§5. INTRODUCTION TO COMPLEX NUMBERS – V.

FIELD AXIOMS.

• Field axioms.

We have devoted the last four lectures studying the complex number system \( \mathbb{C} \). We have focused on the arithmetic on \( \mathbb{C} \). The following summarizes what we have already learned:

Summary.

(i) The complex number system \( \mathbb{C} \) contains \( \mathbb{R} \) as its subsystem. In other words, \( \mathbb{C} \) is an enlargement of \( \mathbb{R} \) as a number system.

(ii) The usual ‘common sense’ arithmetic holds in \( \mathbb{C} \): The associativity and commutativity of multiplication, distributivity, and the feasibility of reciprocating a complex number. Here, the commutativity of multiplication cannot be taken for granted, because there is another number system called the quaternionic number system \( \mathbb{H} \) wherein the same fails.

(iii) There are two “super-formal” ways of defining \( \mathbb{C} \):

(iii-a) Define \( \mathbb{C} \) as \( \mathbb{R}^2 \) with implementation of the artificial multiplication ‘*’:

\[
\begin{bmatrix} a \\ b \end{bmatrix} \star \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac - bd \\ ad + bc \end{bmatrix}.
\]

(iii-b) Alternatively, define \( \mathbb{C} \) as the following set, with the usual matrix addition and multiplication:

\[
\mathbb{C} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}.
\]
(iv) There is the notion called the complex conjugate of a complex number. Also, there is the notion of the absolute value of a complex number.

(v) Any complex numbers can be square-rooted. More precisely:

(v-a) For an arbitrary \( \alpha \in \mathbb{C} ; \; \alpha \neq 0 \), there exist exactly two distinct \( \xi \in \mathbb{C} \) such that \( \xi^2 = \alpha \). They are negatives of each other.

(v-b) There exists one and only one \( \xi \in \mathbb{C} \) such that \( \xi^2 = 0 \), namely, \( \xi = 0 \).

(vi) The notion of quadratic equations makes sense. By virtue of (i), the general form of a quadratic equation with \( \mathbb{C} \)-coefficients is

\[
\alpha z^2 + \beta z + \gamma = 0 \quad (\alpha, \beta, \gamma \in \mathbb{C}; \; \alpha \neq 0),
\]

where \( z \) is the unknown. Any quadratic equation as above always has roots within \( \mathbb{C} \). The number of roots are at most two. More precisely, the formula for the roots of the above equation is

\[
z = \frac{-\beta \pm \sqrt{\beta^2 - 4 \alpha \gamma}}{2 \alpha},
\]

where \( \pm \sqrt{\beta^2 - 4 \alpha \gamma} \) signifies the two (mutually negative) square-roots of the complex number \( \beta^2 - 4 \alpha \gamma \) conforming to (v). (When \( \beta^2 - 4 \alpha \gamma \) equals 0 then the quadratic equation has exactly one root.) The fact that any quadratic equation has at least one, and at most two, roots should not be taken for granted: Over \( \mathbb{R} \), \( x^2 + 1 = 0 \) has no root, whereas over \( \mathbb{H} \), \( w^2 + 1 = 0 \) has infinitely many roots.
In the last four lectures we were thoroughly covering these. So, what’s the point after all? There are two major points we need complex numbers:

**Point Number One.**

\( \mathbb{C} \) encapsulates many important mathematical features – ‘the essence of arithmetics’. Mathematicians have extracted and crystallized them. One big part of the ‘essence’ is the so-called ‘Field Axioms’. \( \mathbb{C} \) fulfills all the ‘Field Axioms’, so \( \mathbb{C} \) is an example of a field. This is the main topic that we study today. Now, as is self-evident (once you see the ‘Field Axioms’), \( \mathbb{R} \) fulfills all the ‘Field Axioms’ too, so \( \mathbb{R} \) is another example of a field. So, in other words, the ‘Field Axioms’ alone does not differentiate \( \mathbb{C} \) from \( \mathbb{R} \). And that’s where the other big part of the ‘essence of arithmetics’ comes in, namely, \( \mathbb{C} \) possesses a very pleasant property in addition to being a field: As I have highlighted in item (v):

> “Any *quadratic* equation having coefficients in \( \mathbb{C} \) has roots within \( \mathbb{C} \)."

I have to stress that this is remarkable, because, as I mentioned above, if you replace \( \mathbb{C} \) with \( \mathbb{R} \) in the above sentence, then the same sentence is not true any more. Now, the next thing I say is extremely important, so listen carefully:

> “Any *algebraic equation, not just quadratic, but of an arbitrary degree*, having coefficients in \( \mathbb{C} \), has roots within \( \mathbb{C} \)."

This is actually due to the Great master Gauss.* If you have a good memory, you remember that a few lectures ago (‘Review of Lectures – XXXI, page 3) I mentioned the name ‘Fundamental Theorem of Algebra’, as well as the name Gauss. ‘Fundamental Theorem of Algebra’ refers to this very fact. Now, another terminology lesson. Suppose a ‘field’ \( F \) (which I am going to define shortly) satisfies this property, namely:

> “Any algebraic equation, not just quadratic, but of an arbitrary degree, having coefficients in \( F \), has roots within \( F \).”

Then we say \( F \) is an ‘algebraically closed field’. So, \( \mathbb{C} \) is an example of an ‘algebraically closed field’. On the other hand, \( \mathbb{R} \) is clearly not an ‘algebraically closed field’, though \( \mathbb{R} \) is still a field (as we will see shortly).

---

*Carl Friedrich Gauss (1777–1855).
$\mathbb{C}$ is actually the first example humans have ever encountered of an algebraically closed field. You might want to know if there is any other. I want to give you one right way. Technically, though, for that I must first define the notion of a field. But let me be a little loose here, so I’ll do it in the following way: I first define the notion of ‘algebraic numbers’. Then I will say that the entire set of algebraic numbers is an example of an algebraically closed field. At that point you are motivated to hear the definition of a field. That’s where I define fields. Now, to that end, I want to first cover the following. I wanted to cover this at some point. This is a good place to do it. Do me one favor: Please don’t prematurely judge the level of difficulty.

**Definition (Rational numbers).**

A rational number is a real number which can be written as $\frac{b}{a} \quad (a, b: \text{an integer, } a \neq 0)$.

Note that an integer is a rational number, because an integer $a$ can be written as $\frac{a}{1}$. Now, there is another, equivalent, definition of a rational number:

**Alternative Definition (Rational numbers).**

A rational number is a real number which falls into either (i) or (ii):

(i) its decimal expression stops after finitely many digits under the decimal point (this includes an integer), or

(ii) its decimal expression contains a portion (‘unit’) made of a finite number of consecutive digits, and the whole decimal expression of that number is an infinite times iteration of that unit, except possibly a finite number of leading digits.

**Example.**

1. $0.52 = \frac{13}{25}$, and $0.3125 = \frac{5}{16}$ are both rational numbers. These fall into (i).

2. $0.003636363636... = \frac{1}{275}$, and $10.9142857142857142857... = \frac{764}{70}$ are both rational numbers. These fall into (ii).
Definition (Irrational number). A real number which is not a rational number is called an irrational number.

