

Publications mathématiques de Besançon

ALGÈBRE ET THÉORIE DES NOMBRES

Karim Belabas, Dominique Bernardi, et Bernadette Perrin-Riou

Polygones fondamentaux d'une courbe modulaire

2020, p. 27-59.

<http://pmb.centre-mersenne.org/item?id=PMB_2020____27_0>

© Presses universitaires de Franche-Comté, 2020, tous droits réservés.

L'accès aux articles de la revue « Publications mathématiques de Besançon » (<http://pmb.centre-mersenne.org/>), implique l'accord avec les conditions générales d'utilisation (<http://pmb.centre-mersenne.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques
de Besançon, UMR 6623 CNRS/UFC*

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.centre-mersenne.org/>*

POLYGONES FONDAMENTAUX D'UNE COURBE MODULAIRE

par

Karim Belabas, Dominique Bernardi et Bernadette Perrin-Riou

Résumé. — Quelques pages de Siegel [9, p. 115 (§2)] décrivent la construction d'une base symplectique de l'homologie d'une surface de Riemann compacte à partir d'un polygone fondamental. Cette note reprend cette construction en l'appliquant au cas de la surface de Riemann associée à un sous-groupe d'indice fini de $\mathrm{PSL}_2(\mathbb{Z})$. On en déduit par des procédés classiques un système de générateurs indépendants de $H_1(X, \mathbb{Z})$ ayant un nombre minimal d'éléments hyperboliques et une présentation du $\mathbb{Z}[P^1(\mathbb{Q})]$ -module des éléments de $\mathbb{Z}[P^1(\mathbb{Q})]$ de degré 0.

Abstract. — (*Fundamental Polygons of Modular Curves*) A few pages in Siegel [9, p. 115 (§2)] describe how, starting with a fundamental polygon for a compact Riemann surface, one can construct a symplectic basis of its homology. This note retells that construction, specializing to the case where the surface is associated to a subgroup of finite index in $\mathrm{PSL}_2(\mathbb{Z})$. One then obtains by classical procedures a generating system for $H_1(X, \mathbb{Z})$ with a minimal number of hyperbolic elements and a presentation of the $\mathbb{Z}[P^1(\mathbb{Q})]$ -module of the elements of $\mathbb{Z}[P^1(\mathbb{Q})]$ of degree 0.

Soit $H = H_1(P^1(\mathbb{Q}))$ le demi-plan de Poincaré complété et soit Γ un sous-groupe d'indice fini de $\mathrm{PSL}_2(\mathbb{Z})$ tel que le test d'appartenance $z \in \Gamma$ soit calculable, par exemple un sous-groupe de congruence. Il lui est associé (de manière non unique) un symbole de Farey qui par définition est essentiellement la donnée d'un polygone hyperbolique convexe de H dont les sommets sont dans $P^1(\mathbb{Q})$ et d'une involution sur les chemins géodésiques de son bord (voir la définition 1.3 pour un énoncé précis), ce qui permet de trouver un domaine fondamental dans H pour le quotient $X(\Gamma) = H/\Gamma$.

De tels symboles fournissent des outils pour manipuler algorithmiquement le groupe Γ , par exemple un système de générateurs indépendants ou un test déterminant si Γ est un sous-groupe de congruence ainsi que son niveau. Ils admettent une construction effective : les algorithmes principaux sont dus à Kulkarni [4] développant des idées remontant à Poincaré [7]. Les invariants usuels comme le nombre de points elliptiques, le nombre de pointes ou le genre g de la courbe modulaire $X(\Gamma)$ se lisent directement sur le symbole. Il suffit d'un test effectif d'appartenance à Γ pour le construire, mais il fournit aussi réciproquement un tel test. Ces algorithmes sont disponibles dans plusieurs systèmes de calcul formel. Sans prétendre être exhaustif, citons une implantation dans Sage basée sur le paquet `KFarey` [5], le paquet `Congruence` [3] pour Gap et une implantation dans Magma adaptée de Verrill [10]. Pour

un sous-groupe de congruence, la motivation principale est la manipulation des espaces de formes modulaires associées en calculant des espaces de symboles modulaires et l'action de l'algèbre de Hecke, voir par exemple Cremona [2]. Le lien entre symboles modulaires et symboles de Farey est repris de façon éclairante par Pollack et Stevens [8], qui ramènent le calcul d'un espace de symboles modulaires $\text{Hom}(Z[P^1(\mathbb{Q})]_0, V)$ pour une représentation V de Γ au calcul de la structure du groupe $Z[P^1(\mathbb{Q})]_0$ des diviseurs de degré 0 sur $P^1(\mathbb{Q})$ comme Γ -module, laquelle est indépendante de V et est une conséquence immédiate de l'algorithme de Kulkarni.

Dans cette note, nous nous éloignons des motivations usuelles des espaces de symboles modulaires ou de la représentation exacte des sous-groupes de congruences et définissons une notion de symbole de Farey *normalisé* qui fournit un système de générateurs indépendants contenant exactement $2g$ éléments hyperboliques et une base symplectique pour $H_1(X(\Gamma), \mathbb{Q})$. Nous donnons un algorithme pour passer d'un symbole de Farey à un symbole de Farey normalisé, ce qui fournit une dissection (ou représentation) canonique de la surface de Riemann $X(\Gamma)$. Précisons d'emblée que cette notion de symbole normalisé n'a à notre connaissance pas d'intérêt algorithmique : l'algorithme de normalisation fournit des générateurs de taille bien plus importante que ceux associés au symbole utilisé en entrée, sans permettre d'opération nouvelle.

Dans la première partie, nous faisons des rappels sur les symboles de Farey et introduisons la notion de symbole de Farey normalisé. Nous rappelons le lien avec les polygones fondamentaux de la surface de Riemann $X(\Gamma)$ associée à un sous-groupe Γ de $\text{PSL}_2(\mathbb{Z})$ ainsi qu'une application connue sur la structure de $Z[P^1(\mathbb{Q})]_0$ en tant que Γ -module, qui reste valable en utilisant les symboles de Farey étendus et qui est fondamentale dans la construction de symboles modulaires de Pollack et Stevens.

Dans la seconde partie, nous donnons l'algorithme de calcul d'un symbole de Farey normalisé à partir d'un symbole de Farey quelconque. Dans l'appendice, nous donnons des exemples calculés dans Pari/GP, système dans lequel nous avons fait l'implantation de cet algorithme dans le cas particulier du sous-groupe de Hecke $\Gamma_0(N)$.

Nous remercions le rapporteur pour ses remarques qui nous ont permis de rendre plus clair le contenu de ce texte (nous l'espérons en tout cas).

1. Polygone fondamental associé à un sous-groupe de $\text{PSL}_2(\mathbb{Z})$

On note H le demi-plan de Poincaré et $H^* = H \cup P^1(\mathbb{Q})$ le demi-plan complété.

1.1. Lemme préliminaire. — Si r et s sont deux éléments distincts de $P^1(\mathbb{Q})$, on note $a = (r, s)$ l'arc géodésique dans H menant de r à s , et $A_a = \begin{pmatrix} x_a & y_a \\ z_a & t_a \end{pmatrix}$ une matrice de $M_2(\mathbb{Z})$ primitive et de déterminant strictement positif représentant a : on a donc $r = \frac{x_a}{z_a}$ et $s = \frac{y_a}{t_a}$ avec $\gcd(x_a, z_a) = \gcd(y_a, t_a) = 1$. La matrice A_a est unique au signe près. Son déterminant est appelé la largeur de l'arc a . La matrice

$$A_a^- = \begin{pmatrix} y_a & -x_a \\ t_a & -z_a \end{pmatrix} = A_a \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

représente l'arc $\bar{a} = (s, r)$ opposé à a .

On dit que des points r_1, \dots, r_n de $P^1(\mathbb{Q})$ avec $n \geq 3$ sont dans l'ordre circulaire si leurs images R_1, \dots, R_n dans le cercle unité par la transformation de Cayley $z \mapsto \frac{i-z}{i+z}$ sont dans cet ordre lorsqu'on parcourt le cercle dans le sens trigonométrique.

Lemme 1.1. — Soient r, s, t et u quatre éléments de $P^1(\mathbb{Q})$ tels que $r = s, t = u$ et tels que r, s, t, u soient dans l'ordre circulaire. On pose $a = (r, s)$ et $a^- = (t, u)$.

1. La matrice $M_a = A_a(A_a^-)^{-1}$ de $GL_2(\mathbb{Q})$ vérifie $a = \overline{a^-}$.
 - (a) Si $s = t$, alors la matrice M_a est hyperbolique.
 - (b) Si $s \neq t$, alors la matrice M_a est parabolique si et seulement si $\det(M_a) = 1$ et hyperbolique sinon.
2. La matrice $M_a = A_a \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} A_a^{-1} = A_a(A_a^-)^{-1}$ est une matrice de $SL_2(\mathbb{Q})$ vérifiant $a = \overline{a^-}$. Elle est d'ordre 2 dans $PSL_2(\mathbb{Q})$.

3. La matrice

$$M_a = A_a^- \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} (A_a^-)^{-1} = A_a^- \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} (A_a^-)^{-1}$$

est d'ordre 3 et vérifie $1 + M_a + M_a^2 = 0$. Les arcs $(a, a^-, a^2 a)$ forment un chemin fermé.

Démonstration. — Nous utiliserons les faits suivants : si M appartient à $GL_2^+(\mathbb{Q})$, elle est parabolique si $\text{trace}(M)^2 = 4 \det(M)$ et hyperbolique si elle a deux points fixes dans $P^1(\mathbb{R})$. Elle est elliptique si $\text{trace}(M)^2 < 4 \det(M)$ c'est-à-dire si elle n'a pas de points fixes dans $P^1(\mathbb{R})$.

1. On vérifie que dans chacun des cas, la matrice M_a vérifie la propriété annoncée.
 - (a) Si $s = t$, montrons que M_a est hyperbolique. Elle induit une application continue de $P^1(\mathbb{R})$ dans $P^1(\mathbb{R})$. L'image par M_a^{-1} du segment $[r, s]$ de $P^1(\mathbb{R})$ est le segment $[u, t]$ qui contient $[r, s]$; par le théorème des valeurs intermédiaires, M_a^{-1} a un point fixe dans le segment $[r, s]$, donc M_a a un point fixe dans le segment $[r, s]$. De même, l'image du segment $[t, u]$ par M_a est le segment $[s, r]$ qui contient $[t, u]$, donc M_a a un point fixe dans le segment $[t, u]$. Ayant deux points fixes dans $P^1(\mathbb{R})$, M_a est hyperbolique.
 - (b) Si $s \neq t$, un calcul explicite montre que le déterminant de M_a est $\det(A_a^-)/\det(A_a)$ et que sa trace est $1 + \det(M_a)$. On en déduit que $\text{trace}(M_a)^2 - 4 \det(M_a) = (1 - \det(M_a))^2$ et donc que M_a est parabolique si et seulement si elle est de déterminant 1. Dans le cas contraire, comme M_a a un point fixe dans $P^1(\mathbb{Q})$, elle est nécessairement hyperbolique.

2. La vérification de 2 et 3 est un calcul explicite.

Remarque 1.2. — Les formules dans le cas elliptique sont obtenues de la manière suivante.

1. La matrice $M_a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 2 et transforme les points $r, i, 0$ en $0, i, r$, respectivement. La matrice

$$M_a = A_a \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} A_a^{-1}$$

transforme les points $r, A_a(i), s$ en $s, A_a(i), r$.

2. Posons $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. La matrice $A_\omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 3, laisse ω et envoie les points $1; 0; 1$ sur $0; 1; 1$. Si T est le triangle hyperbolique de sommets $(0; \omega; 1)$, le triangle hyperbolique de sommets $(1; 0; 1)$ est ω par A_ω , est réunion des trois triangles hyperboliques T , $A_\omega T$ et $A_\omega^2 T$, et contient l'unique point ω de \mathbb{H} . Ainsi, la matrice $A_a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} (A_\omega)^{-1}$ de $SL_2(\mathbb{Q})$ laisse ω le triangle hyperbolique $(s; r; A_\omega(1))$.

1.2. Symbole de Farey étendu.

Définition 1.3. On appelle symbole de Farey étendu la donnée $(V; \omega; \ell)$

F1. d'un polygone hyperbolique convexe orienté dont les sommets $(r_1; \dots; r_n)$ sont dans $P^1(\mathbb{Q})$; son bord est donc une suite ω d'arcs consécutifs $(a_1; \dots; a_n)$ avec $a_1 = (r_1; r_2)$, $a_2 = (r_2; r_3); \dots; a_n = (r_n; r_1)$; on suppose que l'un des a_i est l'arc $(1; 0)$;

F2. d'une involution $\omega : a \mapsto \bar{a}$ de V ;

F3. d'une application ℓ de l'ensemble V_{ℓ} des points ω de V à valeurs dans $\mathbb{Z}/3\mathbb{Z}$;

tels que

F4. si $a \in V \setminus V_{\ell}$, la matrice $A_a = A_\omega(A_\omega)^{-1}$ est dans $SL_2(\mathbb{Z})$;

si $a \in V_{\ell}$ et $\ell(a) = 2$, la matrice $A_a = A_\omega(A_\omega)^{-1}$ est dans $SL_2(\mathbb{Z})$;

si $a \in V_{\ell}$ et $\ell(a) = 3$, la matrice $A_a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} (A_\omega)^{-1}$ est dans $SL_2(\mathbb{Z})$.

