### D: Functions

A function $f : X \to Y$ is an assignment of an element of $Y$ to <u>each</u> 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 that $|X| \leq |Y|$.

2. $f$ is **surjective** if:
$$\forall y \in Y; \exists x \in X : y = f(x)$$
and this implies that $|X| \geq |Y|$.

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. $x \circ y = xy \in G$
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 <span style="color:red">Abelian group</span> $V := (V, +)$ 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. $\lambda(\boldsymbol{v} + \boldsymbol{w}) = (\lambda\boldsymbol{v}) + (\lambda\boldsymbol{w})$
2. $(\lambda + \mu)\boldsymbol{v} = (\lambda\boldsymbol{v}) + (\mu\boldsymbol{v})$
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:
$$\mathrm{pr}_i : X_1 \times \cdots \times X_n \to X_i;$$
$$(x_1, \ldots, x_n) \mapsto x_i.$$

### 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 <u>smallest</u> 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** <u>generating set</u> in $V$.

### T1.5.11: Basis evaluation mappings

Let $V$ be a $F$-vector space.

Then $A = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ is a basis of $V$ **iff** the following <span style="color:red">evaluation mapping</span>:
$$\Phi_A : F^r \to V;$$
$$(\alpha_1, \ldots, \alpha_r) \mapsto \alpha_1\boldsymbol{v}_1 + \cdots + \alpha_r\boldsymbol{v}_r$$
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 $E \setminus \{\boldsymbol{e}\}$ 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:

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

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

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

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

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:

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

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

$\exists \boldsymbol{e} \in E \setminus M : \left( E \setminus \boldsymbol{e} \right) \cup \{\boldsymbol{w}\}$ 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 of its basis.

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

## 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:

$$\dim(U + W) + \dim(U \cap W)$$
$$= \dim(U) + \dim(W)$$

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 $f : V \to W$ 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. Given 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 direct sum of vector subspaces is bijective:

$$\oplus : V_1 \times V_2 \to V; (\boldsymbol{v}_1, \boldsymbol{v}_2) \mapsto \boldsymbol{v}_1 + \boldsymbol{v}_2.$$

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:

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

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

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

## 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 $g \circ f = \text{id}_V$. i.e. it has a **left inverse**.

2. If $f$ is surjective, there exists map $g : W \to V$ such that $f \circ g = \text{id}_W$. 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:

$$\text{im}(f) := f(V)$$
$$= \{\boldsymbol{w} \in W : \forall \boldsymbol{v} \in V; \boldsymbol{w} = f(\boldsymbol{v})\}$$

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 a vector subspace of $V$.

$\boldsymbol{0} = e_H$ for group homomorphisms.

## 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:

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

### T2.1.1: Matrix mappings

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

Then there exists a <u>bijection</u>:

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

$$f \mapsto [f]$$

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

### Remark

The set of $n \times m$ matrices in $F$ is defined:

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

i.e. matrices with $n$ rows and $m$ columns.

### D2.1.6: Matrix products

The product $A \circ B = AB$ for $A$ is $n \times m$, $B$ is $m \times \ell$ and $AB$ is $n \times \ell$ is defined as:

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

with the following 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 $A, A'$ 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 <u>product</u> of elementary matrices.

### D2.2.4: Smith normal form

Matrices with **only** non-zero entries along the diagonal are in Smith normal form:

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

### T2.2.5

Let $A$ be an $n \times m$ matrix. Then:

$$PAQ \text{ is of Smith normal form}$$

where $P$ and $Q$ are invertible.

### Remark

$\mathrm{rank}(A) = \mathrm{rank}(PAQ)$.

### 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 $A$ be $n \times m$ with entries in $F$.
$A$ is **full rank** if $\mathrm{rank}(A) = \min(m, n)$.

Let $A = [a]$ with mapping $a : F^m \to F^n$. Then $\dim\big(\mathrm{im}(a)\big) := \mathrm{rank}(A)$.

### T2.3.1: Representing matrices

Let $V$ and $W$ be $F$-vector spaces with bases $A = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ s.t. $\langle A \rangle = V$ and $B = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ s.t. $\langle B \rangle = W$.

