Linear Algebra 1: Lecture 9

Irena Penev

Winter 2022/2023

1 One-to-one linear transformations

Recall that, given a linear transformation $f : U \to V$, where U and V are vector spaces over a field $\mathbb{F}$, the *kernel* of f is defined to be the set

$$\text{Ker}(f) := \{\mathbf{u} \in U \mid f(\mathbf{u}) = \mathbf{0}\}.$$

Theorem 1.1. *Let U and V be vector spaces over a field $\mathbb{F}$, and let $f : U \to V$ be a linear transformation. Then the following are equivalent:*

(i) f is one-to-one;

(ii) $Ker(f) = \{\mathbf{0}\}$.

Proof. Suppose first that (i) holds; we must show that (ii) holds. Since f is one-to-one, there is at most one vector $\mathbf{u} \in U$ such that $f(\mathbf{u}) = \mathbf{0}$, i.e. $|\text{Ker}(f)| \leq 1$. On the other hand, Proposition 1.4 from Lecture Notes 8 guarantees that $\mathbf{0} \in \text{Ker}(f)$, and so $\mathbf{0} \in \text{Ker}(f)$. So, $\text{Ker}(f) = \{\mathbf{0}\}$, i.e. (ii) holds.

Suppose now that (ii) holds; we must show that (i) holds. Fix $\mathbf{u}_1, \mathbf{u}_2 \in U$ such that $f(\mathbf{u}_1) = f(\mathbf{u}_2)$. Then

$$\begin{array}{rcll} f(\mathbf{u}_1 - \mathbf{u}_2) & = & f(\mathbf{u}_1 + (-1)\mathbf{u}_2) & \text{because } (-1)\mathbf{u} = -\mathbf{u} \text{ for all } \mathbf{u} \in U \\ & & & \text{(by Prop. 2.3(d) from Lec. Notes 6)} \\ & = & f(\mathbf{u}_1) + (-1)f(\mathbf{u}_2) & \text{because } f \text{ is linear} \\ & = & f(\mathbf{u}_1) - f(\mathbf{u}_2) & \text{because } (-1)\mathbf{v} = -\mathbf{v} \text{ for all } \mathbf{v} \in V \\ & & & \text{(by Prop. 2.3(d) from Lec. Notes 6)} \\ & = & \mathbf{0} & \text{because } f(\mathbf{u}_1) = f(\mathbf{u}_2), \end{array}$$

and it follows that $\mathbf{u}_1 - \mathbf{u}_2 \in \text{Ker}(f)$. So, by (ii), $\mathbf{u}_1 - \mathbf{u}_2 = \mathbf{0}$, and consequently, $\mathbf{u}_1 = \mathbf{u}_2$. It follows that f is one-to-one, i.e. (i) holds. □

As a corollary of Theorem 1.1 and of the rank-nullity theorem for linear transformation, we get the following.

Corollary 1.2. *Let U and V be finite-dimensional vector spaces over a field $\mathbb{F}$, and assume that $dim(U) = dim(V)$. Let $f : U \to V$ be a linear transformation. Then f is one-to-one if and only if f is onto V.*

Proof. By the rank-nullity theorem for linear transformations, we have that $\text{rank}(f) + \dim(\text{Ker}(f)) = \dim(U)$. We now have the following sequence of equivalences.

f is one-to-one	$\Longleftrightarrow$	$\text{Ker}(f) = \{\mathbf{0}\}$	by Theorem 1.1
	$\Longleftrightarrow$	$\dim(\text{Ker}(f)) = 0$	
	$\Longleftrightarrow$	$\text{rank}(f) = \dim(U)$	by the rank-nullity theorem
	$\Longleftrightarrow$	$\dim(\text{Im}(f)) = \dim(U)$	by the definition of $\text{rank}(f)$
	$\Longleftrightarrow$	$\dim(\text{Im}(f)) = \dim(V)$	because $\dim(U) = \dim(V)$
	$\Longleftrightarrow$	$\text{Im}(f) = V$	by Theorem 1.12 from Lecture Notes 7
	$\Longleftrightarrow$	f is onto V	

We have now shown that f is one-to-one if and only if f is onto V. This completes the argument. □

2 Linear Transformations and Bases

We begin by recalling the following theorem from Lecture Notes 7.

Theorem 1.3 from Lecture Notes 7. *Let V be a vector space over a field $\mathbb{F}$, and let $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Then the following are equivalent:*

(i) $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ *is a basis of V;*

(ii) for all $\mathbf{v} \in V$, there exist unique scalars $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that $\mathbf{v} = \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n$.

For a positive integer n and a basis $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ of a vector space V over a field $\mathbb{F}$, the *coordinate vector* of a vector $\mathbf{v} \in V$ with respect to the basis $\mathcal{B}$ is the (unique) vector

$$[\mathbf{v}]_{\mathcal{B}} := \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

in $\mathbb{F}^n$ such that $\mathbf{v} = \alpha_1 \mathbf{b}_1 + \cdots + \alpha_n \mathbf{b}_n$. The fact that the vector $[\mathbf{v}]_{\mathcal{B}}$ is well-defined follows immediately from Theorem 1.3 from Lecture Notes 7 (see above).