On appelle les éléments de ω les arcs du symbole de Farey étendu et les A_a pour $a \in V \setminus V_{\ell}$ ses données de recollement. Combinatoirement, nous considérerons V comme un collier : c'est l'orbite du mot $a_1 \dots a_n$ sous l'action du groupe $Z = n\mathbb{Z}$ des permutations circulaires. Nous appellerons facteur de V un mot $a_i a_{i+1} \dots a_j a_{j-1} a_j$ formé de lettres consécutives, en considérant $i; j$ dans $Z = n\mathbb{Z}$.

Pour $n \geq 2 \neq 3$, on note $V_{\ell; n}$ l'image réciproque de n par ℓ . Si $a \in V_{\ell}$, on dit que a est un arc elliptique d'ordre $\ell(a)$. Ainsi,

pour $a \in V_{\ell; 3}$, on a $a = \bar{a}$;

pour $a \in V_{\ell; 3}$, le triangle hyperbolique $(a; \bar{a}; \frac{2}{3}a)$ est invariant par A_a .

Définition 1.4. On appelle groupe du symbole de Farey étendu le sous-groupe $PSL_2(\mathbb{Z})$ engendré par les données de recollement $\omega, a \in V$.

Définition 1.5. Un symbole de Farey étendu $F = (V; \omega; \ell)$ est unimodulaire si les arcs de F sont de largeur 1, autrement dit si les matrices A_a pour $a \in V$ sont de déterminant 1. La condition F4 est alors trivialement vérifiée.

Graphiquement, nous représenterons les arcs de ω par des points sur un cercle et l'involution ω sur l'ensemble des arcs de ω en reliant par un trait un arc (représenté par un point) et son image par ω . Les éléments de $V_{\ell; 3}$ (resp. $V_{\ell; 2}$) sont indiqués par un point plein (resp. creux), voir figure 1.

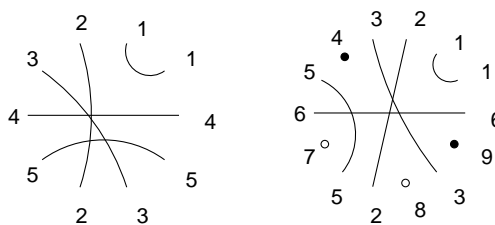


Figure 1. Exemples de représentation de l'involution

Remarque 1.6 . Ces notions sont introduites par Kulkarni [4], qui appelle simplement symbole de Farey ce que nous appelons symbole de Farey unimodulaire. Dans la suite, nous définissons un algorithme de normalisation qui abandonne l'unimodularité : notre normalisation conservera la propriété $a \in SL_2(\mathbb{Z})$ pour les données de recollement, sans qu'on ait nécessairement $A_a \in SL_2(\mathbb{Z})$ pour chaque arca de V .

Si $V = (a_1; \dots; a_n)$, on définit la distance de a_i à a_j par $d(a_i; a_j) = \min(|j - i|; |n - i + j|)$. Par exemple, $d(a_1; a_n)$ est égale à 1. Le lemme suivant est une conséquence du lemme 1.1.

Lemme 1.7 . Soit $F = (V; \dots; \text{ell})$ un symbole de Farey étendu de groupe. Si $d(a; a) \geq 2$, alors A_a est une matrice hyperbolique. Si $d(a; a) = 1$, alors A_a est une matrice parabolique. Si $d(a; a) = 0$, alors A_a est une matrice elliptique.

On note V_{hyp} (resp. V_{par}) l'ensemble des arcs à distance ≥ 2 (resp. 1) de leur image par σ . L'ensemble V_{ell} déjà défini est l'ensemble des arcs à distance 0 de leur image par σ .

Définition 1.8 . Si $F = (V; \dots; \text{ell})$ est un symbole de Farey étendu, on définit le polygone hyperbolique $P(F)$ de H^2 dont les côtés sont

- les arcs géodésiques $\sigma^{-1}V$ tels que a n'est pas un point fixe de σ ;
- les arcs géodésiques $(r; t)$ et $(t; s)$ où $(r; t; s)$ est l'image de $(0; i; 1)$ (resp. de $(0; j; 1)$) par un élément de $PSL_2(\mathbb{Q})$ et où $(r; s)$ appartient à $V_{\text{ell}; 2}$ (resp. à $V_{\text{ell}; 3}$).

On note $U(F)$ l'enveloppe convexe de $P(F)$ dans H^2 .

Le polygone $P(F)$ est un polygone spécial au sens de [4] à condition d'enlever la condition d'unimodularité. La figure 2 montre une partie d'un polygone hyperbolique associé à un symbole de Farey étendu ayant des arcs elliptiques et son enveloppe convexe. Le symbole \bullet désigne un point elliptique d'ordre 2 et le symbole \circ désigne un point elliptique d'ordre 3.

Remarque 1.9 . Le choix de définir A_a par $a = A_a \bar{a}$ (voir [8]) plutôt que par $\bar{a} = A_a a$ (voir [4]) permet de voir A_a comme l'unique élément de $PSL_2(\mathbb{Q})$ modulo Id tel que le côté a du polygone $P(F)$ soit un côté commun de $P(F)$ et de $A_a P(F)$.

Théorème 1.10 ([4, 6]). Soit Γ un sous-groupe d'indice fini de $PSL_2(\mathbb{Z})$.

1. Il existe un symbole de Farey unimodulaire de groupe Γ .

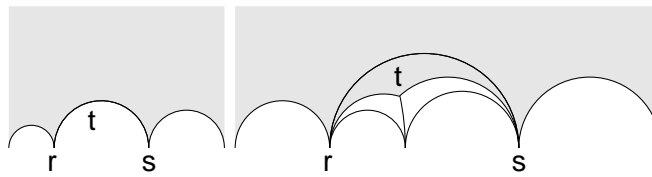


Figure 2. Points elliptiques sur le bord de polygones hyperboliques

2. Soit $F = (V; ;_{ell})$ un symbole de Farey étendu de groupe contenu dans $PSL_2(Z)$. Alors, $U(F)$ est un domaine fondamental admissible au sens [4] pour l'action de H sur H .

Les a pour $a \in V$ forment un système de générateurs de H . On dit aussi que $P(F)$ est un polygone fondamental pour H .

Démonstration. On peut trouver une démonstration de l'existence du symbole de Farey unimodulaire F de groupe H dans [4] (théorème 3.3). La deuxième partie se démontre comme le théorème 3.2 de [4].

Remarque 1.11. Si s est l'extrémité d'un arc $a = (s; t)$ de $V \setminus V_{ell}$ et si a est la donnée de recollement associée à cet arc d'origine s , on appelle successeur de s le point $a^{-1}s$. Soit $(s_0 = s; \dots; s_{l-1})$ l'orbite de $s : s_{j+1} = a_j^{-1}s_j$, avec $a_j = (s_j; t_j) \in V$, et $s_0 = a_{l-1}^{-1}s_{l-1}$. Alors, le produit $a_{l-1}^{-1} \dots a_0^{-1}$ est un générateur du stabilisateur de s dans H et est conjugué à $(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix})$ où $w > 0$ est la largeur de la pointe. En effet, posons $a = a_0 = (s; t)$; la matrice $A_a = a_0^{-1}$ envoie s sur t . Notons r l'image de t par A_a et $b = (r; s) \in V$. Nécessairement, r, s et t sont dans l'ordre circulaire et $A_b A_a^{-1}$ est à un scalaire près. Si g est un élément de $SL_2(Q)$ qui envoie t sur s , par exemple $g = \begin{smallmatrix} s & 1 \\ 1 & 0 \end{smallmatrix}$, alors $g^{-1} g$ stabilise t et vaut à un scalaire près

$$\frac{\det(A_a)}{0} = \frac{y_r y_s + y_s y_t}{\det(A_b)} ; \text{ avec } A_a = \begin{smallmatrix} x_s & x_t \\ y_s & y_t \end{smallmatrix} \text{ et } A_b = \begin{smallmatrix} x_r & x_s \\ y_r & y_s \end{smallmatrix} :$$

Comme $\det(A_a) = (s - t)y_s y_t > 0$, on en déduit que $y_s y_t < 0$; de même $y_r y_s < 0$. Ceci démontre que $a_{l-1}^{-1} \dots a_0^{-1}$ est conjugué à $(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix})$ avec $w > 0$.

1.3. Symbole de Farey normalisé.

Définition 1.12. Soit $F = (V; ;_{ell})$ un symbole de Farey étendu. Deux éléments distincts a et b de V sont dits liés si les quatre arcs (a, b) , (a, a) et (b, b) sont dans l'ordre a, b, a, b ou a, b, a, b dans V (à permutation circulaire près). Cette notion est symétrique et stable par conjugaison.

Définition 1.13. Un symbole de Farey étendu $F = (V; ;_{ell})$ est dit désentrelacé si pour tout couple $(a; b)$ d'éléments liés, les distances de a à a et de b à b sont égales à 2. Il est dit normalisé si pour tout élément a , la distance de a à a est inférieure ou égale à 2, l'égalité ayant lieu si et seulement si a est lié à un autre élément.

Un symbole de Farey étendu normalisé est désentrelacé.

Exemple .

1. Si a, b, c et d des arcs qui ne sont pas liés par $abca$ ou $accba$ ne sont pas désentrelacés a et b sont liés mais $d(a; a)$ est égal à 3 dans le premier cas et à 4 dans le second cas.

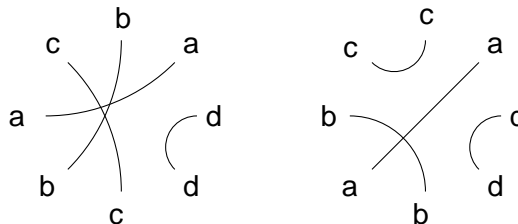


Figure 3. Involution de symboles non désentrelacés

2. Si a, b et c des arcs qui ne sont pas liés par abc et d un arc lié par cd , $abacdc$ est désentrelacé et n'est pas normalisé $cad(c; c) = 2$, mais c n'est pas lié à un autre élément.

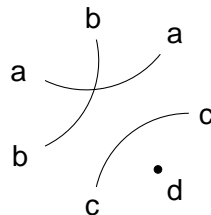


Figure 4. Involution d'un symbole désentrelacé mais non normalisé

Les exemples suivants se déduisent des calculs que nous détaillerons plus tard.

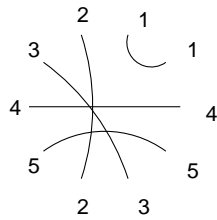
Exemple (${}_0(15)$). Le symbole de Farey unimodulaire

$$1 \left\{ \begin{array}{c} 1 \\ 1 \end{array} \right\} 0 \left\{ \begin{array}{c} 1 \\ 5 \end{array} \right\} \left\{ \begin{array}{c} 1 \\ 4 \end{array} \right\} \left\{ \begin{array}{c} 1 \\ 3 \end{array} \right\} \left\{ \begin{array}{c} 2 \\ 5 \end{array} \right\} \left\{ \begin{array}{c} 1 \\ 2 \end{array} \right\} \left\{ \begin{array}{c} 3 \\ 5 \end{array} \right\} \left\{ \begin{array}{c} 2 \\ 3 \end{array} \right\} 1$$

est associé à ${}_0(15)$. Les arcs 2 et 3 sont liés mais la distance entre 2 et 2 est $4 > 2$ donc le symbole de Farey étendu n'est pas désentrelacé. On a

$$V_{\text{par}} = f_{1g}; \quad V_{\text{hyp}} = f_{2; 3; 4; 5g}; \quad V_{\text{ell}} = ; :$$

L'involution est représentée de la manière suivante :



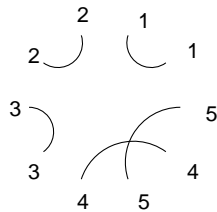
Le symbole de Farey étendu

$$1 \} 1 \} 0 \} \frac{1}{12} \} \frac{5}{59} \} \frac{3}{35} \} \frac{13}{151} \} \frac{1}{8} \} \frac{3}{13} \} \frac{8}{19} \} 1$$

est aussi associé à $\hat{\alpha}_0(15)$ et est normalisé. Remarquons au passage que l'on voit sur ce symbole de Farey étendu qu'il y a 3 pointes non équivalentes autres que la pointe θ , qu'il n'y a pas de points elliptiques et que le genre de la courbe est 1 :

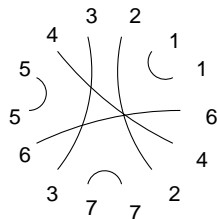
$$V_{\text{par}}^{\text{norm}} = = f \quad 1; \quad 2; \quad 3g; \quad V_{\text{hyp}}^{\text{norm}} = = f \quad 4; \quad 5g; \quad V_{\text{ell}}^{\text{norm}} = ; \quad ;$$

$$1 \} \boxed{1} \} 0 \} \boxed{\frac{1}{12}} \} \boxed{\frac{5}{59}} \} \boxed{\frac{3}{35}} \} \boxed{\frac{13}{151}} \} \boxed{\frac{1}{8}} \} \boxed{\frac{3}{13}} \} \boxed{\frac{8}{19}} \} 1$$



Exemple ($\hat{\alpha}_0(20)$). Le symbole de Farey étendu suivant associé à $\hat{\alpha}_0(20)$ est unimodulaire mais non normalisé :

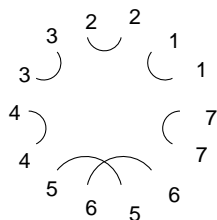
$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{2}{7} \} \frac{3}{10} \} \frac{1}{3} \} \frac{3}{8} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$



$$V_{\text{par}} = = f \quad 1; \quad 5; \quad 7g; \quad V_{\text{hyp}} = = f \quad 2; \quad 3; \quad 4; \quad 6g; \quad V_{\text{ell}} = ; \quad ;$$

Le symbole de Farey étendu suivant associé à $\hat{\alpha}_0(20)$ est normalisé :

$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{4}{19} \} \frac{3}{14} \} \frac{11}{51} \} \frac{107}{496} \} \frac{524}{2429} \} \frac{8}{37} \} \frac{3}{11} \} \frac{73}{253} \} \frac{20}{69} \} \frac{3}{10} \} 1$$



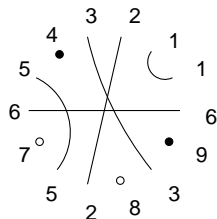
$$V_{\text{par}}^{\text{norm}} = = f \ 1; \ 2; \ 3; \ 4; \ 7g; \quad V_{\text{hyp}}^{\text{norm}} = = f \ 5; \ 6g; \quad V_{\text{ell}}^{\text{norm}} = ; :$$

On voit que la taille des rationnels intervenant dans le symbole de Farey étendu a augmenté.

