Manin symbols over number fields

Maite Aranés
University of Warwick

Sage Days 16

Introduction

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

- for some real quadratic fields,
- for some imaginary quadratic fields with small class number.

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

- Over $\mathbb{Q}$: begin with tessellation of $\mathcal{H}^* = \mathcal{H} \cup \{\infty\}$ on which $PSL(2, \mathbb{Z})$ acts.

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

> Over K imaginary quadratic field: begin with tessellation of extended hyperbolic 3-space $\mathcal{H}_3^*$ on which $GL(2, R)$ acts (where $\mathcal{H}_3 = \mathbb{C} \times \mathbb{R}_+ = \{(z, t) | z, t \in \mathbb{C}, t \geq 0\}$).

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

Over K: begin with tessellation of certain completed upper half space on which $GL(2, R)$ acts.

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

Over K: begin with tessellation of certain completed upper half space on which $GL(2, R)$ acts.

- vertices of the tessellation (cusps)
- edges of the tessellation, which consist of certain geodesic paths between cusps (Manin symbols)

Introduction

Let K be a number field, R its ring of integers.

For some classes of fields, spaces of cusp forms of weight 2 for $GL(2, K)$ have been computed using modular symbols.

Modular symbols method: duality between homology and the space of cusp forms.

Computing homology:

Over K: begin with tessellation of certain completed upper half space on which $GL(2, R)$ acts.

vertices of the tessellation (cusps)

edges of the tessellation, which consist of certain geodesic paths between cusps (Manin symbols)

The geometry is different for each number field but the theory for cusps and Manin symbols applies to all number fields.

Overview

Cusps and Manin symbols over $\mathbb{Q}$

- Cusps over $\mathbb{Q}$
- $\mathbf{\Gamma}$- equivalence of rational cusps
- Manin symbols and $\mathbf{\Gamma_0(N)}$ - equivalence
- Number of $\mathbf{\Gamma_0(N)}$- equivalence classes of cusps

Cusps and Manin symbols over number fields

- Cusps over a number field
- $(\mathfrak{a}, \mathfrak{b})$-matrices
- Cusp equivalence under $\mathbf{\Gamma}$
- Cusp equivalence under $\mathbf{\Gamma_0(\mathfrak{n})}$
- Manin symbols over number fields
- Number of $\mathbf{\Gamma_0(\mathfrak{n})}$- equivalence classes of cusps

Cusps and Manin symbols over $\mathbb{Q}$

Cusps over $\mathbb{Q}$

Cusps over $\mathbb{Q}$

By a *cusp* of $\mathbb{Q}$ we mean an element of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

Cusps over $\mathbb{Q}$

By a *cusp* of $\mathbb{Q}$ we mean an element of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

Each cusp $\alpha \in \mathbb{P}^1(\mathbb{Q})$ may be represented as $\alpha = p/q$, with $\gcd(p, q) = 1$. This representation is unique up to multiplication of p and q by -1.

Cusps over $\mathbb{Q}$

By a *cusp* of $\mathbb{Q}$ we mean an element of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

Each cusp $\alpha \in \mathbb{P}^1(\mathbb{Q})$ may be represented as $\alpha = p/q$, with $\gcd(p, q) = 1$. This representation is unique up to multiplication of p and q by -1.

The groups $\Gamma = PSL(2, \mathbb{Z})$ and $\Gamma_0(N)$, defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \; c \equiv 0 \pmod{N} \right\}$$

for a positive integer N, act on the set of cusps by linear fractional transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\frac{p}{q} \right) = \frac{ap + bq}{cp + dq}, \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Γ- equivalence of rational cusps

Γ- equivalence of rational cusps

All cusps over $\mathbb{Q}$ are Γ- equivalent.

Γ- equivalence of rational cusps

All cusps over $\mathbb{Q}$ are Γ- equivalent.

Let α be a cusp of $\mathbb{Q}$ with representative p/q. There exist $r, s \in \mathbb{Z}$ such that $ps - qr = 1$ and we can then complete the column vector $\binom{p}{q}$ to a matrix $M_\alpha = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$ in Γ, and $M_\alpha \cdot \infty = p/q$.

In particular, given $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{Q})$ we have that $\left(M_{\alpha_2} M_{\alpha_1}^{-1}\right) \alpha_1 = \alpha_2$.

Γ- equivalence of rational cusps

All cusps over $\mathbb{Q}$ are Γ- equivalent.

Let α be a cusp of $\mathbb{Q}$ with representative p/q. There exist $r, s \in \mathbb{Z}$ such that $ps - qr = 1$ and we can then complete the column vector $\left(\begin{smallmatrix} p \\ q \end{smallmatrix}\right)$ to a matrix $M_\alpha = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$ in Γ, and $M_\alpha \cdot \infty = p/q$.

In particular, given $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{Q})$ we have that $\left(M_{\alpha_2} M_{\alpha_1}^{-1}\right) \alpha_1 = \alpha_2$.

NOTE: We may regard the column vector $\left(\begin{smallmatrix} p \\ q \end{smallmatrix}\right)$ as the first column of a matrix in Γ, and study the action of Γ and its subgroups on $\mathbb{P}^1(\mathbb{Q})$ via its action by left multiplication on Γ itself.

Manin symbols and $\Gamma_0(N)$ - equivalence

Manin symbols and $\Gamma_0(N)$ - equivalence

Right coset representatives for $\Gamma_0(N)$ in Γ:

PROPOSITION: *For* $j = 1, 2$ *let* $M_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \in \Gamma$. *The following are equivalent:*

1. *The right cosets* $\Gamma_0(N)M_1$ *and* $\Gamma_0(N)M_2$ *are equal.*
2. $c_1 d_2 \equiv c_2 d_1 \pmod{N}$.
3. $c_1 \equiv u c_2$ *and* $d_1 \equiv u d_2 \pmod{N}$, *with* $\gcd(u, N) = 1$.

