Math 3032 Lecture 19 (1 April 2021)

Final HW due April 6

Last time: "norms" on a ring. Best behaved version:

Defn: Let R be an integral domain. A multiplicative norm on R is a function

$N : R \to \mathbb{Z}$ s.t.

($\star$) $N(ab) = N(a)N(b)$

($\star\star$) $N(a) = 0$ iff $a = 0$.

if $a, b \neq 0$, $|N(ab)| = \underbrace{|N(a)|}_{\geq 1} |N(b)| \geq |N(b)|$

Niceness, not obligatory, property:

($\star\star\star$) If $N(a) = \pm 1$ then a is a unit. converse is automatic.

Lemma: ($\bigstar$, $\bigstar\bigstar$, $\bigstar\bigstar\bigstar$) imply: if $\alpha, \beta \in R$ and $\alpha, \beta \neq 0$ and β is not a unit, then $|N(\alpha\beta)| > |N(\alpha)|$

Pf: If $\beta \neq 0$ not a unit, then $|N(\beta)| \geq 2$.

$\bigstar\bigstar$: $|N(\beta)| \neq 0$ $\bigstar\bigstar\bigstar$: $|N(\beta)| \neq 1$

Cor: If $\pi \in R$ and $N(\pi) = p$ is a nonzero prime in $\mathbb{Z}$, then π is irred in R.

Pf: Contrapositively, if $\pi = \alpha\beta$ for α, β both not units, then $N(\pi) = N(\alpha)N(\beta)$ would be a factorization into two non-units in $\mathbb{Z}$. $\square$

Our main example of a normed ring is

<u>Gaussian integers</u> $\mathbb{Z}[i] = \{a+ib \text{ s.t. } a,b\in\mathbb{Z}\}$
$\subseteq \mathbb{C}$

$N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$ if $\alpha = a+ib$.

This norm is <u>Euclidean</u>:

($\star\star\star\star$) Given α, β nonzero, $\exists\, q, r$
s.t. $\alpha = q\beta + r$ and $|N(r)| < |N(\beta)|$.

This implied that $\mathbb{Z}[i]$ is a PID and thus a UFD.

Let's work out what are all of its primes.

We'll find out that the Cor on previous slide is almost iff.

Let's suppose $\pi \in \mathbb{Z}[i]$ is prime.

We'll study $N(\pi) = \pi \cdot \overline{\pi}$. ring automorphism.

<u>Observe</u>: If π is prime then so its complex conj. $\overline{\pi}$.

Indeed, if $\overline{\pi} = \alpha\beta$ then $\pi = \overline{\alpha}\overline{\beta}$.

In $\mathbb{Z}[i]$, $N(\pi)$ factors into a product of exactly two primes. Since $\mathbb{Z}[i]$ is a UFD, this factorization is unique (up to association). So "two" is sharp.

So in particular $N(\pi)$ cannot have more than two factors in $\mathbb{Z}$.

using: if $n \in \mathbb{Z}$ not a unit, then it is still a unit in $\mathbb{Z}[i]$.

Two cases:

(1) $N(\pi) = p$ is prime in $\mathbb{Z}$.

This is the case in the cor.

(2) $N(\pi) = p \cdot q$ where p, q are primes in $\mathbb{Z}$.

(perhaps $p = q$).

Lemma: In case (2), indeed $p = q$.

Pf: $N(\pi) = \pi \cdot \bar{\pi}$ both prime.

$N(\pi) = p \cdot q$ valid factorizations in $\mathbb{Z}[i]$.

So up to $p \leftrightarrow q$, must have $\pi \sim p$, $\bar{\pi} \sim q$. i.e. $\pi = \pm p, \pm ip$

$\bar{\pi} \sim \bar{p} = p$.

so $p \sim q$ in $\mathbb{Z}[i]$

so $p = q$.

