Binary cubic forms over a ring $R$

A binary cubic form is an expression

$$f(u, v) = a u^3 + b u^2 v + c u v^2 + d v^3 : a, b, c, d \in R$$

It admits an action of $GL_2(R)$ given by

$$(f \circ g)((x, y)) = f(g(x, y)).$$

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), $\mathcal{A}_K$ (adeles)

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

Recall. We already studied binary quadratic forms

$$f(u, v) = a u^2 + b u v + c v^2$$

same action of $GL_2$. What did we prove about them?

1. There is an invariant, called the discriminant,
   $$\Delta(f) = b^2 - 4ac,$$
   for which
   $$\text{Disc}(fg) = (\text{det } g)^2 \cdot \text{Disc}(f),$$
   for which
   $$\Delta(f) = 0 \iff \exists \Delta \in \mathbb{R} \setminus \{0\}$$
   has a double root.

2. A form properly represents an integer $m$ iff it is $SL_2(\mathbb{Z})$-equivalent to $m x^2 + b x y + c y^2$ for some $b, c \in \mathbb{Z}$. 
(3) There is a reduction theory:
Suppose $D < 0$. Then, each BQF is equivalent to a unique reduced form for which:
1. $|b| \leq a_0 \leq c$,
2. $b \geq 0$ if either $|b| = a$ or $a = c$.

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

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

(5) $h(D) \neq 0 \iff D \equiv 0, 1 \pmod{4}$

(6) In fact, get a theorem $BQF(\mathbb{Z})/SL_2(\mathbb{Z})$ ~ ideals of $\mathbb{Z}[\sqrt{-D}]$.

(6) We had explicit formulas:

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

(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 barty*

*stabilize groups are infinite.*

Q. What translates to binary cubic forms?

**Defn.** A binary $n$-ic form is an expression

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

with an action of $GL_n(\mathbb{R})$:

$$(f, g)(u, v) = f(g(u), v).$$
It turns out, $n=2$ and $n=3$ are special.
You get a \underline{prehomogeneous vector space}.
We will see why this matters.

Binary cubic forms.
\underline{What are we counting?}

\textbf{Def.} The \underline{discriminant} of a binary cubic form
\[ f(u,v) = au^3 + bu^2v + cuv^2 + dv^3 \]
is\[ \text{Disc}(f) = b^2c^2 + 18abcd - 4a^3 - 4b^3d - 27a^2d^2. \]

\textbf{Theorem.} If $g \in \text{GL}_2(\mathbb{R})$, then
\[ \text{Disc}(f \circ g) = (\det g)^6 \text{Disc}(f). \]

\underline{Note.} This is very big.

\underline{Shitty proof.} For general \[ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \]
\[ f(\ell,\delta) \circ g(u,v) \circ g(u,v) = f(au+bv, cu+dv). \]
FOIL it out. Plug into the formula above.
\underline{(Coerce Sage into doing this.)}

Think about what we want to generalize.

\textbf{Def.} The \underline{discriminant} of a monic cubic polynomial
\[ f(u) = u^3 + bu^2 + cu + d \]
is\[ \text{Disc}(f) = b^2c^2 + 18bcd - 4c^3 - 4b^3d - 27d^2. \]
Also, if \( f(u) = (u - \theta_1)(u - \theta_2)(u - \theta_3) \) (possibly over some extension), then \( \text{Disc}(f) = \left( (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3) \right)^2 \).

**Properties.**

(*) \( \text{Disc}(f) = 0 \quad \iff \quad f \text{ has a multiple root}. \)

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 every auto-distinct factor.

Suppose for simplicity \( R \) is a field.

Then \( R[u]/(u - \theta_1)(u - \theta_2)(u - \theta_3) \) maps \( \sim \) \( \frac{R[u]}{u - \theta_1} \times \frac{R[u]}{u - \theta_2} \times \frac{R[u]}{u - \theta_3} \)

by the natural reduction map.

(This is the Chinese remainder theorem.)

