Binary Quadratic Forms over $\mathbb{F}[T]$ and PID's

Jeff Beyerl
Clemson University
Masters in Mathematical Sciences Defense
April 14, 2009

What is a Quadratic Form?

- A function

$$f = \sum_{i_1+i_2+\cdots+i_n=2} r_{(i_1,i_2,\ldots,i_n)} x_1^{i_1} x_2^{i_2} \cdot \cdots \cdot x_n^{i_n} \in R[x_1, x_2, \ldots, x_n].$$

- R is a ring
- $R[x_1, x_2, \ldots, x_n]$ is the polynomial ring over R.

What is a Binary Quadratic Form?

- A function
$$f = ax^2 + bxy + cy^2 \in R[x, y].$$

What is a Binary Quadratic Form?

- A function
$$f = ax^2 + bxy + cy^2 \in R[x, y].$$
- Alternate Notation 2: $f = [a, b, c]$

What is a Binary Quadratic Form?

- A function
$$f = ax^2 + bxy + cy^2 \in R[x, y].$$
- Alternate Notation 2: $f = [a, b, c]$
- Alternate Notation 3: $f = [a, b, *]_D$

$f = [a, b, *]_D$, what is D???

- $D = Disc(f)$ is the discriminant of f

$$D = Disc(f) := b^2 - 4ac$$

$f = [a, b, *]_D$, what is D???

- $D = Disc(f)$ is the discriminant of f

$$D = Disc(f) := b^2 - 4ac$$

- f is uniquely defined by a, b and either c or D.

$f = [a, b, *]_D$, what is D???

- $D = Disc(f)$ is the discriminant of f

$$D = Disc(f) := b^2 - 4ac$$

- f is uniquely defined by a, b and either c or D.
- ...At least if R is an integral domain, $char(R) \neq 2$.

Some Algebra Review

- A ring is an additive group and multiplicative semigroup such that the operations are distributive.

Some Algebra Review

- A ring is an additive group and multiplicative semigroup such that the operations are distributive.
- An integral domain is commutative ring with no zero divisors.

Some Algebra Review

- A ring is an additive group and multiplicative semigroup such that the operations are distributive.
- An integral domain is commutative ring with no zero divisors.
- The characteristic of a ring with [multiplicative] identity is the smallest positive n such that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

Some Algebra Review

- A ring is an additive group and multiplicative semigroup such that the operations are distributive.
- An integral domain is commutative ring with no zero divisors.
- The characteristic of a ring with [multiplicative] identity is the smallest positive n such that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

- A semigroup is a set of elements with an operation which is associative (e.g. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$)

Some Algebra Review

- A ring is an additive group and multiplicative semigroup such that the operations are distributive.
- An integral domain is commutative ring with no zero divisors.
- The characteristic of a ring with [multiplicative] identity is the smallest positive n such that

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$$

- A semigroup is a set of elements with an operation which is associative (e.g. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$)
- A group is a semigroup with an identity (e.g. $a + 0 = 0$) and inverses (e.g. $a + (-a) = 0$).

Some Algebra Review

- An ideal of a commutative ring is a subring which is closed under multiplication of ring elements.

Some Algebra Review

- An ideal of a commutative ring is a subring which is closed under multiplication of ring elements.
- A principal ideal of a ring is an ideal which is generated by a single element: $I = \langle a \rangle_R$ for some $a \in R$.

Some Algebra Review

- An ideal of a commutative ring is a subring which is closed under multiplication of ring elements.
- A principal ideal of a ring is an ideal which is generated by a single element: $I = \langle a \rangle_R$ for some $a \in R$.
- A Principal Ideal Domain is an integral domain in which every ideal is principal.

Some Algebra Review

- An ideal of a commutative ring is a subring which is closed under multiplication of ring elements.
- A principal ideal of a ring is an ideal which is generated by a single element: $I = \langle a \rangle_R$ for some $a \in R$.
- A Principal Ideal Domain is an integral domain in which every ideal is principal.
- ...They're really nice

Some Algebra Review

- An ideal of a commutative ring is a subring which is closed under multiplication of ring elements.
- A principal ideal of a ring is an ideal which is generated by a single element: $I = \langle a \rangle_R$ for some $a \in R$.
- A Principal Ideal Domain is an integral domain in which every ideal is principal.
- ...They're really nice
- ...Unfortunately

Some Algebra Review

- $GL_2(R)$ is the group of 2×2 with entries in R which are invertible in $R^{2\times 2}$.

