Review: Quadratic forms $Q_2 = Q_1 \circ \gamma$, $(Q_1 \sim Q_2)$.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in SL_2(\mathbb{Z})$, $[A_2, B_2, C_2] \leftarrow [A_1, B_1, C_1]$.

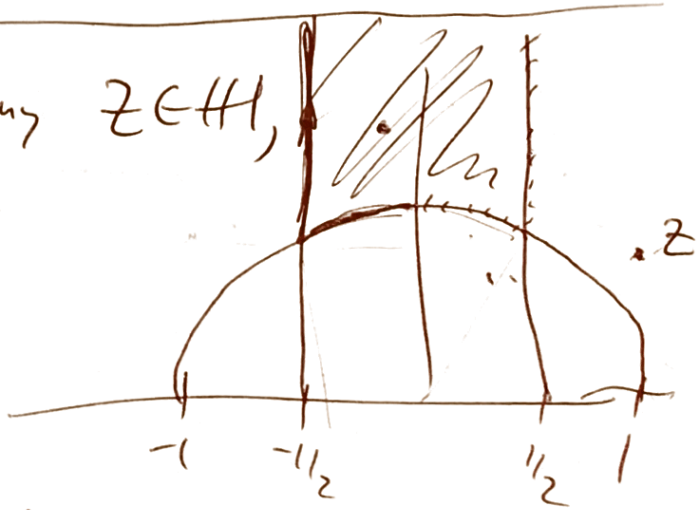
$D = B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2$ (Consider <0, definite forms).

roots: $\alpha_{Q_1} = \frac{-B_1 + \sqrt{D}}{2A_1} \in \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$.

$\Rightarrow \alpha_{Q_2} = \gamma^{-1} \circ \alpha_{Q_1}$ fractional linear transformations.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$.

Reduction algorithm: For any $z \in \mathbb{H}$,



① Use T or T^{-1}, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ to make $|\mathrm{Re}| \le \frac{1}{2}$.

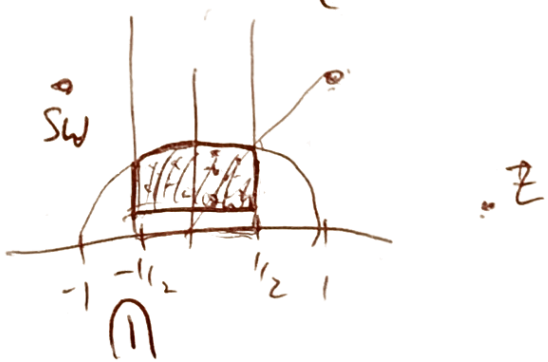
② Use $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, so make outside unit circle

fundamental domain

Then $\exists\, z_1 = \gamma \circ z \in \mathcal{F} = \{z \in \mathbb{H} \mid |\mathrm{Re}(z)| \le 1/2,\ |z| \ge 1\}$.

Thm: ↑

"pf":



① Doesn't change Im.

② Increases it.

As we move z by S & T's, If we need to apply S, it's because $z_1 (= \gamma_1 \circ z)$ is in $\left\{ w \in \mathbb{H} \;\middle|\; \begin{array}{l} |\mathrm{Re}(w)| \le \frac{1}{2}, \\ |w| \ge 1, \end{array} \mathrm{Im}(w) \ge \mathrm{Im}\, z \right\}$.

Compact ⇒ If this process went on forever, we would get a limit point. But matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, have $a, b, c, d \in \mathbb{Z}$, so action is "discrete", so there can't be limit points. So process halts, does so once in $\mathcal{F}$.

Why is resulting form Q with $\alpha_Q \in \mathcal{F}$ "reduced"?

$$\alpha = \frac{-B + \sqrt{|D|}\, i}{2A} \in \mathcal{F} \iff |\mathrm{Re}(\alpha)| = \left|\frac{-B}{2A}\right| \le \frac{1}{2}.$$

$\Leftrightarrow |B| \le |A|$. (assume Q is pos def, $Q(1,0) = A > 0$).

