CHAPTER 12: COMPLEX NUMBERS $\mathbb{C}$

WAYNE AITKEN AND LINDA HOLT

Summer 2019 Edition

1. Introduction

Although $\mathbb{R}$ is a complete ordered field, mathematicians do not stop at real numbers. The real numbers are limited in various ways. For example, not every polynomial with real coefficients factors into linear polynomials with real coefficients. This is related to the fact that there are real polynomials such as $x^2 + 1$ or $x^4 + 2x^2 + 5$ that have no real roots. The need to solve polynomial equations gave rise to the complex numbers.

As we know from basic algebra, when we work with quadratic equations sometimes the discriminant $b^2 - 4ac$ is negative, and in those cases we need to use complex numbers to find roots. The complex numbers allow us to use the quadratic equation successfully in all circumstances. However, the complex numbers did not arise first from quadratic equations. When a quadratic equation has no real solutions, why look for any solution at all? Wouldn't be easier to declare the problem unsolvable? This was the tactic used by early algebraists. It was later, in Renaissance Italy when the cubic and quartic equations were investigated, that square roots of negative numbers were first used. In fact, these so-called "imaginary numbers" are needed in the cubic equation even when looking for real solutions. Imaginary quantities arise in intermediate steps. For real solutions, the imaginary parts cancel out by the last step, but complex number arithmetic is required in intermediate computations. This means that you cannot avoid the complex numbers even when your goal is to find real solutions.

At first the complex numbers were viewed as fictitious numbers which were useful sometimes in finding "real" solutions. Later, about 1800, the idea arose of treating complex numbers as points in the plane. This made the complex numbers into tangible, non-fictitious objects. We will follow this approach and define $\mathbb{C}$ as $\mathbb{R} \times \mathbb{R}$. After defining addition and multiplication on $\mathbb{C}$, our goal will be to establish that $\mathbb{C}$ is a field. However, this field cannot be made into an ordered field. Even though it is not an ordered field, we can still define an absolute value on $\mathbb{C}$. We consider some of the properties of this absolute value including the triangle inequality.

The topics of finding roots of complex numbers and roots of polynomials are treated in appendices. These topics are very important, but fall out of the regular scope of this book which aims to treat number systems axiomatically in a self-contained manner. These topics fall out of this scope since will need to rely on trigonometry and other subjects to make further progress in the complex numbers.

2. Basic definitions

Definition 1. Define the set $\mathbb{C}$ of complex numbers as follows:

$$\mathbb{C} \stackrel{\text{def}}{=} \{(x, y) \mid x, y \in \mathbb{R}\}.$$

Remark 1. Recall that in set theory if S is a set then S^2 is defined to be $S \times S$ where $\times$ is the Cartesian product. So, as a set, $\mathbb{C}$ is just $\mathbb{R}^2$. There are differences between $\mathbb{C}$ and $\mathbb{R}^2$ when we start talking about binary operations. For example, the complex numbers $\mathbb{C}$ have a multiplication defined as a true binary operation, but $\mathbb{R}^2$ is typically given only a scalar multiplication.[1]

We now consider addition and a multiplication on $\mathbb{C}$.

Definition 2. Suppose that (x_1, y_1) and (x_2, y_2) are in $\mathbb{C}$. Then

$$(x_1, y_1) + (x_2, y_2) \stackrel{\text{def}}{=} (x_1 + x_2,\ y_1 + y_2)$$

and

$$(x_1, y_1) \cdot (x_2, y_2) \stackrel{\text{def}}{=} (x_1 x_2 - y_1 y_2,\ x_1 y_2 + x_2 y_1).$$

The addition and multiplication on the right hand side of these equations are the addition and multiplication in $\mathbb{R}$ defined in Chapter 10.

Remark 2. Thus $\mathbb{C}$ has two binary operations: addition $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ and multiplication $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$.

Exercise 1. Prove the following theorem.

Theorem 1. *Addition and multiplication on $\mathbb{C}$ are associative.*

Exercise 2. Prove the following two theorems.

Theorem 2. *Addition and multiplication on $\mathbb{C}$ are commutative.*

Theorem 3. *Addition and multiplication on $\mathbb{C}$ satisfy the distributive law.*

---

[1] However, vector addition in $\mathbb{R}^2$ and addition in $\mathbb{C}$ do correspond.