Manin symbols and $\Gamma_0(N)$ - equivalence

Right coset representatives for $\Gamma_0(N)$ in Γ:

PROPOSITION: *For* $j = 1, 2$ *let* $M_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \in \Gamma$*. The following are equivalent:*

1. *The right cosets* $\Gamma_0(N)M_1$ *and* $\Gamma_0(N)M_2$ *are equal.*
2. $c_1 d_2 \equiv c_2 d_1 \pmod{N}$*.*
3. $c_1 \equiv u c_2$ *and* $d_1 \equiv u d_2 \pmod{N}$*, with* $\gcd(u, N) = 1$*.*

We define the *M-symbol* or *Manin symbol of level* N $(c : d)$ to be an equivalence class of a pair $(c, d) \in \mathbb{Z}^2$ such that $\gcd(c, d, N) = 1$, modulo the relation:

$$(c_1, d_1) \sim (c_2, d_2) \Longleftrightarrow c_1 d_2 \equiv c_2 d_1 \pmod{N}$$

The set of these M-symbols modulo N is $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

NOTE: Given an M-symbol $(c : d)$, the integers c and d are only determined modulo N, and we can always choose them such that $\gcd(c, d) = 1$.

NOTE: Given an M-symbol $(c:d)$, the integers c and d are only determined modulo N, and we can always choose them such that $\gcd(c,d)=1$.

There is a bijection:

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) & \longleftrightarrow & [\Gamma:\Gamma_0(N)] \\ (c:d) & \leftrightarrow & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{array}$$

where $a,b\in\mathbb{Z}$ are such that $ad-bc=1$.

NOTE: Given an M-symbol $(c : d)$, the integers c and d are only determined modulo N, and we can always choose them such that $\gcd(c, d) = 1$.

There is a bijection:

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) & \longleftrightarrow & [\Gamma : \Gamma_0(N)] \\ (c : d) & \leftrightarrow & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{array}$$

where $a, b \in \mathbb{Z}$ are such that $ad - bc = 1$.

The right coset action of Γ on $[\Gamma : \Gamma_0(N)]$ induces an action on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$:

$$(c : d) \begin{pmatrix} p & q \\ r & s \end{pmatrix} = (cp + dr : cq + ds)$$

To test $\Gamma_0(N)$- equivalence:

PROPOSITION: *Let α_1 and α_2 be cusps with representatives p_1/q_1 and p_2/q_2. The following are equivalent:*

1. $\alpha_2 = M(\alpha_1)$ *for some* $M \in \Gamma_0(N)$.
2. $q_2 \equiv uq_1 \pmod N$ *and* $up_2 \equiv p_1 \pmod{\gcd(q_1, N)}$, *with* $\gcd(u, N) = 1$.
3. $s_1q_2 \equiv s_2q_1 \pmod{\gcd(q_1q_2, N)}$, *where* s_j *satisfies* $p_js_j \equiv 1 \pmod{q_j}$.

To test $\boldsymbol{\Gamma_0(\mathrm{N})}$- equivalence:

PROPOSITION: *Let α_1 and α_2 be cusps with representatives p_1/q_1 and p_2/q_2. The following are equivalent:*

1. $\alpha_2 = M(\alpha_1)$ *for some* $M \in \Gamma_0(N)$.
2. $q_2 \equiv uq_1 \pmod N$ *and* $up_2 \equiv p_1 \pmod{\gcd(q_1, N)}$, *with* $\gcd(u, N) = 1$.
3. ***$\boldsymbol{s_1 q_2 \equiv s_2 q_1 \pmod{\gcd(q_1 q_2, N)}}$, where $\boldsymbol{s_j}$ satisfies $\boldsymbol{p_j s_j \equiv 1 \pmod{q_j}}$.***

Number of $\Gamma_0(\mathrm{N})$- equivalence classes of cusps

Number of $\Gamma_0(\mathrm{N})$- equivalence classes of cusps

Our only Γ- orbit of cusps splits into a finite union of $\Gamma_0(N)$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(N)\backslash\Gamma/\Gamma_\infty$, where Γ_∞ is the stabilizer of ∞.

Number of $\Gamma_0(\mathbf{N})$- equivalence classes of cusps

Our only Γ- orbit of cusps splits into a finite union of $\Gamma_0(N)$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(N)\backslash\Gamma/\Gamma_\infty$, where Γ_∞ is the stabilizer of ∞.

There is a bijection between M-symbols and $[\Gamma : \Gamma_0(N)]$: we only need to consider the action of Γ_∞ on M-symbols.

Number of $\Gamma_0(\mathrm{N})$- equivalence classes of cusps

Our only Γ- orbit of cusps splits into a finite union of $\Gamma_0(N)$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(N)\backslash\Gamma/\Gamma_\infty$, where Γ_∞ is the stabilizer of ∞.
There is a bijection between M-symbols and $[\Gamma : \Gamma_0(N)]$: we only need to consider the action of Γ_∞ on M-symbols.

We observe that M-symbols modulo N satisfy:

- $(c : d) = (c' : d') \Longrightarrow \gcd(c, N) = \gcd(c', N)$
- $(c : d) = (c : d') \Longleftrightarrow d \equiv d' \pmod{N/c}$

Number of $\Gamma_0(\mathrm{N})$- equivalence classes of cusps

Our only Γ- orbit of cusps splits into a finite union of $\Gamma_0(N)$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(N)\backslash\Gamma/\Gamma_\infty$, where Γ_∞ is the stabilizer of ∞.
There is a bijection between M-symbols and $[\Gamma : \Gamma_0(N)]$: we only need to consider the action of Γ_∞ on M-symbols.

We observe that M-symbols modulo N satisfy:

- $(c : d) = (c' : d') \Longrightarrow \gcd(c, N) = \gcd(c', N)$
- $(c : d) = (c : d') \Longleftrightarrow d \equiv d' \pmod{N/c}$

and the action of Γ_∞ on M-symbols is given by:

$$(c : d)\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = (c : cn + d)$$

Algorithm: Find a set of representatives of the $\Gamma_0(N)$- equivalence classes of rational cusps.

Loop over $c|N$:

- Set $g = \gcd(c, N/c)$, and loop over $d \pmod g$, with $\gcd(d, g) = 1$:
  - Lift d to d' such that:

    $$\gcd(c, d') = 1$$

    $$d' \equiv d \pmod g$$

  - Find $a, b \in \mathbb{Z}$ such that $ac - bd' = 1$. Output $\boldsymbol{a/c}$.

Algorithm: Find a set of representatives of the $\Gamma_0(N)$- equivalence classes of rational cusps.

