

CONSTRUCTION COMBINATOIRE D'UN GROUPE D'HURWITZ

TRAVAIL PRÉSENTÉ PAR
PAUL LIBBRECHT
POUR L'OBTENTION DU
DIPLOME DE MATHÉMATHICIEN

SOUS LA DIRECTION DU PROFESSEUR OSCAR BURLET ET
L'EXPERTISE DU PROFESSEUR MARC TROYANOV

Introduction

En 1893, Adolf Hurwitz a prouvé par des moyens analytiques qu'une surface complexe de genre g supérieur ou égal à 2 ne pouvait avoir plus de $84 \cdot (g - 1)$ transformations conformes. Depuis, de nombreuses personnes ont modélisés la géométrie conforme complexe en la géométrie hyperbolique, à commencer par Poincaré, Klein et Siegel.

Le théorème était là mais il a été difficile d'aller plus loin, c'est-à-dire de donner la liste des groupes de transformations conformes qui atteignaient cette borne maximale, ils s'appelleront les groupes d'Hurwitz. Le travail est encore, selon notre connaissance inachevé.

Le présent travail de diplôme se propose de redémontrer les étapes essentielles de ce théorème en appliquant le formalisme de la géométrie hyperbolique et en parallèle de construire un exemple de groupe d'Hurwitz par un moyen combinatoire privilégié: le graphe de Cayley d'un groupe. L'exemple sera le groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ agissant sur une surface de genre 3.

Nous admettrons les connaissances élémentaires de géométrie différentielle (pour cela, le livre [*Berger-Gostiaux (1987)*] peut constituer un excellent rappel), de la théorie des revêtements (c.f. [*Wolf (1974)*, pp 31-42]) et de la géométrie hyperbolique (un livre élémentaire peut y introduire [*Lyndon (1984)*], des énoncés plus conséquents se trouvent dans [*Zieschang (1981)*, pp 10-43], enfin [*Magnus (1974)*] peut donner une bonne culture générale).

Le texte est organisé de la façon suivante: les trois premiers chapitres introduisent aux outils combinatoires étudiés ici, les trois suivants démontrent les théorèmes géométriques qui nous serviront; les deux derniers chapitres font une synthèse de ces deux facettes afin de prouver que notre groupe est bien un groupe d'Hurwitz et de s'approcher d'une réalisation abordable de la surface et de son pavage.

Plus précisément, le chapitre premier donne les premières définitions nécessaires à l'observation du groupe qui deviendra groupe d'Hurwitz, il prouve en outre la simplicité des groupes $\mathrm{PSL}_n(\mathbb{K})$; le chapitre II a pour ambition de donner un cadre parfaitement rigoureux aux graphes de Cayley en s'approchant le plus possible d'une "utilisation pratique" de cet outil; le chapitre III utilise les deux précédents pour déterminer une présentation de PSL_2 ; le chapitre IV est sans commentaire; le chapitre V nous construit l'élément le plus difficile à atteindre du théorème d'Hurwitz, à savoir l'existence de groupes triangulaires, le chapitre VI achève la démonstration. Au chapitre VII nous synthétiserons les précédents pour exhiber de manière abstraite la surface sur laquelle agit $\mathrm{PSL}_2(\mathbb{F}_7)$ et montrer qu'il est un groupe d'Hurwitz. Le dernier chapitre s'occupe essentiellement de simplifier la structure des 168 éléments de $\mathrm{PSL}_2(\mathbb{F}_7)$ afin d'obtenir une surface véritablement réalisable.

Je voudrais chaleureusement remercier mon directeur de diplôme, le professeur Oscar Burlet, pour m'avoir introduit une si belle matière et je voudrais remercier également le professeur Marc Troyanov pour les longues heures de patience passées avec moi.

Paul Libbrecht
Lausanne, le 19 août 94

Transformations homographiques de $\widehat{\mathbb{K}}$

Ce premier chapitre est la première approche des groupes linéaires projectifs. Des propriétés essentielles de $\mathrm{PSL}_2(\mathbb{K})$ sont étudiées ici, avec un éclairage particulier sur les générateurs et relations qui les lient. L'étude est faite de manière "géométrique" au sens où les $\mathrm{PSL}_2(\mathbb{K})$ sont considérés comme des groupes agissant homographiquement sur $\mathbb{P}_1\mathbb{K}$, on rencontrera donc des êtres comme des inversions, des translations, etc. Le but final est la démonstration de la simplicité de presque tous les $\mathrm{PSL}_2(\mathbb{K})$.

Définition cadre

Soit \mathbb{K} un corps commutatif quelconque et n un entier ≥ 2 . Le groupe linéaire $GL_n(\mathbb{K})$ est le groupe de toutes les matrices inversibles (i.e. de déterminant non-nul) de taille $n \times n$. On considère l'action matricielle multiplicative de $GL_n(\mathbb{K})$ sur \mathbb{K}^n . Par mesure de cohérence, on appellera μ cette action, c'est-à-dire que μ est un morphisme de groupe $GL_n(\mathbb{K}) \rightarrow \mathrm{Perm}(\mathbb{K}^n)$.

Pour des raisons de mise en page, on notera un élément de \mathbb{K}^n indifféremment (x_1, \dots, x_n) ou $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$; dans tous les cas, la multiplication d'un vecteur par une matrice est la multiplication à gauche en considérant que le vecteur est écrit en colonne.

Au chapitre des notations, précisons encore que si G est une matrice, on écrira $(G)_{l,c}$ pour sa composante à la ligne l et la colonne c . De même, si $v = (x_1, \dots, x_n)$ est un vecteur de \mathbb{K}^n alors on notera $(v)_i$ sa $i^{\text{ème}}$ composante.

Lemme $GL_n(\mathbb{K})$ agit fidèlement sur \mathbb{K}^n .

DEMO En effet, supposons que $\mu(G)$ soit l'identité pour une certaine matrice G de $GL_n(\mathbb{K})$. Si l'on appelle $(e_i)_{i=1}^n$ la base ordonnée canonique de \mathbb{K}^n , $(e_i)_j = \delta_{ij}$ (Kronecker), alors on a :

$$(\mu(G)(e_i))_k = (G)_{i,k}$$

Puisque $\mu(G)$ est l'identité, on a donc que $\mu(G)(e_i) = e_i$ ainsi $(G)_{i,k} = \delta_{ik}$ et donc G ne peut être que la matrice identité.

□

Définition projective

Soit $n \geq 2$ et \mathbb{K} un corps, appelons $Scal_n(\mathbb{K})$ le sous-groupe de $GL_n(\mathbb{K})$ composé des matrices scalaires $A = \lambda \cdot I$. Clairement $Scal_n(\mathbb{K})$ est isomorphe au groupe (\mathbb{K}^*, \cdot) .

On appellera alors $\mathbb{P}_{n-1}\mathbb{K}$ le quotient de l'ensemble des vecteurs non-nuls de \mathbb{K}^n par l'action du groupe $Scal_n(\mathbb{K})$.

Lemme

$$Z(GL_n(\mathbb{K})) = Scal_n(\mathbb{K})$$

DEMO $Z(GL_n(\mathbb{K})) \supset Scal_n(\mathbb{K})$: Cette affirmation est claire puisque tout $A \in Scal_n(\mathbb{K})$ s'écrit de manière unique comme $\lambda \cdot I$: $A \cdot B = \lambda \cdot I \cdot B = \lambda \cdot B \cdot I = B \cdot (\lambda I) = BA$.

$Z(GL_n(\mathbb{K})) \subset Scal_n(\mathbb{K})$: Pour chaque $i \neq j = 1, \dots, n$, posons C_{ij} comme la matrice n'ayant que des 1 sur la diagonale et un 1 en i, j :

$$(C_{ij})_{l,c} = \begin{cases} 1 & \text{si } l = c \\ 1 & \text{si } l = i \text{ et } c = j \\ 0 & \text{sinon} \end{cases}$$

On obtient alors que:

$$\begin{aligned} \begin{cases} (A)_{l,c} & \text{si } l \neq i \\ (A)_{j,c} + (A)_{l,c} & \text{si } l = i \end{cases} &= \sum_{k=1}^n (C_{ij})_{l,k} \cdot A_{k,c} = (C_{ij} \cdot A)_{l,c} = \\ &= (A \cdot C_{ij})_{l,c} = \sum_{k=1}^n (A)_{l,k} \cdot (C_{ij})_{k,c} = \begin{cases} (A)_{l,c} & \text{si } c \neq j \\ (A)_{l,i} + (A)_{l,c} & \text{si } c = j \end{cases} \end{aligned}$$

Pour chaque $c \neq j$ on a: $(A)_{j,c} + (A)_{i,c} = (C_{ij} \cdot A)_{i,c} = (A \cdot C_{ij})_{i,c} = (A)_{i,c}$ ainsi $(A)_{j,c} = 0$, ceci étant valable pour n'importe quel j , on obtient que les composantes de la matrice A sont nulles en dehors de la diagonale. Donc, si A est dans le centre de $GL_n(\mathbb{K})$, elle est forcément diagonale. En outre $(A)_{j,j} + (A)_{i,j} = (C_{ij} \cdot A)_{i,j} = (A \cdot C_{ij})_{i,j} = (A)_{i,i} + (A)_{i,j}$ pour chaque $i \neq j$ et dès lors $(A)_{j,j} = (A)_{i,i}$ ce qui signifie que toutes les composantes de la diagonale sont égales et donc que toute matrice du centre de $GL_n(\mathbb{K})$ est une matrice scalaire.

☐

Lemme L'action de $GL_n(\mathbb{K})$ passe au quotient de \mathbb{K}^n par $Scal_n(\mathbb{K})$.

DEMO Il s'agit d'une conséquence immédiate du lemme précédent:

Quel que soit $x \in \mathbb{K}^n$ et $\forall G \in GL_n(\mathbb{K})$ on a que

$$\mu(G)(\mu(Scal_n(\mathbb{K}))(x)) = \mu(G \cdot Scal_n(\mathbb{K}))(x) = \mu(Scal_n(\mathbb{K}) \cdot G)(x) = \mu(Scal_n(\mathbb{K}))(\mu(G)(x))$$

Ce qui signifie que si deux vecteurs de \mathbb{K}^n sont équivalents par l'action de $Scal_n(\mathbb{K})$, leurs images par la multiplication de n'importe quelle matrice de $GL_n(\mathbb{K})$ sont également équivalentes. Donc l'action μ peut descendre aux classes.

☐

Corollaire On a donc une application $\tilde{\mu}: GL_n(\mathbb{K}) \longrightarrow Perm(\mathbb{P}_{n-1}\mathbb{K})$ dont le noyau est $Scal_n(\mathbb{K})$. Le morphisme d'action passe donc au quotient de $GL_n(\mathbb{K})$ par $Scal_n(\mathbb{K})$. Il s'agit bien d'un groupe qui sera nommé $PGL_n(\mathbb{K})$. Ainsi l'action de $PGL_n(\mathbb{K})$ est fidèle également.

DEMO Soit $G \in GL_n(\mathbb{K})$ telle que $\tilde{\mu}(G)$ est l'identité. Cela est équivalent à ce que G soit telle que $\forall x \in \mathbb{K}^n \exists \lambda \in \mathbb{K}^*$ avec $\mu(G)(x) = \lambda \cdot x$ alors pour chaque i , on peut trouver λ_i tel que $\mu(G)(e_i) = \lambda_i \cdot e_i$ donc $(G)_{i,j} = \lambda_i \cdot \delta_{ij}$ ainsi la matrice G doit être diagonale. De plus appelons v le vecteur qui ne contient que des 1, on peut également trouver un λ tel que $\mu(G)(v) = \lambda \cdot v$, mais puisque la matrice est diagonale, on a que $(\mu(G)(v))_i = \lambda_i$ ainsi $\lambda_i = \lambda$ et donc G doit être une matrice scalaire.

Que $PGL_n(\mathbb{K})$ soit un groupe vient du fait qu'il est le quotient d'un groupe par son centre qui est bien un sous-groupe normal. En conséquence $ker \tilde{\mu} = Scal_n(\mathbb{K})$ et donc $\tilde{\mu}$ redescendu au quotient de $GL_n(\mathbb{K})$ par $ker \tilde{\mu} = Scal_n(\mathbb{K})$ est un morphisme injectif $PGL_n(\mathbb{K}) \longrightarrow Perm(\mathbb{P}_{n-1}\mathbb{K})$ et donc l'action de $PGL_n(\mathbb{K})$ sur $\mathbb{P}_{n-1}\mathbb{K}$ est fidèle.

☐

Définition

A chaque groupe $GL_n(\mathbb{K})$ on associe un morphisme bien connu, le déterminant $GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^*$. Nous allons considérer son noyau qui est l'ensemble des matrices de déterminant 1 et sera écrit $SL_n(\mathbb{K})$.

Lemme Le centre de $SL_n(\mathbb{K})$ est $SL_n(\mathbb{K}) \cap Scal_n(\mathbb{K})$ qui est l'ensemble des matrices scalaire $\lambda \cdot I$ ou λ est une racine n^{ieme} de l'identité.

DEMO Lorsque nous avons montré que le centre $GL_n(\mathbb{K})$ est $Scal_n(\mathbb{K})$, nous avons montré que toute matrice qui commutait avec les matrices C_{ij} était une matrice scalaire. Or ces matrices sont toutes triangulaires (supérieures ou inférieures) ne contenant que des 1 dans la diagonale, leur déterminant est donc 1, i.e. $C_{ij} \in SL_n(\mathbb{K})$. Donc toute matrice qui est dans le centre de $SL_n(\mathbb{K})$ doit être scalaire.

Réciproquement toute matrice scalaire commute avec toutes les matrices de $SL_n(\mathbb{K})$ puisqu'elle commute avec toutes les matrices de $GL_n(\mathbb{K})$. Ainsi donc le centre de $SL_n(\mathbb{K})$ est l'ensemble des matrices scalaires de déterminant 1.

Enfin si une matrice est diagonale, son déterminant est le produit des éléments diagonaux, il résulte que le déterminant d'une matrice scalaire $\lambda \cdot I$ vaut λ^n et, également, 1 (puisque'elle est dans $SL_n(\mathbb{K})$) ainsi λ est une racine n^{ieme} de 1.

□

Définition

On appellera $PSL_n(\mathbb{K})$ le quotient de $SL_n(\mathbb{K})$ par son centre. Il s'agit bien d'un groupe puisque le centre est un sous-groupe normal.

Diagrammes En appelant p et q les projections de quotient, on a le diagramme suivant :

$$\begin{array}{ccccccc}
 1 & \longrightarrow & SL_n(\mathbb{K}) & \xrightarrow{\text{incl.}} & GL_n(\mathbb{K}) & \xrightarrow{\text{det}} & (\mathbb{K}^*, \cdot) \longrightarrow 1 \\
 & & \downarrow p & & \downarrow q & & \\
 & & PSL_n(\mathbb{K}) & & PGL_n(\mathbb{K}) & & \\
 & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & &
 \end{array}$$

Celui-ci peut être complété :

$$\begin{array}{ccccccc}
 1 & \longrightarrow & SL_n(\mathbb{K}) & \xrightarrow{\text{incl}} & GL_n(\mathbb{K}) & \xrightarrow{\text{det}} & (\mathbb{K}^*, \cdot) \longrightarrow 1 \\
 & & \downarrow p & & \downarrow q & & \downarrow f \\
 1 & \longrightarrow & PSL_n(\mathbb{K}) & \xrightarrow{i} & PGL_n(\mathbb{K}) & \xrightarrow{d} & \mathbb{K}^*/\mathbb{K}^{n*} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
 \end{array}$$

On a noté ici \mathbb{K}^{n*} pour signifier l'ensemble $\{k^n \in \mathbb{K} \mid k \neq 0\}$.

DEMO Le fait essentiel de cette démonstration est que :

$$\text{incl}^{-1}(\ker q) = \{G \in SL_n(\mathbb{K}) \mid \text{incl}(G) = G \in Scal_n(\mathbb{K})\} = \ker p \quad \text{et} \quad \text{det}(Scal_n(\mathbb{K})) = \mathbb{K}^{n*}$$

Grâce à cela nous allons pouvoir construire i et d . Quant à f il est défini comme la projection de quotient du groupe (\mathbb{K}^*, \cdot) par le sous-groupe $\text{det}(Scal_n(\mathbb{K})) = \mathbb{K}^{n*}$.

On construit i de la façon suivante: soit $[G]$ un élément de $PSL_n(\mathbb{K})$, on a donc $p(G) = [G]$ et l'on pose $i(G) = q \circ \text{incl}(G)$. L'application i est bien définie sur $PSL_n(\mathbb{K})$ puisque si $p(H) = [H] = [G] = p(G)$ on a que $i(G) = q \circ \text{incl}(G) = q(G) = q(H) = q \circ \text{incl}(H) = i(H)$ puisque $\text{incl}(\ker p) \subset \ker q$.

De même on construit $d([G])$ comme $f \circ \det(G)$ qui est indépendant du choix de G puisqu'on a $\det(\ker q) = \det(\text{Scal}_n(\mathbb{K})) = \mathbb{K}^{n*} = \ker f$.

Il nous reste à prouver que l'on a bien une suite exacte: par définition il est clair qu'on a $\text{im } i = \text{im}(q \circ \text{incl}) = q(\text{im } \text{incl}) = q(\ker \det)$, de plus:

$$\ker d = q(\ker(f \circ \det)) = q(\det^{-1}(\ker f)) = q(\det^{-1}(\det(\ker q))) = q(\ker \det \cdot \ker q) = q(\ker \det)$$

Ainsi donc $\text{im } i = \ker d$.

Il est clair que d est surjective puisque f et \det sont surjectives. En outre i est injective puisque $\ker i = p(\ker(q \circ \text{incl})) = p(\text{incl}^{-1}(\ker q)) = p(\ker p) = 1$.

☐

Droite complétée, action fractionnaire

Nous allons étudier ici le rapprochement entre les transformations projectives d'une droite projective et les transformations fractionnelles ainsi qu'elles sont pratiquées en géométrie hyperbolique. Ce sera sur ce second modèle que nous nous appuyerons pour obtenir les conclusions de notre chapitre.

Définitions

Appelons $\widehat{\mathbb{K}}$ l'ensemble composé des éléments de \mathbb{K} et d'un élément supplémentaire nommé infini et noté ∞ .

Lemme On a une bijection canonique entre $\mathbb{P}_1\mathbb{K}$ et $\widehat{\mathbb{K}}$.

DEMO Posons

$$\beta: \mathbb{P}_1\mathbb{K} \longrightarrow \widehat{\mathbb{K}}$$

$$\begin{array}{l} [(x, y)] \text{ avec } y \neq 0 \longmapsto \frac{x}{y} \\ [(x, 0)] \longmapsto \infty \end{array}$$

Cette application est bien définie puisque si $[(x, y)] = [(a, b)]$ on peut trouver $\lambda \in \mathbb{K}^*$ tel que $(x, y) = (\lambda \cdot a, \lambda \cdot b)$. Alors, si $y = 0$, on a que $\lambda \cdot b = 0$ i.e. $b = 0$ et donc $\beta([(a, b)]) = \infty = \beta([(x, y)])$.

Si $y \neq 0$ alors $b \neq 0$ et donc:

$$\beta([(x, y)]) = \frac{x}{y} = \frac{a \cdot \lambda}{b \cdot \lambda} \stackrel{\lambda \neq 0}{=} \frac{a}{b} = \beta([(a, b)])$$

Elle est bijective car on peut lui trouver l'inverse suivant: $\gamma: \widehat{\mathbb{K}} \longrightarrow \mathbb{P}_1\mathbb{K}$

$$\begin{array}{l} x \neq \infty \longmapsto [(x, 1)] \\ \infty \longmapsto [(1, 0)] \end{array}$$

En effet $\gamma \circ \beta: \mathbb{P}_1\mathbb{K} \longrightarrow \mathbb{P}_1\mathbb{K}$ et, de même, $\beta \circ \gamma: \widehat{\mathbb{K}} \longrightarrow \widehat{\mathbb{K}}$

$$\begin{array}{l} [(x, 0)] \longmapsto [(1, 0)] \\ [(x, y)] \text{ avec } y \neq 0 \longmapsto [(x, y)] \end{array} \quad \begin{array}{l} x \neq \infty \longmapsto x \\ \infty \longmapsto \infty \end{array}$$

☐

Définition

Étant donnée une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $GL_2(K)$, on lui associe l'application $\widehat{\mathbb{K}} \longrightarrow \widehat{\mathbb{K}}$ appelée $\omega(A)$ et définie comme suit:

- si $c \neq 0$, on définira $\omega(A): \widehat{\mathbb{K}} \longrightarrow \widehat{\mathbb{K}}$

$$\begin{array}{l} x \in \mathbb{K} \setminus \{-\frac{d}{c}\} \longmapsto \frac{a \cdot x + b}{c \cdot x + d} \\ x = -\frac{d}{c} \longmapsto \infty \\ x = \infty \longmapsto \frac{a}{c} \end{array}$$

- si $c = 0$, on définira $\omega(A): \widehat{\mathbb{K}} \longrightarrow \widehat{\mathbb{K}}$

$$\begin{array}{l} x \in \mathbb{K} \longmapsto \frac{a}{d} \cdot x + \frac{b}{d} \\ x = \infty \longmapsto \infty \end{array} \quad \begin{array}{l} \text{(ce qui est possible puisque} \\ c = 0 \Rightarrow ad \neq 0 \Rightarrow a, d \neq 0) \end{array}$$

Lemme

Pour toute matrice $A \in GL_n(\mathbb{K})$, la transformation $\beta^1 \circ \omega(A) \circ \beta$ est une transformation de $\mathbb{P}_1\mathbb{K}$ qui fait le même travail que la transformation matricielle multiplicative $\tilde{\mu}(A)$.

DEMO Posons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a donc $\forall \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{P}_1\mathbb{K}$ on a $\tilde{\mu}(A)\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \cdot x + b \cdot y \\ c \cdot x + d \cdot y \end{bmatrix}$. De l'autre côté:

$$\bullet c = 0: \beta^1 \circ \omega(A) \circ \beta: \begin{bmatrix} x \\ 0 \end{bmatrix} \mapsto \beta \circ \omega(A)(\infty) \mapsto \beta^1(\infty) \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix}$$

$$y \neq 0 \quad \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \beta \circ \omega(A)\left(\frac{x}{y}\right) \mapsto \beta^1\left(\frac{a \frac{x}{y} + b}{d}\right) \mapsto \begin{bmatrix} ax+by \\ dy \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$$

$$\bullet c \neq 0: \beta^1 \circ \omega(A) \circ \beta: \begin{bmatrix} x \\ 0 \end{bmatrix} \mapsto \beta \circ \omega(A)(\infty) \mapsto \beta^1\left(\frac{a}{c}\right) \mapsto \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$$

$$y \neq 0 \quad \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \beta \circ \omega(A)\left(\frac{x}{y}\right) \mapsto \beta^1\left(\frac{a \frac{x}{y} + b}{c \frac{x}{y} + d}\right) \mapsto \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$$

En conséquence, $\beta^1 \circ \omega(A) \circ \beta\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \tilde{\mu}(A)\left(\begin{bmatrix} x \\ y \end{bmatrix}\right)$ pour tout $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{P}_1\mathbb{K}$.

□

Corollaire

L'application ω ainsi construite définit une action de $GL_2(\mathbb{K})$ sur $\widehat{\mathbb{K}}$. Son noyau est le même que celui de $\tilde{\mu}$, c'est-à-dire $Scal_2(\mathbb{K})$ et donc $PGL_2(\mathbb{K})$ agit, par l'action ω , de manière fidèle sur $\widehat{\mathbb{K}}$.

DEMO L'application ω associe à chaque matrice de $GL_2(\mathbb{K})$ une transformation de $\widehat{\mathbb{K}}$ et $\beta^1 \circ \omega \circ \beta$ associe à chaque matrice $GL_2(\mathbb{K})$ une transformation de $\mathbb{P}_1\mathbb{K}$. Le lemme précédent montre que $\beta^1 \circ \omega \circ \beta = \tilde{\mu}: GL_2(\mathbb{K}) \rightarrow Perm(\mathbb{P}_1\mathbb{K})$ et donc que $\omega(A) = \beta \circ \tilde{\mu}(A) \circ \beta^1$. ω est donc un morphisme $GL_2(\mathbb{K}) \rightarrow Perm(\widehat{\mathbb{K}})$ puisque

$$\omega(A) \circ \omega(B) = \beta \circ \tilde{\mu}(A) \circ \beta^1 \circ \beta \circ \tilde{\mu}(B) \circ \beta^1 = \beta \circ \tilde{\mu}(A) \circ \tilde{\mu}(B) \circ \beta^1 = \beta \circ \tilde{\mu}(A \cdot B) \circ \beta^1 = \omega(A \cdot B)$$

De même, $\omega(G) = Id \iff \beta^1 \circ \omega(G) \circ \beta = Id \iff \tilde{\mu}(G) = Id \iff G \in Scal_2(\mathbb{K})$. Donc $\ker \omega = Scal_2(\mathbb{K})$. Ainsi le passage au quotient $\bar{\omega}$ de ω est une action fidèle de $PGL_2(\mathbb{K})$ sur $\widehat{\mathbb{K}}$.

□

Corollaire-Définition

$\bar{\omega}$ étant une action fidèle de $PGL_2(\mathbb{K})$ sur $\widehat{\mathbb{K}}$, elle l'est pour tous les sous-groupes de $PGL_2(\mathbb{K})$. En se rappelant que $PSL_2(\mathbb{K})$ s'injecte dans $PGL_2(\mathbb{K})$, on a donc une action fidèle de $PSL_2(\mathbb{K})$ sur $\widehat{\mathbb{K}}$. Nous la nommerons également $\bar{\omega}$, de même que ω est une action de $SL_2(\mathbb{K})$ sur $\widehat{\mathbb{K}}$. De plus on nommera l'image de $PSL_2(\mathbb{K})$ par $\bar{\omega}$ dans $Perm(\widehat{\mathbb{K}})$ l'ensemble des transformations homographiques de $\widehat{\mathbb{K}}$, on le notera $\mathcal{H}(\widehat{\mathbb{K}})$. Étant l'image d'un groupe par un morphisme, il s'agit encore d'un groupe.

CLAIR

Remarques

Il s'agit là très certainement d'un abus de langage, puisque c'est, a priori, l'image de $PGL_2(\mathbb{K})$ qui devrait porter ce nom. Le fait est que l'on s'intéresse à $PSL_2(\mathbb{K})$ pour ses propriétés de groupe et que la technique choisie est justement de considérer l'action d'un point de vue "géométrique". Nous aurions pu maintenir l'étude des deux groupes en parallèle mais cela doublerait probablement le nombre d'énoncés dans les deux parties qui vont suivre. En outre les propriétés essentielles de $PSL_2(\mathbb{K})$ telle que celle qui est démontrée dans le Lemme "Engendré Encore" restent apparemment inatteignables pour $PGL_2(\mathbb{K})$. Nous décidons donc de n'étudier plus que $PSL_2(\mathbb{K})$.

Description de $\mathcal{H}(\widehat{\mathbb{K}})$

Le but de cette partie est la découverte de quelques propriétés essentielles des homographies de $\widehat{\mathbb{K}}$. Ses générateurs sont en tous cas d'un intérêt tout particulier. Munis des outils de cette partie nous pourrons affronter sans trop de difficulté la démonstration de la simplicité des $\mathrm{PSL}_2(\mathbb{K})$. Commençons par un lemme qui nous rappelle que nous avons refusé d'étudier tout $\mathrm{PGL}_n(\mathbb{K})$.

Lemme Une homothétie $h: \widehat{\mathbb{K}} \rightarrow \widehat{\mathbb{K}}$ de rapport λ est une homographie si et seulement s'il existe $\mu \in \mathbb{K}^*$ tel que $\mu^2 = \lambda$.

DEMO Une homothétie est une transformation qui fixe ∞ et envoie $x \in \mathbb{K}$ sur $\lambda \cdot x$; si, donc $A \in \mathrm{SL}_2(\mathbb{K})$ et $\omega(A)$ est une homothétie, on aurait $\omega(A)(0) = 0$ i.e. $\frac{b}{d} = 0 \Rightarrow b = 0$ et $\omega(A)(\infty) = \infty$ i.e. $c = 0$.

Ainsi donc, une homothétie est l'image par ω d'une matrice diagonale $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{K})$. Alors $\omega(A)(x) = \frac{a}{d} \cdot x \ \forall x \in \mathbb{K}^*$ et $\det(A) = a \cdot d = 1$ i.e. $a = \frac{1}{d}$ ou $b = \frac{1}{a}$.

Donc $\omega(A)(x) = a \cdot \frac{1}{a} \cdot x = a^2 \cdot x$. Le rapport doit donc être un carré de \mathbb{K} .

D'autre part pour $A = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$ on a $\omega(A): \infty \mapsto \infty$ i.e. $\omega(A)$ est une homothétie de $\widehat{\mathbb{K}}$.

☐

Notation: On écrira \mathbb{K}^{2*} l'ensemble des carrés non-nuls du corps \mathbb{K} .

Remarque

Le but de ce chapitre est donc d'étudier $\mathrm{PSL}_2(\mathbb{K})$ mais cela revient au même que d'étudier $\mathcal{H}(\widehat{\mathbb{K}})$ puisque ce sont deux groupes isomorphes. Le travail va donc se faire géométriquement.

Générateurs de $\mathcal{H}(\widehat{\mathbb{K}})$

Le groupe $\mathcal{H}(\widehat{\mathbb{K}})$ est engendré par les éléments que voici:

- une inversion (prononcer *iota*)

$$\iota: \begin{array}{l} x \mapsto -\frac{1}{x} \\ 0 \mapsto \infty \\ \infty \mapsto 0 \end{array} \quad \iota = \omega \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

- des homothéties de rapport $l \in \mathbb{K}^{*2}$

$$\eta_l: \begin{array}{l} \infty \mapsto \infty \\ x \mapsto l \cdot x \end{array} \quad \eta_l = \omega \begin{pmatrix} \sqrt{l} & 0 \\ 0 & \frac{1}{\sqrt{l}} \end{pmatrix}$$

- des translations d'amplitude $t \in \mathbb{K}^*$

$$\tau_t: \begin{array}{l} \infty \mapsto \infty \\ x \mapsto x + t \end{array} \quad \tau_t = \omega \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

DEMO Pour un $\chi: x \mapsto \frac{ax+b}{cx+d} \in \mathcal{H}(\widehat{\mathbb{K}})$ il y a deux traitements possibles:

- soit $c = 0$ alors $a \cdot d = 1$ donc $a, d \neq 0$ et $d = \frac{1}{a}$; on a alors $x \mapsto \frac{a}{d} \cdot x + \frac{b}{d} = a^2 \cdot x + \frac{b}{d}$ et $\infty \mapsto \infty$, mais alors χ a exactement le même comportement que $\tau_{\frac{b}{d}} \circ \eta_{a^2}$ et lui est donc égal.

- soit $c \neq 0$ et alors $\forall x \in \mathbb{K}^* \ \chi \circ \tau_{-\frac{d}{c}}(x) = \frac{ax + (b - \frac{ad}{c})}{cx} = \frac{a}{c} + \frac{bc - ad}{-c^2} \cdot \frac{-1}{x} = \frac{a}{c} + \frac{1}{c^2} \cdot \frac{-1}{x}$,
 $\chi \circ \tau_{-\frac{d}{c}}(0) = \chi \left(\frac{-d}{c} \right) = \infty$ et $\chi \circ \tau_{-\frac{d}{c}}(\infty) = \frac{a}{c}$.

Or mais $\tau_{\frac{a}{c}} \circ \eta_{\frac{1}{c^2}} \circ \iota$ a exactement le même comportement d'où $\tau_{\frac{a}{c}} \circ \eta_{\frac{1}{c^2}} \circ \iota = \chi \circ \tau_{-\frac{d}{c}}$ mais $(\tau_x)^{-1} = \tau_{-x}$ et alors $\chi = \tau_{\frac{a}{c}} \circ \eta_{\frac{1}{c^2}} \circ \iota \circ \tau_{\frac{d}{c}}$.

☐

Engendré encore

Toute homothétie de rapport $k^2 \in \mathbb{K}^{*2}$ est produit d'inversions et de translations, en fait :

$$\eta_{k^2} = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k} \circ \iota$$

Par conséquent, on peut affirmer que les homographies de $\widehat{\mathbb{K}}$ sont engendrées par les translations et l'inversion.

DEMO Pour prouver ceci, nous avons besoin du petit lemme suivant :

Lemme

Soit $\varphi \in \mathcal{H}(\widehat{\mathbb{K}})$ qui fixe 0 et ∞ alors φ est un homothétie de rapport $\varphi(1)$

DEMO Puisque $\varphi \in \mathcal{H}(\widehat{\mathbb{K}})$, on trouve $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{K})$ avec $\omega\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varphi$

Détaillons $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sachant que φ fixe 0 et ∞ :

- $\varphi(\infty) = \infty \Leftrightarrow c = 0$
- $\varphi(0) = 0 \Leftrightarrow \frac{b}{d} = 0 \Leftrightarrow b = 0$

Ainsi $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice diagonale d'où :

$$\forall x \in \mathbb{K} \varphi(x) = \omega\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}(x) = \frac{a}{d} \cdot x \text{ et } \varphi(\infty) = \omega\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}(\infty) = \infty$$

et donc φ est bien une homothétie de rapport $\frac{a}{d} = \frac{a}{d} \cdot 1 = \varphi(1)$.

Q.E.D.

Pour prouver l'énoncé de "Engendré Encore", il nous suffira, en vertu du lemme précédent, de montrer que :

$$\begin{array}{lcl} \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k} \circ \iota & \text{applique} & 0 \longmapsto 0 \\ & & \infty \longmapsto \infty \\ & & 1 \longmapsto k^2 \end{array}$$

Faisons donc les calculs :

$$\begin{aligned} \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k} \circ \iota(0) &= \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k}(\infty) = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota(\infty) = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}}(0) \\ &= \tau_{-k} \circ \iota(-\frac{1}{k}) = \tau_{-k}(k) = 0 \end{aligned}$$

$$\begin{aligned} \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k} \circ \iota(\infty) &= \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k}(0) = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota(-k) \\ &= \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}}(\frac{1}{k}) = \tau_{-k} \circ \iota(0) = \tau_{-k}(\infty) = \infty \end{aligned}$$

$$\tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k} \circ \iota(1) = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota \circ \tau_{-k}(-1) = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}} \circ \iota(-1-k)$$

$$\begin{aligned} \bullet \text{ si } k \neq 1 : & \quad = \tau_{-k} \circ \iota \circ \tau_{-\frac{1}{k}}(\frac{1}{1+k}) = \tau_{-k} \circ \iota(\frac{-1}{k^2+k}) \quad \text{car } \frac{1}{1+k} - \frac{1}{k} = \frac{k-1-k}{k^2+k} = \frac{-1}{k^2+k} \\ & \quad = \tau_{-k}(k^2+k) = k^2 \end{aligned}$$

$$\bullet \text{ si } k = -1 : \quad = \tau_1 \circ \iota \circ \tau_1(\infty) = \tau_1 \circ \iota(\infty) = \tau_1(0) = 1 = (-1)^2 = k^2$$

∩

Corollaire

On a la relation suivante entre ι et τ_1 qui nous dit que l'homothétie de rapport $1 = -1^2 = 1^2$ est l'identité :

$$\tau_1 \circ \iota \circ \tau_1 \circ \iota \circ \tau_1 \circ \iota = Id \quad \text{et de même} \quad \tau_{-1} \circ \iota \circ \tau_{-1} \circ \iota \circ \tau_{-1} \circ \iota = Id$$

Q.E.D.

Proposition

Appelons T l'ensemble des translations, nous allons montrer que l'application qui, à chaque translation $\tau_k \in \mathcal{H}(\widehat{\mathbb{K}})$ associe son amplitude k est un isomorphisme de groupe.

DEMO

L'application qui à tout $k \in \mathbb{K}$ associe $\omega\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ est :

- un morphisme puisque ω en est un et que $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & k' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k'+k \\ 0 & 1 \end{pmatrix}$
- injective puisque $\omega\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right) = Id \iff \exists \lambda \in \mathbb{K}^* \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff k = 0$.
- est surjective puisque, par définition, une translation est toujours $\omega\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$. Ainsi cette application est un isomorphisme de groupe et on a le résultat.

Q

Proposition

Le sous-groupe des homothéties de $\mathcal{H}(\widehat{\mathbb{K}})$ est isomorphe à (\mathbb{K}^{2*}, \cdot) .

DEMO

L'application qui associe à tout $k^2 \in \mathbb{K}^{2*}$ la transformation $\omega\left(\begin{smallmatrix} k & 0 \\ 0 & \frac{1}{k} \end{smallmatrix}\right)$ est : par

- un morphisme ω en est un que $\begin{pmatrix} k & 0 \\ 0 & \frac{1}{k} \end{pmatrix} \cdot \begin{pmatrix} k' & 0 \\ 0 & \frac{1}{k'} \end{pmatrix} = \begin{pmatrix} kk' & 0 \\ 0 & \frac{1}{k \cdot k'} \end{pmatrix}$
- injective puisque $\omega\left(\begin{smallmatrix} k & 0 \\ 0 & \frac{1}{k} \end{smallmatrix}\right) = Id \iff \exists \lambda \in \mathbb{K}^{2*} \begin{pmatrix} k & 0 \\ 0 & \frac{1}{k} \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \implies k = \lambda$ et $\frac{1}{k} = \lambda \implies k^2 = 1 \implies k = \pm 1$ et $\lambda = k = \pm 1$
- est surjective puisque toute homothétie est, par définition, $\omega\left(\begin{smallmatrix} 1 & 0 \\ 0 & \frac{1}{k} \end{smallmatrix}\right)$. Ainsi cette application est bien un isomorphisme de groupe.

Q

Proposition

ι est une involution. Le sous-groupe engendré par l'inversion $\langle \iota \rangle$ est isomorphe à \mathbb{Z}_2

DEMO

$$\begin{aligned} \iota^2: \infty &\longmapsto 0 \longmapsto \infty \\ 0 &\longmapsto \infty \longmapsto 0 \\ x \in \mathbb{K}^* &\longmapsto -\frac{1}{x} \longmapsto -\frac{1}{-\frac{1}{x}} = x \end{aligned}$$

Donc ι^2 est bien la transformation identité ainsi $\iota^2 = Id$.

Q

Équivalence des similitudes

Soit $\rho \in \mathcal{H}$ alors les trois assertions suivantes sont équivalentes :

- $\rho(\infty) = \infty$
- ρ est l'image par ω d'une matrice triangulaire supérieure.
- $\rho = \tau_p \circ \eta_k$ où $p \in \mathbb{K}$ et $k \in \mathbb{K}^{2*}$ avec $p = \rho(0)$ et $k = \tau_{-p} \circ \rho(1)$.

DEMO

- $(i) \iff (ii)$ Dans la définition de ω , on a $\forall \rho = \omega\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{H}(\widehat{\mathbb{K}}) \quad \rho(\infty) = \infty \iff c = 0$ et donc $\rho(\infty) = \infty$ est équivalent à dire que ρ est l'image par ω d'une matrice triangulaire supérieure.
- $(ii) \implies (iii)$ Supposons que $\rho = \omega\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \text{SL}_2(\mathbb{K})$, alors, d'après la définition de ω , on a que $\rho(x) = \frac{a}{d} \cdot x + \frac{b}{d}$ et que $\rho(\infty) = \infty$.
Or $ad - b \cdot 0 = 1 = ad$ donc $a, d \neq 0$ et $d = \frac{1}{a}$ d'où $\frac{a}{d} = a^2 \in \mathbb{K}^{2*}$ donc $\rho(x) = a^2 \cdot x + b \cdot a \quad \forall x \in \mathbb{K}$.
Mais $\tau_{b \cdot a} \circ \eta_{a^2}$ envoie $x \in \mathbb{K} \mapsto a^2 \cdot x + b \cdot a$ et $\infty \mapsto \infty$ donc $\rho = \tau_{b \cdot a} \circ \eta_{a^2}$ puisque ces deux transformations ont le même effet sur $\widehat{\mathbb{K}}$.

Maintenant $\rho(0) = \tau_{b \cdot a} \circ \eta_{a^2}(0) = \tau_{b \cdot a}(0) = b \cdot a$ et

$$\tau_{-b \cdot a} \circ \rho(1) = \tau_{-b \cdot a} \circ \tau_{b \cdot a} \circ \eta_{a^2}(1) = \eta_{a^2}(1) = a^2$$

L'assertion (iii) est bien vérifiée.

(iii) \Rightarrow (i) L'homothétie applique ∞ sur lui même et la translation de même, donc la composée $\rho = \tau_p \circ \eta_k$ également alors $\rho(\infty) = \infty$.

☺

Définitions

Les transformations de $\mathcal{H}(\widehat{\mathbb{K}})$ qui satisfont les trois conditions énoncées dans le lemme ci-dessus sont appelées les similitudes de $\mathcal{H}(\widehat{\mathbb{K}})$. On écrira $\mathcal{H}_\infty(\widehat{\mathbb{K}})$ l'ensemble des similitudes.

Énumération

Dans le cas de corps finis il pourra s'avérer pratique de compter les similitudes, voici une application d'énumération:

$$\begin{aligned} \varepsilon: \mathbb{K} \times \mathbb{K}^{2*} &\longrightarrow \mathcal{H}_\infty(\widehat{\mathbb{K}}) \\ (p, k) &\longmapsto \tau_p \circ \eta_k \end{aligned}$$

On montre ici que c'est une bijection. Toutefois, nous verrons dans le lemme suivant qu'il ne s'agit pas d'un isomorphisme avec la structure groupe sur $\mathbb{K} \times \mathbb{K}^{2*}$ fournie par le produit cartésien.

DEMO Cette application est surjective puisque toute similitude ρ peut, grâce au lemme précédent, s'exprimer comme $\tau_p \circ \eta_k$.

Pour l'injection, prenons (p, k) et $(p', k') \in \mathbb{K} \times \mathbb{K}^{2*}$ donc $\varepsilon(p, k) = \tau_p \circ \eta_k$ et $\varepsilon(p', k') = \tau_{p'} \circ \eta_{k'}$. Supposons que $\varepsilon(p, k) = \varepsilon(p', k')$ et montrons qu'alors $(p, k) = (p', k')$.

