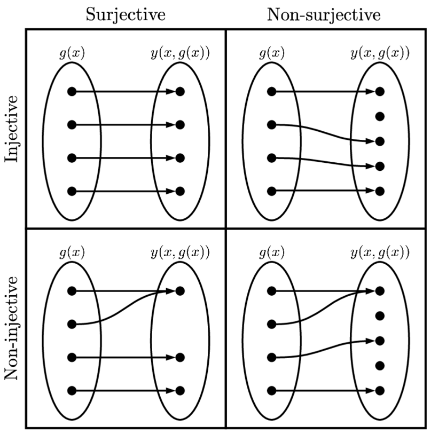
D: Functions

A function $f : X \to Y$ is an assignment of an element of Y to each element of X.

1. f is **injective** if:
$$\forall x_1, x_2 \in X; f(x_1) = f(x_2) \implies x_1 = x_2$$
and this implies $|X| \leq |Y|$.
2. f is **surjective** if:
$$\forall y \in Y; \exists x \in X : y = f(x)$$
and this implies $|X| \geq |Y|$.
3. f is **bijective** if it is injective and surjective.



D: Groups

A group G is a set with a composition operator $(\circ)$ such that $\forall x, y, z, \in G$:

1. $x \circ y = xy$
2. $(xy)z = x(yz)$
3. $\exists e \in G : ex = xe = x$
4. $\exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$

G is **Abelian** if $\forall x, y \in G; xy = yx$.

D1.2.1(i): Fields

A field F is a set defined with addition and multiplication such that:

1. $(+) : F \times F \to F; (\lambda, \mu) \mapsto \lambda + \mu$
2. $(\cdot) : F \times F \to F; (\lambda, \mu) \mapsto \lambda \cdot \mu$
3. $\exists(-\lambda) \in F : \lambda + (-\lambda) = 0_F$
4. $\exists(\lambda^{-1}) \in F : \lambda \cdot (\lambda^{-1}) = 1_F$ except when $\lambda = 0$.
5. $(+)$ and $(\cdot)$ are associative, commutative and distributive.

Remark

$(F, +)$ and $(F \setminus \{0_F\}, \cdot)$ are groups.

Remark

Let n be prime or a prime power. Then $\mathbb{F}_n$ is a finite field with n elements under modulo n. Also, $\mathbb{Q}$ and $\mathbb{R}$ are fields.

D1.2.1(ii): Vector spaces

A vector space V over a field F is an Abelian group $V := (V, +)$ with mapping:
$$F \times V \to V; (\lambda, \boldsymbol{v}) \mapsto \lambda \boldsymbol{v}$$
where for $\forall \lambda, \mu \in F$ and $\forall \boldsymbol{v}, \boldsymbol{w} \in V$:

1. $\lambda(\boldsymbol{v} + \boldsymbol{w}) = (\lambda \boldsymbol{v}) + (\mu \boldsymbol{w})$
2. $(\lambda + \mu)\boldsymbol{v} = (\lambda \boldsymbol{v}) + (\mu \boldsymbol{w})$
3. $\lambda(\mu \boldsymbol{v}) = (\lambda \mu)\boldsymbol{v}$
4. $1_F \boldsymbol{v} = \boldsymbol{v}$

and is known as a F-vector space.

Remark

Let V be a F-vector space and $\boldsymbol{v} \in V$.

1. $0\boldsymbol{v} = 0$
2. $(-1)\boldsymbol{v} = -\boldsymbol{v}$
3. $\lambda \boldsymbol{0} = \boldsymbol{0}$ for $\forall \lambda \in F$.

D: Cartesian products

The **cross product** of sets $X_1, \ldots, X_n$ is:
$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i\}$$
with bijection $X^n \times X^m \to X^{n+m}$.

