Composition Laws

Melanie Matchett Wood

American Institute of Mathematics
and Stanford University

ECC 2010

Goals:

Goals:

- review two familiar examples of explicit group laws

Goals:

- review two familiar examples of explicit group laws
- see how they are pieces of a larger story

Goals:

- review two familiar examples of explicit group laws
- see how they are pieces of a larger story
- suggest several open problems in computational number theory (and algebraic geometry)

The most classical example...

The most classical example...

Theorem (Dedekind–Dirichlet)

There is a bijection

The most classical example...

Theorem (Dedekind–Dirichlet)

There is a bijection

$$\left\{ \begin{array}{c} \textit{(twisted) } \mathrm{GL}_2(\mathbb{Z})\textit{-classes} \\ \textit{of primitive binary} \\ \textit{quadratic forms over } \mathbb{Z} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C,[I]), \textit{ with } C \textit{ a} \\ \textit{quadratic ring, and } [I] \textit{ an} \\ \textit{element of the class} \\ \textit{group of } C \end{array} \right\}$$

The most classical example...

Theorem (Dedekind–Dirichlet)

There is a bijection

$$\left\{ \begin{array}{c} \text{(twisted) } \mathrm{GL}_2(\mathbb{Z})\text{-classes} \\ \text{of primitive binary} \\ \text{quadratic forms over } \mathbb{Z} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[I]), \text{ with } C \text{ a} \\ \text{quadratic ring, and } [I] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[I])$$

$$a, b, c \in \mathbb{Z}$$

The most classical example...

Theorem (Dedekind–Dirichlet)

There is a bijection

$$\left\{\begin{array}{c}\text{(twisted) } \mathrm{GL}_2(\mathbb{Z})\text{-classes}\\ \text{of primitive binary}\\ \text{quadratic forms over } \mathbb{Z}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{isomorphism classes of}\\ (C,[I]),\text{ with } C \text{ a}\\ \text{quadratic ring, and } [I] \text{ an}\\ \text{element of the class}\\ \text{group of } C\end{array}\right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[I])$$

$$a, b, c \in \mathbb{Z}$$

- group law on the right-hand side (for fixed C),

The most classical example...

Theorem (Dedekind–Dirichlet)

There is a bijection

$$\left\{ \begin{array}{c} \textit{(twisted) } \mathrm{GL}_2(\mathbb{Z})\textit{-classes} \\ \textit{of primitive binary} \\ \textit{quadratic forms over } \mathbb{Z} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C,[I]),\ \textit{with } C \textit{ a} \\ \textit{quadratic ring, and } [I] \textit{ an} \\ \textit{element of the class} \\ \textit{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[I])$$

$$a, b, c \in \mathbb{Z}$$

- group law on the right-hand side (for fixed C), and thus on the left-hand side

- group law on binary quadratic forms over $\mathbb{Z}$ can be given explicitly in terms of a, b, c by polynomial formulas and gcd operations

- group law on binary quadratic forms over $\mathbb{Z}$ can be given explicitly in terms of a, b, c by polynomial formulas and gcd operations
- reduction theory to find a unique reduced representative of each $\mathrm{GL}_2(\mathbb{Z})$ class

- group law on binary quadratic forms over $\mathbb{Z}$ can be given explicitly in terms of a, b, c by polynomial formulas and gcd operations
- reduction theory to find a unique reduced representative of each $\mathrm{GL}_2(\mathbb{Z})$ class
- discrimiant $b^2 - 4ac$ is the discriminant of the corresponding quadratic ring

Another familiar example...

Another familiar example... Let q be a power of a prime.

Another familiar example... Let q be a power of a prime.

Theorem

There is a bijection

Another familiar example... Let q be a power of a prime.

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]),\text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t],\text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

Another familiar example... Let q be a power of a prime.

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-}\textit{classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]),\ \textit{with } C \textit{ a} \\ \textit{quadratic extension of} \\ \mathbb{F}_q[t],\ \textit{and } [D] \textit{ an} \\ \textit{element of the class} \\ \textit{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C, [D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

Another familiar example... Let q be a power of a prime.

