CHAPTER 1

GTLA

1.1. Matrices and operations

Let $\mathbb{F}$ be a field. Let $m, n \in \mathbb{Z}_{>0}$.

- An $m \times n$ matrix with entries in $\mathbb{F}$ is a table of elements of $\mathbb{F}$ with m rows and n columns. More precisely, an $m \times n$ matrix with entries in $\mathbb{F}$ is a function
$$A\colon \{1, \dots, m\} \times \{1, \dots, n\} \longrightarrow \mathbb{F}.$$
- A *column vector of length* n is an $n \times 1$ matrix.
- A *row vector of length* n is an $1 \times n$ matrix.
- The (i, j) *entry of a matrix* A is the element $A(i, j)$ in row i and column j of A.
$$A = \begin{pmatrix} A(1,1) & A(1,2) & \cdots & A(1,m) \\ A(2,1) & A(2,2) & \cdots & A(2,m) \\ \vdots & & & \vdots \\ A(n,1) & A(n,2) & \cdots & A(n,m) \end{pmatrix}$$

Let $M_{m\times n}(\mathbb{F})$ be the set of $m \times n$ matrices with entries in $\mathbb{F}$.

- The *sum* of $m \times n$ matrices A and B is the $m \times n$ matrix $A + B$ given by
$$(A + B)(i, j) = A(i, j) + B(i, j), \qquad \text{for } i \in \{1, \dots, m\} \text{ and } j \in \{1, \dots, n\}.$$
- The *scalar multiplication* of an element $c \in \mathbb{F}$ with an $m \times n$ matrix A is the $m \times n$ matrix $c \cdot A$ given by
$$(c \cdot A)(i, j) = c \cdot A(i, j), \qquad \text{for } i \in \{1, \dots, m\} \text{ and } j \in \{1, \dots, n\}.$$
- The *product* of an $m \times n$ matrix A and an $n \times p$ matrix B is the $m \times p$ matrix AB given by
$$\begin{aligned}(AB)(i, k) &= \sum_{j=1}^{n} A(i, j)B(j, k) \\ &= A(i, 1)B(1, k) + A(i, 2)B(2, k) + \cdots + A(i, n)B(n, k),\end{aligned}$$
for $i \in \{1, \dots, m\}$ and $k \in \{1, \dots, p\}$.

The *zero matrix* is the $m \times n$ matrix $0 \in M_{m\times n}(\mathbb{F})$ given by
$$0(i, j) = 0, \qquad \text{for } i \in \{1, \dots, m\} \text{ and } j \in \{1, \dots, n\}.$$

The *negative* of a matrix $A \in M_{m\times n}(\mathbb{F})$ is the matrix $-A \in M_{m\times n}(\mathbb{F})$ given by

$$(-A)(i,j) = -A(i,j), \qquad \text{for } i \in \{1,\ldots,m\} \text{ and } j \in \{1,\ldots,n\}.$$

The following proposition says that $M_{m\times n}(\mathbb{F})$ is an $\mathbb{F}$-vector space.

Proposition 1.1.1. — *Let $m,n \in \mathbb{Z}_{>0}$ and let $M_{m\times n}(\mathbb{F})$ be the set of $m\times n$ matrices with entries in $\mathbb{F}$.*
(a) *If $A,B,C \in M_{m\times n}(\mathbb{F})$ then $A+(B+C) = (A+B)+C$.*
(b) *If $A,B \in M_{m\times n}(\mathbb{F})$ then $A+B = B+A$.*
(c) *If $A \in M_{m\times n}(\mathbb{F})$ then $0+A = A$ and $A+0 = A$.*
(d) *If $A \in M_{m\times n}(\mathbb{F})$ then $(-A)+A = 0$ and $A+(-A) = 0$.*
(e) *If $A \in M_{m\times n}(\mathbb{F})$ and $c_1,c_2 \in \mathbb{F}$ then $c_1\cdot(c_2\cdot A) = (c_1c_2)\cdot A$.*
(f) *If $A \in M_{m\times n}(\mathbb{F})$ and $1 \in \mathbb{F}$ is the identity in $\mathbb{F}$ then $1\cdot A = A$.*

The *Kronecker delta* is given by

$$\delta_{ij} = \begin{cases} 1, & \text{if } i=j, \\ 0, & \text{otherwise.} \end{cases}$$

The *identity matrix* is the $n\times n$ matrix $1 \in M_{n\times n}(\mathbb{F})$ given by

$$1(i,j) = \delta_{ij}, \qquad \text{for } i \in \{1,\ldots,m\} \text{ and } j \in \{1,\ldots,n\}.$$

The following proposition says that $M_n(\mathbb{F})$ is a ring (usually noncommutative).