Careful! Not true over rings in general. The map

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

\[ \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \]

is not surjective. Nothing maps to \((1, 0, 0)\).
Say we have a repeated root. (again, \( R \) a field)

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

Then \( u-\theta_i \) is a nilpotent element.

(Example. \( f \) is the min poly of a field extension, look at its mod primes, i.e. in finite fields, \( \mathbb{F}_p \) for \( q \) )

\[
\text{Disc}(f) = 0 \quad \text{in} \quad \mathbb{F}_p \quad \Rightarrow \quad \mathbb{F}_p[u]/(f) \quad \text{is not an integral domain.}
\]

\[
p \mid \text{Disc}(f)
\]

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

\[
\text{Disc}(f) = (\theta_1 - \theta_2)^2
\]

\[
\begin{align*}
= (\theta_1 + \theta_2)^2 - 4\theta_1 \theta_2 \\
= b^2 - 4c.
\end{align*}
\]

For cubic polynomials,

\[
(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 + bx^2 + cx + d
\]

\[
= x^3 - [\theta_1 + \theta_2 + \theta_3] x^2 + [\theta_1 \theta_2 + \theta_1 \theta_3 + \theta_2 \theta_3] x - \theta_1 \theta_2 \theta_3.
\]

You can do this. There are shortcuts.

Now, more generally, the discriminant of \((a_i x - b_i y)(a_i x - b_i y) \cdots (a_n x - b_n y)\) is

\[
\left[ \prod_{i \neq j} (a_i b_j - a_j b_i) \right]^2
\]
Exercise.

(1) Given a binary form with leading coefficient, prove

\[
\text{Disc} \left( \sum_{i=0}^{n} a_i x^i \right) = \text{Disc} \left( \sum_{i=0}^{n-1} a_i x^i \right)
\]

more generally, if \( a_n \neq 0 \):

\[
= a_n \cdot 2^{n-2} \cdot \text{Disc} \left( \sum_{i=0}^{n-1} a_i x^i \right)
\]

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

\[
= a_{n-1} \cdot 2^{n-2} \cdot \text{Disc} \left( \sum_{i=0}^{n-2} a_i x^i \right)
\]

If \( a_n = 0 \) and \( a_{n-1} = 0 \):

\[
= 0
\]

How to prove these formulas?

(1) "But it out." Symmetric polynomials. (See Hw)

(2) Use resultants.

(3) Lie algebras / differentiable manifolds proof.

Homework:

(1) Familiar to Jesse veterinary.

(2) 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.

\[
\begin{align*}
u^3 + bu^2 + cu + d &= v^3 + \left( c - \frac{b^2}{3} \right) v + \left( d - \frac{bc}{3} + \frac{2b^3}{27} \right) \\
&= v^3 + Cv + D \\
&= (v - P)(v - S)(v - T).
\end{align*}
\]

Now, \( \text{Disc } (F) = F'(P) F'(S) F'(T) \)

\[
\begin{align*}
&= (3P^2 + C)(3S^2 + C)(3T^2 + C) \\
&= \ldots \\
&= -27D^2 - 4C^3.
\end{align*}
\]
Delone - Faddeev over fields. (Think: \( K = \mathbb{Q} \))

**Proposition.** Let \( K \) be a field. There is a bijection

\[
\text{Irr. } \text{BCF}(K) / \text{GL}_2(K) \leftrightarrow \text{cubic field extensions } L/K.
\]

You get it as follows. (Two equivalent descriptions)

1. Given \( au^3 + bu^2v + cuv^2 + dv^3 = (r_1u - s_1v)(r_2u - s_2v)(r_3u - s_3v) \) over \( K \), take \( K\left(\frac{s_1}{r_1}\right) \) over \( K \).

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 \( 2(u^3 + uv^2 + v^3) \)

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

Fields generated by \( \frac{s_1}{1} \) and \( \frac{3\sqrt{2}s_1}{3\sqrt{2}} \). Same field.

