Q: Why do we need to check closure first?

Field: has closed under $+, \cdot$

Q: How do you prove that

$$-\xi - 1 = \xi + 1 \quad \text{in} \quad \mathbb{Z}_2$$

$$\mathbb{Z}_2 = \{0, 1\}$$

"[0]" "[1]"

In $\mathbb{Z}$ under relation of equivalence modulo 2,

$$[1] = \{\ldots, -7, -5, -3, -1, 1, 3, \ldots\}$$

same in $\mathbb{Z}_2$

Another way to look @ this:

"$-\xi$" is the additive inverse of ξ

BINARY: $\xi + \xi = 0$

so $-\xi = \xi$

FIELD: $\mathbb{F}$, closed under binary ops $+, \cdot$

(F1) Commutativity

(F2) Associativity

(F3) Identity

(F4) Inverses (always for $+$; when nonzero for $\cdot$)

(F5) Distributive

THM (Cancellation Laws) For arbitrary a, b, c in a field $\mathbb{F}$, the following hold:

(i) If $a + b = c + b$, then $a = c$.

(ii) If $ab = cb$ and $b \neq 0$, then $a = c$.

Pf (i) Let $a, b, c \in \mathbb{F}$, assume $a + b = c + b$.

$$\begin{aligned} a &= a + 0 && \text{(Identity)} \\ &= a + (b + (-b)) && \text{(Inverses)} \\ &= (a + b) + (-b) && \text{(Assoc.)} \\ &= (c + b) + (-b) \\ &= c + (b + (-b)) && \text{(Assoc.)} \\ &= c + 0 && \text{(Inverses)} \end{aligned}$$

$= c$

(ii) Essentially the same proof, but replace "+" w/ "·" and "0" w/ "1" □

Cor The additive identity 0 and multiplicative identity 1 are unique. Furthermore, if $x \in \mathbb{F}$, the additive inverse of x is unique, and, if $x \neq 0$, then the mult. inverse of x is unique.

Pf Suppose $0, e$ are additive identities, that is, $x + 0 = x$ for all $x \in \mathbb{F}$, $x + e = x$ for all $x \in \mathbb{F}$.

$$e = e + 0 = 0 + e = 0$$
(Add. Id.) (Comm) (Add Id.)

If $1, f$ are mult. identities, then

$$1 = 1 \cdot f = f \cdot 1 = f$$

Now suppose y, z are both additive inverses of x.

Thm $x + y = 0 = x + z$

$\Rightarrow y + x = z + x$ (Comm.)

$\Rightarrow y = z$ (Cancellation)

Similar for mult. inverses. □

NOTATION $-x$: the additive inverse of x

x^{-1} : the mult. inverse of x

$x - y := x + (-y)$

$\frac{x}{y} := x \cdot y^{-1}$ (assuming $y \neq 0$)

THM Let $a, b \in \mathbb{F}$, a field. Then:

(a) $a \cdot 0 = 0$

(b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(c) $(-a) \cdot (-b) = a \cdot b$

Pf (a) $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0)$ (Dist)

$= a \cdot 0$ (Id)

$= a \cdot 0 + 0$ (Id)

$= 0 + a \cdot 0$ (Comm)

By Cancellation, $a \cdot 0 = 0$. □

(b), (c): Exploit the uniqueness of additive inverses

To show $(-a)\cdot b = -(a \cdot b)$,
show that $ab + (-a)b = 0$.
Since additive inverses are unique,
$(-a)b = -(ab)$. □

COR The additive identity of a field has no multiplicative inverse.

Pf Suppose x is a mult inverse of 0.

Then $1 = 0 \cdot x$
$= x \cdot 0$ (Comm)
$= 0$ (above)

But $0, 1$ distinct, $\Rightarrow \Leftarrow$ □

COMPLEX NUMBERS

DEF The complex numbers are defined as

$$\mathbb{C} := \mathbb{R}[i] = \{ a + bi : a, b \in \mathbb{R}, i^2 = -1 \}.$$

If $z = x + iy \in \mathbb{C}$, then the <u>real part</u> of z is $\mathrm{Re}(z) := x$ and the <u>imaginary part</u> of z is $\mathrm{Im}(z) := y$.

