MAT240. Sept. 19, 2006

F1, F2, F3, F5 are mechanical. $\Rightarrow$ involve no guessing, straightforward

F4: $-(a,b) = (-a,-b)$ $\Rightarrow$ have to write a formula & then

$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ becomes mechanical (verifying it)

* don't need to memorize this

$:=$ LHS is defined by RHS.

$$(a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \overset{\text{by def}}{=} \left(a\cdot\frac{a}{a^2+b^2} - b\cdot\frac{-b}{a^2+b^2}, a\frac{-b}{a^2+b^2} + b\frac{a}{a^2+b^2}\right)$$

$$= \left(\frac{a\cdot a - b(-b)}{a^2+b^2}, \frac{a(-b)+ba}{a^2+b^2}\right) = (1, 0) = 1_{\mathbb{C}}$$

$a^2+b^2=0 \Leftrightarrow a=0$ and $b=0$, $a,b \in \mathbb{R}$.

$\Leftrightarrow (a,b)=(0,0)$

$\square \Rightarrow$ proves that F4 holds true for $\mathbb{C}$, when proving $\mathbb{C}$ is a

<u>Notation</u>

$(0,1) \sim i$ $(0,1)^2 = (0,1)\cdot(0,1) = (0-1\cdot1, 0\cdot1+1\cdot0) = (-1,0) = -(1$

$= -1_{\mathbb{C}}$

$(0,1)^2 = -1$

$(a,0) \sim a$ ~~a~~

Now, $(a,b) = a+bi$

Indeed $(a,0)+(b,0)\cdot(0,1) = (a,0)+(0,b)$

$= (a,b)$

$\square$

Def. If $z = a+bi$ $(=(a,b))$ is a complex number; define $\overline{z}$ = "the conjugate of z" $= a-bi$ $(=(a,-b))$

Eg. $\overline{-157+240i} = -157-240i$

$\overline{-157-240i} = -157+240i$

Thm. $\overline{\overline{z}} = z$. □ → proof is very easy, so he won't show it.

Easy Claims

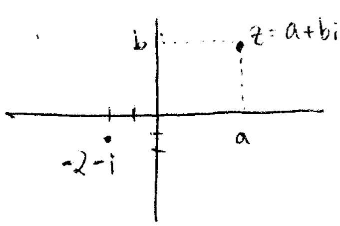
1. $\overline{z+w} = \overline{z}+\overline{w}$
2. $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$
3. $\overline{-z} = -\overline{z}$
4. $z \neq 0$, $\overline{z^{-1}} = \overline{z}^{-1}$

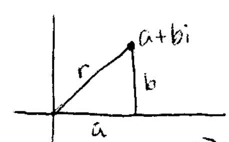
Proofs are mechanical:
Set $z = a+bi$, $w = c+di$
Then sub def'ns into equ'ns & follow def'ns.

$z\cdot\overline{z} = (a+bi)(a-bi) = a^2-(bi)^2 = a^2+b^2 =: |z|^2$
if $z = a+bi$

I.e., define $|z| = \sqrt{a^2+b^2} = \sqrt{z\cdot\overline{z}}$

1. Geometry





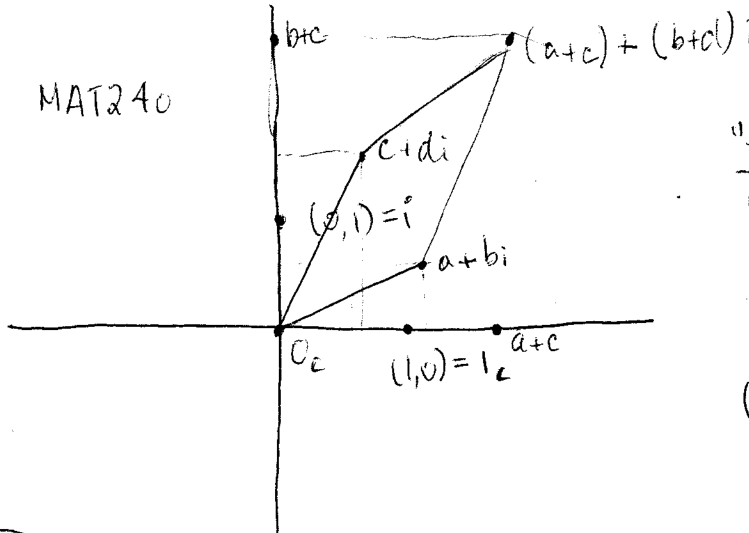
$r^2 = a^2+b^2$
$\Rightarrow r = \sqrt{a^2+b^2} = |z|$

2. Algebra.

if $|z|^2 \neq 0$, $z \neq 0$

remember this $\quad z\overline{z} = |z|^2 \Rightarrow z\cdot\dfrac{\overline{z}}{|z|^2} = 1 \Rightarrow z^{-1} = \dfrac{\overline{z}}{|z|^2}$

MAT240



$\boxed{\text{Addition}}$:

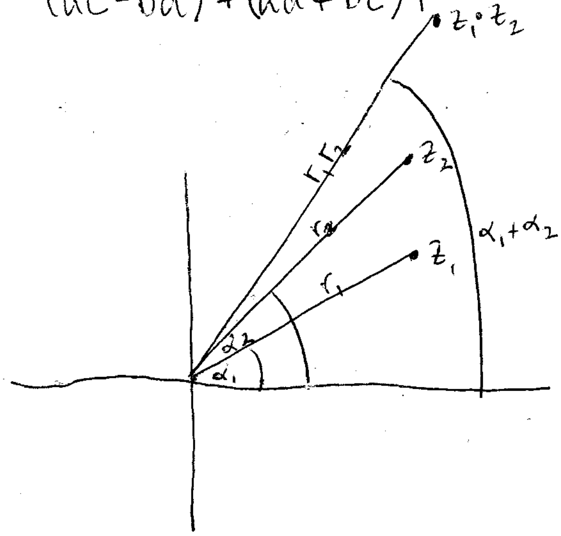
"the parallelogram law"

↳ take one line & add x & y coordinates of other line to it.

$(a+c)+(b+d)i$

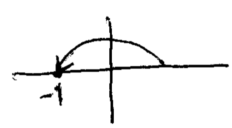
$\boxed{\text{Multiplication}}$

$(ac-bd)+(ad+bc)i$

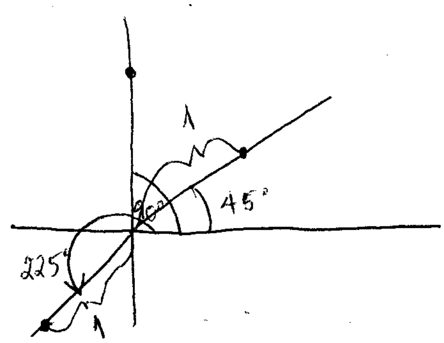


$i = 1 \cdot e^{i\frac{\pi}{2}}$

$i^2 = 1 \cdot 1 \cdot e^{i\left(\frac{\pi}{2}+\frac{\pi}{2}\right)}$
$= 1 \cdot e^{i\pi}$



$\sqrt{i} = ?$



$\sqrt{i} = 1 \cdot e^{i\frac{\pi}{4}} = 1\cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$

or

$\sqrt{i} = 1 \cdot e^{i\left(\pi+\frac{\pi}{4}\right)}$

$\sqrt{-1} = i$ or $-i$

ck: $1 = \sqrt{1} = \sqrt{(-1)\cdot(-1)} = \sqrt{-1}\sqrt{-1} = i \cdot i = -1.$

$1 = \sqrt{1} = -1.$ Masking that has 2 vals: $\pm r$

Remainders.

Divide 240 by 7, what's the remainder?

$$240 = 238 + 2$$
$$= 34 \times 7 + \underbrace{2}_{\text{remainder}}$$

Claim: (Thm that won't prove).
Let $n > 1$ and x be integers. Then there are unique integers q and r. (q = quotient & r = remainder)
s.t. $x = q \cdot n + r$ and $0 \leq r \leq n-1$

Def In this case
$r =: x \bmod n$
x remainder of x when divided by n.
x rem n.

Ex. 240 rem 7 = 2
(-240) rem 7
$= -240 = -245 + r, \quad 0 \leq r \leq 6.$
$= (-35)(7) + 5$

MAT240.

Def. $\mathbb{Z}/n = \{0,1,2,\ldots,n-1\} \Rightarrow$ possible remainders. read "Z mod n"

$\mathbb{Z}/2 = \{0,1\}$

$0_{\mathbb{Z}/n} = 0 \qquad 1_{\mathbb{Z}/n} = 1$

If r_1 & $r_2 \in \mathbb{Z}/n$,

$r_1 +_{\mathbb{Z}_n} r_2 = \underbrace{r_1 + r_2}$ rem n → this may overflow : be larger than allowed set, so take rem n.

$r_1 \times_{\mathbb{Z}/n} r_2 := (r_1 r_2)$ rem n

Ex. $\mathbb{Z}/5 = \{0,1,2,3,4\} \Rightarrow$ digits in base 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Thm.

1. $\mathbb{Z}/n$ with the operations just defined satisfies F1, F2, F3, F4 for addition at least, F5.
2. If n is a prime s.t. $n = 5, 7$ ~~n=26~~.
   then F4 for multiplication holds too.
   So $\mathbb{Z}/n$ is a field in this case.

↳ called F_5 to emphasize that it is a field

Ex In $\mathbb{Z}/5$

$-1 = 4$ $\qquad 1^{-1} = 1$

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

$-3 = 2$ $\qquad 3^{-1} = 2$

$-4 = 1$ $\qquad 4^{-1} = 4$

$\cancel{0^{-1}} =$

Try w/ $\mathbb{Z}$ mod 4, which is not prime:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

x	0	1	2	3
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
1	~~0~~	1	2	3
2	~~0~~	2	0	2
3	~~0~~	3	2	1

Here, every # has a negative, b/c there is a 0 in every row.

To have multiplicative inverse, every row has to have a 1, except crossed.
2^{-1} does not exist.
$\therefore$ $\mathbb{Z}/4$ is not a field

If n is a prime, you normally call it p, and then
$\mathbb{Z}/n \to F_p$ = "the field with p elements $0 \dots p-1$"