Lecture Notes on Algebra for MATH3208

Tsukasa Yashiro

Sultan Qaboos University
College of Science
Department of Mathematics and Statistics

Preface

These lecture notes algebra are written for classes of the course MATH3208 (Algebra and History of Mathematics) at Sultan Qaboos University. This course is designed for giving mathematical background to the future mathematics teachers in Oman.

Algebra appeared when people established the first civilization in Mesopotamia. They solved quadratic equations with geometric interpretation. In the Western culture, for thousand years, numbers were viewed as a geometric quantities such as the length of a line segment or the area and volumes of geometric objects. In fifteenth century Viète(1540-1603) introduced alphabetical letters as numbers. Although these letters were still connected with geometric meaning, it was a first time to introduce a generalized algebra. On the other hand, in the Eastern culture, numbers were free from the geometric interpretations.

As the notation was developed for describing mathematics, the theory of equation was developed. By the end of the 16th century, the formulea of polynomial equations of degree less than 5 had been discovered. However, finding formula for solving the fifth or higher degree polynomial equations had not been successful. In 19th century finally, Abel proved that it is impossible to find an algebraic formula. Galois went beyond Abel's proof and discovered the concept of a group. This discovery opened the door to the modern (abstract) algebra as well as it gives the base of modern mathematics.

The organization of these notes are the following. In Chapter 1 we briefly review the sets and functions. In Chapter 2 we introduce the algebraic structures such as groups, rings and fields. In Chapter 3 we construct natural numbers following the Peano's axioms. Then construct integers, rational numbers from natural numbers and finally we introduce real numbers as limits of rational Cauchy sequences. Chapter 4 discusses elementary number theory including modular arithmetic, primes, Euclidean algorithm and polynomials. Chapter 5 introduces Theory of Equations in which we learn quadratic equation, cubic equations and their formulae. Then we will see the Abel's impossible theorem. Chapter 6 discusses permutations and com-

binations. In Chapter 7, we learn multibase arithmetic and their additions, multiplications and divisions. Finally we discuss linear transformations on the plane including rotations, reflections etc. Appendices include Dedekind cuts and Pell's equation.

Contents

Chapter 1

Sets and Functions

Sets and functions are basic tools for modern mathematics. In this chapter we will learn the basic concepts of sets and functions.

1.1 Sets

Definition 1.1.1. A *set* is a collection of certainly defined objects. An *element* of a set is an object of the set.
If A and B are sets, then A is called a *subset* of B, written $A \subset B$ if, and only if, every element of A is also an element of B.
Let A and B be sets. A is a *proper subset* of B if and only if, $\forall x \in A$, $x \in B$ and $\exists y \in B$ such that $y \notin A$.
Let A and B be sets. $A = B$ if and only if $A \subset B$ and $B \subset A$.

1.2 Operations on Sets

Let A, B be subsets of U.

Definition 1.2.1.

1. The *union* of A and B, denoted $A \cup B$, is the set of all elements x in U such that $x \in A$ or $x \in B$.

2. The *intersection* of A and B, denoted $A \cap B$, is the set of all elements x in U such that $x \in A$ and $x \in B$.

3. The *difference* of B minus A (or *relative complement* of A in B), denoted $B - A$, is the set of all elements x in U such that x is in B and x is not in A.

4. The *complement* of A, denoted A^c, is the set of all elements in U such that $x \notin A$.

Symbolically:

$$\begin{aligned} A \cup B &= \{\, x \in U \mid x \in A \text{ or } x \in B \,\}, \\ A \cap B &= \{\, x \in U \mid x \in A \text{ and } x \in B \,\}, \\ B - A &= \{\, x \in U \mid x \in B \text{ and } x \notin A \,\}, \\ A^c &= \{\, x \in U \mid x \notin A \,\}. \end{aligned}$$

Definition 1.2.2. Two sets A and B are called disjoint if and only if $A \cap B = \emptyset$.

Definition 1.2.3. Sets $A_1, \ldots, A_n$ are mutually disjoint (or pairwise disjoint or nonoverlapping) if, and only if, no two sets A_i and A_j with distinct subscripts have any elements in common. More precisely, for all $i, j = 1, 2, \ldots, n$,

$$A_i \cap A_j = \emptyset \quad \text{whenever} \quad i \neq j.$$

Example 1.2.4. See Figure 1.1.

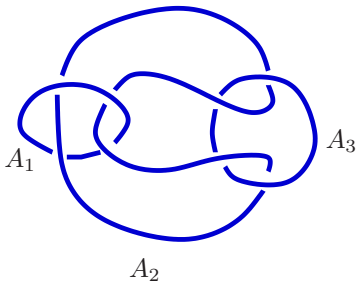


Figure 1.1: A_1, A_2 and A_3 are mutually disjoint.

Definition 1.2.5. A collection of nonempty sets $\{A_1, A_2, \ldots, A_n\}$ is a partition of A if, and only if,

1. $A = A_1 \cup A_2 \cup \cdots \cup A_n$;

2. $A_1, A_2, \ldots, A_n$ are mutually disjoint.

Example 1.2.6. $A_1 = \{(x_1, x_2) \in \mathbf{R}^2 \mid x_1^2 + x_2^2 < 1 \}$, $A_2 = \{(x_1, x_2) \in \mathbf{R}^2 \mid 1 \leq x_1^2 + x_2^2 < 4 \}$, $A_3 = \{(x_1, x_2) \in \mathbf{R}^2 \mid 4 \leq x_1^2 + x_2^2 \leq 9 \}$ and $D = \{(x_1, x_2) \in \mathbf{R}^2 \mid x_1^2 + x_2^2 \leq 9 \}$.
$D = A_1 \cup A_2 \cup A_3$, $A_i \cap A_j = \emptyset$ for $i \neq j$, $i, j \in \{1, 2, 3\}$ See Figure1.2.

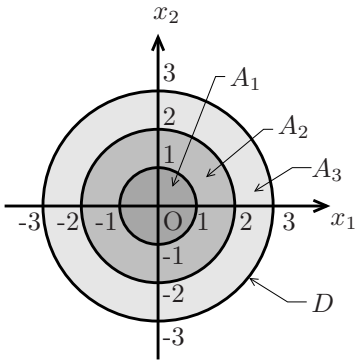


Figure 1.2: A partition of D.

Definition 1.2.7. Given a set A, the *power set* of A denoted $\mathcal{P}(A)$, is the set of all subset of A.

Example 1.2.8. $A = \{a, b, c\}$. The power set $\mathcal{P}(A)$ is $\{\emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$.

Definition 1.2.9. For two ordered n-tuples, $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$, $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$ if, and only if, $x_1 = y_1$, $x_2 = y_2, \ldots, x_n = y_n$.

Definition 1.2.10. Cartesian Product of A and B denoted $A \times B$ is the set:

$$A \times B = \{\ (a, b) \mid a \in A, b \in B\ \}$$

$$A_1 \times A_2 \times \cdots \times A_n = \{\ (a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots, n\ \}$$

1.3 Relations

BINARY RELATION

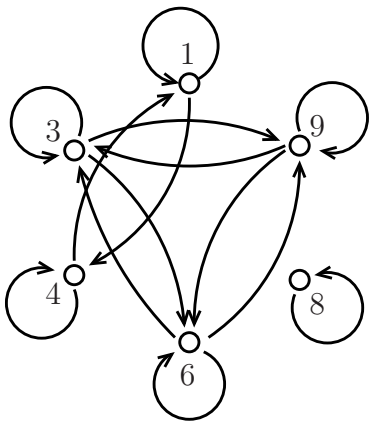
Let A and B be sets. A *relation* R from A to B is a subset of $A \times B$.

$$xRy \iff (x, y) \in R.$$

Example 1.3.1. $R = \{\ (x_1, x_2) \mid x_1^2 + x_2^2 = 1\ \}$ is a subset of $\mathbf{R}^2$. Thus it is a relation from $\mathbf{R}$ to $\mathbf{R}$.

A *binary relation* on a set A is a binary relation from A to A.

Example 1.3.2. A binary relation can be expressed by a directed graph
Let $A = \{\ 1, 3, 4, 6, 8, 9\ \}$. Define xRy by $3|(x - y)$.



EQUIVALENCE RELATION

Let R be a binary relation on A.

1. R is *reflexive* if, and only if, for all $x \in A$, xRx.
2. R is *symmetric* if, and only if, for all $x, y \in A$, if xRy, then yRx.
3. R is *transitive* if, and only if, for all $x, y, z \in A$, if xRy and yRz, then xRz.

If R satisfies all 1, 2 and 3 above, then R is called an *equivalence relation.*

In Example 1.3.2, the set A is divided into three subsets $\{1, 4\}$, $\{3, 6, 9\}$ and $\{8\}$. Each subset is called an equivalent class. The set of the classes under the equivalence relation is called a *quotient set.*

Example: For the set of natural numbers $\mathbf{N}$, "=" in usual sense is a binary relation and this is an equivalence relation.

Example: For $\mathbf{N}$, "$\leq$" in usual sense, is a binary relation but not an equivalent relation.

1.4 Functions

DEFINITION Let X and Y be sets. A *correspondence* or a *relation* is a subset of $X \times Y$.
A *function* $f : X \to Y$ is a correspondence such that if $(x, y), (x, y') \in f \subset$

$X \times Y$, then $y = y'$. We denote this relation $y = f(x)$. In other words, every $x \in X$ has a unique destination $f(x)$.
Let $f : X \to Y$ be a function. Then X is called the *domain* of f and Y is called the *co-domain* of f. Also the set of all $f(x)$ for all $x \in X$ is called the *image of X under f* or *range of f*.

$$\textit{image of } X \textit{ under } f = \textit{range of } f = \{\ y \in Y \mid y = f(x) \ \text{ for some } x \in X\ \}.$$

If $f(x) = y$, then x is called a *preimage of y* or an *inverse image of y*. The set of all inverse images of y is called the *inverse image of y*.

$$\textit{inverse image of } y = \{\ x \in X \mid f(x) = y\ \}.$$

We denote the inverse image of y by $f^{-1}(y)$.
Let $B \subset Y$, We define $f^{-1}(B)$ by the set of all $x \in X$ such that $f(x) \in B$:

$$f^{-1}(B) = \{\ x \mid f(x) \in B\ \}$$

Note that for a function $f : X \to Y$, there is a correspondence f^{-1} from $f(X) \subset Y$ to X. The correspondence f^{-1} is however not always a function.
Example 1. Let X and Y be sets. Let $f : X \to Y$ be a function.
Prove that for any subsets A, B of Y,

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

Solution.
For every $x \in f^{-1}(A \cap B)$,

$$\begin{aligned} f(x) \in A \cap B &\iff f(x) \in A \wedge f(x) \in B \\ &\iff x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

This shows that $f^{-1}(A \cap B) \subset f^{-1}(A) \cap f^{-1}(B)$.
For every $x \in f^{-1}(A) \cap f^{-1}(B)$,

$$\begin{aligned} f(x) \in A \wedge f(x) \in B &\iff f(x) \in A \cap B \\ &\iff x \in f^{-1}(A \cap B). \end{aligned}$$

This shows that $f^{-1}(A) \cap f^{-1}(B) \subset f^{-1}(A \cap B)$. Therefore, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
Definition. Injection, Surjection and Bijection Let X and Y be sets. A function $f : X \to Y$ is called an *injection* (one-to-one function) if for any $x, x' \in X$, if $f(x) = f(x')$, then $x = x'$.

A function $f : X \to Y$ is called a *surjection* (onto function) if for any $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

A function $f : X \to Y$ is called a *bijection* if the function is both injective and surjective.
Example 1. The function $\tan^{-1}(x)$ is a bijection from $\mathbf{R}$ to $(-\pi/2, \pi/2)$.

Proof. It is known that $(d/dx)\tan^{-1}(x) = \dfrac{1}{1+x^2} > 0$ for all $x \in \mathbf{R}$. This implies that $\tan^{-1}$ is a strictly increasing. Suppose that for $x, x' \in \mathbf{R}$ with $x < x'$, since $\tan^{-1}$ is strictly increasing, $\tan^{-1}(x) < \tan^{-1}(x')$. This shows that $\tan^{-1}$ is an injection.
For every $y \in (-\pi/2, \pi/2)$, $y = \tan^{-1}(x)$ has a solution $x = \tan(y)$. This shows that $\tan^{-1}$ is a surjection. □

Example 1.4.1. Prove that there exists a bijection between $\mathbf{R}$ and an interval $(0, 1)$.
Solution. We know that $\tan^{-1}(x)$ is a bijection from $\mathbf{R}$ to $(-\pi/2, \pi/2)$. We can define a bijection h from $(-\pi/2, \pi/2)$ to $(0, 1)$ by $h(x) = (1/\pi)x + 1/2$ for all $x \in (-\pi/2, \pi/2)$.
For $x, x' \in (-\pi/2, \pi/2)$ with $x \neq x'$, suppose $h(x) = h(x')$. Then $(1/\pi)x + 1/2 = (1/\pi)x' + 1/2$ and this implies that $x = x'$. Therefore, h is an injection.
For every $y \in (0, 1)$, $y = (1/\pi)x + 1/2$ can be solved for x. In fact, $x = \pi(y - 1/2)$. Therefore, h is a surjection.

The composite $h \circ (\tan^{-1})$ is a bijection. In the following X, Y and Z are sets.

Well Defined Function

When we define a function $f : X \to Y$ we have to check if $f(x)$ is uniquely determined for each $x \in X$. If so, we say the function is **well defined**.

Example 1.4.2. Consider the partition of $\mathbb{Z}$: $M_{3,i} = \{n \mid n = 3q + i\}$ for $i = 0, 1, 2$. Each $M_{3,i}$ is represented by an element j in $M_{3,i}$ denoted by $[j]$ for example, $[0] = [3] = [6]$. Let the set $X = Y = \{[0], [1], [2]\}$. Define $f; X \to Y$ by $f([i]) = [2i]$. We need to check if the function f is well defined.

Definition 1.4.3. Let $f : X \to Y$ and $g : Y \to Z$ be functions with $f(X) \subset Y$.
Define $g \circ f : X \to Z$ as follows:

$$(g \circ f)(x) = g(f(x)) \text{ for all } x \in X.$$

The function $g \circ f$ is called the *composition* of f and g.
If a function $f : X \to X$ send x to x itself, then f is called the **identity function** denoted by i_X.
For a function $f : X \to Y$, $(f \circ i_X)(x) = f(i_X(x)) = f(x)$.

If $f : X \to Y$ is a bijection with inverse function f^{-1}, then

1. $f^{-1} \circ f = i_X$,
2. $f \circ f^{-1} = i_Y$.

Let $f : X \to Y$ and let $g : Y \to Z$ be functions.

1. Prove that if $g \circ f$ is surjective, then g is surjective.
2. Prove that if $g \circ f$ is injective, then f is injective.

Cardinalities of Sets

It is possible that the number of elements of a finite set is generalized to infinite sets. Let A and B be sets. If there is a bijection between A and B, then the *cardinality* of A is equal to the cardinality of B. We write this as:

$$textbf{card}(A) = textbf{card}(B).$$

Floor and Ceiling Functions

Define $F : \mathbf{R} \to \mathbb{Z}$ by

$$F(x) = \lfloor x \rfloor = \text{ the greatest integer that is less than or equal to } x$$

This function is called the *floor function*.
Define $G : \mathbf{R} \to \mathbb{Z}$ by

$$G(x) = \lceil x \rceil = \text{ the least integer that is greater than or equal to } x$$

This function is called the *ceiling function*.

Exercies 1.4

---

1. $F(x) = 3x$ and $G(x) = \lfloor x/3 \rfloor$ for all real numbers x. Determine whether or not $F \circ G = G \circ F$.

2. Suppose $f : X \to Y$ and $g : Y \to Z$ are both bijective (one-to-one and onto). Prove that $(g \circ f)^{-1}$ exists and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

3. Let X and Y be sets. Let $f : X \to Y$ be a function.
   Prove that for subsets A, B of Y,

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B).$$

1.5 Basic Functions

There are very basic and common functions.

Function	The graph
$y = x$	The line with the slope 1 passing through the origin.
$y = x^2$	The parabola
$y = \dfrac{1}{x}$	The hyperbola with asymptotes $y = 0$ and $x = 0$.
$y = \sqrt{x}$	The graph of inverse function of $y = x^2$ with $x \geq 0$.

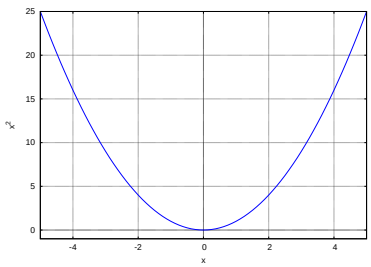


Figure 1.3: The graph of $y = x^2$.

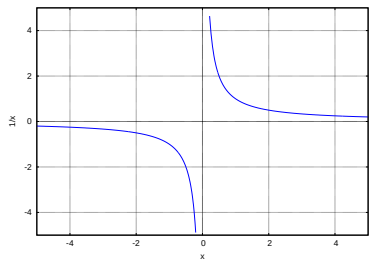


Figure 1.4: The graph of $y = 1/x$.

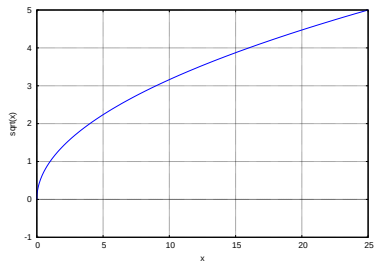


Figure 1.5: The graph of $y = \sqrt{x}$.

The graph of the function $y = f(x-a)+b$ is obtained by shifting the graph of $y = f(x)$ $|a|$ unites in the x-axis and $|b|$ units in the y-axis. Further if $a > 0$, the graph is shfted to the right and to the left if $a < 0$.
This is because the function is

$$y - b = f(x - a).$$

Let $Y = y - b$ and $X = x - a$. Then the function is

$$Y = f(X).$$

In the XY-plane, the origin $(0, 0)$ is (a, b) in the xy-plane. Therefore, the graph is obtained by shifting $y = f(x)$ to (a, b).

Example 1.5.1. The graph of $y = (x-2)+3$ is obtained by translating the graph of $y = x$ to $(2, -3)$.

Example 1.5.2. The graph of the function $y = e^{x+3} - 2$ is obtained by shifting the graph $y = e^x$ to $(-3, -2)$.

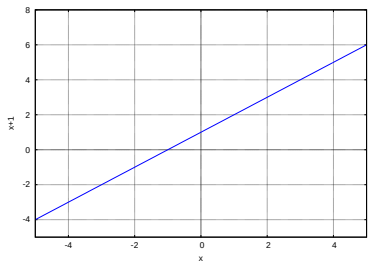


Figure 1.6: The graph of $y = (x - 2) + 3$.

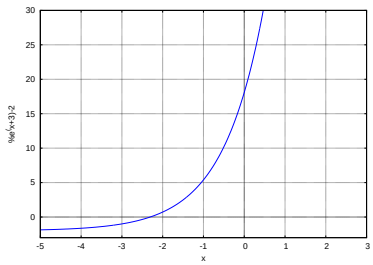


Figure 1.7: The graph of $y = e^{x+3} - 2$.

1.6 Inequalities

A line in the xy-plane is expressed by the function $y = mx + n$. The inequalities:

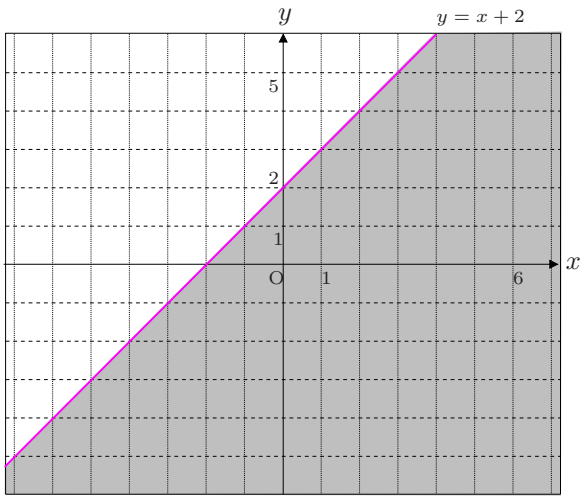
$$y > mx + n \tag{1.1}$$
$$y < mx + n \tag{1.2}$$

express the upper region and the lower region of the line $y = mx + n$.

Example 1.6.1. Draw the region given by $x - y + 2 \geq 0$

Solution. The given inequalty is $y \leq x + 2$. Thus the lower region of the

line $y = x + 2$ and the line itself.



Definition 1.6.2. A circle C with radius r centred at O is the set of points P such that $|OP| = r$:

$$C = \{P \mid |OP| = r\}.$$

This defintion induces the following expression. A circle in the xy-plane with radius r centred at (a, b) is the set expressed by

$$\{(x, y) \mid \sqrt{(x-a)^2 + (y-b)^2} = r\}.$$

Take square both sides of the condition to obtain:

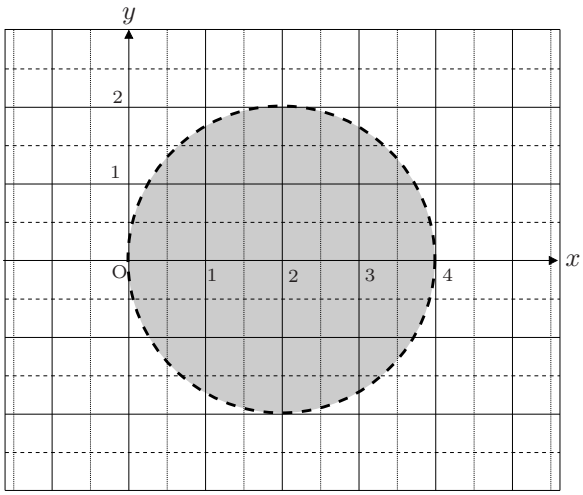
$$(x-a)^2 + (y-b)^2 = r^2$$

By the definition of a circle, the set of interior points of the circle is expressed by

$$(x-a)^2 + (y-b)^2 < r^2$$

Example 1.6.3. Draw the region given by $(x-2)^2 + y^2 < 4$

Solution.



Example 1.6.4. Draw the region expressed by the inequality.

$$(x + 2y - 1)(x - y + 1) > 0.$$

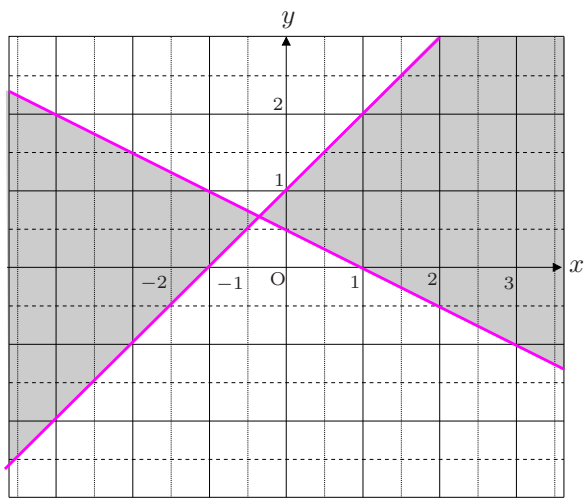
Solution. There are two cases.

$$\begin{aligned} x + 2y - 1 &> 0 \\ x - y + 1 &> 0 \end{aligned}$$

or

$$\begin{aligned} x + 2y - 1 &< 0 \\ x - y + 1 &< 0. \end{aligned}$$

Therefore, the region is the following.



Exercies 1.5- 1.6

---

1. Draw the graph of the following functions.
   (a) $f(x) = \sqrt{x-2}$ (b) $y = e^{x-1}$
   (c) $f(x) = x^2 - x + 2$ (d) $\frac{x^2}{4} + \frac{y^2}{9} = 1$
   (e) $f(x) = x + y = 1$ (f) $x^2 + (y-1)^2 = 16$

2. Draw the regions.
   (a) $y > 2x - 1$ (b) $3x + y - 1 \leq 0$
   (c) $(2x + 3y)(x^2 + (y+1)^2 - 1) \leq 0$ (d) $(x + y - 2)(3x - y + 2) < 0$

Chapter 2

Algebraic Structures

It is known that quadratic equations were solved by people in the ancient civilisations. For thousand years, the main topic in algebra is to find a formula of roots for polynomial equations. From the 16th century to the 18th century many mathematicians made a great effort to find formulae of polynomial equations. By the end of 18th century formulae for polynomial equations of degree up to four had been found. In the early 19th century two genius mathematicians appeared, Niels Henrik Abel (1802-1829) and Evariste Galois (1811-1832). Abel proved that there is no algebraic solution for a polynomial equation of degree greater than 4; that is, there is no general formula for these equations. While Galois independently reached a point beyond the main idea of Abel's proof; that is the discovery of the concept of groups. From this point algebra was changed from a subject to study equations to a subject to study algebraic structures. He opened the door to the modern mathematics.

