Sous-groupes normaux des groupes de matrices

Pierre-Alain JACQMIN

Promoteur : Pierre-Emmanuel CAPRACE

Université catholique de Louvain
Faculté des Sciences
École de Mathématique

2010–2011

Remerciements

Avant de débuter ce travail, je tiens à remercier tous ceux qui m'ont permis de mener à bien ce projet. En particulier, mon promoteur, Monsieur Pierre-Emmanuel CAPRACE, professeur de mathématiques à l'Université Catholique de Louvain, pour la pertinence du sujet proposé, l'intérêt porté à mon travail, ses explications précises et ses divers conseils.

Table des matières

1 Introduction et rappels

1.1 Introduction

Le but de ce travail est d'étudier les groupes de matrices sur un corps et sur un anneau. Nous nous intéresserons en particulier à l'existence de quotients non-triviaux.

Il est bien connu qu'un nombre premier est un naturel qui ne possède que deux diviseurs. Par ailleurs, en théorie des groupes, nous avons également une relation de divisibilité. En effet, si $H \leq G$, le quotient G/H définit un groupe si et seulement si H est un sous-groupe normal de G. Nous pouvons dès lors définir le correspondant des nombres premiers en théorie des groupes. Nous dirons donc qu'un groupe est simple, s'il n'est divisible que par $\{1\}$ et par lui-même, c'est-à-dire qu'il ne possède aucun sous-groupe normal non trivial. Nous sommes alors amenés à nous poser une question légitime : connaissons-nous des exemples de groupes simples ? Évidemment, grâce au théorème de Lagrange, il est trivial de citer $\{1\}$ et tous les groupes d'ordre premier. Mais y en a-t-il d'autres ? Et comment vérifier qu'un groupe est simple ? Cette dernière question n'est en général pas évidente.

Iwasawa, mathématicien japonais du XX^{e} siècle, a trouvé une famille d'exemples de groupes simples en travaillant sur le groupe des matrices de déterminant 1. Nous désignerons par $SL_n(\mathbb{R})$ et $SL_n(\mathbb{Z})$ les groupes des matrices $n \times n$ de déterminant 1 sur $\mathbb{R}$ et $\mathbb{Z}$ respectivement. Puisque le centre de ces groupes n'est pas réduit à l'identité si n est pair, nous ne pouvons pas dire qu'ils sont simples. C'est pourquoi, nous nous intéresserons aux quotients de ces groupes par leur centre que nous noterons $PSL_n(\mathbb{R})$ et $PSL_n(\mathbb{Z})$ respectivement. Grâce à l'inversibilité de tous les éléments non nuls de $\mathbb{R}$, Iwasawa prouva, pour $n \geq 2$, que $PSL_n(\mathbb{R})$ est simple. Il généralisa même ce résultat aux corps $\mathbb{K}$ quelconques, sous la condition $n > 2$ ou $|\mathbb{K}| > 3$. Dans la première partie de ce travail, nous présenterons une démonstration complète de ce théorème, en établissant au préalable une proposition assurant, sous quelques hypothèses, la simplicité d'un groupe quelconque. Nous vérifierons donc ensuite ces hypothèses dans le cas du groupe $PSL_n(\mathbb{K})$.

Malheureusement, $\mathbb{Z}$ n'étant pas un corps, nous ne pouvons pas conclure que $PSL_n(\mathbb{Z})$ est également simple. De plus, pour chaque $m \in \mathbb{N}_0$, l'ensemble $N_{n,m}$ des matrices de $SL_n(\mathbb{Z})$ qui sont congrues à l'identité modulo m, forme un sous-groupe normal non trivial de $SL_n(\mathbb{Z})$. En passant au quotient, nous venons donc de trouver une infinité de sous-groupes normaux non triviaux de $PSL_n(\mathbb{Z})$. Cependant, le mathématicien allemand Mennicke, prouva, en 1960, que tout sous-groupe non trivial de $SL_n(\mathbb{Z})$ contient un sous-groupe de la forme $N_{n,m}$. Ce théorème n'est valide que si $n > 2$. Nous montrerons en effet un contre-exemple pour le cas $n = 2$. Comme corollaire du théorème de Mennicke, nous pouvons dire que tout quotient non trivial de $SL_n(\mathbb{Z})$ est d'ordre fini. Dans la seconde partie du travail, nous présenterons une démonstration détaillée du théorème de Mennicke, en procédant par induction sur $n \geq 3$. La preuve sera basée sur un résultat de Brenner, qui assure que l'ensemble $N_{n,m}$ est le plus petit sous-groupe normal de $SL_n(\mathbb{Z})$ contenant la matrice $I + me_{21}$, où e_{21} est la matrice dont l'entrée $(2, 1)$ est 1, les autres étant nulles. Nous terminerons en montrant que l'hypothèse $n \geq 3$ est essentielle à la validité du théorème de Mennicke. En effet, nous verrons que ses conclusions ne sont pas satisfaites par le groupe $SL_2(\mathbb{Z})$.

On peut conclure que les groupes de matrices ont tendance à admettre peu de quotients non-triviaux. Dans le cas de coefficients dans un corps (d'ordre au moins 4), les groupes de matrices $PSL_n(\mathbb{K})$ sont même simples. En passant à des coefficients dans l'anneau des entiers, on a vu que les groupes $PSL_n(\mathbb{Z})$ cessent d'être simples : ils admettent des quotients de congruence. Toutefois, le théorème de Mennicke assure que ces quotients sont en fait essentiellement les seuls possibles pour les groupes de matrices $n \times n$ avec $n > 2$. La conclusion que les groupes de matrices sur les entiers ont "peu de quotients" s'impose donc à nouveau, à ceci près qu'il faut dans ce cas exclure le groupe des matrices 2×2 qui, sur les entiers, admet beaucoup plus de quotients. Insistons donc sur le fait, quelque peu surprenant, que la différence entre les comportements des matrices 2×2 et $n \times n$ avec $n > 2$ apparaît de façon cruciale sur les anneaux, alors qu'elle ne joue aucun rôle sur les corps d'ordre au moins 4.

1.2 Rappels

Dans cette section, nous rappellerons quelques résultats utilisés dans la suite. Commençons par de l'arithmétique :

Définition 1.1. *Soit $a \in \mathbb{R}$. La **partie entière** de a est notée $\lfloor a \rfloor$.*

Définition 1.2. *Soient $a, b \in \mathbb{Z}$. Si a divise b, nous écrirons $\mathbf{a} \mid \mathbf{b}$.*

Définition 1.3. *Soient $a, b, m \in \mathbb{Z}$ tels que $m \neq 0$. On dit que a est **congru à b modulo m** si et seulement si m divise $a - b$. On notera alors*

$$a \equiv b \ (mod\ m).$$

De même, si $n \in \mathbb{N}_0$, $A = (a_{ij}) \in \mathbb{Z}^{n \times n}$ et $B = (b_{ij}) \in \mathbb{Z}^{n \times n}$, alors $A \equiv B \ (mod\ m)$ si et seulement si pour tout $i, j \in \{1, \ldots, n\}$, $a_{ij} \equiv b_{ij} \ (mod\ m)$.