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]),\text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t],\text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

- group law on the right-hand side (for fixed C),

Another familiar example... Let q be a power of a prime.

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-}\textit{classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C,[D]),\ \textit{with } C \textit{ a} \\ \textit{quadratic extension of} \\ \mathbb{F}_q[t],\ \textit{and } [D] \textit{ an} \\ \textit{element of the class} \\ \textit{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

- group law on the right-hand side (for fixed C), and thus on the left-hand side

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C, [D]),\text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t],\text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C, [D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]), \text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t], \text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

- a *quadratic extension of* $\mathbb{F}_q[t]$ is just a double cover of $\mathbb{A}^1_{\mathbb{F}_q}$, (a.k.a a hyperelliptic curve)

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]), \text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t], \text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

- a *quadratic extension of* $\mathbb{F}_q[t]$ is just a double cover of $\mathbb{A}^1_{\mathbb{F}_q}$, (a.k.a a hyperelliptic curve)
- the *class group* of a (smooth) hyperelliptic curve is its Jacobian

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]),\text{ with } C \text{ a} \\ \text{quadratic extension of} \\ \mathbb{F}_q[t],\text{ and } [D] \text{ an} \\ \text{element of the class} \\ \text{group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a, b, c \in \mathbb{F}_q[t]$$

- a *quadratic extension of* $\mathbb{F}_q[t]$ is just a double cover of $\mathbb{A}^1_{\mathbb{F}_q}$, (a.k.a a hyperelliptic curve)
- the *class group* of a (smooth) hyperelliptic curve is its Jacobian
- $b^2 - 4ac$ is the branch locus of the map from C to $\mathbb{A}^1$

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.
- This isn't one of them.

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.
- This isn't one of them.

Let R be any ring

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.
- This isn't one of them.

Let R be any ring (variety, scheme, ...)

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.
- This isn't one of them.

Let R be any ring (variety, scheme, ...)

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

- There are lots of analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$.
- This isn't one of them.

Let R be any ring (variety, scheme, ...)

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{\begin{array}{c}\textit{equivalence classes of}\\ \textit{primitive binary}\\ \textit{quadratic forms over } R\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{isom. classes of } (C,[D]),\\ \textit{with } C \textit{ a quadratic}\\ R\textit{-algebra, and } [D]\in \textit{ the}\\ \textit{class group of } C\end{array}\right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$),

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C,[D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{ the} \\ \textit{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$), e.g. of $\mathbb{F}_q[t]$ as the line $\mathbb{A}^1$ over $\mathbb{F}_q$,

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C,[D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$), e.g. of $\mathbb{F}_q[t]$ as the line $\mathbb{A}^1$ over $\mathbb{F}_q$, then just a double cover of the geometric space

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$), e.g. of $\mathbb{F}_q[t]$ as the line $\mathbb{A}^1$ over $\mathbb{F}_q$, then just a double cover of the geometric space
- the *class group* is the group of invertible R-modules,

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$), e.g. of $\mathbb{F}_q[t]$ as the line $\mathbb{A}^1$ over $\mathbb{F}_q$, then just a double cover of the geometric space
- the *class group* is the group of invertible R-modules, or when quadratic cover smooth,

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \text{equivalence classes of} \\ \text{primitive binary} \\ \text{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isom. classes of } (C,[D]), \\ \text{with } C \text{ a quadratic} \\ R\text{-algebra, and } [D] \in \text{the} \\ \text{class group of } C \end{array} \right\}$$

- A *quadratic R-algebra* is an R-algebra that is locally free rank 2 as an R-module
- if we think of R geometrically ($\operatorname{Spec} R$), e.g. of $\mathbb{F}_q[t]$ as the line $\mathbb{A}^1$ over $\mathbb{F}_q$, then just a double cover of the geometric space
- the *class group* is the group of invertible R-modules, or when quadratic cover smooth, the Jacobian group $\operatorname{Div} / \operatorname{PrinDiv}$