3. The canonical embedding

We want to view the complex numbers as an extension of the real numbers. In other words, we want to think of $\mathbb{R}$ as a subset of $\mathbb{C}$. Our definition (Definition 1) does not define $\mathbb{C}$ in such a way to make $\mathbb{R}$ automatically a subset. In order to regard $\mathbb{R}$ as a subset of $\mathbb{C}$ we need an injective function that embeds $\mathbb{R}$ into $\mathbb{C}$.

Definition 3. The *canonical embedding* $\mathbb{R} \to \mathbb{C}$ is the function defined by the rule

$$x \mapsto (x, 0).$$

Theorem 4. *The canonical embedding $\mathbb{R} \to \mathbb{C}$ is injective.*

Proof. Call the canonical embedding F. To show that $F : \mathbb{R} \to \mathbb{C}$ is injective we must show that, for all $a, b \in \mathbb{R}$, if $F(a) = F(b)$ then $a = b$.

Suppose $F(a) = F(b)$ where $a, b \in \mathbb{R}$ are arbitrary. Then $(a, 0) = (b, 0)$. By the definition of ordered pair (in set theory), this implies that the first coordinates are equal and that the second coordinates are equal. Since the first coordinates are equal, $a = b$ as desired. □

If we identify $x \in \mathbb{R}$ with its image $(x, 0)$ in $\mathbb{C}$, then we can think of $\mathbb{R}$ as a subset of $\mathbb{C}$. So, from now on, if $x \in \mathbb{R}$ then we will think of x and $(x, 0)$ as being the same number.

In particular, $0 \in \mathbb{R}$ can be identified with $(0, 0)$, and $1 \in \mathbb{R}$ can be identified with $(1, 0)$.

Theorem 5. *The number 0 is an additive identity for $\mathbb{C}$ and 1 is a multiplicative identity for $\mathbb{C}$.*

Proof. Identify 0 with $(0, 0)$. We must show that $(0, 0)$ is the additive identity. This follows from Definition 2 and the fact that $\mathbb{R}$ is a ring (Ch. 10):

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y)$$

for all $(x, y) \in \mathbb{C}$. Likewise, $(0, 0) + (x, y) = (x, y)$ by the commutative law. Checking that 1 is a multiplicative identity is left as an exercise. □

Exercise 3. Check that 1 is a multiplicative identity for $\mathbb{C}$.

Since we now think of $\mathbb{R}$ as a subset of $\mathbb{C}$ we have to be careful with $+$ and $\cdot$ in $\mathbb{R}$. We defined these operations for $\mathbb{R}$ in one way in Chapter 10, and then defined them for $\mathbb{C}$ in the current chapter. Do we get the same answer for real numbers $a, b \in \mathbb{R}$ as for the corresponding complex numbers $(a, 0)$ and $(b, 0)$? The answer is yes since, using Definition 2,

$$(a, 0) + (b, 0) = (a + b,\ 0 + 0) = (a + b,\ 0)$$

and

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

We summarize the above observations as follows.

Theorem 6. *Consider $\mathbb{R}$ as a subset of $\mathbb{C}$. Then the addition and multiplication operations on $\mathbb{C}$ extend the corresponding binary operations on $\mathbb{R}$.*

4. The square root of -1

The complex numbers possesses a number whose square is -1.

Definition 4. Let i be the complex number $(0,1)$.

Remark 3. Observe that i is not in the image of the canonical embedding $\mathbb{R} \to \mathbb{C}$. In other words, it is not a real number.

We now show the key property of i.

Theorem 7. *The number $i \in \mathbb{C}$ satisfies the equation*

$$i^2 = -1.$$

Exercise 4. Use Definition 2 and the canonical embedding to prove the theorem.

Remark 4. Because of this theorem, we call i the *square root of* -1. However, this terminology is a bit deceptive: the square root of -1 is not unique since $(0,-1)$ is also a square root of -1.

Informal Exercise 5. Show that $i = (0,1)$ and $(0,-1)$ are the only square roots of -1. Hint: suppose that $(x,y)\cdot(x,y) = (-1,0)$ and show that $x = 0$ and $y = \pm 1$. You can use the fact that, for real numbers, the only square roots of positive 1 are ± 1. You also know that $x^2 \geq 0$.

