Infrastructure of Function Fields

Renate Scheidler

rscheidl@math.ucalgary.ca

Conference in Number Theory
Carleton University, Ottawa, June 29, 2011

Research supported in part by NSERC of Canada

Finite Cyclic Groups

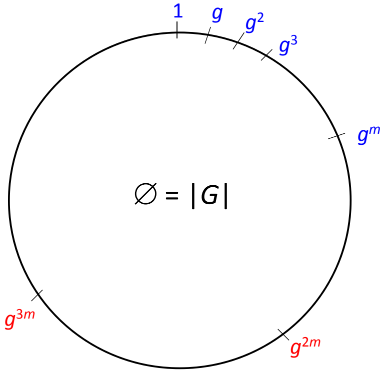
$G = \langle g \rangle$

Finite Cyclic Groups

$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Finite Cyclic Groups

$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

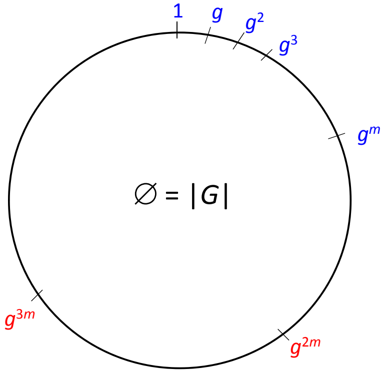


Finite Cyclic Groups

$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$



Finite Cyclic Groups

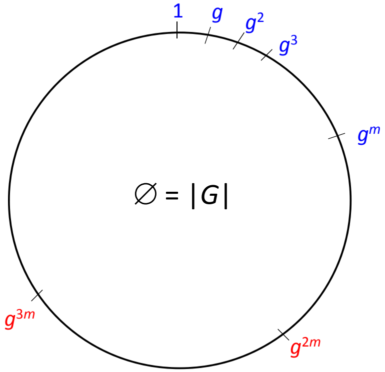
$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$



Finite Cyclic Groups

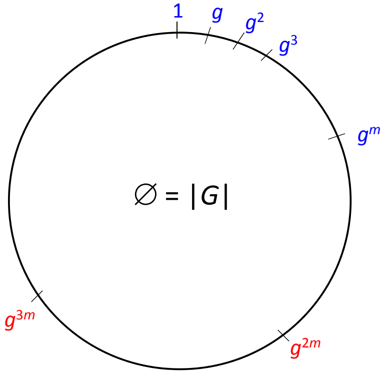
$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

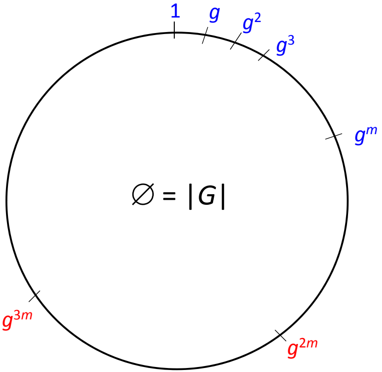
$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$



To find $|G| = \mathrm{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops

Finite Cyclic Groups



$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$

To find $|G| = \text{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops
- Smarter way — $O(\sqrt{|G|})$ ops

Finite Cyclic Groups

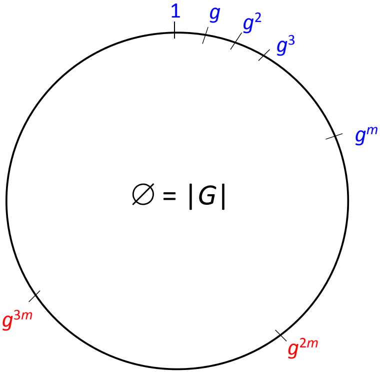
$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$



To find $|G| = \mathrm{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops
- Smarter way — $O(\sqrt{|G|})$ ops
  - baby steps $1, g, g^2, \ldots g^m$, $m \approx \sqrt{|G|}$

Finite Cyclic Groups

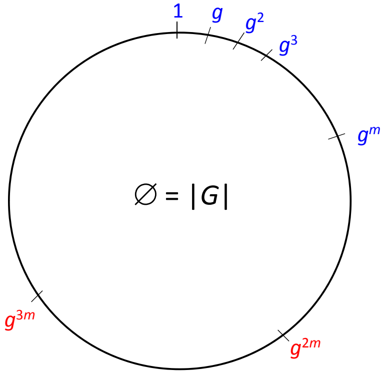
$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$

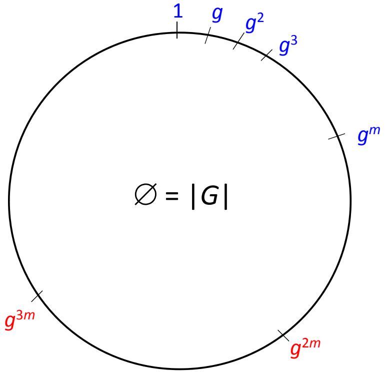


To find $|G| = \mathrm{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops
- Smarter way — $O(\sqrt{|G|})$ ops
  - baby steps $1, g, g^2, \ldots g^m$, $\; m \approx \sqrt{|G|}$
  - giant steps $g^{2m}, g^{3m}, \ldots, g^{km}$, $\; k \approx \sqrt{|G|}$

Finite Cyclic Groups

$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i



Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$

To find $|G| = \mathrm{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops
- Smarter way — $O(\sqrt{|G|})$ ops
  - baby steps $1, g, g^2, \ldots g^m, \quad m \approx \sqrt{|G|}$
  - giant steps $g^{2m}, g^{3m}, \ldots, g^{km}, \quad k \approx \sqrt{|G|}$
  - $g^{km} = g^i$ (a baby step) $\implies |G| = |km - i|$

Finite Cyclic Groups

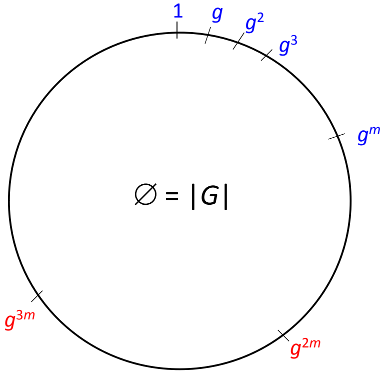
$G = \langle g \rangle, \quad \delta(g^i) = i$ **distance** of g^i

Baby Step: $g^i \to g^{i+1} = g^i * g$

$\delta(g^{i+1}) = i + 1 = \delta(g^i) + 1$

Giant Step: $(g^i, g^j) \to g^i * g^j = g^{i+j}$

$\delta(g^i * g^j) = i + j = \delta(g^i) + \delta(g^j)$



To find $|G| = \mathrm{ord}(g)$:

- Dumb way: baby steps $g, g^2, \ldots, g^{|G|}$ — $O(|G|)$ ops
- Smarter way — $O(\sqrt{|G|})$ ops
  - baby steps $1, g, g^2, \ldots g^m$, $\; m \approx \sqrt{|G|}$
  - giant steps $g^{2m}, g^{3m}, \ldots, g^{km}$, $\; k \approx \sqrt{|G|}$
  - $g^{km} = g^i$ (a baby step) $\implies |G| = |km - i|$

