Chapter 1

The Real and Complex Number Systems

1.1. Introduction

Notation. We begin with the **natural numbers**

$$\mathbf{N} = \{1, 2, 3, \cdots\}.$$

In **N** we can do addition and multiplication, but in order to do subtraction we need to extend **N** to the **integers**

$$\mathbf{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

In **Z** we can do addition, subtraction and multiplication, but in order to perform division we need to extend **Z** to the **rational numbers** or **rationals**,

$$\mathbf{Q} = \{\text{all fractions } \tfrac{p}{q} \text{ where } p \text{ and } q \text{ are integers with } q \neq 0\}.$$

In **Q** we have a *field* structure: addition and multiplication are defined with commutative, associative and distributive properties and the existence of additive and multiplicative inverses.

Also **Q** has a natural *order* structure defined on it (based on the ordering in **N**). Given any two rational numbers r and s, exactly one of the following is true:

$$r < s; \quad r = s; \quad s < r.$$

However, **Q** is inadequate for many purposes. For instance, if we have a square with each side of length 1, can we measure the length of its diagonal with a rational number? The answer is No. (See the proof below.) This leads to the introduction of so-called "irrational numbers", for example, $\sqrt{2}$.

Theorem 1.1. *There is no rational number whose square is 2.*

Proof. The theorem asserts that no rational numbers r exist such that $r^2 = 2$; that is, if r is any rational number then $r^2 \neq 2$. Since any rational number r is given by $r = \frac{p}{q}$ for some integers p and q with $q \neq 0$. Therefore, what we need to show is that no matter what such p and q are chosen it is never the case $(p/q)^2 = 2$. The line of attack is indirect, using a method of proof by contradiction; the idea is to show the opposite cannot be true. That is, assume there *exist* some integers p and q with $q \neq 0$ such that $(p/q)^2 = 2$ and we want to reach a conclusion that is unacceptable (absurd). We can also assume p and q have no common factors greater than 1 since any such common factors can be canceled out, leaving the fraction $\frac{p}{q}$ unchanged. From $(p/q)^2 = 2$ we have

$$p^2 = 2q^2;$$

hence we know p^2 is an *even* number, and hence p itself must be even (otherwise p is odd and p^2 would be odd). So write $p = 2k$ where k is an integer. Then $p^2 = 4k^2 = 2q^2$. Hence we have $q^2 = 2k^2$, which again implies q must be an even number. However, in the beginning, we assumed p and q have no common factors greater than 1, but we have reached a conclusion that p and q are both even and so have a common factor 2. This contradiction shows that the statement that *there exist some integers p and q with $q \neq 0$ such that* $(p/q)^2 = 2$ must be false. This proves the original statement of the theorem. □

EXAMPLE 1.1. We now examine the situation a little closely. Let A be the set of all positive rationals p such that $p^2 < 2$ and let B be the set of all positive rationals p such that $p^2 > 2$. We show that *A contains no largest number and B contains no smallest number.*

More explicitly, we show that, for every p in A (in B, respectively) we can find a rational q in A (in B, respectively) such that $q > p$ ($q < p$, respectively).

To do this, given each rational $p > 0$, let

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}.$$

Then q is also rational and

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2}.$$

Therefore, if $p \in A$ then $q \in A$ and $q > p$, and if $p \in B$ then $q \in B$ and $q < p$.

Definition 1.1. A **set** is any collection of objects. These objects are referred to as the **elements** of the set. A set containing no element is called the **empty set** and is denoted by $\emptyset$.

Given a set A, if x is an element of A then we write $x \in A$ (and say x is in A or belongs to A or x is an element of A). If x is not an element of A then we write $x \notin A$.

Given two sets A and B, if every element of A is an element of B, then we write $A \subseteq B$ or $B \supseteq A$; in this case, we say A is a **subset** of B. Note that two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

1.2. Ordered Sets

Definition 1.2. Let S be a set. An **order** on S is a relation, denoted by $<$, with the following two properties:

(1) If $x \in S$ and $y \in S$, then *one and only one* of the statements

$$x < y, \quad x = y, \quad y < x$$

is true.

