Proper and improper equivalence of quadratic forms

K = field, $2 \in K^\times$, $f = f(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$, $a_{ij} = a_{ji}$ quadratic form of $\dim = n$ over K

$f(x) = {}^t x M x$, $M = {}^t M = (a_{ij})_{1 \le i,j \le n} \in M_n(K)$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\det(f) = \det(M) \in K$.

change of variables: $U \in GL_n(K)$, $(f|U)(x) = f(Ux) = {}^t x M' x$, $M' = {}^t U M U$

$\det(f|U) = \det(f) \det(U)^2$, so if f is non-degenerate $(\det(f) \neq 0)$, then:

$\det(f|U) = \det(f) \iff \det(U) = \pm 1 \iff U \in SL_n^{\pm}(K)$.

Notation: A ring, $SL_n(A) = \{ U \in GL_n(A) \mid \det(A) = 1 \}$

$SL_n^{\pm}(A) = \{ \text{---}''\text{---} \mid \det(A)^2 = 1 \}$ $\quad SL_n^{\pm}(\mathbb{Z}) = GL_n(\mathbb{Z})$

Def: $A \subset K$ subring

$O(f)(A) = \{ U \in GL_n(A) \mid f|U = f \}$ $(\subset SL_n^{\pm}(A))$ orthogonal group

$O(f)^+(A) = \{ U \in SL_n(A) \mid \text{---}''\text{---} \} = SO(f)(A)$ special ---''---

$O(f)^-(A) = O(f)(A) \setminus O(f)^+(A)$

Def: f, f' non-degenerate quadratic forms over K with $\dim(f) = \dim(f')$, $\det(f) = \det(f')$

$A \subset K$ subring

f and f' are { properly / improperly } equivalent over A if $\exists\, U \in GL_n(A)$ $f' = f|U$ and $\det(U) = \{+1, -1\}$.

In our case ($n=2$, $A = \mathbb{Z}$), the difference between proper and improper equivalence is absolutely crucial, as discovered by Gauss (and missed by Legendre).

Ex: (1) $f = \underbrace{ax^2 + bxy + cy^2}_{[a,b,c]}$ is improperly equivalent (over $\mathbb{Z}$) to $f|\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = cx^2 + bxy + ay^2 = [c,b,a]$ and $f|\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = ax^2 - bxy + cy^2 = [a,-b,c]$

and properly equivalent to $f|\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = [c,-b,a]$.

(2) $f = x^2 + 2y^2$ is both properly and improperly equivalent (over $\mathbb{Z}$) to

$f|\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = f|\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = 2x^2 + y^2$

(3) f is both properly and improperly equivalent over A to some f'

$\iff \exists\, U, U' \in GL_n(A)$, $\det(U) = 1 = -\det(U')$ $f|U = f|U'$

$\iff \exists\, T = U'U^{-1} \in O(f)^-(A)$

always true if $A = K$: $f = \langle a_1 \rangle \perp g$, $T = \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix}$

---''--- if $A = \mathbb{Z}_p$ (proof later)

Summary: proper equivalence classes over $A = SL_n(A)$-orbits for the action $f \longmapsto f|U$ on (non-degenerate) quadratic forms

---

Reduction theory of quadratic forms: process of finding "small" representatives of proper equivalence classes over $\mathbb{Z}$

Reduction Theory of Binary quadratic forms

Notation: $f = ax^2+bxy+cy^2 = [a,b,c] = f\left(\binom{x}{y}\right)$, $M = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, $\det(f) = ac - \frac{b^2}{4} = \frac{-\Delta(f)}{4}$

$\Delta(f) = b^2 - 4ac$

Def: For $\Delta \in \mathbb{Z}$, $\Delta \equiv 0,1 \pmod 4$, $\sqrt{\Delta} \notin \mathbb{Z}$

$\mathrm{Quad}(\Delta) = \{ f = [a,b,c] \mid a,b,c \in \mathbb{Z},\ b^2-4ac = \Delta,\ f \text{ positive definite if } \Delta < 0 \}$

$\cup$

$\mathrm{Quad}(\Delta)_{\mathrm{prim}} = \{$ ——— " ———, $\underbrace{\gcd(a,b,c)=1}_{f \text{ is primitive}} \}$

The group $GL_2(\mathbb{Z}) = SL_2^{\pm}(\mathbb{Z})$ acts on $\mathrm{Quad}(\Delta)$ by $(f|U)\binom{x}{y} = f\left(U\binom{x}{y}\right)$.

Def $Cl^+(\Delta) = \mathrm{Quad}(\Delta)_{\mathrm{prim}} / SL_2(\mathbb{Z})$ = the set of proper equivalence classes over $\mathbb{Z}$ of primitive binary quadratic forms of discriminant Δ (positive definite if $\Delta<0$).

Goal:
- show that $|\mathrm{Quad}(\Delta)/SL_2(\mathbb{Z})|$ is finite
- find small ("reduced") forms in each class $\mathcal{C} \in Cl^+(\Delta)$
- for each $f \in \mathrm{Quad}(\Delta)$ find a reduced form in the same class as f

---

The case $\Delta < 0$

Special elements of $SL_2(\mathbb{Z})$: $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $T^{\pm 1} = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ $\left[S^2 = -I,\ ST = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},\ (ST)^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},\ (ST)^3 = I \right]$

$f = ax^2+bxy+cy^2 = [a,b,c] \Rightarrow f|S = [c,-b,a]$, $f|T^{\pm 1} = [a, b \pm 2a, a \pm b + c]$

If $f \in \mathrm{Quad}(\Delta)$ $(\Rightarrow a,c>0)$, we can iterate the following operations:

- application of S: ensures that $a \le c$
- —— " —— $T^{\pm m}$: —— " —— $|b| \le a$

Repeated application must stop (it decreases $a \in \mathbb{Z}_{>0}$) $\Rightarrow$ yields a form with $|b| \le a \le c$.

If $a=c$: S yields $[a,b,a]|S = [a,-b,a] \Rightarrow$ can ensure $b \ge 0$

If $-b=a$: T —" — $[a,-a,c]|T = [a,a,c] \Rightarrow$ —— " ——.

Def. A positive definite real quadratic form $ax^2+bxy+cy^2$ is reduced if

(*) $|b| \le a \le c$ and [if an equality occurs, then $b \ge 0$].

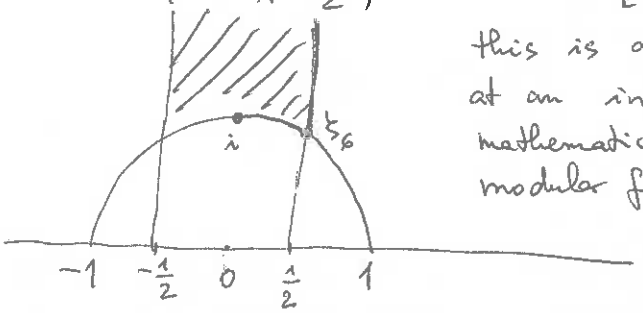
Ex: The principal form $x^2 - (\Delta/4)y^2$ (resp. $x^2+xy+\frac{1-\Delta}{4}y^2$) is reduced ($\Delta<0$).

Prop. Every $f \in \mathrm{Quad}(\Delta)$ ($\Delta<0$) is properly ($=SL_2(\mathbb{Z})$) equivalent to a reduced form, which is unique.

