Hecke continued fractions and orders in relative quadratic extensions

Ayberk Zeytin, Université Galatasaray
Journées Arithmétiques 2023

Outline

1. (Hecke) continued fractions
2. Picard group of a number field
3. Çarks and the Picard Group

(Hecke) continued fractions

Some notation

The following elements generate $\mathrm{PSL}(2,\mathbb{Z})$:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } L_3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \text{ so that } L_3S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and induce the isomorphism : $\mathrm{PSL}(2,\mathbf{Z}) \cong (\mathbf{Z}/2\mathbf{Z}) * (\mathbf{Z}/3\mathbf{Z})$

The element

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is not an element of $\mathrm{PSL}(2,\mathbb{Z})$, but satisfies : $U(L_3S)U = L_3^2S$.

(Hecke) continued fractions

The Möbius action

The group PSL(2,**R**) acts on the upper half plane :

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot z \mapsto \frac{pz+q}{rz+s}$$

This action can be extended to the boundary $\mathbf{R} \cup \{\infty\}$.

We have :

$$U \cdot z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot z = \frac{1}{z}, \quad (LS)^n \cdot z = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot z = z + n$$

(Hecke) continued fractions

Continued fractions as words in U, L and S

A standard continued fraction can be interpreted as :

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}};\ \text{with } a_0 \in \mathbf{Z}, a_1, a_2, \ldots \in \mathbf{Z}_+$$

$$= (LS)^{a_0}\left(\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}\right)$$

$$= (L_3S)^{a_0}U\left(a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}\right)$$

$$= (L_3S)^{a_0}U(L_3S)^{a_1}U(L_3S)^{a_2}U\ldots$$

(Hecke) continued fractions

Continued fractions as words in L and S

The identity $U(L_3S)U = L_3^2S$ further gives : $U(L_3S)^nU = (L_3^2S)^n$. So :

$$[a_0; a_1, a_2, \ldots] = \Big((L_3S)^{a_0}\big(U(L_3S)^{a_1}U\big)\Big)(L_3S)^{a_2}U\ldots$$

$$= \big((L_3S)^{a_0}(L_3^2S)^{a_1}\big)\,\big((L_3S)^{a_2}(L_3^2S)^{a_3}\big)\ldots$$

Conclusion: to every continued fraction corresponds a word in S, L_3(and L_3^2).

(Hecke) continued fractions

Continued fractions as elements of a *completion*

Each infinite continued fraction is identified with the corresponding infinite word in S, L and L^2 (or corresponding infinite path on bipartite Farey tree starting at I).

Each finite continued fraction is identified with the following infinite word on bipartite Farey tree starting at I :

$$(LS)^{n_0}\cdots(LS)^{n_{k+1}}(L^2S)^\infty \text{ and } (LS)^{n_0}\cdots(LS)^{n_k}(L^2S)(LS)^\infty, \qquad (k \text{ even})$$

$$(LS)^{n_0}\cdots(L^2S)^{n_{k+1}}(LS)^\infty \text{ and } (LS)^{n_0}\cdots(L^2S)^{n_k}(LS)(L^2S)^\infty, \qquad (k \text{ odd})$$

(Hecke) continued fractions

Generalization

For any integer $q \geq 3$, the Hecke group H_q is generated by :
$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\tau_q = \begin{pmatrix} \lambda_q & -1 \\ 1 & 0 \end{pmatrix}$; where $\lambda_q = \cos(\pi/q) \in \mathbf{R}$. For $q = 3$ we recover PSL(2,$\mathbf{Z}$).

The above choice induces the isomorphism $H_q \cong \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/q\mathbf{Z}$.

The corresponding continued fractions algorithm can be described explicitly as :

0. [input] a real number x, an integer $q > 2$. Set **word** to be the empty word,
1. [preliminary computations] Set $\texttt{ver} = (\texttt{ver}_1, \ldots, \texttt{ver}_{q-1})$ to be the set of finite vertices of P_q and $\texttt{int} = (\texttt{int}_1, \ldots, \texttt{int}_q)$ to be the list of intervals determined by the vertices of P_q.
2. [check] if $x = \texttt{ver}_i$, then set $\texttt{word} = L_q^{q-i}S$ and terminate the algorithm. We get $x = L_q^{q-i+1}S(0)$.
3. [Euclidean step] if $x \in \texttt{int}_i$, then concatenate $L_q^{q-i+1}S$ to **word**, and set $x = SL_q^{i-1}(x)$, $P_q = (L_q^{q-i+1}S)(P_q)$ and update **ver** and **int**.
4. [Finished?] if $x = 0$, return **word**, else go to the Euclidean step.

