Announcements:

- no class tomorrow
- next week and onward: TR 11:30 – 1. online next week.
  After that LSC 202.

- 1 week extension to Hw2.

Today: Spend some more time inside some number rings.

Before today:

Hw2 (2): about $\mathbb{H}$.

$\overline{(a+bi)} = a-bi$ in $\mathbb{C}$

$\overline{a+bi+cj+dk} = a-bi-cj-dk$ in $\mathbb{H}$

in $\mathbb{C}$, $z\cdot\bar{z} = a^2+b^2 > 0$. $\in \mathbb{R}$

in $\mathbb{H}$ $z\cdot\bar{z} = a^2+b^2+c^2+d^2 > 0$ unless all 0.

"$N(z)$.

$z^{-1} = \frac{\bar{z}}{N(z)}$.

Roughly speaking: A number ring is a subring of $\mathbb{C}$ which feels "integerish".

(unital)

[Defn: A number ring is a unital subring $R \subseteq \mathbb{C}$ s.t. as an additive gp, $R \cong \mathbb{Z}^{\oplus n}$ (free ab. gp on finitely many gen). n = "rank"]

Eg: • $\mathbb{Z}[\sqrt{-1}] := \{ a+ib : a,b \in \mathbb{Z} \}$.

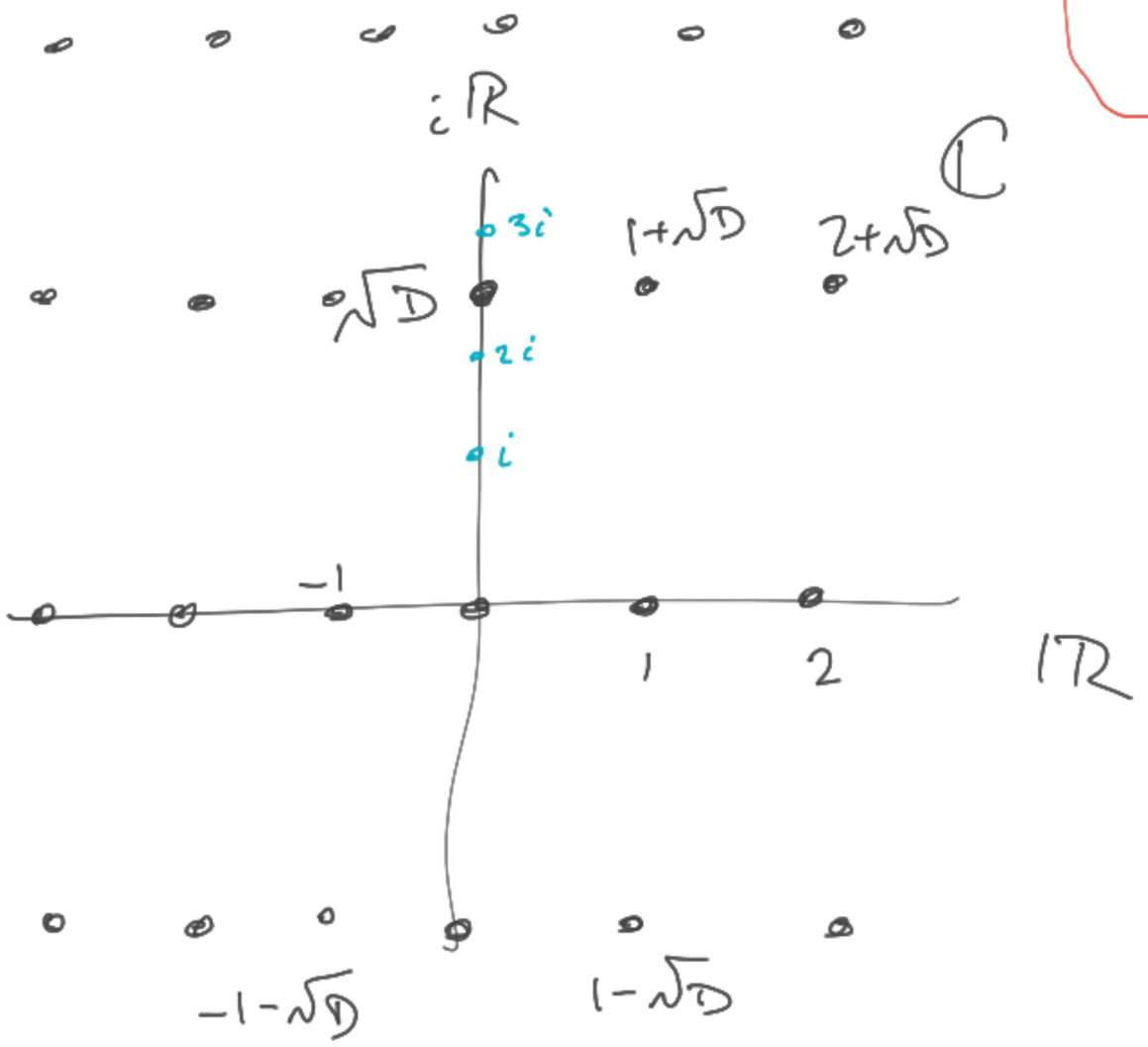
• $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \underset{\text{ab gp}}{\cong} \mathbb{Z}^2$