Similar technique solves **discrete logarithm/distance problem**):

given g^i, find $\delta(g^i) = i$

Infrastructures

$$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$$

Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

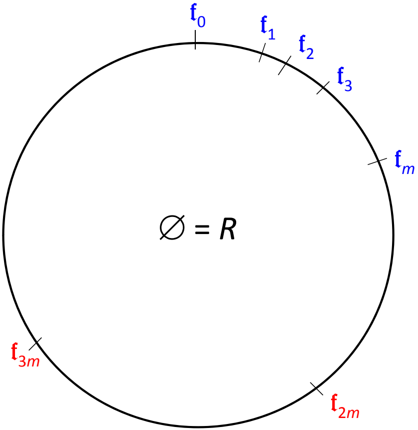
circumference R

Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

circumference R



Infrastructures

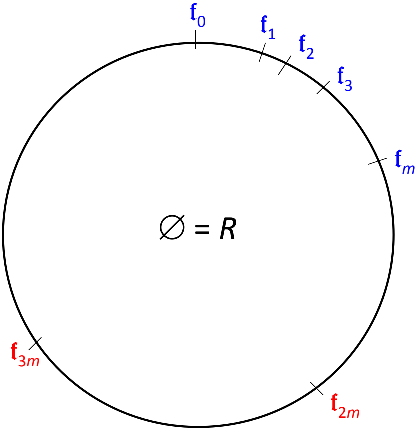
$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

circumference R

Baby Step: $\mathfrak{f}_i \to \mathfrak{f}_{i+1}$

$\delta(\mathfrak{f}_{i+1}) \approx i + 1 \approx \delta(\mathfrak{f}_i) + 1$



Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

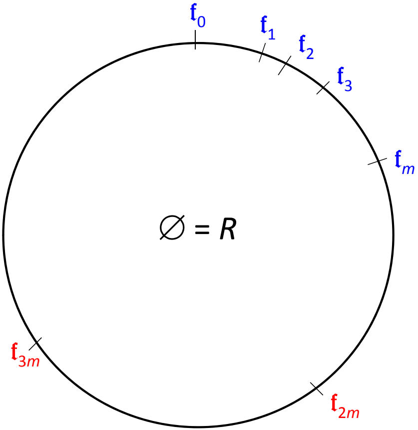
circumference R

Baby Step: $\mathfrak{f}_i \to \mathfrak{f}_{i+1}$

$\delta(\mathfrak{f}_{i+1}) \approx i + 1 \approx \delta(\mathfrak{f}_i) + 1$

Giant Step: $(\mathfrak{f}_i, \mathfrak{f}_j) = \mathfrak{f}_i * \mathfrak{f}_j$

$\delta(\mathfrak{f}_i * \mathfrak{f}_j) \approx i + j \approx \delta(\mathfrak{f}_i) + \delta(\mathfrak{f}_j)$



Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

circumference R

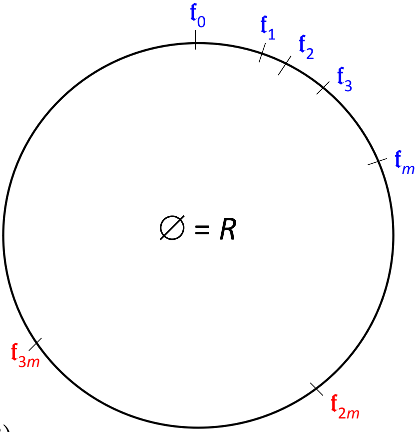
Baby Step: $\mathfrak{f}_i \to \mathfrak{f}_{i+1}$

$\delta(\mathfrak{f}_{i+1}) \approx i + 1 \approx \delta(\mathfrak{f}_i) + 1$

Giant Step: $(\mathfrak{f}_i, \mathfrak{f}_j) = \mathfrak{f}_i * \mathfrak{f}_j$

$\delta(\mathfrak{f}_i * \mathfrak{f}_j) \approx i + j \approx \delta(\mathfrak{f}_i) + \delta(\mathfrak{f}_j)$

"Errors" are known and of order $\log(R)$



Infrastructures

$\mathcal{R} = \{\mathfrak{f}_0, \mathfrak{f}_1, \ldots, \mathfrak{f}_s\}$,

$\delta(\mathfrak{f}_i) \approx i$ **distance** of $\mathfrak{f}_i$

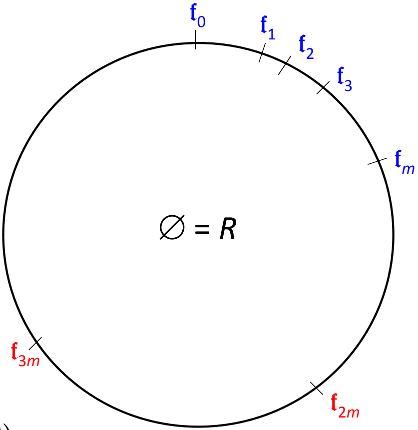
circumference R

Baby Step: $\mathfrak{f}_i \to \mathfrak{f}_{i+1}$

$\delta(\mathfrak{f}_{i+1}) \approx i + 1 \approx \delta(\mathfrak{f}_i) + 1$

Giant Step: $(\mathfrak{f}_i, \mathfrak{f}_j) = \mathfrak{f}_i * \mathfrak{f}_j$

$\delta(\mathfrak{f}_i * \mathfrak{f}_j) \approx i + j \approx \delta(\mathfrak{f}_i) + \delta(\mathfrak{f}_j)$



"Errors" are known and of order $\log(R)$

Can use a similar baby step giant step technique to

- find circumference R of $\mathcal{R}$
- solve distance problem

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y]$$

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Roots of $f(x,1) = Ax^2 + Bx + C$: $\quad \tau_{\pm} = \dfrac{B \pm \sqrt{D}}{2A} \in \mathbb{R}$

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Roots of $f(x,1) = Ax^2 + Bx + C$: $\quad \tau_\pm = \dfrac{B \pm \sqrt{D}}{2A} \in \mathbb{R}$

f is **reduced** if $0 < -\tau_- < 1 < \tau_+ \quad (0 < \sqrt{D} - B < 2A < \sqrt{D} + B)$

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Roots of $f(x,1) = Ax^2 + Bx + C$: $\quad \tau_\pm = \dfrac{B \pm \sqrt{D}}{2A} \in \mathbb{R}$

f is **reduced** if $0 < -\tau_- < 1 < \tau_+ \quad (0 < \sqrt{D} - B < 2A < \sqrt{D} + B)$

Infrastructure $\mathcal{R} = \{f \sim f_0 \text{ reduced}\}, \qquad \delta(f_{i+1}) = \delta(f_i) + \log(\tau_{+,i})$

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Roots of $f(x,1) = Ax^2 + Bx + C$: $\quad \tau_\pm = \dfrac{B \pm \sqrt{D}}{2A} \in \mathbb{R}$

f is **reduced** if $0 < -\tau_- < 1 < \tau_+ \quad (0 < \sqrt{D} - B < 2A < \sqrt{D} + B)$