Définition 1.4. *Soit I un ensemble d'au moins deux éléments et des entiers $x_i \in \mathbb{Z}$, $i \in I$ non tous nuls. Alors*

$$(x_i, i \in I)$$

*désigne le **plus grand commun diviseur** (p.g.c.d.) des entiers x_i.*

Proposition 1.1 (Algorithme d'Euclide)**.** *Soit I un ensemble fini d'au moins deux éléments et des entiers $x_i \in \mathbb{Z}$, $i \in I$ non tous nuls. Notons $d = (x_i, i \in I)$. L'algorithme suivant permet de calculer d en un nombre fini d'opérations du type $x_i - x_j$ ou $x_i + x_j$, où $i, j \in I$:*

1. *Soit $j \in I$ tel que $x_j = min\{|x_i| \mid i \in I,\ x_i \neq 0\}$.*
2. *Si $|x_j| = d$, aller au point 4.*
3. *Pour tout $i \in I \setminus \{j\}$, remplacer x_i par $x_i - \left\lfloor \frac{x_i}{x_j} \right\rfloor x_j$. Aller au point 1.*
4. *Si $x_j = d$, nous avons fini. Si $x_j = -d$, en appliquant la même transformation qu'au point 3, nous obtenons un $i \in I \setminus \{j\}$ tel que $x_i = 0$. Il suffit alors de remplacer x_i par $x_i - x_j$.*

Lemme 1.2 (Bézout)**.** *Soit I un ensemble d'au moins deux éléments et des entiers $x_i \in \mathbb{Z}$, $i \in I$ non tous nuls. Alors, il existe $J \subset I$ fini et $k_j \in \mathbb{Z}$ pour tout $j \in J$ tels que*

$$\sum_{j \in J} k_j x_j = (x_i, i \in I).$$

Définition 1.5. *Soit $n \in \mathbb{N}_0$. Le cardinal de $\{k \in \mathbb{N} \mid 1 \leq k \leq n,\ (k,n) = 1\}$ est noté* $\boldsymbol{\varphi(n)}$.

Proposition 1.3. *Soit $n \in \mathbb{N}_0$ et soit $n = \prod_{i=1}^{t} p_i^{a_i}$ la factorisation première de n. Alors,*

$$\varphi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).$$

Définition 1.6. *Soient $a, n \in \mathbb{N}_0$ deux naturels premiers entre eux. L'* ***ordre*** *de a modulo n est le plus petit entier strictement positif m tel que $a^m \equiv 1 \ (mod\ n)$. Le fait que a soit premier avec n garantit l'existence de ce nombre.*

Proposition 1.4. *Soient $a, n \in \mathbb{N}_0$ deux naturels premiers entre eux. Notons m l'ordre de a modulo n. Alors $m \mid \varphi(n)$.*

Théorème 1.5 (Dirichlet)**.** *Soient $a, b \in \mathbb{N}_0$ deux naturels premiers entre eux. Alors il existe une infinité de nombres premiers p tels que $p \equiv a \ (mod\ b)$.*

Passons maintenant aux rappels sur la théorie des groupes. Nous ne mentionnons évidemment pas toute la théorie utilisée ici. Pour plus de détails, voir [2].

Définition 1.7. *Soit G un groupe. Le* ***sous-groupe dérivé*** *de G, noté $[G, G]$, est le plus petit sous-groupe de G contenant tous les éléments de la forme $aba^{-1}b^{-1}$ où $a, b \in G$.*

Théorème 1.6 (Lagrange)**.** *Soient G un groupe fini et H un sous-groupe de G. Alors*

$$|G : H| = \frac{|G|}{|H|}.$$

Théorème 1.7 (Troisième Théorème d'isomorphisme)**.** *Soient G un groupe et $H \subset K \subset G$ avec $K \lhd G$ et $H \lhd G$. Alors K/H est un sous-groupe normal de G/H et il y a un isomorphisme*

$$G/K \simeq \frac{G/H}{K/H}.$$

2 Simplicité des groupes des matrices sur un corps

Nous étudierons dans ce chapitre le groupe des matrices $n \times n$ de déterminant 1 définies sur un corps $\mathbb{K}$. Nous l'appellerons le groupe spécial linéaire d'ordre n sur $\mathbb{K}$ et nous le noterons $SL_n(\mathbb{K})$. Nous verrons que le centre de ce groupe est le sous-groupe des matrices scalaires de $SL_n(\mathbb{K})$, c'est-à-dire les multiples de la matrice identité. Nous définirons également le groupe projectif spécial linéaire, $PSL_n(\mathbb{K})$, comme étant le quotient de $SL_n(\mathbb{K})$ par son centre.

Nous introduirons aussi la notion de groupes simples, c'est-à-dire, de groupes qui ne possèdent pas de sous-groupe normal non trivial. Un groupe simple est donc un groupe qui ne peut pas être divisé de façon non-triviale. Par analogie, les groupes simples sont aux groupes quelconques, ce que les nombres premiers sont aux entiers.

Le but de ce chapitre sera de prouver le théorème d'Iwasawa qui affirme que $PSL_n(\mathbb{K})$ est un groupe simple, sauf dans le cas $n = 2$ et $|\mathbb{K}| \leq 3$.

2.1 Quelques propriétés des actions de groupe

Le but de cette section est d'établir quelques propriétés sur les actions de groupe afin de les utiliser dans le cas particulier des matrices de déterminant 1.

Ici, G désignera un groupe quelconque, S un ensemble et

$$\bullet : G \times S \to S$$

une action de groupe.

Commençons par quelques définitions :

Définition 2.1. *L'action $\bullet$ est dit **transitive** si et seulement si pour tout $x_1, x_2 \in S$, il existe $g \in G$ tel que $g \bullet x_1 = x_2$.*
*L'action $\bullet$ est dit **k-fois transitive** si et seulement si pour tout $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in S^k$ k-uples d'éléments distincts de S, il existe $g \in G$ tel que, pour tout $i \in \{1, \ldots, k\}$, $g \bullet x_i = y_i$.*

Il suit immédiatement de cette définition qu'être 1-fois transitive est équivalent à être transitive.

Définition 2.2. *Si $\pi(S)$ est une partition de S, on dit que $\pi(S)$ est **stable** par l'action de G sur S si et seulement si, pour tout $g \in G$ et pour tout $A \in \pi(S)$,*

$$g \bullet A := \{g \bullet a \mid a \in A\} \in \pi(S).$$

Exemple 2.1. Les partitions de S

$$\pi_0(S) := \{\{s\} \mid s \in S\} \text{ et } \pi_1(S) := \{S\}, \tag{2.1}$$

sont stables par l'action de G sur S.