Remark 5. The complex numbers $\mathbb{C}$ cannot be thought of as an ordered field. To see this, consider $i^2 = -1$. In an ordered field, all squares are nonnegative but -1 is always negative (since 1 must be positive).

5. Standard form of complex numbers

We do not typically write complex numbers as ordered pairs: we like to write $x + yi$ for (x,y). We now establish that (x,y) and $x+yi$ are indeed the same complex number:

Theorem 8. *Let $(x,y) \in \mathbb{C}$ be a complex number. Then*

$$(x,y) \;=\; x + yi.$$

Proof. Observe that

$$\begin{aligned} x + yi &= (x,0) + (y,0)i && \text{(Canonical Embed.)} \\ &= (x,0) + (y,0)\cdot(0,1) && \text{(Def. 4)} \\ &= (x,0) + (y\cdot 0 - 0\cdot 1,\; y\cdot 1 + 0\cdot 0) && \text{(Def. 2)} \\ &= (x,0) + (0,y) && \text{(Laws in Ch. 10: } \mathbb{R} \text{ is a ring)} \\ &= (x,y) && \text{(Def. 2)} \end{aligned}$$

□

Remark 6. By the above theorem, we can think of the set $\mathbb{C}$ as follows:

$$\mathbb{C} \;=\; \{x + yi \mid x,y \in \mathbb{R}\}.$$

Theorem 9. *Let $x+yi$ and $v+wi$ be complex numbers where $x, y, v, w \in \mathbb{R}$. Then*

$$x + yi = v + wi \quad \Longleftrightarrow \quad x = v \text{ and } y = w.$$

Proof. The ($\Leftarrow$) direction uses the substitution law (of equality).

We wish to prove the ($\Rightarrow$) direction, so suppose $x + yi = v + wi$. By Theorem 8,

$$(x, y) = x + yi \quad \text{and} \quad (v, w) = v + wi.$$

Thus $(x, y) = (v, w)$. By set theory, two ordered pairs are equal if and only if their components are equal. So $x = v$ and $y = w$. □

Remark 7. The above theorems shows that every complex number can be written uniquely in the form $x + yi$ where $x, y \in \mathbb{R}$.

6. Ring properties

We almost have everything we need to establish that $\mathbb{C}$ is a commutative ring: we have commutative, associative, distributive laws, and additive and multiplicative identities. We also need additive inverses:

Theorem 10. *Every complex number has an additive inverse. In fact, if $x + yi$ be a complex numbers with $x, y \in \mathbb{R}$, then $(-x) + (-y)i$ is the additive inverse of $x + yi$. In other words,*

$$-(x + yi) = (-x) + (-y)i$$

where the inverse on the left denotes additive inverse in $\mathbb{C}$, while the inverses on the right denote additive inverses in $\mathbb{R}$.

Proof. Observe that

$$\begin{aligned} \big((-x) + (-y)i\big) + (x + yi) &= (-x, -y) + (x, y) \quad \text{(Thm. 8)} \\ &= (-x + x, -y + y) \quad \text{(Def. 2)} \\ &= (0, 0) \qquad \text{(Chapter 10 laws about } \mathbb{R}) \\ &= 0 \qquad \text{(Use of canonical embed.)} \end{aligned}$$

Since $\big((-x) + (-y)i\big) + (x + yi) = 0$, and since addition is commutative, the result follows. □

We now have everything we need for the following:

Theorem 11. *The set of complex numbers $\mathbb{C}$ is a commutative ring.*

Exercise 6. Review the definition of commutative ring, and verify that we have indeed proved everything we need for the above theorem. Cite where each was done.

Remark 8. Now we can use all the laws that hold in general rings. For example, we know that if z is a complex number, then $0 \cdot z = 0$. Of course we could verify this directly, but the point is we do not have to: such a law holds in all rings. Likewise, $-(-z) = z$ for all $z \in \mathbb{C}$ since such an identity is true in all rings. Furthermore, if $z, w \in \mathbb{C}$ then

$$-(zw) = (-z)w = z(-w)$$

since such a law holds in all rings. Also $(-1)z = -z$ and $(-z)(-w) = zw$ and $-(z + w) = (-z) + (-w)$ for all $z, w \in \mathbb{C}$ since such laws holds in all rings.