(2) For $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

The statement “$x < y$” may be read as “x is less than y” or “x is smaller than y” or “x precedes y”.

Sometimes we write $x < y$ equivalently as $y > x$. The notation $x \leq y$ means $x < y$ or $x = y$. In other words, $x \leq y$ is the negation of $x > y$. The notation $x \geq y$ has a similar meaning.

Definition 1.3. An **ordered set** is a set S in which an order $<$ is defined; sometimes an ordered set is denoted by $(S, <)$.

For example, in $\mathbf{Q}$, we define $r < s$ if (and only if) $s - r$ is a positive rational number. Then $(\mathbf{Q}, <)$ is an ordered set.

Least Upper Bound and Greatest Lower Bound.

Definition 1.4. Suppose $(S, <)$ is an ordered set, and $E \subseteq S$. We say that E is **bounded above** if there exists a $\beta \in S$ such that $x \leq \beta$ for all $x \in E$. Any such a $\beta \in S$ is called an **upper-bound** of E.

Similarly, a set $E \subseteq S$ is called **bounded below** if there exists a $\beta \in S$ such that $x \geq \beta$ for all $x \in E$. Any such a $\beta \in S$ is called a **lower-bound** of E.

Definition 1.5. Suppose $(S, <)$ is an ordered set, $E \subseteq S$ and $\alpha \in S$. We say that α is a **least upper-bound** of A if α satisfies the following two criteria:

(i) α is an upper-bound of E.

(ii) If $\gamma < \alpha$, then γ is not an upper-bound of E.

A least upper bound α of a set E, if exists, must be unique: If α_1 and α_2 are both least upper-bound of E, then, by the criteria (ii) of the definition (see also (ii”) below), we must have that $\alpha_1 \leq \alpha_2$ and $\alpha_2 \leq \alpha_1$; thus $\alpha_1 = \alpha_2$. We also call the least upper bound α of E the **supremum** of E and write

$$\alpha = \sup E.$$

In the same manner, the **greatest lower bound** α, or **infimum**, of a set $E \subseteq S$ is defined and denoted by

$$\alpha = \inf E.$$

If $\sup E \in E$, then we call $\sup E$ the **maximum** of E and denote it also by $\max E$.

Similarly, if $\inf E \in E$ then we say $\inf E$ is the **minimum** of E and denote it by $\min E$.

Note that the criteria (ii) for least upper-bound is equivalent to each of the following two statements.

(ii’) If $\gamma < \alpha$, then there exists a $y \in E$ such that $\gamma < y$.

(ii”) If γ is an upper-bound of E, then $\alpha \leq \gamma$. (*This is the contrapositive of* (ii).)

Definition 1.6. An ordered set S is said to have the **least-upper-bound property** if the following is true:

Every nonempty subset of S that is bounded above has the least upper-bound in S.

Similarly one defines the **greatest-lower-bound property**.

Example 1.2. The ordered set $\mathbf{Q}$ does not have the least-upper-bound property.

Proof. Consider the sets A and B defined in Example 1.1. Clearly $A \subseteq \mathbf{Q}$ is nonempty, and every number in set B is an upper bound of set A (use the fact $\forall \alpha > 0, \beta > 0, \alpha^2 < \beta^2 \Rightarrow \alpha < \beta$). We show A has no least upper bound in $\mathbf{Q}$. Suppose $\alpha = \sup A$ existed in $\mathbf{Q}$. Then $\alpha^2 \neq 2$; hence either (i) $\alpha^2 < 2$ or (ii) $\alpha^2 > 2$.

In case (i), $\alpha \in A$ and by the proof in Example 1.1, there exists a $\beta \in A$ such that $\alpha < \beta$; but $\beta \leq \alpha$ since α is an upper bound of A, which gives the desired contradiction.