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{ the} \\ \textit{class group of } C \end{array} \right\}$$

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{\begin{array}{c}\textit{equivalence classes of}\\ \textit{primitive binary}\\ \textit{quadratic forms over } R\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{isom. classes of } (C,[D]),\\ \textit{with } C \textit{ a quadratic}\\ R\textit{-algebra, and } [D] \in \textit{ the}\\ \textit{class group of } C\end{array}\right\}$$

Warning: Binary quadratic forms over R

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Warning: Binary quadratic forms over R are not in general given as $ax^2 + bxy + cy^2$ with $a, b, c \in R$!

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Warning: Binary quadratic forms over R are not in general given as $ax^2 + bxy + cy^2$ with $a, b, c \in R$! This is only the case when all locally free modules over R are free,

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, ..., W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Warning: Binary quadratic forms over R are not in general given as $ax^2 + bxy + cy^2$ with $a, b, c \in R$! This is only the case when all locally free modules over R are free, for example

- when R is a Dedekind Domain of class number 1

Theorem (Kaplansky, Butts, Dulin, Towber, Kneser, . . . , W.)

There is a bijection

$$\left\{ \begin{array}{c} \textit{equivalence classes of} \\ \textit{primitive binary} \\ \textit{quadratic forms over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isom. classes of } (C, [D]), \\ \textit{with } C \textit{ a quadratic} \\ R\textit{-algebra, and } [D] \in \textit{the} \\ \textit{class group of } C \end{array} \right\}$$

Warning: Binary quadratic forms over R are not in general given as $ax^2 + bxy + cy^2$ with $a, b, c \in R$! This is only the case when all locally free modules over R are free, for example

- when R is a Dedekind Domain of class number 1
- when $R = k[x_1, \ldots, x_n]$ for a field k (Quillen–Suslin theorem)

Theorem

There is a bijection

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t_1, t_2])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t_1, t_2] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C, [D]),\ \text{with } C \text{ a} \\ \text{quadratic} \\ \mathbb{F}_q[t_1, t_2]\text{-algebra, and} \\ [D] \text{ an element of the} \\ \text{class group of } C \end{array} \right\}$$

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t_1, t_2])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t_1, t_2] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C, [D]),\text{ with } C \text{ a} \\ \text{quadratic} \\ \mathbb{F}_q[t_1, t_2]\text{-algebra, and} \\ [D] \text{ an element of the} \\ \text{class group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C, [D])$$

$$a, b, c \in \mathbb{F}_q[t_1, t_2]$$

Theorem

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2(\mathbb{F}_q[t_1,t_2])\text{-classes of} \\ \text{primitive binary} \\ \text{quadratic forms over} \\ \mathbb{F}_q[t_1,t_2] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C,[D]),\text{ with } C \text{ a} \\ \text{quadratic} \\ \mathbb{F}_q[t_1,t_2]\text{-algebra, and} \\ [D] \text{ an element of the} \\ \text{class group of } C \end{array} \right\}$$

$$ax^2 + bxy + cy^2 \qquad\qquad (C,[D])$$

$$a,b,c \in \mathbb{F}_q[t_1,t_2]$$

- The C on the right correspond, geometrically, to surfaces with degree 2 maps to the plane $\mathbb{A}^2$ over $\mathbb{F}_q$.

How do forms correspond to elements of the class group?

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$,

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$, but the idea works over any ring, or even variety or scheme (with additional technical details).

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$, but the idea works over any ring, or even variety or scheme (with additional technical details).

We consider

$$\mathbb{A}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q},$$

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$, but the idea works over any ring, or even variety or scheme (with additional technical details).

We consider

$$\mathbb{A}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q},$$

- $\mathbb{A}^1$ has the coordinate t
- $\mathbb{P}^1$ has coordinates x, y

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$, but the idea works over any ring, or even variety or scheme (with additional technical details).

