E1.1.

Def. A quadratic field is

$$\mathbb{Q}(\sqrt{d}) = \{ a + b\sqrt{d} : a, b \in \mathbb{Q} \}.$$

~~the ring~~

Its ring of integers is

$$\mathcal{O} = \begin{cases} a + b\sqrt{d} : a, b \in \mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4 \\ \dfrac{a + b\sqrt{d}}{2} : a, b \text{ same parity} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

It is:

$$\mathcal{O} = \left\{ x \in \mathbb{Q}(\sqrt{d}) : x \text{ satisfies a monic poly. with coeffs in } \mathbb{Z} \right\}$$

$$= \text{maximal f.g. subring of } \mathbb{Q}(\sqrt{d}).$$

Its discriminant is $(\mathrm{Tr}(\alpha_i \alpha_j)) = \det \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4\sqrt{d}$

or $\det \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix} = \sqrt{d}$

as above,

so for squarefree d, $\mathrm{Disc}(\mathcal{O}) = \mathrm{Disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$

Prop. The set of quadratic fields is in bijection with the set of fundamental discriminants, other than 1.

Notation. Let K be a QF and $\mathcal{O}$ its ring of integers.

Thm. $\mathcal{O}$ admits unique factorization of ideals into prime ideals.

If p is a prime of $\mathbb{Q}$, then $p\mathcal{O}_K$ is:

prime in $\mathcal{O}$ (inert)

$\mathfrak{p} \cdot \bar{\mathfrak{p}}$ in $\mathcal{O}$ (split)

or $\mathfrak{p}^2$ in $\mathcal{O}$. (ramified)

Def. A fractional ideal of $\mathcal{O}$ is an f.g. $\mathcal{O}$ - submodule of K.

It is principal if it is $x \cdot \mathcal{O}$ for some $x \in K$.

Both are groups under multiplication, $I(K)$ and $P(K)$.

Def. The class group $Cl(K) := I(K)/P(K)$.

Units. Let $\mathcal{O}^\times$ be the group of units.

Then
$$|\mathcal{O}^\times| = \begin{cases} 6 \text{ if } & K = \mathbb{Q}(\sqrt{-3}) \\ 4 \text{ if } & K = \mathbb{Q}(\sqrt{-4}) \\ 2 \text{ if } & K = \mathbb{Q}(\sqrt{D}), \ D < -4 \\ \text{infinite if } & D > 0. \end{cases}$$

Theorem. If K is a (the) quadratic field of discriminant D, then
$$Cl(K) \cong Cl(D).$$

Proof. (Sketch. See Cox, 5.30, 7.7)

Construct a map
$$\text{BQFs} \longrightarrow \text{Ideals of } \mathcal{O}:$$
$$ax^2 + bxy + cy^2 \longrightarrow \left[a, \frac{-b+\sqrt{D}}{2}\right] = a \cdot \left[1, \frac{-b+\sqrt{D}}{2a}\right].$$

In other words:
$$a(x+\theta y)(x+\theta' y) \longrightarrow a[1, \theta].$$

Now, let $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ act on $ax^2 + bxy + cy^2$.

Get $a\left([\alpha x + \beta y] + [\gamma x + \delta y]\theta\right) \cdot \text{conj}.$

$$= a\left([\alpha + \gamma\theta]x + [\beta + \delta\theta]y\right) \cdot \text{conj}.$$

$$= a \cdot (\alpha + \gamma\theta)\left(x + \frac{\beta + \delta\theta}{\alpha + \gamma\theta}\, y\right) \cdot \text{conj}.$$

So maps to $a \cdot (\alpha + \gamma\theta)\left[1, \frac{\beta + \delta\theta}{\alpha + \gamma\theta}\right]$

$$= a\left[\alpha + \gamma\theta,\ \beta + \delta\theta\right].$$

$$= a \cdot [1, \theta] \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

We wrote an ideal of $\mathcal{O}$ ~~as~~ in terms of its $\mathbb{Z}$-basis which we simply permuted.

So it's well defined.

You can go backwards too, so injective.

Why is it surjective? Given $[\alpha, \beta]$ for some $\alpha, \beta \in K$.

WLOG $\tau := \frac{\beta}{\alpha}$ is in $\mathbb{H}$.

Then $[\alpha, \beta] \sim [1, \tau]$ in $Cl(K)$.

Let $ax^2 + bx + c$ be min poly of τ.

Check: This maps to it.

E1.4. **Corollary.** $Cl(D)$ is a group.