Loop over $c|N$:

- Set $g = \gcd(c, N/c)$, and loop over $d \pmod g$, with $\gcd(d, g) = 1$:
  - Lift d to d' such that:

    $$\gcd(c, d') = 1$$

    $$d' \equiv d \pmod g$$

    Output $\boldsymbol{d'/c}$.

Algorithm: Find a set of representatives of the $\Gamma_0(N)$- equivalence classes of rational cusps.

Loop over $c|N$:

- Set $g = \gcd(c, N/c)$, and loop over $d \pmod g$, with $\gcd(d, g) = 1$:
  - Lift d to d' such that:

    $$\gcd(c, d') = 1$$
    $$d' \equiv d \pmod g$$

    Output $\boldsymbol{d'/c}$.

The number of $\Gamma_0(N)$ - orbits of rational cusps is:

$$\sum_{d|N} \varphi(\gcd(d, N/d)),$$

where $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Cusps and Manin symbols over number fields

Cusps over a number field

Cusps over a number field

Let K be a number field with ring of integers R and class number h_K. A *cusp* of K is an element of $\mathbb{P}^1(K) = K \cup \{\infty\}$.

Cusps over a number field

Let K be a number field with ring of integers R and class number h_K. A *cusp* of K is an element of $\mathbb{P}^1(K) = K \cup \{\infty\}$.

For $h_K = 1$ we may represent cusps in the form a/b where $a, b \in R$ are coprime. This representation is unique up to multiplication of a and b by a unit of R, and things will be very similar to the situation over $\mathbb{Q}$.

Cusps over a number field

Let K be a number field with ring of integers R and class number h_K. A *cusp* of K is an element of $\mathbb{P}^1(K) = K \cup \{\infty\}$.

For $h_K = 1$ we may represent cusps in the form a/b where $a, b \in R$ are coprime. This representation is unique up to multiplication of a and b by a unit of R, and things will be very similar to the situation over $\mathbb{Q}$.

In general, cusps may be represented in the form a/b with $a, b \in R$ not both zero, but this representation is not unique.

Cusps over a number field

Let K be a number field with ring of integers R and class number h_K. A *cusp* of K is an element of $\mathbb{P}^1(K) = K \cup \{\infty\}$.

For $h_K = 1$ we may represent cusps in the form a/b where $a, b \in R$ are coprime. This representation is unique up to multiplication of a and b by a unit of R, and things will be very similar to the situation over $\mathbb{Q}$.

In general, cusps may be represented in the form a/b with $a, b \in R$ not both zero, but this representation is not unique.

To each representation $\alpha = a/b$ we may associate the ideal $\langle a, b\rangle$ and its class $[\langle a, b\rangle]$.

Cusps over a number field

Let K be a number field with ring of integers R and class number h_K. A *cusp* of K is an element of $\mathbb{P}^1(K) = K \cup \{\infty\}$.

For $h_K = 1$ we may represent cusps in the form a/b where $a, b \in R$ are coprime. This representation is unique up to multiplication of a and b by a unit of R, and things will be very similar to the situation over $\mathbb{Q}$.

In general, cusps may be represented in the form a/b with $a, b \in R$ not both zero, but this representation is not unique.

To each representation $\alpha = a/b$ we may associate the ideal $\langle a, b\rangle$ and its class $[\langle a, b\rangle]$.

Note that:

1. if $a/b = a'/b' \in \mathbb{P}^1(K)$, then $[\langle a, b\rangle] = [\langle a', b'\rangle]$, but the ideals $\langle a, b\rangle$ and $\langle a', b'\rangle$ need not be equal,
2. given any ideal $\mathfrak{a}$ in $[\langle a, b\rangle]$, there is a representative a'/b' of the cusp a/b such that $\mathfrak{a} = \langle a', b'\rangle$.

Let Γ be $GL(2,R)$. For a nonzero ideal $\mathfrak{n}$ of R, that we call *level*, we have:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,|\, c \in \mathfrak{n} \right\}.$$

Let Γ be $GL(2, R)$. For a nonzero ideal $\mathfrak{n}$ of R, that we call *level*, we have:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,|\, c \in \mathfrak{n} \right\}.$$

We have a natural map

$$\begin{array}{ccc} R^2 \setminus \{0\} & \longrightarrow & \mathbb{P}^1(K) \\ \binom{a}{b} & \longmapsto & a/b \end{array}$$

which is Γ- equivariant.

Let Γ be $GL(2, R)$. For a nonzero ideal $\mathfrak{n}$ of R, that we call *level*, we have:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,|\, c \in \mathfrak{n} \right\}.$$

We have a natural map

$$\begin{array}{rcl} R^2 \setminus \{0\} & \longrightarrow & \mathbb{P}^1(K) \\ \binom{a}{b} & \longmapsto & a/b \end{array}$$

which is Γ- equivariant.

Γ and $\Gamma_0(\mathfrak{n})$ act on the set of cusps by linear fractional transformations, and on the set of representatives $\binom{a}{b} \in R^2 \setminus \{0\}$ by left multiplication.

$(\mathfrak{a}, \mathfrak{b})$-matrices

$(\mathfrak{a}, \mathfrak{b})$-matrices

Given $\mathfrak{a}, \mathfrak{b}$ nonzero ideals of R in inverse classes, we have an isomorphism of R-modules $\mathfrak{a} \oplus \mathfrak{b} \cong R \oplus R$.

$(\mathfrak{a}, \mathfrak{b})$-matrices

Given $\mathfrak{a}, \mathfrak{b}$ nonzero ideals of R in inverse classes, we have an isomorphism of R-modules $\mathfrak{a} \oplus \mathfrak{b} \cong R \oplus R$.

An $(\mathfrak{a}, \mathfrak{b})$-matrix is any matrix M in $\mathrm{Mat}(2, R)$ such that $(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}$. We can explicitly construct such a matrix.

$(\mathfrak{a}, \mathfrak{b})$-matrices

Given $\mathfrak{a}, \mathfrak{b}$ nonzero ideals of R in inverse classes, we have an isomorphism of R-modules $\mathfrak{a} \oplus \mathfrak{b} \cong R \oplus R$.

An $(\mathfrak{a}, \mathfrak{b})$-matrix is any matrix M in $\mathrm{Mat}(2, R)$ such that $(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}$. We can explicitly construct such a matrix.

