Expression de $\mathrm{SL}_2(K)$ comme produit amalgamé de deux sous-groupes

Salim Rostam

Premier semestre 2014–2015

Le but de ce séminaire, qui a pour origine le livre *Arbres, amalgames,* SL_2 de Jean-Pierre Serre [1] est de démontrer le théorème 1.8. Avant d'énoncer ce théorème, on aura besoin de quelques notions.

Table des matières

1 Mise en place

1.1 Cadre et rappels

Soit K un corps (commutatif) muni d'une *valuation discrète* v, c'est-à-dire que :
— l'application v est un isomorphisme de K^* sur $\mathbb{Z}$;
— on a la relation $\forall x, y \in K, v(x+y) \geq \min(v(x), v(y))$ avec la convention $v(0) := +\infty$.

On note $\mathcal{O}$ l'anneau de valuation de K, c'est-à-dire $\mathcal{O} := \{x \in K : v(x) \geq 0\}$; en particulier, $K = \mathrm{Frac}(\mathcal{O})$.

Exemple 1.1. En définissant, pour un entier $n \in \mathbb{Z}^*$, la quantité $v_p(n)$ par $n = p^{v_p(n)}m$ où p est un nombre premier et $p \nmid m$, l'application v_p définit une valuation discrète sur $\mathbb{Q}$ (avec $v_p(\frac{a}{b}) := v_p(a) - v_p(b)$), d'anneau de valuation $\mathbb{Z}_{\langle p \rangle}$.

1. J.-P. Serre, *Arbres, amalgames,* SL_2 (3e édition). Astérisque N° 46, 1983.

Exemple 1.2. On définit de la même façon une valuation v sur $K[[X]]$ (l'anneau des séries formelles) par $F = X^{v(F)}G$ où le terme constant de $G \in K[[X]]$ est non nul, que l'on étend au corps des fractions $K((X))$; l'anneau de valuation est exactement $K[[X]]$.

On vérifie que $\mathcal{O}^\times = \{x \in \mathcal{O} : v(x) = 0\}$; ainsi, $\mathcal{O}$ est un anneau local d'unique idéal maximal $\{x \in \mathcal{O} : v(x) > 0\}$. De plus, si $\pi \in \mathcal{O}$ est un élément de valuation 1, on montre que tout idéal de $\mathcal{O}$ est de la forme $\langle \pi^n \rangle$ pour $n \in \mathbb{N}$, ainsi $\mathcal{O}$ est un anneau principal. En fait, on a même le résultat suivant.

Lemme 1.3. $\forall x \in K^*, x\mathcal{O} = \pi^{v(x)}\mathcal{O}$

Finalement, on note $k := \mathcal{O}/\pi\mathcal{O}$ le corps résiduel.

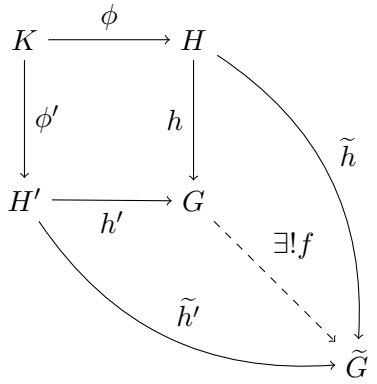
1.2 Produit amalgamé de deux groupes

(Dans cette section, la notation K ne désigne pas le corps précédent.) Soient H, H', K trois groupes et soient $\phi : K \to H$, $\phi' : K \to H'$ deux morphismes.

Théorème 1.4. *Il existe un unique groupe G et des uniques morphismes $h : H \to G$, $h' : H' \to G$ tels que :*

- *on a $h \circ \phi = h' \circ \phi'$;*
- *(PU) si $\widetilde{G}$ est un groupe et si $\widetilde{h} : H \to \widetilde{G}$, $\widetilde{h'} : H' \to \widetilde{G}$ sont deux morphismes qui vérifient $\widetilde{h} \circ \phi = \widetilde{h'} \circ \phi'$ alors il existe un unique morphisme $f : G \to \widetilde{G}$ tel que $\widetilde{h} = f \circ h$ et $\widetilde{h'} = f \circ h'$.*

Autrement dit, tout commute dans le diagramme suivant.



Démonstration. **Existence.** C'est en fait assez simple : on peut définir un tel groupe G par générateurs et relations par :

$$G := \langle H \amalg H' : \text{relations dans } H, H' \text{ et } \phi(y)\phi'(y)^{-1}\ \forall y \in K \rangle$$

(note [2]), les morphismes h et h' étant ceux induits par les inclusions (attention, h et h' ne sont pas nécessairement injectifs) ; en outre, on a bien $h \circ \phi = h' \circ \phi'$.

2. Un amalgame est (en métallurgie) un alliage : ici, c'est un peu comme si l'on faisait des chaînes de maillons les éléments de H ou H', en soudant sur K.

La propriété universelle découle directement de celle d'un groupe défini par générateurs et relations, que l'on peut utiliser car $h(\phi(y))h'(\phi'(y))^{-1} = 1 \ \forall y \in K$.

Unicité. Si $\widehat{G}$ est un groupe qui vérifie la propriété universelle avec les morphismes $\widehat{h}$ et $\widehat{h'}$, en considérant les morphismes $f : G \to \widehat{G}$ et $\widehat{f} : \widehat{G} \to G$ induits par les PU on trouve par unicité que f est un isomorphisme, d'inverse $\widehat{f}$.

□

Définition 1.5. *On dit que le groupe obtenu est le* produit amalgamé *de H et H' suivant K au moyen de ϕ, ϕ' ; on le note $H *_K H'$.*

Énonçons finalement deux lemmes.

Lemme 1.6. *Si $\alpha : H \to \alpha(H)$, $\alpha' : H' \to \alpha'(H')$ et $\beta : K \to \beta(K)$ sont des isomorphismes de groupes alors $H *_K H' \simeq \alpha(H) *_{\beta(K)} \alpha'(H')$ où le dernier amalgame se fait au moyen de $\psi := \alpha \circ \phi \circ \beta^{-1}$, $\psi' := \alpha' \circ \phi' \circ \beta^{-1}$.*

Démonstration. Il suffit de vérifier la propriété universelle de $\alpha(H) *_{\beta(K)} \alpha'(H')$. □

Soit G l'amalgame de H, H' suivant K au moyen de ϕ, ϕ' ; pour $s \in H \amalg H'$, on note $h^*(s) := \begin{cases} h(s) \text{ si } s \in H \\ h'(s) \text{ si } s \in H' \end{cases}$ (où h, h' sont les fonctions données par le théorème).

Lemme 1.7. *Pour tout $g \in G = H *_K H'$, il existe un unique $n \in \mathbb{N}$ et une unique suite $(s, s_1, \ldots, s_n)$ avec $s \in K$ et $s_i \in H \amalg H'$ qui vérifie :*

- *si $s_i \in H$ (resp. H') alors $s_{i+1} \in H'$ (resp. H) ;*
- *$s_i \notin K$;*
- *$g = h^*(s)h^*(s_1)\cdots h^*(s_n)$.*

Démonstration. C'est le théorème 1 ch. 1 du livre de Serre. □

1.3 Le théorème principal

On peut maintenant énoncer le théorème qui est l'objet de ce séminaire.

