Part IB — Linear Algebra

Based on lectures by Prof. P. Raphael and notes by thirdsgames.co.uk

Michaelmas 2022

Contents

§1 Vector spaces and linear dependence

§1.1 Vector spaces

Definition 1.1 (F-vector space)

Let F be an arbitrary field. A **F-vector space** is an abelian group $(V, +)$ equipped with a function

$$F \times V \to V; \quad (\lambda, v) \mapsto \lambda v$$

such that

1. $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$
2. $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$
3. $\lambda(\mu v) = (\lambda\mu)v$
4. $1v = v$

Such a vector space may also be called a *vector space over* F.

Example 1.1

Let $n \in \mathbb{N}$. F^n is the space of column vectors of length n with entries in F.

$$v \in F^n, v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, x_i \in F, 1 \leq i \leq n.$$

$$v + w = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{bmatrix}, \quad \lambda v = \begin{bmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{bmatrix}.$$

F^n is a F-vector space.

Example 1.2

Let X be a set, and define $\mathbb{R}^X = \{f : X \to \mathbb{R}\}$ (set of real valued functions on X). Then $\mathbb{R}^X$ is an $\mathbb{R}$-vector space:

- $(f_1 + f_2)(x) = f_1(x) + f_2(x)$.

- $(\lambda f)(x) = \lambda f(x), \lambda \in \mathbb{R}$.

Example 1.3

Define $M_{n,m}(F)$ to be the set of $n \times m$ F-valued matrices. This is an F-vector space, where the sum of matrices is computed elementwise.

Remark 1. The axioms of scalar multiplication imply that $\forall v \in V,\ 0_F \cdot v = 0_V$.

§1.2 Subspaces

Definition 1.2 (Subspace)

Let V be an F-vector space. The subset $U \subseteq V$ is a vector subspace of V, denoted $U \leq V$, if

1. $0_V \in U$
2. $u_1, u_2 \in U \implies u_1 + u_2 \in U$
3. $(\lambda, u) \in F \times U \implies \lambda u \in U$

Conditions (ii) and (iii) are equivalent to

$$\forall \lambda_1, \lambda_2 \in F, \forall u_1, u_2 \in U, \lambda_1 u_1 + \lambda_2 u_2 \in U$$

This means that U is *stable* by vector addition and scalar multiplication.

Proposition 1.1

If V is an F-vector space, and $U \leq V$, then U is an F-vector space.

Example 1.4

Let $V = \mathbb{R}^{\mathbb{R}}$ be the space of functions $\mathbb{R} \to \mathbb{R}$. The set $C(\mathbb{R})$ of continuous real functions is a subspace of V. The set $\mathbb{P}(\mathbb{R})$ of real polynomials is a subspace of $C(\mathbb{R})$ so $\mathbb{P}(\mathbb{R}) \leq V$.

Example 1.5

Consider the subset of $\mathbb{R}^3$ such that $x_1 + x_2 + x_3 = t$ for some real t. This is a subspace for $t = 0$ only, since no other t values yields the origin as a member of the subset.

Proposition 1.2 (Intersection of two subspaces is a subspace)
Let V be an F-vector space. Let $U, W \leq V$. Then $U \cap W$ is a subspace of V.

Proof. First, note $0_V \in U, 0_V \in W \implies 0_V \in U \cap W$. Now, consider stability:

$$\lambda_1, \lambda_2 \in F, v_1, v_2 \in U \cap W \implies \lambda_1 v_1 + \lambda_2 v_2 \in U, \lambda_1 v_1 + \lambda_2 v_2 \in W$$

Hence stability holds. □

§1.3 Sum of subspaces

Warning 1.1
The union of two subspaces is not, in general, a subspace. For instance, consider $\mathbb{R}, i\mathbb{R} \subset \mathbb{C}$. Their union does not span the space; for example, $1 + i \notin \mathbb{R} \cup i\mathbb{R}$.

Definition 1.3 (Subspace Sum)
Let V be an F-vector space. Let $U, W \leq V$. The sum $U + W$ is defined to be the set

$$U + W = \{u + w \colon u \in U, w \in W\}$$

Proposition 1.3
$U + W$ is a subspace of V.

Proof. First, note $0_{U+W} = 0_U + 0_W = 0_V$. Then, for $\lambda_1, \lambda_2 \in F$ and $f, g \in U + W$ we have

$$f = f_1 + f_2$$
$$g = g_1 + g_2$$

with $f_1, g_1 \in U$ and $f_2, g_2 \in W$. Hence

$$\begin{aligned} \lambda_1 f + \lambda_2 g &= \lambda_1(f_1 + f_2) + \lambda_2(g_1 + g_2) \\ &= \underbrace{(\lambda_1 f_1 + \lambda_2 g_1)}_{\in U} + \underbrace{(\lambda_1 f_2 + \lambda g_2)}_{\in W} \in U + W. \end{aligned}$$

□

Proposition 1.4

The sum $U + W$ is the smallest subspace of V that contains both U and W.

Proof. Left as an exercise. □

§1.4 Quotients

Definition 1.4 (Quotient)

Let V be an F-vector space. Let $U \leq V$. The **quotient space** V/U is the abelian group V/U equipped with the scalar multiplication function

$$F \times V/U \to V/U; \quad (\lambda, v + U) \mapsto \lambda v + U$$

Note. We must check that the multiplication operation is well-defined. Indeed, suppose $v_1 + U = v_2 + U$. Then,

$$v_1 - v_2 \in U \implies \lambda(v_1 - v_2) \in U \implies \lambda v_1 + U = \lambda v_2 + U \in V/U$$

Proposition 1.5

V/U is an F-vector space.

Proof. Left as an exercise □

§1.5 Span

Definition 1.5 (Span of a family of vectors)

Let V be an F-vector space. Let $S \subset V$ be a subset (so S is a set of vectors). We define the **span** of S, written $\langle S \rangle$, as the set of finite linear combinations of elements of S. In particular,

$$\langle S \rangle = \left\{ \sum_{s \in S} \lambda_s v_s \colon \lambda_s \in F, v_s \in S, \text{only finitely many nonzero } \lambda_s \right\}$$

By convention, we specify

$$\langle \varnothing \rangle = \{0\}$$

so that all spans are subspaces.

