

Computing fundamental domains for cofinite Fuchsian groups

John Voight

University of Vermont

Computations with Modular Forms

University of Bristol

Bristol, United Kingdom

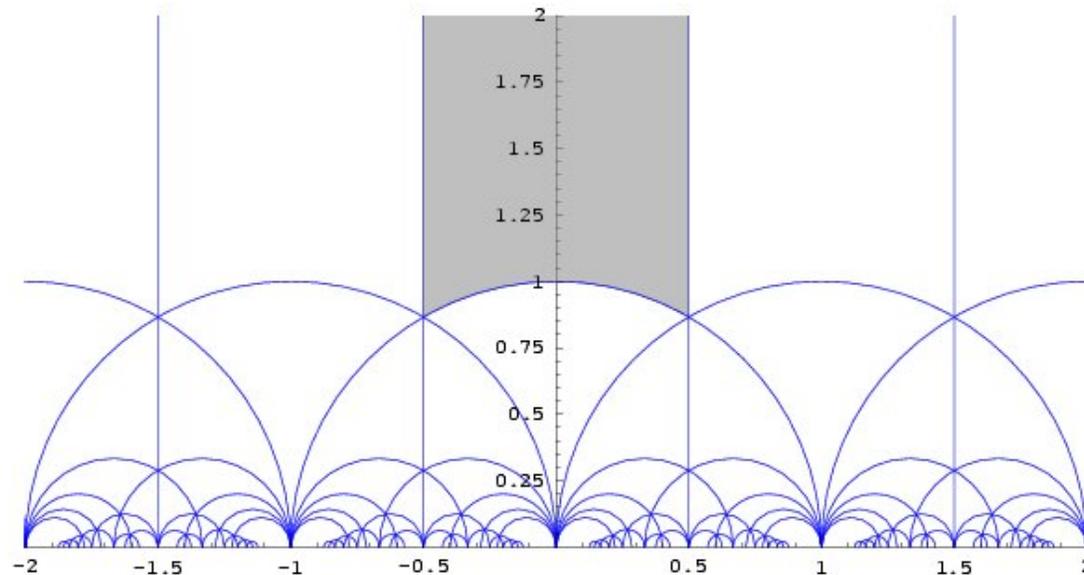
20 August 2008

Fundamental domains

Let $\Gamma \subset PSL_2(\mathbb{R})$ be a finitely generated *Fuchsian group*, a discrete group of orientation-preserving isometries of the upper half-plane \mathfrak{H} with hyperbolic metric d . A *fundamental domain* for Γ is a closed domain $D \subset \mathfrak{H}$ such that:

- (i) $\Gamma D = \mathfrak{H}$, and
- (ii) $gD^\circ \cap D^\circ = \emptyset$ for all $g \in \Gamma \setminus \{1\}$, where $^\circ$ denotes the interior.

In particular, the translates gD for $g \in \Gamma$ give a *tesselation* of \mathfrak{H} . For example, for $\Gamma = SL_2(\mathbb{Z})$, we have the usual picture:



Fundamental domains: $SL_2(\mathbb{Z})$

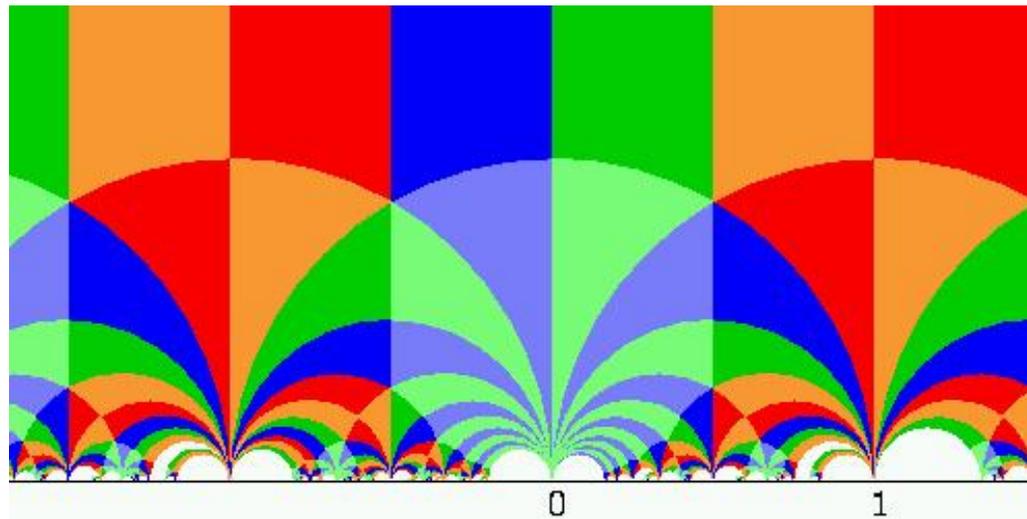
Or more artistically:



Regular Division of the Plane VI (1957–1958), M.C. Escher.

Fundamental domains: Subgroups of $SL_2(\mathbb{Z})$

For congruence (and some noncongruence) subgroups of $SL_2(\mathbb{Z})$, e.g. $\Gamma_0(N)$ for $N \in \mathbb{Z}_{>0}$, there is a method which uses *Farey symbols* to compute a fundamental domain (Verrill).



Here, the choice of any 6 triangles each of different color gives a fundamental domain for $\Gamma_0(2)$.

For a Fuchsian group Γ , there are a clearly many possible fundamental domains. Indeed, if D is a fundamental domain then so is gD for any $g \in G$. We seek out the most ones which are most natural (and useful).

Dirichlet domains

Let $p \in \mathfrak{H}$ be a point with trivial stabilizer $\Gamma_p = \{1\}$. We define the *Dirichlet domain* centered at p to be

$$D(p) = \{z \in \mathfrak{H} : d(z, p) \leq d(gz, p) \text{ for all } g \in \Gamma\}.$$

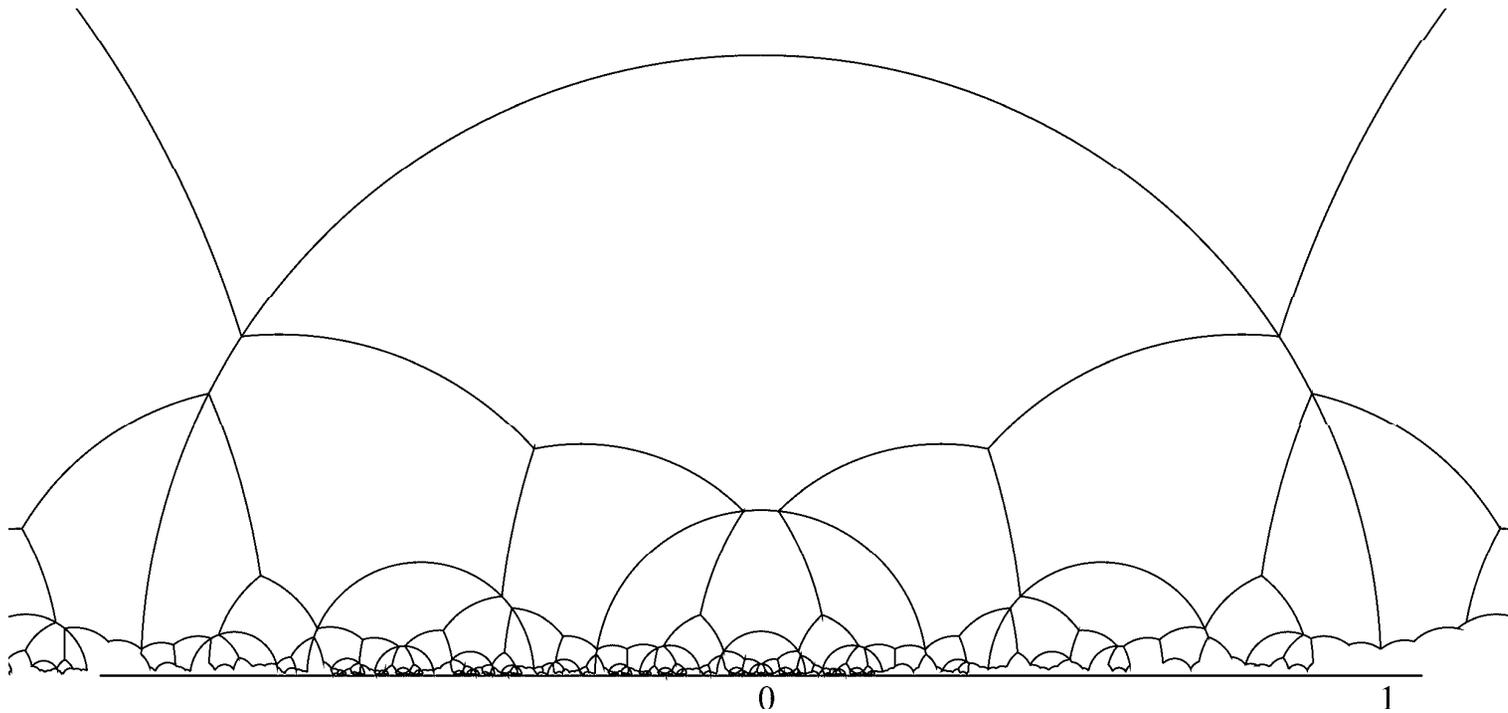
The set $D(p)$ is a fundamental domain for Γ , and is a *generalized hyperbolic polygon*, a closed, connected, and hyperbolically convex domain whose boundary consists of finitely many geodesic segments, called *sides*, along with possibly segments of the real axis.

(The Dirichlet construction works whenever a discrete group Γ acts on a locally compact space X with an *intrinsic* metric, so that there exists an equidistant point $y \in X$ from any two points $x_1, x_2 \in X$.)

From now on, we assume that the group Γ is *cofinite*, the orbit space $\Gamma \backslash \mathfrak{H}$ has finite hyperbolic area. Of particular and relevant interest is the class of *arithmetic Fuchsian groups*, those groups commensurable with groups associated to unit groups in certain quaternion algebras over totally real fields.

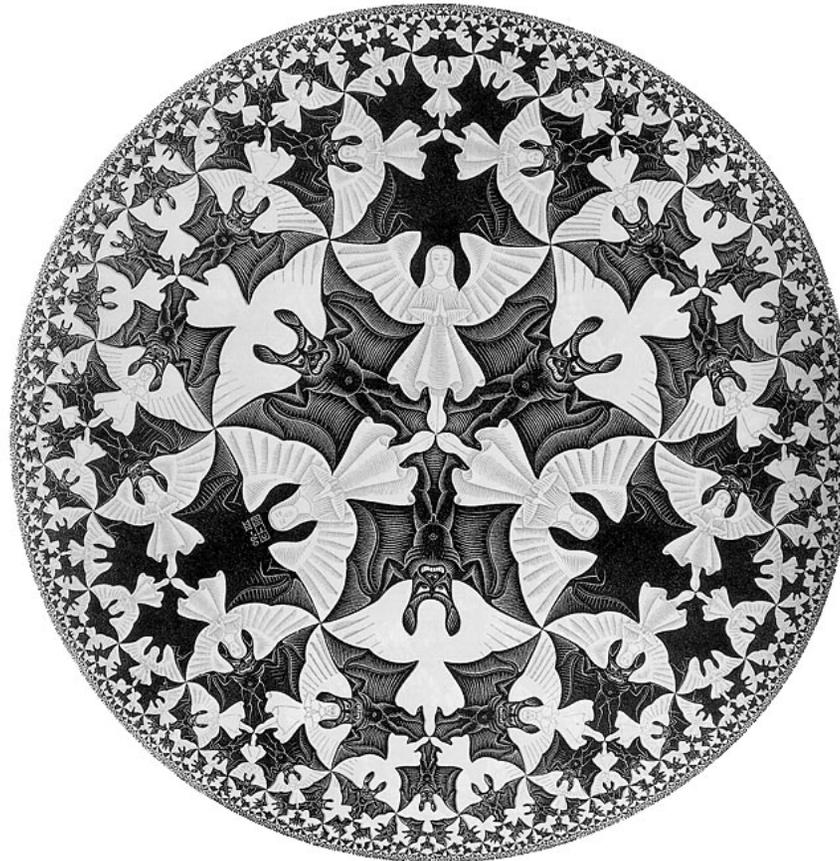
Dirichlet domains: $\Gamma^6(1)$

Here is an example of a tessellation of \mathfrak{H} from a Dirichlet domain for the arithmetic Fuchsian group $\Gamma^6(1)$, associated to the quaternion algebra of discriminant 6 over \mathbb{Q} :



Dirichlet domains: $(2, 4, 6)$ -triangle group

Here is Escher's rendition in the hyperbolic unit disc for the $(2, 4, 6)$ -triangle group, which contains $\Gamma^6(1)$ with index 4:



Circle Limit IV (1960), by M.C. Escher.

Side pairings

Let $D \subset \mathfrak{H}$ be a generalized hyperbolic polygon. Let $S = S(D)$ denote the set of sides of D , with the following convention.

If $g \in \Gamma$ is an element of order 2 which fixes a side s of D , and s contains the fixed point of g , we instead consider s to be the union of two sides meeting at the fixed point of g .

We define a labeled equivalence relation on S by

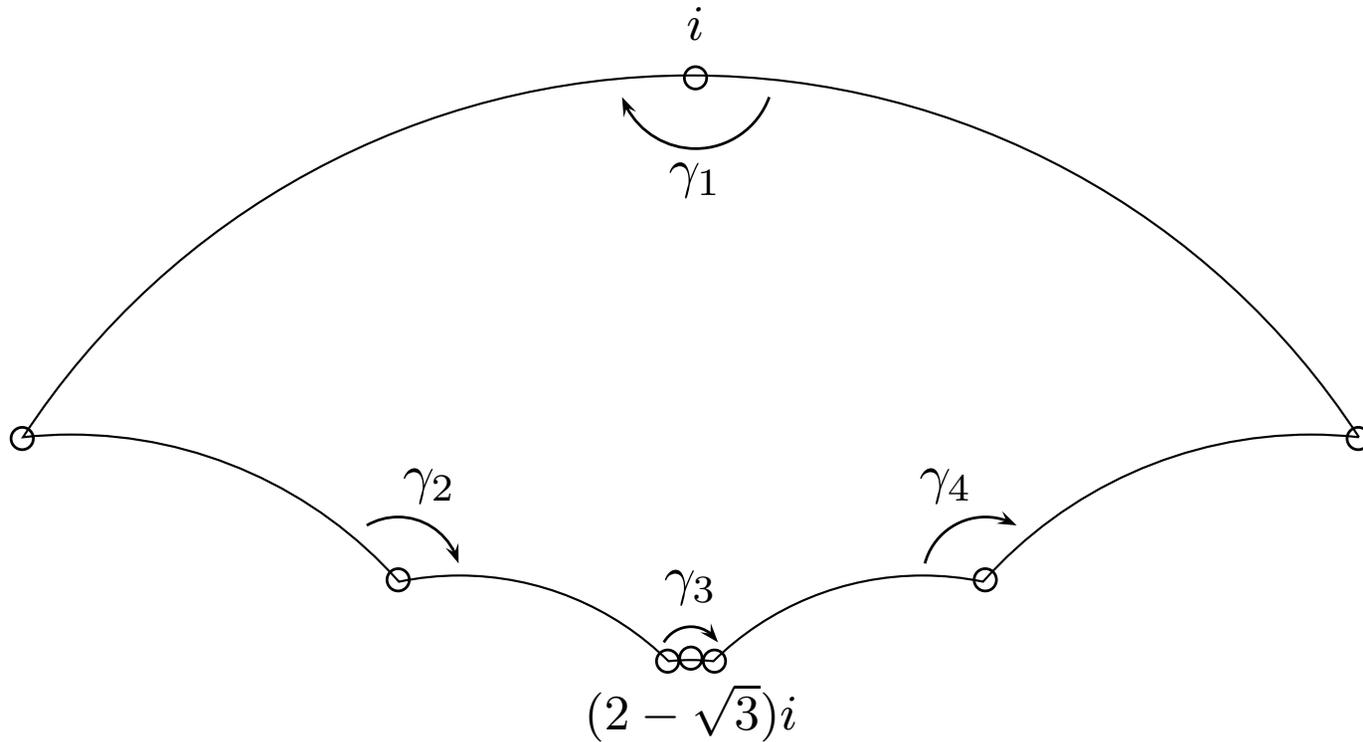
$$P = \{(g, s, s^*) : s^* = g(s)\} \subset \Gamma \times (S \times S).$$

We say that P is a *side pairing* for D if P induces a partition of S into pairs, and we denote by $G(P)$ the projection of P to Γ .

Proposition. *The Dirichlet domain $D(p)$ has a side pairing P , and the set $G(P)$ generates Γ .*

Side pairings: $\Gamma^6(1)$

For the group $\Gamma^6(1)$, we have the following side pairing:



0

1

Algorithm

From now on, we assume that Γ is *exact*, specified by a finite set of generators $G \subset SL_2(K)$ with $K \hookrightarrow \mathbb{R} \cap \overline{\mathbb{Q}}$.

We specify the Dirichlet domain $D(p)$ centered at p by a sequence of vertices, oriented counterclockwise around p . We represent elements of \mathfrak{H} using exact complex arithmetic; in practice, we use fixed (sufficiently large) precision, since round-off errors will occur rarely in practice.

Our main theorem is as follows.

Theorem. *There exists an algorithm which, given a (cofinite, exact) Fuchsian group Γ and a point $p \in \mathfrak{H}$ with $\Gamma_p = \{1\}$, returns the Dirichlet domain $D(p)$, a side pairing for $D(p)$, and a finite presentation for Γ with a minimal set of generators.*

So fundamental domains are good for more than just pictures! This algorithm also provides an efficient solution to the word problem for the computed presentation of Γ .

Arithmetic Fuchsian groups

Let F be a number field with ring of integers \mathbb{Z}_F . A *quaternion algebra* B over F is an F -algebra with generators $\alpha, \beta \in B$ such that

$$\alpha^2 = h, \quad \beta^2 = k, \quad \beta\alpha = -\alpha\beta$$

with $h, k \in F^*$; such an algebra is denoted $B = \left(\frac{h, k}{F} \right)$ and is specified in bits by h, k .

An element $\gamma \in B$ is represented by $\gamma = x + y\alpha + z\beta + w\alpha\beta$ with $x, y, z, w \in F$, and we define the *reduced trace* and *reduced norm* of γ by $\text{trd}(\gamma) = 2x$ and $\text{nrd}(\gamma) = x^2 - hy^2 - kz^2 + hkw^2$.

Let B be a quaternion algebra over F . A place v of F is *split* or *ramified* according as $B \otimes_F F_v \cong M_2(F_v)$ or not, where F_v denotes the completion of F at v . The product of all ramified finite primes $\mathfrak{p} \subset \mathbb{Z}_F$ is the *discriminant* of B .

Arithmetic Fuchsian groups

Let \mathbb{Z}_F denote the ring of integers of F . An *order* $\mathcal{O} \subset B$ is a finitely generated \mathbb{Z}_F -submodule with $F\mathcal{O} = B$ which is also subring; an order is *maximal* if it is not properly contained in any other order. We represent an order by a *pseudobasis* over \mathbb{Z}_F .

Suppose that F is a totally real field and that B is split at exactly one real place corresponding to $\iota_\infty : B \hookrightarrow M_2(\mathbb{R})$. Let $\mathcal{O} \subset B$ be a maximal order and let \mathcal{O}_1^* denote the group of units of reduced norm 1 in \mathcal{O} . The group

$$\Gamma^B(1) = \iota_\infty(\mathcal{O}_1^*/\{\pm 1\}) \subset PSL_2(\mathbb{R})$$

is a cofinite (and hence finitely generated) Fuchsian group.

An *arithmetic Fuchsian group* Γ is a group commensurable with $\Gamma^B(1)$ for some choice of B . One can, for instance, recover the usual modular groups in this way, taking $F = \mathbb{Q}$, $\mathcal{O} = M_2(\mathbb{Z}) \subset M_2(\mathbb{Q}) = B$, and $\Gamma \subset PSL_2(\mathbb{Z})$ a subgroup of finite index.