Proposition 2.1. *Let U be a vector space over a field $\mathbb{F}$. Assume that U is non-trivial (i.e. contains at least one non-zero vector) and finite-dimensional. Let $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ be a basis of U. Then the function $f : U \to \mathbb{F}^n$ given by $f(\mathbf{u}) = [\mathbf{u}]_{\mathcal{B}}$ is an "isomorphism," i.e. a bijective linear transformation.*

Proof. Let us show that f is linear.

1. Fix $\mathbf{x}, \mathbf{y} \in U$. We must show that $f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$. Set $[\mathbf{x}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$ and $[\mathbf{y}]_{\mathcal{B}} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$. Then $\mathbf{x} = \alpha_1 \mathbf{u}_1 + \cdots + \alpha_n \mathbf{u}_n$ and $\mathbf{y} = \beta_1 \mathbf{u}_1 + \cdots + \beta_n \mathbf{u}_n$; consequently, $\mathbf{x}+\mathbf{y} = (\alpha_1+\beta_1)\mathbf{u}_1 + \cdots + (\alpha_n+\beta_n)\mathbf{u}_n$, and so $[\mathbf{x}+\mathbf{y}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1+\beta_1 \\ \vdots \\ \alpha_n+\beta_n \end{bmatrix}$. We now have that

$$\begin{aligned} f(\mathbf{x}+\mathbf{y}) &= [\mathbf{x}+\mathbf{y}]_{\mathcal{B}} \\ &= \begin{bmatrix} \alpha_1+\beta_1 \\ \vdots \\ \alpha_n+\beta_n \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \\ &= [\mathbf{x}]_{\mathcal{B}} + [\mathbf{y}]_{\mathcal{B}} \\ &= f(\mathbf{x}) + f(\mathbf{y}). \end{aligned}$$

2. Fix $\mathbf{u} \in U$ and $\alpha \in \mathbb{F}$. Set $[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$. Then $\mathbf{u} = \alpha_1 \mathbf{u}_1 + \cdots + \alpha_n \mathbf{u}_n$; consequently, $\alpha\mathbf{u} = \alpha\alpha_1 \mathbf{u}_1 + \cdots + \alpha\alpha_n \mathbf{u}_n$, and so $[\alpha\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_n \end{bmatrix}$. We now have that

$$f(\alpha\mathbf{u}) = [\alpha\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_n \end{bmatrix} = \alpha \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha[\mathbf{u}]_{\mathcal{B}} = \alpha f(\mathbf{u}).$$

By 1. and 2., f is linear.

It remains to show that f is a bijection, i.e. that it is one-to-one and onto V. Since U and $\mathbb{F}^n$ are both n dimensional, Corollary 1.2 guarantees that f is one-to-one if and only if f is onto $\mathbb{F}^n$. So, it is enough to show that f is onto $\mathbb{F}^n$. Fix $\begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T \in \mathbb{F}$. Set $\mathbf{u} := \alpha_1\mathbf{u}_1 + \dots + \alpha_n\mathbf{u}_n$. Then $f(\mathbf{u}) = [\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$. So, f is onto $\mathbb{F}^n$. This completes the argument. □

Theorem 2.2. *Let U and V be vector spaces over a field $\mathbb{F}$, and assume that U is non-trivial (i.e. contains at least one non-zero vector) and finite-dimensional. Let $\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ be a basis of U, and let $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$.*[1] *Then there exists a unique linear transformation $f : U \to V$ such that $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$. Moreover, this unique linear transformation $f : U \to V$ is defined as follows: for all $\mathbf{u} \in U$, we set*

$$f(\mathbf{u}) \quad = \quad \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n,$$

where $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ are such that $[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$.

Proof. **Existence.** Let $f : U \to V$ be defined as in the statement of the theorem, i.e. for all $\mathbf{u} \in U$, we set

$$f(\mathbf{v}) \quad = \quad \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n,$$

where $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ are such that $[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$. Note that this means that for all $\alpha_1, \dots, \alpha_n \in \mathbb{F}$, we have that

$$f(\alpha_1\mathbf{u}_1 + \dots + \alpha_n\mathbf{u}_n) \quad = \quad \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n.$$

Let us show that f is linear and satisfies $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$. For the latter, we note that for all $i \in \{1, \dots, n\}$, we have that

$$\begin{aligned} f(\mathbf{u}_i) &= f(0\mathbf{u}_1 + \dots + 0\mathbf{u}_{i-1} + 1\mathbf{u}_i + 0\mathbf{u}_{i+1} + \dots + 0\mathbf{u}_n) \\ &= 0\mathbf{v}_1 + \dots + 0\mathbf{v}_{i-1} + 1\mathbf{v}_i + 0\mathbf{v}_{i+1} + \dots + 0\mathbf{v}_n \\ &= \mathbf{v}_i. \end{aligned}$$

This proves that $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$.

Let us now show that f is linear. We verify that f satisfies the two conditions from the definition of a linear function.

1. Fix $\mathbf{x}, \mathbf{y} \in U$. We must show that $f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$. Set $[\mathbf{x}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$ and $\mathbf{y} = \begin{bmatrix} \beta_1 & \dots & \beta_n \end{bmatrix}^T$. Then $[\mathbf{x} + \mathbf{y}]_{\mathcal{B}} =$

[1] Here, $\mathbf{v}_1, \dots, \mathbf{v}_n$ are arbitrary vectors in V. They are not necessarily pairwise distinct.