Théorème 1.8 (Ihara)**.** *On a l'isomorphisme suivant :*

$$\mathrm{SL}_2(K) \simeq \mathrm{SL}_2(\mathcal{O}) \underset{\Gamma}{*} \mathrm{SL}_2(\mathcal{O})$$

où $\Gamma := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) : c \in \langle \pi \rangle\}$, l'amalgame se faisant suivant les morphismes suivants :

$$\Gamma \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{\phi}{\mapsto} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O})$$

$$\Gamma \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{\phi'}{\mapsto} \begin{pmatrix} a & \pi b \\ \pi^{-1} c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O})$$

Remarque 1.9. Le morphisme ϕ' est bien à valeurs dans $\mathrm{SL}_2(\mathcal{O})$ car comme $c \in \langle \pi \rangle$ on a $\pi^{-1}c \in \mathcal{O}$.

Tout d'abord, on peut se demander à quoi sert ce théorème. On peut donner une application aux représentations linéaires de $\mathrm{SL}_2(\mathbb{Q}_p)$ (note [3]) : l'anneau de valuation de $(\mathbb{Q}_p, v_p)$ étant $\mathbb{Z}_p$ qui est compact, le groupe $\mathrm{SL}_2(\mathbb{Z}_p)$ est également compact. On peut alors appliquer la théorie des représentations des groupes compacts via l'amalgame précédent pour étudier les représentations de $\mathrm{SL}_2(\mathbb{Q}_p)$.

Le théorème va en fait être un cas particulier du théorème 2.1 ; avant d'énoncer ce dernier théorème, on a besoin de quelques notions supplémentaires.

1.4 Longueur d'un module

Dans cette courte partie, on va présenter la notion de longueur d'un module.

Définition 1.10. *Soit M un $\mathcal{O}$-module ; la* longueur *de M, notée $\ell(M)$, est définie comme étant le plus grand entier n tel qu'il existe une chaîne $\{0\} \subseteq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n \subseteq M$ de sous-$\mathcal{O}$-modules de M.*

Remarque 1.11. Si k est un corps, la longueur d'un k-module est sa dimension en tant que k-espace vectoriel.

Propriété 1.12. *Pour $n \in \mathbb{N}$ on a $\ell(\mathcal{O}/\pi^n\mathcal{O}) = n$.*

On retrouve en outre la propriété fondamentale vérifiée par la dimension pour les espaces vectoriels.

Proposition 1.13. *Si M est un $\mathcal{O}$-module de longueur finie et si N est un sous-$\mathcal{O}$-module de M, alors N et M/N sont de longueur finie et on a :*

$$\ell(M/N) = \ell(M) - \ell(N)$$

Démonstration. Voir Bourbaki, *Algèbre I*, ch. II, §1, n° 10, Proposition 16. □

1.5 Réseaux, classes de réseaux

Soit V un K-espace vectoriel de dimension 2.

Définition 1.14. *Un* réseau *de V est un sous-$\mathcal{O}$-module L de V de type fini qui engendre V en tant que K-espace vectoriel.*

Proposition 1.15. *Tout réseau de V est libre de rang 2.*

Démonstration. Soit L un réseau de V : comme le $\mathcal{O}$-module L est de type fini et que $\mathcal{O}$ est principal, on sait par le théorème de structure qu'il existe $r \in \mathbb{N}$ et $d_1, \ldots, d_s \in \mathcal{O}$ tels que $L \simeq \mathcal{O}^r \oplus \mathcal{O}/d_1\mathcal{O} \oplus \cdots \oplus \mathcal{O}/d_s\mathcal{O}$. Comme L est un sous-$\mathcal{O}$-module de V et comme V est un K-espace vectoriel (rappelons que $K = \mathrm{Frac}(\mathcal{O})$), on en déduit que V est sans torsion, et donc L également. Ainsi, $s = 0$ et $L \simeq \mathcal{O}^r$. On conclut que $r = 2$ *i.e.* L est libre de rang 2 car le K-espace vectoriel engendré par L est de dimension 2 (c'est V). □

3. Le corps $\mathbb{Q}_p$ des nombres p-adiques est défini comme étant la complétion de l'espace métrique $(\mathbb{Q}, |\cdot|_p)$ où $|r|_p := p^{-v_p(r)}$; en particulier, v_p s'étend à $\mathbb{Q}_p$.

Lemme 1.16. *Soient L et L' deux réseaux de V. Alors il existe $a \in \mathcal{O} \setminus \{0\}$ tel que $aL' \subseteq L$.*

Démonstration. Il suffit de multiplier une base de L' par un dénominateur commun. □

Corollaire 1.17. *Soient L, L' deux réseaux de V. Alors il existe (e_1, e_2) une $\mathcal{O}$-base de L et $a, b \in \mathbb{Z}$ tels que $(\pi^a e_1, \pi^b e_2)$ soit une $\mathcal{O}$-base de L'. De plus, $L' \subseteq L$ ssi $a, b \geq 0$.*

Démonstration. Immédiat par le lemme précédent et le théorème de la base adapté (que l'on peut appliquer car l'anneau $\mathcal{O}$ est principal). □

On a déjà utilisé le fait que si L est un réseau de V et si $x \in K^*$ alors xL reste un réseau de V ; on dit que L et xL sont des réseaux *équivalents*. Ainsi, le groupe K^* agit sur l'ensemble des réseaux de V et l'on définit l'ensemble des orbites :

$$X := \{\text{réseaux de V}\}/\text{réseaux équivalents}$$

Proposition 1.18. *Avec les notations du corollaire 1.17, l'entier $|a - b|$ ne dépend que des classes de L et L' dans X.*

Démonstration. En effet, pour $x, y \in K^*$ alors $(\pi^{v(x)} e_1, \pi^{v(x)} e_2)$ est une base de xL et $(\pi^{a+v(y)} e_1, \pi^{b+v(y)} e_2)$ est une base de yL' et on a bien $|(a+v(y)-v(x))-(b+v(y)-v(x))| = |a - b|$. La dépendance vis-à-vis de la base découle de l'invariance des coefficients dans le théorème de la base adaptée du corollaire 1.17. □

Cette proposition rend alors possible la définition suivante.

Définition 1.19. *Pour $\Lambda, \Lambda' \in X$, on note $d(\Lambda, \Lambda')$ l'entier $|a - b|$ précédent.*

Lemme 1.20. *Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Alors il existe $L' \in \Lambda'$ tel que $L' \subseteq L$, et de plus les trois conditions suivantes sont équivalentes :*

(i) L' est maximale (parmi les éléments de Λ' inclus dans L) ;

(ii) $L' \nsubseteq \pi L$;

(iii) L/L' est monogène.

