1/30/15

HW 1 due NOW.

Today: HW 1 Discussion.

Let $\mathbb{F}$ be a field (for example: $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$), and consider the ring of polynomials in one variable:

$$\mathbb{F}[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots : a_i \in \mathbb{F} \text{ and } a_i = 0 \text{ for all but finitely many } i \}$$

Q: When are two polynomials equal?

$$\sum_{k \geq 0} a_k x^k \overset{?}{=} \sum_{k \geq 0} b_k x^k$$

A: If and only if $a_k = b_k$ for all $k \geq 0$ (they have the same coefficients).

We can take this as a <u>definition</u>, or we can prove it by means of the derivative:

$$\left(\sum_{k \geq 0} a_k \cdot x^k \right)' = \sum_{k \geq 1} a_k \cdot k x^{k-1}.$$

Given $f(x) = \sum a_k x^k \in \mathbb{F}[x]$, we can think of $f(x)$ as a function

$$\begin{aligned} f : \mathbb{F} &\to \mathbb{F} \\ \alpha &\mapsto f(\alpha) \end{aligned}$$

by "evaluation". Given $g(x) = \sum b_k x^k$, we will say that $f(x) = g(x)$ if f and g are <u>equal as functions</u>, that is, if

$$f(\alpha) = g(\alpha) \text{ for all } \alpha \in \mathbb{F}.$$

Clearly if $a_k = b_k \ \forall k$ then $f(x) = g(x)$.

On the other hand, suppose that we have $f(\alpha) = g(\alpha) \ \forall \alpha \in \mathbb{F}$. Does it follow that $a_k = b_k \ \forall k$?

First note that

$$a_0 = f(0) = g(0) = b_0.$$

How can we show that $a_1 = b_1$? Well, if $f(\alpha) = g(\alpha) \ \forall \alpha$ then we <u>should</u> also have $f'(\alpha) = g'(\alpha) \ \forall \alpha$.

Letting $\alpha = 0$ gives

$$\cancel{1} a_1 = f'(0) = g'(0) = \cancel{1} \cdot b_1$$

Continuing, we get

$$\cancel{2} \cdot a_2 = f''(0) = g''(0) = \cancel{2} \cdot b_2 .$$
$$\cancel{3} \cdot a_3 = f'''(0) = g'''(0) = \cancel{3} \cdot b_3$$

etc.

This proof only really works over $\mathbb{R}$ (and $\mathbb{C}$), but this is the idea that motivates the general definition. ///

It may happen over <u>certain</u> <u>fields</u> that different polynomials ($f(x) \neq g(x)$) yield the same function ($f(\alpha) = g(\alpha)\ \forall \alpha$).

Example: Consider the very smallest field $\mathbb{F}_2 := \{0, 1\}$, with operations

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

.

The polynomials $f(x) = x + 1$ and $g(x) = x^2 + 1$ are *not* equal; however, we do have

$$f(0) = 0 + 1 = 1$$
$$g(0) = 0^2 + 1 = 1$$

$$f(1) = 1 + 1 = 0$$
$$g(1) = 1^2 + 1 = 0.$$

So $f(\alpha) = g(\alpha) \quad \forall\ \alpha \in \mathbb{F}_2$. ///

In practice we will write $f(x) = g(x)$ *only* when they have the same coefficients.

Q: To what extent is a polynomial determined by its roots?

A: Consider $f(x), g(x) \in \mathbb{F}[x]$ with $\deg(f) = \deg(g) = 2$.

Suppose $f(x)$ and $g(x)$ have the *same* roots $r \neq s \in \mathbb{F}$.

↓

Then by Descartes' Factor Theorem we have

$$f(x) = (x-r)\, f_r(x)$$
$$g(x) = (x-r)\, g_r(x)$$

where $\deg(f_r) = \deg(g_r) = 1$.

We also know that

$$f(s) = (s-r)\, f_r(s) = 0$$
$$g(s) = (s-r)\, g_r(s) = 0$$

Since $s \neq r$ $(s-r \neq 0)$ this implies that

$$f_r(s) = g_r(s) = 0 .$$

Does this mean that $f_r(x) = g_r(x)$ as polynomials? Not quite!

Suppose $f_r(x) = ax + b \quad (a \neq 0)$
$g_r(x) = cx + d \quad (c \neq 0)$.

Then $f_r(s) = as + b = 0$
$$a\left(s + \frac{b}{s}\right) = 0$$

Implies that $s + \frac{b}{a} = 0 \implies s = -\frac{b}{a}$

We conclude that $f_r(x) = a(x-s)$, and hence

$$f(x) = a\ (x-r)(x-s).$$

Similarly we have

$$g(x) = c\ (x-r)(x-s).$$

So $f(x)$ and $g(x)$ are not necessarily equal, but they are equal up to a constant multiple.

For this reason we make a definition:

Consider $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$. If $a_n \neq 0$ we call it the leading coefficient.

Summary: If $f(x) \in \mathbb{F}[x]$ has degree 2 and two distinct roots $r, s \in \mathbb{F}$, then

$$f(x) = k\ (x-r)(x-s)$$

where k is the leading coefficient.

More generally, we have

☆ Theorem: Suppose $f(x) \in \mathbb{F}[x]$ has degree n and n distinct roots $r_1, r_2, r_3, \ldots, r_n \in \mathbb{F}$. Then

$$f(x) = k(x-r_1)(x-r_2)\cdots(x-r_n)$$

where k is the leading coefficient.