Pf: Existence – see above. Uniqueness: later (from a more general geometric fact).

Reformulation of (*): $f = a(x+\alpha y)(x+\bar{\alpha} y)$, $\alpha = \frac{b+i\sqrt{|\Delta|}}{2a}$, $\mathrm{Re}(\alpha) = \frac{b}{2a}$, $|\alpha| = \frac{c}{a}$

(*) $\Leftrightarrow$ $|\mathrm{Re}(\alpha)| \le \frac{1}{2}$, $|\alpha| \ge 1$ and [if an equality occurs, then $\mathrm{Re}(\alpha) \ge 0$]



this is an extremely important picture, at an intersection of several areas of mathematics: quadratic forms, elliptic functions, modular forms, non-Euclidean geometry

Exercise: Deduce that $SL_2(\mathbb{Z})$ is generated by S and $T^{\pm 1}$.

Finding reduced forms of given $\Delta(f) = \Delta < 0$: $f = [a,b,c] \in \mathrm{Quad}(\Delta)$ reduced

$\Rightarrow$ $|b| \le a \le c$, $|\Delta| = 4ac - b^2 \ge 4a^2 - a^2 = 3a^2 \Rightarrow \boxed{1 \le a \le \sqrt{|\Delta|/3}}$, $|b| \le a$,

$b \equiv \Delta \pmod 2$, $ac = \frac{b^2 + |\Delta|}{4}$ $\Rightarrow$ there are only finitely many possibilities for a, b, c

$\Rightarrow$ $|\mathrm{Quad}(\Delta)/SL_2(\mathbb{Z})| < \infty$; $\boxed{|Cl^+(\Delta)| < \infty}$.

Ex: if $|\Delta| < 12 \Rightarrow a = 1$, $b = \begin{cases} 0 & \text{if } 2 \mid \Delta \\ 1 & \text{if } 2 \nmid \Delta \end{cases} \Rightarrow f =$ the principal form.

-3	$[1,1,1]$	x^2+xy+y^2
-7	$[1,1,2]$	$x^2+xy+2y^2$
-11	$[1,1,3]$	$x^2+xy+3y^2$

-4	$[1,0,1]$	x^2+y^2
-8	$[1,0,2]$	x^2+2y^2

$|Cl^+(\Delta)| = 1$

Ex: $\Delta = -12$: $2 \mid b$, $|b| \le a \le 2$, $a \le c$, $ac = (b/2)^2 + 3$; $b = 0 \Rightarrow ac = 3$, $a = 1, c = 3$; $|b| = 2 \Rightarrow ac = 4$, $a = c = 2$, $b = 2$

$[1,0,3]$ x^2+3y^2, $[2,2,2]$ $2x^2+2xy+2y^2$ (not primitive)

$|Cl^+(-12)| = 1$

Ex: $\Delta = -15$: $2 \nmid b$, $|b| \le a \le 2$, $a \le c$, $ac = (b^2+15)/4 \Rightarrow |b| = 1$, $ac = 4$ $\quad \boxed{|Cl^+(-15)| = 2}$

$a = 1, c = 4 \Rightarrow b = 1$; $a = c = 2 \Rightarrow b = 1$ $\quad [1,1,4]$ $x^2+xy+4y^2$; $[2,1,2]$ $2x^2+xy+2y^2$

Exercise: $\Delta = -20 \Rightarrow \{\text{reduced forms in } \mathrm{Quad}(\Delta)\} = \{[1,0,5],\ [2,2,3]\}$

$\Delta = -56 \Rightarrow$ ——— " ——— $= \{[1,0,14],\ [2,0,7],\ [3,\pm 2,5]\}$

Ex: $\Delta = -23$: $2 \nmid b$, $|b| \le a \le 2$, $a \le c$, $ac = (b^2+23)/4 \Rightarrow |b| = 1$, $ac = 6$

$a = 1, c = 6 \Rightarrow b = 1$; $a = 2, c = 3, b = \pm 1$ $\quad [1,1,6]$, $[2,\pm 1,3]$ $\quad |Cl^+(-23)| = 3$

Lattices and $GL_n(\mathbb{Z})$-equivalence of quadratic forms

Data: $K \supset \mathbb{Q}$ field, F = quadratic form on $V = K^n = \left\{ \begin{pmatrix} * \\ \vdots \\ * \end{pmatrix} \mid * \in K \right\}$ (with coefficients in K)

Goal: geometric interpretation of $\underbrace{GL_n(\mathbb{Z})}_{SL_n^{\pm}(\mathbb{Z})}$-equivalence of quadratic forms on K^n equivalent to F over K

Def: a "lattice" in V is a subgroup $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n \subset V$ such that $v_1, \dots, v_n$ is a basis of V over K

The basis $\{v_i\}$ defines a quadratic form on K^n

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = f(x) = F(v_1x_1 + \cdots + v_nx_n) = F\left(\underbrace{(v_1 | \cdots | v_n)}_{M_n(K)} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right)$$

Note:
(1) If $v_i = e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow f = F$
(2) $f \sim F$ over K

For $U \in GL_n(K)$

$$(f|U)(x) = F((v_1|\cdots|v_n)Ux)$$

Another choice of basis of $L \iff$ the above action of some $U \in GL_n(\mathbb{Z}) = SL_n^{\pm}(\mathbb{Z})$:

$$(v_1|\cdots|v_n)U = (v_1'|\cdots|v_n'), \quad f'(x) = F(v_1'x_1 + \cdots + v_n'x_n) = f(Ux) = (f|U)(x)$$

$L = \mathbb{Z}v_1' \oplus \cdots \oplus \mathbb{Z}v_n'$

If $K \subset \mathbb{R}$, then $U \in SL_n(\mathbb{Z}) \iff \{v_i\}$ and $\{v_i'\}$ have the same orientation.

Summary: study of f up to $\begin{Bmatrix} GL_n(\mathbb{Z}) \\ SL_n(\mathbb{Z}) \end{Bmatrix}$-equivalence

$\Updownarrow$

study of $\begin{Bmatrix} \text{bases} \\ \text{oriented bases} \end{Bmatrix}$ of L and their relation to F

Exercise (1) $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{Z}^n$ can be completed to a basis of $\mathbb{Z}^n \iff \gcd(a_1, \dots, a_n) = 1$

$\Updownarrow$

v is primitive ($\forall m \in \mathbb{Z}_{>1} \quad v \notin m\mathbb{Z}^n$)

(2) $\{v_1, \dots, v_j\} \subset \mathbb{Z}^n$ can be completed to a basis of $\mathbb{Z}^n$

$\Updownarrow$

$A = (v_1 | v_2 | \cdots | v_j) \in M_{n \times j}(\mathbb{Z})$ ——— " ——— matrix in $GL_n(\mathbb{Z})$

$\Updownarrow$

$\gcd(j \times j\text{-minors of } A) = 1$

[Hint: use the Smith normal form $gAh = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & 0 \end{pmatrix}$]

Minkowski's reduction of positive definite quadratic forms over $\mathbb{R}$

Data: $L \subset V = \mathbb{R}^n$ lattice, $F: \mathbb{R}^n \to \mathbb{R}$ positive definite quadratic form
($\Leftrightarrow \forall M>0 \quad |\{u \in L \mid F(u) \le M\}| < \infty$)

