MATH 2040 Linear Algebra II
Supplementary Notes by Martin Li

Pre-requisite on complex numbers [1]

For the purpose of algebra, the set of real numbers $\mathbb{R}$ is often not sufficient. For example, there is no real roots to the quadratic equation $x^2 + 1 = 0$. In many situations, we would like to work with *complex numbers* which have similar algebraic properties with $\mathbb{R}$ but enjoy an extra property that any polynomial equation with complex coefficients must have at least one root. This property is so important that it is often called the "*Fundamental Theorem of Algebra*". In this short note, we will review some of the basic concepts about complex numbers.

Definition 1. *A* ***complex number*** *is an expression of the form $z = a + bi$, where $a, b \in \mathbb{R}$ are called the* ***real part*** *and* ***imaginary part*** *of z, denoted by $\operatorname{Re} z$ and $\operatorname{Im} z$, respectively. The* ***sum*** *and* ***product*** *of two complex numbers are defined by*

$$(a + bi) + (c + di) := (a + c) + (b + d)i,$$

$$(a + bi)(c + di) := (ac - bd) + (ad + bc)i,$$

where $a, b, c, d \in \mathbb{R}$. The set of all complex numbers is denoted by $\mathbb{C}$.

Using the multiplication defined above, one can verify that $i^2 = -1$. You can recover the definition of complex multiplication above by recalling that $i^2 = -1$ and then using the usual rules of arithmetic. The symbol $i = \sqrt{-1}$ was first introduced by Euler in 1777.

Any real number $a \in \mathbb{R}$ can be regarded as a complex number by identifying $a+0i$ with a. Therefore, we can think of $\mathbb{R}$ as a subset of $\mathbb{C}$. On the other hand, any complex number of the form $z = 0 + bi$, where $0 \neq b \in \mathbb{R}$, is called **purely imaginary**. Notice that the product of two purely imaginary numbers in $\mathbb{C}$ is real.

Example 1. *Let $z = 2 + 3i$ and $w = 4 + 5i$ be two complex numbers in $\mathbb{C}$. Then,*

$$z + w = (2 + 3i) + (4 + 5i) = (2 + 4) + (3 + 5)i = 6 + 8i,$$

$$zw = (2 + 3i)(4 + 5i) = (2 \cdot 4 - 3 \cdot 5) + (2 \cdot 5 + 3 \cdot 4)i = -7 + 22i.$$

Proposition 2. *Complex numbers satisfy the following algebraic properties:*

(i) (commutativity) $z + w = w + z$ and $zw = wz$ for all $z, w \in \mathbb{C}$.

(ii) (associativity) $(z + u) + w = z + (u + w)$ and $(zu)w = z(uw)$ for all $z, u, w \in \mathbb{C}$.

(iii) (identities) $z + 0 = z$ and $1z = z$ for all $z \in \mathbb{C}$.

(iv) (additive inverse) $\forall z \in C$, $\exists$ a unique $w \in \mathbb{C}$ such that $z + w = 0$.

(v) (multiplicative inverse) $\forall z \in C$ with $z \neq 0$, $\exists$ a unique $w \in \mathbb{C}$ such that $zw = 1$.

[1] last revised on September 5, 2017

(vi) (distributive property) $u(z+w) = uz + uw$ *for all* $u, z, w \in \mathbb{C}$.

Proof. The properties above are proved using familiar properties of real numbers and the definition of complex addition and multiplication. For example, to prove that $zw = wz$ for all $z, w \in C$, let $z = a + bi$ and $w = c + di$ where $a, b, c, d \in \mathbb{R}$, then

$$zw = (ac - bd) + (ad + bc)i = (ca - db) + (da + cd)i = wz.$$

The proof of the other properties are left as an exercise. □

Exercise 1. *Prove all the properties in the proposition above.*

Exercise 2. *Suppose* $a, b \in \mathbb{R}$, *not both zero. Find* $c, d \in \mathbb{R}$ *such that* $1/(a + bi) = c + di$.

Exercise 3. *Let* $z = \frac{-1+\sqrt{3}i}{2}$. *Show that* $z^3 = 1$.

Exercise 4. *Find two distinct* $z \in \mathbb{C}$ *such that* $z^2 = i$.

Definition 3. *Given a complex number* $z = a + bi \in \mathbb{C}$, *where* $a, b \in \mathbb{R}$, *the* ***complex conjugate*** *of* z, *denoted by* $\overline{z}$, *is the complex number* $\overline{z} = a - bi$.

Example 2. *The complex conjugates of the complex numbers* $1+2i$, $3i$, 5 *are given by* $1-2i$, $-3i$ *and* 5 *respectively.*

It is easy to see that $z + \overline{z} = 2 \operatorname{Re} z$ and $z - \overline{z} = 2i \operatorname{Im} z$. Moreover, we have the following:

Proposition 4. *Complex conjugation satisfies the following properties:*

(a) $\overline{\overline{z}} = z$ *for all* $z \in \mathbb{C}$.