Exemple ($0(37)$). Le symbole de Farey unimodulaire suivant pour $0(37)$

$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{1}{3} \} \frac{3}{8} \} \frac{2}{5} \} \frac{3}{7} \} \frac{1}{2} \} \frac{4}{7} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

$\begin{matrix} 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 5 & 2 & 8 & 3 & 9 & 6 \\ 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 5 & 2 & 8 & 3 & 9 & 6 \end{matrix}$



représenté plus simplement par

$$1 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 5 \ 2 \ 8 \ 3 \ 9 \ 6$$

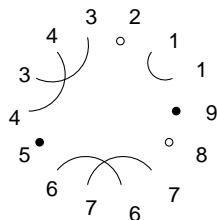
est un symbole de Farey associé à $0(37)$. Il n'est pas désentrelacé car, par exemple, 2 et 3 sont liés mais la distance de 2 à 2 est strictement supérieure à 2. Dans cet exemple, il n'y a que deux points non équivalentes. Par contre, il n'y a que deux matrices paraboliques correspondant à 1 et à 1 . On a

$$V_{\text{par}} = = f \ 1g; \quad V_{\text{hyp}} = = f \ 2; \ 3; \ 5; \ 6g; \quad V_{\text{ell}} = f \ 4; \ 7; \ 8; \ 9g :$$

Un symbole de Farey étendu normalisé obtenu par notre algorithme est

$$1 \} 1 \} 0 \} \frac{1}{6} \} \frac{2}{11} \} \frac{1}{5} \} \frac{1}{4} \} \frac{11}{43} \} \frac{21}{82} \} \frac{10}{39} \} \frac{6}{23} \} \frac{5}{19} \} \frac{51}{193} \} \frac{7}{26} \} 1$$

$\begin{matrix} 1 & 2 & 3 & 4 & 3 & 4 & 5 & 6 & 7 & 6 & 7 & 8 & 9 \\ 1 & 1 & 2 & 3 & 4 & 3 & 4 & 5 & 6 & 7 & 6 & 7 & 8 & 9 \end{matrix}$



On a

$$V_{\text{par}}^{\text{norm}} = f_{1g}; \quad V_{\text{hyp}}^{\text{norm}} = f_{3; 4; 6; 7g}; \quad V_{\text{ell}}^{\text{norm}} = f_{2; 5; 8; 9g} :$$

Lemme 1.14 . Soit $F = (V; ;_{\text{ell}})$ un symbole de Farey étendu normalisé de groupe.

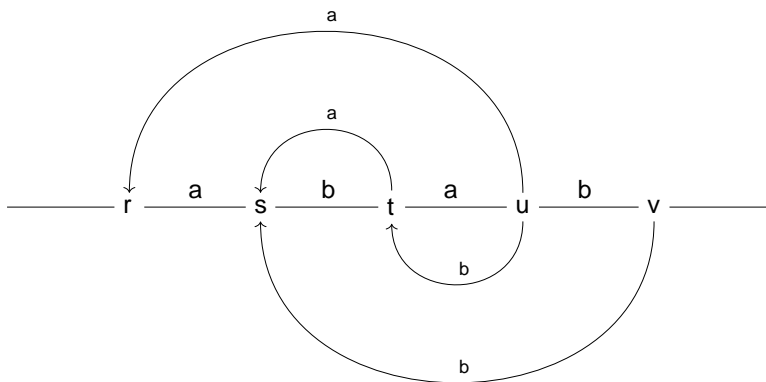
1. Les extrémités des arcs qui sont à la distance 0 ou 2 de leur image parson toutes équivalentes modulo ainsi que les extrémités externes des facteurs c pour $c \in V_{\text{par}}$.
2. Soit P_0 la classe d'équivalence commune. L'application

$$V_{\text{par}} \rightarrow \mathbb{P}^1(Q) / P_0g$$

qui associe à la classe de son extrémité commune avec est une bijection.

Démonstration. Le collier V est formé de facteurs de la forme aba , cc et d avec $cd = d$. Dans le cas aba , on a $\bar{a} = a$ et $\bar{b} = b$. Si $a = (r; s)$ et $b = (s; t)$, on a nécessairement

$$u = a^{-1}r; \quad s = a^{-1}b^{-1}r; \quad t = a^{-1}br; \quad v = b^{-1}a^{-1}r :$$



Donc les extrémités des arcs a, b, a, b sont toutes équivalentes modulo . Dans le cas d'un facteur de la forme d avec $d = d$, on a soit $d = d$, soit $d + d + d = 0$; dans les deux cas, les extrémités d et d sont équivalentes modulo . Finalement, dans le cas d'un facteur de la forme cc , les extrémités externes sont équivalentes puisque $c^{-1}c = \bar{c}$.

On en déduit que toutes les extrémités externes de tous les facteurs de la forme aba , cc et $d = d$ sont équivalentes ainsi que les extrémités internes des facteurs de la forme aba . Cela termine la démonstration de la partie 1.

Il reste à regarder ce qui se passe pour la seconde extrémité d lorsque $c \in V_{\text{par}}$ (facteur du type cc avec $c \in c$). Les éléments de $\mathbb{P}^1(Q)$ qui ne sont pas équivalents à P_0 sont nécessairement équivalents modulo à une des extrémités des arcs d et donc à une extrémité de c pour un c de V_{par} . Il su t donc de démontrer que pour deux facteurs distincts du type c_1c_1 et c_2c_2 , le point s_1 commun à c_1 et c_1 et le point s_2 commun à c_2 et c_2 ne sont pas équivalents modulo . Prenons un petit disque ouvert dont le bord contient s_1 et inclus dans H . Son image dans la surface nH est un disque épointé et ne peut pas contenir l'image d'un point proche de s_2 . Par continuité, s_1 et s_2 ne peuvent pas être équivalents modulo .

Remarque 1.15 . Résumons les résultats précédents ainsi que des résultat connus (voir par exemple [4]). Soit $g()$ le genre de $X()$, $\nu_1()$ le nombre de pointes de $X()$, $\nu_2()$ et $\nu_3()$ le nombre de points elliptiques d'ordre 2 et 3. Soit un symbole de Farey étendu normalisé $F = (V; ;_{ell})$. Alors, V est formé de

1. $g()$ facteurs du type aba avec $les a, b, a$ et b distincts deux à deux (a et $b \in V_{hyp}$);
2. $\nu_1()$ - 1 facteurs de type ccc avec $c \in V_{par}$;
3. $\nu_2() + \nu_3()$ points c par l'involution $(c \in V_{ell})$.

Le groupe fondamental $\pi_1(Y())$ est libre de rang $r = 2g + \nu_1 - 1$. Le nombre d'arcs du domaine fondamental associé à F est $2(r + \sum \nu_{ell;2} + \sum \nu_{ell;3})$. Le groupe est isomorphe à un produit libre de $\sum \nu_{ell;2}$ exemplaires de $Z=2Z$, de $\sum \nu_{ell;3}$ exemplaires de $Z=3Z$ et de r exemplaires de Z ([4, prop. 3.4 et prop. 7]).

1.4. Structure de $Z[P^1(Q)]_0$. Soit $\mathcal{D} = Z[P^1(Q)]$ le groupe des diviseurs sur $P^1(Q)$ et \mathcal{D}_0 le sous-groupe des diviseurs de degré 0. L'action naturelle de $GL_2(Q)$ sur $P^1(Q)$ induit une action de G sur \mathcal{D} . Si $c \in P^1(Q)$, on note $f_c g$ le diviseur associé à c dans $Z[P^1(Q)]$. Si c_1 et c_2 sont dans $P^1(Q)$, on note $(c_1; c_2)$ le diviseur $f_{c_2} g - f_{c_1} g$ associé dans \mathcal{D}_0 . On parlera aussi du chemin $(c_1; c_2)$: dans l'interprétation géométrique, il s'agit du chemin géodésique reliant les deux pointes c_1 et c_2 du demi-plan de Poincaré complété \mathbb{H} . Le groupe \mathcal{D}_0 est engendré par les diviseurs de la forme $(c_1; c_2) = f_{c_2} g - f_{c_1} g$ avec $c_1, c_2 \in P^1(Q)$. Les résultats de Pollack et Stevens se transposent de la manière suivante.

Théorème 1.16 . Soit F un symbole de Farey étendu $(V; ;_{ell})$ et (a) ses données de recollement pour $a \in V$. Le $Z[\]$ -module \mathcal{D}_0 est défini par générateurs et relations de la manière suivante : l'image de V dans \mathcal{D}_0 forme un système de générateurs vérifiant les relations

1. $\sum_{a \in 2V} a = 0$;
2. $a + a_a = 0$ si $a \in V_{ell;3}$;
3. $a + a_a + a_a^2 = 0$ si $a \in 2V_{ell;3}$.

Pour la démonstration, voir [8]. On peut facilement extraire un système de générateurs minimal. Soit $(V \setminus V_{ell}) =$ un ensemble formé de représentants du quotient de $V \setminus V_{ell}$ par l'involution σ . Le premier élément de $(V \setminus V_{ell}) =$ est supposé être le chemin $(1; 0)$. On note $A = (V \setminus V_{ell}) = V_{ell}$.

Corollaire 1.17 . Le $Z[\]$ -module $\mathcal{D}_0 = Z[P^1(Q)]_0$ est le quotient du $Z[\]$ -module libre engendré par les éléments de A par les relations

$$\begin{aligned} & \left(\sum_{a \in 2A} a \right) = 0 \\ & a_a = 0 \text{ pour } a \in 2V_{ell} \end{aligned}$$

avec

1. $a_a = 1$ pour $a \in (V \setminus V_{ell}) =$ et $a_a = 1$ pour $a \in 2V_{ell}$;

$$2. \quad a = \prod_{s=0}^{p-1} a_s \text{ pour } a \in V_{\text{ell}}.$$

On en déduit que \mathcal{O} admet une présentation en tant que $Z[\]$ -module de la forme

$$W_1 \rightarrow W_0 \rightarrow \mathcal{O} \rightarrow 0$$

où W_1 et W_0 sont des $Z[\]$ -modules libres :

$$\begin{aligned} W_0 &= \bigoplus_{a \in A} Z[\] \\ W_1 &= \bigoplus_{a \in V_{\text{ell}}} Z[\] \end{aligned}$$

La \mathcal{O} -structure de W_0 dans \mathcal{O} est donnée par

$$(w_a)_{a \in A} \mapsto \sum_{a \in A} w_a a$$

La \mathcal{O} -structure de W_1 dans W_0 est donnée par

$$(v; (w_a)_{a \in V_{\text{ell}}}) \mapsto v(a)_{a \in A} + (w_a a)_{a \in V_{\text{ell}}}$$

Plus précisément, le $Z[\]$ -module \mathcal{O} admet une résolution projective de la forme

$$\dots \rightarrow W_n \rightarrow W_{n-1} \rightarrow W_{n-2} \rightarrow \dots \rightarrow W_0 \rightarrow \mathcal{O} \rightarrow 0$$

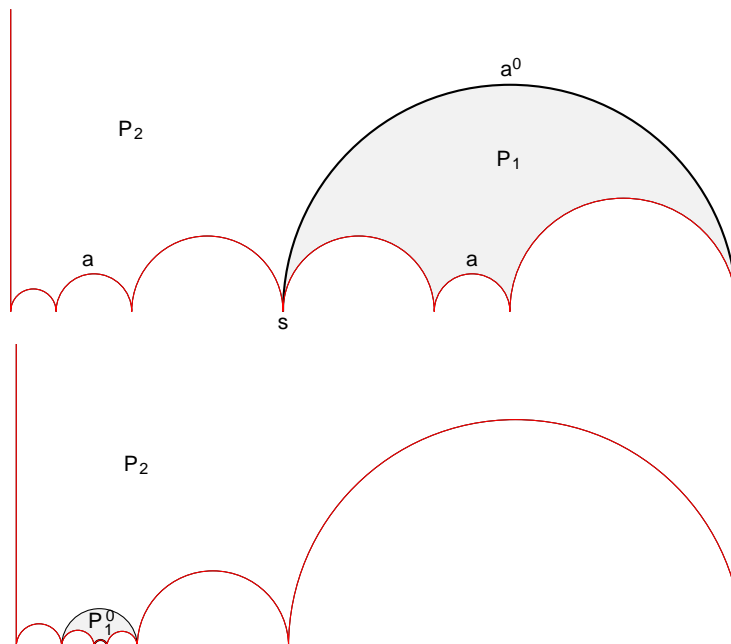
où $W_n = \bigoplus_{a \in V_{\text{ell}}} Z[\]$ pour $n \geq 2$. Pour $m = 1$, les \mathcal{O} -structures sont données par

$$\begin{aligned} W_{2m} \rightarrow W_{2m-1} & \quad W_{2m+1} \rightarrow W_{2m} \\ (w_a)_{a \in V_{\text{ell}}} \mapsto (w_a(a-1))_{a \in V_{\text{ell}}} & \quad (w_a)_{a \in V_{\text{ell}}} \mapsto (w_a a)_{a \in V_{\text{ell}}} \end{aligned}$$

