Math 310
November 30, 2020 Lecture

Steven G. Krantz

November 25, 2020

Figure: This is your instructor.

Key Properties of the Real Numbers

We resume our study of Dedekind cuts as a means to construct the real number system. It will turn out, as we shall see momentarily, that the collection of all Dedekind cuts *is* the real number sysem $\mathbb{R}$.

It is now routine to verify that the set of all cuts, with this definition of multiplication, satisfies field axioms **M1**–**M5**. The proofs follow those for **A1**–**A5** rather closely.

For the distributive property, one first checks the case when all the cuts are positive, reducing it to the distributive property for the rationals. Then one handles negative cuts on a case-by-case basis.

The two properties of an ordered field are also easily checked for the set of all cuts.

We now know that the collection of all cuts forms an ordered field. Denote this field by the symbol $\mathbb{R}$ and call it the *real number system*. We next verify the crucial property of $\mathbb{R}$ that sets it apart from $\mathbb{Q}$:

Theorem:

The ordered field $\mathbb{R}$ satisfies the Least Upper Bound Property.

This result is obviously the whole point of our work up to this point. Because we know, on account of this theorem, that the set of Dedekind cuts is an ordered field containing the rationals (see below) that satisfies the Least Upper Bound Property. Everything that we proved about the reals in the previous two lectures relied entirely on this fact.

Proof: Let S be a subset of $\mathbb{R}$ which is bounded above. That is, there is a cut α such that $s < \alpha$ for all $s \in S$. Define

$$\mathcal{S}^* = \bigcup_{\mathcal{C} \in S} \mathcal{C}.$$

Then $\mathcal{S}^*$ is clearly nonempty, and it is therefore a cut since it is a union of cuts. It is also clearly an upper bound for S since it contains each element of S. It remains to check that $\mathcal{S}^*$ is the least upper bound for S.

In fact, if $\mathcal{T} < \mathcal{S}^*$, then $\mathcal{T} \subset \mathcal{S}^*$ and there is a rational number q in $\mathcal{S}^* \setminus \mathcal{T}$. But, by the definition of $\mathcal{S}^*$, it must be that $q \in \mathcal{C}$ for some $\mathcal{C} \in S$. So $\mathcal{C} > \mathcal{T}$, and $\mathcal{T}$ cannot be an upper bound for S. Therefore $\mathcal{S}^*$ is the least upper bound for S, as desired. $\square$

We have shown that $\mathbb{R}$ is an ordered field that satisfies the least upper bound property. It remains to show that $\mathbb{R}$ contains (a copy of) $\mathbb{Q}$ in a natural way. In fact, if $q \in \mathbb{Q}$ we associate to it the element $\varphi(q) = \mathcal{C}_q \equiv \{x \in \mathbb{Q} : x < q\}$. Then $\mathcal{C}_q$ is obviously a cut. It is also routine to check that

$$\varphi(q + q^*) = \varphi(q) + \varphi(q^*) \quad \text{and} \quad \varphi(q \cdot q^*) = \varphi(q) \cdot \varphi(q^*).$$

Therefore we see that φ is a ring homomorphism (see [LAN]) and hence represents $\mathbb{Q}$ as a "subfield" of $\mathbb{R}$.

The Complex Number System

The way that we are taught about the complex numbers in high school is completely misleading. We are led to believe that this number system is some mysterious object containing "imaginary numbers," one of which plays the role of the square root of -1.

This is the wrong way to look at things. Just as with our other number systems, we shall *construct* the complex numbers. It will follow from this construction that there is an element i that satisfies $i \cdot i = -1$. This will just be true for reasons of algebra.

So what we will see is that the complex numbers are just $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ equipped with two binary operations: addition and multiplication. And here they are:

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

and

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y)\,.$$

Although it is tempting to define multiplication by

$$(x, y) \cdot (x', y') = (xx', yy'),$$

this would be a mistake. For this defintion would allow the product of two nonzero elements to be 0: $(1, 0) \cdot (0, 1) = (0, 0)$. It would also fail to have a number of other desirable properties. You will see that it is much more productive to use the somewhat mysterious definition of multiplication given on the previous screen.

If you are puzzled by this definition of multiplication, then do not worry. In a few moments you will see that it gives rise to the notion of multiplication of complex numbers that you have seen before. In any event, this notion of multiplication has the properties we need, and gives the answers that we want.

It is interesting to note that, unlike the integers and the rational numbers, the new number system $\mathbb{C}$ is *not* a collection of equivalence classes. Instead, $\mathbb{C}$ is the Euclidean plane equipped with some new algebraic operations.