Example. \( \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6} \) are all irrational numbers. More generally, \( \sqrt{a} \), where \( a \) is a positive integer which is not square of another integer, is an irrational number.

Example. \( 3\sqrt{2}, 4\sqrt{3}, 6\sqrt{7}, \cdots \), are all irrational numbers. More generally, \( m\sqrt{a} \), where \( m \) is an integer, \( m \geq 2 \), and \( a \) is a positive integer which is not the \( m \)-th power of another integer, is an irrational number.

But the truth is that there are many many more examples of an irrational number. Actually, ‘anecdotally’, 99.999...% of real numbers are irrational. Rational numbers are extremely sparse inside \( \mathbb{R} \). Making it precise requires the notion of ‘cardinality’ which I would rather spare today.

Notation. In mathematics, it is common to denote the entire set of rational numbers by \( \mathbb{Q} \).

Side-track: Certain real numbers are unknown to be either rational or irrational. Probably the following is one of the most famous examples of a real number whose rationality/irrationality is still an open problem, that is, it is “up in the air”. The number in question is called the Euler’s constant:

\[
\gamma = \lim_{m \to \infty} \left[ \left( \sum_{k=1}^{m} \frac{1}{k} \right) - \log (m + 1) \right] = \int_{x=0}^{1} \left( \frac{1}{\log(1-x)} + \frac{1}{x} \right) dx.
\]

The decimal expression of \( \gamma \) (only the first 30 digits under the decimal point):

\[\gamma = 0.577215664901532860606512090082...\]

What nobody knows is if that decimal expression falls into either (i) or (ii) or not. You will become famous if you settle this question, namely, if you manage to prove that this number \( \gamma \) is irrational (or rational), before somebody else proves it.
• Algebraic numbers and transcendental numbers.

Now, with all that in mind, let’s turn our attention to \( \mathbb{C} \). The following may actually be considered inside \( \mathbb{R} \) but nothing stops me from considering it inside \( \mathbb{C} \). We are going to define the notion of algebraic numbers. In one line, algebraic numbers are roots of an algebraic equation (of any degree) having rational number coefficients. Here is the more precise definition:

**Definition.** A root in \( \mathbb{C} \) of an equation

\[
  a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = 0,
\]

where \( d \) is a positive integer and \( a_d, a_{d-1}, \ldots, a_1, a_0 \) are rational numbers, is called an algebraic number.

First, clearly all rational numbers are algebraic. Indeed, let \( c \) be a rational number. Then clearly \( c \) is a root of \( x - c = 0 \). In particular, integers are all algebraic. Some examples of algebraic numbers that are irrational:

**Example.** The following numbers are all algebraic:

\[
  \sqrt{2}, \quad \sqrt{3}, \quad \sqrt{-1}, \quad 3\sqrt{2}, \quad \frac{-1 + \sqrt{-3}}{2},
\]

\[
  \sqrt{2} + \sqrt{3}, \quad \sqrt{2} + \sqrt{-1}, \quad 3\sqrt{2} + 4\sqrt{3},
\]

\[
  6\sqrt{\frac{7}{4}}, \quad \sqrt{\frac{2 - \sqrt{5}}{4}}, \quad 3\sqrt{-13} + \sqrt{-27},
\]

\[
  1 + \sqrt{2} + \sqrt{3} + \sqrt{6}, \quad \left(1 - 5\sqrt{2}\right)^5,
\]

are all examples of algebraic numbers.

But there are many, many more. You can actually create countless many examples of algebraic numbers out of known algebraic numbers (such as integers). Namely:
(a) You add or multiply two algebraic numbers and the outcome is an algebraic number.

(b) You negate or reciprocate a (non-zero) algebraic number and the outcome is an algebraic number.

(c) You take the radical (m-th root) of an algebraic number, and the outcome is an algebraic number. Here, ‘the m-th root’ is as a complex number, which exists, as explained briefly in “Review of Lectures – XXXIII”.

Now, the above statements (a), (b) and (c) may not be too trivial to you. Although I am not saying that it is unimportant, proofs of these statements are not exactly the main theme of today’s lecture. It’s just way too much off the track. So, let’s not worry about the proofs, but let’s just accept the validity of (a), (b) and (c). (However, see Example in page 26.) Now, that said, I want you to agree with me on the following:

“The examples of algebraic numbers listed above are all obtained by iterating the procedures (a), (b) and (c), starting with (an) integer(s), so they all have a finite expression involving integers and addition, subtraction, multiplication, division and radicals (square-root, cube-root, 4-th root, 5-th root, ..).”

Why would I bother to make a statement like this? Because I want to say something very important, some subtlety concerning this notion of algebraic numbers. Please read the following carefully:

“Those numbers that have a finite expression involving integers and addition, subtraction, multiplication, division and radicals (square-root, cube-root, 4-th root, 5-th root, ..) are actually the minority in numbers among the population of algebraic numbers. The vast majority of algebraic numbers have no such expression.”

If you are puzzled, let me throw two examples:
Example. Let $a$ be an arbitrary real number (fixed). Consider the equation

\begin{equation}
(1) \quad x^5 + 5^4 a x^3 + 6 \cdot 5^4 \left(a^2 - a\right) x^2 \\
+ 5^5 \left(2a^3 - 3a^2 + 2a\right) x + 5^5 \left(a^4 - 2a^3 + 2a^2 - a\right) = 0.
\end{equation}

Despite its rather complex appearance, the equation (1) can actually be solved. Indeed, the equation has five roots in $\mathbb{C}$, and one of those five is

$$x = 1 - a - \left(1 - 5\sqrt[5]{a}\right)^5.$$ 

The other four roots can be easily concocted from this root. But that is not our interest now. (We will revisit this example later.)

Example. Let $a$ be an arbitrary real number (fixed). Consider the equation

\begin{equation}
(2) \quad x^5 + x + a = 0.
\end{equation}

If $a$ takes a certain value, such as $a = 0$, $2$, or $-34$, then you can find one root of the equation (2) ‘by speculation’. However, surprisingly enough, if $a$ is general, then there is no formula for the roots of this equation (2) using addition, subtraction, multiplication, division and radicals. The existence of five roots of the equation (2) is guaranteed by fundamental theorem of algebra. (More precisely, it is proved that, if $a$ is real then the equation (2) indeed has five distinct roots in $\mathbb{C}$, and moreover precisely one of the five roots is in $\mathbb{R}$.) However, there is just no way to physically write out the roots only using integers, addition, subtraction, multiplication, division and radicals.*

There is actually a history behind this. For a long time in the history of mathematics, it has been widely believed that there would be a formula that expresses the roots of a general algebraic equation (with a single unknown) of any degree using radicals. There indeed exists such a formula for the general cubic, and the general quartic (=degree 4) equations, known as Cardano’s formula, and Ferrari’s formula, respectively. Mathematicians have tried hard to generalize them to the general quintic (=degree 5) equations, and no one succeeded. Then a Norwegian mathematician called Abel has shocked the world by proving that such formula does not exist. Almost at the same time, a French mathematician called Galois investigated what types of algebraic equations can have roots that have a finite expression using radicals.*

*As for proof, see, for example, D. Fuchs–S. Tabachnikov “Mathematical Omnibus”, AMS.
*Niels Henrik Abel (1802–1829); Evariste Galois (1811–1832).
Now, the following is another series of examples of algebraic numbers:

**Example.** The following complex numbers are all algebraic:

\[
\cos (r \pi), \quad \sin (r \pi) \quad \text{(where } r \text{ is a rational number)},
\]

and also

\[
e^{\sqrt{-1} r \pi} = \cos (r \pi) + \sqrt{-1} \sin (r \pi) \quad \text{(where } r \text{ is a rational number}).
\]

In particular:

**Example.**

\[
\cos \frac{2}{11} \pi, \quad \sin \frac{2}{11} \pi,
\]

and also

\[
e^{\sqrt{-1} \frac{2\pi}{11}} = \left( \cos \frac{2}{11} \pi \right) + \sqrt{-1} \cdot \left( \sin \frac{2}{11} \pi \right)
\]

are all algebraic numbers.