Applications: Group invariants, automorphic forms

As a first application, we compute invariants of Γ . The group Γ has finitely many orbits with nontrivial stabilizer, known as *elliptic cycles* and *parabolic cycles* according as the stabilizer is finite or infinite. The coset space $X = \Gamma \backslash \mathfrak{H}$ can be given the structure of a Riemann surface, and we say that Γ has *signature* $(g; m_1, \dots, m_t; s)$ if X has genus g and Γ has t elliptic cycles of orders m_1, \dots, m_t and s parabolic cycles.

Corollary. *There exists an algorithm which, given a Fuchsian group Γ returns the signature of Γ and a set of representatives for the elliptic and parabolic cycles in Γ .*

For example, $\Gamma^6(1)$ has signature $(0; 2, 2, 3, 3; 0)$.

Next, we give an application relevant to the evaluation of automorphic forms (to high precision).

Corollary. *There exists an algorithm which, given a Fuchsian group Γ and $z, p \in \mathfrak{H}$ with $\Gamma_p = \{1\}$, returns a point $z' \in \mathfrak{H}$ and $g \in \Gamma$ such that $z' = g(z)$ and $z' \in D(p)$.*

Application: principalization, group cohomology

We obtain from the algorithm a finite presentation with a minimal set of generators for the group \mathcal{O}_1^* , which is a noncommutative generalization of the problem of computing a system of fundamental units of a (totally real) number field.

In analogy with $SL_2(\mathbb{Z})$, this is likely to yield an explicit method for the principalization of right ideals in \mathcal{O} or equivalently a reduction theory for quaternary quadratic forms arising in this context.

In joint work with Matt Greenberg (Calgary), we use the solution to the word problem corresponding to this explicit reduction theory to compute the action of the Hecke operators on the cohomology group $H^1(\Gamma, \mathbb{Z})$, which (modulo torsion) encodes the space of modular forms on Γ of weight 2. In this way, one obtains explicit q -expansions for modular forms associated to (modular) elliptic curves over totally real fields!

Isometric circles

Our algorithms work in the hyperbolic unit disc \mathfrak{D} . We map $\phi : \mathfrak{H} \rightarrow \mathfrak{D}$ with $p \mapsto 0$. We transfer the notion of Dirichlet domain so $\phi(D(p)) = D(0)$. To ease notation, we identify Γ with $\Gamma^\phi = \phi\Gamma\phi^{-1} \subset SU(1, 1)$.

A matrix $g = \begin{pmatrix} a & c \\ \bar{c} & \bar{a} \end{pmatrix} \in SU(1, 1)$ multiplies lengths by $|g'(z)| = |\bar{c}z + \bar{a}|^{-2}$. Thus, Euclidean lengths (and areas) are preserved if and only if $|\bar{c}z + \bar{a}| = 1$. We define the *isometric circle* of g to be

$$I(g) = \{z \in \mathbb{C} : |\bar{c}z + \bar{a}| = 1\}.$$

When $c \neq 0$, $I(g)$ is a circle of radius $1/|c|$ and center $-\bar{a}/c$; if $c = 0$, then g fixes p and we have $I(g) = \mathbb{C}$.

Isometric circles

We then have the following alternative description of $D(0)$.

Proposition. *The domain $D(0)$ is the closure in \mathfrak{D} of*

$$\bigcap_{g \in \Gamma \setminus \{1\}} \text{ext}(I(g)),$$

where *ext* (resp. *int*) denotes the exterior (resp. interior).

For $G \subset \Gamma$, we define $\text{ext}(G) = \bigcap_{g \in G \setminus \{1\}} \text{ext}(I(g))$, so that $D(0)$ is the closure of $\text{ext}(\Gamma)$. By definition

$$D(0) = \{z \in \mathfrak{D} : d(z, 0) \leq d(gz, 0) \text{ for all } g \in \Gamma\}.$$

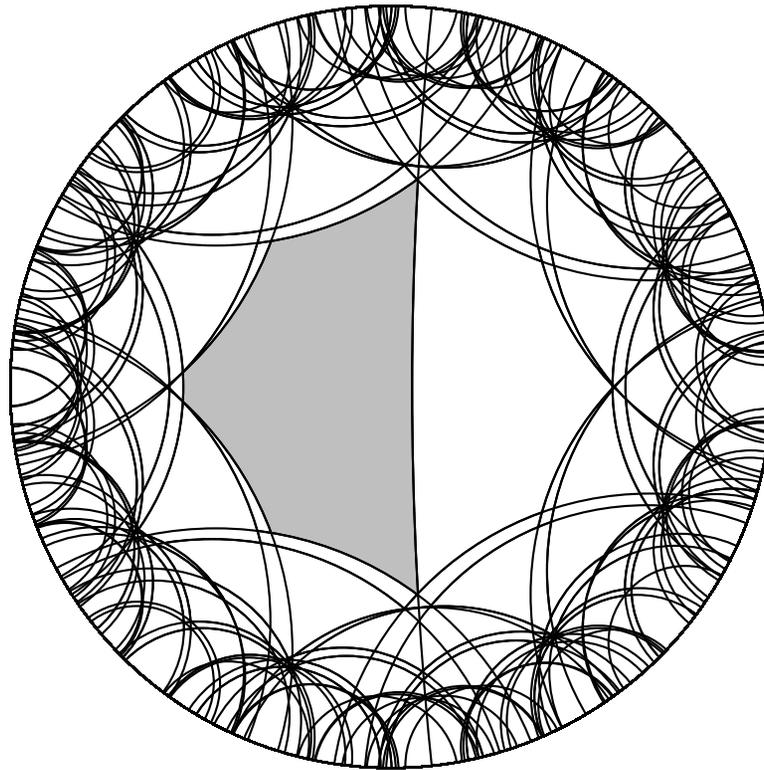
so the above proposition follows from the following lemma.

Lemma. *For any $g \in SU(1, 1)$, we have*

$$d(z, 0) \begin{cases} < \\ = \\ > \end{cases} d(gz, 0) \text{ according as } \begin{cases} z \in \text{ext}(I(g)), \\ z \in I(g), \\ z \in \text{int}(I(g)). \end{cases}$$

Isometric circles: $\Gamma_6(1)$

Those $g \in \Gamma$ with isometric circle $I(g)$ having sufficiently small radius do not contribute to the Dirichlet domain.



(The Dirichlet domain for the group $\Gamma^6(1)$ associated to the quaternion algebra of discriminant 6.)

Inverse radius

We now relate isometric circles to the arithmetic of B . A short calculation shows that if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, then the isometric circle of $g^\phi = \phi g \phi^{-1} \in SU(1, 1)$ has radius $\frac{2 \operatorname{Im}(p)}{|f_g(p)|}$, where

$$f_g(t) = ct^2 + (d - a)t - b$$

is the polynomial whose roots are the fixed points of g .

The map

$$\operatorname{invrad} : M_2(\mathbb{R}) \rightarrow \mathbb{R}$$

$$g \mapsto \frac{2}{\operatorname{rad}(g)^2} + \det(g)$$

is a positive definite quadratic form on $M_2(\mathbb{R})$: indeed, if $p = i$, then simply

$$\operatorname{invrad} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a^2 + b^2 + c^2 + d^2.$$

Absolute reduced norm

For the real ramified places v of F , the reduced norm form $\text{nrd}_v : B \rightarrow \mathbb{R}$ by $g \mapsto v(\text{nrd}(g))$ is positive definite. Putting these together, we have the *absolute reduced norm*

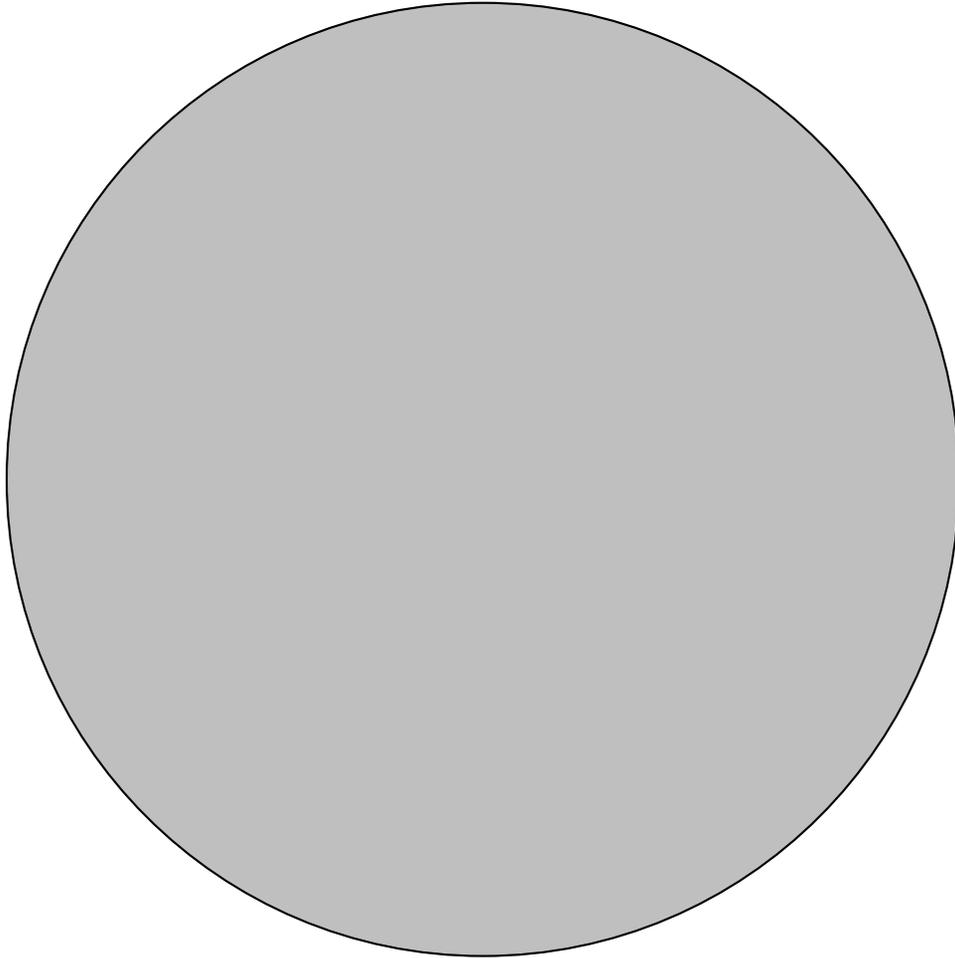
$$N : B \rightarrow \mathbb{R}$$

$$g \mapsto \text{invrad}(g) + \sum_{\substack{v|\infty \\ \text{ramified}}} \text{nrd}_v(g) = \frac{2}{\text{rad}(g)^2} + \text{Tr}_{F/\mathbb{Q}} \text{nrd}(g)$$

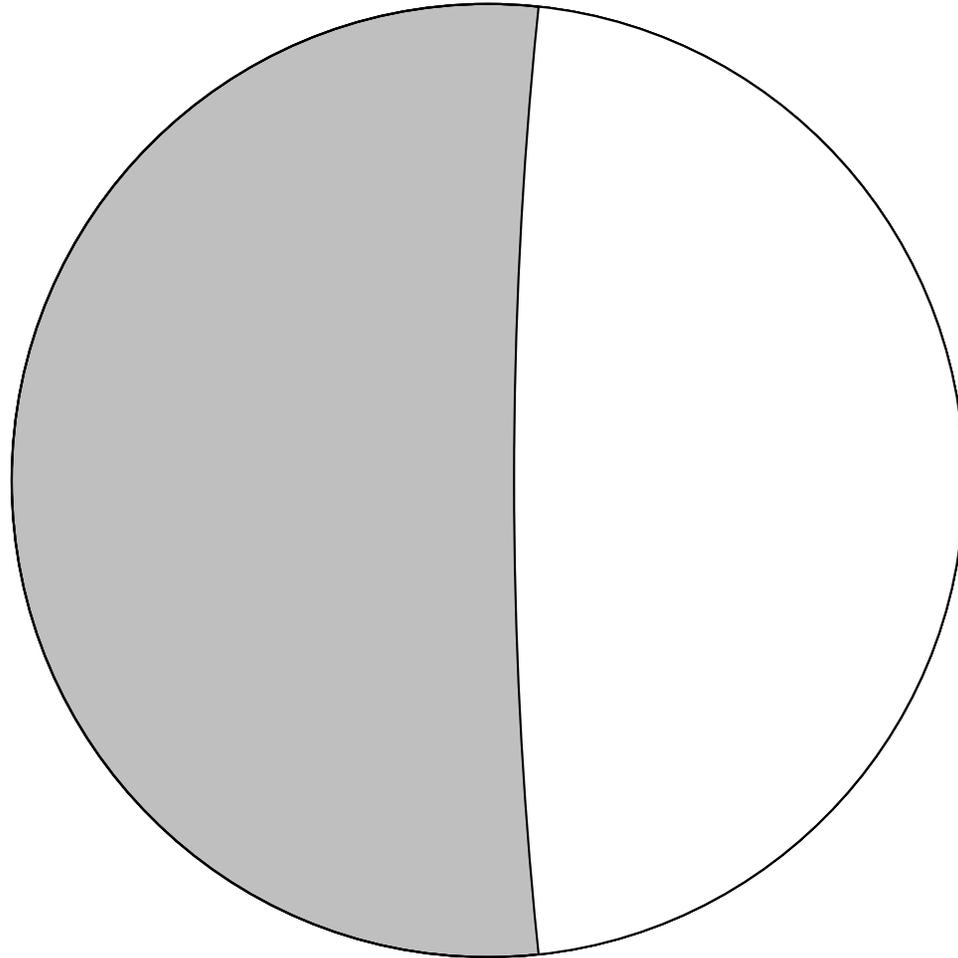
which is positive definite and gives \mathcal{O} the structure of a lattice of rank $4n$.

The elements $g \in \mathcal{O}$ with small absolute reduced norm N are those such that $\text{Tr}_{F/\mathbb{Q}} \text{nrd}(g)$ is small and $\text{rad}(g)$ is large. In particular, this will include those $g \in \mathcal{O}_1^*$ with large $\text{rad}(g)$. Hence, one simple idea to construct $D(0)$ for an arithmetic Fuchsian group would be to enumerate all elements of \mathcal{O}_1^* by increasing N and stop when the exterior of the isometric circles of these elements has area equal to $\mu(\Gamma \backslash \mathfrak{H})$ (which may be computed independently by a formula involving the arithmetic invariants of Γ).

