~~Spring~~ Fall 2024 — The geometry of numbers. LC 109 9:40 — 10:30.

- Index cards.
- Syllabus quickly.
- Seminar on Friday afternoons.
- 8/28 and 8/30. Grad courses for the spring.
- PANTS, 9/21-22, Wake Forest (w/funding!)

What is "the geometry of numbers"?

Roughly speaking:

(1) Various NT problems can be described in terms of lattices. ~~point counting problems~~

(2) Various methods can be used to count, ~~to~~ or prove facts about, lattice points.

Examples. (1) Let $K/\mathbb{Q}$ be a number field, deg n.
[Check: do people know alg NT?]

Then $\mathcal{O}_K \cong \mathbb{Z}^n$ as abelian groups.

Have $\mathcal{O}_K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ (r: # real embeddings, s: # ~~pairs~~ cpx embeddings, $n = r + 2s$.)

Image is a lattice.

Minkowski's First Theorem. Given $\Gamma \subseteq \mathbb{R}^n$ lattice.

K = convex centrally symmetric body.

If $\mathrm{vol}(K) > 2^n \mathrm{vol}(\mathbb{R}^n/\Gamma)$, then K contains a nonzero vector in Γ.

Now, we have $\mathrm{vol}(\mathbb{R}^n/\Gamma) = \sqrt{|\mathrm{Disc}(K)|}$.

Consequence:

$$|\mathrm{Disc}(K)| \geq \left(\frac{\pi}{4}\right)^{2s} \left(\frac{n^n}{n!}\right)^2 .$$

Further consequence:

If $K \neq \mathbb{Q}$, then $\mathrm{Disc}(K) \neq 1$.

Further further consequence.

If $K \neq \mathbb{Q}$, at least one prime ramifies in K.

Example 2.

Look at integral binary quadratic forms

$f(u,v) = au^2 + buv + cv^2$.

$\mathrm{Disc}(f) = b^2 - 4ac$, tells you definite or indefinite.

Consider two such forms equivalent if there is an invertible integer change of variables sending one to another.

e.g. $u^2 + v^2 \longrightarrow (u+3v)^2 + v^2 = u^2 + 6uv + 10v^2$

(Typically also demand det = 1 and not -1.)

$f(\alpha x + \beta y, \gamma x + \delta y) = g(x,y)$

$\alpha\delta - \beta\gamma = 1$.

Some facts:

* If $D \neq 0$, there are only finitely many equivalence classes of discriminant D.

  Write $h(D)$, the class number.

788. 1.3.

Then $h(D) = 1$ sometimes, e.g. if $D = -4$.
$h(D) > 1$ often.

If $D < 0$ and $h(D) = 1$ then
$D \in \{-3, -4, -7, -8, \ldots, -67, -163\}$.

Conjectured (more or less) by Gauss 1798.
Proved: Heegner 1952.

Also if $D < 0$, $h(D) \approx \sqrt{|D|}$ on average.

Algebraic interpretation:

Gauss described a "higher composition law".

Essentially, equivalence classes of disc D = ab. gp.

It turns out, for negative D, is equivalent to the <u>ideal class group</u> of disc D.

Dirichlet class number formula:

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field,

$$\zeta_{\mathbb{Q}(\sqrt{D})}(s) := \sum_{\underline{a} \trianglelefteq \mathcal{O}_K} (N\underline{a})^{-s} = \zeta(s) \cdot L(s, \chi_D)$$

$$= \zeta(s) \cdot \sum_n \left(\frac{d}{n}\right) n^{-s}.$$

~~Then,~~

$$\cancel{\operatorname{Res}_{s=1} \zeta_{\mathbb{Q}(\sqrt{D})}(s) = L(1, \chi_D) = \Big\{}$$

788: 1.4 = 2.1.