Now here is what’s interesting: \( e^{\sqrt{-1} \frac{2\pi}{11}} \) is an 11-th root of 1, needless to say. Indeed, recall

\[
\left( e^{\sqrt{-1} \phi} \right)^m = e^{\sqrt{-1} \phi}
\]

(from “Review of Lectures – XXXIII”, page 22). For \( m = 11 \) and \( \phi = 2 \pi \), this reads

\[
\left( e^{\sqrt{-1} \frac{2\pi}{11}} \right)^{11} = e^{\sqrt{-1} \cdot 2 \pi} = 1.
\]
On the other hand, neither of

\[ \cos \left( \frac{2}{11} \pi \right), \; \text{nor} \; \sin \left( \frac{2}{11} \pi \right) \]

has a finite expression only involving integers and addition, subtraction, multiplication, division and radicals. Don’t get disappointed. We still have:

**Fact 1.**

\[ x = 2 \cos \left( \frac{2}{11} \pi \right) \]

satisfies the equation

\[ (*) \quad x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0. \]

Indeed, the five roots of the equation \((*)\) are

\[ x = 2 \cos \left( \frac{2}{11} \pi \right), \; 2 \cos \left( \frac{4}{11} \pi \right), \; 2 \cos \left( \frac{6}{11} \pi \right), \; 2 \cos \left( \frac{8}{11} \pi \right), \; 2 \cos \left( \frac{10}{11} \pi \right). \]

**Fact 2.**

\[ x = 2 \sin \left( \frac{2}{11} \pi \right) \]

satisfies the equation

\[ (***) \quad x^5 - \sqrt{11} x^4 + 3 \sqrt{11} x^2 - 11x + \sqrt{11} = 0. \]

Indeed, the five roots of the equation \((***)\) are

\[ x = 2 \sin \left( \frac{2}{11} \pi \right), \; -2 \sin \left( \frac{4}{11} \pi \right), \; 2 \sin \left( \frac{6}{11} \pi \right), \; 2 \sin \left( \frac{8}{11} \pi \right), \; 2 \sin \left( \frac{10}{11} \pi \right). \]
In Fact 2 above, the negative sign in front of \(2 \sin \frac{4}{11} \pi\) is not a typo. You might say that that destroys symmetry, but the truth is, with that negative sign there is a desirable symmetry. To be precise, if you like, you may write the above five roots of (**) as

\[
x = 2 \sin \left( \frac{1 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{4 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{9 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{16 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{25 \cdot 2 \pi}{11} \right).
\]

(Verify this.) Notice that what’s inside the parentheses are \(\frac{2}{11} \pi\) times \(1^2, 2^2, 3^2, 4^2\) and \(5^2\).

You might ask why we discriminate against

\[
2 \sin \left( \frac{6^2 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{7^2 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{8^2 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{9^2 \cdot 2 \pi}{11} \right), \quad 2 \sin \left( \frac{10^2 \cdot 2 \pi}{11} \right).
\]

A good point, but they are exactly the negatives of the first five, in the reverse order. (Verify this.) Then the next one

\[
2 \sin \left( 11^2 \cdot \frac{2 \pi}{11} \right) = 2 \sin \left( 121 \cdot \frac{2 \pi}{11} \right)
\]

is precisely 0. From that point onwards, the same pattern repeats.

Now, in contrast, in Fact 1 there is no negative sign in front of the five roots of (*). You can probably explain why. The reason is because those are
\[x = 2 \cos \left( 1 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 4 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 9 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 16 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 25 \cdot \frac{2\pi}{11} \right).\]

This time around,
\[2 \cos \left( 36 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 49 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 64 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 81 \cdot \frac{2\pi}{11} \right), \quad 2 \cos \left( 100 \cdot \frac{2\pi}{11} \right),\]

are exactly the first five (as opposed to the negative of the first five), in the reverse order. Now, what’s behind the scene in these examples is the notion of the so-called ‘Gauss sum’. Gauss sum is not exactly the main theme of today’s lecture though I am tempted to delve into it a little. Rather, I throw the following exercises:

**Exercise 1.** Use Fact 1 and Fact 2 to evaluate

1a) \(\cos \frac{2}{11} \pi + \cos \frac{4}{11} \pi + \cos \frac{6}{11} \pi + \cos \frac{8}{11} \pi + \cos \frac{10}{11} \pi.\)

1b) \(\sin \frac{2}{11} \pi - \sin \frac{4}{11} \pi + \sin \frac{6}{11} \pi + \sin \frac{8}{11} \pi + \sin \frac{10}{11} \pi.\)

2a) \(\left( \cos \frac{2\pi}{11} \right) \left( \cos \frac{4\pi}{11} \right) \left( \cos \frac{6\pi}{11} \right) \left( \cos \frac{8\pi}{11} \right) \left( \cos \frac{10\pi}{11} \right).\)

2b) \(\left( \sin \frac{2\pi}{11} \right) \left( \sin \frac{4\pi}{11} \right) \left( \sin \frac{6\pi}{11} \right) \left( \sin \frac{8\pi}{11} \right) \left( \sin \frac{10\pi}{11} \right).\)

**Exercise 2.** Out of (**) in Fact 2, create an algebraic equation of degree 10 with rational number coefficients which has \(2 \sin \frac{2}{11} \pi\) as one of its roots. What are the other nine roots?
In case you are curious, here are some examples of algebraic numbers of the form \( \cos \left( r \pi \right) \) and \( \sin \left( r \pi \right) \) \((r: \text{a rational number})\) that indeed have a finite expression involving integers and addition, subtraction, multiplication, division and radicals (the list is incomplete):