We consider

$$\mathbb{A}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q},$$

- $\mathbb{A}^1$ has the coordinate t
- $\mathbb{P}^1$ has coordinates x, y

We have a map

$$\mathbb{A}^1 \times \mathbb{P}^1 \to \mathbb{A}^1.$$

How do forms correspond to elements of the class group?

We will illustrate over $R = \mathbb{F}_q[t]$, but the idea works over any ring, or even variety or scheme (with additional technical details).

We consider

$$\mathbb{A}^1_{\mathbb{F}_q} \times \mathbb{P}^1_{\mathbb{F}_q},$$

- $\mathbb{A}^1$ has the coordinate t
- $\mathbb{P}^1$ has coordinates x, y

We have a map

$$\mathbb{A}^1 \times \mathbb{P}^1 \to \mathbb{A}^1.$$

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$,

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra
- intersect C with the line $y = 0$, to obtain a divisor on C, which gives an element of the class group

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra
- intersect C with the line $y = 0$, to obtain a divisor on C, which gives an element of the class group (In general, we pull back the $\mathcal{O}(1)$ sheaf from the $\mathbb{P}^1$.)

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra
- intersect C with the line $y = 0$, to obtain a divisor on C, which gives an element of the class group (In general, we pull back the $\mathcal{O}(1)$ sheaf from the $\mathbb{P}^1$.)
- could have taken $x = 0$ or other similar lines, and obtained equivalent divisors

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra
- intersect C with the line $y = 0$, to obtain a divisor on C, which gives an element of the class group (In general, we pull back the $\mathcal{O}(1)$ sheaf from the $\mathbb{P}^1$.)
- could have taken $x = 0$ or other similar lines, and obtained equivalent divisors
- agrees with the classical (Dedekind–Dirichlet) correspondence between classes of binary quadratic forms and ideal classes of quadratic rings over $\mathbb{Z}$

The form $a(t)x^2 + b(t)xy + c(t)y^2$ with $a(t), b(t), c(t) \in \mathbb{F}_q[t]$, cuts out a curve C in $\mathbb{A}^1 \times \mathbb{P}^1$.

- C has a degree 2 map to $\mathbb{A}^1$, a double cover of $\mathbb{A}^1$, or a quadratic $\mathbb{F}_q[t]$-algebra
- intersect C with the line $y = 0$, to obtain a divisor on C, which gives an element of the class group (In general, we pull back the $\mathcal{O}(1)$ sheaf from the $\mathbb{P}^1$.)
- could have taken $x = 0$ or other similar lines, and obtained equivalent divisors
- agrees with the classical (Dedekind–Dirichlet) correspondence between classes of binary quadratic forms and ideal classes of quadratic rings over $\mathbb{Z}$
- taking (a, b) over $\mathbb{F}_q[t]$ gives Mumford representation of points on the Jacobian of a hyperelliptic curve

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- in characteristic not 2, we have that C is also given by the equation $z^2 = f(w)$ in $\mathbb{A}^2$

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- in characteristic not 2, we have that C is also given by the equation $z^2 = f(w)$ in $\mathbb{A}^2$

Let C' be the curve defined by $z^2 = f(w)$ in $\mathbb{A}^2$.

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- in characteristic not 2, we have that C is also given by the equation $z^2 = f(w)$ in $\mathbb{A}^2$

Let C' be the curve defined by $z^2 = f(w)$ in $\mathbb{A}^2$. We give an isomorphism

$$\begin{array}{ccc} C & \longrightarrow & C' \\ (t, [x:y]) & \mapsto & (z = \frac{2cy}{x} + b = -\frac{2ax}{y} - b, w = t) \end{array}.$$

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- in characteristic not 2, we have that C is also given by the equation $z^2 = f(w)$ in $\mathbb{A}^2$

Let C' be the curve defined by $z^2 = f(w)$ in $\mathbb{A}^2$. We give an isomorphism

$$\begin{array}{ccc} C & \longrightarrow & C' \\ (t, [x:y]) & \mapsto & (z = \frac{2cy}{x} + b = -\frac{2ax}{y} - b, w = t) \end{array}.$$