Infrastructure $\mathcal{R} = \{f \sim f_0 \text{ reduced}\}, \qquad \delta(f_{i+1}) = \delta(f_i) + \log(\tau_{+,i})$

Baby Step: $(A, B, C) \to (C - qB + q^2A,\ 2qA - B,\ A), \quad q = \lfloor \tau \rfloor$

(Continued fraction algorithm applied to τ_+)

Example 1 – Indefinite Binary Quadratic Forms (Shanks 1971)

$$f(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y], \qquad D = B^2 - 4AC > 0$$

Roots of $f(x,1) = Ax^2 + Bx + C$: $\quad \tau_\pm = \dfrac{B \pm \sqrt{D}}{2A} \in \mathbb{R}$

f is **reduced** if $0 < -\tau_- < 1 < \tau_+ \quad (0 < \sqrt{D} - B < 2A < \sqrt{D} + B)$

Infrastructure $\mathcal{R} = \{f \sim f_0 \text{ reduced}\}, \qquad \delta(f_{i+1}) = \delta(f_i) + \log(\tau_{+,i})$

Baby Step: $(A,B,C) \to (C - qB + q^2A,\ 2qA - B,\ A), \quad q = \lfloor \tau \rfloor$
(Continued fraction algorithm applied to τ_+)

Giant Step:

- **Composition** (Gauß): $(A', B', C') \circ (A'', B'', C'') = (A, B, C)$
  where (assuming $\gcd(A', A'', (B' + B'')/2) = 1$):

$$A = A'A'', \qquad B \equiv \begin{cases} 2A' \pmod{B'}, \\ 2A'' \pmod{B''}, \end{cases} \qquad C = \frac{B^2 - D}{4A}$$

- followed by approximately $\log(D)/2$ baby steps

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Example 2 – Ideals of Real Quadratic Orders
(H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\quad \mathfrak{a} = [A, B] = \mathbb{Z}\, A \oplus \mathbb{Z}\, \frac{B + \sqrt{D}}{2}$, $\quad 4A \mid B^2 - D$

Example 2 – Ideals of Real Quadratic Orders
(H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\quad \mathfrak{a} = [A, B] = \mathbb{Z}\, A \oplus \mathbb{Z}\, \dfrac{B + \sqrt{D}}{2}\,, \quad 4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\Longleftrightarrow f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\quad \mathfrak{a} = [A, B] = \mathbb{Z}\, A \oplus \mathbb{Z}\, \dfrac{B + \sqrt{D}}{2}\,, \quad 4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\Longleftrightarrow f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a}$ reduced and principal$\}$:

- $\mathcal{R}$ is closed under giant steps

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\mathfrak{a} = [A, B] = \mathbb{Z}\,A \oplus \mathbb{Z}\,\dfrac{B + \sqrt{D}}{2}$, $4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\Longleftrightarrow f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a}$ reduced and principal$\}$:

- $\mathcal{R}$ is closed under giant steps
- giant steps are commutative

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, ...)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\quad \mathfrak{a} = [A, B] = \mathbb{Z}\, A \oplus \mathbb{Z}\, \dfrac{B + \sqrt{D}}{2}\,, \quad 4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\iff f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a} \text{ reduced and principal}\}$:

- $\mathcal{R}$ is closed under giant steps
- giant steps are commutative
- $\mathcal{O}_D$ is the identity under giant steps

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\mathfrak{a} = [A, B] = \mathbb{Z} A \oplus \mathbb{Z} \frac{B + \sqrt{D}}{2}$, $4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\Longleftrightarrow f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a}$ reduced and principal$\}$:

- $\mathcal{R}$ is closed under giant steps
- giant steps are commutative
- $\mathcal{O}_D$ is the identity under giant steps
- $\overline{\mathfrak{a}} = [A, \overline{B}]$ is the inverse under giant steps of $\mathfrak{a} = [A, B]$ where $\overline{B} \equiv -B \pmod{2A}$; $\delta(\overline{\mathfrak{a}}) = R + \log(A) - \delta(\mathfrak{a})$

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, . . .)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\quad \mathfrak{a} = [A, B] = \mathbb{Z}\,A \oplus \mathbb{Z}\,\dfrac{B+\sqrt{D}}{2}\ , \quad 4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\Longleftrightarrow f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a}$ reduced and principal$\}$:

- $\mathcal{R}$ is closed under giant steps
- giant steps are commutative
- $\mathcal{O}_D$ is the identity under giant steps
- $\overline{\mathfrak{a}} = [A, \overline{B}]$ is the inverse under giant steps of $\mathfrak{a} = [A, B]$ where $\overline{B} \equiv -B \pmod{2A}$; $\delta(\overline{\mathfrak{a}}) = R + \log(A) - \delta(\mathfrak{a})$
- $\mathcal{R}$ is "almost" associative under giant steps, in the sense that $(\mathfrak{a} * \mathfrak{b}) * \mathfrak{c}$ and $\mathfrak{a} * (\mathfrak{b} * \mathfrak{c})$ are very close to each other in $\mathcal{R}$. So $\mathcal{R}$ is "almost" an abelian group under giant steps!

Example 2 – Ideals of Real Quadratic Orders (H. Williams 1987, ...)

Let $\mathcal{O}_D$ be a quadratic order of discriminant $D > 0$

Ideals in $\mathcal{O}_D$: $\mathfrak{a} = [A, B] = \mathbb{Z}A \oplus \mathbb{Z}\dfrac{B + \sqrt{D}}{2}$, $4A \mid B^2 - D$

Theorem $\mathfrak{a} = [A, B]$ is an $\mathcal{O}_D$-ideal $\iff f = (A, B, (B^2 - D)/4A)$ is a binary quadratic form of discriminant D

Properties of infrastructure $\mathcal{R} = \{\mathfrak{a}$ reduced and principal$\}$:

- $\mathcal{R}$ is closed under giant steps
- giant steps are commutative
- $\mathcal{O}_D$ is the identity under giant steps
- $\overline{\mathfrak{a}} = [A, \overline{B}]$ is the inverse under giant steps of $\mathfrak{a} = [A, B]$ where $\overline{B} \equiv -B \pmod{2A}$; $\delta(\overline{\mathfrak{a}}) = R + \log(A) - \delta(\mathfrak{a})$
- $\mathcal{R}$ is "almost" associative under giant steps, in the sense that $(\mathfrak{a} * \mathfrak{b}) * \mathfrak{c}$ and $\mathfrak{a} * (\mathfrak{b} * \mathfrak{c})$ are very close to each other in $\mathcal{R}$. So $\mathcal{R}$ is "almost" an abelian group under giant steps!
- R is the regulator of O_D

Example 3 – Divisors of Real Hyperelliptic Curves (Stein 1992/2009; Jacobson, S. & Stein 2007, . . .)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g + 2$ (q odd)

Example 3 – Divisors of Real Hyperelliptic Curves

(Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g + 2$ (q odd)

Regulator $R = \mathrm{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

Example 3 – Divisors of Real Hyperelliptic Curves (Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g + 2$ (q odd)