PROPOSITION. *Let* $\mathfrak{a} = \langle a_1, a_2 \rangle, \mathfrak{b}$ *be ideals in inverse classes, with* $\mathfrak{a}\mathfrak{b} = \langle g \rangle$. *Then* $g = a_1 b_2 - a_2 b_1$ *with* $b_1, b_2 \in \mathfrak{b}$ *and* $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ *satisfies*

$$(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}.$$

$(\mathfrak{a}, \mathfrak{b})$-matrices

Given $\mathfrak{a}, \mathfrak{b}$ nonzero ideals of R in inverse classes, we have an isomorphism of R-modules $\mathfrak{a} \oplus \mathfrak{b} \cong R \oplus R$.

An $(\mathfrak{a}, \mathfrak{b})$-matrix is any matrix M in $\mathrm{Mat}(2, R)$ such that $(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}$. We can explicitly construct such a matrix.

PROPOSITION. *Let $\mathfrak{a} = \langle a_1, a_2 \rangle$, $\mathfrak{b}$ be ideals in inverse classes, with $\mathfrak{a}\mathfrak{b} = \langle g \rangle$. Then $g = a_1 b_2 - a_2 b_1$ with $b_1, b_2 \in \mathfrak{b}$ and $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ satisfies*

$$(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}.$$

Let α be a cusp with representative a_1/a_2. We may regard the column vector $\binom{a_1}{a_2}$ as the first column of an $(\mathfrak{a}, \mathfrak{b})$-matrix, and study the action of Γ and its subgroups on the set of representatives of cusps via its action by left multiplication on $(\mathfrak{a}, \mathfrak{b})$-matrices.

$X_{\mathfrak{a},\mathfrak{b}}$ will denote the set of all $(\mathfrak{a}, \mathfrak{b})$-matrices for fixed ideals $\mathfrak{a}$, $\mathfrak{b}$ in inverse classes.

$X_{\mathfrak{a},\mathfrak{b}}$ will denote the set of all $(\mathfrak{a},\mathfrak{b})$-matrices for fixed ideals $\mathfrak{a}$, $\mathfrak{b}$ in inverse classes.

> NOTE: For $\mathfrak{a}=\mathfrak{b}=R$ an $(\mathfrak{a},\mathfrak{b})$-matrix M, which is then characterized by $(R\oplus R)M=R\oplus R$, is just an element of Γ ($\Gamma=GL(2,R)$ can be characterized as the stabilizer of the lattice $R\oplus R$).

$X_{\mathfrak{a},\mathfrak{b}}$ will denote the set of all $(\mathfrak{a}, \mathfrak{b})$-matrices for fixed ideals $\mathfrak{a}$, $\mathfrak{b}$ in inverse classes.

> NOTE: For $\mathfrak{a} = \mathfrak{b} = R$ an $(\mathfrak{a}, \mathfrak{b})$-matrix M, which is then characterized by $(R \oplus R)M = R \oplus R$, is just an element of Γ ($\Gamma = GL(2, R)$ can be characterized as the stabilizer of the lattice $R \oplus R$).

Define

$$\Gamma^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mid x, \, w \in R, \, y \in \mathfrak{a}^{-1}\mathfrak{b}, \, z \in \mathfrak{a}\mathfrak{b}^{-1}, xw - yz \in R^{\times} \right\}.$$

$X_{\mathfrak{a},\mathfrak{b}}$ will denote the set of all $(\mathfrak{a}, \mathfrak{b})$-matrices for fixed ideals $\mathfrak{a}$, $\mathfrak{b}$ in inverse classes.

> NOTE: For $\mathfrak{a} = \mathfrak{b} = R$ an $(\mathfrak{a}, \mathfrak{b})$-matrix M, which is then characterized by $(R \oplus R)M = R \oplus R$, is just an element of Γ ($\Gamma = GL(2, R)$ can be characterized as the stabilizer of the lattice $R \oplus R$).

Define

$$\Gamma^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mid x,\, w \in R,\; y \in \mathfrak{a}^{-1}\mathfrak{b},\; z \in \mathfrak{a}\mathfrak{b}^{-1}, xw - yz \in R^{\times} \right\}.$$

Note that $\Gamma^{\mathfrak{a},\mathfrak{b}} = \Gamma$ when $\mathfrak{a} = \mathfrak{b}$.

$X_{\mathfrak{a},\mathfrak{b}}$ will denote the set of all $(\mathfrak{a}, \mathfrak{b})$-matrices for fixed ideals $\mathfrak{a}$, $\mathfrak{b}$ in inverse classes.

> NOTE: For $\mathfrak{a} = \mathfrak{b} = R$ an $(\mathfrak{a}, \mathfrak{b})$-matrix M, which is then characterized by $(R \oplus R)M = R \oplus R$, is just an element of Γ ($\Gamma = GL(2, R)$ can be characterized as the stabilizer of the lattice $R \oplus R$).

Define

$$\Gamma^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mid x,\, w \in R,\, y \in \mathfrak{a}^{-1}\mathfrak{b},\, z \in \mathfrak{a}\mathfrak{b}^{-1}, xw - yz \in R^{\times} \right\}.$$

Then:

PROPOSITION. *Let $\mathfrak{a}, \mathfrak{b}$ be two ideals (not necessarily in inverse ideal classes). Then for $\gamma \in GL(2, K)$:*

$$(\mathfrak{a} \oplus \mathfrak{b})\gamma = \mathfrak{a} \oplus \mathfrak{b} \Longleftrightarrow \gamma \in \Gamma^{\mathfrak{a},\mathfrak{b}}$$

We need a few more definitions:

$$\Gamma_\infty^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \,|\, x,\, w \in R,\, y \in \mathfrak{a}^{-1}\mathfrak{b},\, xw \in R^\times \right\};$$

$$\Gamma_1^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} 1 & y \\ 0 & w \end{pmatrix} \,|\, y \in \mathfrak{a}^{-1}\mathfrak{b},\, w \in R^\times \right\};$$

$$\Gamma_{1,1}^{\mathfrak{a},\mathfrak{b}} = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \,|\, y \in \mathfrak{a}^{-1}\mathfrak{b} \right\}.$$