We have $y = 0$ on C exactly when $a(z) = 0$ and $z = b(z)$ on C',

- $b^2 - 4ac$ is the discriminant of the quadratic R-algebra, or branch locus of the quadratic cover

Over $\mathbb{F}_q[t]$, let $f = b^2 - 4ac$,

- in characteristic not 2, we have that C is also given by the equation $z^2 = f(w)$ in $\mathbb{A}^2$

Let C' be the curve defined by $z^2 = f(w)$ in $\mathbb{A}^2$. We give an isomorphism

$$\begin{array}{ccc} C & \longrightarrow & C' \\ (t, [x : y]) & \mapsto & (z = \frac{2cy}{x} + b = -\frac{2ax}{y} - b, w = t) \end{array}.$$

We have $y = 0$ on C exactly when $a(z) = 0$ and $z = b(z)$ on C',

giving the usual Mumford representation of the divisor in C' coordinates.

- composition law can be given uniformly in terms of polynomials and gcd operations

- composition law can be given uniformly in terms of polynomials and gcd operations (as it always pulls back from composition on the universal primitive form)

- composition law can be given uniformly in terms of polynomials and gcd operations (as it always pulls back from composition on the universal primitive form)
- over each R the best method for computation of the composition might differ

- composition law can be given uniformly in terms of polynomials and gcd operations (as it always pulls back from composition on the universal primitive form)
- over each R the best method for computation of the composition might differ
- for each R, the reduction theory to find a unique representative in equivalence classes of forms is a potentially new problem, both theoretically and algorithmically

Other examples that would be interesting to study:

Other examples that would be interesting to study:

- Other orders $\mathcal{O}_K$ in number fields with $\mathrm{Cl}(\mathcal{O}_K) = 1$.

Other examples that would be interesting to study:

- Other orders $\mathcal{O}_K$ in number fields with $\mathrm{Cl}(\mathcal{O}_K) = 1$.
- $\mathbb{F}_q[t_1, t_2]$

Other examples that would be interesting to study:

- Other orders $\mathcal{O}_K$ in number fields with $\mathrm{Cl}(\mathcal{O}_K) = 1$.
- $\mathbb{F}_q[t_1, t_2]$

Main interesting aspects: reduction theory, efficient implementation

If locally free R-modules are not necessarily free...

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V,

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L,

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \mathrm{Sym}^2 V \otimes L$.

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \operatorname{Sym}^2 V \otimes L$.

Example

If V and L are free, so $V = Rx \oplus Ry$, and $L = R$, If locally free R-modules are not necessarily free. . .

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \mathrm{Sym}^2 V \otimes L$.

Example

If V and L are free, so $V = Rx \oplus Ry$, and $L = R$, then we have forms $ax^2 + bxy + cy^2$ with $a, b, c \in R$.

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \mathrm{Sym}^2 V \otimes L$.

Example

If V and L are free, so $V = Rx \oplus Ry$, and $L = R$, then we have forms $ax^2 + bxy + cy^2$ with $a, b, c \in R$.

- if R is a Dedekind domain (maximal order in a number field, or smooth affine curve),

If locally free R-modules are not necessarily free...

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \mathrm{Sym}^2 V \otimes L$.

Example

If V and L are free, so $V = Rx \oplus Ry$, and $L = R$, then we have forms $ax^2 + bxy + cy^2$ with $a, b, c \in R$.

- if R is a Dedekind domain (maximal order in a number field, or smooth affine curve), then there is a "type" of binary quadratic form over R for each element of $\mathrm{Cl}(R)$

If locally free R-modules are not necessarily free. . .

Definition

A *binary quadratic form* over R is a locally free rank 2 R-module V, a locally free rank 1 R-module L, and an element $p \in \mathrm{Sym}^2 V \otimes L$.

Example

If V and L are free, so $V = Rx \oplus Ry$, and $L = R$, then we have forms $ax^2 + bxy + cy^2$ with $a, b, c \in R$.