2.1 Groups

We introduce a basic algebraic structure called a "group". This is a non-empty set with an associative binary operation and having the identity and inverse elements:

DEFINITION

A non-empty set G with an operation $*$ is a *group* if it satisfies the following axioms.

(G1) The operation $*$ is associative ($a*(b*c) = (a*b)*c$),

(G2) There is an element e in G such that $a*e = e*a = a$

(G3) For every element a in G, there is an element a^{-1} in G such that $a*a^{-1} = e$ and $a^{-1}*a = e$.

If only condition (G1) is satisfied, then $(G,*)$ is called a *semi-group* and if (G1) and (G2) are satisfied, then it is called a *monoid*.
If a group $(G,*)$ satisfies the commutative law, then it is called an *abelian group*.
The cardinality of a group G is called the *order* of G denoted by $|G|$.

Example 2.1.1.

1. $(\mathbb{Z},+)$ is a group under the usual addition as its operation.

2. Let $G = \{0,1,2\}$. The operation on G can be given by the operation table below. Under this operation $(G,*)$ is a group.

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3. The set of integers $(\mathbb{Z},+)$ is an abelian group.

4. The set of even integers is an commutative semi-group.

5. The set of permutations on the set $\{1,2,...,n\}$ is a group under the composition.

6. Let $\omega \neq 1$ be a root of $x^3 - 1 = 0$. Then $\{1,\omega,\omega^2\}$ is a group under the usual multiplication.

2.2 Symmetric groups

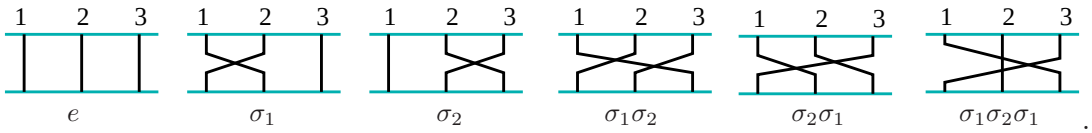
Let n be a positive number. Consider the set $\{1,2,\ldots,n\}$. The set of all permutations of this set will form a group called the extit symmetric group on n symbols (or "of degree n"). We denote this group by S_n.

Let $S = \{1, 2, 3\}$. Consider the operations that changes the order of the elements of S:

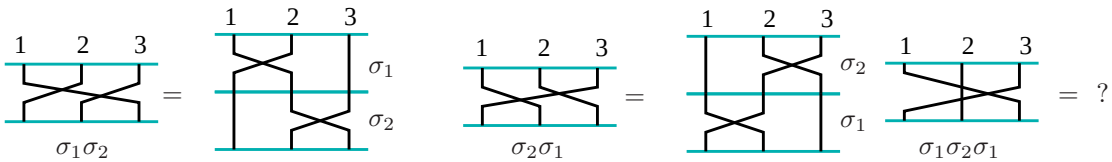
$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$
$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_1\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$S_3 = \{e, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1\}.$$

The set of these six operations forms a group:



We can see that $\sigma_1 \circ \sigma_1 = \sigma_1^2 = e$, $\sigma_2 \circ \sigma_2 = \sigma_2^2 = e$.



A permutation that exchanges only two terms, is called a *transposition*. Every permutation of degree n is expressed as a product of transpositions. If a permutation is expressed as a product of even number of transpositions, then it is called *even permutation*. If it is odd, then the permutation is called an *odd permutation*.
The set of even permutations of S_n is denoted by A_n.

Theorem 2.2.1. *A presentation of the symmetric group S_n is given by*

$$\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i^2 = 1, (\sigma_i\sigma_j)^3 = 1 \text{ if } |i-j| = 1, (\sigma_i\sigma_j)^2 = 1 \text{ if } |i-j| > 1 \rangle$$

See Appendix 1 for the proof of the theorem.

Exercises

1. Find $|S_3|$.
2. Find $|S_5|$.
3. Find $|S_n|$, $n \geq 3$.

2.3 Rings

For a group we consider only one binary operation. Here we consider a set with two kinds of binary operations.

DEFINITION

A non-empty set R with two operations $+$ and $*$ is a *ring* if it satisfies the following axioms.

(R1) $(R, +)$ is an abelian group.

(R2) For $a, b, c \in R$, $a*(b+c) = a*b+a*c$ and $(a+b)*c = a*c+b*c$.

(R3) $(R - \{0\}, *)$ is a semi-group.

If $a * b = b * a$ for all $a, b \in R$, then $(R, +, *)$ is called a *commutative ring.*

Definition 2.3.1. Let R be a ring. The element $a \in R$ is a *unit* if there is $a' \in R$ such that $a * a' = a' * a = e$, where e is the identity element.

Example 2.3.2. The set of integers with the usual addition and the usual multiplication: $(\mathbb{Z}, +, \times)$ is a commutative ring. $\mathbb{Z}$ has the identity 1 and the unit ± 1.

Example 2.3.3. $(\mathbf{Q}, +, \times)$ and $(\mathbf{R}, +, \times)$ are commutative ring. All non-zero elements of $\mathbf{Q}$ and $\mathbf{R}$ are units.

Definition 2.3.4. Let R be a commutative ring. A *polynomial* $p(X)$ over R is a linear sum in the form:

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

where $a_i \in R$ for $i = 0, 1, \ldots, n$ and $a_n \neq 0$.

Example 2.3.5. Let R be a commutative ring. Define $R[X]$ as the set of polynomials over R. Then $R[X]$ is a ring.

2.4 Fields

DEFINITION

A non-empty set F with two operations $+$ and $*$ is a *field* if it satisfies the following axioms.

(F1) $(F, +)$ is an abelian group.

(F2) For $a, b, c \in F$, $a*(b+c) = a*b+a*c$ and $(a+b)*c = a*c+b*c$.

(F3) $(F - \{0\}, *)$ is an abelian group.

Here a field is a commutative ring and every $a \in F - \{0\}$ has the inverse a^{-1}.

Example 2.4.1. Let K be a field. The set of polynomials over K denoted by $K[X]$ is a ring.

Exercises 2.1-2.4

1. Prove that $(\mathbb{Z}, +)$ is an abelian group.
2. Prove that every subgroup H of $(\mathbb{Z}, +)$ is an abelian group.
3. Prove that the set of even integers is a commutative semi-group.
4. Show that $(\mathbb{Z}, +, \times)$ is a commutative ring.
5. The set of polynomials:

   $$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Z}(i = 0, 1, \ldots, n),\ a_n \neq 0,$$

   is a commutative ring.
6. Prove that for a field K, $K[X]$ is a commutative ring.
7. Let S_n be the symmetric group of degree n.
   (a) Find the number of elements of S_n.
   (b) Prove that

   $$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad i = 1, 2, \ldots, n-1.$$

8. Prove that $(\mathbf{Q}, +, \times)$ is a field.
9. Prove that $(\mathbf{R}, +, \times)$ is a field.

Chapter 3

Numbers

In the Western culture, traditionally the numbers and the quantities had been strictly distinguished for 2000 years. This tradition however, became fetters to develop the concept of numbers. For instance, negative numbers had not been recognised as numbers until in the 17th century. While in the Eastern culture such as Hindu and Chinese, the numbers and quantities were not strictly distinguished. Therefore, negative numbers were naturally recognised as numbers in the textbook in the early period of the history of Eastern mathematics. In modern mathematics, the systems of numbers are established that is independent from the quantity. A real number is described by a pair of subsets of the set of the rational numbers (see Appendices) or limits of Cauchy sequences of rational numbers, a rational number is described by a pair of integers and an integer is described by a pair of natural numbers (see Section 3.5). Therefore, the set of natural numbers is the base of the number system. In this chapter, we introduce an axiomatic method to define the natural numbers. Then we construct integers and rational numbers from natural numbers, finally, we introduce real numbers as limits of Cauchy sequences of rational numbers.

3.1 Natural Numbers

Peano's axioms

Let $\mathbf{N}$ be a set which satisfies the following conditions:

(P1) $1 \in \mathbf{N}$

(P2) There is a rule that assigns $x \in \mathbf{N}$, $x + 1 \in \mathbf{N}$.

(P3) If $x + 1 = y + 1$, then $x = y$.

(P4) For all $x \in \mathbf{N}$, $x + 1 \neq 1$.

(P5) The set $\mathbf{N}$ is the minimal set satisfying from (P1) to (P4); that is, any proper subset $S \subset \mathbf{N}$, S does not satisfy all (P1), (P2), (P3) and (P4).

Then the set $\mathbf{N}$ is called the set of *natural numbers*, and every element of $\mathbf{N}$ is called a *natural number*.

The set of natural number $\mathbf{N}$ can be constructed by

$$\{1, 1+1, (1+1)+1, ((1+1)+1)+1, \dots, \}.$$

Ascending sequences

Let K be a subset $\mathbf{N}$. K is called an *ascending sequence* if

$$x \in K \Rightarrow x + 1 \in K.$$

The intersection of all ascending sequences containing an element $a \in \mathbf{N}$ will be denoted by $K(a)$:

$$K(a) = \bigcap_{a \in K} K,$$

where K is an ascending sequence.

Properties of Natural Numbers

The set of natural numbers $\mathbf{N}$ has the following properties.

(1) $K(1)$ is only one and $\mathbf{N} = K(1)$.

(2) For a subset $M \subset \mathbf{N}$, if

(a) $1 \in M$,

(b) $k \in M \Rightarrow k+1 \in M$,

then $\mathbf{N} = M$.

(3) For all $x \in \mathbf{N}$, if $x \neq 1$, then there uniquely exists $z \in \mathbf{N}$ such that $x = z + 1$. This element z will be denoted by $x - 1$. It is called *predecessor* of x.

(4) For every non-empty subset $M \subset \mathbf{N}$, there exists unique $m \in M$ such that $M \subset K(m)$. This m is called the *minimal element* of M

Proof. (1) Let K be an ascending sequence containing 1. (P1) is satisfied. By definition, for $k \in K$, $k+1 \in K$. So, (P2) is satisfied. Suppose that for $x, y \in K \subset \mathbf{N}$, if $x+1 = y+1$, then $x = y$ thus (P3) is satisfied. If there exists $x \in K$ such that $k+1 = 1$, then $x \notin \mathbf{N}$ and thus $x \notin K$. This is a contradiction and (P4) is satisfied.

(2) M is an ascending sequence containing 1, thus by (1), $M = \mathbf{N}$.

(3) Let $Q = \{a \in \mathbf{N} \mid a \neq 1 \text{ and } \forall x, a \neq x+1 \}$.

Let $\mathbf{N}' = \mathbf{N} - Q$; that is, $\mathbf{N}' = \{a \in \mathbf{N} \mid a = 1 \text{ or } \exists x \text{ such that } a = x+1\}$. For arbitrary $x \in N'$, $x+1 \notin Q$; that is, $x+1 \in N'$. Since N' is an ascending sequence containing 1, $\mathbf{N}' = \mathbf{N}$. This implies that $Q = \emptyset$.

(Uniqueness) For fixed $a, b \in \mathbf{N}$, a sequence $S = \{a, a+1, (a+1)+1, \ldots, b\}$ is uniquely determined. If two sequences exist, say S_1 and S_2, removing $S_1 - S_2$ from $\mathbf{N}$, we obtain an ascending sequence containing 1. This contradicts with the minimality of $\mathbf{N}$. Suppose that there are z and z' such that $z+1 = z'+1$. Then there are two sequences $S = \{1, 1+1, (1+1)+1, \ldots, z, z+1\}$ and $S' = \{1, 1+1, (1+1)+1, \ldots, z', z'+1\}$. This is a contradiction.

(4) Suppose that $M \neq \emptyset$. If $1 \in M$, then $M \subset K(1) = \mathbf{N}$. Suppose $1 \notin M$. Let

$$R = \{x \mid M \subset K(x) \}.$$

Since $1 \in R$, $R \neq \emptyset$. There exists $a \in R$ such that $a+1 \notin R$. (If not, $R = \mathbf{N}$.

But for $x \in \mathbf{N}$, $x \notin K(x+1)$, so $\bigcap_{x\in\mathbf{N}} K(x) = \emptyset$; that is,

$$M \subset \bigcap_{x\in N=R} K(x) = \emptyset.$$

This contradicts $M \neq \emptyset$.)
Therefore, $M \not\subset K(a+1)$. Thus there is $m \in M \subset K(a)$ such that $m \notin K(a+1)$. Thus $m = a$ and so $M \subset K(m)$.
Suppose that two such elements m and m' exist. Then $m \in K(m)$ and $m' \in K(m)$ and hence two sequences from m to m' exist. This is a contradiction. □

The property (4) is called the *well ordering property.*

Order on N

For $x, y \in \mathbf{N}$,

1. write $x > y$ if $K(x) \subsetneq K(y)$, and
2. write $x = y$ if $K(x) = K(y)$.

3.2 Principle of Mathematical Induction

Principle of Mathematical Induction

Let $P(n)$ be a property defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

(1) $P(a)$ is true.

(2) For all integers $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a$, $P(n)$" is true.

Let $S(n)$ denote the sum of numbers $1, 2, \ldots, n$:

$$\begin{array}{rl} & 1+2+\cdots+n \\ + & n+n-1+\cdots+1 \\ & \text{– – – – – – – – – – – – – – – – –} \\ & (n+1)+\cdots+(n+1) = n(n+1) \end{array} \tag{3.1}$$

Thus this equals to $2S(n)$.

$$S(n) = \frac{n(n+1)}{2}$$

We need to prove this formula.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. Let $P(n)$ be $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for $n \geq 1$.
For $n = 1$, the LHS$= 1$ and RHS$= \frac{1(1+1)}{2} = 1$.
$\therefore$ $P(1)$ is true.
Suppose that $P(k)$ is true for $k \geq 1$. We want to show that $P(k+1)$ is true.

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

Therefore, $P(k+1)$ is true. Therefore, $P(n)$ is true for all $n \geq 1$. □

Exercises 3.2

---

1. Use Mathematical Induction to prove:
   (a) $\sum_{i=1}^{n} 2i - 1 = n^2$ (b) $\sum_{k=1}^{n}(2k-1) = n^2$
   (c) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ (d) $\sum_{j=1}^{n}(2j-1)^2 = \frac{1}{3}n(2n-1)(2n+1)$
   (e) $\sum_{j=1}^{n} j(j+2) = \frac{1}{6}n(n+1)(2n+4)$

3.3 Addition of Natural Numbers

Addition of natural numbers

For $x, y \in \mathbf{N}$, we define $x + y$ as follows.

(1) If $y = 1$, then $x + y = x + 1$.

(2) For $y > 1$, if $x + (y - 1)$ is defined, then $x + y = (x + (y - 1)) + 1$.

Then $x + y$ is uniquely determined.

Theorem 3.3.1. *The addtion has the following properties. For $x, y, z \in \mathbf{N}$,*

(i) $(x + y) + z = x + (y + z)$.

(ii) $x + y = y + x$.

(iii) If $x < y$, then $x + z < y + z$.

Proof. (i) We prove $(x + y) + z = x + (y + z)$ by mathematical induction on z.
If $z = 1$, then $x + (y + 1) = (x + y) + 1$ by Theorem 3.3.1(i).
Suppose that for z, it holds.

$$\begin{aligned}(x + y) + (z + 1) &= ((x + y) + z) + 1 \\ &= (x + (y + z)) + 1 \\ &= x + ((y + z) + 1) \\ &= x + (y + (z + 1))\end{aligned}$$

Therefore, (i) holds for all $z \in \mathbf{N}$.
(ii) First, we prove that $x + 1 = 1 + x$ by mathematical induction on x. If $x = 1$, then $x + 1 = 1 + 1$ and $1 + x = 1 + 1$. Suppose that $x + 1 = 1 + x$ holds.
We want to show that $(x + 1) + 1 = 1 + (x + 1)$.

$$\begin{aligned}LHS &= (1 + x) + 1 \\ &= 1 + (x + 1) \\ &= RHS.\end{aligned}$$

Therefore, $x + 1 = 1 + x$ holds for all $x \in \mathbf{N}$.

We prove (ii) by mathematical induction on y. If $y = 1$, then $x + 1 = 1 + x$ is proved above. Suppose that $x + y = y + x$. We want to show that $x + (y + 1) = (y + 1) + x$.

$$\begin{aligned} LHS &= (x + y) + 1 \\ &= (y + x) + 1 \\ &= y + (x + 1) \\ &= y + (1 + x) \\ &= (y + 1) + x = RHS. \end{aligned} \tag{3.2}$$

Therefore, for all $x, y \in \mathbf{N}$, $x + y = y + x$. □

Example 3.3.2. Denote 1+1 by 2. By the axiom (P2), 1+1 $\in \mathbf{N}$. Therefore, $1 + 1 = 2$ and it is in $\mathbf{N}$.

3.4 Multiplication of Natural Numbers

MULTIPLICATION OF NATURAL NUMBERS

Theorem 3.4.1. *For $x, y \in \mathbf{N}$, $x \cdot y$ is defined as follows.*

1. *If $y = 1$, then $x \cdot y = x$.*
2. *For $y > 1$, if $x \cdot (y-1)$ is defined then*

$$x \cdot y = (x \cdot (y-1)) + x.$$

Then $x \cdot y$ is uniquely determined and it has the following properties. For $x, y, z \in \mathbf{N}$,

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(ii) $x \cdot y = y \cdot x$.

(iii) If $x < y$, then $x \cdot z < y \cdot z$.

(iv) $x \cdot (y + z) = x \cdot y + x \cdot z$.

(v) If $x < y$, then there exists $n \in \mathbf{N}$ such that $y < n \cdot x$

UNIQUENESS OF $\mathbf{N}$

The set $\mathbf{N}$ satisfies the axioms (P1), (P2), (3), (P4) and (P5) is unique. (up to isomorphism).

Proof. Suppose that $\mathbf{N}'$ is another set satisfying the set of axioms. Then we show that there exists a one-to-one function $f : \mathbf{N} \to \mathbf{N}'$ such that

1. $f(1) = 1$,
2. $f(x+1) = f(x) + 1$ for $x \in \mathbf{N}$ and $x \neq 1$.

Let $\mathbf{N}_n = \{1, 2, \ldots, n\}$. We define $f_n : \mathbf{N}_n \to \mathbf{N}$ as follows.
(i) If $n = 1$, then $f_1(1) = 1$.
(ii) Suppose $f_k(x)$ is defined. Then we define $f_{k+1} : \mathbf{N}_{k+1} \to \mathbf{N}$ by

$$\begin{aligned} f_{k+1}(x) &= f_k(x) \quad \text{for} \quad x = 1, 2, \ldots, k, \\ f_{k+1}(k+1) &= f_k(k) + 1. \end{aligned}$$

Then we define $f : \mathbf{N} \to \mathbf{N}$ with $f_n(x)$ by

$$f(x) = f_x(x) \quad x \in \mathbf{N}.$$

From the construction $f(\mathbf{N})$ is an ascending sequence in $\mathbf{N}'$ containing 1. Therefore,

$$f(\mathbf{N}) = \mathbf{N}'.$$

We will show that f is injective. The function f has the following property:

$$f(x+1) = f_{x+1}(x+1) = f_x(x) + 1 = f(x) + 1.$$

For $i \neq 1$,

$$f(i) = f((i-1)+1) = f_{(i-1)+1}((i-1)+1) = f_{i-1}(i-1) + 1 = f(i-1) + 1,$$

where $i-1$ is the predecessor of i.
For $i, j > 1$, suppose $f(i) = f(j)$. Thus

$$f(i-1) + 1 = f(j-1) + 1,$$

$f(i-1) = f(j-1)$.
If $i > j$, then repeating the process to obtain $f(i-j+1) = f(1) = 1$. Then by the definition of f, $i - j + 1 = 1$. Thus $i - j$ does not exist in $\mathbf{N}$ and so $i \not> j$. Similarly $j \not> i$. Therefore, $i = j$ so f is injective. □

3.5 Construction of integers

Let $\mathbf{N}$ be the set of natural numbers. The set of integers can be constructed with $\mathbf{N} \times \mathbf{N} = \{\ (x, y) \mid x, y \in \mathbf{N}\ \}$.

INTEGERS

For $\mathbf{N} \times \mathbf{N}$, we define the binary relation "$\sim$" as follows.

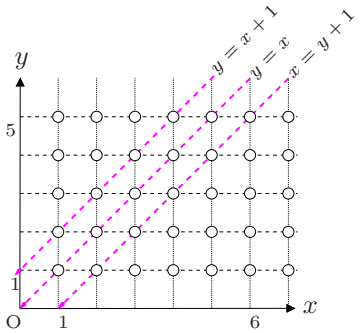
$$(a, b) \sim (c, d) \Longleftrightarrow a + d = b + c. \tag{3.3}$$

This is an equivalence relation on $\mathbf{N} \times \mathbf{N}$.

Consider the relation $a + d = b + c$. If we use (x, y) and (x', y') instead, this relation can be rewritten as

$$x - y = x' - y'.$$

Let $x - y = d$. Then this is a line in the plane and $x' - y' = d$ is the same line. Therefore, we can visualise this equivalence relation.



For an element $(a, b) \in \mathbf{N} \times \mathbf{N}$, the set $\{\ (c, d) \mid (c, d) \sim (a, b)\ \}$ will be denoted by $[a, b]$ and it is called an equivalent class of (a, b).
On $\mathbf{N} \times \mathbf{N}/_\sim$ we define two binary operations "$+$" and "$\cdot$".

$$[a, b] + [c, d] := [a + c, b + d], \tag{3.4}$$

$$[a, b] \cdot [c, d] := [ac + bd, ad + bc]. \tag{3.5}$$

The ring $(\mathbf{N} \times \mathbf{N}/_\sim, +, \cdot)$ will be denoted by $\mathbb{Z}$.
There is a one to one map $\mathbf{N} \to \mathbf{N} \times \mathbf{N}/_\sim$ defined by $x \mapsto [x + a, a]$.
We write $x = [x + a, a]$ for $x \in \mathbf{N}$. For $x, a \in \mathbf{N}$, we write $-x = [a, x + a]$ and $0 = [a, a]$.

Integral domain

An *integral domain* is a commutative ring which has no nonzero zero divisors; that is, if $ab = 0$, then $a = 0$ or $b = 0$.

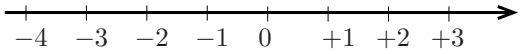
Theorem 3.5.1. $(\mathbb{Z}, +, \cdot)$ *is an integral domain.*

Exercises 3.5

1. Prove that the binary relation "$\sim$" at (3.3) is an equivalence relation on $\mathbf{N} \times \mathbf{N}$.
2. Prove that "$+$" at (3.7) and "$\cdot$" at (3.5) are well defined.
3. Prove that $(\mathbf{N} \times \mathbf{N}/_\sim, +, \cdot)$ forms a ring.
4. Define -1.
5. Verify that $(-2) \cdot (-3) = 6$
6. Prove that $(-1) \cdot (-1) = 1$

3.6 Negative and Positive Numbers

For example, in the refrigerator, if the thermometer shows 5°C, then we write +5°C and read "plus (or positive) 5°C". If it is 4 degrees less than 0°C, then we write −4°C and read "negative (or minus) 4°C.
The notation "+" and "−" are called **positive (or plus) sign** and **negative (or minus) sign** respectively.
Numbers greater than 0 are called **positive numbers** and the numbers less than 0 are called **negative numbers**. 0 is neither positive nor negative.
As we have seen there is an order on $\mathbb{Z}$; that is, for any $x, y \in \mathbb{Z}$, we have either $x \leq y$ or $y \leq x$. Withe this order, we can arrange the integers on the line:



The point of 0 is called the **origin**. The distance between the origin and an integer x is called an **absolute number** of x denoted by $|x|$.
For integers a and b, $a - b$ means $a + (-b)$

Exercises 3.6

---

1. Arrange the number in the ascending order: +12, −120, +110, −3, 0 3, 5, −10.

2. Discuss how you should teach the following calculations.
   (a) $(-7) + (+4)$ (b) $(-10) + (+9)$ (c) $0 + (-5)$ (d) $9 + (-11)$
   (e) $8 - (-7)$ (f) $0 - (-10)$ (g) $(-5) - (-5)$ (h) $(-9) - (-11)$

3.7 Constructing Rationals

We can construct the set of rational numbers a subset of $\mathbb{Z} \times \mathbb{Z}$.