\[
\begin{align*}
\cos \frac{\pi}{3} &= \frac{1}{2}, & \sin \frac{\pi}{3} &= \frac{\sqrt{3}}{2}, \\
\cos \frac{\pi}{4} &= \frac{1}{\sqrt{2}}, & \sin \frac{\pi}{4} &= \frac{1}{\sqrt{2}}, \\
\cos \frac{\pi}{6} &= \frac{\sqrt{3}}{2}, & \sin \frac{\pi}{6} &= \frac{1}{2}, \\
\cos \frac{\pi}{8} &= \frac{\sqrt{2 + \sqrt{2}}}{2}, & \sin \frac{\pi}{8} &= \frac{\sqrt{2 - \sqrt{2}}}{2}, \\
\cos \frac{\pi}{12} &= \frac{\sqrt{2 + \sqrt{3}}}{2}, & \sin \frac{\pi}{12} &= \frac{\sqrt{2 - \sqrt{3}}}{2}, \\
\cos \frac{\pi}{16} &= \frac{\sqrt{2 + \sqrt{2 + \sqrt{2}}}}{2}, & \sin \frac{\pi}{16} &= \frac{\sqrt{2 - \sqrt{2 + \sqrt{2}}}}{2}, \\
\cos \frac{2\pi}{5} &= -\frac{1 + \sqrt{5}}{4}, & \sin \frac{2\pi}{5} &= \frac{\sqrt{10 + 2\sqrt{5}}}{4},
\end{align*}
\]
\[
\cos \frac{2\pi}{7} = \frac{1}{6} \left( -1 + 3\sqrt{\frac{7}{2}} \left( 3\sqrt{1 + 3\sqrt{-3}} + 3\sqrt{1 - 3\sqrt{-3}} \right) \right),
\]

\[
\sin \frac{2\pi}{7} = \frac{1}{6} \left( \sqrt{7} + 6\sqrt{\frac{7}{4}} \left( 3\sqrt{-13 + 3\sqrt{-3}} + 3\sqrt{-13 - 3\sqrt{-3}} \right) \right),
\]

\[
\cos \frac{2\pi}{17} = \frac{-(1 - \sqrt{17} - \sqrt{34 - 2\sqrt{17}}) + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}}{16},
\]

\[
\sin \frac{2\pi}{17} = \frac{\sqrt{136 - 8\sqrt{17} + (6 - 2\sqrt{17})\sqrt{34 - 2\sqrt{17} + 8\sqrt{34 + 2\sqrt{17}}} + 4 \left( 1 - \sqrt{17} - \sqrt{34 - 2\sqrt{17}} \right)\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}}}{16}.
\]

**Remark.** Notice that in the expressions of \( \cos \frac{2\pi}{7} \) and \( \sin \frac{2\pi}{7} \) above, there is some ambiguity. Namely, the cube-roots \( 3\sqrt{-13 + 3\sqrt{-3}}, \ 3\sqrt{1 + 3\sqrt{-3}}, \ etc. \) are not uniquely determined, indeed, each of those cube-roots designates three distinct complex numbers. Thus the above expressions of \( \cos \frac{2\pi}{7} \) and \( \sin \frac{2\pi}{7} \) should be understood as “where the cube-roots in sight are appropriately chosen”. On the other hand, radicals of positive real numbers should always be understood to be real and positive. Thus there is no ambiguity in the above expression of each of \( \cos \theta \) and \( \sin \theta \) with

\[
\theta = \frac{\pi}{3}, \ \frac{\pi}{4}, \ \frac{\pi}{6}, \ \frac{\pi}{8}, \ \frac{\pi}{12}, \ \frac{\pi}{16}, \ \frac{2\pi}{5}, \ \frac{2\pi}{17}.
\]
Here are some related facts which I feel are worthy to highlight:

**Facts.**

(1) The complex conjugate of an algebraic number is algebraic.

(2) The real and the imaginary parts of an algebraic number are both algebraic.

(3) Suppose a complex number has both its real part and its imaginary part algebraic. Then the original complex number is algebraic.

On the other hand, here is another important fact:

**Fact.** Not all complex numbers are algebraic.

**Definition.** A complex number which is not algebraic is called a _transcendental_ number.

So, a paraphrase of the above fact is:

**Fact above paraphrased.**

There are some complex numbers that are transcendental.

Actually, ‘anecdotally’, 99.999..% of complex numbers are transcendental. Algebraic numbers are extremely special. Making it precise requires the notion of ‘cardinality’ which I would rather spare today.

So, you might want to know what complex numbers are transcendental.

**Example.** (1) $e$ is transcendental. (2) $\pi$ is transcendental.

The transcendence of $e$ was proved by Hermite in 1873. The transcendence of $\pi$ was proved by Lindemann in 1882.* These are very non-trivial results.

---

*Charles Hermite (1822-1901); Ferdinand von Lindemann (1852–1939).
Now, do you remember what I said about why I am going over algebraic and transcendental numbers? Yes, I was going to provide one concrete example of a field other than \( \mathbb{C} \) which is algebraically closed. Here is my answer: If you consider the entire set of algebraic numbers, then it turns out it forms a field:

**Notation.** In mathematics, it is common to denote the entire set of algebraic numbers by \( \overline{\mathbb{Q}} \).

Remember, an algebraic number is a complex number of a certain kind, so \( \overline{\mathbb{Q}} \) is a subset of \( \mathbb{C} \) on the one hand. On the other hand, remember also that a rational number is an algebraic number, so \( \overline{\mathbb{Q}} \) is an ‘overset’ of \( \mathbb{Q} \), meaning \( \mathbb{Q} \) is a subset of \( \overline{\mathbb{Q}} \). In short:

\[
\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}.
\]

Now, most importantly, it turns out that \( \overline{\mathbb{Q}} \) is a field. Moreover, it turns out that the field \( \overline{\mathbb{Q}} \) is ‘algebraically closed’. Now you are perhaps more motivated than ever about hearing the definition of a field. Yes, I oblige. However, let me finish ‘Point Number Two’ first.

**Point Number Two.**

In geometry, we deal with matrices. As is well-known, eigenvalues of a matrix with real number entries are not always real. The eigenvalues of matrices are complex numbers. Now, there is something more. Somewhat out of the blue, there is an abstract algebra notion called ‘groups’. In geometry, groups play a pivotal role. I haven’t defined the notion of groups yet. Below is only a ‘sneak-preview’. In the rest of this paragraph you don’t have to know what groups are. All you have to know is a group is basically a multiplicative system. (It has to satisfy a certain set of rules, or ‘axioms’, however.) The definition of groups, called ‘group axioms’ (like field axioms), actually has nothing to do with \( \mathbb{C} \). The group axioms are very ‘abstract’ looking. Contrary to your first impression after having memorized the group axioms, however, you quickly come to learn that \( \mathbb{C} \) plays an indispensable role in group theory. A little more precisely, many (most) examples of groups we encounter are best understood when they are represented as either multiplicative systems of complex numbers, or (multiplicative) groups of _matrices_. Here, the former is clearly a special case of the latter, because a number is a size \( 1 \times 1 \) matrix.
In representative examples, the group structure is best described when represented in a matrix form. So, in principle, groups of matrices are the majority of what we deal with as far as groups are concerned. But, you’d ask: “Is it always feasible to represent an abstract group in a matrix form?”

That’s an excellent question. The answer is actually “yes”, when the group consists of finitely many elements. This is a striking fact, because, once again, the definition of groups has nothing to do with matrices.* On the other hand, the answer to the same question is “not always”, when the group consists of infinitely many elements. Yet many representative, mathematically meaningful, examples of groups carrying infinitely many elements are indeed ones represented in a matrix form. There is one big subdiscipline of mathematics, called Representation Theory. An over-simplified description of Representation Theory is it is about representing groups and other algebraic systems as matrix systems. The ideas and methods in Representation Theory infiltrate into almost all pure mathematics, including geometry. Now, what exactly is the relation between Representation Theory and group theory? That’s another excellent question. Just roughly: First, Representation Theory is not a group theory. Still a big part of representation theory is to represent groups, and Lie groups in particular (naturally another part of it is to represent other related objects such as ‘Lie algebras’). Conversely, if you dig group theory deep, then you are eventually led to the theory of group representations.