Then for every linear map $f : V \to W$ there exists a **representing matrix**:

$$(_B[f]_A)_{ij} = a_{ij}$$

$$f(\boldsymbol{v}_j) = a_{1j}\boldsymbol{w}_1 + \cdots + a_{nj}\boldsymbol{w}_n \in W$$

which produces the following bijection:

$$M_B^A : \hom_F(V, W) \to \mathrm{mat}(n \times m; F);$$

$$f \mapsto {}_B[f]_A$$

and $M_B^A(f) = {}_B[f]_A$ is the representing matrix of linear mapping $f$ with respect to bases $A$ and $B$.

If $A$ and $B$ are standard bases then $[f]$.

### T2.3.2

Let $U, V, W$ be $F$-vector spaces with finite dimension and bases $A, B, C$ respectively.

If $f : U \to V$ and $g : V \to W$ are linear mappings then $_C[g \circ f]_A = {}_C[g]_B \circ {}_B[g]_A$.

### D2.3.3: Vector representations

Let $V$ be a finite dimensional vector space with basis $A = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$. Then:

$$\Phi_A^{-1} : V \to F^r; \boldsymbol{v} \mapsto {}_A[\boldsymbol{v}]$$

is a bijection and the column vector $_A[\boldsymbol{v}]$ is known as the <span style="color:red">representation of vector $\boldsymbol{v}$ with respect to basis $A$</span>.

### T2.3.4

Let $V, W$ be finite dimensional $F$-vector spaces with bases $A$ and $B$ respectively.

Let $f : V \to W$ be a linear mapping. Then $_B[f(\boldsymbol{v})] = {}_B[f]_A \circ {}_A[\boldsymbol{v}]$ for $\forall \boldsymbol{v} \in V$.

### D2.4.1

Let $V$ be a $F$-vector space and let sets $A = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ and $B = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ be bases of $V$. The representation matrix of the identity mapping:

$$\mathrm{id}_V : V \to V; \boldsymbol{v} \mapsto \boldsymbol{v}$$

is a **change of basis matrix** $_B[\mathrm{id}_V]_A$ with entries $a_{ij}$ given by definition:

$$\boldsymbol{v}_j = \sum_{i=1}^{n} a_{ij}\boldsymbol{w}_i.$$

### T2.4.3: Change of basis

Let $V$ and $W$ be finite dimensional vector spaces with linear mapping $f : V \to W$. Let $A, A'$ be ordered bases of $V$ and $B, B'$ be ordered bases of $W$. Then:

$$_{B'}[f]_{A'} = {}_{B'}[\mathrm{id}_W]_B \circ {}_B[f]_A \circ {}_A[\mathrm{id}_V]_{A'}.$$

### C2.4.4

Let $V$ be a finite dimensional vector space and let $f : V \to V$ be an endomorphism. Let $A, A'$ be bases of $V$. Then:

$$_{A'}[f]_{A'} = {}_A[\mathrm{id}_V]_{A'}^{-1} \circ {}_A[f]_A \circ {}_A[\mathrm{id}_V]_{A'}.$$

### T2.4.5

Let $V$ and $W$ be finite dimensional vector spaces and let $f : V \to W$ be linear.

Then there exists a basis $A$ of $V$ and a basis $B$ of $W$ such that the representing matrix $_B[f]_A$ has nonzero entries only on the diagonal.

### D2.4.6: Trace

The trace of a $n \times n$ matrix $A$ is the sum of its diagonal entries:

$$\text{tr}(A) = \sum_{i=1}^{n} a_{ii}.$$

### D3.1.1: Rings

A **ring** $R$ is a set equipped with <u>addition</u> and <u>multiplication</u> that satisfy:

1. $(R, +)$ is an **Abelian group** with additive identity $0_R \in R$.

2. $(R, \cdot)$ is a **monoid**, meaning that:

   $$(\cdot) : R \times R \to R; (a, b) \mapsto a \cdot b$$

   is associative with identity element $1 = 1_R \in R$ such that:

   $$\forall a, b, c \in R; (a \cdot b) \cdot c = a \cdot (b \cdot c),$$

   $$a \cdot 1 = 1 \cdot a = a$$

   yet $a \cdot b \neq b \cdot a$ in general.

3. Multiplication in $R$ with respect to addition is distributive:

   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

   $$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

   for $\forall a, b, c \in R$.

For **nonzero** rings $0_R \neq 1_R$.