Some Algebra Review

- $GL_2(R)$ is the group of 2×2 with entries in R which are invertible in $R^{2\times 2}$.
- $SL_2(R)$ is the group of 2×2 with entries in R and determinant 1 (and thus is invertible in $R^{2\times 2}$).

Some Algebra Review

- $GL_2(R)$ is the group of 2×2 with entries in R which are invertible in $R^{2\times 2}$.
- $SL_2(R)$ is the group of 2×2 with entries in R and determinant 1 (and thus is invertible in $R^{2\times 2}$).
- $\langle a_1, a_2, ..., a_l \rangle_R = \{a_1 r_1 + a_2 r_2 + \cdots + a_l r_l | r_i \in R\}$ is the ideal generated by $\{a_1, a_2, ..., a_l\}$.

Methodology

- Choose R.

Methodology

- Choose R.
- Do stuff.

Methodology

- Choose R.
- Do stuff.
- Fail to do stuff.

Methodology

- Choose R.
- Do stuff.
- Fail to do stuff.
- Add properties to R.

Methodology

- Choose R.
- Do stuff.
- Fail to do stuff.
- Add properties to R.
- Go to step 2.

The [primary] sources of insight

- My Advisers
- Primes of The Form $x + ny^2$, by David Cox.

The [primary] sources of insight

- My Advisers
- Primes of The Form $x + ny^2$, by David Cox.
- ...an overpriced Wiley book with a 6 page eratta

The [primary] sources of insight

- My Advisers
- Primes of The Form $x + ny^2$, by David Cox.
- ...an overpriced Wiley book with a 6 page eratta
- ...that's actually quite good.

Overview of my work

$$
\begin{tikzcd}
Q(D) \arrow[r, "\varphi'"] \arrow[d, "{[\cdot]}"] & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim \arrow[r, hook, two heads, "\varphi"] & I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}
$$

- $Q(D)$ is the set of all primitive forms with discriminant D.
- $Q(D)/\backsim$ is $Q(D)$ modulo $\backsim$, where $\backsim$ denotes proper equivalence.
- $I(\mathcal{O})$ is the group of all proper fractional ideals of a quadratic extension of $\mathbb{F}[T]$
- $I(\mathcal{O})/P(\mathcal{O})$ is the ideal class group of the same quadratic extension of $\mathbb{F}[T]$

Setup (for now)

- A is a principle ideal domain

Setup (for now)

- A is a principle ideal domain
- 2^{-1} exists and is in A.

Setup (for now)

- A is a principle ideal domain
- 2^{-1} exists and is in A.
- D will be reserved for the discriminant of our forms.

More on $Q(D)$

- $Q(D)$ is the set of all primitive forms with discriminant D.
- ...So if $[a, b, c] \in Q(D)$, then $b^2 - 4ac = D$.

More on $Q(D)$

- $Q(D)$ is the set of all primitive forms with discriminant D.
- ...So if $[a, b, c] \in Q(D)$, then $b^2 - 4ac = D$.
- If $\langle a, b, c\rangle_A = \langle 1\rangle_A$, then f is said to be <u>primitive</u>.

More on $Q(D)/\backsim$

- $Q(D)/\backsim = Q(D)$ modulo $\backsim$, where $f \backsim g$ is an equivalence relation called proper equivalence.

More on $Q(D)/\backsim$

- $Q(D)/\backsim = Q(D)$ modulo $\backsim$, where $f \backsim g$ is an equivalence relation called proper equivalence.
- If $f = [a, b, c], g = [a', b', c'] \in Q(D)$, then f is said to be properly equivalent to g if there is a $\gamma \in SL_2(A)$ so that $\gamma f = g$

More on $Q(D)/\backsim$

- $Q(D)/\backsim = Q(D)$ modulo $\backsim$, where $f \backsim g$ is an equivalence relation called proper equivalence.
- If $f = [a, b, c], g = [a', b', c'] \in Q(D)$, then f is said to be properly equivalent to g if there is a $\gamma \in SL_2(A)$ so that $\gamma f = g$
- ...where $\gamma f = \begin{bmatrix} p & q \\ r & s \end{bmatrix} f := f(px + qy, rx + sy) = [f(p, r), 2apq + bqr + bps + 2crs, f(q, s)]$.