Calculons: $p = \tau_p(0) = \tau_p \circ \eta_k(0) = \varepsilon(p, k)(0) \stackrel{\text{supposition}}{=} \varepsilon(p', k')(0) = \tau_{p'} \circ \eta_{k'}(0) = \tau_{p'}(0) = p'$

Mais alors, on a aussi: $k = \eta_k(1) = \tau_{-p} \circ \tau_p \circ \eta_k(1) = \tau_{-p} \circ \varepsilon(p, k) = \tau_{-p} \circ \varepsilon(p', k')(1) = \tau_{-p}$

$$\stackrel{p=p'}{=} \tau_{-p'} \circ \varepsilon(p', k') = \tau_{-p'} \circ \tau_{-p'} \circ \eta_{k'}(1) = \eta_{k'}(1) = k'$$

On a donc montré que $\varepsilon(p, k) = \varepsilon(p', k') \Rightarrow p = p'$ et $k = k' \Leftrightarrow (p, k) = (p', k')$.

☺

Sous-groupes normaux de $\mathcal{H}(\widehat{\mathbb{K}})$

Dans cette partie nous voulons montrer que tout sous-groupe normal est soit trivial soit tout $\mathcal{H}(\widehat{\mathbb{K}})$, il va nous falloir, pour cela, passer par quelques calculs et, hélas, restreindre l'ensemble des corps envisagés.

Lemme

Nous avons trois sortes de générateurs de $\mathcal{H}(\widehat{\mathbb{K}})$, voici deux façons de les permuter:

$$\forall p \in \mathbb{K} \quad k \in \mathbb{K}^{2*} \quad \text{(i) } \iota \circ \eta_k = \eta_{\frac{1}{k}} \circ \iota \quad \text{(ii) } \eta_k \circ \tau_p = \tau_{p \cdot k} \circ \eta_k$$

DEMO

$$\begin{aligned} \text{(i) } \iota \circ \eta_k: \quad 0 &\longmapsto 0 \longmapsto \infty & \eta_{\frac{1}{k}} \circ \iota: \quad 0 &\longmapsto \infty \longmapsto \infty \\ \infty &\longmapsto \infty \longmapsto 0 & \infty &\longmapsto 0 \longmapsto 0 \\ x \in \mathbb{K}^* &\longmapsto k \cdot x \longmapsto -\frac{1}{k \cdot x} = \frac{1}{k} \cdot -\frac{1}{x} & x \in \mathbb{K}^* &\longmapsto -\frac{1}{x} \longmapsto \frac{1}{x} \cdot -\frac{1}{x} \end{aligned}$$

Donc $\iota \circ \eta_k$ et $\eta_{\frac{1}{k}} \circ \iota$ ont le même effet sur $\widehat{\mathbb{K}}$, ces deux transformations sont donc égales.

$$\begin{aligned} \text{(ii) } \tau_{pk} \circ \eta_k: \quad \infty &\longmapsto \infty \longmapsto \infty & \eta_k \circ \tau_p: \quad \infty &\longmapsto \infty \longmapsto \infty \\ x \in \mathbb{K} &\longmapsto k \cdot x \longmapsto k \cdot x + p \cdot k = k \cdot (x+p) & x \in \mathbb{K} &\longmapsto x+p \longmapsto k \cdot (x+p) \end{aligned}$$

Donc ces deux transformations agissent de la même manière sur $\widehat{\mathbb{K}}$, elles sont donc égales.

☺

Corollaire

De ce résultat découlent directement la manière de conjuguer: $\forall k \in \mathbb{K}^{2*}$ et $\forall p \in \mathbb{K}$

$$(i) \quad \iota \circ \eta_k \circ \iota = \iota \circ \eta_k \circ \iota^{-1} = \eta_{\frac{1}{k}}$$

$$(ii) \quad \eta_k \circ \tau_p \circ \eta_k^{-1} = \eta_k \circ \tau_p \circ \eta_{\frac{1}{k}} = \tau_{pk} \text{ et } \eta_k \circ \tau_p \circ \eta_k = \tau_{\frac{p}{k}}$$

Q.E.D.

Remarque

$\mathcal{H}(\widehat{\mathbb{K}})$ peut être très grand, et il est très difficile de donner les propriétés d'une homographie quelconque de $\widehat{\mathbb{K}}$. Par exemple la recherche d'un point fixe revient à la résolution d'une équation polynômiale du second degré. La classification que l'on établit de $PSL_2(\mathbb{R})$ en géométrie hyperbolique est impossible à reproduire pour n'importe quel corps puisque l'existence de points fixes est donnée par les zéros d'un polynôme.

Voici un petit exemple qui montre le problème: l'inversion $\iota = \omega \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ admet un point fixe si et seulement si le corps admet une racine de -1 . En effet $\iota: 0 \mapsto \infty$ et $\infty \mapsto 0$ donc elle ne fixe pas 0 ou ∞ , de plus $x \in \mathbb{K}^* \mapsto -\frac{1}{x}$ alors $x \in \mathbb{K}^*$ est fixe si et seulement si $x = -\frac{1}{x}$ i.e. $x \neq 0$ et $x^2 = -1$.

Or il y a beaucoup de corps où -1 n'est pas carré, par exemple, \mathbb{Q}, \mathbb{F}_7 ou $\mathbb{F}_{27} \dots$

Nous allons choisir la technique suivante: on s'intéresse aux similitudes dans les sous-groupes normaux de $\mathcal{H}(\widehat{\mathbb{K}})$ et ceci suffira pour tout reconstruire.

Définition

Pour prouver les résultats qui suivent, il va falloir restreindre les corps envisagés: on dira d'un corps \mathbb{K} qu'il possède suffisamment de carrés s'il existe dans le groupe (\mathbb{K}^{2*}, \cdot) un élément d'ordre > 2 .

Acquisition d'une similitude

Si \mathbb{K} admet suffisamment de carrés, tout sous-groupe normal non-trivial de $\mathcal{H}(\widehat{\mathbb{K}})$ contient une similitude non triviale.

DEMO Appelons H ce sous-groupe non-trivial, donc H contient une homographie non triviale. Si cette homographie est une similitude, nous avons déjà gagné. Supposons qu'elle ne le soit pas: par le résultat *Générateurs de $\mathcal{H}(\widehat{\mathbb{K}})$* cette transformation peut s'écrire comme composée de la forme: $\tau_p \circ \eta_k \circ \iota \circ \tau_q$ avec $p, q \in \mathbb{K}$ et $k \in \mathbb{K}^{2*}$. Nous pouvons alors conjuguer par τ_{-q} tout en restant dans H (normalité):

$$\tau_q \circ \tau_p \circ \eta_k \circ \iota \circ \tau_q \circ \tau_{-q} \stackrel{\text{isom. des translations}}{=} \tau_{p+q} \circ \eta_k \circ \iota \in H$$

Il me faut, avant de continuer, écarter deux exceptions que on traitera ensuite: ($k^2 = 1$ et $q + p = 0$) ou ($k^2 = 1$ et $q + p \neq 0$).

On suppose donc que $k^2 \neq 1$ et l'on conjugue encore par l'inversion ι :

$$\iota \circ \tau_{p+q} \circ \eta_k \circ \iota \circ \iota^{-1} = \iota \circ \tau_{p+q} \circ \eta_k \in H \text{ normal}$$

Mais H est un sous-groupe donc le produit de deux éléments de H est encore dans H :

$$\tau_{p+q} \circ \eta_k \circ \iota \circ \iota \circ \tau_{p+q} \circ \eta_k \stackrel{\text{involution}}{=} \tau_{p+q} \circ \eta_k \circ \tau_{p+q} \circ \eta_k \stackrel{\substack{\text{lemme de commutation} \\ \text{isomorphismes}}}{=} \tau_{(p+q)(k+1)} \circ \eta_{k^2} \in H$$

Cette similitude est donc dans H et elle n'est pas triviale car elle est image par la bijection d'énumération ε de $((p+q)(k+1), k^2)$ qui est distinct de $(0, 1)$ car $k^2 \neq 1$.

Première exception: si $k^2 = 1$ et $p + q = 0$ alors $\tau_{p+q} \circ \eta_k \circ \iota$ devient $\eta_k \circ \iota$ qui est donc dans H . Prenons c , un élément permettant à \mathbb{K} d'avoir suffisamment de carrés. H est normal donc il contient: $\eta_c \circ \eta_k \circ \iota \circ \eta_{\frac{1}{c}} = \eta_c \circ \eta_k \circ \eta_c \circ \iota = \eta_{c^2 k} \circ \iota$. Et puisque H est un sous-groupe $\eta_{c^2 k} \circ \iota \circ (\eta_k \circ \iota)^{-1} = \eta_{c^2 k} \circ \iota \circ \iota^{-1} \circ \eta_k^{-1} = \eta_{c^2 k} \circ \eta_{\frac{1}{k}} = \eta_{c^2} \in H$ qui est donc une similitude non triviale car c est d'ordre > 2 .

Seconde exception: si $k^2 = 1$ et $p + q \neq 0$, prenons à nouveau $c \in \mathbb{K}^{2*}$ d'ordre > 2 alors (normal) $\eta_c \circ \tau_{p+q} \circ \eta_k \circ \iota \circ \eta_{\frac{1}{c}} = \tau_{c(p+q)} \circ \eta_{kc^2} \circ \iota \in H$. Mais on a vu, dans le cas général, que $\iota \circ \tau_{p+q} \circ \eta_k \in H$ alors:

$(\tau_{c(p+q)} \circ \eta_{kc^2} \circ l) \circ (l \circ \tau_{p+q} \circ \eta_k) = \tau_{c(p+q)} \circ \tau_{kc^2(p+q)} \circ \eta_{kc^2} \circ \eta_k = \tau_{(p+q)c(kc+1)} \circ \eta_{k^2c^2} \in H$
qui n'est pas triviale car $k^2c^2 = 1 \cdot c^2 = c^2 \neq 1$ car c est d'ordre > 2 .

Q

Portée

Tentons maintenant d'examiner l'orbite d'une quelconque similitude par l'action de conjugaison de l'ensemble des similitudes: dans cette proposition, on obtient que si on a une similitude non triviale, elle peut être décomposée d'après le lemme de description des similitudes $\tau_a \circ \eta_r$ avec $(a, r) \in \mathbb{K} \times \mathbb{K}^{2*}$, alors l'application d'action de conjugaison:

$$\begin{aligned} \kappa: \mathbb{K} \times \mathbb{K}^{2*} &\longrightarrow \mathcal{H}_\infty(\widehat{\mathbb{K}}) \\ (p, k) &\longmapsto (\tau_p \circ \eta_k)^{-1} \circ (\tau_a \circ \eta_r) \circ (\tau_p \circ \eta_k) \end{aligned}$$

a comme image: $\left\{ \tau_{l \cdot a} \mid l \in \mathbb{K}^{2*} \right\}$ si $r = 1$ et $\left\{ \tau_q \circ \eta_r \mid q \in \mathbb{K} \right\}$ si $r \neq 1$.

DEMO Il suffit d'écrire:

$$\begin{aligned} \kappa(p, k) &= (\tau_p \circ \eta_k)^{-1} \circ (\tau_a \circ \eta_r) \circ (\tau_p \circ \eta_k) \stackrel{\text{isomorphismes}}{=} \eta_{\frac{1}{k}} \circ \tau_{a-p} \circ \eta_r \circ \tau_p \circ \eta_k \\ &\stackrel{\text{commutation}}{=} \tau_{\frac{a-p}{k}} \circ \eta_{\frac{1}{k}} \circ \tau_p \circ \eta_k \stackrel{\text{isomorphismes}}{=} \tau_{\frac{a-p}{k}} \circ \tau_{\frac{pr}{k}} \circ \eta_{\frac{1}{k}} \circ \eta_k = \tau_{\frac{1}{k}(a+p(r-1))} \circ \eta_r \end{aligned}$$

Il nous reste maintenant à voir qu'ainsi viennent toutes les translations désirées. Il est temps de séparer les deux cas pour examiner l'image de l'application:

$$\begin{aligned} \varphi: \mathbb{K} \times \mathbb{K}^{2*} &\longrightarrow \mathbb{K} \\ (p, k) &\longmapsto \frac{1}{k} \cdot (a + p(r-1)) \end{aligned}$$

- Si $r \neq 1$, on peut poser, pour chaque $q \in \mathbb{K}$, $p = \frac{q-a}{r-1}$ et donc $\varphi(p, 1) = a + \frac{q-a}{r-1}(r-1) = a + (q-a) = q$; donc dans cas, φ admet n'importe quel $q \in \mathbb{K}$ dans son image et donc n'importe que $\tau_q \circ \eta_k$ est atteint par κ (avec le k fixé).
- Si $r = 1$, $a \neq 0$, $\kappa(p, k)$ devient $\tau_{\frac{a}{k}} \circ \eta_1 = \tau_{\frac{a}{k}}$. Pour tout $l \in \mathbb{K}^{2*}$, on peut trouver $k \in \mathbb{K}^{2*}$ (en fait $\frac{1}{k}$); tel que $\frac{1}{k} = l$ alors toute translation $\tau_{a \cdot l}$ est atteinte par κ et on a bien le résultat.

Q

Suffisance

Étant donné un corps de caractéristique non 2 et un sous-groupe normal H_∞ de $\mathcal{H}_\infty(\widehat{\mathbb{K}})$ qui contient une translation non-triviale alors H_∞ contient toutes les translations.

Lemme

Si \mathbb{K} n'est pas de caractéristique 2 alors pour tout $x \in \mathbb{K}$, il existe $c, d \in \mathbb{K}$ tels que $c^2 - d^2 = x$.

DEMO En posant $c = 1 - d$, notre équation devient:

$$c^2 - d^2 = (c+d)(c-d) = x \stackrel{\text{caract} \neq 2}{=} (1-d+d)(1-2d) = (1-2d)$$

$$\Leftrightarrow x = 1 - 2d \Leftrightarrow 2d = 1 - x \Leftrightarrow d = \frac{1}{2}(1-x) \Rightarrow c = 1 - \frac{1}{2}(1-x) = \frac{1}{2}(1+x)$$

Alors tout se vérifie $(c+d)(c-d) = \left(\frac{1}{2}(1+x) + \frac{1}{2}(1-x)\right) \left(\frac{1}{2}(1+x) - \frac{1}{2}(1-x)\right)$ ce qui vaut $\left(\frac{1}{2} \cdot 2\right) \left(\frac{1}{2} \cdot 2x\right) = x$. On observe alors que si $x \neq \pm 1$, c et d sont non nuls.

Q.E.D.

DEMO Soit $a \neq 0$ l'amplitude de la translation non-triviale qu'on a trouvée dans H_∞ puisque H est un sous-groupe on a déjà les translations τ_a et $\tau_{-a} = \tau_a^{-1}$. De plus, on a vu dans le lemme de conjugaison que $\forall k \in \mathbb{K}^{2*} \eta_k \circ \tau_a \circ \eta_{\frac{1}{k}} = \tau_{ak}$.

Quelle que soit la translation d'amplitude $p \neq \pm a$ que l'on cherche, le lemme nous donne l'existence de $e, f \in \mathbb{K}^{2*}$ tels que $e - f = \frac{p}{a}$. Soient alors les translations:

$$\gamma = \eta_e \circ \tau_a \circ \eta_{\frac{1}{e}} = \tau_{ac} \quad \delta = \eta_f \circ \tau_a \circ \eta_{\frac{1}{f}} = \tau_{af}$$

Elles sont aussi dans H_∞ puisqu'elles sont des conjuguées de τ_a par des similitudes.
Mais puisque H est sous-groupe, $\gamma\delta^{-1} \in H_\infty$ et donc :

$$\gamma\delta^{-1} = \tau_{ae} \circ \tau_{af}^{-1} \stackrel{\text{isomorphismes}}{=} \tau_a(e-f) \stackrel{\text{déf. de } e, f}{=} \tau_a \cdot \left(\frac{e}{a}\right) = \tau_p$$

et donc $\tau_p \in H_\infty$ quel que soit $p \in \mathbb{K}$.

Q

Résumé

Prenons un corps qui n'est pas de caractéristique 2 et qui a suffisamment de carrés, soit H un sous-groupe normal de $\mathcal{H}(\widehat{\mathbb{K}})$. Par la proposition, nous savons l'existence d'une similitude non-triviale, disons $\tau_a \circ \eta_k$ dans H . Par l'étude de la portée de la conjugaison de cette transformation, on sait que :

- si $k \neq 1$ on a, par conjugaison, tout l'ensemble $\{\tau_q \circ \eta_k | q \in \mathbb{K}\}$ dans H . Choisissons $q \in \mathbb{K}^*$ et $p \in \mathbb{K}^*$ en sorte que $p - q \neq 0$ (suffisamment de carrés). Puisque H est un sous-groupe, on a donc :

$$(\tau_p \circ \eta_k) \circ (\tau_q \circ \eta_k)^{-1} = \tau_p \circ \eta_k \circ \eta_{\frac{1}{k}} \circ \tau_{-q} = \tau_{p-q} \in H$$

Puisque $p - q$ est non nul, on a donc une translation non-triviale; enfin par la *suffisance* nous pouvons donc affirmer que toutes les translations se trouvent dans H ; en effet, $H \cap \mathcal{H}_\infty(\widehat{\mathbb{K}})$ est encore un sous-groupe et il est normal puisque le conjugué d'une similitude par une similitude reste une similitude.

- si $k = 1$, on a déjà une translation non-triviale; ici, comme au tiret précédent, on a que $H \cap \mathcal{H}_\infty(\widehat{\mathbb{K}})$ est un sous-groupe normal dans $\mathcal{H}_\infty(\widehat{\mathbb{K}})$; enfin, grâce à la *suffisance* on trouve toutes les translations.

Donc, tout sous-groupe normal contient toutes les translations.

CLAIR

Cadeau de l'inversion

Si \mathbb{K} est un corps de caractéristique non 2 et qui a suffisamment de carrés alors tout sous-groupe normal H contient l'inversion.

DEMO Par le résumé précédent, H contient toutes les translations, en particulier la translation d'ampitude 1 que nous nommerons τ . Alors $\iota \circ \tau \circ \iota^{-1} = \iota \circ \tau \circ \iota \in H$ (normal).

Mais H est un sous-groupe donc $\tau \circ (\iota \circ \tau \circ \iota) \circ \tau$ étant un produit d'éléments de H est dans H . Or mais le corollaire de *Engendré encore* dit que $\tau \circ \iota \circ \tau \circ \iota \circ \tau \circ \iota = Id$ qui est l'élément neutre de $\mathcal{H}(\widehat{\mathbb{K}})$ donc $\iota = \iota^{-1} = \tau \circ \iota \circ \tau \circ \iota \circ \tau$, mais on vient de voir que $\tau \circ (\iota \circ \tau \circ \iota) \circ \tau = \tau \circ \iota \circ \tau \circ \iota \circ \tau$ était dans H donc l'inversion est dans H .

Q

Théorème

Soit \mathbb{K} un corps de caractéristique non 2 et qui a suffisamment de carrés alors tout sous-groupe normal de $\mathcal{H}(\widehat{\mathbb{K}})$ est soit trivial, soit l'entier de $\mathcal{H}(\widehat{\mathbb{K}})$.

En bref $\mathcal{H}(\widehat{\mathbb{K}})$ est simple et, par conséquent, $\text{PSL}_2(\mathbb{K})$ est simple également.

DEMO On a vu que si H est un sous-groupe normal non-trivial de $\mathcal{H}(\widehat{\mathbb{K}})$ alors il contient toutes les translations (*Résumé*) et l'inversion (*Cadeau*). Or, dans *Engendré encore*, on prouve que toute homothétie est produit d'inversions et de translations; tous les produits de cette nature étant dans H , on a donc toutes les homothéties dans H .

Enfin, le premier résultat d'engendrement nommé *Générateur de $\mathcal{H}(\widehat{\mathbb{K}})$* montrait que tout élément de $\mathcal{H}(\widehat{\mathbb{K}})$ était produit d'homothéties, translations et de l'inversion; donc vu que les translations, les homothéties et l'inversion sont dans H , tout élément de $\mathcal{H}(\widehat{\mathbb{K}})$ est dans H et donc $H = \mathcal{H}(\widehat{\mathbb{K}})$.

Ainsi $\mathcal{H}(\widehat{\mathbb{K}})$ est simple.

Dans le *Corollaire-définitions* des homographies on a montré que $\mathrm{PSL}_2(\mathbb{K})$ était isomorphe à $\mathcal{H}(\widehat{\mathbb{K}})$. Donc, $\mathrm{PSL}_2(\mathbb{K})$ est simple.

□

Graphes de Cayley

Ce chapitre est une reformulation combinatoire de la théorie des revêtements pour les graphes. Un intérêt tout spécial est porté sur les graphes de Cayley donnés par la présentation d'un groupe. Le but final est de développer un outil "artisanal" pour déterminer la présentation d'un groupe. Cet outil sera utilisé dans le chapitre suivant.

Les premières définitions et théorèmes sont extraits de *Lyndon-Schupp (1977)*.

Définition

On appellera graphe un quadruplet $(S, A, \varepsilon, \iota)$ où

- S (les sommets) et A (les arêtes) sont des ensembles quelconques.
- L'application d'extrémités ε va de $A \rightarrow S \times S$. On dira qu'une arête a va de p à q si $\varepsilon(a) = (p, q)$. La donnée de ε revient à la donnée de deux applications α et $\beta: A \rightarrow S$ en définissant $\varepsilon = (\alpha, \beta)$.
- $\iota: A \rightarrow A$ (l'application d'inverse) est une involution telle que $\varepsilon(a) = (p, q) \Rightarrow \varepsilon(\iota(a)) = (q, p)$ (ou, de manière équivalente, $\alpha \circ \iota = \beta$).

Soit $C = (S, A, \varepsilon, \iota)$. Pour chaque $S' \subset S$ et $A' \subset A$, en sorte que $\varepsilon(A') \subset S' \times S'$ et $\iota(A') \subset A'$, le quadruplet $(S', A', \varepsilon|_{A'}, \iota|_{A'})$ est un graphe et on l'appellera sous-graphe de C .

Étant donnés deux graphes $(S, A, \varepsilon, \iota)$ et $(S', A', \varepsilon', \iota')$, soient $f_S: S \rightarrow S'$ et $f_A: A \rightarrow A'$, on appellera la paire (f_S, f_A) morphisme de graphe si elle préserve l'incidence et les inverses, c'est-à-dire que, pour chaque a dans A :

$$\varepsilon(a) = (p, q) \Rightarrow \varepsilon'(f_A(a)) = (f_S(p), f_S(q)) \text{ c'est-à-dire } \alpha' \circ f_A = f_S \circ \alpha \text{ et } \omega' \circ f_A = f_S \circ \omega$$

$$\iota' \circ f_A = f_A \circ \iota$$

Un morphisme de graphe (f_S, f_A) sera nommé un isomorphisme de graphe si f_S et f_A sont des bijections. La paire (f_S^{-1}, f_A^{-1}) est alors également un morphisme de graphe. Cela se montre en utilisant directement les conditions pour que (f_S, f_A) soit un morphisme de graphe:

$$\varepsilon \circ f_A = (f_S, f_S) \circ \varepsilon' \Rightarrow (f_S^1, f_S^1) \circ \varepsilon = \varepsilon' \circ f_A^1 \quad \text{de même } \iota' \circ f_A = f_A \circ \iota \Rightarrow f_A^1 \circ \iota' = \iota \circ f_A^1$$

Enfin, on appellera *revêtement de graphe* un morphisme de graphe (f_S, f_A) en sorte que f_A et f_S soient surjectives et que, “restreint à l'étoile de chaque point”, f_A soit une bijection. Cette dernière condition revient à faire la construction suivante :

On a donc $(f_S, f_A): (S, A, \varepsilon, \iota) \longrightarrow (S', A', \varepsilon', \iota')$. Pour chaque sommet $p \in S$, appelons E_p l'ensemble $\{a \in A \mid \alpha(a) = p\}$. De même, pour chaque $p' \in A'$ on définit $E'_{p'}$. La condition exigée est que la restriction de f_A allant de E_p à $E'_{p'}$ soit une bijection.

Chemins, concaténation, boucles

Soit $C = (S, A, \varepsilon, \iota)$ un graphe, on appelle *chemin*, une suite finie (éventuellement vide) $a_1 \dots a_n$ d'arêtes “qui se suivent” (i.e. telles que $\omega(a_i) = \alpha(a_{i+1}) \quad \forall i = 1, \dots, n-1$).

On dira d'un graphe qu'il est *connexe* si pour chaque paire de sommets on peut trouver un chemin $a_1 \dots a_n$ allant de p à q .

Ainsi pour un graphe connexe qui possède au moins une arête on a que chaque sommet s est l'image par ω (et donc par α également grâce à ι) d'une arête, on peut donc dire que $\omega(A) = S = \alpha(A) = \varepsilon(A \times A)$.

On définit la *concaténation* ou *produit* de deux chemins $a_1 \dots a_n$ et $b_1 \dots b_m$ s'ils se suivent (c'est-à-dire que $\omega(a_n) = \alpha(b_1)$) comme le chemin $\frac{a_1 \dots a_n \circ b_1 \dots b_m}{a_1 \dots a_n b_1 \dots b_m}$.

La concaténation du chemin vide (que l'on notera \emptyset) avec un chemin $a_1 \dots a_n$, se définit, de manière évidente, comme $\emptyset \circ a_1 \dots a_n = a_1 \dots a_n$. De même $a_1 \dots a_n \circ \emptyset = a_1 \dots a_n$. Ce chemin vide est donc un élément neutre de la concaténation. On remarque, de plus, que la concaténation est associative, en effet, si $a_1 \dots a_n, b_1 \dots b_m$ et $c_1 \dots c_l$ sont des chemins qui se suivent alors :

$$a_1 \dots a_n \circ (b_1 \dots b_m \circ c_1 \dots c_l) = a_1 \dots a_n b_1 \dots b_m c_1 \dots c_l = (a_1 \dots a_n \circ b_1 \dots b_m) \circ c_1 \dots c_l$$

Si s est un sommet du graphe, on parle de *boucle en s* pour un chemin $a_1 \dots a_n$ tel que $\alpha(a_1) = s = \omega(a_n)$. Deux boucles en s peuvent donc toujours être concaténées. L'ensemble des boucles en s muni de la concaténation est donc un semi-groupe avec un élément neutre.

Simplifications, amplifications, groupe fondamental

Soit un chemin $a_1 \dots a_n$, s'il existe $1 \leq i < n$ avec $a_i = \iota(a_{i+1})$, on dira qu'on peut *simplifier* $a_1 \dots a_n$ *en* $a_1 \dots a_{i-1} a_{i+2} \dots a_n$ qui est encore un chemin puisque: $\omega(a_{i-1}) = \alpha(a_i)$ or $\varepsilon(a_i) = (\alpha(a_i), \omega(a_i))$ donc $\varepsilon(a_{i+1}) = \varepsilon(\iota(a_i)) = (\omega(a_i), \alpha(a_i))$ ainsi, on a bien $\alpha(a_{i+2}) = \omega(a_{i+1}) = \alpha(a_i) = \omega(a_{i-1})$.

Réciproquement, si on a $M = a_1 \dots a_n$ et une arête b telle que $\alpha(b) = \omega(a_i)$ pour un i alors on dira qu'on peut *amplifier* M *en* le chemin $M' = a_1 \dots a_i \circ b \circ a_{i+1} \dots a_n$ puisque le début et la fin du chemin $b \circ \iota(b)$ sont bien $\omega(a_i) = \alpha(a_{i+1})$.

On peut alors définir la relation d'équivalence *modulo allers-retours*. On dira que deux chemins M et M' sont équivalents modulo allers-retours, on écrira $M \sim M'$ si l'on peut trouver une suite de chemins $M = M_1 \rightarrow M_2 \rightarrow \dots \rightarrow M_k = M'$ en sorte que l'on puisse simplifier ou amplifier M_i en M_{i+1} ($i = 1 \dots n-1$). Puisque les amplifications et simplifications ne changent ni le début ni la fin d'un chemin, on voit tout de suite que deux chemins équivalents modulo allers-retours ont même début et même fin.

On montre facilement que c'est une relation d'équivalence puisque :

Réflexivité: Pour tout chemin M , on a $M \sim M$ grâce à la suite composée d'un seul mot M .

Transitivité: En ayant $M \sim M'$ et $M' \sim M''$ via les suites $M = M_1 \rightarrow \dots \rightarrow M_h = M'$ et $M' = N_1 \rightarrow \dots \rightarrow N_k = M''$, on a $M \sim M''$ via :

$$M = M_1 \rightarrow \dots \rightarrow M_h = M' = N_1 \rightarrow \dots \rightarrow N_k = M''$$

Symétrie: On remarque d'abord que $a_1 \dots a_n$ peut être simplifié en $a_1 \dots a_{i-1} a_{i+2} \dots a_n$ si et seulement si $a_1 \dots a_{i-1} a_{i+2} \dots a_n$ peut être amplifié en $a_1 \dots a_n$, en effet, on a dans les deux cas $a_i = \iota(a_{i+1})$ et $\alpha(a_i) = \omega(a_{i-1})$. Ainsi, on peut amplifier un mot en un autre si et seulement si on peut simplifier l'autre en l'un. Alors, si $M \sim M'$ via une suite d'amplifications-simplifications $M = M_1 \rightarrow \dots \rightarrow M_n = M'$, alors on peut associer à chacune des opérations transformant M_i en M_{i+1} son inverse transformant M_{i+1} en M_i et on obtient: $M' = M_n \rightarrow \dots \rightarrow M_1 = M$.

On parlera de chemin réduit pour une suite d'arête $a_1 \dots a_n$ qui ne puisse pas être simplifiée c'est-à-dire en sorte que $a_i \neq \iota(a_{i+1}) \quad \forall i = 1, \dots, n-1$. Dans chaque classe il en existe au moins un qui est une suite contenant le moins d'arêtes possibles.

On peut alors montrer que la concaténation est compatible avec la relation d'allers retours : En effet, pour chaque $M = a_1 \dots a_m \rightsquigarrow b_1 \dots b_n = N$ via $M = M_1 \rightarrow \dots \rightarrow M_h = N$ et $O = c_1 \dots c_o \rightsquigarrow d_1 \dots d_p = P$ via $O = O_1 \rightarrow \dots \rightarrow O_k = P$, alors on obtient que $M \circ O \rightsquigarrow N \circ P$ via la suite:

$$M \circ O = M_1 \circ O \rightarrow \dots \rightarrow M_h \circ O = N \circ O = N \circ O_1 \rightarrow \dots \rightarrow N \circ O_k = N \circ P$$

Soit $C = (S, A, \varepsilon, \iota)$ un graphe et $s \in S$. On appelle groupe fondamental, et on note $\pi_1(C, s)$, le quotient de l'ensemble des chemins partant de et arrivant en s quotienté par la relation d'équivalence d'allers-retours \rightsquigarrow . L'opération est héritée de la concaténation des boucles en s qui passe aux classes puisque cette opération est compatible avec la relation. On notera cette opération par le même signe. On a donc $[M] \circ [M'] = [M \circ M']$. L'associativité et l'élément neutre $[\emptyset]$ en découlent également.

Il reste à prouver que l'on a bien des inverses: pour une boucle $a_1 \dots a_n$, la suite $\iota(a_n) \dots \iota(a_1)$ est également une boucle puisque $\omega(\iota(a_{i+1})) = \alpha(a_{i+1}) = \omega(a_i) = \alpha(\iota(a_i))$ et $\omega \circ \iota(a_1) = \alpha(a_1) = s$ et $\alpha \circ \iota(a_n) = \omega(a_n) = s$, de plus on vérifie à l'oeil que l'on a bien $a_1 \dots a_n \circ \iota(a_n) \dots \iota(a_1) \rightsquigarrow \emptyset$ et de la même manière que $\iota(a_n) \dots \iota(a_1) \circ a_1 \dots a_n \rightsquigarrow \emptyset$.

Arbres et ses propriétés

Un graphe C connexe en sorte que $\pi_1(C, s)$ est le groupe trivial est appelé un arbre, on dira qu'il est simplement connexe.

Montrons que cette définition (appelons la (i)) est équivalente à la définition suivante, peut-être plus connue: un arbre est un graphe si chaque paire de points n'est reliée que par un unique chemin réduit (ii).

(i) \Rightarrow (ii): Admettons qu'entre deux point p et q il existe deux chemins réduits distincts $a_1 \dots a_n$ et $b_1 \dots b_m$. Puisque $\alpha(a_1) = p = \alpha(b_1)$ et que $\omega(a_n) = q = \omega(b_m)$, on peut construire la boucle en q : $a_n \dots a_1 \iota(b_1) \dots \iota(b_m)$. Puisque $a_1 \dots a_n \neq b_1 \dots b_m$, on a certains i en sorte que $a_i \neq b_i$, prenons le plus petit tel i . Ainsi $\iota(a_n) \dots \iota(a_1) b_1 \dots b_m \rightsquigarrow \iota(a_n) \dots \iota(a_i) b_i \dots b_m$ et ce chemin est réduit puisqu'aucune autre simplification n'est possible (chacune des parties $\iota(a_1) \dots \iota(a_i)$ et $b_i \dots b_m$ sont des mots réduits et $\iota(a_i) \neq \iota(b_i)$ puisque $a_i \neq b_i$).

Ainsi donc cette boucle n'est pas équivalente au chemin vide. Appelons alors J un chemin joignant s à q et J^{-1} le chemin inverse alors $J \circ \iota(a_n) \dots \iota(a_i) b_i \dots b_m \circ J^{-1}$ est une boucle en s qui ne peut pas être équivalente à \emptyset (sinon, en vertu de la compatibilité de la concaténation avec la relations d'allers-retours, $\iota(a_n) \dots \iota(a_i) b_i \dots b_m$ serait équivalente à la première boucle aussi). On a donc obtenu une boucle en s non-équivalente à \emptyset alors que $\pi_1(C, s)$ est trivial. Absurdité! Donc $a_1 \dots a_n = b_1 \dots b_m$

(ii) \Rightarrow (i): Prenons une boucle en s qui ne soit pas équivalente à \emptyset , alors on peut trouver une boucle réduite $a_1 \dots a_n$ qui lui est équivalente. Par non trivialité $n \geq 1$, choisissons alors un i entre 1 et n et soit $p = \omega(a_i)$. Le chemin $a_1 \dots a_i$ est un chemin réduit (puisque $a_1 \dots a_n$ l'est) et il relie s à p ; de même, le chemin $\iota(a_n) \dots \iota(a_1)$ est également réduit (car $\iota(a_i) \neq a_{i+1} \Rightarrow \iota \circ \iota(a_{i+1}) \neq \iota(a_i)$) et il relie également s à p . Ces deux chemins étant distincts, on conclut à l'absurdité ! Notre supposition que l'on pouvait trouver une boucle non-équivalente au chemin trivial était donc fausse. Et on a bien que $\pi_1(C, s)$ est le groupe trivial.

Lemme Soit C un graphe non-vide. L'ensemble des sous-graphes de C qui sont des arbres peut être ordonné partiellement, ainsi (Zorn), on peut trouver un arbre maximal dans C qui, si C est connexe, contient tous les sommets du graphe.

DEMO On parlera d'arbre dans C au lieu de sous-graphe de C qui est un arbre. Remarquons d'abord qu'il existe au moins un arbre dans C : le graphe étant non-vide, on peut trouver un sommet s , le graphe composé de ce seul sommet est déjà un arbre. Prenons $T' = (S', A', \varepsilon', \iota')$ et $T'' = (S'', A'', \varepsilon'', \iota'')$ deux arbres dans C . On dira que T' est *inclus* dans T'' (on notera $T' \prec T''$) si $A' \subset A''$ (inclusion stricte). On a, dans ce cas, que T' est un sous-graphe de T'' puisque (connexité) $S'' = \omega(A'') \subset \omega(A') = S'$ et $\varepsilon'' = \varepsilon|_{A''} = (\varepsilon|_{A'})|_{A''} = \varepsilon'|_{A''}$.

On a bien un ordre puisque $T' \prec T''$ et $T'' \prec T'''$ implique que $A' \subset A'' \subset A'''$, donc $A' \subset A'''$ ainsi $T' \prec T'''$; de plus $T \not\prec T$ puisque $A = A$ et donc $A \not\subset A$. Si maintenant on se donne un sous-ensemble $O = (T_i)_{i \in I} = (S_i, A_i, \varepsilon|_{A_i}, \iota|_{A_i})$ totalement ordonné de l'ensemble des arbres dans C alors on construit O_M comme le graphe $(S_M, A_M, \varepsilon|_{A_M}, \iota|_{A_M})$ tel que :

$$S_M = \bigcup_{i \in I} S_i \qquad A_M = \bigcup_{i \in I} A_i$$

Il est clair que c'est un graphe. Il est connexe puisque pour chaque paire de points, on peut trouver un S_i dans lesquels ils sont, S_i étant un arbre, on peut rejoindre la paire de points par une suite d'arêtes de $A_i \subset A_M$. De plus, pour chaque boucle $a_1 \dots a_n$, on peut trouver un O_i qui la contient (puisque'on peut trouver un O_{i_k} qui contient l'arête a_k , il suffit alors de prendre le plus grand de ces O_{i_k} ce qui est possible puisqu'il n'y en a qu'un nombre fini); or ce O_i est un arbre donc on peut simplifier cette boucle en l'identité, la simplification se fera aussi dans O_M puisque le ι est le même sur les arêtes de O_i , de O_M et de C . Ainsi donc O_M est un arbre.

On a donc un ensemble partiellement ordonné pour lequel tout sous-ensemble totalement ordonné admet une borne supérieure, le lemme de Zorn nous permet donc d'affirmer qu'il existe un arbre dans C qui ne peut être inclus dans un autre arbre sans lui être égal. Puisque un arbre composé d'un seul sommet est déjà un arbre dans C , on peut être sur que cet arbre contient au moins un sommet.

Il reste à voir qu'un tel arbre maximal contient tous les sommets de C . Supposons par l'absurde qu'il existe un sommet p de C qui ne soit pas un des sommets de l'arbre maximal. Puisque C est connexe on peut donc relier p à l'un des sommets de l'arbre par un chemin $a_1 \dots a_n$. On prend le plus grand i en sorte que a_i ne soit pas dans l'arbre et que $\alpha(a_i)$ non plus (au moins a_1 sinon p serait dans l'arbre) alors, en posant $S_M' = S_M \cup \{\alpha(a_i)\}$ et $A_M' = A_M \cup a_i$ on obtient un sous-graphe $O_M' = (S_M', A_M', \varepsilon|_{A_M'}, \iota|_{A_M'})$. Celui-ci est encore un arbre puisque toute boucle en s qui ne passe pas par a_i est équivalente modulo allers-retours à \emptyset (car O_M est un arbre) et si une boucle $b_1 \dots b_m$ passe par a_i , disons $b_k = a_i$ alors on a forcément $b_{k+1} = \iota(a_i)$ et donc elle est simplifiable en $b_1 \dots b_{k-1} b_{k+2} \dots b_m$, donc toute boucle est encore équivalente, modulo allers-retours, à \emptyset et O_M' est donc un arbre dans C qui est strictement inclus dans O_M . Absurdité ! Donc O_M contient tous les sommets.

☐

Outil Réciproquement, si $O_M = (T, B, \varepsilon|_B, \iota|_B)$ est un sous-graphe simplement connexe de $(S, A, \varepsilon, \iota)$ tel que $T = S$ alors $(T, B, \varepsilon|_B, \iota|_B)$ est un arbre maximal.

DEMO Supposons que O_M n'est pas maximal, alors il existerait un arbre $O_M' = (T', B', \varepsilon|_{B'}, \iota|_{B'})$ tel que $B \subset B'$ et $B \neq B'$. Soit alors une arête b un élément de $B' \setminus B$. Puisque T contient tous les sommets de $(S, A, \varepsilon, \iota)$, on a $\alpha(b)$ et $\omega(b) \in T$ et donc il existe un unique chemin réduit dans O_M allant de $\alpha(b)$ et à $\omega(b)$. Et, puisque O_M est un sous-graphe de O_M' , ce chemin est réduit dans O_M . Puisque O_M' il est donc l'unique chemin réduit allant de $\alpha(b)$ à $\omega(b)$. De plus ce chemin est différent du chemin composé l'unique arête b , puisqu'il est dans O_M alors que b est dans $B' \setminus B$, en outre, le chemin b est réduit. On a donc deux chemins réduits distincts joignant $\alpha(b)$ à $\omega(b)$. Absurdité !

☐

Théorème Pour n'importe quel graphe C connexe, le $\pi_1(C, s)$ est un groupe libre. De plus, si $T_M = (S_M, A_M, \varepsilon|_{A_M}, \iota|_{A_M})$ est un arbre maximal dans C , on a une bijection entre $A \setminus A_M$ et X où X est une base famille symétrique du groupe libre $\pi_1(C, s)$.

DEMO Définissons φ une application allant de A dans l'ensemble des chemins depuis s qui a tout $a \in A$ associe l'unique chemin réduit $\varphi(a)$ de T_M joignant s à $\alpha(a)$. De même, on définit $\varphi'(a)$ comme l'unique chemin réduit dans T_M joignant $\omega(a)$ à s ; on adopte ici la convention d'écrire $\iota(a_1 \dots a_n)$

au lieu de $\iota(a_n) \dots \iota(a_1)$, et l'on appelle \bar{a} le chemin composé de l'unique arête a . Alors on peut construire :

$$\begin{aligned} \chi: A &\longrightarrow \pi_1(C, s) \\ a &\longmapsto [\varphi(a)^c \bar{a}^c \varphi'(a)] \end{aligned}$$

Montrons que $\chi(A)$ engendre tout $\pi_1(C, s)$:

Prenons un $[a_1 \dots a_n] \in \pi_1(C, s)$ alors :

$$\begin{aligned} [\chi(a_1)^c \dots \chi(a_n)] &= [\varphi(a_1)^c \bar{a}_1^c \varphi'(a_1)^c \dots \varphi(a_n)^c \bar{a}_n^c \varphi'(a_n)] \\ &\stackrel{\alpha(a_i) = \omega(a_{i+1})}{=} [\varphi(a_1)^c \bar{a}_1 \dots \bar{a}_n^c \varphi'(a_n)] \stackrel{\alpha(a_1) = s = \omega(a_n)}{=} [a_1 \dots a_n] \\ &\Rightarrow \varphi'(a_i) = \iota \circ \varphi(a_{i+1}) \Rightarrow \varphi(a_1) = \emptyset = \varphi'(a_n) \end{aligned}$$

Donc tout élément de $\pi_1(C, s)$ est exprimable comme produit d'éléments de $\chi(A)$. On appellera X l'ensemble $\chi(A) \dot{-} \{[\emptyset]\}$. On le munit de l'opération d'inverse suivante : $\chi(a)^{-1} = \chi \circ \iota(a)$. Vérifions alors que cela correspond à l'opération d'inverse dans le groupe fondamental :

$$\chi(\iota(a)) = [\varphi(\iota(a))^c \overline{\iota(a)}^c \varphi'(\iota(a))] = [\iota(\varphi'(a))^c \overline{\iota(a)}^c \iota(\varphi(a))] = [\iota(\varphi(a)^c \bar{a}^c \varphi'(a))] = [\varphi(a)^c \bar{a}^c \varphi'(a)]^{-1}$$

Ainsi donc X est un ensemble symétrique engendrant $\pi_1(C, s)$. On observe ensuite que $\chi(a) = [\emptyset]$ si a est dans A_M , en effet, la boucle $\varphi(a)^c \bar{a}^c \varphi'(a)$ n'est composée que d'arêtes dans T_M , il s'agit donc d'une boucle dans T_M . Or T_M est simplement connexe, ainsi $\chi(a)$ est simplifiable dans T_M en \emptyset ; puisque T_M est un sous-graphe de C , on peut dire que les simplifications peuvent alors se faire dans C et donc $a \in A_M \Rightarrow \chi(a) = [\emptyset]$. On a donc que $X = \chi(A) \dot{-} \{[\emptyset]\} = \chi(A \dot{-} A_M)$

Pour montrer que $\pi_1(C, s)$ est bien un groupe libre, il nous faut encore montrer que chaque mot sur l'alphabet X qui représente un élément trivial est un mot simplifiable.

