

**D: Functions**

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

1.  $f$  is **injective** if:

$$\begin{aligned} \forall x_1, x_2 \in X; f(x_1) = f(x_2) \\ \implies x_1 = x_2 \end{aligned}$$

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.  $(+) : F \times F \rightarrow F; (\lambda, \mu) \mapsto \lambda + \mu$
2.  $(\cdot) : F \times F \rightarrow F; (\lambda, \mu) \mapsto \lambda \cdot \mu$
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:

$$F \times V \rightarrow V; (\lambda, \mathbf{v}) \mapsto \lambda \mathbf{v}$$

where for  $\forall \lambda, \mu \in F$  and  $\forall \mathbf{v}, \mathbf{w} \in V$ :

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

and is known as a  **$F$ -vector space**.

**Remark**

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

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

**D: Cartesian products**

The **cross product** of sets  $X_1, \dots, X_n$  is:

$$X_1 \times \dots \times X_n := \{(x_1, \dots, x_n) : x_i \in X_i\}$$

with bijection  $X^n \times X^m \rightarrow X^{n+m}$ .

The **projection** of a cross product is:

$$\begin{aligned} \text{pr}_i : X_1 \times \dots \times X_n &\rightarrow X_i; \\ (x_1, \dots, x_n) &\mapsto x_i. \end{aligned}$$

**D1.4.1: Vector subspaces**

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

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

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:

$$\text{span}(T) = \langle T \rangle_F \subset V$$

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:

$$\text{span}(T) = V$$

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:

$$\begin{aligned} \bigcup_{U \in \mathcal{U}} U &:= \{x \in X : (\exists U \in \mathcal{U} : x \in U)\} \\ \bigcap_{U \in \mathcal{U}} U &:= \{x \in X : \forall U \in \mathcal{U}; x \in U\}. \end{aligned}$$

**D1.5.1: Linear independence**

Let  $V$  be a  $F$ -vector space and  $L \subseteq V$ . Subset  $L$  is **linearly independent** if:

$$\begin{aligned} \alpha_1 \mathbf{v}_1 + \dots + \alpha_r \mathbf{v}_r &= \mathbf{0} \\ \implies \alpha_1 = \dots = \alpha_r &= 0 \end{aligned}$$

for  $\mathbf{v}_i \in L$  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  $A = \{\mathbf{v}_1, \dots, \mathbf{v}_r\}$  is a basis of  $V$  **iff** the following **evaluation mapping**:

$$\Phi : F^r \rightarrow V;$$

$$(\alpha_1, \dots, \alpha_r) \mapsto \alpha_1 \mathbf{v}_1 + \dots + \alpha_r \mathbf{v}_r$$

is a bijection.

**Remark**

$\Phi$  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  $E \setminus \{\mathbf{e}\}$  is not a basis for  $\forall \mathbf{e} \in E$ .
3.  $E$  is maximal amongst all linearly independent subsets. i.e.  $E \cup \{\mathbf{v}\}$  is linearly dependent for  $\forall \mathbf{v} \in V$ .

**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:

$$\text{maps}(X, F) := \{f : (\forall f : X \rightarrow F)\}$$

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

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

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

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  $(v_i)_{i \in I}$  is a basis for  $V$  iff:

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

**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  $\phi : L \rightarrow E$  such that:

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

**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  $\exists w \in E \setminus M$  such that set  $M \cup \{w\}$  is linearly independent then:

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

**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 of its basis.

For infinite vector spaces:  $\dim(V) = \infty$ . We also define  $\dim(\{0\}) := 0$ .

**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: Dimension theorem**

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

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

where  $U + W := \langle U \cup W \rangle \subseteq V$ .

**D1.7.1: Linear mappings**

Let  $V$  and  $W$  be  $F$ -vector spaces.

A mapping  $f : V \rightarrow W$  is  **$F$ -linear** or a **homomorphism** of vector spaces if for  $\forall v_1, v_2 \in V$  and  $\forall \lambda \in F$ :

1.  $f(v_1 + v_2) = f(v_1) + f(v_2)$
2.  $f(\lambda v_1) = \lambda f(v_1)$ .

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. Given mapping  $f : X \rightarrow X$  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 **direct sum** of vector subspaces is bijective:

$$\oplus : V_1 \times V_2 \rightarrow V; (v_1, v_2) \mapsto v_1 + v_2.$$

i.e.  $V_1 \oplus V_2 = V$ .

**T1.7.7**

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

**L1.7.8**

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

$$\text{hom}_F(V, W) \rightarrow \text{maps}(B, W); f \mapsto f_B$$

is a bijection. The set of all linear maps or homomorphisms from  $V$  to  $W$  is:

$$\text{hom}_F(V, W) \subseteq \text{maps}(B, W).$$

**P1.7.9**

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

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

**D1.8.1: Image and kernel**

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

$$\begin{aligned} \text{im}(f) &:= f(V) \\ &= \{w \in W : \forall v \in V; w = f(v)\} \end{aligned}$$

and is a vector subspace of  $W$ .

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

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

and is a vector subspace of  $V$ .

**L1.8.2**

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

**T1.8.4: Rank-nullity theorem**

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

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

**T2.1.1: Matrix mappings**

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

Then there exists a bijection:

$$M : \operatorname{hom}_F(F^m, F^n) \rightarrow \operatorname{mat}(n \times m; F);$$

$$f \mapsto [f]$$

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

**Remark**

We define the set of matrices with  **$n$  rows** and  **$m$  columns** with entries in field  $F$  as:

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

**D2.1.6: Matrix products**

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

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

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

$$\begin{aligned} &\operatorname{mat}(n \times m; F) \times \operatorname{mat}(m \times \ell; F) \\ &\rightarrow \operatorname{mat}(n \times \ell; F); (A, B) \mapsto AB. \end{aligned}$$

**T2.1.8**

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

**P2.1.9**

Let  $A, A'$  be  $n \times m$ ,  $B, B'$  be  $m \times \ell$  and  $C, C'$  be  $\ell \times k$ . 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  $A \in \operatorname{mat}(n \times m; F)$ , there exists invertible matrices  $P$  and  $Q$  such that  $PAQ$  is of Smith normal form.

**D2.2.7: Column and row rank**

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

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