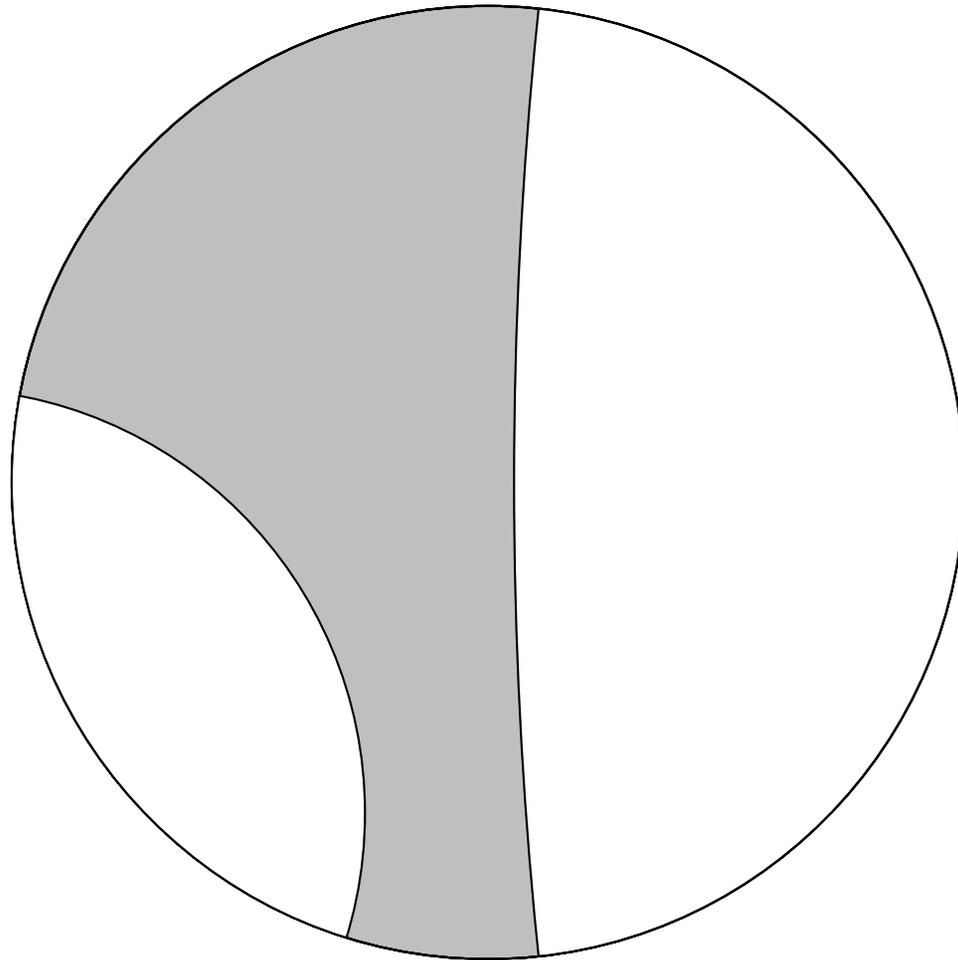
Absolute reduced norm: $\Gamma^6(1)$



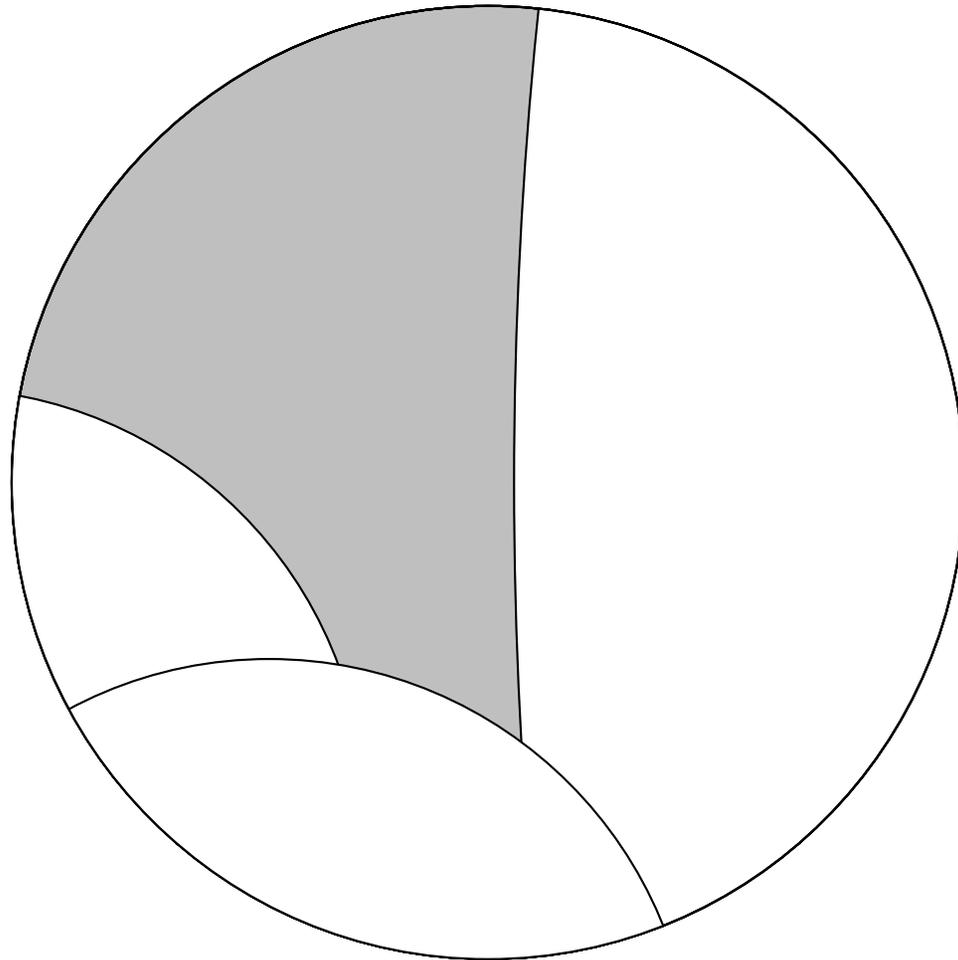
Absolute reduced norm: $\Gamma^6(1)$



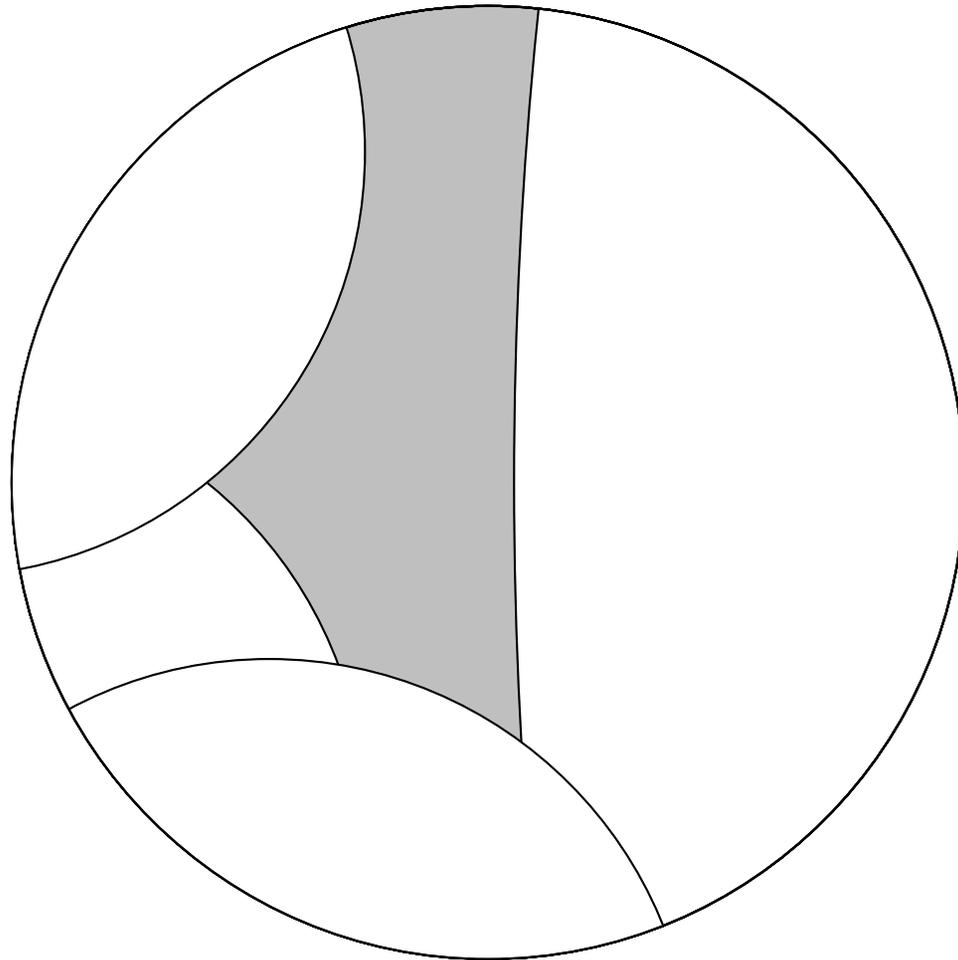
Absolute reduced norm: $\Gamma^6(1)$



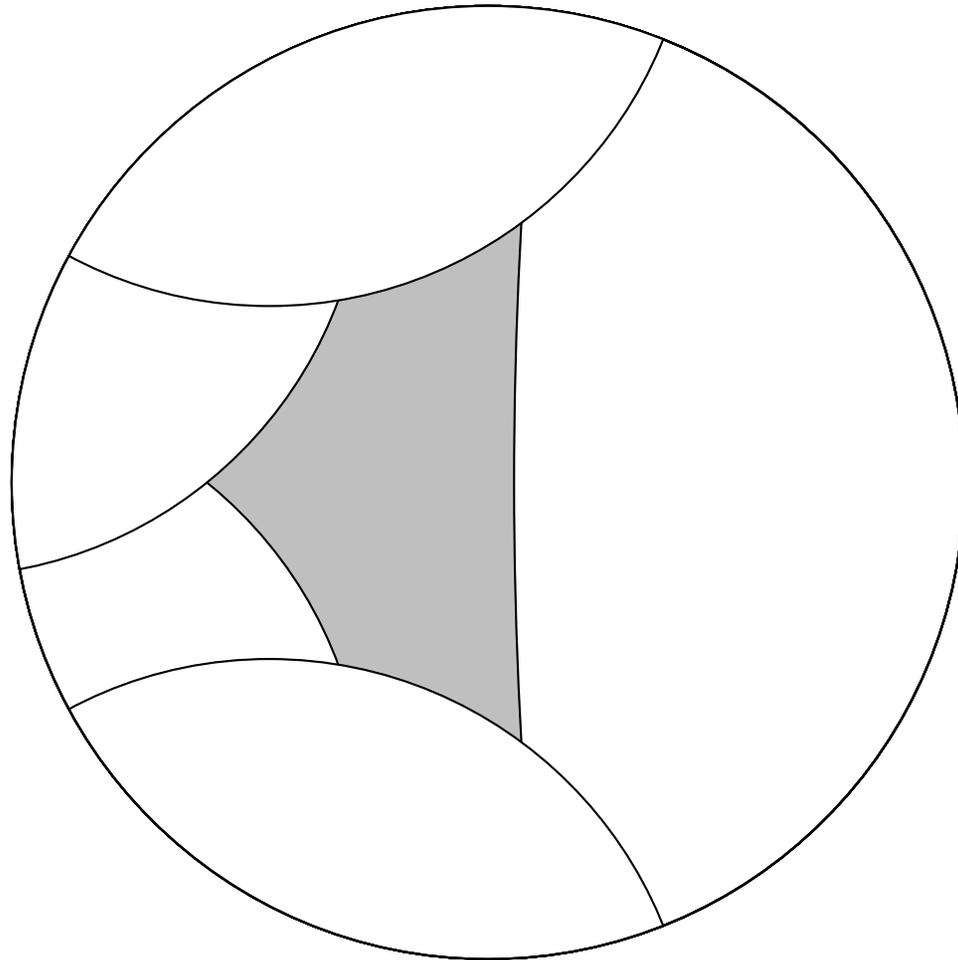
Absolute reduced norm: $\Gamma^6(1)$



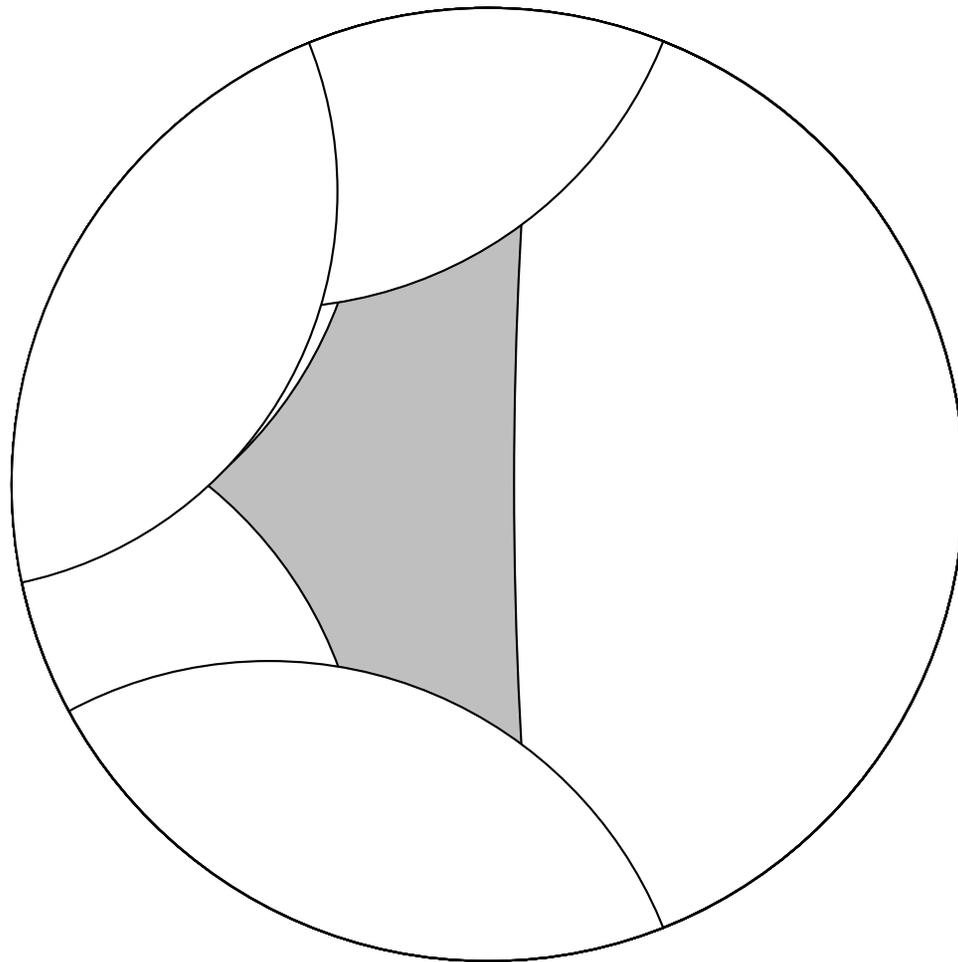
Absolute reduced norm: $\Gamma^6(1)$



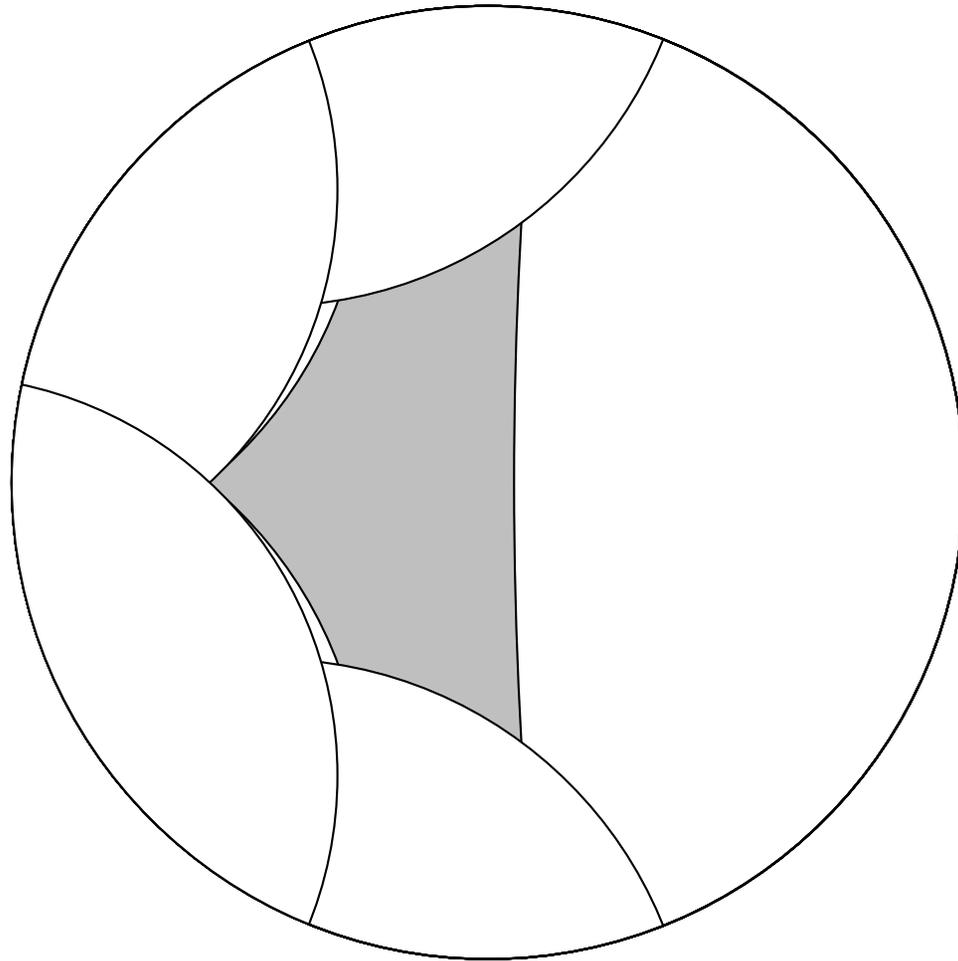
Absolute reduced norm: $\Gamma^6(1)$



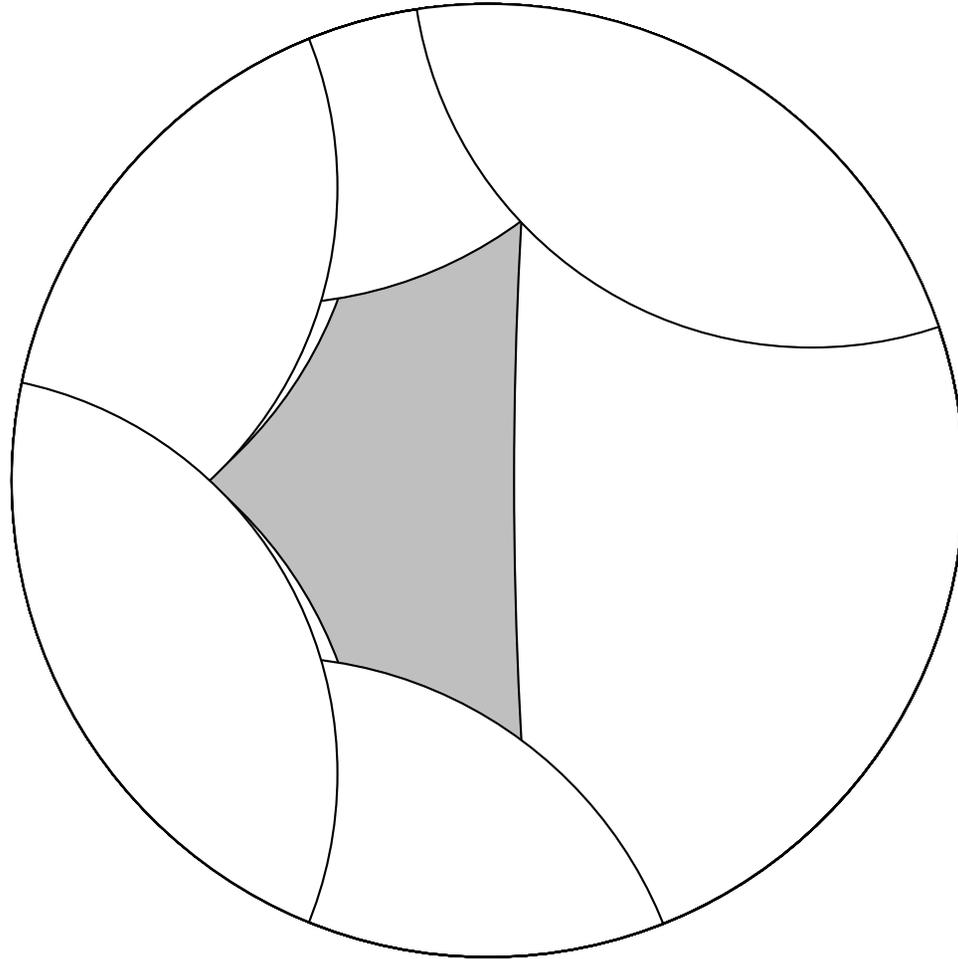
Absolute reduced norm: $\Gamma^6(1)$



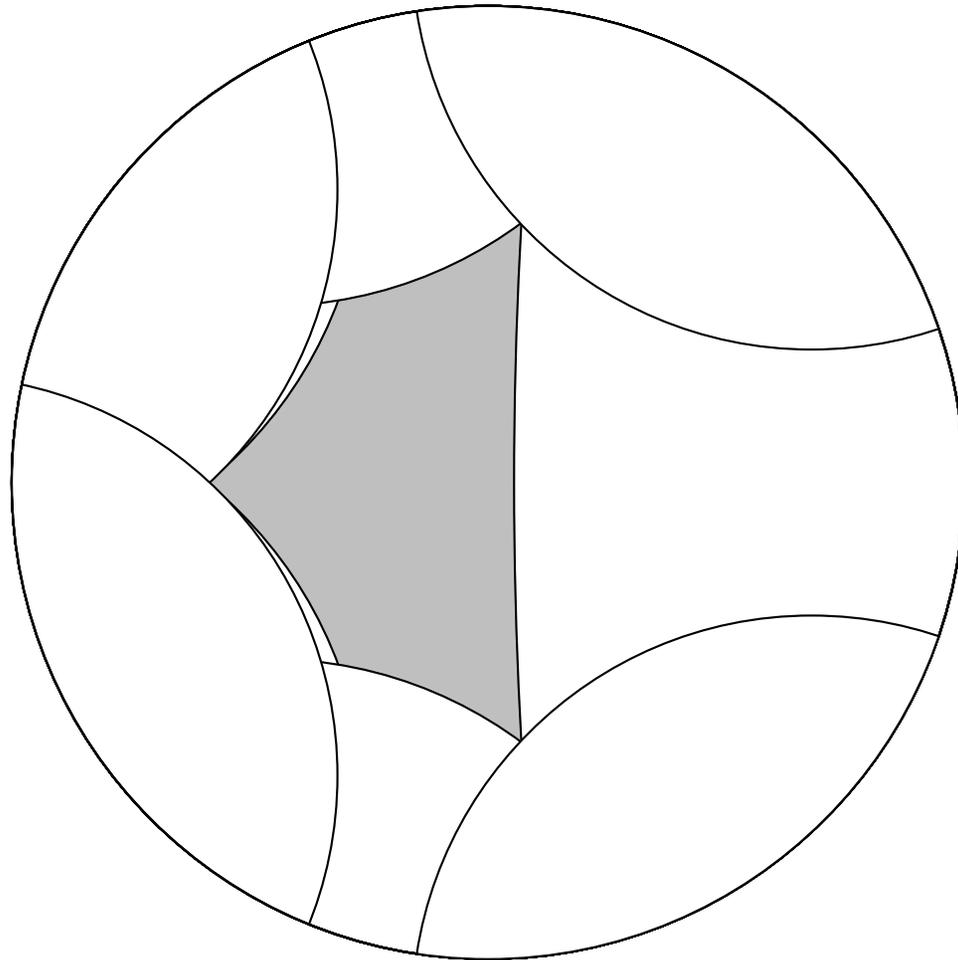
Absolute reduced norm: $\Gamma^6(1)$



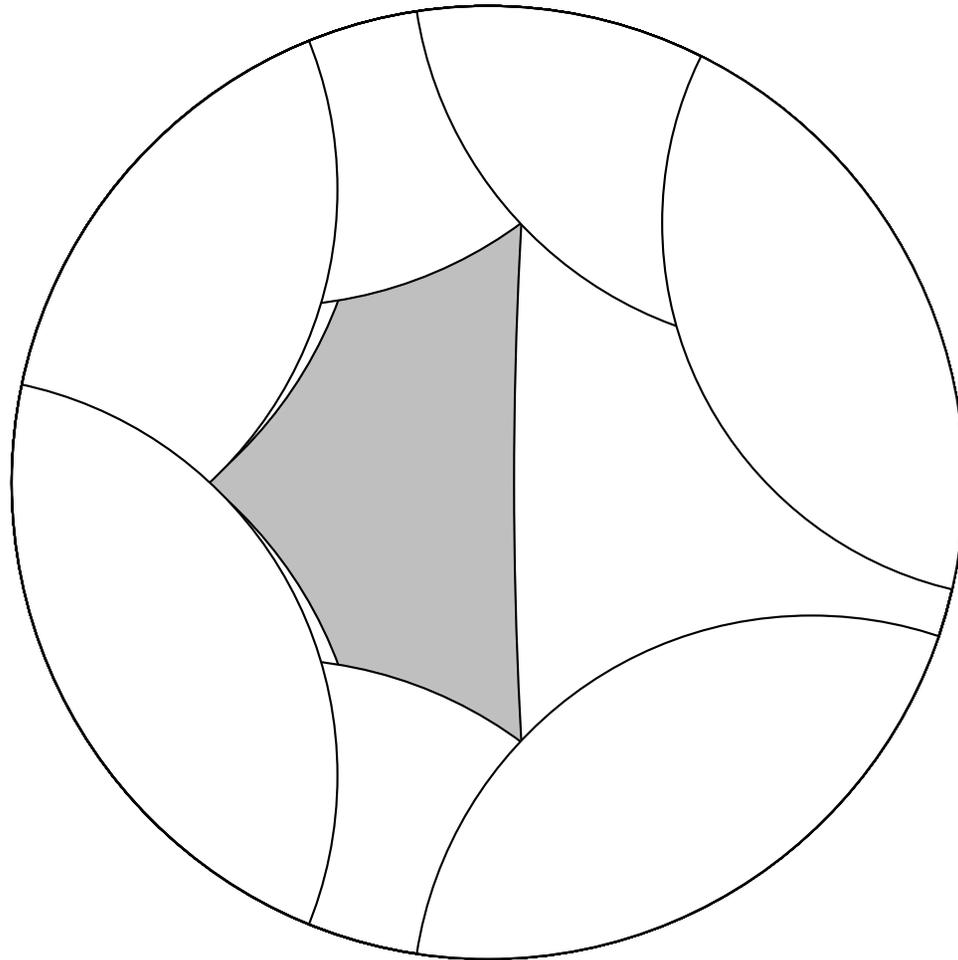
Absolute reduced norm: $\Gamma^6(1)$



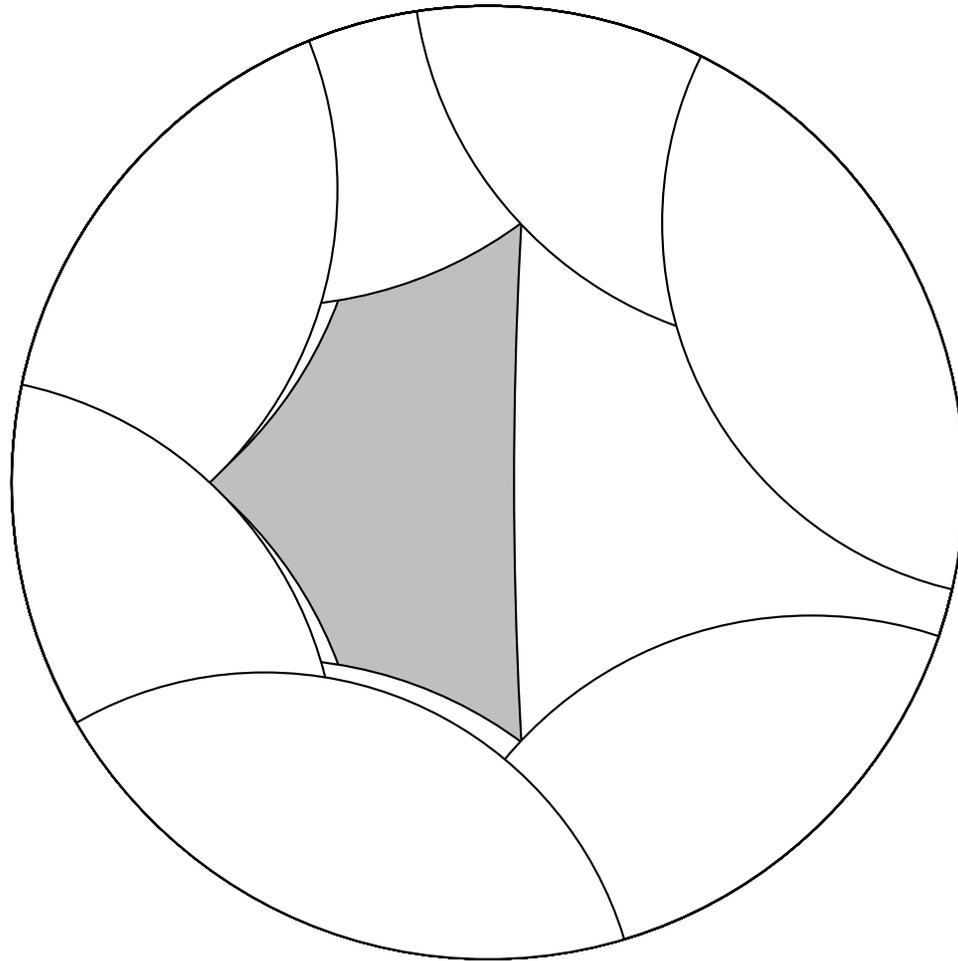
Absolute reduced norm: $\Gamma^6(1)$



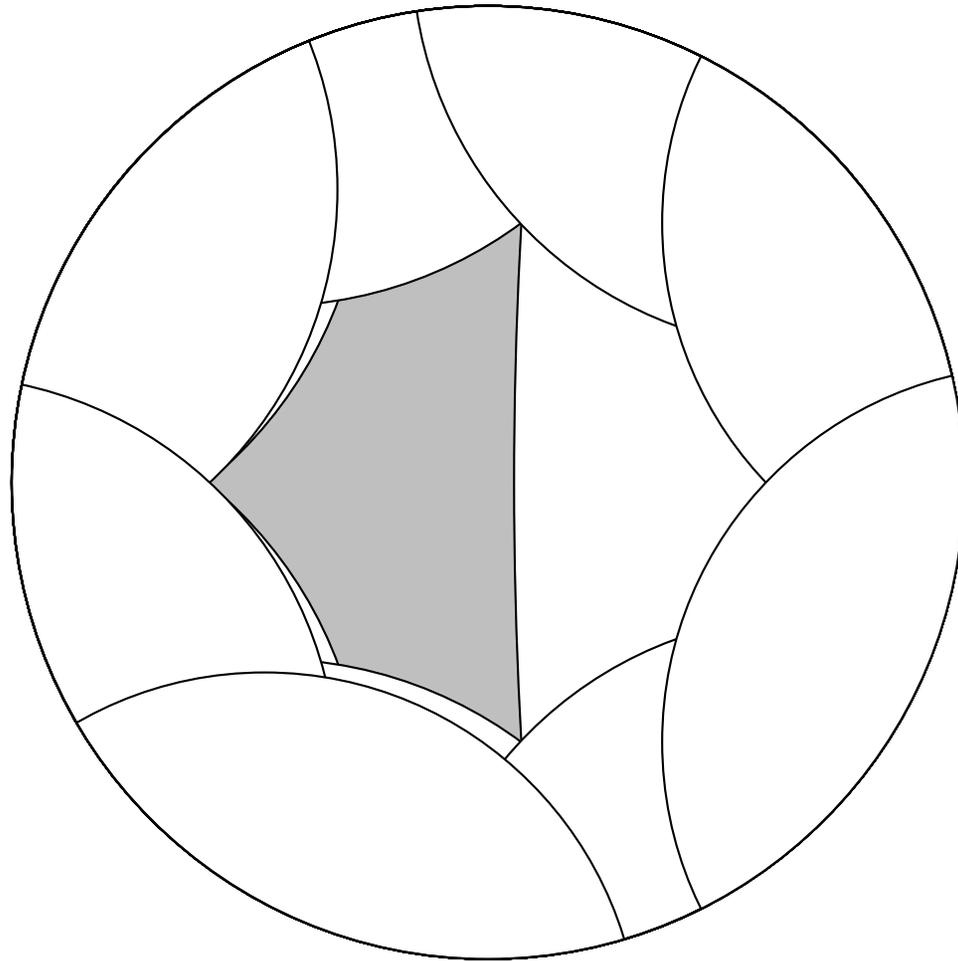
Absolute reduced norm: $\Gamma^6(1)$



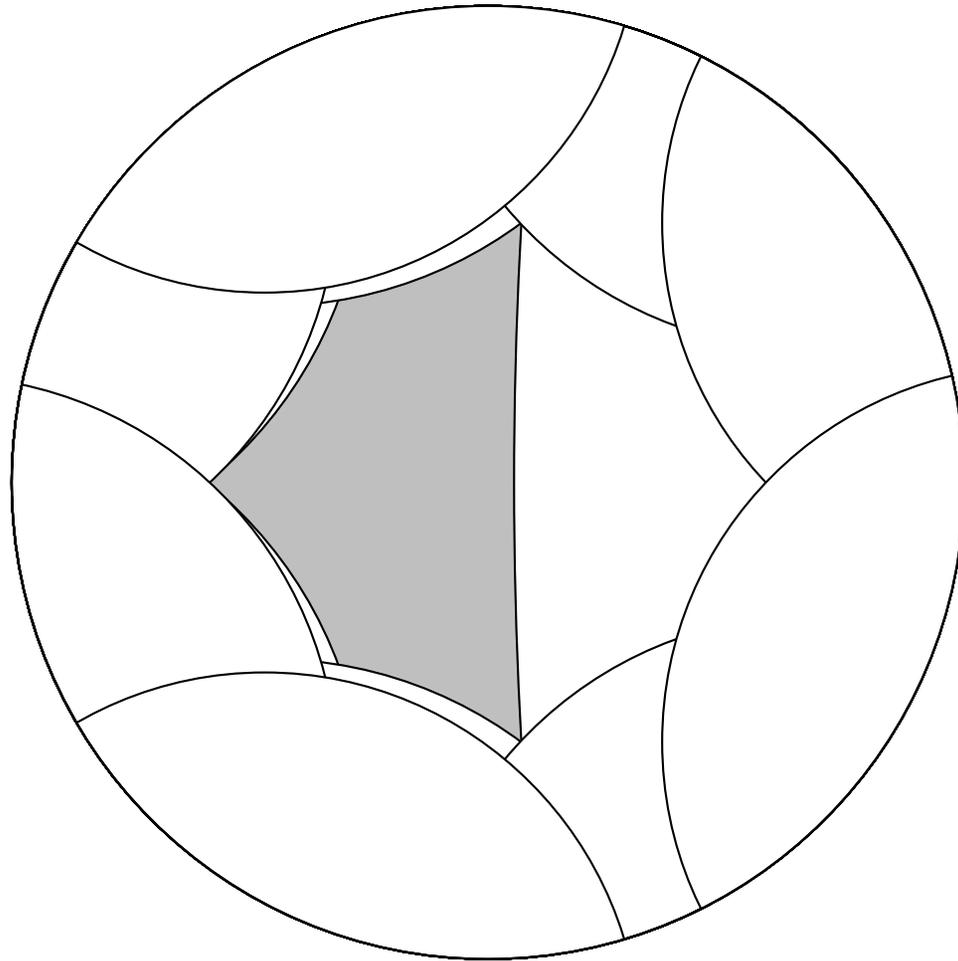
Absolute reduced norm: $\Gamma^6(1)$



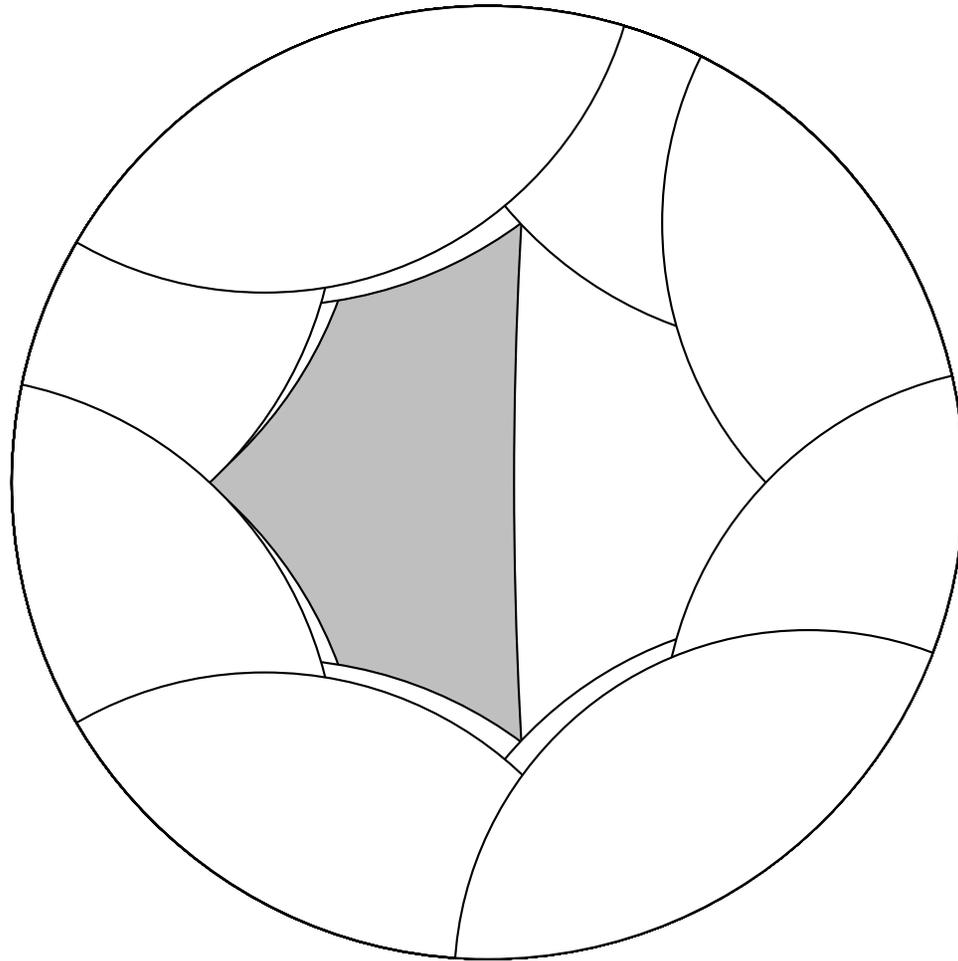
Absolute reduced norm: $\Gamma^6(1)$



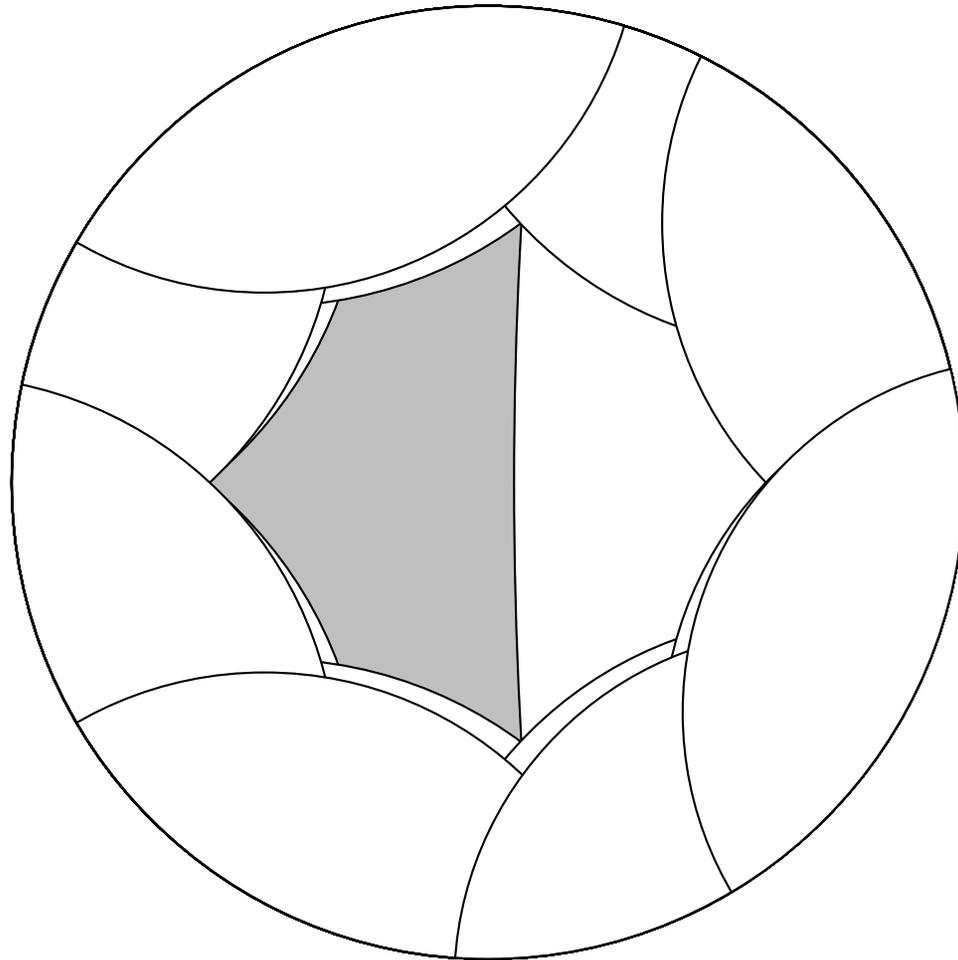
Absolute reduced norm: $\Gamma^6(1)$



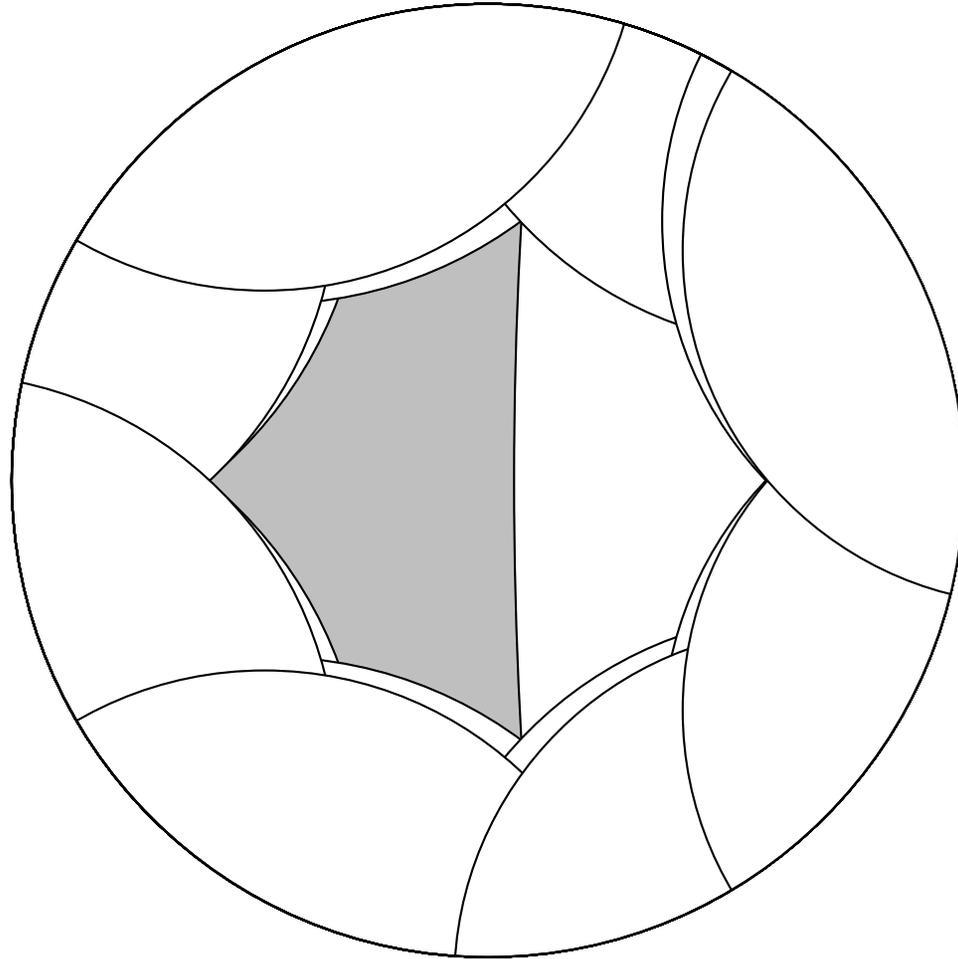
Absolute reduced norm: $\Gamma^6(1)$



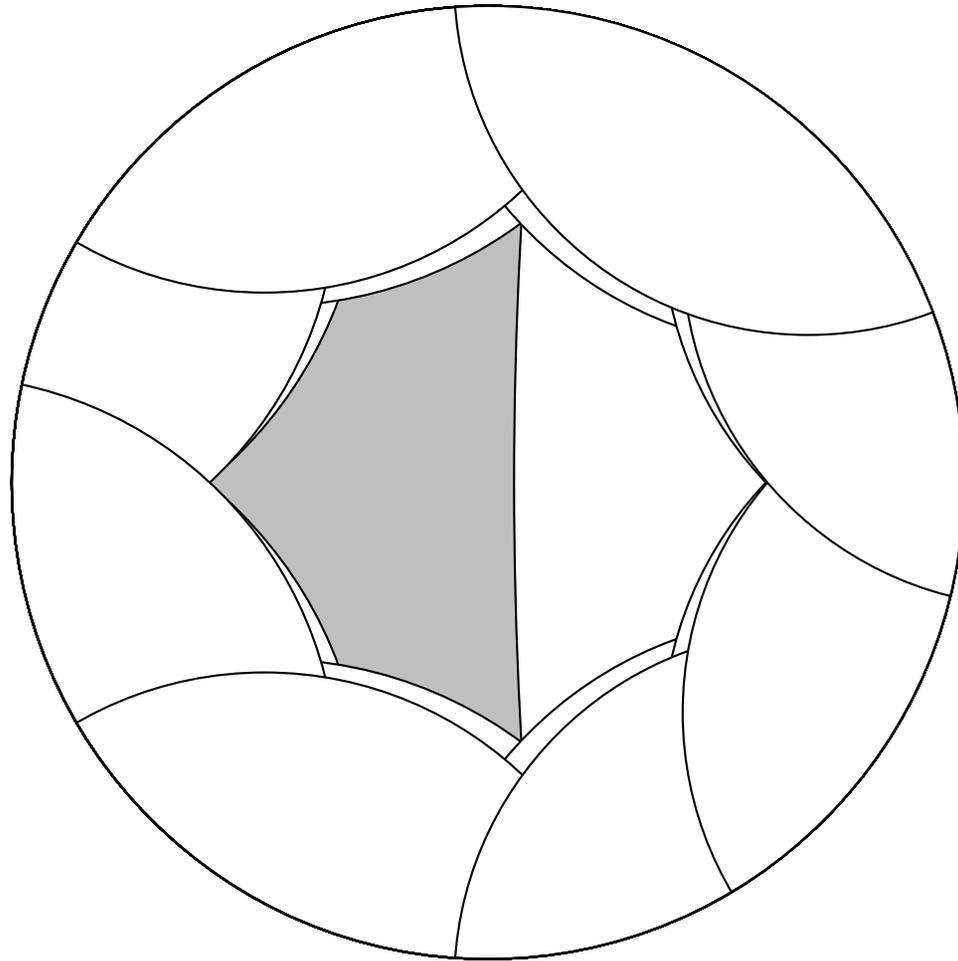
Absolute reduced norm: $\Gamma^6(1)$



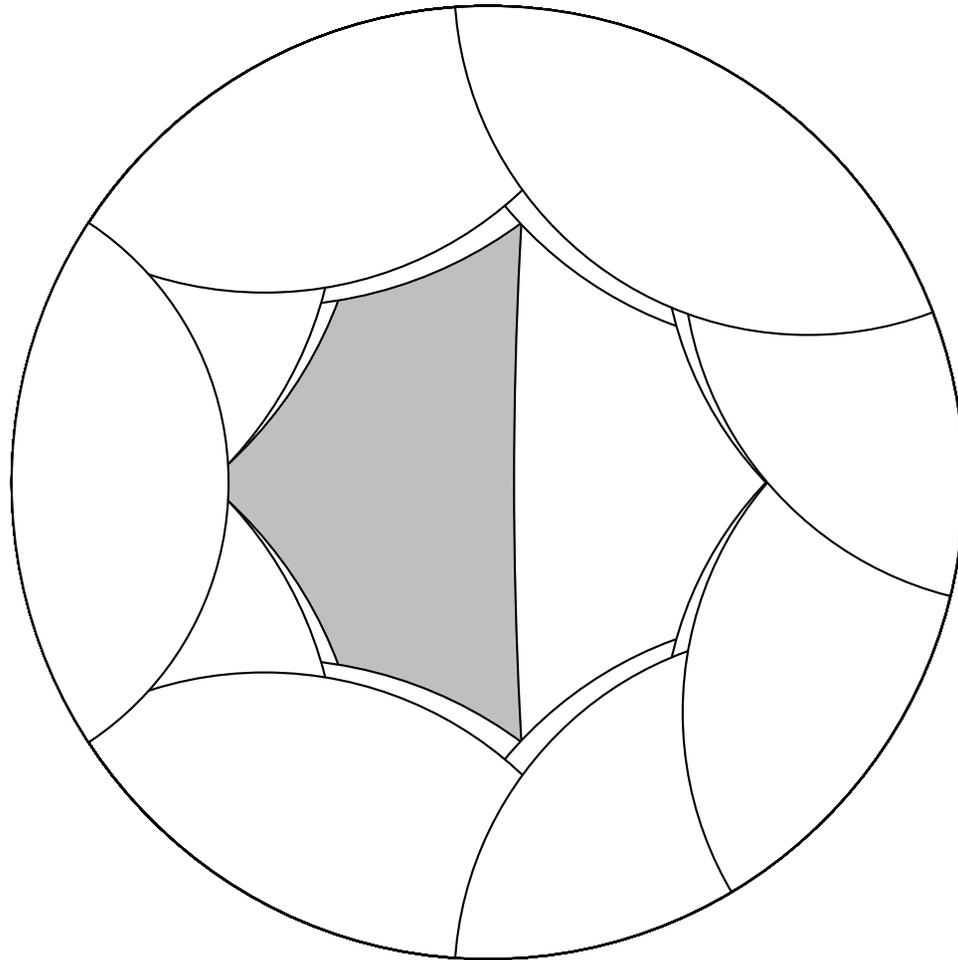
Absolute reduced norm: $\Gamma^6(1)$



Absolute reduced norm: $\Gamma^6(1)$



Absolute reduced norm: $\Gamma^6(1)$



(Finished!)

The reduction algorithm

We can improve upon this naïve algorithm as follows. Recall that

$$d(z, 0) < d(gz, 0) \Leftrightarrow z \in \text{ext}(I(g)).$$