Remark 2. $\langle S \rangle$ is the smallest vector subspace of V containing S.

Example 1.6

Let $V = \mathbb{R}^3$, and

$$S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -2 \\ -4 \end{pmatrix} \right\}$$

Then we can check that

$$\langle S \rangle = \left\{ \begin{pmatrix} a \\ b \\ 2b \end{pmatrix} : (a, b) \in \mathbb{R} \right\}$$

Example 1.7

Let $V = \mathbb{R}^n$. We define

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where the 1 is in the ith position. Then $V = \langle (e_i)_{1 \le i \le n} \rangle$.

Example 1.8

Let X be a set, and $\mathbb{R}^X = \{f : X \to \mathbb{R}\}$. Then let $S_x : X \to \mathbb{R}$ be defined by

$$S_x(y) = \begin{cases} 1 & y = x \\ 0 & \text{otherwise} \end{cases}$$

Then, $\langle (S_x)_{x \in X} \rangle = \left\{ f \in \mathbb{R}^X : f \text{ has finite support} \right\}$, where the support of f is defined to be $\{x : f(x) \neq 0\}$.

§1.6 Dimensionality

Definition 1.6

Let V be an F-vector space. Let $S \subset V$. We say that S spans V if $\langle S \rangle = V$. If S spans V, we say that S is a generating family of V.

Definition 1.7 (Finite dimensional)

Let V be an F-vector space. V is **finite dimensional** if it is spanned by a finite set.

Definition 1.8 (Infinite dimensional)

Let V be an F-vector space. V is **infinite dimensional** if there is no family S with finitely many elements which span V.

Example 1.9

Consider the set $V = \mathbb{P}[x]$ which is the set of polynomials on $\mathbb{R}$. Further, consider $V_n = \mathbb{P}_n[x]$ which is the subspace with degree less than or equal to n. Then V_n is spanned by $\{1, x, x^2, \ldots, x^n\}$, so V_n is finite-dimensional.

Conversely, V is infinite-dimensional; there is no finite set S such that $\langle S \rangle = V$. The proof is left as an exercise.

§1.7 Linear independence

Definition 1.9 (Linear independence)

We say that $v_1, \ldots, v_n \in V$ are **linearly independent** or **free**, if, for $\lambda_i \in F$,

$$\sum_{i=1}^{n} \lambda_i v_i = 0 \implies \forall i, \lambda_i = 0.$$

Remark 3. Linear dependence implies $\exists\ \lambda_i \in F$ and $j \in [1, n]$ s.t. $\sum_{i=1}^{n} \lambda_i v_i = 0$ and $\lambda_j \neq 0$. This implies $v_j = -\frac{1}{\lambda_j} \sum_{i \neq j}^{n} \lambda_i v_i$, i.e. one of the vectors can be written as a linear combination of the remaining ones.

Remark 4. If $(v_i)_{1 \leq i \leq n}$ are linearly independent, then

$$\forall i \in \{1, \ldots, n\}, v_i \neq 0$$

§1.8 Bases

Definition 1.10 (Basis)

$S \subset V$ is a basis of V if

1. $\langle S \rangle = V$
2. S is a linearly independent set

So, a basis is a linearly independent/free generating family.

Example 1.10

Let $V = \mathbb{R}^n$. The *canonical basis* (e_i) is a basis since we can show that they are free and span V. Proof is left as an exercise.

Example 1.11

Let $V = \mathbb{C}$, considered as a $\mathbb{C}$-vector space. Then $\{1\}$ is a basis. If V is a $\mathbb{R}$-vector space, $\{1, i\}$ is a basis.

Example 1.12

Consider again $\mathbb{P}[x]$, polys on $\mathbb{R}$. Then $S = \{x^n : n \geq 0\}$ is a basis of $\mathbb{P}$.

Lemma 1.1 (Unique decomposition for everything equivalent to being a basis)

Let V be an F-vector space. Then, $(v_1, \ldots, v_n)$ is a basis of V if and only if any vector $v \in V$ has a *unique* decomposition

$$v = \sum_{i=1}^{n} \lambda_i v_i, \lambda_i \in F$$

Remark 5. In the above definition, we call $(\lambda_1, \ldots, \lambda_n)$ the *coordinates* of v in the basis $(v_1, \ldots, v_n)$.

Proof. Suppose $(v_1, \ldots, v_n)$ is a basis of V. Then $\forall v \in V$ there exists $\lambda_1, \ldots, \lambda_n \in F$ such that

$$v = \sum_{i=1}^{n} \lambda_i v_i$$

So there exists a tuple of λ values. Suppose two such λ tuples exist. Then

$$v = \sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \lambda_i' v_i \implies \sum_{i=1}^{n} (\lambda_i - \lambda_i') v_i = 0 \implies \lambda_i = \lambda_i'$$

since v_i linearly independent. The converse is left as an exercise. □

Lemma 1.2 (Some subset of a spanning set is a basis)

If $\langle \{v_1, \dots, v_n\} \rangle = V$, then some subset of this set is a basis of V.

Proof. If $(v_1, \dots, v_n)$ are linearly independent, this is a basis. Otherwise, one of the vectors can be written as a linear combination of the others. So, up to reordering,

$$\begin{aligned} v_n \in \langle \{v_1, \dots, v_{n-1}\} \rangle &\implies \langle \{v_1, \dots, v_n\} \rangle = \langle \{v_1, \dots, v_{n-1}\} \rangle \\ &\implies \langle \{v_1, \dots, v_{n-1}\} \rangle = V \end{aligned}$$

So we have removed a vector from this set and preserved the span. By induction, we will eventually reach a basis. □

§1.9 Steinitz exchange lemma

Theorem 1.1 (Steinitz exchange lemma)

Let V be a finite dimensional F-vector space. Let $(v_1, \dots, v_m)$ be linearly independent, and $(w_1, \dots, w_n)$ span V. Then,

1. $m \leq n$; and
2. up to reordering, $(v_1, \dots, v_m, w_{m+1}, \dots w_n)$ spans V.