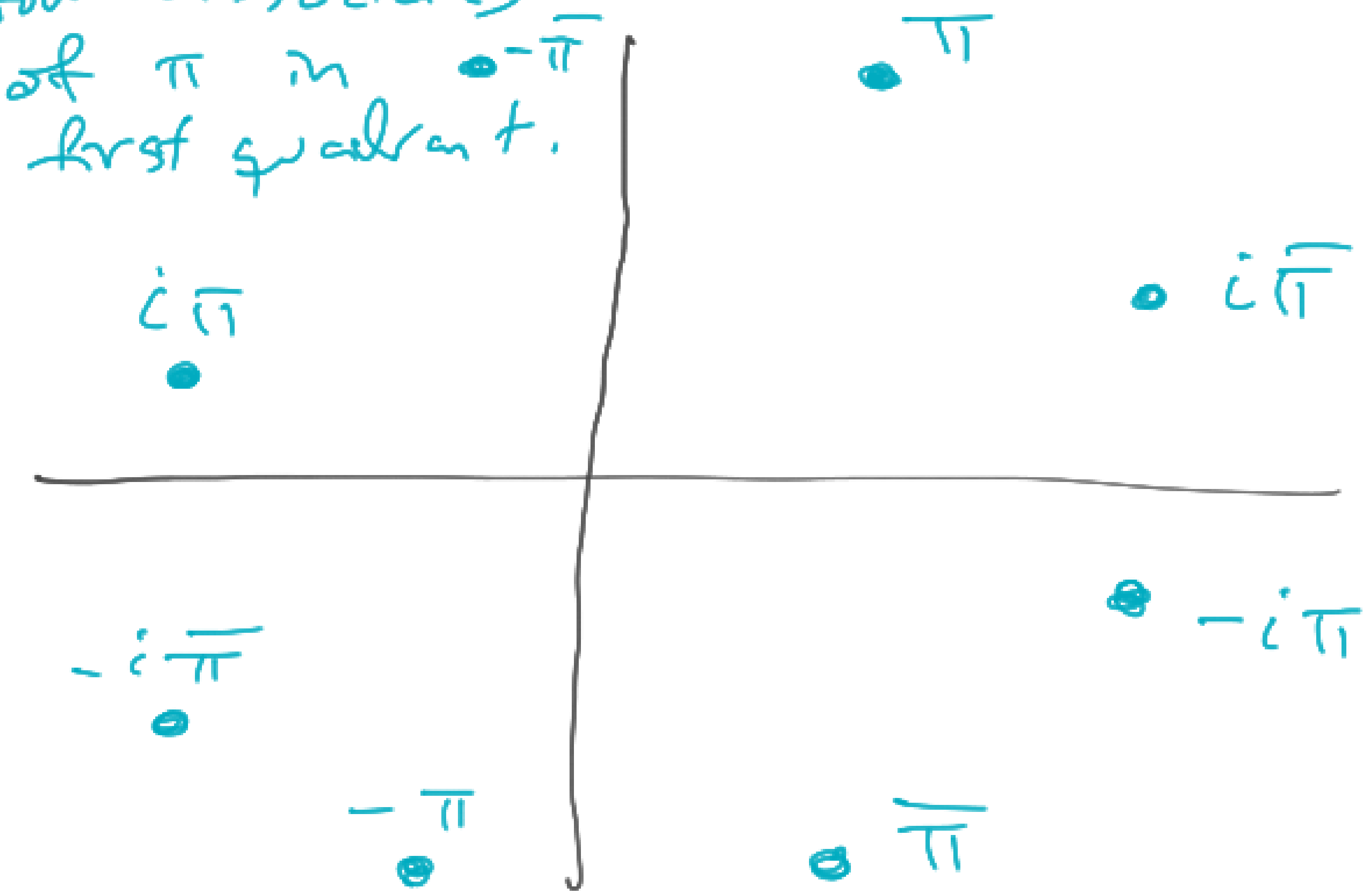
Summary: nonzero Primes $\pi \in \mathbb{Z}[i]$ come in two sets:

(1) $N(\pi) = p$

is prime in $\mathbb{Z}$.

$\pi \notin \mathbb{Z}$ otherwise $N(\pi) = \pi^2$ would be a square integer.