Regulator $R = \mathrm{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \mathrm{supp}(D_x)$, $\;v_P(D) \geq 0$ for all $P \in \mathrm{supp}(D_x)$
- $P = (a, b) \in \mathrm{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \mathrm{supp}(D_x)$
- $P = \overline{P} \in \mathrm{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Example 3 – Divisors of Real Hyperelliptic Curves
(Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g+2$ (q odd)

Regulator $R = \mathrm{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \mathrm{supp}(D_x)$, $\;v_P(D) \geq 0$ for all $P \in \mathrm{supp}(D_x)$
- $P = (a, b) \in \mathrm{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \mathrm{supp}(D_x)$
- $P = \overline{P} \in \mathrm{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Remark The Mumford coefficients A, B of D correspond to a reduced $\mathbb{F}_q[x, y]$-ideal $\mathfrak{a} = [A, B]$

Example 3 – Divisors of Real Hyperelliptic Curves
(Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g+2$ (q odd)

Regulator $R = \mathrm{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \mathrm{supp}(D_x)$, $\; v_P(D) \geq 0$ for all $P \in \mathrm{supp}(D_x)$
- $P = (a, b) \in \mathrm{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \mathrm{supp}(D_x)$
- $P = \overline{P} \in \mathrm{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Remark The Mumford coefficients A, B of D correspond to a reduced $\mathbb{F}_q[x, y]$-ideal $\mathfrak{a} = [A, B]$

Properties of the infrastructure $\mathcal{R} = \{D \text{ reduced and principal}\}$

Baby steps: $\delta(0) = 0$, $\; \delta(D_1) = g + 1$, $\; 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$

Example 3 – Divisors of Real Hyperelliptic Curves (Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C: y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g+2$ (q odd)

Regulator $R = \mathrm{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \mathrm{supp}(D_x)$, $\;v_P(D) \geq 0$ for all $P \in \mathrm{supp}(D_x)$
- $P = (a, b) \in \mathrm{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \mathrm{supp}(D_x)$
- $P = \overline{P} \in \mathrm{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Remark The Mumford coefficients A, B of D correspond to a reduced $\mathbb{F}_q[x, y]$-ideal $\mathfrak{a} = [A, B]$

Properties of the infrastructure $\mathcal{R} = \{D \text{ reduced and principal}\}$

Baby steps: $\delta(0) = 0$, $\;\delta(D_1) = g+1$, $\;1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$

Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d$, $\quad 0 \leq d \leq 2g$

Example 3 – Divisors of Real Hyperelliptic Curves (Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g + 2$ (q odd)

Regulator $R = \operatorname{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \operatorname{supp}(D_x)$, $\ v_P(D) \geq 0$ for all $P \in \operatorname{supp}(D_x)$
- $P = (a, b) \in \operatorname{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \operatorname{supp}(D_x)$
- $P = \overline{P} \in \operatorname{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Remark The Mumford coefficients A, B of D correspond to a reduced $\mathbb{F}_q[x, y]$-ideal $\mathfrak{a} = [A, B]$

Properties of the infrastructure $\mathcal{R} = \{D \text{ reduced and principal}\}$

Baby steps: $\delta(0) = 0$, $\ \delta(D_1) = g + 1$, $\ 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$

Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d$, $\quad 0 \leq d \leq 2g$

divisor addition, followed by at most $\lceil g/2 \rceil$ baby steps

Example 3 – Divisors of Real Hyperelliptic Curves
(Stein 1992/2009; Jacobson, S. & Stein 2007, ...)

$C : y^2 = D(x) \in \mathbb{F}_q[x]$ monic, square-free, of degree $2g + 2$ (q odd)

Regulator $R = \text{ord}([\overline{\infty} - \infty]) \approx q^g$ $\quad$ (∞, $\overline{\infty}$ the poles of x)

A degree 0 divisor $D = D_x - \deg(D_x)\infty + \delta(D)(\overline{\infty} - \infty)$ is **reduced** if

- D is defined over $\mathbb{F}_q$ (i.e. invariant under Frobenius)
- $\infty, \overline{\infty} \notin \text{supp}(D_x)$, $\; v_P(D) \geq 0$ for all $P \in \text{supp}(D_x)$
- $P = (a, b) \in \text{supp}(D_x) \Rightarrow \overline{P} = (a, -b) \notin \text{supp}(D_x)$
- $P = \overline{P} \in \text{supp}(D_x) \Rightarrow v_{\overline{P}}(D) = 1$
- $\deg(D_x) \leq g$ and $0 \leq \delta(D) < R$

Remark The Mumford coefficients A, B of D correspond to a reduced $\mathbb{F}_q[x, y]$-ideal $\mathfrak{a} = [A, B]$

Properties of the infrastructure $\mathcal{R} = \{D \text{ reduced and principal}\}$

Baby steps: $\delta(0) = 0$, $\; \delta(D_1) = g + 1$, $\; 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$

Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d$, $\quad 0 \leq d \leq 2g$

divisor addition, followed by at most $\lceil g/2 \rceil$ baby steps

$\mathcal{R}$ is embeddable into the cyclic group $\langle [\overline{\infty} - \infty] \rangle$ of order R (Fontein 2008)

Example 4 – Global Cubic Fields

Example 4 – Global Cubic Fields

The distinguished fractional ideals of a complex cubic number field form an infrastructure:

Example 4 – Global Cubic Fields

The distinguished fractional ideals of a complex cubic number field form an infrastructure:

- Baby steps: Voronoi's algorithm
- Giant steps: Ideal multiplication, followed by Voronoi baby steps

(Voronoi 1896, Delone & Fadeev 1964, Williams et al 1970/80s)

Example 4 – Global Cubic Fields

The distinguished fractional ideals of a complex cubic number field form an infrastructure:

- Baby steps: Voronoi's algorithm
- Giant steps: Ideal multiplication, followed by Voronoi baby steps

(Voronoi 1896, Delone & Fadeev 1964, Williams et al 1970/80s)

The distinguished divisors of a cubic extension of $\mathbb{F}_q(x)$ with two poles at x form an infrastructure:

Example 4 – Global Cubic Fields

The distinguished fractional ideals of a complex cubic number field form an infrastructure:

- Baby steps: Voronoi's algorithm
- Giant steps: Ideal multiplication, followed by Voronoi baby steps

(Voronoi 1896, Delone & Fadeev 1964, Williams et al 1970/80s)

The distinguished divisors of a cubic extension of $\mathbb{F}_q(x)$ with two poles at x form an infrastructure:

- Baby steps and giant steps analogous to cubic number fields

(S. & Stein 1998/2000, S. 2001, Landquist 2009, research ongoing)

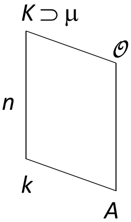
So for what global fields to (circle) infrastructures arise?