(b) $\overline{z + w} = \overline{z} + \overline{w}$ *and* $\overline{zw} = \overline{z}\,\overline{w}$ *for all* $z, w \in \mathbb{C}$.

(c) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$ *for all* $z, w \in \mathbb{C}$ *with* $w \neq 0$.

(d) $\overline{z} = z$ *if and only if* $z \in \mathbb{R}$

(e) $\overline{z} = -z$ *if and only if* z *is purely imaginary.*

Proof. Exercise. □

Definition 5. *Let* $z = a + bi \in \mathbb{C}$ *where* $a, b \in \mathbb{R}$. *The* ***absolute value*** *or* ***modulus*** *of* z, *denoted by* $|z|$, *is defined by*

$$|z| := a^2 + b^2.$$

Note that by definition $|z|$ is always a non-negative real number. Moreover, $|z| = 0$ if and only of $z = 0$. Clearly, we have $|\operatorname{Re} z| \leq |z|$, $|\operatorname{Im} z| \leq |z|$ and $|z| = |\overline{z}|$ for all $z \in \mathbb{C}$.

Proposition 6. *Let* $z, w \in \mathbb{C}$. *Then the following statements are true:*

(a) $z\overline{z} = |z|^2$

(b) $|zw| = |z|\,|w|$.

(c) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ *whenever* $w \neq 0$.

(d) $||z| - |w|| \leq |z + w| \leq |z| + |w|$.

Proof. (a) Let $z = a + ib$, where $a, b \in \mathbb{R}$. Then

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2.$$

(b) By (a) and Proposition 4 (b)

$$|zw|^2 = (zw)\overline{(zw)} = (zw)(\overline{z}\,\overline{w}) = (z\overline{z})(w\overline{w}) = |z|^2|w|^2.$$

Taking square root on both sides gives the desired result.

(c) It follows from (b) by considering $|z| = \left|\frac{z}{w}\right| |w|$ and dividing by $|w| \neq 0$ on both sides.

(d) We first prove the second inequality. The first inequality will follow from the second by considering

$$|z| = |(z + w) - w| \leq |z + w| + | - w| = |z + w| + |w|$$

and subtracting $|w|$ on both sides. To prove that $|z + w| \leq |z| + |w|$ (also known is the *triangle inequality*), first notice that for any complex number $u = a + bi$, we have

$$u + \overline{u} = (a + bi) + (a - bi) = 2a \leq 2\sqrt{a^2 + b^2} = 2|u|.$$

Applying the above with $u = w\overline{z}$, we have

$$|z + w|^2 = (z + w)\overline{(z + w)} = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + w\overline{z} + \overline{w}z + w\overline{w}$$

$$\leq |z|^2 + 2|w\overline{z}| + |w|^2 = |z|^2 + 2|w||z| + |w|^2 = (|z| + |w|)^2.$$

Taking square root on both sides gives the required inequality.

□

The properties of complex conjugate and absolute value above provides some additional tools in manipulating complex numbers.

Example 3. *Compute the quotient* $\frac{1-i}{1+i}$ *as follows:*

$$\frac{1 - i}{1 + i} = \frac{(1 - i)\overline{(1 + i)}}{(1 + i)\overline{(1 + i)}} = \frac{(1 - i)^2}{|1 + i|^2} = \frac{-2i}{2} = -i.$$

Exercise 5. *Compute* $\frac{2-i}{3+4i}$.

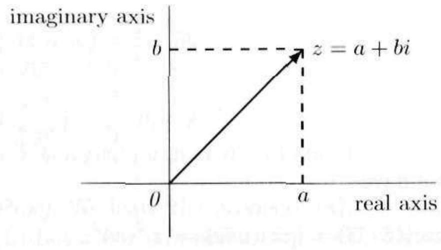

Figure 1: The complex plane

It is interesting that complex numbers have both a geometric and algebraic representation. Suppose $z = a + bi$ where $a, b \in \mathbb{R}$. We can draw z as a point in the plane $\mathbb{R}^2$ with coordinates (a, b). In this way, we identify $\mathbb{C}$ with the plane $\mathbb{R}^2$ where the x-axis is called the **real axis** and the y-axis is called the **imaginary axis** respectively. Under this identification, the addition of complex numbers is simply the vector addition in the plane, and $|z|$ gives the length of the vector z (from the origin). See Figure 1.

One can also introduce some kind of "*polar coordinates*" on the complex plane as follows. First, we define for any $\theta \in \mathbb{R}$,

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

This is the famous **Euler's formula** [2]. Using the picture of the complex plane above, $e^{i\theta}$, $\theta \in \mathbb{R}$, lies on the unit circle in the complex plane and thus one can express any non-zero complex number z as:

$$z = |z|e^{i\phi},$$

where ϕ is the angle that the vector z makes with the real axis (see Figure 2). Note that if $z = |z|e^{i\phi}$ and $w = |w|e^{i\omega}$, then $zw = |z||w|e^{i(\phi+\omega)}$ (can you prove this?). This gives a geometric meaning of complex multiplications.

