Last time: def. of $\mathbb{C}$ - the field of complex numbers

(will define)

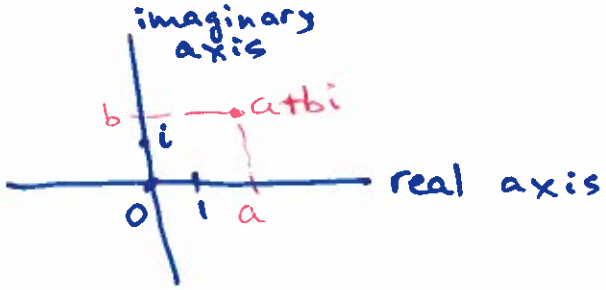
Two ways to think of an element of $\mathbb{C}$ (a complex number):

- $a+bi$, where $a, b \in \mathbb{R}$
- (a,b) where $a, b \in \mathbb{R}$

Examples: i) Converting between these two ways:

the number i itself is the pair

$\mathbb{C}$



$i = (0,1)$

Any real number a is $(a,0) \in \mathbb{C}$

$a+0\cdot i$

Def $a+bi$, $\mathrm{Re}(a+bi) = a$

real part

$\mathrm{Im}(a+bi) = b$

the imaginary part.

Example: Find $\mathrm{Re}\left((3+2i)\cdot i\right)$

$(3+2i)\cdot i = 3i + 2i^2 = 3i - 2$

$\mathrm{Re}(3i-2) = -2.$

What is a field (§2.5 "for Mathematicians")

"set of numbers"

expect: $+, -, \times, \div$

informally, a field is a set F with two operations:

$+, \cdot$ that satisfy "reasonable properties":

F is an "abelian group" with respect to +

1) $(x+y)+z = x+(y+z)$ – associative
2) $x+y = y+x$ – commutative
3) $\exists\ 0 : x+0 = x$ for all x (existence of "the unit element for +")
4) $\forall x \in F$, $\exists\ (-x) \in F$ s.t. $x+(-x)=0$.

$F \setminus \{0\}$ is an abelian group

5) $x\cdot(y\cdot z) = (x\cdot y)\cdot z$ – associativity
6) $x\cdot y = y\cdot x$
7) $\exists\ 1 \in F$, $1\cdot x = x$ for all $x \in F$ (existence of the unit element)
8) $\forall\ x \neq 0$ in F, $\exists\ x^{-1}$ (or $\frac{1}{x}$) s.t. $x\cdot x^{-1} = 1$.

with respect to $\cdot$

9) $x(y+z) = xy+xz$ – distributivity.

Remark: difference between a vector space over $\mathbb{R}$ and a field:

in a vector space: it is also an abelian group with respect to addition, but multiplication is only by scalars that live in $\mathbb{R}$ (not in our vector space).

in a field, you are multiplying elements of the field.

Important point: Given a field F,

we can define a vector spaces over F:

it is a set V, which is an abelian group with respect to $+$

and has multiplication by scalars from F.

(try to write down the axioms: what does this mean?)

Back to examples: 1) Is $\mathbb{C}$ a field?

- With respect to $+$, $\mathbb{C}$ and $\mathbb{R}^2$ are the same.
- $\mathbb{C}$ is also a vector space over $\mathbb{R}$
  (you can multiply complex numbers by real scalars).
  With respect to this, it is "the same" as $\mathbb{R}^2$
- (magic!) we have $\cdot$ on $\mathbb{C}$ that makes it into a field!

  Need to check: 1. $(a_1+b_1i)(a_2+b_2i) = (a_2+b_2i)(a_1+b_1i$
  - easy (exer).

2. associativity: messy.
   exer for those who want it.

3. existence of x^{-1}:

   $(a+bi)^{-1} = ?$

   unpleasant way: $(a+bi)(x+yi)=1$

   system of linear equations $\begin{cases} ax-by=1 & \leftarrow \text{real part} \\ bx+ay=0 & \leftarrow \text{imaginary part} \end{cases}$

(Treat a, b as given constants, not both zero!,

x, y - unknown.

You can solve the system.

Clever way: Observe $(a+bi)(a-bi) = a^2+b^2$ ← real!

Now: $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \underbrace{\frac{1}{a^2+b^2}}_{\in \mathbb{R}}(a-bi)$

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

Def: if $z = a+bi \in \mathbb{C}$, Its complex conjugate is $\bar{z} = a-bi$.

Other examples of fields: ← the rationals

1) Quadratic extensions of $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{d}) = \{ a+b\sqrt{d} \mid a, b \in \mathbb{Q} \}.$$

Let $d \in \mathbb{R}$, if $d > 0$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$

not a square of a rational number

$d < 0$ $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$.

addition, multiplication come from $\mathbb{C}$.

See homework.

2) Finite fields Let p be a prime number.

Consider $\{0, 1, 2, \ldots, p-1\}$ - p elements

$\mathbb{F}_p$ $\{0\} \cup \mathbb{N}$

but with slightly different operations:
addition and multiplication modulo p

meaning: you add and multiply as usual,
but if you get a number $\geq p$,
divide by p and take the remainder.

Example $p = 3$. the zero and 1.

$\mathbb{F}_3 = \{0, 1, 2\}$

$2 + 2 = 1$

what about inverses? here, $2^{-1} = 2$!

$p = 5$: $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$.

$2^{-1} = 3$ ($2 \cdot 3 = 6$, gives remainder 1 modulo 5)

$-4 = 1$

$4^{-1} = 4$ ($4 \cdot 4 = 16$, remainder 1 mod 5).

Why does every element of $\mathbb{F}_p$ have a multiplicative inverse?

(have to believe: take 312 !)

↑ follows from: "Chinese remainder theorem"

or from Euclidean algorithm for the greatest common divisor.

(elementary Number Theory)