Math 3032 (30 March 2021)

OH today 12-2pm.
HW 8 due today.
HW 9 (last one) due next week.

last week: gave lots of criteria that implied UFD.
e.g. PID, PID[x].

In $\mathbb{Z}$, $\mathbb{F}[x]$ we showed these were PIDs by using long division. Essence was:

Given $a, b \neq 0$, can find q, r s.t.

$$a = bq + r$$

and either $r = 0$ or r smaller than b.

don't need unique.

in $\mathbb{Z}$, "smaller" could mean $|r| < |b|$.

in $\mathbb{F}[x]$, it meant $\deg(r) < \deg(b)$.
$[\deg(0) = -\infty]$

Defn: Let R an integral domain.

A Euclidean norm on R is a function

$$\nu : R \setminus \{0\} \longrightarrow \mathbb{N} = \{0, 1, 2, \dots\}$$

s.t.

- if $a, b \in R \setminus \{0\}$ then $\nu(ab) \geq \nu(a)$
- $\forall\, a, b \in R \setminus \{0\}$, $\exists\, q, r$ s.t.

  $a = bq + r$

  and either $r = 0$

  or $\nu(r) < \nu(b)$.

(R, ν) is a Euclidean domain

convenience

often but not always, ν will be multiplicative

i.e. • $\nu(ab) = \nu(a)\nu(b)$.

• if $\nu(a) = 0$ then $a = 0$.

Examples: $|-|$ is a Euclidean norm on $\mathbb{Z}$.

$\deg(-)$ is a Euclidean norm on $\mathbb{F}[x]$.

Example of a mult norm: $|-|$ on $\mathbb{Z}$, $2^{\deg(-)}$ on $\mathbb{F}[x]$. $2^{-\infty} = 0$.

Let's review why division $\Rightarrow$ PID.

<u>Thm:</u> Euclidean domains are PIDs.

<u>Pf:</u> Suppose E a Euclidean domain, $I \subseteq E$ ideal.

Then if $I = \{0\}$, done. Otherwise, choose $b \in I$ s.t. $\nu(b) \leq \nu(r)$ $\forall\, r \in I \setminus \{0\}$.

Then $\forall\, a \in I$, $\exists\, q, r$ s.t. $a = bq + r$.

$\in I$

Then $r \in I$. But if $r \neq 0$, then $\nu(r) < \nu(b)$ which is ruled out by assumption on b.

So $I = \langle b \rangle$. $\square$

<u>Cor:</u> Euclidean Domains are Noetherian UFDs.

The reason for the name "Euclidean" is because in *The Elements*, Euclid gave an algorithm for finding g.c.d.s. "Euclidean algorithm"

↑ fast / easy.

Remind: In any UFD, any two elements a, b have a gcd, well defined up to association. $g = \gcd(a,b)$ if $g \mid a$ and $g \mid b$ and if $h \mid a$ and $h \mid b$ then $h \mid g$.

One way to find it: factor a, b into products of primes, compare prime factors.

Factorization is slow / hard.

<u>Euclid's algorithm</u>: Let E be a Euclidean domain, $a,b \in E$.

Set a_0 to be whichever of a,b has larger $\nu(-)$.

a_1 to be the other one.

$\gcd(a,b) = \gcd(a_0, a_1)$ associate $\exists\, q, r$ s.t. $a_0 = a_1 q + r$

either $r=0$ or $\nu(r) < \nu(a_1)$.

<u>Claim</u>: $\gcd(a_0, a_1) \sim \gcd(a_1, r)$.

<u>Pf</u>: If $g \mid a_0$ and $g \mid a_1$ then $g \mid r$ $\Big] \Rightarrow \gcd(a_0,a_1) \mid \gcd(a_1,r)$

$a_0 = m_0 g$ $\quad a_1 = m_1 g$ $\quad r = a_0 - a_1 q = (m_0 - m_1 q) g$

Similarly If $g \mid a_1$ and $g \mid r$ then $g \mid a_0$. $\Big] \Rightarrow \gcd(a_1,r) \mid \gcd(a_0,a_1)$.

Set $a_2 := r$. Then divide a_2 into a_1. Set $a_3 =$ remainder.

