

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

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

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

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

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

### Remark

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

1.  $0v = 0$
2.  $(-1)v = -v$
3.  $\lambda 0 = 0$  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  $0 \in U$ .
2. Let  $u, v \in U$  and  $\lambda \in F$ . Then  $u + v \in U$  and  $\lambda u \in U$ .

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:

$$\begin{aligned} \alpha_1 v_1 + \dots + \alpha_r v_r &= 0 \\ \implies \alpha_1 = \dots = \alpha_r &= 0 \end{aligned}$$

for  $v_i \in L$  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: Basis evaluation mappings

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

Then  $A = \{v_1, \dots, v_r\}$  is a basis of  $V$  **iff** the following **evaluation mapping**:

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

$$(\alpha_1, \dots, \alpha_r) \mapsto \alpha_1 v_1 + \dots + \alpha_r v_r$$

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

**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**

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

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

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:

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

**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 **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**

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

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

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

**T2.3.1: Representing matrices**

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

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

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

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

which produces the following bijection:

$$M_B^A : \operatorname{hom}_F(V, W) \rightarrow \operatorname{mat}(n \times m; F);$$

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

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

**D2.3.3: Vector representations**

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

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

is a bijection and the column vector  ${}_A[\mathbf{v}]$  is known as the **representation of vector  $\mathbf{v}$  with respect to basis  $A$** .

**T2.3.4**

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

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

**D2.4.1**

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

$$\operatorname{id}_V : V \rightarrow V; \mathbf{v} \mapsto \mathbf{v}$$

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

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

**T2.4.3: Change of basis**

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

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

**C2.4.4**

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

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

**T2.4.5**

Let  $V$  and  $W$  be finite dimensional vector spaces and let  $f : V \rightarrow W$  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 addition and multiplication that satisfy:

1.  $(R, +)$  is an **Abelian group** with additive identity  $0_R \in R$ .
2.  $(R, \cdot)$  is a **monoid**, meaning that:

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

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 divisible by 3.

**D3.1.8: Fields**

A **field**  $F$  is a nonzero **commutative** ring with **multiplicative** inverses to every **nonzero** 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 inverse**:

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

**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**

Integral 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  $f : R \rightarrow R$  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  $P \in R[X]$ :

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

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:

$$Q = q_0 + \cdots + q_mX^m$$

where  $q_m = 1$ .

**D3.3.6**

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

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

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

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

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:

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

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

**D3.4.1: Ring homomorphisms**

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

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

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

**L3.4.5**

Let  $R$  and  $S$  be rings. Let  $f : R \rightarrow S$  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  $i \in \{1, \dots, m\}$  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  $f : R \rightarrow S$  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  $f : R \rightarrow S$  be a ring homomorphism.

1. If  $R'$  is a subring of  $R$  then  $f(R')$  and  $\text{im}(f)$  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:

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

We also define a **surjective** map:

$$\text{can} : X \rightarrow (X/\sim); x \mapsto E(x)$$

known as the **canonical mapping**.

**Remark**

A mapping  $f : X \rightarrow Z$  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  $\bar{f}$ :

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

where  $f = \bar{f} \circ \text{can}$ .

**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  $\forall x, y \in R$ :

$$(x + I) + (y + I) = (x + y) + I$$

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

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

**T3.6.7**

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

1.  $\text{can} : R \rightarrow R/I$  is a surjective ring homomorphism with kernel  $I$ .
2. Let  $f : R \rightarrow S$  where  $f(I) = \{0_S\}$  and that  $f$  is a ring homomorphism.

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

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

**T3.6.9: FIT for rings**

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

$$\bar{f} : R/\ker(f) \rightarrow \text{im}(f)$$

where  $\bar{f}$  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**  $(M, +)$  and the following mapping:

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

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

$$r(a + b) = (ra) + (rb)$$

$$(r + s)a = (ra) + (sa)$$

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

$$1_R a = a$$

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  $f : M \rightarrow N$  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 bijjective 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.  $ra \in M'$ .