As Dirichlet discovered, if
$$f(x,y) = ax^2 + bxy + cy^2$$
$$g(x,y) = a'x^2 + b'xy + c'y^2$$
with $\gcd\left(a, a', \frac{b+b'}{2}\right) = 1$

both of disc D, then their composition is

$$aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the unique integer (mod $2aa'$) with
$$B \equiv b \pmod{2a}$$
$$B \equiv b' \pmod{2a'}$$
$$B^2 \equiv D \pmod{4aa'}.$$

Proof. Multiply ideals!

Claim. If f is a form of disc D, then
$$\mathrm{Aut}(f) \cong \mathcal{O}^\times.$$

Proof. Let $\frac{u+v\sqrt{d}}{2}$ be a unit, with $\left(\frac{u+v\sqrt{d}}{2}\right)\left(\frac{u-v\sqrt{d}}{2}\right) = 1.$
(Similar if -1.)

$$ax^2 + bxy + cy^2 = a(x+\theta y)(x+\theta' y)$$
$$= a\underbrace{\left(\frac{u+v\sqrt{d}}{2}\right)(x+\theta y)\left(\frac{u-v\sqrt{d}}{2}\right)(x+\theta' y)}_{\text{FOIL.}}$$

Get a change of variables.

E1.5.

The zeta function.

Def. If $\underline{a}$ is an (integral) ideal then $N(\underline{a}) = [\mathcal{O} : \underline{a}]$.

If $\underline{a} = (\alpha)$ then $N(\underline{a}) = N(\alpha)$.

Def. If $\mathcal{O}$ is the ring of integers of (any) number field K then its Dedekind zeta function is

$$\zeta_K(s) = \sum_{\underline{a} \triangleleft \mathcal{O}} (N\underline{a})^{-s} = \prod_{\underline{p}} \left(1 + (N\underline{p})^{-s} + (N\underline{p})^{-2s} + \dots\right) = \prod_{\underline{p}} \left(1 - (N\underline{p})^{-s}\right)^{-1}.$$

Ex. If $K = \mathbb{Q}$ then $\zeta_K(s) = \zeta(s)$.

Ex. $\mathbb{Z}[i]$ is a PID, with unit group 4, so

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4} \sum_{(x,y) \neq (0,0)} (x^2 + y^2)^{-s}.$$

Prop. For any number field K we have

$$\zeta_K(s) = \zeta(s) \cdot L(s, \chi_D).$$

Proof. For each prime p, RHS is: $(1 - p^{-s})^{-2}$ if p splits $\left(\frac{D}{p}\right) = 1$.

$(1 - p^{-s})^{-1}$ if ramified

$(1 - p^{-2s})^{-1}$ if inert.

Implies: # of ideals of norm n is

$$\sum_{d \cdot e = n} 1 \cdot \left(\frac{D}{e}\right) = \sum_{e \mid n} \left(\frac{D}{e}\right),$$

i.e. # of inequivalent representations.

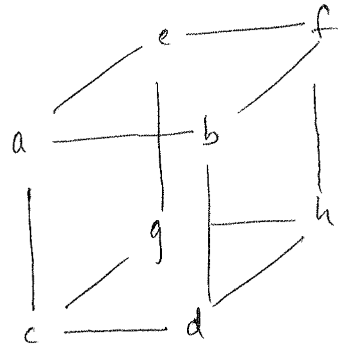
We recognize this now!

§2.1.

Bhargava's cube law.

Goal: Prove that binary quadratic forms, up to $SL_2(\mathbb{Z})$, form a group.

Consider a $2\times 2\times 2$ cube of integers:



Can slice three ways:

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

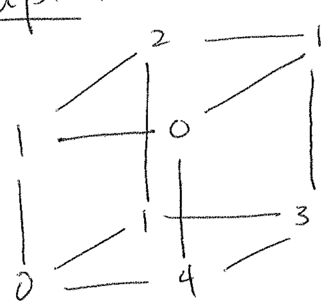
$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix} \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix} \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.$$

We can cook up a binary quadratic form!

Define $Q_i(x,y) = -\det(M_i x + N_i y)$.

Example.



$$\begin{aligned} Q_1(x,y) &= -\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} x + \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} y\right) \\ &= -\det\begin{bmatrix} x+2y & y \\ y & 4x+3y \end{bmatrix} \\ &= -\left((x+2y)(4x+3y) - y^2\right) \\ &= -\left[4x^2 + 11xy + 6y^2 - y^2\right] \\ &= -4x^2 - 11xy - 5y^2, \end{aligned}$$

of disc $121 - 80 = 41$.