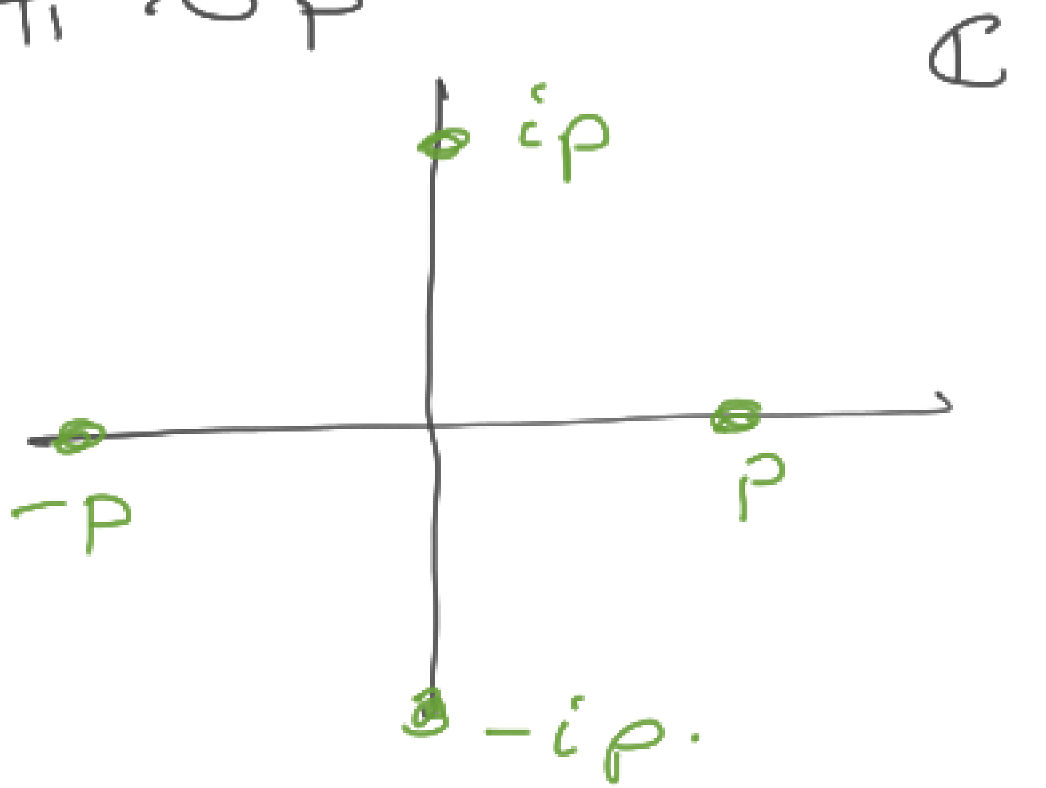
One of the four associates of π in first quadrant.



(2) $N(\pi) = p^2$

p is prime in $\mathbb{Z}$

$\pi \sim p$



Need to decide: which case is which?

i.e. given $p \in \mathbb{Z}$ prime, is it prime in $\mathbb{Z}[i]$ or $N(\pi)$?

Let

$\pi = a + ib$.

$N(\pi) = a^2 + b^2$

$$= \begin{matrix} 0+0 \\ 0+1 \\ 1+0 \\ 1+1 \end{matrix} \mod 4$$

If $\overset{2k}{a =}$ even, then

$$\underset{\underset{4k^2}{\shortparallel}}{a^2} = 0 \mod 4.$$

If $\underset{\underset{2k+1}{\shortparallel}}{a}$ odd

$$\underset{\underset{4k^2+4k+1}{\shortparallel}}{a^2} = 1 \mod 4.$$

In other words,

if $n = 3 \mod 4$

then $n \neq N(\alpha)$ for any $\alpha \in \mathbb{Z}[i]$.

So if $p = 3 \mod 4$ is prime $3, 7, 11, 19, \ldots$

then p is in case (2), i.e. it is prime in $\mathbb{Z}[i]$.

$p = 2$ is the only even prime. It is (i):
$2 = N(1+i)$. $1+i$ is therefore prime.

left to study: $p \equiv 1 \mod 4$.

Punchline will be this is case (i).