Then,

$$h(D) = \begin{cases} \cancel{}\ \dfrac{w \cdot \sqrt{|D|}}{2\pi} L(1, \chi) & (D < 0) \\ \dfrac{\sqrt{D}}{2 \log(\varepsilon)} L(1, \chi) & (D > 0) \end{cases}$$

w: 2, 4, or 6 – number of units

ε: essentially a fundamental unit $\frac{1}{2}(t + u\sqrt{D})$ where (t, u) min. solution to $t^2 - Du^2 = 4$.

We'll prove this! Elegant application of the theory.

Example 3. Counting cubic fields.

Let $N_3(X) := \#\{K : [K:\mathbb{Q}] \leq 3,\ |\mathrm{Disc}(K)| < X\}$.

Davenport – Heilbronn Theorem. (1971)

We have

$$N_3(X) \sim \frac{1}{3\zeta(3)} X.$$

Indeed, $N_3(X) = \frac{1}{3\zeta(3)} X + \frac{4(1+\sqrt{3})\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} X^{5/6} + O(X^{2/3}(\log X)^3)$

788 1.5 = 2.2.

Two parts of the proof.

The "Delone - Faddeev correspondence". There exists a bijection

{ cubic rings (commutative } ⟷ { integral binary cubic forms, up to invertible change of variable }.

It preserves the discriminant, among much else.

Count those cubic rings which are maximal irreducible nondegenerate.

So how to do that? This is a lattice point counting problem, a messy one but a doable one.

Goal for the course: describe several of the algebraic theorems;
develop several of the analytic techniques.

Slide: B. HCL IV p. 56.
B - Ho Coregular spaces.
B - S Avg rank bounded.

Some basics around lattice point counting.

Def. A (complete) lattice in $\mathbb{R}^n$ is a set Λ s.t.

(1) Λ is an abelian group under addition;

(2) $\Lambda \cong \mathbb{Z}^n$ ("Λ is of rank n")

(3) The induced topology is discrete

(4) Λ spans $\mathbb{R}^n$ over $\mathbb{R}$.

Note that (3) $\longleftrightarrow$ (4) given (1) and (2).

The covolume of Λ is $\begin{cases} \text{the volume of } \mathbb{R}^n/\Lambda \text{ under the quotient measure} \\ \text{the volume of a fundamental region} \\ |\det(v_1, \ldots, v_n)|, \text{ where } \{v_1, \ldots, v_n\} \text{ any basis.} \end{cases}$

Here a fundamental region is

$D := a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$, $a_i \in [0,1)$.
$\{v_1, \ldots, v_n\}$ any basis.

It has the property that any $v \in \mathbb{R}^n$ can be written uniquely as $v = d + \lambda$, where $d \in D$, $\lambda \in \Lambda$.

Example. Let K be a NF of degree n.

Write $n = r + 2s$, $r = \#$ real embeddings

$s = \#$ cpx conj embeddings.

Have $\mathcal{O}_K \hookrightarrow \mathbb{R}^n$

$$a \longrightarrow (\underbrace{\rho_1(a), \dots, \rho_r(a)}_{\text{real embeddings}}, \sigma_1(a), \dots, \sigma_s(a))$$

Here if $\sigma : \mathcal{O}_K \hookrightarrow \mathbb{C}$ is an embedding so is

$\mathcal{O}_K \hookrightarrow \mathbb{C} \underset{\substack{\uparrow \\ \text{conjugation}}}{\longrightarrow} \mathbb{C}$ choose one from each pair.

And use $\mathbb{C} \cong \mathbb{R}^2$ by $a + bi \to (a, b)$.

Then $\mathcal{O}_K$ embeds as a lattice in $\mathbb{R}^n$.

We have $\operatorname{covol}(\mathcal{O}_K) = 2^{-s} |\operatorname{Disc}(K)|^{1/2}$.

why 2^{-s}?

Ex. $\mathbb{Z}[i]$. Choose the integral basis $\{1, i\}$

$1 \longrightarrow 1 + 0i \sim (1, 0)$

$i \longrightarrow 0 + 1i \quad (0, 1)$.

$\operatorname{covol}(\mathcal{O}_K) = 1$.