Proposition 1.1.2. — *Let $n \in \mathbb{Z}_{>0}$ and let $M_n(\mathbb{F})$ be the set of $n\times n$ matrices in $\mathbb{F}$.*
(a) *If $A,B,C \in M_n(\mathbb{F})$ then $A+(B+C) = (A+B)+C$.*
(b) *If $A,B \in M_n(\mathbb{F})$ then $A+B = B+A$.*
(c) *If $A \in M_n(\mathbb{F})$ then $0+A = A$ and $A+0 = A$.*
(d) *If $A \in M_n(\mathbb{F})$ then $(-A)+A = 0$ and $A+(-A) = 0$.*
(e) *If $A,B,C \in M_n(\mathbb{F})$ then $A(BC) = (AB)C$.*
(f) *If $A,B,C \in M_n(\mathbb{F})$ then $(A+B)C = AC+BC$ and $C(A+B) = CA+CB$.*
(g) *If $A \in M_n(\mathbb{F})$ then $1A = A$ and $A1 = A$.*

The *transpose* of an $m\times n$ matrix A is the $n\times m$ matrix A^t given by

$$A^t(i,j) = A(j,i), \qquad \text{for } i \in \{1,\ldots,n\} \text{ and } j \in \{1,\ldots,m\}.$$

The following proposition says that transpose is an antiautomorphism of the ring $M_n(\mathbb{F})$.

Proposition 1.1.3. — *Let $m,n \in \mathbb{Z}_{>0}$, let $M_{m\times n}(\mathbb{F})$ be the set of $m\times n$ matrices with entries in $\mathbb{F}$, and let $M_n(\mathbb{F})$ be the set of $n\times n$ matrices in $\mathbb{F}$.*
(a) *If $A,B \in M_{m\times n}(\mathbb{F})$ then $(A+B)^t = A^t+B^t$,*
(b) *If $A \in M_{m\times n}(\mathbb{F})$ and $c \in \mathbb{F}$ then $(c\cdot A)^t = c\cdot A^t$,*
(c) *If $A,B \in M_n(\mathbb{F})$ then $(AB)^t = B^tA^t$.*
(d) *If $A \in M_n(\mathbb{F})$ then $(A^t)^t = A$.*

1.2. Vector spaces and linear transformations

Let $\mathbb{F}$ be a field. A $\mathbb{F}$-*vector space* is a set V with functions

$$\begin{array}{ccc} V\times V & \to & V \\ (v_1,v_2) & \mapsto & v_1+v_2 \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{K}\times V & \to & V \\ (c,v) & \mapsto & cv \end{array}$$

(*addition* and *scalar multiplication*) such that

(a) If $v_1, v_2, v_3 \in V$ then $(v_1+v_2)+v_3 = v_1+(v_2+v_3)$,
(b) There exists $0 \in V$ such that if $v \in V$ then $0+v = v$ and $v+0 = v$,
(c) If $v \in V$ then there exists $-v \in V$ such that $v+(-v) = 0$ and $(-v)+v = 0$,
(d) If $v_1, v_2 \in V$ then $v_1+v_2 = v_2+v_1$,
(e) If $c \in \mathbb{F}$ and $v_1, v_2 \in V$ then $c(v_1+v_2) = cv_1+cv_2$,
(f) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then $(c_1+c_2)v = c_1v+c_2v$,
(g) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then $c_1(c_2v) = (c_1c_2)v$,
(h) If $v \in V$ then $1v = v$.

Linear transformations are for comparing vector spaces.