Supposons en effet qu'il y ait une suite d'arêtes $(a_i)_{i=1}^n$ tel que $\chi(a_1)^c \dots \chi(a_n) = [\emptyset]$. Donc la boucle $M = \varphi(a_1)^c \bar{a}_1^c \varphi'(a_1)^c \dots \varphi(a_n)^c \bar{a}_n^c \varphi'(a_n)$ serait simplifiable en \emptyset . Mais les arêtes a_i sont dans $A \dot{-} A_M$ tandis que les arêtes des $\varphi(a_i)$ et $\varphi'(a_i)$ sont dans A_M ainsi donc on ne pourrait simplifier que les a_i entre eux et les $\varphi(a_i)$ et $\varphi'(a_i)$ entre eux. D'où $\varphi'(a_i)^c \varphi(a_i) \sim \emptyset$, i.e. on aurait $\alpha \circ \varphi'(a_i) = \omega \circ \varphi(a_{i+1})$. Donc M serait simplifiable en $a_1 \dots a_n$ qui lui-même serait encore simplifiable en \emptyset donc on aurait un i tel que $a_i = \iota(a_{i+1})$ mais alors $\chi(a_{i+1}) = \chi(a_i)^{-1}$ et donc le mot serait simplifiable dans l'alphabet symétrique X .

Afin d'obtenir la bijection, il convient alors de montrer que χ est injective : prenons a et b deux arêtes de $A \dot{-} A_M$ et supposons que $\chi(a) = \chi(b)$. On aurait alors que $\chi(a)^c \chi(b)^{-1} = \chi(a)^c \chi(\iota(b)) = [\emptyset]$ et donc, d'après le raisonnement précédent, $ab^{-1} \sim \emptyset$ i.e. $a = b$. Ainsi χ est injective et donc bijective de $A \dot{-} A_M$ dans X .

☞

Revêtement universel

Désormais, nous ne considérerons que les graphes connexes. Soit $C = (S, A, \varepsilon, \iota)$ un graphe. On choisit un sommet $s \in S$. On définit C_s comme l'ensemble des chemins partant de s . Rappelons que l'on appelle chemin les suites finies d'arêtes qui se suivent et que l'on a égalité de deux chemins $a_1 \dots a_n$ avec $b_1 \dots b_m$ si et seulement si $m = n$ et $a_i = b_i \quad \forall i = 1 \dots n$. Adoptons la convention suivante : si $p = a_1 \dots a_n$, on écrira $\omega(p)$ au lieu de $\omega(a_n)$ et $\alpha(p)$ au lieu de $\alpha(a_1)$. On définit \tilde{S} comme le quotient C_s / \sim .

On définit alors l'ensemble \tilde{A} comme :

$$\tilde{A} = \left\{ ([p], a) \in \tilde{S} \times A \mid \omega(p) = \alpha(a) \right\}$$

L'incidence se définit comme : $\tilde{\varepsilon}([p], a) = ([p], [p^c a])$, on définit donc $\tilde{\alpha}$ et $\tilde{\omega}$.

Alors on pose $\tilde{\iota}: \tilde{A} \longrightarrow \tilde{A}$
 $[p], a \longmapsto ([p^c a], \iota(a))$

En effet $p^c a$ est un chemin (car $\omega(p) = \alpha(a)$) et $([p^c a], \iota(a))$ est une arête puisque $\omega(p^c a) = \omega(a) = \alpha \circ \iota(a)$.

Le quadruplet $\tilde{C} = (\tilde{S}, \tilde{A}, \tilde{\varepsilon}, \tilde{\iota})$ est alors un graphe puisque :

$$\tilde{\varepsilon}(\tilde{\iota}([p], a)) = \tilde{\varepsilon}([p^c a], \iota(a)) = ([p^c a], [p^c a \iota(a)]) = ([p^c a], [p]) = (\tilde{\omega}([p], a), \tilde{\alpha}([p], a))$$

On peut alors construire $\sigma: \tilde{S} \rightarrow S$
 $[p] \mapsto \omega(p)$

Cette application est bien définie puisque les simplifications ou amplifications ne changent pas les extrémités d'un chemin, en outre elle est surjective car le graphe est connexe.

On peut également redescendre les arêtes, on construit $\rho: \tilde{A} \rightarrow A$
 $([p], a) \mapsto a$

Il s'agit montrer que le couple (σ, ρ) est bel et bien un morphisme de graphe et même un revêtement.

Le fait qu'il s'agit d'un morphisme de graphe découle des deux raisonnements suivants :

On a $\varepsilon(\rho([p], a)) = \varepsilon(a)$ or :

$$(\sigma, \sigma) \circ \tilde{\varepsilon}([p], a) = (\sigma, \sigma)([p], [p^c a]) = (\omega(p), \omega(p^c a)) = (\alpha(a), \omega(a)) = \varepsilon(a)$$

On a commutation entre les inversions et ρ puisque $\rho \circ \tilde{\iota}([p], a) = \rho([p^c a], \iota(a)) = \iota(a) = \iota(\rho([p], a))$.

Montrons maintenant que (σ, ρ) est un revêtement i.e. que restreint sur l'étoile de chaque point, ρ est une bijection et que ρ est surjective.

bijection locale : soit $p = a_1 \dots a_n$ et donc $[p]$ un sommet de \tilde{C} , définissons les ensembles :

$$E_\alpha = \{a \in A \mid \alpha(a) = \sigma([p])\} \quad \tilde{E}_\alpha = \{([p], a) \in \tilde{A}\}$$

Il est clair, en vertu de l'incidence, que $\rho(\tilde{E}_\alpha) \subset E_\alpha$. Le travail consiste maintenant à montrer que $\rho: \tilde{E}_\alpha \rightarrow E_\alpha$ est bijective.

La surjection vient directement : soit $a \in E_\alpha$ alors $\alpha(a) = \sigma(p) = \omega(p)$ on a alors un arête $([p], a)$ dans \tilde{E}_α avec $\rho([p], a) = a$.

Pour montrer l'injectivité de cette application, prenons $([q], a)$ et $([r], b)$ deux arêtes de \tilde{E}_α qui ont la même image par ρ . On a donc $[q] = \tilde{\alpha}([q], a) = [p] = \tilde{\alpha}([r], b) = [r]$, en outre $a = \rho([q], a) = \rho([r], b) = b$ ainsi $([q], a) = ([r], b)$. Donc $\rho: \tilde{E}_\alpha \rightarrow E_\alpha$ est injective.

ρ surjective : soit a une arête de C , puisque C est connexe on sait qu'il existe un chemin p avec $\omega(p) = \sigma(p) = \alpha(a)$. Alors $([p], a)$ est une arête de \tilde{A} avec $\rho([p], a) = a$. Donc $\rho: \tilde{A} \rightarrow A$ est surjective.

En résumé, on vient de construire pour chaque graphe C un graphe \tilde{C} et un revêtement $(\sigma, \rho): \tilde{C} \rightarrow C$. La paire $(C, (\sigma, \rho))$ sera appelé le revêtement universel de C .

Lemme Le graphe \tilde{C} du revêtement universel d'un graphe C est un arbre, c'est-à-dire qu'il est simplement connexe.

DEMO Prenons une boucle $A_1 \dots A_n$ non triviale en $[\emptyset]$. Puisque c'est une boucle, on aurait $\tilde{\alpha}(A_1) = [\emptyset]$ et $\tilde{\omega}(A_n) = [\emptyset]$. Appelons $([p_i], a_i)$ les arêtes successives, donc, puisque $A_1 \dots A_n$ est un chemin, on a $\forall i = 1 \dots n-1$ que $\tilde{\omega}(A_i) = [p_i^c a_i] = \tilde{\alpha}(A_{i+1}) = [p_{i+1}]$; or $[p_1] = [\emptyset]$ ainsi $[p_i] = [a_1 \dots a_{i-1}]$. Alors, puisque $A_1 \dots A_n$ est une boucle $\tilde{\omega}(A_1 \dots A_n) = [p_n^c a_n] = [a_1 \dots a_n] = [\emptyset]$. Donc le chemin $a_1 \dots a_n$ est équivalent à \emptyset dans C .

Ainsi, si \tilde{C} n'était pas simplement connexe, on pourrait trouver une boucle $A_1 \dots A_n$ en $[\emptyset]$ qui serait un chemin réduit ($\tilde{\iota}(A_i) \neq A_{i+1}$ pour $i = 1 \dots n-1$) et non trivial ($n > 0$). Alors, en vertu de la bijection locale ρ au points $\tilde{\omega}(A_i)$, on aurait que $\iota(a_i) \neq a_{i+1}$ pour $i = 1 \dots n-1$ donc le chemin $a_1 \dots a_n$ serait un chemin réduit dans C et non trivial, donc $a_1 \dots a_n \not\sim \emptyset$ et $\tilde{\omega}(A_1 \dots A_n) = [a_1 \dots a_n] \neq [\emptyset]$ donc $A_1 \dots A_n$ ne serait pas une boucle. Absurdité.

☐

Définition

Soit (σ, ρ) un revêtement entre C et C' . On appelle transformation de revêtement un isomorphisme de graphe (τ_S, τ_A) de C dans C' en sorte que $\sigma \circ \tau_S = \tilde{\sigma}$ et $\rho \circ \tau_A = \tilde{\rho}$. Il est clair que l'ensemble de ces transformations muni de l'opération de composition est un groupe.

Lemme Le groupe des transformations de revêtements d'un revêtement universel $(\sigma, \rho): \tilde{C} \longrightarrow C$ est isomorphe à $\pi_1(C, s)$ où s est le sommet choisi pour construire le revêtement universel.

DEMO Remarquons d'abord que la fibre $\sigma^{-1}(s)$ est l'ensemble des chemins qui partent de et arrivent en s quotienté par la relation d'allers retours, il s'agit donc du groupe fondamental $\pi_1(C, s)$.

Appelons G l'ensemble des transformations de revêtement.

On construit une application $\varphi: \sigma^{-1}(s) \longrightarrow G$ où τ_S^p et τ_A^p sont définis comme suit:

$$p \longmapsto (\tau_S^p, \tau_A^p)$$

Prenons un sommet $[p] \in \pi_1(C, s)$ alors pour chaque sommet $[r]$ j'ai que $\alpha(r) = s = \omega(p)$ et donc que $[p^c r]$ est un sommet de \tilde{C} , de même, pour chaque arête $([r], a)$, j'ai que $[p^c r] \in \tilde{S}$ et que $\sigma(p^c r) = \omega(r) = \alpha(a)$ donc $([p^c r], a) \in \tilde{A}$. Il est donc correct de poser:

$$\begin{aligned} \tau_S^p: \tilde{S} &\longrightarrow \tilde{S} & \tau_A^p: \tilde{A} &\longrightarrow \tilde{A} \\ [r] &\longmapsto [p^c r] & ([r], a) &\longmapsto ([p^c r], a) \end{aligned}$$

Il s'agit bien d'un morphisme de graphe puisque:

$$\tau_A^p \circ \iota([r], a) = \tau_A^p([r^c a], \iota(a)) = ([p^c r^c a], \iota(a)) = \tilde{\iota}([p^c r], a) = \tilde{\iota} \circ \tau_A^p([r], a)$$

$$\tilde{\alpha} \circ \tau_A^p([r], a) = \tilde{\alpha}([p^c r], a) = [p^c r] = \tau_S^p([r]) = \tau_S^p \circ \tilde{\alpha}([r], a)$$

$$\tilde{\omega} \circ \tau_A^p([r], a) = \tilde{\omega}([p^c r], a) = [p^c r^c a] = \tau_S^p([r^c a]) = \tau_S^p \circ \tilde{\omega}([r], a)$$

Prenons p et q dans $\pi_1(C, s)$ et déterminons le morphisme $(\tau_S^p \circ \tau_S^q, \tau_A^p \circ \tau_A^q)$. Pour tout sommet r et arête A : $\tau_S^p \circ \tau_S^q([r]) = [p^c q^c r] = \tau_S^o$ où $o = p^c q$, de même:

$$\tau_A^p \circ \tau_A^q([r], a) = ([p^c q^c r], a) = \tau_A^o([r], a) \text{ où } o = p^c q$$

Sachant, de plus, que $\tau_S^{\emptyset}([r]) = [\emptyset^c r] = [r]$ et que $\tau_A^{\emptyset}([r], a) = ([\emptyset^c r], a) = ([r], a)$, on a donc que $(\tau_S^{\emptyset}, \tau_A^{\emptyset})$ est la transformation identité. Ainsi, pour $[p] \in \pi_1(C, s)$ on peut trouver $[p^{-1}] \in \pi_1(C, s)$ et alors $\tau_S^p \circ \tau_S^{p^{-1}} = \tau_S^{\emptyset} = Id_{\tilde{S}}$ et $\tau_A^p \circ \tau_A^{p^{-1}} = \tau_A^{\emptyset} = Id_{\tilde{A}}$. Ainsi chaque endomorphisme de graphe (τ_S^p, τ_A^p) admet un endomorphisme inverse, donc tous les (τ_S^p, τ_A^p) sont des isomorphismes de graphes de \tilde{C} dans \tilde{C} .

Enfin, vérifions que ces isomorphismes sont des transformations de revêtement:

$$\sigma \circ \tau_S^p([r]) = \sigma([p^c r]) = \omega(p^c r) = \omega(r) = \sigma([r]), \text{ et } \rho \circ \tau_A^p([r], a) = \rho([p^c r], a) = a = \rho([r], a)$$

On vient donc de montrer que $\varphi: \pi_1(C, s) \longrightarrow G$ est un morphisme de groupe.

$$[p] \longmapsto (\tau_S^p, \tau_A^p)$$

Il ne nous reste plus qu'à montrer que φ est un isomorphisme de groupe:

Surjection: soit (μ, ν) une transformation de revêtement alors on pose $p = \mu([\emptyset])$. Nous allons montrer que $\mu = \tau_S^p$ et $\nu = \tau_A^p$. Pour cela prenons, pour un point $[r]$ et une arête $A = ([r], a)$, l'unique (puisqu'arbre) chemin $A_1 \dots A_n$ entre $[\emptyset]$ et $[r]$. Posons $r = r_1 \dots r_k$, puisque $([\emptyset], r_1) \dots ([r_1 \dots r_{k-1}], r_k)$ en est un, on a que $k = n + 1$ et $A_i = ([r_1 \dots r_{i-1}], r_i)$. On considère le chemin $\nu(A_1) \dots \nu(A_n)$: $\nu(A_1)$ est une arête partant de $\mu([\emptyset]) = p$, or $\rho \circ \nu(A_1) = \rho(A_1) = r_1$ donc $\nu(A_1) = ([p], r_1) = \tau_A^p(A_1)$

Récurrence: pour i allant de 2 à n on suppose que $\nu(A_i) = \tau_A^p(A_i)$. Alors $\nu(A_{i+1})$ est une arête partant de $\tilde{\omega}(\nu(A_i)) = \tilde{\omega}(\tau_A^p(A_i)) = [p^c r_1 \dots r_i]$ et telle que $\rho \circ \nu(A_{i+1}) = \rho(A_{i+1}) = r_{i+1}$, ainsi $\nu(A_{i+1}) = ([p^c r_1 \dots r_i], r_{i+1}) = \tau_A^p(A_{i+1})$.

De même, $\nu(A)$ est une arête qui part de $\tilde{\omega}(\nu(A_n)) = [p^c r_1 \dots r_k]$ et telle que $\rho \circ \nu(A) = \rho(A) = a$ ainsi $\nu(A) = ([p^c r], a) = \tau_A^p(A)$. Mais alors l'incidence nous permet de dire que $\mu([r]) = \mu(\tilde{\alpha}(A)) = \tilde{\alpha} \circ \nu(A) = \tilde{\alpha}([p^c r], a) = [p^c r] = \tau_S^p([r])$.

On vient donc de montrer que si (μ, ν) est une transformation de revêtement alors elle est égale à un (τ_S^p, τ_A^p) pour $p = \mu([\emptyset])$. Ainsi $\varphi: \pi_1(C, s) \longrightarrow G$ est surjective.

Injection: Supposons que nous avons deux éléments distincts $[q]$ et $[p]$ de $\pi_1(C, s)$ alors $\tau_S^p([\emptyset]) = [p^c \emptyset] = [p] \neq [q] = [q^c \emptyset] = \tau_S^q([\emptyset])$, ainsi $\tau_S^p \neq \tau_S^q$ et donc $\varphi([p]) = (\tau_S^p, \tau_A^p) \neq (\tau_S^q, \tau_A^q) = \varphi([q])$. Ainsi φ est injective.

Ainsi donc φ est un isomorphisme de groupe.

☐

Lemme Soit $C = (S, A, \varepsilon, \iota)$ un graphe et $\tilde{C} = (\tilde{S}, \tilde{A}, \tilde{\varepsilon}, \tilde{\iota})$ son revêtement universel. Alors C est le quotient de \tilde{C} par l'action du groupe G des transformation de revêtement.

DEMO La démarche de cette preuve consiste à montrer que (σ, ρ) passent au quotient et deviennent alors des isomorphismes de graphe. On commence par montrer que deux sommets (resp. deux arêtes) sont équivalents si et seulement si σ (resp. ρ) les envoie sur la même image.

Soient $[r]$ et $[q]$ deux sommets de \tilde{C} et en sorte que $\sigma(r) = \sigma(q)$ alors $\omega(r) = \sigma([r]) = \sigma([q]) = \omega(q)$, alors $\alpha(\iota(r)) = \omega(r) = \omega(q)$ ainsi $q\iota(r)$ est un chemin partant de $\alpha(q) = s$ et revenant en $\omega(\iota(r)) = \alpha(r) = s$, donc une boucle en s . Ainsi $[q\iota(r)] \in \pi_1(C, s)$, d'où $\exists p \in \pi_1(C, s)$ tq $[r] = [p\circ q] = \tau_S^p(q)$.

Réciproquement, s'il existe $p \in \pi_1(C, s)$ tel que $[r] = \tau_S^p(q) = [p\circ q]$ alors $\sigma(r) = \sigma(q)$ puisque τ_S^p est une transformation de revêtement.

De même, on a $a = \rho([r], a) = \rho([q], b)$ et $([r], a), ([q], b) \in \tilde{A}$ si et seulement si $\sigma(r) = \alpha(a) = \alpha(b) = \sigma(q)$ et $a = b \in A$. Mais, par ce que nous venons de montrer, cette dernière assertion est équivalente à dire que $a = b$ et qu'il existe $p \in \pi_1(C, s)$ tel que $[r] = [p\circ q]$. Ceci revient à dire qu'il existe $p \in \pi_1(C, s)$ tel que $\tau_A^p([q], b) = ([r], a)$.

On a donc construit une relation \approx sur les sommets qui est définie comme :

$$[r] \approx [q] \Leftrightarrow \exists p \in \pi_1(C, s) \text{ t.q. } [r] = [p\circ q] \Leftrightarrow \exists (\mu, \nu) \in G \text{ t.q. } \mu([r]) = [q] \Leftrightarrow \sigma([r]) = \sigma([q])$$

Il s'agit bien d'une relation d'équivalence, puisqu'elle vient de l'action d'un groupe.

De même, on a construit une relation \cong sur les arêtes de \tilde{A} qui est définie comme :

$$([r], a) \cong ([q], b) \Leftrightarrow \rho([r], a) = a = b = \rho([q], b) \Leftrightarrow \exists (\mu, \nu) \in G \text{ t.q. } \nu([r], a) = ([q], b)$$

Cette relation est bien une relation d'équivalence puisqu'elle vient de l'action d'un groupe.

Appelons $S' = \tilde{S}/\approx$ et $A' = \tilde{A}/\cong$. Il est clair que $\tilde{\varepsilon}$ et $\tilde{\iota}$ passe au quotient :

$$A \cong A' \Rightarrow \exists (\mu, \nu) \in G \text{ t.q. } \nu(A) = A' \Rightarrow \tilde{\varepsilon}(A') = \tilde{\varepsilon}(\nu(A)) = (\mu, \mu)(\tilde{\varepsilon}(A)) \approx \tilde{\varepsilon}(A)$$

$$\text{et } \tilde{\iota}(A') = \tilde{\iota} \circ \nu(A) = \nu \circ \tilde{\iota}(A) \cong \tilde{\iota}(A)$$

D'après la surjectivité de ρ et σ et d'après cette la définition des relations, on a donc que ρ' et σ' (le passage au quotient de ρ et σ) sont des applications surjectives et injectives. Il est clair, de plus, que (ρ', σ') est un morphisme de graphe, donc (ρ', σ') est un isomorphisme de graphe. On peut donc dire que C est le quotient de \tilde{C} par l'action de G .

□

Graphes de Cayley

Le propos de cette partie est de définir un graphe associé à un groupe qui nous permettra de "visualiser" le groupe. Nous commencerons notre étude par celle de graphes dits génériques, une propriété qui est conservée par revêtement. Puisque le but de ce chapitre est de donner un outil pour montrer qu'un groupe admet la présentation qu'on attend, nous allons réduire ce problème à la question de savoir si un graphe est isomorphe au graphe de Cayley d'un groupe. Pour ce, nous allons étudier les revêtements universels d'un graphe de Cayley pour passer, dans la partie suivante, aux revêtements d'un graphes sur les tous petits graphes.

Soit G un groupe et X un ensemble symétrique de générateurs (i.e. X engendre G et $X^{-1} \subset X$). On appellera graphe de Cayley le graphe $C(G, X) = (G, G \times X, \varepsilon_G, \iota)$ donné comme : l'ensemble des sommets est G , l'ensemble des arêtes A_G est $G \times X$. On construit alors $\varepsilon_G(g, x) = (g, g \cdot x)$ et $\iota(g, x) = (g \cdot x, x^{-1})$. Il s'agit bien d'un graphe puisque :

$$\alpha_G \circ \iota(g, x) = \alpha_G(g \cdot x, x^{-1}) = g \cdot x = \omega_G(g, x) \quad \text{et} \quad \omega_G \circ \iota(g, x) = \omega_G(g \cdot x, x^{-1}) = g \cdot x \cdot x^{-1} = g = \alpha_G(g, x)$$

De plus $C(G, X)$ est connexe : en effet, prenons g et h deux sommets de $C(G, X)$. Puisque G est engendré par X , on peut trouver $x_1, \dots, x_n \in X$ en sorte que $g^{-1} \cdot h = x_1 \cdot \dots \cdot x_n$. Alors, la suite :

$$(g, x_1)(g \cdot x_1, x_2) \dots (g \cdot x_1 \cdot x_{n-1}, x_n)$$

est un chemin puisque $\omega(g \cdot x_1 \dots x_{i-1}, x_i) = g \cdot x_1 \dots x_i = \alpha(g \cdot x_1 \dots x_i, x_{i+1})$, il part de $\alpha(g, x_1) = g$ et arrive en $\omega(g \cdot x_1 \dots x_{n-1}, x_n) = g \cdot x_1 \dots x_n = g \cdot g^{-1} \cdot h = h$.

On dira d'un graphe qu'il est générique de degré p si de chaque sommet partent le même nombre d'arêtes.

Lemme Deux arbres génériques de même degré p sont isomorphes.

DEMO Appelons ces arbres $C = (S, A, (\alpha, \omega), \iota)$ et $D = (T, B, (\beta, \zeta), \kappa)$. Choisissons $s \in S$ et $t \in T$.

Et définissons $\forall x \in S$ l'ensemble $E_x = \{a \in A \mid \alpha(a) = x\}$, de même $\forall y \in t$, on définit l'ensemble $E_y = \{b \in B \mid \beta(b) = y\}$. Puisque les arbres sont du même degré, on peut choisir une bijection $e: E_s \rightarrow E_t$. Puisque C est générique, on a, pour chaque $x \in S$ une bijection $h_x: E_s \rightarrow E_x$; on a, de même, $\forall y \in T$ une bijection $k_y: E_t \rightarrow E_y$.

On veut donc construire un isomorphisme de graphe $(\mu, \nu): C \rightarrow D$. Soit $x \in S$ et $a \in E_x$. Puisque C est un arbre, il existe un unique chemin $a_1 \dots a_n$ joignant s à x . On pose alors $b_1 = e(a_1) \in E_t$. Puis, $\forall i = 2 \dots n$ on pose $b_i = k_{\zeta(b_{i-1})} \circ e \circ h_{\omega(a_{i-1})}(a_i)$. La suite $b_1 \dots b_n$ est alors un chemin de D puisque $\alpha(b_i) = \alpha(h_{\omega(b_{i-1})}(\dots)) = \omega(b_{i-1})$. On dira que $b_1 \dots b_n$ est le transporté génériquement de $a_1 \dots a_n$. Il faut savoir que ce transport dépend de b , des h_x et des k_y , ceux-ci pourront être modifiés en fonction des besoins.

On pose alors $\mu(x) = \omega(b_n)$ et $\nu(a) = k_{\zeta(b_n)} \circ e \circ h_{\omega(a_n)}(a)$.

Puisque $\nu(a) = k_{\zeta(b_n)}(\dots) \in E_{\zeta(b_n)}$, on a que $\alpha \circ \nu(a) = \zeta(b_n) = \mu(x) = \mu \circ \alpha(a)$. De même, on remarque que $a_1 \dots a_n a$ est l'unique chemin allant de s à $\omega(a_n)$, par définition de $\nu(a)$, on a que $b_1 \dots b_n \nu(a)$ est le transporté génériquement de $a_1 \dots a_n a$ donc $\mu \circ \omega(a_n) = \zeta \circ \nu(a)$.

De plus si a est cette même arête alors $a_1 \dots a_n a$ est l'unique chemin allant de s à $\alpha \circ \iota(a) = \omega(a)$ alors $b_1 \dots b_n b$ est bien le transporté génériquement de $a_1 \dots a_n a$ et $\nu \circ \iota(b)$ est donc une arête allant de $\beta \circ \nu \circ \iota(a) = \mu \circ \alpha \circ \iota(b) = \mu \circ \omega(a) = \zeta \circ \nu(a)$ à $\zeta \circ \nu \circ \iota(a) = \mu \circ \omega \circ \iota(a) = \mu \circ \alpha(a) = \beta \circ \nu(a)$. Or il n'y a qu'un seul chemin allant entre ces deux points et les arêtes $\nu \circ \iota(a)$ et $\kappa \circ \nu(a)$ le font, donc $\nu \circ \iota(a) = \kappa \circ \nu(a)$.

On a donc défini (μ, ν) comme un morphisme de graphe, il reste à vérifier que c'est une bijection : Pour cela, on montre qu'il existe un inverse de μ . En effet, pour tout sommet y de D , appelons $d_1 \dots d_m$ l'unique chemin joignant t à y . On refait alors la même construction avec b^1 : on pose $c_1 = e^{-1}(d_1)$ et $c_i = h_{\omega(c_{i-1})} \circ e^{-1} \circ k_{\zeta(d_{i-1})}(d_i)$ et l'on pose $\mu'(y) = \omega(c_m)$.

On a bien alors que $d_1 \dots d_m$ est le transporté génériquement de $c_1 \dots c_m$ ainsi $\mu(\omega(c_m)) = \omega(d_m)$ et donc $\mu \circ \mu'(y) = y$. Réciproquement, dans la construction de μ , on a obtenu que $a_i = h_{\omega(a_{i-1})} \circ e^{-1} \circ k_{\zeta(b_{i-1})}(b_i)$ donc que $\mu'(\omega(b_n)) = \omega(a_n)$ i.e. $\mu' \circ \mu(x) = \omega(a_n) = x$. Ainsi μ est bijective.

Pour trouver un inverse à ν il est alors évident de poser que, si b est une arête partant de y , $\nu'(b) = h_{\omega(c_n)} \circ e^{-1} \circ k_{\zeta(d_n)}(b)$. On obtient alors que $\nu' \circ \nu(a) = a$ et que $\nu \circ \nu'(b) = b$ par définition.

On vient donc de construire un morphisme de graphe $(\mu, \nu): C \rightarrow D$ qui est bijectif et donc qui est un isomorphisme.

☐

Lemme Tout graphe de Cayley $C(G, X) = (G, G \times X, \varepsilon, \iota)$ est un graphe générique de degré $|X|$.

DEMO En effet, on a, pour tout $g \in G$ que l'ensemble E_g des arêtes partant de g est :

$$E_g \{ (f, x) \in G \times X \mid f = \alpha(f, x) = g \} = \{g\} \times X$$

Donc E_g est en bijection avec E_f via $h_f^g: (g, x) \mapsto (f, x)$.

☐

Corollaire Le graphe de Cayley $C(F_X, X)$ d'un groupe libre $\langle X \rangle$ à base symétrique X est un arbre générique de degré $|X|$.

DEMO D'après le lemme, on a déjà que $C(X, \emptyset)$ est générique de degré $|X|$, il nous reste à vérifier que ce graphe est simplement connexe. Prenons une boucle $(g_1, x_1) \dots (g_n, a_n)$ au sommet e (l'élément neutre du groupe). Comme d'habitude on obtient que $g_1 = \alpha(g_1, x_1) = e$, puis que $g_i = \alpha(g_i, x_i) = \omega(g_{i-1}, x_{i-1}) = g_{i-1} \cdot x_{i-1}$ ainsi $g_i = x_1 \cdot \dots \cdot x_{i-1} \quad \forall i = 2 \dots n$. Mais il s'agit d'une boucle en e donc $e = \omega(g_n, x_n) = g_n \cdot x_n = x_1 \cdot \dots \cdot x_{n-1} \cdot x_n = x_1 \dots x_n$. Or, si dans G $x_1 \dots x_n = e$, cela veut dire que via la suppression de $x_i x_i^{-1}$, on peut simplifier $x_1 \dots x_n$ en e . Or toute simplification d'un mot $y_1 \dots y_n$ en $y_1 \dots y_{i-1} y_{i+2} \dots y_n$ implique $\iota(f_i, y_i) = (f_i^c y_i, y_i^{-1}) = (f_{i+1}, y_{i+1})$, donc la simplification du chemin. Dans notre cas donc, on a que $(g_1, x_1) \dots (g_n, x_n)$ est donc équivalent à \emptyset modulo les allers retours.

☐

Lemme Pour que le revêtement universel d'un graphe soit un arbre générique de degré p , il faut et il suffit que le graphe soit générique de degré p .

DEMO Évident en vertu de la bijection locale d'un revêtement.

☐

Corollaire Le revêtement universel d'un graphe de Cayley $C(G, X)$ est un arbre générique de degré $|X|$, il est donc isomorphe au graphe de Cayley du groupe libre $C(F_X, X)$. CLAIR

Bouquets et catalogues

Tous les isomorphismes donnés jusqu'à présent sont implicites. Afin de pouvoir donner des isomorphismes explicites et des critères implicites nous allons introduire le catalogage, c'est-à-dire une nomination des arêtes qui nous permettra de passer d'un graphe à un autre le long de chemins.

La base de l'outil que nous allons développer est la proposition suivante qui sera, au fur et à mesure du développement, transformée en une vérification en un nombre fini d'étape (pour des graphes finis).

Proposition de base Soient $C = (S, A, (\alpha, \omega), \iota)$ et $D = (T, B, (\beta, \zeta), \kappa)$ deux graphes en sorte qu'il existe un isomorphisme $(\theta_S, \theta_A): \tilde{C} \rightarrow \tilde{D}$, supposons de plus que $\theta_S(\pi_1(C, s)) \subset \pi_1(D, t)$ alors il existe un revêtement $(\sigma, \rho): C \rightarrow D$.

DEMO Rappelons-nous que nous avons un isomorphisme entre le groupe fondamental et le groupe des transformations de revêtement universel. Appelons G le groupe des transformations du revêtement universel \tilde{C} et H celui de \tilde{D} . On a les isomorphismes de groupe: $i: \pi_1(C, s) \rightarrow G$ et $j: \pi_1(D, t) \rightarrow H$.

Étape 1: $\pi_1(C, s) \subset \pi_1(D, t) \iff \theta_S \circ g \circ \theta_S^{-1} \in H \quad \forall g \in G$: Remarquons que pour tout sommet $[b_1 \dots b_n]$ de \tilde{D} , on a

$$[b_1 \dots b_n] = \omega_{\tilde{D}}([\emptyset, b_1] \dots ([b_1 \dots b_{n-1}], b_n))$$

Or, tout $g = i([p_1 \dots p_k]) \in G$ est exprimable comme: $g_S([x_1 \dots x_l]) = [p_1 \dots p_k^c x_1 \dots x_l]$ et $g_A([x_1 \dots x_n], x) = ([p_1 \dots p_n^c x_1 \dots x_n], x)$

Ainsi, grâce au fait que (θ_S, θ_A) préserve l'incidence et les inverses, on a unique chemin réduit $a_1 \dots a_n$ tel que $\theta_A^{-1}([\emptyset, b_1]) = (\theta_S^{-1}([\emptyset]), a_1)$ et $\theta_A^{-1}([b_1 \dots b_i], b_{i+1}) = (\theta_S^{-1}([\emptyset])^c [a_1 \dots a_i], a_{i+1})$. L'image par g est alors:

$$g \left((\theta_S^{-1}([\emptyset]), a_1) \dots (\theta_S^{-1}([\emptyset])^c [a_1 \dots a_{n-1}], a_n) \right) = ([p_1 \dots p_k]^c \theta_S^{-1}([\emptyset]), a_1) \dots ([p_1 \dots p_k]^c \theta_S^{-1}([\emptyset])^c [a_1 \dots a_{n-1}], a_n)$$

Or $\theta_A([p_1 \dots p_k]^c \theta_S^1([\emptyset]^c [a_1 \dots a_i], a_{i+1}))$ est une arête allant de $\theta_S([p_1 \dots p_k]^c [\emptyset]^c [b_1 \dots b_i])$ jusqu'à $\theta_S([p_1 \dots p_k]^c [\emptyset]^c [b_1 \dots b_{i+1}])$ en vertu de l'incidence préservée par (θ_S, θ_A) . Or l'arête $(\theta_S([p_1 \dots p_k]^c [b_1 \dots b_i]), b_{i+1})$ fait exactement le même chemin, en vertu de l'unicité du chemin réduit joignant deux points, on conclut que ces arêtes sont égales. On vient donc de montrer que $\theta_A \circ g_A \circ \theta_A^1([b_1 \dots b_i], b_{i+1}) = (\theta_S([p_1 \dots p_k]^c [b_1 \dots b_i]), b_{i+1})$. Ainsi la condition $\theta_S(\pi_1(C, s)) \subset \pi_1(D, t)$ est équivalente à $\theta_S \circ g \circ \theta_S^1 \in H \quad \forall g \in G$.

Remarquons que si x et y sont des sommets de \tilde{C} : $\sigma_C(x) = \sigma_C(y) \Rightarrow \sigma_D \circ \theta_S(x) = \sigma_D \circ \theta_S(y)$. En effet, on se rappelle que C est un quotient de \tilde{C} par G et que D est un quotient de \tilde{D} par H , on avait donc $\sigma_C(x) = \sigma_C(y) \Leftrightarrow \exists g_S \in G$ tel que $x = g_S(y)$ et, de même, on avait $\sigma_D(u) = \sigma_D(v) \Leftrightarrow \exists h \in H$ tel que $u = h(v)$. Dans notre cas, on a donc un $g \in G$ tel que $x = g_S(y)$ alors $\theta_S(x) = \theta_S \circ g_S \circ \theta_S^1(\theta_S(y))$ et, puisque $\theta_S \circ g_S \circ \theta_S^1 \in H$, on obtient bien que $\sigma_D \circ \theta_S(x) = \sigma_D \circ \theta_S(y)$.

De ces mêmes quotients, on tirait aussi que pour a et b arêtes de C , $\rho_C(a) = \rho_C(b) \Leftrightarrow \exists g \in G$ en sorte que $g_A(a) = b$; pour \tilde{D} on obtient donc que si on a c et d des arêtes de \tilde{D} alors $\sigma_D(c) = \sigma_D(d) \Leftrightarrow \exists h \in H$ en sorte que $h_A(c) = d$. Soit alors a, b deux arêtes de \tilde{C} telles que $\sigma_D(a) = \sigma_D(b)$ on a $g \in G$ en sorte que $a = g_A(b)$ et donc $\theta_A(a) = \theta_A \circ g_A \circ \theta_A^1(\theta_A(b))$ donc $\sigma_D \circ \theta_A(a) = \sigma_D \circ \theta_A(b)$.

On définit alors $\sigma: \text{Sommets}(C) \rightarrow \text{Sommets}(D)$ de la façon suivante: pour chaque sommet u de C , il existe par surjectivité de σ_C un sommet x de \tilde{C} en sorte que $\sigma_C(x) = u$ et on pose $\sigma(u) = \sigma_D \circ \theta_S(x)$. Le sommet $\sigma(u)$ ne dépend alors pas du choix de x par ce que nous venons de montrer. De même, on définit $\rho: \text{Arr}(C) \rightarrow \text{Arr}(D)$: pour chaque arête e de C , il existe v arête de \tilde{C} telle que $\rho_C(v) = e$ (surjection de ρ) alors $\rho(e) = \rho_D \circ \theta_A(v)$ qui ne dépend pas du choix de v par ce que nous venons de montrer.

Montrons alors que (σ, ρ) est bien un revêtement de graphe: il nous faut la surjection, la bijection locale et le morphisme de graphe.

Surjection : Puisque (σ_D, ρ_D) et (θ_S, θ_A) sont surjectives, il suffit de montrer que pour chaque arête ou sommet de \tilde{C} , il existe une arête ou un sommet en sorte que l'image des premiers par (σ_C, ρ_C) soit un élément quelconque de C , ce qui est toujours vrai. Donc (σ, ρ) sont surjectifs.

Morphisme : Soit a une arête de C et prenons une arête v arête de \tilde{C} en sorte que $\rho_C(v) = a$ alors $\alpha_{\tilde{C}}(v)$ est un choix pour définir $\sigma \circ \alpha_C(a)$, et de même $\omega_{\tilde{C}}(v)$ est un choix possible pour définir $\sigma \circ \omega_C(a)$, donc $\sigma \circ \alpha_C(a) = \sigma_D \circ \theta_S \circ \alpha_{\tilde{C}}(v) = \alpha_D \circ \rho(a)$, de même $\sigma \circ \omega_C(a) = \sigma_D \circ \theta_S \circ \omega_{\tilde{C}}(v) = \omega_D \circ \rho(a)$.

Pour vérifier que (σ, ρ) préserve les inverses, on procède de même: $\iota_{\tilde{C}}(v)$ est un choix pour définir $\rho \circ \iota_C(a)$, donc $\rho \circ \iota_C(a) = \rho_D \circ \theta_A \circ \iota_{\tilde{C}} = \iota_D \circ \rho(a)$.

Bijection locale : Soit u un sommet de C alors il existe x sommet de \tilde{C} en sorte que $\sigma_C(x) = u$ on alors une bijection de l'ensemble des arêtes partant de x vers l'ensemble des arêtes partant de u . En prenant l'inverse de cette bijection, puis en la composant avec θ_A puis avec ρ_D restreinte à l'ensemble des arêtes partant de $\theta_S(x)$ on obtient, une bijection de l'ensemble des arêtes partant de u vers l'ensemble des arêtes partant de $\sigma(u)$.

On a donc construit morphisme de graphe de C dans D qui est un revêtement.

☐

Corollaire Soit X un ensemble symétrique (i.e. muni d'une involution ι), alors il existe un graphe composé d'un seul sommet o et ayant X comme ensemble des arêtes. Un tel graphe sera appelé bouquet à base $|X|$.

Ce graphe a un revêtement universel générique de degré $|X|$ et pour n'importe quel graphe C générique de degré $|X|$, on peut trouver un revêtement de C dans le bouquet à base $|X|$.

DEMO Ce graphe *bouquet* est défini comme suit: l'ensemble des sommets ne contient qu'un élément, disons o , l'ensemble des arêtes est X et l'on définit $\varepsilon(x) = (o, o)$, l'inverse ι est déjà défini

dans la donnée de X . La condition de graphe est trivialement vérifiée. On écrira ce graphe $B_X = (\{o\}, X, \varepsilon, \iota)$.

Il est clair que B_X est un graphe générique puisque B_X n'a qu'un seul sommet. Dès lors il admet comme revêtement universel un arbre générique de degré $|X|$ et donc tous les graphes génériques de degré $|X|$ admettent un revêtement universel isomorphe.

Enfin, on remarque que, dans B_X tout chemin est une boucle, par conséquent tout point du revêtement universel est dans le groupe fondamental. Ainsi pour tout graphe générique C de degré $|X|$, l'isomorphisme transportera $\pi_1(C, s)$ dans l'arbre et donc $\pi_1(C, s)$ sera inclu dans le groupe fondamental de B_X . La proposition précédente nous permet alors de dire qu'il y a un revêtement de C dans B_X .

∩

Définition

Un graphe générique de degré $|X|$ muni d'un revêtement (μ_C, ν_C) sur B_X sera dit *catalogué par* (μ_C, ν_C) . De même si C et D sont deux graphes génériques de même degré $|X|$ et si $(\theta_S, \theta_A): C \rightarrow D$, on dira que le morphisme (θ_S, θ_A) est catalogué si $\mu_D \circ \theta_S = \mu_C$ et $\nu_D \circ \theta_A = \nu_C$.