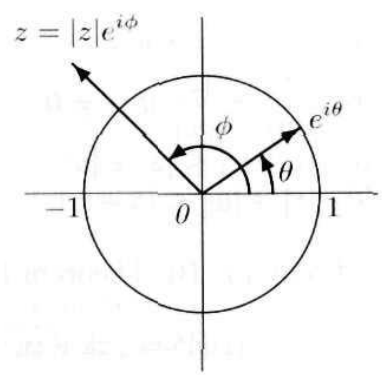

Figure 2: The polar coordinates on $\mathbb{C}$

The major reason for us to introduce complex numbers is that it is **algebraically closed**. Precisely, it means the following:

[2] Using this one can define the exponential of a complex number $z = a + bi$ (where $a, b \in \mathbb{R}$) by $e^z := e^a e^{ib} = e^a(\cos b + i\sin b)$.

Theorem 7 (The Fundamental Theorem of Algebra)**.** *Any non-constant polynomial with complex coefficients has at least one root in* $\mathbb{C}$*, i.e., for any* $p(z) = a_0 + a_1 z + \cdots + a_n z^n \in \mathcal{P}(\mathbb{C})$ *where* $a_n \neq 0$ *with* $n \geq 1$*, there exists some* $z_0 \in \mathbb{C}$ *such that* $p(z_0) = 0$*.*

There are many proofs of the theorem above using real or complex analysis, for example.

Additional topic: fields

Part of the reason why the real and complex numbers are so useful is that they are examples of an algebraic structure called a *field*. Roughly speaking, a *field* is a "number system" for which you can add, subtract, multiply and divide (by a non-zero number). More precisely, a field is defined as follows.

Definition 8. *A* ***field*** *is a set* $\mathbb{F}$ *on which two operations* $+$ *and* $\cdot$ *(called* ***addition*** *and* ***multiplication*** *respectively) are defined so that, for each pair of* $x, y \in \mathbb{F}$*, there are unique elements* $x + y$ *and* $x \cdot y$ *in* $\mathbb{F}$ *such that all the following properties are satisfied: for all* $a, b, c \in \mathbb{F}$*,*

(F1) (commutativity) $a + b = b + a$ *and* $a \cdot b = b \cdot a$

(F2) (associativity) $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(F3) (identity elements) there exist distinct elements 0 *and* 1 *in* $\mathbb{F}$ *such that* $0 + a = a$ *and* $1 \cdot a = a$ *for all* $a \in \mathbb{F}$

(F4) (inverses) For each $a \in \mathbb{F}$*, there exists* $b \in \mathbb{F}$ *such that* $a + b = 0$*. For each* $a \in \mathbb{F}$*,* $a \neq 0$*, there exists* $b \in \mathbb{F}$ *such that* $a \cdot b = 1$

(F5) (distributive law) $a \cdot (b + c) = a \cdot b + a \cdot c$

Of course, $\mathbb{R}$ and $\mathbb{C}$ are examples of a field. A less trivial example is the set of all rational numbers $\mathbb{Q}$. The following two are some interesting examples of a field.

Example 4. *The set* $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ *with the usual addition and multiplication is a field.*

Example 5. *The set* $\mathbb{Z}_2 = \{0, 1\}$ *with the operations defined by the following:*

$$0 + 0 = 0, \qquad 0 + 1 = 1 + 0 = 1, \qquad 1 + 1 = 0,$$

$$0 \cdot 0 = 0, \qquad 0 \cdot 1 = 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1,$$

is a field. This is the simplest example of a ***finite field****.*

Exercise 6. *Verify that* $\mathbb{Z}_2$ *is a field.*

Exercise 7. *Can you given an example of a field with exactly* 3 *elements?*

***Exercise 8.** *Can you given an example of a field with exactly* 4 *elements?*

Exercise 9. *Show that the set of all integers* $\mathbb{Z}$ *is not a field.*

One can derive a number of algebraic properties satisfied by any field (e.g. cancellation laws). We refer the readers to any textbook on abstract algebra for a more detailed treatment of fields.

In an arbitrary field $\mathbb{F}$, it may as well happen that $1 + 1 + \cdots + 1$ (p summands) equals 0 for some positive integer p. If such a p exists, the smallest positive integer p for which a sum of p 1's equals 0 is called the **characteristic** of $\mathbb{F}$. If no such p exists, we say that $\mathbb{F}$ has **characteristic zero**. For example, $\mathbb{Z}_2$ has characteristic 2 and both $\mathbb{R}$ and $\mathbb{C}$ has characteristic zero. In fact, almost all the theorems covered in this course holds for any field $\mathbb{F}$ of characteristic zero. However, for fields of characteristic p, many unnatural phenomenon appear. It is a challenging exercise to check which theorems fail for example in $\mathbb{Z}_2$ instead of $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.