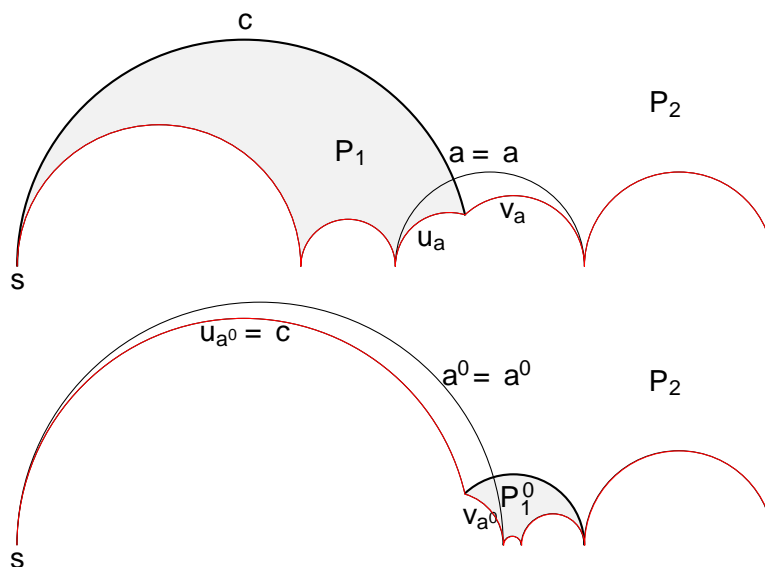
2. Construction d'un symbole de Farey étendu normalisé

Construction . L'algorithme décrit dans ce paragraphe permet de construire à partir d'un symbole de Farey étendu F de groupe Γ un symbole de Farey étendu normalisé F^{norm} de même groupe Γ . Cette construction est inspirée d'un paragraphe de Siegel dans [9, p. 115, §2] et met en oeuvre l'opération de dissection sur les surfaces de Riemann ([1]).

2.1. Interprétation géométrique. Nous avons vu qu'à un symbole de Farey étendu F de groupe Γ est associé naturellement un domaine fondamental $U(F)$ pour l'action de Γ sur H . Donnons la description géométrique des opérations de Siegel. Soit un élément de V tel que $a \in A$, c'est un arc du bord de $U(F)$. On choisit deux sommets s et t non elliptiques de $U(F)$ tels que la géodésique α^0 reliant s et t sépare a et a^{-1} (s ou t peut être une extrémité de a ou de a^{-1}). On découpe le domaine le long de α^0 en deux polygones P_1 et P_2 et on translate le polygone contenant a (disons P_1) par $a^{-1} : P_1^0 = a^{-1}P_1$: ainsi a (resp. a^{-1}) est un côté du polygone P_2 (resp. P_1^0) et l'on peut recoller les deux polygones P_1^0 et P_2 le long de a . On obtient un nouveau domaine fondamental pour Γ .

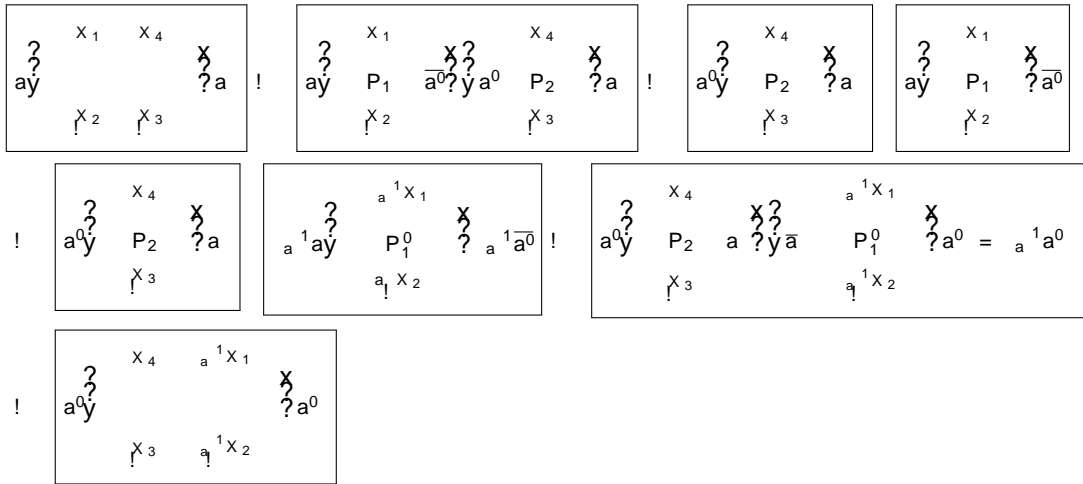


Lorsque $a = a$, on choisit une coupure c dont l'une des extrémité est le point elliptique associé à a et l'autre extrémité un point non elliptique s et la suite du procédé est le même. Le dessin suivant représente un cas de chemin elliptique d'ordre 3.



Les deux paragraphes qui suivent décrivent ces opérations en termes de symboles de Farey uniquement. Dans la suite, $(V; \dots; \text{ell})$ désigne un symbole de Farey étendu. On pose $V = (a_1; \dots; a_n)$ et on note $(a)_{a_2 V}$ les données de recollement associées. Les lettres majuscules désigneront des facteurs de V , donc formés d'arcs consécutifs. En particulier, V est le facteur $a_1 a_2 \dots a_n$. Les lettres minuscules réfèrent en général aux arcs de V .

2.2. Opération de base (cas non elliptique). Choisissons un élément de V tel que $a \in a$ et un découpage de V de la forme suivante $V = (X_1 a X_2 X_3 a X_4)$. On construit un nouveau symbole de Farey étendu $F^0 = (V^0; \begin{smallmatrix} 0 \\ \text{ell} \end{smallmatrix})$ par une opération de base de découpage et recollement de la manière suivante : on introduit l'arc a^0 reliant l'extrémité droite du facteur X_4 (qui est aussi l'extrémité gauche du facteur X_1) à l'extrémité droite du facteur X_2 (qui est aussi l'extrémité gauche du facteur X_3) et on recolle les arcs opposés a et $a^{-1}(a)$:

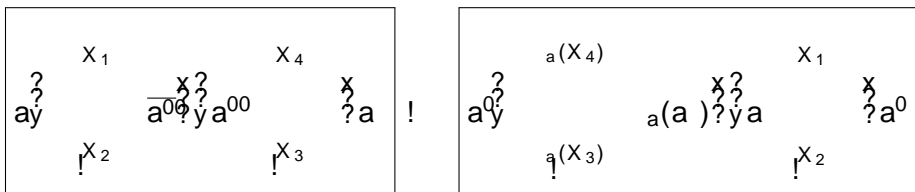


Cette opération est la traduction en termes de symbole de Farey étendu de la description géométrique sur les domaines fondamentaux du paragraphe 2.1. Décrivons le nouveau symbole de Farey étendu $F^0 = (V^0; \begin{smallmatrix} 0 \\ \text{ell} \end{smallmatrix})$. On a

$$V^0 = (a^0 X_3 a^{-1}(X_2) a^0 a^{-1}(X_1) X_4) :$$

Si v est un élément de V , notons v^0 l'élément correspondant dans V^0 . Pour v élément de a et a^{-1} , selon la position de v , on a $v^0 = v$ ou $v^0 = a^{-1}v$. L'involution sur F^0 respecte la transformation $v \mapsto v^0$, autrement dit $(v^0)^0 = v^0$. Les données de recollement se déduisent de celles de F . On a par construction $a^0 = a$. Pour v élément de a et a^{-1} , selon les positions respectives de v et de v^0 , on a $a^{-1}v^0 = v$, $a^{-1}v^0 = a^{-1}v$, $v a^0$ ou $a^{-1}v a^0$. On en déduit que v^0 appartient encore à $SL_2(\mathbb{Z})$ (et bien sûr à Γ) et donc que le nouveau symbole de Farey étendu vérifie la propriété (F4). Si v est élément de a et de a^{-1} , la largeur de v^0 (déterminant de A_{v^0}) est égale à la largeur de v . Cela n'est pas vrai pour a^0 et $a^0 = a^{-1}a^0$. Le groupe associé au nouvel symbole de Farey étendu F^0 est encore Γ .

Une transformation similaire est obtenue en échangeant les rôles de a et de a^{-1} : on choisit alors d'appliquer a^{-1} au deuxième polygone obtenu par découpage selon $a^0 = a^{-1}(a^0)$:



Nous représentons ces opérations de la manière suivante

$$(a X_2 j X_3 a X_4 j X_1) \mapsto (a^0 X_3 a^{-1}(X_2) a^0 a^{-1}(X_1) X_4)$$

resp.

$$aX_2 j X_3^a X_4 j X_1 \ 7! \ a^0_a(X_3)X_2a^0 X_1 \ a(X_4) :$$

Les pivots a et a que l'on remplace sont soulignés. Les coupures sont indiquées par un trait vertical. La partie $f::$ entre deux coupures indique les chemins transformés par a^{-1} (resp. a). De manière équivalente, les opérations peuvent être représentées par

$$(X_1^a X_2 j X_3^a X_4 j) \ 7! \ (X_4 a^0 X_3 \ a^{-1}(X_2) a^0 \ a^{-1}(X_1))$$

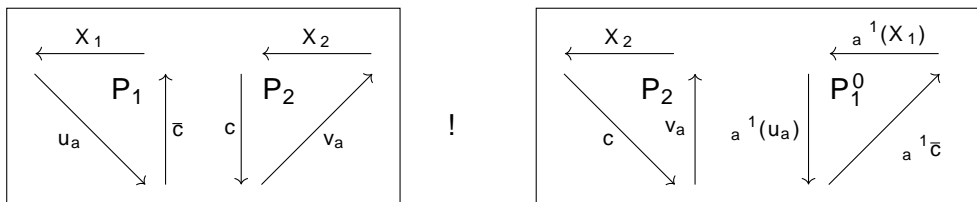
resp.

$$(X_1 a X_2 j X_3^a X_4 j) \ 7! \ (\ a(X_4) a^0 \ a(X_3) X_2 a^0 X_1) :$$

2.3. Opération de base (cas elliptique). Supposons maintenant que $a = a$. Les opérations de base sont les suivantes

$$(X_1^a j X_2 j) \ ! \ (a^0 X_1 \ a(X_2)) \ \text{resp.} \ (X_1 a j X_2 j) \ ! \ (a^0 \ a^{-1}(X_1) X_2) :$$

Pour comprendre l'opération, il faut se souvenir que le polygone fondamental construit à partir de F ne contient pas $a = (r_a; s_a)$ comme bord, mais les arcs $u_a = (r_a; t_a)$ et $v_a = (t_a; s_a)$ où t_a appartient au demi-plan de Poincaré H . La coupure $c = (s; t_a)$ est faite entre t_a et le sommets extrémité commune de X_1 et X_2 . La dissection faite sur ce polygone est alors (dans le premier cas)



On a $a^{-1}(u_a) = \overline{v_a}$ et si $a^0 = cc$ avec $c = a^{-1}c$, on a $a^0 = a$. Le second cas se traite de la même manière en appliquant a à P_2 .

2.4. Étape de Siegel. Notons W un facteur initial de V qui est normalisé (c'est-à-dire lui-même formé de facteurs de la forme aba , aa ou a avec $a = a$) et posons $V = (WX)$. L'étape de Siegel que nous allons décrire permet de remplacer le symbole de Farey étendu initial F par un symbole de Farey étendu F^0 avec $V^0 = (W^0 X^0)$ et W^0 strictement plus long que W en (au plus) 4 opérations de base.

Dans la suite, on omettra les 0 dans la notation : par exemple,

$$(X_1^a X_2 j X_3^a X_4 j) \ 7! \ (X_4 a^0 X_3 \ a(X_2) a^0 \ a(X_1)) = (X_4^0 a^0 X_3^0 X_2^0 a^0 X_1^0)$$

sera simplement écrit

$$(X_1^a X_2 j X_3^a X_4 j) \ 7! \ (X_4 a X_3 X_2 a X_1) :$$

En pratique, nous supposerons que W contient l'arc $(1; 0)$. Le choix de la coupure qui sera modifiée par un élément de Γ est fait de manière à ne pas transformer l'arc $(1; 0)$, ce qui revient à ne pas appliquer un élément de Γ sur W . Expérimentalement, cela diminue de manière drastique la taille des coefficients des matrices et le temps de calcul.

1. Cas parabolique. On considère un arc a à distance 1 de a (appelé pivot). On peut supposer qu'il précède a quitte à changer de notation. La longueur de W augmente de 2 avec l'une des deux opérations suivantes

$$(WXaa Y) = (WX \underline{a} j \underline{a} \hat{\Psi} j) ! \quad (aa WXY)$$

ou

$$(WXaa Y) = (W j \hat{\Psi} \underline{a} j \underline{a} Y) ! \quad (aa XYW) \stackrel{\text{rotation}}{!} (Waa XY) :$$

2. Cas hyperbolique. On considère deux arcs a et b liés avec a précédant b dans V (appelés pivots de l'étape). Plusieurs suites d'opérations sont possibles. Quand il y a plusieurs choix possibles, les coupures sont choisies de manière à ce que le pivot non utilisé soit dans le même facteur que son image par l'involution. Dans tous les cas, la longueur de W augmente de 4. En pratique, nous n'avons utilisé que le premier cas.