Let $\mathbb{F}$ be a field and let V and W be $\mathbb{F}$-vector spaces. A *linear transformation from V to W* is a function $f\colon V \to W$ such that

(a) If $v_1, v_2 \in V$ then $f(v_1+v_2) = f(v_1)+f(v_2)$,
(b) If $c \in \mathbb{F}$ and $v \in V$ then $f(cv) = cf(v)$.

One vector space can be a subspace of another.

Let V be an $\mathbb{F}$-vector space. A *subspace of* V is a subset $W \subseteq V$ such that

(a) If $w_1, w_2 \in W$ then $w_1+w_2 \in W$,
(b) $0 \in W$,
(c) If $w \in W$ then $-w \in W$,
(d) If $w \in W$ and $c \in \mathbb{F}$ then $cw \in W$.

The tiniest vector space is the zero space.

The *zero space*, (0), is the set containing only 0 with the operations $0+0=0$ and $c\cdot 0$, for $c \in \mathbb{F}$.

1.3. Kernels and images

The *kernel*, or *null space*, of a linear transformation $f\colon V \to W$ is the set

$$\ker(f) = \{v \in V \mid f(v) = 0\}.$$

The *image* of a linear transformation $f\colon V \to W$ is the set

$$\mathrm{im}(f) = \{f(v) \mid v \in V\}.$$

Proposition 1.3.1. — *Let $f\colon V \to W$ be a linear transformation. Then*

(a) $\ker f$ *is a subspace of* V, *and*
(b) $\mathrm{im}\, f$ *is a subspace of* W.

Let S and T be sets and let $f\colon S \to T$ be a function.
The function $f\colon S \to T$ is *injective* if f satisfies:

$$\text{if } s_1, s_2 \in S \text{ and } f(s_1) = f(s_2) \quad \text{then } s_1 = s_2.$$

The function $f\colon S \to T$ is *surjective* if f satisfies:

$$\text{if } t \in T \text{ then there exists } s \in S \text{ such that } f(s) = t.$$

Proposition 1.3.2. — *Let $f\colon V \to W$ be a linear transformation. Then*

(a) $\ker f = \{0\}$ *if and only if f is injective, and*
(b) $\operatorname{im} f = W$ *if and only if f is surjective.*

The *rank* of a linear transformation $f\colon V \to W$ is the dimension of the image of f and the *nullity* of a linear transformation f is the dimension of the kernel of f,

$$\operatorname{rank}(f) = \dim(\operatorname{im}(f)) \qquad \text{and} \qquad \operatorname{nullity}(f) = \dim(\ker(f)).$$

1.4. Bases and dimension

Let $\mathbb{F}$ be a field and let V be a vector space over $\mathbb{F}$. Let $\{v_1, v_2, \ldots, v_k\}$ be a subset of V.

- The *span* of the set $\{v_1, \ldots, v_k\}$ is

$$\operatorname{span}\{v_1, \ldots, v_k\} = \{c_1v_1 + c_2v_2 + \cdots + c_kv_k \mid c_1, c_2, \ldots, c_k \in \mathbb{F}\}.$$

- A *linear combination* of $v_1, v_2, \ldots, v_k$ is an element of $\operatorname{span}\{v_1, \ldots, v_k\}$.
- The set $\{v_1, \ldots, v_k\}$ is *linearly independent* if it satisfies:

$$\text{if } c_1, \ldots, c_k \in \mathbb{F} \text{ and } c_1v_1 + \cdots + c_kv_k = 0 \quad \text{then} \quad c_1 = 0,\ c_2 = 0,\ \ldots,\ c_k = 0.$$

- A *basis* of V is a subset $B \subseteq V$ such that
  (a) $\operatorname{span}(B) = V$,
  (b) B is linearly independent.
- The *dimension* of V is the cardinality (number of elements) of a basis of V.