(Hecke) continued fractions

Example

The output the algorithm is then a sequence of words in $L_q, L_q^2, \ldots, L_q^{q-1}$ and S

$$\begin{aligned}[0,1,12,1,1,1,2,1,5,1,15,1,2] &= \frac{46333}{50000} \\ &= (L_5^3 S)(L_5 S)^2 (L_5^3 S)(L_5 S)^3 (L_5 S)^5\end{aligned}$$

Of course, the matrix obtained from this argument is different :

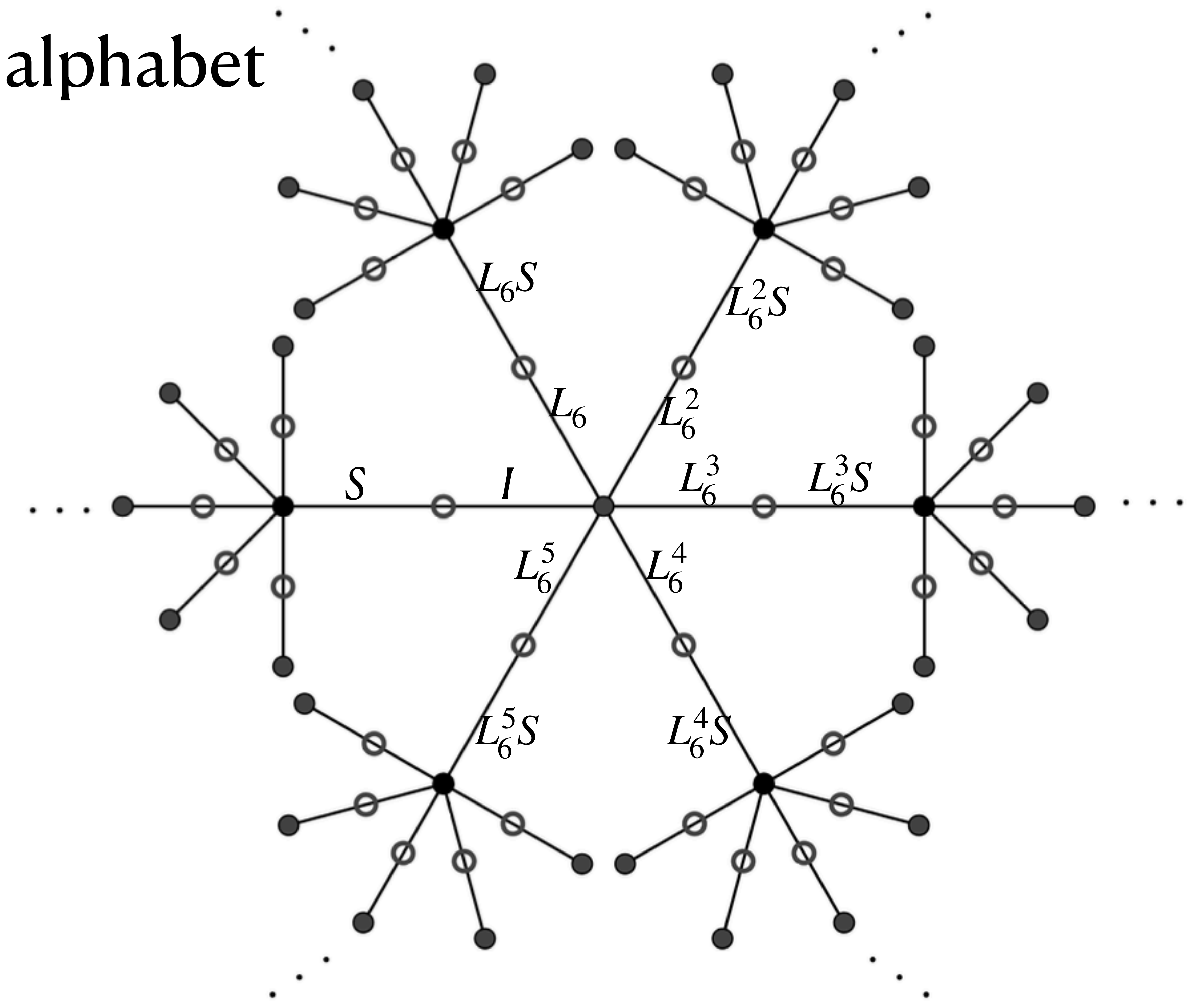
$$\begin{pmatrix} 6+3\sqrt{5} & 89+39\sqrt{5} \\ 7+3\sqrt{5} & 94+43\sqrt{5} \end{pmatrix}$$