Now, when you talk about matrices, it is certainly the case that those matrices have to have entries. As entries of the matrices, mathematicians usually use complex numbers. (Sometimes they stray away from it.) So, in short, in ‘Group Theory’, \( \mathbb{C} \) serves a fundamental role as the basic underlying number system. This is the reason number two why we were investing our time on studying \( \mathbb{C} \): It is due to such a necessity arising from the Group Theory.

- Now, back to what I said earlier: “\( \mathbb{C} \) encapsulates many important mathematical features”. As is common in mathematics, we want to break those down, isolate them, and study what’s common about different mathematical objects sharing those features. But for that you might say I have already done that, as in I have already highlighted those features of \( \mathbb{C} \) in (i) through (vi). But in mathematics, we do it more formally, and abstractly. Right now I am only concerned about the item (ii) on page 1. In mathematics, item (ii) is ‘crystallized’ into the following set of ‘axioms’:

*The fact that a group having finitely many elements is always a group of matrices is called (or is a consequence of) the so-called Cayley’s theorem. Proof is elementary.
• Field axioms for $\mathbb{C}$.

For $\alpha, \beta, \gamma \in \mathbb{C}$, the following hold.

(F1) $\alpha + \beta = \beta + \alpha$, $\alpha \beta = \beta \alpha$,

(F2) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\alpha (\beta \gamma) = (\alpha \beta) \gamma$,

(F3) $(\alpha + \beta) \gamma = \alpha \gamma + \beta \gamma$,

(F4) $0 + \alpha = \alpha$, $1 \cdot \alpha = \alpha$,

(F5) $\alpha + (-\alpha) = 0$, $\alpha \alpha^{-1} = 1$ (the latter assumes $\alpha \neq 0$).

• Let's take a look at it one by one. (F1) is commutativity of addition and of multiplication. Actually, in mathematics, you will never see a single example of an object whose addition does not commute. Meanwhile, I have explained that, we often deal with objects whose multiplication does not commute. A representative example is $\mathbb{H}$, which I briefly touched last time. So, you may say “while I understand the necessity to include $\alpha \beta = \beta \alpha$, as a part of (F1), why do I also need to include $\alpha + \beta = \beta + \alpha$, as another part of (F1)? This makes the subject look silly.” That is a legitimate inquiry. It is kind of hard to answer, because I do not know of a single concrete example where the commutativity of addition is not self-evident. (In contrast, the commutativity of multiplication in $\mathbb{C}$ was not too self-evident.) All right, here is my best shot:

Mathematicians are not masochists. Mathematicians do not do anything as to purposely making themselves look silly, by proclaiming that something as plain looking as

$\alpha + \beta = \beta + \alpha$

is an important part of what they study. Rather, including something like this as a part of the axiom is a reflection of some profound philosophy of modern mathematics, namely, “building everything from the scratch philosophy”.* It works as follows:

*Or, ‘tabula rasa’ (in Latin) philosophy.
1. Include what is true in the ‘axioms’.

2. Do not use how trivial or silly it looks as a basis of your decision as to whether to include something in the ‘axioms’.

3. Anything else that is true and not included in the ‘axioms’ one should be able to deduce from what are already included in the ‘axioms’.

4. Reduce the content of ‘axioms’ to minimal, namely, to the extent there is no redundancy in the set of axioms.

We officially call the philosophy as summarized in 1–4 above as ‘axiomatic mathematics’. The adjective ‘axiomatic’ is actually one key word that distinguishes, and characterizes, the twentieth century mathematics from mathematics in the preceding centuries. The idea is, since

$$\alpha + \beta = \beta + \alpha$$

is true, we can potentially include it as a part of our axiom. And we do indeed decide to include that as a part of our axiom, because without it, we cannot even say that, for example,

$$z^2 + 1 = 0 \quad \text{and} \quad 1 + z^2 = 0$$

are the same equation.

Next, (F2) is associativity of addition and of multiplication. Actually, you are probably not going to see a single example of an object which does not satisfy associativity in either addition or multiplication.* Yet, with the same spirit, we include them as a part of our axioms. It is by virtue of (F2) that writing of each of

$$\alpha + \beta + \gamma \quad \text{and} \quad \alpha \beta \gamma$$

without \(( \cdot )\) makes sense. Most importantly, (F2) does not follow from (F1).

---

*We know \( \mathbb{R} \), \( \mathbb{C} \) and \( \mathbb{H} \). These are 1, 2, and 4, dimensional number system, respectively. Actually, there is yet another number system, called the octonionic number system \( \mathbb{O} \). This is an 8 dimensional number system, wherein the associativity of multiplication fails. Historically, it is the discovery of \( \mathbb{O} \) that the importance of associativity was recognized.
Next, as for (F3). This is distributivity. Without it, we cannot factor
\[ z^2 + z \]
as
\[ (z + 1)z, \]
or factor
\[ z^2 - 1 \]
as
\[ (z + 1)(z - 1). \]
Most importantly, (F3) does not follow from (F1) and (F2).

As for (F4), if you just look at (F4), then this might make little sense. Again, this gives you an impression that I have highlighted something trivial, or silly. But let’s look at (F4) and (F5) together. The combination of (F4) and (F5) has an important implication: ‘Cancellation’.

It is by virtue of (F4) and (F5) that we can simplify
\[ z^2 + 3z + 1 - 3z - 1 \]
as
\[ z^2, \]
or simplify
\[ (z \alpha^{-1}) (\beta z^{-1}) (\alpha^{-1}) = \frac{z}{\alpha} \cdot \frac{\beta}{z} \cdot \frac{\alpha}{\beta} \]
as
1.
Now, most importantly, neither of (F4) nor (F5) follows from (F1), (F2), (F3).
So, how do you feel? Do you see why I am isolating (F1) through (F5) from the complex number arithmetic? No? Okay. I know that today’s job is not easy. I am half-way there, to convince you that isolating (F1) through (F5) is meaningful. Let me try a slightly different approach. I would like you to agree with the following:

Claim. (F1) through (F5) are not peculiar to \( \mathbb{C} \). Indeed, (F1) through (F5) are all true, for each of \( \mathbb{R} \), and \( \mathbb{Q} \).

Agreed? Good. If you want to ask about \( \mathbb{Q} \), don’t worry. I will deal with it later. So, there are different number systems that share some common features, namely, (F1) through (F5) above, and the complex number system \( \mathbb{C} \) is one of them. In mathematics, we attach a general name with any number system that satisfies (F1) through (F5) above. That is, a ‘field’.