Theorem 1.4.1. — *(Characterization of a basis) Let V be a vector space and let B be a subset of V. The following are equivalent:*
(a) *B is a basis of V;*
(b) *B is a minimal element of $\{S \subseteq V \mid \operatorname{span}(S) = V\}$, ordered by inclusion;*
(c) *B is a maximal element of $\{L \subseteq V \mid L$ is linearly independent$\}$, ordered by inclusion.*

Theorem 1.4.2. — *(Existence of a basis) Let V be a vector space over a field $\mathbb{F}$. Then*
(a) *V has a basis, and*
(b) *Any two bases of V have the same number of elements.*

1.5. Addition, scalar multiplication and composition of linear transformations

The *sum* of two linear transformations $f_1 \colon V \to W$ and $f_2 \colon V \to W$ is the linear transformation $(f_1 + f_2) \colon V \to W$.

$$(f_1 + f_2)(v) = f_1(v) + f_2(v), \qquad \text{for } v \in V.$$

Let $f \colon V \to W$ be a linear transformation and let $c \in \mathbb{F}$. The *scalar multiplication* of f by c is the linear transformation $(cf) \colon V \to W$ given by

$$(cf)(v) = c \cdot f(v), \qquad \text{for } v \in V.$$

The *composition* of a linear transformation $f_2 \colon V \to W$ and a linear transformation $f_1 \colon W \to Z$ is the linear transformation $(f_1 \circ f_2) \colon V \to Z$ given by

$$(f_1 \circ f_2)(v) = f_1(f_2(v)), \qquad \text{for } v \in V.$$

1.6. Matrices of linear transformations and change of basis matrices

Let V and W be $\mathbb{F}$-vector spaces. Let B be a basis of V and let C be a basis of W. Let $f \colon V \to W$ be a linear transformation. The *matrix of $f \colon V \to W$ with respect to the bases B and C* is the matrix

$$f_{CB} \in M_{C \times B}(\mathbb{F}) \qquad \text{given by} \qquad f(b) = \sum_{c \in C} f_{CB}(c, b)c \quad \text{for } b \in B$$

(here we view matrices in $M_{C \times B}(\mathbb{F})$ as functions $A \colon C \times B \to \mathbb{F}$ so that the (c, b) entry of the matrix A is the value $A(c, b)$).

Proposition 1.6.1. — *Let V and W and Z be $\mathbb{F}$-vector spaces with bases B, C and D, respectively. Let*

$$f \colon V \to W, \quad g \colon V \to W, \quad h \colon W \to Z \quad \textit{be linear transformations}$$

and let $c \in \mathbb{F}$. Then

$$(cf)_{CB} = c \cdot f_{CB}, \qquad f_{CB} + g_{CB} = (f + g)_{CB} \qquad \textit{and} \qquad (h \circ g)_{DB} = h_{DC} g_{CB}.$$

Let V be an $\mathbb{F}$-vector space and let B and C be bases of V. The *change of basis matrix from B to C* is the matrix $P_{CB} \in M_{C \times B}(\mathbb{F})$ given by

$$b = \sum_{c \in C} P_{CB}(c, b)c, \qquad \text{for } b \in B. \tag{1.6.1}$$

Proposition 1.6.2. — *Let $g \colon V \to W$ and $f \colon V \to V$ be linear transformations. Let*

$$B_1 \textit{ and } B_2 \textit{ be bases of } V, \quad \textit{and let} \quad C_1 \textit{ and } C_2 \textit{ be bases of } W,$$

and let $P_{B_1 B_2}$ and $P_{C_2 C_1}$ be the change of basis matrices defined as in (1.6.1). *Then*

$$g_{C_2 B_2} = P_{C_2 C_1} g_{C_1 B_1} P_{B_1 B_2} \qquad \textit{and} \qquad f_{B_2 B_2} = P_{B_1 B_2}^{-1} f_{B_1 B_1} P_{B_1 B_2}.$$

Proposition 1.6.3. — *Let $P \in M_n(\mathbb{F})$. The matrix P is invertible if and only if the columns of P are linearly independent in $\mathbb{F}^n$.*

1.6.1. Minimal and characteristic polynomials (annihilators of $\mathbb{F}[x]$-modules). — Let $A \in M_n(\mathbb{F})$. Let

$$\begin{array}{rccc} \varphi_A\colon & \mathbb{F}[x] & \to & M_n(\mathbb{F}) \\ & c_0 + c_1x + \cdots + c_rx^r & \mapsto & c_0 + c_1A + \cdots c_rA^r \end{array}$$

The *kernel* of φ_A is

$$\ker(\varphi_A) = \{p(x) \in \mathbb{F}[x] \mid \varphi_A(p(x)) = 0.\}$$

Proposition 1.6.4. — *There exists a unique monic polynomial $m(x) \in \mathbb{F}[x]$ such that $\ker(\varphi_A) = m(x)\mathbb{F}[x]$.*

Let $A \in M_n(\mathbb{F})$.

