Gauss composition and integral arithmetic invariant theory

David Zureick-Brown (Emory University)
Anton Gerschenko (Google)

Connections in Number Theory
Fall Southeastern Sectional Meeting

University of North Carolina at Greensboro, Greensboro, NC

Nov 8, 2014

Sums of Squares

Recall (p prime)

$$p = x^2 + y^2 \text{ if and only if } p = 1 \bmod 4 \text{ or } p = 2.$$

For products

$$(x^2 + y^2)(z^2 + w^2) = (xz + yw)^2 + (xw - yz)^2$$

Sums of Squares

Recall (p prime)

$p = x^2 + dy^2$ if and only if **[more complicated condition]**.

Example

$p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p = 1, 3 \mod 8$.

Example

$p = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p = 3$ or $p = 1 \mod 3$.

Sums of Squares

Recall (p prime)

$p = x^2 + dy^2$ if and only if **[more complicated condition]**.

For products

$$(x^2 + dy^2)(z^2 + dw^2) = (xz + dyw)^2 + d(xw - yz)^2$$

Integers represented by a quadratic form

General quadratic forms (initiated by Lagrange)

$$Q(x, y) \in \mathbb{Z}[x, y]_2$$

Recall (p prime)

$p = Q(x, y)$ for some $x, y \in \mathbb{Z}$ if and only if **[more complicated condition]**.

Composition law?

$$Q(x, y)Q(z, w) = Q(a, b)$$

Sums of Squares (Euler's conjecture)

Example

$p = x^2 + 14y^2$ for some $x, y \in \mathbb{Z}$ if and only if $\left(\frac{-14}{p}\right) = -1$ and $(z^2+1)^2 = 8$ has a solution mod p.

Example

$p = 2x^2 + 7y^2$ for some $x, y \in \mathbb{Z}$ if and only if $\left(\frac{-14}{p}\right) = -1$ and $(z^2+1)^2 - 8$ factors into two irreducible quadratics mod p.

Integers represented by a quadratic form (equivalence)

Equivalence of forms

1. $Q(x, y) \in \mathbb{Z}[x, y]_2$
2. $M \in \mathrm{SL}_2(\mathbb{Z})$, $Q^M(x, y) := Q(ax + by, cx + dy)$
3. $n \in \mathbb{Z}$ is represented by Q iff it is represented by Q^M.
4. **Reduced forms:** $|b| \leq a \leq c$ and $b \geq 0$ if $a = c$ or $a = |b|$.

Example

$$29x^2 + 82xy + 58y^2 \sim x^2 + y^2.$$

Gauss composition

Theorem (Gauss composition)

The reduced, non-degenerate positive definite forms of discriminant $-D$ form a finite abelian group, isomorphic to the class group of $\mathbb{Q}(\sqrt{-D})$.

Example ($D = -56$)

$$x^2 + 14y^2,\ 2x^2 + 7y^2,\ 3x^2 \pm 2xy + 5y^2$$

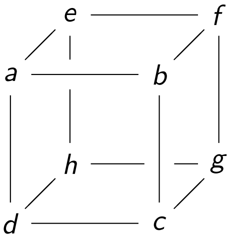
Remark

1. Gauss's proof was long and complicated; difficult to compute with.
2. Later reformulated by Dirichlet.
3. Much later reformulated by Bhargava.

Bhargava cubes

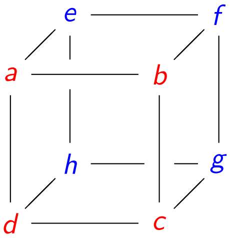
$$
\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] & \\
& h \arrow[rr, dash] \arrow[dl, dash] & & g \arrow[dl, dash] \\
d \arrow[rr, dash] & & c &
\end{tikzcd}
$$

Bhargava cubes



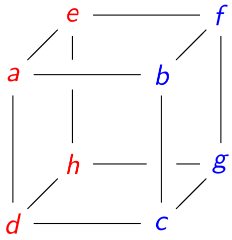
1. $a, b, d, c, e, f, h, g \in \mathbb{Z}$,
2. Cube is really an element of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, with a natural $\mathrm{SL}_2(\mathbb{Z})^3$ action