E2.2.

$$Q_2(x,y) = -\det\left(\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} x + \begin{bmatrix} 0 & 4 \\ 1 & 3 \end{bmatrix} y\right)$$

$$= -\det \begin{bmatrix} x & 4y \\ 2x+y & x+3y \end{bmatrix}$$

$$= -\left[(x^2+3xy) - (8xy + 4y^2)\right]$$

$$= -x^2 + 5xy + 4y^2, \text{ of disc } 25+16 = 41$$

$$Q_3(x,y) = -\det\left(\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} 0 & 1 \\ 4 & 3 \end{bmatrix} y\right)$$

$$= -\det \begin{bmatrix} x & 2x+y \\ 4y & x+3y \end{bmatrix}$$

$$= -\left[(x^2+3xy) - (8xy+4y^2)\right]$$

= same as above.

Proposition. Q_1, Q_2, and Q_3 all have the same discriminant.

Proof 1. Cut it out. (Or make Sage do it.)

Proof 2. Define $\Gamma := SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$. $(= \Gamma_1 \times \Gamma_2 \times \Gamma_3)$

Then Γ acts on a cube A.

Given $A = (M_i, N_i)$, $\Gamma_i = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ acts by

$$(M_i, N_i) \longrightarrow (rM_i + sN_i,\ tM_i + uN_i),$$

and the actions of the three $SL_2(\mathbb{Z})$ factors all commute.

Now, how does Γ_i act on the quadratic forms?

$$Q_i(x,y) = -\det(M_i x + N_i y)$$

if $j \neq i$, then Γ_j acts on M_i and N_i individually by row and column operations.

Multiply $M_i x + N_i y$ by an elt. of $SL_2(\mathbb{Z})$.

If $j = i$, get

$$r_j \cdot Q_i(x,y) \overset{-\det}{=} ((rM_i + sN_i)x + (tM_i + uN_i)y)$$
$$= -\det(M_i(rx+ty) + N_i(sx+uy)).$$

So standard (transpose) action on binary quadratic forms!

So: the unique polynomial invariant, up to scalars, for the action of $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ on cubes is $\mathrm{Disc}(Q_1)$.

But, it's also $\mathrm{Disc}(Q_2)$

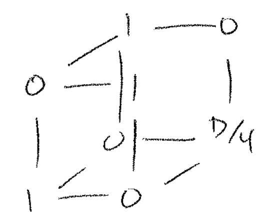
also $\mathrm{Disc}(Q_3)$. (up to scalars. check).

So, they're all equal!

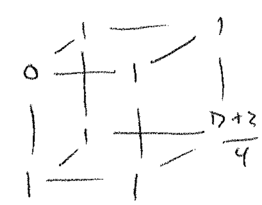
<u>The cube law</u>. Given a cube A w/ forms Q_1^A, Q_2^A, Q_3^A.

Declare $Q_1^A + Q_2^A + Q_3^A = 0$.

<u>Theorem</u>. This turns the set of $SL_2(\mathbb{Z})$ - equiv classes of primitive binary quad forms into a group!



The identity: If $D \equiv 0 \pmod 4$, $x^2 - \frac{D}{4}y^2$



If $D \equiv 1 \pmod 4$, $x^2 + xy - \frac{D-1}{4}y^2$

why $SL_2(\mathbb{Z})$ - equivalence classes?

If $\gamma = \gamma_1 \times \mathrm{id} \times \mathrm{id}$ acts on A,

$Q_1, Q_2, Q_3 \rightarrow \gamma_1 Q_1, Q_2, Q_3$.

Note: this is the <u>left</u> action

$\begin{pmatrix} r & s \\ t & u \end{pmatrix} f(x,y) = f(rx+ty, sx+uy)$.

E2.4.

How to get Dirichlet composition.

We saw $SL_2(\mathbb{Z})$ - equivalence.

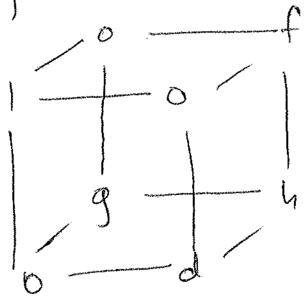
By acting by matrices in Γ, get:

top left to be 1.

(for a <u>projective</u> cube: QFs are all primitive)

Adjacent elts to be 0.