$\gcd(a,b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \gcd(a_2, a_3) = \dots = \gcd(a_n, 0)$.

$\nu(a_0) \geq \nu(a_1) > \nu(a_2) > \dots \geq 0$ So alg. must stop. $\Big]$ "a_n".

Summary: $\gcd(a,b)$ is the last nonzero remainder after sequence of Quisims.

<u>Remark:</u> Euclid's algorithm is special case of Gröbner's algorithm.

<u>Note:</u> Euclid's algorithm provides more than just a value of $\gcd(a,b)$.

"E-linear combination"

It computes $m,n \in E$ s.t. $\gcd(a,b) = ma + nb$. ⟸ set of elements " ideal $\langle a,b \rangle$.

High powered reason: the computation was inside ideal $\langle a,b \rangle$.

$$a_0 = q_1 a_1 + a_2 \qquad a_0 - q_1 a_1 = a_2$$

$$a_1 = q_2 a_2 + a_3 \qquad \vdots$$

$$\cdots$$

$$a_{n-3} = q_{n-2} a_{n-2} + a_{n-1} \qquad a_{n-3} - q_{n-2} a_{n-2} = a_{n-1}$$

$$a_{n-2} = q_{n-1} a_{n-1} + a_n \qquad a_{n-2} - q_{n-1} a_{n-1} = a_n$$

$$\left(a_{n-1} = q_n a_n + 0. \right) \rightsquigarrow \gcd = a_n.$$

$$a_n = a_{n-2} - q_{n-1} (a_{n-3} - q_{n-2} a_{n-2})$$

$$= -q_{n-3} + \underline{(1 + q_{n-1} q_{n-2})} a_{n-2} \quad (a_{n-4} - \underline{q_{n-3} a_{n-3}})$$

$$= (1 + q_{n-1} q_{n-2}) a_{n-4} + (-1)(1 + q_{n-1} q_{n-2})(-q_{n-3}) a_{n-3}.$$

If E is a Euclidean domain, choice of ν does not change $+, \times$.

Does constrain $+, \times$. (e.g. by forcing E to be a PID.)

ν tells you about elements.

Prop: Let E a Euc. Dom. Then $u \in E$ is a unit ~~iff~~ if only if $\nu(u) = \nu(1)$. And $\nu(1)$ is the smallest value of ν on $R \setminus \{0\}$.

Pf: If u is a unit, then for any $m \in E$,

$$\nu(m) = \nu(\underbrace{(mu^{-1})}_{a}\underbrace{u}_{b}) \geq \nu(b) = \nu(u).$$

If $\nu(u) = \nu(1)$, then write $1 = qu + r$.

Then $\nu(r) < \nu(u)$ impossible or $r = 0$. So $1 = qu$. u.

Some examples of (Euclidean) domains from theory of numbers.

<u>Defn</u>: Let R be an integral domain. (E.g. any subring of $\mathbb{C}$.)

A <u>multiplicative norm</u> on R is a function $N : R \to \mathbb{Z}$ ($\xrightarrow{1-1} \mathbb{N}$) if want, can make positive by $|N(-)|$.

s.t. $N(ab) = N(a)\,N(b)$

$\Rightarrow$ "$N(0^2) = N(0)$" $N(0)^2$

$N(1)^2 = N(1^2) = N(1)$

so $N(0), N(1) \in \{0,1\}$.

and if $N(a) = 0$ then $a = 0$.

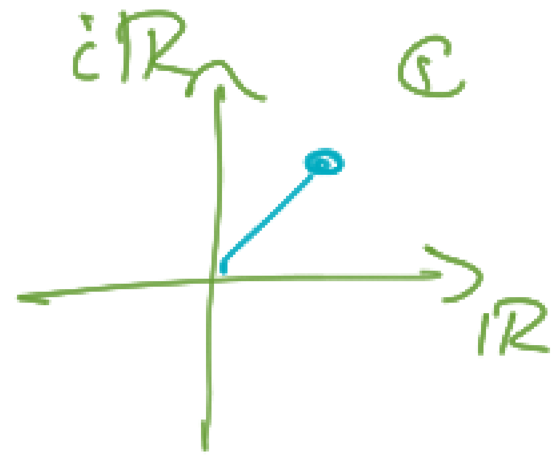
<u>Remark</u>: $|N(ab)| \geq |N(a)|$ if $a, b \neq 0$.