Remark 9. Theorem 10 says that

$$-(x + yi) = (-x) + (-y)i$$

where the left-hand use of $-$ is additive inverse in $\mathbb{C}$, and the right hand use of $-$ is additive inverse in $\mathbb{R}$. When $y = 0$ we get $-x = -x$ where left-hand use of $-$ is additive inverse in $\mathbb{C}$, and the right hand use of $-$ is additive inverse in $\mathbb{R}$. Thus the two definitions of inverse agree. In other words, the additive inverse of $\mathbb{C}$ extends that of $\mathbb{R}$.

As in any ring, we define $z - w$ as $z + (-w)$. Since both the additive inverse in $\mathbb{C}$ and the addition in $\mathbb{C}$ extends the corresponding operations in $\mathbb{R}$, we can conclude that subtraction in $\mathbb{C}$ extends subtraction in $\mathbb{R}$.

Since $\mathbb{C}$ is a ring, $-(z - w) = w - z$, $(z + w) - w = z$, $(z - w) + w = z$, etc. are automatically true.

Remark 10. Now that we know $\mathbb{C}$ is a ring, we can rederive and provide some motivation for Definition 2. In other words, if we forget Definition 2, we can rederive formulas for addition and multiplication. For addition:

$$\begin{aligned} (x + yi) + (v + wi) &= (x + v) + (yi + wi) && \text{(Assoc. and Comm.)} \\ &= (x + v) + (y + w)i && \text{(Distributive Law)} \end{aligned}$$

(here the first step combines several uses of the associative and commutative laws). For multiplication:

$$\begin{aligned} (x + yi)(v + wi) &= x(v + wi) + (yi)(v + wi) && \text{(Distributive Law)} \\ &= xv + x(wi) + (yi)v + (yi)(wi) && \text{(Distributive Law)} \\ &= xv + (xw)i + (yv)i + (yw)i^2 && \text{(Assoc./comm. for mult)} \\ &= xv + (xw)i + (yv)i + (yw)(-1) && \text{(Thm. 7)} \\ &= xv - yw + (xw)i + (yv)i && \text{(Properties of rings)} \\ &= (xv - yw) + (xw + yv)i && \text{(Distr. law)} \end{aligned}$$

Another way of saying this is that the formulas for addition and multiplication are a result of the fact that $i^2 = -1$ and that $\mathbb{C}$ is a ring. If someone constructed the complex numbers in another way such $i \in \mathbb{C}$ with $i^2 = -1$, such that this version of $\mathbb{C}$ is a ring, and such that every element is of the form $x + yi$ with $x, y \in \mathbb{R}$, then that person would have the same formulas for addition and multiplication as we do.[2]

[2] A fancy way of saying this is that all rings with these properties are canonically isomorphic.

7. Complex conjugation

We need to show that $\mathbb{C}$ is not just a ring, but is a field. To do this we need to show that every nonzero element has a multiplicative inverse. We will need complex conjugation to show how to form the multiplicative inverses.

Definition 5. Suppose $z \in \mathbb{C}$ where $z = x + yi$ with $x, y \in \mathbb{R}$. Then

$$\overline{z} \stackrel{\text{def}}{=} x - yi.$$

The complex number $\overline{z}$ is called the *complex conjugate* of z.

Theorem 12. *Let $z \in \mathbb{C}$. Then $\overline{z} = z$ if and only if z is a real number.*

Exercise 7. Show the above theorem. Hint: use Theorem 9 and properties of the real numbers.

Exercise 8. Prove the following two theorems.