**Division rings** are rings where nonzero elements have multiplicative inverses.

### P3.1.7

A natural number is divisible by 3 if the sum of its digits is divisble by 3.

### D3.1.8: Fields

A **field** $F$ is a nonzero commutative ring with **multiplicative** inverses to every <u>nonzero</u> element:

$$\forall a \in F; \exists a^{-1} \in F : aa^{-1} = a^{-1}a = 1.$$

i.e. a commutative division ring.

### P3.1.11

$\mathbb{Z}/m\mathbb{Z}$ is a field **iff** $m$ is prime.

### L3.2.1

Let $R$ be a ring and $a, b \in R$. Then:

1. $0a = a0 = 0$

2. $(-a)b = -(ab) = a(-b)$

3. $(-a)(-b) = ab$.

### D3.2.3

Let $m \in \mathbb{Z}$. Then $m$th multiple $ma$ of $a \in (R, +)$ is $ma = \underbrace{a + \cdots + a}_{m \text{ times}}$ if $m > 0$.

$0a := 0$ and if $m < 0$, $(-m)a = -(ma)$.

### L3.2.4

Let $R$ be a ring where $a, b \in R$ and $m, n \in \mathbb{Z}$. Then:

1. $m(a + b) = ma + mb$

2. $(m + n)a = ma + na$

3. $m(na) = (mn)a$

4. $m(ab) = (ma)b = a(mb)$

5. $(ma)(nb) = (mn)(ab)$.

### D3.2.6: Units

Let $R$ be a ring. An element $r \in R$ is a **unit** if it has a multiplicative <u>inverse</u>:

$$\exists r^{-1} \in R : rr^{-1} = r^{-1}r = 1_R.$$

### P3.2.9: Group of units

$R^{\times}$ is the **set of units** in ring $R$ and forms a group under multiplication.

### D3.2.11: Divisor of zero

Let $r \neq 0_R \in R$ where $R$ is a ring. Then element $r$ is a **divisor of zero** if:

$$\exists s \in R : rs = 0_R \text{ or } sr = 0_R.$$

### D3.2.12: Integral domains

Intgeral domains are commutative rings with **no** divisors of zeros.

### P3.2.15: Cancellation law

Let $a, b, c \in R$ for $R$ is an integral domain. If $ab = ac$ and $a \neq 0$ then $b = c$.

### P3.2.16

Let $m \in \mathbb{N}$. Then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain **iff** $m$ is prime.

### T3.2.17

Every finite integral domain is a field.

### Remark

If $|R| < \infty$ then $f : R \to R$ is surjective.

### D3.3.2: Polynomial rings

$R[X]$ is a ring of polynomials over $R$ with zero and identity: $0, 1 \in R$. If $P \in R[X]$:

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

with $\deg(P) = m \geq 0$ and $a_i \in R$.

### L3.3.3

Let $R$ be a ring and let $P, Q \neq 0 \in R[X]$.

1. $\deg(PQ) = \deg(P) + \deg(Q)$

2. If $R$ is an integral domain then so is polynomial ring $R[X]$.

### T3.3.4

Let $R$ be an integral domain and let $P, Q \in R[X]$ where $\deg(Q) \leq \deg(P)$ and that polynomial $Q$ is a **monic**.

Then $\exists! A, B \in R[X] : P = AQ + B$ and either $\deg(B) < \deg(Q)$ or $B = 0$.

### Remark

A polynomial $Q$ is monic if:

$$Q = q_0 + \cdots + q_m X^m$$

where $q_m = 1$.

### D3.3.6

Let $R$ be a commutative ring and let $P \in R[X]$ be a polynomial. Then:

$$R[X] \to \text{maps}(R, R)$$

where we **evaluate** $P(\lambda)$ for $\lambda \in R$:

$$P(X) \mapsto \{P_\lambda : R \to R; \lambda \mapsto P(\lambda)\}.$$

If $P(\lambda) = 0$ then $\lambda$ is a **root** of $P$.

### P3.3.9

Let $R$ be a commutative ring, let $\lambda \in R$ and $P(X) \in R[X]$. Then $P(\lambda) = 0$ **iff**:

$$P(X) = (X - \lambda)Q(X)$$

where $Q(X) \in R[X]$.