$\underset{\| }{}$ $|N(a)| \cdot \underbrace{|N(b)|}_{\geq 1}$

won't demand divisim.

Extremely nice example:

The Gaussian integers $\mathbb{Z}[i] \subseteq \mathbb{C}$



$$\mathbb{Z}[i] = \{a+bi \text{ s.t. } a,b\in\mathbb{Z}\} \underset{\text{as gp}}{\cong} \mathbb{Z}^2.$$

Set $N(a+bi) = |a+bi|^2 = a^2+b^2$.

- integer? Yes because $a,b\in\mathbb{Z}$.
- $N(a+bi)=0 \Rightarrow a+bi=0$? Yes because if $a^2+b^2=0$, $a^2, b^2 \geq 0$ so must have $a^2=b^2=0$. So $a=b=0$.
- multiplicative? Set $\overline{a+ib} = a-ib$.

Given $\alpha \in \mathbb{C}$ set $\bar{\alpha} := a - ib$.
$\alpha = a + ib$

if $\alpha \in \mathbb{Z}[i]$ then so is $\bar{\alpha}$.

$\alpha \mapsto \bar{\alpha}$ is an $\underbrace{\text{involution}}_{\bar{\bar{\alpha}} = \alpha}$ of $\mathbb{Z}[i]$.

and a ring hom.

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta} \qquad \overline{\alpha\beta} = \bar{\alpha}\bar{\beta}.$$

Recognize: $N(\alpha) = \alpha \cdot \bar{\alpha}$.

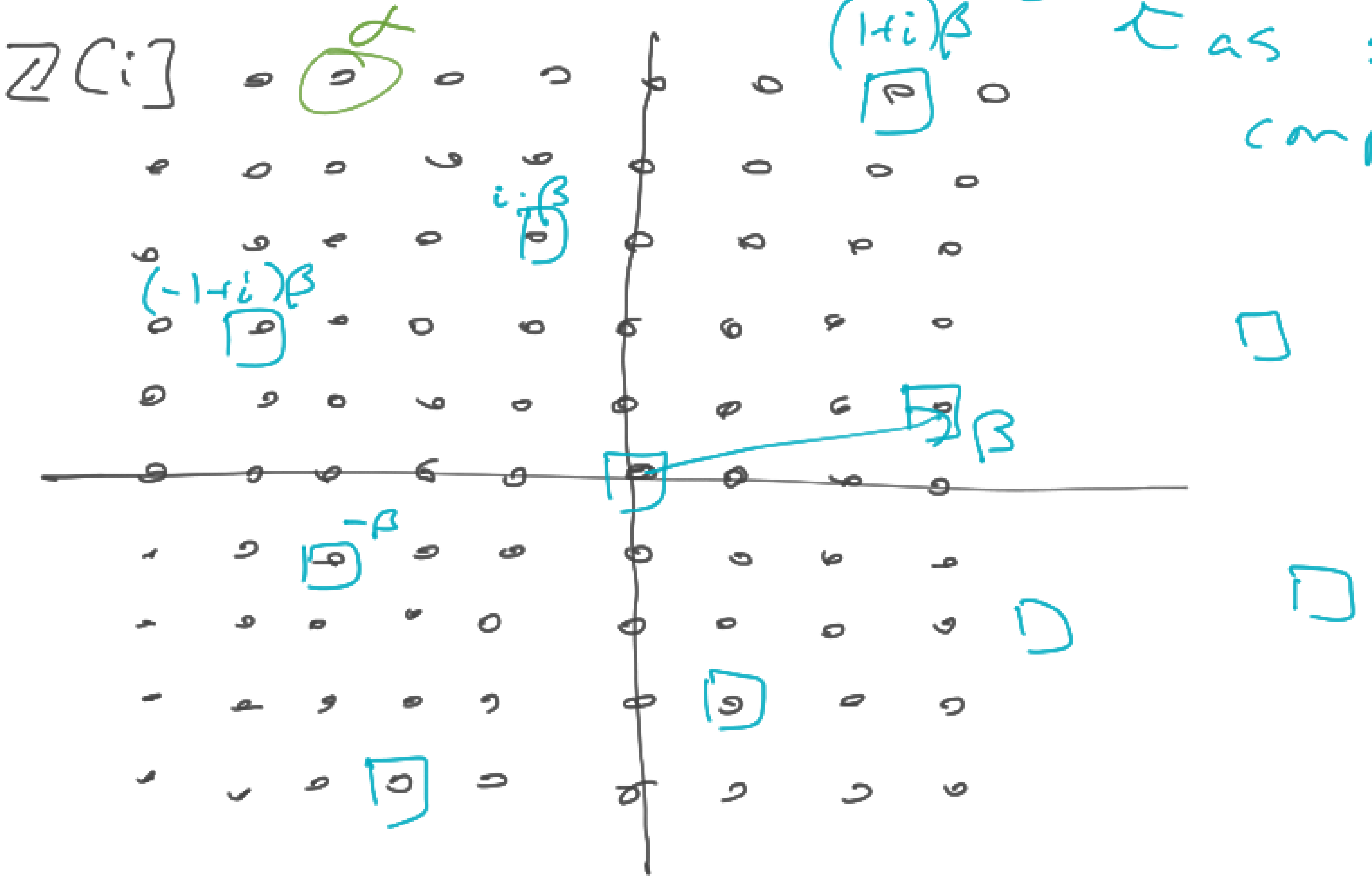
Then $N(\alpha\beta) = \alpha\beta\,\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta}$

