HW on Fridays
feedback by Mon.
revisions by Wed.

Office Hours This week:

Monday 3:10-4 Elisa
Tuesday " "
Thurs 2-3 me (and by appointment)
2-3:50 Elisa

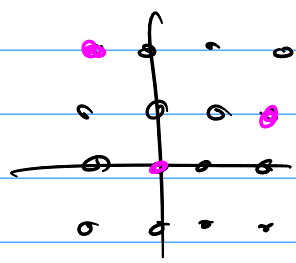
no reading this weekend

$R =$ commutative ring, e.g. $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$

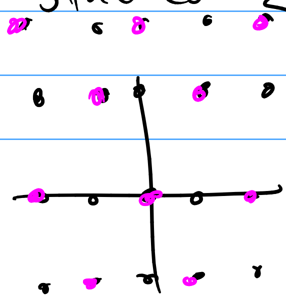
a subset $I \subset R$ is an <u>ideal</u> if
$\forall a, b \in I$ have $a+b \in I$
$\forall a \in I$ $\forall r \in R$ have $ra \in I$

e.g. in $\mathbb{Z}$, $\langle 6 \rangle$ = all multiples of $6 \subset \mathbb{Z}$
$\langle 10 \rangle$ ---

in $\mathbb{Z}[i]$, drew $\langle 1+2i \rangle$



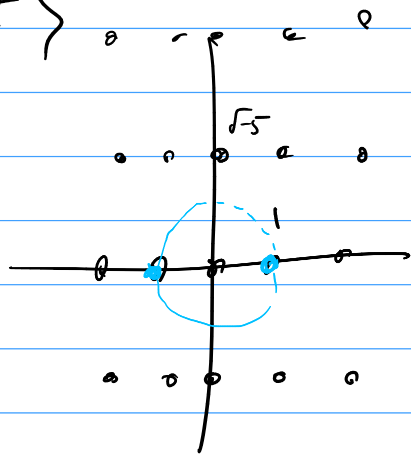
in $\mathbb{Z}[\sqrt{-5}]$, studied $\langle 2, 1+\sqrt{-5} \rangle$



saw that it's not <u>principal</u>
but needs 2 generators.

$R = \mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$

subring of $\mathbb{C}$



for an element $z = a + b\sqrt{-5}$

have $|z|^2 = a^2 + 5b^2 \in \mathbb{Z}$

found that $|z \cdot v|^2 = |z|^2 \cdot |v|^2$

so if $\underset{\text{in } R}{\underline{\underline{z \mid w}}}$ then $\underset{\text{in } \mathbb{Z}}{\underline{\underline{|z|^2 \mid |w|^2}}}$

Prop let $u \in R$. Then u is a unit iff $|u|^2 = 1$.

Corollary: only units are ± 1

Pf of prop: if u is a unit, write $uv = 1$ for some $v \in R$.

then $|u|^2 \cdot |v|^2 = 1$ so $|u|^2 = 1$ and $|v|^2 = 1$

conversely, if $|u|^2 = 1$, then $u \cdot \bar{u} = |u|^2 = 1$

so $\bar{u}$ is an inverse for u.

(if $u = a + b\sqrt{-5}$ then $\bar{u} = a - b\sqrt{-5}$ and $u \cdot \bar{u} = a^2 + 5b^2$.) $\boxed{\text{☺}}$

Later: same proof will show that the units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Prop: in $\mathbb{Z}[\sqrt{-5}]$, 2 can only be factored as $2\cdot 1$ or $(-2)\cdot(-1)$.

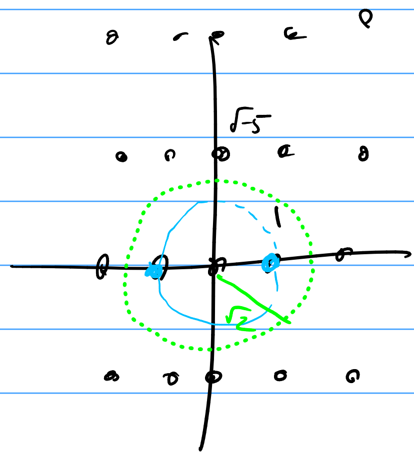
Proof: if $2 = z\cdot w$ then $4 = |z|^2\cdot|w|^2$

might factor $4 = 4\cdot 1 \longrightarrow w = \pm 1$

or $4 = 2\cdot 2 \longrightarrow$ can't happen!

or $4 = 1\cdot 4 \longrightarrow z = \pm 1$

Can't get $z, w \in R$ with $|z|^2 = 2 = |w|^2$. $\square$



Similarly, 3 can only be factored as $3\cdot 1$ or $(-3)\cdot(-1)$

because $|3|^2 = 9 = 1\cdot 9 = \underbrace{3\cdot 3}_{\text{no } z \in R \text{ with } |z|^2 = 3} = 9\cdot 1$

Also, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ have $|1\pm\sqrt{-5}| = 6 = 6\cdot 1 = 3\cdot 2$

can't be factored in an interesting way.

Do these elements of R deserve to be called **prime**?

Maybe not: $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

Euclid's lemma fails: $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$

but $2 \nmid (1+\sqrt{-5})$ and $2 \nmid (1-\sqrt{-5})$

(because $4 \nmid 6$).

Unique factorization fails in $R = \mathbb{Z}[\sqrt{-5}]$ even though it's an int. domain.

ideals were invented to fix this problem

resolution will be:

$$\left.\begin{array}{l} I = (2, 1+\sqrt{-5}) \\ J = (3, 1+\sqrt{-5}) \\ K = (3, 1-\sqrt{-5}) \end{array}\right\} \text{"prime ideals"}$$

Then $I^2 = (2)$ $\qquad J \cdot K = (3)$

$I \cdot J = (1+\sqrt{-5})$ $\qquad I \cdot K = (1-\sqrt{-5})$

$$(6) = (I^2)(J \cdot K) = (I \cdot J)(I \cdot K)$$

no more shocking than $60 = 4 \cdot 15 = 6 \cdot 10$