Dans ce cas, on a $L/L' \simeq \mathcal{O}/\pi^n\mathcal{O}$ où $n := \ell(L/L') = d(L, L')$.

Remarque 1.21. En particulier :
- $d(\Lambda, \Lambda') = 0 \iff \Lambda = \Lambda'$;
- $d(\Lambda, \Lambda') = 1 \iff$ il existe $L \in \Lambda, L' \in \Lambda', L' \subseteq L$ tels que $L/L' \simeq k$ $(= \mathcal{O}/\pi\mathcal{O})$.

Remarque 1.22. Si L est un réseau de V alors L est un $\mathcal{O}$-module de longueur infinie. On peut quand même utiliser la proposition 1.13 sous la forme suivante : si $L'' \subseteq L' \subseteq L$ sont trois réseaux de V alors $\ell(L/L'') = \ell(L/L') + \ell(L'/L'')$ (car $L/L' \simeq (L/L'')/(L'/L'')$).

Démonstration. Tout d'abord, l'existence de $L' \in \Lambda'$ qui vérifie $L' \subseteq L$ est garantie par le lemme 1.16.

$(i) \implies (ii)$ Comme L' est maximale dans Λ' parmi les éléments inclus dans L, comme $L' \subsetneq \pi^{-1}L'$ on en déduit que $\pi^{-1}L' \nsubseteq L$ *i.e.* $L' \nsubseteq \pi L$.

$(ii) \implies (iii)$ Par le corollaire 1.17 il existe une base (e_1, e_2) de L et des entiers $a, b \geq 0$ tels que $(\pi^a e_1, \pi^b e_2)$ est une base de $L' \subseteq L$. Ainsi, comme $L' \nsubseteq \pi L = \mathcal{O}\pi e_1 \oplus \mathcal{O}\pi e_2$ on en déduit que a ou b est nul. Comme $L/L' \simeq \mathcal{O}/\pi^a\mathcal{O} \oplus \mathcal{O}/\pi^b\mathcal{O}$ on en déduit donc que L/L' est monogène.

$(iii) \implies (i)$ Le quotient L/L' est monogène donc par ce qui précède on en déduit qu'il existe une base (e_1, e_2) de L et un entier $n \in \mathbb{N}$ tel que $(\pi^n e_1, e_2)$ est une base de L'. Soit maintenant $\widetilde{L'} \in \Lambda'$ qui vérifie $L' \subseteq \widetilde{L'} \subseteq L$. On sait que $\exists x \in K^*$ tel que $\widetilde{L'} = xL'$. Comme $L' \subseteq \widetilde{L'}$ on en déduit que $m := v(x) \leq 0$. De plus, $(\pi^{n+m} e_1, \pi^m e_2)$ est alors une base de $xL' \subseteq L$ donc nécessairement que $m \geq 0$. Ainsi, $m = 0$ et donc $x \in \mathcal{O}^\times$ d'où $\widetilde{L'} = L'$ qui est donc maximal.

Finalement, si l'une de ces conditions équivalentes est vérifiée, alors on a $L/L' \simeq \mathcal{O}/\pi^n\mathcal{O}$ et donc $\ell(L/L') = n$, et par définition de d on a également $n = d(L, L')$. □

Remarque 1.23. On peut choisir L' vérifiant les trois conditions équivalentes précédentes.

2 Le théorème principal

On va dans cette section déduire le théorème 1.8 du théorème suivant, que l'on démontrera dans la section suivante.

Notons $G := \mathrm{SL}(V)$; pour $s \in G$ et L un réseau, l'ensemble sL reste un réseau et le groupe G agit ainsi sur l'ensemble des réseaux de V. De plus, comme pour $x \in K^*$ on $x \cdot sL = s \cdot xL$, le groupe G agit également sur X.

Théorème 2.1. *Si $\Lambda, \Lambda' \in X$ vérifient $d(\Lambda, \Lambda') = 1$, le groupe G est la somme de ses sous-groupes G_Λ et $G_{\Lambda'}$ amalgamée suivant $G_{(\Lambda,\Lambda')}$ (au moyen des inclusions).*

Remarque 2.2. La notation G_Λ désigne le stabilisateur de Λ pour l'action de G sur X. De plus, on a $G_{(\Lambda,\Lambda')}$ (stabilisateur de (Λ, Λ') pour l'action de G sur $X \times X$) $= G_\Lambda \cap G_{\Lambda'}$.

Lemme 2.3. *Soit $s \in G$ et soit L un réseau de V. On suppose que (e_1, e_2) est une base de L telle qu'il existe $a, b \in \mathbb{Z}$ tels que $(\pi^a e_1, \pi^b e_2)$ soit une base de sL. Alors $a + b = 0$.*

Démonstration. On peut écrire :

$$S := \mathrm{mat}_{(e_1,e_2)}\, s = \begin{pmatrix} \alpha\pi^a & \beta\pi^a \\ \gamma\pi^b & \delta\pi^b \end{pmatrix} \text{ avec } \alpha, \beta, \gamma, \delta \in \mathcal{O}$$

donc en notant $D := \left(\begin{smallmatrix} \pi^a & 0 \\ 0 & \pi^b \end{smallmatrix}\right)$ et $S' := \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ on a $S = DS'$. La matrice S' est à coefficients dans $\mathcal{O}$ et par la relation précédente elle est inversible. Avec $S' = \mathrm{mat}_{(e_1,e_2)}\, s'$ et $D' = \mathrm{mat}_{(e_1,e_2)}\, d'$, on a d'une part $s = ds'$ et d'autre part $sL = \mathcal{O}\pi^a e_1 \oplus \mathcal{O}\pi^b e_2 = dL$ d'où $s'L = L$. Ainsi, $s'^{-1}L = L$ donc $S'^{-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est à coefficients dans $\mathcal{O}$, d'où $S' \in \mathrm{GL}_2(\mathcal{O})$ et donc $\det S' \in \mathcal{O}^\times$. Finalement, en passant au déterminant dans l'égalité $S = DS'$ on trouve $1 = \pi^{a+b} \det S'$ donc $\pi^{a+b} \in \mathcal{O}^\times$ *i.e.* $a + b = 0$. □

Lemme 2.4. *Si $L \in \Lambda \in X$ alors $G_L = G_\Lambda$.*

Démonstration. Si s est un élément de G_L alors on a $sL = L$. Ainsi, on a également $s \cdot xL = x \cdot sL = xL$ pour tout $x \in K^*$ donc on a $s \in G_\Lambda$ Ainsi, $G_L \subseteq G_\Lambda$.