Proof. Suppose that we have replaced $\ell \geq 0$ of the w_i.

$$\langle v_1, \dots, v_\ell, w_{\ell+1}, \dots w_n \rangle = V$$

If $m = \ell$, we are done. Otherwise, $\ell < m$. Then, $v_{\ell+1} \in V = \langle v_1, \dots, v_\ell, w_{\ell+1}, \dots w_n \rangle$ Hence $v_{\ell+1}$ can be expressed as a linear combination of the generating set. Since the $(v_i)_{1 \leq i \leq m}$ are linearly independent (free), one of the coefficients on the w_i are nonzero. In particular, up to reordering we can express $w_{\ell+1}$ as a linear combination of $v_1, \dots, v_{\ell+1}, w_{\ell+2}, \dots, w_n$. Inductively, we may replace m of the w terms with v terms. Since we have replaced m vectors, necessarily $m \leq n$. □

§1.10 Consequences of Steinitz exchange lemma

Corollary 1.1

Let V be a finite-dimensional F-vector space. Then, any two bases of V have the same number of vectors. This number is called the dimension of V, $\dim_F V$.

Proof. Suppose the two bases are $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$. Then, $(v_1, \ldots, v_n)$ is free and $(w_1, \ldots, w_m)$ is generating, so the Steinitz exchange lemma shows that $n \leq m$. Vice versa, $m \leq n$. Hence $m = n$. □

Corollary 1.2

Let V be an F-vector space with finite dimension n. Then,

1. Any independent set of vectors has at most n elements, with equality if and only if it is a basis.
2. Any spanning set of vectors has at least n elements, with equality if and only if it is a basis.

Proof. Exercise. □

§1.11 Dimensionality of sums

Proposition 1.6

Let V be an F-vector space. Let U, W be subspaces of V. If U, W are finite-dimensional, then so is $U + W$, with

$$\dim_F(U + W) = \dim_F U + \dim_F W - \dim_F(U \cap W)$$

Proof. Consider a basis $(v_1, \ldots, v_n)$ of the intersection. Extend this basis to a basis $(v_1, \ldots, v_n, u_1, \ldots, u_m)$ of U and $(v_1, \ldots, v_n, w_1, \ldots, w_k)$ of W. Then, we will show that $(v_1, \ldots, v_n, u_1, \ldots, u_m, w_1, \ldots, w_k)$ is a basis of $\dim_F(U + W)$, which will conclude the proof. Indeed, since any component of $U + W$ can be decomposed as a sum of some element of U and some element of W, we can add their decompositions together. Now we must show that this new basis is free.

$$\sum_{i=1}^{n} \alpha_i v_i + \sum_{i=1}^{m} \beta_i u_i + \sum_{i=1}^{k} \gamma_i w_i = 0$$

$$\underbrace{\sum_{i=1}^{n} \alpha_i v_i + \sum_{i=1}^{m} \beta_i u_i}_{\in U} = \underbrace{\sum_{i=1}^{k} \gamma_i w_i}_{\in W}$$

$$\sum_{i=1}^{k} \gamma_i w_i \in U \cap W$$
$$\sum_{i=1}^{k} \gamma_i w_i = \sum_{i=1}^{n} \delta_i v_i$$
$$\sum_{i=1}^{n} (\alpha_i + \delta_i) v_i + \sum_{i=1}^{m} \beta_i u_i = 0$$
$$\beta_i = 0, \alpha_i = -\delta_i$$
$$\sum_{i=1}^{n} \alpha_i v_i + \sum_{i=1}^{k} \gamma_i w_i = 0$$
$$\alpha_i = 0, \gamma_i = 0$$

□

Proposition 1.7

If V is a finite-dimensional F-vector space, and $U \leq V$, then U and V/U are also finite-dimensional. In particular, $\dim_F V = \dim_F U + \dim_F(V/U)$.

Proof. Let $(u_1, \ldots, u_\ell)$ be a basis of U. We extend this basis to a basis of V: $(u_1, \ldots, u_\ell, w_{\ell+1}, \ldots, w_n)$. We claim that $(w_{\ell+1} + U, \ldots, w_n + U)$ is a basis of the vector space V/U. □

Remark 6. If V is an F-vector space, and $U \leq V$, then we say U is a proper subspace if $U \neq V$. Then if U is proper, then $\dim_F U < \dim_F V$ and $\dim_F(V/U) > 0$ because $(V/U) \neq \varnothing$.

§1.12 Direct sums

Definition 1.11

Let V be an F-vector space and U, W be subspaces of V. We say that $V = U \oplus V$, read as the direct sum of U and V, if $\forall v \in V, \exists! u \in U, \exists! w \in W, u + w = v$. We say that W is *a* direct complement of U in V; there is no uniqueness of such a complement.

Lemma 1.3

Let V be an F-vector space, and $U, W \leq V$. Then the following statements are equivalent.

1. $V = U \oplus W$
2. $V = U + W$ and $U \cap W = \{0\}$
3. For any basis B_1 of U and B_2 of W, $B_1 \cup B_2$ is a basis of V

Proof. First, we show that (ii) implies (i). If $V = U + W$, then certainly $\forall v \in V, \exists u \in U, \exists w \in W, v = u + w$, so it suffices to show uniqueness. Note, $u_1 + w_1 = u_2 + w_2 \implies u_1 - u_2 = w_2 - w_1$. The left hand side is an element of U and the right hand side is an element of W, so they must be the zero vector; $u_1 = u_2, w_1 = w_2$.

Now, we show (i) implies (iii). Suppose B_1 is a basis of U and B_2 is a basis of W. Let $B = B_1 \cup B_2$. First, note that B is a generating family of $U + W$. Now we must show that B is free.

$$\underbrace{\sum_{u \in B_1} \lambda_u u}_{\in U} + \underbrace{\sum_{w \in B_2} \lambda_w w}_{\in W} = 0$$

Hence both sums must be zero. Since B_1, B_2 are bases, all λ are zero, so B is free and hence a basis.

