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

Salim Rostam
Sous la direction de Yongquan Hu

Premier semestre 2014–2015

Sommaire

Cadre

On considère l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie par $n = p^{v_p(n)}m$; elle s'étend de manière naturelle à $\mathbb{Q}$ (avec la convention $v_p(0) := +\infty$).

Cadre

On considère l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie par $n = p^{v_p(n)} m$; elle s'étend de manière naturelle à $\mathbb{Q}$ (avec la convention $v_p(0) := +\infty$). L'application $|\cdot|_p : \mathbb{Q} \to \mathbb{Q}_+$ définie par $|r|_p := p^{-v_p(r)}$ définit une métrique sur $\mathbb{Q}$; on note $\mathbb{Q}_p$ son complété.

Cadre

On considère l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie par $n = p^{v_p(n)} m$; elle s'étend de manière naturelle à $\mathbb{Q}$ (avec la convention $v_p(0) := +\infty$). L'application $|\cdot|_p : \mathbb{Q} \to \mathbb{Q}_+$ définie par $|r|_p := p^{-v_p(r)}$ définit une métrique sur $\mathbb{Q}$; on note $\mathbb{Q}_p$ son complété. L'application v_p s'étend également à $\mathbb{Q}_p$; on note

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$$

Cadre

On considère l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie par $n = p^{v_p(n)}m$; elle s'étend de manière naturelle à $\mathbb{Q}$ (avec la convention $v_p(0) := +\infty$). L'application $|\cdot|_p : \mathbb{Q} \to \mathbb{Q}_+$ définie par $|r|_p := p^{-v_p(r)}$ définit une métrique sur $\mathbb{Q}$; on note $\mathbb{Q}_p$ son complété. L'application v_p s'étend également à $\mathbb{Q}_p$; on note

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$$

L'anneau $\mathbb{Z}_p$ est principal : ses idéaux sont les $\langle p^n \rangle$ pour $n \geq 0$. De plus, l'idéal $p\mathbb{Z}_p$ est un idéal maximal de $\mathbb{Z}_p$; le corps résiduel vérifie

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$$

Produit amalgamé

Soient H, H', K trois groupes et soient $\phi : K \to H$, $\phi' : K \to H'$ deux morphismes.

Produit amalgamé

Soient H, H', K trois groupes et soient $\phi : K \to H$, $\phi' : K \to H'$ deux morphismes.

Théorème

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

- on a $h \circ \phi = h' \circ \phi'$;

Produit amalgamé

Soient H, H', K trois groupes et soient $\phi : K \to H$, $\phi' : K \to H'$ deux morphismes.

Théorème

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 $\widetilde{h'} = f \circ h'$.

Produit amalgamé

Soient H, H', K trois groupes et soient $\phi : K \to H$, $\phi' : K \to H'$ deux morphismes.

Théorème

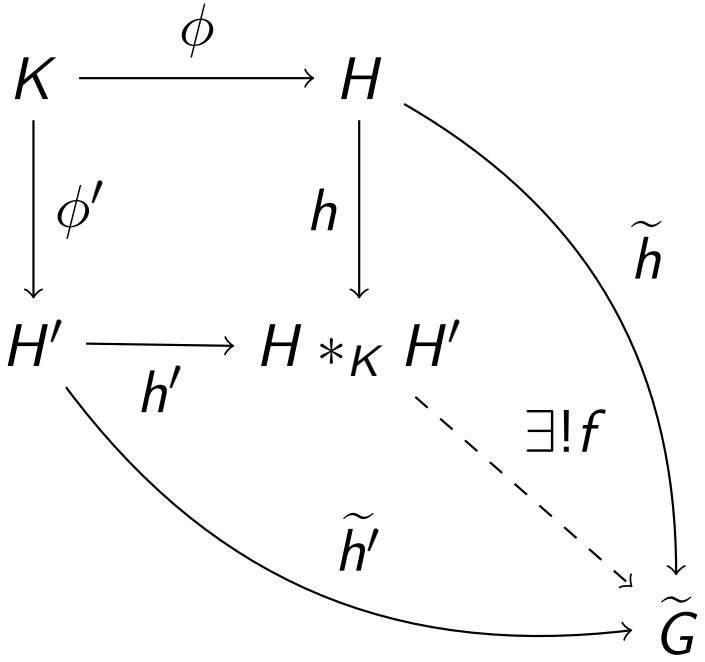
Il existe un unique groupe G et des uniques morphismes $h : H \to G$, $h' : H' \to G$ tels que :

- 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 $\widetilde{h'} = f \circ h'$.

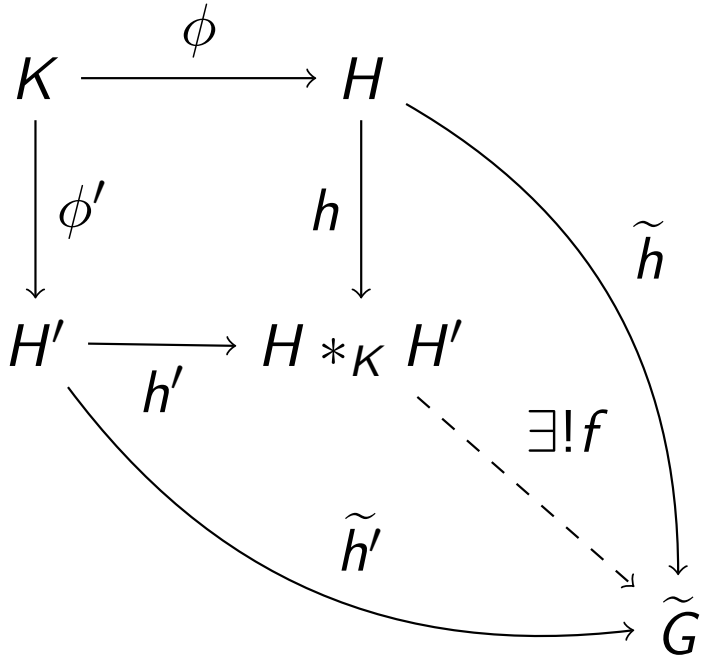
Définition (Produit amalgamé)