Prouvons maintenant l'inclusion réciproque ; soit $s \in G_\Lambda$. Ainsi, il existe $x \in K^*$ tel que $sL = xL$ et on veut prouver que $sL = L$. D'après le corollaire 1.17, il existe une base (e_1, e_2) de L et $a, b \in \mathbb{Z}$ tels que $(\pi^a e_1, \pi^b e_2)$ soit une base de sL. Ainsi, par le lemme précédent on a $a + b = 0$. Or, avec $c := v(x)$ la famille $(\pi^c e_1, \pi^c e_2)$ est une base de xL ; comme $xL = sL$ on en déduit que a et b sont égaux à c, et donc par la relation précédente on obtient $2c = 0$ *i.e.* $c = 0$ *i.e.* $x \in \mathcal{O}^\times$ et donc $xL = L$, d'où $s \in G_L$. □

Ainsi, par le lemme précédent on déduit du théorème 2.1 que si L et L' sont deux réseaux de V qui vérifient $d(L, L') = 1$ alors le groupe G est la somme de ses sous-groupes G_L et $G_{L'}$ amalgamée suivant leur intersection (qui n'est rien d'autre que $G_{(L,L')}$). Il reste encore un peu de travail à faire pour aboutir au théorème 1.8.

Lemme 2.5. *Soit L un réseau de V et soit $\mathcal{B}$ une base de L. Alors $G_L \simeq \mathrm{SL}_2(\mathcal{O})$ via l'isomorphisme* $\mathrm{mat}_\mathcal{B}$.

Démonstration. Soit $\mathcal{B} := (e_1, e_2)$ une base de L. Considérons l'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(K)$; c'est un isomorphisme sur son image. Cette image est bien constituée uniquement de matrices à coefficients dans $\mathcal{O}$; il reste donc à montrer qu'elle est $\mathrm{SL}_2(\mathcal{O})$ tout entier. Pour cela, soit $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O})$; on sait déjà qu'il existe $s \in \mathrm{SL}(V)$ tel que $\mathrm{mat}_\mathcal{B} s = M$. Ainsi, $sL \subseteq L$ et comme $M^{-1} \in \mathrm{SL}_2(\mathcal{O})$ on conclut que $s \in G_L$. □

Soit L un réseau de V et soit $\mathcal{B} = (e_1, e_2)$ une base de L. Soit $L' \subseteq L$ un réseau qui vérifie $L/L' \simeq k$: c'est possible, il suffit par exemple de poser $L' := \mathcal{O}e_1 \oplus \mathcal{O}\pi e_2$. Avec Λ (resp. Λ') la classe de L (resp. L') dans X, d'après la remarque 1.21 on est ainsi dans les hypothèses du théorème 2.1 ; il reste à comprendre ce qu'est l'image de $G_{L'}$ et de $G_L \cap G_{L'}$ par le morphisme $\mathrm{mat}_\mathcal{B}$ (qui est bien sûr défini sur $\mathrm{GL}(V)$ tout entier).

Remarque 2.6. On vient de montrer que (si X est non vide, cf. partie 3.2.2) X n'est pas réduit à un point, et même qu'il existe $\Lambda, \Lambda' \in X$ tels que $d(\Lambda, \Lambda') = 1$.

Lemme 2.7. *Avec les notations précédentes, pour $s \in \mathrm{SL}(V)$ en notant $\mathrm{mat}_\mathcal{B} s = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ on a :*

$$s \in G_{L'} \text{ ssi } \begin{cases} a, d \in \mathcal{O} \\ c \in \mathcal{O}\pi \\ b \in \mathcal{O}\pi^{-1} \end{cases}$$

Démonstration. Supposons que $s \in G_{L'}$. Ainsi, $sL' = L'$ donc en particulier $se_1 = ae_1 + ce_2 \in L' = \mathcal{O}e_1 \oplus \mathcal{O}\pi e_2$ donc $a \in \mathcal{O}$ et $c \in \mathcal{O}\pi$. De même on trouve $b\pi \in \mathcal{O}$ et $d \in \mathcal{O}$; on vérifie que ces conditions sont suffisantes. □

On peut maintenant démontrer le théorème 1.8 ; on garde les notations précédentes. Considérons l'application suivante :

$$f : \left| \begin{array}{ccc} \mathrm{mat}_\mathcal{B}(G_{L'}) & \longrightarrow & \mathrm{SL}_2(\mathcal{O}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} a & \pi b \\ \pi^{-1} c & d \end{pmatrix} \end{array} \right.$$

Tout d'abord, f arrive bien dans SL_2, et bien dans les matrices à coefficients dans $\mathcal{O}$ par le lemme précédent. On vérifie que f est un morphisme, injectif et surjectif. Ainsi, on sait par le théorème 2.1 que $G \simeq G_L *_{G_L \cap G_{L'}} G_{L'}$ (au moyen des inclusions) donc par le lemme 1.6 on a, avec $\Gamma := \mathrm{mat}_{\mathcal{B}}(G_L \cap G_{L'})$:

$$G \simeq \mathrm{mat}_{\mathcal{B}}(G_L) \underset{\Gamma}{*} f(\mathrm{mat}_{\mathcal{B}}(G_{L'})) = \mathrm{SL}_2(\mathcal{O}) \underset{\Gamma}{*} \mathrm{SL}_2(\mathcal{O})$$

au moyen de $\psi = \mathrm{mat}_{\mathcal{B}} \circ \iota \circ \mathrm{mat}_{\mathcal{B}}^{-1} = \iota$ et $\psi' = f \circ \mathrm{mat}_{\mathcal{B}} \circ \iota \circ \mathrm{mat}_{\mathcal{B}}^{-1} = f|_\Gamma$ où ι désigne à chaque fois l'inclusion adéquate.

Finalement, il reste à expliciter le groupe Γ. Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O})$; on peut écrire de manière unique $M = \mathrm{mat}_{\mathcal{B}}\, s$ avec $s \in G_L$. Ainsi, $M \in \Gamma$ ssi $s \in G_L \cap G_{L'}$ ssi $c \in \mathcal{O}\pi$ par le lemme précédent (car $b \in \mathcal{O} \subseteq \mathcal{O}\pi^{-1}$). On a bien démontré le théorème 1.8.

3 Démonstration du théorème 2.1

3.1 Quelques éléments de théorie des graphes

On peut oublier dans cette section les notations X, G que l'on a attribuées.

3.1.1 Graphes

Définition 3.1. *Un* graphe Γ *est la donnée d'un ensemble de sommet S, d'un ensemble d'arêtes A et de deux applications*

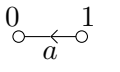
$$\left|\begin{array}{ccc} A & \to & S \times S \\ a & \mapsto & (o(a), t(a)) \end{array}\right. \quad \textit{et} \quad \left|\begin{array}{ccc} A & \to & A \\ a & \mapsto & \bar{a} \end{array}\right.$$

qui vérifient pour tout $a \in A$ les conditions suivantes :

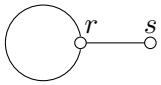
- $\bar{\bar{a}} = a$;
- $\bar{a} \neq a$;
- $o(a) = t(\bar{a})$.

Remarque 3.2.
- La définition implique que $o(\bar{a}) = t(\bar{\bar{a}}) = t(a)$.
- L'ensemble A n'est pas forcément un sous-ensemble de $S \times S$. On gardera surtout à l'esprit les conditions sur l'application $a \mapsto \bar{a}$; en particulier, on peut avoir $o(a) = t(a)$ (voir exemple 3.4).