The **projection** of a cross product is:
$$\mathrm{pr}_i : X_1 \times \cdots \times X_n \to X_i; \quad (x_1, \ldots, x_n) \mapsto x_i.$$

D1.4.1: Vector subspaces

A vector subspace U of F-vector space V has the following properties:

1. $U \subset V$ and $\boldsymbol{0} \in U$.
2. Let $\boldsymbol{u}, \boldsymbol{v} \in U$ and $\lambda \in F$. Then $\boldsymbol{u} + \boldsymbol{v} \in U$ and $\lambda \boldsymbol{u} \in U$.

and is also a vector space.

P1.4.5

Let $T \subset V$ where V is a F-vector space. Then for all vector subspaces containing T, there exists a smallest vector subspace:
$$\mathrm{span}(T) = \langle T \rangle_F \subset V$$
known as the vector subspace generated by T, or the span of T.

D1.4.7: Generating set

Let $T \subset V$ where V is a F-vector space. Set T is a **generating set** of V if:
$$\mathrm{span}(T) = V$$
and is the linear combination of vectors in T over field F. V is **finitely generated** if its generating set T is finite.

D1.4.9: Power sets

The power set of set X is:
$$\mathcal{P}(X) := \{U : U \subseteq X\}.$$
Let $\mathcal{U} \subseteq \mathcal{P}(X)$. Then:
$$\bigcup_{U \in \mathcal{U}} U := \{x \in X : (\exists U \in \mathcal{U} : x \in U)\}$$
$$\bigcap_{U \in \mathcal{U}} U := \{x \in X : \forall U \in \mathcal{U}; x \in U\}.$$

D1.5.1: Linear independence

Let V be a F-vector space and $L \subseteq V$. Subset L is **linearly independent** if:
$$\alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_r \boldsymbol{v}_r = \boldsymbol{0} \implies \alpha_1 = \cdots = \alpha_r = 0$$
for $\boldsymbol{v}_i \in L$ and is pairwise distinct.

Remark

L is linearly dependent if some $\alpha_i \neq 0$.

D1.5.8: Basis

A basis of a vector space V is a **linearly independent** generating set in V.

T1.5.11

Let V be a F-vector space.

Then $A = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ is a basis of V **iff** the following evaluation mapping:
$$\Phi : F^r \to V; \quad (\alpha_1, \ldots, \alpha_r) \mapsto \alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_r \boldsymbol{v}_r$$
is a bijection.

Remark

Φ is surjective if A is generating.

T1.5.12

Let V be a vector space and $E \subseteq V$. Then the following statements are equivalent:

1. E is a basis of V.
2. E is minimal among all generating sets, or that $E \setminus \{\boldsymbol{e}\}$ is not a basis for $\forall \boldsymbol{e} \in E$.
3. E is maximal amongst all linearly independent subsets. i.e. $E \cup \{\boldsymbol{v}\}$ is linearly dependent for $\forall \boldsymbol{v} \in V$.

C1.5.13

Every finitely generated vector space has a finite basis.

T1.5.14

Let V be a vector space.

1. Let $L \subseteq V$ be linearly independent and set E be minimal amongst all generating sets of V. Let $L \subseteq E$. Then E is a basis of V.
2. Let $E \subseteq V$ be a generating set and L be maximal amongst all linearly independent subsets of V.

   Let $L \subseteq E$. Then E is a basis of V.

D1.5.15

Let X be a set and F be a field. Then:

$$\operatorname{maps}(X, F) := \{f : (\forall f : X \to F)\}$$

and is a F-vector space under pointwise addition and multiplication via scalars.

Let $F\langle X\rangle \subseteq \operatorname{maps}(X, F)$ be the subset of all mappings that sends all but finitely many elements of X to 0:

$$F\langle X\rangle := \big\{f : \big(\forall f : X \to \{0\}\big)\big\}.$$

It contains all linear combinations of X in F and forms a vector subspace.

T1.5.16

Let V be a F-vector space.

