Math 3032 Final lecture

HW 9 due today

OH 12 – 2 pm

Don't forget to schedule your final exam.

Last week we discussed two rings

$$\mathbb{Z}[\sqrt{-1}], \quad \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$$

Gaussian integers

$$\{ a + b\zeta, \quad a, b \in \mathbb{Z} \}$$

$$\zeta = \sqrt{-1} = i \qquad \zeta = \sqrt{-5}$$

Eisenstein integers: $\zeta = \frac{1+\sqrt{-3}}{2}$.

What are all of the "rank 2" subrings $R \subseteq \mathbb{C}$?

ie $\exists\, \zeta \in \mathbb{C}$ s.t. $R = \{a + b\zeta,\ a, b \in \mathbb{Z}\}$

(no redundancy, i.e. $\zeta \notin \mathbb{Q}$)

To be a ring:

- $R, +$ ab gp? Yes. $(a+b\zeta) + (a'+b'\zeta) = (a+a') + (b+b')\zeta$ ($0 = 0 + 0\zeta$; $a+a' \in \mathbb{Z}$, $b+b' \in \mathbb{Z}$)
- unital? $1 = 1 + 0\zeta$ ✓.
- closed under $\times$?

$$(a+b\zeta)\cdot(a'+b'\zeta) = aa' + (ab' + a'b)\zeta + bb'\zeta^2.$$

($aa' \in \mathbb{Z}$, $ab' + a'b \in \mathbb{Z}$, need $\zeta^2 \in R$.)

In other words, $\{a+b\zeta\} \subseteq \mathbb{C}$

$\mathbb{Z}[\zeta] \cong \mathbb{Z}^{\oplus 2}$

is a ring iff $\exists\, m, n \in \mathbb{Z}$ s.t.

$$\zeta^2 = m\zeta + n$$

i.e. ζ must solve a quadratic equation

$$p(\zeta) = 0 \quad \text{where } p(x) = x^2 - mx - n \in \mathbb{Z}[x].$$

is monic

Defn: An algebraic integer is a complex soln to a monic poly in $\mathbb{Z}[x]$.

Thm (won't prove): {alg. integers} is a ring.

In these lectures, we showed that
if $p(x) \in \mathbb{Z}[x]$ is monic and
has a zero in $\mathbb{Q}$, then that zero is in $\mathbb{Z}$.

$\Leftrightarrow$ $\{\text{algebraic integers}\} \cap \mathbb{Q} = \mathbb{Z}$.

"rational integers"

If $\deg(p) = n$ p irred. Pick $\xi \in \mathbb{C}$
$p(x) = x^n + \text{lower order}$ s.t. $p(\xi) = 0$.

Then $\mathbb{Z}[\xi] = \mathbb{Z} \oplus \mathbb{Z}\xi \oplus \mathbb{Z}\xi^2 \oplus \cdots \oplus \mathbb{Z}\xi^{n-1}$

e.g. $1 + 2\xi + \xi^2 - \xi^4$

is a ring.

why is $\mathbb{Z}[\zeta]$ a ring? Obv. an add gp.

If you multiply, you might end up with $m \cdot \zeta^N$ $n \leq N < 2n$

$\sim m\zeta^{N-n}(\zeta^n)$

ζ^n = expressible in $1, \dots, \zeta^{n-1}$

$p(\zeta) = 0$

$\zeta^n + \dots$

$\mathbb{Z}[x] \xrightarrow{\text{ring hom}} \mathbb{Z}[\zeta] \subseteq \mathbb{C}$

poly. ring $\quad x \longmapsto \zeta$

x: indeterminate; ζ: chosen complex #.

surjective ✓.

$$\frac{\mathbb{Z}[x]}{\langle p(x) \rangle} = \frac{\mathbb{Z}[x]}{\text{kernel}} \cong \mathbb{Z}[\zeta]$$

We were interested in quadratic extensions

$\mathbb{Z}[\zeta] \qquad \zeta^2 = m\zeta + n.$

$\zeta' = \zeta \pm 1$

$\{a+b\zeta\}_{a,b\in\mathbb{Z}} = \{a+b\zeta'\}_{a,b\in\mathbb{Z}}.$

$(a \pm b) + b\zeta = a + b\zeta'$

$$(\zeta')^2 = (m \pm 2)\zeta' + (n \mp m - 1)$$

Can pick ζ s.t. m is either 0 or 1.