2. Simplicité des groupes des matrices sur un corps

Définition 2.3. *Si les seules partitions de S stables par l'action de G sur S sont $\pi_0(S)$ et $\pi_1(S)$, on dit que $\bullet$ est* ***primitive****.*

Le lemme suivant caractérise les actions primitives :

Lemme 2.1. *Si $\bullet$ est transitive, alors $\bullet$ n'est pas primitive si et seulement si il existe $A \subsetneqq S$ tel que $|A| \geq 2$ et pour tout $g \in G$, $g \bullet A = A$ ou $g \bullet A \cap A = \varnothing$.*

Démonstration. Supposons d'abord que $\bullet$ n'est pas primitive. Donc, il existe une partition $\pi(S)$ de S différente de $\pi_0(S)$ et de $\pi_1(S)$ qui est stable par l'action de G sur S. Donc, il existe $A \in \pi(S)$ tel que $A \neq S$ et $|A| \geq 2$. Soit $g \in G$. Il faut montrer que $g \bullet A = A$ ou $g \bullet A \cap A = \varnothing$. Supposons que $g \bullet A \cap A \neq \varnothing$. Comme $\pi(S)$ est stable par l'action de G sur S, $g \bullet A \in \pi(S)$. Comme $\pi(S)$ est une partition, $g \bullet A = A$.
Dans l'autre sens, supposons qu'il existe $A \subsetneqq S$ tel que $|A| \geq 2$ et pour tout $g \in G$, $g \bullet A = A$ ou $g \bullet A \cap A = \varnothing$. Prouvons que $\pi(S) := \{g \bullet A \mid g \in G\}$ est une partition de S :
Si $g \in G$, $g \bullet A \neq \varnothing$ car $A \neq \varnothing$.
D'autre part, si $s \in S$: on sait qu'il existe $a \in A$ et comme $\bullet$ est transitive, il existe $g \in G$ tel que $g \bullet a = s$. Donc $s \in g \bullet A$.
Enfin, si $g, g' \in G$ sont tels que $g \bullet A \neq g' \bullet A$, prouvons par l'absurde que $g \bullet A \cap g' \bullet A = \varnothing$:
Supposons qu'il existe $a, a' \in A$ tels que $g \bullet a = g' \bullet a'$. Alors $a = g^{-1}g' \bullet a'$. Donc $(g^{-1}g') \bullet A \cap A \neq \varnothing$. Par conséquent, $(g^{-1}g') \bullet A = A$, et donc $g' \bullet A = g \bullet A$, ce qui est absurde. Donc $\pi(S)$ est une partition de S.
De plus, si $g, g' \in G$, $g' \bullet (g \bullet A) = (g'g) \bullet A \in \pi(S)$. Donc $\pi(S)$ est stable par l'action de G sur S. Or, $1 \bullet A = A \in \pi(S)$, $A \neq S$ et $|A| \geq 2$. Dès lors, $\pi(S) \neq \pi_0(S)$ et $\pi(S) \neq \pi_1(S)$. L'action $\bullet$ n'est donc pas primitive.

□

Rappelons les notions de stabilisateur et d'orbite :

Définition 2.4. *Soit $x \in S$. Le* ***stabilisateur*** *de x est le sous-groupe*

$$G_x := \{g \in G \mid g \bullet x = x\}. \tag{2.2}$$

Définition 2.5. *Soit $x \in S$. L'* ***orbite*** *de x est l'ensemble*

$$\omega(x) := \{y \in S \mid \exists g \in G,\ g \bullet x = y\}. \tag{2.3}$$

Il est trivial de vérifier que les orbites forment une partition de S.

Définition 2.6. *Soit H un sous-groupe de G. On dit que H est un sous-groupe* ***maximal*** *de G si et seulement si il n'existe pas de sous-groupe K de G tel que $H \subsetneqq K \subsetneqq G$.*

Exemple 2.2. Si S_n est le groupe symétrique d'ordre n (le groupe des permutations de n éléments), et si A_n est le groupe alterné sur n éléments (sous-groupe des permutations paires) ; alors, par le théorème de Lagrange, A_n est un sous-groupe maximal de S_n (voir [2], pages 43 et 54).

Grâce à cette définition, nous avons une autre caractérisation des actions primitives :

Proposition 2.2. *Si $\bullet$ est transitive, alors $\bullet$ est primitive si et seulement si pour tout $x \in S$, G_x est un sous-groupe maximal de G.*

Démonstration. Supposons d'abord qu'il existe $x \in S$ tel que G_x n'est pas un sous-groupe maximal de G. Donc il existe un sous-groupe H de G tel que $G_x \subsetneqq H \subsetneqq G$. Soit $A = \{h \bullet x \mid h \in H\} \subset S$. Soit $y \in G \setminus H$. Si $y \bullet x \in A$, alors il existe $h \in H$ tel que $y \bullet x = h \bullet x$, donc $(h^{-1}y) \bullet x = x$. Par conséquent, $h^{-1}y \in G_x \subset H$. Donc $y \in H$, ce qui est absurde. Donc $y \bullet x \in S \setminus A$, et donc $A \subsetneqq S$.
De plus, $1 \bullet x = x \in A$. Soit $z \in H \setminus G_x$. Donc $z \bullet x \neq x$ et $z \bullet x \in A$. Donc $|A| \geq 2$.
Soit $g \in G$. Prouvons que $g \bullet A = A$ ou $g \bullet A \cap A = \varnothing$:
Supposons que $g \bullet A \cap A \neq \varnothing$. Il existe donc $h, h' \in H$ tels que $g \bullet (h \bullet x) = h' \bullet x$. Par conséquent, $h'^{-1}gh \in G_x \subset H$, ce qui implique que $g \in H$. Donc $g \bullet A = A$.
On peut dès lors utiliser le lemme 2.1, et en déduire que $\bullet$ n'est pas primitive.

Dans l'autre sens, supposons que $\bullet$ n'est pas primitive. Soit $A \subsetneqq S$ donné par le lemme 2.1. Soit $x \in A$. Prouvons que G_x n'est pas un sous-groupe maximal de G :
Soit $H = \{g \in G \mid g \bullet A = A\}$. Il est évident que H est un sous-groupe de G.
Montrons que $G_x \subset H$: Soit $g \in G_x$. Donc $g \bullet x = x$. Comme $x \in A$, $g \bullet A \cap A \neq \varnothing$. Donc, par définition de A, $g \bullet A = A$, donc $g \in H$ et par conséquent, $G_x \subset H$
De plus, comme $|A| \geq 2$, il existe $x' \in A$ tel que $x' \neq x$. Par transitivité de $\bullet$, il existe $g_1 \in G$ tel que $g_1 \bullet x = x'$. Donc $g_1 \notin G_x$. Pourtant, $x' \in g_1 \bullet A \cap A$, donc $g_1 \bullet A = A$ et donc $g_1 \in H$. Nous pouvons donc en déduire que $G_x \subsetneqq H$
Il reste à montrer que $H \neq G$: Comme $A \neq S$, il existe $s \in S \setminus A$. Par transitivité de $\bullet$, il existe $g_2 \in G$ tel que $g_2 \bullet x = s$. Donc $g_2 \bullet A \neq A$. Par conséquent, $g_2 \notin H$. Ce qui conclut la preuve.