$\begin{bmatrix} \alpha_1+\beta_1 & \dots & \alpha_n+\beta_n \end{bmatrix}^T$,[2] and we see that

$$\begin{aligned} f(\mathbf{x}+\mathbf{y}) & \overset{(*)}{=} & (\alpha_1+\beta_1)\mathbf{v}_1+\dots+(\alpha_n+\beta_n)\mathbf{v}_n \\ & = & (\alpha_1\mathbf{v}_1+\dots+\alpha_n\mathbf{v}_n)+(\beta_1\mathbf{v}_1+\dots+\beta_n\mathbf{v}_n) \\ & \overset{(**)}{=} & f(\mathbf{x})+f(\mathbf{y}), \end{aligned}$$

where both (*) and (**) follow from the construction of f.

2. Fix $\mathbf{u} \in U$ and $\alpha \in \mathbb{F}$. We must show that $f(\alpha\mathbf{u}) = \alpha f(\mathbf{u})$. Set $[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$. Then $[\alpha\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha\alpha_1 & \dots & \alpha\alpha_n \end{bmatrix}^T$,[3] and we see that

$$\begin{aligned} f(\alpha\mathbf{u}) & \overset{(*)}{=} & (\alpha\alpha_1)\mathbf{v}_1+\dots+(\alpha\alpha_n)\mathbf{v}_n \\ & = & \alpha(\alpha_1\mathbf{v}_1+\dots+\alpha_n\mathbf{v}_n) \\ & \overset{(**)}{=} & \alpha f(\mathbf{u}), \end{aligned}$$

where both (*) and (**) follow from the construction of f.

By 1. and 2., we see that f is linear. This completes the proof of existence.

Uniqueness. Let $f_1, f_2 : U \to V$ be linear transformations such that $f_1(\mathbf{u}_1) = \mathbf{v}_1, \dots, f_1(\mathbf{u}_n) = \mathbf{v}_n$ and $f_2(\mathbf{u}_1) = \mathbf{v}_1, \dots, f_2(\mathbf{u}_n) = \mathbf{v}_n$. We must show that $f_1 = f_2$. Fix $\mathbf{u} \in U$. We must show that $f_1(\mathbf{u}) = f_2(\mathbf{u})$. Set

---

[2] Indeed, since $[\mathbf{x}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$ and $\mathbf{y} = \begin{bmatrix} \beta_1 & \dots & \beta_n \end{bmatrix}^T$, we have that

$$\begin{aligned} \mathbf{x}+\mathbf{y} & = & (\alpha_1\mathbf{u}_1+\dots+\alpha_n\mathbf{u}_n)+(\beta_1\mathbf{u}_1+\dots+\beta_n\mathbf{u}_n) \\ & = & (\alpha_1+\beta_1)\mathbf{u}_1+\dots+(\alpha_n+\beta_n)\mathbf{u}_n, \end{aligned}$$

and so $[\mathbf{x}+\mathbf{y}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1+\beta_1 & \dots & \alpha_n+\beta_n \end{bmatrix}^T$.

[3] Indeed, since $[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$, we have that $\mathbf{u} = \alpha_1\mathbf{u}_1+\dots+\alpha_n\mathbf{u}_n$. Consequently, $\alpha\mathbf{u} = (\alpha\alpha_1)\mathbf{u}_1+\dots+(\alpha\alpha_n)\mathbf{u}_n$, and so $[\alpha\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha\alpha_1 & \dots & \alpha\alpha_n \end{bmatrix}^T$.

$[\mathbf{u}]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix}^T$. Then

$$\begin{aligned}
f_1(\mathbf{u}) &= f_1(\alpha_1\mathbf{u}_1 + \cdots + \alpha_n\mathbf{u}_n) \\
&= \alpha_1 f_1(\mathbf{u}_1) + \cdots + \alpha_n f_1(\mathbf{u}_n) && \text{because } f_1 \text{ is linear} \\
&= \alpha_1\mathbf{v}_1 + \cdots + \alpha_n\mathbf{v}_n && \text{because } f_1(\mathbf{u}_1) = \mathbf{v}_1, \dots, f_1(\mathbf{u}_n) = \mathbf{v}_n \\
&= \alpha_1 f_2(\mathbf{u}_1) + \cdots + \alpha_n f_2(\mathbf{u}_n) && \text{because } f_2(\mathbf{u}_1) = \mathbf{v}_1, \dots, f_2(\mathbf{u}_n) = \mathbf{v}_n \\
&= f_2(\alpha_1\mathbf{u}_1 + \cdots + \alpha_n\mathbf{u}_n) && \text{because } f_2 \text{ is linear} \\
&= f_2(\mathbf{u}).
\end{aligned}$$

Thus, $f_1 = f_2$. This proves uniqueness. □

3 Isomorphisms

Given vector spaces U and V over a field $\mathbb{F}$, an *isomorphism* between U and V is a linear transformation $f : U \to V$ that is also a bijection between U and V.

Proposition 2.1 gives one example of an isomorphism. Here are a couple of others.

Example 3.1. *Let $\mathbb{F}$ be a field, and let $f : \mathbb{F}^{2\times 3} \to \mathbb{F}^6$ be given by*

$$f\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}\right) = \begin{bmatrix} a_{11} \\ a_{12} \\ a_{13} \\ a_{21} \\ a_{22} \\ a_{23} \end{bmatrix}$$

for all $a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23} \in \mathbb{F}$. Then f is an isomorphism.