RATIONAL NUMBERS

Let

$$T = \{\ (a, b) \mid a, b \in \mathbb{Z}, b \neq 0\ \}.$$

We define the binary relation on T by

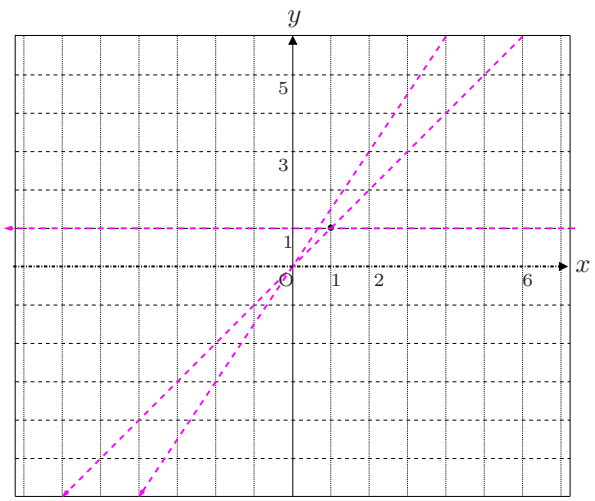
$$(a, b) \sim (c, d) \Longleftrightarrow a \cdot d = b \cdot c. \tag{3.6}$$

We define "+" and "·" by

$$[a,b]+[c,d] := [a\cdot d + b\cdot c, b\cdot d], \tag{3.7}$$

$$[a,b]\cdot[c,d] := [ac, bd]. \tag{3.8}$$

This field $T/_\sim$ is called the *rational number field* denoted by $\mathbf{Q}$.
In the graph, the reciprocal of the slope of the line passing through the origin represents the corresponding rational number. Integers appear on the line $y = 1$.



3.8 Properties of Rational Numbers

We have seen how we can construct rational numbers. Every rational number is expressed as a pair of integers, for example, for $r \in \mathbf{Q}$, there exist $a, b \in \mathbb{Z}$ such that $b \neq 0$, a and b do not have common divisors and

$$r = \frac{a}{b}$$

Every rational number is expressed by a fraction, and the fraction is expressed by a decimal number for example, $1/3 = 0.333333\cdots$, $3/22 = 1.363636\cdots$.

Decimal Numbers

Every decimal numbers is either recurring decimals or non-recurring decimals. Every rational number is expressed as a recurring decimals.

The recurring decimal $0.123123123123\cdots$ will be denoted by $0.\dot{1}2\dot{3}$.

$$
\begin{aligned}
a &= 0.123123123123\cdots \\
1000a &= 123.123123123123\cdots \\
999a &= 123 \\
\therefore \quad a &= \frac{123}{999}
\end{aligned}
$$

Exercises 3.7-3.8

---

1. Prove that the relation "$\sim$" (3.6) on T is an equivalence relation.
2. Prove that "$+$" (3.7) and "$\cdot$" (3.8) on $T/_\sim$ are well defined.
3. Show that $(T/_\sim, +, \cdot)$ is a field.
4. Express the following recurring decimals in fractions.
   (a) $0.\dot{1}$ (b) $0.\dot{2}3\dot{4}$
   (c) $6.\dot{3}\dot{4}$ (d) $0.\dot{5}\dot{2}$

3.9 The Real Numbers

It is possible to extend the system of rational numbers, $\mathbf{Q}$, to the system of real numbers, $\mathbf{R}$. We can construct the real numbers from rational numbers by considering appropriate equivalence classes of Cauchy sequences or by the method of *Dedekind cuts* (see Appendix 2). Here, we will construct the real numbers with Cauchy sequences of reational numbers.

3.9.1 Cauchy Sequence

A real number can be viewed as the limit of rational numbers.
We deonte a sequence of rational numbers,

$$a_1, a_2, \ldots, a_n, \ldots$$

by $\{a_n\}_{n=1}^{\infty}$.

A sequence $\{a_n\}_{n=1}^{\infty}$ is a *Cauchy sequence* if for every $\varepsilon > 0$, there exists $N \in \mathbf{N}$ such that for $n, m \in \mathbf{N}$,

$$|a_m - a_n| < \varepsilon.$$

Let $\mathcal{R}$ be the set of Cauchy sequences of rational numbers.

Proposition 3.9.1. *For very national number $\varepsilon > 0$, there exists $N \in \mathbf{N}$ such that $N\varepsilon > 1$.*

Two Cauchy sequences $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ are *equivalent* if for every $\varepsilon > 0$, there exists $N \in \mathbf{N}$ such that for $v \geq N$,

$$|a_n - b_n| < \varepsilon.$$

This is an equivalent relation on $\mathcal{R}$. The set of equivalent classes of Cauchy sequences: $\mathcal{R}/_{\sim}$ is called the *real numbers* denoted by $\mathbf{R}$.

Definition 3.9.1. A sequence $\{a_n\}_{n=1}^{\infty}$ is bounded if there exists M such that $|a_n| \leq M$ for all $n \in \mathbf{N}$.

Theorem 3.9.2. *Every Cauchy sequence of rational nubmers is bounded.*

Proof. Let $\{a_n\}_{n=1}^{\infty}$ be a Cauchy sequence. Take $\varepsilon = 1$. Then there exists $N \in \mathbf{N}$ such that for all $m, n \in\geq N$, $|a_n - a_m| \leq 1$. Let

$$M = \max\{|a_1|, |a_2|, \ldots, |a_{N-1}|, |a_N| + 1\}.$$

Then $a_n \leq |a_m| + |a_m - a_n| \leq |a_m| + 1 \leq M$. □

Definition 3.9.3. The quotient set $\mathcal{R}/\sim$ modulo the equivalence relation '$\sim$' will be denoted by $\mathbf{R}$.

Lemma 3.9.1. *Let $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ be Cauchy sequences. Then*

1. *$\{a_n + b_n\}_{n=1}^{\infty}$ is also a Cauchy sequence.*
2. *$\{a_n b_n\}_{n=1}^{\infty}$ is also a Cauchy sequence.*
3. *Suppose that $\{b_n\}_{n=1}^{\infty}$ is not 0. Then there exist ε_0 and N such that for all $n \geq N$,*
$$|b_n| > \frac{1}{2}\varepsilon_0 > 0.$$
4. *Suppose that $\{b_n\}_{n=1}^{\infty}$ is not 0 and $b_n \neq 0$ for $n = 1, 2, \ldots$. Then $\left\{\frac{a_n}{b_n}\right\}_{n=1}^{\infty}$ is a Cauchy sequence.*

Proof. Take a rational number ε. Then there exists $N_1 \in \mathbf{N}$ such that

$$|a_m - a_n| < \varepsilon/2$$

for all $m,\ n > N_1$. Similarly, there exists $N_2 \in \mathbf{N}$ such that

$$|b_m - b_n| < \varepsilon/2$$

for all $m,\ n > N_2$.
Let $N = \max\{N_1, N_2\}$.

$$\begin{aligned} |(a_m + b_m) - a_n + b_n)| &= |a_m - a_n + b_m - b_n| \\ &\leq |a_m - a_n| + |b_m - b_n| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \end{aligned}$$

for all $m,\ n > N$. Therefore, $\{a_n + b_n\}$ is a Cauchy sequence. □

The classes of $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ will be deonted by α and β.

Definition 3.9.4. Let α and β be elements of $\mathbf{R}$ represented by Cauchy sequences $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ respectively.

1. The sum $\alpha + \beta$ is defined by the class of $\{a_n + b_n\}_{n=1}^{\infty}$.
2. The difference $\alpha - \beta$ is defined by the class of $\{a_n - b_n\}_{n=1}^{\infty}$.
3. The multiplication $\alpha \cdot \beta$ is defined by the class of $\{a_n \cdot b_n\}_{n=1}^{\infty}$.
4. If $\{b_n\}_{n=1}^{\infty} \neq 0$, The quotient $\alpha \div \beta$ is defined by the class of $\{a_n/b_n\}_{n=1}^{\infty}$.

3.10 Order of Cauchy sequences

Definition 3.10.1. Let $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ be Cauchy sequences of rational numbers. $\{a_n\}_{n=1}^{\infty} \leq \{b_n\}_{n=1}^{\infty}$ if for every $\varepsilon > 0$, there exists a number N such that for $n \geq N$, $b_n - a_n > -\varepsilon$.
Let α and β be elements of $\mathbf{R}$ represented by Cauchy sequences $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ respectively. $\alpha \leq \beta$ if $\{a_n\}_{n=1}^{\infty} \leq \{b_n\}_{n=1}^{\infty}$.

Definition 3.10.2. A rational number sequence $\{\{a_{m,n}\}_{n=1}^{\infty}\}_{m=1}^{\infty}$ is a *sequecne of Cauchy sequences*, if for each $m \in \mathbf{N}$, $\{a_{m,n}\}_{n=1}^{\infty}$ is a Cauchy sequence.

Definition 3.10.3. A sequence of Cauchy seuquences of rational numbers, $\{\alpha_m\}_{m=1}^{\infty} = \{\{a_{m,n}\}_{n=1}^{\infty}\}_{m=1}^{\infty}$ is a *Cauchy sequence* if for every Cauchy sequence of rational numbers, $\varepsilon = \{\varepsilon_n\}_{n=1}^{\infty} > 0$, there exists $N \in \mathbf{N}$ such that if $n, m > N$, then

$$-\varepsilon < \alpha_m - \alpha_n < \varepsilon.$$

Definition 3.10.4. Let $\alpha = \{a_n\}_{n=1}^{\infty}$ be a sequence of rational numbers. A sequence of Cauchy seuquences of rational numbers, $\{\alpha_m\}_{m=1}^{\infty} = \{\{a_{m,n}\}_{n=1}^{\infty}\}_{m=1}^{\infty}$ *converges* to α if for every Cauchy sequence of rational numbers, $\varepsilon = \{\varepsilon_n\}_{n=1}^{\infty} > 0$, there exists $N \in \mathbf{N}$ such that if $n, m > N$, then

$$-\varepsilon < \alpha_m - \alpha < \varepsilon.$$

Theorem 3.10.5. *For a Cauchy sequence $\alpha = \{a_n\}_{n=1}^{\infty}$ of rational numbers, the constant sequence $\alpha_m = \{a_m\}_{n=1}^{\infty}$ converges to α.*

Theorem 3.10.6. *Every Cauchy sequence of Cauchy sequence of rational numbers is convergent.*

Definition 3.10.7. Let A be a subset of $\mathbf{R}$. Then A has an *upper bound* if there exists M such that if $a \in A$, then $a \leq M$.

Theorem 3.10.8. *Let A be a subset of $\mathbf{R}$. If A has an upper bound, then there exists the least upper bound M_0; that is,*

1. *If $a \in A$, then $a \leq M_0$.*
2. *If $m < M_0$, then there exists $a \in A$ such that $a > m$.*

3.11 Summary

In the previous sections we constructed real numbers as the set of classes of rational Cauchy sequences. This set of real numbers $\mathbf{R}$ satisfies the following properties.

1. $(\mathbf{R}, +)$ is an abelian group under the operation '+'.
2. $(\mathbf{R}, +, \times)$ is a field.
3. $\mathbf{R}$ is a totally ordered set.
4. $\mathbf{R}$ is complete.
5. $\mathbf{R}$ contains $\mathbf{Q}$ as a subset and every real number is expressed by a limit of a rational sequence.

Exercises 3.9

1. Prove Lemma 3.9.1 (2).
2. Prove Lemma 3.9.1 (3).
3. Prove Lemma 3.9.1 (4).

Chapter 4

Numbers and Polynomials

The set of integers forms a group under the addition as well as a ring under the addition and the multiplication. The integer ring has no non-trivial zero-divisor. The set of polynomials with real coefficients also has the same property. In this chapter, we learn properites of integers and polynomials.

4.1 Modular Arithmetic

Definition

Let a and b be integers with $a \neq 0$. *a divides b* if there is an integer c such that $b = ac$. Here, a is a *factor* of b and that b is a *multiple* of a. We write

$$a \mid b$$

If a does not divide b, then we write $a \nmid b$

Example 4.1.1. $3 \mid 12$ but $3 \nmid 13$.

Theorem 4.1.2. *Let a, b and c be integers. Then*

1. *if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;*
2. *if $a \mid b$, then $a \mid bc$ for all integers c;*
3. *if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Definition

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$. We write $a \equiv b \pmod{m}$.
If a and b are not congruent modulo m, then we write $a \not\equiv b \pmod{m}$.

Theorem 4.1.3. *Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.*

Proof. By the division algorithm we have:

$$\begin{aligned} a &= qm + r \qquad 0 \leq r < m \\ b &= q'm + r' \qquad 0 \leq r' < m \end{aligned}$$

Since $a \equiv b \pmod{m}$, $m \mid (a - b) = (q - q')m + r - r'$. This implies that $m \mid (r - r')$ thus $r - r' = km$ for some $k \in \mathbb{Z}$. Here $|r - r'| = |k|m < m$ and thus $|r - r'| = 0$. Therefore $r = r'$. □

Theorem 4.1.4. *Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.*

Theorem 4.1.5. *Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.*

4.2 Primes and Greatest Common Divisor

DEFINITION

A positive integer greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

Theorem 4.2.1 (The Fundamental Theorem Of Arithmetic)**.** *Every positive integer n greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size:*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

where $p_1 < p_2 < \cdots, < p_m$ are primes and $e_1, e_2, \ldots, e_m$ are non-negative integers.

Example 4.2.2. The prime factorisation of 100, 641 and 1024 are: $100 = 2^2 5^2$, $641 = 641$, $1024 = 2^{10}$.

Theorem 4.2.3. *If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.*

Theorem 4.2.4. *There are infinitely many primes.*

Theorem 4.2.5. *The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound.*

Exercises 4.2

---

1. Show that 149 is prime.
2. Prove Theorem 4.2.3.
3. Prove Theorem 4.2.4.

4.3 GCD and LCM

Definition

Let a and b be integers, not both zero. The integer d such that $d \mid a$ and $d \mid b$ is called a *common divisor* of the integers. The greatest common divisor of them is called the *greatest common divisor* denoted by $\gcd(a, b)$.

Example 4.3.1. $\gcd(24, 36) = 12$.

Definition

The integers a and b are relatively prime (coprime) if $\gcd(a, b) = 1$.

Definition

The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Definition

Let a and b be positive integers. There are integers that is divisible by both a and b and called *common multiples*. 0 is also a common multiple. The least common multiple other than 0 is called the *least common multiple* of a and b denoted by $\text{lcm}(a, b)$.

Example 4.3.2. The least common multiple of $a = 2^3 3^4 7^2$ and $b = 2^2 3^5 11^2$ is:

$$\mathrm{lcm}(a, b) = 2^3 3^5 7^2 11^2$$

Theorem 4.3.3. *Let $a > 0, b > 0$ be integers. If the least common multiple of a and b is $l > 0$ and the greatest common divisor of a and b is $m > 0$, then*

$$ab = lm \tag{4.1}$$

Proof. Since l is a common multiple of a and b, there exist a' and b' such that

$$l = ab' = ba' \tag{4.2}$$

The number ab is a multiple of l as it is a common multiple of a and b (Theorem A.5.2). Thus there exists d such that

$$ab = dl \tag{4.3}$$

Substituting (4.14) to l we obtain

$$b = db', \qquad a = da' \tag{4.4}$$

Therefore, d is a common divisor of a and b. There is an integer e such that $m = de$.
$m|a$ and $m|b$ means that $de|da'$ and $de|db'$ thus $e|a'$ and $e|b'$. This implies that there exist a'' and b'' such that $a' = ea''$ and $b' = eb''$. Substituting them to (4.14), we obtain

$$l = ab''e = ba''e \tag{4.5}$$

If $e > 1$, then $l/e < l$. Also l/e is a common multiple of a and b. This is a contradiction. Therefore, $e = 1$ and thus $m = d$. From (4.3) $ab = lm$. □

4.4 Representations of Integers

Theorem 4.4.1. *Let bi be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

where k is a nonnegative integer, $a_0 l$, $a_1, \ldots, a_k$ are nonnegative integers less than n, and $a_k \neq 0$.

The expression in Theorem A.3.4 is called the *base b expression of n* denoted by $(a_k a_{k-1} \dots a_1 a_0)_b$.

Definition

The base 2 expansion of $n \in \mathbb{Z}^+$ is called the *binary expansion* of n. The base 16 expansion of $n \in \mathbb{Z}^+$ is called the *hexadecimal expansion* of n. The hexadecimal digits used are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E$ and F.

Example 4.4.2. The binary expansion $(1011001)_2$ is:

$$1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 = (89)_{10}$$

The hexadecimal expansion $(34AF0C)_{16}$ is:

$$3 \cdot 16^5 + 4 \cdot 16^4 + 10 \cdot 16^3 + 15 \cdot 16^2 + 0 \cdot 16 + 12 = (342684)_{10}$$

Base Conversion

An algorithm for constructing the base b expansion of an integer n is: First, divide n by b to obtain a quotient and remainder:

$$n = bq_0 + a_0 \qquad 0 \leq a_0 < b.$$

The remainder a_0 is the rightmost digit in the base b expansion of n. Next, divide q_0 by b to obtain

$$q_0 = bq_1 + a_1 \qquad 0 \leq a_1 < b.$$

a_1 is the second digit from the right in the base b expansion of n. Continue this process til we obtain a quotient equal to zero.

Example 4.4.3. Find the base 8 or *octal*, expansion of $(12345)_{10}$.
Solution. First, divide 12345 by 8 to obtain

$$12345 = 8 \cdot 1543 + 1$$

Successively dividing quotients by 8 gives

$$\begin{aligned} 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

Thus $(12345)_{10} = (30071)_8$.

4.5 Euclidean Algorithm

There is an algorithm to find the greatest common divisor of two integers called *Euclidean Algorithm*.

Example 4.5.1. gcd(1234, 74) is obtained by the following procedure: First divide 1234 by 74:

$$1234 = 16 \cdot 74 + 50$$

Next, divide 74 by 50:

$$74 = 1 \cdot 50 + 24$$

Continue this procedure

$$\begin{aligned} 50 &= 2 \cdot 24 + 2 \\ 24 &= 12 \cdot 2 + 0 \end{aligned}$$

Then the gcd is the last nonzero remainder 2.

Lemma 4.5.1. *Let $a = bq + r$ where a, b, q and r are integers. Then* $i\gcd(a, b) = \gcd(b, r)$.

EUCLIDEAN ALGORITHM

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Example 4.5.2. Find gcd(20160611, 8313).

$$\begin{aligned} 20160611 &= 8313 \times 2425 + 1586 \\ 8313 &= 1586 \times 5 + 383 \\ 1586 &= 383 \times 4 + 54 \\ 383 &= 54 \times 7 + 5 \\ 54 &= 5 \times 10 + 4 \\ 5 &= 4 \times 1 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned}$$

$$\therefore \quad (20160611, 8313) = 1$$

Theorem 4.5.3. *If a and b are positive integers, then there exist integers s and t such that* $\gcd(a, b) = sa + tb$.

Lemma 4.5.2. *If a, b and c are positive integers such that* $\gcd(a, b) = 1$ *and $a \mid bc$, then $a \mid c$.*

Lemma 4.5.3. *If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$, for some i.*

Theorem 4.5.4. *Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc$ (**mod** m) and* $\gcd(c, m) = 1$, *then $a \equiv b$ (**mod** m).*

Example 4.5.5. The congruence $28 \equiv 18$ (**mod** 5) holds, and both sides of this congruence can be divided by 2 as $\gcd(2, 5) = 1$: $14 \equiv 9$ (**mod** 5).

Example 4.5.6. The congruence $15 \equiv 9$ (**mod** 6) holds, but both sides of this congruence cannot be divided by 3 because $15/3 = 5$ and $9/3 = 3$, but $5 \not\equiv 3$ (**mod** 6).

4.6 Linear Congruence

Let $a, b \in \mathbb{Z}$ and let x be a variable. The congruence of the form

$$ax \equiv b \pmod{m}$$

is called a *linear congruence.*

Theorem 4.6.1. *Let $a, m \in \mathbb{Z}$ with* $\gcd(a, m) = 1$ *and $m > 1$. Then the inverse of a modulo m exists. This inverse is unique modulo m.*

Example. Solve $4x \equiv 5 \pmod{9}$.
Since $\gcd(4, 9) = 1$, there is an inverse of 4. From $9 = 2 \cdot 4 + 1$, $1 = 9 - 2 \cdot 4$, the inverse is $-2 \equiv 7 \pmod{9}$. Multiply 7 to both sides to get $28x \equiv x \equiv 35 \equiv 8 \pmod{9}$

Theorem 4.6.2 (The Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive numbers and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system*

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_n \ (mod\ m_n) \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

The simultaneous solution is given by:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n,$$

where $M_k = m_1 m_2 \cdots m_n / m_k = m/m_k$ and y_k is an inverse of M_k modulo m_k.

Example 4.6.3. Solve:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Solution. Let $M = 3 \cdot 4 \cdot 5 = 60$. Then $M_1 = 20$, $M_2 = 15$ and $M_3 = 12$. We need to find an inverse of $M_1 = 20$ modulo 3 that is 2 and so $y_1 = 2$. An inverse of $M_2 = 15$ modulo 4 is 3 and so $y_2 = 3$. For $M_3 = 12$, an inverse $y_3 = 3$.
Therefore, the solution is:

$$x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}.$$

4.7 Congruent Classes

Let p be a prime number. Let $\mathbb{Z}_p$ denote the set of congruent classes modulo p. Denote a class of $\mathbb{Z}_p$ represented by n by $[n]_p$.

Definition 4.7.1. For $[n]_p, [m]_p \in \mathbb{Z}_p$,

$$[n]_p + [m]_p := [n+m]_p \tag{4.6}$$

The definition is well defined.
Suppose $n \equiv n' \pmod p$ and $m \equiv m' \pmod p$. Then $[n+m]_p = [n'+m']_p$ as $n + m - (n' + m') = (n - n') + (m - m') = p \cdot k$ for some $k \in \mathbb{Z}$.

Definition 4.7.2. For $[n]_p, [m]_p \in \mathbb{Z}_p$,

$$[n]_p \cdot [m]_p := [n \cdot m]_p \tag{4.7}$$

The definition is well defined.
Suppose $n \equiv n' \pmod p$ and $m \equiv m' \pmod p$. Then $n' - n = kp$ for some $k \in \mathbb{Z}$ and thus $n' = n + kp$. Similarly $m' = m + lp$ for some $l \in \mathbb{Z}$. Therefore,

$$\begin{aligned} n' \cdot m' &= (m + lp) \cdot (m + lp) \\ &= nm + (nl + kl + klp)p \end{aligned}$$

Hence $[n \cdot m]_p = [n' \cdot m']_p$.

Example 4.7.3. Let n be a positive number. Suppose that

$$n = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0,$$

where $a_n \neq 0, a_{n-1}, \ldots, a_1, a_0$ are non-negative integers. Then

$$\begin{aligned}[n]_9 &= [a_n \times 10^n]_9 + [a_{n-1} \times 10^{n-1}]_9 + \cdots + [a_1 \times 10]_9 + [a_0]_9 \\ &= [a_n]_9 + [a_{n-1}]_9 + \cdots + [a_1]_9 + [a_0]_9 \\ &= [a_n + a_{n-1} + \cdots + a_0]_9\end{aligned}$$

Therefore, n is divisible by 9 if and only if $a_n + a_{n-1} + \cdots + a_0$ is divsible by 9.

