A Concise Interpretation of the Infrastructure of a Global Field

Felix Fontein

CISaC, University of Calgary

May 12, 2009

Overview

Overview

One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

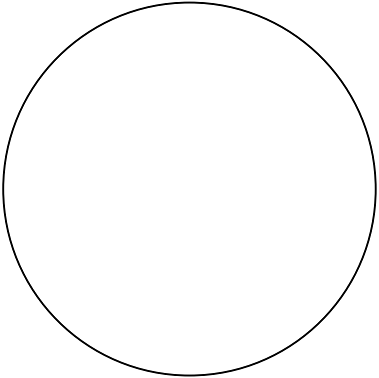
- a finite set $X \neq \emptyset$;

One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;



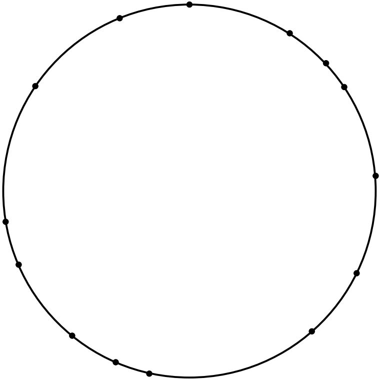
One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map

$$d : X \to \mathbb{R}/R\mathbb{Z}.$$

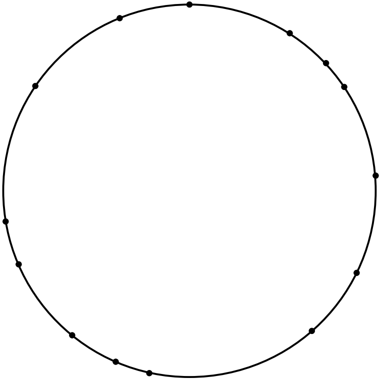


One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map
$$d : X \to \mathbb{R}/R\mathbb{Z}.$$



- Two operations:

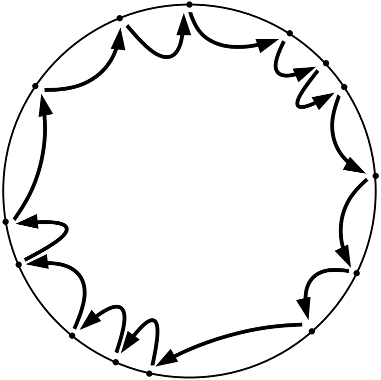
One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map

$$d : X \to \mathbb{R}/R\mathbb{Z}.$$



- Two operations:
  - baby steps;

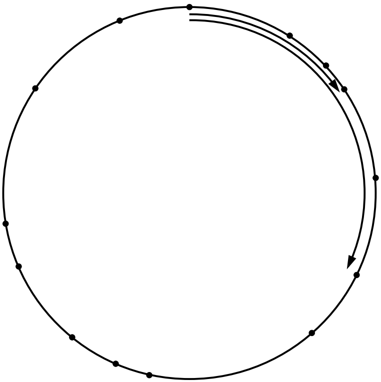
One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map

$$d : X \to \mathbb{R}/R\mathbb{Z}.$$



- Two operations:
  - baby steps;
  - giant steps.

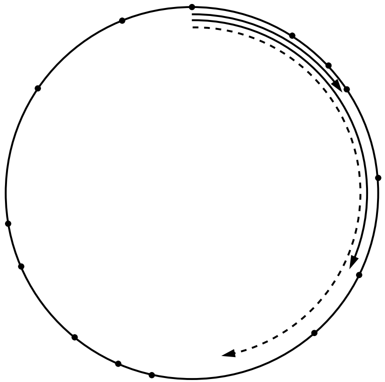
One-Dimensional Infrastructure

Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map

$$d : X \to \mathbb{R}/R\mathbb{Z}.$$



- Two operations:
  - baby steps;
  - giant steps.