(Hecke) continued fractions

Generalization

As in the previous case, we may identify such continued fractions with infinite words in $L_q, L_q^2, \ldots, L_q^{q-1}$ and S (or infinite paths on the corresponding Farey tree, denoted $\mathcal{F}_q$).

and conversely, infinite words in this alphabet determine a unique real number.



The case $q = 6$

Picard group of a number field

Some notation

A number field K is a finite extension of $\mathbf{Q}$.

Let $Id(K)$denote the multiplicative group of fractional ideals of K.

Given a number field K of degree n, there are $n = r + 2s$ distinct embeddings of K into $\mathbf{C}$. The first r of these are called real embeddings as their image lie in $\mathbf{R} \subset \mathbf{C}$, and the next $2s$ of these are called complex embeddings. An embedding σ of K is identified with its complex conjugate $\overline{\sigma}$ (an equivalence relation). There are $r + s$ many such classes.

We associate the étale algebra $K_{\mathbf{R}} := K \otimes_{\mathbf{Q}} \mathbf{R}$ to the number field K. In $K_{\mathbf{R}}$ addition and multiplication are usual componentwise addition and multiplication. As a vector space over $\mathbf{R}$, $K_{\mathbf{R}}$ is isomorphic to $\mathbf{R}^r \times \mathbf{C}^s$.

The unit group of $K_{\mathbf{R}}$ is $K_{\mathbf{R}}^{\times} = \prod_{i=1}^{r} \mathbf{R}^{\times} \times \prod_{i=1}^{s} \mathbf{C}^{\times}$.

Picard group of a number field

The divisor class group

The norm map is defined as :

$$N : Id(K) \times K_{\mathbb{R}}^{\times} \to \mathbf{R}^{\times}$$

$$(I, (u_1, \ldots, u_{r+s})) \mapsto [\mathbf{Z}_K : I] \cdot \prod_{i=1}^{r} u_i \cdot \prod_{i=r+1}^{r+s} |u_i|^2$$

The number field K can be embedded into $K_{\mathbf{R}}$ (by sending each $x \in K$ to $(\sigma_1(x), \ldots, \sigma_{r+s}(x))$ and into $Id(K)$ (by sending each $x \in K$ to the fractional ideal generated by x^{-1}) :

$$K \to Id(K) \times K_{\mathbf{R}}$$

The kernel of the norm map (denoted $Div^0(K)$) contains the image of K and the cokernel of this map is defined as the **Picard group** of K, $Pic^0(K)$.

Picard group of a number field

Structure of the Picard group

Theorem(Schoof, 2008) :