- The **minimal polynomial** of A is the monic polynomial $m(x) \in \mathbb{F}[x]$ such that
$$\ker \varphi_A = m(x)\mathbb{F}[x].$$
- The matrix $x - A \in M_n(\mathbb{F}[x])$. The **characteristic polynomial** of A is $\det(x - A)$.

Proposition 1.6.5. — *(Cayley-Hamlton theorem) Let $A \in M_n(\mathbb{F})$ and let $m(x)$ be the minimal polynomial of A. Then*

$$\det(x - A) \in m(x)\mathbb{F}[x].$$

1.6.2. Diagonalization (simple and semisimple $\mathbb{F}[x]$-modules). — Let $\mathbb{F}$ be a field and let $A \in M_n(\mathbb{F})$.

- A subspace $U \subseteq \mathbb{F}^n$ is *A-invariant*, or U is an *A-submodule of* $\mathbb{F}^n$, if U satisfies:
$$\text{if } u \in U \text{ then } Au \in U.$$
- Let $\lambda \in \mathbb{F}$. An *eigenvector of A of eigenvalue* λ is $p \in \mathbb{F}^n$ such that $p \neq 0$ and
$$Ap = \lambda p.$$
- The matrix A is *diagonalizable* if there exist $P \in GL_n(\mathbb{F})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that
$$P^{-1}AP = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

HW: Show that p is an eigenvector of A if and only if $\mathbb{F}p$ is A-invariant.

HW: Show that p is an eigenvector of A if and only if $p \in \ker(A - \lambda)$.

HW: Show that if $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ and $P^{-1}AP = D$ then

$$\det(A) = \lambda_1 \cdots \lambda_n \quad \text{and} \quad \det(x - A) = (x - \lambda_1) \cdots (x - \lambda_n).$$

Proposition 1.6.6. — *Let $\mathbb{F}$ be a field and let $A \in M_n(\mathbb{F})$.*
(a) If $p_1, \ldots, p_k$ are eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_k$ and $\lambda_1, \ldots, \lambda_k$ are all distinct then $p_1, \ldots, p_k$ are linearly independent.
(b) Let $A \in M_n(\mathbb{F})$. Then A is diagonalizable if and only if there exist n linearly independent eigenvectors of A.
(c) If $\mathbb{F}$ is algebraically closed then A has an eigenvector.

1.6.3. Some proofs. —

Proposition 1.6.7. — *Let V and W and Z be $\mathbb{F}$-vector spaces with bases B, C and D, respectively. Let*

$$f\colon V\to W,\quad g\colon V\to W,\quad h\colon W\to Z\quad \text{be linear transformations}$$

and let $c\in\mathbb{F}$. Then

$$(cf)_{CB}=c\cdot f_{CB},\qquad f_{CB}+g_{CB}=(f+g)_{CB}\qquad\text{and}\qquad (h\circ g)_{DB}=h_{DC}g_{CB}.$$