We want \( u^3 + uv^2 + v^3 \) and \( 2(u^3 + uv^2 + v^3) \) to be equivalent. Change the action.

**Def.** The twisted action of \( \text{GL}_2 \) on binary cubic forms is

\[
(f \circ g)(u, v) = \frac{1}{\det g} f(g(u, v)).
\]
Proposition. With the twisted action, scalar matrices $(\lambda\lambda)$ act as multiplication by $\lambda$.

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

Then $(f \circ (\lambda\lambda))(uv) = \frac{1}{\det(\lambda\lambda)} f((\lambda\lambda)(uv))$

$= \frac{1}{\lambda^2} f(\lambda uv)$

$= \frac{1}{\lambda^2} \left[ a\lambda^3 u^3 + b\lambda^2 u^2 v + c\lambda uv^2 + d\lambda^3 v^3 \right]$

$= \lambda \cdot f$.

The proposition is true with the twisted action.

Examples.

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

$k = \mathbb{C}$. Cubic field 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 BCFSs over $\mathbb{F}_p$ and they are all $GL_2(\mathbb{F}_p)$-equivalent.
Proof of DF over a field.

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

\[
= (r_1u - s_1v)(r_2u - s_2v)(r_3 - s_3v).
\]

Then \( f \circ \left( \begin{array}{c}
\frac{a}{f} \\
\frac{b}{f} \\
\frac{c}{f} \\
\frac{d}{f}
\end{array} \right)(v) = f \left( \begin{array}{c}
au + bv \\
u + dv
\end{array} \right) \)

\[
= \left( r_1[a + \beta v] - s_1 \right) \left( yu + \delta v \right) \times \text{two more}
\]

\[
= \left( [r_1 + s_1 \delta]u + [r_1 \beta - s_1 \delta]v \right) \times \text{two more}.
\]

So your "field" is \( K \left( \frac{s_1 \delta - r_1 \beta}{r_1 + s_1 \delta} \right) \).

If \( r_1u - s_1v \) were defined over \( K \) (contrary to assumption),
then so would \( [r_1 + s_1 \delta]u + [r_1 \beta - s_1 \delta]v \).

Because we have a group action and can consider
\[
\left( \begin{array}{c}
\frac{a}{f} \\
\frac{b}{f} \\
\frac{c}{f} \\
\frac{d}{f}
\end{array} \right)^{-1},
\]
shows that \( [r_1 + s_1 \delta]u + [r_1 \beta - s_1 \delta]v \)

is not defined over \( K \). So action sends \( \text{irred} \) \( \rightarrow \text{irred} \).

So, in particular, we do get a field.

\[
K \left( \frac{s_1 \delta - r_1 \beta}{r_1 + s_1 \delta} \right) \subseteq K \left( \frac{s_1}{r_1} \right).
\]

By reversing the action or arguing using degrees, these
must be equal.
Now let $\theta = \frac{s_1}{r_1}$ and suppose that $L = K(\theta')$ for some $\theta'$. We must argue there is some element of $GL_2(K)$ taking $\theta$ to $\theta'$.

It suffices to prove, $\theta' = \frac{r\theta + s}{t\theta + u}$ 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

$$(x_0 + x_1\theta + x_2\theta^2)(t\theta + u) = r\theta + s \text{ in } r, s, t, u.$$

Foil it and use the min poly:

$$\left(x_0u - \frac{d}{a}x_2t\right) + \theta\left(x_1u + x_0 + \frac{c}{a}x_2t\right) + \theta^2\left(x_2u + x_1 + \frac{b}{a}x_2t\right) = r\theta + s.$$

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

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

That takes care of the $\theta^2$ term.

Get to pick $r$ and $s$, so we win for free. $\Box$.

Note: We can see this would not work for quartic fields.

Would have to solve

$$(x_0 + x_1\theta + x_2\theta^2 + x_3\theta^3)(t\theta + u) = r\theta + s \text{ in } r, s, t, u.$$

We're only interested in $[r : s : t : u] \in P^3(K)$.

3-dimensional space of solutions.

