$\boxed{\text{Ch.13}}$

$d=2 \text{ or } 3\ (4)$ $\quad$ $d\equiv 1\ (\text{mod } 4)$

$R = \text{RoIoi } \mathbb{Q}\#F = \mathbb{Z}[\delta]$ or $\mathbb{Z}[\eta]$

$d =$ sq-free, $\delta = \sqrt{d}$, $\eta = \frac{1+\delta}{2}$

$d<0$

(= elts of $\underbrace{\mathbb{Q}(\delta)}_{\text{smallest field cont } \mathbb{Q},\ \delta}$ that are zeros of $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$)

$\boxed{Q}$ Is R a PID?

If not, how close is it?

By 13.8: Alg for deciding in any particular case of d.

$\underline{\text{Defn}}$ A, B ideals of R. $A \sim B \iff \underbrace{A = \alpha B}_{A,B \text{ same shape}}$ $\quad$ $\alpha \neq 0$ $(\alpha \in \mathbb{C})$

All non-0 prin. ideals $(a) \sim (b)$

since $(b) = \frac{b}{a}(a)$

So R PID $\iff$ one equiv class

equiv classes = class # of R.

$\boxed{13.3}$ geom pf that class # of $\mathbb{Z}[\sqrt{-5}] = 2$.

(Other class: $(2, 1+\delta)$)

Q Is $\underbrace{\mathbb{Z}[\sqrt{-3}]}_{\text{not RoI of QNF}}$ a PID?

Classify shapes of ideals in $\mathbb{Z}[\sqrt{-3}]$.

Two principles: $A \subseteq \mathbb{Z}[\delta] = R$

1. A ideal of $R \iff A$ sublattice of R and $\delta A \subseteq A$.

(same for η instead of δ)

2. A lattice in $\mathbb{C}$, $\underbrace{v = \min|\alpha|}_{\text{length of min vec.}}$ $\left(\begin{matrix}\alpha \in A \\ \alpha \neq 0\end{matrix}\right)$

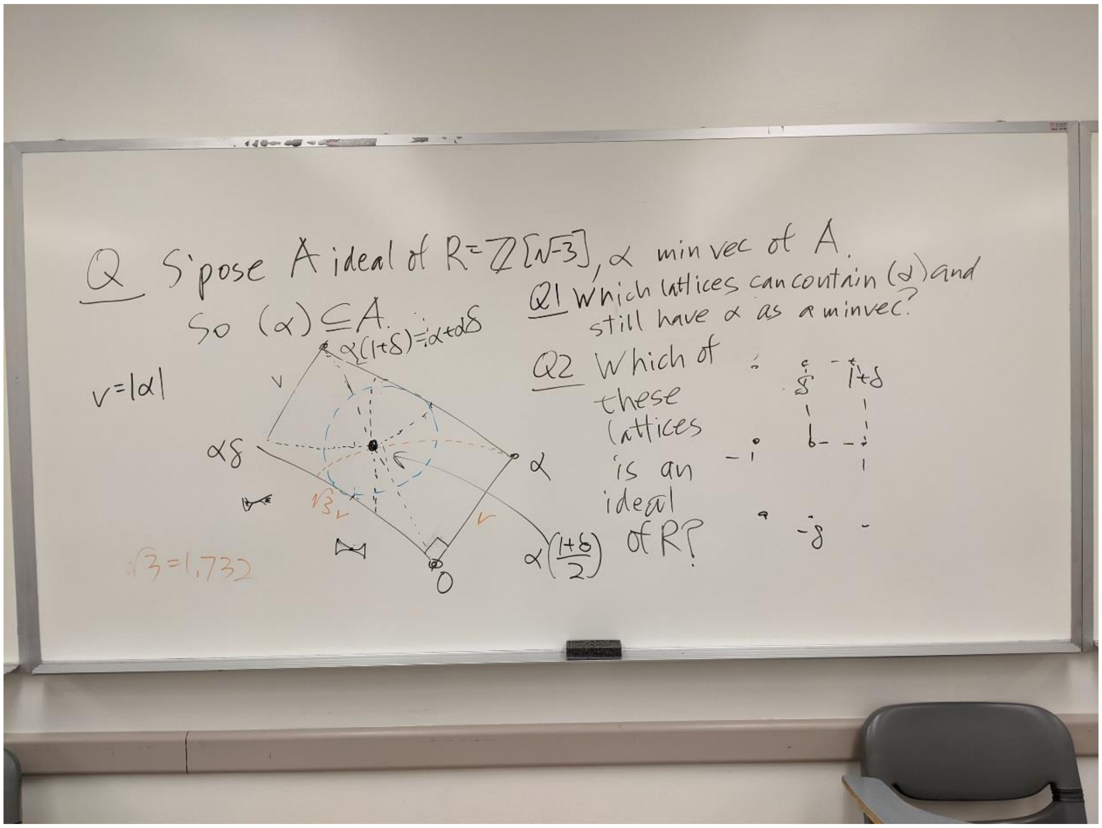
If $\gamma \in A$, $n \geq 1$

Interior of disk of rad $\frac{1}{n} v$ around $\frac{1}{n}\gamma$ contains no elt of A except $\frac{1}{n}\gamma$.

