

# Mathematics

P. Tansuntorn

Last updated July 11, 2019



# Contents

<b>I</b>	<b>Part IA</b>	<b>1</b>
<b>1</b>	<b>Numbers and Sets</b>	<b>3</b>
<b>2</b>	<b>Groups</b>	<b>5</b>
2.1	Examples of Groups . . . . .	5
2.1.1	Axioms for groups . . . . .	5
2.1.2	Examples from geometry . . . . .	6
2.1.3	Permutation on a set . . . . .	6
2.1.4	Subgroups and homomorphisms . . . . .	7
2.1.5	Symmetry groups . . . . .	8
2.1.6	The Möbius group . . . . .	8
2.2	Lagrange's Theorem . . . . .	10
2.2.1	Cosets . . . . .	10
2.2.2	Lagrange's theorem . . . . .	11
2.2.3	Group of small order (up to 8) . . . . .	11
2.2.4	Quaternions . . . . .	11
2.2.5	Fermat-Euler theorem . . . . .	11
2.3	Group actions . . . . .	11
2.3.1	Group actions . . . . .	12
2.3.2	Orbit-stabilizer theorem . . . . .	12
2.3.3	Cayley's theorem . . . . .	12
2.3.4	Conjugacy classes . . . . .	12
2.3.5	Cauchy's theorem . . . . .	12
2.4	Quotient groups . . . . .	12
2.4.1	Normal subgroups . . . . .	12
2.4.2	Quotient groups . . . . .	12
2.4.3	The isomorphism theorem . . . . .	12
2.5	Matrix groups . . . . .	12
2.5.1	The general and special linear groups . . . . .	12
2.5.2	The orthogonal and special orthogonal groups . . . . .	12
2.5.3	Basis change . . . . .	12
2.6	Permutations . . . . .	12
2.6.1	Permutations, Cycles and Transpositions . . . . .	12
2.6.2	Sign of Permutations . . . . .	14

2.6.3	Conjugacy in $S_n$ and $A_n$ . . . . .	14
2.6.4	Simple Groups . . . . .	14
<b>3</b>	<b>Vectors and Matrices</b>	<b>15</b>
3.1	Vectors . . . . .	15
3.1.1	Vector Algebra in $\mathbb{R}^3$ . . . . .	15
3.1.2	Vectors in $\mathbb{R}^n$ and $\mathbb{C}^n$ . . . . .	15
3.1.3	Concepts in linear algebra . . . . .	16
3.2	Matrices . . . . .	16
3.2.1	Algebra of Matrices . . . . .	16
3.2.2	Matrix as linear transformation . . . . .	16
3.3	Eigenvalues and Eigenvectors . . . . .	16
<b>4</b>	<b>Differential Equations</b>	<b>17</b>
4.1	Basic Calculus . . . . .	17
4.2	1st-order LDEs . . . . .	17
4.2.1	Equations with constant coefficients . . . . .	17
4.2.2	Equations with non-constant coefficients . . . . .	17
4.3	Nonlinear first-order equations . . . . .	17
4.4	Higher-order LDEs . . . . .	17
4.5	Multivariate Functions . . . . .	17
<b>5</b>	<b>Analysis I</b>	<b>19</b>
5.1	Limit and Convergences . . . . .	20
5.1.1	Series and sequences in $\mathbb{R}$ and $\mathbb{C}$ . . . . .	20
5.1.2	Sums, products and quotients . . . . .	21
5.1.3	Absolute convergence . . . . .	22
5.1.4	Bolzano-Weierstrass theorem . . . . .	22
5.1.5	Comparison and ratio test . . . . .	22
5.1.6	Alternating series test . . . . .	22
5.2	Continuity . . . . .	22
5.2.1	Continuity of real and complex function . . . . .	22
5.2.2	The intermediate value theorem . . . . .	22
5.3	Differentiability . . . . .	22
5.3.1	Differentiability of functions from $\mathbb{R}$ to $\mathbb{R}$ . . . . .	22
5.3.2	Derivative of sums and products . . . . .	22
5.4	Power series . . . . .	22
5.5	Integration . . . . .	22
5.5.1	Integrability of monotonic functions . . . . .	22
<b>6</b>	<b>Probability</b>	<b>23</b>
6.1	Basic concepts . . . . .	23
6.2	Axiomatic approach . . . . .	23
6.3	Discrete random variables . . . . .	23

6.4	Continuous random variables . . . . .	23
6.5	Inequalities and limits . . . . .	23
6.5.1	Markov's and Chebyshev's inequality . . . . .	23
6.5.2	Weak law of large numbers . . . . .	23
6.5.3	Convexity and Jensen's inequality . . . . .	23
6.5.4	AM-GM inequality . . . . .	23
<b>7</b>	<b>Vector Calculus</b>	<b>25</b>
7.1	Curves in $\mathbb{R}^3$ . . . . .	25
<b>II</b>	<b>Part IB</b>	<b>27</b>
<b>8</b>	<b>Linear Algebra</b>	<b>29</b>
8.1	Vector Spaces . . . . .	29
8.2	Linear maps . . . . .	29
8.3	Determinant . . . . .	29
8.4	Eigenvalues and Eigenvectors . . . . .	29
8.5	Duals . . . . .	29
8.6	Bilinear Forms . . . . .	29
8.7	Inner Product Spaces . . . . .	29
<b>9</b>	<b>Groups, Rings and Modules</b>	<b>31</b>
9.1	Groups . . . . .	31
9.1.1	Basics concepts . . . . .	31
9.1.2	Normal subgroups . . . . .	31
9.1.3	Sylow subgroups and Sylow theorems . . . . .	31
9.2	Rings . . . . .	31
9.2.1	Definition . . . . .	31
9.2.2	Ideals . . . . .	32
9.2.3	Fields . . . . .	32
9.2.4	Factorisation in rings . . . . .	32
9.2.5	Rings $\mathbb{Z}[a]$ of algebraic integers . . . . .	32
9.3	Modules . . . . .	32
9.3.1	Definition . . . . .	32
9.3.2	Submodules . . . . .	32
9.3.3	Equivalence of matrices . . . . .	32
9.3.4	Finitely generated modules over Euclidean domains . . . . .	32
<b>10</b>	<b>Analysis II</b>	<b>33</b>
10.1	Uniform Convergence . . . . .	33
10.2	Uniform Continuity and Integration . . . . .	33
10.3	$\mathbb{R}^n$ as a Normed Space . . . . .	33
10.4	Differentiation from $\mathbb{R}^m$ to $\mathbb{R}^n$ . . . . .	33