Step 1: $M_1 = \inf_{u \in L \setminus \{0\}} F(u) = F(v_1)$ for some $v_1 \in L \setminus \{0\}$ $\Rightarrow$ v_1 primitive (can be completed to a basis of L)

Step 2: $M_2 = \inf \{F(u) \mid u \in L \setminus \{0\},\ v_1, u$ can be completed to a basis of $L\}$
$= F(v_2)$ for some v_2 such that v_1, v_2 ——— " ———

etc. $\Rightarrow L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ such that $f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = F(v_1x_1 + \cdots + v_nx_n)$ is a quadratic form on $\mathbb{R}^n$ such that:
basis $\{v_i\}$

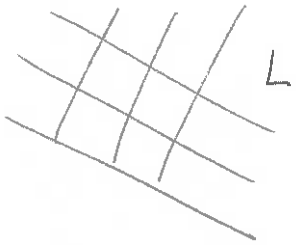
$e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j^{th}$ row

(1) f is equivalent to F over $\mathbb{R}$

(2) $\forall j = 1, \dots, n \quad f(e_j') \ge f(e_j)$ for every $e_j' \in \mathbb{Z}^n$ such that $e_1, \dots, e_{j-1}, e_j'$ can be completed to a basis of $\mathbb{Z}^n$.

The case $n=2$

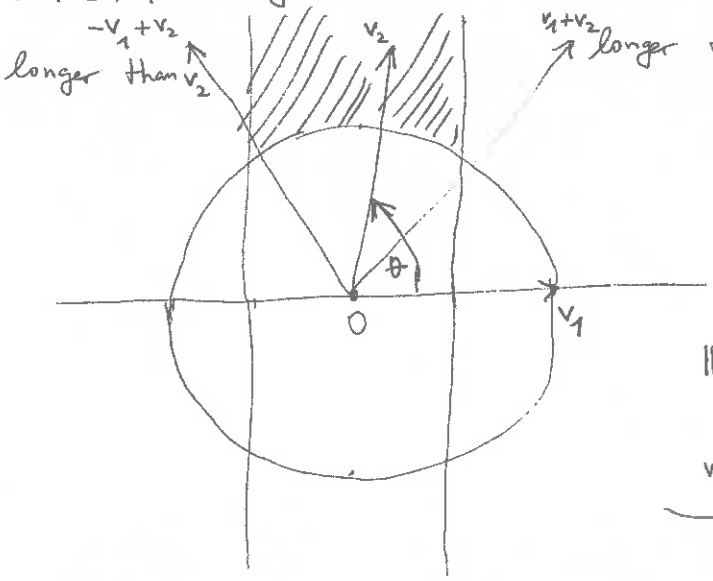
$F(x) = \|x\|^2 = x_1^2 + x_2^2 : \mathbb{R}^2 \to \mathbb{R}$, $L \subset \mathbb{R}^2$ lattice



Step 1: v_1 = the shortest vector among $L \setminus \{0\}$

Step 2: v_2 = ——— " ——— $L \setminus \mathbb{R}v_1$

Also want: (v_1, v_2) positively oriented : $0 < \theta = \sphericalangle v_1 v_2 < \pi$



$\|v_2\| \ge \|v_1\|$

Fact: $L = \mathbb{Z}v_1 + \mathbb{Z}v_2$

Pf: if not, $\exists\, \ell \ge 2$, $k \in \mathbb{Z}$, $|k| \le \ell/2$

$\frac{kv_1 + v_2}{\ell} = v \in L \setminus \mathbb{R}v_1$

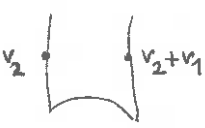
$\Downarrow$

$\|v\| < \frac{k}{\ell}\|v_1\| + \frac{\ell}{\ell}\|v_2\| \le \frac{1}{2}(\|v_1\| + \|v_2\|) \le \|v_2\|$

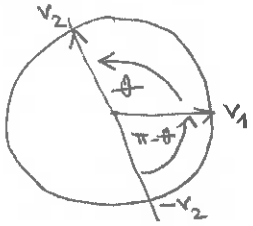
$v_2 \notin \mathbb{R}v_1$ — contradiction

We end up with the same picture as before!

Possible non-uniqueness: (a) $\|v_2\| > \|v_1\|$ ($\Rightarrow v_1$ unique up to $\pm v_1$)
but $\|v_2 \pm v_1\| = \|v_2\|$



(b) $\|v_2\| = \|v_1\|$: can replace (v_1, v_2) by $(-v_2, v_1)$



Complex formulas: $\mathbb{R}^2 = \mathbb{C}$, $\binom{u}{v} \longmapsto u+vi$, $\left\|\binom{u}{v}\right\|^2 = |u+vi|^2$

For every lattice $L \subset \mathbb{C}$ $\exists$ basis $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ such that

- $\mathrm{Im}\left(\frac{w_2}{w_1}\right) > 0$ ($\Leftrightarrow$ (w_1, w_2) is positively oriented)
- $|w_1| = \min\{|u|;\ u \in L \setminus \{0\}\}$, $|w_2| = \min\{|u|;\ u \in L \setminus \mathbb{R}w_1\}$

$\Downarrow$

$\tau = \frac{w_2}{w_1}$ satisfies $\mathrm{Im}(\tau) > 0$, $|\mathrm{Re}(\tau)| \le \frac{1}{2}$, $|\tau| \ge 1$

τ is unique except: $|\mathrm{Re}(\tau)| = \frac{1}{2}$ (can replace τ by $\tau \pm 1$)

OR

$|\tau| = 1$ (can replace τ by $-\frac{1}{\tau}$)

Cor. Every positive definite real quadratic form $Ax^2 + Bxy + Cy^2$ is $SL_2(\mathbb{Z})$-equivalent to a unique reduced form

$f\binom{x}{y} = |xw_1 + yw_2|^2 = |w_1|^2 |x + \tau y|^2 = ax^2 + bxy + cy^2$ τ as above

(and $\mathrm{Re}(\tau) \ge 0$ if $|\mathrm{Re}(\tau)| = \frac{1}{2}$ or $|\tau| = 1$)

The right action of $U \in GL_2(\mathbb{R})$ on $\mathbb{R}$-bases $(z_2 | z_1)$ of $\mathbb{C} = \mathbb{R}^2$ $(z_2|z_1) \longmapsto (z_2|z_1)U$ defines a left action of $GL_2(\mathbb{R})$ on $\left\{\frac{z_2}{z_1}\right\} = \mathbb{C} \setminus \mathbb{R}$ by transposition: $\binom{z_2}{z_1} \longmapsto {}^tU \binom{z_2}{z_1} = \binom{az_2 + bz_1}{cz_2 + dz_1}$, $z = \frac{z_2}{z_1} \longmapsto \frac{az+b}{cz+d}$

the action of $GL_2(\mathbb{R})^+ = \{U \in GL_2(\mathbb{R}) \mid \det(U) > 0\}$ leaves stable both

$\mathcal{H} = \mathcal{H}^+ = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ and $\mathcal{H}^- = \{z \in \mathbb{C} \mid \mathrm{Im}(z) < 0\}$