Prop: If $p \equiv 1 \mod 4$, then
-1 is a square mod p.

i.e. "-1 is a quadratic residue".

Pf: We want to show that there is
$a \in \mathbb{Z}_p^\times$ s.t. $a^2 = -1$ in $\mathbb{Z}_p$.

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p^\times$ is a abelian
gp of order $p-1 = 4K$. We showed a month ago
that it was cyclic $\mathbb{Z}_{p-1} \cdot g$. g^K would have order 4.

Claim: $\mathbb{Z}_p^\times$ contains an element of exact order 4. i.e. $\exists a \in \mathbb{Z}_p^\times$ s.t. $a^4 = 1$ but $a^2 \neq 1$.

Pf of claim: Since $\mathbb{Z}_p^\times$ has order $4k$ and ab,

$$\mathbb{Z}_p^\times \supseteq \mathbb{Z}_4 \text{ cyclic gp of order 4}$$

or

$$\mathbb{Z}_2^2 \text{ Klein-4 gp.}$$

In the latter case, there would be $\geq$ four solns to $x^2 = 1$. Impossible since $\mathbb{Z}_p$ is a field. Proves the claim.

So $a^4 = 1$ so $(a^2)^2 = 1$ but $a^2 \neq 1$ so $a^2 = -1$.

$\square$

Spelled out, the proposition says

$\exists\, n \in \mathbb{Z}$ s.t. $n^2 \equiv -1 \mod p$

i.e. $n^2 = l \cdot p - 1$ i.e. $n^2+1 = l \cdot p$.

$n^2+1 = N(\overbrace{n+i}^{\alpha})$. $p \mid n^2+1$

$= \alpha\bar{\alpha}$

Since we're in a UFD and $p \mid \alpha\bar{\alpha}$,

the same prime factor in $\mathbb{Z}[i]$ of p divides α or $\bar{\alpha}$.

If p itself were prime in $\mathbb{Z}[i]$, i.e. if p is case (2)

then $p \mid \alpha$ or $\bar{\alpha}$ i.e. $p \mid n \pm i$.

If $p \mid n \pm i$ then $\exists\, \beta = (a+ib)$, $a, b \in \mathbb{Z}$.

s.t. $p\beta = n \pm i$

$\quad\; \parallel$

$pa + ipb$ so $pb = \pm 1$ impossible.

<u>Thm:</u> If $p \in \mathbb{Z}$ is prime then

(1)
- $p = 2$ or $p \equiv 1 \bmod 4 \iff p = N(\pi)$ for some prime $\pi \in \mathbb{Z}[i]$.

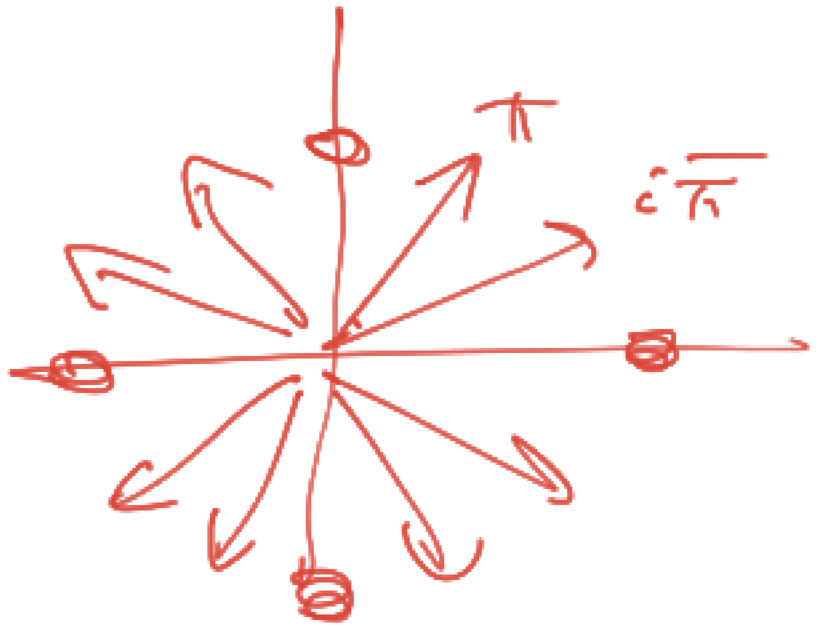
(2)
- $p \equiv 3 \bmod 4 \iff p$ is prime in $\mathbb{Z}[i]$.