10.5	Metrice Spaces . . . . .	33
10.6	The Contraction Mapping Theorem . . . . .	33
<b>11</b>	<b>Metric and Topological Spaces</b>	<b>35</b>
11.1	Metrics . . . . .	35
11.1.1	Definition and examples . . . . .	35
11.1.2	Limits and continuity . . . . .	35
11.1.3	Open sets and neighbourhoods . . . . .	35
11.1.4	Characterising limits and continuity . . . . .	35
11.2	Topology . . . . .	35
11.2.1	Metric topologies . . . . .	35
11.3	Connectedness . . . . .	35
11.4	Compactness . . . . .	35
<b>12</b>	<b>Complex Analysis</b>	<b>37</b>
12.1	Analytic Functions . . . . .	37
12.2	Contour Integration and Cauchy's Theorem . . . . .	37
12.3	Expansions and Singularities . . . . .	37
12.4	The Residue Theorem . . . . .	37
<b>13</b>	<b>Complex Methods</b>	<b>39</b>
13.1	Analytic Functions . . . . .	39
13.2	Contour Integration and Cauchy's Theorem . . . . .	39
13.3	Residue Calculus . . . . .	39
13.4	Fourier and Laplace Transforms . . . . .	39
<b>14</b>	<b>Geometry</b>	<b>41</b>
<b>III</b>	<b>Part II</b>	<b>43</b>
<b>15</b>	<b>Number Theory</b>	<b>45</b>
15.1	Basics . . . . .	45
15.2	Chinese Remainder Theorem . . . . .	45
15.3	Law of Quadratic Reciprocity . . . . .	45
15.4	Binary Quadratic Forms . . . . .	45
15.5	Distribution of the Primes . . . . .	45
15.6	Continued fractions and Pell's equation . . . . .	45
15.7	Primality testing . . . . .	45
15.8	Factorisation . . . . .	45
<b>16</b>	<b>Topics in Analysis</b>	<b>47</b>
<b>17</b>	<b>Coding and Cryptography</b>	<b>49</b>

<b>18 Automata and Formal Languages</b>	<b>51</b>
18.1 Register machines . . . . .	51
18.2 Regular languages and finite-state automata . . . . .	51
18.3 Pushdown automata and context-free languages . . . . .	51
<b>19 Logic and Set Theory</b>	<b>53</b>
19.1 Ordinals and Cardinals . . . . .	53
19.1.1 Well-orderings and order-types . . . . .	53
19.2 Posets and Zorn’s Lemma . . . . .	53
19.3 Propositional Logic . . . . .	53
19.4 Predicate Logic . . . . .	53
19.5 Set Theory . . . . .	53
19.6 Consistency . . . . .	53
<b>20 Graph Theory</b>	<b>55</b>
20.1 Introduction . . . . .	55
20.2 Connectivity and matchinhs . . . . .	55
20.3 Extremal graph theory . . . . .	55
20.4 Eigenvalue methods . . . . .	55
20.5 Graph colouring . . . . .	55
20.6 Ramsey theory . . . . .	55
20.7 Probabilistic methods . . . . .	55
<b>21 Galois Theory</b>	<b>57</b>
21.1 Fields extensions . . . . .	57
<b>22 Representation Theory</b>	<b>59</b>
22.1 Representations of Finite Groups . . . . .	59
22.1.1 Representations on vector spaces . . . . .	59
22.2 Character Theory . . . . .	59
22.3 Arithmetic Properties of Characters . . . . .	59
22.4 Tensor Products . . . . .	59
22.5 Representations of $S^1$ and $SU_2$ . . . . .	59
22.6 Further Worked Examples . . . . .	59
<b>23 Number Fields</b>	<b>61</b>
23.1 Algebraic Number Fields . . . . .	61
23.2 Ideals . . . . .	61
23.3 Units . . . . .	61
23.4 Ideal classes . . . . .	61
23.5 Dedekind’s theorem on the factorisation of primes . . . . .	61

<b>24 Algebraic Topology</b>	<b>63</b>
24.1 The Fundamental Group . . . . .	63
24.2 Covering Spaces . . . . .	63
24.3 The Seifert-Van Kampen Theorem . . . . .	63
24.4 Simplicial Complexes . . . . .	63
24.5 Homology . . . . .	63
24.6 Homology Calculations . . . . .	63
<b>25 Linear Analysis</b>	<b>65</b>
<b>26 Analysis of Functions</b>	<b>67</b>
<b>27 Riemann Surfaces</b>	<b>69</b>
<b>28 Algebraic Geometry</b>	<b>71</b>
<b>29 Differential Geometry</b>	<b>73</b>
<b>30 Probability and Measure</b>	<b>75</b>



**Part I**

**Part IA**



# Chapter 1

## Numbers and Sets



# Chapter 2

## Groups

### 2.1 Examples of Groups

#### 2.1.1 Axioms for groups

**Definition 2.1.1.** A *group* is a set  $G$ , together with a binary operation  $*$  on  $G$  with the following properties.

1. (Closure axiom) for all  $g$  and  $h$  in  $G$ ,  $g * h \in G$ ;
2. (Associativity) for all  $f, g$  and  $h$  in  $G$ ,  $g * h \in G$ ,  $f * (g * h) = (f * g) * h$ ;
3. (Existence of identity) there is a unique  $e$  in  $G$  such that for all  $g$  in  $G$ ,  $g * e = g = e * g$ ;
4. (Existence of inverse) if  $g \in G$  there is some  $h$  in  $G$  such that  $g * h = e = h * g$ .

These results follow nicely.

**Lemma 2.1.1.** Let  $G$  be any group. Then, given  $g \in G$ , there is only one element  $h$  such that  $g * h = e = h * g$ . Particularly  $(g^{-1})^{-1} = g$ .

**Lemma 2.1.2** (Cancellation law). Suppose that  $a, b$  and  $x$  are in a group  $G$ . If  $a * x = b * x$  then  $a = b$ .

**Lemma 2.1.3.** Suppose that  $a$  and  $b$  are in a group  $G$ . Then the equation  $a * x = b$  has a unique solution  $x = a^{-1} * b$ .

**Lemma 2.1.4.** In any group  $G$ ,  $e$  is the unique solution of  $x * x = x$ .

Notice that we do not include the familiar assumption that  $f * g = g * f$  normally found in arithmetic. In fact, for some interesting groups this equality does not hold.

**Definition 2.1.2.** Let  $G$  be a group with respect to  $*$ . The elements  $f$  and  $g$  *commute* if  $f * g = g * f$ . We call  $G$  *abelian* if for all  $f$  and  $g$  in  $G$ , we have  $f * g = g * f$ .

We adopt the notation  $gh$  as equivalent to  $g * h$  for simplicity.

### 2.1.2 Examples from geometry

In this section we examine the idea of group in geometry, using polygons.

### 2.1.3 Permutation on a set

In this section we will show that permutations of a non-empty set  $X$ , in fact, form a group. We start with the definition of permutations acting on a set, although only for finite sets, before developing the idea further into arbitrary sets.