Now it remains to show that (iii) implies (ii). We must show that $V = U + W$ and $U \cap W = \{0\}$. Now, suppose $v \in V$. Then, $v = \sum_{u \in B_1} \lambda_u u + \sum w \in B_2 \lambda_w w$. In particular, $V = U + W$, since the λ_u, λ_w are arbitrary. Now, let $v \in U \cap W$. Then

$$v = \sum_{u \in B_1} \lambda_u u = \sum_{w \in B_2} \lambda_w w \implies \lambda_u = \lambda_w = 0$$

□

Definition 1.12

Let V be an F-vector space, with subspaces $V_1, \ldots, V_p \leq V$. Then

$$\sum_{i=1}^{p} V_i = \{v_1, \ldots, v_\ell, v_i \in V_i, 1 \leq i \leq \ell\}$$

We say the sum is direct, written

$$\bigoplus_{i=1}^{p} V_i$$

if the decomposition is unique. Equivalently,

$$V = \bigoplus_{i=1}^{p} V_i \iff \exists! v_1 \in V_1, \dots, v_n \in V_n, v = \sum_{i=1}^{n} v_i$$

Lemma 1.4

The following are equivalent:

1. $\sum_{i=1}^{p} V_i = \bigoplus_{i=1}^{p} V_i$
2. $\forall 1 \leq i \leq l$, $V_i \cap \left(\sum_{j \neq i} V_j\right) = \{0\}$
3. For any basis B_i of V_i, $B = \bigcup_{i=1}^{n} B_i$ is a basis of $\sum_{i=1}^{n} V_i$.

Proof. Exercise. □

§2 Linear maps

§2.1 Linear maps

Definition 2.1

If V, W are F-vector spaces, a map $\alpha \colon V \to W$ is *linear* if

$$\forall \lambda_1, \lambda_2 \in F, \forall v_1, v_2 \in V, \alpha(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 \alpha(v_1) + \lambda_2 \alpha(v_2)$$

Example 2.1

Let M be a matrix with n rows and m columns. Then the map $\alpha \colon \mathbb{R}^m \to \mathbb{R}^n$ defined by $x \mapsto Mx$ is a linear map.

Example 2.2

Let $\alpha \colon \mathcal{C}([0,1], \mathbb{R}) \to \mathcal{C}([0,1], \mathbb{R})$ defined by $f \mapsto a(f)(x) = \int_0^x f(t)\,\mathrm{d}t$. This is linear.

Example 2.3

Let $x \in [a, b]$. Then $\alpha \colon \mathcal{C}([a,b], \mathbb{R}) \to \mathbb{R}$ defined by $f \mapsto f(x)$ is a linear map.

Remark 7. Let U, V, W be F-vector spaces. Then,

1. The identity function $i_V \colon V \to V$ defined by $x \mapsto x$ is linear.

2. If $\alpha\colon U \to V$ and $\beta\colon V \to W$ are linear, then $\beta \circ \alpha$ is linear.

Lemma 2.1

Let V, W be F-vector spaces. Let B be a basis for V. If $\alpha_0\colon B \to V$ is *any* map (not necessarily linear), then there exists a unique linear map $\alpha\colon V \to W$ extending α_0: $\forall v \in B, \alpha_0(v) = \alpha(v)$.

Proof. Let $v \in V$. Then, given $B = (v_1, \ldots, v_n)$.

$$v = \sum_{i=1}^{n} \lambda_i v_i$$

By linearity,

$$\alpha(v) = \alpha\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{i=1}^{n} \alpha(\lambda_i v_i) = \sum_{i=1}^{n} \alpha_0(\lambda_i v_i)$$

□

Remark 8. This lemma is also true in infinite-dimensional vector spaces. Often, to define a linear map, we instead define its action on the basis vectors, and then we 'extend by linearity' to construct the entire map.

Remark 9. If $\alpha_1, \alpha_2\colon V \to W$ are linear maps, then if they agree on any basis of V then they are equal.

§2.2 Isomorphism

Definition 2.2

Let V, W be F-vector spaces. A map $\alpha\colon V \to W$ is an *isomorphism* if and only if

1. α is linear
2. α is bijective

If such an α exists, we say that V and W are isomorphic, written $V \simeq W$.

Remark 10. If α in the above definition is an isomorphism, then $\alpha^{-1}\colon W \to V$ is linear. Indeed, if $w_1, w_2 \in W$ with $w_1 = \alpha(v_1)$ and $w_2 = \alpha(v_2)$,

$$\alpha^{-1}(w_1 + w_2) = \alpha^{-1}(\alpha(v_1) + \alpha(v_2)) = \alpha^{-1}\alpha(v_1 + v_2) = v_1 + v_2 = \alpha^{-1}(w_1) + \alpha^{-1}(w_2)$$

Similarly, for $\lambda \in F, w \in W$,

$$\alpha^{-1}(\lambda w) = \lambda \alpha^{-1}(w)$$

Lemma 2.2

Isomorphism is an equivalence relation on the class of all vector spaces over F.

Proof. 1. $i_V : V \to V$ is an isomorphism

2. If $\alpha : V \to W$ is an isomorphism, $\alpha^{-1} : W \to V$ is an isomorphism.
3. If $\beta : U \to V, \alpha : V \to W$ are isomorphisms, then $\alpha \circ \beta : U \to W$ is an isomorphism.

The proofs of each part are left as an exercise. □

Theorem 2.1

If V is an F-vector space of dimension n, then $V \simeq F^n$.

Proof. Let $B = (v_1, \dots, v_n)$ be a basis for V. Then, consider $\alpha : V \to F^n$ defined by

$$v = \sum_{i=1}^{n} \lambda_i v_i \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

We claim that this is an isomorphism. This is left as an exercise. □

Remark 11. Choosing a basis for V is analogous to choosing an isomorphism from V to F^n.

Theorem 2.2

Let V, W be F-vector spaces with finite dimensions n, m. Then,

$$V \simeq W \iff n = m$$

Proof. If $\dim V = \dim W = n$, then there exist isomorphisms from both V and W to F^n. By transitivity, therefore, there exists an isomorphism between V and W.