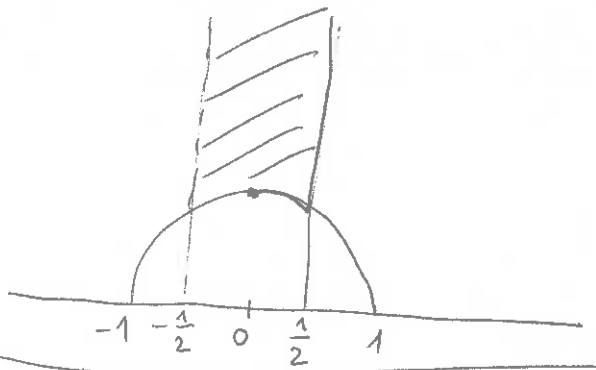
$\mathcal{H}$ with this action of $SL_2(\mathbb{R}) \subset GL_2(\mathbb{R})^+$

= the Poincaré model of the non-Euclidean plane

$\{$lattices $L \subset \mathbb{C}\}/\mathbb{C}^* =$ $GL_2(\mathbb{Z})$-orbits in $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^+ \cup \mathcal{H}^-$

$=$ $SL_2(\mathbb{Z})$-orbits in $\mathcal{H}$

$= \{\tau \in \mathcal{H} \mid |\mathrm{Re}(\tau)| \le \frac{1}{2}, |\tau| \ge 1,$ if equality $\Rightarrow \mathrm{Re}(\tau) \ge 0\}$



Exercise: A positive definite real quadratic form $ax^2 + bxy + cy^2 = f(x,y)$ satisfies $|b| \le a \le c$ $\Leftrightarrow$ $f(1,0) \le f(0,1) \le f(1,\pm 1)$

$\Leftrightarrow$ the 3 smallest values of $f|_{\mathbb{Z}^2 \setminus \{0\}}$ are $f(1,0) \le f(0,1) \le f(-\mathrm{sgn}(b), 1)$

Hermite's reduction of positive definite quadratic forms over $\mathbb{R}$

Let $f(x)=\sum_{i,j=1}^{n} f_{ij}x_ix_j$, $f_{ij}=f_{ji}\in\mathbb{R}$ $(n\geq 1)$, $\det(f)=\det\left((f_{ij})_{1\leq i,j\leq n}\right)$ $\underbrace{\sum_1^n x_i^2}$

Assume: f is positive definite: $\forall a\in\mathbb{R}^n$ $f(a)>0$ $(\Longrightarrow \exists c>0\ \forall a\in\mathbb{R}^n\ |f(x)|\geq c\|x\|^2)$

Def: $M_f=\inf_{a\in\mathbb{Z}^n\smallsetminus\{0\}} f(a)$ $\left(=\min_{a\in\mathbb{Z}^n\smallsetminus\{0\}} f(a)\right.$, thanks to $\nearrow$ $\left.\right)$

If $M_f=f(a)\Longrightarrow$ $a\in\mathbb{Z}^n$ is primitive $(\forall m\in\mathbb{Z}_{>1}\ a\notin m\mathbb{Z}^n)$

$\Longrightarrow \exists$ basis of $\mathbb{Z}^n$ of the form $\mathbb{Z}a+\cdots+\cdot$

$\Longrightarrow$ after replacing f by $f|U$ for some $U\in SL_n(\mathbb{Z})$ $a=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$

$\Longrightarrow$ $M_f=f_{11}\Rightarrow f=f_{11}\left(x_1+\frac{f_{12}}{f_{11}}x_2+\cdots+\frac{f_{1n}}{f_{11}}x_n\right)^2+g(x_2,\dots,x_n)$

Furthermore, after replacing x_1 by $x_1+\sum_{j>1} m_jx_j$ $(m_j\in\mathbb{Z})$ we get $\forall j>1$ $\left|\frac{f_{1j}}{f_{11}}\right|\leq\frac{1}{2}$.

Def. Any (positive definite) f of $\dim=n=1$ is Hermite reduced.

If $n>1$, f is Hermite reduced if $f=f_{11}\left(x_1+\sum_{j>1}\frac{f_{1j}}{f_{11}}x_j\right)^2+g(x_2,\dots,x_n)$ and

(1) $f_{11}=M_f$, (2) $\forall j>1$ $|f_{1j}/f_{11}|\leq\frac{1}{2}$, (3) $g(x_2,\dots,x_n)$ (of $\dim=n-1$) is Hermite reduced

---

Cor. Every positive definite f is properly equivalent over $\mathbb{Z}$ (by $U\in SL_n(\mathbb{Z})$) to a Hermite reduced form

---

Prop. f Hermite reduced $\Longrightarrow f=t_1(x_1+c_{12}x_2+\cdots+c_{1n}x_n)^2+t_2(x_2+c_{23}x_3+\cdots+c_{2n}x_n)^2+\cdots+t_nx_n^2$,

$\forall i,j$ $0<t_j\leq\frac{4}{3}t_{j+1}$, $|c_{ij}|\leq\frac{1}{2}$ ("Siegel's condition with parameters $\left(\frac{4}{3},\frac{1}{2}\right)$")

$\det(f)=t_1\cdots t_n$

Pf. By definition, $t_1=M_f$, $|c_{1j}|=\left|\frac{f_{1j}}{f_{11}}\right|\leq\frac{1}{2}$, $t_2=M_g$. If $b'=\begin{pmatrix}b_2\\\vdots\\b_n\end{pmatrix}\in\mathbb{Z}^{n-1}\smallsetminus\{0\}$,

$g(b')=M_g\Rightarrow\exists\, b_1\in\mathbb{Z}$ $|b_1+c_{12}b_2+\cdots+c_{1n}b_n|\leq\frac{1}{2}\Rightarrow b=\begin{pmatrix}b_1\\b'\end{pmatrix}\in\mathbb{Z}^n\smallsetminus\{0\}$ satisfies

$t_1=M_f\leq f(b)\leq t_1\left(\frac{1}{2}\right)^2+\underbrace{g(b')}_{t_2}\Longrightarrow t_1\leq\frac{4}{3}t_2$, etc.

Cor. f positive definite $\Longrightarrow$ $\boxed{M_f\leq\det(f)^{1/n}\left(\frac{4}{3}\right)^{\frac{n-1}{2}}}$ (Hermite's bound)

Pf. We can assume f Hermite reduced. Then $\det(f)=t_1\cdots t_n$, $M_f=t_1$,

$t_j\geq\left(\frac{3}{4}\right)^{j-1}t_1\Rightarrow\det(f)\geq t_1^n\left(\frac{3}{4}\right)^{1+2+\cdots+(n-1)}=\left(t_1\left(\frac{3}{4}\right)^{\frac{n-1}{2}}\right)^n$.

Cor. For each $d\in\mathbb{Z}_{>0}$ and $n\geq 1$ there are only finitely many proper equivalence classes over $\mathbb{Z}$ ($=SL_n(\mathbb{Z})$-orbits) of classically integral ($\forall i,j$ $f_{ij}\in\mathbb{Z}$) positive quadratic forms of $\dim=n$, $\det=d$.

Exercise: For $d=1$, $n\leq 5$ there is only one such class (that of $x_1^2+\cdots+x_n^2$).

Minkowski's bound: $K_R=\{x\in\mathbb{R}^n\mid f(x)\leq R\}$, $\mathrm{vol}(K_R)=\frac{R^{n/2}}{\det(f)^{1/2}}\frac{\Gamma\left(\frac{1}{2}\right)^n}{\Gamma\left(\frac{n}{2}+1\right)}$.