**Definition 2.1.3.** A *permutation*  $\alpha: X \rightarrow X$  is a bijection from  $X$  to itself. We say that  $\alpha$  acts on the set  $X$ . The set of all permutations of  $X$  is denoted  $\mathcal{P}(X)$ .

This set is indeed a group.

**Theorem 2.1.** The set  $\mathcal{P}(X)$  forms a group under composition of functions. We shall write  $\alpha\beta(x)$  in place of  $\alpha(\beta(x))$ .

*Proof.* We will show that all group axioms are satisfied.

1. It is obvious that if  $\alpha, \beta$  are permutations, then  $\alpha\beta$  is also a permutation. Thus the set  $\mathcal{P}(X)$  is closed under composition.
2. For any permutations  $\alpha, \beta, \gamma$ , let  $\mu = \alpha\beta$  and  $\nu = \beta\gamma$ . Then for every  $x$  in  $X$ ,

$$\begin{aligned}
 (\alpha(\beta\gamma))(x) &= (\alpha\nu)(x) \\
 &= \alpha(\nu(x)) \\
 &= \alpha(\beta(\gamma(x))) \\
 &= \mu(\gamma(x)) \\
 &= (\mu\gamma)(x) \\
 &= ((\alpha\beta)\gamma)(x).
 \end{aligned} \tag{2.1}$$

Thus the permutations are commutative under composition.

3. The identity permutation  $\iota(x) = x$  is the identity of  $\mathcal{P}(X)$ , since  $\alpha\iota(x) = \alpha(x) = \iota\alpha(x)$ .
4. For any element  $\alpha$  of  $X$ , the inverse is simply its functional inverse  $\alpha^{-1}$ . Direct verification shows that  $\alpha\alpha^{-1} = \iota = \alpha^{-1}\alpha$ .

□

The above proof lets us write  $\alpha\beta\gamma$  for any composition of three or more permutations without any confusion.

Setting  $X = \{1, \dots, n\}$ , the study of permutation groups is simpler. We shall give a name for such group.

**Definition 2.1.4.** The *symmetric group*  $S_n$  is a set of permutations of  $\{1, \dots, n\}$ . We say that the group is of degree  $n$ .

**Theorem 2.2.** The order of  $S_n$  is  $n!$ .

*Proof.* Evidently, there are  $n!$  permutations on a set with  $n$  elements. □

We now introduce a customary notation for permutation  $\rho(x)$  in the form

$$\rho = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \rho(1) & \rho(2) & \rho(3) & \cdots & \rho(n) \end{pmatrix},$$

which mean that the image of the permutation  $\rho(i)$  is underneath  $i$  in the first row. For example, let  $\alpha$  be a permutation on  $\{1, 2, 3, 4\}$  with  $\alpha(1) = 1, \alpha(2) = 4, \alpha(3) = 2$  and  $\alpha(4) = 3$ , then

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

**Example 2.1.1.** There are 6 permutations in  $S_3$ , they are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Note that

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Therefore  $S_3$  is not abelian. More generally  $S_n$  is not abelian for  $n \geq 3$ . We will study permutations in more details later on.

## 2.1.4 Subgroups and homomorphisms

**Definition 2.1.5.** A *subgroup* of a group  $G$  is a subset of  $G$  which itself form a group under the operation taken from  $G$ .

**Theorem 2.3.** Let  $H$  be a subgroup of  $G$ , then the identity element of  $H$  is that of  $G$ .

A group  $G$  always at least admits two subgroup, namely  $G$  and the singleton  $\{e\}$ . We call  $\{e\}$  the *trivial subgroup* of  $G$ , and we say that  $H$  is the *non-trivial subgroup* of  $G$  if  $H \neq \{e\}$ . We say that  $H$  is a *proper subgroup* of  $G$  if  $H \neq G$ .

We now give a test for a subset to be a subgroup.

**Theorem 2.4** (A test for subgroup). Let  $G$  be a group, and  $H$  be a non-empty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if

1. if  $g \in H$  and  $h \in H$ , then  $gh \in H$ , and
2. if  $g \in H$  then  $g^{-1} \in H$ .

Another test is similar and follows from the above theorem.

**Theorem 2.5.** Let  $G$  be a group, and  $H$  be a non-empty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if  $xy^{-1} \in H$  whenever  $x, y \in H$ .

The following property of the class of subsets of  $G$  is important.

**Theorem 2.6.** Let  $G$  be any group, then the intersection of any collection of subgroups of  $G$  is itself a subgroup of  $G$ .

*Proof.* Note that the intersection  $\cap_t H_t$  of the subgroups of  $G$ , defined as  $H_t$  for some  $t$  in the index set  $T$ , is not empty. Then for every elements  $g \in \cap_t H_t$  and  $h \in \cap_t H_t$ , they also lie in  $H_t$  for every  $t$ . And thus  $gh \in H_t$ , so  $gh \in \cap_t H_t$ . Any element  $g \in \cap_t H_t$  also has its inverse in every subgroup  $H_t$ . It then follows that  $g^{-1} \in \cap_t H_t$ . Therefore  $\cap_t H_t$  forms a subgroup under the operation of  $G$ .  $\square$

As a consequence, we see that for any non-empty subset  $G_0$  of  $G$ , we can consider the intersection of the collection of all subgroups  $H$  of  $G$  than contain  $G_0$ . The collection is not empty, since  $G$  is itself in the collection. It follows that the intersection is itself not empty, and is a subgroup of  $G$  that contain  $G_0$ . In fact, it is the *smallest subgroup* to contain  $G_0$ . This allows us to propose the next definition.

**Definition 2.1.6.** Let  $G_0$  be a non-empty subset of a group  $G$ . The subgroup of  $G$  *generated by*  $G_0$  is the smallest subgroup of  $G$  that contains  $G_0$ .

The idea of subgroup is expanded into the notion of a **coset**, which will be explored later.

**Definition 2.1.7.** Let  $G, G'$  be groups. A function  $\phi: G \rightarrow G'$  is a *homomorphism* if it takes the action of  $G$  to that of  $G'$ , namely

$$\phi(gh) = \phi(g)\phi(h),$$

for all  $g, h \in G$ .

## 2.1.5 Symmetry groups

### 2.1.6 The Möbius group

We first begin with the definition of Möbius transformation.

**Definition 2.1.8.** A *Möbius transformation* is a function  $f$  of a complex variable  $z$  in the form

$$f(z) = \frac{az + b}{cz + d},$$

for some complex numbers  $a, b, c$  and  $d$ , with the condition that  $ad - bc \neq 0$ .