□

Lemme 2.3. *Si $\bullet$ est 2-fois transitive, alors $\bullet$ est primitive.*

Démonstration. Prouvons-le par l'absurde : Supposons que $\bullet$ n'est pas primitive. Soit $A \subsetneqq S$ donné par le lemme 2.1. Comme $|A| \geq 2$, on peut trouver $x, y \in A$ tels que $x \neq y$. Comme $A \neq S$, il existe $z \in S \setminus A$. Donc $x \neq z$. Comme $\bullet$ est 2-fois transitive, il existe $g \in G$ tel que $g \bullet x = x$ et $g \bullet y = z$. Donc $x \in g \bullet A \cap A$. Donc, par définition de A, $g \bullet A = A$, ce qui est absurde car $g \bullet y = z \notin A$.

□

Lemme 2.4. *Soit H un sous-groupe normal de G tel que*

$$H \not\subseteq \mathrm{Ker}(\bullet) := \{g \in G \mid g \bullet x = x \ \forall x \in S\}.$$

Si $\bullet$ est primitive, alors sa restriction à H est une action transitive sur S.

Démonstration. Soit $\bullet'$ la restriction de $\bullet$ à H. Nous savons que les orbites de $\bullet'$ forment une partition de S. Prouvons que cette partition est stable par l'action de G sur S : Soient $g \in G$ et $x \in S$. Il faut prouver que $g \bullet \omega_{\bullet'}(x)$ est une orbite pour $\bullet'$. Pour cela, montrons que $g \bullet \omega_{\bullet'}(x) = \omega_{\bullet'}(g \bullet x)$: Nous savons que

$$g \bullet \omega_{\bullet'}(x) = \{g \bullet h \bullet x \mid h \in H\}$$

et

$$\omega_{\bullet'}(g \bullet x) = \{h \bullet g \bullet x \mid h \in H\}.$$

Or, comme H est un sous-groupe normal de G, $gH = Hg$, et donc $g \bullet \omega_{\bullet'}(x) = \omega_{\bullet'}(g \bullet x)$. La partition des orbites de $\bullet'$ est donc stable par l'action de G sur S. Or, puisque $H \not\subseteq \mathrm{Ker}(\bullet)$, il existe $h \in H$ et $x \in S$ tels que $h \bullet x \neq x$. Donc $\omega_{\bullet'}(x) \neq \{x\}$. Donc la partition considérée n'est pas $\pi_0(S)$. Comme $\bullet$ est primitive, la partition considérée est $\pi_1(S)$. Il n'y a donc qu'une seule orbite pour $\bullet'$. Donc $\bullet'$ est transitive.

□

Lemme 2.5. *Si H un sous-groupe de G tel que la restriction de $\bullet$ à H est transitive, alors pour tout $x \in S$, $G = HG_x$.*

Démonstration. Soit $x \in S$. Il faut montrer que $G = HG_x$. Soit $g \in G$. Il faut donc prouver qu'il existe $h \in H$ et $k \in G_x$ tels que $g = hk$. Comme la restriction de $\bullet$ à H est transitive, il existe $h \in H$ tel que $h \bullet x = g \bullet x$. Donc $h^{-1}g \in G_x$. Pour conclure, il suffit de poser $k = h^{-1}g$.

□

Définition 2.7. *On dit que G est **simple** si et seulement si les seuls sous-groupes normaux de G sont $\{1\}$ et G.*

Exemple 2.3. Grâce au théorème de Lagrange, tout groupe fini d'ordre premier est simple.

Définition 2.8. *Le groupe G est **parfait** si et seulement si $G = [G, G]$.*

Proposition 2.6. *Le groupe G est parfait si et seulement si G est le seul sous-groupe normal K de G tel que G/K est abélien.*

Démonstration. Supposons d'abord que G est parfait. Soient $K \lhd G$ tel que G/K est abélien et $a, b \in G$. Alors,

$$[a, b]K = (aK)(bK)\left(a^{-1}K\right)\left(b^{-1}K\right) = (aK)\left(a^{-1}K\right)(bK)\left(b^{-1}K\right) = 1K.$$

Or, puisque G est parfait, il est engendré par les éléments de la forme $[a, b]$ où $a, b \in G$. Donc $G/K = \{1K\}$, ce qui implique que $K = G$. Dans l'autre sens, nous savons que $[G, G] \lhd G$ et que $G/[G, G]$ est abélien (voir [2], page 33). Donc $G = [G, G]$.

□

La dernière proposition de cette section va nous permettre de prouver que certains groupes sont simples. La fin de ce chapitre va avoir pour but de vérifier toutes les hypothèses de celle-ci dans le cas particulier des matrices de déterminant 1.

Proposition 2.7. *Supposons que $\bullet$ est primitive, que G est parfait et qu'il existe $x \in S$ tel que G_x contienne un sous-groupe normal abélien A_x tel que G est engendré par les éléments de la forme ga_xg^{-1} où $g \in G$ et $a_x \in A_x$. Soit $K := \mathrm{Ker}(\bullet)$. Alors G/K est simple.*

Démonstration. Étant donné qu'une action peut être vue comme un morphisme $\phi : G \to \mathrm{S}(S)$ où $(\mathrm{S}(S), \circ, Id_S)$ est le groupe des permutations sur S (voir [2], page 45) ; $\mathrm{Ker}(\bullet) = \mathrm{Ker}(\phi) \lhd G$. G/K est donc bien défini.
Prouvons maintenant par l'absurde que G/K est simple : Supposons qu'il existe un sous-groupe normal H' de G/K tel que $H' \neq \{K\}$ et $H' \neq G/K$. Posons

$$H = \{h \in G \mid hK \in H'\}.$$

Comme H' est un sous-groupe normal de G/K, il est évident que H est un sous-groupe normal de G. De plus, comme $H' \neq \{K\}$, $H \not\subseteq K$. Donc, comme $\bullet$ est primitive, par le lemme 2.4, on peut dire que la restriction de $\bullet$ à H est transitive. Donc, par lemme 2.5, $G = HG_x$.
Montrons que HA_x est un sous-groupe de G :
Il est évident que $1 \in HA_x$.
De plus, si $h \in H$ et $a \in A_x$,

$$a^{-1}h^{-1} = a^{-1}h^{-1}aa^{-1} \in HA_x$$

car $a^{-1}h^{-1}a \in H$ puisque H est un sous-groupe normal de G.
Enfin, si $h, h' \in H$ et $a, a' \in A_x$,

$$hah'a' = hah'a^{-1}aa' \in HA_x$$

car $ah'a^{-1} \in H$ puisque H est un sous-groupe normal de G.
Remarquons que si $g \in G$ et si $a \in A_x$, comme $G = HG_x$, il existe $h \in H$ et $g' \in G_x$ tel que $g = hg'$. Donc

$$gag^{-1} = hg'ag'^{-1}h^{-1} = h\left(g'ag'^{-1}\right)h^{-1}\left(g'ag'^{-1}\right)^{-1}\left(g'ag'^{-1}\right).$$