$$Pic^0(K) \cong T^0 \times Cl^+(K)$$

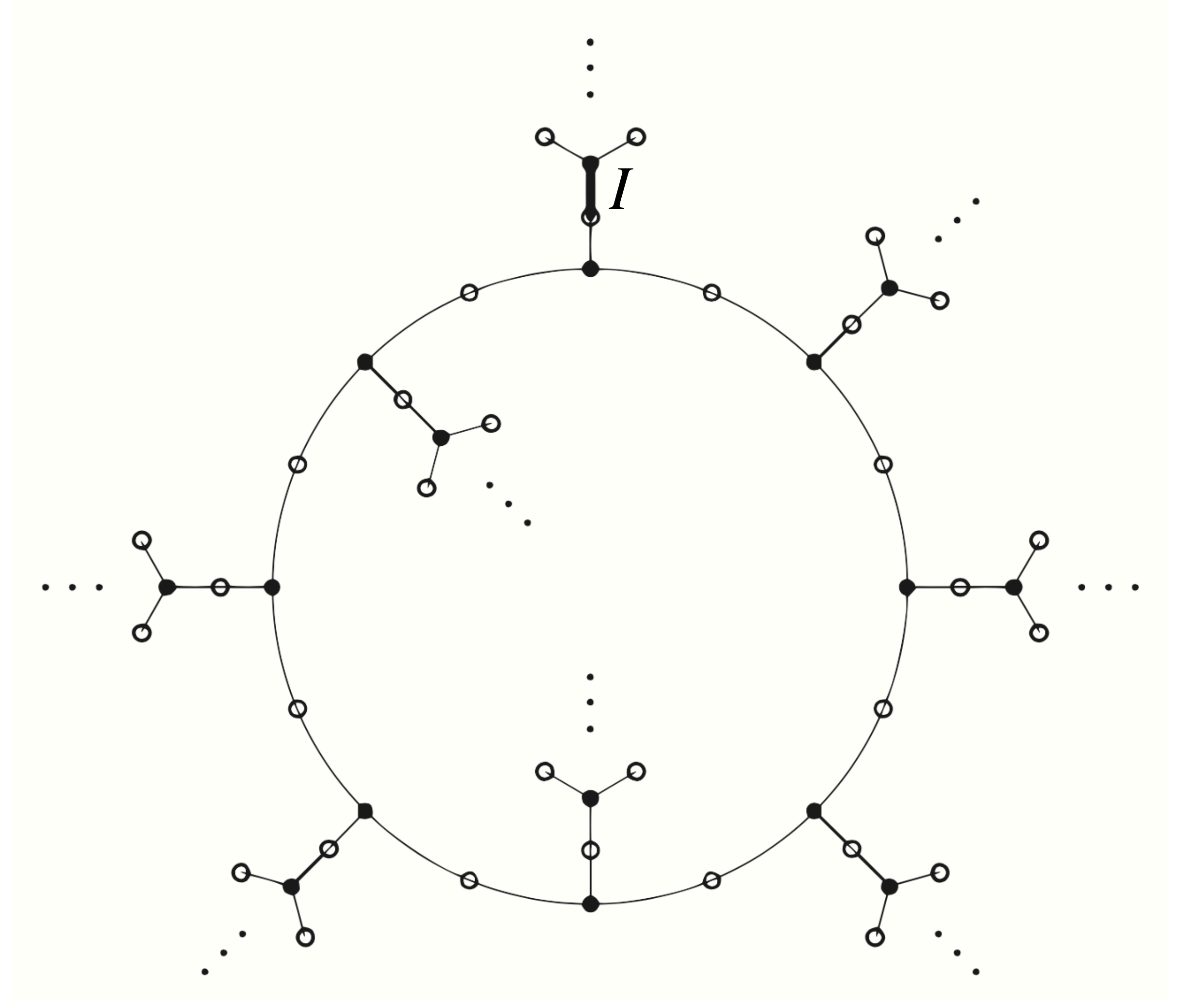
where T^0 is a torus of dimension $n - 1$ and $Cl^+(K)$ is the narrow class group of K. In fact, T^0 is isomorphic to $H/\mathbf{Z}_{K,+}^\times$, where H is a hyperplane in $K_\mathbf{R}$.