$\mathrm{vol}(K_{R_0})=2^n\Longleftrightarrow R_0^n/\det(f)=\left(\frac{4}{\pi}\right)^n\Gamma\left(\frac{n}{2}+1\right)^2$.

Minkowski's Thm $\Longrightarrow$ $\boxed{M_f\leq R_0=\det(f)^{1/2}\frac{4}{\pi}\Gamma\left(\frac{n}{2}+1\right)^{2/n}}$ (Minkowski's bound)

Exercise: $\left(\frac{4}{3}\right)^{\frac{n-1}{2}}<\frac{4}{\pi}\Gamma\left(\frac{n}{2}+1\right)^{2/n}\Longleftrightarrow n\leq 8$.

Reduction theory for $[a,b,c] = ax^2+bxy+cy^2$, $\Delta > 0$

Let $f = f_0 = [A_0, B_0, C_0]$, $A_0, B_0, C_0 \in \mathbb{Z}$, $\Delta = \Delta(f) = B_0^2 - 4A_0C_0 > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$

The Reduction sequence $(f_0, f_1, f_2, \dots)$ of f_0 consists of the following properly ($= SL_2(\mathbb{Z})$-) equivalent forms $f_n = [A_n, B_n, C_n]$, where $f_{n+1} = f_n \left| \begin{pmatrix} 0 & -1 \\ 1 & d_n \end{pmatrix} \right.$ for suitable $d_n \in \mathbb{Z}$: write $f_n(x,y) = C_n(\beta_n x + y)(\beta_n' x + y)$ with $\beta_n = \frac{B_n + \sqrt{\Delta}}{2C_n}$, where $\alpha_n = |\beta_n|$ come from the continued fraction of $\alpha_0 = |\beta_0| = [a_0, \dots, a_n, \alpha_{n+1}]$, and $\forall n \geq 0$ $\beta_n \beta_{n+1} < 0$. This sign change is necessary, since the matrices $\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$ appearing in the theory of continued fractions have $\det = -1$ and lead to improperly equivalent quadratic forms.

Dictionary

Quadratic forms

$$f_n(x_n, y_n) = A_n x_n^2 + B_n x_n y_n + C_n y_n^2 =$$
$$= C_n(\beta_n x_n + y_n)(\beta_n' x_n + y_n) =$$
$$= k \, (x_n \; y_n) \begin{pmatrix} \mu_n \\ \mu_{n+1} \end{pmatrix} (\mu_n' \;\; \mu_{n+1}') \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$
$$= f_{n+1}(x_{n+1}, y_{n+1})$$

$$(x_n \; y_n) \begin{pmatrix} \mu_n \\ \mu_{n+1} \end{pmatrix} = (x_n \; y_n) \begin{pmatrix} d_n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu_{n+1} \\ \mu_{n+2} \end{pmatrix}$$
$$\underbrace{\qquad\qquad}_{(x_{n+1} \;\; y_{n+1})}$$

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & d_n \end{pmatrix} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix}, \quad f_n \left| \begin{pmatrix} 0 & -1 \\ 1 & d_n \end{pmatrix} \right. = f_{n+1}$$

$$A_{n+1} x_{n+1}^2 + B_{n+1} x_{n+1} y_{n+1} + C_{n+1} y_{n+1}^2 =$$
$$= f_n(-y_{n+1}) \, x_{n+1} + d_n y_{n+1}) =$$
$$= C_n x_{n+1}^2 + (2d_n C_n - B_n) x_{n+1} y_{n+1} + (\dots) y_{n+1}^2$$

$\boxed{A_{n+1} = C_n}$ $\boxed{B_{n+1} + B_n = 2d_n C_n}$

Continued fractions

$$\beta_n = \frac{B_n + \sqrt{\Delta}}{2C_n} = \frac{\mu_n}{\mu_{n+1}}, \quad \beta_n' = \frac{B_n - \sqrt{\Delta}}{2C_n} = \frac{2A_n}{B_n + \sqrt{\Delta}}$$

$\beta_n = (-1)^n s \alpha_n$, $s \in \{\pm 1\}$, $\alpha_n > 0$ ($\Longrightarrow \beta_n \beta_{n+1} < 0$)

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} (\alpha_{n+1})$$

$$\beta_n = \underbrace{(-1)^n s \, a_n}_{d_n} - \frac{1}{\beta_{n+1}} = \begin{pmatrix} d_n & -1 \\ 1 & 0 \end{pmatrix} (\beta_{n+1})$$

$$\begin{pmatrix} \mu_n \\ \mu_{n+1} \end{pmatrix} = \begin{pmatrix} d_n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu_{n+1} \\ \mu_{n+2} \end{pmatrix}, \quad \boxed{d_n = (-1)^n s \, a_n}$$

$$\beta_{n+1} = \frac{B_{n+1} + \sqrt{\Delta}}{2C_{n+1}}, \quad \beta_{n+1}' = \frac{B_{n+1} - \sqrt{\Delta}}{2C_{n+1}}$$

$$N(\beta_n) = \beta_n \beta_n' = \frac{A_n}{C_n}$$

$$N(\beta_{n+1}) = \beta_{n+1} \beta_{n+1}' = \frac{A_{n+1}}{C_{n+1}} = \frac{C_n}{C_{n+1}}$$

$$\alpha_{n+1} = |\beta_{n+1}| = \left| \frac{2A_{n+1}}{B_{n+1} - \sqrt{\Delta}} \right| = \left| \frac{2C_n}{B_{n+1} - \sqrt{\Delta}} \right|$$

$\alpha_0 = [a_0, \dots, a_n, \alpha_{n+1}]$ is the continued fraction of $\alpha_0 \Longleftrightarrow$ [illegible]

$$\boxed{|B_{n+1} - \sqrt{\Delta}| < |2C_n|} \iff \forall n \geq 0 \quad \alpha_{n+1} > 1$$

$$\forall n \geq 0 \quad \beta_n \beta_{n+1} < 0$$

$$\boxed{(B_n + \sqrt{\Delta})(B_{n+1} - \sqrt{\Delta}) < 0} \iff (C_n \beta_n)(C_{n+1} \beta_{n+1}') = C_n^2 \frac{\beta_n}{\beta_{n+1}} < 0$$

These 4 properties (together with $\Delta(f_{n+1})=\Delta(f_n)$) determine f_{n+1} uniquely from f_n:

Def. Given $f=[a,b,c]$ with $\Delta(f)=\Delta$, its **right neighbour** $f'=Rf=[a',b',c']$ is the unique form f' with $\Delta(f')=\Delta$ such that

(1) $a'=c$ (2) $b'+b\equiv 0 \pmod{2c}$ (3) $|b'-\sqrt{\Delta}|<|2c|$ (4) $(b+\sqrt{\Delta})(b'-\sqrt{\Delta})<0$.

($\Rightarrow$ $f'=f\left|\begin{pmatrix}0&-1\\1&d\end{pmatrix}\right.$, $b+b'=2cd'$, hence f' is properly equivalent to f).

Def. The **reduction sequence** of f is $\{f_n\}_{n\ge 0}$, $f_{n+1}=Rf_n$, $f_0=f$.
It is given by the above formulas $f_n=[A_n,B_n,C_n]$.

Def. f is **reduced** if the number $\alpha=\left|\underbrace{\frac{b+\sqrt{\Delta}}{2c}}_{\beta}\right|$ is reduced.