More on $Q(D)/\backsim$

- $Q(D)/\backsim = Q(D)$ modulo $\backsim$, where $f \backsim g$ is an equivalence relation called proper equivalence.
- If $f = [a, b, c], g = [a', b', c'] \in Q(D)$, then f is said to be properly equivalent to g if there is a $\gamma \in SL_2(A)$ so that $\gamma f = g$
- ...where $\gamma f = \begin{bmatrix} p & q \\ r & s \end{bmatrix} f := f(px + qy, rx + sy) =$ $[f(p, r), 2apq + bqr + bps + 2crs, f(q, s)]$.
- Proper equivalence is equivalent to saying that f and g properly represent the same things

More on $Q(D)/\backsim$

- $Q(D)/\backsim = Q(D)$ modulo $\backsim$, where $f \backsim g$ is an equivalence relation called proper equivalence.
- If $f = [a, b, c], g = [a', b', c'] \in Q(D)$, then f is said to be properly equivalent to g if there is a $\gamma \in SL_2(A)$ so that $\gamma f = g$
- ...where $\gamma f = \begin{bmatrix} p & q \\ r & s \end{bmatrix} f := f(px + qy, rx + sy) = [f(p, r), 2apq + bqr + bps + 2crs, f(q, s)]$.
- Proper equivalence is equivalent to saying that f and g properly represent the same things
- ...If $f(\alpha, \beta) = m$ and $\langle \alpha, \beta \rangle_A = \langle 1 \rangle_A$, then m is said to be properly represented by f.

More on $Q(D)/\backsim$

Theorem

$Q(D)/\backsim$ is an abelian group.

Comments on the proof that $Q(D)/\backsim$ is a group

Comments on the proof that $Q(D)/\backsim$ is a group

- Given our operation, associative, identity, and inverses are all mostly easy.

Comments on the proof that $Q(D)/\backsim$ is a group

- Given our operation, associative, identity, and inverses are all mostly easy.
- Showing that the operation is well defined is not quite so easy.

Comments on the proof that $Q(D)/\backsim$ is a group

- Given our operation, associative, identity, and inverses are all mostly easy.
- Showing that the operation is well defined is not quite so easy.
- ...What is this operation?

An operation on $Q(D)/\backsim$

- To define an operation, we will use the following proposition:

Proposition

Let $D \in A$, $M \in A \setminus \{0\}, \mathcal{C}_1, \mathcal{C}_2 \in Q(D)/\backsim$. Then there are $f_1 \in \mathcal{C}_1$ and $f_2 \in \mathcal{C}_2$ such that

$$f_1 = [a_1, B, a_2 C], f_2 = [a_2, B, a_1 C]$$

where $a_i, B, C \in A$, $a_1 a_2 \neq 0$, $\langle a_1, a_2 \rangle_A = \langle 1 \rangle_A$, and $\langle a_1 a_2, M \rangle_A = \langle 1 \rangle_A$. (Forms that look like this are called concordant)

An operation on $Q(D)/\backsim$

- Let $[[a, b, a'c]], [[a', b, ac]] \in Q(D)/\backsim$

An operation on $Q(D)/\backsim$

- Let $[[a, b, a'c]], [[a', b, ac]] \in Q(D)/\backsim$
- Define $[[a, b, a'c]][[a', b, ac]] := [[aa', b, c]]$.

An operation on $Q(D)/\backsim$

- Let $[[a, b, a'c]], [[a', b, ac]] \in Q(D)/\backsim$
- Define $[[a, b, a'c]][[a', b, ac]] := [[aa', b, c]]$.
- ...which gives us a nice little operation to prove well-definedness of.

An operation on $Q(D)/\backsim$

- Let $[[a, b, a'c]], [[a', b, ac]] \in Q(D)/\backsim$
- Define $[[a, b, a'c]][[a', b, ac]] := [[aa', b, c]]$.
- ...which gives us a nice little operation to prove well-definedness of.
- ...which of course I'm not going to do here

An operation on $Q(D)/\backsim$

- Let $[[a, b, a'c]], [[a', b, ac]] \in Q(D)/\backsim$
- Define $[[a, b, a'c]][[a', b, ac]] := [[aa', b, c]]$.
- ...which gives us a nice little operation to prove well-definedness of.
- ...which of course I'm not going to do here
- ...for the health and sanity of the audience

Recap

$$
\begin{tikzcd}
Q(D) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim
\end{tikzcd}
$$

- A is any PID in which 2^{-1} exists and is in A.

Recap

$$\begin{tikzcd} Q(D) \arrow[d, "{[\cdot]}"] \\ Q(D)/\backsim \end{tikzcd}$$

- A is any PID in which 2^{-1} exists and is in A.
- $Q(D)$ is the set of all primitive forms of discriminant D.

