Binary cubic forms.

A binary cubic form over a ring R is an expression

$$f(u,v) = \{ au^3 + bu^2v + cuv^2 + dv^3 : a, b, c, d \in R \}.$$

It admits a right action of $GL_2(R)$ given by

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

Typical R: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{Z}/m\mathbb{Z}, \mathbb{Z}_p$, K (number field), $\mathcal{O}_K$, (ring of ints) $\mathbb{A}_K$ (adeles)

Question for Blake et al. Just "GL_2" means something. Try to figure out what.

Recall. We already studied binary quadratic forms

$$f(u,v) = au^2 + buv + cv^2, \quad \text{same action of } GL_2.$$

what did we prove about them?

(1) There is an invariant, called the discriminant,

$$\Delta(f) = b^2 - 4ac, \text{ for which}$$

$$\mathrm{Disc}(fg) = (\det g)^2 \cdot \mathrm{Disc}(f),$$

for which

$$\Delta(f) = 0 \longleftrightarrow f \text{ has a double root.}$$

(2) A form properly represents an integer m iff it is $SL_2(\mathbb{Z})$-equivalent to $mx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.

22.2.

(3) There is a reduction theory:
Suppose $D<0$. Then each BQF is equivalent to a unique reduced form for which
(1) $|b| \le a_0 \le c$,
(2) $b \ge 0$ if either $|b| = a$ or $a = c$.

Defines a fundamental domain in $BQF(\mathbb{R}) / SL_2(\mathbb{Z})$.

(4) Let $h(D) :=$ number of $SL_2(\mathbb{Z})$-equivalence classes of IBQFs of disc D. Then $h(D)$ is finite, and we can get explicit bounds. (and compute)

(5) $h(D) \neq 0 \longleftrightarrow D \equiv 0, 1 \pmod 4$
~~rather~~ (6) In fact, get a theorem $BQF(\mathbb{Z}) / SL_2(\mathbb{Z}) \hookrightarrow$ ideals in quadratic rings.

(6) We had explicit formulas

$$\cancel{(D<0)} \quad h(D) = \sqrt{|D|} \cdot L(1, \chi_D) \cdot \begin{cases} \frac{2\pi}{w} & (D<0) \\ \frac{1}{\log \varepsilon_D^+} & (D>0) \end{cases}$$

(7) Could count on average, at least for $D<0$,

$$\sum_{0<-D<X} h(D) \sim c \cdot X^{3/2}.$$

For $D>0$, * reduction theory is batty
* stabilizer groups are infinite.

Q. What translates to binary ~~quad~~ cubic forms?

Defn A binary n-ic form is an expression

$$f(u,v) = a_0 u^n + a_1 u^{n-1} v + \dots + a_n v^n,$$

with an action of $GL_n(\mathbb{R})$ $\quad (f \circ g)\begin{pmatrix} u \\ v \end{pmatrix} = f\left(g\begin{pmatrix} u \\ v \end{pmatrix}\right).$

(22.3.) = 23.1.

It turns out, $n=2$ and $n=3$ are special.

You get a prehomogeneous vector space.

We will see why this matters.

Binary cubic forms.

What are we counting?

Def. The discriminant of a binary cubic form

$$f(u,v) = au^3 + bu^2v + cuv^2 + dv^3 \quad \text{is}$$

$$\mathrm{Disc}(f) = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

Theorem. If $g \in GL_2(\mathbb{R})$, then

$$\mathrm{Disc}(f\circ g) = (\det g)^6\, \mathrm{Disc}(f).$$

Note. This is very big.

Shitty proof. For general $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$,

$$f\,\cancel{(u,v)} \circ g\begin{pmatrix} u \\ v \end{pmatrix} \quad f\left(g\begin{pmatrix} u \\ v \end{pmatrix}\right) = f(\alpha u + \gamma v, \beta u + \delta v).$$

FOIL it out. Plug into the formula above.

(Coerce Sage into doing this.)

Think about what we want to generalize.

Def. The discriminant of a monic cubic polynomial

$$f(u) = u^3 + bu^2 + cu + d \quad \text{is}$$

$$\mathrm{Disc}(f) = b^2c^2 + 18bcd - 4c^3 - 4b^3d - 27d^2.$$

22.4. = 23.2,

Also, if $f(u) = (u-\theta_1)(u-\theta_2)(u-\theta_3)$

(possibly over some extension),

then $\mathrm{Disc}(f) = \left[(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_2-\theta_3)\right]^2$.

Properties.

(*) $\mathrm{Disc}(f) = 0 \longleftrightarrow$ f has a multiple root.

What does this mean? If f has coeffs in R (maybe not roots in R),

look at the extension ring $R[u]/f(u)$.

What can this be?

~~Suppose it factors over R into distinct factors.~~

Suppose for simplicity R is a field.

Then $R[u]/(u-\theta_1)(u-\theta_2)(u-\theta_3) \xrightarrow{\sim} \dfrac{R[u]}{u-\theta_1} \times \dfrac{R[u]}{u-\theta_2} \times \dfrac{R[u]}{u-\theta_3}$

$\cong R \times R \times R$

by the natural reduction map.