The usual computation is $\operatorname{Disc}(K) = \det \begin{pmatrix} \sigma_1(1) & \sigma_1(i) \\ \sigma_2(1) & \sigma_2(i) \end{pmatrix}^2$

Do a change of basis. $= \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2$.

Minkowski's theorems.

Convex Body Theorem. Given $\Lambda \subseteq \mathbb{R}^n$ lattice, U a convex centrally symmetric body in $\mathbb{R}^n$.

Then if $\mathrm{vol}(U) > 2^n \cdot \mathrm{covol}(\Lambda)$, U contains a nonzero vector ~~of~~ Λ.

<u>Successive Minima.</u> Let $B(0, r)$ be the ball of radius r centered at 0.

For $i = 1, \dots, n$, the <u>ith successive minimum</u> of Λ is

$$\lambda_i := \inf \left\{ \lambda : \begin{array}{l} B(0,\lambda) \text{ contains } i \text{ linearly} \\ \text{independent vectors of } \Lambda \end{array} \right\}.$$

So: λ_1 is the minimum length of a vector

λ_n is the minimum radius of a ball containing a ~~basis~~ spanning set for Γ.

<u>Minkowski's Second Theorem.</u>

The successive minima satisfy

$$\frac{2^n}{n!} \mathrm{covol}(\Lambda) \le \lambda_1 \lambda_2 \cdots \lambda_n \cdot \mathrm{vol}(B(0,1))$$

$$\le 2^n \mathrm{covol}(\Lambda).$$

Or more succinctly,

$$\lambda_1 \lambda_2 \cdots \lambda_n \asymp_n \mathrm{covol}(\Lambda).$$

~~Note that covol(Λ)~~

4.4.

Above: Any lattice.

Counting lattice points in a general region.

<u>Idea</u>: Given $U \subseteq \mathbb{R}^n$, $\#\{U \cap \mathbb{Z}^n\} \sim \mathrm{Vol}(U)$.

Same idea as Gauss Circle.

<u>Theorem</u>. (Davenport's Lemma) Let $U \subseteq \mathbb{R}^n$ be nice.

Then, $\#\{U \cap \mathbb{Z}^n\} = \mathrm{Vol}(U) + \max_{\tilde{U}}(\mathrm{Vol}(\tilde{U}))$,

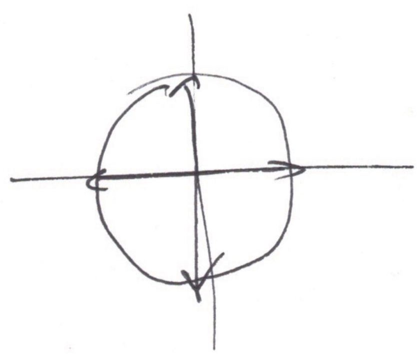
where $\tilde{U}$ ranges over all projections of U onto any proper subset of the coordinate axes.

(For the projection onto 0-dim space, take Vol = 1.)

<u>Ex</u>. (Gauss Circle Again)

U = circle of radius r.

$\pi r^2 + O(r)$.



An ellipse of major axis M, minor axis m.

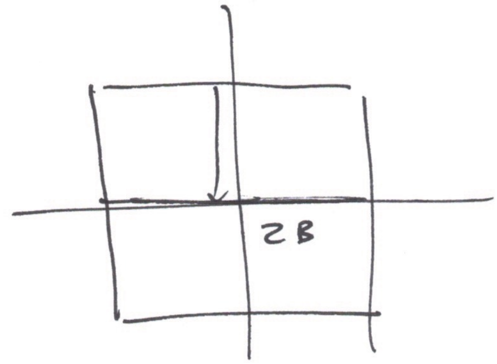
Then get $\pi \cdot Mm + O(M)$.

Gets worse as $m \to 0$, as <u>it has to</u>.

4.5 ≈ 5.1.

Ex. How many lattice points in the square $[-B, B]^2$?

$$= 4B^2 + O(B).$$



This is sharp.

If N is an integer,

$$[-N, N]^2 \cap \mathbb{Z}^2 = (2N+1)^2$$

$$[-N+\varepsilon, N-\varepsilon]^2 \cap \mathbb{Z}^2 = (2N-1)^2.$$

Squares are actually worse.