In case (ii), $\alpha \in B$ and by the proof of Example 1.1 there exists a $\beta \in B$ such that $\beta < \alpha$. Since $\beta \in B$ is an upper-bound of A, we reach a contradiction to (ii) of the definition of $\alpha = \sup A$. □

Theorem 1.2. *Suppose S is an ordered set with the least-upper-bound property. Then S also has the greatest-lower-bound property; that is, every nonempty subset of S that is bounded below has the greatest lower bound in S.*

Proof. Assume $B \subseteq S$ is nonempty and bounded below, with a lower-bound $y \in S$. Let L be the set of all lower-bounds of B in S. Then L is nonempty as $y \in L$. Also L is bounded above, for every element of B is an upper-bound of L. Hence by assumption, $\alpha = \sup L$ exists in S. We now prove

$$\alpha = \inf B$$

by showing the two criteria are true:

(i) α is a lower bound of B, and

(ii) for every $\gamma \in S$ with $\gamma > \alpha$ there exists a $y \in B$ such that $y < \gamma$.

If (i) is false, then there exists a $\beta \in B$ such that $\beta < \alpha$. Since $\alpha = \sup L$, this β is not an upper bound of L. So there exists a $y \in L$ such that $y > \beta$. Note that, as $y \in L$, y is a lower bound of B and hence $y \leq \beta$, a contradiction.

To show (ii), suppose for some $\gamma \in S$ with $\gamma > \alpha$ no such $y \in B$ existed. Then $\gamma \leq y$ for all $y \in B$; so γ is a lower bound of B; that is, $\gamma \in L$, which resulted in $\gamma \leq \sup L = \alpha$, a desired contradiction. □

1.3. Fields

Definition 1.7. A **field** is a set F with two operations, called **addition** and **multiplication**, which satisfy the following so-called **field axioms** (A), (M), and (D):

(A) Axioms for addition:

(A1) If $x \in F$ and $y \in F$, then their **sum** $x + y$ is in F.

(A2) Addition is commutative: $\forall x, y \in F,\ x + y = y + x$.

(A3) Addition is associative: $\forall x, y, z \in F,\ (x + y) + z = x + (y + z)$.

(A4) F contains an element 0 such that $0 + x = x$ for all $x \in F$.

(A5) To every $x \in F$ corresponds an element $-x \in F$ such that

$$x + (-x) = 0.$$

(M) Axioms for multiplication:

(M1) If $x \in F$ and $y \in F$, then their **product** xy is in F.

(M2) Multiplication is commutative: $\forall x, y \in F,\ xy = yx$.

(M3) Multiplication is associative: $\forall x, y, z \in F,\ (xy)z = x(yz)$.

(M4) F contains an element $1 \neq 0$ such that $1x = x$ for all $x \in F$.

(M5) To every $x \in F$ with $x \neq 0$ corresponds an element $x^{-1} \in F$ such that

$$x(x^{-1}) = 1.$$

(D) The distribution law: For all $x, y, z \in F$, it holds that

$$x(y + z) = xy + xz.$$

If F is a field, $E \subseteq F$ and E is itself a field under the addition and multiplication of F, then we say that E is a **subfield** of F.

Remark 1.8. (a) One usually writes $x^{-1} = 1/x = \frac{1}{x}$ or $xy^{-1} = x/y = \frac{x}{y}$ or

$$x + y + z = (x + y) + z, \quad xyz = (xy)z, \quad 2x = x + x, \quad x^3 = xxx, \quad \cdots$$

(b) Using the customary meaning of addition and multiplication of rational numbers, the set $\mathbf{Q}$ is a field.

(c) It is worthwhile that some familiar properties of $\mathbf{Q}$ are also true for general fields.

Lemma 1.3. *The axioms for addition imply the following statements.*

(a) *If $x + y = x + z$ then $y = z$.*

(b) *If $x + y = x$ then $y = 0$.*

(c) *If $x + y = 0$ then $y = -x$.*

(d) $-(-x) = x$.