4-dimensional span 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 reducible cubic forms?

Delhomogenize and take a root.

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

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

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

We'll answer these questions next time.
Claim. There is a bijection
\[ \frac{\text{Irr BCF}(K)}{\text{GL}_2(K)} \rightarrow \text{cubic field exts.} \quad L/K. \]

The action is the twisted action \((f \circ g)(v) = \frac{1}{(\det g)}f(g(v)).\)

Last time.

1. There is a map \(\text{Irr BCF}(K) \rightarrow \text{cubic field exts.}\)
\[ (r, u - s, v) \times \text{[two more]} \rightarrow K\left(\frac{s_1}{r_1}\right). \]

2. It is WD up to the \(\text{GL}_2(K)\) -action, because
\[ \frac{s_1}{r_1} \circ \left(\begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array}\right) = \frac{s_1}{r_1} \left(\begin{array}{cc} \delta - \beta \\ \gamma - s_1 \frac{s_1}{r_1} \delta \end{array}\right). \]

3. It is injective. Can prove if \(L = K(\theta) = K(\theta')\) then \(\theta' = \frac{r\theta + s}{\theta + w}\) for some \(r, s, t \in \text{K}.\)

*4. It is surjective.

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

The cubic form
\[(u - \theta v)(u - \theta' v)(u - \theta'' v) = u^3 + a_2 u^2 + a_1 uv^2 + a_0 v^3\]
yields \(L.\)
The generalization.
Let $R$ be any integral domain commutative.
A cubic ring over $R$ is any ring which is a rank 3 free $R$-module.

Ex. Let $R$ be the field $\mathbb{Q}$.
Then cubic fields are cubic rings over $R$.

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

$$= \mathbb{Z} \oplus \mathbb{Z}[\sqrt[3]{2}] \oplus \mathbb{Z}[\sqrt[3]{-2}]$$
as a $\mathbb{Z}$-module
(i.e. as an abelian group).

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

$\cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.
once again a cubic ring.
not an integral domain.

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

(1). Let $O$ be a cubic ring over $R$.
We can write $O = Rx_1 \oplus Rx_2 \oplus Rx_3$.

If $\theta \in O$, the map $x \mapsto \theta x$ defines an endomorphism $O \rightarrow O$ of $R$-modules.

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

(2). The discriminant of $O$ is

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

for shorthand, $\det \left( \text{Tr}(x_i; x_j) \right)$

or the determinant of the bilinear pairing $\text{Tr}(\theta \lambda)_{\theta, \lambda} \in R^3 \otimes R^3$

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

Warning. This is an element of $O \otimes_R R/(Rx)^2$.

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

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

Example. If $O = \mathbb{Z}$, $O = \mathbb{Z}[x]/(x^3 - 2) = \mathbb{Z}[\sqrt[3]{2}]$

$= \mathbb{Z} \oplus \frac{1}{\sqrt[3]{2}} \mathbb{Z}[\sqrt[3]{4}]$.

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

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


\[ \text{Tr}(1) : \text{ Sends } 1 \rightarrow 1 \]
\[
\begin{align*}
3\sqrt{2} &\rightarrow 3\sqrt{2} \\
3\sqrt{4} &\rightarrow 3\sqrt{4} \\
3\sqrt{4} &\rightarrow 2
\end{align*}
\]
\[ \text{Tr}(1) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 3. \]

\[ \text{Tr}(3\sqrt{2}) : \text{ Sends } 1 \rightarrow 3\sqrt{2} \]
\[
\begin{align*}
3\sqrt{2} &\rightarrow 3\sqrt{2} \\
3\sqrt{4} &\rightarrow 3\sqrt{4} \\
3\sqrt{4} &\rightarrow 2
\end{align*}
\]
\[ \text{Tr}(3\sqrt{2}) \cdot \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 0. \]

\[ \text{Tr}(3\sqrt{4}) : \]
\[ \text{Tr}(3\sqrt{4}) \cdot \begin{bmatrix} 0 & 2 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix} = 0. \]

\[ \text{Tr}(2) = \text{Tr}(2) \cdot \begin{bmatrix} 2 & 2 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 6. \]