One-Dimensional Infrastructure

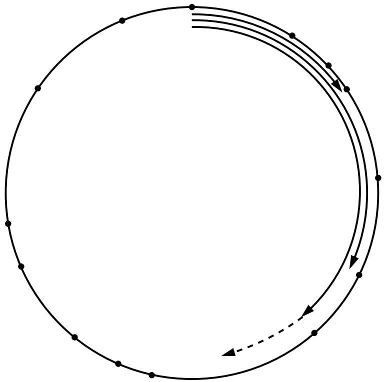
Definition

A one-dimensional infrastructure is:

- a finite set $X \neq \emptyset$;
- a number $R > 0$;
- an injective map

$$d : X \to \mathbb{R}/R\mathbb{Z}.$$

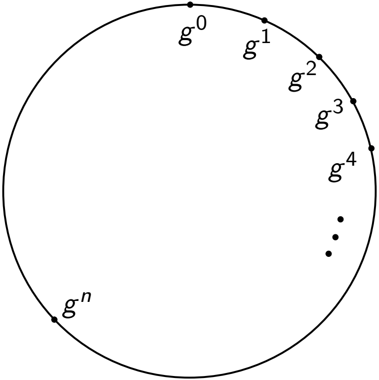
- Two operations:
  - baby steps;
  - giant steps.



A Special Case: The Discrete Logarithm

We have:

- A finite cyclic group $X = \langle g \rangle$;
- $R = |X|$;
- $d : X \to \mathbb{Z}/R\mathbb{Z} \subseteq \mathbb{R}/R\mathbb{Z}$ with $g^{d(h)} = h$.

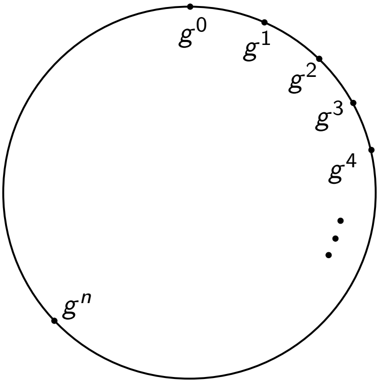


A Special Case: The Discrete Logarithm

We have:

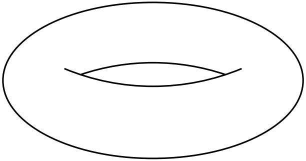
- A finite cyclic group $X = \langle g \rangle$;
- $R = |X|$;
- $d : X \to \mathbb{Z}/R\mathbb{Z} \subseteq \mathbb{R}/R\mathbb{Z}$ with $g^{d(h)} = h$.

- Two operations:
  - baby steps:
  $$h \mapsto gh;$$
  - giant steps:
  $$(h, h') \mapsto hh'.$$



Higher Dimensional Infrastructure

Replace $\mathbb{R}/R\mathbb{Z}$ by $\mathbb{R}^n/\Lambda$, Λ a lattice!



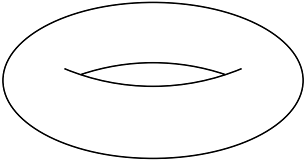
Higher Dimensional Infrastructure

Replace $\mathbb{R}/R\mathbb{Z}$ by $\mathbb{R}^n/\Lambda$, Λ a lattice!

Definition

An *n-dimensional infrastructure* is:

- a finite set $X \neq \emptyset$;
- a lattice $\Lambda \subseteq \mathbb{R}^n$;



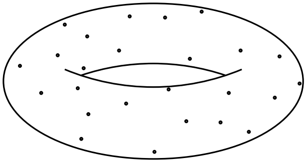
Higher Dimensional Infrastructure

Replace $\mathbb{R}/R\mathbb{Z}$ by $\mathbb{R}^n/\Lambda$, Λ a lattice!

Definition

An *n-dimensional infrastructure* is:

- a finite set $X \neq \emptyset$;
- a lattice $\Lambda \subseteq \mathbb{R}^n$;
- an injective map $d : X \to \mathbb{R}^n/\Lambda$.



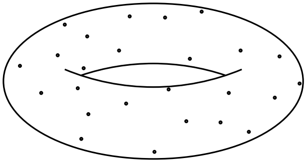
Higher Dimensional Infrastructure

Replace $\mathbb{R}/R\mathbb{Z}$ by $\mathbb{R}^n/\Lambda$, Λ a lattice!