Recap

$$\begin{tikzcd} Q(D) \arrow[d, "{[\cdot]}"] \\ Q(D)/\backsim \end{tikzcd}$$

- A is any PID in which 2^{-1} exists and is in A.
- $Q(D)$ is the set of all primitive forms of discriminant D.
- $Q(D)/\backsim$ is the set of such primitive forms modulo some strange equivalence defined by properly representing the same things.

Recap

$$\begin{array}{c} Q(D) \\ \downarrow{\scriptstyle [\cdot]} \\ Q(D)/\backsim \end{array}$$

- A is any PID in which 2^{-1} exists and is in A.
- $Q(D)$ is the set of all primitive forms of discriminant D.
- $Q(D)/\backsim$ is the set of such primitive forms modulo some strange equivalence defined by properly representing the same things.
- $Q(D)/\backsim$ is a group with some strange operation only defined on very special pairs of representatives from each operand.

Recap

$$\begin{tikzcd} Q(D) \arrow[d, "{[\cdot]}"] \\ Q(D)/\backsim \end{tikzcd}$$

- A is any PID in which 2^{-1} exists and is in A.
- $Q(D)$ is the set of all primitive forms of discriminant D.
- $Q(D)/\backsim$ is the set of such primitive forms modulo some strange equivalence defined by properly representing the same things.
- $Q(D)/\backsim$ is a group with some strange operation only defined on very special pairs of representatives from each operand.
- ...and it actually works!

Recap

$$\begin{tikzcd} Q(D) \arrow[d, "{[\cdot]}"] \\ Q(D)/\backsim \end{tikzcd}$$

- A is any PID in which 2^{-1} exists and is in A.
- $Q(D)$ is the set of all primitive forms of discriminant D.
- $Q(D)/\backsim$ is the set of such primitive forms modulo some strange equivalence defined by properly representing the same things.
- $Q(D)/\backsim$ is a group with some strange operation only defined on very special pairs of representatives from each operand.
- ...and it actually works!
- ...well, up to the fact that my proof only works if A is a blasted PID...

Specializing further to $\mathbb{F}[T]$

- $\mathbb{F} = \mathbb{F}_r = \mathbb{F}_{p^m}$, T an indeterminant.

Specializing further to $\mathbb{F}[T]$

- $\mathbb{F} = \mathbb{F}_r = \mathbb{F}_{p^m}$, T an indeterminant.
- $\mathbb{F}[T] = \{\sum_{i=0}^{n} a_i T^i | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{F}\}$ is the polynomial ring in one variable (T) with coefficients coming from $\mathbb{F}$.

Specializing further to $\mathbb{F}[T]$

- $\mathbb{F} = \mathbb{F}_r = \mathbb{F}_{p^m}$, T an indeterminant.
- $\mathbb{F}[T] = \{\sum_{i=0}^{n} a_i T^i | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{F}\}$ is the polynomial ring in one variable (T) with coefficients coming from $\mathbb{F}$.
- $\mathbb{F}[T]$ is a PID, and much more.

Specializing further to $\mathbb{F}[T]$

- $\mathbb{F} = \mathbb{F}_r = \mathbb{F}_{p^m}$, T an indeterminant.
- $\mathbb{F}[T] = \{\sum_{i=0}^{n} a_i T^i | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{F}\}$ is the polynomial ring in one variable (T) with coefficients coming from $\mathbb{F}$.
- $\mathbb{F}[T]$ is a PID, and much more.
- ...In particular, we have a discrete valuation on $\mathbb{F}[T]$, $\deg_T \left(\sum_{i=0}^{n} a_i T^i\right) = n$ ($\deg_T(0) = -\infty$)

Specializing further to $\mathbb{F}[T]$

- $\mathbb{F} = \mathbb{F}_r = \mathbb{F}_{p^m}$, T an indeterminant.
- $\mathbb{F}[T] = \{\sum_{i=0}^{n} a_i T^i | n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{F}\}$ is the polynomial ring in one variable (T) with coefficients coming from $\mathbb{F}$.
- $\mathbb{F}[T]$ is a PID, and much more.
- ...In particular, we have a discrete valuation on $\mathbb{F}[T]$, $\deg_T \left(\sum_{i=0}^{n} a_i T^i\right) = n$ ($\deg_T(0) = -\infty$)
- ...Actually the negative of the degree, but same idea.

More on $\mathbb{F}[T]$

- Using the degree, we are able to get

Lemma

Denote $f = [a, b, c] \in Q(*)$. *Then* $f \backsim f' = [a', b', c']$ *where* $\deg(b') < \deg(a') \leq \deg(c')$.