Lemme

Soit X un ensemble symétrique au moyen de l'involution ι_B , soient C et D deux graphes génériques de degré $|X|$, (μ_C, ν_C) un revêtement de C dans B_X et (μ_D, ν_D) un revêtement de D dans B_X . Alors on peut construire un isomorphisme (θ_S, θ_A) entre \tilde{C} et \tilde{D} tel que $\nu_C \circ \rho_C = \nu_D \circ \theta_A$, c'est-à-dire qui soit catalogué (on a utilisé les σ et ρ qui sont les morphismes de revêtements universels).

DEMO Il faut, pour construire cet isomorphisme, se rappeler de la démonstration donnant l'isomorphisme entre les arbres génériques. La preuve définissait E_x comme l'ensemble des arêtes partant du sommet x , elle utilisait une bijection e entre E_s et E_t (t et s sont les points choisis pour construire les revêtements universels) et des bijections $h_x: E_s \rightarrow E_x$ et $k_y: E_t \rightarrow E_y$ pour x sommet de \tilde{C} et y sommet de \tilde{D} .

Remarquons que l'on peut définir ces bijections en utilisant les bijections locales des revêtements: on construit e en composant $(\rho_D|_{E_t})^{-1} \circ (\nu_D|_{E_{\rho_D(t)}})^{-1} \circ (\nu_C|_{E_{\rho_C(s)}}) \circ (\rho_C|_{E_s})$ et l'on construit h_x en composant: $(\rho_C|_{E_s})^{-1} \circ (\nu_C|_{E_{\rho_C(s)}})^{-1} \circ (\nu_D|_{E_{\rho_D(x)}}) \circ (\rho_D|_{E_x})$ enfin l'on obtient k_y en composant: $(\rho_D|_{E_t})^{-1} \circ (\nu_D|_{E_{\rho_D(t)}})^{-1} \circ (\nu_D|_{E_{\rho_D(y)}}) \circ (\rho_D|_{E_y})$. Alors l'image d'une arête a de \tilde{C} était donnée par une composition de h_x de e et de k_y , or ces bijections préservent l'image par les $\nu \circ \rho$. En effet, on voit que $\nu_D \circ \rho_D \circ e = \nu_C \circ \rho_C$, que $\nu_C \circ \rho_C \circ h_x = \nu_C \circ \rho_C$ et que $\nu_D \circ \rho_D \circ k_y = \nu_D \circ \rho_D$. Ainsi l'isomorphisme (θ_S, θ_A) construit au moyen de ces bijections est tel que $\nu_D \circ \rho_D \circ \theta_A = \nu_C \circ \rho_C$.

∩

Lemme

Soit $C = (S, A; \varepsilon, \iota)$ un graphe catalogué par un revêtement (μ_C, ν_C) de C dans un bouquet à base symétrique X , alors C est générique et on a une bijection w_C de l'ensemble des mots sur l'alphabet X vers l'ensemble des chemins dans C partant de s . Cette bijection est caractérisé par: $w_C^{-1}(a_1 \dots a_n) = \nu_C(a_1 \dots a_n)$ qui est, définissons-le, $\nu_C(a_1) \dots \nu_C(a_n)$.

De plus, si D est catalogué (μ_D, ν_D) de D sur B_X et que (λ, τ) est un morphisme de graphe de C dans D en sorte que (λ, τ) est catalogué alors $\tau \circ w_C = w_D$. Une telle application sera appelée une *alphabétisation*.

DEMO En vertu du revêtement, il est clair qu'on a une bijection locale b_r entre l'ensemble X des arêtes qui partent de o et l'ensemble E_r des arêtes qui partent de r , explicitement c'est $(\nu_C|_{E_r})^{-1}$. Ainsi C est générique.

On construit $a_1 \dots a_n$, l'image $(x_1 \dots x_n)$ par w_C , de la façon suivante: on pose $a_1 = b_s(x_1)$ ensuite on pose $\forall i = 2 \dots n$ que $a_i = b_{\omega(a_{i-1})}(x_i)$.

On peut aisément construire l'inverse de w_C : $w'(a_1 \dots a_n) = \nu_C(a_1 \dots a_n) = \nu_C(a_1) \dots \nu_C(a_n)$. Montrons alors que $w_C \circ w'$ est l'identité:

$$w_C \circ w'(a_1 \dots a_n) = w_C(\nu_C(a_1) \dots \nu_C(a_n)) = b_s(\nu_C(a_1)) \dots b_{\omega(a_{i-1})}(\nu_C(a_n)) = a_1 \dots a_n$$

Puisque $b_r = (\nu_C|_{E_r})^{-1}$. De même, $w' \circ w_C$ est l'identité car:

$$w' \circ w_C(x_1 \dots x_n) = w'(b_s(x_1) \dots b_{\omega(a_{n-1})}(x_n)) = \nu_C \circ b_s(x_1) \dots \nu_C \circ b_{\omega(a_{n-1})}(x_n) = x_1 \dots x_n$$

Pour prouver la seconde assertion, considérons $a_1 \dots a_n = b_C(x_1 \dots x_n)$ un chemin de C . Ce que l'on cherche à prouver est $\tau \circ w_C(x_1 \dots x_n) = w_D(x_1 \dots x_n)$ or, en vertu de l'inverse de w_C :

$$\nu_D \circ \tau \circ w_C(x_1 \dots x_n) = \nu_C \circ w_C(x_1 \dots x_n) = x_1 \dots x_n$$

La bijection est valable pour n'importe quel graphe ayant un revêtement sur B_X . ν_D comme application des chemins de D dans les chemins de B_X est l'inverse de w_D et donc on a que:

$$\tau \circ w_C(x_1 \dots x_n) = w_D(x_1 \dots x_n)$$

Ceci étant valable pour n'importe quel mot $x_1 \dots x_n$, on a bien $\tau \circ w_C = w_D$.

□

Corollaire Soit $C(G, X)$ un graphe de Cayley alors $C(G, X)$ est catalogué par $\mu: g \mapsto o$ et $\nu: (g, x) \mapsto x$ sur le bouquet à base X . Alors, pour chaque mot $x_1 \dots x_n$ sur l'alphabet X :

$$\omega \circ w_C(x_1 \dots x_n) = x_1 \dots x_n \in G$$

DEMO Le catalogage est clair. On choisit $s = e$, l'élément neutre de G . Si $x_1 \dots x_n$ est un mot dans l'alphabet X alors

$$w_C(x_1 \dots x_n) = (e, x_1)(e \cdot x_1, x_2) \dots (e \cdot x_1 \dots x_{n-1}, x_n)$$

Et donc $\omega \circ w_C(x_1 \dots x_n) = \omega(e \cdot x_1 \dots x_{n-1}, x_n) = e \cdot x_1 \dots x_n = x_1 \dots x_n$.

□

Lemme Soient C et D deux graphes génériques de même degré $|X|$ catalogués par les revêtements:

$$(\mu_C, \nu_C): C \longrightarrow B_X \quad \text{et} \quad (\mu_D, \nu_D): D \longrightarrow B_X$$

Alors on a un revêtement $(\sigma, \rho): C \longrightarrow D$ si pour chaque mot $x_1 \dots x_n$ tel que $w_C(x_1 \dots x_n)$ est une boucle de C , $w_D(x_1 \dots x_n)$ est une boucle de D .

DEMO On considère $\sigma_C, \rho_C: \tilde{C} \longrightarrow C$ et $\sigma_D, \rho_D: \tilde{D} \longrightarrow D$ les revêtements universels. Il est clair d'abord que $(\mu_C \circ \sigma_C, \nu_C \circ \rho_C)$ et $(\mu_D \circ \sigma_D, \nu_D \circ \rho_D)$ sont des revêtements sur B_X puisque ce sont des produits de revêtements. Donc \tilde{C} et \tilde{D} sont catalogués. De plus $(\nu_C \circ \rho_C) = (\nu_C) \circ (\rho_C)$ donc ρ_C est un morphisme catalogué, de même ρ_D est catalogué. On sait, par le lemme suivant la définition de catalogué que, puisque les revêtements universels sont catalogués et qu'ils sont générique de degré $|X|$, l'on peut trouver (θ_S, θ_A) un isomorphisme catalogué de \tilde{C} dans \tilde{D} . On a déjà remarqué que dans un revêtement universel $[a_1 \dots a_n] = \omega([\emptyset], a_1) \dots ([a_1 \dots a_{n-1}], a_n)$. Ainsi, pour tout $x_1 \dots x_n$ tel que $w_C(x_1 \dots x_n)$ est une boucle:

$$\omega_{\tilde{C}} \circ w_{\tilde{C}}(x_1 \dots x_n) = [w_C(x_1 \dots x_n)]$$

Soit $w_C(x_1 \dots x_n)$ une boucle de C . Alors $\rho_C \circ w_{\tilde{C}}(x_1 \dots x_n) = w_C(x_1 \dots x_n)$ et, par la remarque précédente, on a que $\omega_{\tilde{C}} \circ w_{\tilde{C}}(x_1 \dots x_n) = [w_C(x_1 \dots x_n)] \in \pi_1(C, s)$. De plus $w_{\tilde{C}}(x_1 \dots x_n)$ peut atteindre n'importe quelle boucle en s . Donc: $x_1 \dots x_n \mapsto \omega_{\tilde{C}} \circ w_{\tilde{C}}(x_1 \dots x_n)$ est surjective sur les éléments du $\pi_1(C, s)$

De par le catalogage, on a que $\theta_A \circ w_{\tilde{C}}(x_1 \dots x_n) = w_{\tilde{D}}(x_1 \dots x_n)$ puis, on a pour la même raison, $\rho_D \circ w_{\tilde{D}}(x_1 \dots x_n) = w_D(x_1 \dots x_n)$.

L'hypothèse dit donc que $w_D(x_1 \dots x_n)$ est une boucle. Or $\omega_D \circ w_{\tilde{D}}(x_1 \dots x_n) = [w_D(x_1 \dots x_n)]$ est donc inclu dans le $\pi_1(D, t)$. On a que pour chaque élément $\omega_{\tilde{C}} \circ w_{\tilde{C}}(x_1 \dots x_n)$ du $\pi_1(C, s)$:

$$\theta_S \circ \omega_{\tilde{C}} \circ w_{\tilde{C}}(x_1 \dots x_n) = \omega_{\tilde{D}} \circ \theta_A \circ w_{\tilde{C}}(x_1 \dots x_n) = \omega_{\tilde{D}} \circ w_{\tilde{D}}(x_1 \dots x_n) = [w_D(x_1 \dots x_n)] \in \pi_1(D, t)$$

On vient donc de montrer que si les hypothèses sont vérifiées, on a $\theta_S(\pi_1(C, s)) \subset \theta_1(D, t)$, la proposition de base nous permet alors de dire qu'il y a un revêtement de C dans D .

☐

Corollaire Soit C et D deux graphes génériques de même degré $|X|$ catalogués par les revêtements :

$$(\mu_C, \nu_C): C \longrightarrow B_X \quad \text{et} \quad (\mu_D, \nu_D): D \longrightarrow B_X$$

Et appelons $T_M = (S_M, A_M, \varepsilon|_{A_M}, \iota|_{A_M})$ l'arbre maximal. On définit pour chaque arête a , $\varphi(a)$ comme l'unique chemin réduit de l'arbre maximal allant de s à $\alpha(a)$ et $\varphi'(a)$ comme l'unique chemin réduit de l'arbre maximal allant de s à $\omega(a)$.

Alors on a un revêtement $(\sigma, \rho): C \longrightarrow D$ si pour chaque $a \in A$ on a que $x_1 \dots x_n = \nu_C \circ \chi(a) = \nu_C(\varphi(a) \circ a \circ \varphi'(a))$ est tel que $w_D(x_1 \dots x_n)$ est une boucle de D .

DEMO Ce résultat est évident dans la mesure puisque le $\pi_1(C, s)$ est engendré par les $[\varphi(a) \circ a \circ \varphi'(a)]$ pour $a \in A \dot{-} M$ et puisque $\theta_S|_{\pi_1(C, s)}$ est un morphisme de groupe.

☐

Corollaire Prenons $C(G, X)$ un graphe de Cayley et soit $D = (S, A, (\alpha, \omega), \iota)$ un graphe générique de degré $|X|$ catalogué par $(\mu_C, \nu_C): D \longrightarrow B_X$, soit enfin $T_M = (S_M, A_M, (\alpha, \omega)|_{A_M}, \iota|_{A_M})$ un arbre maximal dans D alors on a un revêtement de D sur $C(G, X)$ si pour toute arête, $a \in A \dot{-} A_M$ le mot $x_1 \dots x_n = w_C^{\iota}(\chi(a))$ est tel que $x_1 \dots x_n = e$, l'élément neutre dans G .

De plus si $a \in A \dot{-} A_M$ satisfait cette condition alors l'arête $\iota(a)$ la satisfait aussi.

DEMO En effet, on a montré que, dans un tel cas, $\omega_C \circ w_C(x_1 \dots x_n) = x_1 \dots x_n \in G$ ainsi $w_C(x_1 \dots x_n)$ est une boucle de $C = C(G, X)$ si et seulement si $x_1 \dots x_n = e$.

Dès lors, si pour chaque $a \in A \dot{-} A_M$ le mot $x_1 \dots x_n = w_C^{\iota} \circ \chi(a)$ est tel que $x_1 \dots x_n = e$ on a donc que $w_D(x_1 \dots x_n)$ est une boucle. Le corollaire précédent nous permet alors de dire qu'on a un revêtement de D dans $C(G, X)$.

La seconde assertion est très simple à vérifier :

$$\chi(\iota(a)) = \varphi \circ \iota(a) \circ \overline{\iota(a)} \circ \varphi' \circ \iota(a) = \iota(\varphi'(a)) \circ \overline{\iota(a)} \circ \iota(\varphi(a)) = \iota(\chi(a))$$

Ainsi donc le mot $x_1 \dots x_n = w_C^{\iota} \circ \chi(\iota(a))$ est le mot $x_n^{\iota} \dots x_1^{\iota}$ et donc, dans G il donne $(x_1 \dots x_n)^{\iota}$ qui si $x_1 \dots x_n$ vaut l'élément neutre, sera aussi l'élément neutre.

☐

Nous allons ici énoncer la démarche empirique sur laquelle se baseront les applications. Pour ce, nous sommes contraints, d'admettre un rapport entre les dessins et les mathématiques.

- (i) On admettra que l'on s'est donné un graphe en dessinant les sommets et les traits les reliant. Qu'alors l'ensemble des sommets se voit, que l'ensemble des arêtes est l'ensemble des traits dessinés pris les deux sens chacun, que les applications α et ω se voient à partir d'un trait et d'un sens choisi, enfin que l'inverse envoie un trait dans un sens sur un trait dans l'autre sens.
- (ii) Associons à chaque trait un nom et (éventuellement) une orientation en sorte que deux traits portant le même nom sont tous deux orientés ou ne le sont pas les deux. On peut alors étendre la nomination aux arêtes : pour les traits qui sont orientés, on donne le nom muni du signe $^{\pm}$, pour les traits qui ne sont pas orientés on donne le même nom pour les deux sens. Alors, si, pour l'ensemble des arêtes qui partent d'un sommet, tous les noms sont utilisés (y compris les inverses qui existent) et une seule fois chacun on admettra qu'on a un catalogage sur le bouquet dont la base est l'ensemble des noms et l'application inverse apporte un nom $^{\pm}$ sur le nom, un nom sur le nom $^{\pm}$ s'ils sont orientés, et fixe un nom non-orienté.
- (iii) Si, maintenant on appelle $D = (S, A, \varepsilon, \iota)$ le graphe construit par le dessin, $C = C(G, X)$ le graphe de Cayley d'un groupe, si, enfin, D est catalogué sur le bouquet à base X . On peut dessiner un arbre maximal (i.e. un arbre dans D dont les sommets sont tous les sommets de D). On choisit un point $s \in D$. L'application w_D^{\pm} sera donnée de manière évidente : à un chemin $\chi(a)$ on associe la suite des noms des arêtes. On utilise alors le dernier corollaire : si le mot construit pour chaque chemin $\chi(a)$ $a \in A^{\pm} A_M$ donne, dans le groupe G , l'élément neutre (donc $\chi(\iota(a))$ le donne aussi) alors on a un revêtement de D dans $C(G, X)$.
- (iv) Si on a un revêtement $(\theta_S, \theta_A) : C = (S, A, (\alpha, \omega), \iota) \longrightarrow D = (T, B, (\beta, \zeta), \kappa)$ tel que θ_S est une bijection alors θ_A est bijective : en effet, on peut partitionner A et B en $(E_s)_{s \in S}$ et $(E_t)_{t \in T}$; puisque revêtement, θ_A est une bijection de E_s dans $E_{\theta_S(s)}$ et, puisque θ_S est bijective et puisque morphisme θ_A envoie bijectivement les E_s sur les E_t , donc θ_A est bijective. On a donc un isomorphisme de graphe.

Ce chapitre est sans doute profondément aride, mais les séries de jolis exemples viennent à point maintenant. Le prochain chapitre va utiliser cette démarche pour obtenir "à la main" les présentations de trois groupes.

Le cas de $\mathrm{PSL}_2(\mathbb{F}_7)$

Rappelons que \mathbb{F}_7 est le corps à 7 éléments, i.e. le quotient $\mathbb{Z}/7\mathbb{Z}$.

Ce chapitre va appliquer les généralités du chapitre précédent afin d'obtenir une bonne description de $\mathrm{PSL}_2(\mathbb{F}_7)$. On cherche, en particulier, une présentation de ce groupe, un graphe de Cayley (qui nous donnera une idée de la surface que l'on cherche) et d'autres particularités qui nous permettront de passer plus aisément à la géométrie.

On commence par vérifier que $\mathrm{PSL}_2(\mathbb{F}_7)$ est simple, ainsi il sera impossible de classifier les éléments du groupe au moyen d'un morphisme surjectif. On s'appuyera donc uniquement sur la combinatoire pour l'observer de plus près.

Vérification Le groupe $\mathcal{H}(\widehat{\mathbb{F}}_7) \approx \mathrm{PSL}_2(\mathbb{F}_7)$ admet 21 similitudes et donc 168 éléments. Il est engendré par $\tau = \omega \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\iota = \omega \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et ces générateurs satisfont en tous cas aux relations :

$$\tau^7 = 1 \quad \iota^2 = 1 \quad (\tau\iota)^3 = 1$$

De plus, le corps \mathbb{F}_7 n'est pas de caractéristique 2 et a suffisamment de carrés donc $\mathcal{H}(\widehat{\mathbb{F}}_7) \approx \mathrm{PSL}_2(\mathbb{F}_7)$ est un groupe simple.

DEMO Remarquons d'abord que $\mathbb{F}_7^2 = \{0, 1, 2, 4\}$ et donc que $\mathbb{F}_7^{2*} = \{1, 2, 4\}$. Appliquons alors le corollaire de l'équivalence des similitudes qui énumère les similitudes, il nous donne une bijection :

$$\begin{aligned} \varepsilon: \mathbb{F}_7 \times \mathbb{F}_7^{2*} &\longrightarrow \mathcal{H}_\infty(\widehat{\mathbb{F}}_7) \\ (p, k) &\longmapsto \tau_p \circ \eta_k \end{aligned}$$

Il y a donc bien $\mathrm{Card}(\mathbb{F}_7) \cdot \mathrm{Card}(\mathbb{F}_7^{2*}) = 7 \cdot 3 = 21$ similitudes dans $\mathcal{H}(\widehat{\mathbb{F}}_7)$. Mais l'action de $\mathcal{H}(\widehat{\mathbb{F}}_7)$ sur $\widehat{\mathbb{F}}_7$ est transitive, un petit théorème de théorie des groupes nous dit donc que :

$$\mathrm{Card}(\mathcal{H}(\widehat{\mathbb{F}}_7)) = \mathrm{Card}(\mathrm{Stab}(\infty)) \cdot \mathrm{Card}(\mathrm{Orbite}(\infty)) \stackrel{\text{transitivité}}{=} \mathrm{Card}(\mathcal{H}_\infty(\widehat{\mathbb{F}}_7)) \cdot \mathrm{Card}(\mathbb{F}_7) = 21 \cdot 8 = 168$$

D'après la proposition *Engendré encore*, on sait que $\mathrm{PSL}_2(\mathbb{F}_7) = \mathcal{H}(\widehat{\mathbb{F}}_7)$ est engendré par $\tau = \omega \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\iota = \omega \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Enfin les relations sont vérifiées grâce à cette même proposition et grâce aux isomorphismes $\langle \iota \rangle \approx \mathbb{F}_2$ et $\langle \tau \rangle \approx \mathbb{F}_7$.

Enfin, le corps \mathbb{F}_7 n'est pas de caractéristique 2 puisque 2 n'est pas congru à 0 modulo 7. On a vu que $\mathbb{F}_7^{2*} = \{1, 2, 4\}$ or $2 \cdot 2 = 4 \neq 1$ donc 2 est un élément d'ordre > 2 dans le groupe $(\mathbb{F}_7^{2*}, \cdot)$, on conclut donc que \mathbb{F}_7 a suffisamment de carrés. Le théorème final nous dit donc que $\mathcal{H}(\widehat{\mathbb{F}}_7) \approx \mathrm{PSL}_2(\mathbb{F}_7)$ est un groupe simple.

□

Corollaire Sachant que $\mathcal{H}(\widehat{\mathbb{F}}_7)$ est engendré par τ et ι on a déjà un morphisme surjectif du groupe libre $\langle \tau, \iota \rangle$ sur $\mathcal{H}(\widehat{\mathbb{F}}_7)$. Sachant, de plus, que les relations $\tau^7 = \iota^2 = (\tau\iota)^3$ sont vérifiées, ce morphisme va passer au quotient pour donner un morphisme (surjectif toujours) :

$$\langle \tau, \iota \mid \tau^7 = \iota^2 = (\tau\iota)^3 = 1 \rangle \longrightarrow \mathcal{H}(\widehat{\mathbb{F}}_7) \approx \mathrm{PSL}_2(\mathbb{F}_7)$$

CLAIR

Nous allons maintenant nous intéresser à un sous-groupe de $\mathrm{PSL}_2(\mathbb{F}_7)$ qui est bien connu. Celui-ci va nous permettre d'acquérir la dernière relation nécessaire. Commençons par le décrire, ensuite, nous verrons comment l'injecter.

Lemme (i) Le groupe des permutations sur 4 éléments, dénommé S_4 possède 24 éléments. Si l'on pose $\alpha = (123)$ et $\beta = (24)$, ces deux éléments engendrent S_4 et celui-ci admet la présentation :

$$S_4 \approx U = \langle \alpha, \beta \mid \alpha^3 = \beta^2 = (\beta\alpha)^4 = 1 \rangle$$

(ii) Le groupe des permutations paires sur 4 éléments est un sous-groupe d'indice 2 de S_4 , il contient exactement 12 éléments. De plus, si l'on pose $\gamma = \beta\alpha\beta\alpha = (12)(34)$, ce groupe admet la présentation : $A_4 \approx V = \langle \alpha, \gamma \mid \gamma^2 = \alpha^3 = (\alpha\gamma)^3 = 1 \rangle$

DEMO Que le groupe S_4 possède 24 éléments est chose fort bien connue ($4! = 24$). La génération de S_4 par ces deux éléments se prouve à la main. Je donne ici l'expression en α et β de chacun des 24 éléments de S_4 :

$\begin{smallmatrix} 1234 \\ 1234 \end{smallmatrix} = () = \alpha\alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 1243 \end{smallmatrix} = (43) = \alpha\beta\alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 1324 \end{smallmatrix} = (23) = \beta\alpha\beta\alpha^{-1}\beta$
$\begin{smallmatrix} 1234 \\ 1342 \end{smallmatrix} = (234) = \alpha\beta\alpha^{-1}\beta$	$\begin{smallmatrix} 1234 \\ 1423 \end{smallmatrix} = (432) = \beta\alpha\beta\alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 1432 \end{smallmatrix} = (24) = \beta$
$\begin{smallmatrix} 1234 \\ 2134 \end{smallmatrix} = (12) = \beta\alpha^{-1}\beta\alpha\beta$	$\begin{smallmatrix} 1234 \\ 2143 \end{smallmatrix} = (12)(34) = \alpha^{-1}\beta\alpha^{-1}\beta$	$\begin{smallmatrix} 1234 \\ 2314 \end{smallmatrix} = (123) = \alpha$
$\begin{smallmatrix} 1234 \\ 2341 \end{smallmatrix} = (1234) = \alpha^{-1}\beta\alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 2413 \end{smallmatrix} = (1243) = \alpha\beta$	$\begin{smallmatrix} 1234 \\ 2431 \end{smallmatrix} = (124) = \beta\alpha^{-1}\beta\alpha$
$\begin{smallmatrix} 1234 \\ 3124 \end{smallmatrix} = (132) = \alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 3142 \end{smallmatrix} = (1342) = \beta\alpha^{-1}$	$\begin{smallmatrix} 1234 \\ 3214 \end{smallmatrix} = (13) = \alpha\beta\alpha^{-1}\beta\alpha\beta$
$\begin{smallmatrix} 1234 \\ 3241 \end{smallmatrix} = (134) = \beta\alpha^{-1}\beta$	$\begin{smallmatrix} 1234 \\ 3412 \end{smallmatrix} = (13)(24) = \alpha\beta\alpha^{-1}\beta\alpha$	$\begin{smallmatrix} 1234 \\ 3421 \end{smallmatrix} = (1324) = \alpha^{-1}\beta$
$\begin{smallmatrix} 1234 \\ 4123 \end{smallmatrix} = (1432) = \alpha\beta\alpha$	$\begin{smallmatrix} 1234 \\ 4132 \end{smallmatrix} = (142) = \alpha^{-1}\beta\alpha\beta$	$\begin{smallmatrix} 1234 \\ 4213 \end{smallmatrix} = (143) = \beta\alpha\beta$
$\begin{smallmatrix} 1234 \\ 4231 \end{smallmatrix} = (14) = \alpha^{-1}\beta\alpha$	$\begin{smallmatrix} 1234 \\ 4312 \end{smallmatrix} = (1423) = \beta\alpha$	$\begin{smallmatrix} 1234 \\ 4321 \end{smallmatrix} = (14)(23) = \alpha\beta\alpha\beta$

Les relations données dans la présentation viennent directement :

$$\alpha = \begin{smallmatrix} 1234 \\ 2314 \end{smallmatrix} = (123)$$

est un cycle de longueur 3 donc α^3 est l'identité, de même

$$\beta = \begin{smallmatrix} 1234 \\ 1432 \end{smallmatrix} = (24)$$

est un cycle de longueur 2 donc β^2 est l'identité, enfin

$$\beta\alpha = \begin{smallmatrix} 1234 \\ 4312 \end{smallmatrix} = (1423)$$

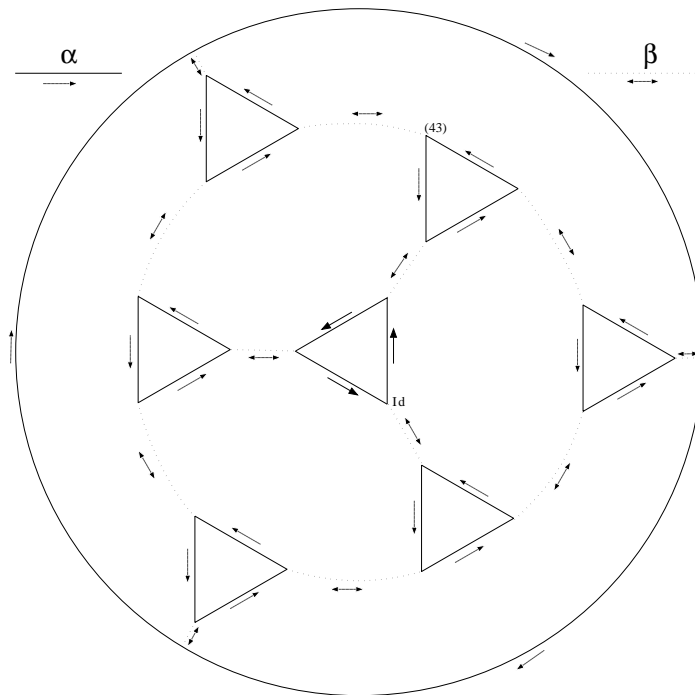
est un cycle de longueur 4 et donc $(\beta\alpha)^4$ est l'identité.

Ces relations sont donc vraies. On a donc un morphisme surjectif du groupe abstrait U donné par la présentation sur S_4 .

Pour vérifier que ce morphisme est un isomorphisme, il faut tracer ce qu'on suppose être le graphe de Cayley (ci-contre), en annexe on montre que l'on a un revêtement de ce graphe dessiné (nous l'appellerons D) dans le graphe de Cayley $C(U, \{\alpha, \alpha^{-1}, \beta\})$ de H .

On a donc une surjection de $\text{Sommets}(D) \twoheadrightarrow U$. En comptant à la main, on obtient que D a 24 sommets. En résumé :

$$\begin{aligned} \text{Sommets}(D) &\twoheadrightarrow U \twoheadrightarrow S_4 \\ 24 = \text{Card}(\text{Sommets}(D)) &\geq \text{Card}(U) \geq \text{Card}(S_4) = 24 \end{aligned}$$



De l'égalité ci-dessous, on doit conclure que ces deux surjections sont des bijections. Ainsi le revêtement est un isomorphisme de graphe et S_4 est isomorphe à H . On a donc obtenu une présentation de S_4 en même temps que son graphe de Cayley.

Remarquons que, puisque β est d'ordre 2, $(\beta\alpha)^4 = 1 \Leftrightarrow \beta(\alpha\beta)^3\alpha = 1 \Leftrightarrow (\alpha\beta)^3\alpha\beta^{-1} = (\alpha\beta)^4 = 1$, ainsi la présentation classique de S_4 est équivalente à celle que nous avons donnée.

Le groupe alterné A_4 est le noyau du morphisme de signature sur les éléments de S_4 , c'est-à-dire l'ensemble des permutations qui s'expriment comme un produit d'un nombre pair de transpositions. Il s'agit donc d'un sous-groupe d'indice 2, il contient donc exactement 12 éléments. Tout d'abord, il est clair que les deux permutations suivantes sont paires, puisqu'elles sont produits de deux transpositions :

$$\alpha = (123) = (31)(21) \quad \gamma = \beta\alpha\beta\alpha = (12)(34)$$

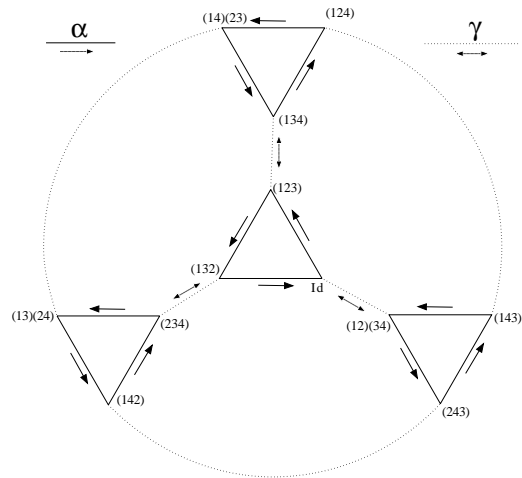
Pour montrer qu'elles engendrent A_4 donnons, comme précédemment, l'expression de chaque permutation paire en termes de ces générateurs :

$$\begin{array}{llll} \begin{array}{l} 1234 \\ 1234 \end{array} = () = \alpha\alpha^{-1} & = () & \begin{array}{l} 1234 \\ 1342 \end{array} = (24)(23) = \alpha^{-1}\gamma & = (234) \\ \begin{array}{l} 1234 \\ 1423 \end{array} = (42)(43) = \gamma\alpha & = (243) & \begin{array}{l} 1234 \\ 2143 \end{array} = (12)(34) = \gamma & = (12)(34) \\ \begin{array}{l} 1234 \\ 2314 \end{array} = (13)(12) = \alpha & = (123) & \begin{array}{l} 1234 \\ 2431 \end{array} = (14)(12) = \gamma\alpha^{-1}\gamma & = (124) \\ \begin{array}{l} 1234 \\ 3124 \end{array} = (12)(13) = \alpha^{-1} & = (132) & \begin{array}{l} 1234 \\ 3241 \end{array} = (14)(13) = \alpha\gamma & = (134) \\ \begin{array}{l} 1234 \\ 3412 \end{array} = (13)(24) = \gamma\alpha\gamma\alpha^{-1} & = (13)(24) & \begin{array}{l} 1234 \\ 4132 \end{array} = (12)(14) = \gamma\alpha\gamma & = (142) \\ \begin{array}{l} 1234 \\ 4213 \end{array} = (13)(14) = \gamma\alpha^{-1} & = (143) & \begin{array}{l} 1234 \\ 4321 \end{array} = (14)(23) = \alpha\gamma\alpha^{-1} & = (14)(23) \end{array}$$

La première relation énoncée a été montrée auparavant, la seconde : vient directement de la première partie de ce lemme :

$$(\beta\alpha\beta\alpha)^2 = (\beta\alpha\beta\alpha)(\beta\alpha\beta\alpha) = (\beta\alpha)^4 = 1$$

Reste à montrer que ce sont bien là toutes les relations. On procède de même qu'avant en traçant E le graphe que l'on suppose être le graphe de Cayley du groupe V donné par la présentation. On montre en annexe que ce graphe admet un revêtement au dessus de $C(V, \{\alpha, \alpha^{-1}, \beta\})$. Ce graphe contient 12 sommets. Donc, il y a maximum 12 sommets dans le groupe donné par la présentation. Puisque celui-ci se surjecte dans A_4 (deux générateurs et relations vérifiées pour eux), il contient exactement 12 éléments et il est isomorphe à A_4 , de plus le revêtement du graphe E est un isomorphisme ce qui nous prouve que le graphe que l'on a dessiné est bien le graphe de Cayley de A_4 .



□

Morphisme premier $\mathcal{H}(\widehat{\mathbb{F}}_7)$ contient une image de A_4 .

DEMO Étant donné que la présentation de A_4 est $A_4 \approx \langle \alpha, \gamma \mid \gamma^2 = \alpha^3 = (\alpha\gamma)^3 = 1 \rangle$, la tactique pour obtenir une image de A_4 est d'arriver à trouver deux éléments de $\mathcal{H}(\widehat{\mathbb{F}}_7)$ qui satisfassent à ces relations. On aura alors forcément un morphisme. En se rappelant le lemme de commutation du chapitre précédent, on trouve que deux bonnes images de α et γ seraient $\tau \circ \eta_{\frac{1}{4}}$ et $\eta_4 \circ \iota$. Les relations $\gamma^2 = \alpha^3 = (\alpha\gamma)^3 = 1$ sont alors vérifiées grâce à ce lemme :

$$\begin{aligned}
\gamma^2 &= \eta_4 \circ \iota \circ \eta_4 \circ \iota \stackrel{\text{commutation}}{=} \eta_4 \circ \eta_{\frac{1}{4}} \circ \iota \circ \iota \stackrel{\text{isomorphismes}}{=} 1 \\
(\alpha\gamma)^3 &= (\eta_4 \circ \iota \circ \tau \circ \eta_{\frac{1}{4}})^3 = \eta_4 \circ (\iota \circ \tau)^3 \circ \eta_{\frac{1}{4}} \stackrel{\text{engendré encore}}{=} \eta_4 \circ \eta_{\frac{1}{4}} \stackrel{\text{isomorphismes}}{=} 1 \\
\alpha^3 &= \tau \circ \eta_{\frac{1}{4}} \circ \tau \circ \eta_{\frac{1}{4}} \circ \tau \circ \eta_{\frac{1}{4}} \stackrel{\text{commutation}}{=} \tau_{1+2} \circ \eta_{\frac{1}{2}} \circ \tau \circ \eta_{\frac{1}{2}} = \tau_{3+\frac{1}{2}} \circ \eta_{\frac{1}{4}} \stackrel{\text{idem}}{=} \tau_{3+4} \circ \eta_1 = 1
\end{aligned}$$

Les trois relations sont vraies, on a donc un morphisme surjectif :

$$\begin{aligned}
\mu: A_4 &\longrightarrow \langle \tau \circ \eta_{\frac{1}{4}}, \eta_4 \circ \iota \rangle \subset \mathcal{H}(\widehat{\mathbb{F}}_7) \\
\alpha &\longmapsto \tau \circ \eta_{\frac{1}{4}} \\
\gamma &\longmapsto \eta_4 \circ \iota
\end{aligned}$$

□

Morphisme second Le morphisme μ énoncé s'étend à tout S_4 .

DEMO Sachant que dans S_4 , A_4 est engendré par α et $\beta\alpha\beta\alpha$, la stratégie consiste à trouver β étant donné α et $\beta\alpha\beta\alpha$, en fait, il suffirait de trouver une "racine carrée" de $\beta\alpha\beta\alpha$ qu'il suffira de multiplier à droite par α^{-1} pour obtenir β .

On a que 2 est l'élément de \mathbb{F}_7 dont le carré est 4, exprimons en détails le générateur γ : $\mu(\gamma) = \mu(\beta\alpha\beta\alpha) = \eta_4 \circ \iota = \tau_{-2} \circ \iota \circ \tau_{-\frac{1}{2}} \circ \iota \circ \tau_{-2} \circ (\iota \circ \iota)$. Or $-\frac{1}{2} = -4 = (-2) + (-2)$ et $-2 = 5$, alors $\mu(\gamma) = \tau_5 \circ \iota \circ \tau_5 \circ \tau_5 \circ \iota \circ \tau_5 = (\tau_5 \circ \iota \circ \tau_5)^2$ qui serait $\mu(\beta\alpha)^2$. On aurait alors $\mu(\beta\alpha) = \tau_5 \circ \iota \circ \tau_5$, ainsi le bon candidat pour notre $\mu(\beta)$ devrait être $\mu(\beta\alpha\alpha^{-1}) = \mu(\beta\alpha) \circ \mu(\alpha)^{-1} = \tau_5 \circ \iota \circ \tau \circ \eta_4$. Acceptons-le. Pour que ce soit un bon, on vérifie alors que les deux relateurs énoncés vérifient les relations de S_4 : l'égalité $\mu(\alpha)^3 = 1$ a déjà été vue plus haut; l'égalité $\mu(\beta\alpha)^4 = 1$ vient de $\mu(\beta\alpha)^4 = \mu(\beta\alpha\beta\alpha)^2 = 1$ comme on l'a montré précédemment. Il reste à vérifier que le candidat $\mu(\beta)$ est bien d'ordre 2:

$$\begin{aligned}
\mu(\beta)^2 &= (\tau_5 \circ \iota \circ \tau \circ \eta_4) \circ (\tau_5 \circ \iota \circ \tau \circ \eta_4) \stackrel{\text{commutation}}{=} \tau_5 \circ \iota \circ \eta_4 \circ \iota \circ \tau \circ \eta_4 \\
&\stackrel{\text{idem}}{=} \tau_5 \circ \iota \circ \iota \circ \tau_{\frac{1}{4}} \circ \eta_{\frac{1}{4}} \circ \eta_4 \stackrel{\text{isomorphismes}}{=} \tau_5 \circ \tau_2 \stackrel{\text{idem}}{=} 1
\end{aligned}$$

On vient donc de montrer que l'on peut appliquer les générateurs α et β de S_4 sur des éléments $\mu(\alpha)$ et $\mu(\beta)$ qui satisfont aux mêmes relations que α et β , on a donc étendu μ en un morphisme surjectif:

$$\mu: S_4 \approx \langle \alpha, \beta \mid \alpha^3 = \beta^2 = (\beta\alpha)^4 = 1 \rangle \longrightarrow \langle \tau \circ \eta_2, \tau_5 \circ \iota \circ \tau \circ \eta_4 \rangle \subset \mathcal{H}(\widehat{\mathbb{F}}_7)$$

□

Corollaire On peut trouver des éléments d'ordre 4 dans $\mathcal{H}(\widehat{\mathbb{F}}_7)$, un sympathique exemple est $\tau^3\iota$.

DEMO Par le fait que le μ est un homomorphisme de S_4 dans $\mathcal{H}(\widehat{\mathbb{F}}_7)$, on peut dire que les images des éléments d'ordre 4 dans S_4 seront, dans $\mathcal{H}(\widehat{\mathbb{F}}_7)$ à la puissance 4, des éléments triviaux. Typiquement, on a que $\mu((1423)) = \mu(\beta\alpha) = \tau_5 \circ \iota \circ \tau_5$ est d'ordre 4. C'est-à-dire que :

$$\begin{aligned}
1 &= (\tau_5 \circ \iota \circ \tau_5)^4 = (\tau_5 \circ \iota \circ \tau_5) \circ (\tau_5 \circ \iota \circ \tau_5) \circ (\tau_5 \circ \iota \circ \tau_5) \circ (\tau_5 \circ \iota \circ \tau_5) \\
&= \tau_2 \circ (\tau_3 \circ \iota) \circ (\tau_3 \circ \iota) \circ (\tau_3 \circ \iota) \circ (\tau_3 \circ \iota) \circ \tau_5 = \tau_2 \circ (\tau_3 \circ \iota)^4 \circ \tau_5
\end{aligned}$$

Dès lors, on peut dire que : $(\tau^3 \circ \iota)^4 \stackrel{\text{isomorphismes}}{=} (\tau_3 \circ \iota)^4 = \tau_2^{-1} \circ \tau_5^{-1} \stackrel{\text{isomorphismes}}{=} \tau_5 \circ \tau_2 \stackrel{\text{idem}}{=} 1$

On vient donc de trouver un élément d'ordre 4 de $\mathcal{H}(\widehat{\mathbb{F}}_7)$ un peu plus simple que ceux de $\mu(S_4)$.

□

Théorème Le groupe $\mathrm{PSL}_2(\mathbb{F}_7) \approx \mathcal{H}(\widehat{\mathbb{F}}_7)$ admet la présentation :

$$H = \langle \tau, \iota \mid \tau^7 = (\tau \circ \iota)^3 = \iota^2 = (\tau^3 \circ \iota)^4 = 1 \rangle$$

DEMO Nous savons depuis le début du chapitre que les trois premières relations sont vérifiées, la quatrième vient d'être vérifiée. On a donc un morphisme surjectif du groupe H donné par la présentation sur $\mathcal{H}(\widehat{\mathbb{F}}_7) \approx \mathrm{PSL}_2(\mathbb{F}_7)$.