(a) b suit a .

$$\begin{aligned} (WXabY a Zb T) &= (WXabY j a \hat{\wedge} Z \underline{b} T j) \\ ! \quad (ba ZY b WXaT) &= (b \hat{\wedge} a ZY j b WX \underline{a} T j) \\ ! \quad (a b WXZY abT) &= (a \underline{b} WXZY a j \hat{\wedge} T j) \\ ! \quad (b WXZY aba T) &= (b WXZY \underline{a} j \hat{\wedge} a T j) \\ ! \quad (aba b WXZY T) & \end{aligned}$$

(b) b suit a (autre méthode).

$$\begin{aligned} (WXabY a Zb T) &= (W j \hat{\Psi} \underline{a} b Y j a Z \underline{b} T) \\ ! \quad (ba ZY b XaTW) &= (b \hat{\wedge} a ZY j b X \underline{a} TW j) \\ ! \quad (a b XZY abTW) &= (a \hat{\Psi} \underline{b} j XZY ab \underline{T} W j) \\ ! \quad (b XZY aba TW) &= (b \hat{\Psi} ZY \underline{a} b j \underline{a} TW j) \\ ! \quad (aba b XZY TW) &\stackrel{\text{rotation}}{!} (Waba b XZY T) \end{aligned}$$

(c) Cas général.

$$\begin{aligned} (WXaUbY a Zb T) &= (WX \underline{a} U b j \hat{\Psi} \underline{a} Z j b T) \\ ! \quad (aY Ubab TWXZ) &= (aY U \underline{b} j \hat{\wedge} \underline{b} T j WXZ) \\ ! \quad (ba b WXZaY UT) &= (b \underline{a} b W j XZ \hat{\wedge} a Y UT j) \\ ! \quad (a XZb WabY UT) &= (a \hat{\wedge} XZ \underline{b} j Wab Y UT j) \\ ! \quad (b Waba XZY UT) &= (b \hat{\wedge} W \underline{a} b j \underline{a} XZY UT j) \\ ! \quad (aba b WXZY UT) & \end{aligned}$$

(d) Cas général avec moins d'étapes.

$$\begin{aligned}
 (W X a U b Y a Z b T) &= (W j \overset{\times}{a} j U b Y \underline{a} Z b T) \\
 ! (W a U b Y a X Z b T) &= (W j a \overset{\circ}{b} Y a j X Z \underline{b} T) \\
 ! (T W b X Z Y a b a U) &= (T W b j X \hat{Z} Y \underline{a} j b a U) \\
 ! (U T W b a b a X Z Y) &\stackrel{\text{rotation}}{=} (W b a b a X Z Y U W)
 \end{aligned}$$

3. Cas elliptique. Le pivot est ici un élément de V_{ell} .

$$(W X \underline{a} Y) ! (W X Y a) \stackrel{\text{rotation}}{=} (a W X Y)$$

Deuxième possibilité :

$$(W j \overset{\times}{a} Y) ! (a W X Y)$$

La longueur de W augmente de 1.

2.5. Algorithme complet. En alternant ces différentes opérations, on obtient l'algorithme suivant. L'algorithme modifie en place un symbole de Farey étendu $(V; ;_{\text{ell}})$ par une suite d'opérations de Siegel. Comme dans le paragraphe précédent, on note le facteur $a_1 a_2 \dots a_n$ de $V = (a_1; \dots; a_n)$ et W est un préfixe de V normalisé, formé de facteurs de la forme $aba b$, aa ou a avec $a = a$.

Algorithme 1 Normalisation d'un symbole de Farey étendu

Entrée: Un symbole de Farey étendu $(V; ;_{\text{ell}})$.

Sortie: Un symbole de Farey étendu normalisé

- 1: $W ; \{\text{le facteur vide}\}$
 - 2: tant que $|jWj| < |jVj|$ faire
 - 3: si il existe un facteur W^0 de V normalisé contenant strictement W alors
 - 4: $W \leftarrow W^0; \{jWj \text{ augmente de } |jW^0j| - |jWj|\}$
 - 5: sinon si il existe a hors de W tel que $d(a; a) = 0$ alors
 - 6: appliquer l'opération de Siegel elliptique de pivot $a; \{jWj \text{ augmente de } 1.\}$
 - 7: sinon si il existe a hors de W tel que $d(a; a) = 1$ alors
 - 8: appliquer l'opération de Siegel parabolique de pivot $a; \{jWj \text{ augmente de } 2.\}$
 - 9: sinon si il existe hors de W deux arcs entrelacés a et b alors
 - 10: appliquer l'opération de Siegel hyperbolique de pivots a et $b; \{jWj \text{ augmente de } 4.\}$
 - 11: retourner le symbole de Farey étendu obtenu.
-

Démonstration. Pour voir que l'algorithme termine, il suffit de remarquer que tant que W est différent de V , au moins l'une des quatre conditions a lieu. En effet, si aucune des trois premières conditions n'est vérifiée, on cherche le premier arc f suivant W tel que f précède f . Ni f , ni f ne sont dans W . On prend alors comme pivot $a = f$ et b l'arc suivant a , les arcs a et b étant alors nécessairement entrelacés.

2.6. Un exemple détaillé : $\Gamma_0(22)$. L'entrée est un symbole de Farey arbitraire pour $\Gamma_0(22)$, ici un symbole de Farey unimodulaire obtenu avec l'algorithme de Kulkarni. La partie W déjà normalisée est indiquée entre parenthèses, les deux pivots choisis pour l'étape sont soulignés :

$1 \} 1 \} 0 \} \frac{1}{4} \} \frac{3}{11} \} \frac{2}{7} \} \frac{1}{3} \} \frac{4}{11} \} \frac{3}{8} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$
 $(\ 1 \ 1) \ 2 \ 3 \ \underline{4} \ 5 \ \underline{4} \ 3 \ 6 \ 7 \ 2 \ 5 \ 6 \ 7$

$1 \} 1 \} 0 \} \frac{1}{4} \} \frac{3}{11} \} \frac{5}{18} \} \frac{7}{25} \} \frac{9}{32} \} \frac{38}{135} \} \frac{447}{1588} \} \frac{409}{1453} \} \frac{20}{71} \} \frac{5}{17} \} \frac{8}{23} \} 1$
 $(\ 1 \ 1) \ 2 \ \underline{3} \ \underline{3} \ 4 \ 5 \ 2 \ 4 \ 5 \ (\ 6 \ 7 \ 6 \ 7$

$1 \} 1 \} 0 \} \frac{1}{4} \} \frac{5}{19} \} \frac{9}{34} \} \frac{40}{151} \} \frac{471}{1778} \} \frac{431}{1627} \} \frac{3}{11} \} \frac{409}{1453} \} \frac{20}{71} \} \frac{5}{17} \} \frac{8}{23} \} 1$
 $(\ 1 \ 1) \ \underline{2} \ \underline{3} \ 4 \ 2 \ 3 \ 4 \ (\ 5 \ 5 \ 6 \ 7 \ 6 \ 7$

$1 \} 1 \} 0 \} \frac{1}{18} \} \frac{11}{197} \} \frac{1}{15} \} \frac{6}{23} \} \frac{94}{355} \} \frac{431}{1627} \} \frac{3}{11} \} \frac{409}{1453} \} \frac{20}{71} \} \frac{5}{17} \} \frac{8}{23} \} 1$
 $(\ 1 \ 1 \ 2 \ 2 \ 3 \ 4 \ 3 \ 4 \ 5 \ 5 \ 6 \ 7 \ 6 \ 7)$

Ce dernier symbole est normalisé.

Proposition 2.1 . On obtient à partir du symbole de Farey étendu \mathcal{F} un système de générateurs de $\mathcal{H}_0 = Z[P^1(\mathbb{Q})]_0$ en tant que $Z[\mathcal{F}_0(N)]$ -module formé des a_i, b_i de type hyperbolique et des c elliptiques et paraboliques de la proposition précédente avec les relations du même type qu'avant.

$$\sum_{i=1}^{g_X(N)} (1 - a_i) a_i + \sum_{i=1}^{g_X(N)} (1 - b_i) b_i + \sum_{c \in V_{\text{par}}} (1 - c) c + \sum_{c \in V_{\text{ell}}} c = 0$$

$(1 + c) c = 0$ pour $c \in V_{\text{ell},2}$
 $(1 + c + \frac{2}{c}) c = 0$ pour $c \in V_{\text{ell},3}$

Proposition 2.2 . Par l'application naturelle $Z[P^1(\mathbb{Q})]_0 \rightarrow H_1(X_0(N); Z)$ ($a \neq 0$), la classe d'homologie des éléments de type elliptique et des éléments de type parabolique est nulle, les classes d'homologie des éléments a_i et b_i de type hyperbolique pour

$i = 1, \dots, g_0(N)$ forment une base symplectique de $H_1(X_0(N); \mathbb{Z})$, c'est-à-dire vérifiant

$$a_i \cdot a_j = 0; \quad b_i \cdot b_j = 0; \quad a_i \cdot b_j = \delta_{ij} \quad b_j \cdot a_i = -\delta_{ij}$$

pour le produit d'intersection de $H_1(X_0(N); \mathbb{Z})$.

```
? [V1,Ast1]=mspolygon(msinit(13,2));
? isnormalized(Ast0)
%294 = ["a1", "a*1", "e2", "e3", "e4", "e5"]
? [V0,Ast0,T]=mspolygon(msinit(13,2),2);
? vector(#T,i,trace(T[i]))
%58 = [-2, 2, -1, 0, 0, -1]
```

Dans ce dernier cas, le polygone unimodulaire calculé par `msinit` est déjà normalisé ! Mais je ne voulais pas prendre de trop grandes valeurs ! La courbe $X_0(N)$ a quatre points elliptiques (deux points elliptiques d'ordre 2, $e3$ et $e4$ correspondant à la trace 0 et deux points elliptiques d'ordre 3, $e2$ et $e5$, correspondant à la trace -1), deux pointes (0 et la pointe ayant une matrice de transition hyperboliques (de trace 2) et est de genre 0.

On a

$$\begin{aligned} \sum_{i=1}^g H_{1; 2i} &= (1)^k H_{2; 1i} \\ H_{1; 1; 0; 1} &= 0 \\ H_{1; 0; 1; 2} &= 0 \end{aligned}$$

2.7. Conclusion. La normalisation d'un symbole de Farey se révèle très coûteuse : la taille des rationnels $p=q$ intervenant dans le symbole normalisé augmente exponentiellement dans notre implantation pour $X_0(N)$. Plus précisément, la hauteur $\max(|jp|; |jq|)$ des rationnels intervenant dans le symbole fourni par l'algorithme de Kulkarni est $O(\log N)$. Nous ne savons pas borner exactement la hauteur des rationnels intervenant dans sa normalisation : elle est trivialement en $O(2^N)$; expérimentalement, elle se révèle un peu inférieure à $N=2$ pour $N \leq 40000$. Notre implantation de l'algorithme de Kulkarni calcule un symbole de Farey unimodulaire pour $X_0(40000)$ en 6 secondes, et il faut environ une heure pour le normaliser.

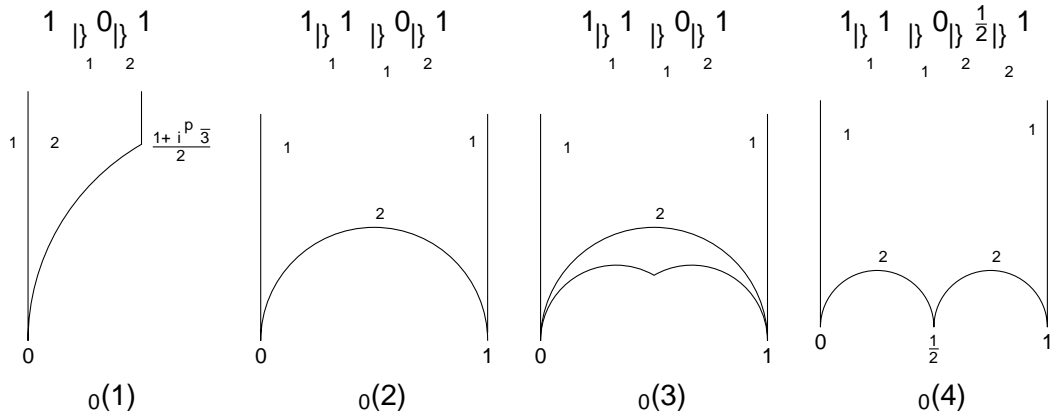
Il serait intéressant d'estimer précisément la taille du symbole de Farey normalisé obtenu, mais surtout de la minimiser, en changeant l'ordre des opérations ou en utilisant d'autres opérations de base. Nous n'y sommes pas parvenus. Nous n'avons pas non plus d'application algorithmique dans laquelle utiliser un symbole normalisé serait plus avantageux qu'utiliser un symbole de Farey unimodulaire. Nous sommes donc intéressés par toute suggestion.