The condition  $ad - bc \neq 0$  might not be obvious, but it follows from the fact that

$$f(z) - f(w) = \frac{(ad - bc)(z - w)}{(cz + d)(cw + d)}.$$

If  $ad - bc = 0$ , then  $f$  is constant. This also shows that  $f$  is injective.

This definition of the Möbius transformation has two problems. First, a Möbius transformation  $f$  is not unique. As for example, the 4-tuples  $(a, b, c, d)$  and  $(ma, mb, mc, md)$  with  $m \neq 0$  will all map a complex number  $z$  to a same number. Thus, given  $f$ , we *cannot* say what are the coefficients.

The second problem stems from the fact that, for example  $1/(z - z_0)$  is not defined at the point  $z_0$ . This means that there is no subset of  $\mathbb{C}$  on which all Möbius maps are defined.

Here is an example of this.

**Example 2.1.2.** Let  $f(z) = (z + 2)/z$  and  $g(z) = (z + 1)/(z - 1)$ . Then,

$$f(g(z)) = \frac{g(z) + 2}{g(z)} = \frac{(z + 1) + 2(z - 1)}{z + 1} = \frac{3z - 1}{z + 1},$$

so that  $fg$  fixes the point 1. However,  $g$  is not defined when  $z = 1$ . What's worse is that, if  $h(z) = 1/z$  then  $hfg(z) = (z + 1)/(3z - 1)$ , although  $g$  is not defined when  $z = 1$ ,  $fg(z)$  is not defined when  $z = -1$ , and  $hfg(z)$  is not defined when  $z = 1/3$ . More generally, a composition  $f_1 \cdots f_n$  of Möbius maps will not be defined at  $n$  distinct points in the complex plane.

The following theorem addresses the first problem.

**Theorem 2.7.** Suppose that  $a, b, c, d, \alpha, \beta, \gamma$  and  $\delta$  are complex numbers with  $(ad - bc)(\alpha\delta - \beta\gamma) \neq 0$ , and such that for at least three distinct values of  $z$  in  $\mathbb{C}$ ,  $cz + d \neq 0$ ,  $\gamma z + \delta \neq 0$ , and

$$\frac{az + b}{cz + d} = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Then there is some non-zero complex number  $\lambda$  such that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (2.2)$$

*Proof.* Consider the quadratic polynomial

$$(az + b)(\gamma z + \delta) = (\alpha z + \beta)(cz + d).$$

The polynomial has three distinct roots, and so it must be a zero polynomial. Therefore,  $a\gamma = c\alpha$ ,  $b\gamma + a\delta = c\beta + d\alpha$  and  $b\delta = d\beta$ , which is equivalent to

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix},$$

where  $\mu^2 = (ad - bc)(\alpha\delta - \beta\gamma) \neq 0$ . We then have

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{\mu}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

□

The first problem is then resolved by showing that the 4-tuple  $(a, b, c, d)$  determines  $f$ , up to non-zero multiple. The second problem will be resolved differently, by joining an extra point, which is called *the point at infinity* to  $\mathbb{C}$ . This point is denoted  $\infty$ .

## 2.2 Lagrange's Theorem

### 2.2.1 Cosets

We have introduced the idea of subgroup in the previous section. Now we come to the idea of constructing a subset of any group  $G$  from its subgroup. For example, we could define a new subset  $XY$  of  $G$  by

$$XY = \{xy : x \in X, y \in Y\}$$

for any subgroup  $X, Y$  of  $G$ . If  $X$  is a singleton, that is  $X = \{x\}$ , we shall adopt a notation  $XY = xY$ . Such constructions which we shall consider are of the form

$$gH = \{gh : h \in H\} \text{ or } Hg = \{hg : h \in H\}$$

for some  $g \in G$ , and  $H$  is a subgroup of  $G$ . The set  $gH$  is called the *left coset* of  $H$  with respect to  $g$ , similarly,  $Hg$  is the *right coset* of  $H$  with respect to  $g$ . Some constructions of this type might turn out to be the same set  $H$ . This is illustrated below.

**Theorem 2.8.** Let  $H$  be a subgroup of  $G$ , and  $g \in G$ . Then  $g \in H$  if and only if  $gH = H$  (or  $Hg = H$ ).

Thus we concern ourselves to the study of  $gH$  when  $g \notin H$ . We will adopt an additive notation  $g + H$  in place of  $gH$  when such subgroups employ addition. The next results show that a group can be divided into disjoint cosets. This is called the *coset decomposition* of  $G$ .

**Theorem 2.9.** Let  $H$  be a subgroup of a group  $G$ , then  $G$  is a union of its left (or right) cosets.

*Proof.* Clearly, for any  $g \in G$ ,  $g \in gH$ . So  $g$  is contained in the union. □

**Theorem 2.10.** Let  $H$  be a subgroup of a group  $G$ , then any two left cosets of  $G$  are either equal or disjoint.

*Proof.* Let  $f, g \in G$  and  $fH, gH$  are the two left cosets. Suppose that  $fH$  and  $gH$  are disjoint, that is, the set  $fH \cap gH$  is not empty. Then there exists an element  $x \in fH \cap gH$ , and so  $fy_1 = gy_2$  for some  $y_1, y_2 \in H$ . Thus  $g^{-1}f = y_2y_1^{-1} \in H$  and so  $g^{-1}fH = H$ ; hence  $gH = gg^{-1}fH = fH$ , hereby proving the theorem. □

**Corollary 2.2.1.** If  $fH = gH$ , then  $g^{-1}f \in H$ .

### 2.2.2 Lagrange's theorem

Recall the definition of an *order* of a group, denoted  $|G|$ . The next theorem shows the connection between the orders of a group and its subgroup.

**Theorem 2.11** (Lagrange's theorem). Let  $H$  be a subgroup of a finite group  $G$ . Then  $|H|$  divides  $|G|$ , and  $|G|/|H|$  is the number of distinct left (or right) cosets of  $H$  in  $G$ .

*Proof.* From the previous theorem we can write a group  $G$  as a union of the pairwise disjoint coset left of  $H$ . Therefore  $G = g_1H \cup g_2H \cup \cdots \cup g_rH$ . Consequently,

$$|G| = |g_1H| + |g_2H| + \cdots + |g_rH|.$$

It remains to show that  $|g_1H| = |g_2H| = \cdots = |g_rH| = |H|$ . Notice that the map  $x \mapsto g_jx$  is a bijection from  $H$  to  $g_jH$ , and so  $|g_1H| = |g_2H| = \cdots = |g_rH| = |H|$ . Therefore  $|G| = r|H|$  and the results follow.  $\square$

One of the corollary of Lagrange's theorem is the following result.

**Corollary 2.2.2.** Let  $g$  be an element of a finite group  $G$ . Then the order of  $g$  divides the order of  $G$ .