Comme A_x est un sous-groupe normal de G_x, $g'ag'^{-1} \in A_x$. Donc comme, H est un sous-groupe normal de G, $gag^{-1} \in HA_x$. Or, G est engendré par les éléments de la forme ga_xg^{-1} où $g \in G$ et $a_x \in A_x$. Donc $G = HA_x$.
Soient $g_1, g_2 \in G$. Alors, il existe $h_1, h_2 \in H$ et $a_1, a_2 \in A_x$ tels que $g_1 = h_1a_1$ et $g_2 = h_2a_2$. Donc

$$g_1g_2g_1^{-1}g_2^{-1} = h_1a_1h_2a_2a_1^{-1}h_1^{-1}a_2^{-1}h_2^{-1}.$$

Or, A_x est abélien. Donc

$$g_1g_2g_1^{-1}g_2^{-1} = h_1a_1h_2a_1^{-1}a_2h_1^{-1}a_2^{-1}h_2^{-1}.$$

Puisque H est un sous-groupe normal de G, $g_1g_2g_1^{-1}g_2^{-1} \in H$. Or, $G = [G, G]$. Donc G est engendré par les éléments de la forme $g_1g_2g_1^{-1}g_2^{-1}$ où $g_1, g_2 \in G$. Dès lors, $H = G$. Par conséquent, $H' = G/K$, ce qui est absurde.

□

2.2 $SL_n(\mathbb{K})$, ses générateurs et son centre

Dans la suite de ce chapitre, $\mathbb{K}$ sera un corps commutatif quelconque et $n \geq 2$ un nombre naturel. Afin de pouvoir utiliser certaines définitions et propositions dans le chapitre suivant, nous nous intéresserons aussi aux cas des matrices définies sur un anneau commutatif.

Définition 2.9. *Si R est un anneau commutatif, le* ***groupe spécial linéaire*** *d'ordre n sur R est*

$$SL_n(R) := \{A \in R^{n\times n} \mid \det(A) = 1\}. \tag{2.4}$$

Pour vérifier que $SL_n(R)$ est un groupe, il suffit de remarquer que si $A, B \in R^{n\times n}$, $\det(AB) = \det(A)\det(B)$ et que toute matrice de $SL_n(R)$ est inversible au vu de la construction de leur inverse grâce à la méthode des cofacteurs.

Dans le cas particulier où R est un corps, nous pouvons remarquer que $SL_n(\mathbb{K})$ est le noyau du morphisme de groupe

$$\det : GL_n(\mathbb{K}) := \{A \in \mathbb{K}^{n\times n} \mid \det(A) \neq 0\} \to \mathbb{K}^* : A \to \det(A). \tag{2.5}$$

Définissons quelques matrices particulières dans $SL_n(R)$:

Définition 2.10. *Soit R un anneau commutatif. Notons alors $\mathbf{e_{ij}} \in R^{n\times n}$ la matrice où toutes les entrées sont nulles, sauf celle en position (i, j) qui vaut 1.*

Définition 2.11. *Soit R un anneau commutatif. Si $b \in R$ et $i, j \in \{1, \ldots, n\}$ tels que $i \neq j$, notons $\mathbf{T_{ij}}(\mathbf{b}) \in R^{n\times n}$ la matrice définie par*

$$T_{ij}(b) := I + be_{ij}. \tag{2.6}$$

Il suit immédiatement de cette définition que $T_{ij}(b) \in SL_n(R)$.

Prouvons divers lemmes faciles, mais très utiles sur ces matrices particulières :

Lemme 2.8. *Soient $i, j, k, l \in \{1, \dots, n\}$. Alors*

$$e_{ij}e_{kl} = \delta_{jk}e_{il}, \tag{2.7}$$

où δ_{jk} est le symbole de Kronecker.

Démonstration. Cela suit immédiatement de la définition 2.10 et du produit matriciel. □

Lemme 2.9. *Soient R un anneau commutatif, $b \in R$ et $i, j \in \{1, \dots, n\}$ tels que $i \neq j$. Alors*

$$T_{ij}^{-1}(b) = T_{ij}(-b). \tag{2.8}$$

Démonstration. On sait que

$$(I - be_{ij})(I + be_{ij}) = I + be_{ij} - be_{ij} - b^2e_{ij}e_{ij} = I,$$

par le lemme 2.8.
De même,

$$(I + be_{ij})(I - be_{ij}) = I - be_{ij} + be_{ij} - b^2e_{ij}e_{ij} = I.$$

Donc

$$T_{ij}^{-1}(b) = I - be_{ij} = T_{ij}(-b).$$

□

Définition 2.12. *Soient R un anneau commutatif et $i, j \in \{1, \dots, n\}$ tels que $i \neq j$. Notons alors $\mathbf{P_{ij}} \in R^{n\times n}$ la matrice définie par*

$$P_{ij} := (I + e_{ij})(I - e_{ji})(I + e_{ij})(I - 2e_{ii}). \tag{2.9}$$

Lemme 2.10. *Soient $i, j \in \{1, \dots, n\}$ tels que $i \neq j$. Alors*

$$P_{ij} = I + e_{ij} + e_{ji} - e_{ii} - e_{jj}. \tag{2.10}$$

Démonstration. D'après la définition 2.12 et le lemme 2.8, on peut déduire que

$$\begin{aligned} P_{ij} &= (I + e_{ij})(I - e_{ji})(I + e_{ij})(I - 2e_{ii}) \\ &= (I - e_{ji} + e_{ij} - e_{ii})(I - 2e_{ii} + e_{ij}) \\ &= I - 2e_{ii} + e_{ij} - e_{ji} + 2e_{ji} - e_{jj} + e_{ij} - e_{ii} + 2e_{ii} - e_{ij} \\ &= I + e_{ij} + e_{ji} - e_{ii} - e_{jj}, \end{aligned}$$

ce qui nous donne le résultat attendu.