Çarks and the Picard Group

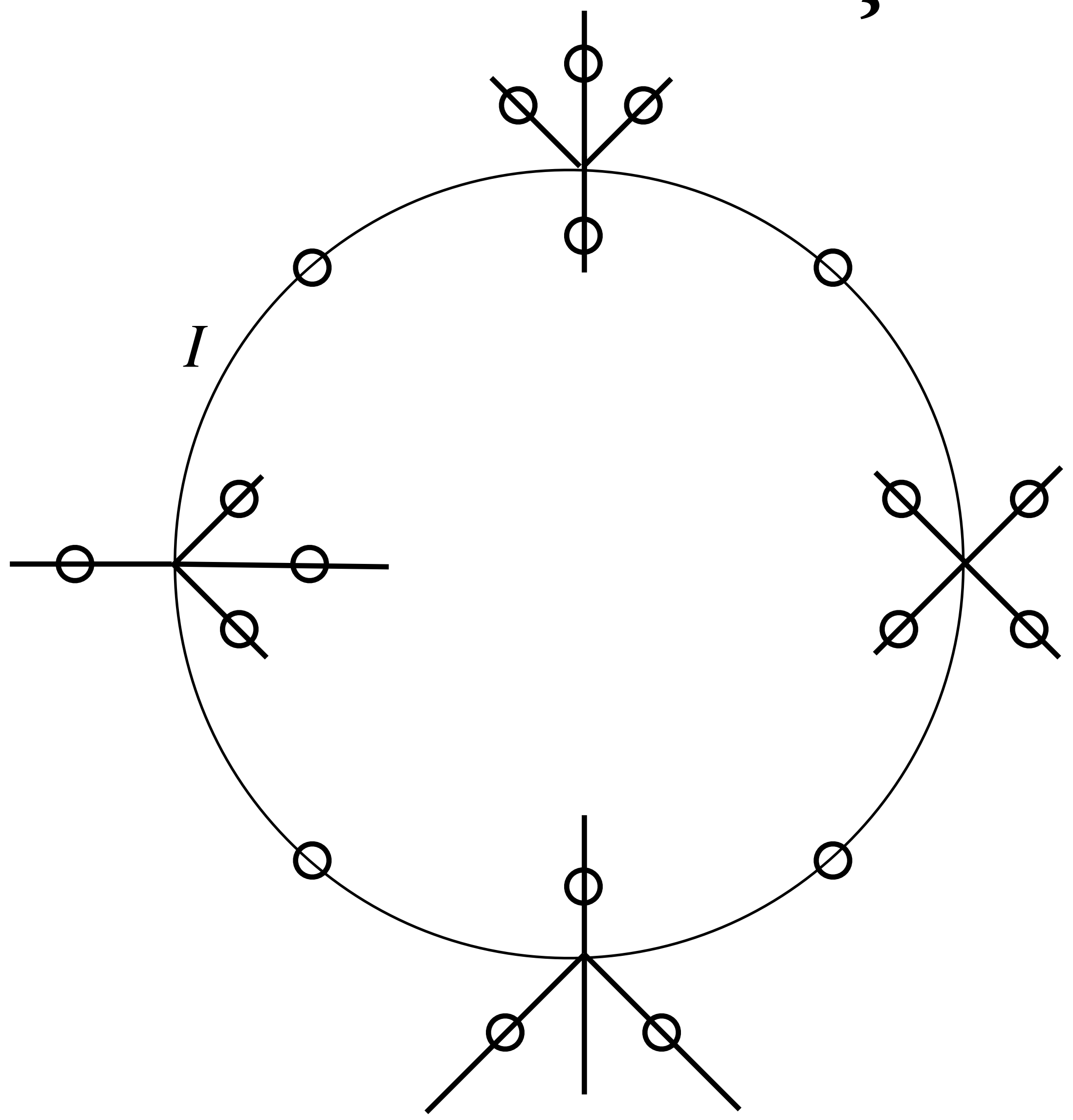
Periodic words, çarks

The periodic words correspond to subgroups generated by one element, say W (assumed to be primitive).

The quotient $\mathcal{F}_q/\langle W \rangle$ is called a **çark.** Its **spine** determines the çark.



$W = S\,[(L_3^2S)^2(L_3S)^2(L_3^2S)(L_3S)^3L_3^2]\,S$ (here $q = 3$)