Gauss composition via Bhargava cubes



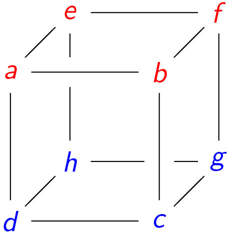
$$Q_1(x,y) := -\mathrm{Det}\left(\begin{pmatrix} a & b \\ d & c \end{pmatrix} x - \begin{pmatrix} e & f \\ h & g \end{pmatrix} y\right)$$

Gauss composition via Bhargava cubes



$$Q_i(x, y) := -\mathrm{Det}\,(M_i x - N_i y)$$

Gauss composition via Bhargava cubes



$$Q_i(x, y) := -\mathrm{Det}\,(M_i x - N_i y)$$

Bhargava's theorem

$$
\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & f \arrow[dl, dash] \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] & \\
& h \arrow[rr, dash] \arrow[dl, dash] & & g \arrow[dl, dash] \\
d \arrow[rr, dash] & & c &
\end{tikzcd}
$$

$$Q_i(x, y) := -\mathrm{Det}\,(M_i x - N_i y)$$

Theorem (Bhargava)

$$Q_1(x, y) + Q_2(x, y) + Q_3(x, y) = 0$$

Lots of parameterizations

Example

binary cubic forms	$\leftrightarrow$	cubic fields
pairs (ternary, quadratic) forms	$\leftrightarrow$	quartic fields
quadruples of quinary alternating bilinear forms	$\leftrightarrow$	quintic fields
binary quartic forms	$\leftrightarrow$	2-Selmer elements of Elliptic curves

Remark

1. 14 more (Bhargava)
2. many more (Bhargava-Ho)

Representation theoretic framework

Space of forms

1. The space V of binary quadratic forms is 3-dimensional vector space (resp. R-module).
2. $V = \operatorname{Sym}^2 \mathbb{C}^2$

Representations

$\mathrm{SL}_2(\mathbb{C}) \circlearrowleft \operatorname{Sym}^2 \mathbb{C}^2$

$\mathrm{SL}_2(\mathbb{R}) \circlearrowleft \operatorname{Sym}^2 \mathbb{R}^2$

$\mathrm{SL}_2(\mathbb{Z}) \circlearrowleft \operatorname{Sym}^2 \mathbb{Z}^2$ etc..

Invariants

1. $\mathbb{C}$-**Invariants**: two non-zero forms f, g are $\mathbb{C}$ equivalent iff $\Delta(f) = \Delta(g)$.
2. $\mathbb{Z}$-**Invariants**: $\Delta(f) = \Delta(g) \not\Rightarrow \mathbb{Z}$ equivalence.

Representation theoretic framework

Invariants

1. $\mathbb{C}$-**Invariants**: two non-zero forms f, g are $\mathbb{C}$ equivalent iff $\Delta(f) = \Delta(g)$.
2. $\mathbb{Z}$-**Invariants**: $\Delta(f) = \Delta(g) \not\Rightarrow \mathbb{Z}$ equivalence.

Example ($D = -14 \cdot 4$)

$x^2 + 14y^2$ is not equivalent to $2x^2 + 7y^2$.

Fundamental object of study

1. $\mathrm{SL}_2(\mathbb{Z})$-orbits of an $\mathrm{SL}_2(\overline{\mathbb{Q}})$-orbit

General representation theoretic framework

Framework

1. $V =$ free R module
2. $G \circlearrowleft V$
3. $R \to R'$ ring extension
4. $v \in V(R)$

Goal

Understand the $G(R)$-orbits of the $G(R')$-orbit of v

Arithmetic invariant theory

"Is every group a cohomology group

$H^1_{\text{ét}}(\operatorname{Spec}\mathbb{Z}, \operatorname{Res}_{\mathcal{O}/\mathbb{Z}}\mathbb{G}_m)$

Arithmetic invariant theory

"Is every group a cohomology group or a Manjul shaped asteroid that fell from the sky?" – Jordan Ellenberg

$H^1_{\text{ét}}(\operatorname{Spec}\mathbb{Z}, \operatorname{Res}_{\mathcal{O}/\mathbb{Z}}\mathbb{G}_m)$

Arithmetic invariant theory

"Is every group a cohomology group or a Manjul shaped asteroid that fell from the sky?" – *Jordan Ellenberg*

$$H^1_{\text{ét}}(\operatorname{Spec}\mathbb{Z}, \operatorname{Res}_{\mathcal{O}/\mathbb{Z}}\mathbb{G}_m)$$