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

Produit amalgamé



Produit amalgamé



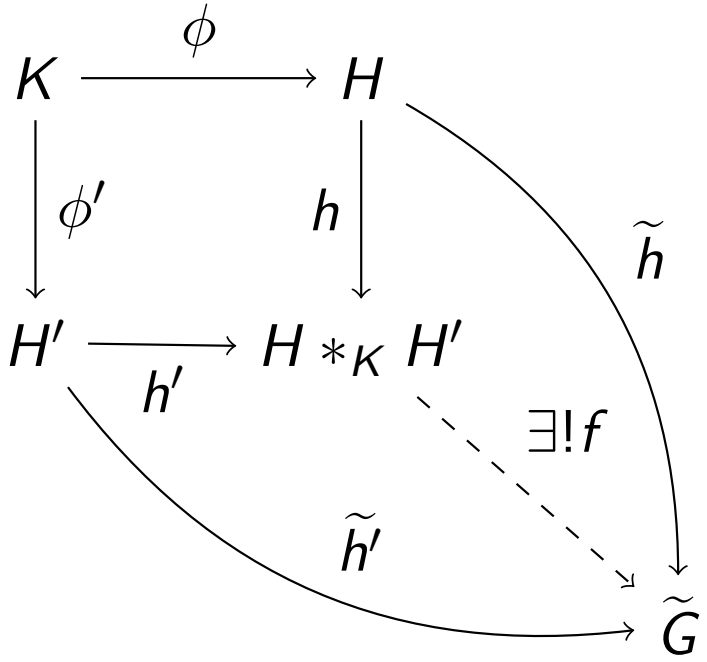
Démonstration du théorème

Le groupe suivant convient :

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

avec $h, h' = \mathrm{id}$

Produit amalgamé



Démonstration du théorème

Le groupe suivant convient :

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

avec $h, h' = \mathrm{id}$; la PU garantit l'unicité.

Le théorème

Théorème (Ihara)

On a l'isomorphisme suivant :

$$\mathrm{SL}_2(\mathbb{Q}_p) \simeq \mathrm{SL}_2(\mathbb{Z}_p) \underset{\Gamma}{*} \mathrm{SL}_2(\mathbb{Z}_p)$$

Le théorème

Théorème (Ihara)

On a l'isomorphisme suivant :

$$\mathrm{SL}_2(\mathbb{Q}_p) \simeq \mathrm{SL}_2(\mathbb{Z}_p) \underset{\Gamma}{*} \mathrm{SL}_2(\mathbb{Z}_p)$$

où $\Gamma := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p) : c \in \langle p \rangle\}$

Le théorème

Théorème (Ihara)

On a l'isomorphisme suivant :

$$\mathrm{SL}_2(\mathbb{Q}_p) \simeq \mathrm{SL}_2(\mathbb{Z}_p) \underset{\Gamma}{*} \mathrm{SL}_2(\mathbb{Z}_p)$$

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

$$\Gamma \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{\phi}{\longmapsto} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$$

$$\Gamma \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{\phi'}{\longmapsto} \begin{pmatrix} a & pb \\ p^{-1}c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$$

Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension 2.

Réseaux

Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension 2.

Définition (Réseau)

Un *réseau* de V est un sous-$\mathbb{Z}_p$-module L de V de type fini qui engendre V en tant que $\mathbb{Q}_p$-espace vectoriel.

Réseaux

Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension 2.

Définition (Réseau)

Un *réseau* de V est un sous-$\mathbb{Z}_p$-module L de V de type fini qui engendre V en tant que $\mathbb{Q}_p$-espace vectoriel.

Proposition

Tout réseau de V est un $\mathbb{Z}_p$-module libre de rang 2.

Réseaux

Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension 2.

Définition (Réseau)

Un *réseau* de V est un sous-$\mathbb{Z}_p$-module L de V de type fini qui engendre V en tant que $\mathbb{Q}_p$-espace vectoriel.

Proposition

Tout réseau de V est un $\mathbb{Z}_p$-module libre de rang 2.

Le groupe $\mathbb{Q}_p^*$ agit par multiplication à gauche sur l'ensemble des réseaux de V et l'on définit l'ensemble des orbites :

$$X := \{\text{réseaux de V}\}/\mathbb{Q}_p^*$$

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Démonstration

- Soit $L'' \in \Lambda'$ et soit (e_1, e_2) une $\mathbb{Z}_p$-base de L''. Il existe $a \in \mathbb{Z}_p \setminus \{0\}$ tel que $ae_i \in L$

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Démonstration

- Soit $L'' \in \Lambda'$ et soit (e_1, e_2) une $\mathbb{Z}_p$-base de L''. Il existe $a \in \mathbb{Z}_p \setminus \{0\}$ tel que $ae_i \in L$: avec $L' := aL'' \in \Lambda'$ on a bien $L' \subseteq L$.

