Bhargava’s cube law and cohomology

Wouter Zomervrucht

Diamant symposium, May 27, 2016

Universiteit Leiden & Freie Universität Berlin
235. Si forma \( AXX + 2BXY + CYY \ldots \)
\( F \) transit in productum e duabus formis \( axx + abxy + cyy \ldots f, \) et \( a'x'x' + 2b'x'y' + c'y'y' \ldots f' \) per substitutionem talem \( X = pxx' + p'xy' + p''yx' + p'''yy', \)
\( Y = qxx' + q'xy' + q''yx' + q'''yy' \) (quod breuitatis causa in sequentibus semper ita exprimemus: \( F \) transit in \( ff' \) per substitutionem \( p, p', p'', p''' ; q, q', q'', q''' *) \),
dicemus simpliciter, formam \( F \) transformabilent esse in \( ff' \); si insuper haec transformatio ita est comparata, vt sex numeri \( pq' - qp', pq'' - qp'', \)
\( pq''' - qp''', p'q'' - q'p'', p'q''' - q'p''', p''q'' - \)
\( q''p''' \) divisorem communem non habeant: formam \( F \) e formis \( f, f' \) compositam vocabimus.
- Carl Friedrich Gauss (1801)
  binary quadratic forms

- Peter Gustav Lejeune Dirichlet (1839)
  quadratic class groups

  higher composition laws
- Carl Friedrich Gauss (1801)
  binary quadratic forms

- Peter Gustav Lejeune Dirichlet (1839)
  quadratic class groups

  higher composition laws
Gauss composition
Bhargava’s cube law
Geometry and cohomology

History
Binary quadratic forms
Class groups

- Carl Friedrich Gauss (1801)
  binary quadratic forms

- Peter Gustav Lejeune Dirichlet (1839)
  quadratic class groups

  higher composition laws
A binary quadratic form is an expression

$$q = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$ 

It is primitive if $\gcd(a, b, c) = 1$.

The group $SL_2(\mathbb{Z})$ acts on binary quadratic forms by variable substitution. The discriminant

$$\Delta q = b^2 - 4ac$$

is invariant under this action.
Let \( D \equiv 0, 1 \mod 4 \). We define

\[
Q_D(\mathbb{Z}) = \{ \text{primitive binary quadratic forms of discriminant } D \}.
\]

**Theorem (Gauss)**

For any two \( q_1, q_2 \in Q_D(\mathbb{Z}) \) there exists a third \( q \in Q_D(\mathbb{Z}) \) and forms \( u, v \in \mathbb{Z}[x_1, y_1, x_2, y_2]_{1,1} \) such that

\[
q_1(x_1, y_1) \cdot q_2(x_2, y_2) = q(u, v).
\]

This makes \( Q_D(\mathbb{Z})/\text{SL}_2(\mathbb{Z}) \) into a finite abelian group.
**Theorem (Gauss)**

For any two \( q_1, q_2 \in \mathbb{Q}_D(\mathbb{Z}) \) there exists a third \( q \in \mathbb{Q}_D(\mathbb{Z}) \) and forms \( u, v \in \mathbb{Z}[x_1, y_1, x_2, y_2]_{1,1} \) such that

\[
q_1(x_1, y_1) \cdot q_2(x_2, y_2) = q(u, v).
\]

This makes \( \mathbb{Q}_D(\mathbb{Z})/\text{SL}_2(\mathbb{Z}) \) into a finite abelian group.

**Example**

Suppose \( D \equiv 0 \mod 4 \). Then

- \( [x^2 - \frac{D}{4}y^2] = 0, \)
- \( [ax^2 + bxy + cy^2]^{-1} = [ax^2 - bxy + cy^2]. \)
Let $\mathcal{O}_D$ be the unique quadratic order of discriminant $D$.

**Example**

Suppose $D \neq 1$ is squarefree. Then $\mathcal{O}_D = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ is the maximal order in $\mathbb{Q}(\sqrt{D})$.

The class group of $\mathcal{O}_D$ is

$$\text{Cl}(\mathcal{O}_D) = \frac{\{\text{invertible fractional ideals}\}}{\{\text{invertible principal ideals}\}}.$$
There is also a *narrow* or *oriented class group* $\text{Cl}^+(\mathcal{O}_D)$ which fits into a short exact sequence

$$1 \longrightarrow \mathbb{Z}/N(\mathcal{O}_D^\times) \longrightarrow \text{Cl}^+(\mathcal{O}_D) \longrightarrow \text{Cl}(\mathcal{O}_D) \longrightarrow 1.$$

**Example**

If $D$ is negative, $\text{Cl}^+(\mathcal{O}_D) = \{\pm 1\} \times \text{Cl}(\mathcal{O}_D)$. 
**Theorem (Dirichlet)**

\[ Q_D(\mathbb{Z})/\text{SL}_2(\mathbb{Z}) \cong \text{Cl}^+(\mathcal{O}_D). \]

Roughly, \([ax^2 + bxy + cy^2]\) corresponds to \([\mathbb{Z} \oplus \frac{-b + \sqrt{D}}{2a} \mathbb{Z}]\).