Example 3.2. *Let $\mathbb{F}$ be a field, and let n be a non-negative integer. Then the function $f : \mathbb{P}^n_{\mathbb{F}} \to \mathbb{F}^{n+1}$ given by $f(a_n x^n + \cdots + a_1 x + a_0) = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix}$, for all $a_n, \dots, a_1, a_0 \in \mathbb{F}$, is an isomorphism.*

Since every isomorphism is a bijection, we see, in particular, that every isomoprhism has an inverse. It turns out that the inverse of an isomorphism is also an isomorphism. This was proven in Lecture Notes 4 in the context of isomorphisms between $\mathbb{F}^n$ and $\mathbb{F}^n$ (see Proposition 1.8 from Lecture Notes 4). We now prove it for general vector spaces (the proof is virtually identical).

Proposition 3.3. *Let U and V be vector spaces over a field $\mathbb{F}$, and let $f : U \to V$ be an isomorphism. Then $f^{-1} : V \to U$ is also an isomorphism.*

Proof. Since $f : U \to V$ is a bijection, we see that $f^{-1} : V \to U$ is defined and is a bijection. It remains to show that f^{-1} is linear.

1. Fix $\mathbf{v}_1, \mathbf{v}_2 \in V$. We must show that $f^{-1}(\mathbf{v}_1 + \mathbf{v}_2) = f^{-1}(\mathbf{v}_1) + f^{-1}(\mathbf{v}_2)$. Fix $\mathbf{u}_1, \mathbf{u}_2 \in U$ such that $\mathbf{v}_1 = f(\mathbf{u}_1)$ and $\mathbf{v}_2 = f(\mathbf{u}_2)$.[4] Then

$$\begin{aligned} f^{-1}(\mathbf{v}_1 + \mathbf{v}_2) &= f^{-1}(f(\mathbf{u}_1) + f(\mathbf{u}_2)) \\ &\overset{(*)}{=} f^{-1}(f(\mathbf{u}_1 + \mathbf{u}_2)) \\ &= \mathbf{u}_1 + \mathbf{u}_2 \\ &= f^{-1}(\mathbf{v}_1) + f^{-1}(\mathbf{v}_2), \end{aligned}$$

where (*) follows from the fact that f is linear.

2. Fix $\mathbf{v} \in \mathbb{F}^n$ and $\alpha \in \mathbb{F}$. We must show that $f^{-1}(\alpha\mathbf{v}) = \alpha f(\mathbf{v})$. Fix $\mathbf{u} \in \mathbb{F}^n$ such that $\mathbf{v} = f(\mathbf{u})$.[5] Then

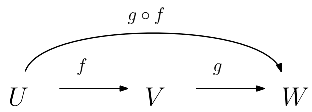
$$\begin{aligned} f^{-1}(\alpha\mathbf{v}) &= f^{-1}(\alpha f(\mathbf{u})) \\ &\overset{(*)}{=} f^{-1}(f(\alpha\mathbf{u})) \\ &= \alpha\mathbf{u} \\ &= \alpha f^{-1}(\mathbf{v}), \end{aligned}$$

where (*) follows from the fact that f is linear.

1. and 2. imply that f^{-1} linear, and we are done. □

Proposition 3.4. *Let U, V, and W be vector spaces over a field $\mathbb{F}$, and let $f : U \to V$ and $g : V \to W$ be isomorphisms. Then $g \circ f : U \to W$ is an isomoprhism.*

[4] Vectors $\mathbf{u}_1$ and $\mathbf{u}_2$ exist because f is onto V.
[5] Vector $\mathbf{u}$ exists because f is onto V.



Proof. Since f and g are bijections, so is $g \circ f$.[6] Since f and g are linear, Proposition 1.3(c) from Lecture Notes 8 guarantees that $g \circ f$ is linear. So, $g \circ f$ is an isomorphism. □

Given vector spaces U and V over a vector space $\mathbb{F}$, we say that U and V are *isomorphic*, denoted by $U \cong V$, if there exists an isomoprhism $f : U \to V$.

Theorem 3.5. *Let $\mathbb{F}$ be a field. Then all the following hold:*

(a) for all vector spaces U over $\mathbb{F}$, we have that $U \cong U$;

(b) for all vector spaces U and V over $\mathbb{F}$, if $U \cong V$, then $V \cong U$;

(c) for all vector spaces U, V, and W over $\mathbb{F}$, if $U \cong V$ and $V \cong W$, then $U \cong W$.

Proof. (a) Fix a vector space U over $\mathbb{F}$. Then the identity function $\mathrm{Id}_U : U \to U$ is an isomorphism,[7] and so $U \cong U$.

(b) Fix vector spaces U and V over $\mathbb{F}$, and assume that $U \cong V$. Then there exists an isomorphism $f : U \to V$. But by Proposition 3.3, $f^{-1} : V \to U$ is also an isomorphism, and it follows that $V \cong U$.

(c) Fix vector spaces U, V, and W over $\mathbb{F}$, and assume that $U \cong V$ and $V \cong W$. Then there exist isomorphisms $f : U \to V$ and $g : V \to W$. By Proposition 3.4, we have that $g \circ f : U \to W$ is an isomorphism, and so $U \cong W$. □

The idea behind the concept of isomorphism is that isomorphic vector spaces are isomorphic if they are "the same" up to a relabeling of elements. An isomorphism f gives a recipe for the relabeling: a vector $\mathbf{u}$ gets relabeled as $f(\mathbf{u})$.