□

Lemme 2.11. *Soient R un anneau commutatif, $b \in R$ et $i, j, k \in \{1, \dots, n\}$ tels que i, j, k soient deux à deux distincts. Alors*

$$T_{ij}(b)(I - 2e_{ii}) = (I - 2e_{ii})T_{ij}(-b), \tag{2.11}$$

$$T_{ij}(b)(I - 2e_{jj}) = (I - 2e_{jj})T_{ij}(-b) \tag{2.12}$$

et

$$T_{ij}(b)(I - 2e_{kk}) = (I - 2e_{kk})T_{ij}(b). \tag{2.13}$$

Démonstration. Il suffit simplement de remarquer que, par le lemme 2.8,

$$\begin{aligned} T_{ij}(b)(I-2e_{ii}) &= (I+be_{ij})(I-2e_{ii}) \\ &= I-2e_{ii}+be_{ij} \\ &= (I-2e_{ii})(I-be_{ij}) \\ &= (I-2e_{ii})T_{ij}(-b) \end{aligned}$$

et

$$\begin{aligned} T_{ij}(b)(I-2e_{jj}) &= (I+be_{ij})(I-2e_{jj}) \\ &= I-2e_{jj}+be_{ij}-2be_{ij} \\ &= I-2e_{jj}-be_{ij} \\ &= (I-2e_{jj})(I-be_{ij}) \\ &= (I-2e_{jj})T_{ij}(-b) \end{aligned}$$

et enfin

$$\begin{aligned} T_{ij}(b)(I-2e_{kk}) &= (I+be_{ij})(I-2e_{kk}) \\ &= I-2e_{kk}+be_{ij} \\ &= (I-2e_{kk})(I+be_{ij}) \\ &= (I-2e_{kk})T_{ij}(b) \end{aligned}$$

□

Lemme 2.12. *Soient R un anneau commutatif, $A \in R^{n\times n}$ et $i,j \in \{1,\dots,n\}$ tels que $i \neq j$.*
La matrice $A \cdot P_{ij}$ est alors obtenue en permutant les colonnes i et j de la matrice A.
De plus, la matrice $P_{ij} \cdot A$ est obtenue en permutant les lignes i et j de la matrice A.

Démonstration. Soient a_{kl} les différentes entrées de A. Donc $A = \sum_{k,l=1}^{n} a_{kl}e_{kl}$. Par conséquent, par les lemmes 2.8 et 2.10,

$$\begin{aligned} A \cdot P_{ij} &= \left(\sum_{k,l=1}^{n} a_{kl}e_{kl}\right)(I+e_{ij}+e_{ji}-e_{ii}-e_{jj}) \\ &= \sum_{k,l=1}^{n} a_{kl}e_{kl} + \sum_{k=1}^{n} a_{ki}e_{kj} + \sum_{k=1}^{n} a_{kj}e_{ki} - \sum_{k=1}^{n} a_{ki}e_{ki} - \sum_{k=1}^{n} a_{kj}e_{kj} \\ &= \sum_{\substack{k,l=1 \\ l\neq i,j}}^{n} a_{kl}e_{kl} + \sum_{k=1}^{n} a_{kj}e_{ki} + \sum_{k=1}^{n} a_{ki}e_{kj}, \end{aligned}$$

ce qui est bien la matrice A où l'on a permuté les colonnes i et j.
De même,

$$\begin{aligned} P_{ij} \cdot A &= (I+e_{ij}+e_{ji}-e_{ii}-e_{jj})\left(\sum_{k,l=1}^{n} a_{kl}e_{kl}\right) \\ &= \sum_{k,l=1}^{n} a_{kl}e_{kl} + \sum_{l=1}^{n} a_{jl}e_{il} + \sum_{l=1}^{n} a_{il}e_{jl} - \sum_{l=1}^{n} a_{il}e_{il} - \sum_{l=1}^{n} a_{jl}e_{jl} \\ &= \sum_{\substack{k,l=1 \\ k\neq i,j}}^{n} a_{kl}e_{kl} + \sum_{l=1}^{n} a_{jl}e_{il} + \sum_{l=1}^{n} a_{il}e_{jl}, \end{aligned}$$

ce qui est bien la matrice A où l'on a permuté les lignes i et j.

□

Lemme 2.13. *Soient R un anneau commutatif, $A \in R^{n\times n}$, $b \in R$ et $i, j \in \{1, \dots, n\}$ tels que $i \neq j$.*
La matrice $A \cdot T_{ij}(b)$ est alors obtenue en remplaçant la colonne j de la matrice A par $a_{*j} + b \cdot a_{*i}$, où a_{*k} est la k^e colonne de A.
De plus, la matrice $T_{ij}(b) \cdot A$ est obtenue en remplaçant la ligne i de la matrice A par $a_{i*} + b \cdot a_{j*}$, où a_{k*} est la k^e ligne de A.

Démonstration. Comme dans la preuve du lemme précédant, définissons $a_{kl} \in \mathbb{K}$ tels que $A = \sum_{k,l=1}^{n} a_{kl}e_{kl}$. Grâce au lemme 2.8, nous pouvons calculer :

$$\begin{aligned} A \cdot T_{ij}(b) &= \left(\sum_{k,l=1}^{n} a_{kl}e_{kl}\right)(I + be_{ij}) \\ &= \sum_{k,l=1}^{n} a_{kl}e_{kl} + b\sum_{k=1}^{n} a_{ki}e_{kj} \\ &= \sum_{\substack{k,l=1 \\ l\neq j}}^{n} a_{kl}e_{kl} + \sum_{k=1}^{n}(a_{kj} + ba_{ki})e_{kj}. \end{aligned}$$

Nous obtenons donc le résultat désiré.
De la même manière, nous pouvons calculer

$$\begin{aligned} T_{ij}(b) \cdot A &= (I + be_{ij})\left(\sum_{k,l=1}^{n} a_{kl}e_{kl}\right) \\ &= \sum_{k,l=1}^{n} a_{kl}e_{kl} + b\sum_{l=1}^{n} a_{jl}e_{il} \\ &= \sum_{\substack{k,l=1 \\ k\neq i}}^{n} a_{kl}e_{kl} + \sum_{l=1}^{n}(a_{il} + ba_{jl})e_{il}, \end{aligned}$$

ce qui conclut la preuve.

□

Dans le but de trouver des générateurs de $SL_n(\mathbb{K})$, énonçons un lemme de factorisation des matrices inversibles :

Lemme 2.14. *Soit $A \in GL_n(\mathbb{K})$. Alors, il existe des matrices $P, Q \in GL_n(\mathbb{K})$, formées de produits finis de matrices de la forme $T_{ij}(b)$ et P_{ij} telles que PAQ soit une matrice diagonale.*

Démonstration. Procédons par récurrence sur n :
Si $n = 1$: la thèse est triviale.
Supposons que la thèse est vérifiée pour $n - 1$ et prouvons-la pour n :
Comme A est inversible, $\det(A) \neq 0$ et donc, il existe une sous-matrice A' de A dans $\mathbb{K}^{(n-1)\times(n-1)}$ telle que $\det(A') \neq 0$ (par sous-matrice de A, nous entendons ici, une matrice obtenue en enlevant une ligne et une colonne à A). Quitte à multiplier A par des matrices

de la forme P_{ij}, on peut supposer, par le lemme 2.12, que A' est formée des $n-1$ premières lignes et $n-1$ premières colonnes de A. Donc $A' \in GL_{n-1}(\mathbb{K})$. Dès lors, par l'hypothèse de récurrence, il existe des matrices $P', Q' \in GL_{n-1}(\mathbb{K})$, formées de produits finis de matrices de la forme $T_{ij}(b)$ et P_{ij} telles que $P'A'Q'$ soit une matrice diagonale. Soient $P_1, Q_1 \in GL_n(\mathbb{K})$ telles que

$$P_1 = \begin{pmatrix} & P' & & 0 \\ & & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} & Q' & & 0 \\ & & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Donc P_1AQ_1 est de la forme :

$$P_1AQ_1 = \begin{pmatrix} d_1 & & & a'_{1,n} \\ & \ddots & & \vdots \\ & & d_{n-1} & a'_{n-1,n} \\ a'_{n,1} & \dots & a'_{n,n-1} & a'_{n,n} \end{pmatrix}.$$