Infrastructure from the Unit Lattice
(Fontein 2011)

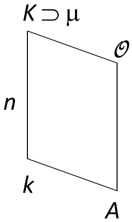
$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity

K a finite algebraic extension of k of degree n

$\mathcal{O}$ the integral closure of A in K (Dedekind domain)



Infrastructure from the Unit Lattice (Fontein 2011)



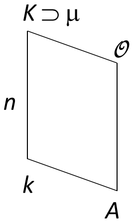
$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity

K a finite algebraic extension of k of degree n

$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

$$S = \begin{cases} \text{set of conjugate mappings (archimedian places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

Infrastructure from the Unit Lattice (Fontein 2011)



$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity

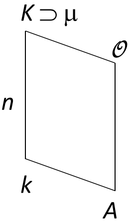
K a finite algebraic extension of k of degree n

$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

$$S = \begin{cases} \text{set of conjugate mappings (archimedean places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

For the **unit group** $\mathcal{O}^*$ of $\mathcal{O}$: $\mathcal{O}^*/\mu \cong \mathbb{Z}^r$ with $r = |S| - 1$

Infrastructure from the Unit Lattice (Fontein 2011)



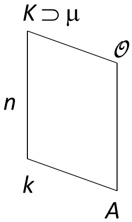
$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity
K a finite algebraic extension of k of degree n
$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

$$S = \begin{cases} \text{set of conjugate mappings (archimedian places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

For the **unit group** $\mathcal{O}^*$ of $\mathcal{O}$: $\mathcal{O}^*/\mu \cong \mathbb{Z}^r$ with $r = |S| - 1$

For $\alpha \in K^*$, define $\phi(\alpha) = (v_{\mathfrak{p}}(\alpha) \deg(\mathfrak{p}) \mid \mathfrak{p} \in S)$

Infrastructure from the Unit Lattice
(Fontein 2011)



$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity
K a finite algebraic extension of k of degree n
$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

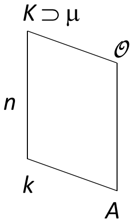
$$S = \begin{cases} \text{set of conjugate mappings (archimedian places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

For the **unit group** $\mathcal{O}^*$ of $\mathcal{O}$: $\mathcal{O}^*/\mu \cong \mathbb{Z}^r$ with $r = |S| - 1$

For $\alpha \in K^*$, define $\phi(\alpha) = (v_{\mathfrak{p}}(\alpha) \deg(\mathfrak{p}) \mid \mathfrak{p} \in S)$

ϕ maps $\mathcal{O}^*/\mu$ into the **unit lattice** $\mathcal{L}$ in $\begin{cases} \mathbb{R}^r & \text{if } k = \mathbb{Q}, \\ \mathbb{Z}^r & \text{if } K = \mathbb{F}_q(x) \end{cases}$

Infrastructure from the Unit Lattice
(Fontein 2011)



$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity
K a finite algebraic extension of k of degree n
$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

$$S = \begin{cases} \text{set of conjugate mappings (archimedean places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

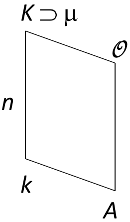
For the **unit group** $\mathcal{O}^*$ of $\mathcal{O}$: $\mathcal{O}^*/\mu \cong \mathbb{Z}^r$ with $r = |S| - 1$

For $\alpha \in K^*$, define $\phi(\alpha) = (v_{\mathfrak{p}}(\alpha)\deg(\mathfrak{p}) \mid \mathfrak{p} \in S)$

ϕ maps $\mathcal{O}^*/\mu$ into the **unit lattice** $\mathcal{L}$ in $\begin{cases} \mathbb{R}^r & \text{if } k = \mathbb{Q}, \\ \mathbb{Z}^r & \text{if } K = \mathbb{F}_q(x) \end{cases}$

Regulator $R = \det(\mathcal{L})$

Infrastructure from the Unit Lattice (Fontein 2011)



$k = \mathbb{Q}$ or $\mathbb{F}_q(x)$, $A = \mathbb{Z}$ or $\mathbb{F}_q[x]$, $\mu \subset K^*$ roots of unity
K a finite algebraic extension of k of degree n
$\mathcal{O}$ the integral closure of A in K (Dedekind domain)

$$S = \begin{cases} \text{set of conjugate mappings (archimedian places)} & \text{if } k = \mathbb{Q} \\ \text{set of poles of } x \text{ (infinite places)} & \text{if } k = \mathbb{F}_q(x) \end{cases}$$

For the **unit group** $\mathcal{O}^*$ of $\mathcal{O}$: $\mathcal{O}^*/\mu \cong \mathbb{Z}^r$ with $r = |S| - 1$

For $\alpha \in K^*$, define $\phi(\alpha) = (v_{\mathfrak{p}}(\alpha)\deg(\mathfrak{p}) \mid \mathfrak{p} \in S)$

ϕ maps $\mathcal{O}^*/\mu$ into the **unit lattice** $\mathcal{L}$ in $\begin{cases} \mathbb{R}^r & \text{if } k = \mathbb{Q}, \\ \mathbb{Z}^r & \text{if } K = \mathbb{F}_q(x) \end{cases}$

Regulator $R = \det(\mathcal{L})$

Infrastructure $\mathcal{R} := \left\{ \begin{array}{ll} \mathbb{R}^r/\mathcal{L} & \text{if } K = \mathbb{Q} \\ \mathbb{Z}^r/\mathcal{L} & \text{if } K = \mathbb{F}_q(x) \end{array} \right\}$ r-dimensional torus

Circle Infrastructures

$$|S| = 1 \quad \Rightarrow \quad r = 0 \quad \Rightarrow \quad \text{no infrastructure}$$
$$|S| = 2 \quad \Rightarrow \quad r = 1 \quad \Rightarrow \quad \text{circle infrastructure}$$

Circle Infrastructures

$$|S| = 1 \quad \Rightarrow \quad r = 0 \quad \Rightarrow \quad \text{no infrastructure}$$
$$|S| = 2 \quad \Rightarrow \quad r = 1 \quad \Rightarrow \quad \text{circle infrastructure}$$

Number Fields:

r_1: number of real embeddings

r_2: number of pairs of complex embeddings

$$r = r_1 + r_2 - 1, \quad n = r_1 + 2r_2, \quad r_1 \geq 0, \quad r_2 \geq 0$$

Circle Infrastructures

$|S| = 1 \quad \Rightarrow \quad r = 0 \quad \Rightarrow \quad$ no infrastructure
$|S| = 2 \quad \Rightarrow \quad r = 1 \quad \Rightarrow \quad$ circle infrastructure

Number Fields:

r_1: number of real embeddings
r_2: number of pairs of complex embeddings

$$r = r_1 + r_2 - 1, \quad n = r_1 + 2r_2, \quad r_1 \geq 0, \quad r_2 \geq 0$$

Solutions for $r = 0$:

$r_1 = 1,\ r_2 = 0,\ n = 1$ — $\mathbb{Q}$
$r_1 = 0,\ r_2 = 1,\ n = 2$ — imaginary quadratic

Circle Infrastructures

$$|S| = 1 \quad \Rightarrow \quad r = 0 \quad \Rightarrow \quad \text{no infrastructure}$$
$$|S| = 2 \quad \Rightarrow \quad r = 1 \quad \Rightarrow \quad \text{circle infrastructure}$$

