Definite quaternion orders with stable cancellation

John Voight
Dartmouth College
(joint with Daniel Smertnig)

Oregon Number Theory Days
Oregon State University
16 February 2019
Let $R = \mathbb{Z}_F$ be the ring of integers of a number field $F$.

We soon ask: how close is $R$ to a PID? We define the *class group*

$$\text{Cl } R := \frac{(\text{invertible}) \text{ fractional ideals of } F}{\text{principal fractional ideals}}$$

an abelian group under multiplication. Alternatively, we could define

$$\text{Cl } R = \{a \subseteq R : a \text{ nonzero ideal}\}/\sim$$

where $a \sim b$ if there exists $c \in F^\times$ such that $a = cb$.

The class group quantifies the failure of (fractional) ideals to be principal.

By the geometry of numbers, we have $h(R) := \# \text{Cl } R < \infty$. 

Gauss and the class number 1 problem

In the language of binary quadratic forms, Gauss conjectured (in Article 303 of *Disquisitiones*) a list of all imaginary quadratic fields $F = \mathbb{Q}(\sqrt{d})$ (with $d < 0$) with class number $h(\mathbb{Z}_F) = 1$.

Further, the series of determinants corresponding to the same given classification (i.e. the given number of both genera and classes) always seems to come to an end. We illustrate this rather remarkable observation by some examples. (The Roman numeral indicates the number of properly primitive positive genera; the Arabic numeral the number of classes contained in each genus; then follows a series of determinants which correspond to this classification. For brevity we omit the negative sign.)

I. $\ldots 1, 2, 3, 4, 7$

I. $\ldots 11, 19, 23, 27, 31, 43, 67, 163$

It would take almost 150 years of work, culminating in work of Heegner, Stark, and Baker, to verify the completeness of this list. (In the recent past, Watkins has enumerated all such fields $F$ with $h(\mathbb{Z}_F) \leq 100$.)
Slightly more generally

But Gauss already considered binary quadratic forms corresponding orders that are not maximal (not integrally closed)—so we too should be more general!

For example, the ring \( R = \mathbb{Z}[\sqrt{-3}] \) (contained in the maximal order \( \mathbb{Z}[(-1 + \sqrt{-3})/2]) \) is not a PID because it is not a UFD:

\[
(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2.
\]

However, we can recover by restricting to invertible ideals: the problematic nonprincipal ideals are not invertible!
Slightly more generally, invertible modules

Let \( R \) be a commutative ring (with 1). We say that an \( R \)-module \( M \) is invertible if there exists an \( R \)-module \( N \) such that \( M \otimes_R N \simeq R \) as \( R \)-modules.

For example, if \( R \) is a domain with field of fractions \( F := \text{Frac}(R) \), then an ideal \( a \subseteq R \) is invertible if and only if

\[
aa^{-1} = R, \quad \text{where} \quad a^{-1} := \{ b \in F : ab \subseteq R \}.
\]

\( M \) is invertible if and only if \( M \) is locally principal, i.e., for all primes \( \mathfrak{p} \subseteq R \) we have

\[
M(\mathfrak{p}) := M \otimes_R R(\mathfrak{p}) \simeq R(\mathfrak{p})
\]

as \( R(\mathfrak{p}) \)-modules, where \( R(\mathfrak{p}) \) is the localization at \( \mathfrak{p} \) (everything not in \( \mathfrak{p} \) becomes a unit, e.g. \( \mathbb{Z}(\mathfrak{p}) = \{ a/b \in \mathbb{Q} : \mathfrak{p} \nmid b \} \)).

In geometry, locally principal \( R \)-modules are called line bundles.
Slightly more generally, Picard group

We then define the *Picard group* 

$$\text{Pic } R := \{\text{invertible } R\text{-modules}\}/\sim$$

to be the (abelian) group of isomorphism classes of invertible $R$-modules under tensor product.