$\Rightarrow \boxed{|B| \le A}$.

$$\Rightarrow |\alpha|^2 = \frac{1}{4A^2}\left[B^2 + |D|\right] = \left(\frac{-B + \sqrt{|D|}\, i}{2A}\right)\left(\frac{-B - \sqrt{|D|}\, i}{2A}\right).$$

$$= \frac{1}{4A^2}\left[B^2 - D\right] = \frac{1}{4A^2}\left[B^2 - (B^2 - 4AC)\right] = \frac{+4AC}{4A^2}$$

$$= C/A.$$

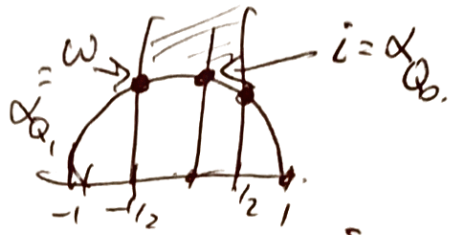
$\boxed{A \le C}$. □

Lemma: $Q=[A,B,C]$ is **reduced** if:

(pos. def) $\rightarrow$ $|B|\le A\le C$

$[14,3,2] \rightsquigarrow [2,1,13]$

Recall: $Q_2\sim Q_1 \Rightarrow D_{Q_2}=D_{Q_1}$



Converse not nec. true!

Ex 1: $Q_0=x^2+y^2$, $D=-4$. Is reduced. $\alpha_Q=i$

Are there other (neq) reduced forms of discr $D=-4$?

$-4=D=B^2-4AC$, $4AC-B^2=4$. $(\Rightarrow B^2\equiv 0(4))$.

$Q_1=[2,2,1]$

$4A^2\le 4AC=4+B^2\le 4+A^2$

$D_{Q_1}=4-4\cdot 2=-4$. **Claim:** $Q_1\sim Q_0$ $\gg$ $3A^2\le 4$

$A^2\le \frac{4}{3}$

$\Rightarrow A=1,0$

$\rightarrow$ if $A=1$, $B\not\equiv 1$, $B^2\equiv 0(4)$, $B=0$, $|B|\le A$, $B\not=1$

$-4=D=B^2-4AC$

$=0-4\cdot C \Rightarrow C=1$,

$\Rightarrow Q=[1,0,1]$.

$\rightarrow$ if ~~$A=0$~~, ~~$\rightarrow B=0$~~, $D=B^2-4AC=0$.

Lemma: If $Q=[A,B,C]$, $D_Q=-4$

$\Rightarrow Q\sim Q_0=[1,0,1]$.

$= [1,-1,1]$.

Ex 2: $Q_1 = x^2 - xy + y^2 = N(x+y\omega)$, reduced, pos def.

$D_{Q_1} = 1-4 = -3 < 0$. **Question:** Are there other reduced forms $\not\sim Q_1$?

$\alpha_{Q_1} = \frac{1+\sqrt{3}i}{2} = \omega + 1$  $\omega+1$.

If $[A,B,C]$ reduced, $|B| \le A \le C$.

& $D = B^2 - 4AC = -3 \Rightarrow$ **B odd.**

$\hookrightarrow 4A^2 \le 4AC = B^2 + 3 \le A^2 + 3$

$\Rightarrow 3A^2 \le 3 \Rightarrow A \le 1$.

$A = 1$ → $B = 1 \Rightarrow -3 = 1 - 4(1)C \Rightarrow C = 1$

~~$B = 0$~~

$B = -1 \Rightarrow -3 = (-1)^2 - 4(1)\cdot C \Rightarrow C = 1$.

$A \neq 0 \Rightarrow B \neq 0 \Rightarrow D \neq 0$

$\Rightarrow Q = [1,1,1]$ or **$Q = [1,-1,1]$, are**

$\alpha = \frac{-1+\sqrt{3}i}{2} = \omega$ $\alpha = \omega + 1$ equivalent (on $\partial\mathcal{F}$).

Need to be careful w/ boundary.

Lemma: If $Q = [A,B,C]$, $D = -3 \Rightarrow Q \sim [1,-1,1]$,

Ex3: $Q_2 = [1,0,5], = x^2+5y^2 = N(x+\sqrt{-5}y)$.

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

$D = B^2 - 4AC = 0 - 4\cdot 1\cdot 5 = -20$.

B is even.

If Q is reduced, $|B| \le A \le C$.