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Démonstration

- Soit $L'' \in \Lambda'$ et soit (e_1, e_2) une $\mathbb{Z}_p$-base de L''. Il existe $a \in \mathbb{Z}_p \setminus \{0\}$ tel que $ae_i \in L$: avec $L' := aL'' \in \Lambda'$ on a bien $L' \subseteq L$.
- Si $L' \subseteq L$, par le théorème de la base adaptée il existe (e_1, e_2) tels que $L = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ et $L' = \mathbb{Z}_p p^{n_1} e_1 \oplus \mathbb{Z}_p p^{n_2} e_2$ avec $n_i \geq 0$

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Démonstration

- Soit $L'' \in \Lambda'$ et soit (e_1, e_2) une $\mathbb{Z}_p$-base de L''. Il existe $a \in \mathbb{Z}_p \setminus \{0\}$ tel que $ae_i \in L$: avec $L' := aL'' \in \Lambda'$ on a bien $L' \subseteq L$.
- Si $L' \subseteq L$, par le théorème de la base adaptée il existe (e_1, e_2) tels que $L = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ et $L' = \mathbb{Z}_p p^{n_1} e_1 \oplus \mathbb{Z}_p p^{n_2} e_2$ avec $n_i \geq 0$, en particulier $L/L' \simeq \mathbb{Z}_p/p^{n_1}\mathbb{Z}_p \oplus \mathbb{Z}_p/p^{n_2}\mathbb{Z}_p$

Lemme

Soient $\Lambda, \Lambda' \in X$ et soit $L \in \Lambda$. Il existe $L' \in \Lambda'$ tel que :

- $L' \subseteq L$;
- L/L' est monogène.

Démonstration

- Soit $L'' \in \Lambda'$ et soit (e_1, e_2) une $\mathbb{Z}_p$-base de L''. Il existe $a \in \mathbb{Z}_p \setminus \{0\}$ tel que $ae_i \in L$: avec $L' := aL'' \in \Lambda'$ on a bien $L' \subseteq L$.
- Si $L' \subseteq L$, par le théorème de la base adaptée il existe (e_1, e_2) tels que $L = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ et $L' = \mathbb{Z}_p p^{n_1} e_1 \oplus \mathbb{Z}_p p^{n_2} e_2$ avec $n_i \geq 0$, en particulier $L/L' \simeq \mathbb{Z}_p/p^{n_1}\mathbb{Z}_p \oplus \mathbb{Z}_p/p^{n_2}\mathbb{Z}_p$; le réseau $p^{-\min(n_i)} L'$ convient.

Distance entre deux réseaux

Proposition / Définition

L'entier n vérifiant $L/L' \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$ ne dépend que de Λ et Λ' ; on le note $d(\Lambda, \Lambda')$.

Distance entre deux réseaux

Proposition / Définition

L'entier n vérifiant $L/L' \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$ ne dépend que de Λ et Λ' ; on le note $d(\Lambda, \Lambda')$.

Remarque

En particulier :

- $d(\Lambda, \Lambda') = 0 \iff \Lambda = \Lambda'$;

Distance entre deux réseaux

Proposition / Définition

L'entier n vérifiant $L/L' \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$ ne dépend que de Λ et Λ' ; on le note $d(\Lambda, \Lambda')$.

Remarque

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 $L/L' \simeq \mathbb{F}_p$ $(\simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/p\mathbb{Z}_p)$.

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Théorème

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).

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Théorème

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).

Reste donc à :

- montrer que cet amalgame est le même que le $\mathrm{SL}_2(\mathbb{Z}_p) *_\Gamma \mathrm{SL}_2(\mathbb{Z}_p)$ précédent

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Théorème

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).

Reste donc à :

- montrer que cet amalgame est le même que le $\mathrm{SL}_2(\mathbb{Z}_p) *_\Gamma \mathrm{SL}_2(\mathbb{Z}_p)$ précédent
- démontrer ce théorème

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Théorème

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).

Reste donc à :

- montrer que cet amalgame est le même que le $\mathrm{SL}_2(\mathbb{Z}_p) *_\Gamma \mathrm{SL}_2(\mathbb{Z}_p)$ précédent (pas trop dur) ;
- démontrer ce théorème

Un autre théorème

Notons $G := \mathrm{SL}(V)$; le groupe G agit sur l'ensemble X des classes de réseaux.

Théorème

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).

Reste donc à :

- montrer que cet amalgame est le même que le $\mathrm{SL}_2(\mathbb{Z}_p) *_\Gamma \mathrm{SL}_2(\mathbb{Z}_p)$ précédent (pas trop dur) ;
- démontrer ce théorème (plus dur).

Stabilisateur G_Λ

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_\mathcal{B}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Démonstration

L'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(\mathbb{Q}_p)$ est un isomorphisme sur son image, il reste donc à montrer que c'est $\mathrm{SL}_2(\mathbb{Z}_p)$:

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_\mathcal{B}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Démonstration

L'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(\mathbb{Q}_p)$ est un isomorphisme sur son image, il reste donc à montrer que c'est $\mathrm{SL}_2(\mathbb{Z}_p)$:

- si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \mathrm{mat}_\mathcal{B}(s)$ alors $se_1 = ae_1 + ce_2 \in L$

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_\mathcal{B}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Démonstration

L'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(\mathbb{Q}_p)$ est un isomorphisme sur son image, il reste donc à montrer que c'est $\mathrm{SL}_2(\mathbb{Z}_p)$:

- si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \mathrm{mat}_\mathcal{B}(s)$ alors $se_1 = ae_1 + ce_2 \in L$ donc $a, c \in \mathbb{Z}_p$ et ainsi $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p)$;

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_\mathcal{B}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Démonstration

L'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(\mathbb{Q}_p)$ est un isomorphisme sur son image, il reste donc à montrer que c'est $\mathrm{SL}_2(\mathbb{Z}_p)$:

- si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \mathrm{mat}_\mathcal{B}(s)$ alors $se_1 = ae_1 + ce_2 \in L$ donc $a, c \in \mathbb{Z}_p$ et ainsi $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p)$;
- si $\mathrm{mat}_\mathcal{B}(s) \in \mathrm{SL}_2(\mathbb{Z}_p)$ alors on a $sL \subseteq L$

Stabilisateur G_Λ

Lemme

Pour $L \in \Lambda \in X$ on a $G_L = G_\Lambda$.