- if R is a Dedekind domain (maximal order in a number field, or smooth affine curve), then there is a "type" of binary quadratic form over R for each element of $\mathrm{Cl}(R)$
- compute this class group once, and then compute class groups of many quadratic extensions of R

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1 + \sqrt{-5})$.)

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1 + \sqrt{-5})$.)

Let $V = \mathcal{O}_K x \oplus I y$ and $L = \mathcal{O}_K$.

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1 + \sqrt{-5})$.)

Let $V = \mathcal{O}_K x \oplus I y$ and $L = \mathcal{O}_K$.

Elements of $\mathrm{Sym}^2 V \otimes L$ are given by $ax^2 + bxy + cy^2$, with $a \in \mathcal{O}_K$, $b \in I$, $c \in I^2$.

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1+\sqrt{-5})$.)

Let $V = \mathcal{O}_K x \oplus I y$ and $L = \mathcal{O}_K$.

Elements of $\mathrm{Sym}^2 V \otimes L$ are given by $ax^2 + bxy + cy^2$, with $a \in \mathcal{O}_K$, $b \in I$, $c \in I^2$.
The group $\mathrm{GL}(V)$ acting on forms (giving equivalence classes) is a group of matrices

$$\begin{pmatrix} \mathcal{O}_K & I \\ I^{-1} & \mathcal{O}_K \end{pmatrix}.$$

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1 + \sqrt{-5})$.)

Let $V = \mathcal{O}_K x \oplus I y$ and $L = \mathcal{O}_K$.

Elements of $\operatorname{Sym}^2 V \otimes L$ are given by $ax^2 + bxy + cy^2$, with $a \in \mathcal{O}_K$, $b \in I$, $c \in I^2$.
The group $\mathrm{GL}(V)$ acting on forms (giving equivalence classes) is a group of matrices

$$\begin{pmatrix} \mathcal{O}_K & I \\ I^{-1} & \mathcal{O}_K \end{pmatrix}.$$

- Reduction theory? (some recent work of Cremona)

Example

Let $\mathcal{O}_K$ be a maximal order in a number field K, and let I be a non-principal ideal of $\mathcal{O}_K$.
(More specifically, we could take $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1+\sqrt{-5})$.)

Let $V = \mathcal{O}_K x \oplus I y$ and $L = \mathcal{O}_K$.

Elements of $\mathrm{Sym}^2 V \otimes L$ are given by $ax^2 + bxy + cy^2$, with $a \in \mathcal{O}_K$, $b \in I$, $c \in I^2$.
The group $\mathrm{GL}(V)$ acting on forms (giving equivalence classes) is a group of matrices

$$\begin{pmatrix} \mathcal{O}_K & I \\ I^{-1} & \mathcal{O}_K \end{pmatrix}.$$

- Reduction theory? (some recent work of Cremona)
- Composition??

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

Understanding the composition law explicitly, in examples where V and L are non-trivial is an interesting problem.

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

Understanding the composition law explicitly, in examples where V and L are non-trivial is an interesting problem.

- $\mathcal{O}_K$ with non-trivial class group

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

Understanding the composition law explicitly, in examples where V and L are non-trivial is an interesting problem.

- $\mathcal{O}_K$ with non-trivial class group
- "R" $= \mathbb{P}^1$ (parametrizes Jacobians of hyperelliptic curves)

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

Understanding the composition law explicitly, in examples where V and L are non-trivial is an interesting problem.

- $\mathcal{O}_K$ with non-trivial class group
- "R" $= \mathbb{P}^1$ (parametrizes Jacobians of hyperelliptic curves)
- "R" an elliptic curve (parametrizes Jacobians of bi-elliptic curves)

While composition is given locally by universal formulas, patching those local formulas together into a global formula is a non-trivial problem.

Understanding the composition law explicitly, in examples where V and L are non-trivial is an interesting problem.

- $\mathcal{O}_K$ with non-trivial class group
- "R" $= \mathbb{P}^1$ (parametrizes Jacobians of hyperelliptic curves)
- "R" an elliptic curve (parametrizes Jacobians of bi-elliptic curves)
- affine elliptic curve, R maximal order in a function field of an elliptic curve (parametrizes Jacobians of bi-elliptic curves)

So far, we have seen forms that parametrized class groups of quadratic algebras (a.k.a. quadratic extensions, double covers).