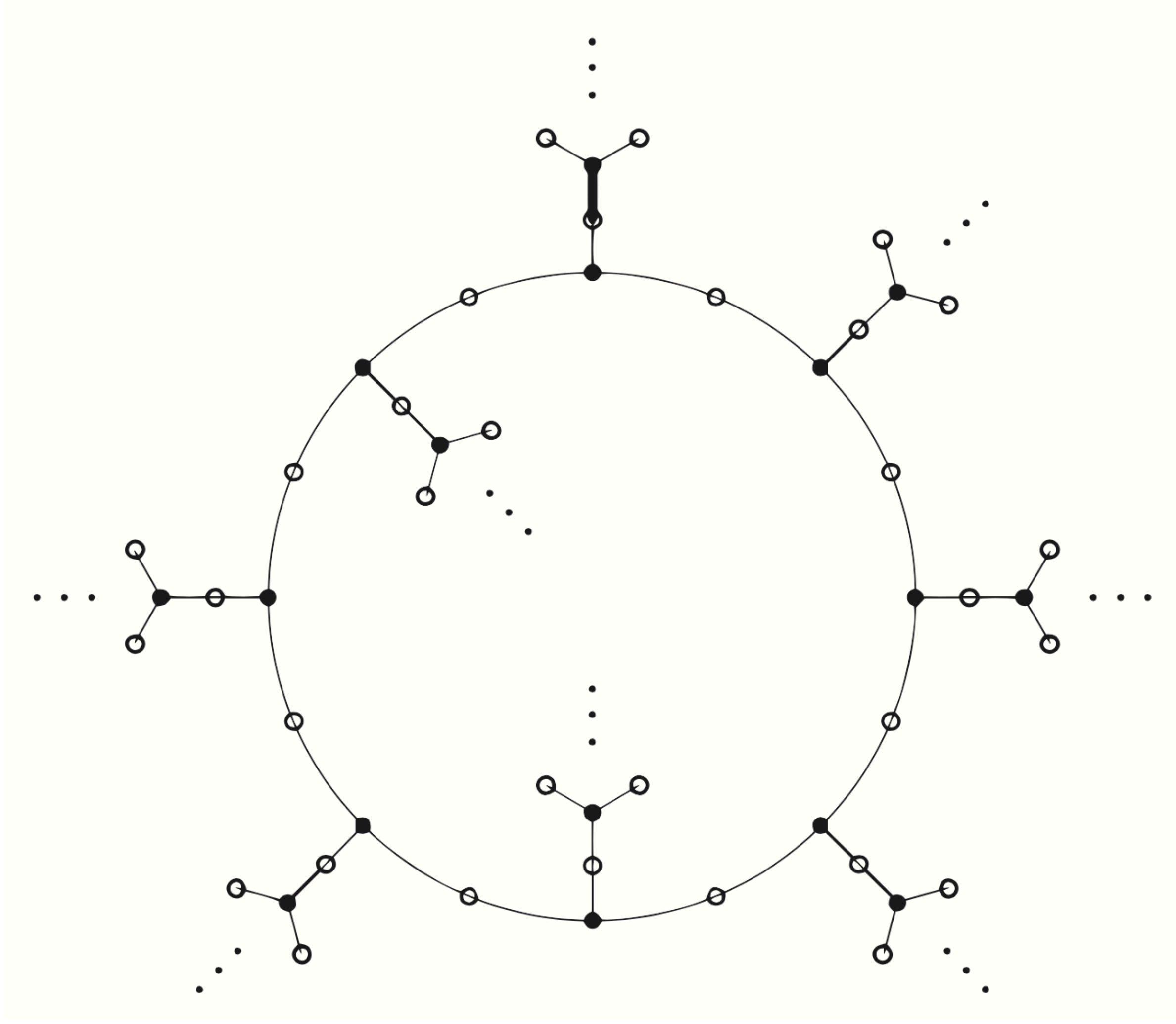


$W = S\,[(L_6^4S)(L_6^2S)(L_6^3S)(L_6^2S)$ (here $q = 6$)

Çarks and the Picard Group

Faces of çarks

A face of a çark determined by $\mathscr{F}_q/\langle W\rangle$ is defined as a bi-infinite left (or right) turn path on $\mathscr{F}_q/\langle W\rangle$.



$W = S\,[(L_3^2S)^2(L_3S)^2(L_3^2S)(L_3S)^3L_3^2]\,S$

A face of a çark $\mathscr{F}_q/\langle W\rangle$ is determined by its **root**. Notice : if the face is spinal, then it has more than one root, otherwise it has a unique root.

Çarks and the Picard Group

The case $q = 3$

Theorem (Çaktı, Z.)

Let $q = 3$. Given a çark (i.e. a primitive periodic word in L_3, L_3^2 and S), there is a real quadratic number field $K = \mathbf{Q}(\sqrt{\Delta})$ and a map, denoted ι, from the set of edges of the çark to the Picard group of K so that

1. if the çark does not have any symmetry, then ι is injective
2. if the çark does have symmetry, then ι is never injective.

Çarks and the Picard Group

The case $q = 3$

Theorem (Z.)