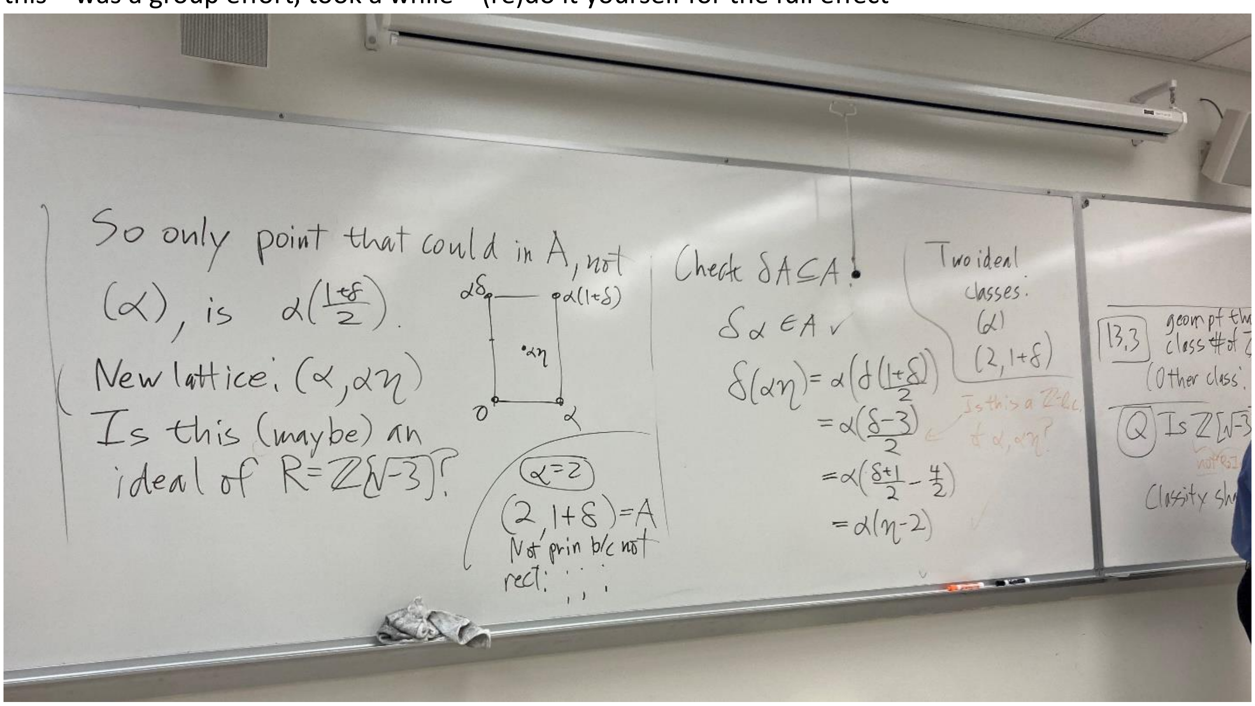
$n=1$

$\beta < v$

γ



this ^ was a group effort, took a while – (re)do it yourself for the full effect



Ideal mult

Ideals multiply like #s in $\mathbb{Z}$! And unique factor!

A, B ideals of R

Defn $AB = \left\{ \sum_{\text{finite sum}} a_i b_i \;\middle|\; a_i \in A,\ b_i \in B \right\}$

Facts

① If $A = (\alpha_1, \dots, \alpha_k)$, $B = (\beta_1, \dots, \beta_m)$ then $AB = (\alpha_i \beta_j)_{1 \le i \le k,\ 1 \le j \le m}$

② $(\alpha)(\beta) = (\alpha\beta)$

③ If $A = (\alpha)$, then $AB = \alpha B$.

12.5: Compare:

$\pi\bar{\pi} = p$ or p^2

Main Lem

$R =$ RoI oi Q#F, A ideal of R

Then $A\bar{A} = (n)$ for some $n \in \mathbb{Z}$ (R-mults)

Pf S'pose $A = (\alpha, \beta)$ (lattice)

So $\bar{A} = (\bar{\alpha}, \bar{\beta})$ "

$$\Rightarrow A\bar{A} = (\underbrace{\alpha\bar{\alpha}, \beta\bar{\beta}}_{\in\mathbb{Z}}, \bar{\alpha}\beta, \alpha\bar{\beta}) \quad \text{alg integers}$$

Also: $\bar{\alpha}\beta + \alpha\bar{\beta} \in \mathbb{Z}$

Let $n = \gcd_{\mathbb{Z}}(\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta}) \in \mathbb{Z} \cap A\bar{A}$

So $nR = (n)_R \subseteq A\bar{A}$; converse?

ETS $\bar{\alpha}\beta$, $\alpha\bar{\beta}$ div by n in R.

So ETS $\underbrace{\frac{\bar{\beta}\alpha}{n}}_{\bar{\gamma}}, \underbrace{\frac{\bar{\alpha}\beta}{n}}_{\gamma} \in R$.

Check $x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} \in \mathbb{Z}[x]$

So $\gamma, \bar{\gamma}$ are alg ints $\Rightarrow \gamma, \bar{\gamma} \in R$.