We need a few more definitions:

$$\begin{aligned}
\Gamma^{\mathfrak{a},\mathfrak{b}}_{\infty} &= \left\{ \begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \mid x, w \in R,\ y \in \mathfrak{a}^{-1}\mathfrak{b},\ xw \in R^{\times} \right\}; \\
\Gamma^{\mathfrak{a},\mathfrak{b}}_{1} &= \left\{ \begin{pmatrix} 1 & y \\ 0 & w \end{pmatrix} \mid y \in \mathfrak{a}^{-1}\mathfrak{b},\ w \in R^{\times} \right\}; \\
\Gamma^{\mathfrak{a},\mathfrak{b}}_{1,1} &= \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathfrak{a}^{-1}\mathfrak{b} \right\}.
\end{aligned}$$

And now we can give a description of the set $X_{\mathfrak{a},\mathfrak{b}}$ of $(\mathfrak{a},\mathfrak{b})$-matrices:

PROPOSITION. *Let $M_0 \in X_{\mathfrak{a},\mathfrak{b}}$ be arbitrary. Then:*

$$X_{\mathfrak{a},\mathfrak{b}} = \Gamma M_0 = M_0 \Gamma^{\mathfrak{a},\mathfrak{b}},$$

Also, the set of $(\mathfrak{a},\mathfrak{b})$-matrices with same first column as M_0 is $M_0\Gamma^{\mathfrak{a},\mathfrak{b}}_1$, and the set of those with same first column and determinant as M_0 is $M_0\Gamma^{\mathfrak{a},\mathfrak{b}}_{1,1}$.

$X_{\mathfrak{a},\mathfrak{b}}$ under the action of $\Gamma_0(N)$:

$\boldsymbol{X_{\mathfrak{a},\mathfrak{b}}}$ under the action of $\boldsymbol{\Gamma_0(N)}$:

PROPOSITION. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals in inverse classes, and* $M_1 = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$,
$M_2 = \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix}$ *any two $(\mathfrak{a}, \mathfrak{b})$-matrices. The following are equivalent:*

1. $M_2 = \gamma M_1$ *with* $\gamma \in \Gamma_0(\mathfrak{n})$
2. $a'_2 b_2 \equiv a_2 b'_2 \pmod{\mathfrak{a}\mathfrak{b}\mathfrak{n}}$.
3. *There exists $u \in R$ coprime to $\mathfrak{n}$ such that*
   (a) $u a_2 \equiv a'_2 \pmod{\mathfrak{a}\mathfrak{n}}$
   (b) $u b_2 \equiv b'_2 \pmod{\mathfrak{b}\mathfrak{n}}$.

PROPOSITION. *Any of the equivalent statements of the above result also implies:*

There exist $u \in R$ *coprime to* $\mathfrak{n}$, $u_0 \in R^\times$ *and* $\mathfrak{d}$ *divisor of* $\mathfrak{n}$ *such that:*

(a) $\langle a_2 \rangle + \mathfrak{a}\mathfrak{n} = \langle a_2' \rangle + \mathfrak{a}\mathfrak{n} = \mathfrak{a}\mathfrak{d}$

(b) $u a_2 \equiv a_2' \pmod{\mathfrak{a}\mathfrak{n}}$

(c) $u_0 a_1 \equiv u a_1' \pmod{\mathfrak{d}\mathfrak{n}}$

Conversely, if the above holds then there exists $\gamma \in \Gamma_0(\mathfrak{n})$ *such that*

$$\gamma M_1 = M_2' = M_2 \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}, \text{ with } w \in \mathfrak{a}^{-1}\mathfrak{b},$$

so that M_2' *is another* $(\mathfrak{a}, \mathfrak{b})$*-matrix with same first column and determinant as* M_2*.*

Cusp equivalence under Γ

Cusp equivalence under Γ

It is easy to check that:

Cusp equivalence under Γ

It is easy to check that:

1. The ideal $\langle a, b\rangle$ associated to $\binom{a}{b}$ is Γ-invariant.
2. If $\langle a, b\rangle = \langle a', b'\rangle$, then $\gamma \binom{a}{b} = \binom{a'}{b'}$ for some $\gamma \in \Gamma$.

Cusp equivalence under Γ

It is easy to check that:

1. The ideal $\langle a, b\rangle$ associated to $\binom{a}{b}$ is Γ-invariant.
2. If $\langle a, b\rangle = \langle a', b'\rangle$, then $\gamma \binom{a}{b} = \binom{a'}{b'}$ for some $\gamma \in \Gamma$.

PROPOSITION. *There is a bijection:*

$$\begin{array}{ccc} \Gamma\backslash\mathbb{P}^1(K) & \longrightarrow & Cl(K) \\ \alpha & \longmapsto & [\alpha] \end{array}$$

where if a/b a representative of α, $[\alpha] = [\langle a, b\rangle]$.

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

Let $\alpha = a_1/a_2$ be a cusp of K. We define the *denominator ideal* $\mathfrak{d}(\alpha)$ as the ideal $\langle a_2 \rangle / \langle a_1, a_2 \rangle$.The denominator ideal is independent of the choice of representative.

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

Let $\alpha = a_1/a_2$ be a cusp of K. We define the *denominator ideal* $\mathfrak{d}(\alpha)$ as the ideal $\langle a_2\rangle/\langle a_1, a_2\rangle$.The denominator ideal is independent of the choice of representative.

Now, to each cusp α we assign the ideal $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}(\alpha) + \mathfrak{n}$, a divisor of $\mathfrak{n}$.

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

Let $\alpha = a_1/a_2$ be a cusp of K. We define the *denominator ideal* $\mathfrak{d}(\alpha)$ as the ideal $\langle a_2 \rangle / \langle a_1, a_2 \rangle$.The denominator ideal is independent of the choice of representative.

Now, to each cusp α we assign the ideal $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}(\alpha) + \mathfrak{n}$, a divisor of $\mathfrak{n}$.

The ideal $\mathfrak{d}_{\mathfrak{n}}$ is $\Gamma_0(\mathfrak{n})$- invariant.