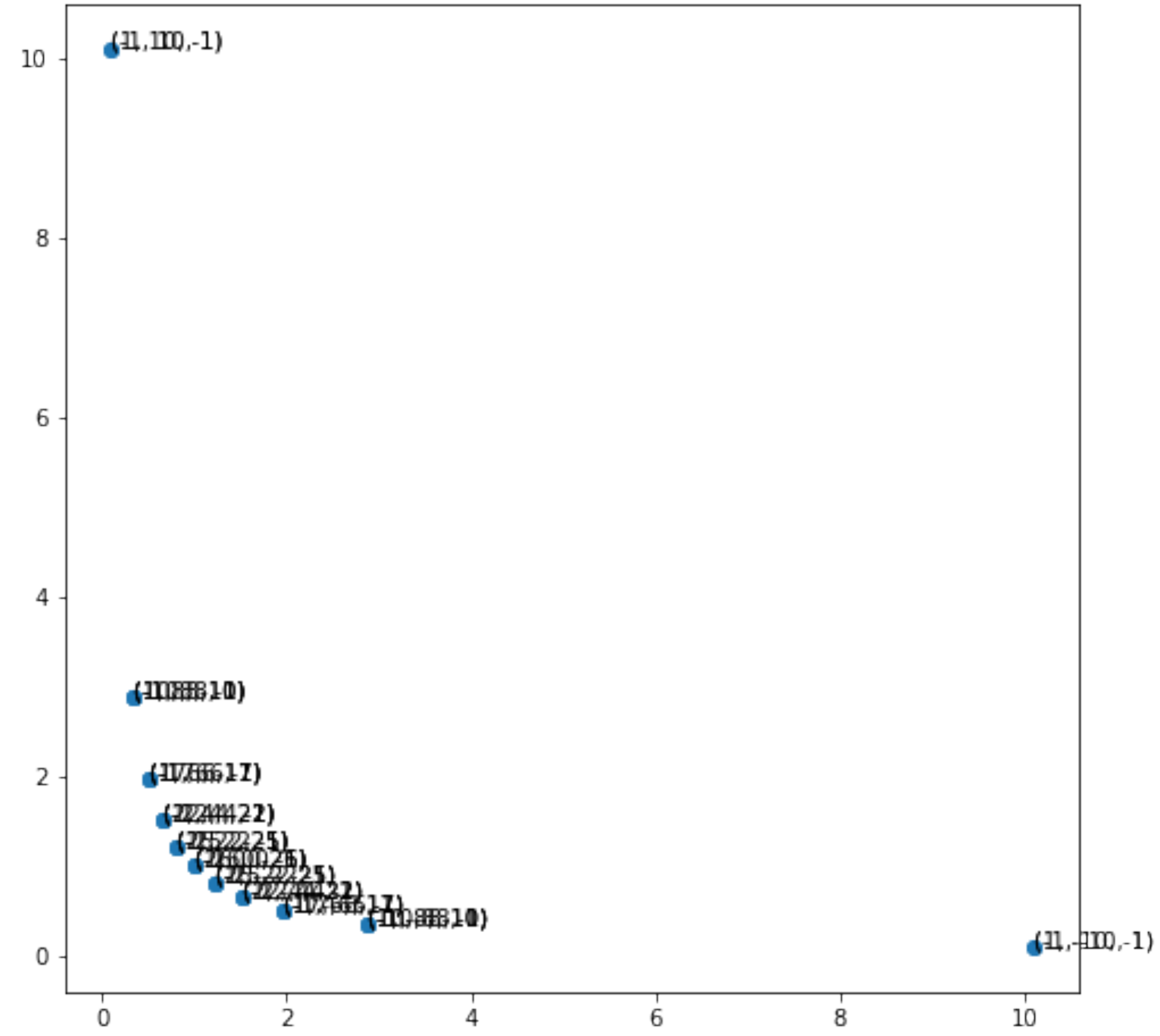
Let $q > 3$ be a prime number. Given a çark (i.e. a primitive periodic word in $L_q, \ldots L_q^{q-1}$ and S), there is a relative quadratic extension of the real cyclotomic number field $K = \mathbf{Q}(\zeta_q + \overline{\zeta_q}, \sqrt{\Delta})$ and a map, denoted ι, from the set of edges of the çark to the Picard group of K so that

1. if the çark does not have any symmetry, then ι is injective
2. if the çark does have symmetry, then ι is never injective.

Çarks and the Picard Group

The case $q = 3$

When $q = 3$, the Picard group of $K = \mathbf{Q}(\sqrt{\Delta})$ becomes a bunch of circles.



The case $\mathbf{Q}(\sqrt{51})$ where $W = (L_3^2 S)^{10}(L_3 S)^{10}$

Thank you!