Number Fields:

r_1: number of real embeddings

r_2: number of pairs of complex embeddings

$$r = r_1 + r_2 - 1, \quad n = r_1 + 2r_2, \quad r_1 \geq 0, \quad r_2 \geq 0$$

Solutions for $r = 0$:

$r_1 = 1,\ r_2 = 0,\ n = 1$ — $\mathbb{Q}$

$r_1 = 0,\ r_2 = 1,\ n = 2$ — imaginary quadratic

Solutions for $r = 1$:

$r_1 = 2,\ r_2 = 0,\ n = 2$ — real quadratic

$r_1 = 1,\ r_2 = 1,\ n = 3$ — complex cubic

$r_1 = 0,\ r_2 = 2,\ n = 2$ — totally complex quartic

Circle Infrastructures

$$|S| = 1 \quad \Rightarrow \quad r = 0 \quad \Rightarrow \quad \text{no infrastructure}$$
$$|S| = 2 \quad \Rightarrow \quad r = 1 \quad \Rightarrow \quad \text{circle infrastructure}$$

Number Fields:

r_1: number of real embeddings

r_2: number of pairs of complex embeddings

$$r = r_1 + r_2 - 1, \quad n = r_1 + 2r_2, \quad r_1 \geq 0, \quad r_2 \geq 0$$

Solutions for $r = 0$:

$r_1 = 1,\ r_2 = 0,\ n = 1$ — $\mathbb{Q}$

$r_1 = 0,\ r_2 = 1,\ n = 2$ — imaginary quadratic

Solutions for $r = 1$:

$r_1 = 2,\ r_2 = 0,\ n = 2$ — real quadratic

$r_1 = 1,\ r_2 = 1,\ n = 3$ — complex cubic

$r_1 = 0,\ r_2 = 2,\ n = 2$ — totally complex quartic

Function Fields: for any r, $n \geq r$ can be anything!

Boxes

Write $S = \{\infty_1, \ldots, \infty_{r+1}\}$, with respective ramification indices e_i

Boxes

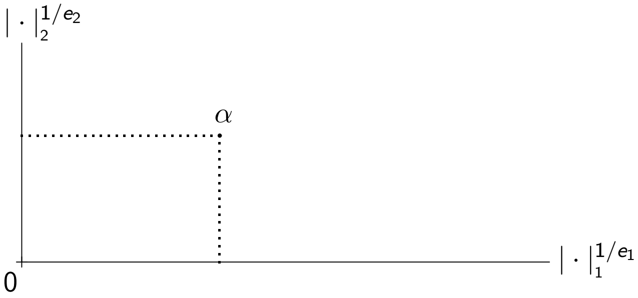
Write $S = \{\infty_1, \ldots, \infty_{r+1}\}$, with respective ramification indices e_i

For $\alpha \in K$, write $|\alpha|_i = q^{-v_{\infty_i}(\alpha)}$.

Boxes

Write $S = \{\infty_1, \ldots, \infty_{r+1}\}$, with respective ramification indices e_i

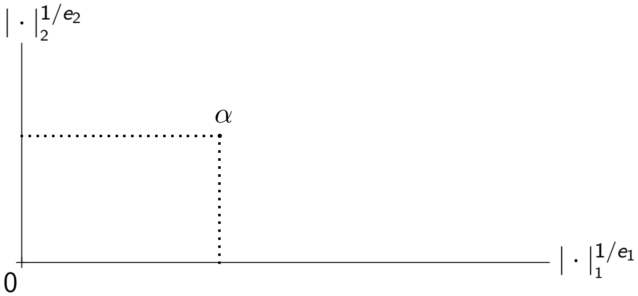
For $\alpha \in K$, write $|\alpha|_i = q^{-v_{\infty_i}(\alpha)}$. Then the values $|\alpha|_i^{1/e_i}$ form a box:



Boxes

Write $S = \{\infty_1, \ldots, \infty_{r+1}\}$, with respective ramification indices e_i

For $\alpha \in K$, write $|\alpha|_i = q^{-v_{\infty_i}(\alpha)}$. Then the values $|\alpha|_i^{1/e_i}$ form a box:



Length function on K: $B(\alpha) = \max_{1 \leq i \leq r+1} |\alpha|_i^{1/e_i}$

Successive Minima of Fractional Ideals

(Minkowski 1910, Mahler 1986, Tang 2011)

Successive Minima of Fractional Ideals
(Minkowski 1910, Mahler 1986, Tang 2011)

First successive minimum of $\mathfrak{f}$: $M_1(\mathfrak{f}) = \min\{B(\alpha) \mid 0 \neq \alpha \in \mathfrak{f}\}$

Successive Minima of Fractional Ideals
(Minkowski 1910, Mahler 1986, Tang 2011)

First successive minimum of $\mathfrak{f}$: $M_1(\mathfrak{f}) = \min\{B(\alpha) \mid 0 \neq \alpha \in \mathfrak{f}\}$

i-**th successive minimum** of L:

Successive Minima of Fractional Ideals
(Minkowski 1910, Mahler 1986, Tang 2011)

First successive minimum of $\mathfrak{f}$: $M_1(\mathfrak{f}) = \min\{B(\alpha) \mid 0 \neq \alpha \in \mathfrak{f}\}$

i-**th successive minimum** of L:

Let $\omega_1, \ldots, \omega_i \in \mathfrak{f}$ be $\mathbb{F}_q[x]$-linearly independent.

$$M_i(\mathfrak{f}) = \min\{B(\alpha) \quad \mid \quad \alpha \in \mathfrak{f} \text{ and } \omega_1, \ldots, \omega_{i-1}, \alpha \text{ are } \mathbb{F}_q[x]\text{-linearly independent}\}$$

Successive Minima of Fractional Ideals (Minkowski 1910, Mahler 1986, Tang 2011)

First successive minimum of $\mathfrak{f}$: $M_1(\mathfrak{f}) = \min\{B(\alpha) \mid 0 \neq \alpha \in \mathfrak{f}\}$

i-**th successive minimum** of L:

Let $\omega_1, \ldots, \omega_i \in \mathfrak{f}$ be $\mathbb{F}_q[x]$-linearly independent.

$$M_i(\mathfrak{f}) = \min\{B(\alpha) \quad | \quad \alpha \in \mathfrak{f} \text{ and } \omega_1, \ldots, \omega_{i-1}, \alpha \text{ are } \mathbb{F}_q[x]\text{-linearly independent}\}$$

Successive minima depend only on $\mathfrak{f}$, not on $\omega_1, \ldots, \omega_n, \alpha$

Distinguished Ideals

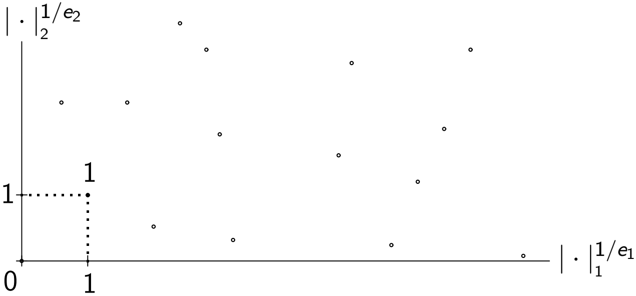
A fractional $\mathcal{O}$-ideal $\mathfrak{f}$ is **distinguished** if for all $\alpha \in \mathfrak{f}$

$$B(\alpha) \leq 1 \implies \alpha \in \mathbb{F}_q$$

Distinguished Ideals

A fractional $\mathcal{O}$-ideal $\mathfrak{f}$ is **distinguished** if for all $\alpha \in \mathfrak{f}$