(This is the Chinese remainder theorem.)

Careful! Not true over rings in general. The map

$\mathbb{Z}[x]/(x-2)(x-4)(x-6) \longrightarrow \dfrac{\mathbb{Z}[x]}{x-2} \times \dfrac{\mathbb{Z}[x]}{x-4} \times \dfrac{\mathbb{Z}[x]}{x-6}$

$\cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

is not surjective.

Nothing maps to $(1,0,0)$.

(22.5) =23.3. Say we have a repeated root. (again, R a field)

$$R[u] / (u-\theta_1)^2 (u-\theta_2) \xrightarrow{\sim} R[u] / (u-\theta_1)^2 \times \frac{R[u]}{u-\theta_2}.$$

Then $u-\theta_1$ is a <u>nilpotent</u> element.

(Example. f is the min poly of a field extension. Look at it mod primes, i.e. in <u>finite</u> <u>fields</u>. $\mathbb{F}_p$. (or $\mathbb{F}_q$)

$\mathrm{Disc}(f) = 0$ in $\mathbb{F}_p$ ⟷ $\mathbb{F}_p[u]/(f)$ is not an integral domain.

$\Updownarrow$

$p \mid \mathrm{Disc}(f)$

For quadratic ~~forms~~ monic polys, $(x-\theta_1)(x-\theta_2) = x^2 - (\theta_1+\theta_2)x + (\theta_1\theta_2)$

$$\begin{aligned}\mathrm{Disc}(f) &= (\theta_1 - \theta_2)^2 \\ &= (\theta_1 + \theta_2)^2 - 4\theta_1\theta_2 \\ &= b^2 - 4c.\end{aligned}$$

For cubic polynomials,

$$\begin{aligned}(x-\theta_1)(x-\theta_2)(x-\theta_3) &= x^3 + bx^2 + cx + d \\ &= x^3 - [\theta_1+\theta_2+\theta_3]x^2 \\ &\quad + [\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3]x \\ &\quad - \theta_1\theta_2\theta_3.\end{aligned}$$

You <u>can</u> do this. There are shortcuts.

<u>Now</u>, more generally, the discriminant of $(a_1x - b_1y)(a_2x - b_2y)\cdots(a_nx - b_ny)$ is

$$\left[\prod_{i \neq j} (a_ib_j - a_jb_i)\right]^2.$$

23.4.

Exercise.

(1) Given a binary form ~~with leading coeffs~~, prove

$$\mathrm{Disc}(a_n u^n + a_{n-1} u^{n-1} v + \cdots + a_0 v^n)$$

if $a_n = 1$:

$$= \mathrm{Disc}(u^n + a_{n-1} u^{n-1} + \cdots + a_0).$$

more generally, if $a_n \neq 0$:

$$= a_n^{2n-2}\, \mathrm{Disc}(u^n + a_{n-1} u^{n-1} + \cdots + a_0)$$

If $a_n = 0$ and $a_{n-1} \neq 0$:

$$= a_{n-1}^2 \cdot \mathrm{Disc}(a_{n-1} u^{n-1} + a_{n-2} u^{n-2} v + \cdots + a_0 v^{n-1})$$

If $a_n = 0$ and $a_{n-1} = 0$:

$$= 0.$$

How to prove these formulas?

(1) "Get it out." Symmetric polynomials. (See HW)

(2) Use resultants.

(3) Lie algebras / differentiable manifolds proof.

(1) Homework.

(2) Familiar to Jesse veterans

(3) Thursday.

23.5.

Sketch of (1).

Dehomogenize, $u^3 + bu^2 + cu + d = (u-r)(u-s)(u-t)$.

Substitute $v = u + \frac{b}{3}$, disc doesn't change

$$u^3 + bu^2 + cu + d = v^3 + \left(c - \frac{b^2}{3}\right)v + \left(d - \frac{bc}{3} + \frac{2b^3}{27}\right)$$

$$= v^3 + Cv + D.$$

$$= (v-R)(v-S)(v-T).$$

Now, $-\operatorname{Disc}(F) = F'(R)\,F'(S)\,F'(T)$

$$= (3R^2 + C)(3S^2 + C)(3T^2 + C)$$

$$= \cdots$$

$$= -27D^2 - 4C^3.$$

24.1

Delone - Faddeev over fields.

(Think: $K = \mathbb{Q}$)

<u>Proposition</u>*. Let K be a field. There is a bijection

$$\text{Irr.}\,BCF(K) \big/ GL_2(K) \longleftrightarrow \begin{array}{c}\text{cubic field extensions}\\ L/K.\end{array}$$

You get it as follows. (Two equivalent descriptions)

(1) Given $\underbrace{au^3 + bu^2v + cuv^2 + dv^3}_{\text{over } K} = \underbrace{(r_1u - s_1v)(r_2u - s_2v)(r_3u - s_3v)}_{\text{over } \overline{K}}$,

take $K\left(\frac{s_1}{r_1}\right)$.

(2) Dehomogenize. Take $v = 1$ and adjoin a root.

The asterisk. The action is slightly "wrong".