3.1 Isomorphism and dimension

Our next goal is to show that two finite-dimensional vector spaces over the same field are isomorphic if and only if they have the same dimension.[8] We begin with a couple of technical propositions.

Proposition 3.6. *Let U and V be vector spaces over a field $\mathbb{F}$, and let $f : U \to V$ be a linear transformation. Let $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$ be such that $\{f(\mathbf{u}_1), \dots, f(\mathbf{u}_k)\}$ is a linearly independent set in V. Then $\mathbf{u}_1, \dots, \mathbf{u}_k$ is a linearly independent set in U.*

[6] You know this from Discrete Math.

[7] The identity function $\mathrm{Id}_U : U \to U$ is given by $\mathrm{Id}_U(\mathbf{u}) = \mathbf{u}$ for all $\mathbf{u} \in U$. It is obvious that Id_U is an isomorphism.

[8] However, not all infinite-dimensional vector spaces over the same field are isomorphic.

Proof. Fix $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ such that $\alpha_1 \mathbf{u}_1 + \cdots + \alpha_1 \mathbf{u}_k = \mathbf{0}$. Then

$$\begin{aligned} \alpha_1 f(\mathbf{u}_1) + \cdots + \alpha_k f(\mathbf{u}_k) &\overset{(*)}{=} f(\alpha_1 \mathbf{u}_1 + \cdots + \alpha_1 \mathbf{u}_k) \\ &\overset{(**)}{=} f(\mathbf{0}) \\ &\overset{(***)}{=} \mathbf{0}, \end{aligned}$$

where (*) follows from the fact that f is linear, (**) follows from the fact that $\alpha_1 \mathbf{u}_1 + \cdots + \alpha_1 \mathbf{u}_k = \mathbf{0}$, and (***) follows from Proposition 1.4 from Lecture Notes 8. Since the set $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is linearly independent, it follows that $\alpha_1 = \cdots = \alpha_k = 0$. □

The following was proven in Lecture Notes 8.

Proposition 2.1 from Lecture Notes 8. *Let U and V be vector spaces over a field $\mathbb{F}$, and let $f : U \to V$ be a linear transformation. Let $\mathbf{u}_1, \ldots, \mathbf{u}_k \in U$, and set $W := Span(\mathbf{u}_1, \ldots, \mathbf{u}_k)$. Then $f[W] = Span\Big(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\Big)$. Moreover, $dim(f[W]) \leq dim(W) \leq k$.*

Proposition 3.7. *Let U and V be vector spaces over a field $\mathbb{F}$, let $f : U \to V$ be an isomorphism, and let $\mathbf{u}_1, \ldots, \mathbf{u}_k \in U$. Then all the following hold:*

(a) $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ is a linearly independent set in U if and only if $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is a linearly independent set in V;

(b) $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ spans U if and only if $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is spans V;

(c) $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ is a basis for U if and only if $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is a basis for V.

Proof. Clearly, (a) and (b) imply (c). So, it suffices to prove (a) and (b).

We first prove (a). If $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is a linearly independent set in V, then Proposition 3.6 guarantees that $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ is a linearly independent set in U. Suppose, conversely, that $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ is a linearly independent set in U. Since f is an isomoprhism, it is a bijection, and in particular, it has an inverse f^{-1}. So, $\mathbf{u}_i = f^{-1}(f(\mathbf{u}_i))$ for all $i \in \{1, \ldots, k\}$. Thus, $\{f^{-1}(f(\mathbf{u}_1)), \ldots, f^{-1}(f(\mathbf{u}_k))\}$ is linearly independent. By Proposition 3.3, f^{-1} an isomorphism, and in particular, it is a linear transformation. So, by Proposition 3.6 applied to f^{-1} and $\{f^{-1}(f(\mathbf{u}_1)), \ldots, f^{-1}(f(\mathbf{u}_k))\}$, we see that $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ is linearly independent in V.

We now prove (b). Suppose first that $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ spans U. By Proposition 2.1 from Lecture Notes 8, we see that $\{f(\mathbf{u}_1), \ldots, f(\mathbf{u}_k)\}$ spans $f[U]$. But since $f : U \to V$ is an isomoprhism (and in particular, onto V), we see that $f[U] = V$. So, $\{f(\mathbf{u}_1), \dots, f(\mathbf{u}_k)\}$ spans $f[U]$. Suppose, conversely, that $\{f(\mathbf{u}_1), \dots, f(\mathbf{u}_k)\}$ spans V. Since f is an isomorphism, Proposition 3.3 guarantees that f^{-1} is an isomorphism; in particular, f^{-1} is a linear transformation. So, by Proposition 2.1 from Lecture Notes 8, $\{f^{-1}(f(\mathbf{u}_1)), \dots, f^{-1}(f(\mathbf{u}_k))\}$ spans $f^{-1}[V]$. But $f^{-1}(f(\mathbf{u}_i)) = \mathbf{u}_i$ for all $i \in \{1, \dots, k\}$, and $f^{-1}[V] = U$. So, $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ spans U. □

Proposition 3.8. *Let U and V be isomorphic vector spaces over a field $\mathbb{F}$. Then U is finite-dimensional if and only if V is finite-dimensional. Moreover, if U and V are finite-dimensional, then they have the same dimension.*

Proof. Since U and V are isomorphic, there exists an isomorphism $f : U \to V$. By Proposition 3.3, $f^{-1} : V \to U$ is also an isomorphism.