Exercises 4.3-4.7

---

1. Convert the following expressions into the expressions with base 10.

   (i) $(100001111010101)_2$. (ii) $(45AF17CD)_{16}$.

2. Find $\gcd(102, 12)$.

3. Find $\gcd(12345678, 987)$.

4. Prove:

   (a) If $n \equiv 1 \pmod 3$, then $n^2 + n + 1$ is divisible by 3 for all integers n.

   (b) If $n \equiv 2 \pmod 3$, then $n^2 - n + 1$ is divisible by 3 for all integers n.

   (c) $n^9 - n^3$ is divisible by 9 for all integers n.

5. For every $n \in \mathbf{N}$ $(n \geq 1)$, prove that

   (a) $11^n - 5^n - 6^n$ is divisible by 5.

   (b) $11^n - 5^n - 6^n$ is divisible by 30.

4.8 Polynomials

As we have seen the set of polyonmials $\mathbf{R}[x]$ forms a commutative ring. Let $f(x)$ and $g(x)$ be polynomial of degrees n and m respectively. The degree of $f(x) + g(x)$ is $\max(n, m)$ and the degree of $f(x)g(x)$ is $n + m$.

Example 4.8.1. Expand the following multiplications:

(1) $(x + 4)(x + 7)$ (2) $(x^2 + x + 1)(x - 1)$

(3) $(x - 2)(x + 2)$ (4) $(x + 2y)(y + 3x)$

Solution.
(1)

$$\begin{aligned}(x-4)(x+7) &= x(x+7) - 4(x+7)\\ &= x^2 + 7x - 4x - 28\\ &= x^2 + 3x - 28\end{aligned}$$

(2), (3) and (4) are left for the readers.

Formulae of Expansions

$$\begin{aligned}(ax + b)(cx + d) &= acx^2 + (ad + bc)x + bd\\ (a + b)^2 &= a^2 + 2ab + b^2\\ (a + b)(a - b) &= a^2 - b^2\end{aligned}$$

4.9 Division

Theorem 4.9.1. *If R is an integral domain, then the polynomial ring $R[x]$ is also an integral domain.*

From Theorem4.9.1, we can solve the polynomial equation with factoring.

Example 4.9.2. Solve $x^2 + 5x + 6 = 0$.
Solution. The polynomial in LHS is in $\mathbf{R}[x]$ which is an integral domain. Factor the LHS:

$$(x + 2)(x + 3) = 0$$

Therefore, $x + 2 = 0$ or $x + 3 = 0$ and thus $x = -2$ or $x = -3$.

Teaching Tips (Factoring)

1. Take out the common factor.
2. Use the formulae:
   (a) $acx^2 + (ad + bc)x + bd = (ax + b)(cx + d)$
   (b) $a^2 + 2ab + b^2 = (a + b)^2$
   (c) $a^2 - b^2 = (a + b)(a - b)$

Polynomials and Equations

$$\begin{aligned} & \frac{2}{3}x - \frac{3}{4}x + \frac{1}{3} \\ = & \frac{8}{12}x - \frac{9}{12}x + \frac{4}{12} \\ = & \frac{8x - 9x + 4}{12} \\ = & \frac{-x + 4}{12} \end{aligned}$$

$$\begin{aligned} \frac{2}{3}x - \frac{3}{4}x &= -\frac{1}{3} \\ \left(\frac{2}{3}x - \frac{3}{4}x\right) \times 12 &= -\frac{1}{3} \times 12 \\ 8x - 9x + 4 &= -4 \\ -x + 4 &= -4 \\ x &= 8 \end{aligned}$$

Common Mistake

The following modification is of course **WRONG** but many students make this type of mistake.

$$\begin{aligned} \frac{2}{3}x - \frac{3}{4}x + \frac{1}{3} &= \left(\frac{2}{3}x - \frac{3}{4}x + \frac{1}{3}\right) \times 12 \\ &= 8x - 9x + 4 \\ &= -x + 4 \end{aligned}$$

Exercises 4.8-4.9

1. Factor the follwoing polynomials.

   (a) $4ax^2 - 12ax - 28a$ (b) $x^3y^2 + 4x^2y^2 + 4xy^2$

   (c) $x^4 - 256$ (d) $15x^2 + 2x - 8$ (e) $(x+2)^2 + (x+2) - 12$

2. Solve the equations.

   (a) $4x^2 - 12x - 28 = 0$ (b) $4x - 1 = 5x + 3$

   (c) $x^4 - 16 = 0$ (d) $x^3 + 2x^2 - 6x - 5 = 0$

3. Let p be a prime number and let n be an integer. Prove that $p \mid n^2$, then $p \mid n$.

4. A woman earns 20% more than her husband. Together they make OMR. 4950 per month. What is the husband's monthly salary?

5. A pot contains 8ℓ of brine at a concentration of $150\text{g}/\ell$. How much of the water should be boiled off to increase the concentratin to $200\text{g}/\ell$?

6. Two men A and B are hired to paint a house. Working together they can paint the house in two-thirds the time that it takes B working alone. A takes six hours to paint a house alone. How long does it take B to paint the house working alone?

4.10 The Division Algorithm

The following is a basic and important theorem in algebra.

Theorem 4.10.1. *Let a, $d > 0$ be integers. Then there exists a unique pair of integers q and r such that*

$$a = qd + r, \qquad 0 \leq r < d \tag{4.8}$$

Definition

In the equality given in the division algorithm: $a = qd + r$, d is called the *divisor*, a is called the *dividend* q is called the *quotient*, and r is called the *remainder*. We write the relation:

$$q = a \textbf{ div } d, r = a \textbf{ mod } d.$$

Example 4.10.2. We divide 131 by 56:

$$131 = 2 \times 56 + 19.$$

We write this relation $2 = 131$ **div** 56 and $19 = 131$ **mod** 56.

Principle of Divison of Polynomials

Theorem 4.10.3. *Let $K[x]$ be a polynomial ring over a field K. For $p(x), d(x) \in K[x]$ with $d(x) \neq 0$. Then there exist a unique pair of polynomials $q(x)$ and $r(x)$ such that*

$$p(x) = q(x)d(x) + r(x), \qquad \deg(r) < \deg(d) \tag{4.9}$$

Proof. (Existence of $q(x)$ and $r(x)$)
Let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $d(x) = \sum_{j=0}^{n} b_j x^j$.
If $m < n$, then letting $q(x) = 0$ and $r(x) = p(x)$, we have the desired result.
Suppose that $n \leq m$. For $m = 0$, $p(x) = a_0$ and $d(x) = b_0$. Let

$$r(x) = p(x) - \frac{a_0}{b_0} d(x)$$

Then $p(x) = \frac{a_0}{b_0} d(x) + r(x)$. Therefore, the theorem is true for $m = 0$. Suppose that the theorem is true for all $0 \leq i < k$ for $k \geq 0$. Let $p(x)$ be a polynomial of degree k and let $d(x)$ be a polynomial of degree $l \leq k$. Let

$$p'(x) = p(x) - \frac{a_k}{b_l} x^{k-l} d(x). \tag{4.10}$$

Then $\deg(p') = k - 1 < k$. Therefore, there are $q'(x)$ and $r'(x)$ such that

$$p'(x) = q'(x)d(x) + r'(x), \quad \deg(r') < \deg(d) \tag{4.11}$$

$$\begin{aligned} p(x) &= (q'(x)d(x) + r'(x)) + \frac{a_k}{b_l} x^{k-l} d(x) \\ &= (q'(x) + \frac{a_k}{b_l} x^{k-l}) d(x) + r'(x) \end{aligned}$$

This is the desired result.
(Uniqueness of $q(x)$ and $r(x)$).
Suppose that there are $q'(x)$ and $r'(x)$ such that

$$p(x) = q'(x)d(x) + r'(x), \qquad \deg(r') < \deg(d). \tag{4.12}$$

Then subtract (4.12) from (4.9) to obtain:

$$\begin{aligned}(q(x) - q'(x))d(x) + (r(x) - r'(x)) &= 0\\ (q(x) - q'(x))d(x) &= (r'(x) - r(x))\end{aligned}$$

The $\deg(q(x) - q'(x))d(x) \geq \deg(d)$ and $\deg(r'(x) - r(x))) < \deg(d)$. This implies that $(q(x) - q'(x) = 0$ and $r'(x) - r(x) = 0$. Therefore, $q(x)$ and $r(x)$ are unique. □

Example 4.10.4. Divide the polynomial $x^3 + 5x^2 + 4x + 3$ by $x^2 - 2$. By the long division we obtain the quotient polynomial $x + 5$ and the remainder $6x + 9$:

$$x^3 + 5x^2 + 4x + 3 = (x + 5)(x^2 - 2) + 6x + 9$$

Example 4.10.5. Let $f(x)$ be a polynomial of degree greater than 2. Let $ax + b$ be the remainder when $f(x)$ is divided by $x^2 - 5x - 6$. If $f(2) = 2$ and $f(3) = 4$, then find a and b
Solution.

$$\begin{aligned}f(x) &= q(x)(x^2 - x - 6) + ax + b\\ &= q(x)(x - 3)(x - 2) + ax + b\end{aligned}$$

$$f(2) = 2a + b = 2 \tag{4.13}$$
$$f(3) = 3a + b = 4 \tag{4.14}$$

Solving the equations (4.13) and (4.14) we have $a = 2$ and $b = -2$.

Exercises 4.10

---

1. Find the maximal natural number n such that the following form is an integer:

$$\frac{5n^2 + 7n + 15}{5n - 3}$$

2. Let $f(x)$ be a polynomial in $\mathbf{R}[x]$. Prove that $f(x)$ is divisible by $x-3$ if and only if $f(3)=0$.

3. Let $f(x)$ be a polynomial of degree greater than 3. Let ax^2+bx+c be the remainder when $f(x)$ is divided by $g(x)=x^3-x$. Also, $f(0)=3$ $f(1)=2$ and $f(-1)=1$. Then find a, b and c.

Chapter 5

Theory of Equations

In the 16th century, Italian mathematicians solved general cubic, quatic equations in terms of their coefficients. They expected to be able to solve the fifthe dgree equation but it was not successful. The problem is:

Can we find a general solution of a quintic equation?

In the 19th century Abel and Galois finally negatively solved this problem. In this chapter we will learn the Tartaglia-Cardano's method to solve the cubic equation and Abel's impossible theorem.

5.1 Square Roots of Numbers

Consider the following question:
Q. If the area of a square with the side s is 5cm^2, what is s?
We know that if $s = 2$, then $s^2 = 4 < 5$ and if $s = 3$, then $5 < s^2 = 9$. Therefore, s must be between 2 and 3.
Also, if $s = 2.2$, then $s^2 = 4.4 < 5$ and if $s = 2.3$, then $5 < 2.3^2 = 5.29$. Therefore, s is between 2.2 an 2.3.
We also know that s is a solution of the equation:

$$x^2 - 5 = 0 \tag{5.1}$$

There are two numbers as the solution; one is positive and the other is negative. These solutions are called **square roots** of 5.
The positive square root is denoted by $\sqrt{5}$ and the negative square root is denoted by $-\sqrt{5}$.
For a positive real number a, the equation

$$x^2 - a = 0 \tag{5.2}$$

has solution $\sqrt{a}$ and $-\sqrt{a}$.

Square roots of small numbers

$$\sqrt{2} = 1.41421356\cdots$$
$$\sqrt{3} = 1.7320508\cdots$$
$$\sqrt{5} = 2.23620679\cdots$$
$$\sqrt{6} = 2.4494989\cdots$$
$$\sqrt{7} = 2.64575\cdots$$

Theorem 5.1.1. *Let a and b be positive real numbers. Then*

$$\sqrt{a} \times \sqrt{b} = \sqrt{ab} \tag{5.3}$$
$$\frac{\sqrt{a}}{\sqrt{b}} = \sqrt{\frac{a}{b}} \tag{5.4}$$

Proof. Proof of (5.3) Square LHS:

$$\begin{aligned}\left(\sqrt{a} \times \sqrt{b}\right)^2 &= \sqrt{a} \times \sqrt{b} \times \sqrt{a} \times \sqrt{b} \\ &= \left(\sqrt{a} \times \sqrt{a}\right) \times \left(\sqrt{b} \times \sqrt{b}\right) \\ &= a \times b\end{aligned}$$

Therefore $\sqrt{a} \times \sqrt{b}$ is a positive square root of $a \times b$; that is, the RHS. The proof of (5.4) is left for the readers as an exercise. □

5.2 Sum and Product of Square Roots

$\sqrt{2} + \sqrt{7}$ cannot be simplified but $\sqrt{2} + \sqrt{8}$ can be simplified as:

$$\begin{aligned}\sqrt{2} + \sqrt{8} &= \sqrt{2} + \sqrt{2^2 \cdot 2} \\ &= \sqrt{2} + 2\sqrt{2} \\ &= 3\sqrt{2}.\end{aligned}$$

Exercises 5.1

1. Calculate:

   (a) $\sqrt{50} - \sqrt{32}$ (b) $\sqrt{125} - \sqrt{245} + \sqrt{20}$

   (c) $\sqrt{45} + \dfrac{20}{\sqrt{5}}$ (d) $-\sqrt{32} + \dfrac{3\sqrt{2}}{\sqrt{3}} - \dfrac{3}{\sqrt{6}}$

2. Find all integers a such that $3.2 < \sqrt{a} < 4.3$

3. Find the least number a such that $\sqrt{72a}$ is a natural number.

4. Let a be the integer part of $\sqrt{5}$ and let b be the decimal number part of $\sqrt{5}$. Find $a^2 + b^2$.

5.3 Symmetric Polynomials

Symmetric polynomial

Let S_n be the symmetric group of degree n. Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial of n variables. For all $\sigma \in S_n$, if $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)$, then $f(x_1, x_2, \ldots, x_n)$ is called a **symmetric polynomial**.

Example 5.3.1. $x_1 + x_2 + \cdots + x_n$ is a symmetric polynomial.

Elementary symmetric polynomials

Let $\Lambda_n = \{1, 2, \ldots, n\}$. Let $|A|$ be the cardinality of the set A. We call the following symmetric polynomial

$$s_{n,k}(x_1, \cdots, x_n) = \sum_{A \subset \Lambda_n, |A|=k} \left(\prod_{t \in A} x_t \right)$$

an **elementary symmetric polynomial** of degree k.
Note that every symmetric polynomial has a polynomial expression in terms of elementary polynomials.

Example 5.3.2. $f(x_1, x_2) = x_1^2 + x_2^2$ is a symmetric polynomial.

$$(x_1, x_2) = (x_1 + x_2)^2 - 2x_1x_2.$$

5.4 Quadratic Equations

Consider the following problem.

Q. There is a rectangle with one side is 3cm longer than the other side and the area is 28cm^2. Find the dimension of the rectangle.

The equation that we need to solve is:

$$x(x+3) = 28 \tag{5.5}$$

Expand the left hand side to obtain:

$$x^2 + 3x - 28 = 0 \tag{5.6}$$

We can solve this equation as follows:

$$\begin{aligned} (x-4)(x+7) &= 0 \\ x-4 = 0, \quad &\text{or} \quad x+7 = 0 \\ \therefore \quad x = 4, \quad & x = -7 \end{aligned}$$

The side of the rectangle must be positive, so the side is 4cm.

Quadratic Equation

A **quadratic equation** of x is an equation in the form:

$$ax^2 + bx + c = 0,$$

where $a, b, c \in \mathbf{R}$ and $a \neq 0$.

There is a formula for the solution.

Quadratic Formula I

The formula for the quadratic equation

$$ax^2 + bx + c = 0,$$

where $a, b, c \in \mathbf{R}$ and $a \neq 0$ is:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We can show the formula as follows:

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) &= 0 \\
a\left(x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) &= 0 \\
a\left(x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2\right) - \frac{b^2}{4a} + \frac{ac}{a} &= 0 \\
a\left(x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2\right) &= \frac{b^2}{4a} - \frac{ac}{a} \\
a\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \pm\sqrt{\frac{b^2 - 4ac}{4a^2}} \\
x &= -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}$$

Teaching Tips (Quadratic Formula II)

If the coefficient of x is even number:

$$ax^2 + 2b'x + c = 0,$$

where $a, b', c \in \mathbf{R}$ and $a \neq 0$, then we can simplify the the quadratic formula:

$$x = \frac{-b' \pm \sqrt{b'^2 - ac}}{a}$$

From the argument above, we can see that every quadratic equation $ax^2 + bx + c = 0$ $(a \neq 0)$ has the form:

$$a(x - h)^2 + k, \tag{5.7}$$

for some numbers h and k. In this case, the value k is the maximal value at $x = h$ if $a < 0$ and minimal value at $x = h$ if $a > 0$.

We also can find maximal and minimal value using the derivatives.

5.5 Applications of Quadratic Equations

Here we consider some applications of quadratic equations.

Example 5.5.1. A box with open top is to be constructed from a rectangular piece of cardboard with dimension a and b by cutting out equal squares at each corner and then folding up the sides.

1. Find the size of the square at a corner when the volume of the box is maximised.

2. Find the maximal volume.

Example 5.5.2. A garden owner wants to fence a rectangular plot with the area 1200m^2. He use two types of fence A and B. A costs 3RO per meter and A costs 4RO per meter. Types A and B are used for each pair of parallel sides respectively. Find the dimension of the rectangular plot when the cost of the fencing is minimised.

5.6 Relation between Roots and Coefficients

Relation between roots and coefficients

Let $f(x)$ be a polynomial function of degree n with zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$:

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x_{n-1} + \cdots + a_1 x + a_0 \\ &= a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n). \end{aligned}$$

Then the relation between roots and coefficients is:

$$s_{n,k}(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad (k = 1, 2, \ldots, n).$$

Discriminants

Let

$$\begin{aligned} P &= (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n) \\ &\quad (x_2 - x_3)\cdots(x_2 - x_n) \\ &\quad \cdots \\ &\quad (x_{n-1} - x_n). \end{aligned} \tag{5.8}$$

Obviously, P itself is **not** a symmetric polynomial but P^2 is a symmetric polynomial.
Let $x_1, x_2, \ldots, x_n$ be roots of

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

The polynomial

$$D = a_n^{2(n-1)} P^2$$

is called the **discriminant** of the equation $f(x) = 0$ or (polynomial $f(x)$). If $D = 0$, then the equation has a multiple root.

Example 5.6.1. Let $f(x) = a_2x^2 + a_1x + a_0$.

$$\begin{aligned} D &= a_2^2(x_1 - x_2)^2 \\ &= a_2^2(x_1^2 - 2x_1x_2 + x_2^2) \\ &= a_2^2((x_1 + x_2)^2 - 4x_1x_2) \\ &= a_1^2 - 4a_2a_0 \end{aligned}$$

Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $n \geq 0$.

Theorem 5.6.2. *Let $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = 0$. Suppose that $f(x) = 0$ has roots x_1, x_2 and x_3, and that $f'(x) = 0$ has roots α and β. Then*

$$D = -27a_3^2 f(\alpha)f(\beta).$$

Proof. Since x_1, x_2 and x_3 are roots of $f(x) = 0$, we have

$$f(x) = a_3(x - x_1)(x - x_2)(x - x_3). \tag{5.9}$$

We have three expressions of $f'(x)$:

$$\begin{aligned} f'(x) &= 3a_3x^2 + 2a_2x + a_1 \\ &= 3a_3(x - \alpha)(x - \beta) \\ &= a_3\left[(x - x_1)(x - x_2) + (x - x_1)(x - x_3) + (x - x_2)(x - x_3)\right]. \end{aligned}$$

Then

$$\begin{aligned} f(\alpha)f(\beta) &= a_3^2(x_1-\alpha)(x_1-\beta)(x_2-\alpha)(x_2-\beta)(x_3-\alpha)(x_3-\beta) \\ &= a_3^2\frac{f'(x_1)}{3a_3}\frac{f'(x_2)}{3a_3}\frac{f'(x_3)}{3a_3} \\ &= -\frac{a_3^2}{27}P^2 = \frac{D}{-27a_3^2}. \end{aligned}$$

Therefore, $D = -27a_3^3 f(\alpha)f(\beta)$.

□

Exercises 5.6

1. Solve $27\,x^3 - 135\,x^2 + 117\,x + 55 = 0$ given that the roots form an arithmetic progression (AP); that is, roots are expressed as $\alpha - \beta$, α and $\alpha + \beta$.

2. Solve $2\,x^3 - 7\,x^2 + 7\,x - 2 = 0$ given that the roots form a geometric progression (GP) with common ratio $\frac{1}{2}$; that is, roots are expressed as 2α, α, $\frac{\alpha}{2}$.

3. Let $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$, $a_i \in \mathbf{R}$ for $i = 0, 1, \ldots, 4$.
   Suppose that $f(x) = 0$ has roots x_1, x_2, …, x_5.

   Let $\Lambda_n = \{1, 2, \ldots, n\}$. We define the symmetric polynomial of $x_1, x_2, \ldots, x_n$ of degree k, $k = 1, 2, \ldots, n$ by

   $$s_{n,k}(x_1, \cdots, x_n) = \sum_{A\subset\Lambda_n, |A|=k} \left(\prod_{t\in A} x_t\right),$$

   where $|A|$ is the number of elements of A.

   (a) Write $s_{5,3}(x_1, \cdots, x_5)$ without using notations $\sum$ and $\prod$.

   (b) Write each of a_4, a_3, a_2, a_1 and a_0 with the notation $s_{5,k}$, $k = 1, \ldots, 5$.

   (c) Suppose that $f''(x) = 0$ has roots α_1, α_2 and α_3.
   Prove that

   $$\frac{s_{3,2}(\alpha_1, \alpha_2, \alpha_3)}{3} = \frac{s_{5,2}(x_1, x_2, x_3, x_4, x_5)}{10}.$$

5.7 Formulae for Solving Cubic Equations

Every polynomial equation degree four or lower has a solution that is constructed by applying the addition, subtraction, multiplication, division and radical to known numbers (coefficients). This solution is called an **algebraic solution**.
Algebraic solutions for cubic and quartic equations were found in 16th century Italy.
First, we introduce Cardano's method, then Lagrange's method to solve the cubic equations.

Cardano's method

$$f(x) = x^3 + a_2x^2 + a_1x + a_0 = 0. \tag{5.10}$$

Let $x = y - \frac{a_2}{3}$. Substituting this to (5.10), we obtain

$$\begin{aligned} & \left(y - \frac{a_2}{3}\right)^3 + a_2\left(y - \frac{a_2}{3}\right)^2 + a_1\left(y - \frac{a_2}{3}\right) + a_0 \\ = \; & y^3 - \frac{1}{3}\left(a_2^2 - 3a_1\right)y + \frac{1}{27}\left(2a_2^3 - 9a_2a_1 + 27a_0\right). \end{aligned}$$

Thus we can consider the following equation.

$$x^3 + ax + b = 0. \tag{5.11}$$

Put

$$x = u + v. \tag{5.12}$$

Then

$$u^3 + v^3 + (3uv + a)(u + v) + b = 0$$

Therefore, if u and v satisfy

$$\begin{aligned} u^3 + v^3 + b &= 0, \\ 3uv + a &= 0, \end{aligned}$$

then $x = u + v$ satisfies (5.11). Thus

$$\begin{aligned} u^3 + v^3 &= -b, \\ uv &= -\frac{a}{3} \end{aligned}$$

and from these, we obtain the quadratic equation.

$$t^2 + bt - \frac{a^3}{27} = 0.$$

This equation is called a **resolvant equation**. We get

$$u^3 = \frac{-b}{2} + \sqrt{R}, \tag{5.13}$$

$$v^3 = -\frac{-b}{2} - \sqrt{R}, \tag{5.14}$$

where $R = \frac{b^2}{4} + \frac{a^3}{27}$.

$$u = \sqrt[3]{\frac{-b}{2} + \sqrt{R}} \qquad v = \sqrt[3]{\frac{-b}{2} - \sqrt{R}}$$

Substituting these to (5.35),

$$x = \sqrt[3]{\frac{-b}{2} + \sqrt{R}} + \sqrt[3]{\frac{-b}{2} - \sqrt{R}}$$

$$v = \frac{-a}{3u}.$$

Let ω be a complex cubic root of 1. Then the roots of (5.13) are u, ωu and $\omega^2 u$ and corresponding roots of (5.14) are v, $\omega^2 v$ and ωv respectively. Thus we have:

$$\begin{aligned} x_1 &= u + v \\ x_2 &= \omega u + \omega^2 v \\ x_3 &= \omega^2 u + \omega v \end{aligned}$$

5.8 Lagrange's method

Quadratic Equations
Consider

$$x^2 + ax + b = 0. \tag{5.15}$$

Let x_1 and x_2 be roots of the equation.
It is known that

$$x_1 + x_2 = -a$$
$$x_1 x_2 = b$$

Let $u = x_1 - x_2$. For $\sigma \in S_2$, we denote applying σ to the variables $\{x_1, x_2\}$ by u^σ. Then for $\sigma = (12) \in S_2$,

$$u^\sigma = -u.$$

We can express the roots x_1 and x_2 by

$$x_1 = \frac{1}{2}(u + (x_1 + x_2)) = \frac{1}{2}(u - a) \tag{5.16}$$

$$x_2 = -\frac{1}{2}(u - (x_1 + x_2)) = -\frac{1}{2}(u + a) \tag{5.17}$$

Consider the equation:

$$\prod_{\sigma \in S_2} (X - u^\sigma) = 0 \tag{5.18}$$

The left hand side is:

$$\begin{aligned}(X-u)(X+u) &= X^2 - u^2 \\ &= X^2 - (x_1 - x_2)^2 \\ &= X^2 - \{(x_1 + x_2)^2 - 4x_1x_2\} \\ &= X^2 - (a^2 - 4b) \\ \therefore \quad X^2 - (a^2 - 4b) &= 0 \\ u &= \sqrt{a^2 - 4b} \quad (x_1 > x_2).\end{aligned}$$

$$x_1 = \frac{1}{2}(-a + \sqrt{a^2 - 4b}),$$
$$x_2 = -\frac{1}{2}(a + \sqrt{a^2 - 4b}).$$

This u is called the resolvent.