Consider $u^3 + uv^2 + v^3$. Generates a perfectly good field.

$$= (u - s_1v)(u - s_2v)(u - s_3v)$$

Now consider $2(u^3 + uv^2 + v^3)$

$$= (\sqrt[3]{2}u - \sqrt[3]{2}s_1v)(\sqrt[3]{2}u - \sqrt[3]{2}s_2v)(\sqrt[3]{2}u - \sqrt[3]{2}s_3v).$$

Fields ~~gg~~ generated by $\frac{s_1}{1}$ and $\frac{\sqrt[3]{2}s_1}{\sqrt[3]{2}}$.

<u>Same field.</u>

We <u>want</u> $u^3 + uv^2 + v^3$ and $2(u^3 + uv^2 + v^3)$ to be equivalent. Change the action.

<u>Def.</u> The <u>twisted</u> <u>action</u> of GL_2 on binary cubic forms is

$$(f \circ g)\begin{pmatrix} u \\ v \end{pmatrix} = \frac{1}{\det g} f\left(g\begin{pmatrix} u \\ v \end{pmatrix}\right).$$

Proposition. With the ~~scalar~~ twisted action, scalar matrices $\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix}$ act as multiplication by λ.

Proof: Let $f = au^3 + bu^2v + cuv^2 + dv^3$.

Then $$\left(f \circ \begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix}\right)\begin{pmatrix}u\\v\end{pmatrix} = \frac{1}{\det\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix}} f\left(\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix}\begin{pmatrix}u\\v\end{pmatrix}\right)$$
$$= \frac{1}{\lambda^2} f\begin{pmatrix}\lambda u\\ \lambda v\end{pmatrix}$$
$$= \frac{1}{\lambda^2}\left[a\lambda^3u^3 + b\lambda^3u^2v + c\lambda^3uv^2 + d\lambda^3v^3\right]$$
$$= \lambda \cdot f.$$

The proposition is true with the twisted action.

Examples.

$K = \mathbb{Q}$. You get lots of cubic fields this way.

$K = \mathbb{C}$. Cubic fields extensions $L/\mathbb{C}$ correspond to irreducible cubic polynomials over $\mathbb{C}$.
Indeed this is true.

$K = \mathbb{F}_p$. There is one cubic extension of $\mathbb{F}_p$.
There are $\frac{1}{3}(p^2-1)(p^2-p)$ irreducible BCFs over $\mathbb{F}_p$ and they are all $GL_2(\mathbb{F}_p)$-equivalent.

Proof of DF over a field.

(1) Let $f = au^3 + bu^2 v + cuv^2 + dv^3$.

$= (r_1 u - s_1 v)(r_2 u - s_2 v)(r_3 - s_3 v)$.

Note: all $r_i, s_i \neq 0$.

Then $f \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix} = f\begin{pmatrix} \alpha u + \beta v \\ \gamma u + \delta v \end{pmatrix}$

$= \left(r_1[\alpha u + \beta v] - s_1[\gamma u + \delta v]\right) \times$ two more

$= \left([r_1 \alpha - s_1 \gamma]u + [r_1 \beta - s_1 \delta]v\right) \times$ two more.

So your "field" is $\mathbb{K}\left(\dfrac{s_1 \delta - r_1 \beta}{r_1 \alpha - s_1 \gamma}\right)$

$= K\left(\dfrac{\frac{s_1}{r_1}\delta - \beta}{\alpha - \frac{s_1}{r_1}\gamma}\right)$.

~~If $\frac{s_1}{r_1} \in K$, so is $\frac{\frac{s_1}{r_1}\delta - \beta}{\alpha - \frac{s_1}{r_1}\gamma}$. (Either that, or you are dividing by 0.)~~

If $r_1 u - s_1 v$ were defined over K (contrary to assumption), then so would $[r_1 \alpha - s_1 \gamma]u + [r_1 \beta - s_1 \delta]v$.

Because we have a group action and can consider $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1}$, shows that $[r_1 \alpha - s_1 \gamma]u + [r_1 \beta - s_1 \delta]v$ is not defined $/K$. So action sends irred. $\to$ irred.

So, in particular, we do get a field.

But $K\left(\dfrac{\frac{s_1}{r_1}\delta - \beta}{\alpha - \frac{s_1}{r_1}\gamma}\right) \subseteq K\left(\dfrac{s_1}{r_1}\right)$.

By reversing the action or arguing using degrees, these must be equal.

>4.4

Now let $\theta = \frac{s_1}{r_1}$ and suppose that $L = K(\theta')$ for some θ'. We must argue, there is some element of $GL_2(K)$ taking θ to θ'.

It suffices to prove, $\theta' = \dfrac{r\theta + s}{t\theta + u}$ for some $r, s, t, u \in K$.

We know $a\theta^3 + b\theta^2 + c\theta + d = 0$.
Can write $\theta' = x_0 + x_1\theta + x_2\theta^2$ for some $x_0, x_1, x_2 \in K$.