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

PROPOSITION. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a'_1/a'_2$ with the same ideal $\mathfrak{a} = \langle a_1, a_2 \rangle = \langle a'_1, a'_2 \rangle$. Then the following are equivalent:*

1. $\gamma(\alpha) = \alpha'$ *for some* $\gamma \in \Gamma_0(\mathfrak{n})$.
2. *there exist* $u \in R$ *coprime to* $\mathfrak{n}$, $u_0 \in R^\times$ *and a divisor* $\mathfrak{d}$ *of* $\mathfrak{n}$ *such that:*
   - (a) $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}_{\mathfrak{n}}(\alpha') = \mathfrak{d}$
   - (b) $a'_2 \equiv u a_2 \pmod{\mathfrak{n}\mathfrak{a}}$
   - (c) $u a'_1 \equiv u_0 a_1 \pmod{\mathfrak{d}\mathfrak{a}}$

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

PROPOSITION. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2 \rangle = \langle a_1', a_2' \rangle$. Then the following are equivalent:*

1. *$\gamma(\alpha) = \alpha'$ for some $\gamma \in \Gamma_0(\mathfrak{n})$.*
2. *there exist $u \in R$ coprime to $\mathfrak{n}$, $u_0 \in R^\times$ and a divisor $\mathfrak{d}$ of $\mathfrak{n}$ such that:*
   - *(a)* $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}_{\mathfrak{n}}(\alpha') = \mathfrak{d}$
   - *(b)* $a_2' \equiv u a_2 \pmod{\mathfrak{n}\mathfrak{a}}$
   - *(c)* $u a_1' \equiv u_0 a_1 \pmod{\mathfrak{d}\mathfrak{a}}$

In case $\mathfrak{a}$ and $\mathfrak{n}$ are coprime, we can replace 2 by the simpler:

2'. *there exist $u \in R$ coprime to $\mathfrak{n}$, $u_0 \in R^\times$ and a divisor $\mathfrak{d}$ of $\mathfrak{n}$ such that:*
   - *(a)* $\langle a_2 \rangle + \mathfrak{n} = \langle a_2' \rangle + \mathfrak{n} = \mathfrak{d}$
   - *(b)* $a_2' \equiv u a_2 \pmod{\mathfrak{n}}$
   - *(c)* $u a_1' \equiv u_0 a_1 \pmod{\mathfrak{d}}$

Over $\mathbb{Q}$:

PROPOSITION: *Let α_1 and α_2 be cusps with representatives p_1/q_1 and p_2/q_2. The following are equivalent:*

1. *$\alpha_2 = M(\alpha_1)$ for some $M \in \Gamma_0(N)$.*
2. *$q_2 \equiv uq_1 \pmod N$ and $up_2 \equiv p_1 \pmod{\gcd(q_1, N)}$, with $\gcd(u, N) = 1$.*
3. ***$s_1 q_2 \equiv s_2 q_1 \pmod{\gcd(q_1 q_2, N)}$, where s_j satisfies $p_j s_j \equiv 1 \pmod{q_j}$.***

COROLLARY. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2 \rangle = \langle a_1', a_2' \rangle$ which is coprime to $\mathfrak{n}$. Let $\mathfrak{b}$ be any ideal in the inverse class to $\mathfrak{a}$, and form $(\mathfrak{a}, \mathfrak{b})$-matrices $M_1 = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ and $M_2 = \begin{pmatrix} a_1' & b_1' \\ a_2' & b_2' \end{pmatrix}$.*

Then α and α' are $\Gamma_0(\mathfrak{n})$-equivalent if and only if

1. $\langle a_2 \rangle + \mathfrak{n} = \langle a_2' \rangle + \mathfrak{n} = \mathfrak{d}$
2. *there exists $u_0 \in R^\times$ such that:*

$$a_2' b_2 \equiv u_0 a_2 b_2' \pmod{\mathfrak{a}\mathfrak{b}\mathfrak{d}^2}$$

Manin symbols over number fields

Manin symbols over number fields

PROPOSITION. *Let* $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Gamma$ *for* $i = 1, 2$. *Then*

$$\Gamma_0(\mathfrak{n})\gamma_1 = \Gamma_0(\mathfrak{n})\gamma_2 \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}.$$

Manin symbols over number fields

PROPOSITION. *Let* $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Gamma$ *for* $i = 1, 2$. *Then*

$$\Gamma_0(\mathfrak{n})\gamma_1 = \Gamma_0(\mathfrak{n})\gamma_2 \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}.$$

The set of coprime pairs $(c, d) \in R \oplus R$ modulo the equivalence relation:

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}$$

is $\mathbb{P}^1(R/\mathfrak{n})$. We call its elements *M-symbols or Manin symbols of level* $\mathfrak{n}$.

Manin symbols over number fields

PROPOSITION. *Let* $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Gamma$ *for* $i = 1, 2$. *Then*

$$\Gamma_0(\mathfrak{n})\gamma_1 = \Gamma_0(\mathfrak{n})\gamma_2 \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}.$$

The set of coprime pairs $(c, d) \in R \oplus R$ modulo the equivalence relation:

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}$$

is $\mathbb{P}^1(R/\mathfrak{n})$. We call its elements *M-symbols or Manin symbols of level* $\mathfrak{n}$.

Let $\mathfrak{a}, \mathfrak{b}$ be ideals of R in inverse classes. We look now at the pairs that can occur as a row of an $(\mathfrak{a}, \mathfrak{b})$-matrix.

Manin symbols over number fields

PROPOSITION. *Let* $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Gamma$ *for* $i = 1, 2$. *Then*

$$\Gamma_0(\mathfrak{n})\gamma_1 = \Gamma_0(\mathfrak{n})\gamma_2 \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}.$$

The set of coprime pairs $(c, d) \in R \oplus R$ modulo the equivalence relation:

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1 d_2 \equiv c_2 d_1 \pmod{\mathfrak{n}}$$

is $\mathbb{P}^1(R/\mathfrak{n})$. We call its elements *M-symbols or Manin symbols of level* $\mathfrak{n}$.

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals of R in inverse classes. We look now at the pairs that can occur as a row of an $(\mathfrak{a}, \mathfrak{b})$-matrix.