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

So, \( \text{Disc}(\theta) = \text{det} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix} = -3 \cdot 6 \cdot 6 \]
\[ = -108. \]

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

\[ \text{Tr}(1) = 3 \text{ as before.} \]
\[ \begin{array}{l}
\text{X sends} \\
1 \rightarrow x \\
x \rightarrow x^2 \\
x^2 \rightarrow 0,
\end{array} \]
\[ \text{Tr}(x^2) = \text{Tr}(x^2) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 0. \]

\[ \text{Disc} \text{ det is} \]
\[ \text{Tr}(x^3) = \text{Tr}(0) = 0. \]
\[ \text{Tr}(x^4) = 0. \]
\[ \text{det} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 0. \]

More examples if time!
Some more trace computations.

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

First:

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

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

$x_1: \text{Tr} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 3$

$x_2: \text{Tr} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 0$

$x_3: \text{Tr} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = 2$

$x_4: \text{Same as } x_2$.

$x_5: \text{Same as } x_3$.

So:

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

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

Theorem. There is a natural, discriminant-preserving bijection

$\mathbb{BCF}(\mathbb{Z}) / \mathbb{GL}_2(\mathbb{Z}) \rightarrow \text{cubic rings}$

Proof. (BST) (1) Get a map $\text{cubic rings} \rightarrow \text{cubic forms}$.

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

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

Why is this? If \( \omega \cdot \theta = r_1 + r_2 \omega + r_3 \theta \),

\[
(w \cdot r_3)(\theta - r_2) = \omega \theta - r_3 \theta - r_2 \omega + r_2 r_3
\]

\(= r_1 + r_2 r_3 \), and

\(\mathbb{Z} \oplus \mathbb{Z} \omega \oplus \mathbb{Z} \theta = \mathbb{Z} \oplus \mathbb{Z}(\omega - r_3) \oplus \mathbb{Z}(\theta - r_2)\).

Write out the multiplication table:

\[
\omega \cdot \theta = n,
\]

\[
\omega^2 = m - \omega \omega + a \theta
\]

\[
\theta^2 = l - d \omega + c \theta
\]

Our form is \(a \omega^3 + b \omega^2 \nu + c \omega \nu^2 + d \nu^3\).

[What?!]

This represents the cubic map

\[
\mathbb{R}/\mathbb{Z} \rightarrow \Lambda^2(\mathbb{R}/\mathbb{Z}) \cong \mathbb{Z}
\]

\(q \mapsto q \wedge q^2\).

If \(q = x \omega + y \theta\),

\[
(x \omega + y \theta)^2 = (x \omega + y \theta)^2
\]

\[
= (x \omega + y \theta)^2 \wedge \left[ x^2 \omega^2 + y^2 \theta^2 + 2xy \omega \theta \right]
\]

\[
= (x \omega + y \theta)^2 \wedge \left[ x^2(m - \omega \omega + a \theta) + y^2(l - d \omega + c \theta) + 2xy \nu \right]
\]

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

\[
= (x \omega + y \theta)^2 \wedge \left[ x^2(b \omega - a \theta) + y^2(d \omega - c \theta) \right]
\]
\[ (26.3) \]
\[
= x^3 w \wedge (bw - a \theta) + x^2 y \theta \wedge (bw - a \theta) \\
+ xy^2 w \wedge (dw - c \theta) + y^3 \theta \wedge (dw - c \theta) \\
= -a \cdot x^3 w \wedge \theta + b x^2 y \theta \wedge w - c x y^2 w \wedge \theta \\
+ d y^3 \theta \wedge \omega w \\
= (a x^3 + b x^2 y + c y^2 + d y^3) \theta \wedge w.
\]

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

\[
\begin{bmatrix}
w' \\
\theta'
\end{bmatrix} = \begin{bmatrix}
a & \beta \\
\gamma & \delta
\end{bmatrix}\begin{bmatrix}
w \\
\theta
\end{bmatrix}
\]

with \( \begin{bmatrix}
a & \beta \\
\gamma & \delta
\end{bmatrix} \in \text{GL}_2(\mathbb{Z}) \)

and then renormalize again.
Get a basis \((1, w', \theta')\) with \(w'' - w' \in \mathbb{Z}
\theta'' - \theta' \in \mathbb{Z}\)

\(w'' \in \mathbb{Z}\).