More on $\mathbb{F}[T]$

- Using the degree, we are able to get

Lemma

Denote $f = [a, b, c] \in Q(*)$. *Then* $f \backsim f' = [a', b', c']$ *where* $\deg(b') < \deg(a') \leq \deg(c')$.

- Which gives

Theorem

$Q(D)/\backsim$ *is finite.*

On $\mathbb{F}[T][\mathfrak{d}]$

- Let $D \in \mathbb{F}[T]$ be an irreducible polynomial.

On $\mathbb{F}[T][\mathfrak{d}]$

- Let $D \in \mathbb{F}[T]$ be an irreducible polynomial.
- $\mathfrak{d} := \sqrt{D}$

On $\mathbb{F}[T][\mathfrak{d}]$

- Let $D \in \mathbb{F}[T]$ be an irreducible polynomial.
- $\mathfrak{d} := \sqrt{D}$
- $\mathcal{O}_K = \mathbb{F}[T][\mathfrak{d}]$, $K = \mathbb{F}(T)[\mathfrak{d}]$

On $\mathbb{F}[T][\mathfrak{d}]$

- Let $D \in \mathbb{F}[T]$ be an irreducible polynomial.
- $\mathfrak{d} := \sqrt{D}$
- $\mathcal{O}_K = \mathbb{F}[T][\mathfrak{d}]$, $K = \mathbb{F}(T)[\mathfrak{d}]$
- ...there's more behind where this comes from that you saw last week.

On $\mathcal{O}$

- A subring $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$ is said to be an <u>order</u> in $\mathbb{F}(T)[\mathfrak{d}]$ when $\mathcal{O}$ is a finitely generated $\mathbb{F}[T]$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$, and contains a basis of $\mathbb{F}(T)[\mathfrak{d}]$ as a $\mathbb{F}(T)$-vector space.

On $\mathcal{O}$

- A subring $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$ is said to be an order in $\mathbb{F}(T)[\mathfrak{d}]$ when $\mathcal{O}$ is a finitely generated $\mathbb{F}[T]$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$, and contains a basis of $\mathbb{F}(T)[\mathfrak{d}]$ as a $\mathbb{F}(T)$-vector space.
- ...For a subring, $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$, this is equivalent to saying that $\mathcal{O}$ is a free $\mathbb{F}[T]$-submodule of rank 2

On $\mathcal{O}$

- A subring $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$ is said to be an <u>order</u> in $\mathbb{F}(T)[\mathfrak{d}]$ when $\mathcal{O}$ is a finitely generated $\mathbb{F}[T]$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$, and contains a basis of $\mathbb{F}(T)[\mathfrak{d}]$ as a $\mathbb{F}(T)$-vector space.
- ...For a subring, $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$, this is equivalent to saying that $\mathcal{O}$ is a free $\mathbb{F}[T]$-submodule of rank 2
- ...So for instance, every order looks like $\langle 1, f\mathfrak{d}\rangle_{\mathbb{F}[T]}$ for some $f \in \mathbb{F}[T]$.

On $I(\mathcal{O})$

- $I(\mathcal{O})$ is the group of all proper fractional ideals of $\mathcal{O}$.

On $I(\mathcal{O})$

- $I(\mathcal{O})$ is the group of all proper fractional ideals of $\mathcal{O}$.
- ...What's a fractional ideal?

On $I(\mathcal{O})$

- $I(\mathcal{O})$ is the group of all proper fractional ideals of $\mathcal{O}$.
- ...What's a fractional ideal?
- ...What's it mean to be proper?

More on $I(\mathcal{O})$

- A <u>fractional ideal</u> $\mathfrak{a}$ of $\mathcal{O}$ is a nonzero $\mathcal{O}$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$ such that there is an $a \in \mathcal{O}$ such that $a\mathfrak{a} \subseteq \mathcal{O}$.

More on $I(\mathcal{O})$

- A <u>fractional ideal</u> $\mathfrak{a}$ of $\mathcal{O}$ is a nonzero $\mathcal{O}$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$ such that there is an $a \in \mathcal{O}$ such that $a\mathfrak{a} \subseteq \mathcal{O}$.
- ...all nonzero finitely generated $\mathcal{O}$ submodules of $\mathbb{F}(T)[\mathfrak{d}]$ are fractional ideals.