Definition

An *n-dimensional infrastructure* is:

- a finite set $X \neq \emptyset$;
- a lattice $\Lambda \subseteq \mathbb{R}^n$;
- an injective map $d : X \to \mathbb{R}^n/\Lambda$.



- This generalizes the Generalized Discrete Logarithm, i.e. writing group elements in terms of a fixed set of generators.

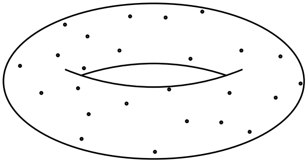
Higher Dimensional Infrastructure

Replace $\mathbb{R}/R\mathbb{Z}$ by $\mathbb{R}^n/\Lambda$, Λ a lattice!

Definition

An *n-dimensional infrastructure* is:

- a finite set $X \neq \emptyset$;
- a lattice $\Lambda \subseteq \mathbb{R}^n$;
- an injective map $d : X \to \mathbb{R}^n/\Lambda$.



- This generalizes the Generalized Discrete Logarithm, i.e. writing group elements in terms of a fixed set of generators.
- But:
  - What should baby steps be?
  - Giant steps can be done, as we will see later...

Overview

f-Representations, Part One

Back to the one-dimensional case!

- The map
$$\begin{aligned} d : X \times \mathbb{R} &\to \mathbb{R}/R\mathbb{Z}, \\ (x, f) &\mapsto d(x) + f \end{aligned}$$
is surjective.
- Idea: Restrict to a subset of $X \times \mathbb{R}$ such that this map gets bijective!

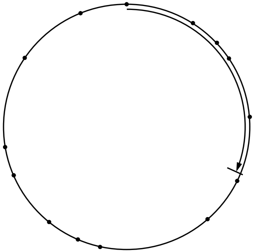
f-Representations, Part One

Back to the one-dimensional case!

- The map

$$\begin{aligned} d : X \times \mathbb{R} &\to \mathbb{R}/R\mathbb{Z}, \\ (x, f) &\mapsto d(x) + f \end{aligned}$$

  is surjective.



- Idea: Restrict to a subset of $X \times \mathbb{R}$ such that this map gets bijective!
- For example:

$$\begin{aligned} & (x, f) \in \mathrm{Rep}^f(X, d) \\ :\Longleftrightarrow {} & f \geq 0 \wedge \forall 0 < g \leq f : d(x) + g \notin d(X); \end{aligned}$$

  then $d|_{\mathrm{Rep}^f(X,d)}$ is bijective.

f-Representations, Part One

Back to the one-dimensional case!

- The map

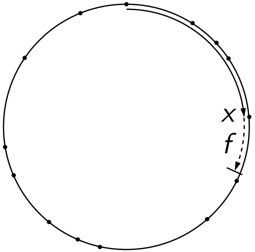
$$d : X \times \mathbb{R} \to \mathbb{R}/R\mathbb{Z},$$
$$(x, f) \mapsto d(x) + f$$

  is surjective.

- Idea: Restrict to a subset of $X \times \mathbb{R}$ such that this map gets bijective!
- For example:

$$(x, f) \in \mathrm{Rep}^f(X, d)$$
$$:\iff f \geq 0 \wedge \forall 0 < g \leq f : d(x) + g \notin d(X);$$

  then $d|_{\mathrm{Rep}^f(X,d)}$ is bijective.



f-Representations, Part Two

- We have bijection
$$d : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}.$$
- Idea: describe arithmetic on $\mathbb{R}/R\mathbb{Z}$ using elements of $\mathrm{Rep}^f(X, d)$.

f-Representations, Part Two

- We have bijection

$$d : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}.$$

- Idea: describe arithmetic on $\mathbb{R}/R\mathbb{Z}$ using elements of $\mathrm{Rep}^f(X, d)$.
- If
  - this can be done efficiently and
  - computation of d is inefficient,

  then one can consider a problem in $\mathrm{Rep}^f(X, d)$ similar to the DLP:

Distance Problem

Given $(x, f) \in \mathrm{Rep}^f(X, d)$, find a $t \in \mathbb{R}$ with $d(x, f) = t + R\mathbb{Z}$.

f-Representations, Part Two

- We have bijection

$$d : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}.$$

- Idea: describe arithmetic on $\mathbb{R}/R\mathbb{Z}$ using elements of $\mathrm{Rep}^f(X, d)$.
- If
  - this can be done efficiently and
  - computation of d is inefficient,

  then one can consider a problem in $\mathrm{Rep}^f(X, d)$ similar to the DLP:

Distance Problem

Given $(x, f) \in \mathrm{Rep}^f(X, d)$, find a $t \in \mathbb{R}$ with $d(x, f) = t + R\mathbb{Z}$.

- In general, the DP is at least as hard as the DLP.

Applications of Infrastructures

- The group $\mathrm{Rep}^f(X, d)$ can be used for a cryptographic key exchange
  - or for digital signatures, or anything else which can be done with groups.

Applications of Infrastructures

- The group $\mathrm{Rep}^f(X, d)$ can be used for a cryptographic key exchange
  - or for digital signatures, or anything else which can be done with groups.
- In Computational Number Theory, one uses infrastructures to compute unit groups:
  - Assume that one has a global field[1] with two infinite places (infinite points, if you prefer curves).
  - Here, R is unknown and the regulator.
  - X is the set of principal reduced ideals.

[1] A finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(x)$.

Applications of Infrastructures

- The group $\mathrm{Rep}^f(X, d)$ can be used for a cryptographic key exchange
  - or for digital signatures, or anything else which can be done with groups.
- In Computational Number Theory, one uses infrastructures to compute unit groups:
  - Assume that one has a global field[1] with two infinite places (infinite points, if you prefer curves).
  - Here, R is unknown and the regulator.
  - X is the set of principal reduced ideals.
  - Daniel Shanks first used the infrastructure to compute the regulator in square root time.

[1] A finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(x)$.

Applications of Infrastructures

- The group $\mathrm{Rep}^f(X, d)$ can be used for a cryptographic key exchange
  - or for digital signatures, or anything else which can be done with groups.
- In Computational Number Theory, one uses infrastructures to compute unit groups:
  - Assume that one has a global field[1] with two infinite places (infinite points, if you prefer curves).
  - Here, R is unknown and the regulator.
  - X is the set of principal reduced ideals.
  - Daniel Shanks first used the infrastructure to compute the regulator in square root time.
  - Hendrik Lenstra later gave a description by embedding the infrastructure into a "circular group", similar to our $\mathrm{Rep}^f(X, d)$.

[1] A finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(x)$.

f-Representations, Part Three: More Dimensions

- How can f-representations be done in several dimensions?
- There is no longer an “obvious” way to write $t \in \mathbb{R}^n/\Lambda$ as $d(x) + f$ with $(x, f) \in X \times \mathbb{R}^n$.

f-Representations, Part Three: More Dimensions

- How can f-representations be done in several dimensions?
- There is no longer an “obvious” way to write $t \in \mathbb{R}^n/\Lambda$ as $d(x) + f$ with $(x, f) \in X \times \mathbb{R}^n$.
- An equivalent formulation: for $t \in \mathbb{R}^n/\Lambda$ we want to find some $x \in X$ with $d(x)$ “near to” t.
  - Such a map $\mathbb{R}^n/\Lambda \to X$ is called reduction map.

f-Representations, Part Three: More Dimensions

- How can f-representations be done in several dimensions?
- There is no longer an "obvious" way to write $t \in \mathbb{R}^n/\Lambda$ as $d(x) + f$ with $(x, f) \in X \times \mathbb{R}^n$.
- An equivalent formulation: for $t \in \mathbb{R}^n/\Lambda$ we want to find some $x \in X$ with $d(x)$ "near to" t.
    - Such a map $\mathbb{R}^n/\Lambda \to X$ is called reduction map.
- Note that f-representations give a giant step: if

$$(x, 0) + (x', 0) = (x'', f) \in \mathrm{Rep}^f(X, d),$$

then we can define $gs(x, x') := x''$.