Remarque

Cela ne serait plus nécessairement vrai avec $G = \mathrm{GL}(V)$.

Lemme

Si $L \in \Lambda \in X$ et si $\mathcal{B}$ est une $\mathbb{Z}_p$-base de L alors $G_L \xrightarrow[\mathrm{mat}_\mathcal{B}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Démonstration

L'application $\mathrm{mat}_\mathcal{B} : G_L \to \mathrm{SL}_2(\mathbb{Q}_p)$ est un isomorphisme sur son image, il reste donc à montrer que c'est $\mathrm{SL}_2(\mathbb{Z}_p)$:

- si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \mathrm{mat}_\mathcal{B}(s)$ alors $se_1 = ae_1 + ce_2 \in L$ donc $a, c \in \mathbb{Z}_p$ et ainsi $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p)$;
- si $\mathrm{mat}_\mathcal{B}(s) \in \mathrm{SL}_2(\mathbb{Z}_p)$ alors on a $sL \subseteq L$ et $s^{-1}L \subseteq L$ d'où $s \in G_L$.

Stabilisateur $G_{\Lambda'}$

Soient $\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = L \in \Lambda \in X$, $\mathcal{B} := (e_1, e_2)$; on vient de voir que $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$.

Stabilisateur $G_{\Lambda'}$

Soient $\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = L \in \Lambda \in X$, $\mathcal{B} := (e_1, e_2)$; on vient de voir que $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$. Soit $L' := \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$: on a $L/L' \simeq 0 \oplus \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ donc $d(\Lambda, \Lambda') = 1$.

Stabilisateur $G_{\Lambda'}$

Soient $\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = L \in \Lambda \in X$, $\mathcal{B} := (e_1, e_2)$; on vient de voir que $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$. Soit $L' := \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$: on a $L/L' \simeq 0 \oplus \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ donc $d(\Lambda, \Lambda') = 1$.

Lemme

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 :

$$s \in G_{L'} \text{ ssi } \begin{cases} a, d \in \mathbb{Z}_p \\ c \in \mathbb{Z}_p p \\ b \in \mathbb{Z}_p p^{-1} \end{cases}$$

Stabilisateur $G_{\Lambda'}$

Soient $\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = L \in \Lambda \in X$, $\mathcal{B} := (e_1, e_2)$; on vient de voir que $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$. Soit $L' := \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$: on a $L/L' \simeq 0 \oplus \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ donc $d(\Lambda, \Lambda') = 1$.

Lemme

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 :

$$s \in G_{L'} \underline{\text{ssi}} \begin{cases} a, d \in \mathbb{Z}_p \\ c \in \mathbb{Z}_p p \\ b \in \mathbb{Z}_p p^{-1} \end{cases}$$

Démonstration

Supposons que $s \in G_{L'}$. Ainsi, $sL' = L'$ donc en particulier $s(pe_2) = bp \cdot e_1 + d \cdot pe_2 \in L' = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$

Stabilisateur $G_{\Lambda'}$

Soient $\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = L \in \Lambda \in X$, $\mathcal{B} := (e_1, e_2)$; on vient de voir que $G_L \xrightarrow[\mathrm{mat}_{\mathcal{B}}]{\sim} \mathrm{SL}_2(\mathbb{Z}_p)$. Soit $L' := \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$: on a $L/L' \simeq 0 \oplus \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ donc $d(\Lambda, \Lambda') = 1$.

Lemme

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 :

$$s \in G_{L'} \text{ ssi } \begin{cases} a, d \in \mathbb{Z}_p \\ c \in \mathbb{Z}_p p \\ b \in \mathbb{Z}_p p^{-1} \end{cases}$$

Démonstration

Supposons que $s \in G_{L'}$. Ainsi, $sL' = L'$ donc en particulier $s(pe_2) = bp \cdot e_1 + d \cdot pe_2 \in L' = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2$ donc $bp \in \mathbb{Z}_p$ et $d \in \mathbb{Z}_p$. De même on trouve $a \in \mathbb{Z}_p$ et $c \in \mathbb{Z}_p p$; on vérifie que ces conditions sont suffisantes.

Démonstration du théorème principal

Considérons maintenant l'isomorphisme suivant :

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

(remarquons que f dans les matrices à coefficients dans $\mathbb{Z}_p$ par le lemme précédent).

Démonstration du théorème principal

Considérons maintenant l'isomorphisme suivant :

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

(remarquons que f dans les matrices à coefficients dans $\mathbb{Z}_p$ par le lemme précédent). Par le théorème on a $G \simeq G_L *_{G_L \cap G_{L'}} G_{L'}$ donc, avec $\Gamma := \mathrm{mat}_{\mathcal{B}}(G_L \cap G_{L'})$:

Démonstration du théorème principal

Considérons maintenant l'isomorphisme suivant :

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

(remarquons que f dans les matrices à coefficients dans $\mathbb{Z}_p$ par le lemme précédent). Par le théorème on a $G \simeq G_L *_{G_L \cap G_{L'}} G_{L'}$ donc, avec $\Gamma := \mathrm{mat}_{\mathcal{B}}(G_L \cap G_{L'})$:

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

au moyen de l'inclusion et de $f|_\Gamma$.