Proof. — Let $b\in B$ and $c'\in C$. Taking the coefficient of c' on each side of

$$\sum_{c\in C}(\alpha f)_{CB}(c,b)c=(\alpha f)(b)=\alpha\cdot f(b)=\alpha\cdot\Big(\sum_{c\in C}f_{CB}(c,b)c\Big)=\sum_{c\in C}\alpha f_{CB}(c,b)c$$

gives $(\alpha f)_{CB}(c',b)=\alpha\cdot f_{CB}(c',b)$.
So $(\alpha f)_{CB}=\alpha\cdot f_{CB}$.
Let $b\in B$ and $c'\in C$. Taking the coefficient of c' on each side of

$$\begin{aligned}\sum_{c\in C}(f+g)_{CB}(c,b)c=(f+g)(b)=f(b)+g(b)&=\sum_{c\in C}(f_{CB}(c,b)c+\sum_{c\in C}g_{CB}(c,b)c\\ &=\sum_{c\in C}(f_{CB}(c,b)c+g_{CB}(c,b)c=\sum_{c\in C}(f_{CB}(c,b)+g_{CB}(c,b))c\end{aligned}$$

gives $(f_{CB}+g_{CB})(c',b)=f_{CB}(c',b)+g_{CB}(c',b)$.
So $f_{CB}+g_{CB}=(f+g)_{CB}$.
Let $b\in B$ and $d'\in D$. Taking the coefficient of d' on each side of

$$\begin{aligned}\sum_{d\in D}(h\circ g)_{DB}(d,b)d=(h\circ g)(b)=h(g(b))&=h\Big(\sum_{c\in C}g_{CB}(c,b)c\Big)\\ &=\sum_{c\in C}g_{CB}(c,b)h(c)=\sum_{c\in C}\sum_{d\in D}g_{CB}(c,b)h_{DC}(d,c)d,\end{aligned}$$

gives $(h\circ g)_{DB}(d',b)=\displaystyle\sum_{c\in C}\sum_{d\in D}h_{DC}(d,'c)g_{CB}(c,b)=(h_{DC}g_{CB})(d',b)$.
So $(h\circ g)_{DB}=(h_{DC}g_{CB})$. □

Proposition 1.6.8. — *Let $g\colon V\to W$ and $f\colon V\to V$ be linear transformations. Let*

$$B_1 \text{ and } B_2 \text{ be bases of } V,\quad \text{and let}\quad C_1 \text{ and } C_2 \text{ be bases of } W,$$

and let $P_{B_1B_2}$ and $P_{C_2C_1}$ be the change of basis matrices defined as in (1.6.1). *Then*

$$g_{C_2B_2}=P_{C_2C_1}g_{C_1B_1}P_{B_1B_2}\qquad\text{and}\qquad f_{B_2B_2}=P^{-1}_{B_1B_2}f_{B_1B_1}P_{B_1B_2}.$$

Proof. — Let $\beta,\beta'\in B_2$. Comparing coefficients of β' on each side of

$$\begin{aligned}\beta&=\sum_{b\in B_1}P_{B_1B_2}(b,\beta)b=\sum_{b\in B_1}P_{B_1B_2}(b,\beta)\sum_{\beta'\in B_2}P_{B_2B_1}(\beta',b)\beta'\\ &=\sum_{b\in B_1}\sum_{\beta'\in B_2}P_{B_2B_1}(\beta',b)P_{B_1B_2}(b,\beta)\beta'=\sum_{b\in B_1}\sum_{\beta'\in B_2}(P_{B_2B_1}P_{B_1B_2})(\beta',\beta)\beta'\end{aligned}$$

gives

$$(P_{B_2B_1}P_{B_1B_2})(\beta',\beta)=\delta_{\beta'\beta}.$$

So $P_{B_2B_1} = P_{B_1B_2}^{-1}$.
Let $\beta \in B_1$ and $c \in B_2$. Taking the coefficient of b' on each side of

$$f(c) = \sum_{c' \in B_2} f_{B_2B_2}(c', c)c' = \sum_{b' \in B_1} f_{B_2B_2}(c', c)P_{B_1B_2}(b', c')b'$$

and

$$f(c) = f\Big(\sum_{b \in B_1} P_{B_1B_2}(b, c)b\Big) = \sum_{b \in B_1} P_{B_1B_2}(b, c)f(b) = \sum_{b \in B_1} P_{B_1B_2}(b, c) \sum_{b' \in B_1} f_{B_1B_1}(b', b)b'$$

gives

$$(P_{B_1B_2}f_{B_2B_2})(\beta, b) = (f_{B_1B_1}P_{B_1B_2})(\beta, b).$$

So

$$P_{B_1B_2}f_{B_2B_2} = f_{B_1B_1}P_{B_1B_2} \qquad \text{and thus} \qquad f_{B_2B_2} = P_{B_1B_2}^{-1}f_{B_1B_1}P_{B_1B_2}.$$