Exemple 3.3. L'ensemble de sommets $S := \{0, 1, 2\}$ et l'ensemble d'arêtes $A := \{(0,1), (1,0)\}$ avec $(o,t)(0,1) := (0,1)$ (et nécessairement $\overline{(0,1)} = (1,0)$) est un graphe, représenté sur la figure suivante (où $a := (1,0)$).



Exemple 3.4. Le graphe suivant :



peut être considéré comme étant constitué de l'ensemble de sommets $S := \{r, s\}$ et de l'ensemble d'arêtes $A := \{(r, r, 0), (r, r, 1), (r, s, 0), (s, r, 0)\}$ avec $\forall (u, v, \epsilon) \in A$:

$$\begin{aligned}(o, t)((u, v, \epsilon)) &:= (u, v)\\ \overline{(u, v, 0)} &:= (v, u, 0) \text{ si } u \neq v\\ \overline{(u, u, \epsilon)} &:= (u, u, 1 - \epsilon)\end{aligned}$$

Définition 3.5. *Soit $\Gamma = (S, A, o, t, \bar{\cdot})$ un graphe ; on dit qu'un groupe G* opère *sur Γ si G opère sur S ainsi que sur A et si ces deux actions sont compatibles avec la structure de graphe, i.e. $\forall g \in G, \forall a \in A, (g \cdot o(a), g \cdot t(a)) = (o(g \cdot a), t(g \cdot a))$ et $\overline{g \cdot a} = g\bar{a}$.*

Définition 3.6. *On dit que G agit* sans inversion *sur un graphe $(S, A, \bar{\cdot})$ si $\forall g \in G, \forall a \in A, ga \neq \bar{a}$.*

Théorème 3.7. *Si G agit* sans inversion *sur un graphe (S, A), on peut munir $(S/G, A/G)$ d'une structure de graphe (on parle de graphe quotient).*

Remarque 3.8. Si G agit sur un ensemble X, on a noté X/G l'ensemble des orbites de X pour l'action de G.

Démonstration. On vérifie simplement les axiomes de la définition d'un graphe.

- L'application $A/G \to X/G \times X/G$ est donnée par $Ga \mapsto (Go(a), Gt(a))$ et l'application $A/G \to A/G$ est donnée par $Ga \mapsto G\bar{a}$. Ces définitions sont bien cohérentes d'après la définition de l'action sur un graphe.
- On a $\overline{\overline{Ga}} = \overline{G\bar{a}} = G\bar{\bar{a}} = Ga$ et $o(Ga) = Go(a) = Gt(\bar{a}) = t(G\bar{a}) = t(\overline{Ga})$.
- On a $\overline{Ga} = G\bar{a} \neq Ga$ car si $G\bar{a} = Ga$ alors il existerait $g, h \in G$ tels que $g\bar{a} = ha$ *i.e.* $\bar{a} = g^{-1}ha$ ce qui est impossible puisque G opère sans inversion.

□

Définition 3.9. *Soient $\Gamma = (S, A, o, t, \bar{\cdot})$ et $\widehat{\Gamma} = (\widehat{S}, \widehat{A}, \hat{o}, \hat{t}, \hat{\cdot})$ deux graphes. On dit que $(\sigma, \alpha) : (S, A) \to (\widehat{S}, \widehat{A})$ est un* morphisme de graphes *de Γ vers $\widehat{\Gamma}$ si :*

- $(\hat{o} \circ \alpha, \hat{t} \circ \alpha) = (\sigma \circ o, \sigma \circ t)$ *i.e.* $\forall a \in A, \hat{o}(\alpha(a)) = \sigma(o(a))$ *et* $\hat{t}(\alpha(a)) = \sigma(t(a))$ *;*
- $\hat{\cdot} \circ \alpha = \alpha \circ \bar{\cdot}$ *i.e.* $\forall a \in A, \widehat{\alpha(a)} = \alpha(\bar{a})$.

Un morphisme est dit injectif *(resp.* surjectif*) si ses deux composantes sont injectives (resp. surjectives).*

Définition 3.10. *Soit G un groupe agissant sans inversion sur un graphe Γ. On dit qu'un sous-graphe T de Γ est un* domaine fondamental *pour l'action de G si la projection canonique $T \to \Gamma/G$ est un isomorphisme de graphes.*

3.1.2 Arbres

Définition 3.11. *Soit $\Gamma = (S, A, o, t, \bar{\cdot})$ un graphe.*
- *Un* chemin *de longueur $n \geq 1$ est une suite d'arêtes $(a_1, \ldots, a_n)$ qui vérifie $\forall i \in [\![1, n-1]\!], t(a_i) = o(a_{i+1})$.*
- *On dit que $s, s' \in S$ sont reliés par un chemin s'il existe un chemin $(a_1, \ldots, a_n)$ qui vérifie $o(a_1) = s$ et $t(a_n) = s'$.*
- *Si $(a_1, \ldots, a_n)$ est un chemin, on dit que (a_i, a_{i+1}) est un* aller-retour *si $a_{i+1} = \bar{a_i}$.*

Remarque 3.12. S'il existe un chemin de s à s' alors il en existe un sans aller-retour.

Définition 3.13. *Un* circuit *dans Γ est un chemin $(a_1, \ldots, a_n)$ (avec $n \geq 1$) sans aller-retour qui vérifie les deux conditions suivantes :*
- *$t(a_n) = o(a_1)$;*
- *les $t(a_i)$, $1 \leq i \leq n$ sont distincts.*

Lemme 3.14. *Si $\gamma = (a_1, \ldots, a_n)$ (avec $n \geq 1$) est un chemin dans Γ sans aller-retour qui vérifie la condition $t(a_n) = o(a_1)$, alors il existe $1 \leq i < j \leq n$ tels que $(a_{i+1}, a_{i+2}, \ldots, a_j)$ soit un circuit dans Γ.*

Démonstration. Il suffit de considérer la première collision des $t(a_j)$. □

Définition 3.15. *On dit qu'un graphe non vide est un* arbre *s'il est connexe (i.e. deux sommets distincts sont toujours reliés par un chemin) et sans circuit.*

3.2 Clé du théorème 2.1

On reprend ici les notations $X = \{\text{réseaux de } V\}/\text{réseaux équivalents}$ et $G = \mathrm{SL}(V)$. Remarquons que l'application d définie lors de la définition 1.19 sur $X \times X$ munit notre ensemble de classes de réseaux X d'une structure de graphe, deux sommets $\Lambda, \Lambda' \in X$ étant reliés par une arête si $d(\Lambda, \Lambda') = 1$ (on peut donc supposer que l'ensemble des arêtes est un sous-ensemble de $X \times X$).