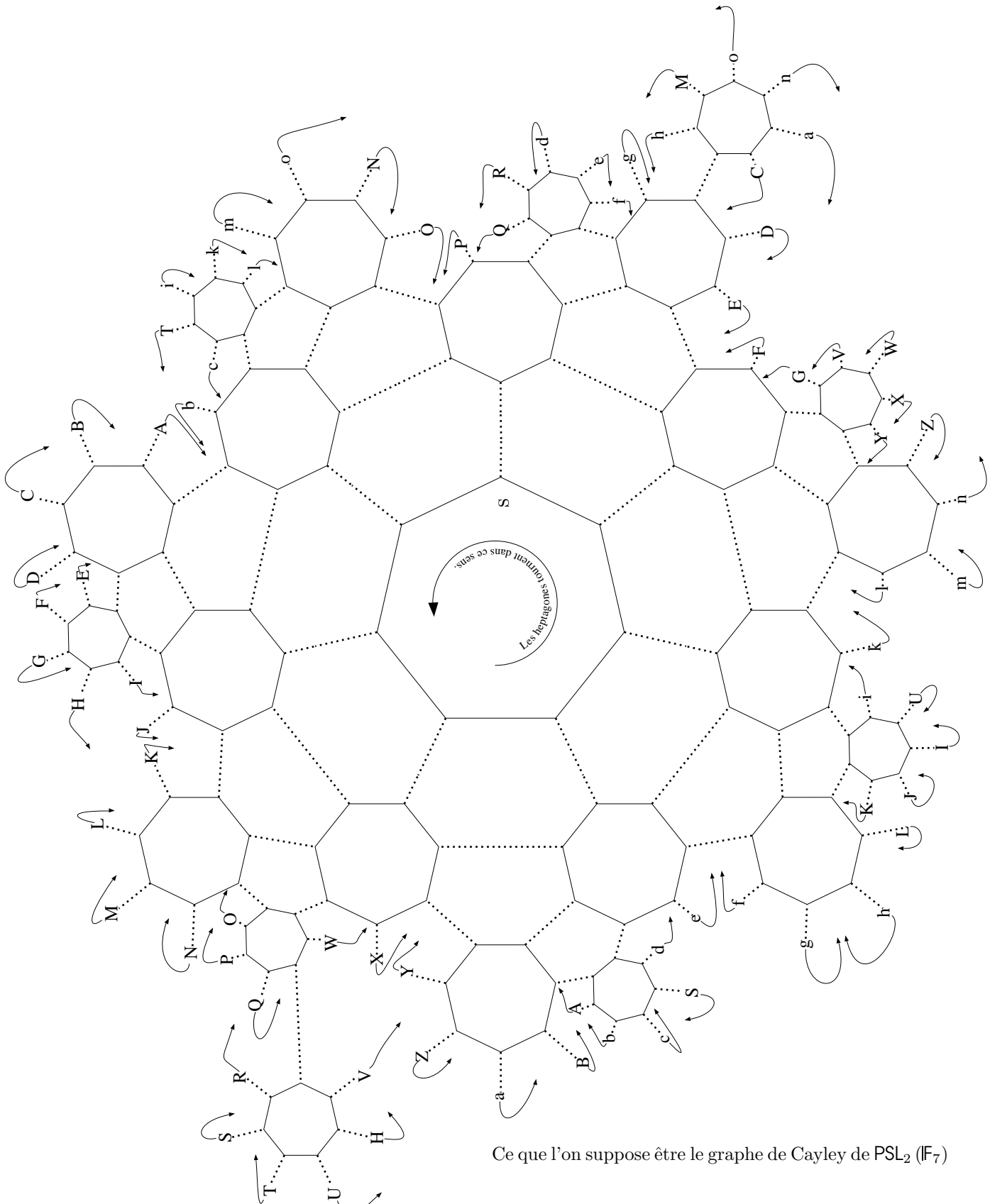
Comme pour chaque groupe, on trace ce que l'on croit être le graphe de Cayley de cette présentation (ci-dessous) et l'on compte 168 sommets sur le graphe.

Au début de ce chapitre, on a montré qu'il y avait bien 168 éléments dans $\mathrm{PSL}_2(\mathbb{F}_7)$. En annexe on vérifie que l'on a un revêtement de F , le graphe dessiné, dans $C(H, \{\tau, \tau^{-1}, \iota\})$. On a donc l'inégalité classique entre le graphe, la présentation et le groupe :

$$\begin{aligned} \text{Sommets}(F) &\longrightarrow H \longrightarrow \mathcal{H}(\widehat{\mathbb{F}}_7) \\ 168 = \text{Card}(\text{Sommets}(F)) &\geq \text{Card}(H) \geq \text{Card}(\mathcal{H}(\widehat{\mathbb{F}}_7)) = 168 \end{aligned}$$

Le morphisme surjectif ne peut donc être qu'un isomorphisme et la conclusion est vraie. De plus le graphe dessiné est bien le graphe de Cayley de $\mathcal{H}(\widehat{\mathbb{F}}_7)$.

☐



Ce que l'on suppose être le graphe de Cayley de $PSL_2(\mathbb{F}_7)$

Isométries d'un quotient

Le but de ce chapitre est de décrire les isométries d'un quotient d'un espace modulo une action proprement discontinue et libre. On s'appuyera, pour cela, sur la théorie des revêtements.

Dans tout le chapitre E est une variété connexe, Γ est un groupe de difféomorphismes agissant librement et proprement discontinûment sur E . Alors on sait que $B = E/\Gamma$ peut être munie d'une unique structure de variété en sorte que la projection de quotient π est un revêtement et un difféomorphisme local. Dans ce cas le groupe Γ est le groupe des transformations de revêtement dont les éléments ont la propriété caractéristique suivante: $\pi \circ \gamma = \pi$.

Si E est munie d'une métrique riemannienne et si Γ est un groupe d'isométries, alors B peut être munie d'une unique métrique riemannienne en sorte que π soit une isométrie locale.

Définition

J'appellerai normalisateur de Γ , et je noterai \mathcal{N} l'ensemble des difféomorphismes I de E en sorte que $I \circ \Gamma = \Gamma \circ I$. Ce qui revient à dire que $I \in \mathcal{N}$ si et seulement si:

$$\forall G \in \Gamma \exists H \in \Gamma \text{ tel que } G \circ I = I \circ H \text{ et } \forall H \in \Gamma \exists G \in \Gamma \text{ tel que } I \circ H = G \circ I$$

Lemme 1 Si I et J sont deux difféomorphismes de E dans E tels que $\pi \circ I = \pi \circ J$ alors il existe $G \in \Gamma$ tel que $I = G \circ J$.

DEMO Cela est tout à fait clair puisque $\pi \circ I = \pi \circ J$ implique que $\pi \circ I \circ J^{-1} = \pi$ et donc que $I \circ J^{-1} \in \Gamma$ ainsi il existe $G \in \Gamma$ tel que $I = G \circ J$.

□

Lemme 2 Si F est un difféomorphisme de E dans E en sorte qu'il existe f un difféomorphisme de B dans B tel que $\pi \circ F = f \circ \pi$ alors $F \circ \Gamma = \Gamma \circ F$.

DEMO Quel que soit $G \in \Gamma$ on a $\pi \circ (F \circ G) = f \circ \pi \circ G = f \circ \pi = \pi \circ F$ donc il existe $H \in \Gamma$ tel que $F \circ G = H \circ F$. Ainsi $F \circ \Gamma \subset \Gamma \circ F$.

Remarquons que l'on a, en vertu des deux bijections f et F :

$$\pi \circ F = f \circ \pi \iff f^{-1} \circ \pi \circ F = \pi \iff f^{-1} \circ \pi = \pi \circ F^{-1}$$

Ainsi, F^{-1} et f^{-1} satisfont à la condition $\pi \circ F^{-1} = f^{-1} \circ \pi$, on peut alors répéter le raisonnement ci-dessus qui nous donne que $F^{-1} \circ \Gamma \subset \Gamma \circ F^{-1}$ i.e. $\Gamma \circ F \subset F \circ \Gamma$ ainsi donc $F \circ \Gamma = \Gamma \circ F$.

□

Corollaire Supposons que Γ est un groupe d'isométries. Si $F: E \rightarrow E$ est une isométrie pour laquelle on peut trouver un difféomorphisme $f: B \rightarrow B$ tel que $\pi \circ F = f \circ \pi$ alors f est une isométrie de B et $F \in \mathcal{N}$

DEMO Par le lemme précédent, on sait déjà que $F \circ \Gamma = \Gamma \circ F$ donc que $F \in \mathcal{N}$.

Il nous reste à montrer que f est une isométrie: appelons g le tenseur métrique de E et h celui de B . Puisque π est une isométrie locale, on a, $\forall v, w \in T_E$, que $h(T_\pi(v), T_\pi(w)) = g(v, w)$; alors, puisque F est une isométrie on a $g(T_f(v), T_f(w)) = g(v, w)$ donc:

$$h(T_f \circ T_\pi(v), T_f \circ T_\pi(w)) = h(T_{f \circ \pi}(v), T_{f \circ \pi}(w)) = h(T_{\pi \circ F}(v), T_{\pi \circ F}(w)) = g(v, w) = h(T_\pi(v), T_\pi(w))$$

Puisque π est un revêtement on a que T_π est surjective et donc que $h(T_f(M), T_f(N)) = h(M, N)$ pour tout $M, N \in T_B$. D'où, f est une isométrie.

☐

Lemme Il existe un morphisme $\alpha: \mathcal{N} \rightarrow \text{Diff}(B)$ appelé abaissement tel que $\forall F \in \mathcal{N}$ on a $\pi \circ F = \alpha(F) \circ \pi$.

DEMO Prenons $F \in \mathcal{N}$. $\forall x, y \in E$ on a $y \sim x$ modulo l'action de Γ si et seulement si $\exists G \in \Gamma$ tel que $G(x) = y$. Or $F \in \mathcal{N}$ donc on peut trouver $H \in \Gamma$ tel que $F \circ G = H \circ F$ et donc $F(y) = F \circ G(x) = H \circ F(x) \sim F(x)$ modulo l'action de Γ . Ainsi, F envoie les classes modulo l'action de Γ sur les classes, c'est-à-dire qu'on peut définir F sur le quotient.

Le passage au quotient de F sera $\alpha(F)$.

Puisque les classes forment une partition de E et que F est une bijection, $\alpha(F)$ est encore une bijection. Montrons que $\alpha(F)$ est un difféomorphisme local: Soit U un ouvert E en sorte que $\pi|_U$ et $\pi|_{F(U)}$ soient des homéomorphismes alors le diagramme ci-contre commute par définition de $\alpha(F)$. Alors $\alpha(F)|_{\pi(U)} = (\pi|_U)^{-1} \circ F|_{\pi(U)} \circ \pi|_{F(U)}$ d'où $\alpha(F)|_{\pi(U)}$ est un difféomorphisme.

$$\begin{array}{ccc} U & \xrightarrow{F} & F(U) \\ \downarrow \pi & & \downarrow \pi \\ \pi(U) & \xrightarrow{\alpha(F)} & \pi \circ F(U) \end{array}$$

Sachant que $\alpha(F)$ est bijective, on a donc montré que $\alpha(F)$ est un difféomorphisme.

$$\begin{array}{ccccc} E & \xrightarrow{F} & E & \xrightarrow{G} & E \\ \downarrow \pi & & \downarrow \pi & & \downarrow \pi \\ B & \xrightarrow{\alpha(F)} & B & \xrightarrow{\alpha(G)} & B \end{array}$$

Il reste alors à voir que $\alpha: \mathcal{N} \rightarrow \text{Diff}(B)$ est un morphisme de groupe. Soient F et G deux éléments de \mathcal{N} alors $F \circ G \in \mathcal{N}$ par définition. On a alors le diagramme suivant qui, encore une fois est commutatif en vertu de la définition de $\alpha(F)$. On a donc $\pi \circ F = \alpha(F) \circ \pi$ et $\pi \circ G = \alpha(G) \circ \pi$ ainsi:

$$\alpha(F \circ G) \circ \pi = \pi \circ (F \circ G) = \alpha(F) \circ \pi \circ G = \alpha(F) \circ \alpha(G) \circ \pi$$

Puisque π est surjective, $\alpha(F \circ G) \circ \pi = \alpha(F) \circ \alpha(G) \circ \pi$ implique $\alpha(F \circ G) = \alpha(F) \circ \alpha(G)$. Donc α est bien un morphisme de groupe.

☐

Corollaire Si l'on restreint α aux isométries contenues dans \mathcal{N} alors α va dans les isométries de B .

DEMO Le corollaire précédent nous disait que, si I est une isométrie et i un difféomorphisme avec $\pi \circ I = i \circ \pi$, alors i est une isométrie. Ainsi α envoie une isométrie sur une isométrie.

☐

Lemme Cet abaissement est unique au sens suivant: si $F \in Diff(E)$ et $f \in Diff(B)$ tels que $\pi \circ F = f \circ \pi$ alors $F \in \mathcal{N}$ et $f = \alpha(F)$.

DEMO Par le lemme 2, on a que $F \in \mathcal{N}$. De plus, par surjectivité de π on peut trouver, pour tout point $x \in B$ un antécédant $y \in E$ par π alors $f(x) = f \circ \pi(y) = \pi \circ F(y) = \alpha(F) \circ \pi(y) = \alpha(F)(x)$ par définition de $\alpha(F)$. Ainsi $f = \alpha(F)$.

☐

Lemme

$$Ker(\alpha) = \Gamma$$

DEMO

$$F \in Ker(\alpha) \Leftrightarrow F \in \mathcal{N} \text{ et } \alpha(F) = Id_B \stackrel{\text{unicité}}{\Leftrightarrow} \pi \circ F = Id_B \circ \pi = \pi \Leftrightarrow F \in \Gamma$$

☐

Proposition Supposons que E est simplement connexe alors tout difféomorphisme de B dans B se remonte en un difféomorphisme de E dans E . Et donc $\alpha: Diff(E) \rightarrow Diff(B)$ est surjective.

DEMO On rappelle le critère de relèvement: soit $g: X \rightarrow B$, choisissons $x \in X$ et $y \in E$ tels que $\pi(y) = g(x)$ alors on a un relèvement $g': X \rightarrow E$ tel que $\pi \circ g' = g$ et $g'(x) = y$ si et seulement si $g_*(\pi_1(X, x)) \subset \pi_*(\pi_1(E, y))$.

Choisissons alors un point $x \in B$, $y \in E$ tel que $\pi(y) = x$ et appliquons ce critère à notre cas, on a donc le diagramme ci-contre pour tout difféomorphisme $f: B \rightarrow B$. On choisit $y' \in E$ tel que $\pi(y') = f(x)$, il est clair que l'application $f \circ \pi: E \rightarrow B$ satisfait aux critères puisque $\pi_1(E, y) = 1$. Donc il existe un relèvement $F: E \rightarrow E$ de $f \circ \pi$ tel que $f \circ \pi = \pi \circ F$. et que $F'(y) = y'$.

$$\begin{array}{ccc} E & & E \\ \pi \downarrow & & \downarrow \pi \\ B & \xrightarrow{f} & B \end{array}$$

Réciproquement, pour les mêmes raisons on a un relèvement $F': E \rightarrow E$ de $\pi \circ f^{-1}$ tel que $\pi \circ F' = f^{-1} \circ \pi$ et $F'(y') = y$.

Mais alors: $\pi \circ F' \circ F = f^{-1} \circ \pi \circ F = f^{-1} \circ f \circ \pi = \pi$ donc $F' \circ F$ est un relèvement de π qui, de plus, envoie y sur y , mais l'identité Id_E est également un relèvement de π puisque $\pi \circ Id_E = \pi$ par unicité du relèvement, on a $F' \circ F = Id_E$.

Dans l'autre sens $\pi \circ F \circ F' = f \circ \pi \circ F' = f \circ f^{-1} \circ \pi = \pi$ donc $F \circ F'$ est un relèvement de π qui, de plus, envoie y' sur y' . Sachant que Id_E a la même propriété, on conclut que $F \circ F' = Id_E$. Ainsi F et F' sont des bijections et $F' = F^{-1}$.

Par restriction aux voisinages on voit que F et F' sont différentiables. Donc F est un difféomorphisme. Enfin, le lemme d'unicité de l'abaissement nous donne que $f = \alpha(F)$ puisque $\pi \circ F = f \circ \pi$. D'où $\alpha: \mathcal{N}(\Gamma) \rightarrow Diff(B)$ est surjective.

☐

Théorème Soit E une variété simplement connexe, B une autre variété avec $\pi: E \twoheadrightarrow B$ un revêtement différentiable et Γ le groupe des transformations de revêtements alors le morphisme d'abaissement $\alpha: \mathcal{N}(\Gamma) \rightarrow Diff(B)$ est un morphisme de groupe surjectif et (on l'a vu) $\ker \alpha = \Gamma$. Donc α fournit $\tilde{\alpha}: \mathcal{N}(\Gamma)/\Gamma \rightarrow Diff(B)$ qui est un isomorphisme de groupes.

CLAIR

Théorème Soit E une variété riemannienne simplement connexe, B une autre variété riemannienne avec un revêtement différentiable $\pi: E \twoheadrightarrow B$ qui est une isométrie locale. Alors le morphisme d'abaissement restreint aux isométries donne des isométries, on a $\alpha: Iso(E) \rightarrow Iso(B)$ qui est surjectif. Et donc on peut définir le passage au quotient du morphisme $\tilde{\alpha}: Iso(E)/\Gamma \rightarrow Iso(B)$ qui est un isomorphisme de groupes.

DEMO Tout ce qu'il faut montrer est que α est surjective, autrement dit que si F est un difféomorphisme relevé d'une isométrie f alors F est une isométrie.

Soit f une isométrie de B . π est une isométrie locale alors soit U un ouvert tel que $\pi: U \rightarrow \pi(U)$ est une isométrie et tel que $\pi: F(U) \rightarrow \pi \circ F(U)$ en est une aussi.

On a $\pi \circ F = f \circ \pi$ donc :

$$\pi|_{F(U)} \circ F|_U = f|_{\pi(U)} \circ \pi|_U \text{ et donc } f|_U = (\pi|_{F(U)})^{-1} \circ f|_{\pi(U)} \circ \pi|_U$$

Donc $f|_U$ est une isométrie donc $f_*g|_{TU} = g|_{TU}$, et puisque les U recouvrent tout E , on a $F_*g = g$ ainsi F est également une isométrie.

□

Groupes triangulaires

Définitions

Dans le plan hyperbolique \mathbb{D}^2 , soient trois sommets a, b et c formant un triangle T dont les angles aux sommets sont respectivement $\frac{\pi}{l}, \frac{\pi}{m}$ et $\frac{\pi}{n}$, où $l, m, n \in \mathbb{N}^*$ en sorte que $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$; on sait qu'un tel triangle existe toujours. Appelons, enfin, L la réflexion dont l'axe est le support du segment $[b, c]$, M la réflexion dont l'axe est le support du segment $[a, c]$ et N la réflexion dont l'axe est le support du segment $[a, b]$.

Lemme On a les relations suivantes valables pour tout triplet L, M et N définis comme ci-dessus :

$$L^2 = M^2 = N^2 = (LM)^n = (LN)^m = (MN)^l = 1$$

DEMO Appelons κ_x la transformation de Moebius positive appliquant x sur 0 dans \mathbb{D}^2 .

Soit $A = L, M$ ou N et soit x un point de l'axe de A alors $\kappa_x^{-1} \circ A \circ \kappa_x$ est une symétrie euclidienne, elle est donc d'ordre 2. Ainsi A est d'ordre 2.

Soit $A \neq B \in \{L, M, N\}$ et soit $\{x\} = Axe(A) \cap Axe(B)$ alors il est clair que $\kappa_x^{-1} \circ A \circ B \circ \kappa_x = (\kappa_x^{-1} \circ A \circ \kappa_x) \circ (\kappa_x^{-1} \circ B \circ \kappa_x)$ est la composition de deux symétries euclidiennes et est donc une rotation dont l'angle est deux fois l'angle entre l'axe de $(\kappa_x^{-1} \circ A \circ \kappa_x)$ et l'axe de $(\kappa_x^{-1} \circ B \circ \kappa_x)$. Or κ_x qui est le même l'angle entre l'axe A et l'axe de B puisque κ_x est conforme. Par définition l'angle inorienté entre les axes de A et B est :

$$\begin{cases} \frac{\pi}{l} & \text{si } \{A, B\} = \{M, N\} \\ \frac{\pi}{m} & \text{si } \{A, B\} = \{L, N\} \\ \frac{\pi}{n} & \text{si } \{A, B\} = \{L, M\} \end{cases} \text{ ainsi donc } \begin{cases} MN \text{ et } NM & \text{sont d'ordre } l \\ LN \text{ et } NL & \text{sont d'ordre } m \\ LM \text{ et } ML & \text{sont d'ordre } n \end{cases}$$

∩

On appellera $\widetilde{\Delta}(l, m, n)$ le groupe engendré par ces trois réflexions dans le groupe \mathcal{M}_{\pm} des transformations de Moebius, positives ou négatives. Appelons, en outre H le groupe abstrait donné par la présentation :

$$H = \langle L, M, N \mid L^2 = M^2 = N^2 = (LM)^n = (LN)^m = (MN)^l = 1 \rangle$$

On a alors un morphisme de groupe surjectif $\pi: H \rightarrow \widetilde{\Delta}(l, m, n)$.

D'autre part, soit A une arête de ce triangle, on appellera *transformations vicinales autour de A* et l'on notera V_A l'ensemble composé de la transformation identité notée 1 et de la réflexion R_A dont l'axe est le support de l'arête A . Soit un x un sommet du triangle, on appellera *transformations vicinales autour de x* le sous-groupe V_x engendré par A et B , où A et B sont les réflexions autour de chacun des axes qui sont le support des arêtes contenant x .

Lemme V_A est isomorphe à \mathbb{F}_2 . V_A est isomorphe au groupe $\langle A, B \mid A^2 = B^2 = (AB)^j = 1 \rangle$ où j est l, m ou n donné par le lemme précédent.

DEMO Soit R_A la réflexion autour de l'axe support de A , on a en vertu du lemme précédent que $R_A^2 = 1$ et donc $\{1, R_A\}$ est un sous-groupe de $\widetilde{\Delta}(l, m, n)$.

Les éléments de $V_x = \langle A, B \rangle \subset \mathcal{M}^{\pm}$ obéissent aux relations énoncées en vertu du lemme précédent. Reste à montrer qu'il n'y a pas d'autres relations. Or cela est clair puisque $\kappa_x^{-1} \circ V_x \circ \kappa_x$ est un groupe engendré par deux symétries euclidiennes d'axes concourant en 0, il s'agit donc du groupe diédral d'ordre j .

Il va s'agir de montrer que le groupe endré par L , M et N est bel et bien un groupe fuchsien dont le domaine fondamental est le triangle T . Pour cela nous allons devoir recoller des homéomorphismes. Voici les lemmes qui nous le permettront :

Lemme Soient A et B deux ouverts disjoints d'un espace topologique X , Y un autre espace topologique et soient $f: \bar{A} \rightarrow Y$ et $g: \bar{B} \rightarrow Y$ deux applications continues qui coïncident sur l'intersection de \bar{A} avec \bar{B} . Alors il existe une application continue notée $f \cup g$ et appelée le recollement de f et g allant de $\bar{A} \cup \bar{B}$ dans Y telle que $(f \cup g)|_{\bar{A}} = f$ et $(f \cup g)|_{\bar{B}} = g$.

DEMO En effet, soit $x \in \bar{A} \cap \bar{B}$ et O un voisinage ouvert de x dans Y alors :

$$h^{-1}(O) = f^{-1}(O) \cup g^{-1}(O) = (U \cap \bar{A}) \cup (V \cap \bar{B})$$

où U et V sont des ouverts de X . Or $x \in f^{-1}(O)$ et $x \in g^{-1}(O)$ donc $x \in U$ et $x \in V$ et donc $U \cap V$ est un ouvert non-vide, voisinage de x . Alors

$$(U \cap V) \cap (\bar{A} \cup \bar{B}) = (U \cap V) \cap A \cup (U \cap V) \cap B \subset (U \cap \bar{A}) \cup (V \cap \bar{B}) = (f \cup g)^{-1}(O)$$

On a donc trouvé, pour tout voisinage de $f(x)$, un voisinage de x contenu dans la préimage du premier. Donc $f \cup g$ est continue aux point $x \in \bar{A} \cap \bar{B}$.

Si $x \in \bar{A} \setminus \bar{B}$ et O est un voisinage de $f(x)$ alors $(f \cup g)^{-1}(O)$ contient $f^{-1}(O) = U \cap \bar{A}$ pour un U ouvert de X . Or \bar{B} est fermé dans X donc $U \cap \bar{B}$ est encore un ouvert de X qui contient toujours x . Alors $\bar{A} \cap (U \cap \bar{B}) = (\bar{A} \cap \bar{B}) \cap (U \cap \bar{B})$ est un ouvert de $\bar{A} \cup \bar{B}$ voisinage de x et contenu dans $f^{-1}(O)$ et donc dans $(f \cup g)^{-1}(O)$. Ainsi tout voisinage de $f(x)$ admet un voisinage de x dans sa préimage. Et donc $f \cup g$ est continue sur $\bar{A} \setminus \bar{B}$.

On montre, exactement de la même manière que $f \cup g$ est continue sur $\bar{B} \setminus \bar{A}$. Donc $f \cup g$ est continue sur tout $\bar{A} \cup \bar{B}$.

Lemme Soient A et B deux ouverts disjoints d'un espace topologique X , R et S deux ouverts disjoints d'un espace topologique Y et deux homéomorphismes $f: \bar{A} \rightarrow \bar{R}$ et $g: \bar{B} \rightarrow \bar{S}$. qui coïncident sur leur intersection et tels que $f(\bar{A} \cap \bar{B}) = \bar{R} \cap \bar{S} = g(\bar{A} \cap \bar{B})$.

Alors le recollement de f et g est aussi un homéomorphisme $f \cup g: \bar{A} \cup \bar{B} \rightarrow \bar{R} \cup \bar{S}$ qui coïncide avec f sur \bar{A} et avec g sur \bar{B} .

DEMO Par le lemme précédent, on sait que $f \cup g$ est continue.

L'application est surjective puisque $\forall x \in \bar{R} \cup \bar{S}$ on a $x \in \bar{R}$ ou $x \in \bar{S}$ et donc $f^{-1}(x)$ ou $g^{-1}(x)$ existe et est un antécédant de x par $f \cup g$.

Elle est injective puisque si $x \neq y$ appartiennent tous deux à \bar{A} ou tous deux à \bar{B} alors, en vertu de l'injectivité de f et de g , on a que $(f \cup g)(x) \neq (f \cup g)(y)$. En outre si $x \neq y$ avec $x \in \bar{A} \setminus \bar{B}$ et $y \in \bar{B} \setminus \bar{A}$ alors $(f \cup g)(x) = f(x) \in \bar{R} \setminus \bar{S}$ puisque $f^{-1}(\bar{R} \cap \bar{S}) = \bar{A} \cap \bar{B}$ et $(f \cup g)(y) = g(y) \in \bar{S} \setminus \bar{R}$ puisque $g^{-1}(\bar{R} \cap \bar{S}) = \bar{A} \cap \bar{B}$, étant dans deux ensembles disjoints, ces deux éléments ne peuvent être égaux.

En outre, on a $f^{-1}: \bar{R} \rightarrow \bar{A}$ et $g^{-1}: \bar{S} \rightarrow \bar{B}$ deux applications continues en sorte que :

$$f^{-1}|_{\bar{R} \cap \bar{S}} = \overset{f(\bar{A} \cap \bar{B}) = \bar{R} \cap \bar{S}}{(f|_{\bar{A} \cap \bar{B}})^{-1}} = \overset{g(\bar{A} \cap \bar{B}) = \bar{R} \cap \bar{S}}{(g|_{\bar{A} \cap \bar{B}})^{-1}} = (g|_{\bar{A} \cap \bar{B}})^{-1} = g^{-1}|_{\bar{R} \cap \bar{S}}$$

Donc $f^{-1} \cup g^{-1}$ existe et est continu, il est même l'inverse de $f \cup g$:

$$(f \cup g)(x) = y \Leftrightarrow \begin{cases} x \in \bar{A} \text{ et } y = f(x) \\ \text{ou} \\ x \in \bar{B} \text{ et } y = g(x) \end{cases} \Leftrightarrow \begin{cases} y \in \bar{R} \text{ et } x = f^{-1}(y) \\ \text{ou} \\ y \in \bar{S} \text{ et } x = g^{-1}(y) \end{cases} \Leftrightarrow (f^{-1} \cup g^{-1})(y) = x$$

On vient donc de montrer que $f \cup g$ est une bijection continue dont l'inverse est continue, il est donc un homéomorphisme.

Corollaire

Soient $(A_i)_{i=1..n}$ une famille finie d'ouverts disjoints d'un espace X et $(B_i)_{i=1..n}$ une famille finie d'ouverts disjoints d'une espace topologique Y tels que $\forall i, j = 1..n$ on ait $f_i|_{\bar{A}_i \cap \bar{A}_j} = f_j|_{\bar{A}_i \cap \bar{A}_j}$ et que $f_i(\bar{A}_i \cap \bar{A}_j) = f_j(\bar{A}_i \cap \bar{A}_j)$ alors il existe un recollement des f_i qui sera écrit $(\bigcup_{i=1}^n f_i)$ Il s'agit d'un homéomorphisme de $\bigcup_{i=1}^n A_i$ sur $\bigcup_{i=1}^n B_i$ tel que $(\bigcup_{i=1}^n f_i)|_{A_i} = f_i$.

DEMO Pour $k = 1..n$, on pose $u_k: \bigcup_{i=1}^k \bar{A}_i \longrightarrow \bigcup_{i=1}^n \bar{A}_i$ qui est bien défini puisque les f_i coïncident sur leurs intersections deux à deux. On a déjà que $u_1 = f_1$ est un homéomorphisme, supposons

alors, par induction, que u_k est un homéomorphisme tel que $u_k|_{\bar{A}_i} = f_i \forall i = 1..k$. Alors:

$$f_{k+1}|_{\bar{A}_{k+1} \cap \bigcup_{i=1}^k \bar{A}_i} = f_{k+1}|_{\bigcup_{i=1}^k \bar{A}_{k+1} \cap \bar{A}_i} \text{ or } f_{k+1}|_{\bar{A}_{k+1} \cap \bar{A}_i} = f_i|_{\bar{A}_{k+1} \cap \bar{A}_i} \text{ donc } f_{k+1}|_{\bar{A}_{k+1} \cap \bigcup_{i=1}^k \bar{A}_i} = u_k|_{\bar{A}_{k+1} \cap \bigcup_{i=1}^k \bar{A}_i}$$

De plus:

$$f_{k+1}(\bar{A}_{k+1} \cap \bigcup_{i=0}^k \bar{A}_i) = f_k(\bigcup_{i=0}^k \bar{A}_{k+1} \cup \bar{A}_i) = \bigcup_{i=0}^n f_i(\bar{A}_{k+1} \cap \bar{A}_i) = \bar{B}_k \cap \bigcup_{i=1}^k \bar{B}_i$$

Ainsi, on peut appliquer le lemme précédent pour obtenir que u_{k+1} est un homéomorphisme tel qu'on le souhaite. Alors u_n est l'homéomorphisme cherché.

□

Remarque

On pourrait étendre facilement ce résultat à une famille dénombrable, cela exigerait, toutefois, la finitude locale de la famille des A_i et de la famille des B_i ce que nous ne pourrions avoir facilement dans notre cas, le développement ne rentre donc pas dans ce cadre.

Construction

Toute la construction qui suit est très largement inspirée du Théorème de Poincaré donné dans le livre de [Maskit (1988), pp. 68-78] Afin de prouver que le triangle T est bien un domaine fondamental de $\widetilde{\Delta}(l, m, n)$, nous allons assembler des copies de ce triangle à la façon avec laquelle on pense que le plan hyperbolique est pavé, puis nous allons montrer que c'est assemblage est, localement, puis globalement homéomorphe au plan hyperbolique. On obtiendra ainsi un pavage du plan hyperbolique et, par la même occasion, un isomorphisme $\pi: H \longrightarrow \widetilde{\Delta}(l, m, n)$.

Introduisons une relation sur $H \times T$ que l'on considère comme le produit de T par l'espace discret H : on dira que:

$$(g, x) \sim (h, y) \Leftrightarrow x = y \text{ et } \begin{cases} x \text{ est dans l'intérieur du triangle et } g = h & (1) \\ x \text{ est dans l'intérieur d'une arête } A \text{ et } hg^{-1} \in V_A & (2) \\ x \text{ est un sommet et } hg^{-1} \in V_x & (3) \end{cases}$$

Vérifions qu'il s'agit bien d'une relation d'équivalence:

réflexive : $(g, x) \sim (g, x)$ puisque $x = x$ et que $g = g$ et puisque 1 est dans V_A et dans V_x .

symétrique : si $(g, x) \sim (h, y)$ avec (1) alors $x = y \in T^\circ$ et $g = h$ donc (1) $(h, y) \sim (g, x)$.

si $(g, x) \sim (h, y)$ avec (2) alors $x = y$ est dans l'intérieur d'une arête A et $g^{-1}h \in V_A$ donc $h^{-1}g \in V_A$ en vertu du sous-groupe et donc (2) $((h, y) \sim (g, x)$.

transitive : si $(g, x) \sim (h, y)$ et $(h, y) \sim (i, z)$ alors $x = y = z$. Si $x \in T^\circ$ alors $g = h = i$ et donc $(g, x) \sim (i, z)$. Si x est dans l'intérieur d'une arête A alors $g^{-1}h \in V_A$ et $h^{-1}i \in V_A$ donc $g^{-1}i = (g^{-1}h)(h^{-1}i) \in V_A$ (sous-groupe) et donc (2) $(g, x) \sim (i, z)$. Enfin, si x est un des sommets alors $g^{-1}h \in V_x$ et $h^{-1}i \in V_x$ donc (sous-groupe) $g^{-1}i = (g^{-1}h)(h^{-1}i) \in V_x$ ainsi (3) $(g, x) \sim (i, z)$.

On appellera alors \widetilde{X} l'espace topologique quotient de $H \times T$ par la relation d'équivalence \sim . On a donc une projection de quotient continue surjective et ouverte $p: H \times T \longrightarrow \widetilde{X}$.

Grâce au morphisme de groupe $\pi: H \longrightarrow \widetilde{\Delta}(l, m, n)$, on peut définir $q: H \times T \longrightarrow \mathbb{D}^2$ qui est

$$(g, x) \longmapsto [\pi(g)](x)$$

donc une application continue. On remarque que l'on a utilisé ici l'inclusion de T dans \mathbb{D}^2 .

On vérifie alors que q passe au quotient modulo \sim :

En effet si $(g, x) \sim (h, y)$ avec (1) alors $(g, x) = (h, y)$ donc $q(g, x) = q(h, y)$.

Si $(g, x) \sim (h, y)$ et $x = y$ est dans l'intérieur d'une arête alors $g^1 h \in V_A$ donc $\pi(g^1 \circ h)$ fixe les points de A et alors $q(g, x) = [\pi(g)](x) = [\pi(g)](\pi(g^1 h))(x) = [\pi(h)](x) = q(h, x) = q(h, y)$.

Si $(g, x) \sim (h, y)$ et $x = y$ est un sommet du triangle alors $g^1 h \in V_x$ et donc $\pi(g^1 h)$ fixe x , on a ainsi que $q(g, x) = [\pi(g)](x) = [\pi(g)]([\pi(g^1 h)](x)) = [\pi(h)](y)$.

L'application continue q peut donc passer au quotient modulo \sim , on obtient une application continue \tilde{q} de \tilde{X} dans \mathbb{D}^2 en sorte que $q = \tilde{q} \circ p$.

En définissant encore $p_2: H \times T \rightarrow T$ comme la projection sur la deuxième composante, on a une application continue. On peut alors résumer la situation en le diagramme suivant :

$$\begin{array}{ccc} H \times T & \xrightarrow{p_2} & T \\ \downarrow p & \searrow q & \downarrow (\text{inclusion}) \\ \tilde{X} & \xrightarrow{\tilde{q}} & \mathbb{D}^2 \end{array}$$

Il va s'agir de montrer maintenant que \tilde{q} est un homéomorphisme local, ceci au moyen des trois lemmes suivants qui traitent respectivement les cas de voisinages d'un point intérieur aux triangles, sur l'intérieur d'une arête ou d'un sommet.

Lemme 2 Soit x un point de l'intérieur de T alors il existe un voisinage U de x tel que $p \circ p_2^{-1}(U)$ est la réunion disjointe de d'ouverts $p(\{g\} \times U)$ en sorte que \tilde{q} restreint à $p(\{g\} \times U)$ est un homéomorphisme arrivant sur une boule de \mathbb{D}^2 .

DEMO Puisque x est dans l'intérieur de T , il existe un rayon δ en sorte que $B(x, \delta)$ ne contienne que des points intérieurs au triangle. On pose $U = B(x, \delta)$, alors $p_2^{-1}(U) = H \times U$. Un point (g, y) de $H \times T$ tel que $y \in T^\circ$ n'est équivalent qu'à lui même modulo \sim donc $p|_{H \times U}$ est une bijection. p étant ouverte c'est un homéomorphisme.

D'un autre côté, choisissons $g \in H$ alors $q|_{\{g\} \times U} = \pi(g)|_U \circ p_2$. L'application p_2 restreinte à un sous-ensemble d'une des copies de T est un homéomorphisme, par définition, $\pi(g)$ en est également un donc $q|_{\{g\} \times U}$ est un homéomorphisme dont l'image est l'image par l'isométrie $\pi(g)$ de la boule U qui est une boule.

Ainsi, pour tout $g \in H$, $p|_{\{g\} \times U}$ et $q|_{\{g\} \times U}$ sont des homéomorphismes et donc :

$$\tilde{q}|_{p(\{g\} \times U)} = q|_{\{g\} \times U} \circ (p|_{\{g\} \times U})^{-1}$$

est un homéomorphisme allant d'un ouvert de \tilde{X} , $p(\{g\} \times U)$, sur une boule $[\pi(g)](U)$ de \mathbb{D}^2 .

□

Lemme 1 Soit $x \in T$ un point se trouvant dans l'intérieur d'une arête A alors il existe un ouvert U de T en sorte que $p_2^{-1}(U)$ soit la réunion disjointe d'une famille d'ouverts $\{U_g | g \in H\}$ tels que \tilde{q} restreint à chaque $p(U_g)$ est un homéomorphisme sur une boule de \mathbb{D}^2 .

DEMO Puisque x est dans l'intérieur d'une arête, on peut trouver δ un rayon tel que $B(x, \delta)$ ne contienne pas de points des autres arêtes que A . On pose $U = B(x, \delta)$, donc $p_2^{-1}(U) = H \times U$, U est l'intersection d'une boule de \mathbb{D}^2 avec le demi-plan dont le bord est le support de A . Les points de (g, y) où y est sur $A \cap U$ sont équivalents aux points (gB, y) où $B \in V_A$, on pose alors

$$U_g = \cup_{B \in V_A} \{gB\} \times U$$

On a bien, en vertu de la topologie quotient que $p(U_g)$ est une ouvert. De plus, il est clair que $p|_{\{gB\} \times U}$ est un homéomorphisme pour chaque $B \in V_A$ (puisque $\{gB\} \times U$ est contenu dans une seule copie de T).

De l'autre côté, $q|_{\{gB\} \times U} = \pi(gB)|_U \circ p_2$ est, pour les mêmes raisons, un homéomorphisme.

Ainsi: $\tilde{q}|_{p(\{gB\} \times U)} = q|_{\{gB\} \times U} \circ (p|_{\{gB\} \times U})^{-1}$ est un homéomorphisme pour chaque $B \in V_A$. De plus V_A n'est composé que de deux éléments disons B et 1 d'où, si $C = U \cap A$:

$$p(\{gB\} \times U \cap \{g\} \times U) = p(\{g\} \times C) = p(\{gB\} \times C) \text{ donc } \tilde{q}|_{p(\{g\} \times C)} = \tilde{q}|_{p(\{gB\} \times C)}$$

Et donc $\tilde{q}(\{g\} \times U \cap \{gB\} \times U) = \tilde{q}(\{g\} \times C) = [\pi(g)](C)$ qui est exactement l'intersection de $[\pi(g)](U)$ avec $[\pi(g)]([\pi(B)](U))$ puisque B est un réflexion autour du support de C et que U n'est que U est la demie-boule d'intersection de $B(x, \delta)$ avec le demi-plan contenant T et limité par le support de C .

On a donc affaire à deux ouverts $p(\{g\} \times (U \cap T^\circ))$ et $p(\{gB\} \times (U \cap T^\circ))$ disjoints de \tilde{X} avec deux homéomorphismes $\tilde{q}|_{p(\{g\} \times U)}$ et $\tilde{q}|_{p(\{gB\} \times U)}$ définis sur l'adhérence de ces ouverts et qui coïncident sur leur intersection et envoient l'intersection sur l'intersection de leurs images des adhérences des ouverts. On a donc rempli les conditions du lemme de recollement des homéomorphismes qui nous donne un homéomorphisme de $U_g = p(\{g\} \times U) \cup p(\{gB\} \times U) = p(U_g)$ vers la réunion de deux demies-boules découpées de chaque côté de C , qui est donc une boule.

∩

Lemme 0 Soit x un sommet de T alors il existe un ouvert U de T tel que $p_2^1(U)$ soit la réunion disjointe d'une famille d'ouverts $\{U_g | g \in H\}$ tels que \tilde{q} restreint à chaque U_g est un homéomorphisme arrivant sur une boule de \mathbb{D}^2 .