Then, where does

\[
x w'' + y \theta'' \to ?
\]

\[
x w'' + y \theta'' = x (a w + \beta \theta) + y (\gamma w + \delta \theta) \quad \text{in } \mathbb{R}/\mathbb{Z}
\]

\[
= \left[ x + y \gamma \right] w + \left[ x \beta + y \delta \right] \theta.
\]

Choose down under the same map.
Get the binary cubic form

\[
a[x_0 + y_1]^3 + b[x_0 + y_1]^2[x_0 + y_2] + c[x_0 + y_1][x_0 + y_2]^2
\]

\[(x_0 + y_1)[x_0 + y_2]^3
\]

\[
= f(x_0 + y_1, x_0 + y_2) = f \left( \begin{bmatrix}
a & \beta \\
\gamma & \delta
\end{bmatrix}\begin{bmatrix}
x_0 \\
y_1
\end{bmatrix} \right) = f \left( \begin{bmatrix}
a & \beta \\
\gamma & \delta
\end{bmatrix}\begin{bmatrix}
x \\
y
\end{bmatrix} \right)
\]

\[
= f \left( \begin{bmatrix}
a & \beta \\
\gamma & \delta
\end{bmatrix}\begin{bmatrix}
x \\
y
\end{bmatrix} \right)
\]
To go back:

Given \( ax^3 + bx^2 y + cxy^2 + dy^3 \).

Write out \( w \theta = n \)

\[
\begin{align*}
w^2 &= m - bw + a \theta \\
\theta^2 &= l - dw + c \theta
\end{align*}
\]

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 \( w(w \theta) = (w^2) \theta \), \( (w^3)(\theta^2) = \theta^3 \).

If these are satisfied, get a cubic ring.

\[
w(w \theta) = nw
\]

\[
(w^2) \theta = (m - bw + a \theta) \theta = \theta^2 - bw \theta + a \theta^2
\]

\[
= \theta^2 - b \cdot n + a \cdot l - adw + ac \theta
\]

\[
= [\theta^2 - bn + al] - [adw] + [ac \theta]
\]

So: \( -bn + al = 0 \), \( ac + m = 0 \), \( -ad = n \), \( w - bu + al = 0 \).

\[
(w \theta) \theta = n \cdot \theta
\]

\[
w \cdot \theta^2 = w(l - dw + c \theta) = w \cdot l + c \cdot n - d[w - bw + a \theta]
\]

\[
= [-dm + cn] + w[l + bd] + \theta[-ad]
\]

\[-ad = n, \]

\( l + bd = 0 \)

\(-dm + cn = 0 \).
So we get
\[ n = -ad, \; m = -ac, \; l = -bd. \]

Two more equations:
\[ -bn + al = 0 \quad \text{Says} \quad bad + a(-bd) = 0 \quad \checkmark \]
\[ -dm + cu = 0 \quad \text{Says} \quad -d(-ac) + c(-ed) = 0. \quad \checkmark \]

So, subject to these conditions, we win.
Ex. Let \( \theta \) be a root of \( x^3 - x - 1 \).

Choose \( \mathbb{Z}[\theta] \) through DF and see what you get.

**Ans.** \( \mathbb{Z}[\theta] \cong \mathbb{Z} \oplus \mathbb{Z} \theta \oplus \mathbb{Z} \theta^2 \),

and \( \theta \cdot \theta^2 = \theta^3 = \theta + 1 \), so

\( \theta \cdot [\theta^2 - 1] = 1 \).