Lemma 1.4. *The axioms for multiplication imply the following statements.*

(a) *If $x \neq 0$ and $xy = xz$ then $y = z$.*

(b) *If $x \neq 0$ and $xy = x$ then $y = 1$.*

(c) *If $x \neq 0$ and $xy = 1$ then $y = 1/x$.*

(d) *If $x \neq 0$ then $1/(1/x) = x$.*

Lemma 1.5. *The field axioms imply the following statements.*

(a) $0x = 0$.

(b) *If $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.*

(c) $(-x)y = -(xy) = x(-y)$.

(d) $(-x)(-y) = xy$.

Definition 1.9. An **ordered field** is a field F which is also an ordered set, such that

(1) if $x, y, z \in F$ and $y < z$, then $x + y < x + z$,

(2) if $x \in F, y \in F, x > 0$ and $y > 0$, then $xy > 0$.

If $x > 0$, we call x **positive**; if $x < 0$, we call x **negative**.

For example, $\mathbf{Q}$ is an ordered field.

All the familiar rules for working with inequalities apply in every ordered field; we have the following theorem.

Lemma 1.6. *The following statements are true in every ordered field.*

(a) *If $x > 0$ then $-x < 0$, and vice versa.*

(b) *If* $x > 0$ *and* $y < z$ *then* $xy < xz$.

(c) *If* $x < 0$ *and* $y < z$ *then* $xy > xz$.

(d) *If* $x \neq 0$ *then* $x^2 > 0$. *In particular,* $1 > 0$.

(e) *If* $0 < x < y$ *then* $0 < 1/y < 1/x$.

1.4. The Real Field

We now state the **existence theorem** which is the core of this chapter.

Theorem 1.7. *There exists an ordered field* $\mathbf{R}$ *which contains* $\mathbf{Q}$ *as a subfield and has the least-upper-bound property.*

The members of $\mathbf{R}$ are called **real numbers**. The proof of this theorem is rather long and based on the **Dedekind cuts** construction, and will not be discussed in the lecture.

First of all, we prove the following property.

Theorem 1.8. (i) (**Archimedean Property**) *If* $x \in \mathbf{R}, y \in \mathbf{R}$ *and* $x > 0$, *then there exists a positive integer* n *such that* $nx > y$.

(ii) (**Density of Q in R**) *For any two real numbers* a, b *with* $a < b$, *there exists a rational number* r *such that* $a < r < b$; *that is,* $\mathbf{Q} \cap (a, b) \neq \emptyset$ *for all intervals* $(a, b) \subseteq \mathbf{R}$.

Proof. We prove (i) by contradiction. Suppose the statement (i) is false; that is, for every $n \in \mathbf{N}$, one has $nx \leq y$. Let A be the set $A = \{nx : n \in \mathbf{N}\}$. Then y is an upper-bound of A. Therefore A is a nonempty set of real numbers that is bounded above. Hence the least-upper-bound property would assert that $\alpha = \sup A$ exists in $\mathbf{R}$. Since $x > 0$, we have $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of A; hence $\alpha - x < mx$ for some $m \in \mathbf{N}$. But then $\alpha < (m+1)x \in A$, contradicting the fact that α is an upper-bound of A.

For (ii), we can reduce the situations to the case where $b > a \geq 0$. (Explain why?)

So assume $a \geq 0$. Let $x = b - a > 0$. The Archimedean Property of (i) above implies that there exists an $n \in \mathbf{N}$ such that $nx > 1$; that is, $\frac{1}{n} < b - a$; hence, $na + 1 < nb$. Consider the set

$$S = \{r \in \mathbf{N} \, : \, r \leq na + 1\}.$$

This set S contains only finitely many elements (for example, let $m_0 \in \mathbf{N}$ be such that $m_0 > na + 1$; then S has at most m_0 elements). So let $m = \max S$. Then $m \leq na + 1$ and $m + 1 > na + 1$ (otherwise $m + 1 \in S$). For this $m \in \mathbf{N}$ we have

$$m - 1 \leq na < m.$$

Since $m \leq na + 1 < nb$, we have $\frac{m}{n} < b$. Since $na < m$, we have $\frac{m}{n} > a$ and hence $a < \frac{m}{n} < b$. □

Example 1.3. Let $A = \{\frac{n}{n+1} \mid n \in \mathbf{N}\} = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots\}$. Show that $\sup A = 1$.