Theorem 13. *Let $w, z \in \mathbb{C}$. Then*

$$\overline{z + w} = \overline{z} + \overline{w} \qquad \text{and} \qquad \overline{zw} = \overline{z}\,\overline{w}.$$

Theorem 14. *If $z \in \mathbb{C}$ then $\overline{\overline{z}} = z$.*

Theorem 15. *If $z \in \mathbb{C}$ then $-\overline{z} = \overline{-z}$.*

Proof. By Theorem 13

$$\overline{-z} + \overline{z} = \overline{(-z) + z} = \overline{0} = 0.$$

Now subtract $\overline{z}$ from both sides. □

Corollary 16. *If $z, w \in \mathbb{C}$ then $\overline{z - w} = \overline{z} - \overline{w}$.*

Proof. This follows from the definition of $z - w$ as $z + (-w)$ together with Theorems 13 and 15. □

Theorem 17. *Let $z \in \mathbb{C}$. If $z = x + yi$ with $x, y \in \mathbb{R}$ then*

$$\overline{z}z = x^2 + y^2.$$

Exercise 9. Prove the above theorem.

Theorem 18. *Let $z \in \mathbb{C}$. Then $z\overline{z}$ is a nonnegative real number. Furthermore, if $z \neq 0$ then $z\overline{z} > 0$.*

Proof. Write z as $x + yi$ with $x, y \in \mathbb{R}$. From Theorem 17 we know that

$$\overline{z}z = x^2 + y^2.$$

In particular, $\overline{z}z$ is a real number since $\mathbb{R}$ is closed under addition and multiplication.

If $z = 0$ the result is nonnegative since $0^2 + 0^2 = 0$.

If $z \neq 0$ then either x or y (or both) is nonzero. Suppose, for example, that x is nonzero. Since the product of two positive numbers is positive, and the product of two negative numbers is also positive, we have $x^2 > 0$

regardless of whether x is positive or negative (ordered fields, Chapter 8). Also $y^2 \geq 0$ (if $y > 0$ it follows as for x, if $y = 0$ then $y^2 = 0$). Thus

$$x^2 + y^2 > 0 + y^2 \geq 0 + 0 = 0$$

by properties of ordered fields (Chapter 8). Thus $\overline{z}z > 0$. A similar argument shows the result if $y \neq 0$. □

8. Field properties

The complex numbers form a field. To see this we need to to check that $1 \neq 0$ which is obvious (since $1 \neq 0$ in $\mathbb{R}$, and since $\mathbb{R}$ embeds into $\mathbb{C}$), and that every nonzero element has a multiplicative inverse. Suppose that $z \in \mathbb{C}$ is nonzero. Then $\overline{z}z$ is a positive real number by Theorem 18. Since $\mathbb{R}$ is a field, and since $\overline{z}z \neq 0$, the multiplicative inverse $(\overline{z}z)^{-1}$ exists in $\mathbb{R}$ (and hence in $\mathbb{C}$). Consider

$$w \stackrel{\text{def}}{=} (\overline{z}z)^{-1}\,\overline{z}.$$

Then

$$wz = (\overline{z}z)^{-1}\,\overline{z}z = 1.$$

So z has a multiplicative inverse. We can use this fact to prove the following.

Theorem 19. *The set of complex numbers $\mathbb{C}$ is a field.*

Exercise 10. Review the definition of *field*, and verify that we have proved everything we need for the above theorem.

Informal Exercise 11. Use the above formula for w to find the multiplicative inverse of $z = 2 + i$. Write your answer in the form $a + bi$ with $a, b \in \mathbb{R}$.

Informal Exercise 12. Find the multiplicative inverses of i and $3i$.

Informal Exercise 13. Convert

$$z = \frac{7 + 2i}{2 + 3i}$$

to the form $x + yi$ with $x, y \in \mathbb{R}$.

Exercise 14. Let $z \in \mathbb{C}$ be nonzero. Show that $\overline{z}^{-1} = \overline{z^{-1}}$. In addition, let $w \in \mathbb{C}$. Show that

$$\overline{\left(\frac{w}{z}\right)} = \frac{\overline{w}}{\overline{z}}.$$

9. Absolute values

In Chapters 9 and 11 we showed that every nonnegative real number x has a unique nonnegative square root $\sqrt{x}$. The square root is used in the definition of absolute value in $\mathbb{C}$.