Conversely, if $V \simeq W$ then let $\alpha : V \to W$ be an isomorphism. Let B be a basis of V, then we claim that $\alpha(B)$ is a basis of W. Indeed, $\alpha(B)$ spans W from the surjectivity of α, and $\alpha(B)$ is free due to injectivity. □

§2.3 Kernel and image

Definition 2.3

Let V, W be F-vector spaces. Let $\alpha\colon V \to W$ be a linear map. We define the kernel and image as follows.

$$N(\alpha) = \ker \alpha = \{v \in V : \alpha(v) = 0\}$$

$$\mathrm{Im}(\alpha) = \{w \in W : \exists v \in V, w = \alpha(v)\}$$

Lemma 2.3

$\ker \alpha$ is a subspace of V, and $\mathrm{Im}\,\alpha$ is a subspace of W.

Proof. Let $\lambda_1, \lambda_2 \in F$ and $v_1, v_2 \in \ker \alpha$. Then

$$\alpha(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 \alpha(v_1) + \lambda_2 \alpha(v_2) = 0$$

Hence $\lambda_1 v_1 + \lambda_2 v_2 \in \ker \alpha$.

Now, let $\lambda_1, \lambda_2 \in F$, $v_1, v_2 \in V$, and $w_1 = \alpha(v_1), w_2 = \alpha(v_2)$. Then

$$\lambda_1 w_1 + \lambda_2 w_2 = \lambda_1 \alpha(v_1) + \lambda_2 \alpha(v_2) = \alpha(\lambda_1 v_1 + \lambda_2 v_2) \in \mathrm{Im}\,\alpha$$

□

Remark 12. $\alpha\colon V \to W$ is injective if and only if $\ker \alpha = \{0\}$. Further, $\alpha\colon V \to W$ is surjective if and only if $\mathrm{Im}\,\alpha = W$.

Theorem 2.3

Let V, W be F-vector spaces. Let $\alpha\colon V \to W$ be a linear map. Then $\overline{\alpha}\colon V/\ker \alpha \to \mathrm{Im}\,\alpha$ defined by

$$\overline{\alpha}(v + \ker \alpha) = \alpha(v)$$

is an isomorphism. *This is the isomorphism theorem from IA Groups.*

Proof. First, note that $\overline{\alpha}$ is well defined. Suppose $v + \ker \alpha = v' + \ker \alpha$. Then $v - v' \in \ker \alpha$, hence

$$\alpha(v - v') = 0 \implies \alpha(v) - \alpha(v') = 0$$

so $\overline{\alpha}$ is indeed well defined.

Linearity of $\overline{\alpha}$ follows from linearity of α.

Now, we show $\overline{\alpha}$ is injective.

$$\overline{\alpha}(v + \ker \alpha) = 0 \implies \alpha(v) = 0 \implies v \in \ker \alpha$$

Hence, $v + \ker \alpha = 0 + \ker \alpha$.

Further, $\overline{\alpha}$ is surjective as if $w \in \operatorname{Im} \alpha$, $\exists\, v \in V$ s.t. $w = \alpha(v) = \overline{\alpha}(v + \ker \alpha)$. □

§2.4 Rank and nullity

Definition 2.4

Rank and nullity The *rank* of α is

$$r(\alpha) = \dim \operatorname{Im} \alpha.$$

The *nullity* of α is

$$n(\alpha) = \dim \ker \alpha.$$

Theorem 2.4 (Rank-nullity theorem)

Let U, V be F-vector spaces such that the dimension of U is finite. Let $\alpha \colon U \to V$ be a linear map. Then,

$$\dim U = r(\alpha) + n(\alpha)$$

Proof. We have proven that $U/\ker \alpha \simeq \operatorname{Im} \alpha$. Hence, the dimensions on the left and right match: $\dim(U/\ker \alpha) = \dim \operatorname{Im} \alpha$.

$$\dim U - \dim \ker \alpha [a] = \dim \operatorname{Im} \alpha$$

and the result follows. □

[a] by proposition 1.7

Lemma 2.4 (Characterisation of isomorphisms)

Let V, W be F-vector spaces with equal, finite dimension. Let $\alpha \colon V \to W$ be a linear map. Then, the following are equivalent.

1. α is injective.
2. α is surjective.

3. α is an isomorphism.

Proof. Clearly, (iii) follows from (i) and (ii) and vice versa. The rest of the proof is left as an exercise, which follows from the rank-nullity theorem. □

Example 2.4

$$V = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 : x + y + z = 0 \right\}$$

$$\begin{aligned} \alpha : \mathbb{R}^3 &\to \mathbb{R} \\ \begin{bmatrix} x \\ y \\ z \end{bmatrix} &\mapsto x + y + z \\ \implies \ker \alpha &= V \\ \operatorname{Im} \alpha &= \mathbb{R}. \end{aligned}$$

So by rank nullity

$$3 = n(\alpha) + 1 \implies \dim V = 2$$

§2.5 Space of linear maps

Let V and W be F-vector spaces. Consider the space of linear maps from V to W. Then $L(V, W) = \{\alpha \colon V \to W \text{ linear}\}$.

Proposition 2.1 (Linear maps form a vector space)
$L(V, W)$ is an F-vector space under the operation

$$\begin{aligned} (\alpha_1 + \alpha_2)(v) &= \alpha_1(v) + \alpha_2(v) \\ (\lambda\alpha)(v) &= \lambda(\alpha(v)) \end{aligned}$$

Further, if V and W are finite-dimensional, then so is $L(V, W)$ with

$$\dim_F L(V, W) = \dim_F V \dim_F W$$

Proof. Proving that $L(V, W)$ is a vector space is left as an exercise. The dimensionality part is proven later, proposition 2.4. □

§2.6 Matrices

Definition 2.5 (Matrix)

An $m \times n$ matrix over F is an array with m rows and n columns, with entries in F.

Notation. We write $M_{m\times n}(F)$ for the set of $m \times n$ matrices over F.

Proposition 2.2

$M_{m\times n}(F)$ is an F-vector space under

$$((a_{ij}) + (b_{ij})) = (a_{ij} + b_{ij});$$

$$\lambda(a_{ij}) = (\lambda a_{ij})$$

Proof. Left as an exercise □

Proposition 2.3

$\dim_F M_{m,n}(F) = mn$.