So get



$$Q_1 = -\det\left(\begin{bmatrix}1 & 0\\ 0 & d\end{bmatrix}x + \begin{bmatrix}0 & f\\ g & h\end{bmatrix}y\right)$$

$$= -\det\begin{pmatrix}x & fy\\ gy & dx+hy\end{pmatrix}$$

$$= -dx^2 - hxy + fgy^2.$$

Similarly $Q_2 = -gx^2 - hxy + dfy^2$

$Q_3 = -fx^2 + hxy + dgy^2$.

So our group law is $Q_1 + Q_2 + Q_3 = 0$.

$-Q_3$ is $dgx^2 - hxy - fy^2$.

Also can show: agrees w/ multiplication in the ideal class group.

<u>Theorem</u>. There is a canonical bijection between:

* nondegenerate Γ-orbits on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$
* isomorphism classes of pairs $(S, (I_1, I_2, I_3))$

S is an oriented quadratic ring

("oriented": two bases are $\langle 1, \tau\rangle$ and $\langle 1, -\tau\rangle$ choose one)

(I_1, I_2, I_3) is an <u>equivalence</u> class of <u>balanced</u> triples of <u>oriented</u> <u>ideals</u> of S.

E 2.5.

What does all this mean?

Oriented ideals: Pairs (I, ε) $\varepsilon = \pm 1$

I = fractional ideal

<u>Balanced</u>: $I_1 I_2 I_3 \subseteq S$ and $N(I_1) N(I_2) N(I_3) = 1$.

<u>Equivalence</u>: $(I_1, I_2, I_3) \sim (I_1', I_2', I_3')$ if

$I_i = \kappa_i I_i'$ for $\kappa_i \in S \otimes \mathbb{Q}$.

<u>Example</u>. If S is the ring of integers of a quadratic field, just a triple of narrow ideal classes whose product is the principal class.

F3.1. BQFs $ax^2 + bxy + cy^2$ over $\mathbb{R}$ or $\mathbb{C}$.

Action of $GL_2(\mathbb{R})$ or $GL_2(\mathbb{C})$.

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

Define <u>Disc(f)</u> to be a polynomial in a, b, c s.t.

$$\text{Disc}(f) = 0 \longrightarrow \text{form has multiple roots.}$$

What should it be?

Given $a(x - \theta y)(x - \theta' y)$,

take $\theta - \theta'$? (no, not a poly. sign ambiguous.)

$$(\theta - \theta')^2 = \left(\frac{-b + \sqrt{b^2 - 4ac}}{2a} - \frac{-b - \sqrt{b^2 - 4ac}}{2a}\right)$$

$$= \frac{b^2 - 4ac}{4a^2}.$$

So $4a^2(\theta - \theta')^2$ is a good bet.

And it is <u>irreducible</u>.

And <u>unique</u> up to <u>scalar multiples</u> and <u>powers</u>.

We <u>did</u> assume $a \neq 0$.

If have $(r_1 x + s_1 y)(r_2 x + s_2 y)$

define its discriminant $= (r_1 s_2 - s_1 r_2)^2$.

Same thing.

ES.2.

Alternatively:

f has multiple roots $\longleftrightarrow$ f, f' share a zero.

Dehomogenize assuming $a \neq 0$.

Take the resultant
$$\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a \cdot b^2 - b(2ab) + c(4a^2)$$
$$= -a(b^2 - 4ac).$$

Once again get $b^2 - 4ac$.

Can dehomogenize the other way.

Transitivity.

Proposition. Let f_1, f_2 be BQFs $/\mathbb{C}$, neither of disc 0.
$\exists\, g \in GL_2(\mathbb{C})$ s.t. $f_1 \circ g = f_2$.

Proof. WLOG $f_1 = xy$. Then $f_2 = (r_1 x + s_1 y)(r_2 x + s_2 y)$.

Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Then $(f_1 \circ g)\begin{pmatrix} x \\ y \end{pmatrix}$
$$= f_1\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right) = f_1\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right)$$
$$= f_1\begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}$$
$$= (\alpha x + \beta y)(\gamma x + \delta y).$$

So take $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} r_1 & s_1 \\ r_2 & s_2 \end{pmatrix}$. Easy enough.

why $\det g \neq 0$?

We know $[r_1 : s_1] \neq [r_2 : s_2]$

So $r_1 s_2 - s_1 r_2 \neq 0$.

E3.3.

<u>Proposition.</u> $\mathrm{Disc}(f\circ g) = (\det g)^{2}\,\mathrm{Disc}(f)$.

<u>Proof 1.</u> Direct computation.