Let $\gamma' \in C_2$ and $\beta \in B_2$. Taking the coefficient of γ on each side of

$$\begin{aligned}
\sum_{\gamma \in C_2} g_{C_2B_2}(\gamma, \beta)\gamma = g(\beta) = g(\sum_{b \in B_1} P_{B_1B_2}(b, \beta)b) &= \sum_{b \in B_1} P_{B_1B_2}(b, \beta)g(b) \\
&= \sum_{b \in B_1} P_{B_1B_2}(b, \beta) \sum_{c \in C_1} g_{C_1B_1}(c, b)c \\
&= \sum_{b \in B_1} P_{B_1B_2}(b, \beta) \sum_{c \in C_1} g_{C_1B_1}(c, b) \sum_{\gamma \in C_2} P_{C_2C_1}(\gamma, c)\gamma \\
&= \sum_{b \in B_1, c \in C_1, \gamma \in C_2} P_{C_2C_1}(\gamma, c)g_{C_1B_1}(c, b)P_{B_1B_2}(b, \beta)\gamma \\
&= \sum_{\gamma \in C_2} (P_{C_2C_1}g_{C_1B_1}P_{B_1B_2})(\gamma, \beta)\gamma
\end{aligned}$$

gives $g_{C_2B_2}(\gamma', \beta) = (P_{C_2C_1}g_{C_1B_1}P_{B_1B_2})(\gamma', \beta)$. So $g_{C_2B_2} = P_{C_2C_2}g_{C_1B_1}P_{B_1B_2}$. □

Proposition 1.6.9. — *Let $P \in M_n(\mathbb{F})$. The matrix P is invertible if and only if the columns of P are linearly independent in $\mathbb{F}^n$.*

Proof. —
$\Rightarrow$: Assume P is invertible. Let $p_1, \ldots, p_n$ be the columns of P.
To show: $\{p_1, \ldots, p_n\}$ is linearly independent.
Assume $c_1, \ldots, c_n \in \mathbb{F}$ and $c_1p_1 + \cdots + c_np_n = 0$.
Let $c = (c_1, \ldots, c_n)^t \in \mathbb{F}^n$.
Since $c_1p_1 + \cdots + c_np_n = 0$ then $Pc = 0$.
So $c = P^{-1}Pc = P^{-1}0 = 0$.
So $c_1 = 0, \ldots, c_n = 0$.
$\Leftarrow$: Assume the columns of P are linearly independent.
To show: There exists $Q \in M_n(\mathbb{F})$ such that $QP = 1$.
Let $p_1, \ldots, p_n$ be the columns of P.
Since $B = \{p_1, \ldots, p_n\}$ is linearly independent and $\dim(\mathbb{F}^n) = n$ then B is a maximal linearly independent set.
Thus, by Theorem 1.4.1, B is a basis.
Let $S = \{e_1, \ldots, e_n)\}$ where e_i has 1 in the ith spot and 0 elsewhere.
Then $P = P_{BS}$, the change of basis matrix from S to B.

Let $Q = P_{SB}$, the change of basis matrix from B to S.
Then $QP = P_{SB}P_{BS} = P_{SS} = 1$.
So P is invertible. $\square$

Proposition 1.6.10. — *There exists a unique monic polynomial $m(x) \in \mathbb{F}[x]$ such that* $\ker(\varphi_A) = m(x)\mathbb{F}[x]$.

Proof. —
Let $r = \min\{\deg(p) \mid p \in \ker(\varphi_A)\}$ and let $p(x) \in \ker(\varphi_A)$ with $\deg(p) = r$ and let

$$m(x) = \frac{1}{a_r}p(x), \qquad \text{where} \quad p(x) = a_r x^r + \cdots + a_1 x + a_0.$$

To show: $\ker(\varphi_A) = m(x)\mathbb{F}[x]$.
To show: (a) $\ker(\varphi_A) \subseteq m(x)\mathbb{F}[x]$.
To show: (b) $\ker(\varphi_A) \supseteq m(x)\mathbb{F}[x]$.