Proof. By the definition of supremum, we need to prove the following two statements.

(i) 1 is an upper-bound of A; that is, $\forall a \in A \; (a \leq 1)$;

(ii) $\forall \gamma < 1 \; \exists a \in A \; (\gamma < a)$. [This is Criterion (ii'), equivalent to Criterion (ii) in the definition of supremum.]

To prove (i), let $a \in A$; then $a = \frac{n}{n+1}$ for some $n \in \mathbf{N}$. Since $1 - a = 1 - \frac{n}{n+1} = \frac{1}{n+1} > 0$, we have $a < 1$ and so (i) is true.

To prove (ii), let $\gamma < 1$; then, by the Archimedean property, there exists a number $n \in \mathbf{N}$ such that $\frac{1}{n} < 1 - \gamma$; so $\frac{1}{n+1} < \frac{1}{n} < 1 - \gamma$. Hence

$$\gamma < 1 - \frac{1}{n+1} = \frac{n}{n+1}.$$

Therefore, the number $a = \frac{n}{n+1}$ is in A and satisfies $\gamma < a$, which proves (ii).

Finally, by definition, $\sup A = 1$. □

Theorem 1.9 (Existence of n-th root)**.** *For every real $x > 0$ and every integer $n > 0$ there exists one and only one positive real number y such that $y^n = x$.* (This number y is called the n**th root** of x and is written $\sqrt[n]{x}$ or $x^{1/n}$.)

Proof. Since $0 < a < b$ implies $0 < a^n < b^n$, it is clear there exists at most one such y. We now prove the existence.

Let E be the set consisting of all positive real numbers t such that $t^n < x$.

If $t = x/(1+x)$ then $0 \le t < 1$. Hence $t^n \le t < x$ and so $t \in E$, and E is nonempty. For all $a \in \mathbf{R}$ with $a > 1 + x$, it follows that $a^n \ge a > x$ and hence $a \notin E$. This implies that if $a \in E$ then $a \le 1 + x$; hence $1 + x$ is an upper-bound of E. By the least-upper-bound property of $\mathbf{R}$,

$$y = \sup E$$

exists in $\mathbf{R}$. We now prove $y^n = x$ by showing that each of the inequalities $y^n < x$ and $y^n > x$ leads to a contradiction.

The identity

$$b^n - a^n = (b - a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$$

yields the inequality

$$b^n - a^n < (b - a)nb^{n-1}$$

whenever $0 < a < b$.

Assume $y^n < x$. Choose h so that $0 < h < 1$ and

$$h < \frac{x - y^n}{n(y+1)^{n-1}}.$$

Put $a = y, b = y + h$. Then

$$(y + h)^n - y^n < hn(y + h)^{n-1} < hn(y + 1)^{n-1} < x - y^n.$$

Thus $(y + h)^n < x$, and $y + h \in E$; so $y + h \le y$, a contradiction.

Assume $y^n > x$. Put

$$k = \frac{y^n - x}{ny^{n-1}}.$$

Then $0 < k < y$. If $t \ge y - k$, then

$$y^n - t^n \le y^n - (y - k)^n < kny^{n-1} = y^n - x,$$

and thus $t^n > x$; hence $t \notin E$. This implies that if $t \in E$ then $t < y - k$. So $y - k$ is an upper-bound of E, thus $y - k \ge y$ as $y = \sup E$ (see, e.g., (ii") above). This gives a desired contradiction.