Proof. Consider the basis defined by, the 'elementary matrix' for all i, j:

$$e_{pq} = \delta_{ip}\delta_{jq}$$

Then (e_{ij}) is a basis of $M_{m\times n}(F)$, since it spans $M_{m\times n}(F)$[a] and we can show that it is free. □

[a] given $A = (a_{ij}) \in M_{n\times n}(F)$, $A = a_{ij}e_{ij}$

§2.7 Linear maps as matrices

Let V, W be F-vector spaces and $\alpha : V \to W$ be a linear map. Consider bases B of V and C of W:

$$B = (v_1, \ldots, v_n);\ C = (w_1, \ldots, w_m)$$

Then let $v \in V$. We have

$$v = \sum_{j=1}^{n} \lambda_j v_j \equiv [v]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in F^n$$

where the vector given is the coordinates in basis B.

Notation. $[v]_B$ is the coordinates of v in basis B.

We can equivalently find $[w]_C$, the coordinates of w in basis C. We can now define a matrix of some linear map α in the B, C basis.

Definition 2.6 (Matrix of linear map)

The matrix representing α wrt B, C basis is

$$[\alpha]_{B,C} = \Big([\alpha(v_1)]_C, \dots, [\alpha(v_n)]_C\Big) \in M_{m\times n}(F)$$

Note. Let $[\alpha]_{B,C} = (a_{ij})$, then by definition

$$\alpha(v_j) = \sum_{i=1}^{m} a_{ij} w_i$$

Lemma 2.5

For all $v \in V$,

$$[\alpha(v)]_C = [\alpha]_{B,C} \cdot [v]_B$$

Proof. We have

$$v = \sum_{i=1}^{n} \lambda_j v_j$$

Hence

$$\alpha\left(\sum_{i=1}^{n} \lambda_j v_j\right) = \sum_{j=1}^{n} \lambda_j \alpha(v_j) = \sum_{j=1}^{n} \lambda_i \sum_{i=1}^{m} a_{ij} w_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij}\lambda_j\right) w_i$$

□

Lemma 2.6

Let $\beta\colon U \to V$ and $\alpha\colon V \to W$ be linear maps. Then, if A, B, C are bases of U, V, W respectively, then

$$[\alpha \circ \beta]_{A,C} = [\alpha]_{B,C} \cdot [\beta]_{A,B}$$

Proof. Let $A = [\alpha]_{B,C}$ and $B = [\beta]_{A,B}$. Consider $u_l \in A$ (basis of U). Then

$$(\alpha \circ \beta)(u_l) = \alpha(\beta(u_l))$$

giving

$$\alpha\left(\sum_j b_{jl} v_j\right) = \sum_j b_{jl}\alpha(v_j) = \sum_j b_{jl} \sum_i a_{ij} w_i = \sum_i \left(\sum_j a_{ij} b_{jl}\right) w_i$$

where $a_{ij}b_{jl}$ is the (i,l) element of AB by the definition of the product of matrices. □

Proposition 2.4

If V, W are F-vector spaces, and $\dim_F V = n, \dim_F W = m$, then

$$L(V,W) \simeq M_{m\times n}(F)$$

which implies the dimensionality of $L(V,W)$ in F is $m \times n$.

Proof. Consider two bases B, C of V, W. We claim that

$$\begin{aligned} \theta \colon L(V,W) &\to M_{m\times n}(F) \\ \alpha &\mapsto [\alpha]_{B,C} \end{aligned}$$

is an isomorphism.

First, note that θ is linear.

$$[\lambda_1\alpha_1 + \lambda_2\alpha_2] = \lambda_1[\alpha_1]_{B,C} + \lambda_2[\alpha_2]_{B,C}.$$

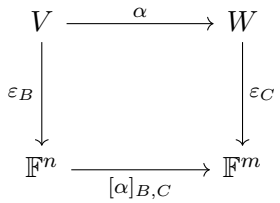
Also, θ is surjective; consider any matrix $A = (a_{ij})$ and consider $\alpha \colon v_j \mapsto \sum_{i=1}^m a_{ij} w_i$ defined on B. Then this is certainly a linear map which extends uniquely by linearity to A, giving $[\alpha]_{B,C} = (a_{ij}) = A$[a].

Now, θ is injective since $[\alpha]_{B,C} = 0 \implies \alpha = 0$. □

[a] Proving this left as an exercise

Remark 13. If B, C are bases of V, W respectively, and $\varepsilon_B \colon V \to F^n$ is defined by

$v \mapsto [v]_B$, and analogously for ε_C, then the following diagram commutes



We can see that

$$[\alpha]_{B,C} \circ \varepsilon_B = \varepsilon_C \circ \alpha$$

so the operations commute.

Example 2.5

Let $\alpha\colon V \to W$ be a linear map and $Y \leq V$, where V, W are finite-dimensional. Then let $\alpha(Y) = Z \leq W$. Consider a basis B of V, such that $B' = (v_1, \ldots, v_k)$ is a basis of Y completed by $B'' = (v_{k+1}, \ldots, v_n)$ into $B = B' \cup B''$. Then let C be a basis of W, such that $C' = (w_1, \ldots, w_\ell)$ is a basis of Z completed by $C'' = (w_{\ell+1}, \ldots, w_m)$ into $C = C' \cup C''$. Then

$$[\alpha]_{B,C} = \begin{pmatrix} \alpha(v_1) & \ldots & \alpha(v_k) & \alpha(v_{k+1}) & \ldots & \alpha(v_n) \end{pmatrix}$$

For $1 \leq i \leq k$, $\alpha(v_i) \in Z$ since $v_i \in Y, \alpha(Y) = Z$. So the matrix has an upper-left $\ell \times k$ block A which is $\alpha\colon Y \to Z$ on the basis B', C'. We can show further that α induces a map $\overline{\alpha}\colon V/Y \to W/Z$ by $v + Y \mapsto \alpha(v) + Z$. This is well-defined; $v_1 + Y = v_2 + Y$ implies $v_1 - v_2 \in Y$ hence $\alpha(v_1 - v_2) \in Z$ as required. The bottom-right block is $[\overline{\alpha}]_{B'',C''}$.