$\underset{\text{com.}}{=} \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta).$

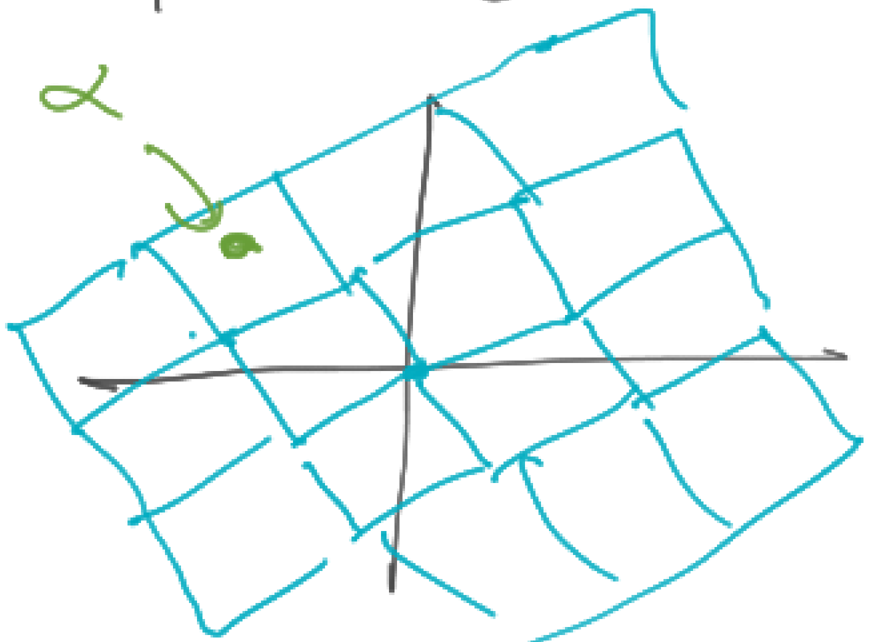
Thm: $(\mathbb{Z}[i], N)$ is Euclidean.