If $R$ is a Dedekind domain, then $\text{Pic } R \sim \text{Cl } R$. If $R \subseteq F$ is an order in a number field, then $\# \text{Pic } R < \infty$.

The Picard group quantifies the failure of locally principal $R$-modules to be free.
But what about $R$-modules of higher rank? Since this is a number theory day, let’s cut back on the generality and let $R \subseteq F$ be an order in a number field $F = \text{Frac} R$.

Let $M$ be a locally (“wannabe”) free, finitely generated $R$-module. Then $M_{(p)} \simeq (R_{(p)})^n$ for some $n \in \mathbb{Z}_{\geq 0}$ called the rank of $M$ (independent of $p$).

For example, we might take a locally free submodule $M \subseteq V$ where $V$ is an $F$-vector space with $\dim_F V = n$ and $FM = V$. We then call $M$ a locally free $R$-lattice in $V$. 
Structure theorem for locally free modules

Let \( R \) be an order in a number field \( F \) and let \( M \) be a locally free \( R \)-module of rank \( n \).

We now add a mild hypothesis: every ideal of \( R \) is generated by at most 2 elements (e.g. \( R = \mathbb{Z}_F \)); we say \( R \) is Bass.

Then \( M \) is isomorphic to the direct sum of invertible \( R \)-modules

\[ M \cong a_1 \oplus \cdots \oplus a_n; \]

and given two such we have

\[ a_1 \oplus \cdots \oplus a_n \cong b_1 \oplus \cdots \oplus b_m \]

if and only if

\[ n = m \quad \text{and} \quad [a_1 \cdots a_n] = [b_1 \cdots b_m] \in \text{Pic} \, R. \]

In particular, we may write \( M \cong R^{n-1} \oplus a \) with \([a] \in \text{Pic} \, R \) unique (Steinitz class). This can also be done algorithmically.

(This generalizes: vector spaces are determined by dimension.)
This structure theorem gives a different way to define the group operation in Pic $R$.

Let $a, b$ be invertible $R$-modules (or fractional $R$-ideals). Then

$$ a \oplus b \simeq R \oplus c $$

with $[c] = [ab] \in \text{Pic } R$ well-defined. (Cool!)

Other fun consequences:

- $R^k \oplus a \simeq R^{k+1}$ if and only if $a$ is principal;
- More generally, $R^k \oplus a \simeq R^k \oplus b$ if and only if $a \simeq b$ as $R$-modules.

(This leads eventually to the construction of Grothendieck group, but let’s pause here.)
Are you ready now to get noncommutative?
For the rest of the talk, let $F$ be a number field and let $R = \mathbb{Z}_F$.

Let $B = \left( \frac{a, b}{F} \right)$ be a *quaternion algebra* over $F$, so

$$B = F \oplus Fi \oplus Fj \oplus Fij$$

subject to the multiplication laws

$$i^2 = a, \quad j^2 = b, \quad ji = -ij \quad \text{and} \quad a, b \in F^\times.$$
Let \( B = \left( \frac{a, b}{F} \right) \). The quaternion algebra \( B \) has a reduced norm

\[
\text{nrd}: B \rightarrow F
\]

\[
\alpha = t + xi + yj + zk \mapsto t^2 - ax^2 - by^2 + abz^2.
\]

We say that \( B \) is totally definite if the quadratic form \( \text{nrd} \) is totally definite; i.e., \( F \) is totally real, and for every embedding \( \nu: F \hookrightarrow \mathbb{R} \) we have \( \nu(a), \nu(b) < 0 \).

A (locally free) \( R \)-lattice \( I \subset B \) is a finitely generated \( R \)-submodule such that \( FI = B \) (equivalently, \( I \) contains an \( F \)-basis for \( B \)).

An \( R \)-order \( \mathcal{O} \subset B \) is an \( R \)-lattice that is a ring (with 1). An \( R \)-order \( \mathcal{O} \) is maximal if it is not properly contained in another order, and Eichler if it is the intersection of two maximal orders.