Cubic Equations

Consider

$$x^3 + ax^2 + bx + c = 0. \tag{5.19}$$

Let x_1, x_2 and x_3 be roots of the equation. The left hand side of the equation is:

$$(x - x_1)(x - x_2)(x - x_3)$$

It can be seen that

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_1x_3 + x_2x_3 &= b \\ x_1x_2x_3 &= -c \end{aligned}$$

By applying every $\sigma \in S_3$ to the coefficients, they are not changed.

Let

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

Let

$$u = x_1 + \omega x_2 + \omega^2 x_3 \tag{5.20}$$
$$v = u^{\sigma_2} = x_1 + \omega^2 x_2 + \omega x_3 \tag{5.21}$$

To find u and v

$$\prod_{\sigma \in S_3} (X - u^\sigma) = 0 \tag{5.22}$$

Here $S_3 = \{e, \sigma_1, \sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1\}$.
The left hand side of (5.22) is:

$$(X-u)(X-u^{\sigma_1\sigma_2})(X-u^{\sigma_2\sigma_1})(X-u^{\sigma_2})(X-u^{\sigma_1})(X-u^{\sigma_1\sigma_2\sigma_1}) \tag{5.23}$$
$$= (X-u)(X-\omega^2 u)(X-\omega u)(X-v)(X-\omega v)(X-\omega^2 v) \tag{5.24}$$
$$= (X^3-u^3)(X^3-v^3) \tag{5.25}$$
$$= (X^3)^2 - (u^3+v^3)X^3 + u^3v^3 \tag{5.26}$$

u^3, v^3 are roots of

$$t^2 - At + B^3 = 0 \tag{5.27}$$

$$a = x_1 + x_2 + x_3 \tag{5.28}$$
$$u = x_1 + \omega x_2 + \omega^2 x_3 \tag{5.29}$$
$$v = x_1 + \omega^2 x_2 + \omega x_3 \tag{5.30}$$

Multiplying $1, 1, 1$ or $1, \omega^2, \omega$ or $1, \omega, \omega^2$ to them and adding them, we obtain

$$x_1 = \frac{1}{3}(a + u + v), \tag{5.31}$$
$$x_2 = \frac{1}{3}(-a + \omega^2 u + \omega v), \tag{5.32}$$
$$x_3 = \frac{1}{3}(-a + \omega u + \omega^2 v). \tag{5.33}$$

Quatic Equations
Consider

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{5.34}$$

We can make rational expressions of roots of the equation x_1, x_2, x_3, x_4 such that by permutation of roots, we obtain three distinct forms.

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_2x_4 \quad y_3 = x_1x_4 + x_2x_3$$

A symmetric expression of y_1, y_2, y_3 can be obtained from coefficients of $f(x)$, since it is symmetric on x_1, x_2, x_3. This implies that y_1, y_2, y_3 are roots of resolvent equation of degree 3.
Let

$$u = (x_1+x_2)-(x_3+x_4), \quad v = (x_1+x_3)-(x_2+x_4), \quad w = (x_1+x_4)-(x_2+x_3).$$

Then every symmetric expression of u_1^2, u_2^2, u_3^2 is symmetric expression of x_1, x_2, x_3, x_4. Setting

$$\begin{aligned} A &= u^2+v^2+w^2 \\ B &= u2v^2+u^2w^2+v^2w^2 \\ C &= uvw, \end{aligned}$$

u^2, v^2, w^2 are roots of the resolvent equation of degree 3:

$$t^3 - At^2 + Bt - C^2 = 0.$$

Let the roots be t_1, t_2 and t_3.

$$u = \pm\sqrt{t_1}, \quad v = \pm\sqrt{t_2}, \quad w = \pm\sqrt{t_3}.$$

$$x_1+x_2+x_3+x_4 = -a, \quad x_1+x_2-x_3-x_4 = \sqrt{t_1},$$
$$x_1-x_2+x_3-x_4 = \sqrt{t_2} \quad x_1-x_2-x_3+x_4 = \sqrt{t_3}.$$

Then we obtain the following.

$$\begin{aligned} 4x_1 &= -a+\sqrt{t_1}+\sqrt{t_2}+\sqrt{t_3}, \\ 4x_2 &= -a+\sqrt{t_1}-\sqrt{t_2}-\sqrt{t_3}, \\ 4x_3 &= -a-\sqrt{t_1}+\sqrt{t_2}-\sqrt{t_3}, \\ 4x_4 &= -a-\sqrt{t_1}-\sqrt{t_2}+\sqrt{t_3}. \end{aligned}$$

5.9 Abel's Theorem

Let $f(x) = 0$ be a polynomial equation with coefficients in a field K. Then the relation between roots and coefficients shows that each coefficient of $f(x)$ is expressed by a symmetric expression of roots. Therefore, every rational expression of coefficients is expressed by a rational expression of roots. This means that the coefficient field K consists of rational expressions of roots.

Example 5.9.1. The set of rational numbers $\mathbf{Q}$, the set of real numbers $\mathbf{R}$ and the set of complex numbers $\mathbf{C}$ are fields.

Lemma 5.9.1. *Let K be a field, and let p be a prime number. Suppose that $r \in K$ and $\sqrt[p]{r} \notin K$. Then every element of $K(\sqrt[p]{r})$ is expressed as*

$$a_0 + a_1\sqrt[p]{r} + a_2(\sqrt[p]{r})^2 + \cdots + a_{p-1}(\sqrt[p]{r})^{p-1},$$

where $a_0, a_1, \ldots, a_{p-1} \in K$.

Example 5.9.2. The equation $x^2 - 2x - 1 = 0$ has roots $x = 1 \pm \sqrt{2} \notin \mathbf{Q}$ but $x = 1 \pm \sqrt{2} \in \mathbf{Q}(\sqrt{2})$.

Definition 5.9.3. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ be a polynomial equation of degree n with coefficients in a field K. The equation $f(x) = 0$ is **solvable by radicals** or **algebraically solvable** if it has roots in a field which is obtained by adding a finite number of radicals to K.

Lemma 5.9.2. *Let $x_1, x_2, \ldots, x_n$ be roots of the equation:*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Then the coefficients of the equation are expressed by an elementary symmetric expressions of $x_1, x_2, \ldots, x_n$.

Lemma 5.9.3. *Suppose that the equation*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with coefficients in a field K, is algebraically solvable. Then every p-th root of the number $r \in K$ in the solution is expressed as a rational expression of roots $x_1, x_2, \ldots, x_n$ of $f(x)$ and p-th roots of 1.

Theorem 5.9.4 (Abel's Impossibility Theorem (1826))**.** *There is no general algebraic solution to polynomial equations of degree five or higher.*

Proof. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{5.35}$$

be an irreducible equation with $a_0, a_1, \ldots, a_{n-1} \in K$. Suppose that $f(x) = 0$ is solvable by radicals. Let $n \geq 2$ and let x_1, x_2, x_n be roots of the equation. Then $x_1, x_2, \ldots, x_n \notin K$ as (5.35) is irreducible.
Take $r \in K$ and suppose that $\sqrt[p]{r}$ is the first radical to add to K, where p is a prime. As $\sqrt[p]{r} \notin K$, it is not expressed as a symmetric expression of $x_1, x_2, \ldots, x_n$. Thus

$$\sqrt[p]{r} = \varphi(x_1, x_2, \ldots, x_n).$$

is a rational expression but not symmetric expression of $x_1, x_2, \ldots, x_n$.
There is a transposition σ such that σ changes φ. We may assume that the transposition, $\sigma = (12)$ changes φ.

$$(\varphi)^\sigma = \varphi' \neq \varphi. \tag{5.36}$$

On the other hand, since φ^p is symmetric,

$$\begin{aligned} (\varphi')^p &= (\varphi^p)^\sigma = \varphi^p \\ \varphi' &= \varepsilon\varphi, \end{aligned} \tag{5.37}$$

where ε is the p-th root of 1.
Since $\varphi = \varphi^{\sigma^2} = (\varphi')^\sigma = \varepsilon(\varphi)^\sigma = \varepsilon\varphi'$, $\varphi = \varepsilon\varphi'$. We have the following.

$$\varphi = \varepsilon\varphi' = \varepsilon(\varepsilon\varphi) = \varepsilon^2\varphi$$

Therefore as $\varepsilon^2 = 1$ and $\varepsilon \neq 1$, $\varepsilon = -1$. Also $\varepsilon^p = 1$ and p is is prime, hence $p = 2$.
This implies that the first radical to be added is the square root of $r \in K$. This must be an alternating expression of $x_1, x_2, \ldots, x_n$.
Every element of $K_1 = K(\sqrt{r})$ is expressed as $k_1 + k_2\sqrt{r}$, where k_1, k_2 are expressed by symmetric expressions of $x_1, x_2, \ldots, x_n$, and $\sqrt{r}$ is expressed by an alternating expression of $x_1, x_2, \ldots, x_n$; and it is not changed by an even permutation of $x_1, x_2, \ldots, x_n$. We denote the next radical to be added to K_1

by $\sqrt[q]{r_1}$ with prime q and $r_1 \in K_1$.
Suppose that $\sqrt[q]{r_1}$ is expressed by a rational expression of roots $x_1, x_2, \ldots, x_n$ and the q-th root of 1:

$$\sqrt[q]{r_1} = \psi(x_1, x_2, \ldots, x_n).$$

Since $\psi \notin K_1$, it will be changed by applying a cyclic permutation of three variables such as $\tau = (1, 2, 3)$:

$$(\psi)^\tau = \psi' \neq \psi. \tag{5.38}$$

But $\psi^q \in K_1$ and it is not changed by τ and thus

$$\begin{aligned}(\psi^q)^\tau &= ((\psi)^\tau)^q \\ &= \psi'^q \\ &= \psi^q \\ \therefore\ \psi^q &= \psi'^q,\end{aligned}$$

Therefore,

$$\psi' = \omega\psi, \quad w^q = 1, \quad \omega \neq 1.$$

That is,

$$\psi' = (\psi(x_1, x_2, x_3, \cdots))^\tau = \psi(x_2, x_3, x_1, \cdots) = \omega\psi(x_1, x_2, x_3, \cdots).$$

On both sides of this equation, applying τ twice, we obtain:

$$\begin{aligned}(\psi(x_2, x_3, x_1, \cdots))^\tau = \psi(x_3, x_1, x_2, \cdots) &= \omega\psi(x_2, x_3, x_1, \cdots) \\ (\psi(x_3, x_1, x_2, \cdots))^\tau = \psi(x_1, x_2, x_3, \cdots) &= \omega\psi(x_3, x_1, x_2, \cdots) \\ &= \omega^2\psi(x_2, x_3, x_1, \cdots) \\ &= \omega^3\psi(x_1, x_2, x_3, \cdots)\end{aligned}$$

Therefore,

$$\omega^3 = 1.$$

Since $\omega \neq 1$, $\omega^3 = 1$, q is a multiple of 3, and q is prime, $q = 3$.

Consider $n \geq 5$. Let $\tau' = (12345)$ be the cyclic permutation of length 5. $(\psi^3)^{\tau'} = \psi^3$ as $\psi^3 = r_1 \in K_1$.

$$\begin{aligned}(\psi^3)^{\tau'} &= ((\psi)^{\tau'})^3, \\ &= \psi^3, \\ \therefore\ (\psi)^{\tau'} &= \omega\psi.\end{aligned}$$

But $\tau'^5 = 1$ and thus we obtain

$$(\psi)^{\tau'^5} = (\omega\psi)^{\tau'^4} = \cdots = \omega^5\psi.$$

This implies that $\omega^5 = 1$. Thus $\omega = 1$. Then ψ is not changed by τ'. However, $(13245)(32154) = (123)$ is a product of two cyclic permutations. This shows that ψ is not changed by $\tau = (123)$. This contradicts (5.38). This implies that it is impossible to have $\psi(x_1, \ldots, x_n)$ for $n \geq 5$ such that ψ is not an alternating expression but ψ^q is an alternating expression. If there

is no such ψ and if $f(x) = 0$ is solvable with radicals, then the radicals are only square roots. Therefore, the root x_1 is expressed as:

$$x_1 = S_1 + PS_1,$$

where S_1 and S_2 are symmetric polynomials and P is the descriminant defined at (5.8). The right hand side is invariant under any even permutation thus it cannot be an identity. Therefore, every polynomial equation with degree greater than four is not solvable by only radicals. □

Exercises 5.7-5.9

1. Use Cardano-Tartalia's method to solve:
   (a) $x^3 - 24x + 72 = 0$
   (b) $x^3 + 3x + 2 = 0$.

Chapter 6

Permutations and Combinations

We often need to enumerate the number of all possible cases. For example, how many possible ways to select three members of a committee from seven members. In this chapter we learn the permutations and combinations, as well as pegionhole principle.

6.1 Permutations

Let A, B, C, D and E be five letters. We want to know the number of arrangements of these letters using each letter **once**.
First, we fix the first letter, say A, then the second choice will be one of 4 letters B, C, D, and E. Fix the second letter, say B, then the third choice will be one of C, D and E ans so on.
This implies that the number of the possible first letter is 5, and then for each first letter, the number of possible letters in the second place is 4, and then for each second letter, the number of possible letters in the third place is 3 and so on. Therefore, the total number of possible sequences is given by

$$5 \times 4 \times 3 \times 2 \times 1.$$

This is denoted by 5!.
If we can use the same letter as many as we want, then the number of arrangements is given by

$$5 \times 5 \times 5 \times 5 \times 5 = 5^5$$

Arrangements of n objects

The number of arrangements of n letters using each letter once is:

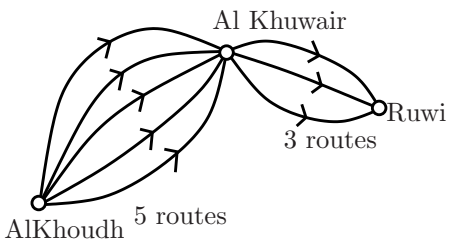
$$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1.$$

If the same letter can be used as many as we want, then the number of arrangements is given by

$$n^n = n \times n \times \cdots \times n \quad (n \text{ times}).$$

Q1. Suppose there are five routes from AlKhoudh to AlKhuwair and three routes from Al Khuwair to Ruwi.

If we use each route once and do not go backwards, how many possible routes exist from AlKhoudh to Ruwi?



Addition Principle

If one operation can be performed in r different ways and a second operation can be performed in s different ways and two operations cannot be performed simultaneously, then there are $r + s$ different ways to perform one of the operations.

6.2 Circular arrangements

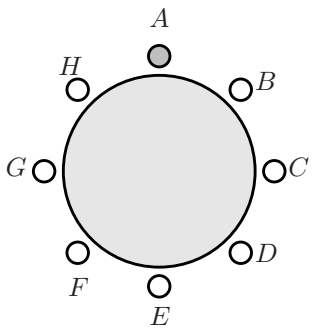
We want to know how many circular arrangements of n distinct objects.

Fix one object. Then the number of arrangements of $n-1$ objects is $(n-1)!$. Suppose that the fixed object moves to another place. Then identical arrangements will be made. This says we do not distinguish these identical arrangement. Therefore, the number of circular arrangements of n distinct objects is $(n-1)!$.

Circular arrangements

The number of circular arrangements of n distinct objects is given by

$$(n-1)! = (n-1) \times (n-2) \times \cdots \times 1.$$



If no distinction is made between clockwise and counter clockwise arrangements, then the total number is half this amount, namely

$$\frac{(n-1)!}{2}.$$

Permutations of n things taken r at a time

The number of permutations of n objects taken r at a time is given by

$$\begin{aligned} {}_nP_r &= n(n-1)(n-2)\cdots(n-(n-1)) \\ &= \frac{n!}{(n-r)!} \end{aligned}$$

6.3 Selections

Let $S = \{A, B, C, D, E\}$ be a set of five letters. We want to know the number of subsets of three letter of S. Here $\{A, B, C\}$ and $\{A, C, B\}$ and $\{B, C, A\}$ are not distinguished.

First, we choose three elements from five; that is the number of selections is ${}_5P_3$. In this counting we do not distinguish 3! of subsets consisting of three elements of S. Therefore, the number of subsets of three elements of S is given by

$$\frac{{}_5P_3}{3!}.$$

Selections of r objects from the set of n objects

The number of ways of selecting r objects from n different objects is called the number of combinations of r objects chosen from n different objects, and is denoted by ${}_nC_r$ or $\begin{pmatrix} n \\ r \end{pmatrix}$.

$$ {}_nC_r = \frac{{}_nP_r}{r!} = \frac{n!}{r!(n-r)!} $$

6.4 Binomial Theorem

Lemma 6.4.1. *For $n \geq 1$,*

$$ {}_nC_r = {}_nC_{n-r} $$

Proof.

$$ \begin{aligned} {}_nC_r &= \frac{n!}{(n-r)!r!} \\ &= \frac{n!}{r!(n-r)!} \\ &= {}_nC_{n-r} \end{aligned} $$

□

Lemma 6.4.2.

$$ {}_kC_{r+1} + {}_kC_r = {}_{k+1}C_{r+1} $$

Proof.

$$ \begin{aligned} \text{LHS} &= \frac{k!}{(k-r-1)!(r+1)!} + \frac{k!}{(k-r)!r!} \\ &= \frac{k!(k-1) + k!(r+1)}{(k-r)!(r+1)!} \\ &= \frac{k!(k-r+r+1)}{(k-r)!(r+1)!} \\ &= \frac{(k+1)!}{(k-r)!(r+1)!} \\ &= {}_{k+1}C_{r+1} \end{aligned} $$

□

Binomial Theorem

$$\begin{aligned}(a+b)^n &= \sum_{r=0}^{n}({}_nC_r)a^{n-r}b^r \\ &= \sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r\end{aligned}$$

Proof. Let $P(n)$ be "$(a+b)^n = \sum_{r=0}^{n} {}_nC_r a^{n-r}b^r$, $(n \geq 0)$".
$n = 0$: The $LHS = (a+b)^0 = 1$ and $RHS = {}_0C_0 a^{0-0}b^0 = 1$. $\therefore$ $P(0)$ is true.
Suppose that $P(k)$ is true for $k \geq 0$:

$$(a+b)^k = \sum_{r=0}^{k} {}_kC_r a^{k-r}b^r \tag{6.1}$$

Consider $(a+b)^{k+1}$:

$$\begin{aligned}(a+b)^{k+1} &= (a+b)\sum_{r=0}^{k} {}_kC_r a^{k-r}b^r \\ &= \sum_{r=0}^{k} {}_kC_r (a+b)a^{k-r}b^r \\ &= \sum_{r=0}^{k} {}_kC_r (a^{k-r+1}b^r + a^{k-r}b^{r+1}) \\ &= \sum_{r=0}^{k} {}_kC_r a^{k-r+1}b^r + \sum_{r=0}^{k} {}_kC_r a^{k-r}b^{r+1}\end{aligned}$$

Let $s = r - 1$. Then $r = s + 1$ and the last hand side is:

$$\begin{aligned}&{}_kC_0 a^{k+1}b^0 + \sum_{s=0}^{k} {}_kC_{s+1} a^{k-s}b^{s+1} + \sum_{r=0}^{k} {}_kC_r a^{k-r}b^{r+1} \\ = \;& {}_kC_0 a^{k+1}b^0 + \sum_{r=0}^{k}({}_kC_{r+1} + {}_kC_r)a^{k-r}b^{r+1}\end{aligned} \tag{6.2}$$

We know that ${}_kC_{r+1} + {}_kC_r = {}_{k+1}C_{r+1}$. Therefore the last term will be:

$${}_kC_0 a^{k+1}b^0 + \sum_{r=0}^{k} {}_{k+1}C_{r+1} a^{k-r}b^{r+1} = \sum_{r=0}^{k+1} {}_{k+1}C_r a^{k+1-r}b^r \tag{6.3}$$

Thus $P(k+1)$ is true. Therefore, $P(n)$ is ture for all $n \geq 0$. □

6.5 Pigeonhole Principle

Pigeonhole Principle

If n items are put in k boxes ($k < m$), then there is at least one box which contains at least

$$\left\lceil \frac{n}{k} \right\rceil$$

items.

Example 6.5.1. There are 31 students in the class. Then at least 3 students have the same birth month.

Solution.
By the peigeonhole principle, at least $\lceil \frac{31}{12} \rceil = 3$ students have the same birth month.

Example 6.5.2. What is the minimum number of students required in a class to be sure that at least six will receive the same grade (possible grades are A, B, C, D, F)?

Exercises 6.1-6.5

---

1. In how many ways can we arrange the letters $AAABBBBCCDDEF$ in a row so that the letters B are separated from one another?

2. For the expansion of $(x + \sqrt{x})^{20}$, find the coefficient of x^{17}.

3. Take 16 distinct integers. Show that there exist at least two distinct pairs of numbers such that the difference of each pair is divisible by 5.

4. Suppose that there is a group of 8 students, A, B, C, D E, F, G and H. Suppose that A, B, C and D are boys and E, F, G and H are girls. In how many ways can we choose 5 students from the group in which each choice includes at least 3 girls? Complete the calculation.

5. In how many ways can 20 books be arranged on a shelf so that 3 particular books are put together?

6. Evaluate ${}_5C_3$ and ${}_5C_2$.

7. Show that ${}_nC_r = {}_n C_{n-r}$.

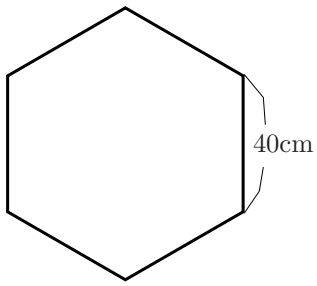
8. How many groups of 5 people can be made from 12 people.

9. Prove the binomial theorem.

10. Suppose there is a group of thirteen people. At least two people exist and they were born in the same month.

11. A square target of dimension 70cm × 70cm. A man shoots against the target 50 shots. All hit the target. Show that there are at least 2 points such that the distance between them is less than 15cm.

12. A man gave 25 shots on a regular hexagonal target. (See the figure below. It is a 6-gon with equal sides and equal inner angles.) All shots hit the target. If the side length is 40cm, then prove that there are at least two shots such that the distance between them is less than 21cm.



13. Let A, B, C, D and E be distinct five points in $\mathbb{Z} \times \mathbb{Z}$. Prove that there is at least one pair of points whose mid point is also in $\mathbb{Z} \times \mathbb{Z}$.