(4 finished here)

The # of points in the n-sphere of radius r is

$$\underbrace{\mathrm{Vol}\left(\mathrm{Ball}_{n\text{-dim}}(0,1)\right)}_{\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}} \cdot r^n + O(r^{n-1}).$$

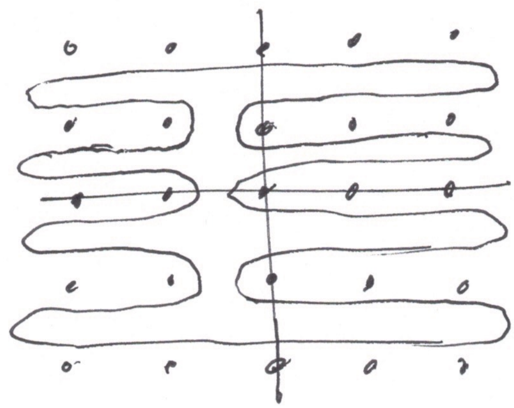
The hyperbola problem: useless if applied naively.

4.6. = 5.2.

What is "nice"?

Davenport's condition:
(0) Closed + bounded.
(1) Any line parallel to one of the n coordinate axes intersects U in a set of points which, if not empty, consists of at most h intervals.
(Error term implicit consts depend on h.)
(2) Same is true for all projections.

What we're ruling out:



etc.

If U is closed and bounded, then +U satisfies the above w/ implied const depending on U.

Bhargava's version:
(1) implied if U defined by a <u>bounded</u> <u>number</u> of polynomial inequalities of <u>bounded</u> degree.

[Same true under any triangular, unipotent transformation.]

4.7. = 5.3 → 6.1 .

Poisson summation formula.

We have

$$\sum_{v \in \mathbb{Z}^n} f(v) = \sum_{w \in \mathbb{Z}^n} \hat{f}(w),$$

where $\hat{f}(w) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i x \cdot w} dx$.

Example. Let $f(v)$ = characteristic function of a ball of radius 1

Then $\hat{f}(w) = |w|^{-n/2} J_{n/2}(|w|)$

~~So in 2-dim~~

and $|\hat{f}(w)| \ll (1+|w|)^{\frac{-n-1}{2}}$.

The right side of the above doesn't converge.
How to make it converge?

Smooth with a bump function.

Gaussian $f(x) = e^{-|x|^2}$. Then $\hat{f}(w) = e^{-|w|^2}$.

Both effectively supported on a ball of radius $O(1)$.

write $f_t(x) = t^{-n} e^{-|x/t|^2}$
Supported on a ball of radius $O(t)$.

Then $\hat{f}_t(w) = e^{-|tw|^2}$.

6.2

Assume, morally

ϕ supported on a ball of radius t

$\hat{\phi}$ supported on a ball of radius $\ll \frac{1}{t}$

ϕ has total mass 1

$|\hat{\phi}(\omega)| \leq 1$,

f_t essentially satisfies them.

But: No such function exists!

Theorem. In $\mathbb{R}^n$, there exists a smooth, nonnegative function ψ supported in $B(0,1)$.

May assume it has total mass 1.

Then, $|\hat{\psi}(\omega)| \ll_A (1+|\omega|)^{-A}$ for every A.

Take $\phi(t) = t^{-n} \cdot \psi(x/t)$.

Then above is true but $\hat{\phi}$ only morally supp on a ball of radius $\ll \frac{1}{t}$.

$$|\hat{\phi}(\omega)| \ll_A (1+|\omega t|)^{-A}$$

6.3

5.4.