Case (0)

$\zeta^2 = C, \quad \zeta \in \mathbb{Z}$ ← not a square

$\zeta = \sqrt{C}$

Case (1)

$\zeta^2 = \zeta + C$

$\zeta = \dfrac{1 \pm \sqrt{4C+1}}{2}$ ← not a square.

$\zeta = \sqrt{c}$ or $\frac{1+\sqrt{4c+1}}{2}$

$\bar{\zeta} := -\sqrt{c}$ or $\frac{1-\sqrt{4c+1}}{2}$

$\bar{\zeta}$ = c.c. of ζ when $c < 0$

Galois conjugate

In general, if you start with $p(x)$ monic of degree n & irred, ζ is a zero, the Galois conjugates of ζ are the n zeros of $p(x)$.

Lemma: If $p(x) \in \mathbb{Q}[x]$ is irred of deg $= n$, then it has n distinct complex zeros.

Pf: $p(x) = \prod_{i=1}^{n} (x - \alpha_i)$, $\alpha_i \in \mathbb{C}$

α_i are the complex zeros of p. might be repeats.

Look at

$$p'(x) = \frac{dp(x)}{dx} \in \mathbb{Q}[x]$$

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

$a_{n-1} \in \mathbb{Q}$

$$p'(x) = n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

$(n-1)a_{n-1} \in \mathbb{Q}$.

$$\frac{d}{dx}\left[p(x) = \prod_{i=1}^{n}(x-\alpha_i)\right]$$

$$p'(x) = \sum_{i=1}^{n}\ \prod_{j\neq i}(x-\alpha_j)$$

If some α is repeated, then $x-\alpha$ will divide both $p(x)$ and $p'(x)$.

Then $\gcd(p(x), p'(x)) \neq 1$.

↑ is computed by Euclid's algorithm in both $\mathbb{Q}[x]$, $\mathbb{C}[x]$ — get the same answer in $\mathbb{Q}[x]$ or $\mathbb{C}[x]$.

↳ If repeated root, $\gcd(p,p') \neq 1$ but $p(x)$ irred

So $\gcd(p,p') = p(x)$

impossible because $\deg(p') = n-1 < \deg(p)$.

□

$R = \mathbb{Z}[\zeta]$

Case (0)

$\zeta = \sqrt{c}$

$\bar{\zeta} := -\sqrt{c}$

$\bar{\zeta} \in R. \qquad = 0 - 1\cdot\zeta$

Case (1)

$\zeta = \dfrac{1+\sqrt{4c+1}}{2}.$

$\bar{\zeta} = 1 - \dfrac{\sqrt{4c+1}}{2}.$

$= 1 - 1\cdot\zeta$

For higher degree $p(x)$, other Galois conj. don't tend to be $\in R$.

$a+b\zeta \mapsto a+b\bar{\zeta}$ is

$\| \qquad \|$

$\overline{a+b\zeta}$

a ring automorphism of R.

$N(r) := r \cdot \bar{r}$ multiplicative.

In higher deg case, $N(r) = \Pi$ (n Galois conj) $\in \mathbb{Q}$. ← constant term in the deg n poly for r.

$r^2 - (2a)r + N(r) = 0$ ↑ $\mathbb{Z}$.

r ∴

$(a + b\zeta)(a + b\bar{\zeta}) = a^2 + ab(\underbrace{\zeta + \bar{\zeta}}) + b^2 \underbrace{\zeta\bar{\zeta}}$.

↑ $\mathbb{Z}$; $\zeta + \bar{\zeta}$: $-\zeta$ or $1-\zeta$ ∈ $\mathbb{Z}$; $\zeta\bar{\zeta}$: 0 or 1 — $-C$

$\zeta\bar{\zeta} = -C$ or $-C$ ↑ $\mathbb{Z}$.

$\zeta = \sqrt{C}$ if $\zeta = \frac{1 + \sqrt{4C+1}}{2}$

Ex: Golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$. $\mathbb{Z}[\varphi]$.

$\overline{\varphi} := 1 - \frac{\sqrt{5}}{2} = -\varphi^{-1}$

real ring of integers.

$N(\varphi) = \varphi\overline{\varphi} = -1$ $\qquad \varphi^2 - \varphi - 1 = 0$

$N(-)$ always enjoys extra property (~~XXXX~~):

$N(r) = \pm 1 \Rightarrow r$ a unit.

Units in $\mathbb{Z}[\varphi] = \pm \varphi^n \quad n \in \mathbb{Z}$.