And all primes in $\mathbb{Z}[i]$ are of this form.

<u>Counting</u>: In case (2), get

for each $\pm$ prime in $\mathbb{Z}$,

$1 \times \underbrace{4}_{\text{associates}}$ primes in $\mathbb{Z}[i]$



In case (1), $p = 1 \bmod 4$

$\pi = a + ib$ $\rightsquigarrow$ up to associates, $a, b > 0$. one even other odd.

$i\bar{\pi} = b + ia$.

$\pi, \bar{\pi} \rightarrow 2 \times \underbrace{4}_{\text{associates}}$ primes in $\mathbb{Z}[i]$.

why not more?

If $N(\pi) = \pi\bar{\pi} = N(\pi') = \pi'\bar{\pi}'$

all primes, so

$\pi \sim \pi'$ or $\bar{\pi}'$

$\bar{\pi} \sim \bar{\pi}'$ or π'.

(a^2+b^2 theorem)

Given $n \in \mathbb{N}$, in how many ways can it be expressed as a^2+b^2?

$N(\alpha)$ $\alpha = a+ib$

Outline of the answer:

- factor n into primes in $\mathbb{Z}$.

$\alpha\bar{\alpha} = 2^{k_2} \cdot 3^{k_3} \cdot 5^{k_5} \cdots$ $k_p \in \mathbb{N}$ all but finitely many zero.

- if any k_p for $p \equiv 3 \mod (4)$ odd, no solutions.

because p prime in $\mathbb{Z}[i]$, divides α iff divides $\bar{\alpha}$.
so $N(\alpha)$ must have even # of p's.

- primes $p \equiv 1 \mod 4$,

$$\alpha \bar{\alpha} = \quad \cdots \quad 5^3 \quad \cdots$$

each of these "5"s factors in $\mathbb{Z}[i]$

as $\pi \cdot \bar{\pi}$

$$\overset{\shortparallel}{(2+i)}(2-i)$$

must assign to $\alpha, \bar{\alpha}$ in some order.

Cont:

- $p = 3 \mod 4 \rightsquigarrow$ k_p must be even, 1 choice up to association, else no solns

- $p = 1 \mod 4 \rightsquigarrow$ 2^{k_p} choices (up to assoc.)

Over the last few weeks, we proved that a bunch of common rings are UFDs.

e.g. $\mathbb{Z}[i][x,y]$.