Reduction Maps

- Solution: add a reduction map *red* $: \mathbb{R}^n/\Lambda \to X$ to the definition!

Definition

An *n-dimensional infrastructure* is:

- A finite set $X \neq \emptyset$, a lattice $\Lambda \subseteq \mathbb{R}^n$
- An injective map $d : X \to \mathbb{R}^n/\Lambda$

Reduction Maps

- Solution: add a reduction map $red : \mathbb{R}^n/\Lambda \to X$ to the definition!
  - We then get giant steps and f-representations for free!

Definition

An *n-dimensional infrastructure* is:

- A finite set $X \neq \emptyset$, a lattice $\Lambda \subseteq \mathbb{R}^n$
- An injective map $d : X \to \mathbb{R}^n/\Lambda$
- A map $red : \mathbb{R}^n/\Lambda \to X$ with $red \circ d = id_X$

Reduction Maps

- Solution: add a reduction map $red : \mathbb{R}^n/\Lambda \to X$ to the definition!
  - We then get giant steps and f-representations for free!
  - This looks a bit like cheating, doesn't it?

Definition

An *n-dimensional infrastructure* is:

- A finite set $X \neq \emptyset$, a lattice $\Lambda \subseteq \mathbb{R}^n$
- An injective map $d : X \to \mathbb{R}^n/\Lambda$
- A map $red : \mathbb{R}^n/\Lambda \to X$ with $red \circ d = id_X$

Reduction Maps

- Solution: add a reduction map $red : \mathbb{R}^n/\Lambda \to X$ to the definition!
  - We then get giant steps and f-representations for free!
  - This looks a bit like cheating, doesn't it?
- We have to find a concrete instance of such a map in the interesting cases.
  - We are interested in infrastructures obtained from global fields.

Definition

An *n-dimensional infrastructure* is:

- A finite set $X \neq \emptyset$, a lattice $\Lambda \subseteq \mathbb{R}^n$
- An injective map $d : X \to \mathbb{R}^n/\Lambda$
- A map $red : \mathbb{R}^n/\Lambda \to X$ with $red \circ d = id_X$

Overview

Number-Geometric Interpretation

- Assume we have a global field K:
  - either a number field
  - or a function field over $\mathbb{F}_q$.

Number-Geometric Interpretation

- Assume we have a global field K:
  - either a number field
  - or a function field over $\mathbb{F}_q$.
- Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{n+1}\}$ be the set of infinite places (points).

Number-Geometric Interpretation

- Assume we have a global field K:
  - either a number field
  - or a function field over $\mathbb{F}_q$.
- Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{n+1}\}$ be the set of infinite places (points).
- Consider

$$\Psi : K^* \to \mathbb{R}^n, \qquad f \mapsto (-\nu_{\mathfrak{p}_1}(f), \dots, -\nu_{\mathfrak{p}_n}(f)).$$

Number-Geometric Interpretation

- Assume we have a global field K:
  - either a number field
  - or a function field over $\mathbb{F}_q$.
- Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{n+1}\}$ be the set of infinite places (points).
- Consider

$$\Psi : K^* \to \mathbb{R}^n, \qquad f \mapsto (-\nu_{\mathfrak{p}_1}(f), \dots, -\nu_{\mathfrak{p}_n}(f)).$$

- Consider the ring of integers $\mathcal{O}$,

$$\mathcal{O} = \{f \in K \mid \nu_{\mathfrak{p}}(f) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Number-Geometric Interpretation

- Assume we have a global field K:
  - either a number field
  - or a function field over $\mathbb{F}_q$.
- Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{n+1}\}$ be the set of infinite places (points).
- Consider

$$\Psi : K^* \to \mathbb{R}^n, \qquad f \mapsto (-\nu_{\mathfrak{p}_1}(f), \dots, -\nu_{\mathfrak{p}_n}(f)).$$

- Consider the ring of integers $\mathcal{O}$,

$$\mathcal{O} = \{f \in K \mid \nu_{\mathfrak{p}}(f) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

- Then $\Lambda := \Psi(\mathcal{O}^*)$ is a lattice in $\mathbb{R}^n$.