So \( \mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z} w \oplus \mathbb{Z} \theta \), with \( w = \theta \) and \( \theta = \theta^2 - 1 \).

\[ \begin{align*}
\omega \cdot \omega &= 1, \\
\theta^2 &= (\theta^2 - 1)^2 \\
&= \theta^4 - 2 \theta^2 + 1 \\
&= \theta^2 + \theta - 2 \theta^2 + 1 \\
&= -\theta^2 + \theta - 1 \\
&= 0 - (-1)w + (-1)\theta \\
&= -\theta + w \\
\omega^2 \theta &= \theta^2 \\
&= (\theta^2 - 1) + 1 \\
&= \theta + 1 \\
&= 1 - 0 \cdot w + 1 \cdot \theta.
\end{align*} \]

So our cubic ring is

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

Exercise. True or false?

Let \( \alpha \) be a root of \( x^3 + bx^2 + cx + d \).

Then the cubic form you always get is \( x^3 + bx^2 \cdot y + cxy^2 + dy^3 \).

If false, are there conditions which make it true?
Ex. Consider the cubic ring \( \mathcal{O} \).
What does it correspond to?

\[ \mathbb{Z} \oplus \mathbb{Z} \omega \oplus 2 \mathcal{O}, \]

with \( \omega \theta = -ad \), \( \omega^2 = -ac - bw - a\theta \), \( \theta^2 = -bd - dw + c\theta \).

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

Proposition. If a cubic ring \( R \) corresponds to a cubic form \( f \), then \( \text{Disc}(R) = \text{Disc}(f) \).

Exercise. Verify it by brute force.

But, we can be a bit more clever.

\[ \text{Disc}(f) = \det \begin{bmatrix} \text{Tr}(1) & \text{Tr}(w) & \text{Tr}(\theta) \\ \text{Tr}(w) & \text{Tr}(w^2) & \text{Tr}(w\theta) \\ \text{Tr}(\theta) & \text{Tr}(w\theta) & \text{Tr}(\theta^2) \end{bmatrix} \]

\[ \text{Tr}(1) = 3. \]
\[ \text{Tr}(w) = \text{Tr} \begin{bmatrix} 0 & -ac & -ad \\ 1 & -b & -a\theta \\ 0 & -d & 0 \end{bmatrix} \]
\[ \text{Tr}(\theta) = \text{Tr} \begin{bmatrix} 0 & -bd & -bd \\ 0 & -a\theta & -d \\ 1 & 0 & c \end{bmatrix} \]

\[ \text{Tr}(w^2) = \begin{bmatrix} -ac & * & * \\ -b & -ac + b^2 & * \\ -a & * & -ad \end{bmatrix} \]

\[ w^2 \cdot w = (-ac - bw - a\theta) \cdot w = -ac \cdot w + b^2 w + (\text{other}) \]
\[ w^2 \cdot \theta = w \cdot -ad. \]
Tr \( \omega \theta \) = Tr \( \omega - \omega d \) = -3ad

\[ \begin{align*}
\text{Tr} (\theta^2) &= \text{Tr} \begin{bmatrix}
-bd & x & x \\
-dw & -ad & x \\
c\theta & x & -bd+c^2
\end{bmatrix} \\
\theta^2 \cdot \theta &= (-bd - dw + c\theta \theta) \cdot \theta \\
&= -bd \theta \theta \cdot x + c\theta \theta \cdot x + (\text{non-} \theta).
\end{align*} \]

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

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 \( \gamma \in \text{SL}_2(\mathbb{C}) \), we get the same value of Disc (R).

So, Disc (R) is a degree 4 polynomial in \( a, b, c, d \) which is \( \text{GL}_2(\mathbb{C}) \) invariant.

So we must have Disc (R) = c \cdot Disc (f) for some c.

(This is "well known".) (BST quote Hilbert 1897.)

What is the constant? c = 1. Compute any example.
Prop. Given a cubic form \( f \), the cubic ring is an integral domain if and only if \( f \) is irreducible over \( \mathbb{K} \).