*Proof.* Let  $d$  be the order of  $g$ . The subgroup  $H = \{e, g, g^1, \dots, g^{d-1}\}$  is a subgroup of order  $d$ . By Lagrange's Theorem,  $|H| \mid |G|$ .  $\square$

### 2.2.3 Group of small order (up to 8)

### 2.2.4 Quaternions

### 2.2.5 Fermat-Euler theorem

## 2.3 Group actions

This section studies **group actions**.

**2.3.1 Group actions****2.3.2 Orbit-stabilizer theorem****2.3.3 Cayley's theorem****2.3.4 Conjugacy classes****2.3.5 Cauchy's theorem****2.4 Quotient groups****2.4.1 Normal subgroups****2.4.2 Quotient groups****2.4.3 The isomorphism theorem****2.5 Matrix groups****2.5.1 The general and special linear groups****2.5.2 The orthogonal and special orthogonal groups****2.5.3 Basis change****2.6 Permutations****2.6.1 Permutations, Cycles and Transpositions**

We have given the definition of permutations before.

**Definition 2.6.1.** Any permutations  $\alpha, \beta$  are said to be *disjoint* if, for every  $k$  in  $\{1, 2, \dots, n\}$ , either  $\alpha(k) = k$  or  $\beta(k) = k$ .

**Theorem 2.12.** Two permutations commute if they are disjoint.

*Proof.* Let the two permutations be  $\alpha$  and  $\beta$ . For any  $k \in \{1, \dots, n\}$ , suppose that  $\alpha$  fixes  $k$ , the case for  $\beta$  can be argued similarly.

Let  $\beta(k) = k'$ . Then  $\alpha\beta(k) = \alpha(k')$  and  $\beta\alpha(k) = \beta(k) = k'$ . We shall prove that indeed  $\alpha(k') = k$ .

If  $\beta(k') \neq k'$  then we are done by the premise. So suppose  $\beta(k') = k'$ , but then  $\beta(k') = k' = \beta(k)$ . This implies  $k = k'$  and so  $\alpha(k') = \alpha(k) = k'$  as required.  $\square$

We shall further simplify the notation, by introducing fixed points.

**Definition 2.6.2.** We call that  $k$  is a *fixed point* of  $\alpha$ , and that  $\alpha$  fixes  $k$ , if  $\alpha(k) = k$ .

And so, by convention, we shall left out any integers fixed by  $\alpha$ . For example, the permutation

$$\alpha = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$$

interchanges 1 and 3, and fixes 2. This notation is still too cumbersome for large  $n$ , this drives us to find a new notation. Let us start by noticing that, if we repeatedly apply any permutation  $\alpha$ , any elements in  $\{1, 2, \dots, n\}$  must eventually return. For example, let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix},$$

then  $\alpha^2(1) = 1, \alpha^3(2) = 1, \alpha^3(3) = 3, \alpha^3(4) = 4$  and  $\alpha^2(5) = 5$ . This is easily proven using the pigeonhole principle. Notice that 1 and 5 form a *cycle* between each other, as  $\alpha$  sends 1 to 5 and also send 5 to 1; this is also the case for 2, 3, 4. The permutation  $\alpha$  sends 2 to 3, 3 to 4, and 4 to 2. This is the motivation to define *cycles*.

**Definition 2.6.3.** A *cycle* between  $n_1, n_2, \dots, n_q$  is the permutation

$$\begin{pmatrix} n_1 & n_2 & \cdots & n_q \\ n_2 & n_3 & \cdots & n_1 \end{pmatrix}.$$

It is denoted by  $(n_1 n_2 \cdots n_q)$ . The cycle is said to be of length  $q$ .

The integers  $n_1, n_2, \dots, n_q$  need not be in an increasing order. By inspection,  $\alpha = (1\ 5)(2\ 3\ 4) = (2\ 3\ 4)(1\ 5)$ . We will show that any permutation can be written in this manner, as the compositions of cycles.

**Theorem 2.13.** Any permutation  $\alpha$  in the symmetric group  $S_n$  can be written as a composition of disjoint cycles.

*Proof.* This will employ the similar strategy used above. For any integer  $k \in \{1, \dots, n\}$ , we apply  $\alpha$  repeatedly, and so we have the sequence  $k, \alpha(k), \alpha^2(k), \dots$ , and so some elements of this sequence must coincide. Let the two such elements be  $\alpha^p(k) = \alpha^q(k)$ , with  $p < q$ . Thus  $\alpha^{q-p}(k) = k$ . Now there exists a smallest positive number  $u$  such that  $\alpha^u(k) = k$ .

The sequence  $k, \alpha(k), \alpha^2(k), \dots, \alpha^{u-1}(k)$  must be distinct. Construct the cycle

$$\gamma_k = (k, \alpha k, \alpha^2(k), \dots, \alpha^{u-1}(k)).$$

Now, two cycles are either disjoint or identical. For if  $y = \alpha^d(x)$  for some integer  $d$ , then  $\gamma_x = \gamma_y$ , and we say that  $x$  and  $y$  belong to the same cycle. Continue doing this for all elements of  $\{1, \dots, n\}$ , we will have a collection of cycles  $\{\gamma_{k_1}, \gamma_{k_2}, \dots, \gamma_{k_m}\}$ , all of them are pairwise disjoint.

Now consider the composition  $\gamma_{k_1} \gamma_{k_2} \cdots \gamma_{k_m}$ . For any  $x \in \{1, \dots, n\}$ , then  $\gamma_{k_d}(x) = \alpha(x)$  if  $x$  and  $k_d$  belong to the same cycle; else  $\gamma_{k_d}(x) = x$ . And so  $\alpha = \gamma_{k_1} \gamma_{k_2} \cdots \gamma_{k_m}$ .  $\square$

The proof above use the idea of constructing the sequence  $k, \alpha k, \alpha^2(k), \dots, \alpha^{u-1}(k)$  of elements of a group. This will be studied further in the notion of **orbits**. This decomposition is also unique up to the order of  $y_{k_i}$ , and it is called the *standard representation* of  $\alpha$ .

Let's try to decompose a permutation using the theorem. Consider

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 1 & 8 & 2 & 7 & 6 \end{pmatrix}$$

with  $\alpha \in S_8$ . The cycle formed by 1 is  $\gamma_1 = (134)$ . Continuing this, we have the collection  $\{(134), (2586), (7)\}$ , and the standard representation of  $\alpha$  is  $(1\ 3\ 4)(2\ 5\ 8\ 6)(7)$

Finally, consider a cycle  $\alpha$  of length  $n$ , then  $\alpha^n = \iota$ . Furthermore, for any positive integer  $d$ ,

$$\alpha^d = (\gamma_{k_1} \gamma_{k_2} \cdots \gamma_{k_m})^d = \gamma_{k_1}^d \gamma_{k_2}^d \cdots \gamma_{k_m}^d.$$

It follows that if  $d$  is the least common multiple of  $n_{k_1}, n_{k_2}, \dots, n_{k_m}$ , where  $n_{k_i}$  is the length of  $\gamma_{k_i}$ , then  $\alpha^d = \iota$ . The least common multiple is indeed the smallest positive integer with such property.