Then $(\boldsymbol{v}_i)_{i\in I}$ is a basis for V **iff**:

$$\forall \boldsymbol{v} \in V; \exists!(a_i)_{i\in I} \subseteq F : \boldsymbol{v} = \sum_{i\in I} a_i \boldsymbol{v}_i.$$

T1.6.1

Let V be a vector space. Let $L \subset V$ be a linearly independent subset and $E \subseteq V$ a generating set. Then $|L| \leq |E|$.

T1.6.2: Steinitz exchange theorem

Let V be a vector space, $L \subset V$ be a finite linearly independent subset and $E \subseteq V$ be a generating set.

Then there exists an **injective** function $\phi : L \to E$ such that:

$\big(E \setminus \phi(L)\big) \cup L$ is a generating set for V.

L1.6.3: Exchange lemma

Let V be a vector space. Let $M \subset V$ be a finite linearly independent subset and $E \subseteq V$ be a generating set where $M \subseteq E$.

If $\exists \boldsymbol{w} \in V \setminus M$ such that set $M \cup \{\boldsymbol{w}\}$ is linearly independent then:

$\exists \boldsymbol{e} \in E \setminus M : \big(E \setminus \boldsymbol{e}\big) \cup \{\boldsymbol{w}\}$ is generating.

C1.6.4

Let V be a finitely generated vector space.

1. V has finite basis.
2. V cannot have infinite basis.
3. Any two basis of V have the same number of elements.

D1.6.5: Dimension

The dimension of finite F-vector space V is the cardinality of one its basis.

For infinite vector spaces: $\dim(V) = \infty$.

C1.6.7

Let V be a finitely generated vector space.

1. Every linearly independent $L \subseteq V$ has **at most** $\dim(V)$ elements and if $|L| = \dim(V)$ then L is a basis.
2. Every generating set $E \subseteq V$ has **at least** $\dim(V)$ elements and if $|E| = \dim(V)$ then E is a basis.

C1.6.8

A proper vector subspace of a vector space with finite dimension has itself a strictly smaller dimension.

T1.6.10

Let V be a vector space and $U, W \subseteq V$ be vector subspaces. Then:

$$\begin{aligned}&\dim(U + W) + \dim(U \cap W)\\&= \dim(U) + \dim(W).\end{aligned}$$

D1.7.1: Linear mappings

Let V and W be F-vector spaces.
A mapping $f : V \to W$ is **F-linear** or a **homomorphism** of vector spaces if for $\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ and $\forall \lambda \in F$:

1. $f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2)$
2. $f(\lambda \boldsymbol{v}_1) = \lambda f(\boldsymbol{v}_1)$.

Furthermore bijective linear mappings are an **isomorphism** of vector spaces.

A homomorphism from a vector space to itself is an **endomorphism**.

An isomorphism of a vector space to itself is an **automorphism**.

D1.7.5: Fixed points

In a linear mapping a fixed point is sent to itself. For mapping $f : X \to X$ the **set of fixed points** is:

$$X^f = \{x \in X : f(x) = x\}.$$

D1.7.6: Complementary subspaces?

Vector subspaces V_1, V_2 of vector space V are **complementary** if the mapping:

$$V_1 \times V_2 \to V$$

is a bijection.

T1.7.7

A F-vector space V is isomorphic to F^n **iff** $\dim(V) = n$, for $n \in \mathbb{N}$ and F a field.

L1.7.8

Let V, W be F-vector spaces and let B be a basis of V. Then the following mapping:

$$\hom_F(V, W) \to \operatorname{maps}(B, W); f \mapsto f_B$$

is a bijection.

Remark

Let V, W be F-vector spaces. The set of all homomorphisms from V to W is:

$$\hom_F(V, W) \subseteq \operatorname{maps}(B, W).$$

P1.7.9

Let $f : V \to W$ be a linear mapping, where V, W are vector spaces.