Proof: Induction. ///

What do we learn from this?

- If $\deg(f) = n$ then $f(x)$ can have no more than n distinct roots.

[Why not?]

- What if $\deg(f) = n$ and $f(x)$ has fewer than n distinct roots?

There are 2 ways this can happen.

↓

(1) Maybe some roots are repeated, e.g.,

$$f(x) = (x-1)(x-1)(x-2).$$

(2) Maybe $f(x)$ has an irreducible factor of degree ≥ 2.

For example, consider the polynomial $x^3 - 1 \in \mathbb{R}[x]$. It can be factored

$$x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}_{\text{irreducible over } \mathbb{R}}$$

But now x^2+x+1 cannot be factored in the ring $\mathbb{R}[x]$. We say it is irreducible over $\mathbb{R}$.

Oh Well.

[Maybe x^2+x+1 can be factored over some bigger field containg $\mathbb{R}$?]

2/2/15

HW 2 TBA, will be due Fri Feb 13.

Exam Schedule:

- Exam 1 Wed Feb 18
- Exam 2 Wed Mar 25
- Exam 3 Fri April 24.

Today we will finally solve the general cubic equation:

$$ax^3 + bx^2 + cx + d = 0. \quad ///$$

Last time we found that equation $x^3 - x + 2 = 0$ has solution

$$x \approx -1.521379707\ldots$$

accurate to ten decimal places. But we would prefer an exact algebraic expression for this number.

To do this we will need some <u>trick</u>, analogous to completing the square. This trick was unknown in the ancient world; it was discovered in the early 1500s in Italy.

☆ Trick: If $x = u+v$ then we have

$$x^3 - 3uv\,x - (u^3+v^3) = 0.$$

Proof: You will verify this later. ///

This may look random but it is exactly what we need to solve the cubic.

Let's start by trying to solve the "depressed cubic"

① $$x^3 + px + q = 0.$$

Now let's complicate things by writing $x = u+v$. The trick says that

② $$x^3 - 3uv\,x - (u^3+v^3) = 0.$$

If equations ① and ② are both true then we must have

$$\begin{cases} p = -3uv \\ q = -(u^3+v^3) \end{cases}$$

↓

We will be done if we can invert this system, to solve for u & v in terms of p & q. Then the solution for x will be

$$x = u(p,q) + v(p,q).$$

<u>Can</u> we do this?

Rewrite the system as

$$\begin{cases} -p^3/27 = u^3 \cdot v^3 \\ -q = u^3 + v^3 . \end{cases}$$

If we know the sum and product of two numbers, then we can find the original numbers using the quadratic formula.

The numbers u^3 & v^3 are the solutions of the quadratic equation

$$(z - u^3)(z - v^3) = 0$$
$$z^2 - (u^3 + v^3)z + u^3 v^3 = 0$$
$$z + qz - p^3/27 = 0.$$

We conclude that

$$u^3, v^3 = \frac{-q \pm \sqrt{q^2 + 4p^3/27}}{2}$$

Finally, the solution of the original equation $x^3 + px + q = 0$ is

$$x = u + v$$

$$x = \sqrt[3]{\frac{-q + \sqrt{q^2 + 4p^3/27}}{2}} + \sqrt[3]{\frac{-q - \sqrt{q^2 + 4p^3/27}}{2}}$$

It simplifies slightly:

$$\boxed{x = \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\left(\frac{q}{2}\right) - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}}$$

"Cardano's Formula".

The Story:

- 1494 Luca Pacioli believes that the cubic equation is "impossible" in the current state of mathematics.
- Scipione del Ferro (Bologna, died 1526) discovers a solution for the depressed cubic. Keeps it secret. Passed the information to student Antonio Fior on his deathbed.
- Fior is less prudent than del Ferro. In 1535 he issues a challenge to Niccolo Tartaglia, sending him 30 depressed cubics to solve.
- Tartaglia works frantically and discovers the solution on Feb 13, 1535. He humiliates Fior.
- Tartaglia divulges the secret to Gerolamo Cardano under oath (1539).
- Cardano extends the solution to all cubic equations and decides to publish his results in "Ars Magna" (The Great Art) 1545.
- Tartaglia is furious.

From the depressed cubic to the general cubic equation:

$$ax^3 + bx^2 + cx + d = 0.$$

Since $a \neq 0$ we may divide by a to get

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0.$$

Our goal is to remove the x^2 term by a change of variables $x = y + \alpha$ for some number α.

Substitute $x = y + \alpha$ to get

$$(y+\alpha)^3 + \frac{b}{a}(y+\alpha)^2 + \frac{c}{a}(y+\alpha) + \frac{d}{a} = 0$$

$$y^3 + 3y^2\alpha + 3y\alpha^2 + \alpha^3 + \frac{b}{a}(y^2 + 2y\alpha + \alpha^2) + \frac{c}{a}(y+\alpha) + \frac{d}{a} = 0$$

$$y^3 + y^2\left(3\alpha + \frac{b}{a}\right) + y\left(3\alpha^2 + \frac{2b}{a}\alpha + \frac{c}{a}\right)$$

$$+ \left(\alpha^3 + \frac{b}{a}\alpha^2 + \frac{c}{a}\alpha + \frac{d}{a}\right) = 0.$$