~~**Assume**: ϕ is supported on a ball of radius $C \cdot t$~~

~~$\hat{\phi}$ on a ball of radius C/t.~~

~~ϕ has total mass 1.~~

~~$|\hat{\phi}(w)| \leq 1$.~~

~~$0 \leq \phi(x) << t^{+n}$~~

~~These assumptions are impossible to satisfy.~~

~~But f_t effectively satisfies them.~~

Let $g(v) = \begin{pmatrix} \text{char fn. of ball} \\ \text{of radius } R + t \end{pmatrix} * \phi$,

where $\psi_1 * \psi_2(x) := \int_{\mathbb{R}^n} \psi_1(t)\, \psi_2(x-t)\, dt$.

Then $g(v) = \begin{cases} 1 \text{ inside a ball of radius } R \\ \text{Between 0 and 1 in between.} \\ 0 \text{ outside a ball of radius } \cancel{R+2Ct}\ R+2t \end{cases}$

And $\hat{g}(v) = \widehat{\begin{pmatrix} \text{char fn. of ball} \\ \text{of radius } R + t \end{pmatrix}} \cdot \hat{\phi}$.

$$\sum_{v \in \mathbb{Z}^n} g(v) = \sum_{w \in \mathbb{Z}^n} \hat{g}(w).$$

The right side.

in two dimensions.

$$\hat{g}(0) = \pi \cdot (R + t)^2 \cdot \hat{\phi}(0)$$

$= \pi (R+t)^2$, the expected main term.

6.4

Get an error $\displaystyle\sum_{0 \neq w \in \mathbb{Z}^n} \left| \widehat{\left(\begin{matrix}\text{char. fn. of} \\ \text{ball of radius } R+t\end{matrix}\right)}(w) \right| \, |\hat{\phi}(w)|$

$$\ll \sum_{0 \neq w \in \mathbb{Z}^n} (R+t)^n \left(1 + |(R+t)w|\right)^{-\frac{n-1}{2}} |\hat{\phi}(w)|$$

$$\ll_A R^n \sum_{0 \neq w \in \mathbb{Z}^n} (1 + R|w|)^{-\frac{n-1}{2}} (1 + t|w|)^{-A}.$$

Solve by dyadic subdivision: $N = 1, 2, 4, 8, \ldots$

There are $\asymp N^n$ points with $|w| \in [N, 2N]$.

Case 1: $N \ll \frac{1}{t}$, then $(1 + t|w|)^{-A} \ll 1$

(trivial bound)

Get a contribution

$$\ll_A R^n \sum_{\substack{N = 1, 2, 4, 8, \ldots \\ N \ll \frac{1}{t}}} (RN)^{-\frac{n-1}{2}} \cdot N^n$$

$$\ll_A R^{\frac{n-1}{2}} \sum_{\substack{N = 1, 2, 4, 8, \ldots \\ N \ll 1/t}} N^{\frac{n-1}{2}} \ll \left(\frac{R}{t}\right)^{\frac{n-1}{2}}.$$

Case 2: $N \gg \frac{1}{t}$, then $(1+t|u|)^{-A} \ll (Nt)^{-A}$.

Get a contribution

$$R^{n} \sum_{N:\text{ power of } 2} (RN)^{\frac{-n-1}{2}} \cdot (Nt)^{-A} \cdot N^{n}$$

$u = Nt$, $N \gg 1/t$

$$\ll R^{n} \sum_{u:\text{ power of } 2} \left(R\frac{u}{t}\right)^{\frac{-n-1}{2}} u^{-A} \left(\frac{u}{t}\right)^{n}$$

$$\ll \left(\frac{R}{t}\right)^{\frac{n-1}{2}} \sum_{u} u^{-\frac{n-1}{2}-A} \ll \left(\frac{R}{t}\right)^{\frac{n-1}{2}}.$$

So:

$$\#\left\{\begin{array}{l}\text{lattice pts in circle}\\ \text{of radius } R\end{array}\right\} \le \pi(R+t)^2 + O\left(\frac{R}{t}\right)^{1/2}$$

$$= \pi R^2 + O(Rt) + O\left(\frac{R}{t}\right)^{1/2}$$

$$Rt = \frac{R^{1/2}}{t^{1/2}} \Rightarrow t^{3/2} = R^{-1/2} \Rightarrow t = R^{-1/3}.$$

Get $\pi R^2 + O(R^{2/3})$.