Prop. $f=[a,b,c]$ is reduced $\iff$ $0<b<\sqrt{\Delta}$, $\sqrt{\Delta}-b<|2a|,|2c|<\sqrt{\Delta}+b$, $\Delta=\Delta(f)$
($\Rightarrow$ $0<|a|,b,|c|<\sqrt{\Delta}$, so there are only finitely many such f with given Δ).

Pf. $\alpha=\beta/u$, $u=\pm 1$; α is reduced $\iff$ $\alpha>1>-\alpha'>0\iff$

$\iff \frac{b+\sqrt{\Delta}}{2cu}>1>\frac{\sqrt{\Delta}-b}{2cu}>0 \Rightarrow \frac{\sqrt{\Delta}}{cu}>1+0=1,\ \frac{b}{cu}>1-1=0 \Rightarrow \begin{matrix}0<cu<\sqrt{\Delta}\\0<b<\sqrt{\Delta}\end{matrix}$

$\Downarrow$

$\left.\begin{matrix}b+\sqrt{\Delta}>2cu=|2c|>\sqrt{\Delta}-b>0\\(2a)(2c)=(b+\sqrt{\Delta})(b-\sqrt{\Delta})\end{matrix}\right\}\Rightarrow \sqrt{\Delta}-b<|2a|<b+\sqrt{\Delta}$. Conversely, if these inequalities are satisfied, then $\alpha=\beta/u$ with $u=\operatorname{sgn}(c)$ and

$1<\alpha=\frac{b+\sqrt{\Delta}}{2cu}=\frac{b+\sqrt{\Delta}}{|2c|}$ and $0<-\alpha'=\frac{-b+\sqrt{\Delta}}{2cu}=\frac{-b+\sqrt{\Delta}}{|2c|}<1$.

Given $f=f_0=[A_0,B_0,C_0]$, $\Delta(f)=\Delta$, let $\beta_0=\frac{B_0+\sqrt{\Delta}}{2C_0}$, $\alpha_0=|\beta_0|$.

Theory of continued fractions $\Rightarrow$ (1) $\alpha_0=[a_0,\dots,a_{k-1},\overline{a_k,\dots,a_{k+\ell-1}}]$

(2) Writing $\alpha_0=[a_0,\dots,a_n,\alpha_{n+1}]$, $\alpha_n=[a_n,a_{n+1},\dots]$, then
$\forall n\ge k$ α_n has a purely periodic continued fraction

$\Updownarrow$

$\forall n\ge k$ α_n is reduced $\iff$ f_n is reduced

(3) $\forall n\ge k$ $\alpha_n=[a_n,\dots,a_{n+\ell-1},\alpha_{n+\ell}]$, $\alpha_{n+\ell}=\alpha_n \Rightarrow f_{n+\ell}=f_n$.

Thm. Given $\Delta\in\mathbb{Z}$, $\Delta\equiv 0,1 \pmod 4$, $\Delta>0$, $\sqrt{\Delta}\notin\mathbb{Z}$:

(1) the reduction sequence of any $f=[a,b,c]$ with $\Delta(f)=\Delta$ ultimately becomes a cycle of reduced forms, (2) there are only finitely many such cycles ($\Rightarrow$ only finitely many classes of f).

(3) Two forms with $\Delta(f)=\Delta(f')=\Delta$ are properly ($=SL_2(\mathbb{Z})$-) equivalent

$\Updownarrow$

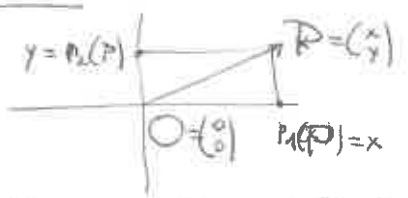
their reduction sequences end with the same cycle.

(Ex: $f_0\to f_1\to f_2=f_8\to f_3\to f_4\to f_5\to f_6\to f_7\to f_2$; $f_2,\dots,f_8$ reduced)

Pf: We only need to show $\Rightarrow$ in (3), assuming f,f' are reduced. This will be done by a geometric argument. It also follows from the fact that $[\exists k,\ell\ \alpha_k=\alpha'_\ell \iff \exists\ M\in GL_2(\mathbb{Z})\ \ \alpha=M(\alpha')]$.

Extreme points of irrational lattices $L \subset \mathbb{R}^2$

$\mathbb{R}^2 \xrightarrow{p_i} \mathbb{R}$, $p_1\begin{pmatrix}x\\y\end{pmatrix} = x$, $p_2\begin{pmatrix}x\\y\end{pmatrix} = y$ two projections



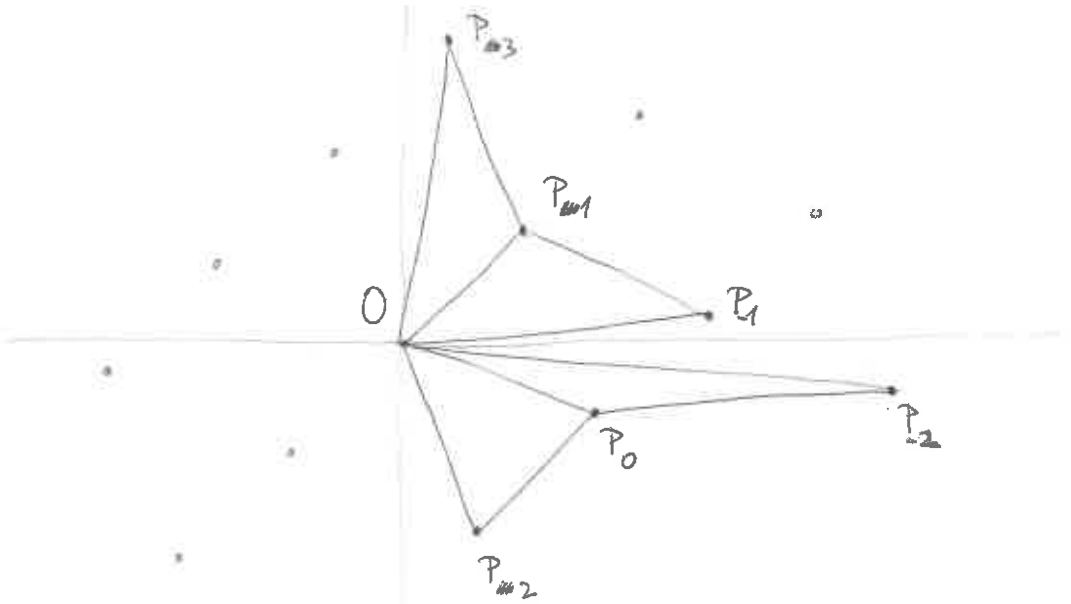
Assume: $L \subset \mathbb{R}^2$ lattice, $L \cap (\mathbb{R} \times \{0\}) = L \cap (\{0\} \times \mathbb{R}) = \{0\}$

$\Uparrow\Downarrow$

the subgroups $pr_1(L)$, $pr_2(L) \subset \mathbb{R}$ are not discrete $\Rightarrow$ they are dense in $\mathbb{R}$, hence

$\forall \varepsilon > 0 \quad \exists \begin{pmatrix}x\\y\end{pmatrix}, \begin{pmatrix}x'\\y'\end{pmatrix} \in L \quad 0 < |x|, |y'| < \varepsilon$.