14. Let a, b, c and d be distinct four integers. Prove that there are two numbers of the four such that the difference of them is divisible by 3.

Chapter 7

Multibase Arithmetic

7.1 Notations

Every number can be expressed as a number to a specific base. For example, 3456.98 is expressed as

$$\begin{aligned} 3456.98 &= (3\times 1000)+(4\times 100)+(5\times 10)+6\times 1+(9\times \frac{1}{10})+(8\times \frac{1}{100}) \\ &= 3\times 10^3+4\times 10^2+5\times 10^1+6\times 10^0+9\times 10^{-1}+8\times 10^{-2} \end{aligned}$$

The number M to base $n>0$ will be denoted by M_n. For example,

$$\begin{aligned} 100011_2 &= 1\times 2^5+1\times 2+1=35_{10} \\ 35_{10} &= 3\times 10+5\times 10^0 \\ 35_{16} &= 2\times 16+3\times 16^0 \\ 35_{60} &= 35\times 60^0 \end{aligned}$$

Usually, for base 16, we use numbers and letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. For example,

$$2AF_{16}=2\times 16^2+10\times 16+15.$$

Example 1. Convert the number 13.35_8 to base 10.

$$\begin{aligned} 13.35 &= 1\times 8+3\times 8^0+3\times \frac{1}{8}5\times \frac{1}{8^2} \\ &= 8+3+\frac{3}{8}+\frac{5}{64} \\ &= \left(11+\frac{29}{64}\right)_{10} \end{aligned}$$

7.2 Conversion From Base 10

We can convert denary numbers into n-ary numbers.

Example Convert 2375_{10} to base 8.

8	$\underline{2375}$		
8	$\underline{296}$	7	$2375 = 8 \times 296 + 7$
8	$\underline{37}$	0	$296 = 8 \times 37 + 0$
8	$\underline{4}$	5	$37 = 8 \times 4 + 5$

$\therefore 2375_{10} = 4507_8$.

7.2.1 Shortcut conversion

We can see that $2375_{10} = 10101000111_2$. As we know $2^3 = 8$: $1000_2 = 8$, each triple from the right hand in the binary expression means the remainder when the number is divided by 8.

$$\begin{aligned} 2375_{10} &= 10\ 101\ 000\ 111_2 \\ &= 4507_8 \end{aligned}$$

Example Convert the number 1101.1011_2 to base 4 and 8.
For $n = 4$, as we know $2^2 = 4$: $100_2 = 4_{10}$, each pair from the decimal point means the remainders when the number is divided by 4.

$$11\ 01.\ 10\ 11_2 = 31.23_4$$

For $n = 8$, we divide the binary number into triples from the decimal point:

$$001\ 101.\ 101\ 100_2 = 15.54_8$$

7.3 Approximation

We often need to have an approximation to the original number. For example, an approximation to the number 39.76_{10} may be suggested by either 39.7_{10} or 39.8_{10}.
Quoting 39.7_{10} is called **rounding down** and quoting 39.8 is called **rounding up**.
Also we offer an n-decimal place approximation. For example,

$$7.805_{10} = 7.81_{10} \quad (2 \text{ dp} = 2 \text{ decimal places.})$$

Examples

$$\begin{aligned} 8.3846_{10} &= 8.385_{10} \ (3 \text{ dp}) \\ 8.3846_{10} &= 8.38_{10} \ (2 \text{ dp}) \\ 8.3856_{10} &= 8.39_{10} \ (2 \text{ dp}) \end{aligned} \tag{7.1}$$

7.4 Addition

We consider the addition of two numbers.
For example, we find the sum of 656.1_7 and 335.4_7.

7^3	7^2	7	7^0	7^{-1}
	6	5	6	1
	3	3	5	4
	9	8	11	5
		9	4	5
	10	2	4	5
1	3	2	4	5

Therefore, $656.1_7 + 335.4_7 = 1324.5_7$

Q. Find the sum of 678_9 and 1756_9.

7.5 Subtraction

We consider the subtraction $656.1_7 - 365.4_7$

7^3	7^2	7	7^0	7^{-1}
	6	5	6	1
	5	$5+7$	5	$1+7$
	3	6	5	4
	2	6	0	4

Therefore, $656.1_7 - 365.4_7 = 260.4_7$

7.6 Multiplication

We have the following law:

$$abcd_n \times 10_n = abcd0_n$$

For example, $123_8 \times 10_8 = 1230_8$.

Therefore, we can multiply two numbers 254_6 and 121_6 as follows:

$$\begin{aligned} 254_6 \times 121_6 &= 254_6 \times 100_6 + 254_6 \times 20_6 + 254_6 \times 1 \\ &= 25400_6 + 5520_6 + 254_6 \\ &= 40014_6 \end{aligned} \tag{7.2}$$

7.7 Division

This is the most difficult operation among the four: $(+, -, \times, \div)$. We need a multiplication table to carry out the division.

Example Divide 5812_{10} by 18_{10}.

Divisor	Quotient	Dividend
18		5812
		58
	3	54
		41
	2	36
		52
	2	36
		16

The result is $5812_{10} \div 18_{10} = 322_{10}$ remainder 16_{10}.

Example We consider $141222_5 \div 33_5$. First we need to provide a times table.

$33_5 \times 1$	33_5
$33_5 \times 2$	121_5
$33_5 \times 3$	204_5
$33_5 \times 4$	242_5
$33_5 \times 10_5$	330_5
$33_5 \times 11_5$	413_5

Divisor	Quotient	Dividend
33_5		141222_5
		141
	2	121
		202
	2	121
		312
	4	242
		202
	2	121
		31

$\therefore 141222_5 \div 33_5 = 2242_5$ remainder 31_5.

Exercises 7.2-7.6

---

1. Convert the numbers to base 10.
   (a) 121_8
   (b) 12.16_7
   (c) 53.14_6
2. Convert the numbers to base n.
   (a) 2375_1; $n = 2$
   (b) 1101.1011_2; $n = 16$
3. Use the table to do $13461_7 \div 25_7$.

$25_7 \times 1$	25_7
$25_7 \times 2$	53_7
$25_7 \times 3$	111_7
$25_7 \times 4$	136_7
$25_7 \times 5$	164_7
$25_7 \times 6$	222_7
$25_7 \times 10_7$	250_7

4. Use the table to do $1234560_7 \div 35_7$.

$35_7 \times 1$	35_7
$35_7 \times 2$	103_7
$35_7 \times 3$	141_7
$35_7 \times 4$	206_7
$35_7 \times 5$	244_7
$35_7 \times 6$	312_7
$35_7 \times 10_7$	350_7

Chapter 8

Linear Transformations

8.1 Vector spaces

DEFINITION A set V is called a **vector space** if it satisfies the following properties.

(V0) $\mathbf{U} + \mathbf{V}$ is defined for all $\mathbf{U}, \mathbf{V} \in V$.

(V1) $\mathbf{U} + \mathbf{V} = \mathbf{V} + \mathbf{U}$ for all $\mathbf{U}, \mathbf{V} \in V$.

(V2) $(\mathbf{U} + \mathbf{V}) + \mathbf{W} = \mathbf{U} + (\mathbf{V} + \mathbf{W})$ for $\mathbf{U}, \mathbf{V}, \mathbf{W} \in V$.

(V3) There exists an element $\mathbf{O} \in V$ such that $\mathbf{V} + \mathbf{O} = \mathbf{O} + \mathbf{V}$ for all $\mathbf{V} \in V$.

(V4) For all $\mathbf{V} \in V$, there exists $\mathbf{V}' \in V$ such that $\mathbf{V} + \mathbf{V}' = \mathbf{V}' + \mathbf{V} = \mathbf{O}$. (We write $\mathbf{V}' = -\mathbf{V}$ called the inverse of $\mathbf{V}$.)

Let K be a field.

(V5) For any $\mathbf{V} \in V$, $d \in K$, $d\mathbf{V}$ is defined.

(V6) $a(\mathbf{U} + \mathbf{V}) = a\mathbf{U} + a\mathbf{V}$ for all $a \in K$.

(V7) $(a + b)\mathbf{V} = a\mathbf{V} + b\mathbf{V}$ for all $a, b \in K$.

(V8) $(ab)\mathbf{V} = a(b\mathbf{V})$ for all $a, b \in K$.

(V9) $1\mathbf{V} = \mathbf{V}$.

Each element $\mathbf{V}$ of V is called a **vector** and $a \in K$ is called a **scalar**.

Example 8.1.1. Let $K = \mathbf{C}$ or $\mathbf{R}$, the set of convergent series:

$$\left\{ \sum_{k=0}^{\infty} x_k \mid x_k \in K \right\}$$

is a vector space.

Example 8.1.2. The set of all polynomials:

$$K[t] = \{ f(t) = a_0 + \cdots + a_n t^n \mid a_i \in K, n = 0, 1, 2 \ldots \}$$

is a vector space.

$$K^{(n)}[t] = \{ f(t) = a_0 + \cdots + a_m t^m \mid 0 \leq m \leq n \}$$

is also a vector space.

Example 8.1.3. The set of all real valued functions defined on $[0, 1]$ is a vector space.

Example 8.1.4. The product space $K^n = K \times K \times \cdots K$ $(n \geq 0)$ is a vector space. For $\mathbf{X} = (x_1, x_2, \ldots, x_n), \mathbf{Y} = (y_1, y_2, \ldots, y_n) \in K^n$, the addition $\mathbf{X} + \mathbf{Y}$ is defined by $(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$.

Proposition 8.1.1. *For a vector space V, $\mathbf{O} \in V$ is unique.*

Proof. Let $\mathbf{O}'$ satisfy the condition $\mathbf{O}' + \mathbf{V} = \mathbf{V} + \mathbf{O}' = \mathbf{V}$ for $\mathbf{V} \in V$. Then if $\mathbf{V} = \mathbf{O}$, then $\mathbf{O}' + \mathbf{O} = \mathbf{O} + \mathbf{O}' = \mathbf{O}$. Also by the property of $\mathbf{O}$, if $\mathbf{V} = \mathbf{O}'$, then $\mathbf{O} + \mathbf{O}' = \mathbf{O}' + \mathbf{O} = \mathbf{O}'$. Therefore, $\mathbf{O} = \mathbf{O}'$. □

Proposition 8.1.2. *Let V be a vector space. For each $\mathbf{V}$, its inverse is unique.*

Proof. Let $\mathbf{V}'$ and $\mathbf{V}''$ be inverses of $\mathbf{V}$, that is, $\mathbf{V}' + \mathbf{V} = \mathbf{V} + \mathbf{V} = \mathbf{O}$ and $\mathbf{V}'' + \mathbf{V} = \mathbf{V} + \mathbf{V}'' = \mathbf{O}$.
Thus $\mathbf{V}' = \mathbf{V}' + \mathbf{O} = \mathbf{V}' + (\mathbf{V} + \mathbf{V}'') = (\mathbf{V}' + \mathbf{V}) + \mathbf{V}'' = \mathbf{O} + \mathbf{V}'' = \mathbf{V}''$. □

Example 8.1.5. Let $V = \mathbf{R}$ and let $K = \mathbf{R}$. Then V is a vector space.

Example 8.1.6. Let $V = \mathbf{R}^2$, and let $K = \mathbf{R}$. Then V is a vector space. For points $(x, y), (u, v) \in V$, $(x, y) + (u, v) = (x + u, y + v)$.

8.2 Vectors in the plane

We denote a point (x, y) in the plane $\mathbf{R}^2$ by $\mathbf{X} = \begin{pmatrix} x \\ y \end{pmatrix}$. We call $\mathbf{X}$ a **vector** in the plane.

The vectors $\mathbb{E}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbb{E}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are called the **basis vectors** of the plane. For every $\mathbf{X} \in \mathbf{R}^2$,

$$\begin{pmatrix} x \\ y \end{pmatrix} = x\mathbb{E}_1 + y\mathbb{E}_2 = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

For every scalar $\lambda \in \mathbf{R}$ and $\mathbf{X} \in \mathbf{R}^2$,

$$\lambda\mathbf{X} = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}.$$

Linear Maps

Let $\mathbf{V}$ and $\mathbf{W}$ be vector spaces over a field K.
A function $f : \mathbf{V} \to \mathbf{W}$ is a *linear map (function)* if

1. $f(\lambda\mathbf{X}) = \lambda f(\mathbf{X})$ for all $\lambda \in K$ and $\mathbf{X} \in \mathbf{V}$.
2. $f(\mathbf{X} + \mathbf{Y}) = f(\mathbf{X}) + f(\mathbf{Y})$ for all $\mathbf{X}, \mathbf{Y} \in \mathbf{V}$.

Example 8.2.1. Let $\mathbf{V} = \mathbf{R}^2$, $\mathbf{W} = \mathbf{R}$ and $K = \mathbf{R}$. For $\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbf{V}$, define $f : \mathbf{V} \to \mathbf{W}$ by $f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 2x_1 + 3x_2$. Then f is a linear map.

Proof. For $\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and $\lambda \in \mathbf{R}$, $f(\lambda\mathbf{X}) = f \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix} = 2\lambda x_1 + 3\lambda x_2 = \lambda f(\mathbf{X})$.

For $\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $\mathbf{Y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$,

$$\begin{aligned} f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) &= 2(x_1 + y_1) + 3(x_2 + y_2) \\ &= (2x_1 + 3x_2) + (2y_1 + 3y_2) \\ &= f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + f \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}. \end{aligned}$$

□

Properties of linear functions

For a linear function $f : \mathbf{V} \to \mathbf{W}$, $f(\mathbf{O}) = \mathbf{O}$.

Proof. The zero $\mathbf{O}$ can be written as $\mathbf{X} - \mathbf{X}$. Thus $f(\mathbf{O}) = f(\mathbf{X} - \mathbf{X}) = f(\mathbf{X}) - f(\mathbf{X}) = \mathbf{O}$. □

Slope of Linear Graphs

If a function $f : \mathbf{R} \to \mathbf{R}$ is linear, then the ratio

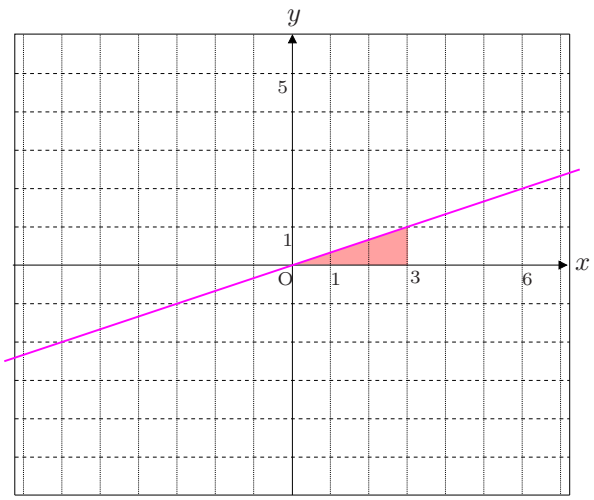
$$\frac{f(x)}{x} = \frac{xf(1)}{x} = f(1) = a \quad \text{for} \quad x \neq 0$$

is constant. This implies $f(x) = ax$ for $x \neq 0$ and $f(0) = 0$. Therefore, $f(x) = ax$ for all x. The constant a is the slope of its graph.

Let $f : \mathbf{R} \to \mathbf{R}$ be a map. Let Δx be some change of x. Let $\Delta y = f(x + \Delta x) - f(x)$. The slope of a line is also expressed by the rate of change:

$$\frac{\text{Change of } y}{\text{Change of } x} = \frac{\Delta y}{\Delta y}$$

Example 8.2.2. Let a function $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = \frac{1}{3}x$. Then f is a linear function. The linear function f has a linear graph:



The slope of the grpah (line) is $\frac{1}{3}$.

Teaching Tips

You may explain the slope $\frac{1}{3}$, "move 3 to the right and move up 1".

Translation of a linear graph

The graph of $y = ax + b$ is obtained by shifting the graph of $y = ax$ vertically by b. The number b is called a *y-intercept*. The solution of $ax + b = 0$: $-\frac{b}{a}$ is called an *x-intercept*.

Teaching Tips

If the slope is a, the line is expressed by $y = ax + b$.

8.3 Length of a vector

For a vector $\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, the length of $\mathbf{X}$ denoted by $|\mathbf{X}|$ is defined by

$$|\mathbf{X}| = \sqrt{x_1^2 + x_2^2}.$$

8.4 Unit Vector and Dot Product

A vector with length equal to unity is called a **unit vector**.
For every non-zero vector $\mathbf{X} \in \mathbf{R}^2$, the vector

$$\frac{\mathbf{X}}{|\mathbf{X}|}$$

is a unit vector with the same direction of $\mathbf{X}$.
Let $\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $\mathbf{Y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$. The dot product $\mathbf{X} \cdot \mathbf{Y}$ is defined by

$$\mathbf{X} \cdot \mathbf{Y} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + x_2 y_2.$$

Obviously, the dot product is a scalor.

The angle between two vectors

Let $\mathbf{A}$ and $\mathbf{B}$ be vectors in the plane. Let θ be the angle from $\mathbf{A}$ to $\mathbf{B}$ measured counterclockwisely. Then the dot prodct of $\mathbf{A}$ and $\mathbf{B}$ is given by

$$\mathbf{A} \cdot \mathbf{B} = |\mathbf{A}||\mathbf{B}| \cos\theta$$

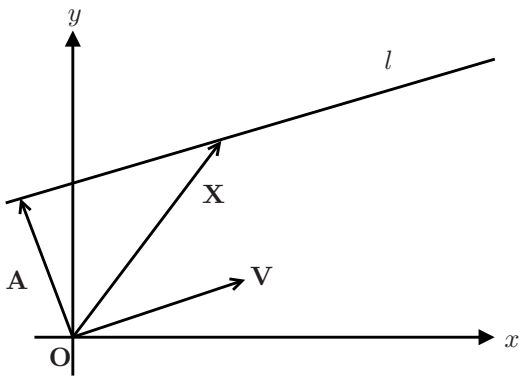
If two vectors $\mathbf{A}$ and $\mathbf{B}$ are perpendicular to each other, then

$$\mathbf{A} \cdot \mathbf{B} = 0$$

PROPERTIES OF DOT PRODUCT

1. $\mathbf{X} \cdot \mathbf{Y} = \mathbf{Y} \cdot \mathbf{X}$
2. $(r\mathbf{X}) \cdot \mathbf{Y} = r(\mathbf{X} \cdot \mathbf{Y})$
3. $\mathbf{A} \cdot (\mathbf{X} + \mathbf{Y}) = \mathbf{A} \cdot \mathbf{X} + \mathbf{A} \cdot \mathbf{Y}$

8.5 Parametric equations of a line in the plane



Suppose that the fixed vectors $\mathbf{V} = \begin{pmatrix} u \\ v \end{pmatrix}$ and $\mathbf{A} = \begin{pmatrix} a \\ b \end{pmatrix}$ are given. The line l parallel to the vector $\mathbf{V}$ is described by the vector $\mathbf{X}$:

$$\mathbf{X} = \mathbf{A} + t\mathbf{V} = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} tu \\ tv \end{pmatrix}.$$

$$\begin{aligned} x_1 &= a + tu \\ x_2 &= b + tv \end{aligned}$$

These equations are called **parametric equations** of the line. From the parametric equations above, we obtain:

$$\begin{aligned} x_1 v &= av + tuv \\ x_2 u &= bu + tuv \end{aligned}$$

This implies that

$$x_1 v - x_2 u = av - bu. \tag{8.1}$$

Let $\mathbf{N}' = \begin{pmatrix} v \\ -u \end{pmatrix}$. Then $\mathbf{N}'$ is perpendicular to $\mathbf{V}$. Therefore, the equation (8.1) is expressed by:

$$\begin{aligned} \mathbf{N}' \cdot \mathbf{X} &= \mathbf{N}' \cdot \mathbf{A} \\ \mathbf{N}' \cdot (\mathbf{X} - \mathbf{A}) &= 0. \end{aligned}$$

8.6 Internal and External Divisions

Let **AB** be a line segment. A point **P internally divides AB** in the ratio $p : q$ if $|\mathbf{P} - \mathbf{A}| : |\mathbf{B} - \mathbf{P}| = p : q$.

Proposition 8.6.1. *If a point* **P** *internally divides the line segment* **AB** *in the ratio* $p : q$*, then the point* **P** *is given by:*

$$\mathbf{P} = \frac{q\mathbf{A} + p\mathbf{B}}{p + q}$$

Proof. We describe the point **P**. The vector $\mathbf{P} - \mathbf{A}$ is parallel to the line segment **AB**. Since $|\mathbf{P} - \mathbf{A}| : |\mathbf{B} - \mathbf{P}| = p : q$,

$$\begin{aligned} \frac{p+q}{p}(\mathbf{P} - \mathbf{A}) &= \mathbf{B} - \mathbf{A} \\ (p+q)(\mathbf{P} - \mathbf{A}) &= p(\mathbf{B} - \mathbf{A}) \\ \mathbf{P} &= \frac{q\mathbf{A} + p\mathbf{B})}{p+q} \end{aligned}$$

□

A point **P externally divides AB** in the ratio $p : q$ if $|\mathbf{P} - \mathbf{A}| : |\mathbf{B} - \mathbf{P}| = p : q$.

Proposition 8.6.2. *If a point* **P** *externally divides the line segment* **AB** *in the ratio* $p : q$*,* $(p > q)$ *then the point* **P** *is given by:*

$$\mathbf{P} = \frac{-q\mathbf{A} + p\mathbf{B}}{p - q}$$

Proof. Without loss of generality, we can assume that **B** lies on a line segment **AP** $(p > q)$. Then **B** internally divides the line segment **AP**. Thus

$$\begin{aligned} \mathbf{B} &= \frac{q\mathbf{A} + (p-q)\mathbf{P}}{p} \\ p\mathbf{B} &= q\mathbf{A} + (p-q)\mathbf{P} \\ \therefore \quad \mathbf{P} &= \frac{p\mathbf{B} - q\mathbf{A}}{(p-q)} \end{aligned}$$

□

8.7 Projection

A vector $\mathbf{U} \in V$ with $|\mathbf{U}| = 1$ is called a **unit vector**. Every unit vector $\mathbf{U} \in \mathbf{R}^2$ has the following expression:

$$\mathbf{U} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix},$$

where θ is the angle from the x-axis to $\mathbf{U}$.
Let $P_{\mathbf{V}}(\mathbf{X})$ denote the projected vector of $\mathbf{X}$ to the line from the origin $\mathbf{O}$ along $\mathbf{V}$. Then we have the following formulas.

$$\begin{aligned} \mathbf{X} \cdot \mathbf{U} &= |P_{\mathbf{U}}(\mathbf{X})| \text{ if } 0 \le \theta \le \frac{\pi}{2} \\ \mathbf{X} \cdot \mathbf{U} &= -|P_{\mathbf{U}}(\mathbf{X})| \text{ if } \frac{\pi}{2} \le \theta \le \pi, \end{aligned}$$

where θ is the angle between $\mathbf{X}$ and $\mathbf{U}$.
Also we have the following formula.

$$P_{\mathbf{V}}(\mathbf{X}) = \mathbf{X} \cdot \left(\frac{\mathbf{V}}{|\mathbf{V}|}\right) \cdot \frac{\mathbf{V}}{|\mathbf{V}|}. \qquad = \frac{\mathbf{X} \cdot \mathbf{V}}{\mathbf{V} \cdot \mathbf{V}}$$

8.8 Distance from a point to a line

Let L be a line $ax + by = 0$. Let $p(x_0, y_0)$ be a point not on the line. Let $\mathbf{P} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$. The normal vector to the line L is $\mathbf{N} = \begin{pmatrix} a \\ b \end{pmatrix}$. The distance of from p to the line L is the length of the projected vector $P_{\mathbf{V}}(\mathbf{P})$, which is the dot product of $\mathbf{P}$ and $\frac{\mathbf{N}}{|\mathbf{N}|}$:

$$\mathbf{P} \cdot \frac{\mathbf{N}}{|\mathbf{N}|} = \frac{ax_0 + by_0}{\sqrt{a^2 + b^2}}$$

Now consider the non-homogeneous case:

$$ax + by = c \quad (c \neq 0).$$

This line also has the same normal vector $\mathbf{N}$:

$$\begin{aligned} \mathbf{N} \cdot \mathbf{X} &= c \\ |\mathbf{N}| \frac{\mathbf{N}}{|\mathbf{N}|} \cdot \mathbf{X} &= c \\ \frac{\mathbf{N}}{|\mathbf{N}|} \cdot \mathbf{X} &= \frac{c}{|\mathbf{N}|}. \end{aligned}$$

Therefore, the absolute value of $\frac{c}{|\mathbf{N}|}$ is the distance from the origin to the line.