(a) Assume $f \in \ker(\varphi_A)$.
Then there exist $q(x), g(x) \in \mathbb{F}[x]$ with $\deg(g(x)) < r$ such that

$$f(x) = q(x)m(x) + g(x).$$

Since $f(x) \in \ker(\varphi_A)$ and $q(x)m(x) \in \ker(\varphi_A)$ then $g(x) \in \ker(\varphi_A)$.
Since $\deg(g(x)) < r$ then $g(x) = 0$.
So $f(x) = q(x)m(x)$.
So $f(x) \in m(x)\mathbb{F}[x]$.

(b) Let $f(x) \in m(x)\mathbb{F}[x]$.
To show: $f(x) \in \ker(\varphi_A)$.
Since $f(x) \in m(x)\mathbb{F}[x]$ there exists $q(x) \in \mathbb{F}[x]$ such that $f(x) = q(x)m(x)$.
So $f(A) = q(A)m(A) = q(A) \cdot 0 = 0$.
So $f(A) \in \ker(\varphi_A)$.

So $\ker(\varphi_A) = m(x)\mathbb{F}[x]$. $\square$

Proposition 1.6.11. — *(Cayley-Hamlton theorem) Let $A \in M_n(\mathbb{F})$ and let $m(x)$ be the minimal polynomial of A. Then*

$$\det(x - A) \in m(x)\mathbb{F}[x].$$

Proof. — Let $p = \det(x - A)$. BY CRAMER'S RULE,

$$(x - A)\mathrm{adj}(x - A) = \det(x - A)1_n, \qquad \text{where } 1_n \text{ is the } n \times n \text{ identity matrix.}$$

Evaluating both sides at A gives that $p(A) = 0$. So $p \in \ker(\varphi_A)$. $\square$

Proposition 1.6.12. — *Let $\mathbb{F}$ be a field and let $A \in M_n(\mathbb{F})$.*
(a) If $p_1, \ldots, p_k$ are eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_k$ and $\lambda_1, \ldots, \lambda_k$ are all distinct then $p_1, \ldots, p_k$ are linearly independent.
(b) Let $A \in M_n(\mathbb{F})$. Then A is diagonalizable if and only if there exist n linearly independent eigenvectors of A.
(c) If $\mathbb{F}$ is algebraically closed then A has an eigenvector.

Proof. — (a) Assume $c_1p_1 + \cdots + c_np_n = 0$.
To show: If $j \in \{1, \ldots, n\}$ then $c_j = 0$.
Assume $j \in \{1, \ldots, n\}$.
Then

$$\begin{aligned} 0 &= (A - d_1) \cdots (A - d_{j-1})(A - d_{j+1}) \cdots (A - d_n)(c_1p_1 + \cdots + c_np_n) \\ &= \cdots \\ &= c_j(d_j - d_1) \cdots (d_j - d_{j-1})(d_j - d_{j+1}) \cdots (d_j - d_n)p_j. \end{aligned}$$

So $c_jp_j = 0$. So $c_j = 0$.
(b) Let $p_1, \ldots, p_n$ be the columns of P. Then $AP = PD$ gives that $p_1, \ldots, p_n$ are eigenvectors of A.

Rewriting this equation as

$$AP = PD, \qquad \text{where} \quad D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n),$$

the eigenvectors of A are the columns of P. By Proposition 1.6.3, P being invertible is equivalent to its n columns being linearly independent.
(c) Since $\mathbb{F}$ is algebraically closed $m(x)$ factors: there exists $a_1, \ldots, a_n \in \mathbb{F}$ such that

$$m(x) = (x - a_1) \cdots (x - a_n).$$

Since $(A-a_2) \cdots (A-a_n) \neq 0$ there exists $w \in V$ such that $v = (A-a_2) \cdots (A-a_n)w \neq 0$. Then $(A - a_1)(v) = m(A)(w) = 0$. So $A(v) = a_1v$. $\square$