DEMO On peut trouver un rayon δ tel que la boule $B(x, \delta) \subset T$ ne coupe aucune autre arête que les deux arêtes qui contiennent x . On pose alors $U = B(x, \delta)$ alors $p_2^1(U)$ est une réunion de *secteurs circulaires*. Pour tout $g \in H$, les points de $\{g\} \times U$ sont séparés en trois types: soit $y \in T^\circ$ alors (g, y) n'est équivalent qu'à lui-même modulo \sim ; soit y est sur le bord d'une arête A alors (g, y) est équivalent à (gB, y) pour chaque $B \in V_A$, soit, enfin, y est un sommet et donc $(g, y) \sim (gB, y)$ pour chaque $B \in V_x$. On pose alors:

$$U_g = \cup_{B \in V_x} \{gB\} \times U$$

D'un côté $q|\{gB\} \times U$ est un homéomorphisme pour chaque $B \in V_x$, de l'autre côté $p|\{gB\} \times U$ est un homéomorphisme puisque $\{gB\} \times U$ est contenu dans une seule copie du triangle. Ainsi (comme précédemment) $\tilde{q}|_{\{gB\} \times U}$ est un homéomorphisme de $p(\{gB\} \times U)$ dans $q(\{gB\} \times U)$ qui est $[\pi(gB)](U)$ c'est-à-dire l'intersection de $[\pi(gB)](B(x, \delta))$ avec $[\pi(gB)](\angle)$ où \angle est l'angle du triangle au sommet x . Ainsi:

$$q(U_g) = \cup_{B \in V_x} q(\{gB\} \times U) \stackrel{\text{isométrie}}{=} [\pi(g)](B)(x, \delta) \cap \cup_{B \in V_x} [\pi(B)](\angle)$$

Mais, puisque $\pi(V_x)$ est le groupe engendré par les réflexions dont les axes sont les côtés de l'angle, on a que $\cup_{B \in V_x} [\pi(B)](\angle)$ remplit tout \mathbb{D}^2 . Par conséquent $q(U_g) = [\pi(g)](B(x, \delta))$.

On montre ensuite que $\tilde{q}: p(U_g) \rightarrow$ satisfait aux conditions du corollaire de recollement. On cherche à recoller $\tilde{q}|_{p(gB \times U)}$. Il est clair que, pour $B, D \in V_x$ on a que $p(\{gB\} \times U) \cap p(\{gD\} \times U)$ est soit le seul sommet x soit l'intersection d'une arête entière avec U . Par le lemme 1, on sait que l'image par \tilde{q} de l'intérieur d'une arête entre deux triangles contigus $p(\{g\} \times T)$ et $p(\{gC\} \times T)$ est exactement l'arête entre les deux images de ces triangles. De plus, quelque soit $B \in V_x$, on a que $\tilde{q}(p(g, x)) = [\pi(g)](x) = [\pi(g)]([\pi(B)](x)) = [\pi(gB)](x) = \tilde{q}(p(gB, x))$ ainsi donc les restrictions de \tilde{q} à $p(gB \times U)$ envoient l'intersection de l'adhérence de leur domaine exactement dans l'intersection des images de l'adhérence de ceux-ci. Puisque les restrictions coïncident (par nature), on a trouvé une famille d'homéomorphismes satisfaisant au corollaire de recollement. On a donc un homéomorphisme depuis $\cup_{B \in V_x} p(\{gB\} \times U) = p(U_g)$ qui est un ouvert de \tilde{X} (en vertu de la topologie quotient) sur $q(U_g) = [\pi(g)](B(x, \delta))$.

∩

Corollaire Pour tout point $x \in \tilde{q}(\tilde{X})$ on a une boule U de \mathbb{D}^2 en sorte que $\tilde{q}^{-1}(U)$ est la réunion disjointe d'ouverts $\{U_g | g \in G\}$ en sorte que $\tilde{q}|_{U_g}$ est un homéomorphisme.

DEMO En effet, tout point de $[(g, y)]$ de \tilde{X} , $y \in T$ alors on a montré qu'il existait un ouvert U de T tel que $p(p_2^1(U))$ est la réunion disjointe d'ouverts $\{U_g | g \in G\}$ et tel que $q(p(p_2^1(U_g))) = \tilde{q}(p(p_2^1(U_g)))$ est une boule de \mathbb{D}^2 . et $\tilde{q}|_{p(p_2^1(U))}$ est un homéomorphisme. Alors $p_2^1(U) = H \times U$ contient donc (g, y) . Ainsi pour tout point $\tilde{q}([(g, y)])$ de $\tilde{q}(\tilde{X})$ on a trouvé un tel ouvert qui est boule centrée centrée en $\tilde{q}([(g, y)])$ et une réunion disjointe d'ouverts $\{U_g | g \in G\}$, où G est un sous-ensemble de H qui contient au moins g , en sorte que $\tilde{q}|_{U_g}$ est un homéomorphisme.

Q

Lemme \tilde{X} est connexe par arc.

DEMO On montre que tout point $[(g, x)]$ de \tilde{X} peut être relié au point x de $Int(T)$ par un chemin. Puisque T est connexe par arc, on aura la connexité par arc de \tilde{X} . On a donc $g \in H$ et $x \in T$. Soit $R_1 \dots R_n$ l'expression de g sur l'alphabet $\{L, M, N\}$. On construit un chemin dans chaque $\{R_i \dots R_n\} \times T$ par induction :

R_n est un réflexion autour d'une arête, appelons la A_n , il existe alors γ_n un chemin dans $Int(T)$ allant de $x \in Int(T)$ jusqu'à un point b_n de l'intérieur de $A_i \subset T$. Supposons que $i \leq n$ et que l'on a construit γ_{i+1} et $b_{i+1} \in A_{i+1} \subset T$ et construisons alors γ_i : R_i est une réflexion autour d'une arête de T , appelons-la A_i et choisissons un point b_i dans l'intérieur de cette arête. Puisque $Int(T)$ est connexe, il existe un chemin allant de b_{i+1} à b_i , ce sera le chemin γ_i .

Remarquons alors que, puisque $b_i \in A_i$ on a que $R_i(b_i) = b_i$ donc $(R_{i+1} \dots R_n, b_i) \sim (R_i \dots R_n, b_i)$ ainsi le début d'un chemin $t \mapsto [(R_i \dots R_n, \gamma_i(t))]$ est la fin du chemin $t \mapsto [(R_{i+1} \dots R_n, \gamma_{i+1}(t))]$ on peut donc "appondre" les chemins $t \mapsto [(R_{i+1} \dots R_n, \gamma_i(t))]$ pour donner un chemin continu entre x et $[(R_1 \dots R_n, x)] = [(g, x)]$.

Q

Corollaire \tilde{q} est un revêtement de \tilde{X} sur \mathbb{D}^2 . Ainsi, puisque \mathbb{D}^2 est simplement connexe et que \tilde{X} est connexe, il s'agit d'un homéomorphisme. Alors $\pi: H \longrightarrow \tilde{\Delta}(l, m, n)$ est un isomorphisme de groupe et l'on obtient que: $\tilde{\Delta}(l, m, n)$ admet la présentation :

$$\langle L, M, N | L^2 = M^2 = N^2 = (LM)^n = (LN)^m = (MN)^l = 1 \rangle$$

Et le triangle est bien un domaine fondamental de $\tilde{\Delta}(l, m, n)$.

DEMO On sait, d'après le corollaire précédent, que \tilde{q} est un revêtement de \tilde{X} sur $\tilde{q}(\tilde{X}) \subset \mathbb{D}^2$. Il suffit donc de montrer que \tilde{q} est surjective.

Pour cela munissons \tilde{X} de la métrique riemannienne déduite de \mathbb{D}^2 par \tilde{q} , ainsi \tilde{q} sera une isométrie locale. Notons d la distance associée à cette métrique.

On remarque qu'avec cette métrique, toutes les applications $t_h: [(g, x)] \mapsto [(hg, x)]$ pour $h \in H$ sont des isométries puisque $\tilde{q} \circ t_h = [\pi(h)] \circ \tilde{q}$. $\{1\} \times T$ est clairement un domaine fondamental de cette action, de plus T en est le quotient puisque les t_h ne changent pas la seconde composante d'un élément de \tilde{X} . On a alors que, $\forall [(g, x)], [(h, y)] \in \tilde{X}$, $d([(g, x)], [(h, y)]) \geq d(x, y)$. Ce qui nous prouve également que \tilde{X} est complet puisque T l'est.

Alors, on peut prolonger à l'infini toute géodésique de \tilde{X} et la projection de toute géodésique par \tilde{q} est également une géodésique (isométrie locale). De plus, par isométrie locale encore, une géodésique de \mathbb{D}^2 peut être relevée localement, son relevé sera une géodésique \tilde{X} qui se prolonge à l'infini et dont la projection coïncidera avec la première. Donc les géodésiques de l'ouvert $\tilde{q}(\tilde{X})$ se prolongent à l'infini et donc, par Hopf-Rinow, $\tilde{q}(\tilde{X})$ est complet. On en déduit que $\tilde{q}(\tilde{X})$ est un ouvert complet de \mathbb{D}^2 , donc un ouvert fermé de \mathbb{D}^2 , ainsi $\tilde{q}(\tilde{X})$ est tout \mathbb{D}^2 .

On a donc montré que \tilde{q} est surjective ce qui implique que \tilde{q} est un revêtement de \tilde{X} sur \mathbb{D}^2 . Mais \mathbb{D}^2 est simplement connexe par conséquent \tilde{X} est simplement connexe et donc la fibre de chaque point de ce revêtement est réduite à un point. Donc \tilde{q} est une isométrie locale bijective, il est donc une isométrie de \tilde{X} dans \mathbb{D}^2 .

Puisque $\{1\} \times T$ est un domaine fondamental de l'action des t_h , et puisque $\pi(g)(\tilde{q}(\{1\} \times T)) = \tilde{q}(\{g\} \times T)$

puisque l'on a bijection entre le groupe et les images du domaine fondamental et puisque T possède trois points en position générale :

$$\pi(g) = \pi(h) \Leftrightarrow [\pi(g)](T) = [\pi(h)](T) \Leftrightarrow \tilde{q}(\{g\} \times T) = \tilde{q}(\{h\} \times T) \Rightarrow g = h$$

Ainsi π est un morphisme injectif, on sait qu'il est surjectif, c'est donc un isomorphisme et donc $\pi(H) = \tilde{\Delta}(l, m, n)$ admet $\tilde{q}(\{1\} \times T) = T$ comme domaine fondamental.

□

Théorème

Soient a, b et c les sommets d'un triangle dont l'angle en a est $\frac{\pi}{l}$, l'angle en b est $\frac{\pi}{m}$ et l'angle en c est $\frac{\pi}{n}$. Soient L la réflexion dont l'axe est le support de $[b, c]$, M la réflexion dont l'axe est le support de $[a, c]$ et N la réflexion dont l'axe est le support de $[a, b]$. Alors le groupe $\tilde{\Delta}(l, m, n)$ engendré par L, M et N est un groupe discontinu d'isométries de \mathbb{D}^2 qui admet le triangle dont les sommets sont a, b et c comme domaine fondamental et qui admet la présentation suivante :

$$\langle L, M, N \mid L^2 = M^2 = N^2 = (LM)^n = (LN)^m = (MN)^l = 1 \rangle$$

DEMO Il ne s'agit que d'un résumé de toute la construction que nous venons de faire depuis le début du chapitre.

□

Lemme

Soit Γ un sous-groupe d'indice fini d'un groupe Fuchsien G , on peut donc trouver une famille finie $Tr = \{\alpha_1, \dots, \alpha_n\} \subset G$ contenant un et un seul représentant de chaque classe modulo Γ (une transversale de Schreier). Alors si Q est un domaine fondamental de G , l'ensemble :

$$O = \cup_{i=1}^n \alpha_i(Q)$$

est un domaine fondamental pour Γ .

DEMO On montre que les images de O par l'action de Γ remplissent \mathbb{D}^2 sans se chevaucher :

Remplissage : soit un point $p \in H^2$ alors (quadrilatère fondamental) il existe $\psi \in G$ en sorte que $\psi(Q) \ni p$. Mais alors (transversale) je peut trouver $\alpha_i \in Tr$ et $\gamma \in \Gamma$ telles que $\psi = \gamma \circ \alpha_i$ et donc $p \in \psi(Q) = \gamma(\alpha_i(Q)) \subset \gamma(O)$.

Non-chevauchement : Soit $p \in \nu(O) \cap \mu(O)$ alors je peut trouver α_i et $\alpha_j \in Tr$ en sorte que $p \in \mu \circ \alpha_i(Q) \cap \nu \circ \alpha_j(Q)$.

(i) $p \in \text{Int}(\mu \circ \alpha_i(Q)) \Rightarrow \mu = \nu$

En effet, on a sous cette hypothèse : $\alpha_i^{-1} \circ \mu^{-1}(p) \in \text{Int}(Q)$, appelons r ce point ; de plus $\alpha_j^{-1} \circ \nu^{-1}(p) \in Q$. Alors $\alpha_j^{-1} \circ \nu^{-1} \circ \mu \alpha_i : r \in \text{Int}(Q) \mapsto \alpha_j^{-1} \circ \nu^{-1}(p) \in Q$ donc cette transformation, qui est dans G envoie un point de l'intérieur du domaine fondamental vers un point du domaine fondamental, elle est donc forcément égale à l'identité. Et alors :

$$\alpha_j^{-1} \circ \nu^{-1} \circ \mu \circ \alpha_i = 1 \iff \alpha_j^{-1} \circ \alpha_i = \nu^{-1} \circ \mu \in \Gamma \Rightarrow \alpha_i = \alpha_j \Rightarrow \nu^{-1} \circ \mu = 1 \Rightarrow \nu = \mu$$

(ii) $\nu \neq \mu$ alors $p \in \partial O$

En vertu de (i), $p \in \partial(\mu \circ \alpha_i(Q))$ et $p \in \partial(\nu \circ \alpha_j(Q))$.

Primo, chaque voisinage de p contient p qui est un point de $\mu \circ \alpha_i(Q) \subset \mu(O)$.

Et puisque $p \in \partial(\nu \circ \alpha_j(\bar{Q}))$, chaque voisinage de p contient un point de $\text{Int}(\nu \circ \alpha_j(\bar{Q}))$. Mais un tel point n'est pas dans $\mu(O)$ puisque $\mu \neq \nu$ et puisque nous avons montré en (i) qu'un point de l'intérieur d'un quadrilatère ne pouvait appartenir qu'à une seule image de O . En résumé, chaque voisinage de p contient un point de $\mu(O)$ et un point qui n'est pas dans $\mu(O)$ donc p est dans le bord de $\mu(O)$.

∩

Corollaire Le sous-groupe $T(l, m, n)$ de $\tilde{\Delta}(l, m, n)$ composé des transformations préservant l'orientation est un sous-groupe d'indice 2 dans $\tilde{\Delta}(l, m, n)$. Abstraitement, il est composé de tous les mots de longueurs paires et il admet la présentation :

$$\langle A, B \mid A^n = (AB)^m = B^l = 1 \rangle$$

Son domaine fondamental est une réunion de deux triangles fondamentaux de $\tilde{\Delta}(l, m, n)$ qui ne sont pas l'image l'un de l'autre par un élément de $T(l, m, n)$.

DEMO Il est clair que h est un mot de longueur paire si et seulement si $\pi(h)$ est une transformation préservant l'orientation. En posant $A = LM$ et $B = MN$ on obtient bien que tous les mots de longueurs paires puisque :

$$LM = A \quad LN = AB \quad MN = B \quad ML = (LM)^{-1} = A^{-1}$$

$$NL = (LN)^{-1} = (AB)^{-1} = B^{-1}A^{-1} \quad NM = (MN)^{-1} = B^{-1}$$

En outre les relations sont vérifiées puisque $A = LM$ donc $A^n = (LM)^n = 1$, $B = MN$ donc $B^l = (MN)^l = 1$ et $LN = AB$ d'où $(AB)^m = (LN)^m = 1$ et ce sont là toutes les relations possibles pour des mots de longueurs paires.

Le fait que le domaine fondamental soit la réunion de deux triangles non-conjugués découle du lemme précédent.

∩

Théorème d'Hurwitz

Dans ce chapitre nous allons prouver le théorème d'Hurwitz qui dit que toute surface hyperbolique compacte de genre $g \geq 2$ ne peut avoir plus de $84 \cdot (g - 1)$ isométries. Nous allons donc étudier l'ensemble des surfaces hyperboliques; pour ce, il convient de définir ce dont il s'agit et de citer les théorèmes que nous accepterons sans preuve.

Définition

Soit S un espace topologique et $(U_i, \varphi_i)_{i \in I}$ une famille de couples tels que U_i est un ouvert de S , φ_i est un homéomorphisme de U_i sur un ouvert $\varphi_i(U_i)$ de \mathbb{D}^2 . Supposons en outre que:

- (i) $(U_i)_{i \in I}$ est un recouvrement de S .
- (ii) Si $U_i \cap U_j \neq \emptyset$ alors $(\varphi_i|_{U_i \cap U_j}) \circ (\varphi_j|_{U_i \cap U_j})^{-1}$ est la restriction à $\varphi_j(U_i \cap U_j)$ d'une isométrie préservant l'orientation de \mathbb{D}^2 .

On appellera alors $(U_i, \varphi_i)_{i \in I}$ un atlas hyperbolique de S , par suite, S munie de cet atlas, sera appelée une surface hyperbolique.

Un sous-groupe F de l'ensemble \mathcal{M}^+ des transformations de Möbius préservant l'orientation de \mathbb{D}^2 est appelé un groupe fuchsien si F est discontinu et est finiment engendré.

Théorème Soit S une surface hyperbolique alors le revêtement universel de S est isométrique à \mathbb{D}^2 . Ce qui revient à dire que S est le quotient de \mathbb{D}^2 par un groupe d'isométries de \mathbb{D}^2 agissant librement et discontinûment sur \mathbb{D}^2 .

Corollaire Soit S une surface hyperbolique compacte alors la surface est de genre deux au moins et le groupe des transformations de revêtement du revêtement universel de S est un groupe fuchsien.

DEMO En effet, le groupe des transformations de revêtement d'un revêtement universel est isomorphe au groupe fondamental de S . Or le groupe fondamental d'une surface compacte est finiment engendré. De plus la surface est forcément orientée, sinon le groupe des transformations de revêtement contiendrait une isométrie de \mathbb{D}^2 qui renverserait son orientation; et les seules telles isométries sont les réflexions autour des droites hyperboliques qui fixent les points des droites; l'action des transformations de revêtement ne serait donc pas libre et la surface ne serait pas lisse partout. Donc S est orientée et les transformations de revêtement préservent toutes l'orientation. Elles forment donc un groupe fuchsien.



Théorème de Fricke

Soit F un groupe fuchsien alors il existe un n -uplet (e_1, \dots, e_n) d'entiers ≥ 2 tels que $n > 2$ (éventuellement ∞ et un entier $g \geq 0$ et un ensemble $n + 2g$ générateurs de F $\{c_1, \dots, c_n, a_1, \dots, a_g, b_1, \dots, b_g\}$ (ou $\{c_1, \dots, c_n\}$ si $g = 0$) en sorte que F admet la présentation :

$$\langle c_1, \dots, c_n, a_1, \dots, a_g, b_1, \dots, b_g | c_1^{e_1} = \dots = c_n^{e_n} = (c_1 \dots c_n)(a_1 b_1 a_1^{-1} b_1^{-1} \dots a_g b_g a_g^{-1} b_g^{-1}) = 1 \rangle$$

Où les a_i et b_i sont des hyperboliques, les c_i sont paraboliques ou elliptiques et l'entier g est le genre de la surface quotient (surface topologique seulement). De plus le domaine fondamental de F est d'aire :

$$2\pi\mu(F) = 2\pi \cdot \left(n + 2 \cdot (g - 1) - \sum_{i=1}^n \frac{1}{e_i} \right)$$

Afin de prouver le théorème d'Hurwitz, nous allons montrer que le groupe triangulaire $T(2, 3, 7)$ est le groupe Fuchsien possédant la plus petite aire du domaine fondamental. Pour cela, on considère tous les couples $((e_1, \dots, e_n), g)$ la fonction $\mu(F)$ décrite ci-dessous. La preuve donnée ci-dessous est inspirée du livre [Burnside (1955), N° 290].

Il faudra ensuite montrer que tout groupe d'isométrie d'une surface de genre $g \geq 2$ n'admet qu'un nombre fini d'isométries, pour cela on se basera sur un extrait du livre [Zieschang (1981), pp 41-42].

Lemme

Parmi tous les couples $((e_1, \dots, e_n), g)$ avec e_1, \dots, e_n des entiers ≥ 2 (éventuellement ∞) et g un entier ≥ 0 , la fonction

$$\mu((e_1, \dots, e_n), g) = n + 2 \cdot (g - 1) - \sum_{i=1}^n \frac{1}{e_i}$$

Atteint son minimum strictement positif avec $\mu((2, 3, 7), 0) = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{7} = \frac{1}{42}$ et lui seul.

DEMO Puisque l'ordre des e_i n'importe pas, on peut les supposer écrits dans un ordre croissant, cela nous facilitera la mise en cas. De plus, on remarque que pour $((e_1, \dots, e_n), g)$ et $((d_1, \dots, d_n), g)$ avec $e_k \geq d_k$ pour un k alors $e_j \geq d_j$ et donc $-\frac{1}{e_j} \geq -\frac{1}{d_j}$ pour $j \geq k$ alors :

$$\mu((e_1, \dots, e_n), g) = n + 2 \cdot (g - 1) - \sum_{i=1}^{k-1} \frac{1}{e_i} - \sum_{i=k}^n \frac{1}{e_i} \geq n + 2 \cdot (g - 1) - \sum_{i=1}^n \frac{1}{d_i} = \mu((d_1, \dots, d_n), g)$$

Observons alors que, si $g \geq 2$ on a, puisque $e_i \geq 2$, que :

$$\mu((e_1, \dots, e_n), g) \geq \mu((2, \dots, 2), g) = n + 2 - \frac{n}{2} = 2 + \frac{n}{2} \geq 2$$

De même, on observe que, si $g = 1$, on a $\mu((e_1, \dots, e_n), g) \geq n - \frac{n}{2} = \frac{n}{2}$ qui vaut 0 si $n = 0$, et est $\geq \frac{1}{2}$ si $n \neq 0$.

Ainsi, s'il existe un minimum strictement positif de μ il est tel que $g = 0$. Dans ce cas, $\mu((2, \dots, 2), 0) = n - 2 - \frac{n}{2} = \frac{n}{2} - 2$

Si $n \geq 5$ alors on a que $\mu((e_1, \dots, e_n), 0) \geq \mu((2, \dots, 2), 0) = \frac{n}{2} - 2 \geq \frac{5}{2} - 2 = \frac{1}{2}$.

Si $n = 4$ on a que $\mu((2, 2, 2, 2), 0) = \frac{n}{2} - 2 = 0$ et que $\mu((2, 2, 2, 3), 0) = \frac{1}{6}$.

Ainsi, puisque toutes les bornes obtenues sont supérieures à $\mu((2, 3, 7), 0)$, un minimum strictement positif de μ n'est possible que sur un couple du type $((e_1, e_2, e_3), 0)$ et dans ce cas :

$$\mu((e_1, e_2, e_3), 0) = 3 - 2 - \frac{1}{e_1} - \frac{1}{e_2} - \frac{1}{e_3} = 1 - \frac{1}{e_1} - \frac{1}{e_2} - \frac{1}{e_3}$$

En premier, on a toujours que $\mu((2, 2, k), 0) = 1 - \frac{1}{2} - \frac{1}{2} - \frac{1}{k} \leq -\frac{1}{k}$ qui est toujours négatif. Ainsi, si l'on a trouvé le plus petit k tel que $\mu((2, 3, k), 0)$ est strictement positif, on aura trouvé un minimum puisque $\forall ((e_1, e_2, e_3), 0)$ on a :

$$\mu((e_1, e_2, e_3), 0) > 0 \Rightarrow e_1 \geq 2 \text{ et } e_3 \geq e_2 \geq 3 \text{ donc } \mu((e_1, e_2, e_3), 0) \geq \mu((2, 3, e_3), 0) \geq \mu((2, 3, k), 0)$$

Le minimum est unique puisque l'égalité impliquerait que

$$1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{e_3} = \mu((2, 3, e_3), 0) = \mu((2, 3, k), 0) = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{e_3} \text{ i.e. } k = e_3$$

Elle implique, en outre que $1 - \frac{1}{e_1} - \frac{1}{e_2} - \frac{1}{e_3} = \mu((e_1, e_2, e_3), 0) = \mu((2, 3, e_3), 0) = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{e_3}$.

Ce qui revient à dire que $\frac{1}{e_1} = \frac{5}{6} - \frac{1}{e_2} = \frac{5e_2 - 6}{6e_2}$ d'où $e_1 = \frac{6e_2}{5e_2 - 6}$, Mais $x \mapsto f(x) = \frac{6x}{5x - 6}$ est

décroissante et $f(3) = \frac{18}{15-6} = 2$ donc $e_2 > 3 \Rightarrow e_3 < 2$. Alors on a forcément $e_2 \leq 3$ ainsi, puisque e_2 ne peut être 2, d'où $e_2 = 3$ et $e_1 = f(e_2) = 2$.

On vient donc de montrer que si k est le plus petit entier tel que $\mu((2, 3, k), 0)$ est positif, alors $\mu((2, 3, k), 0)$ est le minimum strictement positif des $\mu((e_1, e_2, e_3), 0)$ et que si $\mu((e_1, e_2, e_3), 0)$ est cette valeur minimum alors $(e_1, e_2, e_3) = (2, 3, k)$. Donc $\mu((2, 3, k), 0)$ est l'unique minimum strictement positif de $\mu((e_1, e_2, e_3), 0)$

Il reste à trouver k , on a que:

$$\begin{aligned} \mu((2, 3, 3), 0) &= 1 - \frac{7}{6} < 0 & \mu((2, 3, 4), 0) &= 1 - \frac{13}{12} < 0 & \mu((2, 3, 5), 0) &= 1 - \frac{31}{30} < 0 \\ \mu((2, 3, 6), 0) &= 1 - \frac{6}{6} = 0 & \mu((2, 3, 7), 0) &= 1 - \frac{21+14+6}{42} = \frac{1}{42} \end{aligned}$$

Ainsi $\mu((2, 3, 7), 0) = \frac{1}{42}$ est le minimum des $\mu((e_1, e_2, e_3), 0)$ et donc, puisque les bornes de trouvées pour les autres cas que $g = 0$ et $n = 3$

☐

Corollaire

Le groupe triangulaire $T(2, 3, 7)$ est le groupe fuchsien ayant la plus petite aire du domaine fondamental, $\frac{2\pi}{42} = \frac{\pi}{21}$. De plus, si F est un groupe fuchsien qui a la même aire du domaine fondamental, alors, en vertu de l'unicité du minimum démontrée ci-dessus, la signature de F est la même que celle de $T(2, 3, 7)$ et donc (Fricke) F est isomorphe à $T(2, 3, 7)$.

CLAIR

Lemme

Dans un espace métrique quelconque X , soient $\{s_i | i \in \mathbb{N}\}$ une suite d'isométries de X dans X et $x \neq y \in X$ tels que $s_n(x) \xrightarrow{n \rightarrow \infty} y$

Alors il existe une sous-suite $\{s_{k_i} | i \in \mathbb{N}\}$ des s_i telle que:

$$s_{k_n}^{-1} \circ s_{k_{n+1}}(x) \text{ et } (s_{k_n}^{-1} \circ s_{k_{n+1}})^{-1}(x) \xrightarrow{n \rightarrow \infty} x$$

. De plus, s'il existe point p de X telle que $s_n(p) \xrightarrow{n \rightarrow \infty} p$, alors on a toujours $s_{k_n}^{-1} \circ s_{k_{n+1}}(p)$ et $(s_{k_n}^{-1} \circ s_{k_{n+1}})^{-1}(p) \xrightarrow{n \rightarrow \infty} p$.

DEMO Appellons d la fonction de distance de cet espace X . On pose $k_1 = 1$ et l'on construit la suite des k_i par induction: une fois k_i construit, soit $\varepsilon_i = \frac{1}{i+1}$. Alors on peut trouver, en vertu de la convergence, $N_i > k_i$ tel que $k > N_i \Rightarrow d(y, s_{k_{i+1}}(x)) < \varepsilon_i$. On aura alors que:

$$d(x, s_{k_i}^{-1} \circ s_{k_{i+1}}(x)) = d(x, s_{k_{i+1}}^{-1} \circ s_{k_i}(x)) = d(s_{k_i}(x), s_{k_{i+1}}(x)) \leq d(s_{k_{i+1}}(x), y) + d(s_{k_i}(x), y) < \frac{1}{i} + \frac{1}{i+1} = \frac{2i+1}{i^2+i}$$

Puisque cette fonction tend vers 0 lorsque i tend vers ∞ , la suite $s_{k_i}^{-1} \circ s_{k_{i+1}}(x)$ converge vers x .

Enfin, si la suite $s_i(p)$ converge vers p , on a pour tout $\varepsilon > 0$ qu'il existe un $N \in \mathbb{N}$ tel que:

$\forall j > N$ $d(p, s_{k_j}(p)) < \frac{\varepsilon}{2}$ alors:

$$d(p, s_{k_{i+1}}^{-1} \circ s_{k_i}(p)) = d(p, s_{k_i}^{-1} \circ s_{k_{i+1}}(p)) = d(s_{k_i}(p), s_{k_{i+1}}(p)) \leq d(s_{k_i}(p), p) + d(s_{k_{i+1}}(p), p) < \varepsilon$$

D'où la convergence de $s_{k_n}^{-1} \circ s_{k_{n+1}}(p)$ et $(s_{k_n}^{-1} \circ s_{k_{n+1}})^{-1}(p)$ vers p .

☐

Lemme

Soit G un groupe fuchsien dont la surface quotient est compacte et soit H un groupe d'isométries de \mathbb{D}^2 telle que $G \triangleleft H$ alors G est d'indice fini dans H et donc, H est fuchsien.

DEMO Appellons D le domaine fondamental de G qui est compact puisque la surface \mathbb{D}^2/G l'est. De plus, puisque le quotient de \mathbb{D}^2 de G est compact, il est donc une surface de genre ≥ 2 alors, par le théorème de Fricke, G contient au moins deux éléments hyperboliques, disons r et s . Choisissons un point x dans l'intérieur de D et une boule B entièrement contenue dans l'intérieur de D . Supposons que G n'est pas d'indice fini dans H alors on peut trouver une suite a_i d'isométries de H telles que $Ga_i \cap Ga_j = \emptyset \quad \forall i \neq j$. Puisque D est un domaine fondamental de G , je peux

pour chaque i , trouver une isométrie g_i telle que $g_i \circ a_i(x) \in D$. Or D est compact, il existe donc une sous-suite $g_{k_i} \circ a_{k_i}(x)$ convergeant vers un point x_0 de \bar{D} .

Alors soit il y a une sous-suite h_j de la suite des $g_{k_i} \circ a_{k_i}$ telle que $h_j(x) = x_0$ pour les $j > N$, alors la suite $h_j^i \circ h_{j+1}(x)$ tend vers x . Soit il y a une infinité de j tels que $g_{k_i} \circ a_{k_i}(x) \neq x_0$. Le lemme précédent nous donne alors une sous-suite h_j de la suite des $g_{k_i} \circ a_{k_i}$ telle que $h_j^i \circ h_{j+1}(x)$ tend vers x . De plus il est clair que $Gg_i \circ a_i = Ga_i \cap Ga_j = Gg_j \circ a_j \quad \forall i, j$, en particulier $Gh_i \cap Gh_j = \emptyset \quad \forall i, j$ ce qui revient à $h_j^i \circ h_{j+1}G \cap G = \emptyset$ donc $h_j^i \circ h_{j+1} \neq Id$.

Prenons alors r une transformation hyperbolique de G et soit $y = r(x)$. Puisque l'on a pour tout j $d(h_j^i \circ h_{j+1}(x), h_j^i \circ h_{j+1}(y)) = d(x, y)$, et puisque la suite des $h_j^i \circ h_{j+1}(x)$ reste dans un compact, la suite des $h_j^i \circ h_{j+1}(y)$ reste dans un compact et donc on peut extraire une sous-suite d'isométries $c_k = h_{j_k}^i \circ h_{j_k+1}$ telles que $c_k(y)$ converge vers un y_0 . Le lemme ci-dessus nous permet donc de donner l'existence d'une sous-suite $d_l = c_{k_l}$ telle que $d_l^i \circ d_{l+1}(y) \rightarrow y$ et $d_{l+1}^i \circ d_l(y) \rightarrow y$, de même que $d_l^i \circ d_{l+1}(x) \rightarrow x$ et $d_{l+1}^i \circ d_l(x) \rightarrow x$. Appelons $e_l = d_l^i \circ d_{l+1}$.

Prenons alors s , l'autre transformation hyperbolique des générateurs de G donnée par le théorème de Fricke. On pose $z = s(x)$. Par le même argument que précédemment, les $e_l(x)$ restent dans un compact et il existe une sous suite $f_m = e_{l_m}$ qui converge vers un point z_0 . Ainsi le lemme nous dit qu'il existe $g_n = f_{m_n}$ une sous-suite telle que $g_n^i \circ g_{n+1}$ fait tendre x vers x , $y = r(x)$ vers y et $z = s(x)$ vers z , de même que son inverse $g_{n+1}^i \circ g_n$.

On a clairement que $g_n^i \circ r \circ g_n$ fait converger x vers y et donc, il existe un $L \in \mathbb{N}$ tel que $\forall n > L$ les $g_n^i \circ r \circ g_n(x)$ sont dans $r(U)$ ouvert contenu dans l'intérieur de l'image par r de D . Puisque $G \triangleleft H$ et que D est un domaine fondamental, on peut dire que $g_n^i \circ r \circ g_n = g$. D'où les g_n sont hyperbolique le long du même axe que r , pour $n > L$.

De même, on a clairement que $g_n^i \circ s \circ g_n$ fait converger x vers z , les mêmes arguments nous amènent à dire qu'il existe un $N > L$ tel que $\forall n > N$ on a que $g_n^i \circ s \circ g_n = s$. D'où les g_n sont hyperbolique le long du même axe que s .

Mais les axes de s et r sont distincts sinon G contiendrait le conjugué d'un groupe d'homothétie de la forme $\{z \mapsto a^p \cdot b^q | p, q \in \mathbb{Z}\}$ où a et b sont deux réels distincts. Or ce groupe n'est pas du tout discontinu. Absurdité !

Donc G est d'indice fini dans H et donc H est également finiment engendré, c'est donc un groupe fuchsien.

□

Théorème d'Hurwitz

Soit S une surface hyperbolique comacte de genre g alors le groupe des isométries de S ne peut avoir plus de $84 \cdot (g - 1)$ isométries. Et ce maximum est atteint si et seulement si le groupe des isométries est un quotient fini de $T(2, 3, 7)$. On parlera alors de groupe d'Hurwitz.

DEMO Puisque S est une surface hyperbolique compacte, on sait par le corollaire premier qu'elle est le quotient de \mathbb{D}^2 par l'action d'un groupe fuchsien Γ . On sait par le chapitre précédent que le groupe $Iso(S)$ des isométries de S est alors isomorphe à $N(\Gamma)/\Gamma$. Le lemme précédent nous dit que puisque $N(\Gamma) \triangleright \Gamma$, le groupe Γ est d'indice fini dans $N(\Gamma)$ donc que $N(\Gamma)/\Gamma$ est fini.

Ce lemme nous dit aussi que $N(\Gamma)$ est un groupe fuchsien, il admet donc un domaine fondamental D . Son aire est donnée par le théorème de Fricke. Le dernier corollaire montré nous donne alors que cette aire ne peut pas être inférieure à $\frac{\pi}{21}$. Avec égalité si et seulement si la signature de $N(\Gamma)$ est la même que celle de $T(2, 3, 7)$, or deux groupes sont isomorphes s'ils ont même signature, on a donc égalité des aires si et seulement si $N(\Gamma)$ est $T(2, 3, 7)$.

De l'autre côté, l'aire du domaine fondamental de Γ est exactement l'aire de S ; Gauss-Bonnet nous donne l'aire de S en fonction de son genre: $Aire(S) = 4\pi \cdot (g - 1)$.

En résumé, on a $Aire(S) \geq \pi \frac{42}{42}$ avec égalité $\Leftrightarrow N(\Gamma) \approx T(2, 3, 7)$ et donc:

$$Card(Iso(S)) = [\Gamma : N(\Gamma)] = \frac{Aire(S)}{Aire(D)} \leq \frac{4\pi \cdot (g - 1)}{\frac{\pi}{21}} = 84 \cdot (g - 1)$$

$\mathrm{PSL}_2(\mathbb{F}_7)$ est un groupe d'Hurwitz

Le but de ce chapitre final est de montrer un groupe d'Hurwitz. C'est $\mathrm{PSL}_2(\mathbb{F}_7)$ que nous allons réaliser comme groupe d'Hurwitz. On rappelle, du chapitre 3 que l'on a que $\mathrm{PSL}_2(\mathbb{F}_7)$ admet la présentation :

$$\mathrm{PSL}_2(\mathbb{F}_7) \cong \langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = (\tau^3\iota)^4 = 1 \rangle$$

On a, dès lors un morphisme surjectif ρ du groupe libre $\langle \tau, \iota \rangle$ vers $\mathrm{PSL}_2(\mathbb{F}_7)$ qui fait que $\mathrm{PSL}_2(\mathbb{F}_7)$ est le quotient du groupe libre par le plus petit sous-groupe normal contenant les relatateurs.

Or on a vu au chapitre des groupes triangulaires qu'un groupe $T(l, m, n)$ admet une présentation :

$$T(l, m, n) \cong \langle A, B \mid A^n = (AB)^m = B^l = 1 \rangle$$

En particulier le groupe $T(2, 3, 7)$ admet la présentation :

$$\langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = 1 \rangle$$

On obtient donc un morphisme surjectif $\pi: T(2, 3, 7) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_7)$. Appelons Γ le noyau de ce morphisme. Alors $T(2, 3, 7)/\Gamma$ est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$. Puisque Γ est inclu dans le groupe fuchsien $T(2, 3, 7)$, il est clair que Γ est fuchsien lui même. On commence par montrer que Γ agit sans points fixes et qu'il est de domaine fondamental compact. Le quotient de \mathbb{D}^2 par Γ est alors une surface hyperbolique compacte. On montrera alors que $\mathrm{PSL}_2(\mathbb{F}_7)$ est exactement le groupe des isométries de cette surface.

Proposition

Γ agit librement sur \mathbb{D}^2 .

DEMO La preuve s'appuie sur le lemme suivant qui est extrait de Magnus (*Non-Euclidean Tessalations and their Groups, Theorem 2.10*) :

Lemme

Tout élément d'ordre fini d'un $T(l, m, n)$ est le conjugué d'une des puissances de τ, ι ou $\tau\iota$.

DEMO Supposons qu'il existe une transformation ϕ non-triviale d'ordre fini dans $T(l, m, n)$. Puisque ϕ est une transformation de Möbius, elle a exactement un point fixe p .

Or, si Q est le nom du quadrilatère fondamental de $T(l, m, n)$, il existe une tranformation $\psi \in T(l, m, n)$ qui amène p dans \overline{Q} . Mais alors $\theta = \psi \circ \phi \circ \psi^{-1}$ fixe $r = \psi(p)$.

Supposons que r est à l'intérieur de Q , alors celui-ci contiendrait un point et son image par une transformation non triviale de $T(l, m, n)$. Absurdité ! Donc r est dans le bord de Q et θ applique Q sur un des quadrilatères ayant un sommet en commun avec Q . Mais il n'y qu'une telle transformation, donc θ doit être une des puissances des "rotations" autour d'un sommet, c'est-à-dire être $\tau, \iota, \tau\iota$ ou $\iota\tau = \tau^{-1}(\tau\iota)\tau$. On a donc que ϕ est conjuguée par ψ à l'une des puissances de τ, ι ou $\tau\iota$.

□

Remarquons, ensuite, que, par la projection de quotient $\pi: T(2, 3, 7) \twoheadrightarrow G$, les éléments τ, ι et $\tau\iota$ sont envoyés sur des éléments de même ordre : on a montré dans le lemme machinal que $\pi(\tau)$ et $\pi(\iota)$ ne sont pas triviaux, sachant que $\pi(\tau)^7 = \pi(\iota)^2 = 1$ et que 2 et 7 sont des premiers, on ne peut que conclure que leurs ordres respectifs sont bien 7 et 2. Enfin, $\pi(\tau\iota)$ est d'un ordre divisant 3, donc soit 1, soit 3. Mais $\pi(\tau\iota)$ n'est pas d'ordre 1 car sinon $\pi(\tau) = \pi(\iota)^{-1} = \pi(\iota)$ et donc $1 = \pi(\tau)^7 = \pi(\iota)^7 = \pi(\iota)$ ainsi G serait trivial. Absurdité !

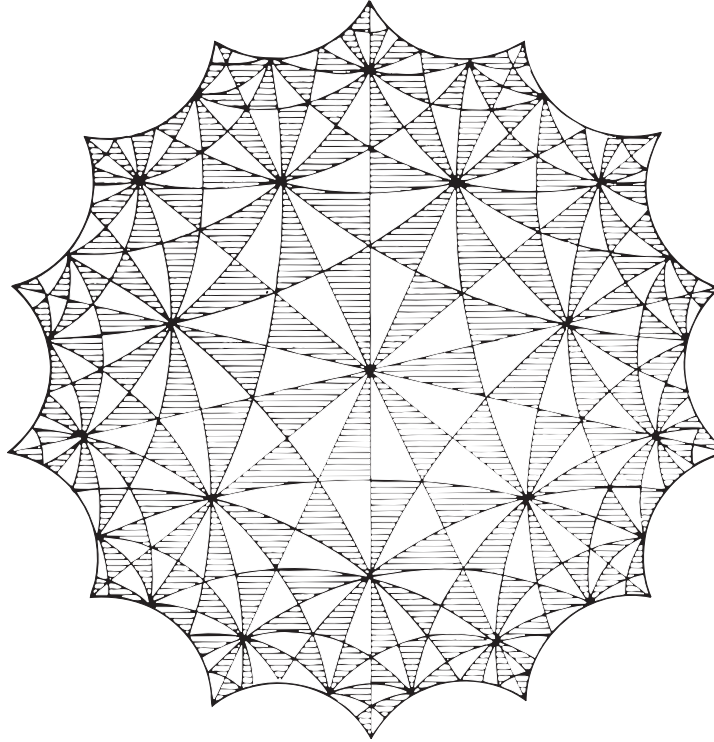
Puisque ces ordres sont des premiers, cette propriété d'être envoyé sur un élément du même ordre s'étend aux puissances de τ , ι ou $\tau\iota$, et donc aussi à leurs conjugués. Ainsi donc, si ϕ est un élément d'ordre fini de $T(2, 3, 7)$, il est envoyé par π sur un élément du même ordre.

Or tout élément de Γ est envoyé par π sur 1, élément d'ordre 1, donc les éléments de Γ ne sont pas d'ordre fini, ils n'ont ainsi pas de point fixe.