PROPOSITION. *Let* $\mathfrak{a}, \mathfrak{b}$ *be ideals in inverse classes. A pair* $(a, b) \in \mathfrak{a} \oplus \mathfrak{b}$ *occurs as a row of an* $(\mathfrak{a}, \mathfrak{b})$*-matrix if and only if*

$$a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R$$

More generally: An *M-symbol of level* $\mathfrak{n}$ *and type* $(\mathfrak{a}, \mathfrak{b})$ is an equivalence class of

$$\left\{(a,b) \in \mathfrak{a} \oplus \mathfrak{b} :\ a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R\right\} / \sim$$

where:

$$\begin{aligned}
(a,b) \sim (a',b') &\iff ab' \equiv a'b \pmod{\mathfrak{a}\mathfrak{b}\mathfrak{n}} \\
&\iff \text{there exists } u \in R \text{ coprime to } \mathfrak{n} \text{ such that} \\
&\qquad ua \equiv a' \pmod{\mathfrak{a}\mathfrak{n}} \\
&\qquad ub \equiv b' \pmod{\mathfrak{b}\mathfrak{n}}
\end{aligned}$$

More generally: An *M-symbol of level* $\mathfrak{n}$ *and type* $(\mathfrak{a}, \mathfrak{b})$ is an equivalence class of

$$\left\{(a,b) \in \mathfrak{a} \oplus \mathfrak{b} : \, a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R\right\} / \sim$$

where, for $\mathfrak{a}\mathfrak{b}$ coprime to $\mathfrak{n}$:

$$\begin{aligned}(a,b) \sim (a',b') \quad &\Longleftrightarrow \quad ab' \equiv a'b \pmod{\mathfrak{n}} \\ &\Longleftrightarrow \quad \text{there exists } u \in R \text{ coprime to } \mathfrak{n} \text{ such that} \\ &\qquad\quad ua \equiv a' \pmod{\mathfrak{n}} \\ &\qquad\quad ub \equiv b' \pmod{\mathfrak{n}}\end{aligned}$$

More generally: An *M-symbol of level* $\mathfrak{n}$ *and type* $(\mathfrak{a}, \mathfrak{b})$ is an equivalence class of

$$\left\{(a,b) \in \mathfrak{a} \oplus \mathfrak{b} :\ a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R\right\} / \sim$$

where, for $\mathfrak{a}\mathfrak{b}$ coprime to $\mathfrak{n}$:

$$\begin{aligned}(a,b) \sim (a',b') \quad &\iff \quad ab' \equiv a'b \pmod{\mathfrak{n}} \\ &\iff \quad \text{there exists } u \in R \text{ coprime to } \mathfrak{n} \text{ such that} \\ &\qquad\quad ua \equiv a' \pmod{\mathfrak{n}} \\ &\qquad\quad ub \equiv b' \pmod{\mathfrak{n}}\end{aligned}$$

Given $\mathfrak{a}, \mathfrak{b}$ ideals in inverse classes, there are bijections:

$$\left\{ \begin{array}{c} \text{M-symbols of level } \mathfrak{n} \\ \text{and type } (\mathfrak{a}, \mathfrak{b}) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Set of orbits} \\ \text{of } \Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Set of orbits} \\ \text{of } \Gamma_0(\mathfrak{n})\backslash \Gamma \end{array} \right\}$$

We have another normalization for M-symbols:

PROPOSITION. *Let* $\mathfrak{a}, \mathfrak{b}$ *be ideals in inverse classes, both coprime to* $\mathfrak{n}$*. Given* $(a, b) \in \mathfrak{a} \oplus \mathfrak{b}$ *such that* $a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} + \mathfrak{n} = R$*, there exist* $(a', b') \in \mathfrak{a} \oplus \mathfrak{b}$ *such that*

$$\begin{aligned} a' &\equiv a \pmod{\mathfrak{n}} \\ b' &\equiv b \pmod{\mathfrak{n}} \\ a'\mathfrak{a}^{-1} + b'\mathfrak{b}^{-1} &= R \end{aligned}$$

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

We know there are h_K Γ- orbits, where h_K is the class number.

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

We know there are h_K Γ- orbits, where h_K is the class number.

Each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, where α is any cusp in the orbit and Γ_α is its stabilizer.

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

We know there are h_K Γ- orbits, where h_K is the class number.

Each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, where α is any cusp in the orbit and Γ_α is its stabilizer.

Using $(\mathfrak{a}, \mathfrak{b})$-matrices. Fix an ideal class, and let $\mathfrak{a}$ be an ideal in this class, and $\mathfrak{b}$ an ideal in the inverse class.

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

We know there are h_K Γ- orbits, where h_K is the class number.

Each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, where α is any cusp in the orbit and Γ_α is its stabilizer.

Using $(\mathfrak{a},\mathfrak{b})$-matrices. Fix an ideal class, and let $\mathfrak{a}$ be an ideal in this class, and $\mathfrak{b}$ an ideal in the inverse class.

> NOTE: All cusps in the class have representations with associated ideal $\mathfrak{a}$. In particular, all cusps in the class are of the form $\alpha = M(\infty)$, where M is an $(\mathfrak{a},\mathfrak{b})$-matrix.

Number of $\Gamma_0(\mathfrak{n})$- equivalence classes of cusps

We know there are h_K Γ- orbits, where h_K is the class number.

Each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, where α is any cusp in the orbit and Γ_α is its stabilizer.

Using $(\mathfrak{a}, \mathfrak{b})$-matrices. Fix an ideal class, and let $\mathfrak{a}$ be an ideal in this class, and $\mathfrak{b}$ an ideal in the inverse class.

> NOTE: All cusps in the class have representations with associated ideal $\mathfrak{a}$. In particular, all cusps in the class are of the form $\alpha = M(\infty)$, where M is an $(\mathfrak{a}, \mathfrak{b})$-matrix.

The $\Gamma_0(\mathfrak{n})$-sub-orbits of $\Gamma\alpha$, are also in bijection with the double cosets $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Gamma_1^{\mathfrak{a},\mathfrak{b}}$.

From a double coset decomposition

$$\Gamma = \coprod \Gamma_0(\mathfrak{n})\gamma_i\Gamma_\alpha$$

where $\{\gamma_i\}_i$ is a set of representatives of $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$,

From a double coset decomposition

$$\Gamma = \coprod \Gamma_0(\mathfrak{n})\gamma_i\Gamma_\alpha$$

where $\{\gamma_i\}_i$ is a set of representatives of $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, we obtain a decomposition:

$$X_{\mathfrak{a},\mathfrak{b}} = \coprod \Gamma_0(\mathfrak{n})M_i\Gamma_\infty^{\mathfrak{a},\mathfrak{b}}$$

with:

- $M_i = \gamma_i M_0$ running through a set of representatives for $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Gamma_\infty^{\mathfrak{a},\mathfrak{b}}$.
- M_0 such that $\alpha = M_0(\infty)$.