Example 8.8.1. Consider the line:

$$2x + 3y = 0 \tag{8.2}$$

with the normal vector

$$\mathbf{N} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

The distance from a point $(4, 7)$ to the line is:

$$d = \frac{|2 \cdot 4 + 3 \cdot 7|}{\sqrt{2^2 + 3^2}} = \frac{33}{\sqrt{13}}.$$

8.9 Area of a parallelogram

Let $\mathbf{A} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$.
Consider the parallelogram with sides $\mathbf{A}$ and $\mathbf{B}$. Suppose the base is $\mathbf{B}$. Denote the vector orthogonal to $\mathbf{B}$ by $\bar{C}$. Here $\mathbf{C} = \begin{pmatrix} b_2 \\ -b_1 \end{pmatrix}$.
Then the height h is given by

$$\begin{aligned} h &= \frac{|\mathbf{A} \cdot \mathbf{C}|}{|\mathbf{C}|} \\ &= \frac{|a_1 b_2 - a_2 b_1|}{\sqrt{b_1^2 + b_2^2}}. \end{aligned}$$

Thus the area of the parallelogram is given by

$$|a_1 b_2 - a_2 b_1|.$$

Exercises 8.1-8.9

---

1. A regular hexagon **ABCDEF** is given. The centre of the hexagon will be denoted by **O**. Let L be the midpoint of EF, let M be the midpoint of BL and let N be the midpoint of CD. Let $\mathbf{a} = \mathbf{B} - \mathbf{A}$ and let $\mathbf{b} = \mathbf{D} - \mathbf{C}$. Explain the following vectors in terms of $\mathbf{a}$ and $\mathbf{b}$.

   (a) $\mathbf{O} - \mathbf{B}$

   (b) $\mathbf{L} - \mathbf{B}$

(c) $\mathbf{N} - \mathbf{M}$

2. Let $\mathbf{A} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ and let $\mathbf{B} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$. Find the angle between $\mathbf{A}$ and $\mathbf{B}$.

3. Let $\mathbf{A}$ and $\mathbf{B}$ be linearly independent vectors. Find t so that $(\mathbf{A} + \mathbf{B})$ is orthogonal to $(\mathbf{A} + t\mathbf{B})$.

4. Write an equation of the line through $\mathbf{P} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ parallel to the vector $\mathbf{V} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

5. Let $\mathbf{A} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

   Find $|\mathbf{A} - \mathbf{B}|$.

6. For vectors $\mathbf{X}$ and $\mathbf{Y}$, if $|\mathbf{X}| = 3$, $|\mathbf{Y}| = 1$ and $|\mathbf{X} + 2\mathbf{Y}| = 2$, then

   (a) Find $\mathbf{X} \cdot \mathbf{Y}$

   (b) Find $|2\mathbf{X} + \mathbf{Y}|$

   (c) For all $t \in \mathbf{R}$, find the minimal value of $|\mathbf{X} + t\mathbf{Y}|$.

7. Let $\mathbf{X} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ and let $\mathbf{Y} = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$. Find $\mathbf{X} \cdot \mathbf{Y}$.

8. Let $\mathbf{X} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ and let $\mathbf{Y} = \begin{pmatrix} -5 \\ t \end{pmatrix}$. If $\mathbf{X} \perp \mathbf{Y}$, then find t.

9. Find the angle θ between $\mathbf{X} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ and $\mathbf{Y} = \begin{pmatrix} -4 \\ -2 \end{pmatrix}$.

8.10 Transformations of the plane

A **transformation of the plane** is a map $T : \mathbf{R}^2 \to \mathbf{R}^2$. Two transformations A and B are equivalent if

$$A(\mathbf{X}) = b(\mathbf{X}) \text{ for every vector } \mathbf{X}.$$

Transformation of projection

The projection which maps $\mathbf{X} = \begin{pmatrix} x \\ y \end{pmatrix}$ to the projected vector $P_{\mathbf{V}}(X)$ along the vector $\mathbf{V} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ is a transformation.

$$P_{\mathbf{V}}(\mathbf{X}) = \left(\frac{\mathbf{X}\cdot\mathbf{V}}{\mathbf{V}\cdot\mathbf{V}}\right)\mathbf{V} = \frac{v_1x + v_2y}{v_1^2 + v_2^2}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

Transformation of reflection

Let S be the transformation which assigns to each vector $\mathbf{X}$ the reflection of $\mathbf{X}$ in the line along the vector $\mathbf{U} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$. This is called the **transformation of reflection** along the vector $\mathbf{U}$.

$$S(\mathbf{X}) = P_{\mathbf{U}}(\mathbf{X}) + (P_{\mathbf{U}}(\mathbf{X}) - \mathbf{X}) = 2P_{\mathbf{U}}(\mathbf{X}) - \mathbf{X}$$

Transformation of stretching

Let D_2 be the transformation which sends each vector into twice itself.

$$D_2(\mathbf{X}) = 2\mathbf{X}.$$

Transformation of rotation

Fix a scalar θ with $0 \leq \theta \leq 2\pi$. Let

$$\mathbf{X} = \begin{pmatrix} x \\ y \end{pmatrix} = |\mathbf{X}|\begin{pmatrix} \cos\phi \\ \sin\phi \end{pmatrix}$$

Then We define the transformation R_θ of rotation by θ radians by

$$R_\theta(\mathbf{X}) = \begin{pmatrix} |\mathbf{X}|\cos(\phi+\theta) \\ |\mathbf{X}|\sin(\phi+\theta) \end{pmatrix}.$$

Appendices

Appendix A

Dedekind Cuts

A.1 Dedekind Cuts and the Real Numbers

In this chapter we will discuss about real numbers, which will be obtained by pairs of non–empty sets of rational numbers. We assume that we already know natural numbers; that is, the numbers $1, 2, \cdots, n, \cdots$. By additions and subtractions the integers is obtained and by divisions the rational numbers are obtained. The aim of this chapter is to understand the real numbers based on the understanding of rational numbers. Topics in this chapter are based on lecture notes written by S. Miyatake. Note that proofs in notes are all direct proofs.

A.2 Rational Numbers on the Line

We can define an order on the rational numbers. Let $q_1, q_2 \in \mathbf{Q}$. We can define $q_1 < q_2$ by that there exists a number $k > 0$ such that kq_1 and kq_2 are integer and $kq_1 < kq_2$. This is an algebraic explanation.
However, we usually use a diagrammatic explanation to define an order; such as q_1 and q_2 are points on the line and $q_1 < q_2$ means that q_1 is left of q_2. We use a set theoretical notations to describe this situation. Let $q_0 \in \mathbf{Q}$.

$$\mathbf{Q}_-(q_0) = \{q \in \mathbf{Q} : \ q < q_0\} \tag{A.1}$$
$$\mathbf{Q}_+(q_0) = \{q \in \mathbf{Q} : \ q_0 \leq q\}. \tag{A.2}$$

We define the order $q_1 < q_2$ by $q_1 \in \mathbf{Q}_-(q_2)$.
We will give an example to express a real number by a pair of non–empty subsets of $\mathbf{Q}$. Take two non–empty sets, each of which is greater than $\sqrt{2}$ or less than $\sqrt{2}$. As we know $\sqrt{2}$ is not rational number, each component of

the partition does not contain $\sqrt{2}$. Therefore, the partition by an irrational number $\sqrt{2}$ is unique.
We write

$$\mathbf{Q}_+(\sqrt{2}) = \{q \in \mathbf{Q} : \ q^2 < 2, \ \text{ or } \ q < 0\} \tag{A.3}$$
$$\mathbf{Q}_-(\sqrt{2}) = \{q \in \mathbf{Q} : \ q^2 < 2 \ \text{ or } \ q < 0\}. \tag{A.4}$$

A.3 Upper Sets, Lower Sets and Cuts

We will define an upper set and lower set of the rational numbers.

Definition A.3.1. Let $\mathbf{Q}$ be the rational numbers. Let $q_0 \in \mathbf{Q}$. We define a set of rational numbers less than q_0 as

$$\mathbf{Q}_-(q_0) = \{q \in \mathbf{Q} : \ q < q_0\}. \tag{A.5}$$

Also we define a set of rational numbers no less than q_0 as

$$\mathbf{Q}_+(q_0) = \{q \in \mathbf{Q} : \ q_0 \leq q\}. \tag{A.6}$$

A subset $\mathbf{Q}_+$ of $\mathbf{Q}$ is an *upper set* if it satisfies:

$$\mathbf{Q}_+ \neq \mathbf{Q}, \mathbf{Q}_+ \neq \emptyset \tag{A.7}$$
$$q_1 \in \mathbf{Q}_+, \ \ q' > q_1, \implies q' \in \mathbf{Q}_+. \tag{A.8}$$

A subset $\mathbf{Q}_-$ of $\mathbf{Q}$ is an *lower set* if it satisfies:

$$\mathbf{Q}_- \neq \mathbf{Q}, \mathbf{Q}_- \neq \emptyset \tag{A.9}$$
$$q_2 \in \mathbf{Q}_-, \ \ q' < q_2, \implies q' \in \mathbf{Q}_-. \tag{A.10}$$

The collection of all upper sets will be denoted by U and let the collections of all lower sets will be denoted by L.
Let $\mathcal{U}$ denote the subcollection of U such that each $\mathbf{Q}_+ \in \mathcal{U}$ does not have the minimum point. Let $\mathcal{L}$ denote the subcollection of L such that each $\mathbf{Q}_- \in L$ does not have the maximum point.
We call $\mathcal{U}$ the *collection of open upper sets of* $\mathbf{Q}$ and call $\mathcal{L}$ the *collection of open lower sets of* $\mathbf{Q}$.

Definition A.3.2. Let $A \subset \mathbf{Q}$. We define the *boundary* of A by

$$\partial A = \bigcap_{n=1}^{\infty} \left\{ q \in \mathbf{Q} : \ \left(\frac{q-1}{k}, \frac{q+1}{k} \right) \cap A \neq \emptyset, \left(\frac{q-1}{k}, \frac{q+1}{k} \right) \cap A^c \neq \emptyset \right\}. \tag{A.11}$$

Let $B \subset \mathbf{Q}$.

$$\mathrm{Int}(B) = \bigcup_{k=1}^{\infty} \left\{ q \in B : \left(\frac{q-1}{k}, \frac{q+1}{k} \right) \subset B \right\}. \tag{A.12}$$

$\mathrm{Int}(B)$ is the set of interior points of B. A point $x \in B$ is an interior point if there exists an $\varepsilon > 0$ such that the interval $(x - \varepsilon, x + \varepsilon) \subset B$.

Definition A.3.3. A *cut* is a pair of non–empty subsets of $\mathbf{Q}$: $\{\mathbf{Q}_1, \mathbf{Q}_2\}$ satisfying:

(1) $\mathbf{Q}_1 \cap \mathbf{Q}_2 = \emptyset$,

(2) $\mathbf{Q}_1 \cup \mathbf{Q}_2 = \mathbf{Q}$.

(3) $q_1 \in \mathbf{Q}_1$, $q_2 \in \mathbf{Q}_2$, then $q_1 < q_2$.

Let $\{\mathbf{Q}_1, \mathbf{Q}_2\}$ be a cut. If $\mathbf{Q}_1$ contains the maximum point, then $\mathbf{Q}_2$ does not contain the minimum point. We can add the maximum point of $\mathbf{Q}_1$ to $\mathbf{Q}_2$ as the minimum point of $\mathbf{Q}_2$ to obtain another cut $\{\mathbf{Q}_1', \mathbf{Q}_2'\}$ but we will not distinguish these two cuts.

Theorem A.3.4. *There exist a one–to–one correspondences between $\mathcal{L}$ and $\mathcal{U}$:*

$$\begin{cases} \mathcal{L} \to \mathcal{U} & \mathbf{Q}_- \mapsto \mathrm{Int}(\mathbf{Q}_-^c) \\ \mathcal{U} \to \mathcal{L} & \mathbf{Q}_+ \mapsto \mathrm{Int}(\mathbf{Q}_+^c). \end{cases} \tag{A.13}$$

A.3.1 The Real Numbers

When we explain the real numbers, we usually use the line as the set of real numbers. However, this explanation is not enough to obtain real numbers from rational numbers. Dedekind (1831–1916) introduced the idea of cuts. He gave the idea that a real number is represented by a way of separation of the rational numbers into an upper set and a lower set. If we define one of them, the other is determined. For a cut, the existence of the boundary point of an upper set or a lower set is not essential. Thus upper sets and lower sets may be considered as open sets.

A.4 Propositions for Theorem A.3.4

Lemma A.4.1. *For subsets $\mathbf{Q}_1, \mathbf{Q}_2 \subset \mathbf{Q}$, the following holds.*

(1) *If* $\mathbf{Q}_1 \subset \mathbf{Q}_2$, *then* $\mathbf{Q}_2^c \subset \mathbf{Q}_1^c$

(2) $$\left(\bigcup_{k=1}^{\infty} \mathbf{Q}_k\right)^c = \bigcap_{k=1}^{\infty} \mathbf{Q}_k^c$$

(3) $$\left(\bigcap_{k=1}^{\infty} \mathbf{Q}_k\right)^c = \bigcup_{k=1}^{\infty} \mathbf{Q}_k^c$$

Proposition A.4.1. *Let* $\mathbf{Q}_+$ *be an upper set and let* $\mathbf{Q}_- = \mathbf{Q} \setminus \mathbf{Q}_+$. *Then if* $q_1 \in \mathbf{Q}_-$ *and* $q_2 \in \mathbf{Q}_+$, *then* $q_1 < q_2$.

Proof. The relation

$$\mathbf{Q}_+(q_2) \subset \mathbf{Q}_+ \tag{A.14}$$

implies that

$$\mathbf{Q}_+^c \subset \mathbf{Q}_+(q_2)^c \Longleftrightarrow \mathbf{Q}_- \subset \mathbf{Q}_-(q_2). \tag{A.15}$$

Then $q_1 \in \mathbf{Q}_- \subset \mathbf{Q}_-(q_2)$. Thus $q_1 < q_2$ follows. □

Proposition A.4.2. *Let* $\mathbf{Q}_+^{(1)}$ *and* $\mathbf{Q}_+^{(2)}$ *be upper sets. Then we have either* $\mathbf{Q}_+^{(1)} \subset \mathbf{Q}_+^{(2)}$ *or* $\mathbf{Q}_+^{(2)} \subset \mathbf{Q}_+^{(1)}$.

Proof. Assume

$$\mathbf{Q}_+^{(1)} \neq \mathbf{Q}_+^{(2)}. \tag{A.16}$$

Then there exists $q_1 \in \mathbf{Q}$ such that

$$q_1 \in \mathbf{Q}_+^{(1)} \quad \text{and} \quad q_1 \notin \mathbf{Q}_+^{(2)} \tag{A.17}$$

or there exists $q_2 \in \mathbf{Q}$ such that

$$q_2 \in \mathbf{Q}_+^{(2)} \quad \text{and} \quad q_2 \notin \mathbf{Q}_+^{(1)}. \tag{A.18}$$

For the first case,

$$q \in \mathbf{Q}_+^{(2)} \quad \text{and} \quad q_1 \in \mathbf{Q}_-^{(2)} \tag{A.19}$$

imply $q_1 < q$.
On the other hand, $q_1 \in \mathbf{Q}_+^{(1)}$ so $q \in \mathbf{Q}_+^{(1)}$. Then $\mathbf{Q}_+^{(2)} \subset \mathbf{Q}_+^{(1)}$. □

Proposition A.4.3. *Let* $\mathbf{Q}_+$ *be an upper set. Then the complement,* $\mathbf{Q}_-$, *is a lower set.*

Proof. Let

$$q_1 \in \mathbf{Q}_- \quad \text{and let} \quad q' \in \mathbf{Q}. \tag{A.20}$$

Assume that

$$q' < q_1. \tag{A.21}$$

$q_1 \notin \mathbf{Q}_+$ and $q_1 \in \mathbf{Q}_+(q_1)$ imply that $\mathbf{Q}_+ \subset \mathbf{Q}_+(q_1)$, and hence,

$$\mathbf{Q}_-(q_1) \subset \mathbf{Q}_-. \tag{A.22}$$

Also $q' < q$ implies that $q' \in \mathbf{Q}_-(q_1)$. Thus $q' \in \mathbf{Q}_-$. □

Proposition A.4.4. *Let* $\{\mathbf{Q}_1, \mathbf{Q}_2\}$ *be a cut. Then* $\mathbf{Q}_1$ *is the lower set and* $\mathbf{Q}_2$ *is the upper set.*

Proof. Let $q_0 \in \mathbf{Q}_1$ be an arbitrary element. Choose q_1 such that

$$q_1 < q_0. \tag{A.23}$$

Then $q_1 \in \mathbf{Q}_-(q_0)$.
By (3) in the definition of a cut,

$$\mathbf{Q}_2 \subset \mathbf{Q}_+(q_0). \tag{A.24}$$

By (1) and (2) of the definition $\mathbf{Q}_1$ is the complement of $\mathbf{Q}_2$ and $\mathbf{Q}_-(q_0)$ is the complement of $\mathbf{Q}_+(q_0)$.
Then

$$\mathbf{Q}_-(q_0) \subset \mathbf{Q}_1 \tag{A.25}$$

hence, $\mathbf{Q}_1$ is the lower set. □

A.5 Open Lower Sets and Sequences

We will consider the family of the open lower sets.

Proposition A.5.1. *Choose* $\mathbf{Q}_- \in \mathcal{L}$ *and we denote the complement of* $\mathbf{Q}_-$ *by* $\mathbf{Q}_+$. *Then there are sequences* $\{q_n : n \in \mathbf{N}\}$ *and* $\{q'_n : n \in \mathbf{N}\}$ *such that* $\{q_n\} \subset \mathbf{Q}_-$ *and* $\{q'_n\} \subset \mathbf{Q}_+$ *and* $q'_n - q_n = 10^{-n}$, $n \in \mathbf{N}$ *and* $q_0 \in \mathbb{Z}$,

$$q_0 \le q_1 \le \cdots \le q_k \le \cdots \tag{A.26}$$
$$q'_0 \ge q'_1 \ge \cdots \ge q'_k \ge \cdots . \tag{A.27}$$

Proof. Note that there exists a number $z_0 \in \mathbb{Z}$ such that

$$q_0 \in \mathbf{Q}_- \quad \text{and} \quad q_0 + 1 \in \mathbf{Q}_+. \tag{A.28}$$

Since $\mathbf{Q}_- \neq \emptyset$, there exist

$$q \in \mathbf{Q}_- \quad \text{and} \quad z \in \mathbb{Z} \tag{A.29}$$

such that $z < q$. Then $z \in \mathbf{Q}_-$. Thus

$$\mathbf{Q}_- \cap \mathbb{Z} \neq \emptyset. \tag{A.30}$$

Similarly, $\mathbf{Q}_+ \cap \mathbb{Z} \neq \emptyset$. If $z \in \mathbf{Q}_- \cap \mathbb{Z}$ and $z' \in \mathbf{Q}_+ \cap \mathbb{Z}$, then $z \in \mathbf{Q}_+ \cap \mathbb{Z}$. Now $a' - z$ is finite so there exists the maximum integer $q_0 \in \mathbf{Q}_-$ such that $z \leq q_0$.
Let $q_0' = q_0 + 1$. Then $q_0' \in \mathbf{Q}_+$.
Take a partition points between q_0 and q_0':

$$q_0 < q_1 + \frac{1}{10} < q_0 + \frac{2}{10} < \cdots < q_0 + \frac{9}{10} < q_0'. \tag{A.31}$$

Set

$$q_1 = \max\left(\left\{q_0 + \frac{i}{10} : \ 0 \leq i \leq 10\right\} \cap \mathbf{Q}_-\right). \tag{A.32}$$

Then $q_1 = q_0 + a_1/10$, where a_1 is one of numbers from 0 to 9, and also $q_1 + 1/10 \in \mathbf{Q}_+$.
Repeat this process to obtain

$$q_n = q_0 + \sum_{k=1}^{n} \left(\frac{a_k}{10^k}\right) \tag{A.33}$$

and $q_n' = q_n + 1/10^n$ so that

$$q_n \in \mathbf{Q}_- \ \text{ and } \ q_n' \in \mathbf{Q}_+. \tag{A.34}$$

□

Note that the sequence $\{q_n\}$ defined the above is not always increasing but it contains an increasing subsequences.

Proposition A.5.2. *Let $\{p_n : \ n \in \mathbf{N}\}$ be a sequence bounded above and let*

$$\mathbf{Q}_-(p_n) = \{q \in \mathbf{Q} : \ q < p_n\}. \tag{A.35}$$

Then

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(p_n) \in \mathcal{L}. \tag{A.36}$$

Proof. Set

$$\mathbf{Q}_- = \bigcup_{n=1}^{\infty} \mathbf{Q}_-(p_n). \tag{A.37}$$

For any $q_1 \in \mathbf{Q}_-$, there exists q_1 such that

$$q_1 \in \mathbf{Q}_-(p_n). \tag{A.38}$$

If $q < q_1$, then $q \in \mathbf{Q}_-(p_n) \subset \mathbf{Q}_-$. There exists $q \in \mathbf{Q}_-(p_n)$ such that $q_1 < q$. Then $q \in \mathbf{Q}_-$. □

Proposition A.5.3. *Let $\mathbf{Q}_-$ and $\mathbf{Q}'_-$ be lower sets. Assume $\mathbf{Q}_- \subset \mathbf{Q}'_-$. Then for any element $q_1 \in \mathbf{Q}_-$ and $\tilde{q}_2 \in (\mathbf{Q}'_-)^c$, there exists $q_0 \in \mathbf{Q}$ such that*

$$d_0 < \tilde{q}_2 - q_1. \tag{A.39}$$

Proof. There is a rational number $q_2 \in \mathbf{Q}'_-$ with $q_2 \notin \mathbf{Q}_-$. Also there exists q'_2 such that $q_2 < q'_2$ $q'_2 \in \mathbf{Q}'_-$ since $\mathbf{Q}_-$ is open. Set

$$d_0 = q'_2 q_2. \tag{A.40}$$

Then Proposition A.4.1 implies that

$$q_1 < q_2, \tag{A.41}$$
$$q'_2 < \tilde{q}_2. \tag{A.42}$$

Therefore, $d_0 = q'_2 - q_2 < \tilde{q}_2 - q_1$. □

Proposition A.5.4. *Let $\mathbf{Q}_- \in \mathcal{L}$ be an arbitrary lower set and let $\mathbf{Q}_+ = \mathbf{Q}_-^c$. Then for the sequence $\{q_n\}$ in Proposition A.5.1,*

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n) = \mathbf{Q}_-, \tag{A.43}$$

where $\mathbf{Q}_-(q_n) = \{q \in \mathbf{Q} : \ q < q_n\}$.

Proof. The set $\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n)$ is an open lower set from Proposition A.5.2. Since $\mathbf{Q}_-$ is a lower set, for every n, $\mathbf{Q}_-(q_n) \subset \mathbf{Q}_-$ hence,

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n) \subset \mathbf{Q}_-. \tag{A.44}$$

Let $\{q_n\} \subset \mathbf{Q}_-$ be a sequence defined in Proposition A.4.1. Then

$$q_n - q'_n = \frac{1}{10^n}. \tag{A.45}$$

From Proposition A.4.2, there exists a positive rational number d_0 such that fro any $q_0 \in \mathbf{Q}_-$, $q_0 < q'_n - d_0$.