### T3.3.10

Polynomial $P \neq 0 \in R[X] \setminus \{0\}$ has at most $\deg(P)$ roots in integral domain $R$.

### D3.3.11: Algebraically closed field

A field $F$ is algebraically closed if every $P \in F[X] \setminus F$ has a root in field $F$.

### T3.3.13: FTA

Field $\mathbb{C}$ is algebraically closed.

### T3.3.14

Let field $F$ be algebraically closed. Then every $P \in F[X] \setminus \{0\}$ decomposes into:

$$P = c(X - \lambda_1) \ldots (X - \lambda_n)$$

where $c \in F^\times$ and $\lambda_1, \ldots, \lambda_n \in F$.

### D3.4.1: Ring homomorphisms

Let $R$ and $S$ be rings. $f : R \to S$ is a ring homomorphism if for all $x, y \in R$:

$$f(x + y) = f(x) + f(y)$$

$$f(xy) = f(x)f(y).$$

### Remark

If $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism and $f(1) = x \in \mathbb{Z}/m\mathbb{Z}$ then:

1. $x^2 = x \pmod{n}$

2. $mx = 0 \pmod{n}$, with $\gcd(m, n)$ evenly spaced solutions.

### L3.4.5

Let $R$ and $S$ be rings. Let $f : R \to S$ be a **ring homomorphism**. Then for all $x, y \in R$ and $m \in \mathbb{Z}$:

1. $f(0_R) = 0_S$

2. $f(-x) = -f(x)$

3. $f(x - y) = f(x) - f(y)$

4. $f(mx) = mf(x)$

since $(R, +)$ is a group.

### D3.4.7: Ideals

Let $I \subset R$ where $R$ is a ring. Then $I$ is an **ideal** of ring $R$ if:

1. $I \neq \emptyset$ and $0_R \in I$

2. $I$ is closed under subtraction.

3. $\forall i \in I; \forall r \in R; ri, ir \in I$

and we denote $I \trianglelefteq R$.

### D3.4.11: Ideal of $R$ generated by $T$

Let $R$ be a commutative ring and $T \subset R$. Then the ideal of $R$ generated by $T$ is:

$$_R\langle T \rangle = \left\{ \sum_i r_i t_i : t_i \in T; \forall r_i \in R \right\}$$

where $i \in \{1, \ldots, m\}$ and $m \leq |T|$.

### P3.4.14

$_R\langle T \rangle$ is the smallest ideal containing $T$.

### D3.4.15: Principle ideal

An ideal of a commutative ring $R$ is the **principle ideal** if:

$$I = {}_R\langle t \rangle \text{ where } t \in R.$$

### P3.4.18

Let $f : R \to S$ be a ring homomorphism. Then $\ker(f)$ is an ideal of ring $R$ where:

$$\ker(f) = \{r \in R : f(r) = 0_S\}$$

and is a subgroup of $(R, +)$.

### L3.4.21 and L3.4.22

The set intersection and addition of ideals also form ideals.

### D3.4.23: Subrings

A subset $R' \subseteq R$ is a subring of ring $R$ if $R'$ also satisfies D3.1.1.

### P3.4.26: Subring test

$R' \subseteq R$ is a subring of $R$ **iff** $\forall a, b \in R'$:

1. $R'$ has multiplicative identity.

2. $a - b \in R'$

3. $ab, ba \in R'$

i.e. that $R'$ is closed under subtraction and multiplication.

### P3.4.28

Let $f : R \to S$ be a ring homomorphism.

1. If $R'$ is a subring of $R$ then $f(R')$ and $\operatorname{im}(f)$ are subrings of $S$.

2. Let $f(1_R) = 1_S$. Then:

$$x \in R^\times \implies f(x) \in S^\times.$$

### D3.5.1: Relations

A **relation** $R$ on set $X$ is a subset of $X \times X$. We denote $(x, y) = xRy \in X \times X$.

$R$ is an **equivalence relation** on set $X$ if $\forall x, y, z \in X$ the following is true:

1. Reflexive: $xRx$

2. Symmetric: $xRy \iff yRx$

3. Transitive: $(xRy \wedge yRz) \implies xRz$.

### D3.5.3: Equivalence classes

Let $\sim$ be an equivalence relation on $X$. Then the **equivalence class** of $x \in X$ is:

$$E(x) = \{z \in X : z \sim x\} \subseteq X$$

where an element of an equivalence class is a **representative** of the class.