Now, suppose that U is finite-dimensional. Then U has a finite basis, say $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$. Then by Proposition 3.7(c), $\{f(\mathbf{u}_1), \dots, f(\mathbf{u}_n)\}$ is a basis for V. So, V is finite-dimensional, and moreover, $\dim(V) = n = \dim(U)$.

An argument completely analogous to the above (only using f^{-1} instead of f) guarantees that if V is finite-dimensional, then so is U, and moreover, $\dim(U) = \dim(V)$. □

Theorem 3.9. *Let U and V be finite-dimensional vector spaces over a field $\mathbb{F}$. Then U and V are isomorphic is and only if $\dim(U) = \dim(V)$.*

Proof. If U and V are isomorphic, then Proposition 3.8 guarantees that $\dim(U) = \dim(V)$. Let now us suppose that $\dim(U) = \dim(V) =: n$; we must show that U and V are isomorphic.

If $n = 0$, then U and V are trivial vector spaces, i.e. $U = \{\mathbf{0}_U\}$ and $V = \{\mathbf{0}_V\}$, and they are obviously isomorphic (indeed, the function $f : U \to V$ given by $f(\mathbf{0}_U) = \mathbf{0}_V$ is an isomorphism).

From now on, we may assume that $n \geq 1$. Let $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ be a basis for U, and let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for V. By Theorem 2.2, there exists a (unique) linear transformation $f : U \to V$ such that $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$. We claim that f is an isomorphism. We already know that f is linear, and so we need only show that f is a bijection, i.e. that f is one-to-one and onto V. But since $\dim(U) = \dim(V)$, Corollary 1.2 guarantees that f is one-to-one if and only if it is onto V. Thus, it suffices to show that f is onto V.

Fix $\mathbf{v} \in V$. Since $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for V, we know that there exist scalars $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that $\mathbf{v} = \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n$. But now

$$\begin{aligned} f(\alpha_1\mathbf{u}_1 + \dots + \alpha_n\mathbf{u}_n) &= \alpha_1 f(\mathbf{u}_1) + \dots + \alpha_n f(\mathbf{u}_n) && \text{because } f \text{ is linear} \\ &= \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n \\ &= \mathbf{v}. \end{aligned}$$

So, f is onto V, and we are done. □

Note that Theorem 3.9 implies that, for all positive integers n and fields $\mathbb{F}$, every n-dimensional vector space over $\mathbb{F}$ is isomorphic to $\mathbb{F}^n$. If we know a basis of V, we can construct an actual isomorphism from V to $\mathbb{F}$ as in Proposition 2.1.

We complete this section with the following proposition, whose proof was actually given as part of the proof of Theorem 3.9. However, for the sake of completeness, we give a full proof of the proposition below.

Proposition 3.10. *Let U and V be finite-dimensional vector spaces over a field $\mathbb{F}$. Assume that $dim(U) = dim(V) =: n$. Let $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ be a basis for U, and let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for V. Then there exists a unique linear transformation $f : U \to V$ such that $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$. Moreover, this linear transformation f is an isomorphism.*

Proof. Suppose first that $n = 0$. Then $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ and $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ are both empty, and $U = \{\mathbf{0}_U\}$ and $V = \{\mathbf{0}\}$. Then there is exactly one function $f : U \to V$, and it satisfied $f(\mathbf{0}_U) = f(\mathbf{0}_V)$. Clearly, this function f is an isomorphism.[9]

From now on, we assume that $n \geq 1$. The existence and uniqueness of the linear transformation f follows from Theorem 2.2. It remains to show that f is a bijection, i.e. that f is one-to-one and onto V. But since $\dim(U) = \dim(V)$, Corollary 1.2 guarantees that f is one-to-one if and only if it is onto V. Thus, it suffices to show that f is onto V.

Fix $\mathbf{v} \in V$. Since $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for V, we know that there exist scalars $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that $\mathbf{v} = \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n$. But now

$$\begin{aligned} f(\alpha_1\mathbf{u}_1 + \dots + \alpha_n\mathbf{u}_n) &= \alpha_1 f(\mathbf{u}_1) + \dots + \alpha_n f(\mathbf{u}_n) && \text{because } f \text{ is linear} \\ &= \alpha_1\mathbf{v}_1 + \dots + \alpha_n\mathbf{v}_n \\ &= \mathbf{v}. \end{aligned}$$

So, f is onto V, and we are done. □

4 An application of isomorphism: transforming polynomials into vectors

By Theorem 3.9, for all positive integers n and fields $\mathbb{F}$, every n-dimensional vector space over $\mathbb{F}$ is isomorphic to $\mathbb{F}^n$. This is useful because we developed powerful computational tools for vectors in $\mathbb{F}^n$. By using isomorphisms, we can reduce problems of computing in an arbitrary n-dimensional vector space to problems of computing in $\mathbb{F}^n$, which we know how to do in many cases. We give a couple of examples involving polynomials.

[9] Since $n = 0$, the requirement that $f(\mathbf{u}_1) = \mathbf{v}_1, \dots, f(\mathbf{u}_n) = \mathbf{v}_n$ is (vacuously) satisfied.

