Gauss composition with level structure

Gene S. Kopp*

Joint work with Olivia Beckwith

*University of Bristol

6 Jan 2021

Spaces of binary quadratic forms

Let $D \equiv 0, 1 \pmod 4$ be a nonsquare integer.

$$\mathcal{Q}^{+}_{\mathrm{prim}}(D) := \left\{ \begin{array}{c} Q(x,y) = ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, \\ b^2 - 4ac = D,\ \gcd(a,b,c) = 1 \\ \text{and } Q \text{ is not negative-definite} \end{array} \right\}.$$

The group $\mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_{\mathrm{prim}}(D)$ by

$$Q^{\gamma}(x,y) = Q(rx + sy, tx + uy)$$

for $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{PSL}(\mathbb{Z})$.

An equivalence class in $\mathcal{Q}_{\mathrm{prim}}(D)/\mathrm{PSL}_2(\mathbb{Z})$ is denoted by $[Q]$.

Gauss composition

Let $Q_1, Q_2 \in \mathcal{Q}^+_{\text{prim}}(D)$. There exists some (non-unique) $Q_3 \in \mathcal{Q}^+_{\text{prim}}(D)$ such that

$$Q_3(X, Y) = Q_1(x_1, y_1)Q_2(x_2, y_2)$$

where

$$X = Ax_1x_2 + Bx_1y_2 + Cy_1x_2 + Dy_1y_2,$$
$$Y = Ex_1x_2 + Fx_1y_2 + Gy_1x_2 + Hy_1y_2.$$

Theorem (Gauss)

The class $[Q_3]$ is uniquely determined by $[Q_1]$ and $[Q_2]$, and setting $[Q_1] \cdot [Q_2] = [Q_3]$ defines an abelian group law on $\mathcal{Q}^+_{\text{prim}}(D)/\mathrm{PSL}_2(\mathbb{Z})$.

Representations of primes

If p is an odd prime number and $Q \in \mathcal{Q}^+_{\text{prim}}(D)$, then

$$Q(m,n) = p \implies D \equiv \square \pmod{p}.$$

The converse does not hold.

Theorem (Gauss)

Every odd prime p such that $\left(\frac{D}{p}\right) = 1$ is representable by exactly one class of binary quadratic forms in $Q \in \mathcal{Q}^+_{\text{prim}}(D)/\mathrm{PGL}_2(\mathbb{Z})$.

Example ($D = -47$)

$[x^2+xy+12y^2]$	$\left\{ \begin{array}{l} [2x^2+xy+6y^2] \\ [2x^2-xy+6y^2] \end{array} \right\}$	$\left\{ \begin{array}{l} [3x^2+xy+4y^2] \\ [3x^2-xy+4y^2] \end{array} \right\}$
47, 83, 191, 197, ...	2, 7, 53, 59, 61, 89, 97, 131, 157, 173, ...	3, 17, 37, 71, 79, 101, 103, 149, ...

The ring class group

In modern language, the group law on classes of binary quadratic forms is isomorphic to the narrow ring class group of a quadratic order of discriminant D.

Definition (Narrow ring class group)

$$\mathrm{Cl}^+(\mathcal{O}) = \frac{\{\text{invertible fractional ideals of } \mathcal{O}\}}{\{\text{principal fractional ideals } \alpha\mathcal{O} \text{ with } \mathrm{Nm}(\alpha) > 0\}}.$$

Theorem (Gauss, Dirichlet, Dedekind)

Let $\mathcal{O}_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$. Then

$$\mathrm{Cl}^+(\mathcal{O}_D) \cong \mathcal{Q}^+_{\mathrm{prim}}(D)/\mathrm{PSL}_2(\mathbb{Z}).$$

Applications and class field theory

The quadratic form interpretation of class groups has widespread applications in number theory:

- Proof of Dirichlet's class number formula
- Computation of/in class groups, cryptographic applications
- Use of (mock) modular forms as generating functions for class numbers

One application is to class field theory.

$$\mathcal{Q}^{+}_{\text{prim}}(D)/\operatorname{PSL}_2(\mathbb{Z}) \cong \operatorname{Cl}^{+}(\mathcal{O}_D) \cong \operatorname{Gal}\left(H^{+}/\mathbb{Q}(\sqrt{D})\right)$$

H^{+} is the narrow Hilbert class field when D is a fundamental discriminant, and the narrow ring class field generally.