Example:

Let $z = (3, -2)$ and $w = (4, 7)$ be two complex numbers. Then

$$z + w = (3, -2) + (4, 7) = (3 + 4, -2 + 7) = (7, 5).$$

Also

$$z \cdot w = (3, -2) \cdot (4, 7) = (3 \cdot 4 - (-2) \cdot 7\,,\; 3 \cdot 7 + (-2) \cdot 4) = (26, 13).$$

As usual, we ought to check that addition and multiplication are commutative, associative, that multiplication distributes over addition, and so forth. We shall leave these tasks to the exercises. Instead we develop some of the crucial properties of our new number system.

Theorem:

The following properties hold for the number system $\mathbb{C}$.

(1) The number $1 \equiv (1,0)$ is the multiplicative identity: $1 \cdot z = z$ for any $z \in \mathbb{C}$.

(2) The number $0 \equiv (0,0)$ is the additive identity: $0 + z = z$ for any $z \in \mathbb{C}$.

(3) Each complex number $z = (x,y)$ has an additive inverse $-z = (-x,-y)$: it holds that $z + (-z) = 0$.

(4) The number $i \equiv (0,1)$ satisfies $i \cdot i = (-1,0) \equiv -1$; in other words, i is a square root of -1.

Proof: These are direct calculations, but it is important for us to work out these facts.

First, let $z = (x, y)$ be any complex number. Then

$$1 \cdot z = (1, 0) \cdot (x, y) = (1 \cdot x - 0 \cdot y, 1 \cdot y + 0 \cdot x) = (x, y) = z.$$

This proves the first assertion.

For the second assertion, we have

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

With z as above, set $-z = (-x, -y)$. Then

$$z + (-z) = (x, y) + (-x, -y) = (x + (-x), y + (-y)) = (0, 0) = 0.$$

Finally, we calculate

$$i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1.$$

Thus, as asserted, i is a square root of -1.

Proposition:

If $z \in \mathbb{C}, z \neq 0$, then there is a complex number w such that $z \cdot w = 1$.

Proof: Write $z = (x, y)$ and set

$$w = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right).$$

Since $z \neq 0$, this definition makes sense. Then it is straightforward to verify that $z \cdot w = 1$. Indeed,

$$\begin{aligned} z \cdot w &= (x, y) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) \\ &= \left(\frac{x \cdot x}{x^2 + y^2} - \frac{y \cdot (-y)}{x^2 + y^2}, \frac{x \cdot (-y)}{x^2 + y^2} + \frac{y \cdot x}{x^2 + y^2} \right) \\ &= (1, 0) \, . \end{aligned}$$

□

Thus every nonzero complex number has a multiplicative inverse. The other field axioms for $\mathbb{C}$ are easy to check. We conclude that the number system $\mathbb{C}$ forms a field. You will prove in the exercises that it is not possible to order this field. If α is a real number, then we associate α with the complex number $(\alpha, 0)$. In this way, we can think of the real numbers as a *subset* of the complex numbers. In fact, the real field $\mathbb{R}$ is a *subfield* of the complex field $\mathbb{C}$. This means that if $\alpha, \beta \in \mathbb{R}$ and $(\alpha, 0), (\beta, 0)$ are the corresponding elements in $\mathbb{C}$, then $\alpha + \beta$ corresponds to $(\alpha + \beta, 0)$ and $\alpha \cdot \beta$ corresponds to $(\alpha, 0) \cdot (\beta, 0) = (\alpha\beta, 0)$.

With the remarks in the preceding paragraphs, we can sometimes ignore the distinction between the real numbers and the complex numbers. For example, we can write

$$5 \cdot i$$

and understand that it means $(5,0) \cdot (0,1) = (0,5)$. Likewise, the expression

$$5 \cdot 1$$

can be interpreted as $5 \cdot 1 = 5$ or as $(5,0) \cdot (1,0) = (5,0)$ without any danger of ambiguity or misunderstanding.