Field of fractions of $\mathbb{Z}[\zeta] \subseteq$ alg integers.

is $\mathbb{Q}[\zeta]$ n-dim

$\| \quad \mathbb{Q} \oplus \mathbb{Q}\zeta \oplus \dots \oplus \mathbb{Q}\zeta^{n-1}$.

$\mathbb{Q}[\zeta] \cap$ alg integers

$\cup 1$

$\mathbb{Z}[\zeta]$

"integral closure of $\mathbb{Z}[\zeta]$"

e.g.

$\mathbb{Z}[2\sqrt{3}] \hookrightarrow \mathbb{Z}[\sqrt{3}]$ "rings of integers"

$\mathbb{Z}[\sqrt{5}] \hookrightarrow \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

$\mathbb{Z}[\zeta']$ for some ζ'

BTW:

Lemma: $\mathbb{Z}[\zeta] \cong \mathbb{Z}[x]/\langle p(x) \rangle$

is Noetherian.

Pf: Let $I \subseteq \mathbb{Z}[\zeta]$ an ideal

WTS it's finitely gen.

$\widetilde{I} = \{ f(x) \text{ s.t. } f(\zeta) \in I \} \subseteq \mathbb{Z}[x]$

is an ideal. ↑ Noetherian.

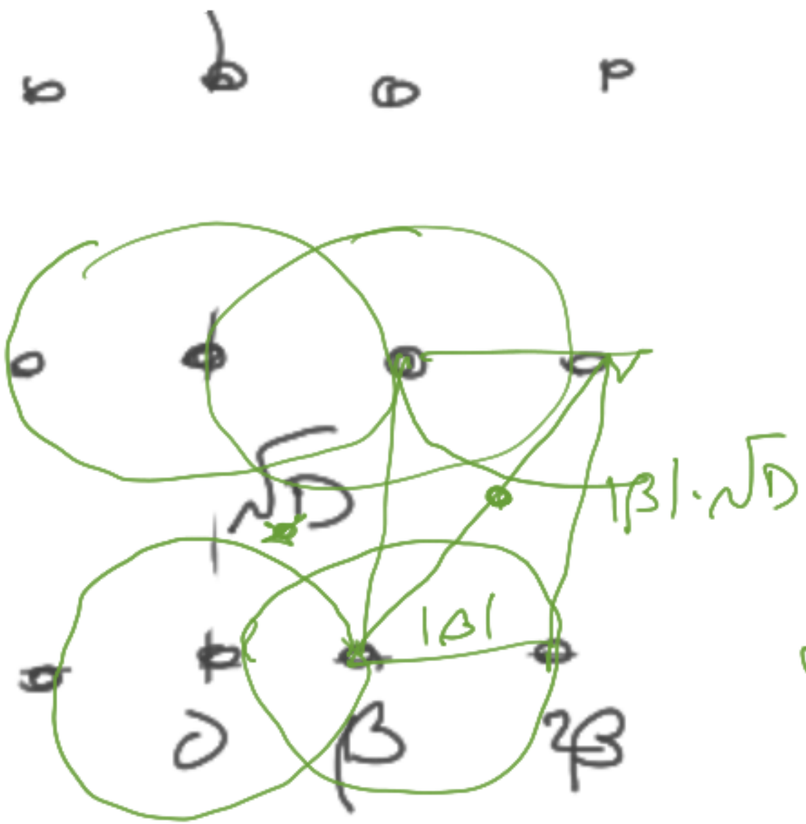
So $\widetilde{I} = \langle g_1(x), \dots, g_n(x) \rangle$.

So $I = \langle g_1(\zeta), \dots, g_n(\zeta) \rangle$. □

When is $\mathbb{Z}[\xi]$, $N(r) := r\bar{r}$ Euclidean?

Definiteness: Imaginary case.

Case (0): $\xi = \sqrt{-D}$ $D \in \mathbb{N}$.
not a square.



want to study $\alpha = q\beta + r$
$\leftrightarrow$ ideal $\langle\beta\rangle$.

For every α, is it w/in $|\beta|$ for a point in $\langle\beta\rangle$?