**Example**

If \(D\) is negative, \(\text{Cl}^+(\mathcal{O}_D) = \{\pm 1\} \times \text{Cl}(\mathcal{O}_D)\). The subgroup \(\text{Cl}(\mathcal{O}_D) \subset \text{Cl}^+(\mathcal{O}_D)\) corresponds to *positive definite* forms.
A cube is a $2 \times 2 \times 2$-matrix of integers

The group $G(\mathbb{Z}) = \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$ acts on cubes. For instance, the first factor acts by

$$(\Box, \Box) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (\alpha \Box + \gamma \Box, \beta \Box + \delta \Box).$$
A *cube* is a $2 \times 2 \times 2$-matrix of integers

The group $G(\mathbb{Z}) = \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$ acts on cubes. For instance, the first factor acts by

$$(\square, \square) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (\alpha \square + \gamma \square, \beta \square + \delta \square).$$
Associated to a cube \( w \) are three binary quadratic forms \( q_1(w), q_2(w), q_3(w) \). For instance,

\[
q_1(\Box, \Box) = \det(\Box x_1 + \Box y_1).
\]

The discriminants satisfy

\[
\Delta q_1(w) = \Delta q_2(w) = \Delta q_3(w)
\]

and this number is the discriminant \( \Delta w \) of the cube.

A cube \( w \) is projective if \( q_1(w), q_2(w), q_3(w) \) are primitive. We define \( W_D(\mathbb{Z}) = \{ \text{projective cubes of discriminant } D \} \).
Theorem (Bhargava)

For any cube \( w \in W_D(\mathbb{Z}) \) the identity

\[
[q_1(w)] + [q_2(w)] + [q_3(w)] = 0
\]

holds in \( Q_D(\mathbb{Z})/SL_2(\mathbb{Z}) \). Conversely, if

\[
[q_1] + [q_2] + [q_3] = 0
\]

holds in \( Q_D(\mathbb{Z})/SL_2(\mathbb{Z}) \), there is a cube \( w \in W_D(\mathbb{Z}) \) satisfying
\( q_1(w) = q_1, q_2(w) = q_2, \) and \( q_3(w) = q_3 \).
Theorem (Bhargava)

There is a unique group law on $W_D(\mathbb{Z})/G(\mathbb{Z})$ such that the maps

$$q_1, q_2, q_3 : W_D(\mathbb{Z})/G(\mathbb{Z}) \rightarrow Q_D(\mathbb{Z})/SL_2(\mathbb{Z})$$

are group homomorphisms.

Theorem (Bhargava)

$$W_D(\mathbb{Z})/G(\mathbb{Z}) \cong \text{Cl}^+(\mathcal{O}_D) \times \text{Cl}^+(\mathcal{O}_D).$$
Theorem (Bhargava)

There is a unique group law on $W_D(\mathbb{Z})/G(\mathbb{Z})$ such that the maps

$$q_1, q_2, q_3 : W_D(\mathbb{Z})/G(\mathbb{Z}) \to Q_D(\mathbb{Z})/SL_2(\mathbb{Z})$$

are group homomorphisms.

Theorem (Bhargava)

$$W_D(\mathbb{Z})/G(\mathbb{Z}) \cong \text{Cl}^+(\mathcal{O}_D) \times \text{Cl}^+(\mathcal{O}_D).$$
Goal: explain class groups geometrically.

- group scheme $\text{SL}_2$ acting on $\mathbb{Q}_D \subset \mathbb{A}^3$
- group scheme $G = \text{SL}_2 \times \text{SL}_2 \times \text{SL}_2$ acting on $\mathbb{W}_D \subset \mathbb{A}^8$

We use arithmetic invariant theory and flat cohomology.
Example

Let $\text{SL}_2$ act on $(\mathbb{P}^1, \mathcal{O}(1))$. On global sections we retrieve the action of $\text{SL}_2(\mathbb{Z})$ on $\mathcal{O}(2)(\mathbb{P}^1) = \mathbb{Z}[x, y]_2$.