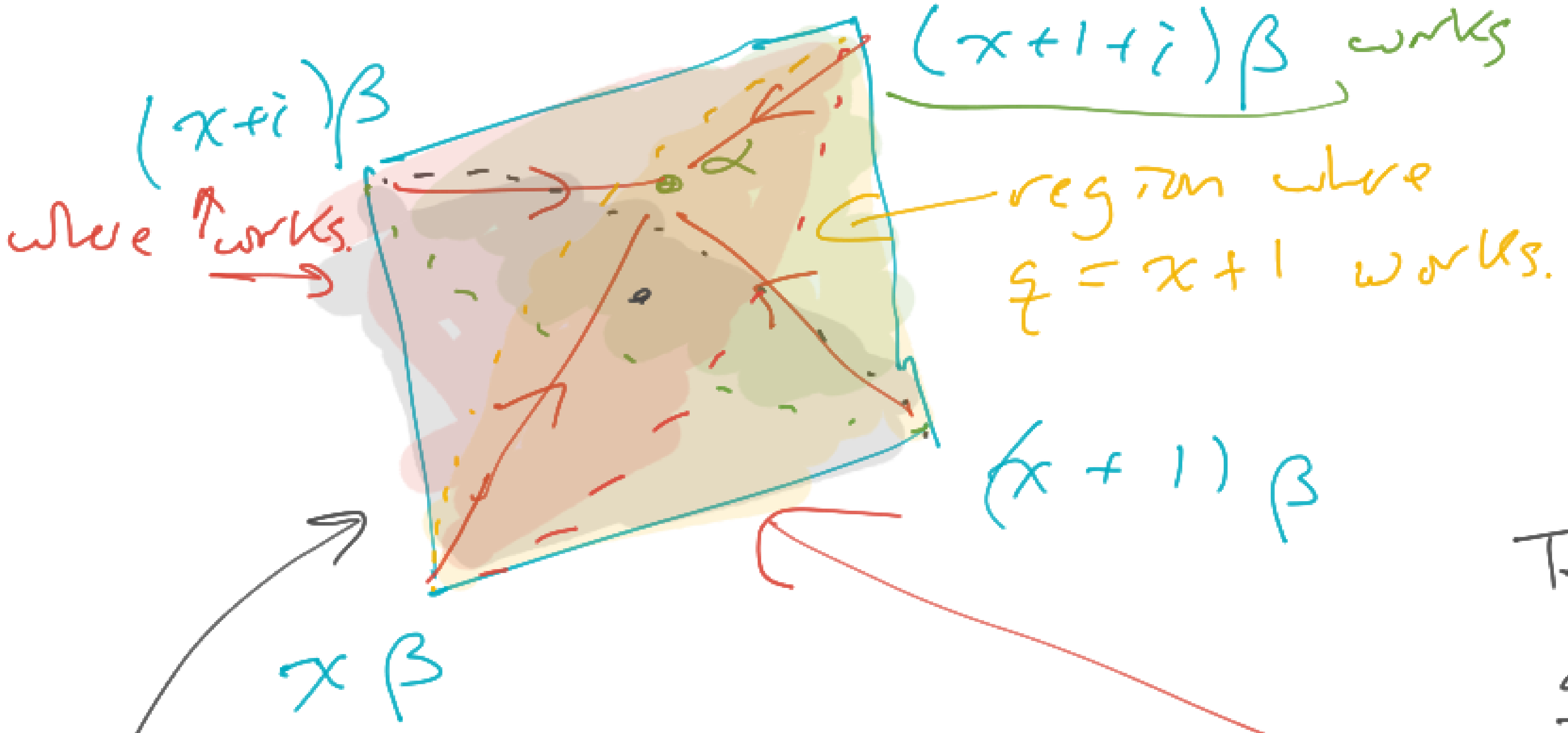
Pf: We need to verify: $\forall \alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$
$\exists q, r$ s.t. $\alpha = \underbrace{q\beta}_{} + r$ and $N(r) < N(\beta)$.

as q varies, these comprise $\langle \beta \rangle$.



$\langle \beta \rangle$ is a rescaled rotated square grid.





So some square contains α (perhaps on border).

Try to set

$q \in \{x, x+1, x+1+i, x+i\}$.

r will be one of these vectors.

We win if at least one of them has $|r|^2 \lneq |\beta|^2$.

all the α's for which $|\alpha - x\beta|^2 \lneq |\beta|^2$.

i.e. ones where $q = x$ works.

Punchline: These quarter circles cover the square. $\square$

Cor: $\mathbb{Z}[i]$ is a UFD.

But factorization in $\mathbb{Z}[i]$

$\neq$ factorization in $\mathbb{Z}$.

$$5 = (2+i)(2-i)$$ so 5 is not prime.

$$= (1+2i)(1-2i)$$

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

$2+i = i \cdot (1-2i)$ i is unit.