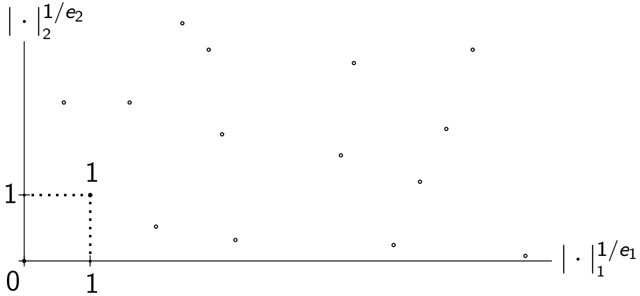
$$B(\alpha) \leq 1 \implies \alpha \in \mathbb{F}_q$$



Distinguished Ideals

A fractional $\mathcal{O}$-ideal $\mathfrak{f}$ is **distinguished** if for all $\alpha \in \mathfrak{f}$

$$B(\alpha) \leq 1 \implies \alpha \in \mathbb{F}_q$$



Properties: Suppose $M_1(\mathfrak{f}) = B(\alpha)$ with $\alpha \in \mathfrak{f}$

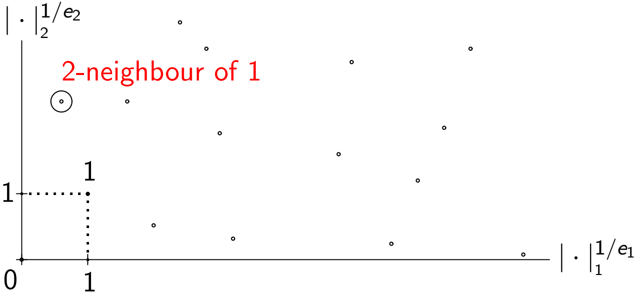
- $M_1(\alpha^{-1}\mathfrak{f}) = 1$
- $\mathfrak{f}$ distinguished $\iff$ $\alpha \in \mathbb{F}_q^*$ (so $M_1(\mathfrak{f}) = 1$) and $M_2(\mathfrak{f}) > 1$

Neighbours

i-**neighbour** of 1 in $\mathfrak{f}$ — next lattice point from 1 in $|\cdot|_i$-direction
without increasing all the other dimensions of the box

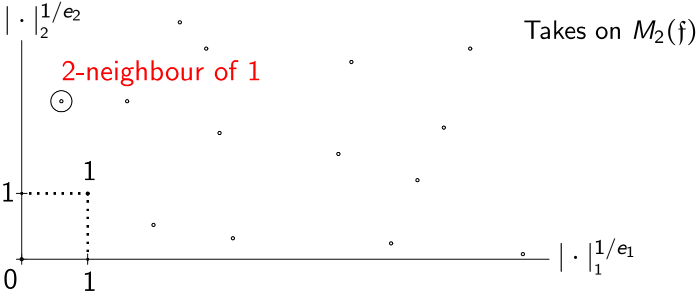
Neighbours

i-**neighbour** of 1 in $\mathfrak{f}$ — next lattice point from 1 in $|\cdot|_i$-direction
without increasing all the other dimensions of the box



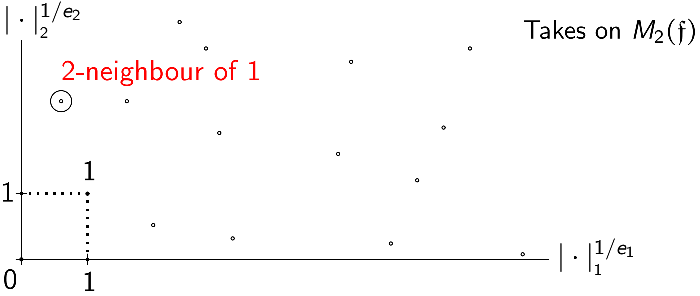
Neighbours

i-**neighbour** of 1 in $\mathfrak{f}$ — next lattice point from 1 in $|\cdot|_i$-direction
without increasing all the other dimensions of the box



Neighbours

i-**neighbour** of 1 in $\mathfrak{f}$ — next lattice point from 1 in $|\cdot|_i$-direction without increasing all the other dimensions of the box



Obtained via a **0-reduced** B-**ordered** $\mathbb{F}_q[x]$-basis of $\mathfrak{f}$

- very technical definition (Schörnig 1996, A. Lenstra 1985)
- computationally highly useful
- takes on the n successive minima of $\mathfrak{f}$
- efficiently computable for $r = 1$, $e_1 = 1$, $e_2 = n - 1$ (Tang 2011)

Infrastructure, Ideal-Theoretic Description (Tang 2011)

$$r = 1, \quad e_1 = 1, \quad e_2 = n - 1$$

Infrastructure, Ideal-Theoretic Description (Tang 2011)

$r = 1, \quad e_1 = 1, \quad e_2 = n - 1$

Infrastructure $\mathcal{R} = \{\mathfrak{f} \sim \mathfrak{f}_0 \text{ distinguished}\}$

Infrastructure, Ideal-Theoretic Description (Tang 2011)

$r = 1, \quad e_1 = 1, \quad e_2 = n - 1$

Infrastructure $\mathcal{R} = \{\mathfrak{f} \sim \mathfrak{f}_0 \text{ distinguished}\}$

Baby step $\mathfrak{f} \to \mathfrak{g}$:

1. $\mathfrak{g} = \eta^{-1}\mathfrak{f}$ with η the 2-neighbour of 1 in $\mathfrak{f}$

$$\delta(\mathfrak{g}) = \delta(\mathfrak{f}) - v_{\infty_2}(\eta)$$

Infrastructure, Ideal-Theoretic Description (Tang 2011)

$r = 1, \quad e_1 = 1, \quad e_2 = n - 1$

Infrastructure $\mathcal{R} = \{\mathfrak{f} \sim \mathfrak{f}_0 \text{ distinguished}\}$

Baby step $\mathfrak{f} \to \mathfrak{g}$:

1. $\mathfrak{g} = \eta^{-1}\mathfrak{f}$ with η the 2-neighbour of 1 in $\mathfrak{f}$

$$\delta(\mathfrak{g}) = \delta(\mathfrak{f}) - v_{\infty_2}(\eta)$$

Giant step $\mathfrak{f}' * \mathfrak{f}''$:

1. Compute ideal product $\mathfrak{f}'\mathfrak{f}''$, 0-reduce & B-order resulting basis
2. Divide by ω where $B(\omega) = M_1(\mathfrak{f})$, 0-reduce & B-order resulting basis
3. Apply one baby step