Class field theory

- Ring class fields do not generate all abelian extensions of a number field.
- To describe the Galois groups of a cofinal set of abelian extensions, we need ray class groups.

Definition

Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ and $S \subseteq \{\text{real embeddings } K \hookrightarrow \mathbb{R}\}$.

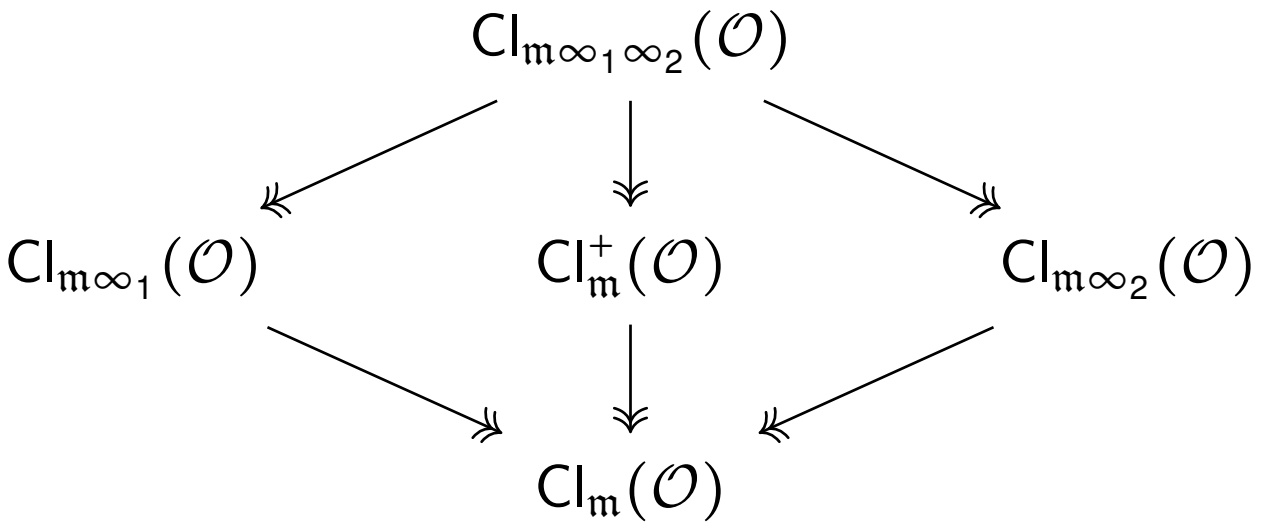
$$\mathrm{Cl}_{\mathfrak{m},S}(\mathcal{O}_K) = \frac{\{\text{fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}\}}{\{\alpha\mathcal{O} \text{ with } \alpha \equiv 1 \pmod{\mathfrak{m}} \text{ and } \rho(\alpha) > 0 \text{ for } \rho \in S\}}.$$

Question

Do ray class groups have a binary quadratic form interpretation?

