, since f is invertible and hence

$f = d(\mathrm{id}_V + d^{-1}n) = du$ with $u := \mathrm{id}_V + d^{-1}n$ unipotent. Further, d and u are polynomials in f. Since from a decomposition $f = du$, we also have a decomposition $f = d + d(u - \mathrm{id}_V)$ in the sense of 11.C.7, the uniqueness of d and u follows (this can be proved directly also)

Theorems 11.C.7 and 11.C.8 can be applied to triagonalisable and invertible triagonalisable operators on finite dimensional K-vector spaces.