More on $I(\mathcal{O})$

- A <u>fractional ideal</u> $\mathfrak{a}$ of $\mathcal{O}$ is a nonzero $\mathcal{O}$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$ such that there is an $a \in \mathcal{O}$ such that $a\mathfrak{a} \subseteq \mathcal{O}$.
- ...all nonzero finitely generated $\mathcal{O}$ submodules of $\mathbb{F}(T)[\mathfrak{d}]$ are fractional ideals.
- Note that if $\mathfrak{a} \subseteq \mathcal{O}$, then $\mathfrak{a}$ is a typical ideal.

More on $I(\mathcal{O})$

- A <u>fractional ideal</u> $\mathfrak{a}$ of $\mathcal{O}$ is a nonzero $\mathcal{O}$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$ such that there is an $a \in \mathcal{O}$ such that $a\mathfrak{a} \subseteq \mathcal{O}$.
- ...all nonzero finitely generated $\mathcal{O}$ submodules of $\mathbb{F}(T)[\mathfrak{d}]$ are fractional ideals.
- Note that if $\mathfrak{a} \subseteq \mathcal{O}$, then $\mathfrak{a}$ is a typical ideal.
- Also note that $\mathcal{O} \subseteq \mathcal{O}_K$.

More on $I(\mathcal{O})$

- Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$

More on $I(\mathcal{O})$

- Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$
- $\mathfrak{a}$ is said to be a <u>proper ideal</u> if $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$

More on $I(\mathcal{O})$

- Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$
- $\mathfrak{a}$ is said to be a proper ideal if $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$
- …" $\subseteq$ " is always true because $\mathfrak{a}$ is an $\mathcal{O}$ module.

More on $I(\mathcal{O})$

- Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$
- $\mathfrak{a}$ is said to be a <u>proper ideal</u> if $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$
- ..." $\subseteq$ " is always true because $\mathfrak{a}$ is an $\mathcal{O}$ module.
- Now the good news: proper fractional ideals are precisely those that are invertible.

More on $I(\mathcal{O})$

- Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$
- $\mathfrak{a}$ is said to be a proper ideal if $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$
- ..." $\subseteq$ " is always true because $\mathfrak{a}$ is an $\mathcal{O}$ module.
- Now the good news: proper fractional ideals are precisely those that are invertible.
- ...!!!!!!

More on $I(\mathcal{O})$

- $I(\mathcal{O})$ is then easily seen to be a group.

More on $I(\mathcal{O})$

- $I(\mathcal{O})$ is then easily seen to be a group.
- The operation is the standard multiplication of fractional ideals.

More on $I(\mathcal{O})$

- $I(\mathcal{O})$ is then easily seen to be a group.
- The operation is the standard multiplication of fractional ideals.
- ...$IJ = \{\sum_{k=0}^{m} i_k j_k | i_k \in I, j_k \in J, m \in \mathbb{Z}_{\geq 1}\}$.

More on $I(\mathcal{O})$

- $I(\mathcal{O})$ is then easily seen to be a group.
- The operation is the standard multiplication of fractional ideals.
- ...$IJ = \{\sum_{k=0}^{m} i_k j_k | i_k \in I, j_k \in J, m \in \mathbb{Z}_{\geq 1}\}$.
- ...And the identity is $\mathcal{O}$.

On $P(\mathcal{O})$

- $P(\mathcal{O})$ is the subgroup of all principal proper fractional ideals.

On $P(\mathcal{O})$

- $P(\mathcal{O})$ is the subgroup of all principal proper fractional ideals.
- ...Now isn't that a mouthful?

On $P(\mathcal{O})$

- $P(\mathcal{O})$ is the subgroup of all principal proper fractional ideals.
- ...Now isn't that a mouthful?
- ...But this is all just like algebraic number theory, except $\mathcal{O}$ is typically not a Dedekind Domain.

On $P(\mathcal{O})$

- $P(\mathcal{O})$ is the subgroup of all principal proper fractional ideals.
- ...Now isn't that a mouthful?
- ...But this is all just like algebraic number theory, except $\mathcal{O}$ is typically not a Dedekind Domain.
- ......(A Dedekind Domain's is an integral domain in which all the fractional ideals are invertible).

On $P(\mathcal{O})$

- $P(\mathcal{O})$ is the subgroup of all principal proper fractional ideals.
- ...Now isn't that a mouthful?
- ...But this is all just like algebraic number theory, except $\mathcal{O}$ is typically not a Dedekind Domain.
- ......(A Dedekind Domain's is an integral domain in which all the fractional ideals are invertible).
- ......Hence why we introduced the notion of proper fractional ideals.

On $I(\mathcal{O})/P(\mathcal{O})$

- We have a group, and a normal subgroup, would anyone not take a gander at their quotient?

