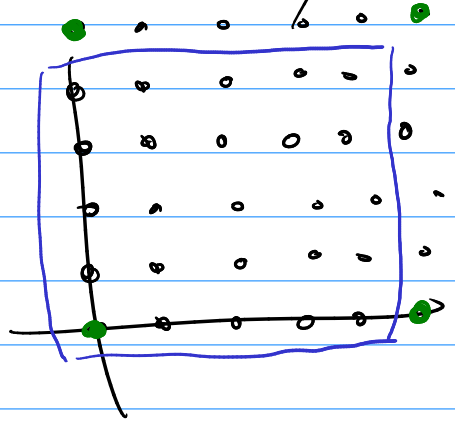
This week: finish up $\mathbb{Z}[i]$ and rings.

Office Hours: back to normal
MT 3:10 - 5 Elisa
W 2 - 3 me
or by appointment

Next week: Groups + symmetry.

Example in the book: $\mathbb{Z}[i]/\langle 5 \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$



this box looks like → $\mathbb{Z}_5 \times \mathbb{Z}_5$ all right.
works for + but not ×

know $\mathbb{Z}[i]/\langle 3 \rangle$ is not $\cong \mathbb{Z}_3 \times \mathbb{Z}_3$
↳ is a field by WS 4 ↳ has zero-divisors

and $\mathbb{Z}[i]/\langle 2 \rangle \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (WS 7 revisited)

So something interesting must be going on.

Last Monday: if $I + J = \langle 1 \rangle$
then $R/IJ \cong R/I \times R/J$
(Chinese Remainder Theorem)

Apply it with $R = \mathbb{Z}[i]$ $I = \langle 2+i \rangle$
$J = \langle 2-i \rangle$

check: $I + J = \langle 1 \rangle$?

$(2+i)(2-i) = 5$ is in I (and J)

$(2+i) + (2-i) = 4$ is in $I + J$

so $5 - 4 = 1$ is in $I + J$

so $\mathbb{Z}[i]/\langle 5 \rangle \cong \mathbb{Z}[i]/\langle 2+i \rangle \times \mathbb{Z}[i]/\langle 2-i \rangle$

$\cong \mathbb{Z}_5$ because $\cong \mathbb{Z}_5$

$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5$

$a + bi \mapsto \bar{a} - \bar{2}\bar{b}$ $\quad \bar{a} + \bar{2}\bar{b}$

is a surj. hom.

with $\ker \varphi = \langle 2+i \rangle$

so 1st iso. thm.

Last time: let $p \in \mathbb{Z}$ be a (non-zero) prime

if p factors in $\mathbb{Z}[i]$

then $p = a^2 + b^2$

so $p \equiv 1$ or $2 \pmod 4$

Contrapositive: if $p \equiv 3 \pmod 4$

then p stays prime in $\mathbb{Z}[i]$

Soon: converse also holds.

+ this accounts for all the irreds. in $\mathbb{Z}[i]$

Factoring from worksheet:

$z = 11+7i$

$|z|^2 = 170 = 2 \cdot 5 \cdot 17$

$|1+i|^2 = 2$ $\qquad \frac{11+7i}{1+i} = 9-2i$

$|9-2i|^2 = 85 = 5 \cdot 17$

$|2+i|^2 = 5$ $\qquad$ but $\frac{9-2i}{2+i} = \frac{16}{5} - \frac{13}{5}i$ yuck!

instead, $\frac{9-2i}{2-i} = 4+i$ $\qquad |4+i|^2 = 17$ prime

$11+7i = (1+i)(2-i)(4+i)$

if you started by doing by $(-i)$

you might get $11+7i = (-i)(2-i)(-1+4i)$

but $-1+4i = (4+i) \cdot i$

$1-i = (1+i) \cdot (-i)$

different factorization, but only different by units.

compare: $30 = 2 \cdot 3 \cdot 5 = (-2) \cdot 3 \cdot (-5)$ in $\mathbb{Z}$

or in $\mathbb{Q}[x]$, $2x^2 - 2x - 3/2 = (x+\frac{1}{2})(2x-3)$

$= (2x+1)(x-3/2)$

Back to main goal:

Next time, we'll prove that

for a prime $p \in \mathbb{Z}$, the following are equiv:

1. p factors in $\mathbb{Z}[i]$
2. $\mathbb{Z}[i]/\langle p \rangle$ is not an integral domain
3. $\mathbb{Z}[x]/\langle x^2+1, p \rangle$ " " " " " "
4. $\mathbb{Z}_p[x]/\langle x^2+1 \rangle$ " " " " " "
5. x^2+1 factors in $\mathbb{Z}_p[x]$
6. x^2+1 has a root in $\mathbb{Z}_p$

seen Friday

$p = 1$ or $2 \bmod 4$

start on today's worksheet