Démonstration du théorème principal

Considérons maintenant l'isomorphisme suivant :

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

(remarquons que f dans les matrices à coefficients dans $\mathbb{Z}_p$ par le lemme précédent). Par le théorème on a $G \simeq G_L *_{G_L \cap G_{L'}} G_{L'}$ donc, avec $\Gamma := \mathrm{mat}_{\mathcal{B}}(G_L \cap G_{L'})$:

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

au moyen de l'inclusion et de $f|_\Gamma$. Reste à s'apercevoir que $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p)$ est dans Γ ssi $c \in \mathbb{Z}_p p$.

Graphe

Définition (Graphe)

Un *graphe* Γ est la donnée d'un ensemble de sommet S, d'un ensemble d'arêtes A

Graphe

Définition (Graphe)

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

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

Définition (Graphe)

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

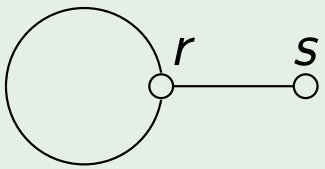
$$\left|\begin{array}{ccc} A & \to & S \times S \\ a & \mapsto & (o(a), t(a)) \end{array}\right. \quad \text{et} \quad \left|\begin{array}{ccc} A & \to & A \\ a & \mapsto & \bar{a} \end{array}\right.$$

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

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

Exemple

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 $\forall (u, v, \epsilon) \in A$:

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

Action d'un groupe sur un graphe

Définition (Opération d'un groupe sur un graphe)

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

Action d'un groupe sur un graphe

Définition (Opération d'un groupe sur un graphe)

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.* $\forall g \in G, \forall a \in A$,

- $g \cdot o(a) = o(g \cdot a)$ et $g \cdot t(a) = t(g \cdot a)$;
- $\overline{g \cdot a} = g\bar{a}$.

Action d'un groupe sur un graphe

Définition (Opération d'un groupe sur un graphe)

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.* $\forall g \in G, \forall a \in A$,

- $g \cdot o(a) = o(g \cdot a)$ et $g \cdot t(a) = t(g \cdot a)$;
- $\overline{g \cdot a} = g\bar{a}$.

On dit que l'action est *sans inversion* si de plus $\forall g \in G, \forall a \in A$, $ga \neq \bar{a}$.

Action d'un groupe sur un graphe

Définition (Opération d'un groupe sur un graphe)

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.* $\forall g \in G, \forall a \in A$,

- $g \cdot o(a) = o(g \cdot a)$ et $g \cdot t(a) = t(g \cdot a)$;
- $\overline{g \cdot a} = g\bar{a}$.

On dit que l'action est *sans inversion* si de plus $\forall g \in G, \forall a \in A$, $ga \neq \bar{a}$.

Théorème

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

Morphisme de graphes et domaine fondamental

Définition (Morphisme de graphes)

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 graphe* de Γ vers $\widehat{\Gamma}$ si $\forall a \in A$:

Morphisme de graphes et domaine fondamental

Définition (Morphisme de graphes)

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 graphe* de Γ vers $\widehat{\Gamma}$ si $\forall a \in A$:

- $\hat{o}(\alpha(a)) = \sigma(o(a))$ et $\hat{t}(\alpha(a)) = \sigma(t(a))$;
- $\widehat{\alpha(a)} = \alpha(\bar{a})$.

Morphisme de graphes et domaine fondamental

Définition (Morphisme de graphes)

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 graphe* de Γ vers $\widehat{\Gamma}$ si $\forall a \in A$:

- $\hat{o}(\alpha(a)) = \sigma(o(a))$ et $\hat{t}(\alpha(a)) = \sigma(t(a))$;
- $\widehat{\alpha(a)} = \alpha(\bar{a})$.

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

Morphisme de graphes et domaine fondamental

Définition (Morphisme de graphes)

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 graphe* de Γ vers $\widehat{\Gamma}$ si $\forall a \in A$:

- $\hat{o}(\alpha(a)) = \sigma(o(a))$ et $\hat{t}(\alpha(a)) = \sigma(t(a))$;
- $\widehat{\alpha(a)} = \alpha(\bar{a})$.

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

Définition (Domaine fondamental)

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.

Arbre

Définition (Chemin)

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 $\forall i \in [\![1, n-1]\!], t(a_i) = o(a_{i+1})$.
- Si $(a_1, \ldots, a_n)$ est un chemin, on dit que (a_i, a_{i+1}) est un *aller-retour* si $a_{i+1} = \bar{a}_i$.

Définition (Chemin)

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 $\forall i \in [\![1, n-1]\!], t(a_i) = o(a_{i+1})$.
- Si $(a_1, \ldots, a_n)$ est un chemin, on dit que (a_i, a_{i+1}) est un *aller-retour* si $a_{i+1} = \bar{a}_i$.

Définition (Circuit)

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.