Take $\alpha = -\frac{1}{3}\frac{b}{a}$ to obtain

$\downarrow$

$$y^3 + 0y^2 + py + q = 0,$$ where

$$p = 3\alpha^2 + \frac{2b\alpha}{a} + \frac{c}{a}$$

$$= \frac{1}{3}\frac{b^2}{a^2} - \frac{2}{3}\frac{b^2}{a^2} + \frac{c}{a}$$

$$= -\frac{1}{3}\frac{b^2}{a^2} + \frac{c}{a},$$

$$q = \alpha^3 + \frac{b}{a}\alpha^2 + \frac{c}{a}\alpha + \frac{d}{a}$$

$$= -\frac{1}{27}\frac{b^3}{a^3} + \frac{1}{3}\frac{b^3}{a^3} - \frac{1}{3}\frac{bc}{a^2} + \frac{d}{a}.$$

Now use Cardono's Formula to solve for y. The solution for x is

$$x = y + \alpha$$

$$= \frac{-b}{3a} + \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{q}{2}\right) + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\left(\frac{q}{2}\right) - \sqrt{\left(\frac{q}{2}\right) + \left(\frac{p}{3}\right)^3}}$$

with p & q as above.

Is it worth simplifying this?

2/4/15

HW 2 will be posted today,
and due on Fri Feb 13.

Exam 1 is Web Feb 18 in class.

Last time we discussed Cardano's solution of the cubic equation, as recorded in the "Ars Magna" (The Great Art), 1545.

He showed that the depressed cubic

$$x^3 + px + q = 0$$

has solution

$$x = \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\left(\frac{q}{2}\right) - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

The general cubic

$$ax^3 + bx^2 + cx + d = 0$$

can be solved by dividing by a and then substituting $x = y - b/3a$

$$\downarrow$$

to obtain a depressed cubic in y,

$$y^3 + py + q = 0,$$

where $$p = \frac{1}{3a^2}(3ac - b^2)$$

$$q = \frac{1}{27a^3}(27a^2d - 9abc + 2b^3).$$

The full solution for x is too long to write down, so I typed it

[See the Handout.]

Today we will examine the cubic formula to see if it makes sense.

Recall the equation

$$x^3 - x + 2 = 0.$$

By the intermediate value theorem we know this has a real root,

↓

and we used Newton's method to approximate the root:

$$x \approx -1.521379707$$

Now we can use Cardano's formula to obtain an exact algebraic expression. Putting $p=-1$ and $q=2$ gives

$$x = \sqrt[3]{-1+\sqrt{(-1)^2+\left(\frac{-1}{3}\right)^3}} + \sqrt[3]{-1 \quad \sqrt{(-1)^2+\left(\frac{-1}{3}\right)^3}}$$

$$x = \sqrt[3]{-1+\sqrt{26/27}} + \sqrt[3]{-1-\sqrt{26/27}}$$

Since $\sqrt[3]{-\alpha} = -\sqrt[3]{\alpha}$ for all α we have

$$x = -\sqrt[3]{1-\sqrt{26/27}} - \sqrt[3]{1+\sqrt{26/27}}\,.$$

[Use your calculator to check that this agrees with $x \approx -1.5213\cdots$]

This is why I knew you would never guess the solution !

Let's try an easier example.

Example: Solve $x^3 - 1 = 0$ for x.

This is a depressed cubic with $p = 0$ and $q = -1$. Cardano's formula gives

$$x = \sqrt[3]{\frac{1}{2} + \sqrt{\frac{1}{4}}} + \sqrt[3]{\frac{1}{2} - \sqrt{\frac{1}{4}}}$$

$$= \sqrt[3]{\frac{1}{2} + \frac{1}{2}} + \sqrt[3]{\frac{1}{2} - \frac{1}{2}}$$

$$= \sqrt[3]{1} + \sqrt[3]{0} = 1.$$

Good. The formula found the easy solution. Now here's a harder one from the "Ars Magna".

↓

Example: $x^3 + 6x - 20 = 0$.

By inspection we see that $x = 2$ is a solution. Cardano's formula with $p = 6$ and $q = -20$ gives

$$x = \sqrt[3]{10 + \sqrt{100+8}} + \sqrt[3]{10 - \sqrt{100+8}}$$

$$= \sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}$$

$$= \sqrt[3]{\sqrt{108} + 10} - \sqrt[3]{\sqrt{108} - 10} .$$

Does this equal 2 ?!

If so, it's not obvious. Are $\sqrt{108} + 10$ and $\sqrt{108} - 10$ the cubes of any numbers we know?

You will need a hint for this, and here it is: Look at $\sqrt{3} \pm 1$.

$$(\sqrt{3}+1)^3 = \sqrt{3}^3 + 3\sqrt{3}^2\cdot 1 + 3\sqrt{3}\cdot 1^2 + 1^3$$

$$= 3\sqrt{3} + 9 + 3\sqrt{3} + 1 .$$

$$= 6\sqrt{3} + 10$$

$$= \sqrt{108} + 10$$

$$(\sqrt{3}-1)^3 = \sqrt{3}^3 - 3\sqrt{3}^2\cdot 1 + 3\sqrt{3}\cdot 1 - 1^3$$

$$= 3\sqrt{3} - 9 + 3\sqrt{3} - 1$$

$$= 6\sqrt{3} - 10$$

$$= \sqrt{108} - 10 .$$

Hmm. That was lucky. We conclude that

$$x = \sqrt[3]{\sqrt{108}+10} - \sqrt[3]{\sqrt{108}-10}$$

$$= (\cancel{\sqrt{3}} + 1) - (\cancel{\sqrt{3}} - 1)$$

$$= 2 \text{, as expected.}$$

That was tricky but at least it makes sense. Here's a harder one.