(Remote: BST state over \( \mathbb{R} \). 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 \( \text{GL}_1(\mathbb{K}) \), we can assume that \( a = 0 \).

i.e. send the linear factor to \( y \).

So \( w_0 = \omega_n = -ad = 0 \).

How to do this?

Suppose \( f(x, y) = (rx + sy) \cdot g(x, y) \).

Then \( f \circ (^r_s) = (rx + sy) \cdot g \circ (^t_u) = (^a_b \cdot ^t_u) \cdot g \).

\[ = (r[a x + \beta y] + s[y x + \delta y]) \cdot g \cdot M \]

Solve \( (r[a x + \beta y] + s[y x + \delta y]) = y \)

i.e. \( qr + sy = 0 \).

\( \beta r + \delta s = 1 \).

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

Find \( \beta \) and \( \delta \) by the Euclidean algorithm.

But have to be a bit careful,

Take \( q = s \), \( r = -s \) (to solve first equation)

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

\[ \det \left[ \begin{array}{cc} s & \beta \\ -r & \delta \end{array} \right] = \pm 1 \] so that \( \left[ \begin{array}{cc} r & \beta \\ s & \delta \end{array} \right] = \pm I \).

How! Look! We win for free.
4/14/14. (25:1)

Counting cubic rings.

Theorem. (Davenport, 1951)

Let \( N^+(X) = \# \{ \text{\#I B C F's f} \} \) be the equivalent classes of \( X \) with \( 0 < \text{Disc}(f) < X \)

\[ N^-(X) = \text{same, } 0 < -\text{Disc}(f) < X. \]

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

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

Ex. Use this to obtain upper bounds on \( N^+(X) \).

(Hint: irreducible \( \implies ad \neq 0. \))

The representative will satisfy

\[ -A < B \leq A < C \text{ with } \]
\[ A = b^2 - 3ac \]
\[ B = hc - 9ad \]
\[ C = c^2 - 3bd. \]
Def. The Hessian covariant of a BCF $\phi$

$$au^3 + bu^2v + cuv^2 + dv^3 \quad \text{is}$$

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

where

$$A = b^2 - 3ac,$$

$$B = bc - 9ad,$$

$$C = c^2 - 3bd.$$

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

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

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

$$\begin{array}{ccc}
\text{BCF} & \overset{SL_2(\mathbb{R})}{\longrightarrow} & \text{BCF} \\
\downarrow\text{Hessian} & & \downarrow\text{Hessian} \\
\text{BCF} & \overset{SL_2(\mathbb{R})}{\longrightarrow} & \text{BCF} \\
\end{array}$$

Note that the discriminant is also a covariant

$$\begin{array}{ccc}
\text{BCF} & \overset{SL_2(\mathbb{R})}{\longrightarrow} & \text{BCF} \\
\downarrow\text{Disc} & & \downarrow\text{Disc} \\
\text{Disc} & \overset{SL_2(\mathbb{R})}{\longrightarrow} & \text{Disc} \\
\end{array}$$

Where $SL_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by $x \cdot f = (\det f) \cdot x$,

(i.e., here, trivially).
Notes: (1) All of this can be computed mechanically.
(2) Gives us a good way to define a reduced BCF: demand that its Hessian be reduced.

We define the Hessian in terms of the determinant

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

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

\[
= \frac{-1}{4} \cdot u^2 \left[ 36ac - 4b^2 \right] + uv \left[ 36 \cdot ad + 4bc - 6bc \right]
\]

\[
+ v^2 \left[ 12bd - 4c^2 \right]
\]

\[
= u^2 \left[ b^2 - 3ac \right] + uv \left[ bc - 9ad \right] + v^2 \left[ c^2 - 3bd \right]
\]

Now, if \( f = (r_1u - s_1v)(r_2u - s_2v)(r_3u - s_3v) \),

\[
\text{Disc}(f) = \prod (s_ir_j - r_is_j)^2
\]