<u>Last time</u>: def. of $\mathbb{C}$ – the <u>field</u> of complex numbers

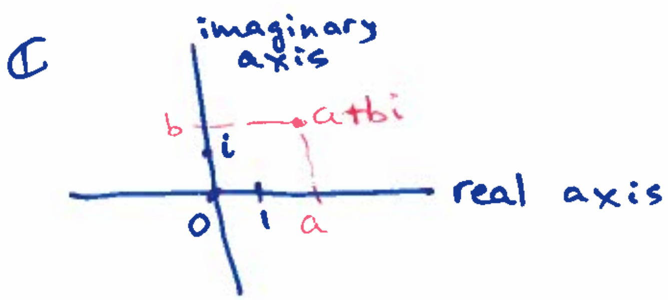
Will define

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

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

<u>Examples</u>: i) Converting between these two ways:

the number i itself is the pair



$i = (0,1)$

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

$\qquad\qquad\quad \overset{\shortparallel}{a+0\cdot i}$

<u>Def</u> $a+bi$, $\underset{\text{real part}}{\mathrm{Re}(a+bi)} = a$

$\underset{\text{the imaginary part.}}{\mathrm{Im}(a+bi)} = b$

<u>Example</u>: 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 with respect to ·

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. $x\cdot x^{-1} = 1$.

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. $(a_1+b_1 i)(a_2+b_2 i) = (a_2+b_2 i)(a_1+b_1 i)$ – 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:

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

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

Let $d \in \mathbb{R}$, not a square of a rational number

if $d>0$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$
$d<0$ $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$.

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

$\{0,1,2,\ldots,p-1\} = \mathbb{F}_p$, $\{0,1,2,\ldots,p-1\} \subset \{0\} \cup \mathbb{N}$

but with slightly different operations:

addition and multiplication <u>modulo</u> p

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

<u>Example</u> $p = 3$.

the zero and 1.

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

$2 + 2 = 1$

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

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

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

$-4 = 1$

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

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

(have to <u>believe</u>: take 312 !)

follows from: "Chinese remainder theorem"

or from Euclidean algorithm for the greatest common divisor.

(elementary Number Theory)

Example: $\quad \mathbb{F}_p^n$ is a set:

$$\mathbb{F}_p^n = \underbrace{\mathbb{F}_p \times \dots \times \mathbb{F}_p}_{n \text{ times}} = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}_p\}.$$

- This set can be naturally thought of as a vector space over the field $\mathbb{F}_p$:
  - it has the usual component-wise addition, and component-wise multiplication by scalars from $\mathbb{F}_p$.

Example $\quad \mathbb{F}_3^4 = \{(a_1, a_2, a_3, a_4) \mid a_i \in \{0,1,2\}\}.$

In $\mathbb{F}_3^4$, $\quad \underset{\mathbb{F}_3}{2} \cdot \underbrace{(0,1,2,1)}_{\mathbb{F}_3^4} = (0,2,1,2).$

$\boxed{\text{a scalar}}$ $\quad \boxed{\text{a vector}}$ $\quad \boxed{\text{a vector}}$

- Magic: $\mathbb{F}_p^n$ can be made into a field
  (will not prove) $\quad$ (it is a field of p^n elements)

- This is very different from the situation over $\mathbb{R}$:
  over $\mathbb{R}$, the set $\mathbb{R}^2$ can be made into a field (this is $\mathbb{C}$ - the field of complex numbers)

And then we have:

- $\mathbb{R}^3$ has "cross product" but you do not have inverses with respect to the cross product, and it is not commutative

- $\mathbb{R}^4$ "magic happens" - can be given a product to convert it to $\mathbb{H}$ - Hamilton's quaternions:

  $(a,b,c,d) \leftrightarrow a+bi+cj+dk$

  i, j, k are symbols, with multiplication defined as:

  $i^2 = j^2 = k^2 = -1$

  $ij = k, \quad jk = i, \quad ki = j$

  $ji = -k \quad kj = -i \quad ik = -j$

  Then all the axioms of a field are satisfied except commutativity of multiplication

- The only other $\mathbb{R}^n$ that has a product structure is $\mathbb{R}^8$ ("the octonions") but that structure is not commutative and not associative

(In short, the only $\mathbb{R}^n$ that can be made into a field is $\mathbb{R}^2$, and you get $\mathbb{C}$)

We are not able to prove any of these facts in this course.

What you'll need for this course is to know several examples of fields:

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

  Also, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ when $d > 0$

- $\mathbb{F}_p$ - the field of p elements.