Hence $y^n = x$, and the proof is complete. □

Corollary 1.10. *For any two positive real numbers a, b and a positive integer n, it follows that*

$$(ab)^{1/n} = a^{1/n} b^{1/n}.$$

Proof. Exercise. □

Decimals*. Let $x > 0$ be real. Let n_0 be the largest integer less than or equal to x. (Existence of such an n_0 is guaranteed by the Archimedean property.) This means

$$n_0 \leq x < n_0 + 1.$$

Let n_1 be the largest integer such that

$$n_0 + \frac{n_1}{10} \leq x.$$

Then $n_1 \in \{0, 1, 2, \cdots, 9\}$. (*Why?*) Suppose $n_1, \cdots, n_{k-1} \in \{0, 1, 2, \cdots, 9\}$ have been defined, let n_k be the largest integer such that

$$n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \cdots + \frac{n_k}{10^k} \leq x.$$

Again $n_k \in \{0, 1, 2, \cdots, 9\}$. Once all integers $n_0, n_1, \cdots, n_k, \cdots$ are defined, let E be the set of numbers

$$n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \cdots + \frac{n_k}{10^k} \quad (k = 0, 1, 2, \cdots).$$

Then $x = \sup E$. The **decimal expansion** of x is

$$x = n_0.n_1n_2n_3 \cdots .$$

Conversely, if $n_0, n_1, \cdots, n_k, \cdots$ are given, then the set E defined above is bounded above, and $\sup E = n_0.n_1n_2n_3 \cdots$.

We don't use decimals, so we omit the details.

The Extended Real Number System

We extend the real numbers $\mathbf{R}$ by adding two symbols, $-\infty$ and $+\infty$. We preserve the order in $\mathbf{R}$ and define

$$-\infty < x < +\infty$$

for every $x \in \mathbf{R}$.

The extended real number system does not form a field, but it is customary to make the following conventions:

(1) If x is real, then

$$x + (+\infty) = +\infty, \quad x - (+\infty) = -\infty, \quad \frac{x}{\pm\infty} = 0.$$

(2) If x is real and $x > 0$, then $x(+\infty) = +\infty$, $x(-\infty) = -\infty$.

(3) If x is real and $x < 0$, then $x(+\infty) = -\infty$, $x(-\infty) = +\infty$.

(4) If a subset E of $\mathbf{R}$ is not bounded above, then we define $\sup E = +\infty$; if E is not bounded below, then we define $\inf E = -\infty$.

1.5. The Complex Field*

Definition 1.10. A **complex number** is an *ordered pair* (a, b), where a, b are real numbers. The set of all complex numbers is denoted by $\mathbf{C}$.

Let $x = (a, b), y = (c, d)$ be two complex numbers. We write $x = y$ if and only if $a = c$ and $b = d$. We define

$$x + y = (a + c, b + d),$$
$$xy = (ac - bd, ad + bc).$$

Theorem 1.11. *The above addition and multiplication turn the set* $\mathbf{C}$ *of all complex numbers into a field, with* $(0, 0)$ *and* $(1, 0)$ *in the role of zero* 0 *and unit* 1 *in* $\mathbf{C}$.

Theorem 1.12. *For any real numbers* a *and* b *we have*

$$(a, 0) + (b, 0) = (a + b, 0), \quad (a, 0)(b, 0) = (ab, 0).$$

Therefore, if we identify every real number $a \in \mathbf{R}$ *with the complex number* $(a, 0) \in \mathbf{C}$, *then* $\mathbf{R}$ *becomes a subfield of* $\mathbf{C}$.

We will write $(a, 0) = a$ for all real numbers a.

Definition 1.11. We define $i = (0, 1)$. Then $i^2 = -1$.

Let $z = (a, b) \in \mathbf{C}$, where $a, b \in \mathbf{R}$. Then $z = a + bi$. We define $\bar{z} = a - bi$ to be the **conjugate** of z. We also write

$$a = \mathrm{Re} z, \quad b = \mathrm{Im} z.$$

Theorem 1.13. *Let* $z, w \in \mathbf{C}$. *Then*

$$\overline{z + w} = \bar{z} + \bar{w}, \quad \overline{zw} = \bar{z}\bar{w},$$
$$z + \bar{z} = 2Rez, \quad z - \bar{z} = 2iImz,$$

and $z\bar{z} > 0$ *if* $z \neq 0$. *We define the* **absolute value** *of* z *to be the real number* $(z\bar{z})^{1/2}$. *Then* $|z| > 0$ *if* $z \neq 0$ *and* $|0| = 0$.