Example: $x^3 - 15x - 4 = 0$.

By inspection we see that $x = 4$ is a solution. Cardano's formula gives

$$x = \sqrt[3]{2+\sqrt{4-125}} + \sqrt[3]{2-\sqrt{4-125}}$$

$$= \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

Does this equal 4? How could the sum of two non-existent numbers possibly equal 4?

Cardano in 1545 was stumped. Thirty years Later in 1572, Rafael Bombelli had the courage to press on.

☆ Bombelli's Idea: Pretend that square roots of negative numbers exist and do algebra with them.

He saw that

$$(2+\sqrt{-1})^3 = 2^3 + 3\cdot 2^2\sqrt{-1} + 3\cdot 2\sqrt{-1}^{\,2} + \sqrt{-1}^{\,3}$$

$$= 8 + 12\sqrt{-1} - 6 - \sqrt{-1}$$

$$= 2 + 11\sqrt{-1} = 2 + \sqrt{-121}$$

$$(2-\sqrt{-1})^3 = 2^3 - 3\cdot 2^2\sqrt{-1} + 3\cdot 2\sqrt{-1}^{\,2} - \sqrt{-1}^{\,3}$$

$$= 8 - 12\sqrt{-1} - 6 + \sqrt{-1}$$

$$= 2 - 11\sqrt{-1} = 2 - \sqrt{-121}\,.$$

He concluded that

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

$$= (2+\cancel{\sqrt{-1}}) + (2-\cancel{\sqrt{-1}})$$

$$= 4\,.$$

This was the first time anyone accepted square roots of negative numbers as legitimate quantities that can be manipulated.

In fact, there is no way to obtain the real answer 4 without passing through the realm of "imaginary" numbers.

2/6/15

HW 2 due Fri Feb 13
Math Club Monday (Origami)
Exam 1 Wed Feb 18.

Last time we discussed the cubic equation $x^3 - 15x - 4 = 0$.

On one hand, we know that $x = 4$ is a solution. On the other hand, Cardano's formula with $p = -15$ and $q = -4$ gives:

$$x = \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\left(\frac{q}{2}\right) - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$= \sqrt[3]{2 + \sqrt{4 - 125}} + \sqrt[3]{2 - \sqrt{4 - 125}}$$

$$= \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

Does this equal 4?

Cardano (1545) was confused.

Rafael Bombelli ("Algebra", 1572) had a bold idea: Let's pretend that $\sqrt{-1}$ is an actual number and do algebra with it. He found that

$$(2+\sqrt{-1})^3 = 2^3 + 3\cdot 2^2\sqrt{-1} + 3\cdot 2\sqrt{-1}^2 + \sqrt{-1}^3$$

$$= 8 + 12\sqrt{-1} - 6 - \sqrt{-1}$$

$$= 2 + 11\sqrt{-1} = 2 + \sqrt{-121}$$

and similarly $(2-\sqrt{-1})^3 = 2 - \sqrt{-121}$.

Hence

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

$$= (2+\cancel{\sqrt{-1}}) + (2-\cancel{\sqrt{-1}})$$

$$= 2+2 = 4.$$

Mystery Solved.

///

But this was very strange:

The only way to obtain the real solution 4 is to view it as a sum of two imaginary numbers!

Mathematicians had a hard time with idea. They had this to say about so-called "imaginary" numbers

"as subtle as they are useless"
— Cardano, 1545

"Imaginary numbers are a fine and wonderful refuge of the divine spirit, almost an amphibian between being and nonbeing." — Leibniz, 1702

"The shortest path between two truths in the real domain passes through the complex [imaginary] domain."
— Hadamard, 1945

Today we are comfortable with these numbers, but we still call them "imaginary".

We have three ways of thinking of them.

(1) Naive.

We simply assume that the real number -1 has two square roots. If we call one of them i then the other one is $-i = -1 \cdot i$.

We define the set of complex numbers

$$\mathbb{C} := \{ a + ib : a, b \in \mathbb{R} \}$$

and we operate with them in the obvious way, so

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$

$$\begin{aligned}(a+ib)(c+id) &= ac + ibc + iad + i^2bd \\ &= ac + ibc + iad - bd \\ &= (ac - bd) + i(ad+bc).\end{aligned}$$

With these operations, $\mathbb{C}$ becomes a ring.

Q: What are the 0, 1 elements?

A: $0 = 0 + i0$ and $1 = 1 + i0$ because

$(0+i0) + (a+ib) = a+ib \quad \forall a,b \in \mathbb{R}$

$(1+i0)(a+ib) = a+ib \quad \forall a,b \in \mathbb{R}$.

Q: Is $\mathbb{C}$ a field? (Can we divide?).