Bhargava–Gross–Wang

Setup

1. $f, g \in V(\mathbb{Q})$
2. $M \in G(\overline{\mathbb{Q}})$ s.t. $g = M \cdot f$
3. $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
4. Then $g = M^\sigma \cdot f$, so $f = M^{-1}M^\sigma \cdot f$, i.e. $M^{-1}M^\sigma \in \mathrm{Stab}_f$

Cohomological framework

The map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Stab}_f;\ \sigma \mapsto M^{-1}M^\sigma$$

is a **cocycle**, and gives an element of $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Stab}_f)$.

Integral arithmetic invariant theory

Remark

1. AIT only works for fields; can't recover Gauss composition
2. Analogue of Galois cohomology is étale cohomology.

Integral arithmetic invariant theory – setup

Setup

1. S any base (e.g. $\mathbb{Z}$);
2. G/S any group scheme (not necessarily smooth, or even flat);
3. X (usually a vector space);
4. $G \circlearrowleft X$ an action.

Example ("Gauss")

$G = \mathrm{SL}_{2,\mathbb{Z}}$, acting on $X = \mathrm{Sym}^2 \mathbb{A}^2_{\mathbb{Z}}$

Main Theorem

Theorem (Giraud; Geraschenko-ZB)

Let $v \in X(S)$. Then there is a functorial long exact sequence (of groups and pointed sets)

$$0 \to Stab_v(S) \to G(S) \xrightarrow{g \mapsto g \cdot v} Orbit_v(S) \to H^1(S, Stab_v) \to H^1(S, G).$$

If $Stab_v$ is commutative, then

$$Orbit_v(S)/G(S) \cong \ker\left(H^1(S, Stab_v) \to H^1(S, G)\right)$$

is a group.

Remark

The image $\mathrm{Orbit}_v(S)/G(S)$ of $X(S)$ is the set of $G(S)$ equivalence classes of $v' \in \mathrm{Orbit}_v(S)$ in the same local orbit as v.

Example: Gauss composition revisited

Example ("Gauss")

$G = \mathrm{SL}_{2,\mathbb{Z}}$ acts on $X = \mathrm{Sym}^2 \mathbb{A}^2_{\mathbb{Z}}$; Stab_v is a non-split torus (thus *commutative*).

Let $f \in X(\mathbb{Z})$ be a *primitive* (non-zero mod all p) integral quadratic form.

$$0 \to \mathrm{Stab}_v(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{g \mapsto g \cdot f} \mathrm{Orbit}_f(\mathbb{Z}) \to H^1(\mathbb{Z}, \mathrm{Stab}_v) \to H^1(\mathbb{Z}, \mathrm{SL}_2).$$

Remark

1. $H^1(\mathbb{Z}, \mathrm{SL}_2) = 0$ (this is Hilbert's theorem 90).
2. $\mathrm{Orbit}_f(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z}) =$ integral equivalence classes of primitive forms with the same discriminantn.
3. $H^1(\mathbb{Z}, \mathrm{Stab}_v) \cong \mathrm{Orbit}_f(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z})$.
4. $H^1(\mathbb{Z}, \mathrm{Stab}_v) \cong \mathrm{Pic}\, \mathbb{Z}[(\Delta_f + \sqrt{\Delta_f})/2] = \mathrm{Cl}\, \mathbb{Q}[\sqrt{\Delta_f}]$.

Example: Gauss composition (non-primitive)

Remark

1. If $f \in \mathbb{Z}^2$ is *not* primitive, then Stab_f is not *flat* over $\operatorname{Spec}\mathbb{Z}$.
2. (Easiest way to not be flat: $\dim \mathrm{Stab}_{f,\mathbb{F}_p}$ is not constant.)
3. Our machinery does not care; and recovers Gauss composition for non-primitive forms.

Still to come

$$\boxed{\text{More applications wanted.}}$$

1. We're currently iterating through the known literature, deriving paramaterizations where possible.
2. E.g. Delone–Faddeev (ternary cubic forms vs cubic rings): stabilizer is a finite flat group scheme.
3. Future predictive power, especially of degenerate objects/orbits.