So, below is the official definition of a field (finally!):

- **Definition.** A **field** is a set \( F \), carrying two distinguishable elements 0 (called the zero element) and 1 (called the multiplicative identity element), where \( 0 \neq 1 \), and within which additive and multiplicative structures are defined, such that

  (F1) \( \alpha + \beta = \beta + \alpha \), \( \alpha \beta = \beta \alpha \),

  (F2) \( \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \), \( \alpha (\beta \gamma) = (\alpha \beta) \gamma \),

  (F3) \( (\alpha + \beta) \gamma = \alpha \gamma + \beta \gamma \),

  (F4) \( 0 + \alpha = \alpha \), \( 1 \cdot \alpha = \alpha \),

  (F5) For each \( \alpha \in F \), there exists \(-\alpha \in F\) such that \( \alpha + (-\alpha) = 0 \),

  and also, for each \( \alpha \in F \), with \( \alpha \neq 0 \), there exists \( \alpha^{-1} \in F \), such that \( \alpha \alpha^{-1} = 1 \).
Examples (of fields). \( \mathbb{C}, \mathbb{R}, \text{ and } \mathbb{Q} \) are all fields.

- On the other hand, the quaternionic number system \( \mathbb{H} \) is **not** an example of a field. In fact, \( \mathbb{H} \) has a non-commutative multiplicative structure. \( \mathbb{H} \) is an example of a so-called 'skew-field', or a 'division ring', which I might officially define later, but basically what it is is it is an object that satisfies all the field axioms (F1) through (F5) except the commutativity of multiplications.

Now, if you have a good memory, you remember what I said earlier about the set \( \mathbb{Q} \) of algebraic numbers.

Another Example (of a field). \( \overline{\mathbb{Q}} \) is a field.

Now, you might say that that is trivial, because (F1) through (F5) are true for complex numbers, and hence (F1) through (F5) are true for algebraic numbers. Indeed, algebraic numbers are a special kind of complex numbers. Good point. However, that logic is less than perfect. You are only half right’. What is important to remember here is this:

> "The definition of a field above requires that all of the identities in (F1) through (F5) have to be inside the same set \( F \)."

In this case, \( F = \overline{\mathbb{Q}} \). So, even though (F1) through (F5) are true for algebraic numbers \( \alpha, \beta \text{ and } \gamma \), it remains to be seen whether \( \alpha + \beta, \alpha \beta \text{ and } \alpha^{-1} \) are algebraic numbers provided \( \alpha \text{ and } \beta \) are algebraic numbers. Is that true? The answer is, “yes, that is indeed true”. I have already addressed this question in page 7 item (a) and item (b). So, the answer is affirmative. So, you can safely conclude that \( F = \overline{\mathbb{Q}} \) is indeed a field. Strictly speaking, you had to make the same observation for \( \mathbb{Q} \) when you agreed earlier that \( \mathbb{Q} \) is a field. However, in case of \( \mathbb{Q} \) it goes without saying that adding, multiplying and reciprocating two rational numbers are rational.

Once again, bear in mind that, by definition, a field has a **commutative** multiplicative structure. It is extremely important to take note of this.
Renaming our familiar number systems.

In view of the aforementioned, we hereby rename our familiar number systems, as follows:

1. We hereby rename $\mathbb{C}$ as the complex number field.
2. We hereby rename $\mathbb{R}$ as the real number field.
3. We hereby rename $\mathbb{Q}$ as the rational number field.
4. We hereby name $\overline{\mathbb{Q}}$ as the field of all algebraic numbers.

As for (4), we don’t call $\overline{\mathbb{Q}}$ as ‘the algebraic number field’. I need to clarify this so as to avoid any potential confusion. Below we will define one important concept associated with the notion of fields, called ‘subfields’. In mathematics, an algebraic number field refers to any subfield of $\overline{\mathbb{Q}}$. Also, actually there is another name for $\overline{\mathbb{Q}}$. That is, ‘the algebraic closure of $\mathbb{Q}$’. You don’t have to worry about the meaning of ‘algebraic closure’ yet.

- **Subfields.**

  In the above I have alerted you that, even though $\overline{\mathbb{Q}}$ is a subset of $\mathbb{C}$, it is not entirely obvious as to why it is a field. The reason why $\overline{\mathbb{Q}}$ is a field is because adding or multiplying two algebraic numbers yields another algebraic number, and reciprocating an algebraic number yields another algebraic number. In short, $\overline{\mathbb{Q}}$ is closed under addition, multiplication and reciprocation. These are rather non-trivial facts.* Also, 1 clearly belongs to $\overline{\mathbb{Q}}$. In other words, $K = \overline{\mathbb{Q}}$ satisfies the following (SF1) through (SF4):

  (SF1) $\alpha + \beta \in K$ whenever $\alpha \in K$ and $\beta \in K$.
  (SF2) $\alpha \beta \in K$ whenever $\alpha \in K$ and $\beta \in K$.
  (SF3) $-\alpha, \alpha^{-1} \in K$ whenever $\alpha \in K$ and $\alpha \neq 0$.
  (SF4) $1 \in K$.

---

*Proof of the algebraicity of the reciprocal of an algebraic number is not so hard.
• More generally, we make the following definition:

**Definition (subfields).**

Let $F$ be a field. Let $K$ be a subset of $F$:

$$F \supseteq K.$$  

$K$ is said to be a subfield of $F$, if it satisfies

(SF1) $\alpha + \beta \in K$ whenever $\alpha \in K$ and $\beta \in K$,

(SF2) $\alpha \beta \in K$ whenever $\alpha \in K$ and $\beta \in K$,

(SF3) $-\alpha, \alpha^{-1} \in K$ whenever $\alpha \in K$ and $\alpha \neq 0$.

(SF4) $1 \in K$.

• If $F$ is a field and $K$ is a subfield, then $K$ itself forms a field, with respect to the addition and multiplication inherited from $F$. The fact that $\mathbb{Q}$ is a field, as I stated several times earlier, is by virtue of the fact that (SF1) through (SF4) hold for $K = \mathbb{Q}$.

• Below are facts that are easy to verify:

**Fact.**  
(a) Let $F$ be a field. Let $K_1$ and $K_2$ be both subfields of $F$. Then the intersection $K_1 \cap K_2$ is a subfield of $F$.

(b) Let $F$ be a field. Let $K_1$ and $K_2$ be both subfields of $F$. Suppose $K_1 \supseteq K_2$. Then $K_2$ is a subfield of $K_1$.

(c) Let $F$ be a field. Let $K_1$ be a subfield of $F$. Let $K_2$ be a subfield of $K_1$. Then $K_2$ is a subfield of $F$.  

24
So, agree:

(1) \( \mathbb{R} \) is a subfield of \( \mathbb{C} \).
(2) \( \mathbb{Q} \) is a subfield of \( \mathbb{R} \).
(3) \( \mathbb{Q} \) is a subfield of \( \mathbb{C} \).
(4) \( \overline{\mathbb{R}} \) is a subfield of \( \mathbb{C} \).
(5) \( \mathbb{Q} \) is a subfield of \( \overline{\mathbb{Q}} \).