Annexe A. Exemples

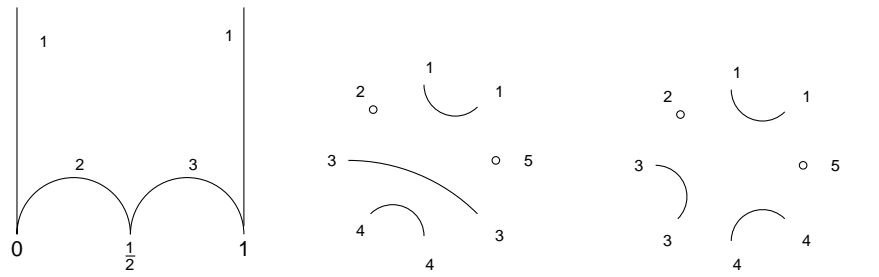
Donnons quelques exemples que l'on peut déduire des implémentations dans Pari/GP. Le groupe $\Gamma_0(N)$ est toujours le sous-groupe de congruence $\Gamma_0(N)$. Dans le cas où le symbole de Farey unimodulaire n'est pas normalisé, nous donnons aussi un symbole de Farey normalisé. La syntaxe GP est

```
mspolygon(N,0) \ \ symbole de Farey unimodulaire
mspolygon(N,1) \ \ symbole de Farey normalisé
```

Nous donnons le symbole de Farey, la représentation de l'involution du symbole de Farey unimodulaire et du symbole de Farey normalisé et dans les petits cas les polygones hyperboliques obtenus. Les noms i permettent de donner l'involution (ils sont bien sûr d'évidents pour le symbole de Farey unimodulaire et le symbole de Farey normalisé).



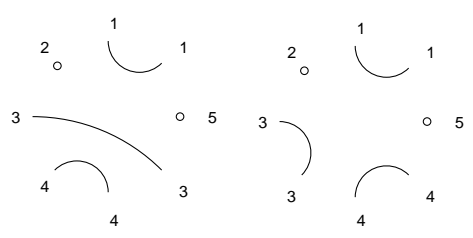
$$\begin{array}{cccc}
 1 \} 0 \} 1 & 1 \} 1 \} 0 \} 1 & 1 \} 1 \} 0 \} 1 & 1 \} 1 \} 0 \} \frac{1}{2} \} 1 \\
 1 \quad 2 & 1 \quad 1 \quad 2 & 1 \quad 1 \quad 2 & 1 \quad 1 \quad 2 \quad 2
 \end{array}$$



$$\begin{array}{ccc}
 1 \} 1 \} 0 \} \frac{1}{2} \} 1 & 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{1}{2} \} \frac{2}{3} \} 1 & 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} 1 \\
 1 \quad 1 \quad 2 \quad 3 & 1 \quad 1 \quad 2 \quad 3 \quad 3 \quad 2 & 1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 3
 \end{array}$$

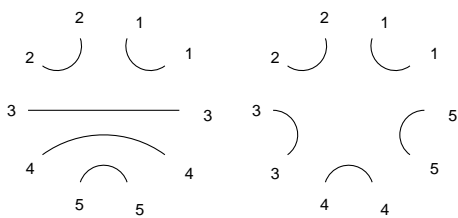
$$\begin{array}{ccc}
 o(7) : 1 \} 1 \} 0 \} \frac{1}{2} \} 1; & o(8) : 1 \} 1 \} 0 \} \frac{1}{4} \} \frac{1}{3} \} \frac{1}{2} \} 1; & o(9) : 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{1}{2} \} \frac{2}{3} \} 1 \\
 1 \quad 1 \quad 2 \quad 3 & 1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 3 & 1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 3
 \end{array}$$

$$\begin{array}{cc}
 o(10) : 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} 1; & 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{2}{5} \} \frac{3}{7} \} \frac{1}{2} \} \frac{2}{3} \} 1 \\
 1 \quad 1 \quad 2 \quad 3 \quad 4 \quad 4 \quad 3 \quad 5 & 1 \quad 1 \quad 2 \quad 3 \quad 3 \quad 4 \quad 4 \quad 5
 \end{array}$$

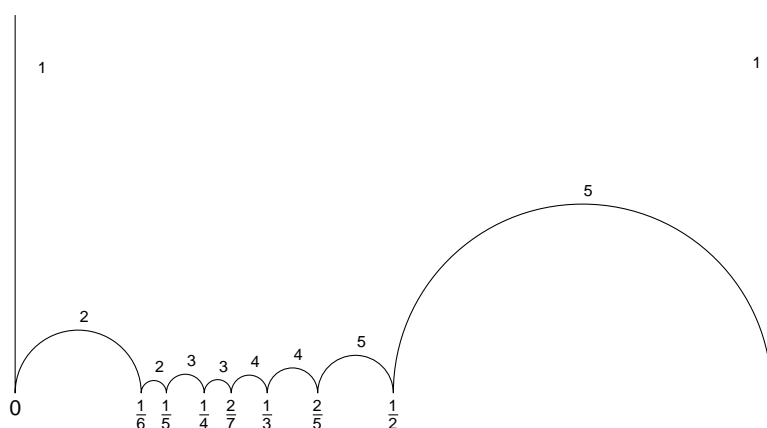
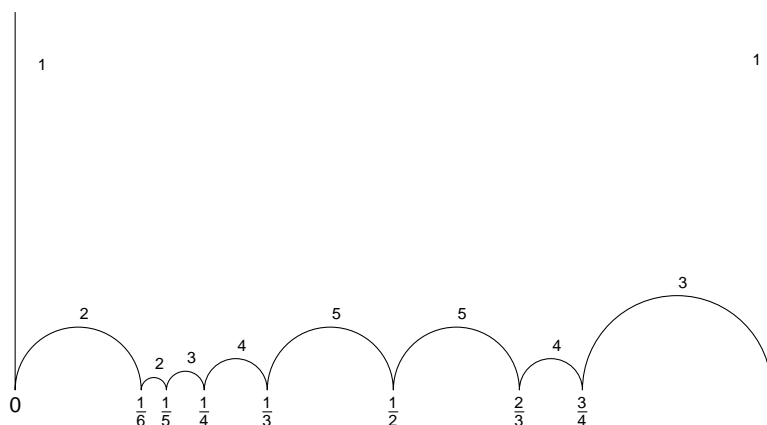


$$o(11) : 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{1}{2} \} \frac{2}{3} \} 1$$

$$o(12) : 1 \} 1 \} 0 \} \frac{1}{6} \} \frac{1}{5} \} \frac{1}{4} \} \frac{1}{3} \} \frac{1}{2} \} \frac{2}{3} \} \frac{3}{4} \} 1; \quad 1 \} 1 \} 0 \} \frac{1}{6} \} \frac{1}{5} \} \frac{1}{4} \} \frac{2}{7} \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} 1$$

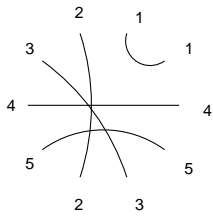


On voit sur ce dernier symbole de Farey étendu que $\mathcal{X}_0(12)$ est de genre 0, n'a pas de points elliptiques et a 4 pointes (les pointes autres que 0 sont en bijection avec les chemins allant de 0 à 0 en passant par p).).



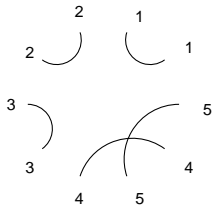
$$o(13) : 1 \} 1 \} 0 \} \frac{1}{3} \} \frac{1}{2} \} \frac{2}{3} \} 1$$

Table 1. N = 15



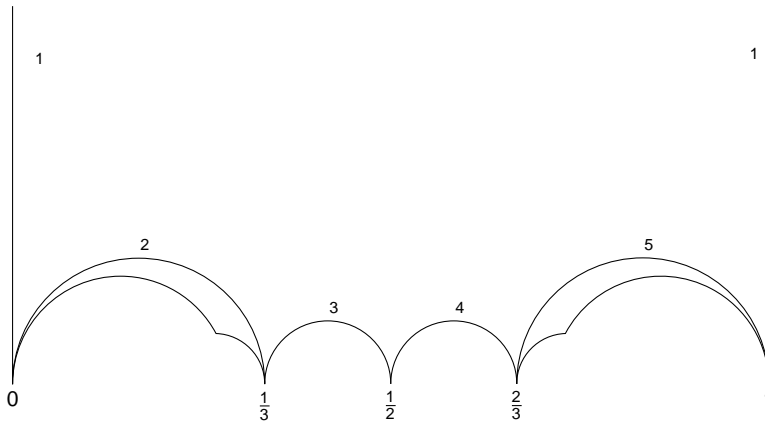
$$1 \left| \right. 1 \left. \right| 0 \left| \right. \frac{1}{5} \left| \right. \frac{1}{4} \left| \right. \frac{1}{3} \left| \right. \frac{2}{5} \left| \right. \frac{1}{2} \left| \right. \frac{3}{5} \left| \right. \frac{2}{3} \left. \right| 1$$

1 1 2 3 4 5 2 3 5 4



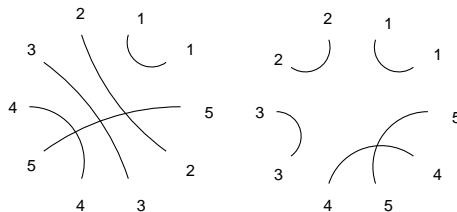
$$1 \left| \right. 1 \left. \right| 0 \left| \right. \frac{1}{12} \left| \right. \frac{5}{59} \left| \right. \frac{3}{35} \left| \right. \frac{13}{151} \left| \right. \frac{1}{8} \left| \right. \frac{3}{13} \left| \right. \frac{8}{19} \left. \right| 1$$

1 1 2 2 3 3 4 5 4 5



$$o(14) : 1 \left| \right. 1 \left. \right| 0 \left| \right. \frac{1}{4} \left| \right. \frac{2}{7} \left| \right. \frac{1}{3} \left| \right. \frac{2}{5} \left| \right. \frac{3}{7} \left| \right. \frac{1}{2} \left| \right. \frac{2}{3} \left. \right| 1; \quad 1 \left| \right. 1 \left. \right| 0 \left| \right. \frac{1}{4} \left| \right. \frac{7}{27} \left| \right. \frac{2}{7} \left| \right. \frac{13}{43} \left| \right. \frac{10}{33} \left| \right. \frac{1}{3} \left| \right. \frac{2}{5} \left. \right| 1$$

1 1 2 3 4 5 4 3 2 5 1 1 2 2 3 3 4 5 4 5



Les arcs α_4 and α_5 du deuxième symbole de Farey étendu se projettent dans $X_0(14)$ en des lacets et donnent une base symplectique de $H_1(X_0(14); \mathbb{Z})$ pour le produit d'intersection. Les arcs α_4 et α_5 sont de type hyperbolique, les arcs α_1 , α_2 et α_3 sont de type parabolique.

Table 2. N = 16

	$1 \rangle 1 \rangle 0 \rangle \frac{1}{4} \rangle \frac{1}{3} \rangle \frac{3}{8} \rangle \frac{2}{5} \rangle \frac{1}{2} \rangle \frac{2}{3} \rangle \frac{3}{4} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 2 3 3 4 4 5 5 </small>
	$1 \rangle 1 \rangle 0 \rangle \frac{1}{4} \rangle \frac{1}{3} \rangle \frac{3}{8} \rangle \frac{2}{5} \rangle \frac{1}{2} \rangle \frac{2}{3} \rangle \frac{3}{4} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 2 3 3 4 4 5 5 </small>

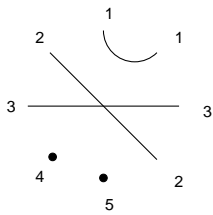
Table 3. N = 17

	$1 \rangle 1 \rangle 0 \rangle \frac{1}{4} \rangle \frac{1}{3} \rangle \frac{2}{5} \rangle \frac{1}{2} \rangle \frac{2}{3} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 3 4 5 3 5 </small>
	$1 \rangle 1 \rangle 0 \rangle \frac{1}{4} \rangle \frac{1}{3} \rangle \frac{3}{8} \rangle \frac{11}{29} \rangle \frac{8}{21} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 3 4 3 4 5 </small>

Table 4. N = 18

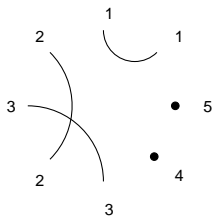
	$1 \rangle 1 \rangle 0 \rangle \frac{1}{6} \rangle \frac{1}{5} \rangle \frac{2}{9} \rangle \frac{1}{4} \rangle \frac{1}{3} \rangle \frac{1}{2} \rangle \frac{5}{9} \rangle \frac{4}{7} \rangle \frac{7}{12} \rangle \frac{3}{5} \rangle \frac{2}{3} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 2 3 4 5 5 4 3 6 6 7 7 </small>
	$1 \rangle 1 \rangle 0 \rangle \frac{1}{6} \rangle \frac{1}{5} \rangle \frac{2}{9} \rangle \frac{3}{13} \rangle \frac{1}{4} \rangle \frac{6}{23} \rangle \frac{1}{3} \rangle \frac{4}{7} \rangle \frac{7}{12} \rangle \frac{3}{5} \rangle \frac{2}{3} \rangle 1$ <small style="display: flex; justify-content: space-around; width: 100%;"> 1 1 2 2 3 3 4 4 5 5 6 6 7 7 </small>

Table 5. N = 19



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{1}{2} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} 1$$

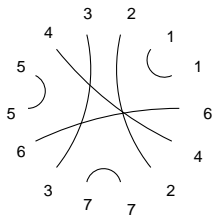
1 1 2 3 4 5 2 3



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{8}{23} \left\} \frac{7}{20} \left\} \frac{4}{11} \left\} 1$$

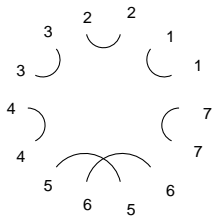
1 1 2 3 2 3 4 5

Table 6. N = 20



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{1}{4} \left\} \frac{2}{7} \left\} \frac{3}{10} \left\} \frac{1}{3} \left\} \frac{3}{8} \left\} \frac{2}{5} \left\} \frac{1}{2} \left\} \frac{3}{5} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} 1$$