Example 4.1. *Consider the following polynomials in* $\mathbb{P}_{\mathbb{Z}_2}$*:*

- $p_1(x) = x^3 + x + 1$;
- $p_2(x) = x^3 + x^2 + 1$;
- $p_3(x) = x^2 + 1$;
- $p_4(x) = x + 1$;
- $p_5(x) = x^2$;
- $p_6(x) = x^3 + 1$.

Let $U = Span(p_1(x), \dots, p_6(x))$*. Find a basis* $\mathcal{B}$ *for* U*. What is* $dim(U)$*? For each* $i \in \{1, \dots, 6\}$ *such that* $p_i(x)$ *is* ***not*** *in the basis* $\mathcal{B}$*, express* $p_i(x)$ *as a linear combination of the basis vectors of* $\mathcal{B}$*.*

Solution. Note that polynomials $p_1(x), \dots, p_6(x)$ are all of degree at most 3, and they all belong to $\mathbb{P}^3_{\mathbb{Z}_2}$. Thus, $U = \text{Span}\big(p_1(x), \dots, p_6(x)\big)$ is a subspace of $\mathbb{P}^3_{\mathbb{Z}_2}$. We know that $\mathcal{A} = \{x^3, x^2, x, 1\}$ is a basis for $\mathbb{P}^3_{\mathbb{Z}_2}$, and we consider the isomorphism $f : \mathbb{P}^3_{\mathbb{Z}_2} \to \mathbb{Z}_2^4$ given by $f(\mathbf{x}) = [\mathbf{x}]_{\mathcal{A}}$ for all $\mathbf{x} \in \mathbb{P}^3_{\mathbb{Z}_2}$. Then

- $f(p_1(x)) = [p_1(x)] = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$;
- $f(p_2(x)) = [p_2(x)] = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$;
- $f(p_3(x)) = [p_3(x)] = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$;
- $f(p_4(x)) = [p_4(x)] = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$;
- $f(p_5(x)) = [p_5(x)] = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$;
- $f(p_6(x)) = [p_6(x)] = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$.

We form the matrix

$$\begin{aligned} A &= \begin{bmatrix} f(p_1(x)) & \dots & f(p_6(x)) \end{bmatrix} \\ &= \begin{bmatrix} [p_1(x)]_{\mathcal{A}} & \dots & [p_6(x)]_{\mathcal{A}} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}, \end{aligned}$$

and by row reducing, we obtain the following (pivot columns are in red, and non-pivot columns are in blue):

$$\text{RREF}(A) \quad = \quad \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

A basis for $\text{Col}(A) = \text{Span}(f(p_1(x)), \ldots, f(p_6(x))) = f[U]$ [10] is formed by the pivot columns of A, and we see from $\text{RREF}(A)$ that those are precisely the first, second, third, and fifth column of A. So, the following is a basis of $\text{Col}(A) = \text{Span}(f(p_1(x)), \ldots, f(p_6(x)) = f[U]$:

$$\mathcal{C} \quad = \quad \Big\{ f(p_1(x)), f(p_2(x)), f(p_3(x)), f(p_5(x)) \Big\}.$$

So, by Proposition 3.7, the following is a basis for $U = \text{Span}(p_1(x), \ldots, p_6(x))$:

$$\mathcal{B} \quad = \quad \{p_1(x), p_2(x), p_3(x), p_5(x)\}.$$

This implies that $\dim(U) = 4$.

(Note: Since U is a 4-dimensional subspace of the 4-dimensional vector space $\mathbb{P}^3_{\mathbb{Z}_2}$, Theorem 1.12 from Lecture Notes 7 implies that $U = \mathbb{P}^3_{\mathbb{Z}_2}$.)

It remains to express $p_4(x)$ and $p_6(x)$ as linear combinations of the polynomials in $\mathcal{B}$. First, we express $f(p_4(x))$ and $f(p_6(x))$ as a linear combination of the basis vectors in $\mathcal{C}$. From $\text{RREF}(A)$, we see that

- $f(p_4(x)) = f(p_1(x)) + f(p_2(x)) + f(p_3(x))$;
- $f(p_6(x)) = f(p_2(x)) + f(p_5(x))$.

Using the linearity of f, we get that

- $f(p_4(x)) = f(p_1(x)) + f(p_2(x)) + f(p_3(x)) = f\Big(p_1(x) + p_2(x) + p_3(x)\Big)$;
- $f(p_6(x)) = f(p_2(x)) + f(p_5(x)) = f\Big(p_2(x) + p_5(x)\Big)$.

Since f is an isomorphism (and in particular, one-to-one), we get that

- $p_4(x) = p_1(x) + p_2(x) + p_3(x)$;
- $p_6(x) = p_2(x) + p_5(x)$.

□

[10] By definition, $\text{Col}(A) = \text{Span}(f(p_1(x)), \ldots, f(p_6(x)))$, since $f(p_1(x)), \ldots, f(p_6(x)$ are the columns of A. On the other hand, by Proposition 2.1 from Lecture Notes 8, since $U = \text{Span}(p_1(x), \ldots, p_6(x))$, we know that $f[U] = \text{Span}(f(p_1(x)), \ldots, f(p_6(x)))$. So, $\text{Col}(A) = \text{Span}(f(p_1(x)), \ldots, f(p_6(x)) = f[U]$.