On $I(\mathcal{O})/P(\mathcal{O})$

- We have a group, and a normal subgroup, would anyone not take a gander at their quotient?
- $I(\mathcal{O})/P(\mathcal{O})$ is called the ideal class group of $\mathcal{O}$.

Recap

$$
\begin{tikzcd}
Q(D) \arrow[d, "{[\cdot]}"] & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim & I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}
$$

- On the left we have quadratic forms over $\mathbb{F}[T]$

Recap

$$
\begin{tikzcd}
Q(D) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}
$$

- On the left we have quadratic forms over $\mathbb{F}[T]$
- On the right we have proper fractional ideals of an order $\mathcal{O} = \langle 1, f\mathfrak{d} \rangle_{\mathbb{F}[T]}$

Recap

$$
\begin{array}{ccc}
Q(D) & \qquad & I(\mathcal{O}) \\
\Big\downarrow [\cdot] & & \Big\downarrow [\cdot] \\
Q(D)/\backsim & & I(\mathcal{O})/P(\mathcal{O})
\end{array}
$$

- On the left we have quadratic forms over $\mathbb{F}[T]$
- On the right we have proper fractional ideals of an order $\mathcal{O} = \langle 1, f\mathfrak{d}\rangle_{\mathbb{F}[T]}$
- $Q(D)/\backsim$ is still a an abelian group.

Recap

$$
\begin{tikzcd}
Q(D) \arrow[d, "{[\cdot]}"] & & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim & & I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}
$$

- On the left we have quadratic forms over $\mathbb{F}[T]$
- On the right we have proper fractional ideals of an order $\mathcal{O} = \langle 1, f\mathfrak{d}\rangle_{\mathbb{F}[T]}$
- $Q(D)/\backsim$ is still a an abelian group.
- $I(\mathcal{O})/P(\mathcal{O})$ is also an abelian group.

Recap

$$\begin{array}{ccc} Q(D) & \qquad & I(\mathcal{O}) \\ \downarrow{\scriptstyle [\cdot]} & & \downarrow{\scriptstyle [\cdot]} \\ Q(D)/\backsim & & I(\mathcal{O})/P(\mathcal{O}) \end{array}$$

- On the left we have quadratic forms over $\mathbb{F}[T]$
- On the right we have proper fractional ideals of an order $\mathcal{O} = \langle 1, f\mathfrak{d} \rangle_{\mathbb{F}[T]}$
- $Q(D)/\backsim$ is still a an abelian group.
- $I(\mathcal{O})/P(\mathcal{O})$ is also an abelian group.
- ...And I drew them next to each other.

On φ'

- Define $\varphi' : Q(D) \to I(\mathcal{O})$ by $[a, b, c] \mapsto \langle a, \tau \rangle_{\mathbb{F}[T]}$

On φ'

- Define $\varphi' : Q(D) \to I(\mathcal{O})$ by $[a, b, c] \mapsto \langle a, \tau \rangle_{\mathbb{F}[T]}$
- ...where $\tau = \frac{-b+\sqrt{D}}{2a}$

On φ'

- Define $\varphi' : Q(D) \to I(\mathcal{O})$ by $[a, b, c] \mapsto \langle a, \tau \rangle_{\mathbb{F}[T]}$
- ...where $\tau = \frac{-b+\sqrt{D}}{2a}$
- ...doesn't τ look familiar?

On φ

- But we don't really care about $Q(D)$ and $I(\mathcal{O})$, so φ' is not our concern.

On φ

- But we don't really care about $Q(D)$ and $I(\mathcal{O})$, so φ' is not our concern.
- Instead consider $Q(D)/\backsim$ and $I(\mathcal{O})/P(\mathcal{O})$ and the induced map:

$$\varphi : Q(D)/\backsim \longrightarrow I(\mathcal{O})/P(\mathcal{O})$$

$$[[a, b, c]] \mapsto \left[\langle a, \tau\rangle_{\mathbb{F}[T]}\right]$$

More on φ

- Is φ well defined?

More on φ

- Is φ well defined?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[\langle a, \tau\rangle_{\mathbb{F}[T]}\right] = \left[\langle a', \tau'\rangle_{\mathbb{F}[T]}\right]$?

More on φ

- Is φ well defined?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[\langle a, \tau\rangle_{\mathbb{F}[T]}\right] = \left[\langle a', \tau'\rangle_{\mathbb{F}[T]}\right]$?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[a\left\langle 1, -b+\sqrt{D}\right\rangle_{\mathbb{F}[T]}\right] = \left[a'\left\langle 1, -b+\sqrt{D}\right\rangle_{\mathbb{F}[T]}\right]$?