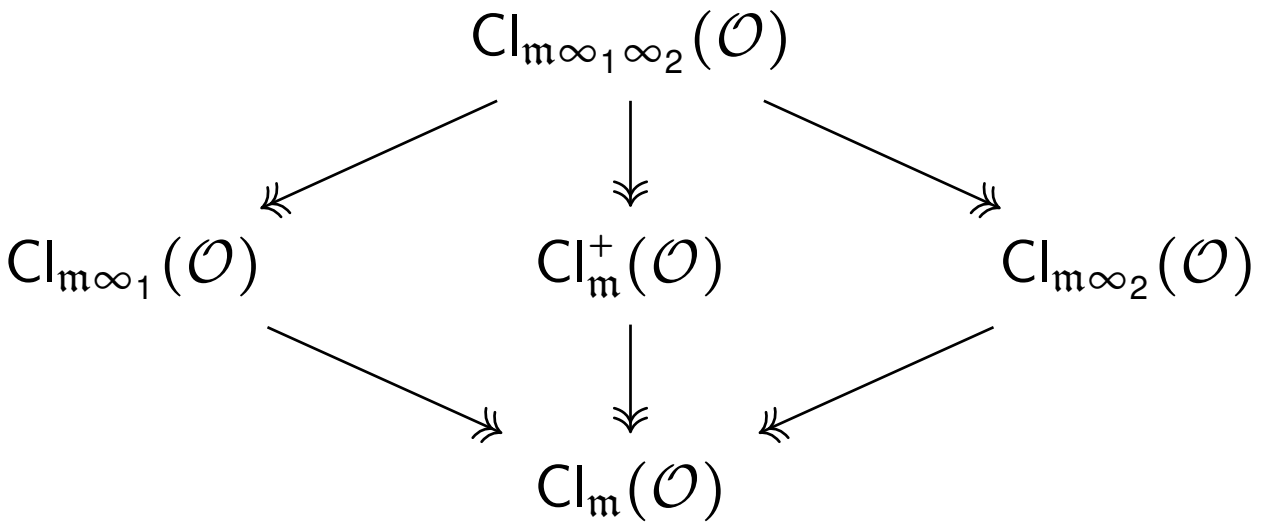
Ray class groups

Yes! For “narrow” ray class groups of rational modulus $\mathfrak{m} = (N)$.
But what does “narrow” mean?



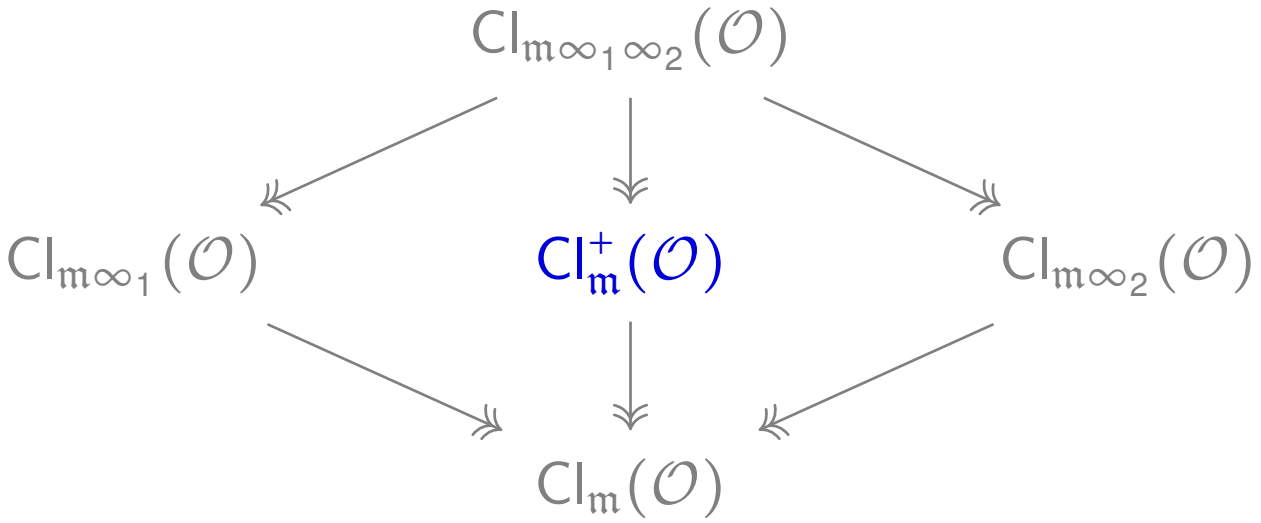
Ray class groups

Yes! For “narrow” ray class groups of rational modulus $\mathfrak{m} = (N)$.
But what does “narrow” mean?



Ray class groups

Yes! For "narrow" ray class groups of rational modulus $\mathfrak{m} = (N)$.
But what does "narrow" mean?



Definition (K and Lagarias, 2021+; Beckwith and K, 2021+)

The narrow ray class group of an order modulo $(\mathfrak{m}, S)$ is

$$\mathrm{Cl}^+_{\mathfrak{m}}(\mathcal{O}) = \frac{\{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}}{\{\alpha\mathcal{O} \text{ with } \alpha \equiv 1 \pmod{\mathfrak{m}} \text{ and } \mathrm{Nm}(\alpha) > 0\}}.$$

Main theorem

$$\mathcal{Q}_{\text{prim}}^{N,+}(D) := \left\{ \begin{array}{c} Q(x,y) = ax^2 + bxy + cy^2 : a,b,c \in \mathbb{Z}, \\ b^2 - 4ac = D,\ \gcd(a,N) = \gcd(a,b,c) = 1, \\ \text{and } Q \text{ is not negative-definite} \end{array} \right\}.$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : \begin{pmatrix} r & s \\ t & u \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Theorem (Beckwith and K, 2021+)

There is a bijection $\mathcal{Q}_{\text{prim}}^{N,+}(D)/\Gamma_1(N) \cong \mathrm{Cl}_{(N)}^{+}(\mathcal{O}_D)$.