### 2.6.2 Sign of Permutations

### 2.6.3 Conjugacy in $S_n$ and $A_n$

### 2.6.4 Simple Groups

# Chapter 3

## Vectors and Matrices

### 3.1 Vectors

#### 3.1.1 Vector Algebra in $\mathbb{R}^3$

Combining two vectors

#### 3.1.2 Vectors in $\mathbb{R}^n$ and $\mathbb{C}^n$

Let us consider the vector in  $\mathbb{R}^n$ , the natural generalisation of  $\mathbb{R}^3$ .

**Definition 3.1.1.** Using the standard basis  $e_1, \dots, e_n$  of  $\mathbb{R}^n$ , if  $x = \sum_j x_j e_j$  and  $y = \sum_j y_j e_j$ , we write

$$x \cdot y = \sum_{j=1}^n x_j y_j, \|x\|^2 = x \cdot x = \sum_{j=1}^n x_j^2,$$

and  $x \perp y$  when  $x \cdot y = 0$ .

Note that  $\|x\| = \|-x\|$ . The distance  $\|x - y\|$  between the points  $x$  and  $y$  is given by the natural extension of Pythagoras' theorem, and importantly, satisfies the *triangle inequality*.

**Theorem 3.1** (The triangle inequality for  $\mathbb{R}^n$ ). For all  $x, y, z$  in  $\mathbb{R}^n$ ,

$$\|x - y\| \leq \|x - y\| + \|y - z\|. \quad (3.1)$$

To prove this assertion, it is sufficient to show that  $|x \cdot y| \leq \|x\| \|y\|$ , so that we have  $\|x + y\| \leq \|x\| + \|y\|$ , which readily implies the triangle inequality. Thus we seek to prove

**Theorem 3.2** (the Cauchy-Schwarz inequality). For all  $x, y \in \mathbb{R}^n$ ,

$$|x \cdot y| \leq \|x\| \|y\|. \quad (3.2)$$

The equality holds if and only if  $\|x\|y = \pm\|y\|x$ , i.e. one vector is a multiple of one another.

*Proof.* Let  $x = (x_1, \dots, x_n)$  and  $y = (y_1, \dots, y_n)$ . The equation holds true when  $x = 0$  and when  $y = 0$ . So we assume that  $\|x\|\|y\| > 0$ .

Consider the equation

$$0 \leq \sum_{j=1}^n (\|x\|y_j - \|y\|x_j)^2 = 2\|x\|\|y\| (\|x\|\|y\| - xy),$$

so  $x \cdot y \leq \|x\|\|y\|$ ; similarly, put  $-x$  as  $x$  and we have  $-x \cdot y \leq \|x\|\|y\|$ . Therefore  $|x \cdot y| \leq \|x\|\|y\|$ . Equality holds if  $\sum_{j=1}^n (\|x\|y_j - \|y\|x_j)^2$  or  $\sum_{j=1}^n (\|x\|y_j + \|y\|x_j)^2$  is equal to zero, which implies  $\|x\|y = \pm\|y\|x$ .  $\square$

### 3.1.3 Concepts in linear algebra

## 3.2 Matrices

**Definition 3.2.1.** An  $n \times m$  matrix is an array of numbers of the form

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

Sometimes it will be denoted by  $(a_{ij})$ , where  $a_{ij}$  is the general element of the matrix.

Notice that  $i$  is the *row* of the element, and  $j$  is the *column* of the element.

### 3.2.1 Algebra of Matrices

### 3.2.2 Matrix as linear transformation

We start with the definition of linear transformations.

**Definition 3.2.2.** A map  $\alpha: V \rightarrow W$  between vector spaces  $V$  and  $W$  is *linear* if, for all scalars  $\lambda_1, \dots, \lambda_n$ , and all vectors  $v_1, \dots, v_n$ ,

$$\alpha(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_1 \alpha(v_1) + \dots + \lambda_n \alpha(v_n).$$

If  $\alpha$  is linear we say that it is a *linear transformation*, or a *linear map*, if for all scalars  $\lambda$  and all vectors  $u$  and  $v$ ,  $\alpha(\lambda x) = \lambda \alpha(x)$  and  $\alpha(x + y) = \alpha(x) + \alpha(y)$ .

The two definitions are equivalent.

**Theorem 3.3** (Rank-nullity theorem). content...

## 3.3 Eigenvalues and Eigenvectors



# Chapter 4

## Differential Equations

### 4.1 Basic Calculus

### 4.2 First-order Linear Differential Equations

#### 4.2.1 Equations with constant coefficients

#### 4.2.2 Equations with non-constant coefficients

### 4.3 Nonlinear first-order equations

### 4.4 Higher-order Linear Differential Equations

### 4.5 Multivariate Functions



# Chapter 5

## Analysis I

A rigorous theory of mathematical analysis must take an axiomatic approach as its foundation. Thus it is preferable to start from the construction of real numbers, and then discover their properties, as not to take them for granted. This foundational rigour is, fortunately, available for us by Dedekind and his model for the real number.

What are the essential properties of  $\mathbb{R}$ ? We have learnt that  $\mathbb{R}$  is a field, with the usual addition and multiplication; the usual subtraction and division is also possible.

Secondly, there is a *total order* on  $\mathbb{R}$ , that is, if  $x, y \in \mathbb{R}$  then either  $x \leq y$  or  $y \leq x$ , and only  $x = y$  when both condition are satisfied. Furthermore, if  $x \leq y$  and  $y \leq z$  then  $x \leq z$ . This means  $\mathbb{R}$  is an *ordered field* and that is, if  $x \leq y$  then  $x + z \leq y + z$ , and if  $w \geq 0$  then  $xw \leq yw$ .

Of course,  $\mathbb{Q}$  is also an ordered field, but it is not *complete*. This is the most important property of  $\mathbb{R}$  to keep in mind. Let's start by a notion of an *upper bound*. If  $A$  is a non-empty subset of  $\mathbb{R}$  and  $b \in \mathbb{R}$ , then  $b$  is an upper bound for  $A$  if  $b \geq a$  for all  $a \in A$ . By saying that  $\mathbb{R}$  is complete, this means that, if  $A$  is a non-empty set of  $\mathbb{R}$  with an upper bound, then  $A$  has a *least upper bound*, or *supremum*  $\sup A$ . This translates to, for any upper bound  $b$  of a set  $A \subset \mathbb{R}$ , should it exist, we have  $\sup A \leq b$ .