$4A^2 \le 4AC = 20 + B^2 \le 20 + A^2$

$\Rightarrow 3A^2 \le 20 \Rightarrow A^2 \le 6$.

$\Rightarrow A = 1$ or 2.

$A = 1 \Rightarrow B = 0 \Rightarrow C = 5 \Rightarrow Q_2 = [1,0,5]$ ←

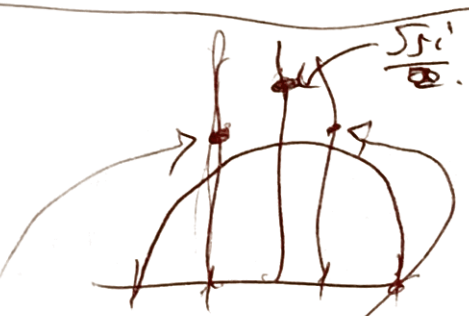
$A = 2$:

- $B = 2 \Rightarrow -20 = 2^2 - 4(2)\cdot C \Rightarrow [2,2,3]$ ←
- $B = 0 \Rightarrow -20 = 0 - 4(2)\cdot C$ ✗
- $B = -2 \Rightarrow \longrightarrow [2,-2,3]$ ←.

$\alpha_{[1,0,5]} = \frac{\sqrt{-20}i}{2} = \sqrt{5}i$

$\alpha_{[2,2,3]} = \frac{-2+\sqrt{-20}i}{4} = -\frac{1}{2} + \frac{\sqrt{5}}{2}i$

$\alpha_{[2,-2,3]} = \frac{2+\sqrt{-20}i}{4} = \frac{1}{2} + \frac{\sqrt{5}}{2}i$



Lemma: If $Q = [A,B,C]$ has $D = -20 \Rightarrow$

either $Q \sim [1,0,5]$ or $Q \sim [2,2,3]$.

Thm (Gauss): Let Q be a pos def form of discr $D<0$. Then $\exists$ finitely many reduced forms of discr D s.t. $Q \sim$ one of them.

I.e. # reduced forms of a given discriminant (<0).
is finite (finiteness of class number),

pf: If Q has discr $D = B^2 - 4AC = -|D|$.
& is reduced, $\boxed{|B| \le A \le C}$.

$$\Rightarrow 4A^2 \le 4AC = B^2 + |D| \le A^2 + |D|.$$

$$\Rightarrow \quad 3A^2 \le |D| \Rightarrow \underline{A \le \sqrt{\frac{|D|}{3}}}.$$

$\Rightarrow$ # A's is finite $\Rightarrow$ # B's finite.

(A & B ($\&D$) determine C). ∎

Review: $x^2 + y^2 = z^2$ Pythagorean Thm

primitive $\mathbb{Z}$ points $\Rightarrow$ $\begin{cases} x = u^2 - v^2 \\ y = 2uv \\ \boxed{z = u^2 + v^2} \end{cases}$

($\mathbb{Q}$ pts on S^1). (6)

Which z are hypotenuses? Rep by u^2+v^2?

Thm: $p = u^2+v^2 \iff p=2$ or $p \equiv 1(4)$.

$n = u^2+v^2 \iff \forall\, p\equiv 3(4),\ \mathrm{ord}_p(n) = \text{even}$.

Came from $\mathbb{Z}[i]$ UFD.

Easy to find (u,v) for $p\equiv 1(4)$.

What about $p = u^2-uv+v^2 \rightsquigarrow \mathbb{Z}[\omega]$.

Thm: $p = u^2-uv+v^2 \iff p=3$ or $p\equiv 1(3)$,

& general statement.

Proof from $\mathbb{Z}[\omega]$, algorithm to find u,v.

Random $a^{\frac{p-1}{3}} \equiv z \neq 1 \Rightarrow z^3 \equiv 1\ (p)$.

$z^3-1 \equiv 0(p)$

$p \mid (z^2+z+1)$.

$(z-\omega)(z-\bar{\omega})$.

$GCD_{\mathbb{Z}[\omega]}(p, z-\omega) = u+v\omega$.

General story: $n = Q(x,y)$ $\quad Q_1 \sim Q_2 \Rightarrow$

rep same numbers, reduction theory,

finiteness of class number.