### D3.5.5

Given an equivalence relation $\sim$ on set $X$, the **set of equivalence classes** is:

$$(X \setminus \sim) := \{E(x) : x \in X\} \subseteq \mathcal{P}(X).$$

We also define a surjective map:

$$\operatorname{can} : X \to (X/\sim); x \mapsto E(x)$$

known as the **canonical mapping**.

### Remark

A mapping $f : X \to Z$ is **well-defined** if there is an equivalence relation $\sim$ on $X$ such that $x \sim y \implies f(x) = f(y)$.

Then there exists a unique mapping $\overline{f}$:

$$\overline{f} : (X/\sim) \to Z; E(x) \mapsto f(x)$$

where $f = \overline{f} \circ \operatorname{can}$.

### D3.6.1: Cosets

Let $I$ be an ideal of ring $R$. Then:

$$x + I = \{x + i : i \in I\} \subseteq R$$

is the coset of $x$ with respect to $I$ in $R$.

### Remark

1. $x + I$ is both a left and right coset of $x$ since $(R, +)$ is Abelian.

2. Ideals of rings are subgroups.

### D3.6.3: Factor rings

Let $I$ be an ideal of ring $R$ and define an equivalence relation on $R$ where:

$$x \sim y \iff x - y \in I.$$

Then the **factor ring** of $R$ by $I$ is the set of cosets of $I$ in $R$ and denoted as $R/I$:

$$R/I = (R/\sim)$$

for each element is an equivalence class:

$$\begin{aligned} E(x) &= \{z \in R : z - x \in I\} \\ &= \{x + i \in R : i \in I\} \\ &= x + I. \end{aligned}$$

### T3.6.4

Let $I$ be an ideal of ring $R$. Then $R/I$ is a ring where $\forall x, y \in R$:

$$(x + I) \dot{+} (y + I) = (x + y) + I$$

$$(x + I) \cdot (y + I) = xy + I$$

where $x + I, y + I \in R/I$.

**T3.6.7**

Let $I$ be an ideal of ring $R$. Then:

1. can $: R \to R/I$ is a surjective ring homomorphism with kernel $I$.

2. Let $f : R \to S$ where $f(I) = \{0_S\}$ and that $f$ is a ring homomorphism.

   Then there is a unique $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \text{can}$ and that $\overline{f}$ is also a ring homomorphism.

$$
\begin{array}{ccc}
R & \xrightarrow{\ \text{can}\ } & R/I \\
 & \searrow{\scriptstyle f} & \Big\downarrow{\scriptstyle \overline{f}} \\
 & & S
\end{array}
$$

**T3.6.9: FIT for rings**

Every ring homomorphism $f : R \to S$ induces a ring isomorphism:

$$\overline{f} : R/\ker(f) \to \text{im}(f)$$

where $\overline{f}$ is a **bijection**. This is the first isomorphism theorem for rings.

**D3.7.1: Left modules**

A left module $M$ over a ring $R$ is a **pair** consisting of an Abelian group $(M, \dot{+})$ and the following mapping:

$$R \times M \to M; (r, a) \mapsto ra$$

such that $\forall r, s \in R$ and $\forall a, b \in M$:

$$r(a \dot{+} b) = (ra) \dot{+} (rb)$$

$$(r + s)a = (ra) \dot{+} (sa)$$

$$r(sa) = (rs)a$$

$$1_R a = a$$

also known as an $R$-**module**.

**L3.7.8**

Let $R$ be a ring and $M$ be a $R$-module. Then $\forall r \in R$ and $\forall a \in M$:

1. $0_R a = 0_M$
2. $r 0_M = 0_M$
3. $(-r)a = r(-a) = -(ra)$.

**D3.7.11: Module homomorphisms**

Let $R$ be a ring, $M$ and $N$ be $R$-modules. Then $f : M \to N$ is an $R$-homomorphism if $\forall r \in R$ and $\forall a, b \in M$:

$$f(a + b) = f(a) + f(b)$$

$$f(ra) = rf(a).$$

$f$ is an $R$-**isomorphism** if it is bijective and we denote that $M \cong N$.