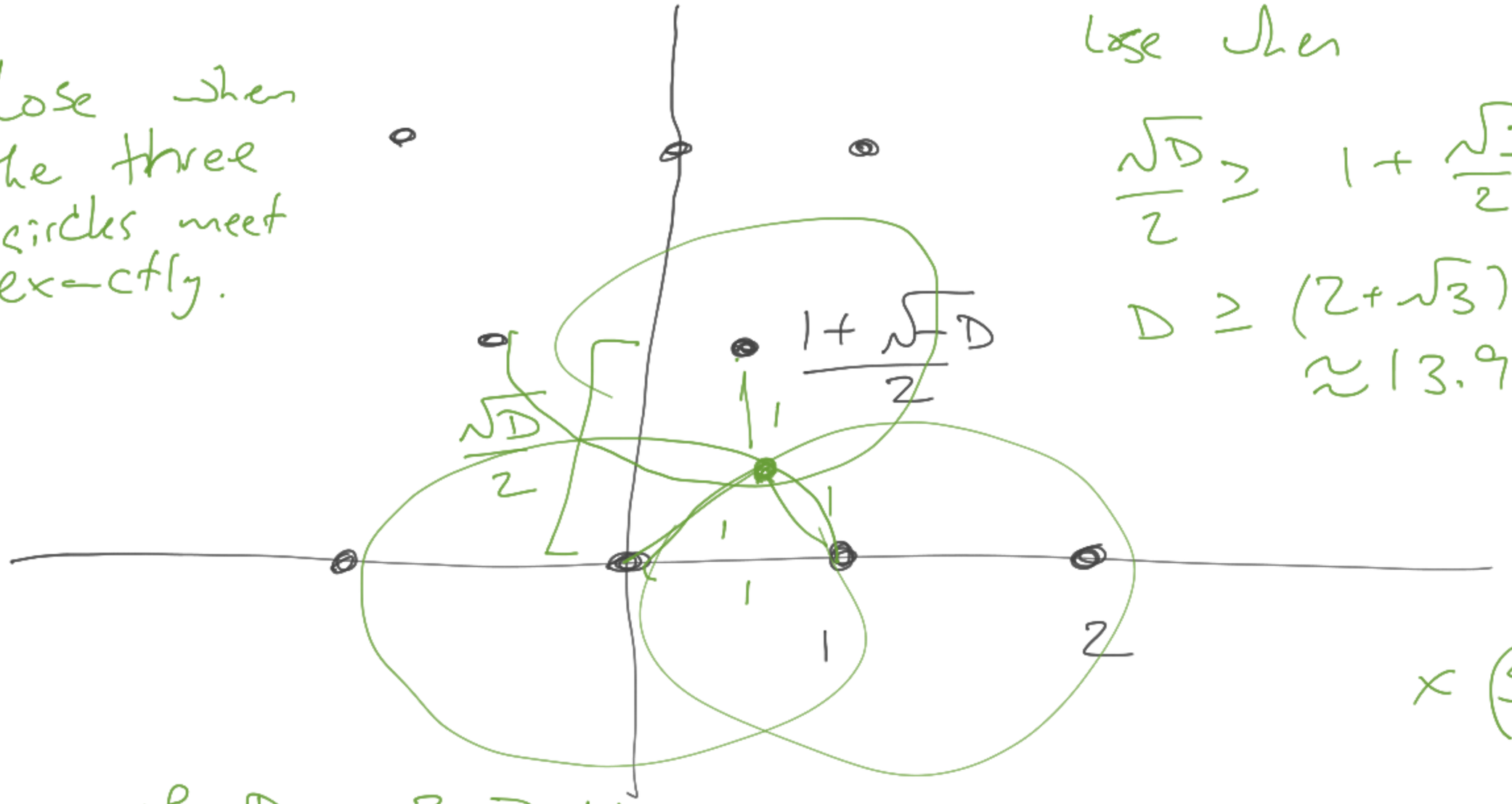
win iff

$$|\beta| \cdot \sqrt{1+D} < |\beta| \cdot 2.$$

$1 + D < 4$ i.e. $D = 1$ or 2.

Case (1) $D = 4K - 1$ $C = -K$.

Lose when the three circles meet exactly.



Lose when

$\frac{\sqrt{D}}{2} \geq 1 + \frac{\sqrt{3}}{2}$.

$D \geq (2+\sqrt{3})^2$

≈ 13.9

$\times \beta$.

win if $D = 3, 7, 11$.

Summary: The following rings are Euclidean, hence UFDs:

$$\mathbb{Z}[\sqrt{-1}],\ \mathbb{Z}[\sqrt{-2}]$$

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right].$$

Thm [Stark-Heegner]: The other imaginary quadratic UFDs

$$\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$$

$$\mathbb{Z}[\sqrt{-67}].$$

$D = 19,\ 43,\ 163$

163 is magic in number thy.