Comme P', Q' et A' sont inversibles, $d_i \neq 0$ pour tout $i \in \{1, \dots, n-1\}$. Par le lemme 2.13, nous savons que la matrice $\prod_{i=1}^{n-1} T_{ni}\left(-a'_{ni}d_i^{-1}\right) \cdot P_1AQ_1$ est de la forme

$$\prod_{i=1}^{n-1} T_{ni}\left(-a'_{ni}d_i^{-1}\right) \cdot P_1AQ_1 = \begin{pmatrix} d_1 & & & b_{1,n} \\ & \ddots & & \vdots \\ & & d_{n-1} & b_{n-1,n} \\ 0 & \dots & 0 & b_{n,n} \end{pmatrix}.$$

De même, la matrice $\prod_{i=1}^{n-1} T_{ni}\left(-a'_{ni}d_i^{-1}\right) \cdot P_1AQ_1 \cdot \prod_{i=1}^{n-1} T_{in}\left(-b_{in}d_i^{-1}\right)$ est diagonale. Donc, en posant

$$P = \prod_{i=1}^{n-1} T_{ni}\left(-a'_{ni}d_i^{-1}\right) \cdot P_1, \quad Q = Q_1 \cdot \prod_{i=1}^{n-1} T_{in}\left(-b_{in}d_i^{-1}\right),$$

nous avons la thèse.

□

Corollaire 2.15. *Soit $A \in GL_n(\mathbb{K})$. Alors, il existe des matrices $P, Q \in GL_n(\mathbb{K})$, formées de produits finis de matrices de la forme $T_{ij}(b)$ telles que PAQ soit une matrice diagonale.*

Démonstration. Grâce à la définition 2.12, on peut dire que les matrices P et Q données par lemme précédant, sont formées de produits finis de matrices de la forme $T_{ij}(b)$ et $I - 2e_{ii}$. Par le lemme 2.11, on peut supposer sans perte de généralité que P et Q sont de la forme $P = P_1P_2$ et $Q = Q_1Q_2$ où P_1 et Q_2 sont des produits finis de matrices de la forme $I - 2e_{ii}$ et P_2 et Q_1 sont des produits finis de matrices de la forme $T_{ij}(b)$. Il suffit alors de remarquer que $I - 2e_{ii}$ est une matrice diagonale inversible ; que l'inverse d'une matrice diagonale est diagonal et que le produit de deux matrices diagonales est diagonal.

□

Lemme 2.16. *Soit $d \in \mathbb{K}^*$. La matrice* $\operatorname{diag}\left\{1, \dots, 1, d^{-1}, d, 1, \dots, 1\right\}$ *est un produit fini de matrices de la forme $T_{ij}(b)$.*

Démonstration. Soit $i \in \{1, \ldots, n-1\}$ tel que d^{-1} se trouve en i^{e} position dans la matrice diagonale $\operatorname{diag}\left\{1, \ldots, 1, d^{-1}, d, 1, \ldots, 1\right\}$. Grâce au lemme 2.13, nous pouvons dire que :

$$T_{i+1,i}\left(d^{-1}\right) \cdot T_{i,i+1}(-d) = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & -d & & & \\ & & & d^{-1} & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

D'où

$$T_{i,i+1}(-d) \cdot T_{i+1,i}\left(d^{-1}\right) \cdot T_{i,i+1}(-d) = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & -d & & & \\ & & & d^{-1} & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

Donc

$$T_{i+1,i}(-1) \cdot T_{i,i+1}(-d) \cdot T_{i+1,i}\left(d^{-1}\right) \cdot T_{i,i+1}(-d) = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & -d & & & \\ & & & d^{-1} & d & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

De là,

$$\begin{aligned} &T_{i,i+1}(1) \cdot T_{i+1,i}(-1) \cdot T_{i,i+1}(-d) \cdot T_{i+1,i}\left(d^{-1}\right) \cdot T_{i,i+1}(-d) \\ &= \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & d^{-1} & 0 & & & \\ & & & d^{-1} & d & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}. \end{aligned}$$

On conclut la preuve, en remarquant que

$$T_{i+1,i}(-1)\cdot T_{i,i+1}(1)\cdot T_{i+1,i}(-1)\cdot T_{i,i+1}(-d)\cdot T_{i+1,i}\left(d^{-1}\right)\cdot T_{i,i+1}(-d)$$
$$=\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & d^{-1} & 0 & & & \\ & & & 0 & d & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

□

Corollaire 2.17. *Si $A \in SL_n(\mathbb{K})$, A est un produit fini de matrices de la forme $T_{ij}(b)$.*

Démonstration. Soient P et Q les matrices données par le corollaire 2.15.
Comme $PAQ = \operatorname{diag}\{d_1,\dots,d_n\}$ et $PAQ \in SL_n(\mathbb{K})$, nous savons que $\prod_{i=1}^{n} d_i = 1$. Donc

$$PAQ = \operatorname{diag}\left\{d_1, d_1^{-1}, 1, \dots, 1\right\}\cdot \operatorname{diag}\left\{1, d_1d_2, d_1^{-1}d_2^{-2}, 1, \dots, 1\right\}$$
$$\cdots \operatorname{diag}\left\{1,\dots,1,\prod_{i=1}^{n-1} d_i, \prod_{i=1}^{n-1} d_i^{-1}\right\}.$$

Pour conclure, il suffit d'utiliser le lemme précédant et le lemme 2.9.

□

Nous connaissons dès lors une famille de générateurs de $SL_n(\mathbb{K})$:

Proposition 2.18. *$SL_n(\mathbb{K})$ est engendré par l'ensemble des matrices de la forme $T_{ij}(b)$.*

Démonstration. Cela découle immédiatement du corollaire précédant.