A: Consider $a+ib \neq 0+i0$. Then we can divide by $a+ib$ as follows:

$$\frac{1}{a+ib} = \frac{1}{a+ib}\left(\frac{a-ib}{a-ib}\right)$$

$$= \frac{a-ib}{(a+ib)(a-ib)}$$

$$= \frac{a-ib}{a^2 + i\cancel{ab} - i\cancel{ab} - i^2 b^2}$$

$$= \frac{a-ib}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) + i\left(\frac{-b}{a^2+b^2}\right)$$

///

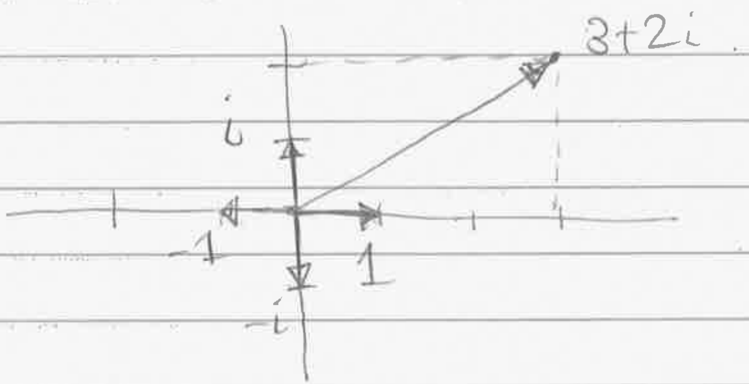
That was a good trick called "rationalizing the denominator".

So $\mathbb{C}$ is a field, but it is not clear from this definition what interpretation it should have.

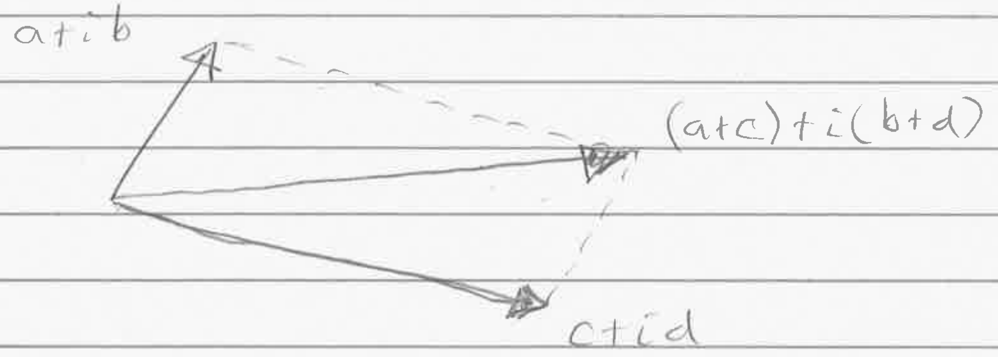
② Geometric.

We define $\mathbb{C} := \mathbb{R}^2$ as the real plane with special operations $+, \times$.

We identify "$a+ib$" $= (a,b)$.
"1" $= (1,0)$
"i" $= (0,1)$.



Addition of complex numbers is just addition of vectors.



"Parallelogram Law"

But multiplication is a little mysterious.

$u \cdot v = ?$

The key insight: We should really think of each complex number $a+ib$ as a <u>function</u>. [What?!]

2/9/15

Math Club Today 6:30pm.
HW 2 due Fri Feb 13
Exam 1 Wed Feb 18 in class.

Last time we began to discuss the field $\mathbb{C}$ of complex numbers. There are a few ways to think about it:

(1) Naive: Let i be a formal symbol with the property $i^2 = -1$ and define

$$\mathbb{C} := \{ a + ib : a, b \in \mathbb{R} \}.$$

This is a ring with the obvious operations

$$(a+ib) + (c+id) = (a+c) + i(b+d)$$

$$(a+ib)(c+id) = (ac-bd) + i(ad+bc).$$

In fact it is a field because we can <u>divide</u>:

$$\frac{1}{a+ib} = \frac{1}{a+ib}\left(\frac{a-ib}{a-ib}\right) = \frac{a-ib}{a^2+b^2}$$

$$= \left(\frac{a}{a^2+b^2}\right) + i\left(\frac{-b}{a^2+b^2}\right).$$

Note that this works for any $a+ib$ such that $a^2+b^2 \neq 0$ (i.e. such that $a+ib \neq 0+i0$).

This suggests that we should define the *conjugate* of a complex number

$$(a+ib)^* := a-ib.$$

Then for any $z \in \mathbb{C}$ we define the absolute value $|z| \in \mathbb{R}_{\geq 0}$ by

$$|z|^2 := z \cdot z^*$$

$$\left[|a+ib|^2 = (a+ib)(a-ib) = a^2+b^2 . \right]$$

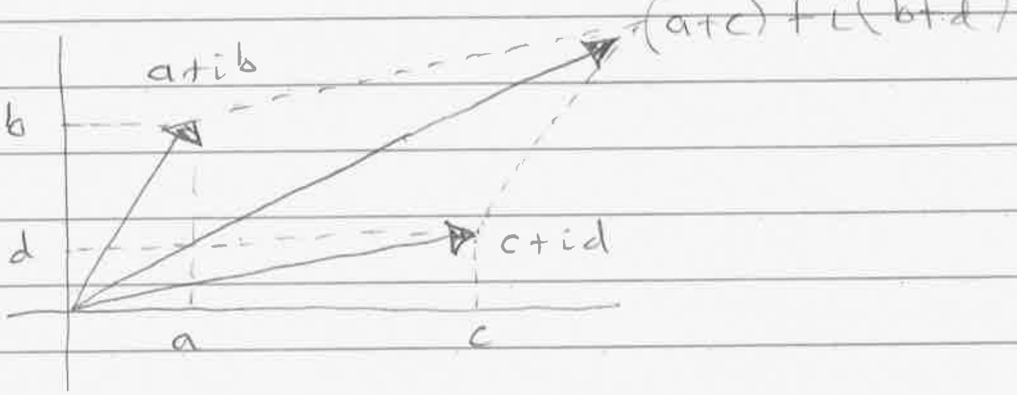
OK, but it is not clear from these definitions what *meaning* to attach to $\mathbb{C}$. We need another point of view.