**D3.7.15: Submodules**

$M' \subseteq M$ is a submodule if it also satisfies D3.7.11 but restricted to itself.

**P3.7.20: Submodule test**

Let $M$ be a $R$-module. $M'$ is a submodule of $M$ **iff** $\forall a, b \in M$ and $\forall r \in R$:

1. $0_M \in M'$
2. $a - b \in M'$
3. $ra \in M'$.

**L3.7.21**

Let $f : M \to N$ be an $R$-homomorphism. Then $\ker(f)$ and $\text{im}(f)$ are submodules.

**D3.7.23: Submodule generated by $T$**

Let $T \subseteq M$ for $M$ is a $R$-module. Then:

$$_R\langle T\rangle = \left\{ \sum_i r_i t_i : t_i \in T; \forall r_i \in R \right\}$$

where $i \in \{1, \dots, m\}$ and $m \le |T|$.

Module $N$ is **cyclic** if $N = {_R}\langle t\rangle$.

**L3.7.29 and L3.7.30**

Intersecting and adding collections of submodules also form submodules.

**D3.7.31: Factor modules**

Let $R$ be a ring, $M$ be a $R$-module and $N$ a submodule of $M$. Let $a \in M$. Then the **coset of $a$ with respect to $N$ in $M$** is:

$$a + N = \{a + b : b \in N\}$$

Every coset is an equivalent class of the following equivalence relation:

$$\forall a, b \in M; a \sim b \iff a - b \in N$$

and we define the **factor module** of $M$ by the submodule $N$ as:

$$M/N = (M/\sim)$$

with the following operators:

$$(a + N) \dot{+} (b + N) = (a + b) + N$$

$$r(a + N) = ra + N$$

and additive identity $0_{M/N} = 0_M + N$.

**T3.7.33: FIT for modules**

Let $M$ and $N$ be $R$-modules. Then every $R$-homomorphism $f : M \to N$ induces a $R$-isomorphism:

$$\overline{f} : M/\ker(f) \to \text{im}(f)$$

where $\overline{f}$ is a bijection.

**D4.1.1: Symmetric group $S_n$**

The set of bijections from $\{1, \dots, n\}$ to itself is a group under composition with $n!$ elements, denoted by $S_n$.

Each bijection $\sigma \in S_n$ is a **permutation**.

**Transpositions** are permutations that swap only two elements in $\{1, \dots, n\}$.

**D4.1.2: Inversions**

Given a permutation $\sigma \in S_n$, an inversion is a pair $(i, j)$ that is interchanged:

$$i < j \text{ and } \sigma(j) < \sigma(i)$$

where $i, j \in \{1, \dots, n\}$. The **length** of $\sigma$ is the number of inversions:

$$\ell(\sigma) := |\{(i, j) : i < j \text{ and } \sigma(j) < \sigma(i)\}|$$

or the number of crossings in a diagram. We define the **sign** of $\sigma$:

$$\text{sgn}(\sigma) = (-1)^{\ell(\sigma)} = \begin{cases} +1 & \text{even } \sigma \\ -1 & \text{odd } \sigma. \end{cases}$$

**Remark**

A cycle $(a_1 \dots a_r)$ sends each element to its right except $a_r$ which is sent to $a_1$.

$$(a_1 a_2 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)$$

Note that order may not be interchanged.

**D: Group homomorphisms**

Let $G$ and $H$ be groups. Then $f : G \to H$ is a group homomorphism if $\forall a, b \in G$:

$$f(ab) = f(a)f(b).$$

**L4.1.5**

sgn $: S_n \to \{+1, -1\}$, which is the sign of permutations, is a group homomorphism:

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$$

for all $\sigma, \tau \in S_n$.

**D4.1.6: Alternating groups**

The alternating group is a subgroup of $S_n$ and is the kernel of sgn function:

$$A_n := \ker(\text{sgn})$$
$$= \{\sigma \in S_n : \text{sgn} = e_{\{\pm 1\}} = +1\}.$$

**D4.2.1: Determinants**

Let $R$ be a commutative ring and $n \in \mathbb{N}$. Then the determinant map is defined as:

$$\det : \text{mat}(n \times n; R) \to R;$$

$$A \mapsto \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

where $(A)_{ij} = a_{ij}$.