Example 4.2. *Consider the following polynomials in $\mathbb{P}_{\mathbb{Z}_3}$:*

- $p_1(x) = x^4 + 2$;
- $p_2(x) = x^3 + x^2$;
- $p_3(x) = x^4 + x^3 + x^2 + 2$;
- $p_4(x) = 2x^4 + x^3 + x^2 + 1$;
- $p_5(x) = 2x + 1$.

*Let $U = \text{Span}(p_1(x), \dots, p_5(x))$. Find a basis $\mathcal{B}$ for U. What is $\dim(U)$? For each $i \in \{1, \dots, 5\}$ such that $p_i(x)$ is **not** in the basis $\mathcal{B}$, express $p_i(x)$ as a linear combination of the basis vectors of $\mathcal{B}$.*

Solution. Note that polynomials $p_1(x), \dots, p_5(x)$ are all of degree at most 4, and they all belong to $\mathbb{P}^4_{\mathbb{Z}_3}$. Thus, $U = \text{Span}\Big(p_1(x), \dots, p_5(x)\Big)$ is a subspace of $\mathbb{P}^4_{\mathbb{Z}_3}$. We know that $\mathcal{A} = \{x^4, x^3, x^2, x, 1\}$ is a basis for $\mathbb{P}^4_{\mathbb{Z}_3}$, and we consider the isomorphism $f : \mathbb{P}^4_{\mathbb{Z}_3} \to \mathbb{Z}_3^5$ given by $f(\mathbf{x}) = [\mathbf{x}]_{\mathcal{A}}$ for all $\mathbf{x} \in \mathbb{P}^4_{\mathbb{Z}_3}$. Then

- $f(p_1(x)) = [p_1(x)]_{\mathcal{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \end{bmatrix}^T$;
- $f(p_2(x)) = [p_2(x)]_{\mathcal{A}} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \end{bmatrix}^T$;
- $f(p_3(x)) = [p_3(x)]_{\mathcal{A}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 2 \end{bmatrix}^T$;
- $f(p_4(x)) = [p_4(x)]_{\mathcal{A}} = \begin{bmatrix} 2 & 1 & 1 & 0 & 1 \end{bmatrix}^T$;
- $f(p_5(x)) = [p_5(x)]_{\mathcal{A}} = \begin{bmatrix} 0 & 0 & 0 & 2 & 1 \end{bmatrix}^T$.

We form the matrix

$$\begin{aligned} A &= \begin{bmatrix} f(p_1(x)) & f(p_2(x)) & f(p_3(x)) & f(p_4(x)) & f(p_5(x)) \end{bmatrix} \\ &= \begin{bmatrix} [p_1(x)]_{\mathcal{A}} & [p_2(x)]_{\mathcal{A}} & [p_3(x)]_{\mathcal{A}} & [p_4(x)]_{\mathcal{A}} & [p_5(x)]_{\mathcal{A}} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 2 & 1 & 1 \end{bmatrix}, \end{aligned}$$

and by row reducing, we obtain the following (pivot columns are in red, and non-pivot columns are in blue):

$$\text{RREF}(A) = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

A basis for $\mathrm{Col}(A) = \mathrm{Span}(f(p_1(x)), \ldots, f(p_5(x)) = f[U]$ [11] is formed by the pivot columns of A, and we see from $\mathrm{RREF}(A)$ that those are precisely the first, second, and fifth column of A. So, the following is a basis of $\mathrm{Col}(A) = \mathrm{Span}(f(p_1(x)), \ldots, f(p_5(x)) = f[U]$:

$$\mathcal{C} \;=\; \{f(p_1(x)), f(p_2(x)), f(p_5(x))\}.$$

So, by Proposition 3.7, the following is a basis for $U = \mathrm{Span}(p_1(x), \ldots, p_5(x))$:

$$\mathcal{B} \;=\; \{p_1(x), p_2(x), p_5(x)\}.$$

This implies that $\dim(U) = 3$.

It remains to express $p_3(x)$ and $p_4(x)$ as linear combinations of the polynomials in $\mathcal{B}$. First, we express $f(p_3(x))$ and $f(p_4(x))$ as linear combinations of the basis vectors in $\mathcal{C}$. From $\mathrm{RREF}(A)$, we see that

- $f(p_3(x)) = f(p_1(x)) + f(p_2(x))$;
- $f(p_4(x)) = 2f(p_1(x)) + f(p_2(x))$.

Using the linearity of f, we get that

- $f(p_3(x)) = f(p_1(x)) + f(p_2(x)) = f\Big(p_1(x) + p_2(x)\Big)$;
- $f(p_4(x)) = 2f(p_1(x)) + f(p_2(x)) = f\Big(2p_1(x) + p_2(x)\Big)$.

Since f is an isomorphism (and in particular, one-to-one), we get that

- $p_3(x) = p_1(x) + p_2(x)$;
- $p_4(x) = 2p_1(x) + p_2(x)$.

□

[11] By definition, $\mathrm{Col}(A) = \mathrm{Span}(f(p_1(x)), \ldots, f(p_5(x))$, since $f(p_1(x)), \ldots, f(p_5(x))$ are the columns of A. On the other hand, by Proposition 2.1 from Lecture Notes 8, since $U = \mathrm{Span}(p_1(x), \ldots, p_5(x))$, we know that $f[U] = \mathrm{Span}(f(p_1(x)), \ldots, f(p_5(x)))$. So, $\mathrm{Col}(A) = \mathrm{Span}(f(p_1(x)), \ldots, f(p_5(x)) = f[U]$.