↓

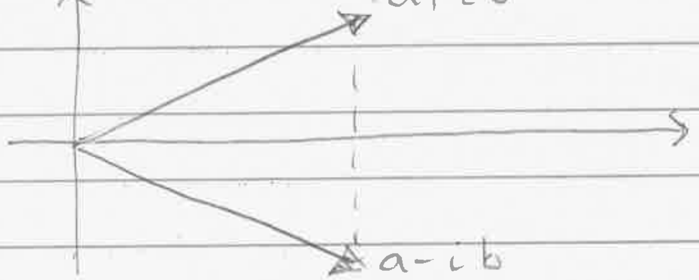
(2) Geometric : We will think of $\mathbb{C}$ as the real Cartesian plane $\mathbb{R}^2$ and identify complex numbers with vectors

$$\text{"}a+ib\text{"} = (a, b)$$

Addition of complex numbers becomes vector addition :

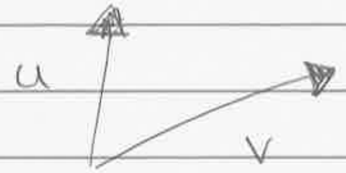


Conjugation is reflection across the "real axis"



and absolute value is vector length.

But multiplication is still mysterious :



$u \cdot v = ?$

The key insight is to think of complex numbers as <u>functions</u> from $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$.

③ Functional :

For each complex number $z \in \mathbb{C}$ we define a function

$$f_z : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

as follows. We think of $\mathbb{R}^2$ as $\mathbb{C}$ and for all $u \in \mathbb{C}$ we define

$$f_z(u) := z \cdot u .$$

If $z = a+ib$ and $u = x+iy$ then we can write this as

↓

$$\begin{aligned} f_{(a+ib)}(x+iy) &= (a+ib)(x+iy) \\ &= (ax-by)+i(ay+bx). \end{aligned}$$

Finally, we can express this purely in terms of real numbers.

$$f_{(a,b)}(x,y) = (ax-by,\ ay+bx).$$

Note that this is a linear function so we can express it as a matrix:

$$f_{(a,b)}(x,y) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

So what?

The whole point is that this gives us a natural interpretation of multiplication of complex numbers: it is just composition of functions.

☆ Theorem: For all $u, v \in \mathbb{C}$ we have

$$\boxed{f_{uv} = f_u \circ f_v}$$

Proof: For all $z \in \mathbb{C}$ we have

$$\begin{aligned} f_{uv}(z) &= (uv)z \\ &= u(vz) \\ &= u f_v(z) \\ &= f_u(f_v(z)) \\ &= (f_u \circ f_v)(z) \end{aligned}$$

///

So what?

Wait a minute! Before we see why this is the best thing ever, let's look at some examples.

The number $1 \in \mathbb{C}$ corresponds to function

$$f_1 : \mathbb{R}^2 \to \mathbb{R}^2$$

that sends $(x,y) \mapsto (x,y)$. In matrix form, this is the identity matrix

$$f_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

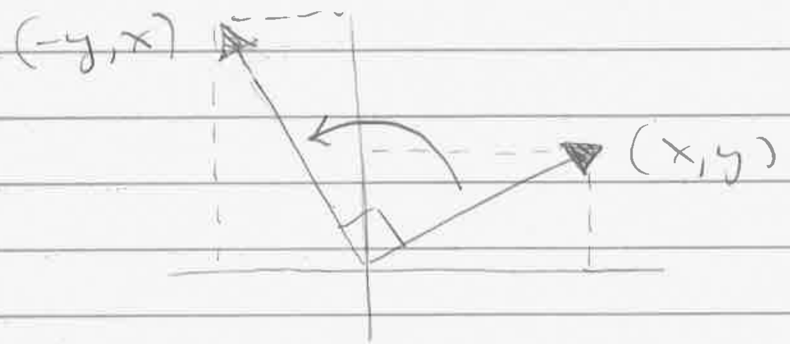
The number $i \in \mathbb{C}$ corresponds to function

$$f_i : \mathbb{R}^2 \to \mathbb{R}^2$$

that sends $(x,y) \longmapsto (-y,x)$. In matrix terms we have

$$f_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Geometrically, this is the function that rotates 90° counterclockwise:



Q: What does the function f_{-i} do?

A: Since $-i = i^3$ we have

$$f_{-i} = f_{i^3} = f_i \circ f_i \circ f_i = (f_i)^3$$

$$\downarrow$$

= rotate 90° counterclockwise
three times

= rotate 270° counterclockwise

= rotate 90° clockwise

Hence

$$f_{-i} = f_i^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thinking Problem:

Can we rotate by other angles?

2/11/15

HW 2 due Friday Feb 13
Review on Monday Feb 16
Exam 1 on Wednesday Feb 18

Recall: There are a few equally correct ways to think about complex numbers.

(1) Complex numbers as numbers.

$$\mathbb{C} = \{ a + ib : a, b \in \mathbb{R} \}$$

where $i^2 = -1$. This is a field with the obvious operations. It also has a conjugation map $\mathbb{C} \to \mathbb{C}$ defined by

$$(a+ib)^* = a - ib.$$

We can use conjugation to invert. Given $z \in \mathbb{C}$ we have

$$z \cdot z^* = |z|^2 \implies \frac{1}{z} = \frac{z^*}{|z|^2}.$$

(2) Complex numbers as vectors.

$$\mathbb{C} = \mathbb{R}^2$$

$$a+ib = (a,b).$$

Addition in $\mathbb{C}$ is the same as addition of vectors in $\mathbb{R}^2$. Conjugation reflects across the real axis. Absolute value is the length of the vector.

$$\text{Multiplication} = ?$$

(3) Complex numbers as functions.