Theorem:

Every complex number can be written in the form $a + b \cdot i$, where a and b are real numbers. In fact, if $z = (a, b) \in \mathbb{C}$, then

$$z = a + b \cdot i.$$

Proof: With the identification of real numbers as a subfield of the complex numbers, we have that

$$a + b \cdot i = (a, 0) + (b, 0) \cdot (0, 1) = (a, 0) + (0, b) = (a, b) = z$$

as claimed. □

Now that we have constructed the complex number field, we will adhere to the usual custom of writing complex numbers as $z = a + b \cdot i$ or, more simply, $a + bi$. We call a the *real part* of z, denoted by Re z, and b the *imaginary part* of z, denoted Im z. In this notation, our algebraic operations become

$$(a + bi) + (a^* + b^* i) = (a + a^*) + (b + b^*)i$$

and

$$(a + bi) \cdot (a^* + b^* i) = (a \cdot a^* - b \cdot b^*) + (a \cdot b^* + a^* \cdot b)i.$$

If $z = a + bi$ is a complex number, then we define its *complex conjugate* to be the number $\bar{z} = a - bi$. We record some elementary facts about the complex conjugate:

Proposition:

If z, w are complex numbers, then

(1) $\overline{z + w} = \overline{z} + \overline{w}$;

(2) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

(3) $z + \overline{z} = 2 \cdot \operatorname{Re} z$;

(4) $z - \overline{z} = 2 \cdot i \cdot \operatorname{Im} z$;

(5) $z \cdot \overline{z} \geq 0$, with equality holding if and only if $z = 0$.

Proof: Write $z = a + bi, w = c + di$. Then

$$\begin{aligned}
\overline{z + w} &= \overline{(a + c) + (b + d)i} \\
&= (a + c) - (b + d)i \\
&= (a - bi) + (c - di) \\
&= \overline{z} + \overline{w}.
\end{aligned}$$

This proves **(1)**. Assertions **(2)**, **(3)**, and **(4)** are proved similarly. For **(5)**, notice that

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 + b^2 \geq 0.$$

Clearly equality holds if and only if $a = b = 0$. □

The expression $|z|$ is defined to be the nonnegative square root of $z \cdot \overline{z}$. In other words

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{(x + iy) \cdot (x - iy)} = \sqrt{x^2 + y^2}.$$

It is called the *modulus* of z and plays the same role for the complex field that absolute value plays for the real field: the modulus of z measures the distance of z to the origin.

The modulus has the following properties.

Proposition:

If $z, w \in \mathbb{C}$, then

(1) $|z| = |\overline{z}|$;

(2) $|z \cdot w| = |z| \cdot |w|$;

(3) $|\text{Re } z| \leq |z| \quad , \quad |\text{Im } z| \leq |z|$;

(4) $|z + w| \leq |z| + |w| \quad .$

Proof: Write $z = a + bi, w = c + di$. Then **(1)**, **(2)**, and **(3)** are immediate. For **(4)** we calculate that

$$\begin{aligned}
|z+w|^2 &= (z+w)\cdot(\overline{z+w}) \\
&= z\cdot\overline{z} + z\cdot\overline{w} + w\cdot\overline{z} + w\cdot\overline{w} \\
&= |z|^2 + 2\mathrm{Re}\,(z\cdot\overline{w}) + |w|^2 \\
&\leq |z|^2 + 2|z\cdot\overline{w}| + |w|^2 \\
&= |z|^2 + 2|z|\cdot|w| + |w|^2 \\
&= (|z| + |w|)^2.
\end{aligned}$$

Taking square roots proves **(4)**. □

Observe that, if z is real, then $z = a + 0i$ and the modulus of z equals the absolute value of a. Likewise, if $z = 0 + bi$ is pure imaginary, then the modulus of z equals the absolute value of b. In particular, the fourth part of the Proposition reduces, in the real case, to the triangle inequality

$$|x + y| \leq |x| + |y|.$$

The most important property of the complex numbers $\mathbb{C}$ is that $\mathbb{C}$ is *algebraically complete*. This means that any polynomial

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_k z^k$$

with complex coefficients has a complex root.

This result was first proved by Carl Friedrich Gauss (1777–1855) in his doctoral dissertation. He ultimately produced five distinct proofs of the result. Gauss's theorem was the capstone of hundreds of years of the development of particular methods for solving specific polynomial equations. Now we may be sure that the polynomial

$$p(z) = 3 - 5z + 9z^2 + 4z^3 - 12z^4 + 23z^5$$

has a root (indeed it has five roots!), even though we may have no idea how to actually *find* them.

Example:

Let us find all the roots of the polynomial

$$p(z) = z^3 + (-3 - i)z^2 + (2 + 3i)z - 2i\,.$$

With some experimentation, we find that $z = 1$ is a root of p. Dividing p by $(z - 1)$, we find that

$$p(z) = (z - 1) \cdot (z^2 + (-2 - i)z + 2i)\,.$$

Of course we can solve the quadratic polynomial using the quadratic formula. We find the two additional roots 2 and i.

Of course this result, the Fundamental Theorem of Algebra, is a deep and difficult theorem.