Def. the set of **extreme points** of L is $L_{ext} = \left\{ \begin{pmatrix}u\\v\end{pmatrix} \in L \setminus \{0\} \;\middle|\; \text{there is no } \begin{pmatrix}x\\y\end{pmatrix} \in L \setminus \{0\} \text{ such that } \begin{matrix}|x| < |u|\\ |y| < |v|\end{matrix} \right\}$



Def. The **neighbours** $N_\pm(P_0) = P_{\pm 1}$ of $P_0 = \begin{pmatrix}u_0\\v_0\end{pmatrix} \in L_{ext}$ with $u_0 > 0$ are the points $P_{-1} = \begin{pmatrix}u_{-1}\\v_{-1}\end{pmatrix} \in \left\{ \begin{pmatrix}x\\y\end{pmatrix} \in L \setminus \{0\} \;\middle|\; |y| < |v_0| \right\}$ with minimal $u_{-1} > 0$

$P_1 = \begin{pmatrix}u_1\\v_1\end{pmatrix} \in \{$ —— " —— $| 0 < x < u_0 \}$ —— " —— $|v_1|$

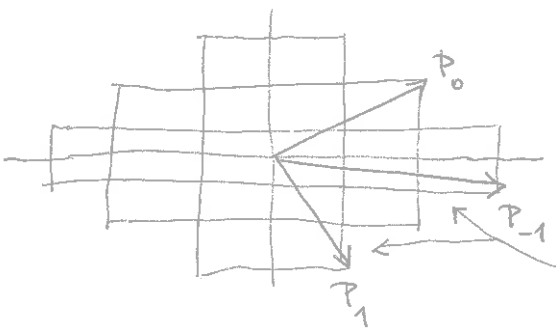
Properties: (1) $v_0 v_{-1} < 0$ (otherwise we could replace P_{-1} by $P_{-1} - P_0$)

$v_0 v_1 < 0$ (—— " —— P_0 by $P_0 - P_1$)

(2) $P_{\pm 1} \in L_{ext}$

(3) $N_+(P_{-1}) = P_0 = N_-(P_1)$

(there are no points of L here



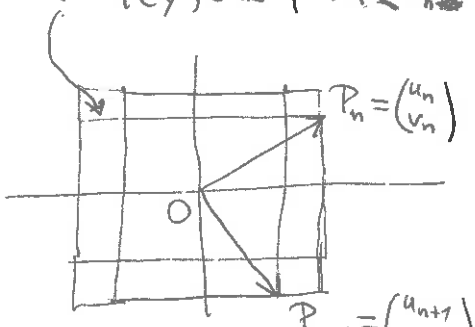
Cor: we obtain a sequence $\{P_n\} \subset L_{ext}$, $N_\pm(P_n) = P_{n\pm1}$)

$P_n = \begin{pmatrix}u_n\\v_n\end{pmatrix}$, $\forall n \in \mathbb{Z}$ $\quad u_n > u_{n+1} > 0$, $\quad |v_n| < |v_{n+1}|$

$v_n v_{n+1} < 0$

(4) $\forall n \quad \underline{L = \mathbb{Z}P_n + \mathbb{Z}P_{n+1} = L_n}$

Pf: the centrally symmetric convex set $K = \{\binom{x}{y} \in \mathbb{R}^2 \mid |x| \leq u_{n+1},\ |y| \leq v_{n+1}\}$ satisfies $K \cap L = \{0\}$



$0 < u_{n+1} < u_n$
$|v_{n+1}| > |v_n|$
$v_{n+1} v_n < 0$

$\Downarrow$ Minkowski's thm

$$\underbrace{\frac{1}{4}\mu(K)}_{u_n |v_{n+1}|} \leq \mu(\mathbb{R}^2/L) = \frac{\mu(\mathbb{R}^2/L_n)}{[L : L_n]}$$

$$u_n |v_{n+1}| < \mu(\mathbb{R}^2/L_n) = |u_n v_{n+1} - u_{n+1} v_n| = \pm u_n |v_{n+1}| + u_{n+1} |v_n| < 2 u_n |v_{n+1}|$$

$\Rightarrow \quad [L : L_n] < 2 \Rightarrow L = L_n$.

---

(5) The bases (P_n, P_{n+1}) and (P_{n+1}, P_{n+2}) have different orientations

$$\Rightarrow \quad \begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_{n+1} \\ P_{n+2} \end{pmatrix} \qquad \text{for some } a_n \in \mathbb{Z},\ a_n \geq 1.$$

Cor: $\lim_{n \to +\infty} |v_n| = \lim_{n \to -\infty} u_n = +\infty \Rightarrow \lim_{n \to -\infty} |v_n| = \lim_{n \to +\infty} u_n = 0$.

---

(6) $L_{ext} = \{\pm P_n \mid n \in \mathbb{Z}\}$ (if $\binom{x}{y} \in L_{ext}, x > 0 \Rightarrow \exists n \ u_{n+1} < x \leq u_n \overset{\text{Q extreme}}{\Longrightarrow} x = u_n \Rightarrow y = v_n$)

Lattices arising from $\mathbb{Q}(\sqrt{\Delta}) \xrightarrow{\sigma = (\sigma_1, \sigma_2)} \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$

If $\gamma, \delta \in \mathbb{Q}(\sqrt{\Delta})$ are linearly independent over $\mathbb{Q}$, then $L = \sigma(\mathbb{Z}\gamma + \mathbb{Z}\delta) \subset \mathbb{R}^2$ is a lattice such that $L \cap (\mathbb{R} \times \{0\}) = L \cap (\{0\} \times \mathbb{R}) = \{0\}$.

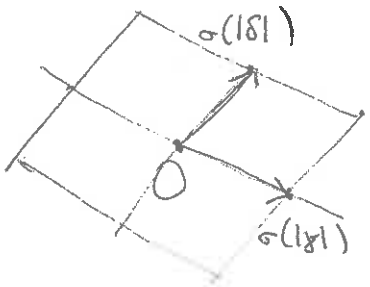
(7) $L_{ext} = \{\pm P_n = \pm\sigma(\lambda_n) \mid n \in \mathbb{Z}\}$, $\lambda_n \in \mathbb{Z}\gamma + \mathbb{Z}\delta$,

$\forall n \in \mathbb{Z} \quad 0 < \lambda_{n+1} < \lambda_n$, $|\lambda'_{n+1}| > |\lambda'_n|$, $\lambda'_{n+1}\lambda'_n < 0 \Rightarrow \alpha_n = \lambda_n/\lambda_{n+1}$ is reduced,
$\alpha_n > 1 > -\alpha'_n > 0$.

(8) Conversely, if $|\gamma/\delta|$ is reduced, then the pair

$$(\underbrace{\sigma(\gamma)}_{\binom{x}{y}}, \underbrace{\sigma(|\delta|)}_{\binom{z}{t}}) = (P_n, P_{n+1}) \qquad \text{for some } n \in \mathbb{Z}$$

$x > z > 0$, $yt < 0$, $|y| < |t|$



Let $f(x,y) = k(\gamma x + \delta y)(\gamma' x + \delta' y) \qquad (k \in \mathbb{Z} \setminus \{0\})$.

the statement (7) $\Rightarrow$ f is (properly) equivalent to a reduced form.

the statements $\{(8)\} \Rightarrow$ every pair of reduced forms $\{(5)\}$

properly equivalent to f belongs to the same reduction cycle (to get the signs right requires an argument, which is left as an exercise).