For $z \in \mathfrak{D}$ and $\gamma \in SU(1, 1)$, we define $\rho(\gamma; z) = d(\gamma z, 0) \in \mathbb{R}_{\geq 0}$.

Given a finite subset $G \subset \Gamma \setminus \{1\}$ we say that γ is (G, z) -reduced if for all $g \in G$, we have $\rho(\gamma; z) \leq \rho(g\gamma; z)$. We see that γ is (G, z) -reduced if and only if γz is in the closure of $\text{ext}(G)$.

We have a straightforward algorithm to obtain a (G, z) -reduced element, which we denote $\gamma \mapsto \text{red}_G(\gamma; z)$: if $\rho(\gamma; z) > \rho(g\gamma; z)$ for some $g \in G$, set $\gamma := g\gamma$ and repeat. The algorithm terminates since Γ is discrete.

This reduction is analogous to the generalized division algorithm in a polynomial ring over a field: if G is a Gröbner basis for an ideal I , then $f \in I$ if and only if the remainder on division by f by G is zero.

Proposition. *Suppose that $\text{ext}(G)$ is a fundamental domain for Γ . Then for any $\gamma \in SU(1, 1)$, we have $\text{red}_G(\gamma; 0) = 1$ if and only if $\gamma \in \Gamma$.*

Computing a basis

Proposition. *Suppose that $\text{ext}(G)$ is a fundamental domain for Γ . Then for any $\gamma \in SU(1, 1)$, we have $\text{red}_G(\gamma; 0) = 1$ if and only if $\gamma \in \Gamma$.*

In particular, this gives us an explicit solution to the word problem in Γ .

A set G is a *basis* for Γ if $\text{ext}(G)$ is a fundamental domain for Γ . Our aim then is to construct a basis.

Recall that the Dirichlet domain has a side pairing, and that the set of side pairing elements generates Γ . Since side pairing elements pair vertices, our strategy very roughly runs as follows:

1. $(G, 0)$ -reduce the elements of G .
2. Compute $E = \text{ext}(G)$. If all vertices of E are paired, return G . Otherwise, given a vertex v on $I(g)$ which is not paired, add $\text{red}_G(g; v)$ to G and return to Step 1.

Computing a basis: example

Let F be the (totally real) cubic subfield of $\mathbb{Q}(\zeta_{13})$ with discriminant $d_F = 169$. We have $F = \mathbb{Q}(b)$ where $b^3 + 4b^2 + b - 1 = 0$. F has class number 1.

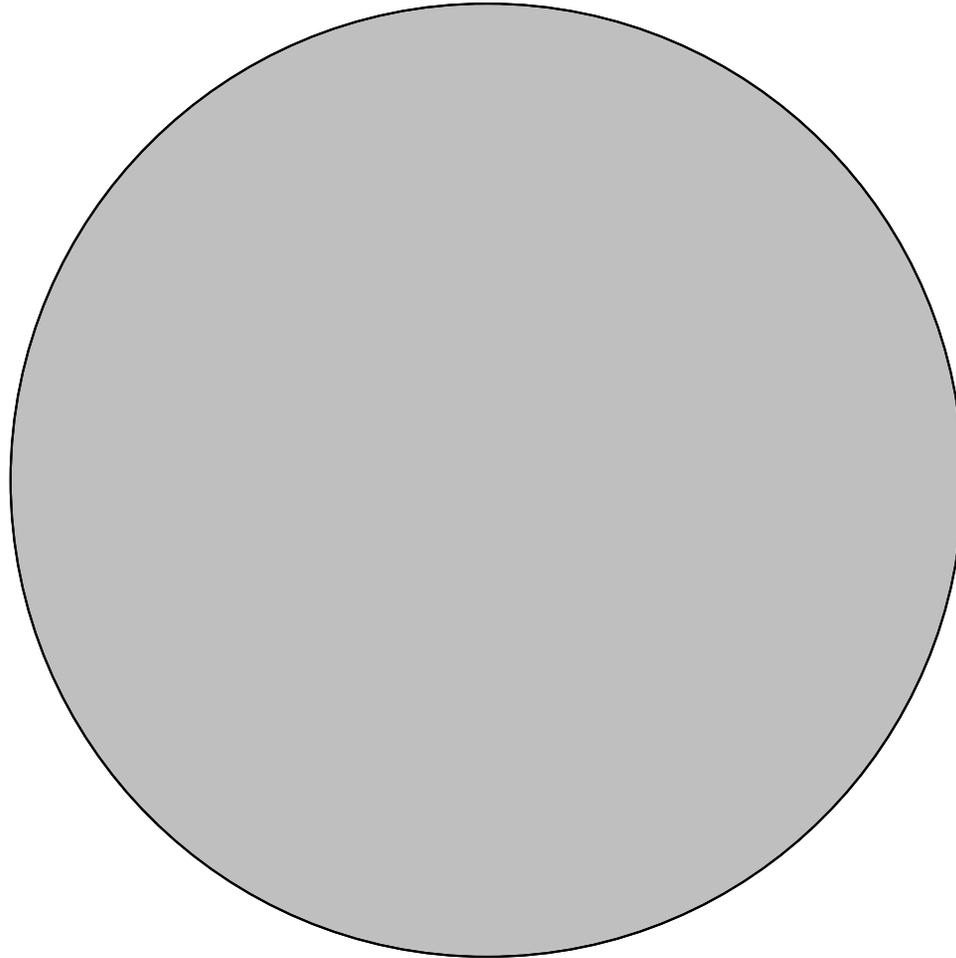
The quaternion algebra $B = \left(\frac{-1, b}{F} \right)$ has discriminant $\mathfrak{D} = (1)$ and is ramified at 2 of the 3 real places of F .

We take \mathcal{O} to be an Eichler order of level $\mathfrak{p} = (b+2)$, a prime ideal of norm 5; explicitly, we have

$$\mathcal{O} = \mathbb{Z}_F \oplus \mathfrak{p}\alpha \oplus \mathbb{Z}_F \frac{b^2 + (b+4)\alpha + \beta}{2} \oplus \mathbb{Z}_F \frac{b + (b^2 + 4)\alpha + \alpha\beta}{2}.$$

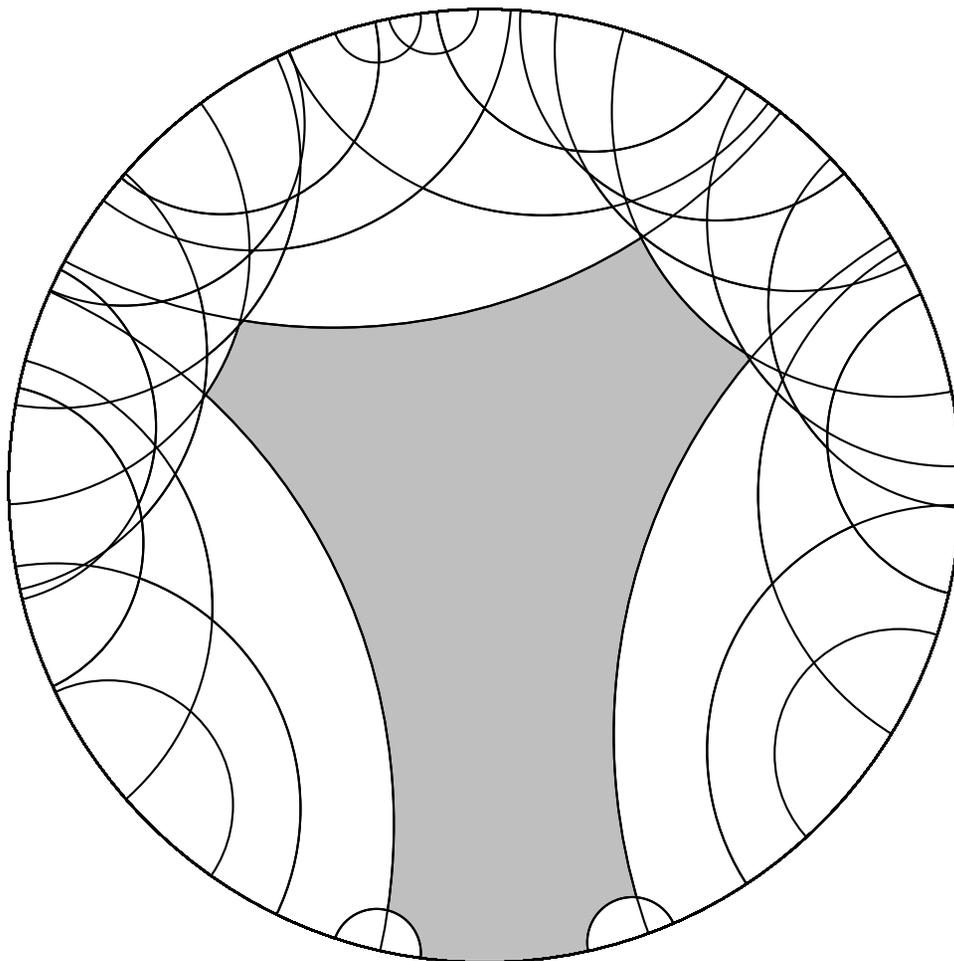
We compute a fundamental domain for the group $\Gamma = \Gamma_0^{(1)}(\mathfrak{p}) = \iota_\infty(\mathcal{O}_1^*)/\{\pm 1\}$. We take $p = 9/10i \in \mathfrak{H}$.

Computing a basis: example



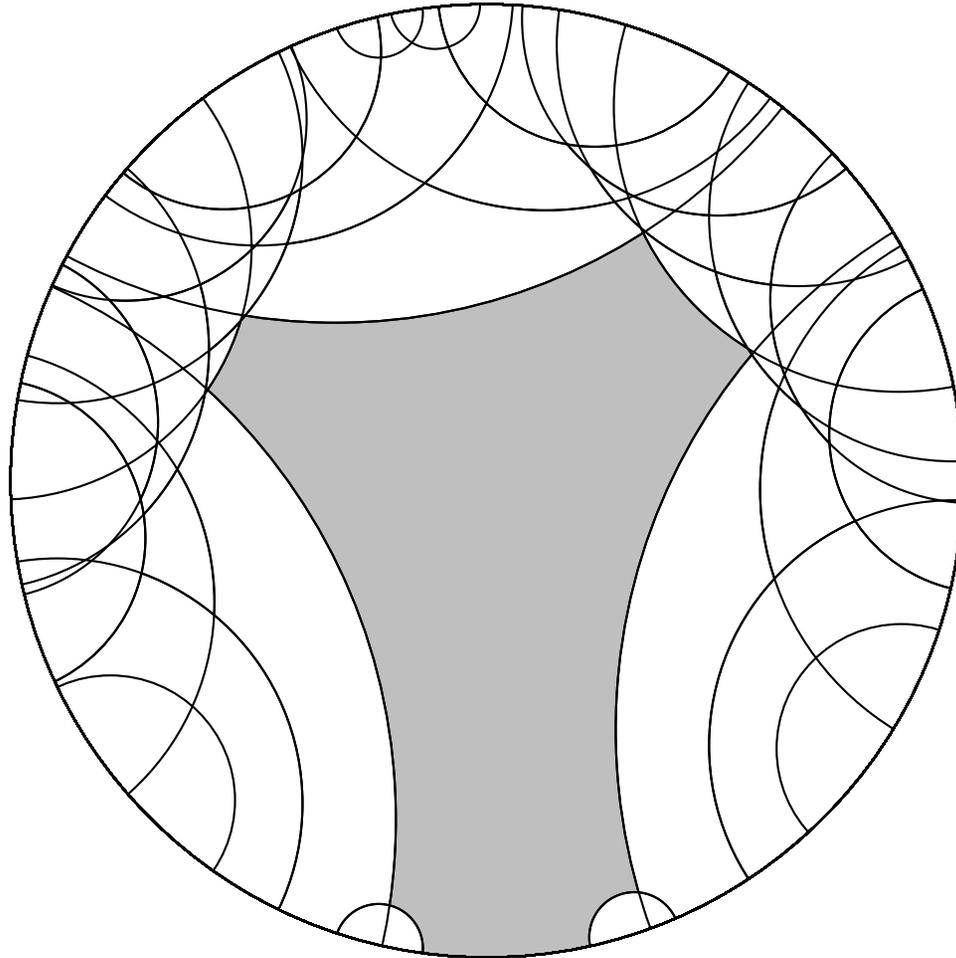
We begin by enumerating elements of \mathcal{O} by their absolute reduced norm. Of the first 260 elements, we find 29 elements of reduced norm 1, yielding the following.

Computing a basis: example



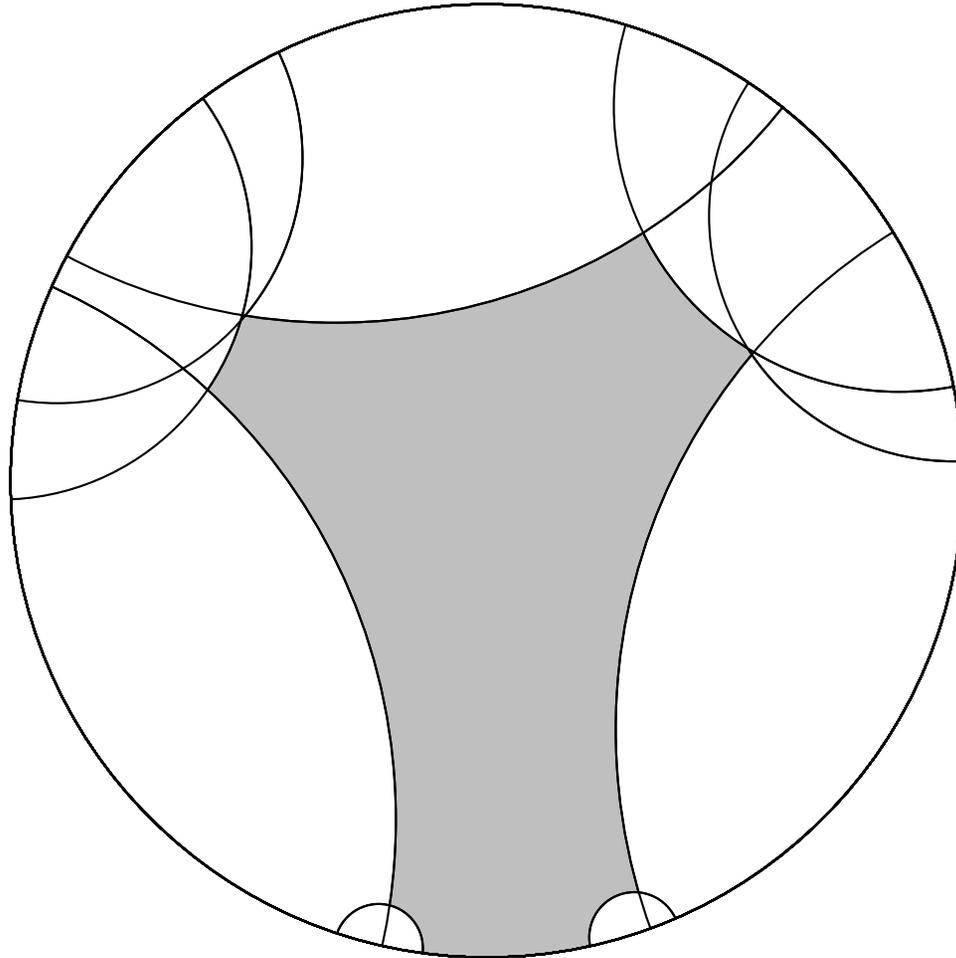
We begin by enumerating elements of \mathcal{O} by their absolute reduced norm. Of the first 260 elements, we find 29 elements of reduced norm 1, yielding the following.