<u>Proof 2.</u> <u>First</u>, note we can reduce to $g \in SL_2(\mathbb{C})$,

because
$$\mathrm{Disc}\left(f\circ\begin{bmatrix}\lambda & \\ & \lambda\end{bmatrix}\right) = \mathrm{Disc}(\lambda^2 f) = \lambda^4\,\mathrm{Disc}(f).$$

Now, use transitivity.

Check only for $f_0 = xy$.

$$\mathrm{Disc}(f) = 1.$$
$$\mathrm{Disc}(f\circ g) = \mathrm{Disc}\big((\alpha x+\beta y)(\gamma x+\delta y)\big) = (\alpha\delta-\beta\gamma)^2.$$

<u>Done.</u>

You could also write out,

$$(xy)\circ\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = (\alpha x+\beta y)(\gamma x+\delta y)$$
$$= \alpha\gamma\,x^2 + [\alpha\delta+\beta\gamma]\,xy + [\beta\delta]\,y^2$$

and check.

$$\mathrm{Disc} = (\alpha\delta+\beta\gamma)^2 - 4\alpha\beta\gamma\delta$$
$$= (\alpha\delta-\beta\gamma)^2.$$

<u>Orbital structure</u>: Generic ($\mathrm{Disc}\neq 0$)

Double root

0.

Note also acts transitively on the double root set:

Need $x^2\circ g = (r_1 x + s_2 y)^2$. So take $g = \begin{bmatrix} r_1 & s_2\\ * & *\end{bmatrix}$.

E3.4.

BQFs / $\mathbb{R}$.

Our argument before shows, transitive on the set of BQFs which you can factor.

But x^2+1 is not in the same orbit.

Can also see because $\mathrm{Disc}(f \circ g) = (\det g)^2 \, \mathrm{Disc}(f)$, and

$$\mathrm{Disc}(f) = \begin{cases} \text{pos.} & \text{if } f \text{ factors over } \mathbb{R} \text{ w/ dist roots} \\ \text{neg} & \text{if } f \text{ doesn't} \\ 0 & \text{if } f \text{ has a repeated root.} \end{cases}$$

Now, given any f which doesn't factor over $\mathbb{C}$.

WTS it is equivalent to x^2+1.

why? Notice $a \neq 0$, so WLOG $a=1$. (rescale)

$$x^2 + bxy + cy = \left(x - \frac{-b + \sqrt{b^2-4c}}{2a} y\right)\left(x - \frac{-b - \sqrt{b^2-4ac}}{2a} y\right)$$

Want to shift roots over by $\frac{-b}{2}$.

$f(x,y) = x^2 + bxy + cy^2$ then

$$f\left(x - \frac{b}{2}y, y\right) = \left(x - \frac{b}{2}y\right)^2 + b\left(x - \frac{b}{2}y\right)y + cy^2$$

$$= x^2 + \left(c - \frac{b^2}{4}\right)y^2.$$

i.e. $x^2 + \left(c - \frac{b^2}{4}\right)y^2 = f(x,y) \circ \begin{pmatrix} 1 & -b/2 \\ 0 & 1 \end{pmatrix}$. All good.

And, then, $c - \frac{b^2}{4} > 0$ (why? discuss)

So act by $\begin{pmatrix} 1 & \\ & \left(c - \frac{b^2}{4}\right)^{-1/2} \end{pmatrix}$ and we're done.

E3.5.

Let us look ahead.

<u>Binary</u> <u>cubic</u> <u>forms</u> are $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$.

$GL_2(\mathbb{C})$ acts by $(f \circ g)\binom{x}{y} = f\left(g\binom{x}{y}\right)$.

Is it <u>transitive</u>?

The <u>discriminant</u> of $(r_1x + s_1y)(r_2x + s_2y)(r_3x + s_3y)$

is $\left[(r_1s_2 - s_1r_2)(r_1s_3 - s_1r_3)(r_2s_3 - s_2r_3)\right]^2$.

By <u>construction</u>, zero iff multiple roots

The discriminant is

$$-27d^2a^2 + b^2c^2 + 18abcd - 4b^3d - 4ac^3.$$

Ugh.

We will see it <u>is</u> transitive.

<u>Moral</u>. $PGL_2(\mathbb{C})$ acts triply transitively on points in $\mathbb{P}^1$.

<u>Indeed</u>. $PGL_{n+1}(\mathbb{C})$ acts transitively on sets of $n+2$ pts. in $\mathbb{P}^n$.

Will see next time!

E4.1. Discriminants via Lie algebras.