Finding all classes of forms with given $\Delta(f) = \Delta > 0$ $(\sqrt{\Delta} \notin \mathbb{Z})$

Step 1. Find all reduced forms of $\Delta(f) = \Delta$

Step 2. Decompose the set of reduced forms into disjoint reduction cycles. Each cycle corresponds to one class.

Rmk. The principal form $f_0 = \begin{cases} x^2 - (\Delta/4)y^2 \\ x^2 + xy - \frac{\Delta-1}{4}y^2 \end{cases}$ is never reduced $(\Delta > 0)$, except when $\Delta = 5$.

If $\Delta \neq 5$, then $\exists\, k \in \mathbb{Z}$ $0 < k < \sqrt{\Delta} < k+2$, $k \equiv \Delta \pmod 2$. The reduced form $f = [1, k, \frac{k^2-\Delta}{4}]$ is then properly equivalent to the principal form $f_0 = f\left|\begin{pmatrix} 1 & -\lfloor k/2 \rfloor \\ 0 & 1 \end{pmatrix}\right.$.

Recall: $[a,b,c]$ is reduced $\iff \left|\frac{b+\sqrt{\Delta}}{2c}\right|$ is reduced $\quad (\Delta = b^2 - 4ac > 0)$

$\iff 0 < b < \sqrt{\Delta}$, $\sqrt{\Delta} - b < |2a|, |2c| < \sqrt{\Delta} + b$

Ex: $\Delta = 17$: $0 < b \leq 4$, $b \equiv \Delta \equiv 1 \pmod 2 \Rightarrow b = 1, 3$;

$-ac = \frac{\Delta - b^2}{4}$, $4 - b < \sqrt{17} - b < |2a|, |2c| < \sqrt{17} + b < 5 + b$

$\beta = \frac{b+\sqrt{17}}{2c}$, $\alpha = |\beta|$

b	1	1	3	3	3	3
a	2	-2	1	-1	2	-2
c	-2	2	-2	2	-1	1
β	$\frac{\sqrt{17}+1}{-4}$	$\frac{\sqrt{17}+1}{4}$	$\frac{\sqrt{17}+3}{-4}$	$\frac{\sqrt{17}+3}{4}$	$\frac{\sqrt{17}+3}{-2}$	$\frac{\sqrt{17}+3}{2}$
α	$\frac{\sqrt{17}+1}{4}$	$\frac{\sqrt{17}+1}{4}$	$\frac{\sqrt{17}+3}{4}$	$\frac{17+3}{4}$	$\frac{\sqrt{17}+3}{2}$	$\frac{\sqrt{17}+3}{2}$

$4 < \sqrt{17} < 5$

$$\underbrace{\frac{\sqrt{17}+1}{4}}_{\alpha_0=\beta_0} = [1, \underbrace{\frac{4}{\sqrt{17}-3}}_{\alpha_1=-\beta_1} = \frac{\sqrt{17}+3}{2}] = [1, 3, \underbrace{\frac{2}{\sqrt{17}-3}}_{\alpha_2=\beta_2} = \frac{\sqrt{17}+3}{4}] = [1,3,1,\underbrace{\frac{4}{\sqrt{17}-1}}_{\alpha_3=-\beta_3} = \frac{\sqrt{17}+1}{4}] =$$

$(\alpha_3 = \alpha_0$, but $\beta_3 = -\beta_0$, since $2 \nmid 3)$

$$= [1,3,1,1,\underbrace{\alpha_1}_{\beta_4}] = [1,3,1,1,3,\underbrace{\alpha_2}_{-\beta_5}] = [1,3,1,1,3,1,\underbrace{\alpha_3}_{\beta_6=\beta_0}] = [\overline{1,3,1}]$$

One cycle of reduced forms:

$$[-2,1,2] \xrightarrow{R} [2,3,-1] \xrightarrow{R} [-1,3,2] \xrightarrow{R} [2,1,-2] \xrightarrow{R} [-2,3,1] \xrightarrow{R} [1,3,-2]$$

$\beta_0 \qquad \beta_1 \qquad \beta_2 \qquad \beta_3 = -\beta_0 \qquad \beta_4 = -\beta_1 \qquad \beta_5 = -\beta_2$

$|Cl^+(17)| = 1$

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix}$, eigenvalues $4 \pm \sqrt{17}$

$\varepsilon = 4 + \sqrt{17}$, $N(\varepsilon) = -1 = (-1)^3$.

$\Delta = 4 \cdot 15 = 60$, $7 < \sqrt{\Delta} < 8$: $0 < b < \sqrt{\Delta}$, $b \equiv \Delta \pmod 2 \Rightarrow 2 \mid b$, $b/2 = 1, 2, 3$

$-ac = 15 - (b/2)^2$, $\sqrt{15} - b/2 < |a|, |c| < \sqrt{15} + b/2 < 4 + b/2$

$b/2$	1	2	3	3	3	3
a	X	X	± 1	± 2	± 3	± 6
c	X	X	∓ 6	∓ 3	∓ 2	∓ 1
α	X	X	$\frac{\sqrt{15}+3}{6}$	$\frac{\sqrt{15}+3}{3}$	$\frac{\sqrt{15}+3}{2}$	$\frac{\sqrt{15}+3}{1}$

$\beta = \frac{(b/2)+\sqrt{15}}{c}$, $|\beta| = \alpha$

$3 < \sqrt{15} < 4$

$\frac{\sqrt{15}+3}{6} = [1, \frac{6}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{1}] = [1, 6, \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6}] = [1, 6, 1, 6, \ldots] = [\overline{1,6}]$

$\alpha_0 = \beta_0$ $\quad \alpha_1 = -\beta_1$ $\quad \alpha_0 = \alpha_2 = \beta_2 = \beta_0$

corresponds to $[-1, 6, 6] \xrightarrow{R} [6, 6, -1] \xrightarrow{R}$ (R)

change of sign

$\alpha_0 = -\beta_0$ $\quad \alpha_1 = \beta_1$

corresponds to $[1, 6, -6] \xrightarrow{R} [-6, 6, 1] \xrightarrow{R}$ (R)

Similarly,

$\frac{\sqrt{15}+3}{3} = [2, \frac{3}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{2}] = [2, 3, \frac{2}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{3}] = [\overline{2,3}]$

$\alpha_0 = \beta_0$ $\quad \alpha_1 = -\beta_1$ $\quad \alpha_0 = \alpha_2 = \beta_2 = \beta_0$

corresponds to $[-2, 6, 3] \xrightarrow{R} [3, 6, -2] \xrightarrow{R}$ (R)

and the change of sign

$\alpha_0 = -\beta_0$ $\quad \alpha_1 = \beta_1$ $\quad \alpha_2 = -\beta_2$

corresponds to $[2, 6, -3] \xrightarrow{R} [-3, 6, 2] \xrightarrow{R}$ (R)

There are 4 classes, $|\mathcal{C}\ell^+(60)| = 4$.

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 6 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}$

eigenvalues satisfy $\lambda^2 - 8\lambda + 1 = 0$

$\varepsilon = 4 + \sqrt{15}$, $N(\varepsilon) = 1 = (-1)^2$