Propriété 3.16. *L'action du groupe G sur l'ensemble X est une action sur le graphe X, l'action sur les arêtes étant donnée par $g \cdot (\Lambda, \Lambda') := (g\Lambda, g\Lambda')$.*

Démonstration. Tout d'abord, il faut vérifier que l'action donnée sur les arêtes envoie bien une arête sur une arête, *i.e.* si $d(\Lambda, \Lambda') = 1$ alors $d(g\Lambda, g\Lambda') = 1$; c'est immédiat car si L, L' sont des bons représentants (cf. lemme 1.20) alors $\ell(gL, gL') = 1$. On vérifie immédiatement le reste de la définition de l'action d'un groupe sur un graphe. □

Voici maintenant la clé du théorème 2.1 (où l'on oublie la notation G).

Théorème 3.17. *Soit y une arête d'un graphe Γ avec $(o, t)(y) = (P, Q)$; soit G un groupe qui agit sans inversion sur Γ et tel que $T := P \overset{y}{\circ\!\!\longrightarrow\!\!\circ} Q$ soit un domaine fondamental pour cette action. Si Γ est un arbre alors le morphisme $G_P *_{G_y} G_Q \to G$ induit par les inclusions est un isomorphisme.*

Remarque 3.18. Rappelons que $G_y = G_P \cap G_Q$; l'amalgame se fait au moyen des deux inclusions.

Pour pouvoir appliquer ce théorème, il suffit donc de :
— montrer que l'action de G sur le graphe X est sans inversion ;
— trouver une arête qui est un domaine fondamental pour X (on va en fait montrer ce point en dernier pour une raison qui apparaitra dans la preuve) ;
— montrer que notre graphe X est un arbre.

Le théorème s'appliquera alors de suite au théorème 2.1, en utilisant le lemme 2.4.

Lemme 3.19. *Soient $\Lambda \in X$ et $s \in G$. Alors $d(\Lambda, s\Lambda)$ est pair.*

Démonstration. Soit $L \in \Lambda$; par le corollaire 1.17 il existe une base (e_1, e_2) de L et des entiers $a, b \in \mathbb{Z}$ tels que $(\pi^a e_1, \pi^b e_2)$ soit une base de sL. D'après le lemme 2.3, on a $a + b = 0$; ainsi, par définition de d on a $d(L, sL) = |a - b| = 2|a|$ qui est pair. Par la proposition 1.18 on a donc $d(\Lambda, s\Lambda) = d(L, sL)$ pair. □

3.2.1 L'action de G sur le graphe X est sans inversion

Soit (Λ, Λ') une arête de X ; on a par définition $d(\Lambda, \Lambda') = 1$. Supposons qu'un élément $s \in G$ inverse cette arête ; en particulier, on a $s\Lambda = \Lambda'$. On a $1 = d(\Lambda, \Lambda') \overset{\text{prop. 1.18}}{=} d(L, sL)$ qui est pair par le lemme 3.19, ce qui est absurde.

3.2.2 Le graphe X est un arbre

Tout d'abord, remarquons que X est non vide car il existe des réseaux de V : il existe une base (e_1, e_2) de V en tant que K-espace vectoriel et $\mathcal{O}e_1 \oplus \mathcal{O}e_2$ est alors un réseau.

Le graphe X est connexe Soit $\Lambda \neq \Lambda'$ deux sommets de X ; d'après le lemme 1.16, on peut trouver des représentants $L \in \Lambda$, $L' \in \Lambda'$ qui vérifient $L' \subseteq L$. Avec $n := d(L, L')$, on sait que $L/L' \simeq \mathcal{O}/\pi^n\mathcal{O}$; ainsi, les seuls sous-$\mathcal{O}$-modules de L/L' sont en bijection avec les $\pi^m\mathcal{O}/\pi^n\mathcal{O}$ pour $0 \leq m \leq n$. Ainsi, la suite $L' = L_n \subseteq \cdots \subseteq L_0 = L$ des sous-$\mathcal{O}$-modules obtenus par image réciproque vérifie $L_m/L_{m+1} \simeq \pi^m\mathcal{O}/\pi^{m+1}\mathcal{O} \simeq k$ d'où $d(L_{m+1}, L_m) = 1$ et $(\Lambda_0, \ldots, \Lambda_n)$ est un chemin reliant Λ à Λ'. (On a en fait donné les sommets du chemin, les arêtes sont les $(\Lambda_i, \Lambda_{i+1})$.)

Le graphe X est sans circuit Soit $\Lambda_0, \ldots, \Lambda_N$ la suite des sommets d'un chemin sans aller-retour ; on veut montrer que $\Lambda_0 \neq \Lambda_N$. D'après le lemme 1.20, on peut trouver des représentants $L_n \in \Lambda_n$ tels que $L_{n-1} \supseteq L_n$ et $L_{n-1}/L_n \simeq k$ (pour n allant de 0 à N).

Montrons par récurrence sur n que $L_n \nsubseteq \pi L_0$ et $d(L_0, L_n) = n$; comme $d(\Lambda_0, \Lambda_n) = d(L_0, L_n)$ on aura bien $d(\Lambda_0, \Lambda_n) = n$ et donc $\Lambda_0 \neq \Lambda_n$.

L'initialisation est claire car $d(L_0, L_1) = 1$ par définition d'une arête et par le lemme 1.20 on a $L_1 \nsubseteq \pi L_0$. Reste à vérifier l'hérédité ; on suppose donc la propriété vraie pour $n - 1 \geq 1$ et montrons-la au rang n.

Tout d'abord, par la remarque 1.22 on a la relation $\ell(L_0/L_n) = \sum_{i=0}^{n-1} \ell(L_i/L_{i+1})$ et comme $L_i/L_{i+1} \simeq k$ on a $\ell(L_i/L_{i+1}) = 1$ et donc $\ell(L_0/L_n) = n$. D'après le lemme 1.20, il suffit donc de montrer que $L_n \nsubseteq \pi L_0$ pour obtenir $d(L_0, L_n) = n$.

— Montrons que $\pi L_{n-1} \subseteq L_n, \pi L_{n-2} \subseteq L_{n-1}$. Comme $L_n \subseteq L_{n-1} \subseteq \cdots \subseteq L_0$, les inclusions $\pi L_{n-1} \subseteq \pi L_{n-1}$ et $L_n \subseteq L_{n-1}$ sont claires. De plus, comme $L_{i-1}/L_i \simeq k = \mathcal{O}/\pi\mathcal{O}$ on a $\pi L_{i-1} \subseteq L_i$ ce qui montre les deux dernières inclusions.

— Ainsi, $L_n/\pi L_{n-1}$ et $\pi L_{n-2}/\pi L_{n-1}$ sont deux sous-k-espaces vectoriels de $L_{n-1}/\pi L_{n-1} \simeq \mathcal{O}/\pi\mathcal{O} \oplus \mathcal{O}/\pi\mathcal{O} \simeq k^2$; montrons que ce sont des droites distinctes.

  — Comme $L_n \neq \pi L_{n-1}$ (conséquence du lemme 1.20) et que $L_n \neq L_{n-1}$ on a nécessairement $\dim_k L_n/\pi L_{n-1} = 1$.