From a double coset decomposition

$$\Gamma = \coprod \Gamma_0(\mathfrak{n})\gamma_i\Gamma_\alpha$$

where $\{\gamma_i\}_i$ is a set of representatives of $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, we obtain a decomposition:

$$X_{\mathfrak{a},\mathfrak{b}} = \coprod \Gamma_0(\mathfrak{n})M_i\Gamma_\infty^{\mathfrak{a},\mathfrak{b}}$$

with:

- $M_i = \gamma_i M_0$ running through a set of representatives for $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Gamma_\infty^{\mathfrak{a},\mathfrak{b}}$.
- M_0 such that $\alpha = M_0(\infty)$.

In particular, since $\Gamma_\infty^{\mathfrak{a},\mathfrak{b}} = R^\times\Gamma_1^{\mathfrak{a},\mathfrak{b}}$, we can take $X_{\mathfrak{a},\mathfrak{b}} = \coprod \Gamma_0(\mathfrak{n})M_i\Gamma_1^{\mathfrak{a},\mathfrak{b}}$.

Since each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Gamma_1^{\mathfrak{a},\mathfrak{b}}$, we can take two different approaches to the enumeration of the equivalence classes:

Since each Γ-orbit splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, which are in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Gamma_1^{\mathfrak{a},\mathfrak{b}}$, we can take two different approaches to the enumeration of the equivalence classes:

- "Vertical approach": we consider the left action of $\Gamma_0(\mathfrak{n})$ on $X_{\mathfrak{a},\mathfrak{b}}/\Gamma_1^{\mathfrak{a},\mathfrak{b}}$. In this case we are basically looking at the action of $\Gamma_0(\mathfrak{n})$ on column vectors.

- "Horizontal approach": we consider the right action of the stabilizer $\Gamma_1^{\mathfrak{a},\mathfrak{b}}$ on $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}$. Since there is a bijection between $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}$ and the set of M-symbols $(c:d)$, we are basically looking at the action of $\Gamma_1^{\mathfrak{a},\mathfrak{b}}$ on row vectors.

PROPOSITION. *Each Γ-orbit in $\mathbb{P}^1(K)$ splits into $\sum_{\mathfrak{d}|\mathfrak{n}} \varphi_{\mathfrak{u}}(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1})$ disjoint $\Gamma_0(\mathfrak{n})$-orbits, with*

$$\varphi_{\mathfrak{u}}(\mathfrak{m}) = \#((R/\mathfrak{m})^\times / U_{\mathfrak{m}})$$

where $U_{\mathfrak{m}}$ denotes the image of $R^\times$ in $(R/\mathfrak{m})^\times$.

Hence the total number of $\Gamma_0(\mathfrak{n})$-orbits of cusps is:

$$h_K \sum_{\mathfrak{d}|\mathfrak{n}} \varphi_{\mathfrak{u}}(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1}).$$

PROPOSITION. *Each Γ-orbit in $\mathbb{P}^1(K)$ splits into $\sum_{\mathfrak{d}|\mathfrak{n}} \varphi_{\mathfrak{u}}(\mathfrak{d} + \mathfrak{n}\mathfrak{d}^{-1})$ disjoint $\Gamma_0(\mathfrak{n})$-orbits, with*

$$\varphi_{\mathfrak{u}}(\mathfrak{m}) = \#((R/\mathfrak{m})^\times / U_{\mathfrak{m}})$$

where $U_{\mathfrak{m}}$ denotes the image of $R^\times$ in $(R/\mathfrak{m})^\times$.
Hence the total number of $\Gamma_0(\mathfrak{n})$-orbits of cusps is:

$$h_K \sum_{\mathfrak{d}|\mathfrak{n}} \varphi_{\mathfrak{u}}(\mathfrak{d} + \mathfrak{n}\mathfrak{d}^{-1}).$$

From the proof of the theorem (choosing the ”horizontal approach”), we obtain the following algorithm to enumerate a set of representatives for $\Gamma_0(N)$-equivalence classes.

- **Algorithm**: Obtaining a set of representatives for $\Gamma_0(\mathfrak{n})$- equivalence classes.

- **Algorithm**: Obtaining a set of representatives for $\Gamma_0(\mathfrak{n})$- equivalence classes. Compute a list of representatives $\mathfrak{a}$, with $\mathfrak{a}$ coprime to $\mathfrak{n}$, for each ideal class in K. For each $\mathfrak{a}$, fix $\mathfrak{b}$ in the inverse class to $\mathfrak{a}$, coprime to $\mathfrak{n}\mathfrak{a}$.

Algorithm: Obtaining a set of representatives for $\Gamma_0(\mathfrak{n})$- equivalence classes.

Loop over $\mathfrak{d}|\mathfrak{n}$:

1. Find $\mathfrak{d}'$ coprime to $\mathfrak{n}\mathfrak{b}$ in inverse class to $\mathfrak{d}\mathfrak{a}$.
2. Find a such that $\mathfrak{d}'\mathfrak{d}\mathfrak{a} = \langle a \rangle$
3. Loop through representatives of cosets in $(R/(\mathfrak{d} + \mathfrak{n}/\mathfrak{d}))^\times / U_{\mathfrak{d}+\mathfrak{n}/\mathfrak{d}}$.

   For each representative x:

   (a) Lift our representative x to a solution b coprime to a and such that $b \in \mathfrak{b}$:

   $$\begin{array}{ccc} (R/\langle a \rangle)^\times & \longrightarrow & \left(R/\left(\mathfrak{d} + \mathfrak{n}\mathfrak{d}^{-1}\right)\right)^\times / U_{\mathfrak{d}+\mathfrak{n}/\mathfrak{d}} \\ b & \longmapsto & x \end{array}$$

   (b) Complete the pair (a, b) to an $(\mathfrak{a}, \mathfrak{b})$-matrix $\begin{pmatrix} a' & b' \\ a & b \end{pmatrix}$.

   Output the cusp a'/a.

Computing cusps and M-symbols over number fields in Sage

(work in progress...)