Therefore, $q_0 < q_n$ fro some n and

$$q_0 \in \bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n), \tag{A.46}$$

so

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n) = \mathbf{Q}_-. \tag{A.47}$$

□

Proposition A.5.5. *Let $\mathbf{Q}_- \in \mathcal{L}$ and let $\mathbf{Q}_+ = \mathbf{Q}_-^c$. Then there exist sequences $\{p_n\}$ and $\{p'_n\} \subset \mathbf{Q}_+$ such that $p_n \uparrow$ and $p'_n \downarrow$.*
Assume that for every k, there exists $\nu \in \mathbf{N}$ such that

$$d_n = p'_n - p_n < \frac{1}{k}, \tag{A.48}$$

for all $n > \nu$. Then $\bigcup_{n=1}^{\infty} \mathbf{Q}_-(p_n)$ belongs to $\mathcal{L}$.

Definition A.5.1. A sequence $\{q_n\}$ is called an *essentially increasing sequence* if it is bounded above and it contains an increasing subsequence.

Theorem A.5.2. *A set $\mathbf{Q}_-$ is in $\mathcal{L}$ if and only if there exists a sequence of rational numbers, each of which has a decimal representation, such that*

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n) = \mathbf{Q}_-. \tag{A.49}$$

Moreover, if there exists $\{p_n\}$ (in Proposition A.5.5)*, then*

$$\bigcup_{n=1}^{\infty} \mathbf{Q}_-(p_n) = \mathbf{Q}_-. \tag{A.50}$$

A.6 Increasing Sequences and Convergences

As we have seen there is a one–to–one correspondence between $\mathbf{Q}_-$ and a sequence $\{q_n\}$ defined in Proposition A.5.1. The term of the sequence is represented by a decimal representation. Thus we denote the rational number by α.
Note that the sequence $\{q_n\}$ in the above corresponds to a decimal representation of a number. We consider a representation with non–zero digits after a certain digits, such as $1.02 = 1.019999\cdots$. Therefore, each lower set in $\mathcal{L}$ uniquely corresponds to a number represented by a decimal representation.

We know that the sequence

$$\left\{a - \frac{1}{n} : \ n \in \mathbf{N}\right\} \tag{A.51}$$

is convergent to a. Thus we may compare a sequence $\{a_n\}$ with $\{a - 1/k\}$ to see whether $\{a_n\}$ is convergent to a.
Notations: For an open lower set $\mathbf{Q}_-$ and $\varepsilon > 0$, define a set

$$\mathbf{Q}_- + \mathbf{Q}_-(-\varepsilon) = \{q - q' : \ q \in \mathbf{Q}_-, q' < -\varepsilon\}. \tag{A.52}$$

Proposition A.6.1.

$$\mathbf{Q}_- + \mathbf{Q}_-(-\varepsilon) = \{q - \varepsilon : \ q \in \mathbf{Q}_-\}. \tag{A.53}$$

Proof. Assume that

$$p \in \mathbf{Q}_- + \mathbf{Q}_-(-\varepsilon) = \{q + q' : \ q \in \mathbf{Q}_-, q' < -\varepsilon\} \tag{A.54}$$

Then there are $q \in \mathbf{Q}_-$ and $q' < -\varepsilon$ such that

$$p = q + q' < q - \varepsilon. \tag{A.55}$$

This implies that $p + \varepsilon < q$ and hence, $p + \varepsilon \in \mathbf{Q}_-$.
Set $p + \varepsilon = q'$. Then

$$p = q' - \varepsilon \in \{q - \varepsilon : \ q \in \mathbf{Q}_-\}. \tag{A.56}$$

Conversely, assume that $p \in \{q - \varepsilon : \ q \in \mathbf{Q}_-\}$. Then there is $q' \in \mathbf{Q}_-$ such that

$$q < q'. \tag{A.57}$$

Then $p = q - \varepsilon$ implies that $q = p + \varepsilon < q'$. Hence,

$$p - q' \ < \ -\varepsilon \ \text{ then} \tag{A.58}$$
$$p - q' \ \in \ \mathbf{Q}_-(-\varepsilon). \tag{A.59}$$

□

Note that:

$$\mathbf{Q}_-^{(1)} + \mathbf{Q}_-^{(2)} = \{q + q' : \ q \in \mathbf{Q}_-^{(1)}, q' \in \mathbf{Q}_-^{(2)}\}. \tag{A.60}$$

Proposition A.6.2. *For every $\mathbf{Q}_- \in \mathcal{L}$ and for $\varepsilon > 0$,*

$$\mathbf{Q}_- - \varepsilon \ \in \ \mathcal{L} \ \text{ and} \tag{A.61}$$
$$\mathbf{Q}_- - \varepsilon \ \subset \ \mathbf{Q}_-. \tag{A.62}$$

Also $\mathbf{Q}_-$ and $\mathbf{Q}_- - \varepsilon$ are distinct.

Proof. For every $q \in \mathbf{Q}_- - \varepsilon$, there exists $q' \in \mathbf{Q}_-$ such that $q = q' - \varepsilon$. Then $q' - \varepsilon < q$ implies $q' - \varepsilon \in \mathbf{Q}_-$.
Fix $q_0 \in \mathbf{Q}_- - \varepsilon$. Let $q_k = q_0 + k\varepsilon$. Then we obtain a sequence $\{q_k\}$. There exists the maximum number k_0 such that

$$q_{k_0} \in \mathbf{Q}_- - \varepsilon. \tag{A.63}$$

Then $q_{k_0+1} \notin \mathbf{Q}_- - \varepsilon$. On the other hand, since $q_{k_0} \in \mathbf{Q}_- - \varepsilon$, there exists $q' \in \mathbf{Q}_-$ such that

$$q_{k_0} = q' - \varepsilon. \tag{A.64}$$

Thus $q' = q_{k_0} + \varepsilon = q_{k_0+1} \in \mathbf{Q}_-$. Therefore, $\mathbf{Q}_-$ and $\mathbf{Q}_- - \varepsilon$ are distinct. □

Proposition A.6.3. *Let a sequence $\{q_n\}$ be bounded above. Set*

$$\mathbf{Q}_- = \bigcup_{n=1}^{\infty} \mathbf{Q}_-(a_n). \tag{A.65}$$

Then for every $\varepsilon > 0$, there exists $\nu \in \mathbf{N}$ such that

$$\mathbf{Q}_- - \varepsilon \subset \mathbf{Q}_-(a_n), \tag{A.66}$$

and $\mathbf{Q}_-\varepsilon$ and $\mathbf{Q}_-(a_n)$ are distinct lower sets.

Proof. From Proposition A.6.2 there exists a rational number q_1 such that $q_1 \in \mathbf{Q}_-$ and $q_1 \notin \mathbf{Q}_- - \varepsilon$. Since $\mathbf{Q}_- = \bigcup_{n=1}^{\infty} \mathbf{Q}_-(a_n)$, there exists $\nu \in \mathbf{N}$ such that $q_1 \in \mathbf{Q}_-(a_n)$. Thus $\mathbf{Q}_- - \varepsilon$ and $\mathbf{Q}_-(a_n)$ are distinct and from Proposition A.4.2, $\mathbf{Q}_- - \varepsilon \subset \mathbf{Q}_-(a_n)$. □

Corollary A.6.1. *In* Proposition A.6.3*, let the sequence $\{a_n\}$ be an essentially increasing sequence. Then for every $\varepsilon > 0$, there exists $\nu \in \mathbf{N}$ such that $\mathbf{Q}_- - \varepsilon \subset \mathbf{Q}_-(a_n)$ for all $n > \nu$.*

Theorem A.6.1. *Let $\mathbf{Q}_-$ be an open lower set. The sequence $\{q_n\}$ defined in* Proposition A.5.1 *gives $\bigcup_{n=1}^{\infty} \mathbf{Q}_-(q_n) = \mathbf{Q}_-$. For every positive rational number ε, there exists a number $\nu(\varepsilon)$ such that $\mathbf{Q}_- - \varepsilon \subset \mathbf{Q}_-(q_n)$ for all $n > \nu(\varepsilon)$.*

Definition A.6.2. Let lower sets $\mathbf{Q}_-^{(1)}$ and $\mathbf{Q}_-^{(2)}$ be distinct and let them correspond to real numbers α_1 and α_2 respectively. Assume that $\mathbf{Q}_-^{(1)} \subset \mathbf{Q}_-^{(2)}$. From Proposition A.4.2 and A.5.3, there is a positive distance between two distinct lower sets. We define the relation between α_1 and α_2 by $\alpha_1 < \alpha_2$.

Definition A.6.3. Let α be a real number corresponding to a lower set $\mathbf{Q}_-$. Theorem A.6.1 implies that for every $\varepsilon > 0$, there is a number $\nu(\varepsilon)$ such that $\alpha - \varepsilon q_n < \alpha$ for all $n > \nu(\varepsilon)$. This means that a real number has a decimal representation and also the concept of convergence is obtained.

A.7 General Sequences and Suprema

In this section we will discuss about a general sequence, which may be a sequence of real numbers.

Definition A.7.1. A sequence of lower sets $\{\mathbf{Q}_-^{(n)} : n \in \mathbf{N}\}$ is *bounded above* if there exists a rational number M such that

$$\mathbf{Q}_-^{(n)} \subset \mathbf{Q}_-(M); \tag{A.67}$$

that is, the corresponding sequence $\{\alpha_n\}$ of real numbers is bounded by M. Similarly, we can define that a sequence of upper sets $\{\mathbf{Q}_+^{(n)}\}$ is *bounced below.*

Theorem A.7.2. *Let* $\{\mathbf{Q}_-^{(n)}\}$ *be a sequence of lower sets and let*

$$\mathbf{Q}_- = \bigcup_{n=1}^{\infty} \mathbf{Q}_-^{(n)}. \tag{A.68}$$

Foe every $\varepsilon > 0$*, there exists a number* $\nu \in \mathbf{N}$ *such that*

$$\mathbf{Q}_- - \varepsilon \subset \mathbf{Q}_+^{(n)} \subset \mathbf{Q}_-(\alpha_n). \tag{A.69}$$

We write $\mathbf{Q}_- = \mathbf{Q}_-(\alpha)$*,* $\mathbf{Q}_-^{(n)} = \mathbf{Q}_-(\alpha_n)$*, where* α *and* α_n *correspond to* $\mathbf{Q}_-$ *and* $\mathbf{Q}_-^{(n)}$ *respectively.*
In other words, for every $\varepsilon > 0$*, there exists* $\nu \in \mathbf{N}$ *such that* $\alpha - \varepsilon < \alpha_n < \alpha$*.*

Definition A.7.3. The number α obtained in Theorem A.7.2 is called a *supremum* of the sequence $\{\alpha_n\}$ and we write $\sup\limits_n \alpha_n$. Similarly, if the sequence $\{\mathbf{Q}_+^{(n)}\}$ is bounded below and $\{\beta_n\}$ is the corresponding sequence of real numbers, then the number β corresponding to $\mathbf{Q}_+ = \bigcup_{n=1}^{\infty} \mathbf{Q}_+$ is called the *infimum* of the sequence $\{\beta_n\}$ and we write $\inf\limits_n \beta_n$.
For every $\varepsilon > 0$, there exits $\nu \in \mathbf{N}$ such that $\beta < \beta_n < \beta_n + \varepsilon$.

For Theorem A.7.2 Let a sequence $\{\alpha_n\}$ be increasing. The number $\nu(\varepsilon)$, determined in Theorem A.7.2 is the number such that it depends on ε and

$$\alpha - \varepsilon < \alpha_n < \alpha \tag{A.70}$$

for all $n > \nu(\varepsilon)$. Then the sequence $\{\alpha_n\}$ is said to be convergent to α and we write

$$\lim_{n\to\infty} \alpha_n = \alpha. \tag{A.71}$$

Note that Theorem A.7.2 holds for a non–monotonic sequences. If the sequence is not monotonic, then there are two cases for supremum.

(1) The supremum α is a term α_k. Then α_k is the maximum of the sequence. In this case it is possible that there is no point other than α in an open interval

$$(\alpha_k - 1/m, \alpha_k + 1/m) \tag{A.72}$$

for some m. This point α_k is called an *isolated point*. It is also possible that there are points in any open interval around α_k.

(2) The supremum α is not a term of the sequence. In this case α is not the maximum of the sequence. Then for every number $j \in \mathbf{N}$, there is $\nu \in \mathbf{N}$ such that

$$\alpha_n \in (\alpha - 1/j, \alpha + 1/j)\,. \tag{A.73}$$

The point α is called an *accumulate point*.

Proof of Theorem A.7.2. The proof is similar to the proof of Theorem A.6.1. We have

$$\mathbf{Q}_-(\alpha) - \varepsilon \subset \mathbf{Q}_-(\alpha). \tag{A.74}$$

There is a rational number q_1 such that

$$q_1 \notin \mathbf{Q}_-(\alpha) - \varepsilon \quad \text{and} \quad q_1 \in \mathbf{Q}_-(\alpha). \tag{A.75}$$

There exists $n \in \mathbf{N}$ such that $q_1 \in \mathbf{Q}_-(\alpha_n)$.
From Proposition A.4.2

$$\mathbf{Q}_-(\alpha) - \varepsilon \subset \mathbf{Q}_-(\alpha_n), \tag{A.76}$$

$$\mathbf{Q}_-(\alpha_n) \subset \mathbf{Q}_-(\alpha). \tag{A.77}$$

□

We will define an *upper limit* of a sequence $\{\alpha_n\}$. Let

$$\beta_j = \sup\{\alpha_n : \ j \leq n\}. \tag{A.78}$$

Then the sequence $\{\beta_j\}$ is a decreasing sequence. The upper limit of $\{\alpha_n\}$ is defined as the supremum of $\{\beta_j\}$.
Similarly, we define a *lower limit* of a sequence $\{\alpha_n\}$ as the infimum of the sequence $\{\gamma_j\}$, where each γ_j is the infimum of

$$\{\alpha_n : \ j \leq n\} \tag{A.79}$$

and $\{\gamma_j\}$ is increasing sequence. We write

$$\gamma = \lim \gamma_j = \liminf \alpha_n, \tag{A.80}$$

$$\beta = \lim \beta_j = \limsup \alpha_n. \tag{A.81}$$

When $\gamma = \beta$, we call the sequence $\{\alpha_n\}$ is called a *Cauchy sequence*. Therefore, every Cauchy sequence is convergent.
Finally, we restate definition of a Cauchy sequence and a convergent sequence.

Definition A.7.4. A sequence $\{\alpha_n\}$ is called a *Cauchy sequence* if for every $\varepsilon > 0$, there exists $\nu(\varepsilon) \in \mathbf{N}$ such that

$$|\alpha_n - \alpha_m| < \varepsilon \tag{A.82}$$

for all $n, m > \nu(\varepsilon)$.
A sequence $\{\alpha_n\}$ is *convergent* to α if for every $\varepsilon > 0$, there exists $\nu(\varepsilon) \in \mathbf{N}$ such that

$$|\alpha_n - \alpha| < \varepsilon \tag{A.83}$$

for all $n > \nu(\varepsilon)$.

Appendix B

Pell's Equation

B.1 Pell's Equation

Definition

Pell's equation is the equation in the form:

$$x^2 - Dy^2 = \pm 1 \tag{B.1}$$

where D is a given positive non-square integer, and x and y are integer solutions.

The general solution was found by Bhaskara II (12th century). Later it was studied by Fermat and Euler.
The equation (B.1) has integer solutions (x, y) other than the trivial solution $(x, y) = (1, 0)$. If a non trivial solution (x, y) is given, then the following are all solutions:

$$x_k + y_k\sqrt{D} = (x + y\sqrt{D})^k. \tag{B.2}$$

Let D be a positive non-square integer. Consider

$$x^2 - Dy^2 = \pm 1$$

Put

$$S = \left\{ (x, y) \mid x^2 - Dy^2 = \pm 1, x, y, \in \mathbb{Z}, x + \sqrt{D}y > 0 \right\}$$

Suppose that S contains a solutions other than $(1, 0)$.
Then

1. for $(a, b), \in S$ and every $n \in \mathbb{Z}$, there is $(A, B) \in S$ such that

$$\left(a + b\sqrt{D}\right)^n = A + B\sqrt{D}.$$

2. for $(a,b),(c,d) \in S$, there is $(A,B) \in S$ such that

$$\frac{c+d\sqrt{D}}{a+b\sqrt{D}} = A + B\sqrt{D}.$$

3. Let (p,q) be an element of S such that $x+\sqrt{D}y > 1$ is minimised. The following holds:

$$S = \left\{ s,t) \mid \left(p+q\sqrt{D}\right)^n = s+t\sqrt{D}, s,t \in \mathbb{Z} \right\},$$

for the matrix $A = \begin{pmatrix} p & Dq \\ q & p \end{pmatrix}$,

$$S = \left\{ (x,y) \mid \begin{pmatrix} x \\ y \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

Proof. 1. By mathematical induction on $n \geq 1$. For $n = 1$ is trivial. Suppose $n = k$, $\left(a+b\sqrt{D}\right)^n = A + B\sqrt{D}$ is a solution. Consider $n = k+1$. $\left(a+b\sqrt{D}\right)^{k+1} = \left(A+B\sqrt{D}\right)\left(a+b\sqrt{D}\right) = Aa + BbD + (Ab+aB)\sqrt{D}$ $(Aa+BbD)^2 - D(Ab_aB)^2 = a^2 - Db^2 = 1$. Therefore, when $n = k+1$, it is a solution. □

Proof. 2.

$$\begin{aligned}
\frac{c+d\sqrt{D}}{a+b\sqrt{D}} &= \frac{c+d\sqrt{D}}{a+b\sqrt{D}} \cdot \frac{a-b\sqrt{D}}{a-b\sqrt{D}} \\
&= \frac{(c+d\sqrt{D})(a-b\sqrt{D})}{a^2-b^2D} \\
&= \frac{(ac-bdD)+(ad-bc)\sqrt{D}}{a^2-b^2D} \\
&= a^2c^2 + b^2d^2D^2 - 2abcdD - Da^2d^2 - Db^2c^2 + 2abcdD \\
&= (a^2-b^2D)(c^2-d^2D) \\
&= c^2 - d^2D = \pm 1
\end{aligned}$$

□

Proof. 3. Let $u = p+q\sqrt{D}$.

$$\begin{aligned}
u^n \leq \quad & s+t\sqrt{D} \quad \leq u^{n+1} \\
1 \leq \quad & \tfrac{s+t\sqrt{D}}{u^n} \quad \leq u
\end{aligned}$$

As u is smallest,

$$\frac{s+t\sqrt{D}}{u^n} = 1$$

$\therefore s + t\sqrt{D} = u^n$. □

Example B.1.1. Given $x^2 - 2y^2 = 1$, find a solution (a, b) and check there are $(A, B) \in S$ such that $(a + b\sqrt{2})^n = A + B\sqrt{2}$ for $n = 2, 3$.
Solution. We can guess the pair $(3, 2)$ is a solution.

$$\begin{aligned} (3+2\sqrt{2})^2 &= 9+8+12\sqrt{2} \\ &= 17+12\sqrt{2} \\ 17^2 - 12^2 \cdot 2 &= 1 \end{aligned} \tag{B.3}$$

$$\begin{aligned} (3+2\sqrt{2})^3 &= (17+12\sqrt{2})(3+2\sqrt{2}) \\ &= 99+70\sqrt{2} \\ 99^2 - 70^2 \cdot 2 &= 1 \end{aligned} \tag{B.4}$$

Example B.1.2. Find a general solution of $x^2 - 2y^2 = 1$.
Solution. We can guess that $(3, 2)$ is a smallest non-trivial solution. Thus the general solution (x, y) is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

In order to find A^n, we diagonalize A. To do this we calculate eigenvalues and eigen vectors:

$$\phi_A(t) = (t-3)(t-3) - 8 = t^2 - 6t + 1$$

Thus the eigenvalues are $3 \pm 2\sqrt{2}$. Then the eigen vectors for $3 + 2\sqrt{2}$ is $\begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}$, for $3 - 2\sqrt{2}$ is $\begin{pmatrix} \sqrt{2} \\ -1 \end{pmatrix}$. Thus

$$P = \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & -1 \end{pmatrix}, \; P^{-1} = \begin{pmatrix} \frac{1}{2\sqrt{2}} & \frac{1}{2} \\ \frac{1}{2\sqrt{2}} & -\frac{1}{2} \end{pmatrix}$$

The diagralized matrix is:

$$B = \begin{pmatrix} 3+2\sqrt{2} & 0 \\ 0 & 3-2\sqrt{2} \end{pmatrix}$$

$$(P^{-1}AP)^n = P^{-1}A^nP = B^n$$

Therefore,

$$A^n = P \begin{pmatrix} (3+2\sqrt{2})^n & 0 \\ 0 & (3-2\sqrt{2})^n \end{pmatrix} P^{-1} = \begin{pmatrix} \frac{(3+2\sqrt{2})^n+(3-2\sqrt{2})^n}{2} & \frac{\sqrt{2}(3+2\sqrt{2})^n-\sqrt{2}(3-2\sqrt{2})^n}{2} \\ \frac{(3+2\sqrt{2})^n-(3-2\sqrt{2})^n}{2\sqrt{2}} & \frac{(3+2\sqrt{2})^n+(3-2\sqrt{2})^n}{2} \end{pmatrix}$$

Thus

$$x = \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}$$
$$y = \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}}$$

Exercises B.1

---

1. Find the general solution of
   (a) $x^2 - 8y^2 = 1$
   (b) $x^2 - 15y^2 = 1$
2. (95 Osaka Prefecture University)
   For $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$.
   $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $(n = 1, 2, 3, \ldots,)$.
   (a) Find x_n and y_n
   (b) Let $a = 2+\sqrt{3}$, $b = 2-\sqrt{3}$. Express a^n and b^n in terms of x_n and y_n. Also points $P_1(x_1, y_1)$, $P_2(x_2, y_2), \ldots, P(x_n, y_n), \ldots$ are all on a curve. Using the fact $ab = 1$, find the equation of the curve.
3. (85 Tokyo Institute of Technology (modified version)) Let
   $G = \{g = a + b\sqrt{2} \mid a^2 - 2b^2 = \pm 1 \text{ and } a + \sqrt{2} > 0 \text{ and } a, b \in \mathbb{Z}\}$.
   Let $u > 1$ be the minimal number of G.

(a) Find u.

(b) Show that an integer n, and an element of G, $gu^n \in G$.

(c) Show that for every $g \in G$, there is an integer $m \in \mathbb{Z}$, $g = u^m$.

Bibliography

[Alc] D. Alcorn, "Lecture notes for introductory analysis", The University of Auckland 2000–2001.

[1] T. M. Apostol, *Calculus* Second edition, Blaisdell Publishing Company, 1967.

[2] Euclid, *Euclid's Elements*, Green Lion Press (2002).

[3] J R. Giles, *Real Analysis, An introductory course* , John Wiley & Sons Australasia Pty Ltd, 1972.

[4] Yoshifumi Khono, On the Proof of Unsolvability of Algebraic Equations of Degree n ($n \geq 5$) : Lectures in Senior High School, Bulletin of theory and practice in secondary education, Hiroshima University Attached school, no. 49, 43-53 (20030328)

[5] S. Miyatake, "Theory of the Real Numbers", (in Japanese "Jissuu no riron") lecture notes, Nara Women's University, July, 2001.

[6] J. Stillwell, Mathematics and Its History, Third Edition, Springer (2010).

[7] T. Okabe and others, Taikei Suugaku 1 (Algebra), 3rd Edtition, (2011) Suken Shuppan, Japan.

[8] T. Okabe and others, Taikei Suugaku 2 (Algebra), 3rd Edtition, (2011) Suken Shuppan, Japan.

[9] J.S. Smart, Modern Geometries, Third Edition, (1988), Brooks/Cole Publishing Company.

[10] J. Suzuki, A history of mathematics, Prentice-Hall Inc (2002).

[11] D. A. Thomas, Modern Geometry, Brooks/Cole (2002).

[12] A. I. Kostrikin, I. R. Shafarevich (Eds.), Algebra I: Basic Notions of Algebra, Springer-Verlag, (1986).

[13] S. MacLane and G. Birkhoff, Algebra, The MacMillan Company, New York, Collier-MacMillan Limited, London, (1968). URL: http://ir.lib.hiroshima-u.ac.jp/00000741

[14] Teiji Takagi, Daisugaku kougi (Lecture notes on algebra), Second edition, Kyoritsu Syuppan (1965).