Let $G$ act on $(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(1, 1, 1))$. On global sections we get an action of $G(\mathbb{Z})$ on

$$\mathcal{O}(1, 1, 1)(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{Z}[x_1, y_1, x_2, y_2, x_3, y_3]_{1,1,1}.$$

Identifying cubes with $1, 1, 1$-forms, this is the action above.
Example

Let $\text{SL}_2$ act on $(\mathbb{P}^1, \mathcal{O}(1))$. On global sections we retrieve the action of $\text{SL}_2(\mathbb{Z})$ on $\mathcal{O}(2)(\mathbb{P}^1) = \mathbb{Z}[x, y]_2$.

Let $G$ act on $(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(1, 1, 1))$. On global sections we get an action of $G(\mathbb{Z})$ on

$$\mathcal{O}(1, 1, 1)(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{Z}[x_1, y_1, x_2, y_2, x_3, y_3]_{1,1,1}.$$  

Identifying cubes with $1, 1, 1$-forms, this is the action above.
Let $G$ act on $(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(1,1,1))$. On global sections we get an action of $G(\mathbb{Z})$ on

$$\mathcal{O}(1,1,1)(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{Z}[x_1, y_1, x_2, y_2, x_3, y_3]_{1,1,1}.$$ Identifying cubes with $1,1,1$-forms, this is the action above.

Example

Let $w \in W_D(\mathbb{Z})$ be a cube. The fibers of

$$Z(w) \xrightarrow{\pi_1} \mathbb{P}^1$$

are degenerate precisely above $Z(q_1(w))$. 
**Principle of transitive actions**

Let $\mathcal{C}/S$ be a site with final object $S$. Let $G$ be a sheaf of groups acting *transitively* on a sheaf of sets $X$. Let $x \in X(S)$ be a global section and $H \subseteq G$ the stabilizer of $x$.

The short exact sequence of sheaves of pointed sets

$$1 \to H \to G \xrightarrow{x} X \to 1$$

induces a longer exact sequence

$$1 \to H(S) \to G(S) \to X(S) \xrightarrow{\delta} H^1(S, H) \to H^1(S, G)$$

where $\delta(y)$ is the transporter $G_{y,x}$.
Principle of transitive actions

Let $\mathcal{C}/S$ be a site with final object $S$. Let $G$ be a sheaf of groups acting transitively on a sheaf of sets $X$. Let $x \in X(S)$ be a global section and $H \subseteq G$ the stabilizer of $x$.

If moreover
- $H$ is abelian,
- $H^1(S, G) = 1$,
then $G(S) \backslash X(S)$ has a $H^1(S, H)$-torsor structure independent of the choice of $x$. 

Wouter Zomervrucht
Let $T_D$ be the norm one unit group with respect to $\mathbb{Z} \to \mathcal{O}_D$. That is, if $\mathcal{O}_D = \mathbb{Z}[\tau]/(\tau^2 - b\tau + c)$, then

$$T_D = \{(u, v) : N(u + v\tau) = 1\} = \{(u, v) : u^2 + buv + cv^2 = 1\}.$$

One has $H^1_{fppf}(\mathbb{Z}, T_D) = \text{Cl}^+(\mathcal{O}_D)$. 
If $H \subset \text{SL}_2$ is the stabilizer of $x^2 + bxy + cy^2$ in $Q_D(\mathbb{Z})$, then

$$H^\flat \cong \mathbb{T}_D.$$ 

Here $H^\flat$ is the scheme-theoretic closure of the generic fiber.

**Theorem**

The set $Q_D(\mathbb{Z})/\text{SL}_2(\mathbb{Z})$ is canonically a torsor under $H^1_{\text{fppf}}(\mathbb{Z}, \mathbb{T}_D)$. 

The same is true if we replace $\mathbb{Z}$ by any Dedekind domain of characteristic not 2.
What is the stabilizer $H \subset G$ of a cube $w \in W_D(\mathbb{Z})$?

Generically, the projection

$$Z(w) \xrightarrow{\pi_{23}} \mathbb{P}^1 \times \mathbb{P}^1$$

is a blowup in two points. So $Z(w)$ is a degree 6 del Pezzo surface. It contains a hexagon of six $-1$-curves.
We find

\[ H^b \cong \ker \left( \mathcal{T}_D \times \mathcal{T}_D \times \mathcal{T}_D \rightarrow \mathcal{T}_D \right). \]

**Theorem**

The set \( W_D(\mathbb{Z})/G(\mathbb{Z}) \) is canonically a torsor under \( H^1_{\text{fppf}}(\mathbb{Z}, \mathcal{T}_D)^2 \).

The same is true if we replace \( \mathbb{Z} \) by any Dedekind domain of characteristic not 2.