Lower bound: approximate within.

In dimension n:

$$\#\left\{\begin{array}{l}\text{lattice pts}\\ \text{in } n\text{-sphere of radius } R\end{array}\right\} \le \mathrm{Vol}_n(B(0,1))\, R^{n} + O(R^{n-1}t) + O\left(\left(\frac{R}{t}\right)^{\frac{n-1}{2}}\right)$$

Choose $t = R^{\frac{-n-1}{n+1}} \Rightarrow O\left(R^{(n-1)\left(1-\frac{1}{n+1}\right)}\right)$

2.4.

Def. An <u>integral</u> <u>binary</u> <u>quadratic</u> <u>form</u> is an expression of the form

$$ax^2 + bxy + cy^2 . \qquad \begin{matrix} a,b,c & \text{integers} \\ x,y & \text{variables} \end{matrix}$$

<u>Questions</u>. Which integers does it represent?

e.g. x^2+y^2 : already discussed this.

x^2-y^2 : Similar to divisor problem.
$(x-y)(x+y)$

$5x^2+7xy+13y^2$. (??)

Def. Given $ax^2+bxy+cy^2$: (i.e. fix a,b,c)

(1) It is positive <u>definite</u> if it only represents ~~positive~~ nonnegative numbers.

(2) Its discriminant is b^2-4ac .

<u>Easy exercise</u>.

(1) It is positive definite $\longleftrightarrow$ $\overset{D=}{b^2-4ac} \le 0$ and it represents at least one positive number.

(2) It has a multiple root if and only if $D=0$.

(3) The discriminant is always $\equiv 0, 1 \pmod 4$.

(4) Can a form be indefinite but represent only positive integers when $x,y \in \mathbb{Z}$?

Binary quadratic forms. (Sources: Cox, Granville)

Define as $ax^2 + bxy + cy^2$.

A function $\mathbb{Z}^2 \to \mathbb{Z}$ or $\mathbb{C}^2 \to \mathbb{C}$. (not a homomorphism)
$\mathbb{R}^2 \to \mathbb{R}$ etc.)

Representations.

An integer m is represented by f if there are ~~coprime~~ x and y with $f(x,y) = m$.

It is properly represented if there are coprime x and y.

Example. $x^2 + 5y^2$ represents 20, but not properly.

Equivalence (the lowbrow version).

Def. Two forms $f(x,y)$ and $g(x,y)$ are properly equivalent if there are $\alpha, \beta, \gamma, \delta$ with

$$f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$$

and

$$\alpha\delta - \beta\gamma = 1.$$

(Lose "properly": allow -1.)

Example. Let $g(x,y) = x^2 + 5y^2$.
Let

$$\begin{aligned} f(x,y) &= g(x, 3x+y) \\ &= x^2 + 5\cdot(3x+y)^2 \\ &= 46x^2 + 30xy + 5y^2. \end{aligned}$$

Then $f \sim g$.

Proposition. Proper equivalence is an equivalence relation.

Proof. (1) $f \sim f$. Clear.

(2) Suppose $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ $\quad \alpha\delta - \beta\gamma = 1$.

Then, $f(\delta x - \beta y, -\gamma x + \alpha y)$

$$= g(\alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y))$$

$$= g([\alpha\delta - \beta\gamma]x, [\alpha\delta - \beta\gamma]y) = g(x,y)$$

and $\delta\alpha - (-\beta)(-\gamma) = 1$.

(3) Now suppose $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ $\quad \alpha\delta - \beta\gamma = 1$

$g(x,y) = h(rx + sy, tx + uy)$ $\quad ru - st = 1$

Then, (ugh) do it yourself.

Proposition. If f and g are properly equivalent, then they represent the same integers.

Proof. Suppose $f \sim g$ so that $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$. Suppose f represents m, i.e. $f(X,Y) = m$ for some integers X, Y.

Then $g(\alpha X + \beta Y, \gamma X + \delta Y) = m$ and so we are done.

Similarly, if g represents m, then f does, because it's an equivalence relation.