By virtue of Fact (a) above, it makes sense to consider the subfield arisen by taking the intersection of \( \mathbb{R} \) and \( \overline{\mathbb{Q}} \). We denote it \( \overline{\mathbb{Q}}_R \):

\[
\overline{\mathbb{Q}}_R = \mathbb{R} \cap \overline{\mathbb{Q}}.
\]

So, \( \overline{\mathbb{Q}}_R \) is the entire set of algebraic numbers which are real. So, agree:

(6) \( \overline{\mathbb{Q}}_R \) is a subfield of \( \mathbb{C} \).
(7) \( \overline{\mathbb{Q}}_R \) is a subfield of \( \mathbb{R} \).
(7) \( \overline{\mathbb{Q}}_R \) is a subfield of \( \overline{\mathbb{Q}} \).
(8) \( \mathbb{Q} \) is a subfield of \( \overline{\mathbb{Q}}_R \).

• That’s pretty much all for today’s lecture. In the next lecture we will get to the ‘Fundamental Theorem of Algebra’. To wrap up today’s lecture, though, let me note a couple of things. One is about algebraic equations. The other is about the rational number field \( \mathbb{Q} \). First, about algebraic equations, we have seen examples through which we learned

(i) When the equation looks simple, it does not mean the expression of its roots is simple. Sometimes there is no way to express its roots (only using radicals).

(ii) When the description of a number looks simple, it does not mean it is easy to concoct an algebraic equation with coefficients in \( \mathbb{Q} \) that has that number as one of its roots.

(iii) Sometimes, in solving an algebraic equation, trigonometric arguments unavoidably comes into the picture.

I want to specifically give you another example that demonstrates (ii):
**Example.** The number \( x = \sqrt[3]{2} + \sqrt[3]{3} \) satisfies

\[
(*) \quad x^{12} - 8x^9 - 9x^8 + 24x^6 - 288x^5 + 27x^4 - 32x^3 - 360x^2 - 216x - 11 = 0.
\]

This is indeed the lowest degree equation with rational number coefficients the same number \( x = \sqrt[3]{2} + \sqrt[3]{3} \) satisfies.

The morale of this example is that you are adding up two ‘simple looking’ numbers \( \sqrt[3]{2} \) and \( \sqrt[3]{3} \). Those are roots of \( x^3 = 2 \) and \( x^3 = 3 \), respectively. However, once you add up those two numbers, all of a sudden the equation satisfied by the outcome of the addition is as complicated as \((*)\). Now, you may correctly point out that the appearance of \((*)\) does not quite reflect \( \sqrt[3]{2} \) or \( \sqrt[3]{3} \). Great observation. As for this, there is actually more to it: Consider

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
43-x^{12} & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
11 & 27 & 43-x^{12} & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
10 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
9 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
8 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
7 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
6 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
5 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
4 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
3 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
2 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
1 & 27 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 & 12 & 16 \\
\hline
\end{array}
\]
This is a $12 \times 12$ determinant. As you can see, three numbers 16, 27 and 43 are its major ingredients. Now, 16, 27 and 43 are obvious reflections of the number

$$3\sqrt{2} + 4\sqrt{3}$$

in question, indeed,

$$3\sqrt{2} + 4\sqrt{3} = 16^{12} + 27^{12},$$

and also $43 = 16 + 27$.

Now, we know we cannot do the above $12 \times 12$ determinants by hand. The bad news is, neither does my computer software. That is not too surprising, indeed, the expansion of a general $12 \times 12$ determinant involves

$$12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 479001600$$

(half a billion ball-park) terms. Nevertheless, there is a way to calculate the above determinant, still relying on the same computer software. Here is precisely how much the above $12 \times 12$ determinant equals:

$$x^{144} = 516 \ x^{132}$$
$$- 7009045134 \ x^{120}$$
$$- 89387946830740 \ x^{108}$$
$$+ 6467880810206639295 \ x^{96}$$
$$- 45828071888701856784264 \ x^{84}$$
$$- 148342466388805364243111556 \ x^{72}$$
$$- 106520452078213618082771534280 \ x^{60}$$
$$+ 4173688609631665803565889736591 \ x^{48}$$
$$- 49538384033398370980853700284788 \ x^{36}$$
$$- 446886364025220364388525353422 \ x^{24}$$
$$- 3193302693380403375314327460 \ x^{12}$$
$$+ 3138428376721 .$$

27
If you say this last polynomial only involves 13 terms, not half a billion, then you are absolutely right. But it was originally half a billion. After combining terms with \( x \) raised to the same exponent it shrunk like this. Agree that this is a polynomial of degree 144. (Worthy to mention: The constant term \( 3138428376721 \) equals \( 11^{12} \), and \( 11 = 27 - 16 \).) Now, here is an interesting part: This last polynomial is factorizable. It factors into two of degree 12 polynomials and five of degree 24 polynomials. One of the two degree 12 factors is indeed

\[
x^{12} - 8x^9 - 9x^8 + 24x^6 - 288x^5 + 27x^4 - 32x^3 - 360x^2 - 216x - 11,
\]

which is precisely the left-hand side of \((\ast)\). Finally, in the above polynomial of degree 144, substitute \( x^{12} \) (a part of each of the twelve main diagonal entries) with \( y \), and equate it with 0:

\[
y^{12} - 516 y^{11} - 7009045134 y^{10} - 89387946830740 y^9 + 6467880810206639295 y^8 - 45828071888701856784264 y^7 - 148342466388805364243111556 y^6 - 106520452078213618082771534280 y^5 + 4173688609631665803565889736591 y^4 - 49538384033398370980853700284788 y^3 - 446886364025220364388525353422 y^2 - 3193302693380403375314327460 y + 3138428376721 = 0.
\]

This equation is indeed the lowest degree equation having coefficients in \( \mathbb{Q} \) which satisfies. It may be a surprise to you that, the coefficients of this last equation are ‘big’, despite the fact neither of \( 3\sqrt{2} \), \( 4\sqrt{3} \), nor their sum is ‘big’. (Also, the decimal expression of \( (3\sqrt{2} + 4\sqrt{3})^{12} \) is \( 85376.8\ldots \).)
• Are questions about $\mathbb{Q}$ all trivial?

Earlier today I covered the definition of $\mathbb{Q}$ and asked you a favor not to underestimate the level of difficulty. Some of you might assume that, in mathematics, $\mathbb{Q}$ is a more primitive object than $\mathbb{R}$, thus problems over $\mathbb{R}$ are generally more difficult than the same problem over $\mathbb{Q}$. The truth is, “not always”. In mathematics, there are very many instances that a non-trivial theorem over $\mathbb{Q}$ has an equivalent counterpart statement over $\mathbb{R}$ which is trivial. A famous example:

Fermat’s Last Theorem (Wiles, Wiles-Taylor 1995).

Let $n$ be an arbitrary integer, $n \geq 3$, fixed. Consider

$$x^n + y^n = 1,$$

regarded as an equation with $x$ and $y$ unknowns. The only roots of this equation in $\mathbb{Q}$ are

$$\left( x, y \right) = \left( 1, 0 \right),$$

$$\left( 0, 1 \right),$$

$$\left( -1, 0 \right) \text{ (only when } n \text{ is even}),$$

$$\left( 0, -1 \right) \text{ (only when } n \text{ is even}).$$

This statement was claimed by Fermat* in the 17th century as true. However, Fermat did not write up a proof. Mathematicians in post Fermat era wondered if Fermat really proved this. Countless number of attempts by mathematicians had been made, all in vain. That is, until 1995. A complete solution to this problem was given in 1995 by Wiles, partially collaborated by Taylor.** Their proof uses the so-called Iwasawa theory, and by way of settling a special case of one central conjecture in number theory, called ‘Taniyama–Shimura conjecture’.*** These are extremely elaborate and difficult mathematics. Mathematicians today believe that Fermat thought he had a proof, but Fermat actually did not prove it.