Each $z \in \mathbb{C}$ defines a function

$$f_z : \mathbb{R}^2 \to \mathbb{R}^2$$

by setting $f_z(u) = z \cdot u$. The Key fact about this is that

$$\boxed{f_{uv} = f_u \circ f_v}$$

Written in vector notation we have

$$f_{(a,b)}(x,y) = (ax - by, bx + ay).$$

This can be expressed in the language of matrix multiplication

$$f_{(a,b)}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax - by \\ bx + ay \end{pmatrix}$$

Thus we can think of $a+ib \in \mathbb{C}$ as the 2×2 matrix

$$[f_{(a,b)}] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

[You will investigate this on HW 2.]

So what? Recall that

$$[f_1] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{the identity function.}$$

$$[f_i] = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \text{rotate } 90^\circ \text{ c.c.w.}$$

$[f_{-i}]$ = rotate 270° c.c.w.
(rotatate 90° c.w.).

Can we rotate by other angles?

Which complex number rotates by θ?

☆ Theorem: Let $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the function that rotates c.c.w. by angle θ. This function is linear and its matrix is given by

$$[R_\theta] = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Note that this is the function corresponding to the complex number

$$\cos\theta + i\sin\theta.$$

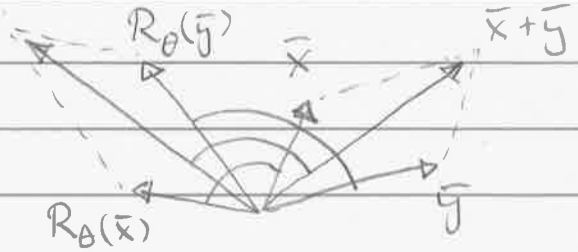
That is, we have

$$f_{\cos\theta + i\sin\theta} = R_\theta.$$

///

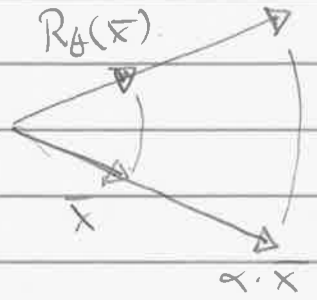
Proof of Theorem:

A linear function preserves vector addition and scalar multiplication. Does rotation do this?



$R_\theta(\bar{x}+\bar{y}) = R_\theta(\bar{x}) + R_\theta(\bar{y})$.

Yes!



$R_\theta(\alpha \cdot \bar{x}) = \alpha \cdot R_\theta(\bar{x})$.

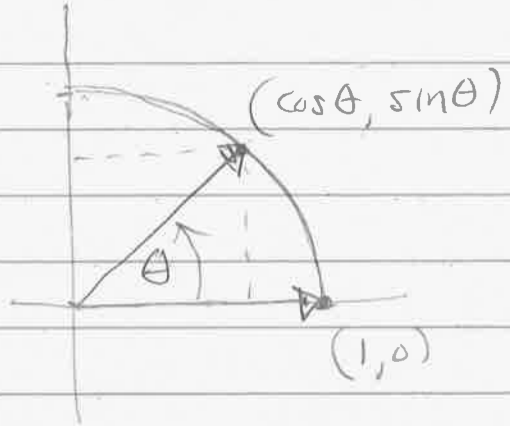
Yes!

So we know that R_θ has a matrix. To compute this matrix we just need to know how R_θ acts on the basis vectors

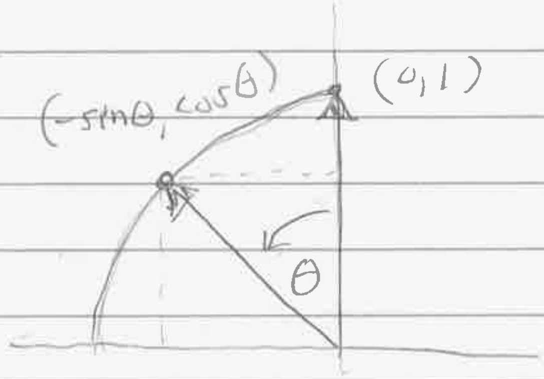
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Check :

$$R_\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$



$$R_\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$



Thus R_θ acting on general vector is

$$R_\theta \begin{pmatrix} a \\ b \end{pmatrix} = R_\theta \left[a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$$

$$= a R_\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b R_\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= a \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} + b \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

▨

So what?

☆ Corollary (De Moivre's Theorem, 1707):

For all integers n we have

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Proof: we have seen that

$$f_{\cos\theta + i\sin\theta} = R_\theta.$$

Note that $(R_\theta)^n = \underbrace{R_\theta \circ R_\theta \circ \cdots \circ R_\theta}_{n \text{ times}} = R_{n\theta}$.

because rotating n times by θ is the same as rotating *once* by $n \cdot \theta$.