Let $V_{\mathbb{R}} = \{ x_1 u^3 + x_2 u^2 v + x_3 u v^2 + x_4 v^3 \}$,

$GL_2(\mathbb{R})$ acts by $(f \circ g)\begin{pmatrix} u \\ v \end{pmatrix} = f\left(g\begin{pmatrix} u \\ v \end{pmatrix}\right)$.

Want to say, $\mathrm{Disc}(f) = 0 \longleftrightarrow f$ has multiple roots.

Today, determine Disc using the existence of a GL_2-action.

Example. Let $f = u^3 + v^3$.

Then $f \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a^3 + c^3) u^3 + [3a^2 b + 3c^2 d] u^2 v$
$+ [3ab^2 + 3cd^2] uv^2$
$+ (b^3 + d^3) v^3$.

Ex. The stabilizer group is

$\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a^3 = d^3 = 1 \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b^3 = c^3 = 1 \right\}$.

In $\mathbb{C}$, size 18, other fields - smaller.

Example. Let $f = u^3$.

Then $f \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a^3 u^3 + a^2 b u^2 v + ab^2 uv^2 + b^3 v^3$.

The stabilizer group is

$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a^3 = 1, b = 0, \ldots \right\}$!!

$= \left\{ \begin{pmatrix} a^3 & 0 \\ c & d \end{pmatrix} : a^3 = 1, d \neq 0 \right\}$. Not finite.

E4.2.

What is the principle?

Thm. $PGL_2(\mathbb{C})$ acts simply triply transitively on $\mathbb{P}^1(\mathbb{C})$.

(simply ? i.e. nothing other than 1 acts trivially)

Example. $f = u^3 + v^3 = (u+v)(u+\zeta_3 v)(u+\zeta_3^2 v)$.

The roots are $[1:-1], [\zeta_3 : -1], [\zeta_3^2 : -1]$.

Have $(ru + sv) \circ g = (ru + sv)\begin{pmatrix} a & b \\ c & d \end{pmatrix} =$

$$r(au+bv) + s(cu+dv)$$
$$= [ar+cs]u + [br+ds]v$$

So the action sends $[s : -r]$ to $[br+ds : -(ar+cs)]$

i.e. $\frac{-r}{s} \longrightarrow \frac{-(ar+cs)}{br+ds}$

$$= \frac{a\cdot\left(\frac{-r}{s}\right) - c}{-b\cdot\left(\frac{-r}{s}\right) + d}$$

There are 6 ways to permute three roots

also three third roots of unity,

so if $\mathrm{Disc}(f) \neq 0$, then $\mathrm{Stab}(f) \leq \mathrm{Sym}(3) \times \mathbb{Z}/3$.

But. If there is a repeated root, there will be lots of stabilizers.

E4.3.

So:

<u>Proposition.</u> We have $f \in V_{\mathbb{C}}$ has discriminant 0 if and only if the action of $GL_2(\mathbb{C})$ has infinite stabilizers.

<u>In fact,</u> $f \in V_{\mathbb{C}}$ has disc 0 if and only if there are $g \in GL_2(\mathbb{C})$ arbitrarily close to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ stabilizing f.

(This is because the stabilizers will have cardinality the same as $\mathbb{C}$.)

To understand this, look at the <u>tangent</u> <u>space</u> to $GL_2(\mathbb{C})$ at the identity.

<u>Def.</u>

~~$gl_2(\mathbb{C}) := \{ \lim_{h \to 0}$~~

$gl_2(\mathbb{C})$ is the set $\left\{ \frac{df}{dt}(0) : f : (-\delta, \delta) \to GL_2(\mathbb{C}) \text{ is a smooth curve, } f(0) = I \right\}$.

In fact, $gl_2(\mathbb{C}) = \mathrm{Mat}_2(\mathbb{C})$.

To see this: Some curves in GL_2:

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}_{(t \in \mathbb{R})} \frac{d}{dt} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

~~$\begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix}_{(t \in \mathbb{R}^+)} \frac{d}{dt} = \begin{pmatrix} -1/2 & 0 \\ 0 & 1 \end{pmatrix}$, I corresponds to $t = 1$.~~

sloppy!

~~So $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$~~

E4.4.

$$\begin{pmatrix} (1+t)^{-1} & \\ & (1+t) \end{pmatrix} \qquad \frac{d}{dt} = \begin{pmatrix} \frac{-1}{1+t^2} & 0 \\ 0 & 1 \end{pmatrix}$$

$(t \in (-1, \infty))$ $\qquad$ At $t = 0$: $\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$.

$$\begin{pmatrix} 1+t & \\ & 1+t \end{pmatrix} \qquad \frac{d}{dt} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

$$\begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix} \qquad \left.\frac{d}{dt}\right|_{t=0} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

And, $\left.\frac{d}{dt}\right|_{t=0} (f(t)\cdot g(t)) = f'(0)g(0) + f(0)g'(0)$
$= f'(0) + g'(0)$.