### D4.3.1: Bilinear forms

Let $U, V$ and $W$ be $F$-vector spaces. Then a **bilinear form** on $U \times V$ with values in $W$ is the mapping $H : U \times V \to W$ where $\forall \boldsymbol{u}_1, \boldsymbol{u}_2 \in U$, $\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ and $\forall \lambda \in F$:

$$H(\boldsymbol{u}_1 + \boldsymbol{u}_2, \boldsymbol{v}_1) = H(\boldsymbol{u}_1, \boldsymbol{v}_1) + H(\boldsymbol{u}_2, \boldsymbol{v}_1)$$

$$H(\lambda\boldsymbol{u}_1, \boldsymbol{v}_1) = \lambda H(\boldsymbol{u}_1, \boldsymbol{v}_1)$$

$$H(\boldsymbol{u}_1, \boldsymbol{v}_1 + \boldsymbol{v}_2) = H(\boldsymbol{u}_1, \boldsymbol{v}_1) + H(\boldsymbol{u}_2, \boldsymbol{v}_2)$$

$$H(\boldsymbol{u}_1, \lambda\boldsymbol{u}_1) = \lambda H(\boldsymbol{v}_1, \boldsymbol{u}_1)$$

or that every entry of $H$ is <u>linear</u>.

Consider a bilinear form $H$ where:

$$H : U \times U \to W.$$

$H$ is **symmetric** if $H(\boldsymbol{u}, \boldsymbol{v}) = H(\boldsymbol{v}, \boldsymbol{u})$.

$H$ is **alternating** if $H(\boldsymbol{u}, \boldsymbol{u}) = 0$, and these must hold for all $\boldsymbol{u}, \boldsymbol{v} \in U$.

### Remark

A bilinear form $H$ that satisfies:

$$H(\boldsymbol{u}, \boldsymbol{u}) + H(\boldsymbol{u}, \boldsymbol{u}) = 0$$

is alternating provided $1_F + 1_F \neq 0_F$.

### D4.3.3: Multilinear forms

Let $V_1, \ldots, V_n, W$ be $F$-vector spaces. Then the map $H : V_1 \times \cdots \times V_n \to W$ is a **multilinear form** if every $V_j \to W$ is linear for all $\boldsymbol{m}_j \in V_j$.

$H$ is **alternating** if $\exists i \neq j : \boldsymbol{v}_i = \boldsymbol{v}_j$ and:

$$H(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_j, \ldots, \boldsymbol{v}_n) = 0.$$

### T4.3.6

Let $F$ be a field. Then the mapping:

$$\det : \mathrm{mat}(n \times n; F) \to F$$

is the unique alternating multilinear form on $n$-tuples of <u>ordered</u> column vectors of the matrix under mapping. Furthermore:

$$\det(I_n) = 1_F.$$

### T4.4.1

Let $A, B \in \mathrm{mat}(n \times n; R)$ where $R$ is a commutative ring. Then:

$$\det(AB) = \det(A)\det(B).$$

### T4.4.2

A square matrix $A$ with entries in a field $F$ *is invertible* **iff** $\det(A) \neq 0$.

### L4.4.4

Let $R$ be a commutative ring. Then: $\det\big(A^T\big) = \det(A)$ for $A \in \mathrm{mat}(n \times n; R)$.

### D4.4.6: Cofactors

Let $R$ be a commutative ring and that $A \in \mathrm{mat}(n \times n; R)$. Let $i, j \in \{1, \ldots, n\}$. We define a **cofactor** of $A$ as:

$$C_{ij} = (-1)^{i+j} \det(M_{ij})$$

where $M_{ij}$ is a *minor* of $A$, obtained from removing the $i^{\text{th}}$ row and $j^{\text{th}}$ column of $A$.