Definition 6 (Absolute Value)**.** Let $z \in \mathbb{C}$. Then the *absolute value* $|z|$ of z is defined as follows:

$$|z| \stackrel{\text{def}}{=} \sqrt{z\overline{z}}.$$

Remark 11. Observe that if z is the point (x, y) then the above definition is equivalent to defining $|z|$ as $\sqrt{x^2 + y^2}$. Informally, we recognize this as the distance from (x, y) to the origin (Pythagorean theorem). This is analogous to the absolute value in $\mathbb{R}$ where the absolute value of a number is (informally) the distance of the number to 0. Observe that $|z| \geq 0$ by definition of square root, and that if z is real then this absolute value gives the same value as the absolute value defined for $\mathbb{R}$.

Finally, In order for this to be a well-behaved absolute value, we would want it to satisfy such familiar properties as the identity $|zw| = |z||w|$ and the i nequality $|z + w| \leq |z| + |w|$. These will be proved below.

Theorem 20. *If $z, w \in \mathbb{C}$ then*

$$|zw| = |z| \cdot |w|.$$

Proof. Observe that

$$\begin{aligned}
(|z| \cdot |w|)^2 &= |z|^2|w|^2 && \text{(Expon. Law, Ch. 5)} \\
&= z\overline{z}\, w\overline{w} && \text{(Def 6)} \\
&= zw\,\overline{z}\,\overline{w} && \text{(Comm./Assoc. Laws)} \\
&= zw\,\overline{zw} && \text{(Thm. 13)} \\
&= |zw|^2. && \text{(Def 6)}
\end{aligned}$$

By a result of Chapter 11, this implies that $|z| \cdot |w| = |zw|$. □

Theorem 21. *If $z \in \mathbb{C}$ then $|-z| = |z|$.*

Proof. By Theorem 20,

$$|-z|\,|-z| = |(-z)(-z)| = |zz| = |z||z|.$$

Thus $|-z|^2 = |z|^2$. So $|-z| = |z|$ by a result of Chapter 11. □

Theorem 22. *Suppose $z \in \mathbb{C}$. Then $|z| = 0$ if and only if $z = 0$.*

Exercise 15. Prove the above theorem.

Theorem 23. *Suppose $z = x + yi$ where $z \in \mathbb{C}$ and $x, y \in \mathbb{R}$. Then*

$$|x| \leq |z| \qquad \text{and} \qquad |y| \leq |z|.$$

Proof. Since $x^2 \geq 0$, we have $x^2 + y^2 \geq x^2$. Observe that $|x|^2 = x^2$ and $|z|^2 = x^2 + y^2$. Thus $|z|^2 \geq |x|^2$. So $|z| \geq |x|$.

A similar argument shows $|z| \geq |y|$. □

Now we wish to show the triangle inequality.

Lemma 24. *If $z \in \mathbb{C}$ then*

$$|z + 1| \leq |z| + 1.$$

Proof. Let $z = x + yi$ where $x, y \in \mathbb{R}$. Then $z + 1 = (x + 1) + yi$. Thus

$$|z + 1|^2 = (x + 1)^2 + y^2 = x^2 + 2x + 1 + y^2 = (x^2 + y^2) + 2x + 1.$$

If $x \geq 0$ then $x \leq |z|$ by Theorem 23. If $x < 0$ then $x \leq |z|$ since $|z| \geq 0$. In either case $x \leq |z|$. So

$$\begin{aligned} |z + 1|^2 &= (x^2 + y^2) + 2x + 1 \\ &= |z|^2 + 2x + 1 \\ &\leq |z|^2 + 2|z| + 1 \\ &= (|z| + 1)^2 . \end{aligned}$$

By a result in Chapter 11, this implies $|z + 1| \leq |z| + 1$. □

Theorem 25 (Triangle Inequality in $\mathbb{C}$)**.** *Let* $z, w \in \mathbb{C}$. *Then*

$$|z + w| \leq |z| + |w|.$$

Proof. If $w = 0$ then the result is clear. So assume $w \neq 0$. Let $u = zw^{-1}$. By Lemma 24,

$$|u + 1| \leq |u| + 1.$$

Multiply both sides by $|w|$: So

$$|u + 1||w| \leq (|u| + 1)|w| = |uw| + |w| = \left|zw^{-1}w\right| + |w| = |z| + |w|.$$

However,

$$|u + 1||w| = |(u + 1)w| = |uw + w| = \left|zw^{-1}w + w\right| = |z + w|.$$

So

$$|z + w| \leq |z| + |w|.$$

□