Theorem 1.14. *Let* $z, w \in \mathbf{C}$. *Then*

$$|\bar{z}| = |z|, \quad |zw| = |z||w|, \quad |Rez| \leq |z|,$$

$$|z + w| \leq |z| + |w|. \tag{1.1}$$

Theorem 1.15 (Schwarz inequality). *Let* $z_1, \cdots, z_n \in \mathbf{C}$ *and* $w_1, \cdots, w_n \in \mathbf{C}$. *Then*

$$\left| \sum_{j=1}^{n} z_j \bar{w}_j \right|^2 \leq \left(\sum_{j=1}^{n} |z_j|^2 \right) \left(\sum_{j=1}^{n} |w_j|^2 \right). \tag{1.2}$$

Proof. Let $A = \sum_{j=1}^n |z_j|^2, B = \sum_{j=1}^n |w_j|^2$ and $C = \sum_{j=1}^n z_j \bar{w}_j$. If $B = 0$ then $w_1 = w_2 = \cdots = w_n = 0$, and (1.2) is trivial. Assume $B > 0$. Then, we have

$$\begin{aligned} 0 \leq \sum_{j=1}^{n} |Bz_j - Cw_j|^2 &= \sum_{j=1}^{n} (Bz_j - Cw_j)(B\bar{z}_j - \bar{C}\bar{w}_j) \\ &= \sum_{j=1}^{n} (B^2|z_j|^2 - B\bar{C}z_j\bar{w}_j - BC\bar{z}_j w_j + |C|^2|w_j|^2) \\ &= B(AB - |C|^2). \end{aligned}$$

Hence $|C|^2 \leq AB$, which is the Schwarz inequality (1.2). □

1.6. Euclidean Spaces

Definition 1.12. For each $n \in \mathbf{N}$, let $\mathbf{R}^n$ denote the set of all *ordered* n**-tuples**

$$\mathbf{x} = (x_1, x_2, \ldots, x_n),$$

where $x_1, \cdots, x_n$ are real numbers, called the **coordinates** of $\mathbf{x}$. The elements in $\mathbf{R}^n$ are called **points**, or **vectors**, especially when $n > 1$. Two points $\mathbf{x}, \mathbf{y}$ in $\mathbf{R}^n$ are equal if and only if all their corresponding coordinates are equal; that is, $x_j = y_j$ for all $j = 1, 2, \ldots, n$. The **origin** or **null vector** is the vector $\mathbf{0}$, all of whose coordinates are zero; that is, $\mathbf{0} = (0, 0, \ldots, 0)$.

Let $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbf{R}^n$, and $\alpha \in \mathbf{R}$.

(1) The **sum of vectors** $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$\mathbf{x} + \mathbf{y} := (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

(2) The **difference of vectors** $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$\mathbf{x} - \mathbf{y} := (x_1 - y_1, x_2 - y_2, \ldots, x_n - y_n).$$

(3) The **scalar multiplication** of vector $\mathbf{x}$ by α is defined by

$$\alpha\mathbf{x} := (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

(4) The **inner product of vectors** $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$\mathbf{x} \cdot \mathbf{y} := x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = \sum_{j=1}^{n} x_j y_j$$

and the **Euclidean norm of vector** $\mathbf{x}$ is defined by

$$\|\mathbf{x}\| := (x_1^2 + \cdots + x_n^2)^{1/2} = (\mathbf{x} \cdot \mathbf{x})^{1/2}.$$

(Note that the double bar "$\|$" is used here for the norm, instead of the single bar "$|$" as was used in the text; this is to distinguish with the absolute value sign.)