Arbre

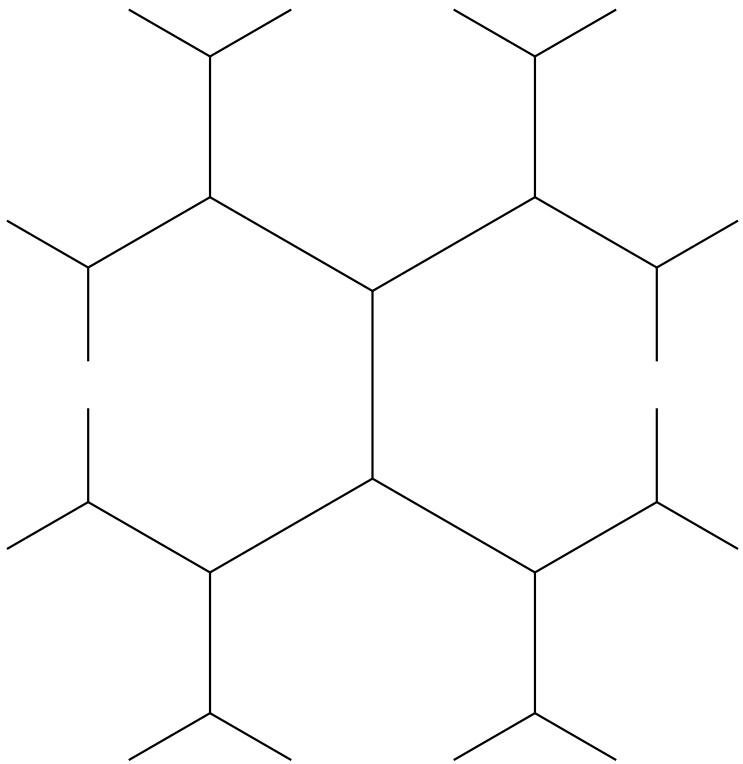
Définition (Arbre)

On dit qu'un graphe non vide est un *arbre* s'il est connexe et sans circuit.

Arbre

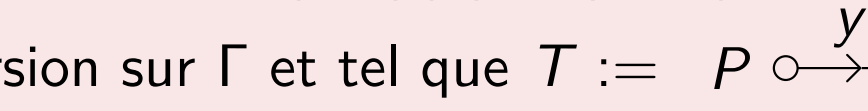
Définition (Arbre)

On dit qu'un graphe non vide est un *arbre* s'il est connexe et sans circuit.



Le théorème clé

Théorème clé

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 $T :=$  soit un domaine fondamental pour cette action.

Le théorème clé

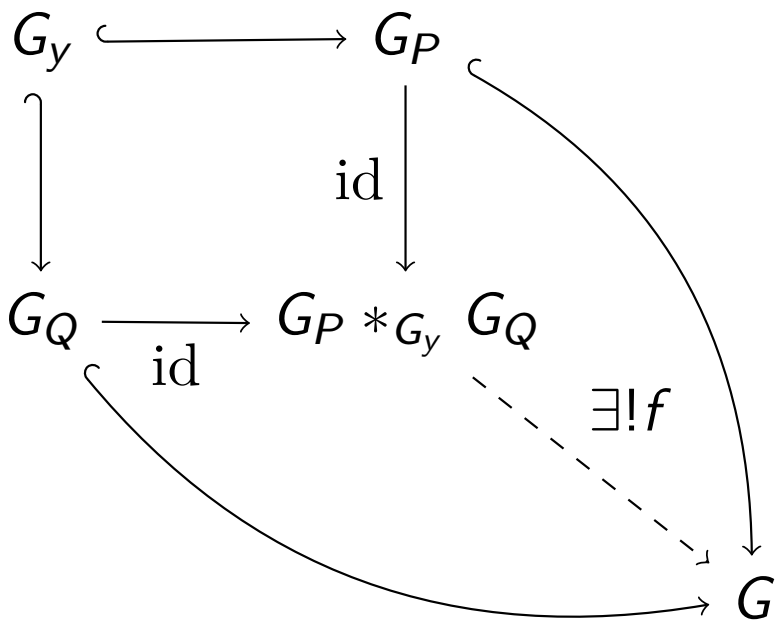
Théorème clé

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 $T := \quad P \overset{y}{\circ\!\!\longrightarrow\!\!\circ} Q$ 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.

Le théorème clé

Théorème clé

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.



Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.

Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).

Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).
- Si (Λ, Λ') est une arête alors $T := \Lambda \circ\!\!\longrightarrow\!\!\circ\, \Lambda'$ est un domaine fondamental de Γ pour l'action de G (i.e. l'application canonique $T \to \Gamma/G$ est un isomorphisme)

Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).
- Si (Λ, Λ') est une arête alors $T := \Lambda \circ\!\!-\!\!\!\rightarrow\!\!-\!\circ \Lambda'$ est un domaine fondamental de Γ pour l'action de G (i.e. l'application canonique $T \to \Gamma/G$ est un isomorphisme) : cela résulte en particulier du fait que les sommets adjacents à Λ sont exactement les droites de $L/pL \simeq \mathbb{F}_p \oplus \mathbb{F}_p$

Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).
- Si (Λ, Λ') est une arête alors $T := \Lambda \circ\!\!-\!\!\!\rightarrow\!\!-\!\circ \Lambda'$ est un domaine fondamental de Γ pour l'action de G (i.e. l'application canonique $T \to \Gamma/G$ est un isomorphisme) : cela résulte en particulier du fait que les sommets adjacents à Λ sont exactement les droites de $L/pL \simeq \mathbb{F}_p \oplus \mathbb{F}_p$; on conclut car $G_L \simeq \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ est surjective et que l'action $\mathrm{SL}_2(\mathbb{F}_p) \curvearrowright \mathbb{P}^1(\mathbb{F}_p)$ est transitive.

Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).
- Si (Λ, Λ') est une arête alors $T := \Lambda \circ\!\!-\!\!\!\rightarrow\!\!-\!\circ \Lambda'$ est un domaine fondamental de Γ pour l'action de G (i.e. l'application canonique $T \to \Gamma/G$ est un isomorphisme) : cela résulte en particulier du fait que les sommets adjacents à Λ sont exactement les droites de $L/pL \simeq \mathbb{F}_p \oplus \mathbb{F}_p$; on conclut car $G_L \simeq \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ est surjective et que l'action $\mathrm{SL}_2(\mathbb{F}_p) \curvearrowright \mathbb{P}^1(\mathbb{F}_p)$ est transitive.
- X est un arbre

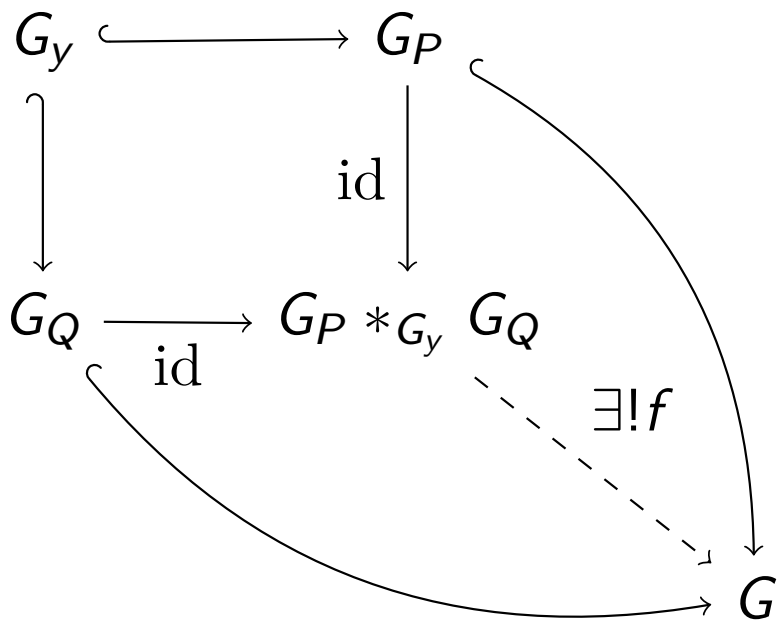
Vérification des hypothèses

- X est un graphe, les arêtes étant les (Λ, Λ') avec $d(\Lambda, \Lambda') = 1$.
- L'action de $\mathrm{SL}_2(\mathbb{Q}_p)$ sur le graphe X est sans inversion (ce serait faux avec $\mathrm{GL}_2(\mathbb{Q}_p)$).
- Si (Λ, Λ') est une arête alors $T := \Lambda \circ\!\!-\!\!\circ \Lambda'$ est un domaine fondamental de Γ pour l'action de G (i.e. l'application canonique $T \to \Gamma/G$ est un isomorphisme) : cela résulte en particulier du fait que les sommets adjacents à Λ sont exactement les droites de $L/pL \simeq \mathbb{F}_p \oplus \mathbb{F}_p$; on conclut car $G_L \simeq \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ est surjective et que l'action $\mathrm{SL}_2(\mathbb{F}_p) \curvearrowright \mathbb{P}^1(\mathbb{F}_p)$ est transitive.
- X est un arbre, la connexité résultant du fait que l'on peut trouver une chaine $(L_0, \ldots, L_n)$ de sous-$\mathbb{Z}_p$-modules entre xL' et L (où $L/xL' \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$) qui vérifient $L_i/L_{i-1} \simeq \mathbb{F}_p$.

Rappel de l'énoncé du théorème

Théorème clé

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.



Si Γ est connexe...

Si Γ est connexe...

Lemme

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

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).
- $G'T \cap (G \setminus G')T = \emptyset$.

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).
- $G'T \cap (G \setminus G')T = \emptyset$. Soit R un sommet de $G'T \cap (G \setminus G')T$: 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 Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).
- $G'T \cap (G \setminus G')T = \emptyset$. Soit R un sommet de $G'T \cap (G \setminus G')T$: 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 $s \in G_P \subseteq G'$ impossible.

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).
- $G'T \cap (G \setminus G')T = \emptyset$. Soit R un sommet de $G'T \cap (G \setminus G')T$: 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 $s \in G_P \subseteq G'$ impossible.
  - Si $R = s'P = sQ$ on obtient un élément de G qui envoie P sur Q : c'est absurde car $T = [P \circ\!\!-\!\!-\!\!\circ Q]$ est un domaine fondamental.

Si Γ est connexe...

Lemme

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

Supposons Γ connexe et définissons $G' := \langle G_P \cup G_Q \rangle \subseteq G$.

- $G'T \cup (G \setminus G')T = \Gamma$ car T est un domaine fondamental (*i.e.* $T \xrightarrow{\sim} \Gamma/G$).
- $G'T \cap (G \setminus G')T = \emptyset$. Soit R un sommet de $G'T \cap (G \setminus G')T$: 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 $s \in G_P \subseteq G'$ impossible.
  - Si $R = s'P = sQ$ on obtient un élément de G qui envoie P sur Q : c'est absurde car $T = [P \circ\!\!-\!\!-\!\!\circ Q]$ est un domaine fondamental.

Le graphe Γ étant connexe et ayant $G'T \neq \emptyset$ on en déduit que $G \setminus G' = \emptyset$, d'où $G = G'$.

Si Γ est sans circuit. . .

Si Γ est sans circuit...

Lemme

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

Si Γ est sans circuit...

Lemme

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

On va en fait montrer que la contraposée : supposons que $G_P *_{G_y} G_Q \to G$ ne soit pas injectif et montrons que Γ possède un circuit.

Si Γ est sans circuit...