$(a+b\sqrt{D})(a'+b'\sqrt{D}) = (aa' + Dbb') + (ab' + a'b)\sqrt{D}$.

$\mathbb{Z}[\sqrt{D}]$ if $D<0$.

if $D>0$, then $\sqrt{D} \in \mathbb{R}$,

so $a+b\sqrt{D} \in \mathbb{R}$,



E.S. $D=-7$.

Pop: Let $D \equiv 1 \bmod 4$ (and not a square.)
(e.g. $D = -7$)

Consider the subgp of $(\mathbb{C}, +)$.

$$\{ a + b\sqrt{D} \text{ s.t. } a \text{ and } b \text{ are both in } \mathbb{Z} \text{ or } a \text{ and } b \text{ are both in } \mathbb{Z} + \tfrac{1}{2} \}.$$

Claim: This subgp is a (with 1) subring.

↳ . is a sub. gp under +.
. contains 1 ✓. obv.
. closed under $\times$.

basically obv.

Interesting part is closure under $\times$.

↳ "suppose a, b either both in $\mathbb{Z}$ or both in $\mathbb{Z}+\frac{1}{2}$, suppose a', b' ... Then $(aa' + Dbb') + (\quad)\sqrt{D}$ ... we'll see that it's ever odd"

supposed ring $= \left\{ a + b\sqrt{D} \text{ s.t. } \begin{array}{c} a,b \in \mathbb{Z} \\ \text{or} \\ a,b \in \mathbb{Z} + \frac{1}{2} \end{array} \right\} = R$

Let's choose some set that generates R as a gp.

i.e. choose a set of elts of R

s.t. every elt is an $\mathbb{Z}$-combo of our generators. ("spanning set").

e.g. $\{1, \sqrt{D}, \frac{1}{2} + \frac{1}{2}\sqrt{D}\}$.

Each $r \in R$ is $m \cdot 1 + n \cdot \sqrt{D} + \ell \cdot (\frac{1}{2} + \frac{1}{2}\sqrt{D})$

not uniquely, I don't care.

WTS: If $r, r' \in R$, then $\underbrace{rr'}_{\in \mathbb{C}} \in R$.

r = some integer combo of my generators.

r' = some other $\mathbb{Z}$-combo of generators.

So by distributive law: $r \cdot r' =$

some integer combo of

products of generators.

I already know R is closed under forming $\mathbb{Z}$-combos.

All I need to know: products of gens are in R.

Prop: If $D \equiv 1 \pmod 4$ (and not a square)

then $\{a + b\sqrt{D} \text{ s.t. } a,b \in \mathbb{Z} \text{ or } a,b \in \mathbb{Z} + \frac{1}{2}\}$.

is a subring of $\mathbb{C}$.

pf: It's obviously and additive subgp.

Let's select the additive generating set

$\{1, \sqrt{D}, \frac{1}{2} + \frac{1}{2}\sqrt{D}\}$.

By dist. law, it suffices to show that products of these gen are in R. Only interesting products:

$\sqrt{D}^2 = D$ ✓. $\sqrt{D} \cdot \left(\frac{1}{2} + \frac{1}{2}\sqrt{D}\right) = \frac{D}{2} + \frac{1}{2}\sqrt{D} \in R$

because D is odd.

$$\left(\frac{1}{2} + \frac{1}{2}\sqrt{D}\right)^2 = \frac{1+D}{4} + \frac{1}{2}\sqrt{D} \stackrel{?}{\in} R$$

yes, this is in R, because $D \equiv 1 \bmod 4$,

so $1+D \equiv 2 \bmod 4$, so $\frac{1+D}{4} \in \mathbb{Z} + \frac{1}{2}$. ✓.

□.

$R = ?$

$D = -7$