Want to solve
$(x_0 + x_1\theta + x_2\theta^2)(t\theta + u) = r\theta + s$ in r, s, t, u.
FOIL it and use the min poly:

$$\left(x_0 u - \frac{d}{a}x_2 t\right) + \theta\left(x_1 u + x_0 t - \frac{c}{a}x_2 t\right) + \theta^2\left(x_2 u + x_1 t - \frac{b}{a}x_2 t\right)$$

$$= r\theta + s.$$

Assume $x_2 \neq 0$. (If $x_2 = 0$, $\theta' = x_0 + x_1\theta = \dfrac{x_0 + x_1\theta}{1 + 0\cdot\theta}$.)

So, choose $t = 1$ and $u = \left(\frac{b}{a} - \frac{x_1}{x_2}\right)$.

That takes care of the θ^2 term.
Get to pick r and s, so we win for free.
QED.

We can see this would not work for quartic fields.

Note. Would have to solve
$(x_0 + x_1\theta + x_2\theta^2 + x_3\theta^3)(t\theta + u) = r\theta + s$ in r, s, t, u.
We're only interested in $[r : s : t : u] \in \mathbb{P}^3(K)$.
3-dimensional space of solutions.
4-dimensional space of parameters.

Quartic (and higher) fields: GL_2-equivalent forms generate the same field. But different orbits can also generate the same field.

Questions this poses.

(1) Quartic fields and beyond?

(2) Can we extend this to <u>reducible</u> cubic forms?

Dehomogenize and take a root.

How do you take a root of $(x-1)^3$?

$(x-1)(x-2)(x-3)$?

0?

(3) How to make this work over a ring?

We'll answer these questions next time.

Let K be a field.

Claim. There is a bijection

$$\text{Irr } BCF(K) \Big/ GL_2(K) \longleftrightarrow \text{cubic field exts. } L/K.$$

The action is the twisted action $(f \circ g)\binom{u}{v} := \frac{1}{(\det g)} f\left(\binom{u}{v}\right)$.

Last time.

(1) There is a map

$$\text{Irr } BCF(K) \longrightarrow \text{cubic field exts.}$$

$$\underbrace{(r_1 u - s_1 v) \cdot [\text{two more}]}_{\text{factor over } \overline{K}} \longrightarrow K\left(\frac{s_1}{r_1}\right).$$

(2) It is WD up to the $GL_2(K)$-action,

because $\frac{s_1}{r_1} \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \dfrac{\frac{s_1}{r_1}\delta - \beta}{\alpha - \frac{s_1}{r_1}\gamma}$.

(3) It is injective. Can prove, if $L = K(\theta) = K(\theta')$

then $\theta' = \dfrac{r\theta + s}{t\theta + w}$ for some $r, s, t, w \in K$.

* (4) It is surjective.

Given $L = K(\theta)$, where $\theta^3 + a_2\theta^2 + a_1\theta + a_0 = 0$.

The cubic form

$$(u - \theta v)(u - \theta' v)(u - \theta'' v) = u^3 + a_2 u^2 v + a_1 u v^2 + a_0 v^3$$

yields L.

The generalization.

Let R be any integral domain.

A cubic ring over R is any commutative ring which is a rank 3 free R-module.

Ex. Let R be the field $\mathbb{Q}$.

Then cubic fields are cubic rings / R.

Consider $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$.

The identity is $(1,1,1)$.

This is not an integral domain, because

$$(1,0,0) \cdot (0,1,0) = (0,0,0).$$

Another example is $\mathbb{Q}[x]/(x^3)$.

Ex. Let $R = \mathbb{Z}$.

Then $\mathbb{Z}[x]/(\text{cubic integral polynomial})$ is always a cubic ring.

e.g.: $\mathbb{Z}[x]/(x^3-2) = \mathbb{Z}[\sqrt[3]{2}]$.

$= \mathbb{Z} \oplus \mathbb{Z}[\sqrt[3]{2}] \oplus \mathbb{Z}(\sqrt[3]{4}]$

as a $\mathbb{Z}$-module (i.e. as an abelian group).

$$\mathbb{Z}[x]/(x^3-x) \cong \mathbb{Z}[x]/(x) \oplus \mathbb{Z}[x]/(x-1) \oplus \frac{\mathbb{Z}[x]}{(x+1)}$$

$$\cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

once again a cubic ring.

not an integral domain.

$\mathbb{Z}[x]/(x^3)$.

$\mathbb{Z}[x]/(x^3-16)$. Not the same as $\mathbb{Z}[x]/(x^3-2)$.

<u>Definition</u>. (discriminant ~~&~~, trace)

(1). Let $\mathcal{O}$ be a cubic ring over R.

We can write $\mathcal{O} = Rx_1 \oplus Rx_2 \oplus Rx_3$.

If $\alpha \in \mathcal{O}$, the map $\begin{matrix} x & \longrightarrow & \alpha x \\ \mathcal{O} & \longrightarrow & \mathcal{O} \end{matrix}$ defines an endomorphism of R-modules.

We say $\mathrm{Tr}(\alpha)$ is the trace of this endomorphism.