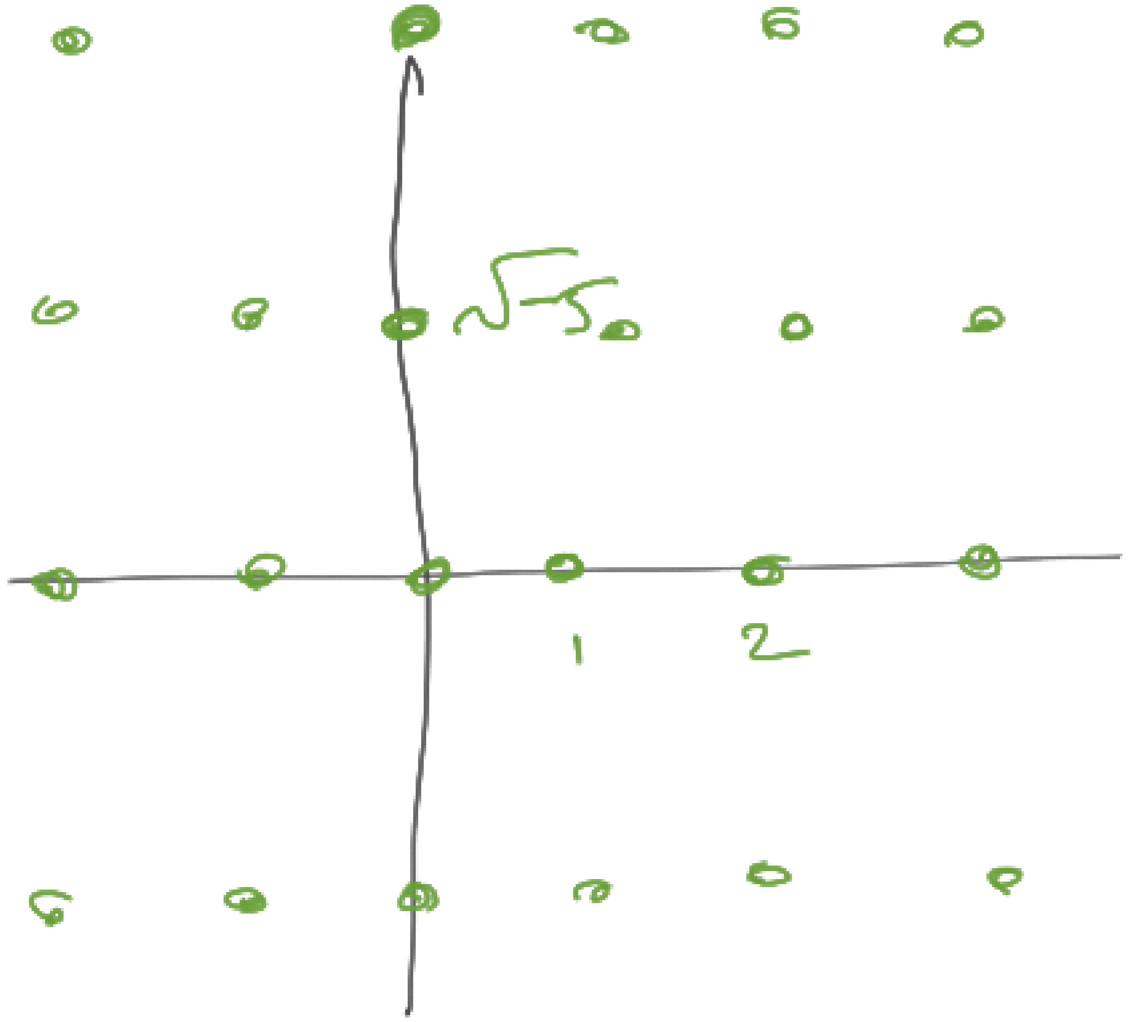
It's past due to describe a non UFD.

The standard example: $\mathbb{Z}[\sqrt{-5}] = \{\overbrace{a+b\sqrt{-5}}^{\alpha}\}$

$\subseteq \mathbb{C}$.