□

Corollaire L'espace topologique $S = \mathbb{D}^2/\Gamma$ est une surface et la projection $\Pi: \mathbb{D}^2 \longrightarrow \mathbb{D}^2/\Gamma$ est un revêtement universel de S .

C L A I R



Domaine fondamental

Γ est d'indice fini $n = 168$, on peut donc trouver une famille finie $Tr = \{\alpha_1, \dots, \alpha_n\} \subset T(2, 3, 7)$ contenant un unique représentant de chaque classe modulo Γ (une transversale de Schreier). Alors si Q est le quadrilatère fondamental de $T(2, 3, 7)$, l'ensemble :

$$O = \cup_{i=1}^n \alpha_i(\bar{Q})$$

est un domaine fondamental pour Γ . Une réalisation sympathique de celui-ci est donnée dans la ci-contre extraite de [Klein et Fricke, 1890, p. 370].

DEMO On montre que les images de O par l'action de Γ remplissent \mathbb{D}^2 sans se chevaucher :

Remplissage : soit un point $p \in \mathbb{D}^2$ alors (quadrilatère fondamental) il existe $\psi \in T(2, 3, 7)$ en sorte que $\psi(\bar{Q}) \ni p$. Mais alors (transversale) je peux trouver $\alpha_i \in Tr$ et $\gamma \in \Gamma$ telles que $\psi = \gamma \circ \alpha_i$ et donc $p \in \psi(\bar{Q}) = \gamma(\alpha_i(\bar{Q})) \subset \gamma(O)$.

Non-chevauchement : Soit $p \in \nu(O) \cap \mu(O)$ alors je peut trouver α_i et $\alpha_j \in Tr$ en sorte que $p \in \mu \circ \alpha_i(\bar{Q}) \cap \nu \circ \alpha_j(\bar{Q})$.

(i) $p \in \text{Int}(\mu \circ \alpha_i(\bar{Q})) \Rightarrow \mu = \nu$

En effet, on a sous cette hypothèse : $\alpha_i^1 \circ \mu^1(p) \in \text{Int}(\bar{Q})$, appelons r ce point ; de plus $\alpha_j^1 \circ \nu^1(p) \in \bar{Q}$. Alors $\alpha_j^1 \circ \nu^1 \circ \mu \alpha_i : r \in \text{Int}(\bar{Q}) \mapsto \alpha_i^1 \circ \nu^1(p) \in \bar{Q}$ donc cette transformation, qui est dans $T(2, 3, 7)$ envoie un point de l'intérieur du domaine fondamental vers un point du domaine fondamental, elle est donc forcément égale à l'identité. Et alors :

$$\alpha_j^1 \circ \nu^1 \circ \mu \circ \alpha_i = 1 \iff \alpha_j^1 \circ \alpha_i = \nu^1 \circ \mu \in \Gamma \Rightarrow \alpha_i = \alpha_j \Rightarrow \nu^1 \circ \mu = 1 \Rightarrow \nu = \mu$$

(ii) $\nu \neq \mu$ alors $p \in \partial O$

En vertu de (i), $p \in \partial(\mu \circ \alpha_i(\bar{Q}))$ et $p \in \partial(\nu \circ \alpha_j(\bar{Q}))$.

Primo, chaque voisinage de p contient p qui est un point de $\mu \circ \alpha_i(\bar{Q}) \subset \mu(O)$.

Et puisque $p \in \partial(\nu \circ \alpha_j(\bar{Q}))$, chaque voisinage de p contient un point de $\text{Int}(\nu \circ \alpha_j(\bar{Q}))$.

Mais un tel point n'est pas dans $\mu(O)$ puisque $\mu \neq \nu$ et puisque nous avons montré en (i) qu'un point de l'intérieur d'un quadrilatère ne pouvait appartenir qu'à une seule image de O . En résumé, chaque voisinage de p contient un point de $\mu(O)$ et un point qui n'est pas dans $\mu(O)$ donc p est dans le bord de $\mu(O)$.

□

Compacité

On a donc trouvé un domaine O qui est une réunion finie de compacts et qui, en image par la projection $\Pi: \mathbb{D}^2 \longrightarrow S$ est tout S donc notre surface est compacte. En outre, elle est orientable puisque $\Gamma \subset \mathcal{M}^+$.

C L A I R

Corollaire

Puisque Γ est exactement d'indice 168 dans $T(2, 3, 7)$, le domaine fondamental O obtenu dans la proposition contient 168 quadrilatères distincts et donc S est d'aire 168 fois l'aire d'un quadrilatère. Or, selon la description $T(2, 3, 7)$ ce quadrilatère est la réunion de deux triangles ayant chacun les angles au sommet $\frac{\pi}{2}$, $\frac{\pi}{3}$ et $\frac{\pi}{7}$. On obtient donc :

$$\text{Aire}(S) = 168 \cdot \text{Aire}(\bar{Q}) = 168 \cdot 2 \cdot (\pi - \frac{\pi}{2} - \frac{\pi}{3} - \frac{\pi}{7}) = 168 \cdot 2 \cdot (\frac{42\pi - 21\pi - 14\pi - 6\pi}{42}) = 168 \cdot 2 \cdot \frac{\pi}{42} = \frac{168 \cdot \pi}{21} = 8 \cdot \pi$$

Gauss-Bonnet nous permet alors de calculer le genre de cette surface :

$$4 \cdot \pi \cdot (g - 1) = \text{Aire}(S) = 8 \cdot \pi \text{ d'où } g - 1 = 2 \text{ i.e. } g = 3$$

C L A I R

Final

On se rappelle, par le paragraphe sur les isométries d'un quotient que l'on a $\text{Iso}(S) \cong N(\Gamma)/\Gamma$ où $N(\Gamma)$ est le normalisateur de Γ dans \mathcal{M}^\pm . Or Γ est un noyau de morphisme, donc il est normal dans $T(2, 3, 7)$ ce qui veut dire que $T(2, 3, 7) \subset N(\Gamma)$. Ainsi $\text{PSL}_2(\mathbb{F}_7)$ s'injecte dans $N(\Gamma)/\Gamma = \text{Iso}(S)$

D'autre part on sait depuis le chapitre 3, que $\text{PSL}_2(\mathbb{F}_7)$ a exactement 168 éléments. Enfin, le théorème d'Hurwitz nous affirme que $N(\Gamma)/\Gamma = \text{Iso}(S)$ n'a pas plus de $84 \cdot (g - 1) = 168$ isométries.

On peut donc conclure que $\text{Iso}(S) = N(\Gamma)/\Gamma$ a exactement 168 isométries et que l'injection $\text{PSL}_2(\mathbb{F}_7) \hookrightarrow N(\Gamma)/\Gamma$ est un isomorphisme de groupe, ainsi, par Hurwitz encore, $\text{Iso}(S)$ est un quotient de $T(2, 3, 7)$, ce qui revient à dire que $N(\Gamma) = T(2, 3, 7)$.

On a donc réalisé $\text{PSL}_2(\mathbb{F}_7)$ comme groupe d'Hurwitz puisque son ordre atteint la borne du théorème d'Hurwitz.

Réalisation

Le propos de ce chapitre est d'utiliser ce que nous avons construit pour réaliser matériellement la surface de genre 3 et le pavage que nous avons décrit au chapitre précédent. Nous avons dit au chapitre des Graphes de Cayley que de tels graphes permettaient de donner une "idée géométrique" du groupe, nous allons justement établir un lien entre le graphe de Cayley d'un groupe agissant par isométries sur une variété riemannienne et le pavage que ce groupe forme par déplacement de son domaine fondamental.

Les conclusions obtenues apparaissent comme des banalités dans la tête de tout un chacun, nous avons préféré les démontrer tout de même puisque nous les utiliserons ensuite pour notre réalisation.

Cadre

Soit S une surface de Riemann connexe et, appelons polygone de S tout ensemble qui est l'adhérence d'un ouvert non vide et dont le bord est une réunion de segments géodésiques, on appellera alors sommet de ce polygone toute intersection de deux segments et côté de ce polygone, un segment géodésique joignant un sommet à une autre.

Soit alors $G < Iso(S)$ admettant un polygone d qui n'a qu'un nombre fini de sommets (et donc de côtés) comme domaine fondamental.

- on appellera pavage, et on notera \mathcal{P} l'ensemble des images de d par les éléments de G , une image sera appelée un pavé.
- on dira d'une isométrie g de G qu'elle est une transformation vicinale si d et $g(d)$ sont des pavés voisins, c'est-à-dire si $d \cap g(d)$ est un côté commun des polygones d et $g(d)$.

Remarquons que $V^{-1} = V$ puisque si $g \in V$ alors $d \cap g(d)$ est un côté des polygones d et $g(d)$ alors $g^{-1}(d \cap g(d)) = g^{-1}(d) \cap d = d \cap g^{-1}(d)$ qui est un côté des polygones $g^{-1}(d)$ et d donc g^{-1} est une transformation vicinale.

Lemme On a une bijection $b: \mathcal{P} \longrightarrow G$ caractérisée par $b(p)(d) = p \quad \forall p \in \mathcal{P}$

DEMO Par définition, d est tel que $\forall x \in S \circ g \in G$ tel que $g^{-1}(x) \in d$ et tel que $g(d) \cap d \subset \partial d$ si $g \neq Id_S$.

Posons $c: G \longrightarrow \mathcal{P}$ qui envoie $g \longmapsto g(d)$. Puisque \mathcal{P} est définie comme l'ensemble des images de d par les éléments de G , on peut dire que c est surjective.

Injection: si $g(d) = h(d)$ alors $g(Int(d)) = h(Int(d))$ et donc $g \circ h^{-1}(Int(d)) \cap Int(d) \neq \emptyset$ d'où $gh^{-1} = Id_S$ i.e. $g = h$.

Donc c est bijective, on pose alors $b = c^{-1}$ qui est bien une bijection.

□

Proposition L'ensemble V des transformations vicinales engendre le groupe G .

DEMO Puisque l'ensemble des sommets des pavés forme un ensemble fermé discret, son complémentaire est un ouvert connexe.

Soit $g \in G$ et $p = b^{-1}(g)$, prenons $x \in Int(p)$. Nous pouvons alors joindre x à $g^{-1}(x)$ par un chemin γ n'intersectant aucun sommet. Donc γ n'intersectera que des intérieurs de pavés et des côtés.

Appelons p_1, \dots, p_m la suite des pavés que le chemin croise. S'il n'y en a qu'un alors $p = d$ et donc $g = Id_S$.

Dans les autres cas, appelons g_i la transformation $b(p_{i+1}) \circ b(p_i)^{-1}$ pour $i = 1, \dots, m-1$. Alors $g_i(p_i) = b(p_{i+1}) \circ b(p_i)^{-1}(p_i) = b(p_{i+1})(d) = p_{i+1}$. Donc g_i apporte p_i sur p_{i+1} or p_i est voisin de p_{i+1} puisque γ ne peut rencontrer que le côté commun en passant de p_i à p_{i+1} , appelons-le c . On a donc :

$$g_i(p_i) \cap p_i = c \implies b(p_i)^{-1} \circ g_i(p_i) \cap b(p_i)^{-1}(p_i) = b(p_i)^{-1}(c) \implies b(p_i)^{-1} \circ g_i \circ b(p_i)(d) \cap d = b(p_i)^{-1}(c)$$

Alors $b(p_i)^{-1}(c)$ est un côté commun de d et de $b(p_i)^{-1} \circ g_i \circ b(p_i)(d)$ donc :

$$b(p_i)^{-1} \circ g_i \circ b(p_i) = b(p_i)^{-1} \circ b(p_{i+1}) \circ b(p_i)^{-1} \circ b(p_i) = b(p_i)^{-1} \circ b(p_{i+1})$$

est une transformation vicinale, appelons-la h_i ($i = 1, \dots, m-1$).

Il est clair que $p_m = d$, donc $b(p_1) = 1$, de même, il est clair que $p_m = p$ donc $b(p_m) = g$. De plus, on observe que, pour chaque $i \leq m-1$:

$$g_i \circ g_{i+1} = b(p_i)^{-1} \circ b(p_{i+1}) \circ b(p_{i+1})^{-1} \circ b(p_{i+2}) = b(p_i)^{-1} \circ b(p_{i+2})$$

Par conséquent $h_1 \circ \dots \circ h_{m-1} = b(p_1)^{-1} \circ b(p_m) = g$. On vient d'exprimer un élément quelconque g de G comme produit de transformations vicinales, ainsi l'ensemble des transformations vicinales engendre G .

☐

Définition

Étant donné le pavage \mathcal{P} , on définit le graphe de proximité du pavage \mathcal{P} , noté $R(\mathcal{P}, S)$, comme le graphe défini comme suit :

- \mathcal{P} est l'ensemble des sommets.
- L'ensemble $Vois(\mathcal{P})$ des arrêtes est l'ensemble $\{(p, q) \in \mathcal{P} \times \mathcal{P} \mid p \text{ est voisin de } q\}$
- L'incidence est : $\varepsilon_R(p, q) = (p, q)$ et l'inverse : $\iota_R(p, q) = (q, p)$ qui est bien une arrête puisque si p est voisin de q alors, par définition, q est voisin de p .

Proposition Le graphe de Cayley $C(G, V)$ est isomorphe à $R(\mathcal{P}, S)$.

DEMO La bijection des sommets est donnée par la bijection du pavage : $b: \mathcal{P} \longrightarrow G$.

L'application β des arrêtes se définit comme suit. Si $p \in \mathcal{P}$ est voisin de $q \in \mathcal{P}$ alors $b(p)^{-1}(p) = d$ est voisin de $b(p)^{-1}(q)$ donc il existe $v(p, q) \in V$ tel que $v(p, q)(d) = b(p)^{-1}(q)$ (en fait $v(p, q) = b(q)^{-1} \circ b(p)$). On pose alors :

$$\beta: (p, q) \longmapsto (b(p), v(p, q))$$

β est **injective** puisque $\beta(p, q) = (b(p), v(p, q)) = (b(p'), v(p', q')) = \beta(p', q')$ alors $p = p'$ et $b(q)^{-1} \circ b(p) = b(q')^{-1} \circ b(p')$ ainsi $b(q) = b(q')$ donc $q = q'$.

β est **surjective** : soit (g, v) une arête de $C(G, X)$ alors $g(d)$ et $g \circ v(d)$ sont deux pavés voisins puisque d et $v(d)$ le sont donc $(g(d), g \circ v(d))$ est une arrête du graphe de proximité, de plus :

$$\beta(g(d), g \circ v(d)) = (b(g(d)), v(g(d), g \circ v(d))) = (b(g(d)), b(g(d))^{-1} \circ b(g \circ v(d))) = (g, g^{-1} \circ g \circ v) = (g, v)$$

Il reste à vérifier que (b, β) est un morphisme de graphe : soit (p, q) une arrête et $(g, v) = \beta^{-1}(p, q)$ i.e. tel que $p = g(d)$ et $q = g \circ v(d)$ alors :

$$\alpha_C \circ \beta(p, q) = \alpha_C(g, v) = g = b(g(d)) = b \circ \alpha_R(g(d), g \circ v(d)) = b \circ \alpha_R(p, q)$$

$$\omega_C \circ \beta(p, q) = \omega_C(g, v) = g \circ v = b(g \circ v(d)) = b \circ \omega_p(g(d), g \circ v(d)) = b \circ \omega_p(p, q)$$

$$\begin{aligned} \iota_C \circ \beta(p, q) &= \iota_C(g, v) = (gv, v^{-1}) = (b(g \circ v(d)), b(g(d))^{-1} \circ b(g \circ v(d))) \\ &= (b(q), v(g \circ v(d), g(d))) = (b(q), v(q, p)) = \beta(q, p) = \beta \circ \iota_R(p, q) \end{aligned}$$

☐

Lemme

Soient E et B deux variétés riemanniennes avec E simplement connexe et soient $\Pi: E \rightarrow B$ un revêtement qui est une isométrie locale et G un groupe discontinu d'isométries de E admettant un domaine fondamental polygonal d et qui passe au quotient (i.e. tel que G est inclus dans le normalisateur du groupe Γ des transformations de revêtement).

Alors le pavage \mathcal{P} associé à d et G passe au quotient, c'est-à-dire que l'ensemble des images de chaque pavé par la projection de revêtement forme un pavage \mathcal{P}' de B associé au groupe G/Γ .

De plus toute transformation vicinale de G est envoyée sur une transformation vicinale de G/Γ .

DEMO On sait, depuis le chapitre sur les isométries d'un quotient que $Iso(S) \approx N(\Gamma)/\Gamma$ via le morphisme d'abaissement α (dont le noyau est Γ). Donc G/Γ est un groupe d'isométries de S . Pour montrer que le pavage passe au quotient, il faut montrer que $\{\Pi(p) \mid p \in \mathcal{P}\}$ est un pavage associé à $\alpha(G) = G/\Gamma$. Pour cela, montrons que $\Pi(d)$ est un domaine fondamental de $\alpha(G) = G/\Gamma$. Remarquons que l'on a :

$$\{\Pi(p) \mid p \in \mathcal{P}\} = \{\Pi \circ g(d) \mid g \in G\} = \{\alpha(g) \circ \Pi(d) \mid g \in G\} \stackrel{\alpha \text{ surjectif}}{=} \{h(\Pi(d)) \mid h \in \alpha(G)\}$$

Ainsi et grâce à la surjection de Π , il est clair que les images de $\Pi(d)$ recouvrent tout S .

Il reste à voir que $h \neq h' \in \alpha(G) \implies h(d) \cap h'(d) \subset \partial h(d)$.

Prenons $h \neq h' \in \alpha(G)$ en supposant que $x \in h(\Pi(d)) \cap h'(\Pi(d))$. Soit alors y tel que $\Pi(y) = x$. Alors on peut trouver $g \in \alpha^{-1}(h)$ tel que $g(d) \ni y$. En effet, si tel n'était pas le cas, on aurait pour chaque $g \in \alpha^{-1}(h)$ que $y \notin g$; or α est surjective, donc on peut trouver $\tilde{g} \in \alpha^{-1}(h)$ et, puisque $\ker \alpha = \Gamma$ on a que $\alpha^{-1}(h) = \Gamma \cdot \tilde{g}$. Ainsi, selon notre hypothèse, on aurait pour tout $\gamma \in \Gamma$ que $y \notin \gamma\tilde{g}(d)$ ou mieux, on aurait pour tout $\gamma, \delta \in \Gamma$ que $y \notin \delta^{-1}\gamma\tilde{g}(d)$ i.e. $\delta y \notin \gamma\tilde{g}(d)$. Alors on aurait que $x = \Pi(y) \notin \Pi \circ \tilde{g}(d) = \alpha(\tilde{g}) \circ \Pi(d) = h \circ \Pi(d)$ ce qui est absurde, on peut donc trouver un tel h . On fait exactement le même raisonnement pour obtenir g' dans $\alpha^{-1}(h')$ tel que $y \in g'(d)$. On obtient donc que $y \in g(d) \cap g'(d)$. Or $h \neq h'$ donc $g \neq g'$, ainsi $y \in \partial g(d)$. Par l'homéomorphisme local de Π autour de y on obtient que $y \in \Pi(\partial g(d)) = \partial h(\Pi(d))$.

On a donc montré que $\Pi(d)$ est un domaine fondamental de G/Γ et que l'ensemble des images par les isométries de G/Γ est le même ensemble que $\{\Pi(p) \mid p \in \mathcal{P}\}$. Observons, en outre que l'image d'une géodésique par Π est une géodésique puisque Π est une isométrie locale et que la propriété d'être une géodésique est une propriété métrique locale. Ainsi donc $\Pi(d)$ est un polygone et donc le pavage image par Π est bien le pavage de G/Γ .

Soit, enfin, $v \in G$ une transformation vicinale alors $v(d) \cap d$ est un segment géodésique ou est tout d . Considérons $\Pi(v(d) \cap d) = \alpha(v)(\Pi(d)) \cap \Pi(d)$. Si c'est tout d alors v est l'identité (domaine fondamental), sinon c'est l'image par Π d'un segment géodésique, c'est donc un segment géodésique. On conclut que $\alpha(v)$ est une transformation vicinale.

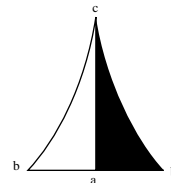
□

Dans notre cas

On se rappelle le chapitre *Groupes Triangulaires*: soit Δabc un triangle ayant angles $\frac{\pi}{2}$, $\frac{\pi}{3}$ et $\frac{\pi}{7}$ respectivement aux sommets a , b et c . Dans ce chapitre on a montré que le groupe triangulaire $T(2, 3, 7)$ était engendré (par exemple) par la rotation d'ordre 2 en a (appelons-la ι) et la rotation d'ordre 7 en c (appelons-la τ) et qu'il admettait la présentation :

$$T(2, 3, 7) \approx \langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = 1 \rangle$$

Dans ce même chapitre on a montré que la réunion du triangle Δabc et de son symétrique par la des réflexions le long d'un quelconque côté était un domaine fondamental de $T(2, 3, 7)$. Choisissons la réflexion le long de $[a, c]$ pour obtenir le triangle $\Delta' = \Delta ab'c$. La réunion de Δ et Δ' est alors encore un triangle, noté d , dont les côtés sont: $[b, b']$ (dont le support est le même que $[b, a]$), $[b, c]$ et $[b', c]$. On vérifie alors que τ et ι sont des transformations vicinales: en effet τ envoie le côté $[c, b]$ sur le côté $[c, b']$ puisque l'angle entre $[c, b]$ et $[c, a]$ est de $\frac{\pi}{7}$, ainsi τ^{-1} en est aussi une. De même ι est une rotation d'angle π donc $[b, b']$ est invariant par ι car le centre a est sur $[b, a]$. Ainsi donc τ et ι sont des transformations vicinales et donc le graphe de Cayley de $T(2, 3, 7)$ est le même que le graphe de proximité du pavage par la réunion de ces deux triangles.



Au chapitre précédent, on a construit une surface S quotient de \mathbb{D}^2 par un sous-groupe Γ de $T(2, 3, 7)$ qui est le plus petit sous-groupe normal de $T(2, 3, 7)$ contenant la transformation $(\tau^3\iota)^4$. On a également montré que le normalisateur de Γ dans $Iso^+(\mathbb{D}^2)$ était exactement $T(2, 3, 7)$. Notons $\Pi: \mathbb{D}^2 \longrightarrow S$, la projection de revêtement.

Lemme Ainsi $Iso^+(S) \approx T(2, 3, 7)/\Gamma$ via le morphisme d'abaissement $\alpha: T(2, 3, 7) \longrightarrow Iso^+(S)$. Appelons encore $\underline{\tau}$ et $\underline{\iota}$ les images de τ et ι par le morphisme d'abaissement. Alors $Iso^+(S)$ satisfait à la présentation:

$$\langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = (\tau^3\iota)^4 = 1 \rangle$$

et est donc isomorphe à $PSL_2(\mathbb{F}_7)$.

DEMO Puisque le morphisme α est surjectif et que τ et ι engendrent tout $T(2, 3, 7)$, il est clair que τ et $\iota \in Iso^+(S)$ engendrent $Iso^+(S)$. Sachant encore (on l'a montré au chapitre des groupes triangulaires) que $T(2, 3, 7)$ admet la présentation $\langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = 1 \rangle$ et que $Iso^+(S)$ est le quotient de $T(2, 3, 7)$ par l'enveloppe normale de $(\tau^3\iota)^4$ on conclut que $Iso^+(S)$ admet la présentation:

$$\langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = (\tau^3\iota)^4 = 1 \rangle$$

Or on a montré en décrivant $PSL_2(\mathbb{F}_7)$ que ce groupe admettait la même présentation. On peut a donc un isomorphisme entre $Iso^+(S)$ et $PSL_2(\mathbb{F}_7)$ en envoyant τ et ι sur les τ et ι construits dans le chapitre premier (la translation d'amplitude 1 et l'inversion). De plus on a, par cet isomorphisme le graphe de Cayley de $Iso^+(S)$ relativement aux générateurs τ et ι .

☐

Lemme $\Pi(d)$ est encore un triangle dans S c'est-à-dire un polygone simplement connexe dont le bord est composé de trois géodésiques.

DEMO Pour montrer cela, on montre que $\Pi|_d$ est encore un homéomorphisme de d sur $\Pi(d)$. Forcément, $\Pi|_d$ est surjective, qu'elle ne soit plus injective alors, il y aurait $x \neq y \in d$ tels que $\Pi(x) = \Pi(y)$. Il y aurait donc $\gamma \in \Gamma$ tel que $\gamma(x) = y$. Puisque $x \neq y$ on a $\gamma \neq Id_{\mathbb{D}^2}$ et donc que x et $y \in \partial d$. Ainsi $y \in \gamma(d) \cap d$.

Mais les pavés qui intersectent d sont des pavés de la forme $\gamma(d)$ où $\gamma \in \{Id|_S, \iota, \tau^k, (\tau\iota)^k, (\iota\tau)^k \mid k \in \mathbb{N}\}$ donc (domaine fondamental) γ est une de ces transformations qui toutes fixent un point. Or on a montré que Γ agissait librement sur \mathbb{D}^2 , c'est-à-dire qu'aucun élément de Γ n'a de point fixe. Absurdité. On en conclut que $\Pi|_d$ est une bijection.

En vertu de l'isométrie locale elle est donc une isométrie de d dans $\Pi(d)$ et donc $\Pi(d)$ est bien un polygone simplement connexe à trois côtés.

☐

Quelques petits sous-groupes de $\mathrm{PSL}_2(\mathbb{F}_7)$

On a donc obtenu un pavage en 168 triangles de notre surface S . La démarche de cette dernière partie est de reprendre le morphisme $\mu: S_4 \rightarrow \mathrm{PSL}_2(\mathbb{F}_7)$ qu'on avait trouvé au chapitre III et d'en trouver un sous-groupe d'ordre 4. Il s'avèrera que ce sous-groupe admettra, comme domaine fondamental, un espace homéomorphe à une sphère où l'on a enlevé trois disques ouverts dont l'adhérence est disjointes. Ce domaine sera un candidat idéal dans la mesure où il représente un des quatre sommets de la surface bord d'un "épaississement" du 1-squelette d'un tétraèdre. Nous pourrions alors facilement assembler ces 4 pièces pour construire (en tissus, en bois ou en pierre) notre surface afin de la rendre visible.

Lemme On a montré dans la description de $\mathrm{PSL}_2(\mathbb{F}_7)$ (chapitre III) que qu'on pouvait trouver un morphisme $\mu: S_4 \rightarrow \mathrm{PSL}_2(\mathbb{F}_7)$. Ce morphisme est injectif et donc $\mu(S_4)$ est un sous-groupe de $\mathrm{PSL}_2(\mathbb{F}_7)$ à 24 éléments. On a même donné explicitement ce morphisme en termes de générateurs et relations: S_4 est engendré par α et β et μ envoie

$$\begin{aligned}\alpha &\longmapsto \tau \circ \eta_{\frac{1}{4}} = \tau \circ (\tau^3 \circ \iota \circ \tau^5 \circ \iota \circ \tau^3 \circ \iota) = \tau^4 \circ \iota \circ \tau^5 \circ \iota \circ \tau^3 \circ \iota \\ \beta &\longmapsto \tau^5 \circ \iota \circ \tau \circ \eta_4 = \tau^5 \circ \iota \circ \tau \circ (\tau^5 \circ \iota \circ \tau^3 \circ \iota \circ \tau^5 \circ \iota) \\ &= \tau^6 \circ (\tau^6 \circ \iota \circ \tau^6 \circ \iota \circ \tau^6) \circ \tau^4 \circ \iota \circ \tau^5 \circ \iota = \tau^6 \circ \iota \circ \tau^4 \circ \iota \circ \tau^5 \circ \iota\end{aligned}$$

Une transversale de l'action à gauche de S_4 est l'heptagone contenant le 1, c'est-à-dire le sous-groupe $Tr_1 = \{\tau^k \mid k = 0, \dots, n\}$ et donc, l'image de S_4 dans $Iso^+(S)$ admet comme domaine fondamental la réunion des 7 triangles $\tau^k(d)$ qui est un heptagone.

DEMO Pour montrer que le morphisme est injectif, il faut construire les images des éléments de S_4 dans $\mathrm{PSL}_2(\mathbb{F}_7)$. On le fait en utilisant la liste des mots donnée dans ce même chapitre III et en construisant son image en suivant le chemin. On obtient effectivement 24 sommets. Dans la mesure où l'on peut faire confiance à la personne qui a dessiné ces chemins, on peut dire que l'image de S_4 par μ contient 24 éléments et donc que μ est injective.

Pour montrer que la transversale proposée en est bien une, on montre que les images de Tr_1 par multiplication à gauche par les éléments de $\mu(S_4)$ sont disjointes. Mais cela se voit directement dans le graphe puisque le sommet représentant $\mu(\sigma)\tau^k$ n'est rien d'autre que le bout du chemin dans le graphe obtenu en suivant k fois les arrêtes τ depuis le sommet représentant $\mu(\sigma)$. On voit effectivement dans le même graphe ci-contre que ces heptagones sont disjointes. Alternativement, on peut se baser sur l'ensemble des sommets représentants les images des éléments de S_4 par μ que l'on a tracé plus haut pour voir que, $\mu(S_4) \cap Tr_1$ ne contient que la translation identité $\tau^0 = \tau^7$. Dès lors si l'on avait ξ et $\zeta \in \mu(S_4)$, tels que $\xi\tau^k = \zeta\tau^l$ avec $\tau^l \neq \tau^k$ on aurait que $\tau^{k-l} = \xi^{-1}\zeta \in \mu(S_4)$ et donc $\tau^{k-l} = 1$ ce qui est absurde. D'où $\{\mu(S_4) \cdot \tau^k \mid k = 0, \dots, n\}$ est une famille disjointe d'éléments de $\mathrm{PSL}_2(\mathbb{F}_7)$.

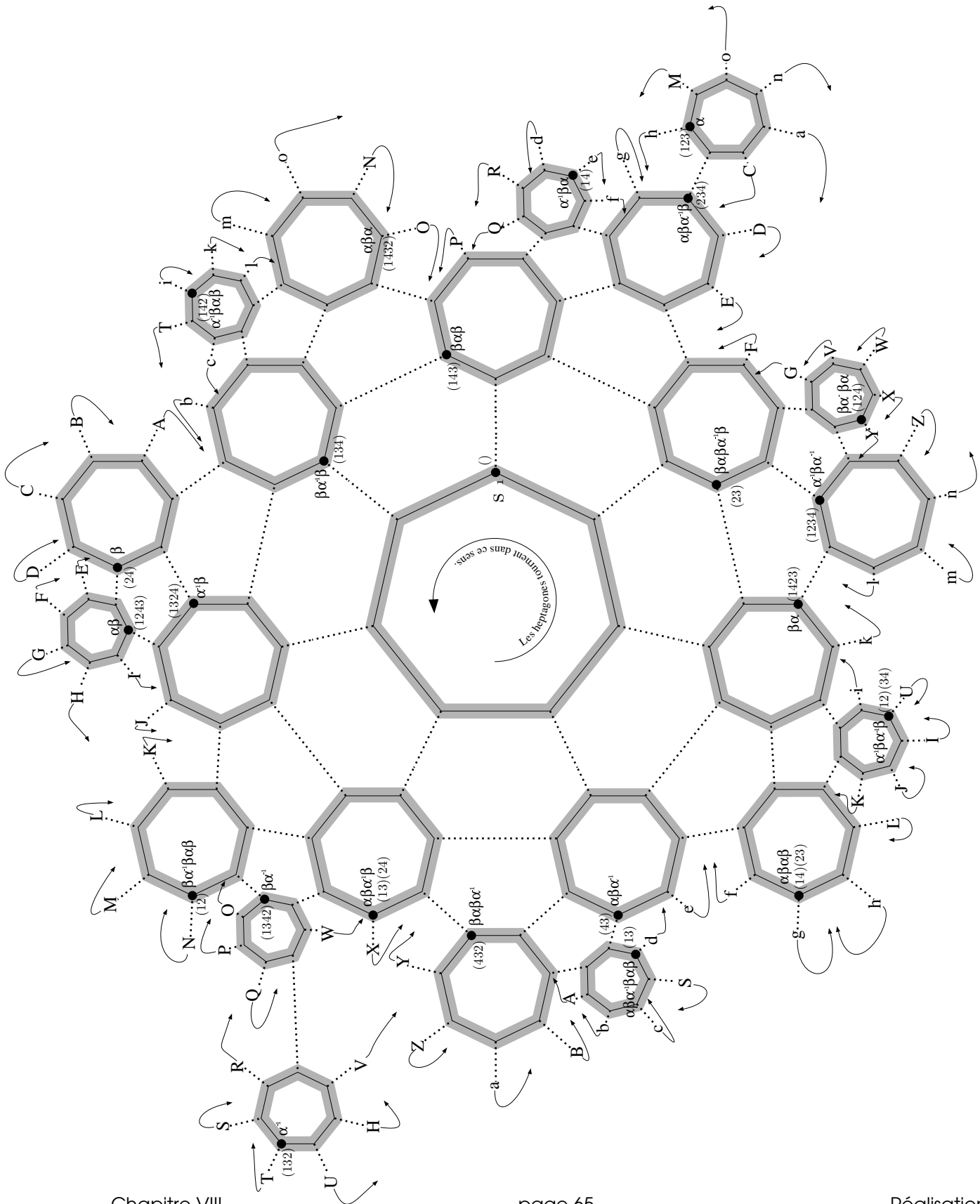
En outre cette famille recouvre tout $\mathrm{PSL}_2(\mathbb{F}_7)$ puisque:

$$\mathrm{Card}(\{\mu(S_4) \cdot \tau^k \mid k \in \mathbb{N}\}) = 168 = 24 \cdot 7 = \mathrm{Card}(S_4) \cdot \mathrm{Card}(\{\tau^k \mid k \in \mathbb{N}\})$$

Et que $\mathrm{PSL}_2(\mathbb{F}_7)$ contient également 168 éléments.

On a donc trouvé une famille Tr_1 qui contient un et un seul représentant de chaque classe de $\mathrm{PSL}_2(\mathbb{F}_7)$ modulo $\mu(S_4)$ à gauche. D'où Tr_1 est bien une transversale de Schreier à gauche de ce sous-groupe.

□



Lemme Le sous-groupe A_4 d'indice 2 dans S_4 est le noyau du morphisme de signature. Ainsi en prenant une permutation paire et une permutation impaire on obtient une transversale de A_4 dans S_4 (à gauche ou à droite puisqu'un noyau est normal). En regardant sur le graphe, on voit que $\cup \mu(\alpha\beta\alpha^{-1})\tau^k(d) = \cup \tau^4\iota\tau^k(d)$ est un heptagone voisin de l'heptagone fondamental $\cup \tau^k(d)$ de plus $(43) = \alpha\beta\alpha^{-1}$ est impaire et l'identité est paire donc $\{(), (43)\}$ forme une transversale de A_4 pour S_4 et donc $\cup \tau^k(d) \cup \tau^4\iota\tau^k(d)$ est un domaine fondamental de l'action de $\mu(A_4)$ dans S .

CLAIR

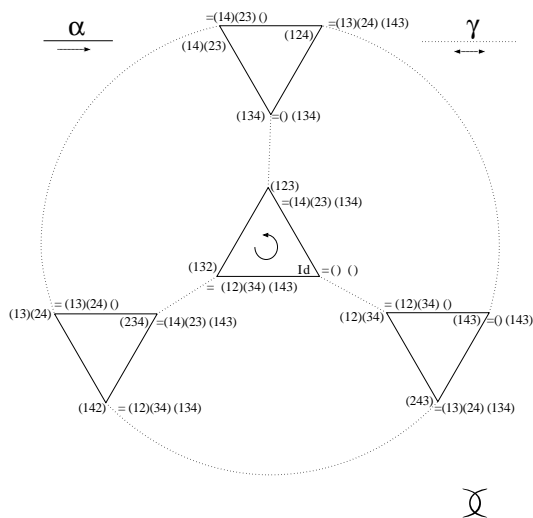
Lemme Puisque $\mu((134)) = \mu(\beta\alpha^{-1}\beta) = \tau\iota$, le pavé $\mu((134))(\cup \tau^k(d) \cup \tau^4\iota\tau^k(d))$ est voisin du domaine fondamental $\cup \tau^k(d) \cup \tau^4\iota\tau^k(d)$ (en effet, l'arrête (τ, ι) les relie). De même, on a que $\mu((143)) = \mu((134)^2) = \tau\iota\tau\iota = \iota\tau^6$ donc l'arrête $(1, \iota)$ relie le domaine fondamental à son image par $\mu((134)^2)$. Ainsi cette transformation est une transformation vicinale.

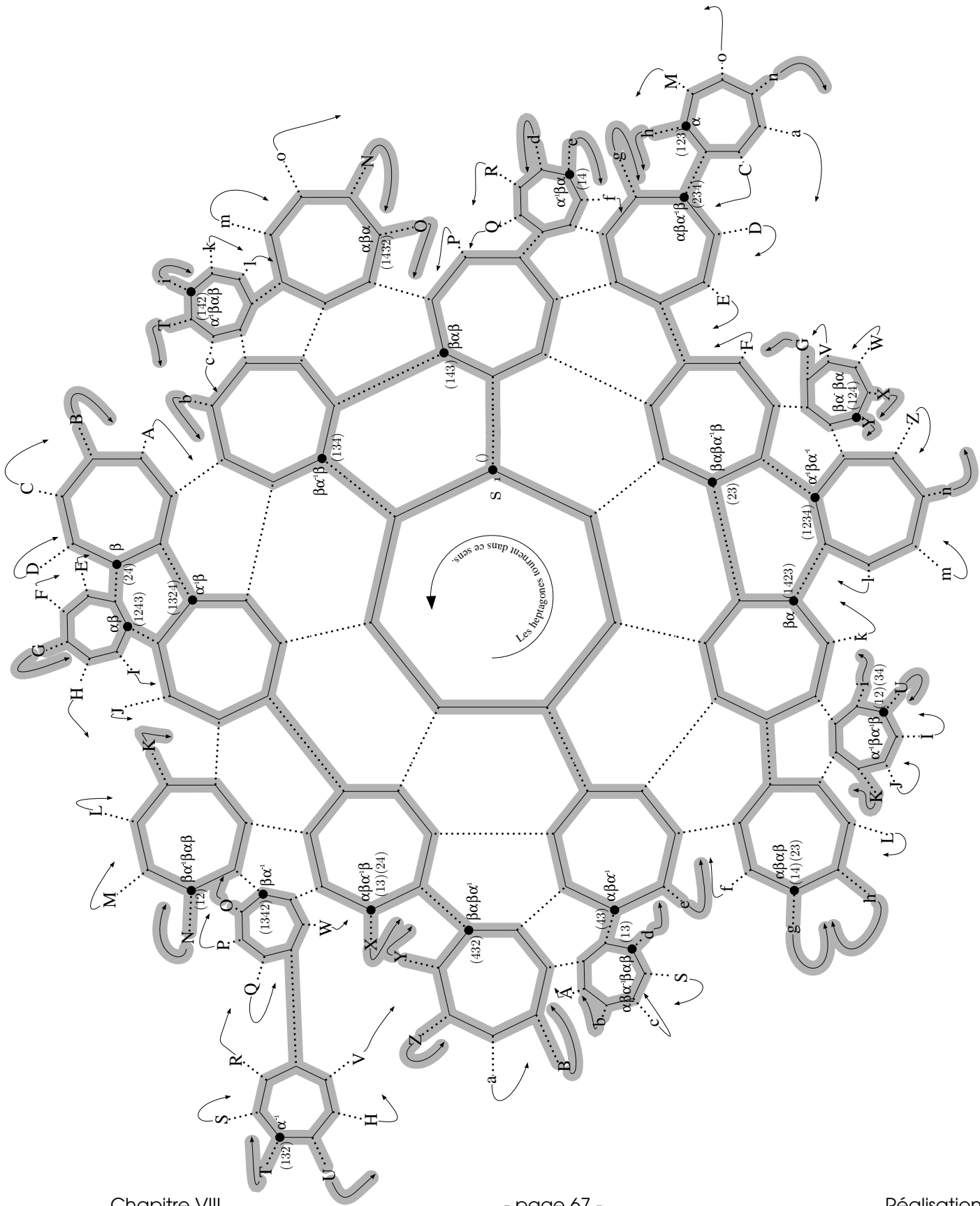
Donc l'image du domaine fondamental choisi pour l'action de $\mu(A_4)$ sur S par le sous-groupe $\Theta = \{\mu(()), \mu((134)), \mu((143))\}$ est encore un domaine connexe.

On montre dans ce lemme que le sous-groupe Ω engendré par $\mu((14)(23))$ et $\mu((12)(34))$ est une transversale pour l'action à droite de Θ et donc que Θ est une transversale de Ω pour son action à gauche. Ainsi les images du domaine fondamental de $\mu(A_4)$ par le sous-groupe Θ forment un domaine fondamental de Ω .

DEMO

On établit l'ensemble des images de l'application $(x, y) \in \Omega \times \Theta \mapsto x \cdot y \in A_4$ dans le graphe. Et l'on voit que cette image est surjective et donc (puisque ces ensembles ont mêmes cardinaux) injective. Ce qui veut dire que dans l'ensemble Ω il y a un et un seul représentant de chaque classe modulo l'action à droite de Θ et que dans Θ il y a un et un seul représentant de chaque classe modulo l'action à gauche de Ω . D'où la conclusion.



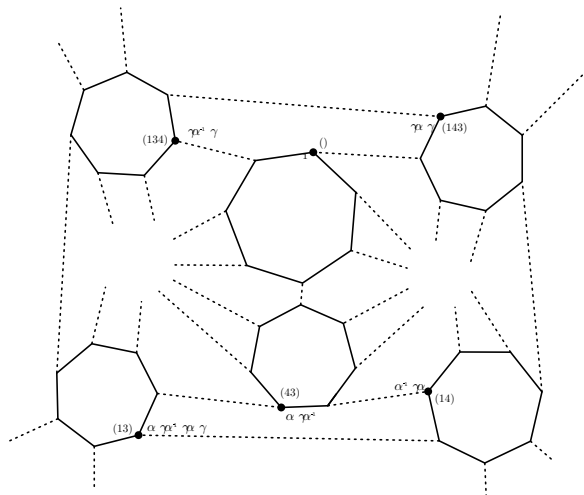


Proposition Le domaine fondamental de Ω est homéomorphe à une sphère où l'on a enlevé trois disques ouverts d'adhérences disjointes. Il s'agit donc d'un "pantalon". La surface S est donc le collage de ces quatre pantalons va donner un surface tubulaire qui peut être représentée comme "l'épaississement du 1-squelette" d'un tétraèdre.