(2). The <u>discriminant</u> of $\mathcal{O}$ is

$$\det \begin{bmatrix} \mathrm{Tr}(x_1^2) & \mathrm{Tr}(x_1x_2) & \mathrm{Tr}(x_1x_3) \\ \mathrm{Tr}(x_1x_2) & \mathrm{Tr}(x_2^2) & \mathrm{Tr}(x_2x_3) \\ \mathrm{Tr}(x_1x_3) & \mathrm{Tr}(x_2x_3) & \mathrm{Tr}(x_3)^2 \end{bmatrix}$$

for shorthand, $\det_{i,j}(\mathrm{Tr}(x_ix_j))$.

<u>or</u> the determinant of the bilinear pairing $\mathrm{Tr}(\alpha\beta)_{\alpha,\beta\in R}$

(Being claimed that it doesn't depend on a basis!)

<u>Warning</u>. This is an element of $R/(R^\times)^2$.

Doesn't give a well-defined element of R.

(But, if $R = \mathbb{Z}$, it does.)

<u>Example</u>. $R = \mathbb{Z}$, $\mathcal{O} = \mathbb{Z}[x]/(x^3-2) = \mathbb{Z}[\sqrt[3]{2}]$

$= \mathbb{Z} \oplus \mathbb{Z}[\sqrt[3]{2}] \oplus \mathbb{Z}[\sqrt[3]{4}]$.

$\{x_1, x_2, x_3\} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Must compute the traces of $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{8}, \sqrt[3]{16}\}$.

$\mathrm{Tr}(1)$: Sends $1 \to 1$, $\sqrt[3]{2} \to \sqrt[3]{2}$, $\sqrt[3]{4} \to \sqrt[3]{4}$

$$\mathrm{Tr}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 3.$$

$\mathrm{Tr}(\sqrt[3]{2})$: Sends $1 \to \sqrt[3]{2}$, $\sqrt[3]{2} \to \sqrt[3]{4}$, $\sqrt[3]{4} \to 2$.

$$\mathrm{Tr}\begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 0.$$

$\mathrm{Tr}(\sqrt[3]{4})$:

$$\mathrm{Tr}\begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix} = 0$$

$$\mathrm{Tr}(2) = \mathrm{Tr}\begin{bmatrix} 2 & & \\ & 2 & \\ & & 2 \end{bmatrix} = 6$$

$$\mathrm{Tr}(\sqrt[3]{16}) = \mathrm{Tr}\begin{bmatrix} 0 & 0 & 4 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = 0.$$

So, $\mathrm{Disc}(\mathcal{O}) = \det\begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix} = -3 \cdot 6 \cdot 6 = -108.$

Ex. $R = \mathbb{Z}$, $\mathbb{Z}[x]/(x^3)$.

$\mathrm{Tr}(1) = 3$ as before.

x sends $1 \to x$, $x \to x^2$, $x^2 \to 0$,

$$\mathrm{Tr}\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 0.$$

$$\mathrm{Tr}(x^2) = \mathrm{Tr}\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = 0.$$

$\mathrm{Tr}(x^3) = \mathrm{Tr}(0) = 0.$ $\mathrm{Tr}(x^4) = 0.$

Disc ~~det~~ is $\det\begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 0.$

More examples if time!

4/9/14. (U26.V) Some more trace computations.

p. 1.

Compute Disc(R) where $R = \mathbb{Z}[x]/(x^3)$ and

$$R = \mathbb{Z}[x]/(x^3 - x).$$

First:

$$\det \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Second: Basis is $\{1, x, x^2\}$

$\times 1$: $\mathrm{Tr} \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} = 3$

$\times x$: $\mathrm{Tr} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = 0$

$\times x^2$: $\mathrm{Tr} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = 2.$

$\times x^3$: Same as $\times x$.

$\times x^4$: same as $\times x^2$.

So: $\det \begin{bmatrix} 3 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix} = 3 \cdot 2 \cdot 2 - 2 \cdot 2 \cdot 2 = 4.$

Delone-Faddeev (over $\mathbb{Z}$).

<u>Theorem</u>. There is a natural, discriminant-preserving bijection

$$BCF(\mathbb{Z}) / GL_2(\mathbb{Z}) \longleftrightarrow \text{cubic rings}.$$

<u>Proof</u>. (BST) (1) Get a map cubic rings $\longrightarrow$ cubic forms.

Start with a cubic ring $R = \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}\theta$.

(Ex. Show you can make one of these $\mathbb{Z}$.)

p. 2. (26.2')

We can assume $w \cdot \theta \in \mathbb{Z}$.

Why is this? If $w \cdot \theta = r_1 + r_2 w + r_3 \theta$,

$$(w - r_3)(\theta - r_2)$$
$$= w\theta - r_3\theta - r_2 w + r_2 r_3$$
$$= r_1 + r_2 r_3, \quad \text{and}$$
$$\mathbb{Z} \oplus \mathbb{Z}w \oplus \mathbb{Z}\theta = \mathbb{Z} \oplus \mathbb{Z}(w - r_3) \oplus \mathbb{Z}(\theta - r_2).$$

Write out the multiplication table:

$$w \cdot \theta = n$$
$$w^2 = m - bw + a\theta$$
$$\theta^2 = l - dw + c\theta.$$

Our form is $au^3 + bu^2v + cuv^2 + dv^3$.