Consequently, $\mathcal{Q}_{\text{prim}}^{N,+}(D)/\Gamma_1(N)$ has an abelian group structure.

A version of this theorem was obtained for the maximal order in the imaginary quadratic case by Eum, Koo, and Shin in 2017.

Mapping forms to ideals

Write $Q(x,y) = ax^2 + bxy + cy^2 = a(x - \tau y)(x - \tau' y)$ with $\tau = \frac{-b+\sqrt{D}}{2a}$. Define $\phi(Q) = a(\mathbb{Z} + \tau\mathbb{Z}) = a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}$.
The factor a matters.

Note that $\mathcal{O}_D = \mathbb{Z} + a\tau\mathbb{Z}$ and $(a\tau)^2 = -b(a\tau) - ac$, so $\phi(Q)$ is an integral $\mathcal{O}_D$-ideal, and $\mathrm{Nm}(\phi(Q)) = a$. So $\phi(Q)$ is coprime to N.

One must then check that...

- $\phi(Q)$ is invertible,
- $\phi(Q^\gamma) \sim \phi(Q)$ in $\mathrm{Cl}^+_{(N)}(\mathcal{O}_D)$ for $\gamma \in \Gamma_1(N)$,
- $[Q] \mapsto [\phi(Q)]$ is injective and surjective.

Representation of primes

Theorem (Beckwith and K, 2021+)

Suppose $N > 2$, and let p be a rational prime with $\gcd(p, ND) = 1$. Fix a binary quadratic form $Q \in \mathcal{Q}^{N,+}_{\text{prim}}(D)$. The following are equivalent:

(1) Q represents p by $Q(m,n) = p$ with $(m,n) \equiv (1,0) \pmod{N}$.

(2) $\phi(Q) \sim \mathfrak{p}$ in $\mathrm{Cl}^+_{(N)}(\mathcal{O}_D)$, where $(p) = \mathfrak{p}\mathfrak{p}'$ in $\mathcal{O}_D$ and ★.

★ (choice of prime) $\mathfrak{p} = \left(am + \frac{-b+\sqrt{D}}{2}n\right)\mathbb{Z} + \left(cn + \frac{b+\sqrt{D}}{2}m\right)\mathbb{Z}$

- By Artin reciprocity, the condition $\phi(Q) \sim \mathfrak{p}$ in (2) is equivalent to $\mathrm{Art}(\phi(Q)) = \mathrm{Frob}_{\mathfrak{p}}$ in $\mathrm{Gal}\left(H^{\mathcal{O}_D,+}_{(N)}/\mathbb{Q}(\sqrt{D})\right)$.
- For p odd, (1) or (2) implies that $\left(\frac{D}{p}\right) = 1$.

Example

Set $D = 12$, so $\mathcal{O}_D = \mathbb{Z}[\sqrt{3}]$, and set $N = 5$. The narrow ray class group $\mathrm{Cl}_5^+\left(\mathbb{Z}[\sqrt{3}]\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has order 8.

$[Q]$	$p = Q(m,n)$: $(m,n) \equiv (1,0) \pmod 5$
$[x^2 - 3y^2]$	37, 97, 157, 277, 337, 397 ...
$[-x^2 + 3y^2]$	3, 23, 83, 263, 383 ...
$[x^2 + 2xy - 2y^2]$	13, 73, 193, 313, 373, ...
$[-x^2 - 2xy + 2y^2]$	2, 47, 107, 167, 227, 347, ...
$[x^2 + 4xy + y^2]$	61, 181, 241, ...
$[-x^2 - 4xy - y^2]$	59, 179, 239, 359, ...
$[11x^2 - 34xy + 26y^2]$	11, 71, 131, 191, 251, 311, ...
$[-11x^2 + 34xy - 26y^2]$	109, 229, 349, ...

Thank you!

Thank you for listening! Any questions?