For example: \( \mathcal{O} = R + Ri + Rj + Rij \) with \( a, b \in R \) is an \( R \)-order; \( \mathcal{O} = M_2(R) \subset M_2(F) \).
A right fractional $\mathcal{O}$-ideal is an $R$-lattice $I \subset B$ such that $I\mathcal{O} \subseteq I$, i.e.,

$$\mathcal{O} \subseteq \mathcal{O}_R(I) := \{\alpha \in B : I\alpha \subseteq I\}.$$ 

(Define similarly on the left.) We say that $I$ is sated if $\mathcal{O} = \mathcal{O}_R(I)$.

For $I$ a right fractional $\mathcal{O}$-ideal, the following are equivalent:

- $I$ is (left) invertible, i.e., there exists an $R$-lattice $J$ such that $JI = \mathcal{O} = \mathcal{O}_R(I)$; and
- $I$ is locally principal, i.e., for all primes $p \subseteq R$, we have

$$I(p) := I \otimes_R R(p) = \alpha_p \mathcal{O}(p) \cong \mathcal{O}(p)$$

for some $\alpha_p \in \mathcal{O}(p)$. 

Let $I, J \subset B$ be sated right fractional $\mathcal{O}$-ideals. Then $I \simeq J$ as right $\mathcal{O}$-modules if and only if there exists $\alpha \in B^\times$ such that $\alpha I = J$.

We define the (right) class set of $\mathcal{O}$:

$$
\text{Cls} \mathcal{O} := \{\text{invertible right fractional } \mathcal{O}\text{-ideals}\}/\simeq
$$

to be the set of isomorphism classes as in the commutative case.

The geometry of numbers again implies that $\# \text{Cls} \mathcal{O} < \infty$. Yay!

Unfortunately, this set does not have a natural group structure: if we were to try to define $[I] \cdot [J] = [IJ]$ we run into the problem

$$
I \alpha J \overset{?}{=} \alpha' IJ.
$$

Less yay.
Group structure from below

We defined $\text{Cls} \mathcal{O} := \{\text{invertible right fractional } \mathcal{O}\text{-ideals}\}/\sim$.

The reduced norm furnishes a surjective map of pointed sets

$$\text{nrd}: \text{Cls} \mathcal{O} \to \text{Cl}_{G(\mathcal{O})} \mathcal{R} := F_{>0}^\times \backslash \hat{F}^\times / \text{nrd}(\hat{\mathcal{O}}^\times)$$

$$[I] \mapsto [\text{nrd}(I)]$$

where $\text{Cl}_{G(\mathcal{O})} \mathcal{R}$ is a certain class group which maps surjectively to $\text{Cl} \mathcal{R}$ with finite kernel.

**Theorem (Consequence of strong approximation)**

*If $B$ is not totally definite, then $\text{nrd}$ is bijective.*

Moral: most of the time, the class set of $\mathcal{O}$ has a natural group structure arising from (and not much more complicated than) the class group of $\mathcal{R}$! (So no new class number problems.)
Class number 1 orders

Theorem (Brzezinski ($R = \mathbb{Z}$), Kirschmer–V (Eichler), Kirschmer–Lorch (general))

There are exactly $144 + 10 = 154$ definite quaternion orders $\mathcal{O}$ with $\# \text{Cls} \mathcal{O} = 1$.

These include the Lipschitz order

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \subseteq B = \left( -\frac{1}{1}, -\frac{1}{1} \right)$$

and a non-Gorenstein order over the ring of integers of the totally real quartic field with defining polynomial

$$x^4 - x^3 - 4x^2 + x + 2$$

of discriminant 2777.
Recall that the group operation on $\text{Pic } R$ could be recovered from direct sums: $a \oplus b \simeq R \oplus ab$.