Thus we have

$$\begin{aligned} f_{(\cos\theta + i\sin\theta)^n} &= (f_{\cos\theta + i\sin\theta})^n \\ &= (R_\theta)^n \\ &= R_{n\cdot\theta} = f_{\cos(n\theta) + i\sin(n\theta)}. \end{aligned}$$

Since $f_{(\cos\theta + i\sin\theta)^n} = f_{\cos(n\theta) + i\sin(n\theta)}$

we conclude that

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

▨

Remark:

This is the *correct* proof of de Moivre's Theorem

"rotate n times by θ =
rotate once by $n \cdot \theta$"

It depends on the idea of complex numbers *as* *functions*.

2/13/15

HW 2 due NOW
Review on Monday
Exam 2 on Wednesday in class

Today: HW 2 Discussion.

Problem 1: Given polynomials $f(x) = \sum a_k x^k$ and $g(x) = \sum b_k x^k$, recall that the product is defined by

$$f(x)g(x) = \sum_{k \geq 0} \left(\sum_{i+j=k} a_i b_j \right) x^k .$$

If $\deg(f) = m$ (i.e., $a_m \neq 0$ and $a_i = 0 \ \forall \ i > m$) and $\deg(g) = n$ (i.e., $b_n \neq 0$ and $b_j = 0 \ \forall \ j > n$) we want to show that $\deg(fg) = m+n$.

So we must examine the coefficient

$$\sum_{i+j=k} a_i b_j$$

When is this zero?

Lemma: If $i+j > m+n$ then $i > m$ or $j > n$.

Proof: We will show the contrapositive. Indeed, if $i \leq m$ and $j \leq n$ then we must have that

$$i+j \leq n+m.$$

///

So what? If $k > n+m$, I claim that

$$\sum_{i+j=k} a_i b_j = 0$$

Indeed, since $i+j = k > m+n$ we must have $i > m$ (hence $a_i = 0$) or $j > n$ (hence $b_j = 0$), so each term in the sum is zero.

We conclude that $\deg(f \cdot g) \leq m+n$. Why is it equal to $m+n$?

We must show that

$$\sum_{i+j=m+n} a_i b_j \neq 0.$$

Note that the sum is

$$a_0 \underset{0}{\cancel{b_{m+n}}} + \underset{0}{\cancel{a_1 b_{m+n-1}}} + \cdots + a_m b_n + \cdots + \underset{0}{\cancel{a_{m+n}}} b_0$$

Every term in this sum is zero except possibly $a_m a_n$, hence

$$\sum_{i+j=m+n} a_i b_j = a_n b_m$$

and $a_n b_m \neq 0$ because $a_n \neq 0$ & $b_m \neq 0$.

That completes the proof. ///

[You do not need to be this thorough; I just wanted you to see what's involved in a rigorous proof.]

Problem 3: Let $\mathbb{F}$ be a field and consider the statement

$P(n)$ = "<u>any</u> polynomial in $\mathbb{F}[x]$ of degree n has at most n distinct roots in $\mathbb{F}$."

We will show by Induction that $P(n)$ is a true statement for all $n \geq 0$.

- Base Case.

Is $P(0)$ true? Yes because a polynomial of deg 0 is just a nonzero constant, which has no roots.

- Induction Step.

Assume for induction that $P(n)$ is true for $n = 0, 1, 2, \ldots, k$. We will show in this case that $P(k+1)$ is also true:

So let $f(x) \in \mathbb{F}[x]$ be any polynomial of degree $k+1$. We will show that $f(x)$ has $\leq k+1$ roots. If f has no roots we're done, so assume that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. By DFT we have

$$f(x) = (x - \alpha)\, g(x)$$

for some $g(x) \in \mathbb{F}[x]$ and by Problem 1(a) we have $\deg(g) = k$.

Since we assumed that $P(k)$ is true, this $g(x)$ has at most k roots in $\mathbb{F}$.
But the roots of f are just α together with the roots of g..

$[\, f(\beta) = 0 \implies (\beta-\alpha)\, g(\beta) = 0 \implies$ if $\beta \neq \alpha$ then $g(\beta) = 0$. $]$

We conclude that $f(x)$ has at most k roots in $\mathbb{F}$.

///

So what?

Corollary: Let $f(x) \in \mathbb{F}[x]$ be a polynomial. If f has infinitely many roots, then

$$f(x) = 0.$$

Proof: If $f(x)$ is a nonzero polynomial, it has a degree, say $f(x) = n$. But then $f(x)$ has $\leq n$ roots. Contradiction.

Hence $f(x) = 0$.

///

Q: $\deg(0) = ?$

There are many reasons why the zero polynomial cannot have a degree. Some people like to say $\deg(0) = +\infty$ or $-\infty$, but this is somewhat arbitrary. ///

Corollary: Let $\mathbb{F}$ be an *infinite* field. If $f(\alpha) = g(\alpha)$ $\forall \alpha \in \mathbb{F}$ then we must have $f(x) = g(x)$ as elements of $\mathbb{F}[x]$.

Proof: Suppose $f(\alpha) = g(\alpha) = 0$ $\forall \alpha \in \mathbb{F}$. Then the polynomial

$$h(x) := f(x) - g(x)$$

has *infinitely* many roots $(h(\alpha) = 0 \ \forall \alpha \in \mathbb{F})$. We conclude that

$$0 = h(x) = f(x) - g(x),$$

hence $f(x) = g(x)$. ///

Remarks :

- We proved this previously over $\mathbb{R}$ and $\mathbb{C}$, but the proof required derivatives. Now we have a purely algebraic proof that also applies to $\mathbb{Q}$.

- Finite fields are interesting but they will not show up much in this course. They are closely related to the subject of "group theory".