Another central theme of analysis regards *absolute value*, that is the function

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ 0 & \text{if } x = 0 \\ -x & \text{if } x \leq 0 \end{cases} . \quad (5.1)$$

Note that  $|x - y| = |y - x|$  and  $|x| \geq 0$  for all  $x \in \mathbb{R}$ .

**Theorem 5.1.** For all  $x, y \in \mathbb{R}$ ,  $|x + y| \leq |x| + |y|$ , with equality when  $xy \geq 0$ .

*Proof.* Trivial proof by case. □

**Theorem 5.2.** (Triangle Inequality) For all  $x, y, z \in \mathbb{R}$ , we have

$$|x - z| \leq |x - y| + |y - z|. \quad (5.2)$$

*Proof.* Simply substitute  $x - y$  and  $y - z$  in place of  $x$  and  $y$ , respectively. □

## 5.1 Limit and Convergences

### 5.1.1 Series and sequences in $\mathbb{R}$ and $\mathbb{C}$

**Definition 5.1.1.** A sequence  $s_n$  is a *null sequence* if, to every positive number  $\epsilon$ , there corresponds an integer  $N$  such that

$$|s_n| < \epsilon \text{ for all values of } n \text{ greater than } N.$$

We can adapt the definition to any sequence whose terms approach any number  $s$ .

**Definition 5.1.2.** A sequence  $s_n$  is said to tend to the limit  $s$  if, given any positive number  $\epsilon$ , there is an integer  $N$  (depending on  $\epsilon$ ) such that

$$|s_n - s| < \epsilon \text{ for all } n > N.$$

We then write  $\lim s_n = s$ .

A more clear notation  $\lim_{n \rightarrow \infty} s_n = s$  can be given.

*Note.* 1. Clearly,  $\lim s_n = s$  if and only if  $s_n - s$  is a null sequence.

2. The inequality  $|s_n - s| < \epsilon$  is equivalent to the two inequalities

$$s - \epsilon < s_n < s + \epsilon.$$

This is clear that  $s_n$  is bounded.

3. A short notation  $s_n \rightarrow s$  stands for  $\lim s_n = s$ . A further symbolism for the above definition may be given:

$$s_n \rightarrow s \text{ if } \epsilon > 0; \quad \exists N. |s_n - s| < \epsilon \text{ for all } n > N.$$

If limits exist, they are unique.

**Theorem 5.3.** If  $a_n \rightarrow s$  as  $n \rightarrow \infty$  and  $a_n \rightarrow l$  as  $n \rightarrow \infty$ , then  $s = l$ .

*Proof.* We will prove this theorem by contradiction. Suppose  $s \neq l$ . Let  $\epsilon = |s - l|/3 > 0$ . There exists  $n_0$  such that  $|a_n - s| < \epsilon$  for  $n \geq n_0$ , and there exists  $m_0$  such that  $|a_n - l| < \epsilon$  for  $n \geq m_0$ . Let  $N = \max(n_0, m_0)$ . Then if  $n \geq N$ ,

$$|l - s| \leq |a_n - l| + |a_n - s| < 2\epsilon = 2|l - s|/3,$$

a contradiction. □

We have discussed on upper bound and lower bound of a set, it is time to introduce a notion of *boundedness*, and expand it to those of sequences in general.

**Definition 5.1.3.** A subset  $A$  of  $\mathbb{R}$  is *bounded* if it is bounded above and bounded below. A sequence  $s_n$  is bounded if the set  $\{s_n : n \in \mathbb{Z}^+\}$  is bounded.

**Theorem 5.4.** If a sequence tends to a limit, then it is bounded.

*Proof.* Let the sequence  $a_n$  tends to the limit  $l$ . We choose an arbitrary  $\epsilon$  so that for any  $n \geq n_0$  the difference  $|a_n - l|$  is less than  $\epsilon$ .

Let  $\epsilon = 1$ , so that  $|a_n - l| < 1$  for all  $n \geq n_0$ . Choose

$$M = \max\{|a_1|, |a_2|, \dots, |a_{n_0}|, |l| + 1\}.$$

Then for all  $n \geq n_0$   $|a_n| \leq |a_n - l| + |l| < 1 + |l|$ . Clearly,  $|a_n| \leq M$  and we are set.  $\square$

Note that the converse of the theorem might not be true; if a sequence is bounded, then it *might not* tends to a limit. Consider the sequence  $a_n = \cos n\pi$ . It is bounded, but  $a_n$  does not tend to a limit.

**Theorem 5.5.** Suppose that  $a_n$  is an increasing sequence of real numbers. If it is bounded then  $a_n \rightarrow \sup\{a_n : n \in \mathbb{Z}^+\}$  as  $n \rightarrow \infty$ ; otherwise  $a_n \rightarrow +\infty$ .

Similarly, for any decreasing sequence  $a_n$ ; and if it is bounded, then  $a_n \rightarrow \inf\{a_n : n \in \mathbb{Z}^+\}$ ; otherwise  $a_n \rightarrow -\infty$ .

One sequence worth considering is the sequence  $a_n = r^n$ . The convergence of the sequence depends on the value of  $r$ .

1. If  $r = 1$  then  $a_n \rightarrow 1$ , and if  $r = 0$  then  $a_n \rightarrow 0$ .
2. If  $r > 1$  then  $r = 1 + k$  for some  $k > 0$ , so we have

$$a_n = (1 + k)^n > 1 + kn$$

by considering the first two terms in the binomial expansion. And so  $a_n \rightarrow +\infty$ .

### 5.1.2 Sums, products and quotients

**Theorem 5.6.** If  $s_n$  and  $t_n$  are null sequences, so is  $s_n + t_n$ .

**Theorem 5.7.** If  $s_n$  is a null sequence and  $t_n$  is a bounded sequence, then  $s_n t_n$  is a null sequence.

**Corollary 5.1.1.** If  $s_n$  is a null sequence and  $c$  is a constant, then  $cs_n$  is a null sequence.

We then now extend the results to general sequences.

**Theorem 5.8.** If  $s_n \rightarrow s$  and  $t_n \rightarrow t$ , then

1.  $s_n + t_n \rightarrow s + t$ ,
2.  $s_n t_n \rightarrow st$ .

**Theorem 5.9.** If  $s_n \rightarrow s$  and  $t_n \rightarrow t$  with  $t \neq 0$ , then

$$\frac{s_n}{t_n} \rightarrow \frac{s}{t}$$

**Theorem 5.10.** If  $s_n \rightarrow s$  and  $t_n \rightarrow t$  and  $s_n \leq b_n$  for all  $n$ , then  $s \leq b$ .