[What?!]

This represents the cubic map

$$R/\mathbb{Z} \longrightarrow \Lambda^2(R/\mathbb{Z}) \cong \mathbb{Z}$$
$$q \longrightarrow q \wedge q^2.$$

If $q = xw + y\theta$,

$$xw + y\theta \longrightarrow (xw + y\theta) \wedge (xw + y\theta)^2$$
$$= (xw + y\theta) \wedge \left[x^2w^2 + y^2\theta^2 + 2xyw\theta\right]$$
$$= (xw + y\theta) \wedge \left[x^2(m - bw + a\theta) + y^2[l - dw + c\theta] + 2xyn\right]$$

Ah! But in $\Lambda^2(R/\mathbb{Z})$

$$= (xw + y\theta) \wedge \left[x^2(bw - a\theta) + y^2[dw - c\theta]\right]$$

p.3. (26.3)

$$= x^3 \omega \wedge (b\omega - a\theta) + x^2 y\, \theta \wedge (b\omega - a\theta)$$
$$+ xy^2 \omega \wedge (d\omega - c\theta) + y^3 \theta \wedge (d\omega - c\theta)$$

$$= -a \cdot x^3 \omega \wedge \theta + b x^2 y\, \theta \wedge \omega - c x y^2 \omega \wedge \theta + d y^3 \theta \wedge \omega$$

$$= (ax^3 + bx^2 y + cxy^2 + dy^3)\, \theta \wedge \omega.$$

(1a). Show the map is basis-independent.

Suppose you write $\begin{bmatrix} \omega' \\ \theta' \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \omega \\ \theta \end{bmatrix}$

with $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GL_2(\mathbb{Z})$

and then renormalize again.

Get a basis $(1, \omega'', \theta'')$ with $\omega'' - \omega' \in \mathbb{Z}$, $\theta'' - \theta' \in \mathbb{Z}$

$\omega'' \theta'' \in \mathbb{Z}$.

Then, where does $x\omega'' + y\theta''$ go?

$$x\omega'' + y\theta'' = x(\alpha\omega + \beta\theta) + y(\gamma\omega + \delta\theta) \quad \text{in } \underline{\underline{R/\mathbb{Z}}}$$
$$= [x\alpha + y\gamma]\,\omega + [x\beta + y\delta]\,\theta.$$

Chase down under the same map.

Get the binary cubic form

$$a[x\alpha + y\gamma]^3 + b[x\alpha + y\gamma]^2[x\beta + y\delta] + c[x\alpha + y\gamma][x\beta + y\gamma]^2 + d[x\beta + y\gamma]^3$$

$$= f(x\alpha + y\gamma,\ x\beta + y\delta) = f\left(\begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}\right) = f \circ \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}.$$

p.4. (26.4)

To go back:

Given $ax^3 + bx^2y + cxy^2 + dy^3$.

Write out
$$w\theta = n$$
$$w^2 = m - bw + a\theta$$
$$\theta^2 = l - dw + c\theta$$

Our cubic ring is $\{1, w, \theta\}$.

But wait:

(1) what are n, m, l?

(2) Really? Surely this must be trickier...

We have equations $w(w\theta) = (w^2)\theta$, $(w^2)(\theta^2) = (w\theta)\theta$.

If these are satisfied, get a cubic ring.

$$w(w\theta) = nw$$
$$(w^2)\theta = (m - bw + a\theta)\theta = m\theta - bw\theta + a\theta^2$$
$$= m\theta - b\cdot n + al - adw + ac\theta$$
$$= [\cancel{m} - bn + al] - [ad\,\cancel{w}]w + [ac + m]\theta.$$

So: $-bn + al = 0$.
$ac + m = 0$
$-ad = n$.

~~So: $ad = -n$~~
~~$ac = 0$~~
~~$m - bn + al = 0$~~

$$(w\theta)\theta = n\cdot\theta.$$
$$w\cdot\theta^2 = w(l - dw + c\theta) = w\cdot l + c\cdot n - d[m - bw + a\theta]$$
$$= [-dm + cn] + w[l + bd] + \theta[-ad]$$

$-ad = n$.
$l + bd = 0$
$-dm + cn = 0$.

p. 5. (126.5)

So we get

$$n = -ad, \quad m = -ac, \quad l = -bd.$$

Two more equations:

$-bn + al = 0$? Says $bad + a(-bd) = 0$ ✓

$-dm + cn = 0$? $-d(-ac) + c(-ad) = 0.$ ✓

So, subject to these conditions, we win.

4/11/14. (27.1)

[From 4/9/14. Review, and do pp. 4-5.]

Ex. Let α be a root of $x^3 - x - 1$.
Chase $\mathbb{Z}[\alpha]$ through DF and see what you get.