Computing a basis: example



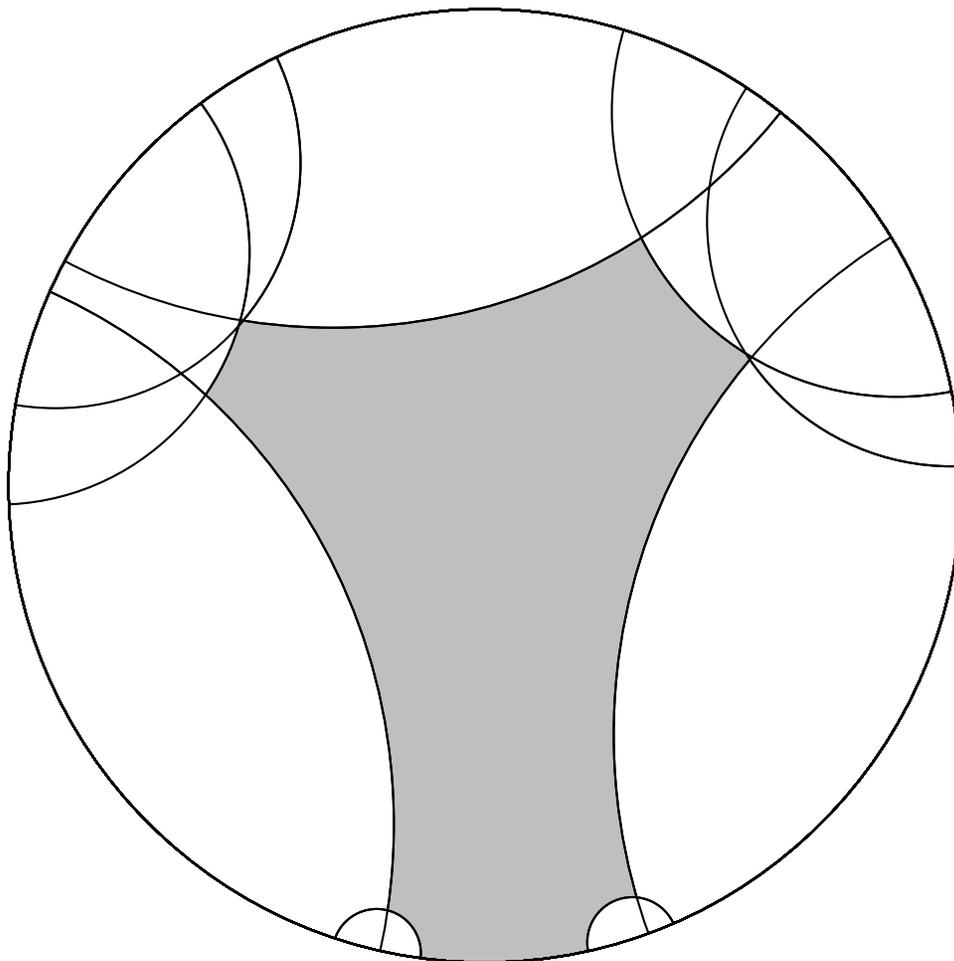
Let G be the set of elements which contribute to the boundary. For each $g \notin G$, we compute $\text{red}_G(g; 0)$. Each in fact reduces to 1, so we are left with 8 elements.

Computing a basis: example



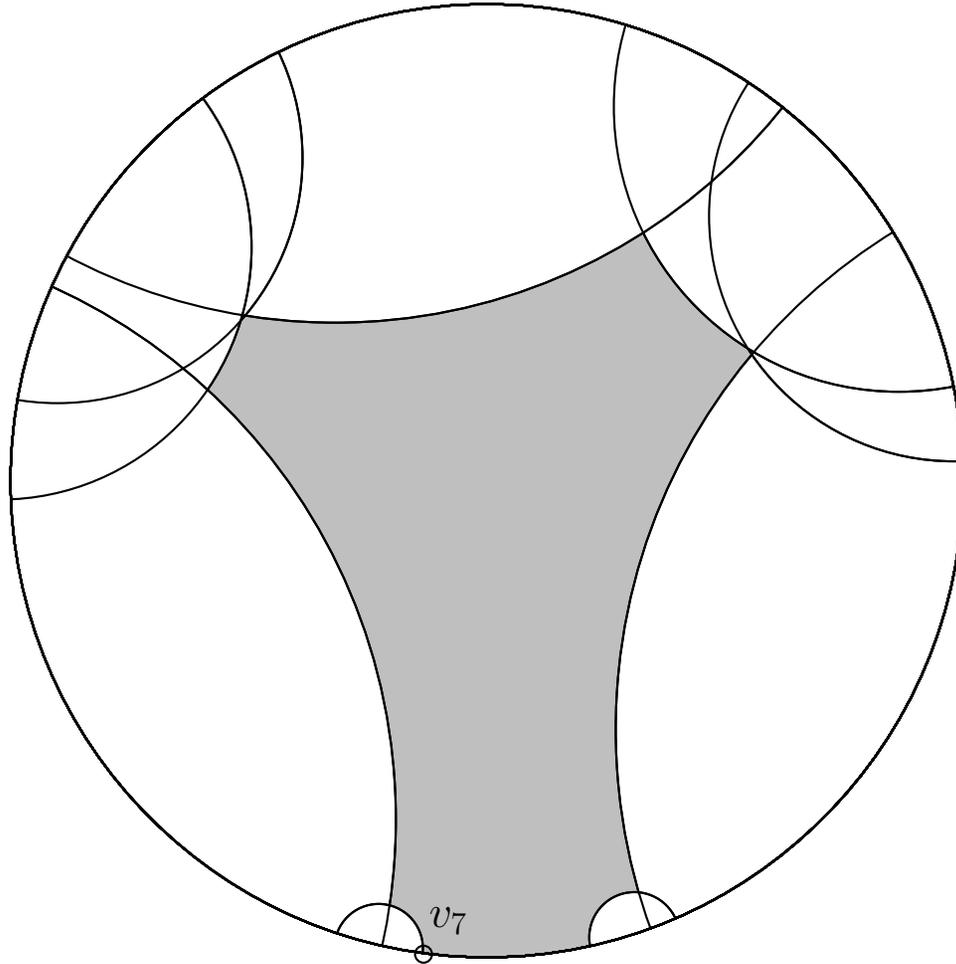
Let G be the set of elements which contribute to the boundary. For each $g \notin G$, we compute $\text{red}_G(g; 0)$. Each in fact reduces to 1, so we are left with 8 elements.

Computing a basis: example



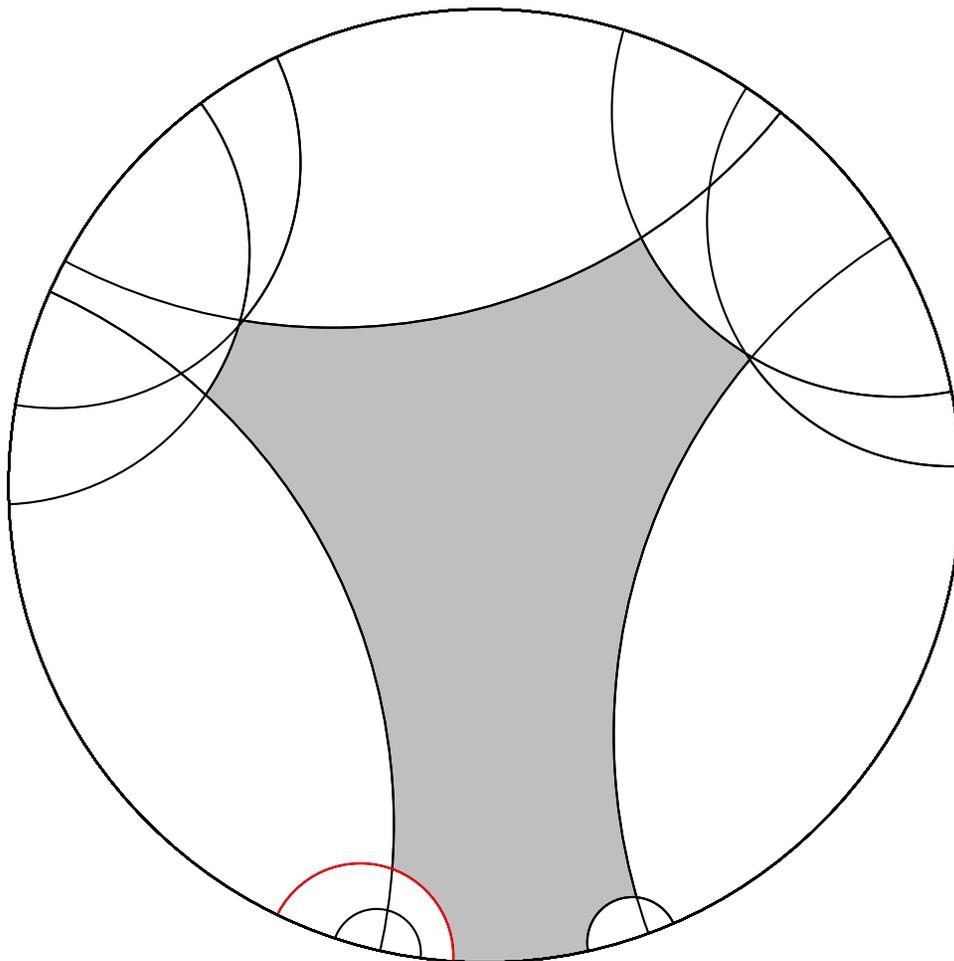
Next, because the domain does not yet have finite area, we enumerate elements of \mathcal{O} by their reduced norm with respect to a point in the direction of the infinite vertex v_7 .

Computing a basis: example



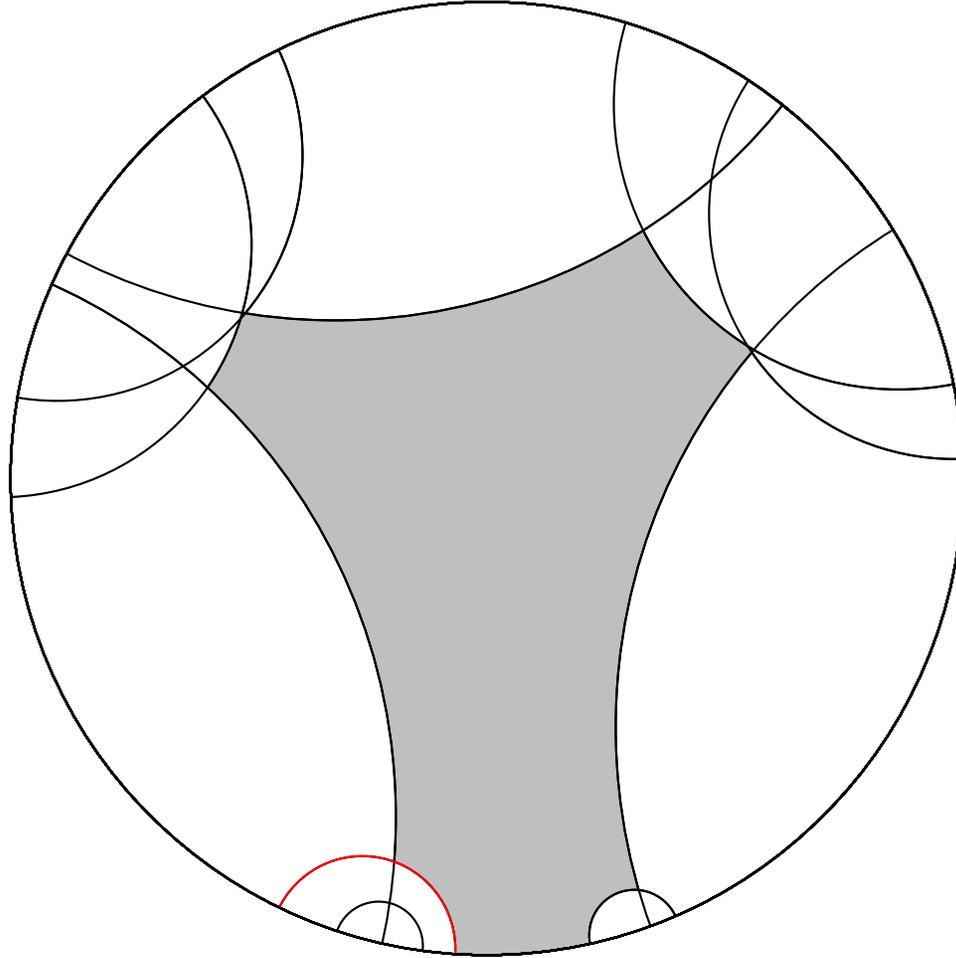
Next, because the domain does not yet have finite area, we enumerate elements of \mathcal{O} by their reduced norm with respect to a point in the direction of the infinite vertex v_7 . We find the following *envelope*.

Computing a basis: example



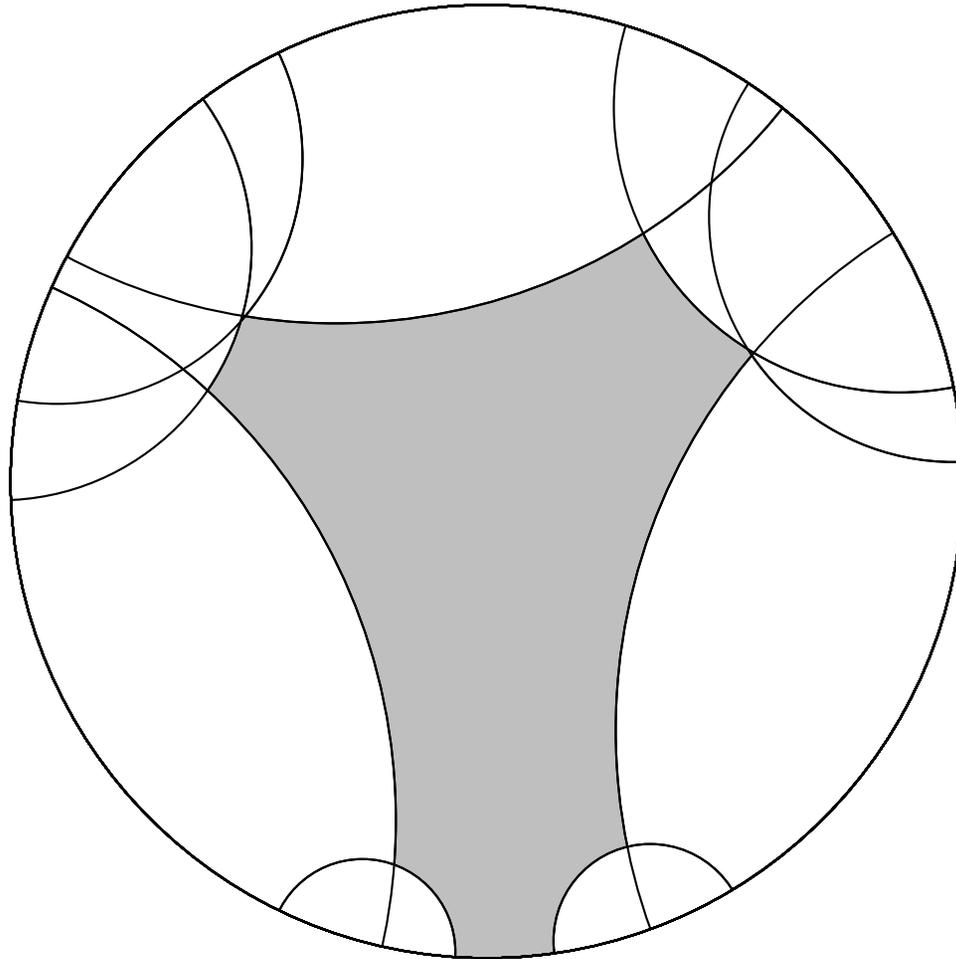
Next, because the domain does not yet have finite area, we enumerate elements of \mathcal{O} by their reduced norm with respect to a point in the direction of the infinite vertex v_7 . We find the following *envelope*.

Computing a basis: example



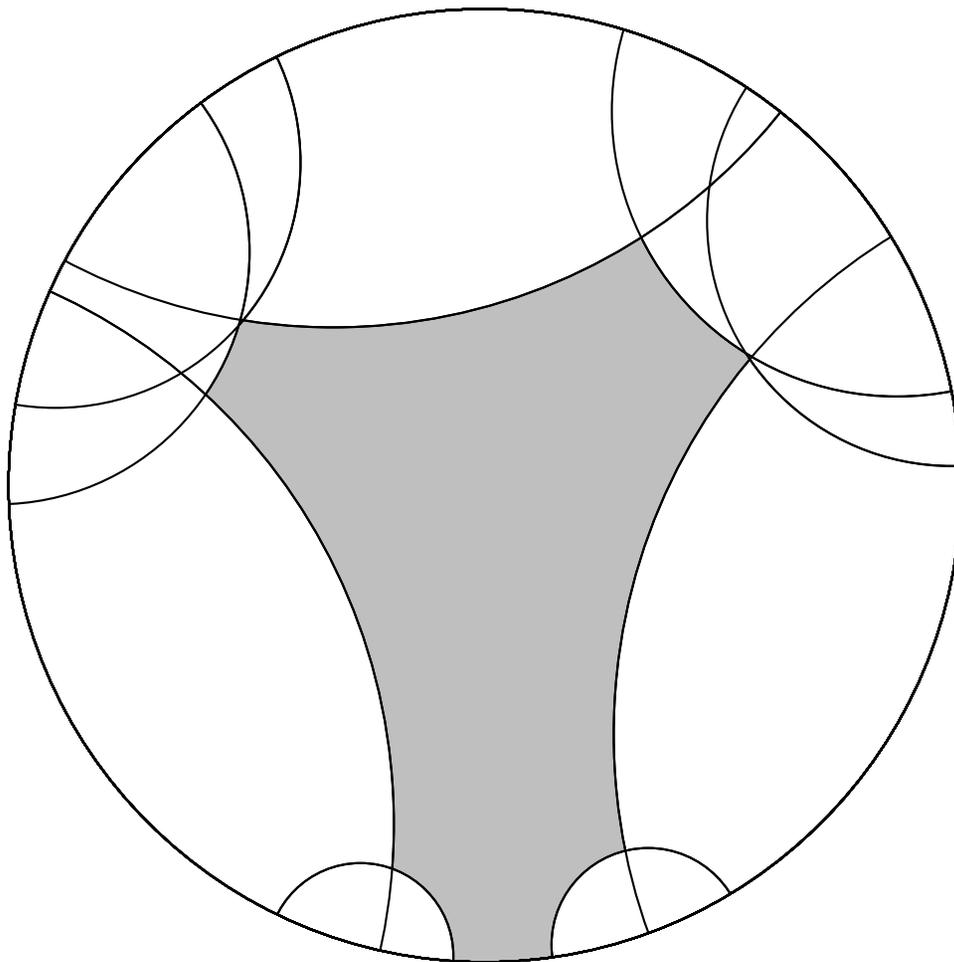
We append the envelope and its inverse.