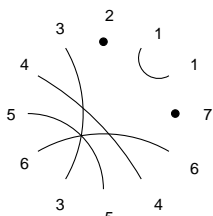
1 1 2 3 4 5 5 6 3 7 7 2 4 6



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{4}{19} \left\} \frac{3}{14} \left\} \frac{11}{51} \left\} \frac{107}{496} \left\} \frac{524}{2429} \left\} \frac{8}{37} \left\} \frac{3}{11} \left\} \frac{73}{253} \left\} \frac{20}{69} \left\} \frac{3}{10} \left\} 1$$

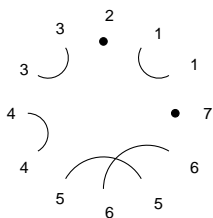
1 1 2 2 3 3 4 4 4 5 6 5 6 7 7

Table 7. N = 21



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{4} \left\} \frac{2}{7} \left\} \frac{1}{3} \left\} \frac{2}{5} \left\} \frac{3}{7} \left\} \frac{1}{2} \left\} \frac{2}{3} \left\} \frac{5}{7} \left\} \frac{3}{4} \left\} 1$$

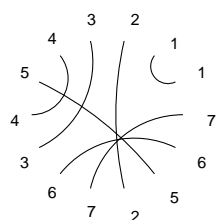
1 1 2 3 4 5 6 3 5 4 6 7



$$1 \left\} 1 \left\} 0 \left\} \frac{1}{4} \left\} \frac{7}{27} \left\} \frac{48}{185} \left\} \frac{89}{343} \left\} \frac{219}{844} \left\} \frac{13}{50} \left\} \frac{3}{10} \left\} \frac{7}{16} \left\} \frac{3}{4} \left\} 1$$

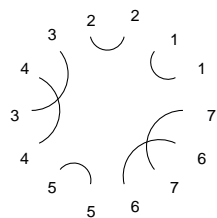
1 1 2 3 3 4 4 4 5 6 5 6 7

Table 8. N = 22



$$1 \} 1 \} 0 \} \frac{1}{4} \} \frac{3}{11} \} \frac{2}{7} \} \frac{1}{3} \} \frac{4}{11} \} \frac{3}{8} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

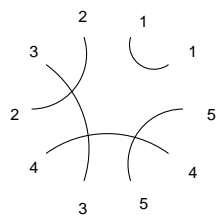
1 1 2 3 4 5 4 3 6 7 2 5 6 7



$$1 \} 1 \} 0 \} \frac{1}{18} \} \frac{11}{197} \} \frac{1}{15} \} \frac{6}{23} \} \frac{94}{355} \} \frac{431}{1627} \} \frac{3}{11} \} \frac{409}{1453} \} \frac{20}{71} \} \frac{5}{17} \} \frac{8}{23} \} 1$$

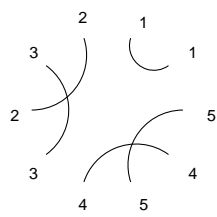
1 1 2 2 3 4 3 4 5 5 6 7 6 7

Table 9. N = 23



$$1 \} 1 \} 0 \} \frac{1}{4} \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

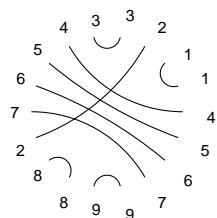
1 1 2 3 2 4 3 5 4 5



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{10}{49} \} \frac{29}{142} \} \frac{19}{93} \} \frac{3}{14} \} \frac{3}{10} \} \frac{7}{19} \} 1$$

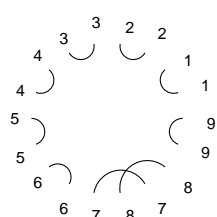
1 1 2 3 2 3 4 5 4 5

Table 10. N = 24



$$1 \} 1 \} 0 \} \frac{1}{7} \} \frac{1}{6} \} \frac{1}{5} \} \frac{1}{4} \} \frac{1}{3} \} \frac{3}{8} \} \frac{5}{13} \} \frac{2}{5} \} \frac{5}{12} \} \frac{3}{7} \} \frac{1}{2} \} \frac{3}{5} \} \frac{5}{8} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

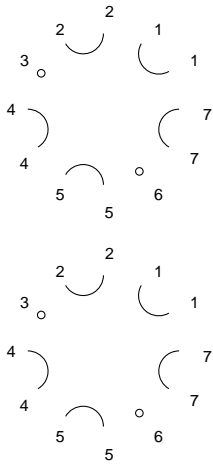
1 1 2 3 3 4 5 6 7 2 8 8 9 9 7 6 5 4



$$1 \} 1 \} 0 \} \frac{1}{12} \} \frac{1}{11} \} \frac{1}{10} \} \frac{5}{49} \} \frac{9}{88} \} \frac{22}{215} \} \frac{4}{39} \} \frac{42}{409} \} \frac{7}{68} \} \frac{105}{1019} \} \frac{3}{29} \} \frac{1}{7} \} \frac{29}{191} \} \frac{9}{59} \} \frac{1}{6} \} 1$$

1 1 2 2 3 3 4 4 5 5 6 6 7 8 7 8 9 9

Table 11. N = 25



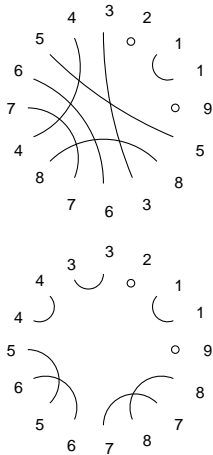
$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{2}{5} \left\} \frac{1}{2} \left\} \frac{3}{5} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} \frac{4}{5} \left\} 1$$

$$1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 4 \quad 4 \quad 5 \quad 5 \quad 6 \quad 7 \quad 7$$

$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{2}{5} \left\} \frac{1}{2} \left\} \frac{3}{5} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} \frac{4}{5} \left\} 1$$

$$1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 4 \quad 4 \quad 5 \quad 5 \quad 6 \quad 7 \quad 7$$

Table 12. N = 26



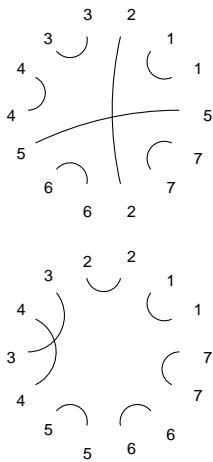
$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{3}{8} \left\} \frac{5}{13} \left\} \frac{2}{5} \left\} \frac{1}{2} \left\} \frac{3}{5} \left\} \frac{8}{13} \left\} \frac{5}{8} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} \frac{4}{5} \left\} 1$$

$$1 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 4 \quad 8 \quad 7 \quad 6 \quad 3 \quad 8 \quad 5 \quad 9$$

$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{8}{39} \left\} \frac{15}{73} \left\} \frac{7}{34} \left\} \frac{76}{369} \left\} \frac{14}{67} \left\} \frac{9}{35} \left\} \frac{115}{439} \left\} \frac{22}{83} \left\} \frac{13}{49} \left\} \frac{1}{3} \left\} \frac{2}{5} \left\} \frac{4}{5} \left\} 1$$

$$1 \quad 1 \quad 2 \quad 3 \quad 3 \quad 4 \quad 4 \quad 5 \quad 6 \quad 5 \quad 6 \quad 7 \quad 8 \quad 7 \quad 8 \quad 9$$

Table 13. N = 27



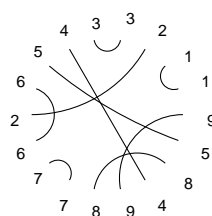
$$1 \left\} 1 \left\} 0 \left\} \frac{1}{5} \left\} \frac{2}{9} \left\} \frac{1}{4} \left\} \frac{1}{3} \left\} \frac{2}{5} \left\} \frac{3}{7} \left\} \frac{4}{9} \left\} \frac{1}{2} \left\} \frac{3}{5} \left\} \frac{2}{3} \left\} \frac{3}{4} \left\} 1$$

$$1 \quad 1 \quad 2 \quad 3 \quad 3 \quad 4 \quad 4 \quad 5 \quad 6 \quad 6 \quad 2 \quad 7 \quad 7 \quad 5$$

$$1 \left\} 1 \left\} 0 \left\} \frac{1}{6} \left\} \frac{3}{17} \left\} \frac{2}{11} \left\} \frac{1}{5} \left\} \frac{7}{34} \left\} \frac{48}{233} \left\} \frac{13}{63} \left\} \frac{17}{82} \left\} \frac{5}{24} \left\} \frac{13}{62} \left\} \frac{2}{9} \left\} 1$$

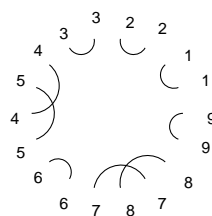
$$1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \quad 4 \quad 5 \quad 5 \quad 6 \quad 6 \quad 7 \quad 7$$

Table 14. N = 28



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{3}{14} \} \frac{2}{9} \} \frac{1}{4} \} \frac{2}{7} \} \frac{1}{3} \} \frac{2}{5} \} \frac{3}{7} \} \frac{1}{2} \} \frac{4}{7} \} \frac{3}{5} \} \frac{5}{8} \} \frac{2}{3} \} \frac{5}{7} \} \frac{3}{4} \} 1$$

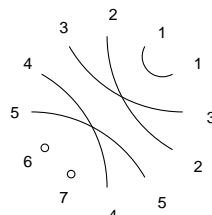
1 1 2 3 3 4 5 6 2 6 7 7 8 9 4 8 5 9



$$1 \} 1 \} 0 \} \frac{1}{24} \} \frac{7}{167} \} \frac{5}{119} \} \frac{33}{785} \} \frac{1}{19} \} \frac{5}{33} \} \frac{151}{965} \} \frac{193}{1233} \} \frac{1}{6} \} \frac{332}{1917} \} \frac{3}{17} \} \frac{8}{39} \} \frac{149}{713} \} \frac{32}{153} \} \frac{3}{14} \} 1$$

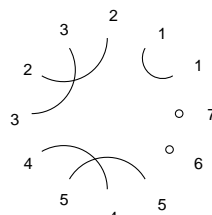
1 1 2 2 3 3 4 5 4 5 6 6 7 8 7 8 9 9

Table 15. N = 29



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} \frac{4}{5} \} 1$$

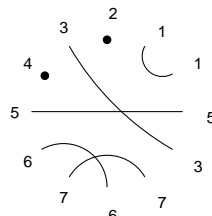
1 1 2 3 4 5 6 7 4 5 2 3



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{16}{63} \} \frac{15}{59} \} \frac{3}{11} \} \frac{3}{8} \} \frac{21}{52} \} \frac{24}{59} \} \frac{7}{17} \} 1$$

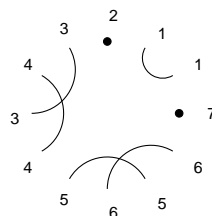
1 1 2 3 2 3 4 5 4 5 6 7

Table 16. N = 31



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{2}{7} \} \frac{1}{3} \} \frac{2}{5} \} \frac{1}{2} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

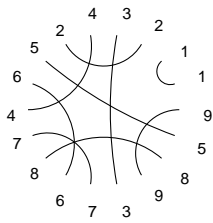
1 1 2 3 4 5 6 7 6 7 3 5



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{4}{15} \} \frac{55}{206} \} \frac{51}{191} \} \frac{34}{127} \} \frac{41}{153} \} \frac{73}{272} \} \frac{18}{67} \} 1$$

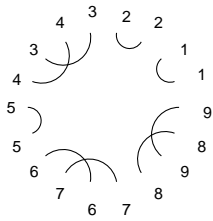
1 1 2 3 4 3 4 5 6 5 6 7

Table 17. N = 35



$$1 \} 1 \} 0 \} \frac{1}{6} \} \frac{1}{5} \} \frac{1}{4} \} \frac{3}{11} \} \frac{2}{7} \} \frac{1}{3} \} \frac{2}{5} \} \frac{3}{7} \} \frac{1}{2} \} \frac{4}{7} \} \frac{3}{5} \} \frac{5}{8} \} \frac{2}{3} \} \frac{5}{7} \} \frac{3}{4} \} 1$$

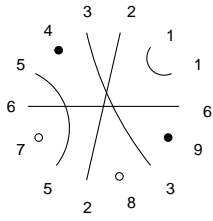
1 1 2 3 4 2 5 6 4 7 8 6 7 3 9 8 5 9



$$1 \} 1 \} 0 \} \frac{1}{7} \} \frac{5}{34} \} \frac{9}{61} \} \frac{4}{27} \} \frac{67}{452} \} \frac{197}{1329} \} \frac{3}{20} \} \frac{790}{5251} \} \frac{229}{1521} \} \frac{55}{356} \} \frac{214}{1369} \} \frac{1085}{6931} \} \frac{8}{51} \} \frac{5}{27} \} \frac{14}{53} \} 1$$

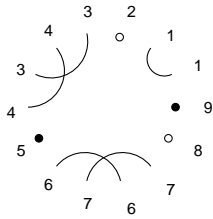
1 1 2 2 3 4 3 4 5 5 6 7 6 7 8 9 8 9 8 9

Table 18. N = 37



$$1 \} 1 \} 0 \} \frac{1}{5} \} \frac{1}{4} \} \frac{1}{3} \} \frac{3}{8} \} \frac{2}{5} \} \frac{3}{7} \} \frac{1}{2} \} \frac{4}{7} \} \frac{3}{5} \} \frac{2}{3} \} \frac{3}{4} \} 1$$

1 1 2 3 4 5 6 7 5 2 8 3 9 6

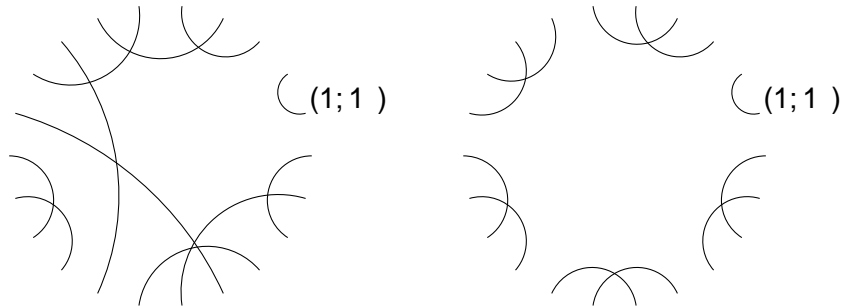


$$1 \} 1 \} 0 \} \frac{1}{6} \} \frac{2}{11} \} \frac{1}{5} \} \frac{1}{4} \} \frac{11}{43} \} \frac{21}{82} \} \frac{10}{39} \} \frac{6}{23} \} \frac{5}{19} \} \frac{51}{193} \} \frac{7}{26} \} 1$$

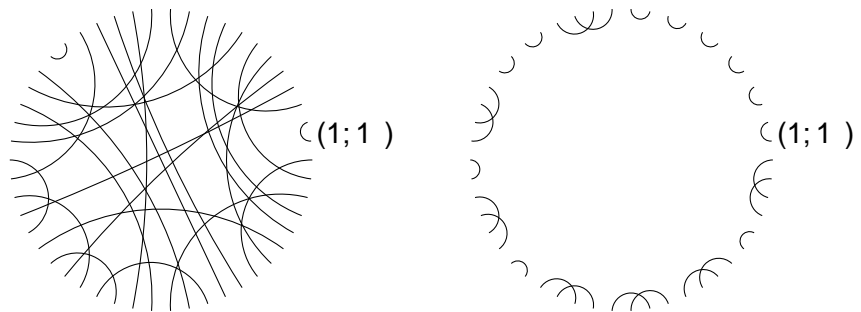
1 1 2 3 4 3 4 5 6 7 6 7 8 9

Nous ne montrons désormais que la représentation des involutions.