The infinitesimal action is

$$\frac{d}{dt}\left(\cancel{g(t)}\, v \circ f(t)\right) = \lim_{t\to 0}\left(\frac{v\circ f(t) - v\circ I}{t}\right).$$

$$= \lim_{t\to 0}\left(\frac{v\circ[I + t\cdot df] - v\circ I}{t}\right).$$

For $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$, $(a,b,c,d)\circ\begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$

$= (a + bt + O(t^2),\ b + 2ct + O(t^2),\ c + 3dt + O(t^2),\ d)$

So $\lim_{t\to 0}\left(\frac{v\circ\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} - v}{t}\right) = (b, 2c, 3d, 0)$.

Similar computations:

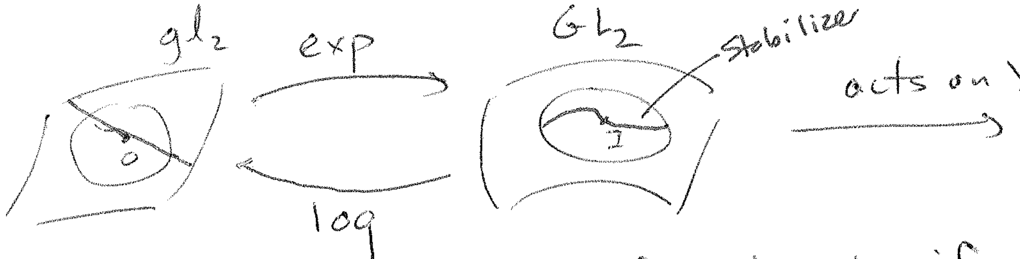
$$\begin{bmatrix} 1-t & \\ & 1+t \end{bmatrix} : \quad (-3a, -b, c, 3d)$$

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} : \quad (-b, -2c+3a, 2b-3d, c).$$

$$\begin{bmatrix} 1+t & \\ & 1+t \end{bmatrix} : \quad (3a, 3b, 3c, 3d).$$

We will have infinite stabilizers iff the action of some element of gl_2 on V is trivial.

why?



So get infinite stabilizers if and only if the vectors

$$(b, 2c, 3d, 0)$$
$$(-3a, -b, c, 3d)$$
$$(-b, -2c+3a, 2b-3d, c)$$
$$(3a, 3b, 3c, 3d)$$

are linearly dependent, i.e. if

$$\det \begin{bmatrix} b & -3a & -b & 3a \\ 2c & -b & -2c+3a & 3b \\ 3d & c & 2b-3d & 3c \\ 0 & 3d & c & 3d \end{bmatrix} = 6\left[b^2c^2 - 4b^3d + 18abcd - 27a^2d^2 - 4ac^3 \right] = 0.$$

E5.2.

To prove, look at $SL_2(\mathbb{R}) = N' A_+ \cdot K$.

Use the action of $SL_2(\mathbb{R})$ on $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$

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

Check. (1) It is an action which does land in $\mathbb{H}$.

What is the stabilizer of i?

$$\frac{ai+b}{ci+d} = i \Rightarrow ai + b = -c + di$$

$$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in SO_2(\mathbb{R}).$$

Look at $N' \cdot A_+ \circ i$.

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \circ i = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \circ t^2 i$$

$$= t^2 i + x.$$

So, given any $z \in \mathbb{H}$, there is $g \in N' A_+$ with $g \circ i = z$.

Suppose $g' \in SL_2(\mathbb{R})$ with $g' \circ i = z$

then $(g')^{-1} \circ z = i$

So $(g')^{-1} \cdot g \circ i = i$

So $(g')^{-1} \cdot g \in \mathrm{Stab}(i) = SO_2(\mathbb{R})$

So $g \cdot k = g'$ for some $k \in SO_2(\mathbb{R})$

i.e. we have written an arbitrary $g' \in SL_2(\mathbb{R})$ as $g \cdot k$ $g \in N' A_+$, $k \in SO_2(\mathbb{R})$ w/ everything uniquely determined.

E5.3.