Computing a basis: example



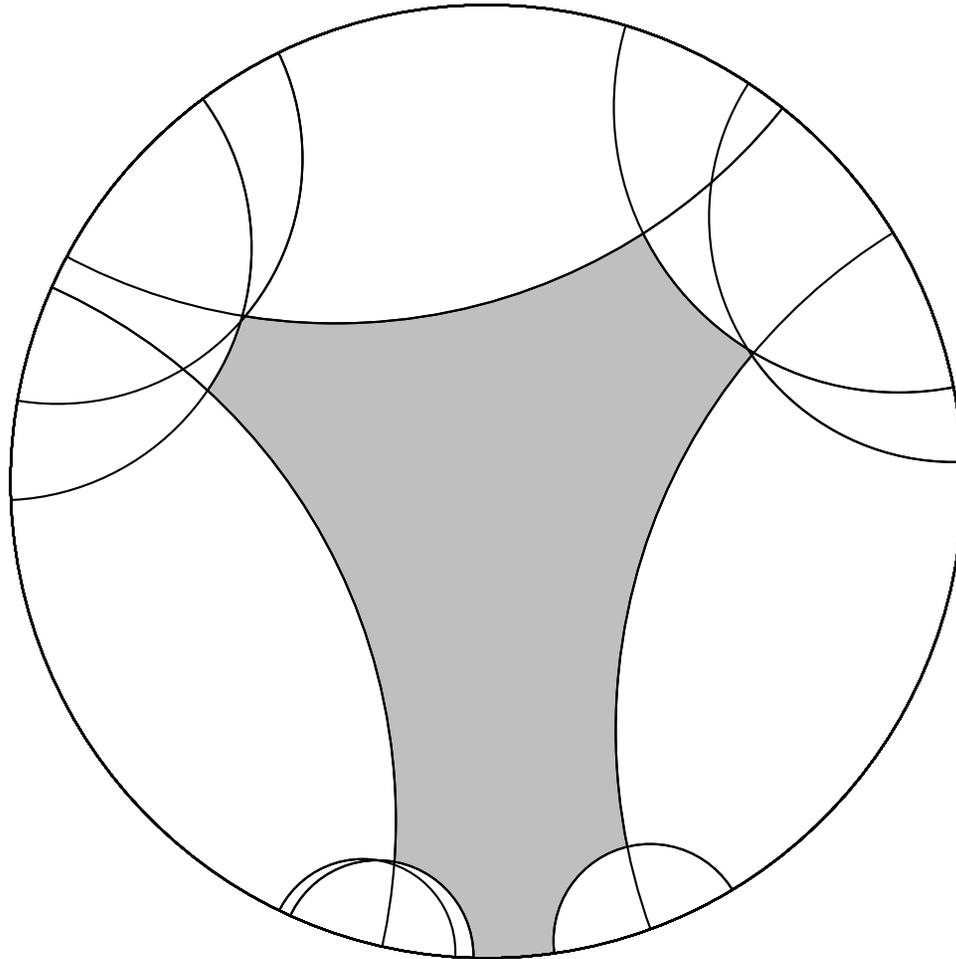
We append the enveloper and its inverse. We then reduce but obtain the same domain.

Computing a basis: example



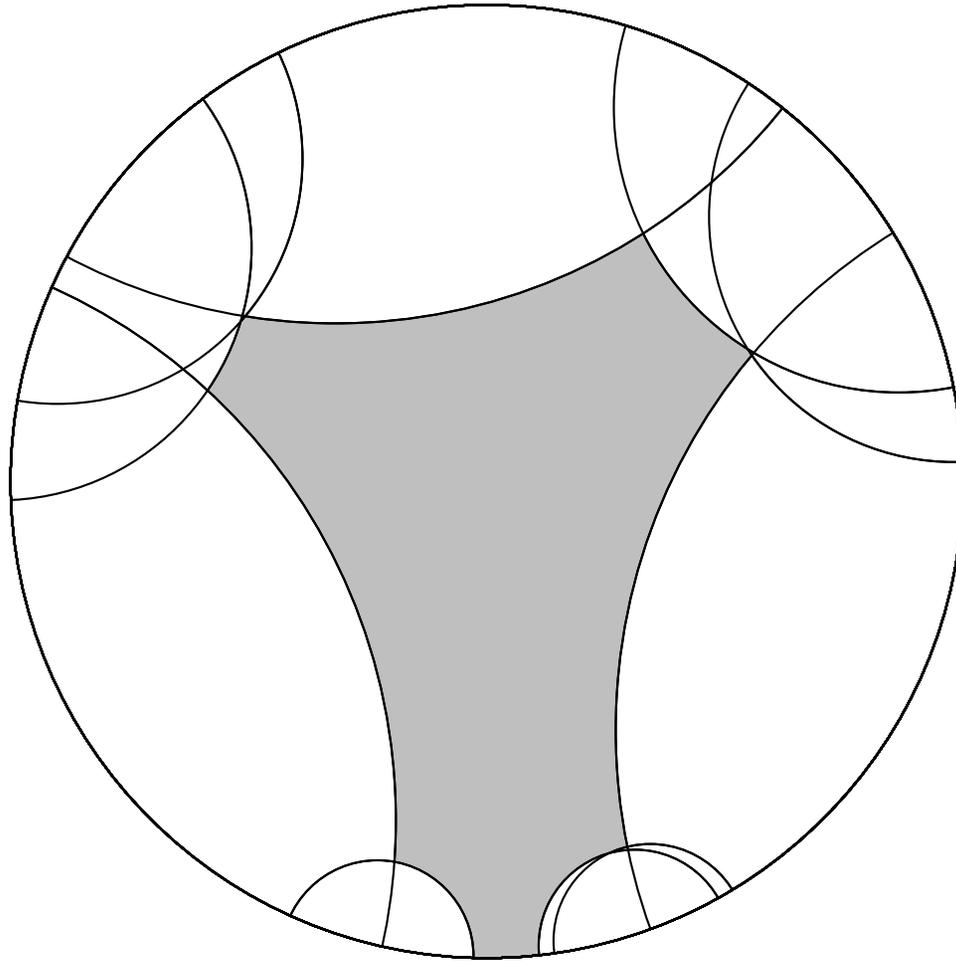
We repeat with the new infinite vertex, finding an envelope and reducing.

Computing a basis: example



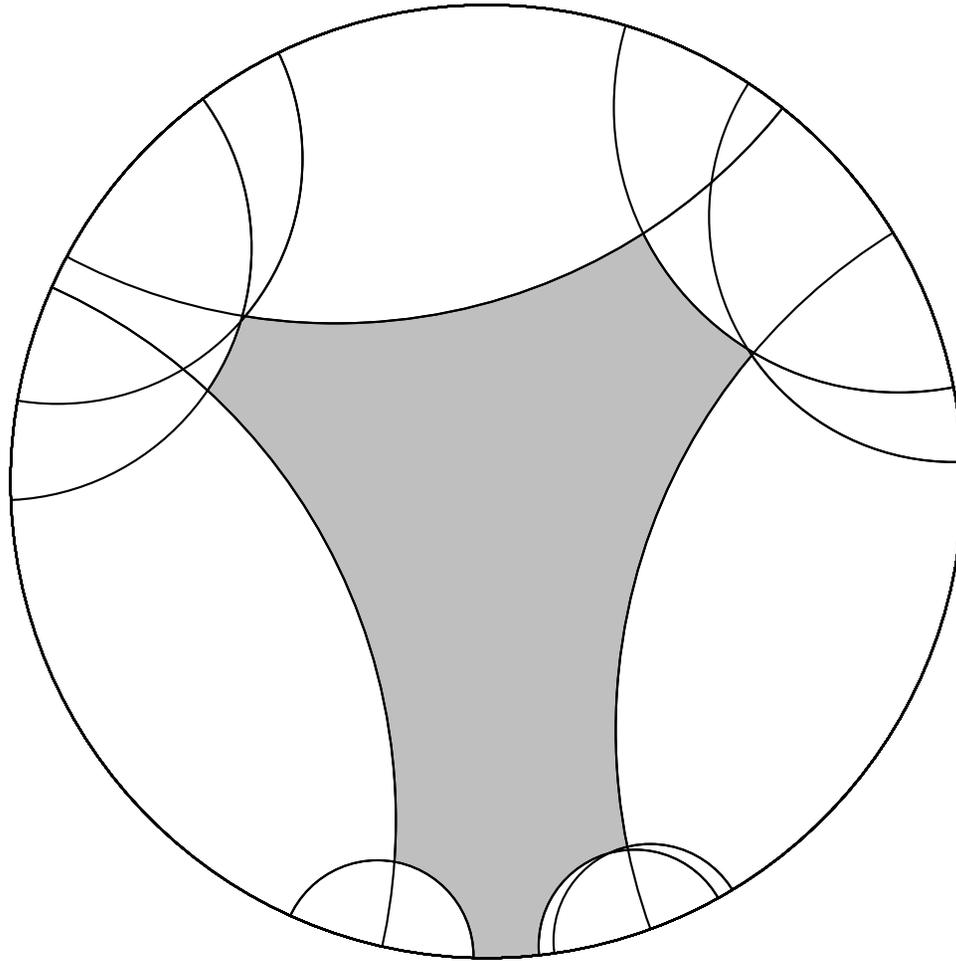
We repeat with the new infinite vertex, finding an envelope and reducing.

Computing a basis: example



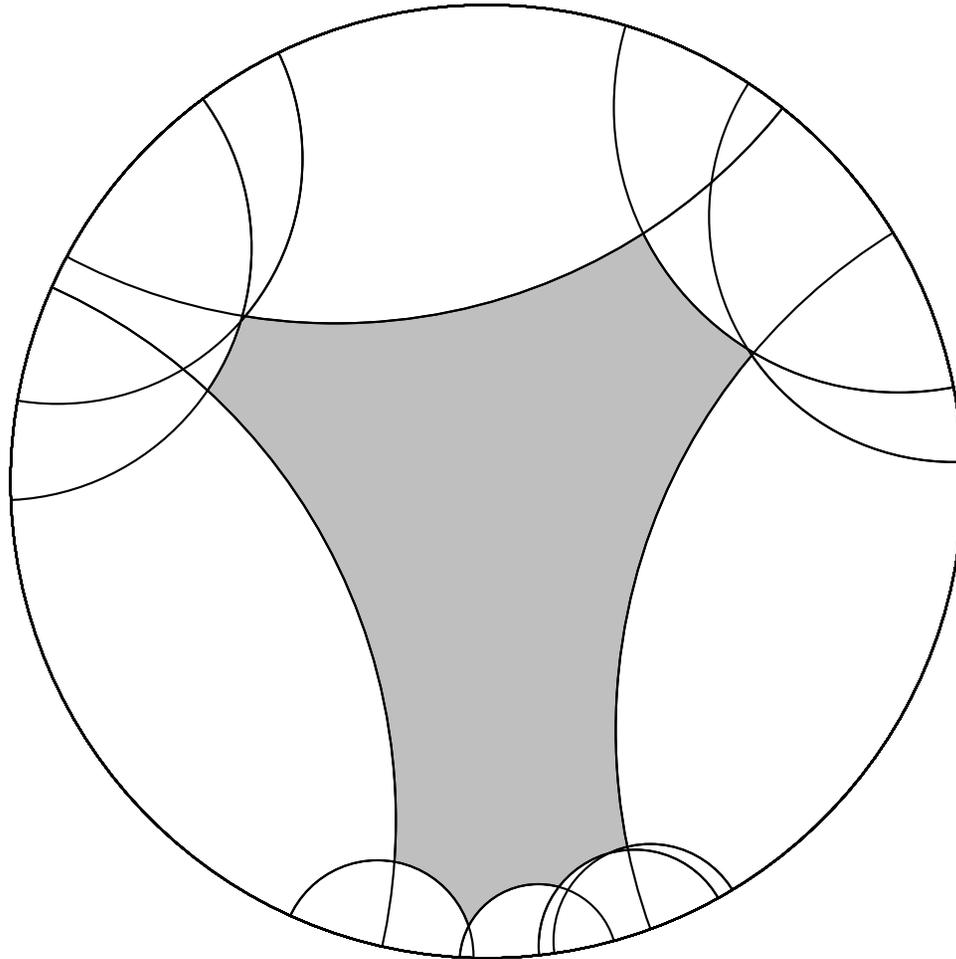
We repeat with the new infinite vertex, finding an envelope and reducing.

Computing a basis: example



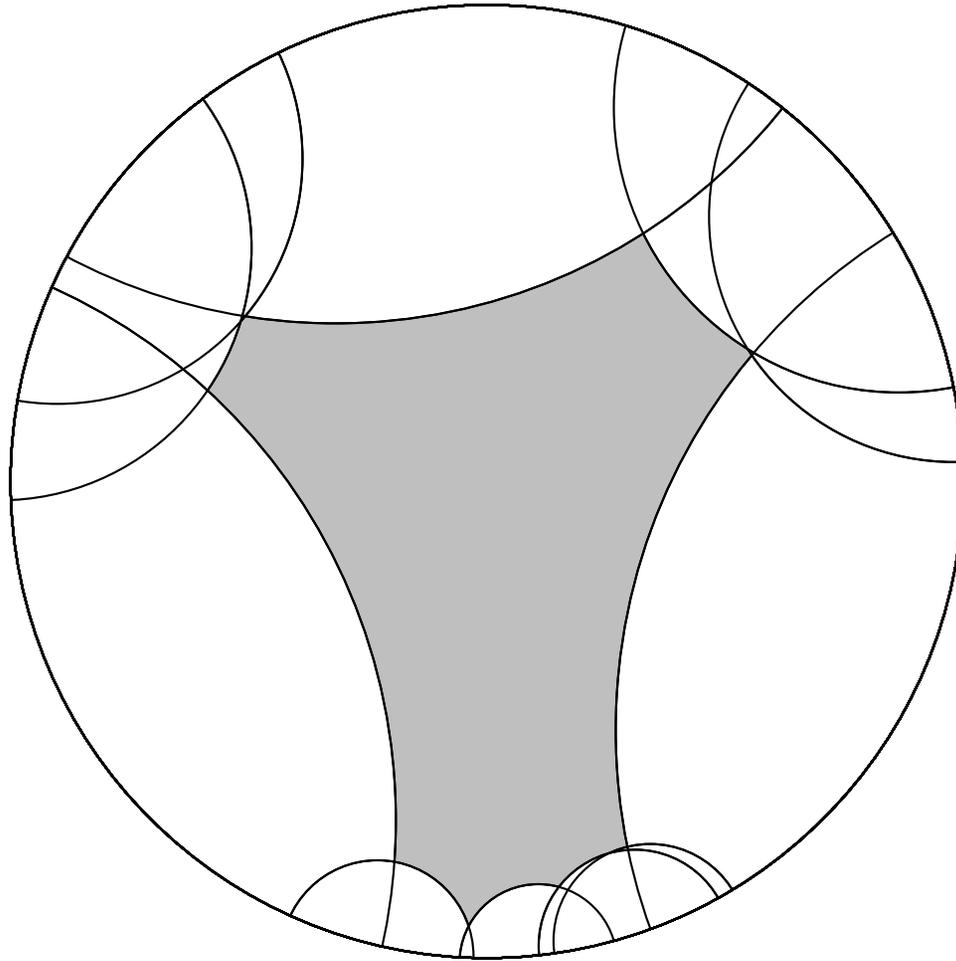
One more time.

Computing a basis: example



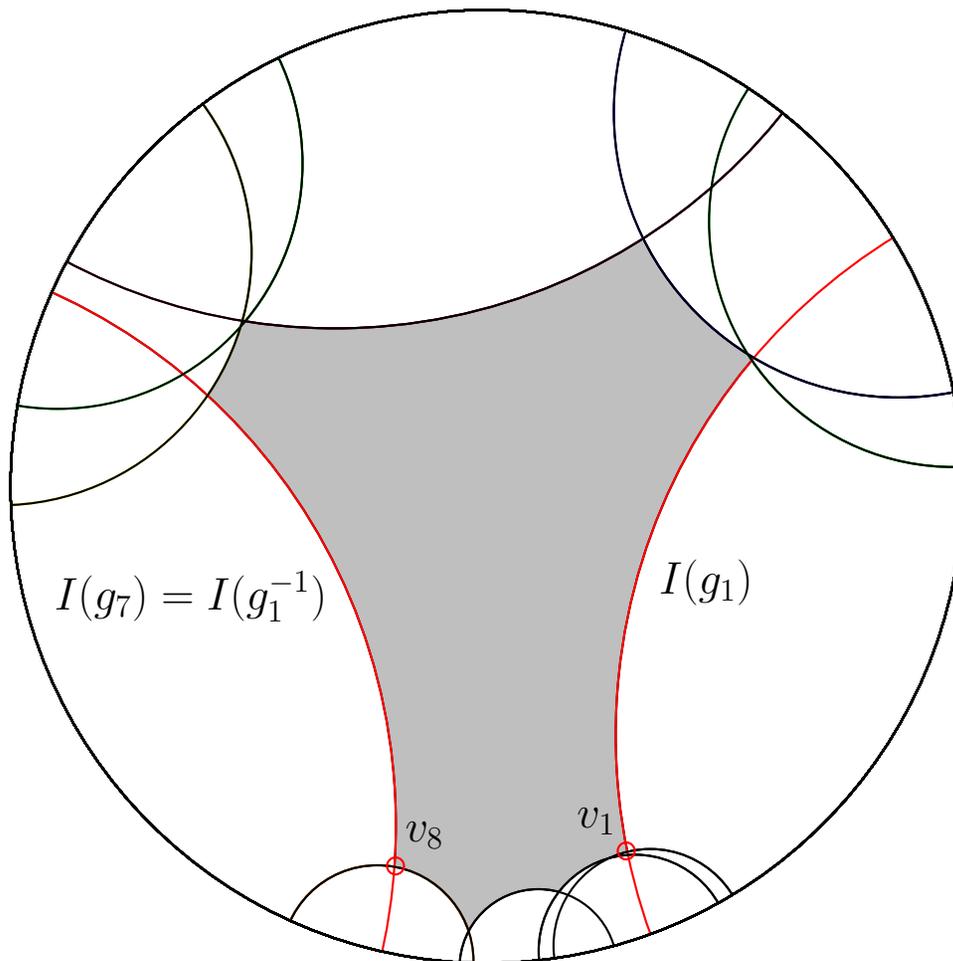
One more time. The domain now has finite area.

Computing a basis: example



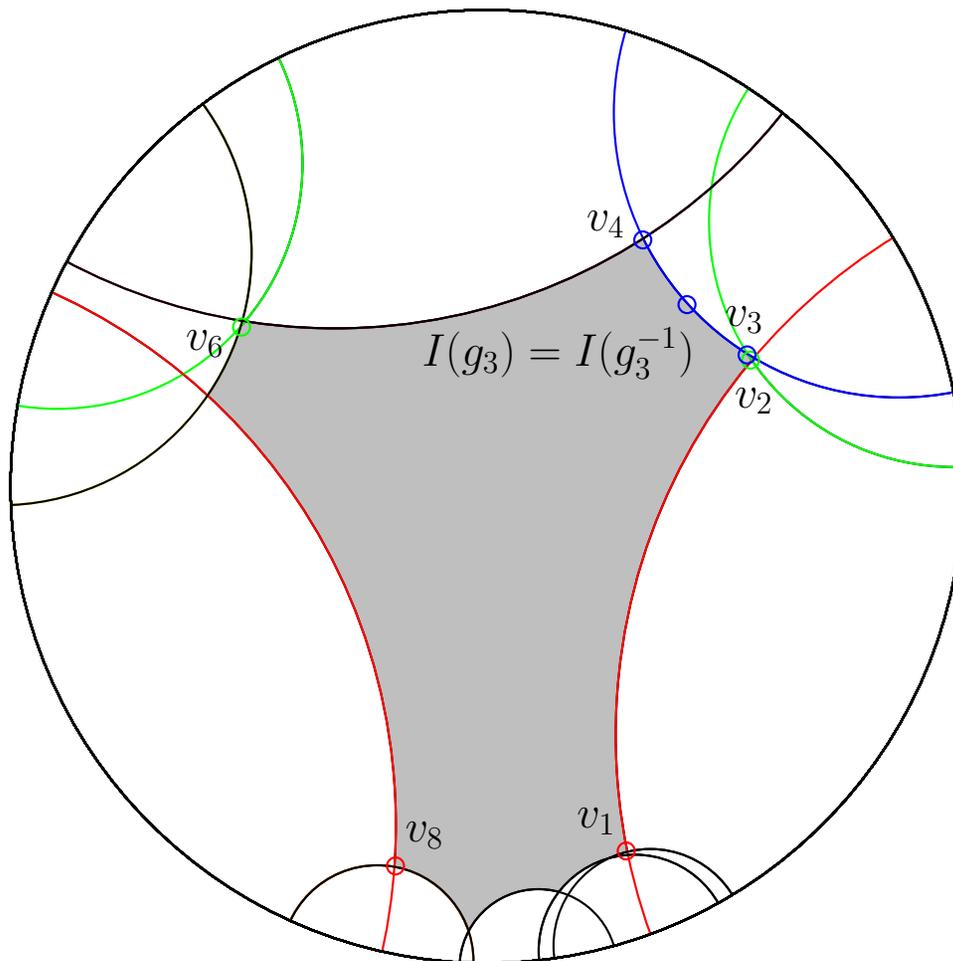
We now attempt to pair each vertex.