The set $\mathbf{R}^n$ equipped with these structures is called a **Euclidean space**.

Theorem 1.16. *Let* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{R}^n$ *and* $\alpha, \beta \in \mathbf{R}$. *Then*

$$\alpha\mathbf{0} = \mathbf{0},\ \ 0\mathbf{x} = \mathbf{0},\ \ \mathbf{0} + \mathbf{x} = \mathbf{x},\ \ \mathbf{x} - \mathbf{x} = \mathbf{0},\ \ 1\mathbf{x} = \mathbf{x},\ \ \mathbf{0} \cdot \mathbf{x} = 0,$$
$$\alpha(\beta\mathbf{x}) = \beta(\alpha\mathbf{x}) = (\alpha\beta)\mathbf{x}, \quad \alpha(\mathbf{x} \cdot \mathbf{y}) = (\alpha\mathbf{x}) \cdot \mathbf{y} = \mathbf{x} \cdot (\alpha\mathbf{y}),$$
$$\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}, \quad \mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}, \quad \mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x},$$
$$\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}, \quad \mathbf{x} \cdot (\mathbf{y} + \mathbf{z}) = \mathbf{x} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{z}.$$

Proof. All these properties follow easily from definition; we omit the details. □

Theorem 1.17 (Basic Properties of the Euclidean Space). *Let* $\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$. *Then*

(1) $\|\mathbf{x}\| \geq 0$ *with equality holding only when* $\mathbf{x} = \mathbf{0}$.

(2) $\|\alpha\mathbf{x}\| = |\alpha|\|\mathbf{x}\|$ *for all* $\alpha \in \mathbf{R}$.

(3) (**Cauchy-Schwarz Inequality**) $|\mathbf{x} \cdot \mathbf{y}| \leq \|\mathbf{x}\|\|\mathbf{y}\|$.

(4) (**Triangle Inequalities**)

$$\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|, \quad \|\mathbf{x} - \mathbf{z}\| \leq \|\mathbf{x} - \mathbf{y}\| + \|\mathbf{y} - \mathbf{z}\|$$

for all $\mathbf{z} \in \mathbf{R}^n$.

Proof. First two properties are immediate from the definition of the norm.

We now prove the Cauchy-Schwarz Inequality. Without loss of generality, assume $\mathbf{y} \neq \mathbf{0}$ and so $\|\mathbf{y}\| > 0$. For each $t \in \mathbf{R}$, we have

$$0 \leq \|\mathbf{x} - t\mathbf{y}\|^2 = (\mathbf{x} - t\mathbf{y}) \cdot (\mathbf{x} - t\mathbf{y}) = \mathbf{x} \cdot \mathbf{x} - 2t\mathbf{x} \cdot \mathbf{y} + t^2\mathbf{y} \cdot \mathbf{y} = \|\mathbf{x}\|^2 - 2t\mathbf{x} \cdot \mathbf{y} + t^2\|\mathbf{y}\|^2.$$

In this inequality, choosing $t = \frac{\mathbf{x}\cdot\mathbf{y}}{\|\mathbf{y}\|^2}$ and simplifying, we obtain the Cauchy-Schwarz Inequality.

Finally we prove the Triangle Inequality. From the **Cauchy-Schwarz Inequality**, we have

$$\|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + 2\mathbf{x} \cdot \mathbf{y} + \|\mathbf{y}\|^2 \leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2 = (\|\mathbf{x}\| + \|\mathbf{y}\|)^2.$$

Hence $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$.

From this, for all $\mathbf{z} \in \mathbf{R}^n$, we have that

$$\|\mathbf{x} - \mathbf{z}\| = \|\mathbf{x} - \mathbf{y} + \mathbf{y} - \mathbf{z}\| \leq \|\mathbf{x} - \mathbf{y}\| + \|\mathbf{y} - \mathbf{z}\|.$$

□

Suggested Homework Problems

Pages 21–23

Problems: 2–7, 19