$\sqrt{-5}$

$\approx 2.2i$



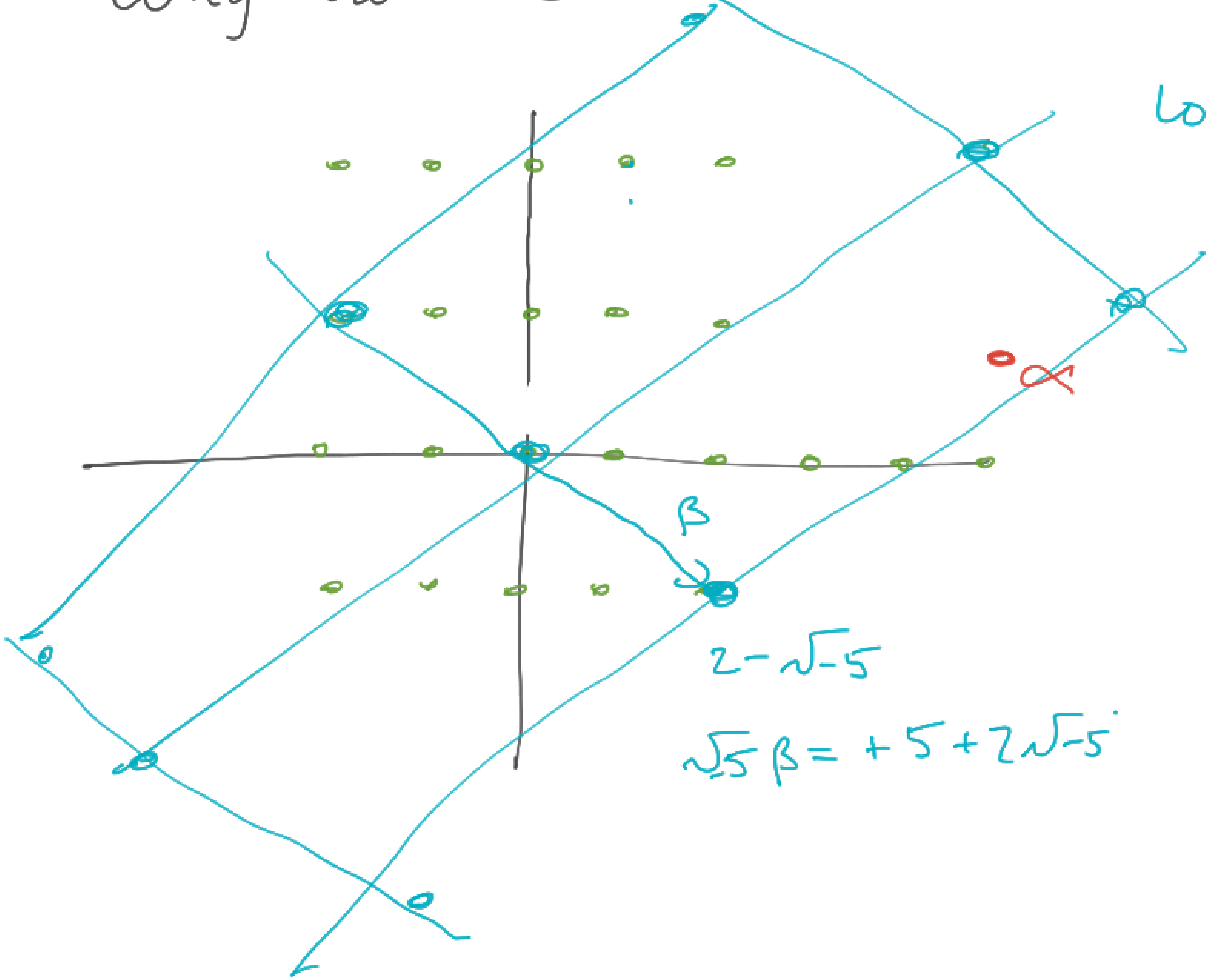
Does have a multiplicative norm.

$N(\alpha) = \alpha\bar{\alpha}$

$= a^2+5b^2$.

$R = \mathbb{Z}[\sqrt{-5}]$

Why not Euclidean?