Computing a basis: example



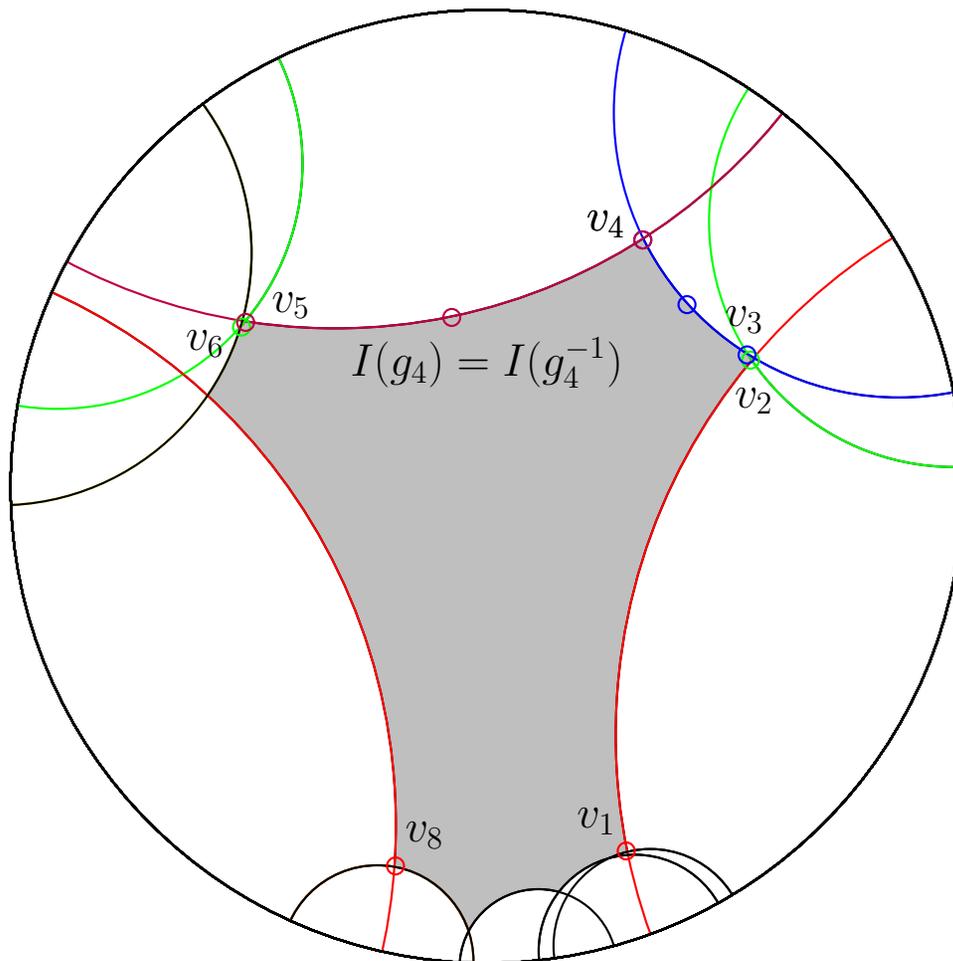
The first vertex v_1 pairs with v_8 , pairing $I(g_1)$ with $I(g_7)$.

Computing a basis: example



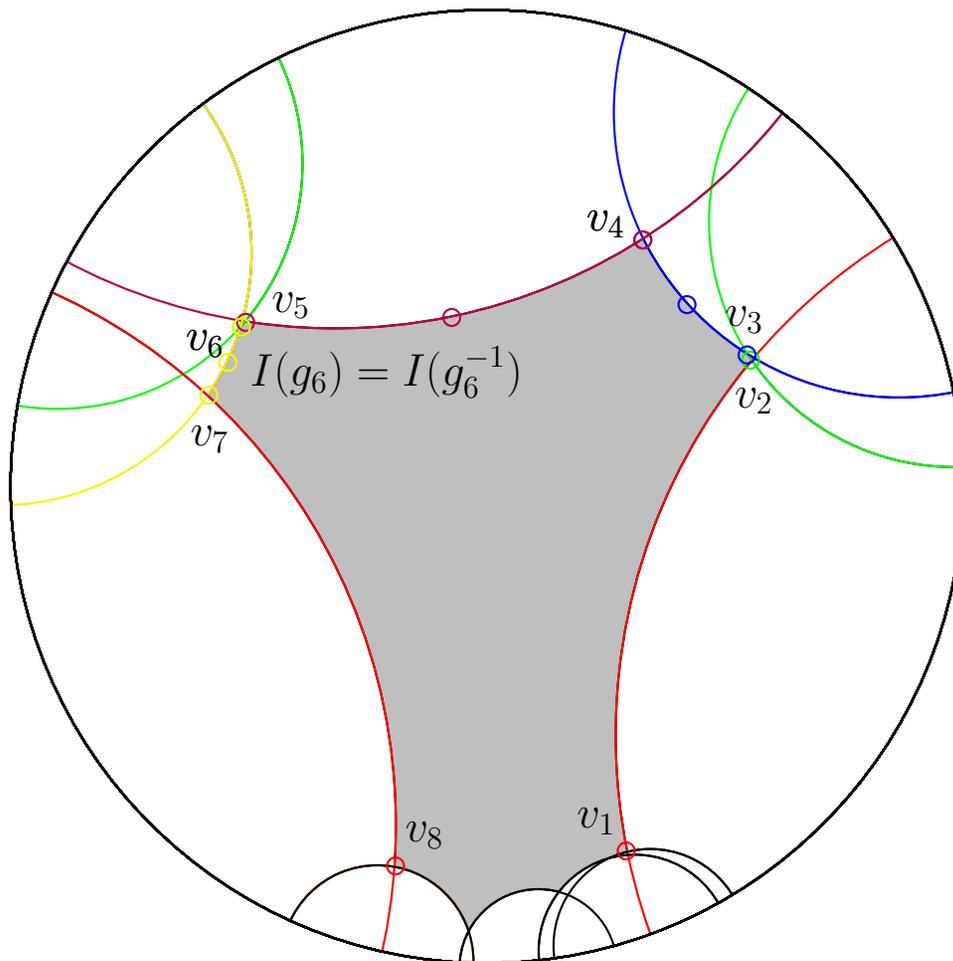
Now v_3 pairs with v_4 ; but since g_3 is an element of order 2, according to our convention, we place another vertex at its fixed point (unnumbered).

Computing a basis: example



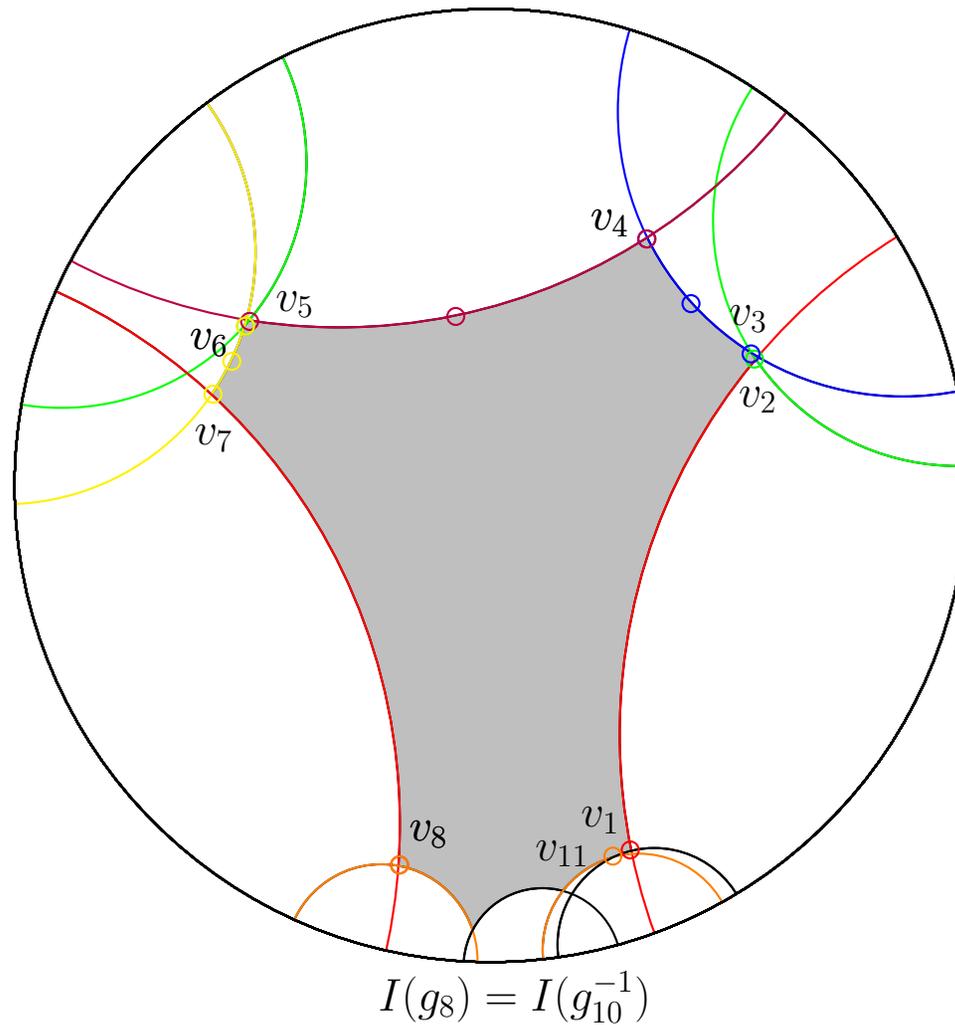
Similarly, g_4 is an element of order 2 pairing v_4 and v_5 .

Computing a basis: example



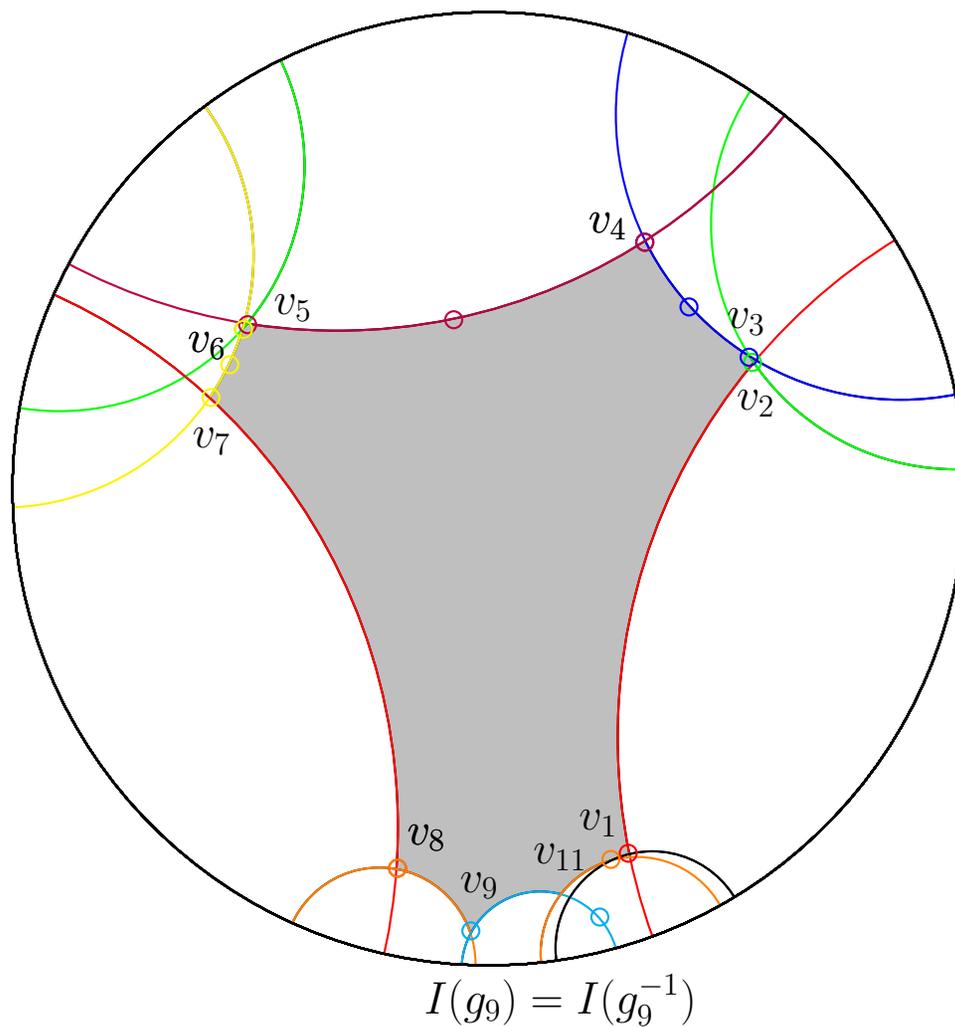
And g_6 is an element of order 2 pairing v_6 and v_7 .

Computing a basis: example



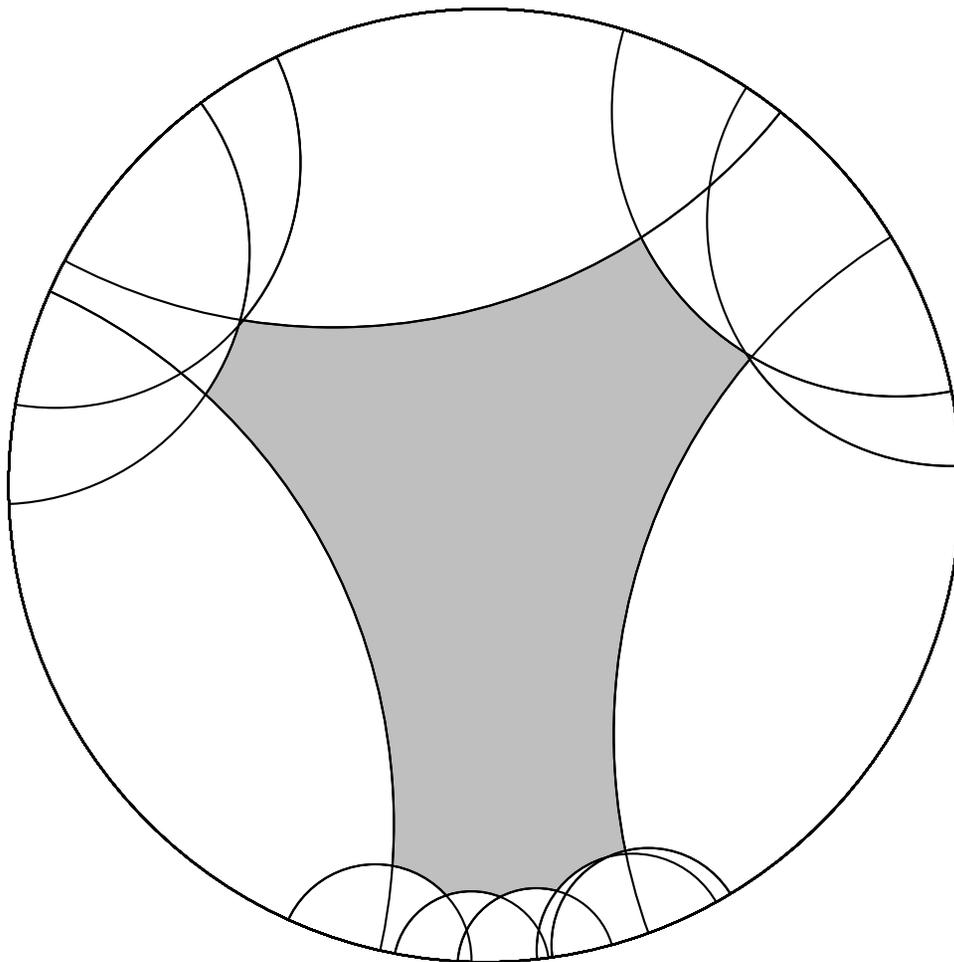
As before, v_8 pairs with v_{11} via g_8 .

Computing a basis: example



Finally: The vertex v_9 does not pair with another vertex; indeed, $g_9(v_9)$ does not lie in the exterior domain. So we compute the reduction $\text{red}_G(g_9; v_9)$.

Computing a basis: example



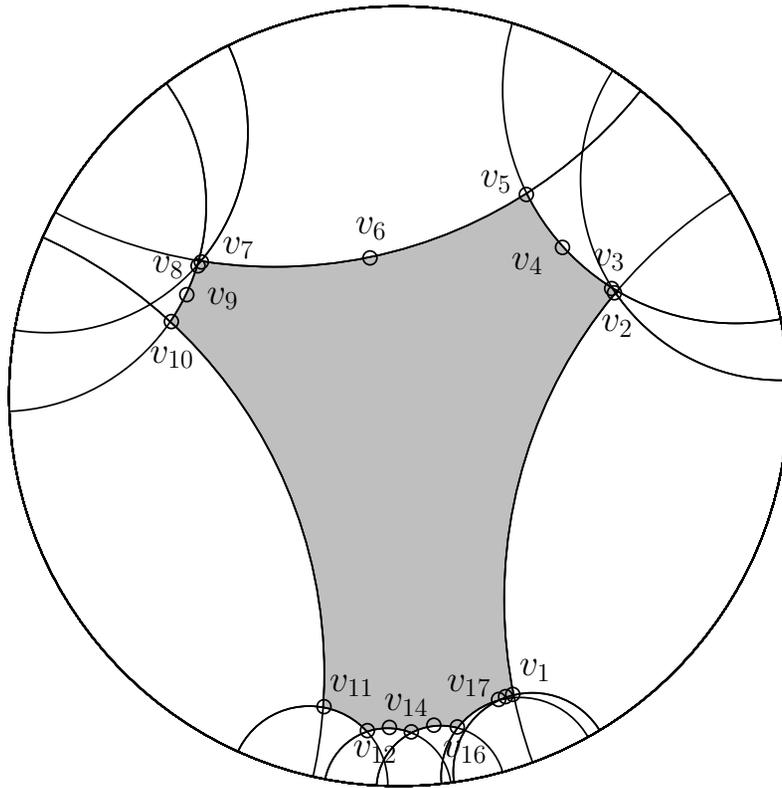
But now the area of the domain is now equal to the coarea of Γ , so we are done!

Generators and relations

Recall that the set of side pairing elements G generates the group Γ . A complete set of relations amongst these generators is obtained from the set of *minimal cycles* amongst the vertices of a Dirichlet domain D , namely, a sequence of vertices v_1, \dots, v_n such that $v_1 = v_n$, $v_i \neq v_j$ for $i \neq j$, and $v_{i+1} = g_i(v_i)$ for some $g_i \in G$.

To each such cycle, we associate the word $g = g_n \cdots g_2 g_1$ and the relation $g^k = 1$ where k is the order of g (where $k = \infty$, corresponding to a parabolic cycle, gives us no relation.)

Generators and relations: example



- g_1 pairs $e_{1,2}$ with $e_{10,11}$
- g_2 pairs $e_{2,3}$ with $e_{7,8}$
- g_3 pairs $e_{3,4}$ with $e_{4,5}$
- g_4 pairs $e_{5,6}$ with $e_{6,7}$
- g_5 pairs $e_{8,9}$ with $e_{9,10}$
- g_6 pairs $e_{11,12}$ with $e_{16,17}$
- g_7 pairs $e_{12,13}$ with $e_{13,14}$
- g_8 pairs $e_{14,15}$ with $e_{15,16}$
- g_9 pairs $e_{17,18}$ with $e_{18,1}$

We have 18 vertices and 9 generators, with the following relations:

$$g_3^2 = g_4^2 = g_6^2 = g_9^2 = g_{10}^2 = g_{12}^2 = 1 \text{ and}$$

$$g_1 g_9^{-1} g_6 = g_2^{-1} g_5^{-1} g_1 = g_3^{-1} g_4^{-1} g_2 = g_6^{-1} g_8 g_7 = 1$$

which simplify to yield a presentation for a group with signature $(0; 2^6; 0)$.