So far, we have seen forms that parametrized class groups of quadratic algebras (a.k.a. quadratic extensions, double covers). This again, is one step in a larger story.

So far, we have seen forms that parametrized class groups of quadratic algebras (a.k.a. quadratic extensions, double covers). This again, is one step in a larger story.

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

So far, we have seen forms that parametrized class groups of quadratic algebras (a.k.a. quadratic extensions, double covers). This again, is one step in a larger story.

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } 3 \times 3 \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{trigonal curve over } \mathbb{F}_q, \\ \textit{and } [D] \textit{ an element of} \\ \textit{the class group of } C \end{array} \right\}$$

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-classes} \\ \text{of primitive pairs } (A, B) \\ \text{of } 3 \times 3 \text{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C, [D]),\ \text{with } C \text{ a} \\ \text{trigonal curve over } \mathbb{F}_q, \\ \text{and } [D] \text{ an element of} \\ \text{the class group of } C \end{array} \right\}$$

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } 3 \times 3 \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{trigonal curve over } \mathbb{F}_q, \\ \textit{and } [D] \textit{ an element of} \\ \textit{the class group of } C \end{array} \right\}$$

- (A, B) is really a 3 dimensional $2 \times 3 \times 3$ “matrix,” or a trilinear form

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-classes} \\ \text{of primitive pairs } (A, B) \\ \text{of } 3 \times 3 \text{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ (C, [D]), \text{ with } C \text{ a} \\ \text{trigonal curve over } \mathbb{F}_q, \\ \text{and } [D] \text{ an element of} \\ \text{the class group of } C \end{array} \right\}$$

- (A, B) is really a 3 dimensional $2 \times 3 \times 3$ "matrix," or a trilinear form
- Writing down (A, B) is giving 18 elements of $\mathbb{F}_q[t]$

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{\begin{array}{c}\mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-classes} \\ \text{of primitive pairs } (A, B) \\ \text{of } 3 \times 3 \text{ matrices over} \\ \mathbb{F}_q[t]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{isomorphism classes of} \\ (C, [D]),\ \text{with } C \text{ a} \\ \text{trigonal curve over } \mathbb{F}_q, \\ \text{and } [D] \text{ an element of} \\ \text{the class group of } C\end{array}\right\}$$

- (A, B) is really a 3 dimensional $2 \times 3 \times 3$ "matrix," or a trilinear form
- Writing down (A, B) is giving 18 elements of $\mathbb{F}_q[t]$
- Reduction theory can be done for GL_2, GL_3, GL_3 separately

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } 3 \times 3 \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{trigonal curve over } \mathbb{F}_q, \\ \textit{and } [D] \textit{ an element of} \\ \textit{the class group of } C \end{array} \right\}$$

- (A, B) is really a 3 dimensional $2 \times 3 \times 3$ "matrix," or a trilinear form
- Writing down (A, B) is giving 18 elements of $\mathbb{F}_q[t]$
- Reduction theory can be done for GL_2, GL_3, GL_3 separately
- trigonal curves are curves with degree 3 covers to the line (here $\mathbb{A}^1$)

Theorem (W., Bhargava 2004 over $\mathbb{Z}$)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } 3 \times 3 \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{trigonal curve over } \mathbb{F}_q, \\ \textit{and } [D] \textit{ an element of} \\ \textit{the class group of } C \end{array} \right\}$$

- (A, B) is really a 3 dimensional $2 \times 3 \times 3$ "matrix," or a trilinear form
- Writing down (A, B) is giving 18 elements of $\mathbb{F}_q[t]$
- Reduction theory can be done for GL_2, GL_3, GL_3 separately
- trigonal curves are curves with degree 3 covers to the line (here $\mathbb{A}^1$)
- For smooth curves, the class group is the same as the Jacobian

The story does not stop with cubic extensions (a.k.a. triple covers).