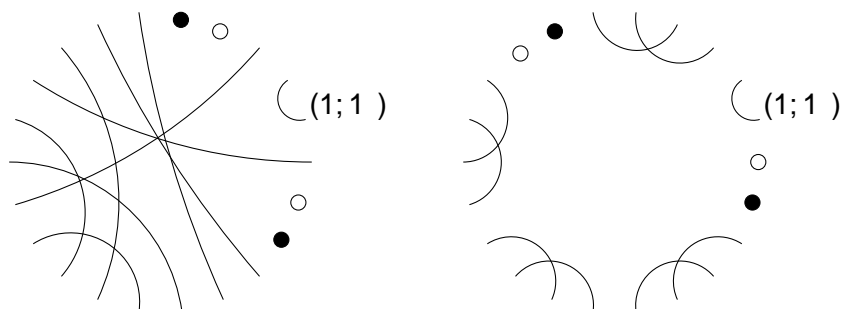
N = 59

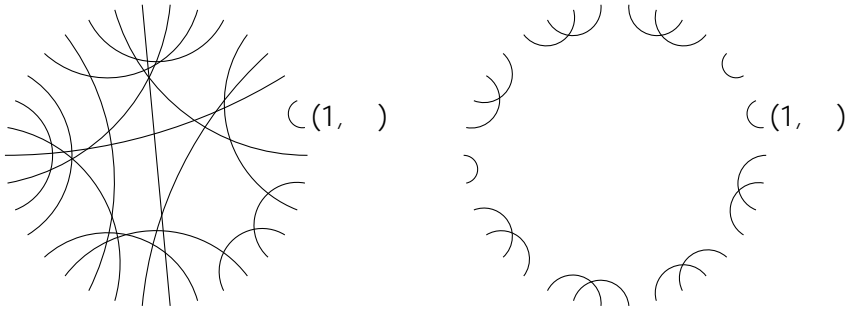
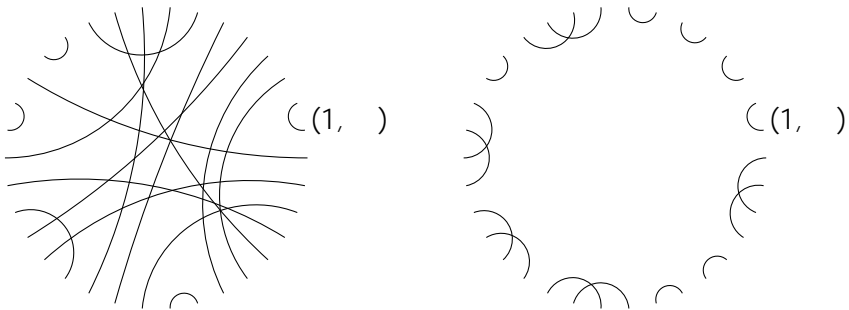
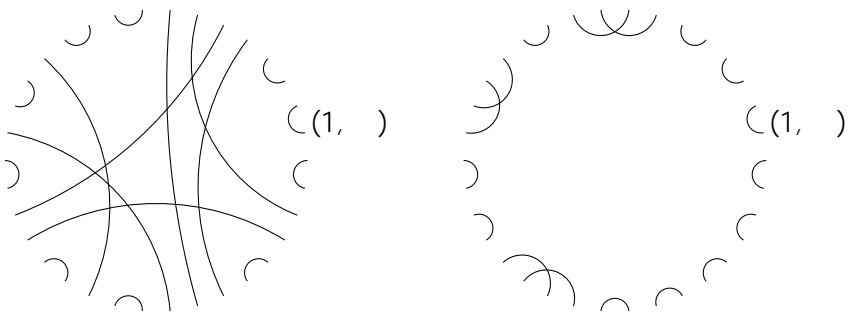


N = 60

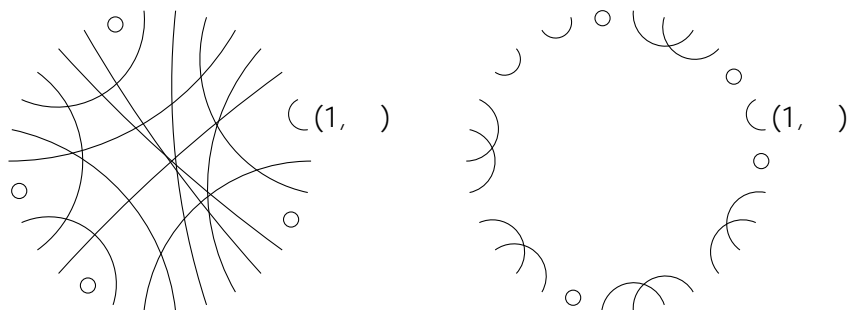


N = 61

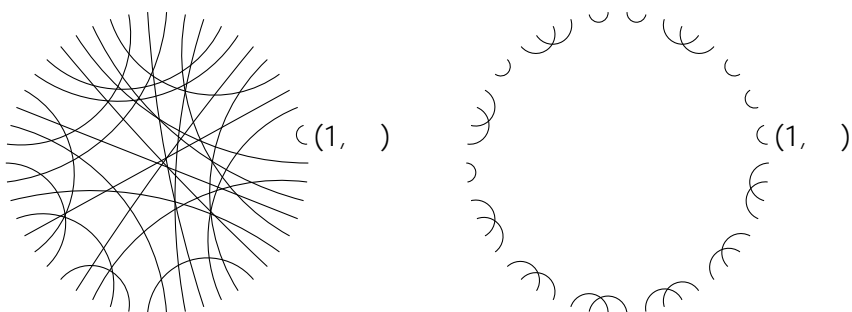


$N = 62$  $N = 63$  $N = 64$ 

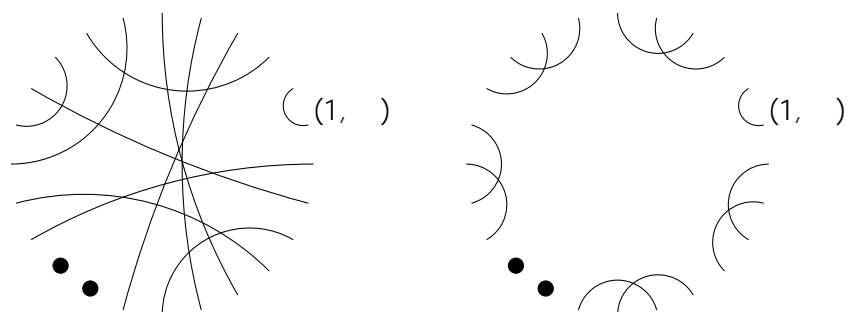
$N = 65$

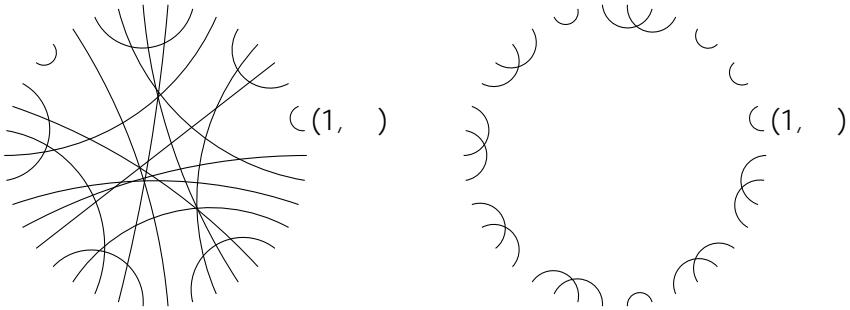
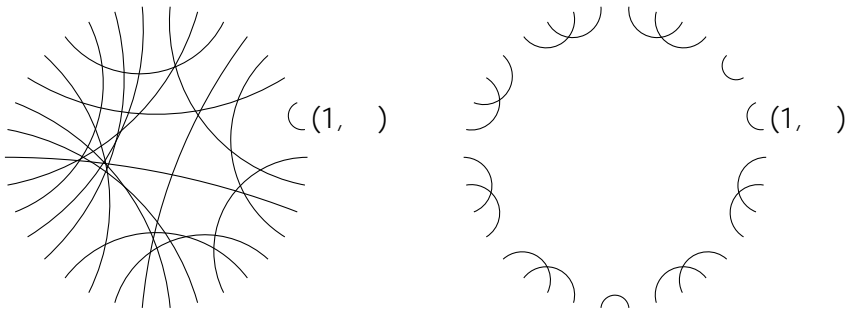
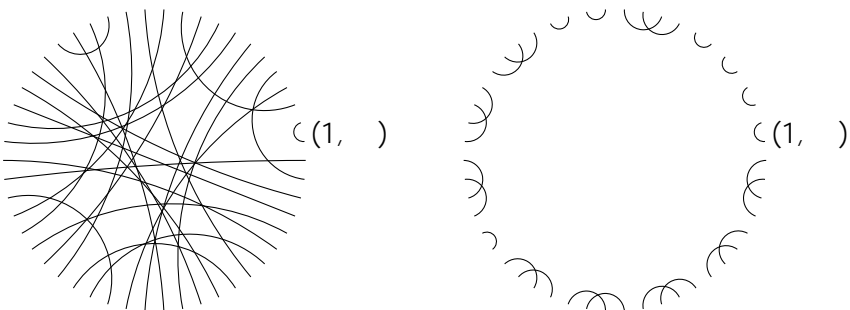


$N = 66$



$N = 67$



$N = 68$  $N = 69$  $N = 70$ 

Références

- [1] J.-B. Bost, « Introduction to Compact Riemann Surfaces, Jacobians, and Abelian Varieties », in *From number theory to physics (Les Houches, 1989)*, Springer, 1989, p. 64-211.
- [2] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.
- [3] A. Doms, E. Jespers, A. Konovalov & H. Verrill, « Congruence - Congruence subgroups of $SL_2(\mathbb{Z})$, Version 1.2.2 », 2018, <https://www.gap-system.org/Packages/congruence.html>.
- [4] R. S. Kulkarni, « An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group », *Am. J. Math.* **113** (1991), n° 6, p. 1053-1133.
- [5] C. A. Kurth & L. Long, « Computations with finite index subgroups of $PSL_2(\mathbb{Z})$ using Farey symbols », in *Advances in algebra and combinatorics*, World Scientific, 2008, p. 225-242.
- [6] B. Maskit, « On Poincaré's Theorem for Fundamental Polygons », *Adv. Math.* **7** (1971), p. 219-230.
- [7] H. Poincaré, « Théorie des groupes fuchsien », *Acta Math.* **1** (1882), p. 1-62.
- [8] R. Pollack & G. Stevens, « Overconvergent modular symbols and p -adic L -functions », *Ann. Sci. Éc. Norm. Supér.* **44** (2011), n° 1, p. 1-42.
- [9] C. L. Siegel, *Topics in complex function theory. Vol. I : Elliptic functions and uniformization theory*, Interscience Tracts in Pure and Applied Mathematics, vol. 25, Wiley-Interscience, 1969.
- [10] H. Verrill, « Fundamental domain drawer », 2000, <https://wstein.org/Tables/fundomain/>.

Karim Belabas, Univ. Bordeaux, CNRS, INRIA, IMB, UMR 5251, F-33400 Talence, France
E-mail : Karim.Belabas@math.u-bordeaux.fr

Dominique Bernardi, Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche, F-75005 Paris, France • *E-mail* : dominique.bernardi@imj-prg.fr

Bernadette Perrin-Riou, Laboratoire de Mathématiques d'Orsay, Univ. Paris-Sud, CNRS, Université Paris-Saclay, F-91405 Orsay, France. • *E-mail* : bernadette.perrin-riou@universite-paris-saclay.fr