§2.8 Change of basis

Suppose we have two bases $B = \{v_1, \ldots, v_n\}, B' = \{v'_1, \ldots, v'_n\}$ of V and corresponding C, C' for W. If we have a linear map $[\alpha]_{B,C}$, we are interested in finding the components of this linear map in another basis, that is,

$$[\alpha]_{B,C} \mapsto [\alpha]_{B',C'}$$

Definition 2.7 (Change of basis matrix)

The **change of basis** matrix P from B' to B is

$$P = \begin{pmatrix} [v'_1]_B & \cdots & [v'_n]_B \end{pmatrix}$$

which is the identity map in B', written

$$P = [I]_{B',B}$$

Lemma 2.7

For a vector v,

$$[v]_B = P[v]_{B'}$$

Proof. We have

$$[\alpha(v)]_C = [\alpha]_{B,C} \cdot [v]_C$$

Since $P = [I]_{B',B}$,

$$[I(v)]_B = [I]_{B',B} \cdot [v]_{B'} \implies [v]_B = P[v]_{B'}$$

as required. □

Remark 14. P is an invertible $n \times n$ square matrix. In particular,

$$P^{-1} = [I]_{B,B'}$$

Indeed,

$$\begin{aligned} [\alpha \circ \beta]_{A,C} &= [\alpha]_{B,C}[\beta]_{A,B} \\ \implies I_n &= [I \cdot I]_{B,B} = [I]_{B',B} \cdot [I]_{B,B'} \end{aligned}$$

where I_n is the $n \times n$ identity matrix.

Warning 2.1

$$\begin{aligned} P &= ([v_1']_B, \ldots, [v_n']_B) \\ \implies [v]_B &= P[v]_{B'} \\ \implies [v]_{B'} &= P^{-1}[v]_B \end{aligned}$$

Proposition 2.5

If α is a linear map from V to W, and $P = [I]_{B',B}, Q = [I]_{C',C}$[a], we have

$$A' = [\alpha]_{B',C'} = [I]_{C,C'}[\alpha]_{B,C}[I]_{B,'B} = Q^{-1}AP$$

where $A = [\alpha]_{B,C}, A' = [\alpha]_{B',C'}$.

[a] P, Q invertible.

Proof.

$$\begin{aligned}
[\alpha(v)]_C &= Q[\alpha(v)]_{C'} \\
&= Q[\alpha]_{B',C'}[v]_{B'} \\
[\alpha(v)]_C &= [\alpha]_{B,C}[v]_B \\
&= AP[v]_{B'} \\
\therefore \forall v,\ QA'[v]_{B'} &= AP[v]_{B'} \\
\therefore QA' &= AP
\end{aligned}$$

as required. □

§2.9 Equivalent matrices

Definition 2.8 (Equivalent matrices)

Matrices $A, A' \in M_{m,n}(F)$ are called **equivalent** if

$$A' = Q^{-1}AP$$

for some invertible $m \times m, n \times n$ matrices Q, P.

Remark 15. This defines an equivalence relation on $M_{m,n}(F)$.

- $A = I_m^{-1} A I_n$;
- $A' = Q^{-1}AP \implies A = QA'P^{-1}$;
- $A' = Q^{-1}AP, A'' = (Q')^{-1}A'P' \implies A'' = (QQ')^{-1}A(PP')$.

Proposition 2.6

Let V, W be vector spaces over F with $\dim_F V = n$, $\dim_F W = m$. Let $\alpha \colon V \to W$ be a linear map. Then there exists a basis B of V and a basis C of W such that

$$[\alpha]_{B,C} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

so the components of the matrix are exactly the identity matrix of size r in the top-left corner, and zeroes everywhere else.

Proof. We first fix $r \in \mathbb{N}$ such that $\dim \ker \alpha = n - r$. Then we will construct a basis $\{v_{r+1}, \dots, v_n\}$ of the kernel. We extend this to a basis of the entirety of V, that is, $\{v_1, \dots, v_n\}$. Then, we want to show that

$$\{\alpha(v_1), \dots, \alpha(v_r)\}$$

is a basis of $\operatorname{Im} \alpha$. Indeed, it is a generating family:

$$\begin{aligned} v &= \sum_{i=1}^{n} \lambda_i v_i \\ \alpha(v) &= \sum_{i=1}^{n} \lambda_i \alpha(v_i) \\ &= \sum_{i=1}^{r} \lambda_i \alpha(v_i) \text{ as } v_{r+i} \in \ker \alpha \end{aligned}$$

Then if $y \in \operatorname{Im} \alpha$, there exists v such that $\alpha(v) = y$. So

$$y = \sum_{i=1}^{r} \lambda_i \alpha(v_i) \in \langle \alpha(v_1), \dots, \alpha(v_r) \rangle.$$

Further, it is a free family:

$$\begin{aligned} \sum_{i=1}^{r} \lambda_i \alpha(v_i) &= 0 \\ \alpha\left(\sum_{i=1}^{r} \lambda_i v_i \right) &= 0 \\ \sum_{i=1}^{r} \lambda_i v_i &\in \ker \alpha \\ \sum_{i=1}^{r} \lambda_i v_i &= \sum_{i=r+1}^{n} \lambda_i v_i \text{ as } v_{r+i} \text{ is a basis of } \ker \alpha. \\ \sum_{i=1}^{r} \lambda_i v_i - \sum_{i=r+1}^{n} \lambda_i v_i &= 0 \end{aligned}$$

But since $\{v_1, \dots, v_n\}$ is a basis, $\lambda_i = 0$ for all i.