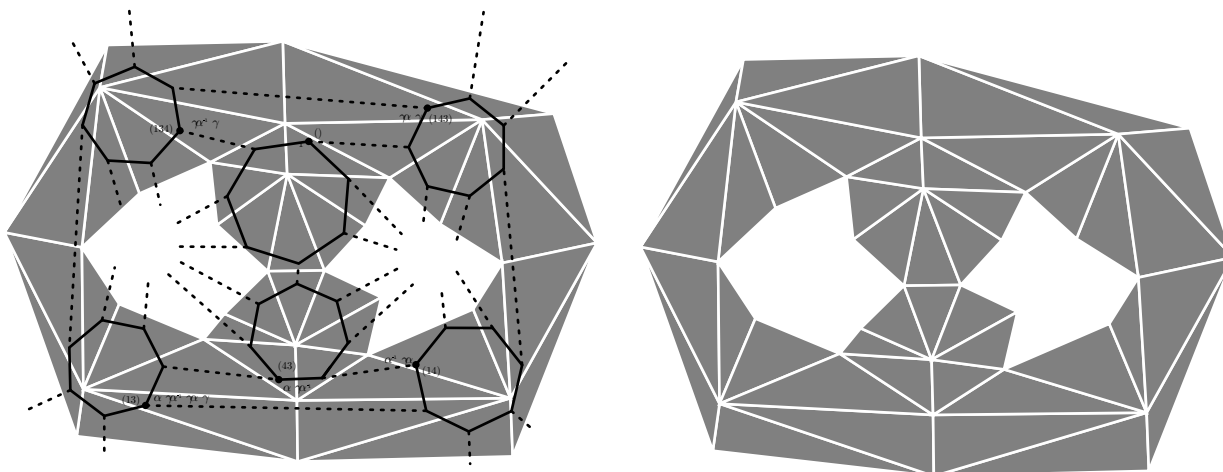
DEMO

En vertu de l'équivalence: p et q sont deux pavés voisins si et seulement s'il y a une arête du graphe de proximité entre p et q (i.e. s'il y a une arête entre $b(p)$ et $b(q)$ dans le graphe de Cayley de $Iso^+(S)$ et puisque l'image de d est encore un triangle, on peut dire que le domaine fondamental de Ω est un "assemblage" de triangles (un 2-polyèdre) et que l'assemblage est décrit par le graphe.

On trace le graphe de ce domaine fondamental en gardant libre les arêtes manquantes et l'on obtient le graphe suivant:



On peut alors dessiner l'assemblage exact de triangles que cela représente et l'on obtient:



On voit donc qu'il s'agit d'un disque percé de deux trous, qui n'est rien d'autre qu'un pantalon. On a donc bien décomposé notre surface en quatre pantalons, il est maintenant aisé de la réaliser manuellement.



VALIDATION DES GRAPHES SUPPOSÉS

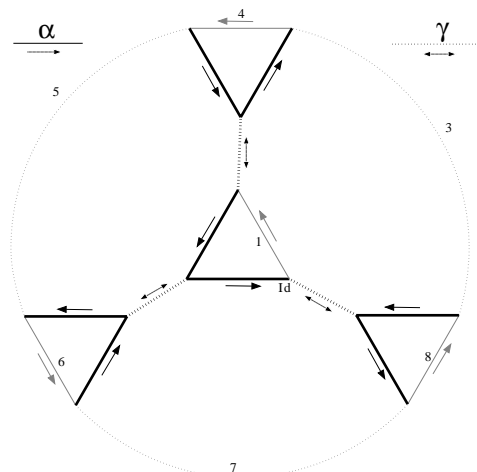
Cet appendice a pour but de démontrer explicitement l'inclusion des groupes fondamentaux entre les graphes que l'on a supposé être le graphes de Cayley de nos groupes et les graphes de Cayley des groupes abstraits. On applique ici la technique décrite à la fin du chapitre I, pour obtenir un revêtement du graphe que l'on a dessiné sur le graphe de Cayley. Il s'agira de calcul symbolique sur les groupes abstraits donnés par les présentations.

L'ARBRE MAXIMAL POUR A_4

Ci-contre se trouve un graphe dessiné, ce qui, on l'a accepté, représente bien un graphe, générique de degré 3 et catalogué sur le bouquet à base $X = \{\alpha, \alpha^1, \gamma\}$. Appelons-le E . Le but est de montrer que l'on a un revêtement de ce graphe sur le graphe de Cayley du groupe abstrait :

$$U = \langle \alpha, \beta | \alpha^3 = \gamma^2 = (\alpha\gamma)^4 = 1 \rangle$$

On dessine, dans ce graphe un arbre (on voit à l'oeil que c'est un arbre) maximal (il atteint tous les sommets). Cela nous permet alors, d'après l'outil énoncé en fin du chapitre I, de vérifier que le groupe fondamental s'envoie, par l'isomorphisme entre les revêtements universels induit par le cataloguage, dans le groupe fondamental de $C(U, \{\alpha, \alpha^1, \gamma\})$. On vérifie pour cela que chaque chemin $\chi(a)$ a comme représentant en mot sur l'alphabet $\{\alpha, \alpha^1, \gamma\}$ un mot que l'on peut simplifier selon les règles de U .



- 1 $\alpha^3 = 1$
- 2 $\alpha^{-2}\gamma\alpha^3\gamma\alpha^2 = (\alpha^{-2}\gamma)(\gamma\alpha^2) = 1$
- 3 $\alpha^{-2}\gamma\alpha^{-1}\gamma\alpha^{-1}\gamma\alpha = \alpha^{-1}(\alpha^{-1}\gamma\alpha^{-1}\gamma\alpha^{-1}\gamma)\alpha = \alpha^{-1}\alpha = 1$
- 4 $\alpha^{-1}\gamma\alpha^3\gamma\alpha = \alpha^{-1}\gamma\gamma\alpha = 1$
- 5 $\alpha^{-1}\gamma\alpha^{-1}\gamma\alpha^{-1}\gamma = 1$
- 6 $\gamma\alpha^3\gamma = 1$
- 7 $\gamma\alpha^{-1}\gamma\alpha^{-1}\gamma\alpha^2 = \gamma\alpha^{-1}\gamma\alpha^{-1}\gamma\alpha^{-1} = 1$

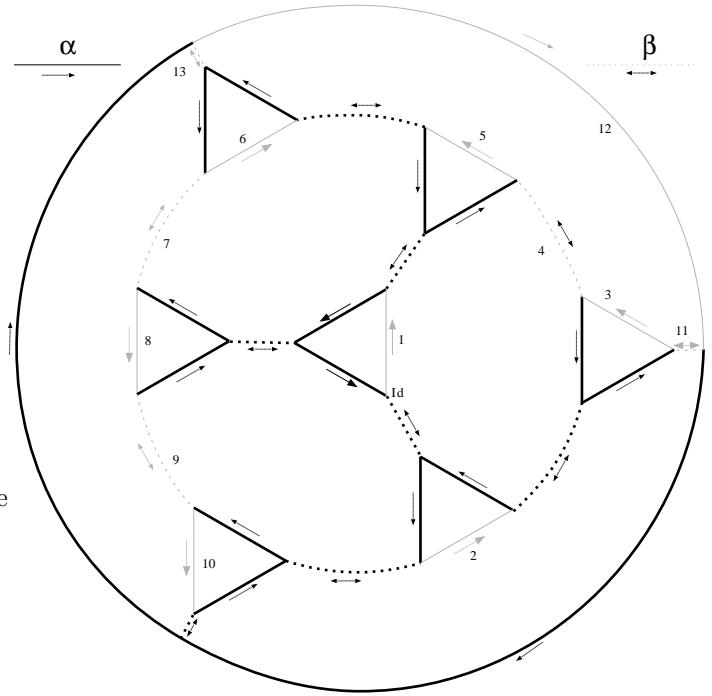
On a donc vérifiée que le groupe fondamental de ce graphe E est bien envoyé dans le groupe fondamental de $C(U, \{\alpha, \alpha^1, \gamma\})$ par l'isomorphisme des revêtements universel induit par les deux cataloguage sur $B(\{\alpha, \alpha^1, \gamma\})$. On peut donc appliquer le théorème final de la théorie des graphes de Cayley qui nous dit alors que l'on a un revêtement du graphe D sur $C(U, \{\alpha, \alpha^1, \gamma\})$.

L'ARBRE MAXIMAL POUR S_4

Ci-contre se trouve un graphe dessiné, ce qui, on l'a accepté, représente bien un graphe, générique de degré 3 et catalogué sur le bouquet à base $X = \{\alpha, \alpha^{-1}, \beta\}$. Le but est de montrer que l'on a un revêtement de ce graphe sur le graphe de Cayley du groupe abstrait :

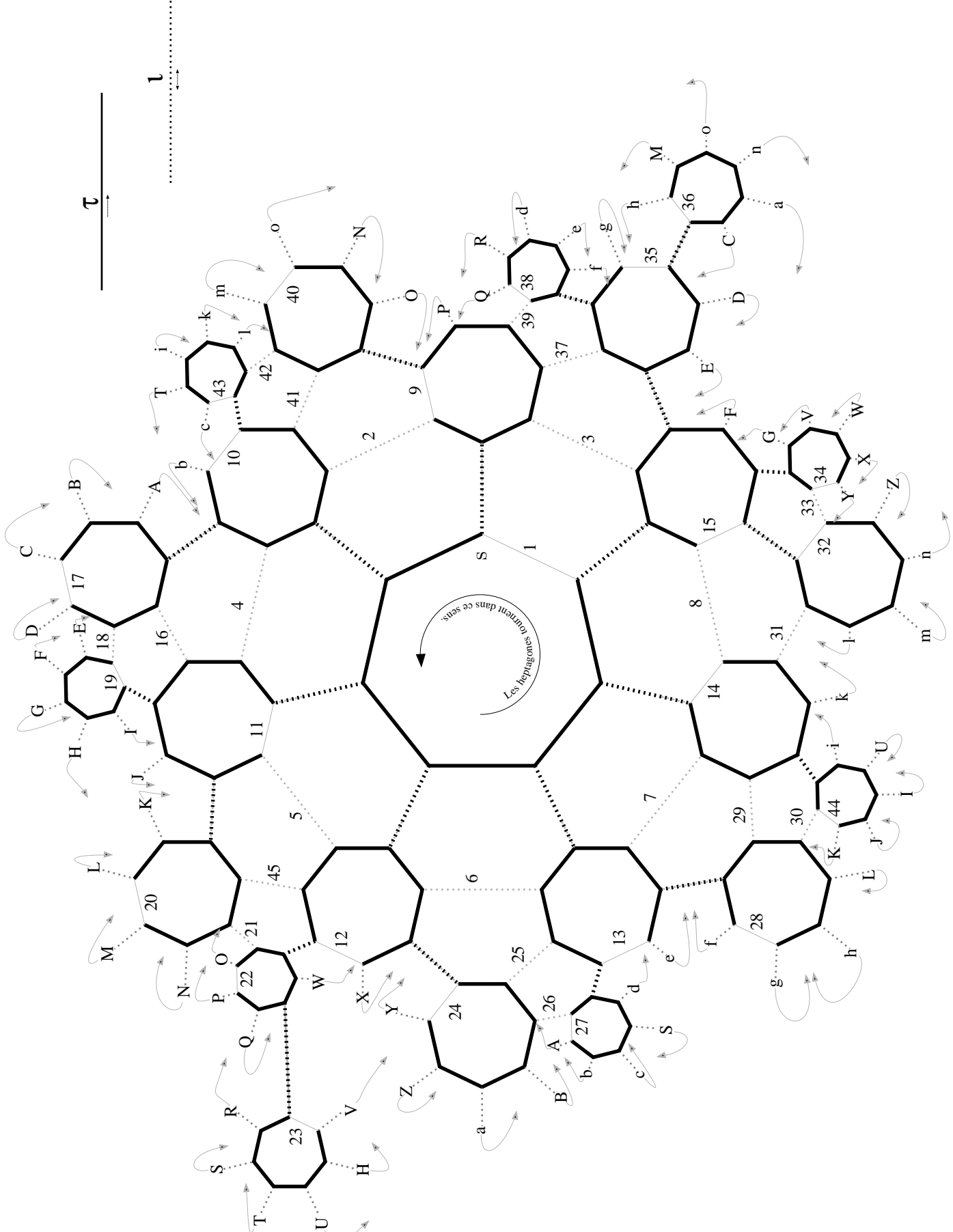
$$U = \langle \alpha, \beta \mid \alpha^3 = \beta^2 = (\beta\alpha)^4 = 1 \rangle$$

On dessine, dans ce graphe un arbre (on voit à l'oeil que c'est un arbre) maximal (il atteint tous les sommets). Cela nous permet alors, d'après l'outil énoncé en fin du chapitre I, de vérifier que le groupe fondamental s'envoie, par l'isomorphisme entre les revêtements universels induit par le cataloguage, dans le groupe fondamental du graphe $C(U, \{\alpha, \alpha^{-1}, \beta\})$. On vérifie pour cela que chaque chemin $\chi(a)$ a comme représentant en mot sur l'alphabet $\{\alpha, \alpha^{-1}, \beta\}$ un mot que l'on peut simplifier selon les règles de U .



- 1 $\alpha^3 = 1$
- 2 $\beta\alpha^3\beta = \beta\beta = 1$
- 3 $\beta\alpha^{-1}\beta\alpha^3\beta\alpha\beta = (\beta\alpha^{-1}\beta)(\beta\alpha\beta) = 1$
- 4 $\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^2 = \alpha(\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta)\alpha^{-2} = 1$
- 5 $\alpha^{-2}\beta\alpha^3\beta\alpha^2 = (\alpha^{-2}\beta)(\beta\alpha^2) = 1$
- 6 $\alpha^{-2}\beta\alpha^{-1}\beta\alpha^3\beta\alpha\beta\alpha^2 = (\alpha^{-2}\beta\alpha^{-1}\beta)(\beta\alpha\beta\alpha^2) = 1$
- 7 $\alpha^{-2}\beta\alpha^{-1}\beta\alpha^2\beta\alpha^{-1}\beta\alpha = \alpha^{-2}(\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1})\alpha^2 = \alpha^{-2}\alpha^2 = 1$
- 8 $\alpha^{-1}\beta\alpha^3\beta\alpha(\alpha^{-1}\beta)(\beta\alpha) = 1$
- 9 $\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta = 1$
- 10 $\beta\alpha\beta\alpha^3\beta\alpha^{-1}\beta = (\beta\alpha\beta)(\beta\alpha^{-1}\beta) = 1$
- 11 $\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha\beta = (\beta\alpha)(\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1})(\alpha^2\beta) = (\beta\alpha)(\alpha^2\beta) = 1$
- 12 $\beta\alpha\beta\alpha^{-1}\beta\alpha^3\beta\alpha\beta\alpha^{-1}\beta = (\beta\alpha\beta\alpha^{-1}\beta)(\beta\alpha\beta\alpha^{-1}\beta) = 1$
- 13 $\beta\alpha\beta\alpha^{-1}\beta\alpha\beta\alpha^{-1}\beta\alpha\beta\alpha^2 = \beta\alpha\beta\alpha(\alpha\beta\alpha\beta\alpha)\alpha\beta\alpha\beta\alpha^2 = \beta\alpha\beta\alpha\beta\alpha^2\beta\alpha\beta\alpha\beta\alpha^2$
 $= (\beta\alpha\beta\alpha\beta\alpha)(\alpha\beta\alpha\beta\alpha\beta\alpha)\alpha = (\beta\alpha\beta\alpha\beta\alpha)(\alpha^2\beta)(\beta\alpha) = 1$

On a donc vérifiée que le groupe fondamental de ce graphe D est bien envoyé dans le groupe fondamental de $C(U, \{\alpha, \alpha^{-1}, \beta\})$ par l'isomorphisme des revêtements universel induit par les deux cataloguage sur $B(\{\alpha, \alpha^{-1}, \beta\})$. On peut donc appliquer le théorème final de la théorie des graphes de Cayley qui nous dit alors que l'on a un revêtement du graphe D sur $C(U, \{\alpha, \alpha^{-1}, \beta\})$.



L'ARBRE MAXIMAL POUR $\text{PSL}_2(\mathbb{F}_7)$

Ci-contre se trouve un graphe dessiné, ce qui, on l'a accepté, représente bien un graphe, générique de degré 3 et catalogué sur le bouquet à base $X = \{\tau, \tau^{-1}, \iota\}$. Appelons-le F . Il faut prendre garde que ce graphe n'est pas planaire mais qu'il se referme sur lui même, cela veut dire qu'il faut prendre garde à tous les renvois pour chacun desquels le dessinateur a pris soin d'indiquer la direction du correspondant.

Le but est de montrer que l'on a un revêtement de ce graphe dans le graphe de Cayley du groupe abstrait :

$$H = \langle \tau, \iota \mid \iota^2 = (\tau\iota)^3 = \tau^7 = (\tau^3\iota)^4 = 1 \rangle$$

On dessine, dans ce graphe un arbre (on voit à l'oeil que c'est un arbre) maximal (il atteint tous les sommets). Cela nous permet alors, d'après l'outil énoncé en fin du chapitre I, de vérifier que le groupe fondamental s'envoie, d'après l'isomorphisme entre les revêtements universels donné par le cataloguage, dans le groupe fondamental de $C(H, \{\tau, \tau^{-1}, \iota\})$. On vérifie pour cela que chaque chemin $\chi(a)$ a comme représentant en mot sur l'alphabet $\{\tau, \tau^{-1}, \iota\}$ un mot que l'on peut simplifier selon les règles de H .

Cette longue vérification se fait à la main en parcourant les arêtes du graphe qui ne sont pas dans l'arbre maximal et en décomposant chacun de ces termes en utilisant les règles de simplifications de H . Par mesure de lisibilité, on ne donner les arguments nous permettant de faire cette simplification.

- 1 $\tau^7 = 1$
- 2 $\tau\iota\tau\iota\tau\iota = 1$
- 3 $\iota\tau\iota\tau\iota\tau^{-6} = \iota\tau\iota\tau\iota\tau = 1$
- 4 $\tau\iota\tau^{-1}\iota\tau^{-1}\iota\tau^{-2} = \tau(\iota\tau^{-1})^3\tau^{-1} = 1$
- 5 $\tau^2\iota\tau^6\iota\tau^{-1}\iota\tau^{-3} = \tau^2(\iota\tau^{-1})^3\tau^{-2} = 1$
- 6 $\tau^3\iota\tau^{-1}\iota\tau^{-1}\iota\tau^{-4} = \tau^{-3}(\iota\tau^{-1})^3\tau^3 = 1$
- 7 $\tau^4\iota\tau^{-1}\iota\tau^{-1}\iota\tau^{-5} = \tau^4(\iota\tau^{-1})^3\tau^{-4} = 1$
- 8 $\tau^5\iota\tau^6\iota\tau^{-1}\iota\tau^{-6} = \tau^5(\iota\tau^{-1})^3\tau^{-5} = 1$
- 9 $\iota\tau^7\iota = 1$
- 10 $\tau\iota\tau^7\iota\tau^{-1} = 1$
- 11 $\tau^2\iota\tau^7\iota\tau^{-2} = 1$
- 12 $\tau^3\iota\tau^7\iota\tau^{-3} = 1$
- 13 $\tau^4\iota\tau^7\iota\tau^{-4} = 1$
- 14 $\tau^5\iota\tau^7\iota\tau^{-5} = 1$
- 15 $\tau^6\iota\tau^7\iota\tau^{-6} = 1$
- 16 $\tau\iota\tau^{-2}\iota\tau^{-1}\iota\tau^{-2}\iota\tau^{-2} = \tau\iota\tau^{-1}(\tau^{-1}\iota\tau^{-1}\iota\tau^{-1})\tau^{-1}\iota\tau^{-2} = \tau\iota\tau^{-1}\iota\tau^{-1}\iota\tau^{-2} = \tau(\iota\tau^{-1})^3\tau^{-1} = 1$
- 17 $\tau\iota\tau^{-2}\iota\tau^3\tau\tau^3\iota\tau^2\iota\tau^{-1} = (\tau\iota\tau^{-2}\iota)(\iota\tau^2\iota\tau^{-1}) = 1$
- 18 $\tau\iota\tau^{-2}\iota\tau^{-2}\iota\tau^6\iota\tau^{-3}\iota\tau^{-2} = \tau\iota\tau^{-2}\iota\tau^{-1}(\tau^{-1}\iota\tau^{-1}\iota\tau^{-1})\tau^{-2}\iota\tau^{-2} = \tau\iota\tau^{-1}(\tau^{-1}\iota\tau^{-1}\iota\tau^{-1})\tau^{-1}\iota\tau^{-2} = \tau(\iota\tau^{-1})^3\tau^{-1} = 1$
- 19 $\tau^2\iota\tau^3\iota\tau^7\iota\tau^{-3}\iota\tau^{-2} = (\tau^2\iota\tau^3\iota)(\iota\tau^{-3}\iota\tau^{-2}) = 1$
- 20 $\tau^2\iota\tau^5\iota\tau^2\tau\tau^4\iota\tau^{-5}\iota\tau^{-2} = (\tau^2\iota\tau^5\iota)(\iota\tau^{-5}\iota\tau^{-2}) = 1$
- 21 $\tau^2\iota\tau^5\iota\tau^{-2}\iota\tau^{-1}\iota\tau^{-3}\iota\tau^{-3} = \tau^2\iota\tau^5\iota\tau^{-1}(\tau^{-1}\iota\tau^{-1}\iota\tau^{-1})\tau^{-2}\iota\tau^{-3} = \tau^2\iota\tau^5(\iota\tau^{-1}\iota\tau^{-1})\tau^{-1}\iota\tau^{-3} = \tau^2\iota\tau^6\tau\iota\tau^{-1}\iota\tau^{-3} = \tau^3(\tau^{-1}\iota\tau^{-1}\iota\tau^{-1})\tau^{-2} = 1$
- 22 $\tau^3\iota\tau^3\iota\tau^2\tau\tau^4\iota\tau^{-3}\iota\tau^{-3} = (\tau^3\iota\tau^3\iota)(\iota\tau^{-3}\iota\tau^{-3}) = 1$

- 23 $\tau^3 \iota \tau^3 \iota \tau^{-2} \iota \tau^6 \tau \iota \tau^2 \iota \tau^{-3} \iota \tau^{-3} \stackrel{\tau^7=1}{=} (\tau^3 \iota \tau^3 \iota \tau^{-2} \iota) (\iota \tau^2 \iota \tau^{-3} \iota \tau^{-3}) = 1$
- 24 $\tau^3 \iota \tau^{-2} \iota \tau \iota \tau^6 \iota \tau^2 \iota \tau^{-3} \stackrel{\tau^7=1}{=} (\tau^3 \iota \tau^{-2} \iota) (\iota \tau^2 \iota \tau^{-3}) = 1$
- 25 $\tau^3 \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-2} \iota \tau^{-4} = \tau^3 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^{-4} \stackrel{(\tau \iota)^3=1}{=} \tau^3 \iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-4} = \tau^3 (\iota \tau^{-1})^3 \tau^{-3} = 1$
- 26 $\tau^3 \iota \tau^{-2} \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-3} \iota \tau^{-4} = \tau^3 \iota \tau^{-2} \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-2} \iota \tau^{-4} = \tau^3 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^4$
 $= \tau^4 (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1} \iota) \tau^{-4} = 1$
- 27 $\tau^4 \iota \tau^3 \iota \tau \tau^5 \iota \tau^{-3} \iota \tau^{-4} = (\tau^4 \iota \tau^3 \iota) (\iota \tau^{-3} \iota \tau^{-4}) = 1$
- 28 $\tau^4 \iota \tau^{-2} \iota \tau \tau^5 \iota \tau^2 \iota \tau^{-4} = (\tau^4 \iota \tau^{-2} \iota) (\iota \tau^2 \iota \tau^{-4}) = 1$
- 29 $\tau^4 \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-2} \iota \tau^{-5} = \tau^4 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^{-5} = \tau^4 (\iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-4} = 1$
- 30 $\tau^4 \iota \tau^{-2} \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-3} \iota \tau^5 = \tau^4 \iota \tau^{-2} \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-2} \iota \tau^5 = \tau^4 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^5$
 $= \tau^5 (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1} \iota) = 1$
- 31 $\tau^5 \iota \tau^5 \iota \tau^{-1} \iota \tau^5 \iota \tau^6 = \tau^5 \iota \tau^6 (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^6 \iota \tau^{-6} = \tau^5 (\iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-5} = 1$
- 32 $\tau^6 \iota \tau^{-5} \iota \tau^6 \iota \tau \iota \tau^5 \iota \tau^{-6} = (\tau^6 \iota \tau^{-5} \iota) (\iota \tau^5 \iota \tau^{-6}) = 1$
- 33 $\tau^6 \iota \tau^{-5} \iota \tau^6 \iota \tau^{-1} \iota \tau^4 \iota \tau^{-6} = \tau^6 \iota \tau^{-5} (\iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^5 \iota \tau^{-6} = (\tau^6 \iota \tau^{-5}) (\tau^5 \iota \tau^{-6}) = 1$
- 34 $\tau^6 \iota \tau^{-4} \iota \tau^2 \iota \tau^5 \iota \tau^4 \iota \tau^{-6} = (\tau^6 \iota \tau^{-4} \iota) (\iota \tau^4 \iota \tau^{-6}) = 1$
- 35 $\tau^6 \iota \tau^{-2} \iota \tau^7 \iota \tau^2 \iota \tau^{-6} = (\tau^6 \iota \tau^{-2} \iota) (\iota \tau^2 \iota \tau^{-6}) = 1$
- 36 $\tau^6 \iota \tau^{-2} \iota \tau^3 \iota \tau^6 \iota \tau^7 \iota \tau^{-3} \iota \tau^2 \iota \tau^{-6} = (\tau^6 \iota \tau^{-2} \iota \tau^3 \iota) (\iota \tau^{-3} \iota \tau^{-2} \iota \tau^{-6}) = 1$
- 37 $\tau^6 \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-2} \iota \tau^6 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota = \tau^{-1} \iota \tau^{-1} \iota \tau^{-1} \iota = 1$
- 38 $\tau^6 \iota \tau^{-2} \iota \tau^{-2} \iota \tau^7 \iota \tau^2 \iota \tau^2 \iota \tau^{-6} = (\tau^6 \iota \tau^{-2} \iota \tau^{-2} \iota) (\iota \tau^2 \iota \tau^2 \iota \tau^{-6}) = 1$
- 39 $\tau^6 \iota \tau^{-2} \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-3} \iota = \tau^6 \iota \tau^{-2} \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-2} \iota$
 $= \tau^6 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota = \tau^{-1} \iota \tau^{-1} \iota = 1$
- 40 $\iota \tau^5 \iota \tau^7 \iota \tau^{-5} \iota = (\iota \tau^5 \iota) (\iota \tau^{-5} \iota) = 1$
- 41 $\iota \tau^5 \iota \tau^{-1} \iota \tau^{-2} \iota \tau^{-1} = \iota \tau^6 \tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^{-1} = \iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-1} = 1$
- 42 $\iota \tau^5 \iota \tau^{-2} \iota \tau^{-1} \iota \tau^{-3} \iota \tau^{-1} = \iota \tau^5 \iota \tau^{-1} (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-2} \iota \tau^{-1} = \iota \tau^6 (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-1} \iota \tau^{-1}$
 $= \iota \tau^{-1} \iota \tau^{-1} \iota \tau^{-1} = 1$
- 43 $\tau \iota \tau^3 \iota \tau^7 \iota \tau^{-3} \iota \tau^{-1} = (\tau \iota \tau^3 \iota) (\iota \tau^{-3} \iota \tau^{-1}) = 1$
- 44 $\tau^5 \iota \tau^3 \iota \tau^7 \iota \tau^{-3} \iota \tau^{-5} = (\tau^5 \iota \tau^3 \iota) (\iota \tau^{-3} \iota \tau^{-5}) = 1$
- 45 $\tau^2 \iota \tau^6 \iota \tau^{-1} \iota \tau^{-2} \iota \tau^{-3} = \tau^2 \iota \tau^5 \iota \tau^6 \iota \tau^5 \iota \tau^4 = \tau^2 \iota \tau^6 (\tau^6 \iota \tau^6 \iota \tau^6) \tau^6 \iota \tau^4 = \tau^2 \iota \tau^6 \iota \tau^6 \iota \tau^4$
 $= \tau^2 (\iota \tau^6 \iota \tau^6 \iota \tau^6) \tau^5 = \tau^2 \tau^5 = 1$
- A $\tau \iota \tau^{-2} \iota \tau \iota \tau^5 \iota \tau^{-3} \iota \tau^{-4} = \tau \iota \tau^{-3} (\tau \iota \tau \iota \tau \iota) \tau^4 \iota \tau^{-3} \iota \tau^{-4} = \tau \iota \tau^{-3} \iota \tau^{-3} \iota \tau^{-3} \iota \tau^{-4}$
 $= \tau (\iota \tau^{-3} \iota \tau^{-3} \iota \tau^{-3} \iota \tau^{-3}) \tau^{-1} = \stackrel{(\tau^3 \iota)^4=1}{=} 1$
- B $\tau \iota \tau^{-2} \iota \tau^2 \iota \tau^3 \iota \tau^2 \iota \tau^{-3} \stackrel{\tau^7=1}{=} \tau \iota \tau^5 \iota \tau^2 \iota \tau^3 \iota \tau^2 \iota \tau^4 = (\tau \iota \tau) \tau^3 (\tau \iota \tau) (\tau \iota \tau) \tau (\tau \iota \tau) (\tau \iota \tau) \tau^3$
 $= \iota \tau^6 \iota \tau^3 \iota \tau^5 \iota \tau \iota \tau^5 \iota \tau^3 = \iota \tau^6 \iota \tau^3 \iota \tau^4 (\tau \iota \tau \iota \tau) \tau^4 \iota \tau^3 = \iota \tau^6 \iota \tau^3 \iota \tau^4 \iota \tau^4 \iota \tau^3$
 $= \iota \tau^6 \iota \tau^6 (\tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4) \tau^6 = \iota \tau^6 \iota \tau^6 \iota \tau^6 = 1$
- C $\tau \iota \tau^{-2} \iota \tau^3 \iota \tau^{-1} \iota \tau^{-3} \iota \tau^2 \iota \tau^{-6} = \tau \iota \tau^{-2} \iota \tau^4 (\tau^{-1} \iota \tau^{-1} \iota \tau^{-1}) \tau^{-2} \iota \tau^2 \iota \tau^{-6} = \tau \iota \tau^5 \iota \tau^4 \iota \tau^{-3} \iota \tau^2 \iota \tau^{-6}$
 $= \tau \iota \tau (\tau^4 \iota \tau^4 \iota \tau^4) \tau \iota \tau^2 \iota \tau = \tau \iota \tau \iota \tau^3 \iota \tau \iota \tau^2 \iota \tau = (\tau \iota \tau \iota \tau) \tau^2 \iota \tau \iota \tau^2 \iota \tau = \iota \tau^2 (\tau^6 \iota \tau^6) \tau^2 \iota \tau = \iota \tau \iota \tau \iota \tau = 1$
- D $\tau \iota \tau^{-2} \tau \iota \tau^{-3} \iota \tau^{-2} \iota \tau^2 \iota \tau^{-6} = \tau \iota \tau^5 \iota \tau^4 \iota \tau^5 \iota \tau^2 \iota \tau = (\tau \iota \tau) (\tau^4 \iota \tau^4 \iota \tau^4) \tau \iota \tau^2 \iota \tau$
 $= (\tau \iota \tau \iota \tau) \tau (\tau \iota \tau \iota \tau) (\tau \iota \tau) = \iota \tau \iota \tau \iota \tau = 1$
- E $\tau^2 \iota \tau^3 \iota \tau^{-5} \iota \tau^{-1} \iota \tau^2 \iota \tau^{-6} = \tau^2 \iota \tau^3 \iota \tau^2 \iota \tau^6 \iota \tau^2 \iota \tau = \tau^6 (\tau^3 \iota \tau^3 \iota \tau^3) (\tau^6 \iota \tau^6 \iota \tau^6) \tau^3 \iota \tau$
 $= \tau^6 \iota \tau^4 \iota \tau^3 \iota \tau = \tau^6 \iota \tau^7 \iota \tau = \tau^6 \tau = 1$
- F $\tau^2 \iota \tau^3 \iota \tau^{-4} \iota \tau^3 \iota \tau^{-6} = \tau^2 \iota \tau^3 \iota \tau^3 \iota \tau^3 \iota \tau = \tau^6 (\tau^3 \iota \tau^3 \iota \tau^3 \iota \tau^3) \tau = 1$

$$\begin{aligned}
\text{c } & \tau^4 \iota \tau^3 \iota \tau^{-3} \iota \tau^{-6} \iota \tau^{-3} \iota \tau^{-1} = \tau^4 \iota \tau^3 \iota \tau^4 \iota \tau \iota \tau^4 \iota \tau^6 = \tau^4 \iota \tau^3 \iota \tau^3 (\tau \iota \tau \iota \tau) \tau^3 \iota \tau^6 = \tau^4 \iota \tau^3 \iota \tau^3 \iota \tau^3 \iota \tau^6 \\
& = \tau (\tau^3 \iota \tau^3 \iota \tau^3 \iota \tau^3 \iota) \tau^6 = 1 \\
\text{d } & \tau^4 \iota \tau^3 \iota \tau^{-1} \iota \tau^{-3} \iota \tau^2 \iota \tau^2 \iota \tau^{-6} = \tau^4 \iota \tau^3 \iota \tau^6 \iota \tau^4 \iota \tau^2 \iota \tau^2 \iota \tau = \tau^4 \iota \tau^4 (\tau^6 \iota \tau^6 \iota \tau^6) \tau^4 (\tau \iota \tau) (\tau \iota \tau) (\tau \iota \tau) \\
& = \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota = 1 \\
\text{e } & \tau^4 \iota \tau^{-3} \iota \tau^{-2} \iota \tau^2 \iota \tau^2 \iota \tau^{-6} = \tau^4 \iota \tau^4 \iota \tau^5 \iota \tau^2 \iota \tau^2 \iota \tau = \tau^4 \iota \tau^4 \iota \tau^4 (\tau \iota \tau) (\tau \iota \tau) (\tau \iota \tau) = \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota = 1 \\
\text{f } & \tau^4 \iota \tau^{-2} \iota \tau \iota \tau^{-1} \iota \tau^2 \iota \tau^2 \iota \tau^{-1} = \tau^4 \iota \tau^5 \iota \tau \iota \tau^6 \iota \tau^2 \iota \tau^2 \iota \tau = \tau^4 \iota \tau^4 (\tau \iota \tau \iota \tau) \tau^4 (\tau \iota \tau) (\tau \iota \tau) (\tau \iota \tau) = \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota = 1 \\
\text{g } & \tau^4 \iota \tau^{-2} \iota \tau^{-5} \iota \tau^3 \iota \tau^2 \iota \tau^{-6} = \tau^4 \iota \tau^5 \iota \tau^2 \iota \tau^3 \iota \tau^2 \iota \tau = \tau^4 \iota \tau^4 (\tau \iota \tau) (\tau \iota \tau) \tau (\tau \iota \tau) (\tau \iota \tau) = \tau^4 \iota \tau^4 \iota \tau^5 \iota \tau \iota \tau^5 \iota \\
& = \tau^4 \iota \tau^4 \iota \tau^4 (\tau \iota \tau \iota \tau) \tau^4 \iota = \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota = 1 \\
\text{h } & \tau^4 \iota \tau^{-2} \iota \tau^{-4} \iota \tau^{-6} \iota \tau^{-3} \iota \tau^2 \iota \tau^{-6} = \tau^4 \iota \tau^5 \iota \tau^3 \iota \tau \iota \tau^4 \iota \tau^2 \iota \tau = \tau^4 \iota \tau^5 \iota \tau^2 (\tau \iota \tau \iota \tau) \tau^2 (\tau \iota \tau) (\tau \iota \tau) \\
& = \tau^4 \iota \tau^5 \iota \tau^2 \iota \tau^2 \iota \tau^5 \iota = \tau^4 \iota \tau^6 (\tau \iota \tau) (\tau \iota \tau) (\tau \iota \tau) \tau^4 \iota = \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota = 1 \\
\text{i } & \tau^5 \iota \tau^3 \iota \tau^{-1} \iota \tau^{-4} \iota \tau^{-3} \iota \tau^{-1} = \tau^5 \iota \tau^3 \iota \tau^6 \iota \tau^3 \iota \tau^4 \iota \tau^6 = \tau^5 \iota \tau^3 \iota \tau^3 (\tau^3 \iota \tau^3 \iota \tau^3 \iota) (\tau \iota \tau) \tau^5 \\
& = \tau^5 \iota \tau^3 \iota \tau^3 (\iota \tau^4 \iota) \iota \tau^6 \iota \tau^5 = \tau^5 (\iota \tau^3 \iota \tau^3 \iota \tau^3 \iota \tau^3) \tau^2 = 1 \\
\text{k } & \tau^5 \iota \tau^4 \iota \tau^{-3} \iota \tau^{-3} \iota \tau^{-1} = \tau^5 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^6 = \tau (\tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota) \tau^6 = 1 \\
\text{l } & \tau^6 \iota \tau^{-5} \iota \tau^2 \iota \tau^{-2} \iota \tau^{-3} \iota \tau^{-1} = \tau^6 \iota \tau^2 \iota \tau^2 \iota \tau^5 \iota \tau^4 \iota \tau^6 = \tau^5 (\tau \iota \tau) (\tau \iota \tau) (\tau \iota \tau) \tau^4 \iota \tau^4 \iota \tau^6 \\
& = \tau^5 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^6 = \tau^5 (\iota \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^4) \tau^2 = 1 \\
\text{m } & \tau^6 \iota \tau^2 \iota \tau^3 \iota \tau^3 \iota \tau^2 \iota = \tau^6 \iota \tau^2 \iota \tau^3 \iota \tau^3 \iota \tau^2 \iota = (\tau^6 \iota \tau^6) (\tau^3 \iota \tau \iota \tau^3 \iota \tau^3) \tau^6 \iota = \tau^6 \iota \tau^6 \iota \tau^6 \iota = 1 \\
\text{n } & \tau^6 \iota \tau^{-5} \iota \tau^4 \iota \tau^{-3} \iota \tau^{-3} \iota \tau^2 \iota \tau^{-6} = \tau^6 \iota \tau^2 \iota \tau^4 \iota \tau^4 \iota \tau^4 \iota \tau^2 \iota \tau \\
& = \tau^6 \iota \tau^5 (\tau^4 \iota \tau^6 \iota \tau^4 \iota \tau^4 \iota) \tau^2 \iota \tau = (\tau^6 \iota \tau^5) (\tau^2 \iota \tau) = 1 \\
\text{o } & \tau^6 \iota \tau^{-2} \iota \tau^3 \iota \tau^4 \iota \tau^3 \iota \tau^5 \iota = \tau^6 \iota \tau^5 \iota \tau^3 \iota \tau^4 \iota \tau^3 \iota \tau^5 \iota = (\tau^6 \iota \tau^6) (\tau^6 \iota \tau^6) (\tau^4 \iota \tau^4 \iota \tau^4) (\tau^6 \iota \tau^6) (\tau^6 \iota \tau^6) \\
& = (\iota \tau^2 \iota) (\iota \tau^3 \iota) (\iota \tau^2 \iota) = \iota \tau^2 \tau^3 \tau^2 \iota = 1
\end{aligned}$$

On a donc vérifiée que le groupe fondamental de ce graphe F est bien envoyé dans le groupe fondamental de $C(H, \{\tau, \tau^{-1}, \iota\})$ par l'isomorphisme des revêtements universel induit par les deux catalogage sur $B(\{\tau, \tau^{-1}, \iota\})$. On peut donc appliquer le théorème final de la théorie des graphes de Cayley qui nous dit alors que l'on a un revêtement du graphe F sur $C(H, \{\tau, \tau^{-1}, \iota\})$.

BIBLIOGRAPHIE

[Berger-Gostiaux (1987)]

Marcel Berger & Bernard Gostiaux, *Géométrie différentielle: variétés, courbes et surfaces*, P.U.F., Paris, 1987

[Burnside (1955)]

W. Burnside, *Theory of Groups of Finite Order* (2nd ed), Dover Publications, New York, 1955

[Klein-Fricke (1890)]

Felix Klein & Robert Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, B.G. Teubner Verlag, Leipzig, 1890

[Maskit (1988)]

Bernard Maskit, *Kleinian Groups*, Springer Verlag, Berlin-Heidelberg, 1988

[Lyndon (1985)]

Roger Lyndon, *Groups and Geometry*, Cambridge University Press, Cambridge, 1985

[Lyndon-Schupp (1977)]

Roger Lyndon & Paul Schupp, *Combinatorial Group Theory*, Springer Verlag, 1977

[Wolf (1974)]

Joseph Wolf, *Spaces of Constant Curvature*, Publish or Perish, Boston, 1974

[Zieschang (1981)]

Heiner Zieschang, *Finite Groups of Mapping Classes of Surfaces*, Springer Verlag, Berlin-Heidelberg-New-York, 1981

TABLE DES MATIÈRES

Introduction.....	3
Chapitre I: Transformations Homographiques de $\widehat{\mathbb{K}}$	5
Droite complétée, action fractionnaire.....	8
Description de $\mathcal{H}(\widehat{\mathbb{K}})$	10
Sous-groupes normaux de $\mathcal{H}(\widehat{\mathbb{K}})$	13
Chapitre II: Graphes de Cayley.....	18
Revêtement universel.....	22
Graphes de Cayley.....	25
Bouquets et Catalogues.....	27
Chapitre III: Le cas de $\text{PSL}_2(\mathbb{F}_7)$	34
Chapitre IV: Isométries d'un quotient.....	40
Chapitre V: Groupes Triangulaires.....	44
Chapitre IV: Théorème d'Hurwitz.....	50
Chapitre VII: $\text{PSL}_2(\mathbb{F}_7)$ est un groupe d'Hurwitz	
Chapitre VIII: Réalisation.....	57
Dans notre cas.....	62
Quelques petits sous-groupes de $\text{PSL}_2(\mathbb{F}_7)$	64
Appendice au chapitre III: Validation des graphes supposés.....	70
Arbre maximal pour A_4	70
Arbre maximal pour S_4	71
Arbre maximal pour $\text{PSL}_2(\mathbb{F}_7)$	72
Bibliographie.....	77
Table des matières.....	78