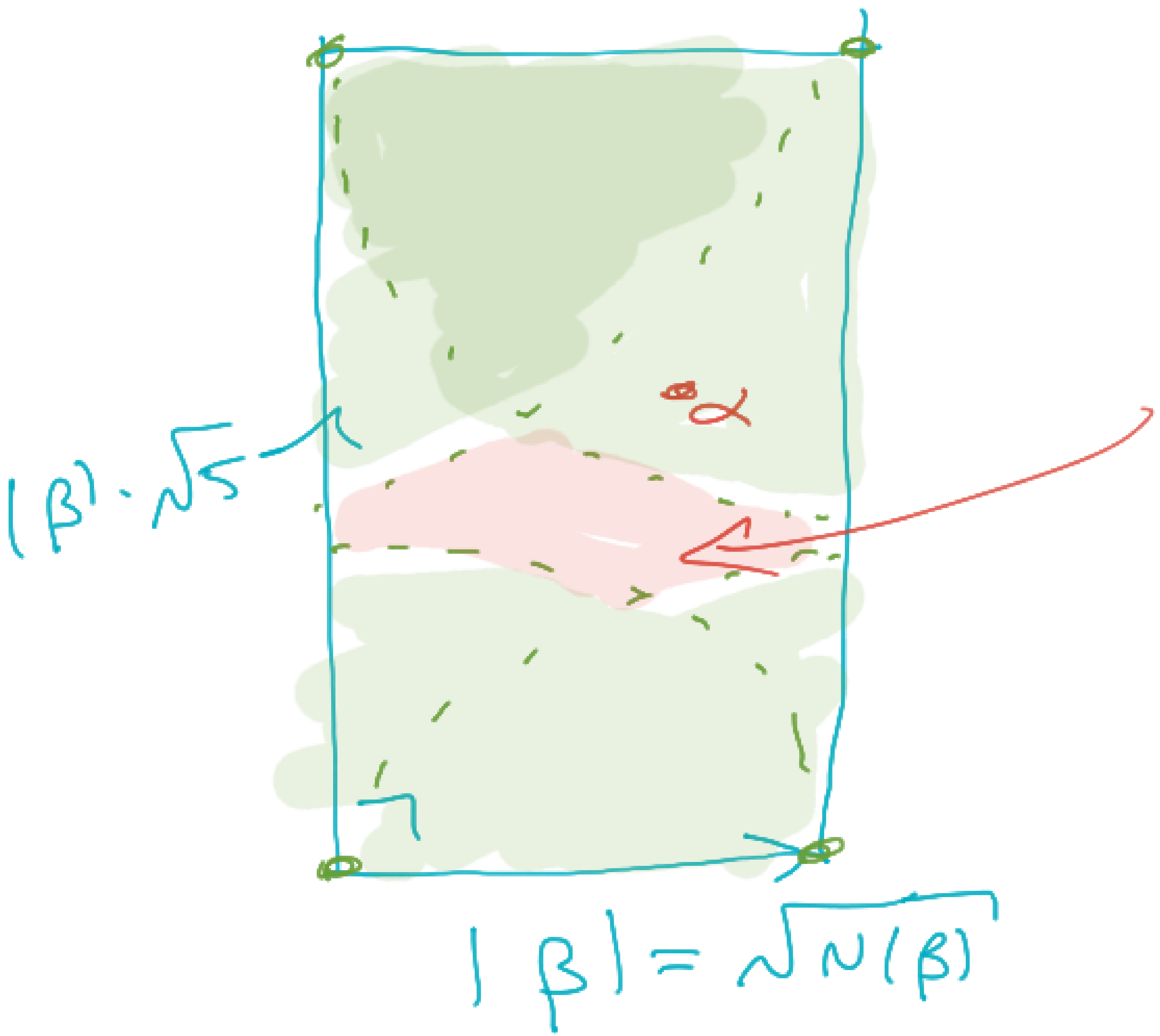
Given $\beta \neq 0$ $\quad q \in R$

look at $\langle \beta \rangle = \{q\beta\}$

It is a rescaled rotated copy of R.

Given α, is there $q\beta$ nearby? Want:

$\alpha = q\beta + r \quad N(r) < N(\beta)$



$$N(\beta) = |\beta|^2$$

Some α's work, not all

region far from any multiple of β.

So $(\mathbb{Z}[\sqrt{-5}], N)$ not Euclidean.

It could still be a UFD.

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

so not a UFD.

Claim: $2, 3, 1\pm\sqrt{-5}$ are non-associate irreds.

$2 \not\sim 1\pm\sqrt{-5}$

because $N(2)=4$ $\quad N(1\pm\sqrt{-5})=6.$ ✓

$N(2)=4.$ If $\cancel{2}\,3$ / $1\pm\sqrt{-5}$ factors nontrivially in $\mathbb{Z}[\sqrt{-5}]$

$N(3)=9$ then it factors as $\alpha\beta$ one, say α,

$N(1\pm\sqrt{-5})=6$ w/ ~~$N(\alpha)=N(\beta)=2\cdot 3$~~ $\quad N(\alpha)=2$, $N(\beta)=3$

But $N(a+b\sqrt{-5}) = \underbrace{a^2}_{\substack{\geq 4 \\ \text{if not} \\ 0 \text{ or } 1}} + \underbrace{5b^2}_{\geq 5 \text{ if not } 0.} \geq 4$ if not 0 or 1.

So not 2. 3.