Ans. $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$,

and $\alpha \cdot \alpha^2 = \alpha + 1$, so

$$\alpha \cdot [\alpha^2 - 1] = 1.$$

So $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}\theta$, with $\omega = \alpha$, $\theta = \alpha^2 - 1$.

$$\omega \cdot \theta = 1.$$

$$\begin{aligned}
\theta^2 &= (\alpha^2 - 1)^2 \\
&= \alpha^4 - 2\alpha^2 + 1 \\
&= \alpha^2 + \alpha - 2\alpha^2 + 1 \\
&= -\alpha^2 + \alpha + 1 \qquad = 0 - (-1)\omega + (-1)\theta \\
&= -\theta + \omega
\end{aligned}$$

$$\begin{aligned}
\omega^2 &= \alpha^2 \\
&= (\alpha^2 - 1) + 1 \\
&= \theta + 1 \qquad = 1 - 0\cdot\omega + 1\cdot\theta.
\end{aligned}$$

So our cubic ring is

$$1\cdot x^3 + 0\cdot x^2 y - xy^2 - y^3.$$

Exercise. True or false?
Let α be a root of $x^3 + bx^2 + cx + d$.
Then the cubic form you always get is $x^3 + bx^2y + cxy^2 + dy^3$.
If false, are there conditions which make it true?

4/11/14. (p.2) (27.2)

Ex. Consider the cubic ring $\mathcal{O}$. What does it correspond to?

$$\mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}\theta,$$

with

$$\omega\theta = -ad \qquad = 0$$

$$\omega^2 = \overset{-ac}{\cancel{ac}} - b\omega - a\theta \qquad = 0$$

$$\theta^2 = -bd - d\omega + c\theta \qquad = 0.$$

So $\mathbb{Z}[\omega, \theta] / (\omega\theta, \omega^2, \theta^2) = \mathbb{Z}[\omega, \theta] / (\omega, \theta)^2$.

<u>Proposition</u>. If a cubic ring R corresponds to a cubic form f, then $\mathrm{Disc}(R) = \mathrm{Disc}(f)$.

<u>Exercise</u>. Verify it by brute force.

<u>But</u>, we can be a bit more clever.

$$\mathrm{Disc}(f) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) & \mathrm{Tr}(\theta) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}(\omega^2) & \mathrm{Tr}(\omega\theta) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\omega\theta) & \mathrm{Tr}(\theta^2) \end{bmatrix}.$$

$\mathrm{Tr}(1) = 3,$

$$\mathrm{Tr}(\omega) = \mathrm{Tr} \begin{bmatrix} 0 & -ac & \overset{-ad}{\cancel{-bd}} \\ 1 & -b & \cancel{-d}\,0 \\ 0 & -d & 0 \end{bmatrix} \qquad \mathrm{Tr}(\omega^2) = \mathrm{Tr} \begin{bmatrix} -ac & * & * \\ -b & -ac+b^2 & * \\ -a & * & -ad \end{bmatrix}$$

$$\mathrm{Tr}(\theta) = \mathrm{Tr} \begin{bmatrix} 0 & -\cancel{b}d & -bd \\ 0 & \cancel{-d}\,0 & -d \\ 1 & 0 & c \end{bmatrix}$$

$\omega^2 \cdot \omega = (-ac - b\omega - a\theta) \cdot \omega$

$= -ac \cdot \omega + b^2\omega + (\text{other})$

$\omega^2 \cdot \theta = \omega \cdot -ad.$

4/11/14 (p. 3). (27.3)

$$\mathrm{Tr}(\omega\theta) = \mathrm{Tr}(-ad) = -3ad$$

$$\mathrm{Tr}(\theta^2) = \mathrm{Tr}\begin{bmatrix} -bd & * & * \\ -d\omega & -ad & * \\ c\theta & * & -bd+c^2 \end{bmatrix}$$

$$\theta^2 \cdot \theta = (-bd - d\omega + c\theta)\,\theta$$
$$= -bd\theta + c^2\theta + (\text{non-}\theta).$$

$$\text{So, } \mathrm{Disc}(R) = \det\begin{bmatrix} 3 & -b & c \\ -b & -2ac+b^2-ad & -3ad \\ c & -3ad & -2bd-ad+c^2 \end{bmatrix}.$$

You could just use SAGE.

But, you could also observe it's homogeneous of degree 4,

and we proved that since you get the same ring for $f\circ\gamma$, for any $\gamma \in GL_2(\mathbb{Z})$, we get the same value of $\mathrm{Disc}(R)$.

So $\mathrm{Disc}(R)$ is a degree 4 polynomial in a, b, c, d which is $GL_2(\mathbb{Z})$-invariant.

So we must have $\mathrm{Disc}(R) = c \cdot \mathrm{Disc}(f)$ for some c.
(This is "well known".) (BST quote Hilbert 1897.)

What is the constant? $c=1$: Compute any example.

4/11/14. (p. 4) (224)

Prop. Given a cubic form f, the cubic ring is an ~~reducible~~ integral domain if and only if f is irreducible over $\mathbb{Z}$.

(Remark: BST state over $\mathbb{Q}$. Prove: Is equivalent!)

Proof. If $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ is
⊛ reducible, then by transforming by an elt. of $GL_2(\mathbb{Z})$
can assume that $a = 0$.

i.e. send the linear factor to y.

So $\omega\theta = n = -ad = 0$.

⊛: How to do this?