  — On a $\pi L_{n-2}/\pi L_{n-1} \simeq L_{n-2}/L_{n-1} \simeq k$ donc c'est bien une droite.

  — Comme le chemin de sommets $\Lambda_{n-2}, \Lambda_{n-1}, \Lambda_n$ est sans aller-retour, on a $\Lambda_{n-2} \neq \Lambda_n$ donc en particulier $\pi L_{n-2} \neq L_n$ donc $\pi L_{n-2}/\pi L_{n-1} \neq L_n/\pi L_{n-1}$.

— Ainsi, comme $L_{n-1}/\pi L_{n-1}$ est un k-plan on a $L_n/\pi L_{n-1} + \pi L_{n-2}/\pi L_{n-1} = L_{n-1}/\pi L_{n-1}$ donc $L_n + \pi L_{n-2} = L_{n-1}$. Par hypothèse de récurrence on a $L_{n-1} \nsubseteq \pi L_0$; ainsi, comme $\pi L_{n-2} \subseteq \pi L_0$ on a bien $L_n \nsubseteq \pi L_0$.

Finalement, on a bien montré que le graphe X est un arbre.

Remarque 3.20. Le graphe X étant un arbre, si Λ, Λ' sont deux sommets de X il existe un unique chemin sans aller-retour reliant Λ à Λ'. La longueur de ce chemin est, par la preuve précédente, exactement $d(\Lambda, \Lambda')$. De plus, si $d(\Lambda, \Lambda') = 1$, par unicité du chemin on obtient (si Λ'' est un troisième sommet) :

$$d(\Lambda, \Lambda'') \text{ et } d(\Lambda', \Lambda'') \text{ n'ont pas la même parité.}$$

En effet, si le chemin γ reliant Λ à Λ'' passe par Λ' on a $d(\Lambda, \Lambda'') = d(\Lambda', \Lambda'') + 1$ et sinon le chemin qui relie Λ' à Λ'' est (Λ', γ) d'où $d(\Lambda, \Lambda'') = d(\Lambda', \Lambda'') - 1$.

3.2.3 Il existe une arête de X qui est un domaine fondamental

Tout d'abord, remarquons que d'après la remarque 2.6 il existe au moins une arête dans le graphe X. Ainsi, soit (Λ_0, Λ_0') une arête du graphe X ; on va montrer que le graphe T donné par $\Lambda_0 \circ\!\!-\!\!-\!\!\circ \Lambda_0'$ est un domaine fondamental de X pour l'action de G.

Pour ce faire, considérons la projection canonique $f : T \to X/G$ et montrons que c'est un isomorphisme. Tout d'abord, l'injectivité de f sur les arêtes est garantie par le fait que l'action de G est sans inversion ; l'injectivité sur les sommets découle du lemme 3.19.

L'application induite sur les sommets est surjective Soit $\Lambda_1 \in X$; on veut montrer qu'il existe $s \in G$ tel que $s\Lambda_1 = \Lambda_0$ ou $s\Lambda_1 = \Lambda_0'$. Compte-tenu du lemme 3.19, on va montrer que l'on est dans le premier cas si $d(\Lambda_0, \Lambda_1)$ est pair, et dans le second sinon (*i.e.* si $d(\Lambda_0', \Lambda_1)$ est pair, cf. remarque 3.20).

Supposons donc que $d(\Lambda_0, \Lambda_1)$ soit pair ; appelons $2n$ cette distance. Par le corollaire 1.17, il existe $L_0 \in \Lambda_0$ et $L_1 \in \Lambda_1$, il existe (e_1, e_2) base de L_0 et $a \geq b \geq 0$ tels que $L_1 = \mathcal{O}\pi^a e_1 \oplus \mathcal{O}\pi^b e_2$. Par la proposition 1.18, on a $2n = |a - b| = a - b$; ainsi, on a $\Lambda_1 \ni \pi^{n-a} L_1 = \mathcal{O}\pi^n e_1 \oplus \mathcal{O}\pi^{-n} e_2$. Si $s \in G$ vérifie $\mathrm{mat}_{(e_1,e_2)}\, s = \begin{pmatrix} \pi^n & 0 \\ 0 & \pi^{-n} \end{pmatrix}$ alors on a $\pi^{n-a} L_1 = sL_0$ et donc $\Lambda_1 = s\Lambda_0$: c'est bien ce que l'on voulait. On conclut par la remarque initiale dans le cas où $d(\Lambda_1, \Lambda_0)$ est impair.

L'application induite sur les arêtes est surjective Soit $\Lambda_1 \circ\!\!-\!\!-\!\!\circ \Lambda_1'$ une arête du graphe X ; par ce qui précède, quitte à permuter Λ_1 et Λ_1', on peut supposer que $\Lambda_0 \in G\Lambda_1$, *i.e.* $\exists s \in G, s\Lambda_1 = \Lambda_0$. On veut en plus prouver que l'on peut choisir un tel s qui vérifie $s\Lambda_1' = \Lambda_0'$: comme $s\Lambda_1'$ est de toutes façons relié à Λ_0, il suffit de montrer que l'action de G_{Λ_0} sur les sommets reliés à Λ_0 est transitive.

Soit $L_0 \in \Lambda_0$ et soit Λ_1 un sommet relié à Λ_0. Par le lemme 1.20, on sait qu'il existe $L_1 \in \Lambda_1$ tel que $L_1 \subseteq L_0$, $L_0/L_1 \simeq k$ et $L_1 \nsubseteq \pi L_0$. Comme avant, on en déduit que $L_1/\pi L_0$ est une droite vectorielle du k-plan $L_0/\pi L_0$.

Il suffit donc de prouver que G_{L_0} ($= G_{\Lambda_0}$ par le lemme 2.4) agit transitivement sur les droites de $L_0/\pi L_0$, l'action étant donnée par celle de $G_{L_0} \subseteq \mathrm{Aut}(L_0/\pi L_0)$ (bien définie car si $s \in G_{L_0}$ alors $sL_0 = L_0$ et $s(\pi L_0) = \pi L_0$). Comme $\dim_k L_0/\pi L_0 = 2$ et que l'action de $\mathrm{SL}_2(k)$ sur $\mathbb{P}^1(k)$ est transitive, il suffit de montrer que l'image de l'application composée $G_{L_0} \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{} \mathrm{SL}_2(\mathcal{O}) \to \mathrm{SL}_2(k)$ est surjective, où $\mathcal{B}$ désigne une base de L_0.