Lemme

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

On va en fait montrer que la contraposée : supposons que $G_P *_{G_y} G_Q \to G$ ne soit pas injectif et montrons que Γ possède un circuit. Par un lemme sur les mots d'un produit amalgamé, l'hypothèse implique qu'il existe $n \geq 2$ et des $g_i \in G_P \amalg G_Q$ qui vérifient :

- si $g_i \in G_P$ (resp. $g_i \in G_Q$) alors $g_{i+1} \in G_Q$ (resp. $g_{i+1} \in G_P$) ;

Si Γ est sans circuit...

Lemme

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

On va en fait montrer que la contraposée : supposons que $G_P *_{G_y} G_Q \to G$ ne soit pas injectif et montrons que Γ possède un circuit. Par un lemme sur les mots d'un produit amalgamé, l'hypothèse implique qu'il existe $n \geq 2$ et des $g_i \in G_P \amalg G_Q$ qui vérifient :

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

Si Γ est sans circuit...

Lemme

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

On va en fait montrer que la contraposée : supposons que $G_P *_{G_y} G_Q \to G$ ne soit pas injectif et montrons que Γ possède un circuit. Par un lemme sur les mots d'un produit amalgamé, l'hypothèse implique qu'il existe $n \geq 2$ et des $g_i \in G_P \amalg G_Q$ qui vérifient :

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

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

Si Γ est sans circuit...

Lemme

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

On va en fait montrer que la contraposée : supposons que $G_P *_{G_y} G_Q \to G$ ne soit pas injectif et montrons que Γ possède un circuit. Par un lemme sur les mots d'un produit amalgamé, l'hypothèse implique qu'il existe $n \geq 2$ et des $g_i \in G_P \amalg G_Q$ qui vérifient :

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

Notons $R_i \in \{P, Q\}$ les points qui vérifient $g_i \in G_{R_i}$ et $z_i \in \{y, \bar{y}\}$ 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 :

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

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- C'est bien un chemin car
  $t(g_1 \cdots g_i z_i) =$
  $= o(g_1 \cdots g_{i+1} z_{i+1})$.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- C'est bien un chemin car
  $t(g_1 \cdots g_i z_i) = g_1 \cdots g_i t(z_i) =$
  $= o(g_1 \cdots g_{i+1} z_{i+1})$.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- C'est bien un chemin car
$$t(g_1 \cdots g_i z_i) = g_1 \cdots g_i t(z_i) = g_1 \cdots g_i o(z_{i+1}) = \\ = o(g_1 \cdots g_{i+1} z_{i+1}).$$

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- C'est bien un chemin car
  $t(g_1 \cdots g_i z_i) = g_1 \cdots g_i t(z_i) = g_1 \cdots g_i o(z_{i+1}) =$
  $g_1 \cdots g_i R_{i+1} = \qquad\qquad = o(g_1 \cdots g_{i+1} z_{i+1})$.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- C'est bien un chemin car
  $t(g_1 \cdots g_i z_i) = g_1 \cdots g_i t(z_i) = g_1 \cdots g_i o(z_{i+1}) =$
  $g_1 \cdots g_i R_{i+1} = g_1 \cdots g_i g_{i+1} R_{i+1} = o(g_1 \cdots g_{i+1} z_{i+1})$.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- 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 $z_{i-1} = g_i \overline{z_i}$

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- 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.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- 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.

On peut maintenant montrer que Γ possède un circuit.

- 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 Γ possède un circuit.

Si Γ est sans circuit alors $G_P *_{G_y} G_Q \hookrightarrow G$

On a $\gamma = (g_1 z_1, \ldots, g_1 \cdots g_n z_n)$.

- 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.

On peut maintenant montrer que Γ possède un circuit.

- 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 Γ possède un circuit.
- Supposons au contraire $z_{n-1} \neq z_1$; considérons le chemin sans aller-retour suivant :

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

et on vérifie qu'il contient un circuit de Γ.

Si Γ est un arbre...

Si Γ est un arbre...

On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$.

Si Γ est un arbre...

On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$.

- Comme Γ est sans circuit le morphisme f est injectif (lemme précédent).

Si Γ est un arbre...

On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$.

- Comme Γ est sans circuit le morphisme f est injectif (lemme précédent).
- Par définition de f on a $\forall g \in G_P \amalg G_Q, f(h_*(g)) = g$ (où $h_* : G_* \to G_P *_{G_y} G_Q$)

Si Γ est un arbre...

On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$.

- Comme Γ est sans circuit le morphisme f est injectif (lemme précédent).
- Par définition de f on a $\forall g \in G_P \amalg G_Q, f(h_*(g)) = g$ (où $h_* : G_* \to G_P *_{G_y} G_Q$) donc l'image de f contient $G_P \cup G_Q$, donc comme Γ est connexe, par le lemme précédent on en déduit que f est surjective.

Si Γ est un arbre...

On suppose que Γ est un arbre ; soit $f : G_P *_{G_y} G_Q \to G$ le morphisme induit par les deux inclusions $G_P, G_Q \hookrightarrow G$.

- Comme Γ est sans circuit le morphisme f est injectif (lemme précédent).
- Par définition de f on a $\forall g \in G_P \amalg G_Q, f(h_*(g)) = g$ (où $h_* : G_* \to G_P *_{G_y} G_Q$) donc l'image de f contient $G_P \cup G_Q$, donc comme Γ est connexe, par le lemme précédent on en déduit que f est surjective.

Finalement, f et un isomorphisme.

Référence

Jean-Pierre Serre, *Arbres, amalgames*, SL_2 (3e édition). Astérisque N° 46, 1983.