Infrastructure, Divisor-Theoretic Description

Distinguished fractional ideal $\mathfrak{f}$ of distance $\delta(\mathfrak{f})$

$\updownarrow$

Distinguished integral ideal $\mathfrak{a} = \mathrm{denom}(\mathfrak{f})\mathfrak{f}$ of distance $\delta(\mathfrak{a}) = \delta(\mathfrak{f})$

$\updownarrow$

Distinguished degree 0 divisor $D = D_x - \deg(D_x)\infty_1 + \delta(D)(\infty_2 - \infty_1)$
with $\delta(D) = \delta(\mathfrak{a})$

Infrastructure, Divisor-Theoretic Description

Distinguished fractional ideal $\mathfrak{f}$ of distance $\delta(\mathfrak{f})$

$\updownarrow$

Distinguished integral ideal $\mathfrak{a} = \mathrm{denom}(\mathfrak{f})\mathfrak{f}$ of distance $\delta(\mathfrak{a}) = \delta(\mathfrak{f})$

$\updownarrow$

Distinguished degree 0 divisor $D = D_x - \deg(D_x)\infty_1 + \delta(D)(\infty_2 - \infty_1)$
with $\delta(D) = \delta(\mathfrak{a})$

Properties:

- Baby steps: $\delta(0) = 0$, $\delta(D_1) \leq g + 1$, $1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$

Infrastructure, Divisor-Theoretic Description

Distinguished fractional ideal $\mathfrak{f}$ of distance $\delta(\mathfrak{f})$

$$\updownarrow$$

Distinguished integral ideal $\mathfrak{a} = \mathrm{denom}(\mathfrak{f})\mathfrak{f}$ of distance $\delta(\mathfrak{a}) = \delta(\mathfrak{f})$

$$\updownarrow$$

Distinguished degree 0 divisor $D = D_x - \deg(D_x)\infty_1 + \delta(D)(\infty_2 - \infty_1)$
with $\delta(D) = \delta(\mathfrak{a})$

Properties:

- Baby steps: $\delta(0) = 0, \;\; \delta(D_1) \leq g + 1, \;\; 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$
- Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d, \quad 0 \leq d \leq 2g$

Infrastructure, Divisor-Theoretic Description

Distinguished fractional ideal $\mathfrak{f}$ of distance $\delta(\mathfrak{f})$

$\updownarrow$

Distinguished integral ideal $\mathfrak{a} = \mathrm{denom}(\mathfrak{f})\mathfrak{f}$ of distance $\delta(\mathfrak{a}) = \delta(\mathfrak{f})$

$\updownarrow$

Distinguished degree 0 divisor $D = D_x - \deg(D_x)\infty_1 + \delta(D)(\infty_2 - \infty_1)$
with $\delta(D) = \delta(\mathfrak{a})$

Properties:

- Baby steps: $\delta(0) = 0, \;\; \delta(D_1) \leq g + 1, \;\; 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$
- Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d, \quad 0 \leq d \leq 2g$
- Baby steps and giant steps are efficiently computable

Infrastructure, Divisor-Theoretic Description

Distinguished fractional ideal $\mathfrak{f}$ of distance $\delta(\mathfrak{f})$

$$\updownarrow$$

Distinguished integral ideal $\mathfrak{a} = \mathrm{denom}(\mathfrak{f})\mathfrak{f}$ of distance $\delta(\mathfrak{a}) = \delta(\mathfrak{f})$

$$\updownarrow$$

Distinguished degree 0 divisor $D = D_x - \deg(D_x)\infty_1 + \delta(D)(\infty_2 - \infty_1)$
with $\delta(D) = \delta(\mathfrak{a})$

Properties:

- Baby steps: $\delta(0) = 0, \;\; \delta(D_1) \leq g + 1, \;\; 1 \leq \delta(D_{i+1}) - \delta(D_i) \leq g$
- Giant steps: $\delta(D' * D'') = \delta(D') + \delta(D'') - d, \quad 0 \leq d \leq 2g$
- Baby steps and giant steps are efficiently computable
- Run time ratio giant steps/baby steps proportional to n^2

Higher-Dimensional Infrastructures

Higher-Dimensional Infrastructures

$r = 2$, purely cubic extensions $K = k(\sqrt[3]{D})$

- Number fields: H. C. Williams et al (1970s and 80s), Buchmann (1980s)
- Function fields: Lee, S. & Yarrish (2003); Fontein, Landquist & S. (in progress)

Higher-Dimensional Infrastructures

$r = 2$, purely cubic extensions $K = k(\sqrt[3]{D})$

- Number fields: H. C. Williams et al (1970s and 80s), Buchmann (1980s)
- Function fields: Lee, S. & Yarrish (2003); Fontein, Landquist & S. (in progress)

Arbitrary r:

- Number Fields: Buchmann (*Habilitationsschrift* 1987)
- Number fields in function field language (Arakelov theory): Schoof (2008)
- Global Fields: Fontein (2011, ongoing)

Wrap-Up

- There are better regulator/class number algorithm than straightforward baby step giant step that use truncated Euler products — $O(|D|^{1/5}) = O(R^{2/5})$
  - Real quadratic number fields: Lenstra 1982, Schoof 1982
  - Real hyperelliptic curves: Stein & Williams 1999, Stein & Teske 2002/2005
  - Cubic function fields: S. & Stein 2007
  - Arbitrary function fields (in principle): S. & Stein 2010

Wrap-Up

- There are better regulator/class number algorithm than straightforward baby step giant step that use truncated Euler products — $O(|D|^{1/5}) = O(R^{2/5})$
  - Real quadratic number fields: Lenstra 1982, Schoof 1982
  - Real hyperelliptic curves: Stein & Williams 1999, Stein & Teske 2002/2005
  - Cubic function fields: S. & Stein 2007
  - Arbitrary function fields (in principle): S. & Stein 2010

- In function fields, infrastructure arithmetic can be advantageous over divisor class group arithmetic due to the much faster baby step operation (real hyperelliptic: Stein & Teske 2005; cubic: Landquist 2007-ongoing; used for cryptography in Jacobson, S. & Stein 2007)

Wrap-Up

- There are better regulator/class number algorithm than straightforward baby step giant step that use truncated Euler products — $O(|D|^{1/5}) = O(R^{2/5})$
  - Real quadratic number fields: Lenstra 1982, Schoof 1982
  - Real hyperelliptic curves: Stein & Williams 1999, Stein & Teske 2002/2005
  - Cubic function fields: S. & Stein 2007
  - Arbitrary function fields (in principle): S. & Stein 2010

- In function fields, infrastructure arithmetic can be advantageous over divisor class group arithmetic due to the much faster baby step operation (real hyperelliptic: Stein & Teske 2005; cubic: Landquist 2007-ongoing; used for cryptography in Jacobson, S. & Stein 2007)

- *Lots* left to do:
  - Improvements to and implementation of Tang's algorithms
  - Other signatures (splitting of infinite place of $\mathbb{F}_q(x)$)
  - Low degree extensions with special arithmetic (cubics? quartics?)
  - ...

$\ast \ \ast \ \ast$ **Thank You!** — **Questions (or Answers)?** $\ast \ \ast \ \ast$