Suppose $f(x,y) = (rx + sy) \cdot \overbrace{h(x,y)}^{\text{quadratic}}$

Then $f \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (rx+sy) \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot h \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

$= (r[\alpha x + \beta y] + s[\gamma x + \delta y]) \cdot h \circ M$

Solve $(r[\alpha x + \beta y] + s[\gamma x + \delta y]) = y$

i.e. $\alpha r + s\gamma = 0$.
$\beta r + \delta s = 1$.

Now assume also $(r,s) = 1$. (If not, shove the factor into h.)

Find β and δ by the Euclidean algorithm.

But have to be a bit careful.

Take $\alpha = s, \gamma = -r$ (to solve first equation)

$\beta r + \delta s = 1$ (second equation)

$\det \begin{bmatrix} s & \beta \\ -r & \delta \end{bmatrix} = \pm 1$ so that $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \pm 1$.

Hey! Look! We win for free.

4/14/14. (28.1)

Counting cubic rings.

Theorem. (Davenport, 1951 ~~and Heilbronn~~)

Let $N^+(X) = \#\{SL_2(\mathbb{Z})\text{-equiv classes of irreducible IBCFs } f \text{ with } 0 < \mathrm{Disc}(f) < X\}$

$N^-(X) =$ same, $0 < -\mathrm{Disc}(f) < X$.

Then $N^+(X) \sim \frac{\pi^2}{36} X$, $N^-(X) \sim \frac{\pi^2}{12} X$.

But we can ask an easier question.

Do we know these are finite?

Lemma. (Davenport)

In the positive case, there is a representative $au^3 + bu^2v + cuv^2 + dv^3$ satisfying

$$|a| < X^{1/4}, \quad |b| < 2X^{1/4}, \quad |ad| < X^{1/2},$$
$$|bc| < 4X^{1/2}, \quad |ac^3| < 8X, \quad |b^3 d| < 8X,$$
$$c^2|bc - 9ad| < 4X.$$

Ex. Use this to obtain upper bounds on $N^{\pm}(X)$.

(Hint: irreducible $\Rightarrow ad \neq 0$.)

The representative will satisfy

$$-A < B \leq A < C \quad \text{with} \quad A = b^2 - 3ac$$
$$\text{or} \quad 0 \leq B \leq A = C \qquad B = bc - 9ad$$
$$C = c^2 - 3bd.$$

Def. The Hessian covariant of a BCF

$$au^3 + bu^2v + cuv^2 + dv^3$$

is

$$Ax^2 + Bxy + Cy^2,$$

where

$$A = b^2 - 3ac,$$
$$B = bc - 9ad,$$
$$C = c^2 - 3bd.$$

Properties. (1) We have $\mathrm{Disc}(H(f)) = -3\,\mathrm{Disc}(f)$.

(Here $\mathrm{Disc}\, H(f) = B^2 - 4AC$.)

(2) It is covariant for the action of $SL_2(\mathbb{Z})$, which means we have a commutative diagram

$$\begin{tikzcd} \mathrm{BCF} \arrow[r, "SL_2(\mathbb{Z})"] \arrow[d, "\text{Hessian}"] & \mathrm{BCF} \arrow[d, "\text{Hessian}"] \\ \mathrm{BQF} \arrow[r, "SL_2(\mathbb{Z})"] & \mathrm{BQF} \end{tikzcd}$$

Note that the discriminant is also a covariant

$$\begin{tikzcd} \mathrm{BCF} \arrow[r, "SL_2(\mathbb{Z})"] \arrow[d] & \mathrm{BCF} \arrow[d] \\ \mathrm{Disc} \arrow[r, "SL_2(\mathbb{Z})"] & \mathrm{Disc} \end{tikzcd}$$

where $SL_2(\mathbb{Z})$ acts on $\mathbb{R}$ by $x \circ \gamma = (\det \gamma) \cdot x$.
(i.e., here, trivially).

Notes: (1) All of this can be computed mechanically.

(2) Gives us a good way to define a <u>reduced</u> BCF: demand that its Hessian be reduced.

We define the Hessian in terms of the determinant

$$-\frac{1}{4}\det\begin{bmatrix} \frac{\partial^2 f}{\partial u^2} & \frac{\partial^2 f}{\partial u \partial v} \\ \frac{\partial^2 f}{\partial u \partial v} & \frac{\partial^2 f}{\partial v^2} \end{bmatrix} = -\frac{1}{4}\det\begin{vmatrix} 6au + 2bv & 2bu + 2cv \\ 2bu + 2cv & 6dv + 2cu \end{vmatrix}$$

$$= -\frac{1}{4}\cdot (6au + 2bv)(6dv + 2cu) - (2bu + 2cv)^2$$

$$= -\frac{1}{4}\cdot u^2[12ac - 4b^2] + uv[36ad + 4bc - 8bc] + v^2[12bd - 4c^2]$$

$$= u^2[b^2 - 3ac] + uv[bc - 9ad] + v^2[c^2 - 3bd].$$

Now, if $f = (r_1 u - s_1 v)(r_2 u - s_2 v)(r_3 u - s_3 v)$,

$$\mathrm{Disc}(f) = \prod_{i,j} (s_i r_j - r_i s_j)^2$$