1. If f is injective, there exists map $g : W \to V$ such that $g \circ f = \mathrm{id}_V$. i.e. it has a **left inverse**.
2. If f is surjective, there exists map $g : W \to V$ such that $f \circ g = \mathrm{id}_W$. i.e. it has a **right inverse**.

D1.8.1: Image and kernel

Let $f : V \to W$ be a linear mapping.
The **image** of this linear mapping f is:

$$\operatorname{im}(f) := f(V) \subseteq W$$

and is a vector subspace of W.

The **kernel** of this linear mapping f is:

$$\ker(f) := f^{-1}(\boldsymbol{0}) = \{\boldsymbol{v} \in V : f(\boldsymbol{v}) = \boldsymbol{0}\}$$

and is the preimage of the zero vector in linear mapping f.

L1.8.2

A linear mapping $f : V \to W$ is injective **iff** $\ker(f) = \{\boldsymbol{0}\}$.

T1.8.4: Rank-nullity theorem

Let $f : V \to W$ be a linear mapping and V, W are vector spaces. Then:

$$\dim(V) = \dim\Big(\ker(f)\Big) + \dim\Big(\operatorname{im}(f)\Big).$$

T2.1.1

Let F be a field and $m, n \in \mathbb{N}$.

Then there exists a bijection:

$$M : \hom_F(F^m, F^n) \to \mathrm{mat}(n \times m; F);$$
$$f \mapsto [f]$$

and attaches each linear mapping f with its **representing matrix** $M(f) := [f]$.

Remark

The set of matrices with n rows and m columns with entries in field F is:

$$\mathrm{mat}(n \times m; F).$$

D2.1.6: Matrix products

The product $A \circ B = AB$ is defined:

$$(AB)_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$

where $A \in \mathrm{mat}(n \times m; F)$, F a field, $B \in \mathrm{mat}(m \times \ell; F)$ and $m, n, \ell \in \mathbb{N}$. This is matrix multiplication, with mapping:

$$\mathrm{mat}(n \times m; F) \times \mathrm{mat}(m \times \ell; F)$$
$$\to \mathrm{mat}(n \times \ell; F);$$
$$(A, B) \mapsto AB.$$

T2.1.8

Let $g : F^\ell \to F^m$ and $f : F^m \to F^n$ be linear mappings. Then $[f \circ g] = [f] \circ [g]$.

P2.1.9

Let $A, A' \in \mathrm{mat}(n \times m; F)$.
Let $B, B' \in \mathrm{mat}(m \times \ell; F)$.
Let $C, C' \in \mathrm{mat}(\ell \times k; F)$.
Let $k, \ell, m, n \in \mathbb{N}$ and denote $I = I_m$ as the $(m \times m)$ identity matrix. Then:

1. $(A + A')B = AB + A'B$
2. $A(B + B') = AB + AB'$
3. $IB = B$
4. $AI = A$
5. $(AB)C = A(BC)$.

D2.2.1: Invertible matrices

A matrix A is **invertible** if:

$$\exists B, C : BA = I \text{ and } AC = I.$$

D2.2.2: Elementary matrices

Elementary matrices are square matrices that differs from the identity matrix by at most one entry.

T2.2.3

Every square matrix with entries in a field can be written as a product of elementary matrices.

D2.2.4: Smith normal form

Matrices with non-zero entries along the diagonal are in Smith normal form. e.g:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

T2.2.5

For every $A \in \mathrm{mat}(n \times m; F)$,
there exists invertible matrices P and Q such that PAQ is of Smith normal form.

D2.2.7: Column and row rank

Let matrix $A \in \mathrm{mat}(n \times m; F)$.

The column rank of A is the dimension of the subspace of F^n generated by the columns of A.

Similarly the row rank of A is the dimension of the subspace of F^m generated by the rows of A.

T2.2.8

Column and row ranks are equal.

D2.2.9: Full rank matrices

Let matrix $A \in \mathrm{mat}(n \times m; F)$.
A is full rank if $\mathrm{rank}(A) = \min(m, n)$.