Proposition. (positive discriminants)

(1) Given any two BCFs ($\mathbb{R}$) f, f' with disc > 0, there is $g \in GL_2(\mathbb{R})$ with $f \circ g = f'$.

(2) For any such f, $|\mathrm{Stab}_{GL_2(\mathbb{R})}(f)| = 6$.

(2) can be seen by Delone – Faddeev.
Or, prove it for $u^2v + uv^2$ by explicit computation, and use (1):
All stabilizers are conjugate
Given $f' = g \circ f$,

$$g_1 f' = f' \longleftrightarrow g_1 g \circ f = g \circ f$$
$$\longleftrightarrow g^{-1} \cdot g_1 g \circ f = f.$$

So, indeed we have a 6 - 1 covering map

$$GL_2(\mathbb{R}) \longrightarrow V^+ = \{ x \in V(\mathbb{R}) : \mathrm{Disc}(x) > 0 \}.$$

Proofs of finiteness of the number of orbits.

Notational issue. Shintani (1973) uses the action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ f(u, v) = f(au + cv, bu + dv)$$

As opposed to our

$$f \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} (u, v) = f(au + bv, cu + dv).$$

These are equivalent because $(M_1 M_2)^T = M_2^T M_1^T$.

~~4/14/2014 p.37~~ ES.4.

Proposition.

Let $S = \{ n(u) \cdot a_t \cdot k_\theta : \quad 0 < t \le 2, \quad |u| \le \frac{1}{2} \}$.

Then, $SL_2(\mathbb{R}) = SL_2(\mathbb{Z}) \cdot S = \underbrace{S'}_{\text{Replace } a_t \text{ with } a_{t^{-1}}} \cdot SL_2(\mathbb{Z})$.

For simplicity, look at positive discriminant cubic forms only.

Set $y = (0,1,1,0)$.

Use the fact that $GL_2(\mathbb{R})$ acts transitively on all (real) binary cubic forms of disc > 0.

This means, $SL_2(\mathbb{R}) \cup \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ acts transitively on all (real) binary cubic forms of disc $= m$, for any $m > 0$.

Also, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \circ u^2 v + uv^2 = -u^2 v + uv^2$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \circ u^2 v + uv^2 = -u^2 v + uv^2$

so in fact $SL_2(\mathbb{R})$ acts transitively on such.

One form is $m^{1/4} y = (0, m^{1/4}, m^{1/4}, 0) = y_m$.

We have all BCFs of disc m are $\in SL_2(\mathbb{R}) \cdot y_m$

and so in $SL_2(\mathbb{Z}) \cdot S \cdot y_m$.

so enough to show the number of integral BCFs in $S \cdot y_m$ is finite.

i.e. bound $V_{\mathbb{Z}} \cap S \cdot y_m$.

E5.5.

Set $E = \{ a_t^{-1} \cdot n(u) \cdot a_t \cdot k_\theta \ : \ 0 < t \le 2, \ |u| \le \frac{1}{2} \}$.

This is compact. why?

$$a_t^{-1} n(u) a_t = \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} \begin{bmatrix} t & \\ & t^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} t^{-1} & 0 \\ t\alpha & t \end{bmatrix} \begin{bmatrix} t & \\ & t^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ t^{2}\alpha & 1 \end{bmatrix}, \quad 0 < t \le 2, \ |u| \le \frac{1}{2}.$$

That's compact and so is SO_2.

So, product of these two groups is compact (closed and bounded).

Thus $\max(x_i) < N$ (abs constant) when $x = (x_1, x_2, x_3, x_4) \in E \cdot y$.

If $x \in V_{\mathbb{Z}} \cap \mathrm{Sym}$, then $a_t^{-1} \cdot \frac{x}{m^{1/4}} \in Ey$.

i.e. $\left(\frac{x_1}{m^{1/4} t^3}, \frac{x_2}{m^{1/4} t}, \frac{x_3 t}{m^{1/4}}, \frac{x_4 t^3}{m^{1/4}} \right) \in Ey$

so all these coeffs are bounded above by N.

We know that not both x_1 and x_2 are 0, so $|x_1| \ge 1$ or $|x_2| \ge 1$.

So $\frac{1}{m^{1/4} t} \le N$, so $t \ge \frac{1}{N m^{1/4}}$.

We get (since $t \le 2$) $|x_1|, |x_2| \le 8 N m^{1/4}$

$|x_3| < N \cdot m^{1/4} t^{-1} \le N^2 m^{1/2}$

$|x_4| < N \cdot m^{1/4} t^{-3} \le N^4 m$.

So all coeffs are bounded. QED.