3.3.1

Equivolence (the highbrow version).

Def. $SL_2(\mathbb{Z})$ is the set of 2×2 metrices $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ with deteminant $\alpha\delta - \beta\gamma = 1$.

Prop. $SL_2(\mathbb{Z})$ is a group.

Proof. * matrix mult. is associative

* inverse $\begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}$ also in $SL_2(\mathbb{Z})$.

Prop. There is a right action of $SL_2(\mathbb{Z})$ on BQFs given by

$$(f\circ g)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Remarks. (1) Think of BQFs as functions $\mathbb{Z}^2 \to \mathbb{Z}$, natural to represent elements of $\mathbb{Z}^2$ as column vectors.

(2) what is being claimed is that

(a) $f\circ I_2 = f$. (trivial)

(b) $(f\circ g)\circ g' = f\circ(gg')$

(3) There is not a left action. Suppose we wrote $g\circ f$ instead of $f\circ g$. Then, would have

$$(gg')\circ f = g'\circ(g\circ f). \quad [\text{UGH.}]$$

Writing actions on the right corresponds to contravariance.

Proof (of 2b)

$$\begin{aligned}
(f\circ(gg'))\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) &= f\left((gg')\begin{pmatrix} x \\ y \end{pmatrix}\right) \\
&= f\left(g\left(g'\begin{pmatrix} x \\ y \end{pmatrix}\right)\right) \\
&= (f\circ g)\left(g'\begin{pmatrix} x \\ y \end{pmatrix}\right) \\
&= ((f\circ g)\circ g')\begin{pmatrix} x \\ y \end{pmatrix}.
\end{aligned}$$

3.4. Idea: Follows directly from the fact that $SL_2(\mathbb{Z})$ acts on $\mathbb{Z}^2$.

Exercise. For an example, verify you do get a right action and not a left one.

Disadvantage of highbrow approach:

Lots of parentheses. Eyes can glaze over.

Advantage: Immediate that equivalence is an equiv. rel'n.

Question. Are all BQFs equivalent?

Definition. The discriminant of a binary quadratic form $ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Proposition / Exercise.

If $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ then

$\operatorname{Disc}(f) = (\alpha\delta - \beta\gamma)^2 \operatorname{Disc}(g)$.

To say exactly the same thing:

If $f = g \circ \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, then

$\operatorname{Disc}(f) = (\det g)^2 \operatorname{Disc}(g)$.

In particular, if $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ then $\operatorname{Disc}(f) = \operatorname{Disc}(g)$.

But. This is not required.

Example. Let $g(x,y) = x^2 + y^2$, $\operatorname{Disc}(g) = -4$.

$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}$.

Then $\left(g \circ \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = g\left(\begin{pmatrix} 2x \\ 5y \end{pmatrix}\right) = 4x^2 + 25y^2$.

$\operatorname{Disc}(g) = -\cancel{4}00$.

$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$. $\left(g \circ \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = g(x + 2y, 0)$

$= (x+2y)^2 = x^2 + 4xy + 4y^2$

$\operatorname{Disc} = 0$.

3.5.

Q. How many BQFs are there of discriminant -4, up to equivalence?

Ex. $2x^2 + 6xy + 5y^2$. Disc $= -4$.

Equivalent to

$$2(x-y)^2 + 6(x-y)y + 5y^2 \qquad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ y \end{pmatrix}$$

$$= 2x^2 - 4xy + 2y^2 + 6xy - 6y^2 + 5y^2$$

$$= 2x^2 + 2xy + y^2.$$

Equivalent to

$$2x^2 + 2x(y-x) + (y-x)^2$$

$$= 2x^2 + 2xy - 2x^2 + y^2 + x^2 - 2xy$$

$$= x^2 + y^2,$$ our old friend.

Can we always do this?

<u>Guess</u>. Given any discriminant D and form f of disc. D. Then any other form g of discriminant D is equivalent to f.

<u>This is not true</u>.

<u>Example</u>. $D = -20$.

Prove that $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are <u>not</u> equivalent.