---

*Pierre de Fermat (1601(?)–1665).

**Andrew Wiles (1953–), professor at Princeton University. Richard Taylor (1962–), professor at Harvard University.

***Yutaka Taniyama (1927–1958), once a faculty at University of Tokyo. Goro Shimura (1930–), professor emeritus at Princeton University.
• If you are a math-major, you really should know the name ‘Fermat’s Last Theorem’, its statement, and the fact that two mathematicians named Andrew Wiles and Richard Taylor proved it in the 1990s. This is probably the most ‘talked-about’ theorem from the recent development of cutting-edge mathematics (along with the solution to the Poincaré conjecture by Grigory Perelman).

Fermat’s Last Theorem falls into one major mathematics discipline called ‘number theory’, and it falls more specifically into “rational points on algebraic curves”. The statement of Fermat’s Last Theorem can be paraphrased as

“The Fermat curve of degree $n \geq 3$ has no non-trivial rational points.”

Here, the Fermat curve of degree $n$ means precisely

$$C_n = \left\{ \left( x, y \right) \in \mathbb{A}^2 \mid x^n + y^n - 1 = 0 \right\},$$

where $\mathbb{A}^2$ denotes the usual affine plane. In the above definition of $C_n$, $x$ and $y$ take values in either $\mathbb{R}$ or $\mathbb{C}$. Also, a rational point is a point in the $xy$-coordinate plane whose both $x$-coordinate reading and $y$-coordinate reading are in $\mathbb{Q}$. There is a subdiscipline of number theory called “Rational points on algebraic curves”. Fermat’s Last Theorem belongs there. This is an extremely challenging branch of number theory. Fermat’s Last Theorem states that $C_n$ has no rational points other than the obvious ones, namely, the $x$- and the $y$-intercepts of $C_n$. Now, to make a contrast, let’s consider

$$D_n = \left\{ \left( x, y \right) \in \mathbb{A}^2 \left| \begin{array}{cccc}
\begin{array}{ccc}
(n-1) x & n x & \cdots & n \frac{n-1}{n} x \\
(n-2) y & (n-1) y & \cdots \end{array} \\
\begin{array}{ccc}
\vdots & \vdots & \\
1 y & 2 y & \cdots \\
\end{array} \\
\begin{array}{ccc}
x+y-1 & y & \cdots \end{array} \\
\end{array} \right| = 0 \right\}.$$
In fact, this latter curve $D_n$ is a ‘cousin’ of the Fermat curve $C_n$, as in there are some similarities, though there are also differences.

First, differences: Unlike the Fermat curve $C_n$ of degree $n \geq 3$, this curve $D_n$ has “dense” rational points, no matter how much $n$ is (provided $n$ is a positive integer). Indeed, $D_n$ has a parametrization

$$x = \left( \cos \theta \right)^{2n}, \quad y = \left( \sin \theta \right)^{2n}.$$ 

In particular, $D_n$ is classified as a so-called rational curve. On the contrary, the Fermat curves of degree $n \geq 3$ are irrational curves. Obviously, the example on page 26 is essentially the substitutions of $x$ with 16 and $y$ with 27 into the homogenization of the defining equation of $D_n$.

About some similarities between $C_n$ and $D_n$: $x^n + y^n$ factors as

$$\prod_{\ell=0}^{n-1} \left( x + e^{-\frac{2\ell \pi}{n}} y \right)$$

$$= \left( x + y \right) \left( x + e^{-\frac{2\pi}{n} y} \right) \left( x + e^{-\frac{4\pi}{n} y} \right) \left( x + e^{-\frac{6\pi}{n} y} \right) \cdots \left( x + e^{-\frac{(n-1)2\pi}{n} y} \right).$$

Meanwhile, the left-hand side of the defining equation of the curve $D_n$ (the determinant) factors as

$$\prod_{\ell=0}^{n-1} \prod_{m=0}^{n-1} \left( e^{-\frac{2\ell \pi}{n}} x^\frac{1}{n} + e^{-\frac{2m \pi}{n}} y^\frac{1}{n} - 1 \right).$$

You realize that one of the factors in the factorization is $x^\frac{1}{n} + y^\frac{1}{n} - 1$. This resembles the left-hand side of the defining equation of the Fermat curve $C_n$. 

31
In the mid nineteenth century (1850c.) Kummer\textsuperscript{1} tried to use the above factorization for $x^n + y^n$ in trying to prove Fermat’s Last Theorem, and partially succeeded, namely, he has proved it for the case $n$ is a so-called ‘regular’ prime.\textsuperscript{2} He did not succeed in it for the general case. However, most importantly, through his failed attempt a new notion called ‘ideal numbers’ grew out, which was later refined by Kronecker and Dedekind.\textsuperscript{3} This ingenious concept subsequently became indispensable to both number theory and algebraic geometry.

So, in any case, please do not prematurely judge that, in mathematics, problems over $\mathbb{Q}$ are generally easy. Once again, Fermat’s Last Theorem belongs to a branch of mathematics called ‘number theory’. The stature of Fermat’s Last Theorem is exceptional for one single theorem. People’s cravings to solve Fermat’s Last Theorem were the major impetus for the development of number theory over centuries. Even putting Fermat’s Last Theorem aside, it is commonly understood that the kind of problems over $\mathbb{Q}$ which number theorists work on are very difficult. Anecdotally, mathematicians working in many different areas see number theory as a hard-core discipline (save that any mathematics discipline is tough). I never seem to meet mathematicians unsympathetic to the quote of Gauss: “number theory is the Queen of mathematics”. Is number theory overrated? Probably not.\textsuperscript{4} What I know is it is true that some number theory branches are really difficult, and some are relatively ‘accessible’. I want to let you have a glimpse of this ‘relatively accessible’ part of number theory before the semester ends, but only if the time permits.

\textsuperscript{1}Ernst Kummer (1810–1893), a German mathematician.

\textsuperscript{2}An integer $p$ with $p \geq 2$ is called a prime number if $p$ cannot be written as $ab$, using two integers $a$ and $b$ with $a, b \geq 2$. It is an elementary fact that there are infinitely many prime numbers (known to Euclid). A prime number $p$ is called ‘regular’ when $p$ does not divide the numerator of $B_k$, for all integers $k$ with $2 \leq k \leq p-3$. It is conjectured that there are infinitely many regular primes, and so far this is open. I want to address Bernoulli numbers at some point in the semester.

\textsuperscript{3}Leopold Kronecker (1823–1891); Richard Dedekind (1831–1916). Both German mathematicians.

\textsuperscript{4}Number theory and algebraic geometry substantially and meaningfully overlap, and that overlapped part is called ‘arithmetic algebraic geometry’, which includes ‘rational points’. My research partner, and esteemed colleague, Professor Pavlos Tzermias, is a number theorist, and one of his specialties is arithmetic algebraic geometry.