Reduced Divisors

- We now assume for simplicity that $\deg \mathfrak{p}_{n+1} = 1$.
  - K number field: means that $\mathfrak{p}_{n+1}$ corresponds to a real embedding.

Reduced Divisors

- We now assume for simplicity that $\deg \mathfrak{p}_{n+1} = 1$.
  - K number field: means that $\mathfrak{p}_{n+1}$ corresponds to a real embedding.

Definition

A divisor D is said to be reduced if

- $D \geq 0$ and the support of D lies outside S;
- $L(D) = \{f \in K \mid (f) \geq -D\} = k$.
  - Here, $k = \mu(K) \cup \{0\}$ (roots of unity and 0) or $k = \mathbb{F}_q$.

Reduced Divisors

- We now assume for simplicity that $\deg \mathfrak{p}_{n+1} = 1$.
  - K number field: means that $\mathfrak{p}_{n+1}$ corresponds to a real embedding.

Definition

A divisor D is said to be reduced if

- $D \geq 0$ and the support of D lies outside S;
- $L(D) = \{f \in K \mid (f) \geq -D\} = k$.
  - Here, $k = \mu(K) \cup \{0\}$ (roots of unity and 0) or $k = \mathbb{F}_q$.

- Then one has finitely many reduced divisors.
- Take those as X whose finite part equals the finite part of a principal divisor.
  - If $D = -(\mu)_{finite}$, define $\Psi(D) = \Psi(\mu) + \Lambda$.
  - This gives an injective map $\Psi : X \to \mathbb{R}^n/\Lambda$.

Reduced Divisors and the Reduction Map

- For $t = (t_1, \dots, t_n) \in \mathbb{R}^n$:

Reduced Divisors and the Reduction Map

- For $t = (t_1, \dots, t_n) \in \mathbb{R}^n$:
  - One can effectively find some $\mu \in \mathcal{O} \setminus \{0\}$ such that
    - $D = -(\mu)_{finite}$ (finite part of divisor) is reduced, and
    - $f = t - \Psi(D) = t - \Psi(\mu) \in \mathbb{R}^n_{\geq 0}$, and
    - we have that f is of size $O(g)$.

Reduced Divisors and the Reduction Map

- For $t = (t_1, \dots, t_n) \in \mathbb{R}^n$:
  - One can effectively find some $\mu \in \mathcal{O} \setminus \{0\}$ such that
    - $D = -(\mu)_{finite}$ (finite part of divisor) is reduced, and
    - $f = t - \Psi(D) = t - \Psi(\mu) \in \mathbb{R}^n_{\geq 0}$, and
    - we have that f is of size $O(g)$.
  - Here, g is the genus of K;
    - for number fields, g is of size $\log \sqrt{|D|}$.

Reduced Divisors and the Reduction Map

- For $t = (t_1, \dots, t_n) \in \mathbb{R}^n$:
  - One can effectively find some $\mu \in \mathcal{O} \setminus \{0\}$ such that
    - $D = -(\mu)_{finite}$ (finite part of divisor) is reduced, and
    - $f = t - \Psi(D) = t - \Psi(\mu) \in \mathbb{R}^n_{\geq 0}$, and
    - we have that f is of size $O(g)$.
  - Here, g is the genus of K;
    - for number fields, g is of size $\log \sqrt{|D|}$.
- Denote this map $t + \Lambda \mapsto D$ by *red*; this is a reduction map!

Overview

Infrastructure

- This allows to define

$$\mathrm{Rep}^f(X, \Psi) := \{(D, f) \mid red(\Psi(D) + f) = D\}.$$

This gives a bijection

$$\Psi : \mathrm{Rep}^f(X, \Psi) \to \mathbb{R}^n/\Lambda, \qquad (D, f) \mapsto \Psi(D) + f$$

whose inverse is the map $t + \Lambda \mapsto (D, f)$ from above.