**Theorem 5.11.** If  $s_n \rightarrow s$  and  $s_{n_k}$  is a subsequence, then  $s_{n_k} \rightarrow s$ .

### 5.1.3 Absolute convergence

### 5.1.4 Bolzano-Weierstrass theorem

**Theorem 5.12.** (Bolzano-Weierstrass theorem) Suppose that  $a_n$  is a bounded sequence of real numbers. There there is a subsequence  $a_{n_k}$  which converges.

### 5.1.5 Comparison and ratio test

### 5.1.6 Alternating series test

## 5.2 Continuity

### 5.2.1 Continuity of real and complex function

### 5.2.2 The intermediate value theorem

## 5.3 Differentiability

### 5.3.1 Differentiability of functions from $\mathbb{R}$ to $\mathbb{R}$

### 5.3.2 Derivative of sums and products

## 5.4 Power series

**Definition 5.4.1.** An infinite series of the form

$$\sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + a_2 z^2 + \cdots$$

composed of multiples of powers of  $z$  is called a *power series*. Both the variable  $z$  and the coefficients  $a_n$  might be real or complex.

There are three possibilities with convergence of a power series.

1. The series converges for all  $z \in \mathbb{C}$ .

## 5.5 Integration

### 5.5.1 Integrability of monotonic functions

# Chapter 6

## Probability

6.1 Basic concepts

6.2 Axiomatic approach

6.3 Discrete random variables

6.4 Continuous random variables

6.5 Inequalities and limits

6.5.1 Markov's and Chebyshev's inequality

6.5.2 Weak law of large numbers

6.5.3 Convexity and Jensen's inequality

6.5.4 AM-GM inequality





# Chapter 7

## Vector Calculus

### 7.1 Curves in $\mathbb{R}^3$



**Part II**

**Part IB**



# Chapter 8

## Linear Algebra

8.1 Vector Spaces

8.2 Linear maps

8.3 Determinant

8.4 Eigenvalues and Eigenvectors

8.5 Duals

8.6 Bilinear Forms

8.7 Inner Product Spaces



# Chapter 9

## Groups, Rings and Modules

### 9.1 Groups

We have gone into details of groups in Part IA.

#### 9.1.1 Basics concepts

#### 9.1.2 Normal subgroups

#### 9.1.3 Sylow subgroups and Sylow theorems

### 9.2 Rings

#### 9.2.1 Definition

Rings are abstraction of systems with addition and multiplication. The prototype of rings are the set  $\mathbb{Z}$  of integers.

We define the general notion of ring in a similar way. We say that a set  $R$  with two operations, addition and multiplication, denoted  $x + y$  and  $x \cdot y$ , respectively. We write  $x \cdot y$  as  $xy$  for comprehensiveness.

**Definition 9.2.1.** A set  $R$  is a ring if the following properties are satisfied:

1.  $R$  forms an abelian group under addition.
2.  $R$  forms a monoid under multiplication.
3. The distributive laws hold true, i.e.

$$x(y + z) = xy + xz, (y + z)x = yx + zx.$$

**9.2.2 Ideals****9.2.3 Fields****9.2.4 Factorisation in rings****9.2.5 Rings  $\mathbb{Z}[a]$  of algebraic integers****9.3 Modules****9.3.1 Definition****9.3.2 Submodules****9.3.3 Equivalence of matrices****9.3.4 Finitely generated modules over Euclidean domains**



# Chapter 10

## Analysis II

10.1 Uniform Convergence

10.2 Uniform Continuity and Integration

10.3  $\mathbb{R}^n$  as a Normed Space

10.4 Differentiation from  $\mathbb{R}^m$  to  $\mathbb{R}^n$

10.5 Metric Spaces

10.6 The Contraction Mapping Theorem



# Chapter 11

## Metric and Topological Spaces

### 11.1 Metrics

#### 11.1.1 Definition and examples

#### 11.1.2 Limits and continuity

#### 11.1.3 Open sets and neighbourhoods

#### 11.1.4 Characterising limits and continuity

### 11.2 Topology

#### 11.2.1 Metric topologies

### 11.3 Connectedness

### 11.4 Compactness



# Chapter 12

## Complex Analysis

12.1 Analytic Functions

12.2 Contour Integration and Cauchy's Theorem

12.3 Expansions and Singularities

12.4 The Residue Theorem



# Chapter 13

## Complex Methods

13.1 Analytic Functions

13.2 Contour Integration and Cauchy's Theorem

13.3 Residue Calculus

13.4 Fourier and Laplace Transforms





# Chapter 14

## Geometry



**Part III**

**Part II**



# Chapter 15

## Number Theory

15.1 Basics

15.2 Chinese Remainder Theorem

15.3 Law of Quadratic Reciprocity

15.4 Binary Quadratic Forms

15.5 Distribution of the Primes

15.6 Continued fractions and Pell's equation

15.7 Primality testing

15.8 Factorisation



## Chapter 16

### Topics in Analysis





# Chapter 17

## Coding and Cryptography



# Chapter 18

## Automata and Formal Languages

18.1 Register machines

18.2 Regular languages and finite-state automata

18.3 Pushdown automata and context-free languages



# Chapter 19

## Logic and Set Theory

### 19.1 Ordinals and Cardinals

#### 19.1.1 Well-orderings and order-types

### 19.2 Posets and Zorn's Lemma

### 19.3 Propositional Logic

### 19.4 Predicate Logic

### 19.5 Set Theory

### 19.6 Consistency



# Chapter 20

## Graph Theory

20.1 Introduction

20.2 Connectivity and matchings

20.3 Extremal graph theory

20.4 Eigenvalue methods

20.5 Graph colouring

20.6 Ramsey theory

20.7 Probabilistic methods





# Chapter 21

## Galois Theory

### 21.1 Fields extensions



# Chapter 22

## Representation Theory

### 22.1 Representations of Finite Groups

#### 22.1.1 Representations on vector spaces

### 22.2 Character Theory

### 22.3 Arithmetic Properties of Characters

### 22.4 Tensor Products

### 22.5 Representations of $S^1$ and $SU_2$

### 22.6 Further Worked Examples



# Chapter 23

## Number Fields

**23.1** Algebraic Number Fields

**23.2** Ideals

**23.3** Units

**23.4** Ideal classes

**23.5** Dedekind's theorem on the factorisation of primes



# Chapter 24

## Algebraic Topology

24.1 The Fundamental Group

24.2 Covering Spaces

24.3 The Seifert-Van Kampen Theorem

24.4 Simplicial Complexes

24.5 Homology

24.6 Homology Calculations





# Chapter 25

## Linear Analysis



## Chapter 26

# Analysis of Functions



# Chapter 27

## Riemann Surfaces



## Chapter 28

# Algebraic Geometry





## Chapter 29

# Differential Geometry



# Chapter 30

## Probability and Measure



# Index

Fixed point, 12

Group, 5

Symmetric group, 6