Hence $\{\alpha(v_1), \dots, \alpha(v_r)\}$ is a basis of $\operatorname{Im} \alpha$. Now, we extend this basis to the whole of W to form

$$\{\alpha(v_1), \dots, \alpha(v_r), w_{r+1}, \dots, w_n\}$$

Now,

$$[\alpha]_{BC} = \begin{pmatrix} \alpha(v_1) & \cdots & \alpha(v_r) & \alpha(v_{r+1}) & \cdots & \alpha(v_n) \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

□

Remark 16. This also proves the rank-nullity theorem:

$$\operatorname{rank}\alpha + \operatorname{null}\alpha = n$$

Corollary 2.1

Any $m \times n$ matrix A is equivalent to a matrix of the form

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

where $r = \operatorname{rank} A$.

§2.10 Column rank and row rank

Definition 2.9

Let $A \in M_{m,n}(F)$. Then, the *column rank* of A, here denoted $r_c(A)$, is the dimension of the subspace of F^n spaned by the column vectors.

$$r_c(A) = \dim \operatorname{span}\{c_1, \ldots, c_n\}$$

Remark 17. If α is a linear map, represented in bases B, C by the matrix A, then

$$\operatorname{rank}\alpha = r_c(A)$$

Proposition 2.7

Two matrices are equivalent if they have the same column rank:

$$r_c(A) = r_c(A')$$

Proof. If the matrices are equivalent, then $A = [\alpha]_{BC}, A' = [\alpha]_{B',C'}$. Then

$$r_c(A) = r_c(\alpha) = r_c(A')$$

Conversely, if $r_c(A) = r_c(A') = r$, then A, A' are equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

By transitivity, A, A' are equivalent. □

Theorem 2.5

Column rank $r_c(A)$ and row rank $r_c(A^\intercal)$ are equivalent.

Proof. Let $r = r_C(A)$. Then,

$$Q^{-1}AP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{m \times n}$$

Then, consider

$$P^\intercal A^\intercal \left(Q^{-1}\right)^\intercal = (Q^{-1}AP)^\intercal = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}^\intercal_{m \times n} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}_{n \times m}$$

Note that we can swap the transpose and inverse on Q because

$$\begin{aligned} (AB)^\intercal &= B^\intercal A^\intercal \\ \left(QQ^{-1}\right)^\intercal &= Q^\intercal \left(Q^{-1}\right)^\intercal \\ I &= Q^\intercal \left(Q^{-1}\right)^\intercal \\ (Q^\intercal)^{-1} &= \left(Q^{-1}\right)^\intercal \end{aligned}$$

Then $r_c(A) = \operatorname{rank}(A) = \operatorname{rank}(A^\intercal) = r_c(A^\intercal)$. □

So we can drop the concepts of column and row rank, and just talk about rank as a whole.

§2.11 Conjugation and similarity

Consider the following special case of changing basis. If $\alpha \colon V \to V$ is linear, α is called an *endomorphism*. If $B = C, B' = C'$ then the special case of the change of basis formula is

$$[\alpha]_{B',B'} = P^{-1}[\alpha]_{B,B}P$$

Then, we say square matrices A, A' are *similar* or *conjugate* if there exists P such that $A' = P^{-1}AP$.

§2.12 Elementary operations

Definition 2.10

An *elementary column operation* is

1. swap columns i, j
2. replace column i by λ multiplied by the column
3. add λ multiplied by column i to column j

We define analogously the elementary row operations. Note that these elementary operations are invertible (for $\lambda \neq 0$). These operations can be realised through the action of elementary matrices. For instance, the column swap operation can be realised using

$$T_{ij} = \begin{pmatrix} I_n & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & I_m \end{pmatrix}; \quad A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & I_k & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

To multiply a column by λ,

$$n_{i,\lambda} = \begin{pmatrix} I_n & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & I_m \end{pmatrix}$$

To add a multiple of a column,

$$c_{ij,\lambda} = I + \lambda E_{ij}$$

where E_{ij} is the matrix defined by elements $(e_{ij})_{pq} = \delta_{ip}\delta_{jq}$. An elementary column (or row) operation can be performed by multiplying A by the corresponding elementary matrix from the right (on the left for row operations). This will essentially provide a constructive proof that any $n \times n$ matrix is equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

We will start with a matrix A. If all entries are zero, we are done. So we will pick $a_{ij} = \lambda \neq 0$, and swap rows $i, 1$ and columns $j, 0$. This ensures that $a_{11} = \lambda \neq 0$. Now we multiply column 1 by $\frac{1}{\lambda}$. Finally, we can clear out row 1 and column 1 by subtracting multiples of the first row or column. Then we can perform similar operations on the $(n-1) \times (n-1)$ matrix in the bottom right block and inductively finish this process.

§2.13 Gauss' pivot algorithm

If only row operations are used, we can reach the 'row echelon' form of the matrix, a specific case of an upper triangular matrix. On each row, there are a number of zeroes

until there is a one, called the pivot. First, we assume that $a_{ij} \neq 0$. We swap rows $i, 1$. Then divide the first row by $\lambda = a_{i1}$ to get a one in the top left. We can use this one to clear the rest of the first column. Then, we can repeat on the next column, and iterate. This is a technique for solving a linear system of equations.

§2.14 Representation of square invertible matrices

Lemma 2.8

If A is an $n \times n$ square invertible matrix, then we can obtain I_n using only row elementary operations, or only column elementary operations.

Proof. We show an algorithm that constructs this I_n. This is exactly going to invert the matrix, since the resultant operations can be combined to get the inverse matrix. We will show here the proof for column operations. We argue by induction on the number of rows. Suppose we can make the form

$$\begin{pmatrix} I_k & 0 \\ A & B \end{pmatrix}$$

We want to obtain the same structure with $k+1$ rows. We claim that there exists $j > k$ such that $a_{k+1,j} \neq 0$. Indeed, otherwise we can show that the vector

$$\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \delta_{k+1,i}$$

is not in the span of the column vectors of A. This contradicts the invertibility of the matrix. Now, we will swap columns $k+1, j$ and divide this column by λ. We can now use this 1 to clear the rest of the $k+1$ row.

Inductively, we have found $AE_1 \dots E_n = I_n$ where E_n are elementary. Thus, we can find A^{-1}. □

Proposition 2.8

Any invertible square matrix is a product of elementary matrices.

The proof is exactly the proof of the lemma above.

§3 Dual spaces