The story does not stop with cubic extensions (a.k.a. triple covers).

Theorem (W.)

There is a bijection

The story does not stop with cubic extensions (a.k.a. triple covers).

Theorem (W.)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_n \times \mathrm{GL}_n\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } n \times n \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{certain kind of } n\textit{-gonal} \\ \textit{curve over } \mathbb{F}_q, \textit{ and } [D] \\ \textit{an element of the class} \\ \textit{group of } C \end{array} \right\}$$

The story does not stop with cubic extensions (a.k.a. triple covers).

Theorem (W.)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_n \times \mathrm{GL}_n\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } n \times n \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{certain kind of } n\textit{-gonal} \\ \textit{curve over } \mathbb{F}_q, \textit{ and } [D] \\ \textit{an element of the class} \\ \textit{group of } C \end{array} \right\}$$

- n-gonal curves are curves with degree n covers to the line (here $\mathbb{A}^1$)

The story does not stop with cubic extensions (a.k.a. triple covers).

Theorem (W.)

There is a bijection

$$\left\{ \begin{array}{c} \mathrm{GL}_2 \times \mathrm{GL}_n \times \mathrm{GL}_n\text{-}\textit{classes} \\ \textit{of primitive pairs } (A, B) \\ \textit{of } n \times n \textit{ matrices over} \\ \mathbb{F}_q[t] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{isomorphism classes of} \\ (C, [D]), \textit{ with } C \textit{ a} \\ \textit{certain kind of } n\textit{-gonal} \\ \textit{curve over } \mathbb{F}_q, \textit{ and } [D] \\ \textit{an element of the class} \\ \textit{group of } C \end{array} \right\}$$

- n-gonal curves are curves with degree n covers to the line (here $\mathbb{A}^1$)
- as with binary quadratic forms, there is a version of this theorem over any ring (variety, scheme...)

Theorem (W.)

There is a bijection

$$\left\{\begin{array}{c}\mathrm{GL}_2 \times \mathrm{GL}_n \times \mathrm{GL}_n\text{-classes} \\ \text{of primitive pairs } (A, B) \\ \text{of } n \times n \text{ matrices over} \\ \mathbb{F}_q[t]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{isomorphism classes of} \\ (C, [D]), \text{ with } C \text{ a} \\ \text{certain kind of } n\text{-gonal} \\ \text{curve over } \mathbb{F}_q, \text{ and } [D] \\ \text{an element of the class} \\ \text{group of } C\end{array}\right\}$$

Theorem (W.)

There is a bijection

$$\left\{\begin{array}{c}\mathrm{GL}_2\times\mathrm{GL}_n\times\mathrm{GL}_n\text{-}\textit{classes}\\ \textit{of primitive pairs } (A,B)\\ \textit{of } n\times n \textit{ matrices over}\\ \mathbb{F}_q[t]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{isomorphism classes of}\\ (C,[D]),\ \textit{with } C \textit{ a}\\ \textit{certain kind of } n\textit{-gonal}\\ \textit{curve over } \mathbb{F}_q,\ \textit{and } [D]\\ \textit{an element of the class}\\ \textit{group of } C\end{array}\right\}$$

Problems: ($n \geq 3$)

- implement these composition laws explicitly

Theorem (W.)

There is a bijection

$$\left\{\begin{array}{c}\mathrm{GL}_2\times\mathrm{GL}_n\times\mathrm{GL}_n\text{-classes}\\ \text{of primitive pairs } (A,B)\\ \text{of } n\times n \text{ matrices over}\\ \mathbb{F}_q[t]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{isomorphism classes of}\\ (C,[D]),\text{ with } C \text{ a}\\ \text{certain kind of } n\text{-gonal}\\ \text{curve over } \mathbb{F}_q,\text{ and } [D]\\ \text{an element of the class}\\ \text{group of } C\end{array}\right\}$$

Problems: ($n \geq 3$)

- implement these composition laws explicitly
- understand reduction theory (even with one n, and one base ring)