More on φ

- Is φ well defined?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[\langle a, \tau\rangle_{\mathbb{F}[T]}\right] = \left[\langle a', \tau'\rangle_{\mathbb{F}[T]}\right]$?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[a\left\langle 1, -b + \sqrt{D}\right\rangle_{\mathbb{F}[T]}\right] = \left[a'\left\langle 1, -b + \sqrt{D}\right\rangle_{\mathbb{F}[T]}\right]$?
- Well, yes.

More on φ

- Is φ well defined?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[\langle a, \tau \rangle_{\mathbb{F}[T]}\right] = \left[\langle a', \tau' \rangle_{\mathbb{F}[T]}\right]$?
- If $[[a, b, c]] = [[a', b', c']]$, does $\left[a \left\langle 1, -b + \sqrt{D} \right\rangle_{\mathbb{F}[T]}\right] = \left[a' \left\langle 1, -b + \sqrt{D} \right\rangle_{\mathbb{F}[T]}\right]$?
- Well, yes.
- ...But again, I'm not going to torture the audience with the details.

More on φ

In fact, φ has some other* nice properties.

More on φ

In fact, φ has some other* nice properties. (*other than existing as a mapping)

More on φ

In fact, φ has some other* nice properties. (*other than existing as a mapping)

- φ is injective.

More on φ

In fact, φ has some other* nice properties. (*other than existing as a mapping)

- φ is injective.
- φ is surjective.

More on φ

In fact, φ has some other* nice properties. (*other than existing as a mapping)

- φ is injective.
- φ is surjective.
- φ is a group homomorphism.

More on φ

In fact, φ has some other* nice properties. (*other than existing as a mapping)

- φ is injective.
- φ is surjective.
- φ is a group homomorphism.
- Together these give

Theorem

$Q(D)/\backsim \cong I(\mathcal{O})/P(\mathcal{O})$ as groups via φ.

Summary

$$\begin{tikzcd} Q(D) \arrow[r, "\varphi'"] \arrow[d, "{[\cdot]}"] & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\ Q(D)/\backsim \arrow[r, hook, two heads, "\varphi"] & I(\mathcal{O})/P(\mathcal{O}) \end{tikzcd}$$

- The form class group, $Q(D)/\backsim$ is a finite group.

Summary

$$\begin{tikzcd}
Q(D) \arrow[rr, "\varphi'"] \arrow[d, "{[\cdot]}"] & & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim \arrow[rr, hook, two heads, "\varphi"] & & I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}$$

- The form class group, $Q(D)/\backsim$ is a finite group.
- The ideal class group of an order, $I(\mathcal{O})/P(\mathcal{O})$ is a group.

Summary

$$\begin{tikzcd}
Q(D) \arrow[rr, "\varphi'"] \arrow[d, "{[\cdot]}"] & & I(\mathcal{O}) \arrow[d, "{[\cdot]}"] \\
Q(D)/\backsim \arrow[rr, hook, two heads, "\varphi"] & & I(\mathcal{O})/P(\mathcal{O})
\end{tikzcd}$$

- The form class group, $Q(D)/\backsim$ is a finite group.
- The ideal class group of an order, $I(\mathcal{O})/P(\mathcal{O})$ is a group.
- $Q(D)/\backsim \cong I(\mathcal{O})/P(\mathcal{O})$ as groups.

Future Ambitions

Future Ambitions

- Continue deeper this stuff. (60%)

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%), Field Theory (60%)

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%), Field Theory (60%)
- Lots of areas that look as if they would be interesting but I know almost nothing about:

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%), Field Theory (60%)
- Lots of areas that look as if they would be interesting but I know almost nothing about: Representation Theory (28%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%), Field Theory (60%)
- Lots of areas that look as if they would be interesting but I know almost nothing about: Representation Theory (28%), cohomology (40%),

Future Ambitions

- Continue deeper this stuff. (60%)
- Try to generalize this to more general settings (65%)
- Continue with Drinfeld Modules (75%)
- Find interesting questions in function fields (70%)
- Lots of other interesting areas to study... Commutative Algebra (65%), Algebraic Geometry (70%), Elliptic Curves (68%), Group Theory (25%), Ring Theory (62%), Field Theory (60%)
- Lots of areas that look as if they would be interesting but I know almost nothing about: Representation Theory (28%), cohomology (40%), Category Theory (70%)

The End

- Thanks for coming!

The End

- Thanks for coming!
- ...For references, see my paper.