Let $M, N$ be right $\mathcal{O}$-modules. We say $M, N$ are *stably isomorphic*, and write $M \simeq_{\text{st}} N$, if there exists $k \in \mathbb{Z}_{\geq 0}$ such that

$$\mathcal{O}^k \oplus M \simeq \mathcal{O}^k \oplus N$$

as right $\mathcal{O}$-modules. We say $M$ is *stably free* if $M \simeq_{\text{st}} \mathcal{O}^m$ for some $m \in \mathbb{Z}_{\geq 0}$.

If $M \simeq N$ then $M \simeq_{\text{st}} N$, but not necessarily vice versa.

Stable isomorphism defines an equivalence relation on the set of invertible (i.e., locally principal) right $\mathcal{O}$-modules, with classes denoted $[I]_{\text{st}} \in \text{StCl } \mathcal{O}$.

The set $\text{StCl } \mathcal{O}$ has the structure of abelian group under $\oplus$:

$$I \oplus J \simeq \mathcal{O} \oplus K$$

for a well-defined $[K]_{\text{st}}$ (!), so we define $[I]_{\text{st}} + [J]_{\text{st}} = [K]_{\text{st}}$. 
We defined the *stable class group* 

\[ \text{StCl} \mathcal{O} := \{ \text{invertible right fractional } \mathcal{O}\text{-ideals} \}/ \sim_{\text{st}} \]

where \( I \sim_{\text{st}} J \) if and only if \( \mathcal{O}^k \oplus I \sim \mathcal{O}^k \oplus J \) for some \( k \).

**Theorem (Fröhlich)**

*The reduced norm defines a map*

\[ \text{nrd}: \text{StCl} \mathcal{O} \rightarrow \text{Cl}_{G(\mathcal{O})} R \]

*which is an isomorphism (of finite abelian groups).*

Moral: although the class set of \( \mathcal{O} \) does not have an immediate group structure, the stable class set does.
There is a natural surjective map of pointed sets

\[ \text{st}: \text{Cls } \mathcal{O} \rightarrow \text{StCl } \mathcal{O} \]

\[ [I] \mapsto [I]_{\text{st}} \]

We say that \( \mathcal{O} \) has *locally free* or *(stable) cancellation* if \( \text{st} \) is bijective, i.e., if \([I]_{\text{st}} = [J]_{\text{st}}\) then \([I] = [J] \). We say that \( \mathcal{O} \) is *Hermite* if \([I]_{\text{st}} = [\mathcal{O}]_{\text{st}}\) implies \([I] = [\mathcal{O}] \).

\[(\# \text{Cls } \mathcal{O} = 1) \Rightarrow \text{ locally free cancellation} \Rightarrow \text{ Hermite}\]

but not conversely in either case (oops!).

**Theorem (Vignéras (< \( \infty \)), Hallouin–Maire (Eichler), Smertnig–V (general))**

*Up to isomorphism, there are exactly 375 definite Hermite quaternion orders, with 316 having locally free cancellation.*
Main result

Theorem (Vignéras (< ∞), Hallouin–Maire (Eichler), Smertnig–V (general))

Up to isomorphism, there are exactly 375 definite Hermite quaternion orders, with 316 having locally free cancellation.

The essential ingredients:

- A mass formula for the class set;
- A lemma that the fibers of st have equal mass;
- Odlyzko bounds to successively bound \([F : \mathbb{Q}]\), then \(d_F\), then \(\text{disc } B\), then \(\text{Nm}(p)\) with \(p \mid \text{discrd } \mathcal{O}\); finally,
- A (hard-earned) four hour computation in Magma.
In this talk, I tried to explain the motivation for and solution to a quaternionic class number problem.

The main result: for definite quaternion orders, there are few hundred orders where the class set has a natural structure of an abelian group coming from the direct sum; these generalize the orders of class number 1.

If you liked this talk, there is work to do in the function field case!

Thank you very much for your attention.