<u>THM</u> The set $\mathbb{C}$ of complex numbers w/ operations addition, mult. is a field.

<u>SKETCH</u>: Main thing (or "most subtle"): multiplicative inverses?

Let $z = x + iy \in \mathbb{C}$, $z \neq 0$.

So: x, y: not both 0.

$$\begin{aligned}(x+iy)(x-iy) &= x^2 - (iy)^2 \\ &= x^2 - i^2 y^2 \\ &= x^2 + y^2\end{aligned}$$

Since x, y are not both 0,

$$x^2 + y^2 \neq 0.$$

$x^2 + y^2 \in \mathbb{R} \Rightarrow$ it has a mult. inverse.

So: $(x+iy) \cdot \left[(x-iy) \cdot (x^2+y^2)^{-1} \right] = 1$

$$(x+iy)\left(\frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}\right) = 1$$

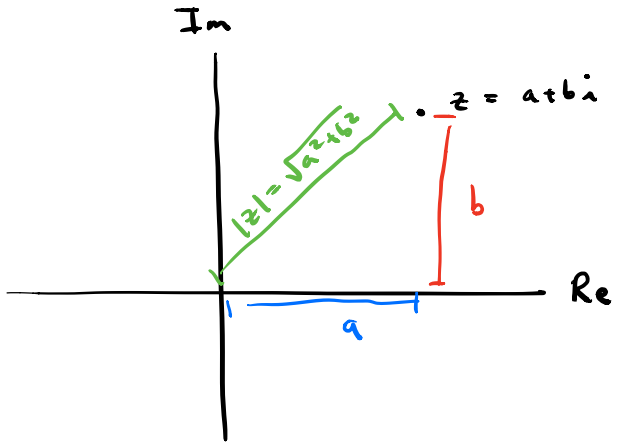
DEF The (complex) conjugate of a complex number $z = a+bi$ is

$$\bar{z} := a-bi.$$

DEF Let $z = a+bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$.
The absolute value (or modulus) of z is the real number

$$|z| := \sqrt{a^2+b^2} = \sqrt{z\bar{z}}$$

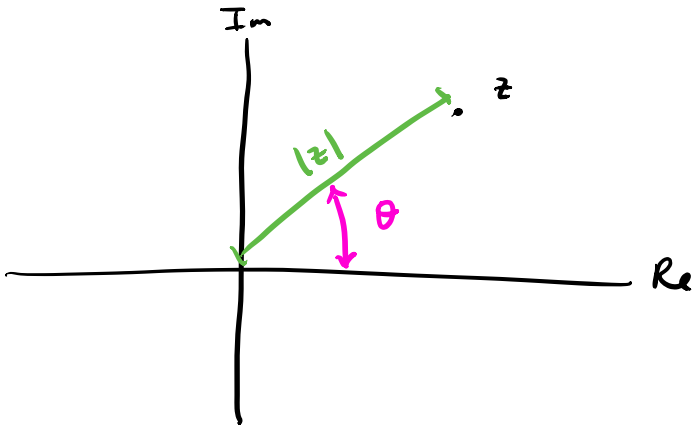
IDEA:



EULER'S FORMULA $e^{i\theta} = \cos(\theta) + i\sin(\theta)$

For any $z \in \mathbb{C}$, $z = |z|e^{i\theta}$,

where



THM (THE FUNDAMENTAL THM OF ALGEBRA)

Suppose $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a polynomial in $\mathbb{C}[x]$ of degree $n \geq 1$. Then $p(x)$ has a zero; that is, there is $z \in \mathbb{C}$ such that $p(z) = 0$.

COR If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a polynomial of degree $n \geq 1$ w/ complex coefficients, then there exist complex numbers $z_1, \dots, z_n$ (not necessarily distinct) such that $p(x) = a_n (x - z_1)(x - z_2) \cdots (x - z_n)$

DEF A field $\mathbb{F}$ is called **algebraically closed** if every polynomial of degree

$n \geq 1$ in $\mathbb{F}[x]$ factors as a product of n polynomials of degree 1.

($\mathbb{C}$: algebraically closed)

READ : §1.1 – 1.2