Par le lemme 2.5, l'application $\mathrm{mat}_{\mathcal{B}}$ induit un isomorphisme de G_{L_0} sur $\mathrm{SL}_2(\mathcal{O})$ donc il reste à montrer que la flèche $\mathrm{SL}_2(\mathcal{O}) \to \mathrm{SL}_2(k)$ est surjective. Soit $\overline{M} = \left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{smallmatrix}\right) \in \mathrm{SL}_2(k)$ avec $a, b, c, d \in \mathcal{O}$. Comme $\det \overline{M} = 1$, l'un des coefficients de $\overline{M}$ est non nul, disons $\bar{d}$ (les autres cas se traitant de la même façon). Ainsi, $d \notin \langle \pi \rangle$ donc comme $\langle \pi \rangle$ est l'unique idéal maximal de l'anneau $\mathcal{O}$ on en déduit que $d \in \mathcal{O}^\times$. Avec $u \in \mathcal{O}$ vérifiant $ad - bc = 1 + \pi u$, la matrice $M := \left(\begin{smallmatrix} a - \pi u d^{-1} & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathcal{O})$ a pour image $\overline{M}$ dans $\mathrm{SL}_2(k)$ et son déterminant est $ad - bc - \pi u = 1$.

3.2.4 Démonstration du théorème 3.17

Précisons encore une fois que dans le théorème 3.17, l'amalgame $G_P *_{G_y} G_Q$ se fait par rapport aux inclusions $G_y \hookrightarrow G_P, G_Q$ et le morphisme $G_P *_{G_y} G_Q$ et celui qui est induit par les inclusions $G_P, G_Q \hookrightarrow G$ (cf. propriété universelle).

Lemme 3.21. *Si le graphe Γ est connexe alors $G = \langle G_P \cup G_Q \rangle$.*

Démonstration. Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$; on va montrer que $G'T \sqcup (G \setminus G')T = \Gamma$. Comme T est un domaine fondamental, la réunion fait bien Γ tout entier et il reste donc à montrer que cette réunion est disjointe.

Soit R un sommet du graphe $G'T \cap (G \setminus G')T$; il existe $s' \in G'$ et $s \in G \setminus G'$ tels que $R \in \{s'P, s'Q\}$ et $R \in \{sP, sQ\}$. Si $R = s'P = sP$ alors $s^{-1}s' \in G_P$ donc $s \in G_P \subseteq G'$ ce qui est impossible ; le cas $R = s'Q = sQ$ étant analogue, on a nécessairement $R = s'P = sQ$ ou $R = s'Q = sP$. Dans les deux cas, on obtient un élément de G qui envoie P sur Q : c'est absurde car $T = [P \circ\!\!-\!\!-\!\!\circ Q]$ est un domaine fondamental de Γ pour l'action de G et donc $T \xrightarrow{\sim} \Gamma/G$. Finalement, un tel R n'existe donc pas *i.e.* $G'T \cap (G \setminus G')T = \emptyset$.

Le graphe Γ étant connexe et ayant $G'T \neq \emptyset$ (car $G' \neq \emptyset$), par la décomposition précédente on a ($\Gamma = G'T$ et en particulier) $G \setminus G' = \emptyset$, d'où $G = G'$. □

Lemme 3.22. *Si le graphe Γ est sans circuit alors $G_P *_{G_y} G_Q \to G$ est injectif.*

Démonstration. On va en fait montrer que la contraposée : supposons que $\mathcal{G} := G_P *_{G_y} G_Q \to G$ ne soit pas injectif est montrons que Γ possède un circuit. Par hypothèse, il existe un élément $g \in \mathcal{G}$, $g \neq 1$, tel que l'image de g dans G soit triviale. Appliquant le lemme 1.7, on sait qu'il existe $n \in \mathbb{N}, s \in G_y$ et $s_1, \dots, s_n \in G_P \amalg G_Q$ qui vérifient :

— si $s_i \in G_P$ (resp. G_Q) alors $s_{i+1} \in G_Q$ (resp. G_P) ;
— $s_i \notin G_y$;
— $g = h^*(s)h^*(s_1)\cdots h^*(s_n)$ (notation h^* du lemme 1.7).

Comme l'image de $g \neq 1_{\mathcal{G}}$ dans G est 1_G on a nécessairement $n \geq 1$. En notant $g_1 := ss_1$ et $g_i := s_i \ \forall i \in [\![2, n]\!]$, on a $g_i \in G_P \amalg G_Q$ ainsi que les conditions suivantes :

— si $g_i \in G_P$ (resp. $g_i \in G_Q$) alors $g_{i+1} \in G_Q$ (resp. $g_{i+1} \in G_P$) ;
— $g_i \notin G_y$;
— $g_1 \cdots g_n = 1_G$;

remarquons que en particulier $n \geq 2$ (sinon $g_1 = 1_G \in G_y$).

Notons $R_i \in \{P, Q\}$ les points qui vérifient $g_i \in G_{R_i}$ et $z_i \in \{y, \overline{y}\}$ les arêtes qui vérifient $o(z_i) = R_i$; on a en particulier $R_i \neq R_{i+1}$ et $z_{i+1} = \overline{z_i}$. On considère alors le chemin suivant :

$$\gamma := (g_1 z_1, g_1 g_2 z_2, \dots, g_1 \cdots g_{n-1} z_{n-1}, g_1 \cdots g_n z_n)$$

— C'est bien un chemin car $t(g_1 \cdots g_i z_i) = g_1 \cdots g_i t(z_i) = g_1 \cdots g_i o(z_{i+1}) = g_1 \cdots g_i R_{i+1} = g_1 \cdots g_i g_{i+1} R_{i+1} = o(g_1 \cdots g_{i+1} z_{i+1})$.
— Ce chemin est sans aller-retour car si $g_1 \cdots g_{i-1} z_{i-1} = \overline{g_1 \cdots g_i z_i}$ alors $z_{i-1} = g_i \overline{z_i}$ donc $g_i \in G_{z_{i-1}} = G_y$ ce qui est impossible.

Construisons maintenant un circuit à partir de γ.

— Si $z_{n-1} = z_1$, comme alors $z_n = \overline{z_1}$, on a $t(g_1 \cdots g_n z_n) = t(z_n) = o(z_1) = o(g_1 z_1)$ donc on peut appliquer le lemme 3.14 à γ pour en déduire que Γ possède un circuit.
— Supposons au contraire $z_{n-1} \neq z_1$; considérons le chemin sans aller-retour suivant :

$$\check{\gamma} := (g_1 z_1, g_1 g_2 z_2, \dots, g_1 \cdots g_{n-1} z_{n-1})$$

On a $z_{n-1} = \overline{z_1}$, $R_{n-1} \neq R_1 = R_n$ et $z_n = z_1$. Ainsi, $t(g_1 \cdots g_{n-1} z_{n-1}) = o(g_1 \cdots g_n z_n) = o(z_n) = o(z_1) = o(g_1 z_1)$. On peut donc appliquer le lemme 3.14 à $\check{\gamma}$ pour en déduire que Γ possède un circuit.

□

Démonstration du théorème 3.17. On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$. D'une part, comme Γ est sans circuit le lemme 3.22 nous garantit que le morphisme f est injectif. D'autre part, par définition de f on a $\forall g \in G_P \amalg G_Q, f(h^*(g)) = g$ donc l'image de f contient $G_P \cup G_Q$: comme le graphe Γ est connexe, on en déduit par le lemme 3.21 que le morphisme f est surjectif. Finalement, f et un isomorphisme. □