Infrastructure

- This allows to define

$$\mathrm{Rep}^f(X, \Psi) := \{(D, f) \mid red(\Psi(D) + f) = D\}.$$

This gives a bijection

$$\Psi : \mathrm{Rep}^f(X, \Psi) \to \mathbb{R}^n/\Lambda, \qquad (D, f) \mapsto \Psi(D) + f$$

whose inverse is the map $t + \Lambda \mapsto (D, f)$ from above.

- One can pull the addition of $\mathbb{R}^n/\Lambda$ over to $\mathrm{Rep}^f(X, \Psi)$ using this bijection.
  - One can describe this induced operation on $\mathrm{Rep}^f(X, \Psi)$ without using the map Ψ.
  - This allows effective computation of this group operation without the need to evaluate Ψ or Ψ^{-1}.

Relation to the Divisor Class Group

- The map
$$\Phi : \mathrm{Rep}^f(X, \Psi) \to \mathrm{Pic}^0(K),$$
$$(D, f) \mapsto D + \sum_{i=1}^{n} f_i \mathfrak{p}_i - (\dots)\, \mathfrak{p}_{n+1}$$
is injective.
  - Function fields: only use elements of $\mathrm{Rep}^f(X, \Psi)$ whose f-part has integer coefficients.

Relation to the Divisor Class Group

- The map
$$\Phi : \mathrm{Rep}^f(X, \Psi) \to \mathrm{Pic}^0(K),$$
$$(D, f) \mapsto D + \sum_{i=1}^{n} f_i \mathfrak{p}_i - (\dots)\, \mathfrak{p}_{n+1}$$
is injective.
  - Function fields: only use elements of $\mathrm{Rep}^f(X, \Psi)$ whose f-part has integer coefficients.
- Its image is the set of divisor classes of linear combinations of
$$\mathfrak{p}_1 - \mathfrak{p}_{n+1} \deg \mathfrak{p}_1, \qquad \dots, \qquad \mathfrak{p}_n - \mathfrak{p}_{n+1} \deg \mathfrak{p}_n.$$

Relation to the Divisor Class Group

- The map
$$\Phi : \mathrm{Rep}^f(X, \Psi) \to \mathrm{Pic}^0(K),$$
$$(D, f) \mapsto D + \sum_{i=1}^{n} f_i \mathfrak{p}_i - (\dots)\, \mathfrak{p}_{n+1}$$
is injective.
  - Function fields: only use elements of $\mathrm{Rep}^f(X, \Psi)$ whose f-part has integer coefficients.
- Its image is the set of divisor classes of linear combinations of
$$\mathfrak{p}_1 - \mathfrak{p}_{n+1} \deg \mathfrak{p}_1, \qquad \dots, \qquad \mathfrak{p}_n - \mathfrak{p}_{n+1} \deg \mathfrak{p}_n.$$
- If combined with the bijection $\mathrm{Rep}^f(X, \Psi) \to \mathbb{R}^n/\Lambda$, one obtains a group isomorphism
$$\mathbb{R}^n/\Lambda \to \mathrm{img}(\Phi) \quad \text{resp.} \quad \mathbb{Z}^n/\Lambda \to \mathrm{img}(\Phi) \subseteq \mathrm{Pic}^0(K).$$

Overview

Conclusion

- Infrastructures can be seen as a generalization of abelian groups.
- We can obtain n-dimensional infrastructures from global fields, together with a reduction map.
- The obtained f-representations allow effective arithmetic in the infrastructure.
- The infrastructure can be seen as lying in the divisor class group;
  - by considering all reduced divisors and another formulation of the definition of $\mathrm{Rep}^f(X, \Psi)$, one obtains the whole divisor class group!
- The currently known algorithms for solving the DLP in $\mathrm{Pic}^0(K)$ also solve the Distance Problem in the infrastructure.

Research Problems

- Find more efficient algorithms to compute in the infrastructure.
  - Current ones are very general methods and *very slow*.
  - This question is related to finding efficient arithmetic in $\mathrm{Pic}^0(K)$.
- Find good generalization of baby steps.
  - In particular, in context of "abstract" n-dimensional infrastructures.
- Find more information on the distribution of reduced divisors in the function field case.
- How hard is computing Ψ, i.e. how hard is the Distance Problem?

Thank you
for your patience!