### T4.4.7: Laplace's expansion

Let $R$ be a commutative ring, $A = (a_{ij})$ where $A \in \mathrm{mat}(n \times n; R)$. Then:

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij} \quad (i^{\text{th}} \text{ row})$$

$$= \sum_{i=1}^{n} a_{ij} C_{ij}. \quad (j^{\text{th}} \text{ column})$$

### D4.4.8: Adjugate matrices

Let $R$ be a commutative ring and let $A \in \mathrm{mat}(n \times n; R)$. Then the **adjugate matrix** $\mathrm{adj}(A)$ is the $n \times n$ matrix where:

$$\mathrm{adj}(A)_{ij} = C_{ji}.$$

### T4.4.9: Cramer's rule

Let $R$ be a commutative ring and let $A \in \mathrm{mat}(n \times n; R)$. Then:

$$A \cdot \mathrm{adj}(A) = (\det A)I_n.$$

### C4.4.11

Let $R$ be a commutative ring and let $A \in \mathrm{mat}(n \times n; R)$. Then $A$ is *invertible* **iff** $\det(A) \in R^{\times}$.

### T4.4.14: Jacobi's formula

Let $A = (a_{ij})$ where $a_{ij} = a_{ij}(t)$. Then:

$$\frac{\mathrm{d}}{\mathrm{d}t} \det(A) = \mathrm{tr}(\mathrm{adj}\, A) \frac{\mathrm{d}A}{\mathrm{d}t}.$$

### D4.5.1: Eigenspaces

Let $f : V \to V$ be an endomorphism of $F$-vector space $V$. An **eigenvalue** $\lambda \in F$ of $f$ is a scalar such that $f(\boldsymbol{v}) = \lambda\boldsymbol{v}$ with eigenvector $\boldsymbol{v} \neq \boldsymbol{0}$. The **eigenspace** of map $f$ with eigenvalue $\lambda$ is defined as:

$$E(\lambda, f) = \{\boldsymbol{v} \in V : f(\boldsymbol{v}) = \lambda\boldsymbol{v}\}.$$

### T4.5.4

Let $V$ be a nonzero *finite* $F$-vector space where $F$ is an algebraically closed field. Then each endomorphism of the vector space $V$ has an eigenvalue.

### D4.5.6: Characteristic polynomials

Let $R$ be a commutative ring and let $A \in \mathrm{mat}(n \times n; R)$. The **characteristic polynomial** of matrix $A$ is defined as:

$$\chi_A(x) := \det(xI_n - A) \in R[x].$$

### T4.5.8

Let $F$ be a field and $A \in \mathrm{mat}(n \times n; F)$. Then the eigenvalues of the linear map $A : F^n \to F^n$ are the roots of $\chi_A$.

### P4.6.1: Triangularisability

Let $f : V \to V$ be an endomorphism of a *finite* $F$-vector space. Then the following two statements are equivalent:

1. Vector space $V$ has an *ordered* basis $B = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ such that:

$$f(\boldsymbol{v}_1) = a_{11}\boldsymbol{v}_1$$
$$\cdots$$
$$f(\boldsymbol{v}_n) = a_{1n}\boldsymbol{v}_1 + \cdots + a_{nn}\boldsymbol{v}_n$$

or that its representation matrix is:

$$_B[f]_B = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{nn} \end{pmatrix}.$$

i.e. $f$ is **triangularisable**.

2. $\chi_f(x)$ may be written as a *product of linear factors* in $F[x]$.

### D4.6.6

Consider an endomorphism $f : V \to V$ where $V$ is a $F$-vector space. Then $f$ is **diagonalisable** if the set of eigenvectos of $f$ forms a basis of $V$.

If $V$ is finite dimensional then there exists an *ordered* basis $B$ such that $_B[f]_B$ is a <u>diagonal matrix</u> of eigenvalues.

A square matrix $A \in \mathrm{mat}(n \times n; F)$ is diagonalisable if its corresponding linear map is diagonalisable. This implies that $A$ is conjugate to a diagonal matrix.

### T4.6.10: Cayley-Hamilton

Let $R$ be a commutative ring and let $A \in \mathrm{mat}(n \times n; R)$. Then $\chi_A(x = A) = 0$.

### D4.7.5: Markov matrices

A **Markov matrix** $M$ has non-negative entries, and every column sums to 1.

**L4.7.6**

**T4.7.10**

**D5.1.1: Inner product spaces**

real and complex

**D5.1.5: Inner product norm**

**D5.1.7: Orthonormal family**

include explicit calculation

**T5.1.10**

**D5.2.1**

**P5.2.2**

**D5.2.3: Orthogonal projections**

**P5.2.4**

**T5.2.5: Cauchy-Schwarz**

**C5.2.6**

**T5.2.7**

**Remark: Gram-Schmidt**