□

Nous pouvons à présent prouver la première hypothèse de la proposition 2.7 pour le groupe $SL_n(\mathbb{K})$:

Proposition 2.19. *Si $n > 2$ ou si $|\mathbb{K}| > 3$, alors $SL_n(\mathbb{K})$ est parfait.*

Démonstration. Grâce à la proposition précédente, il nous suffit de montrer que $T_{ij}(b) \in [SL_n(\mathbb{K}), SL_n(\mathbb{K})]$ pour un $b \in \mathbb{K}$ et des $i, j \in \{1,\dots,n\}$ tels que $i \neq j$ quelconques.
Supposons d'abord que $n > 2$:
Dans ce cas, il existe $k \in \{1,\dots,n\}$ tel que i, j, k sont deux à deux distincts. Donc, par le lemme 2.9 :

$$\begin{aligned} T_{ik}(b)\cdot T_{kj}(1)\cdot T_{ik}(b)^{-1}\cdot T_{kj}(1)^{-1} &= (I+be_{ik})(I+e_{kj})(I-be_{ik})(I-e_{kj}) \\ &= (I+e_{kj}+be_{ik}+be_{ij})(I-e_{kj}-be_{ik}+be_{ij}) \\ &= I-e_{kj}-be_{ik}+be_{ij}+e_{kj}+be_{ik}-be_{ij}+be_{ij} \\ &= I+be_{ij} \\ &= T_{ij}(b), \end{aligned}$$

d'où $T_{ij}(b) \in [SL_n(\mathbb{K}), SL_n(\mathbb{K})]$.
Supposons maintenant que $n = 2$ et $|\mathbb{K}| > 3$:
Remarquons d'abord que, si $d \in \mathbb{K}^*$ et si $c \in \mathbb{K}$:

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} d & dc \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} d^{-1} & -cd^{-1} \\ 0 & d \end{pmatrix}$$
$$= \begin{pmatrix} 1 & c(d^2-1) \\ 0 & 1 \end{pmatrix}.$$

Puisque $|\mathbb{K}| > 3$, on peut trouver $d \in \mathbb{K}$ tel que $d \notin \{-1, 0, 1\}$. Donc d et $d^2 - 1$ sont inversibles. En prenant $c = b(d^2-1)^{-1}$, on obtient que $T_{12}(b) \in [SL_n(\mathbb{K}), SL_n(\mathbb{K})]$. De manière symétrique, on obtient que $T_{21}(b) \in [SL_n(\mathbb{K}), SL_n(\mathbb{K})]$, ce qui conclut la démonstration.
□

Remarquez l'importance des hypothèses $n > 2$ et $|\mathbb{K}| > 3$ dans la démonstration de cette proposition.

Corollaire 2.20. *Si $n > 2$ ou si $|\mathbb{K}| > 3$, alors*

$$SL_n(\mathbb{K}) = [GL_n(\mathbb{K}), GL_n(\mathbb{K})]. \tag{2.14}$$

Démonstration. L'inclusion $SL_n(\mathbb{K}) \subset [GL_n(\mathbb{K}), GL_n(\mathbb{K})]$ découle directement de la proposition précédente. Pour l'autre inclusion, il suffit de remarquer que, si $A, B \in GL_n(\mathbb{K})$, alors

$$\det\left(ABA^{-1}B^{-1}\right) = 1.$$

□

Pour conclure cette section, nous décrirons précisément le centre de $SL_n(R)$. Ceci nous permettra de mieux comprendre la notion de groupe projectif spécial linéaire dans la section suivante.

Proposition 2.21. *Soit R un anneau commutatif. Alors*

$$Z(SL_n(R)) = \{kI \mid k \in R \text{ et } k^n = 1\}. \tag{2.15}$$

Démonstration. Soit $k \in R$ tel que $k^n = 1$. Alors $\det(kI) = k^n = 1$, donc $kI \in SL_n(R)$. De plus, si $A \in SL_n(R)$,

$$kI \cdot A = kA = kAI = A \cdot kI.$$

Donc $\{kI \mid k \in R \text{ et } k^n = 1\} \subset Z(SL_n(R))$.
Si $A = (a_{ij}) \in Z(SL_n(R))$ et si $i, j \in \{1, \ldots, n\}$ tels que $i \neq j$, alors :

$$T_{ij}(1)A = AT_{ij}(1).$$

Donc

$$(I + e_{ij})A = A(I + e_{ij}),$$

D'où

$$e_{ij}A = Ae_{ij}.$$

En regardant cette relation aux positions (i, j) et (i, i), nous obtenons que $a_{jj} = a_{ii}$ et $a_{ji} = 0$. Comme i et j sont quelconques, nous pouvons dire qu'il existe $k \in R$ tel que $A = kI$. Puisque $\det(A) = 1$, $k^n = 1$ et nous avons que $Z(SL_n(R)) \subset \{kI \mid k \in R \text{ et } k^n = 1\}$.
□

Exemple 2.4. Dans le cas des matrices entières, cela peut se réécrire en deux cas : si n est pair, $Z(SL_n(\mathbb{Z})) = \{\pm I\}$ et si n est impair, $Z(SL_n(\mathbb{Z})) = \{I\}$.

Exemple 2.5. Il est immédiat de remarquer que $|Z(SL_n(\mathbb{C}))| = n$.

2.3 Théorème d'Iwasawa

Le centre d'un groupe étant toujours un sous-groupe normal de celui-ci, nous pouvons ainsi définir le groupe projectif spécial linéaire, qui est l'objet du théorème d'Iwasawa.

Définition 2.13. *Le* ***groupe projectif spécial linéaire*** *d'ordre n sur $\mathbb{K}$ est le quotient*

$$PSL_n(\mathbb{K}) := SL_n(\mathbb{K})/Z(SL_n(\mathbb{K})). \tag{2.16}$$

Définition 2.14. *L'****espace projectif*** *de dimension $n-1$ sur $\mathbb{K}$ est l'ensemble*

$$P_{n-1}(\mathbb{K}) := \{\mathbb{K}x \mid x \in \mathbb{K}^n \setminus \{0\}\} \tag{2.17}$$

où $\mathbb{K}x := \{kx \mid k \in \mathbb{K}\}$.

$P_{n-1}(\mathbb{K})$ est donc l'ensemble des droites dans $\mathbb{K}^n$ passant par l'origine.
En ayant toujours pour but d'utiliser la proposition 2.7, nous définissons $\bullet$ de la manière suivante :

$$\bullet : SL_n(\mathbb{K}) \times P_{n-1}(\mathbb{K}) \to P_{n-1}(\mathbb{K}) : (A, \mathbb{K}x) \to A \bullet \mathbb{K}x := \mathbb{K}(Ax). \tag{2.18}$$

Remarquons que cette fonction est bien définie car si $A \in SL_n(\mathbb{K})$ et si $x \in \mathbb{K}^n \setminus \{0\}$, alors $Ax \in \mathbb{K}^n \setminus \{0\}$ puisque A est inversible et $x \neq 0$. De plus, il est trivial de vérifier que c'est bien une action.
Nous noterons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$.

Le lemme suivant nous montre le lien entre la proposition 2.7 et les définitions de $PSL_n(\mathbb{K})$ et $\bullet$:

Lemme 2.22. *Le noyau de l'action définie par* (2.18) *est*

$$\mathrm{Ker}(\bullet) = Z(SL_n(\mathbb{K})). \tag{2.19}$$

Démonstration. Par la proposition 2.21, nous savons que

$$Z(SL_n(\mathbb{K})) = \{kI \mid k \in \mathbb{K} \text{ et } k^n = 1\}.$$

Soit $k \in \mathbb{K}$ tel que $k^n = 1$ et soit $\mathbb{K}x \in P_{n-1}(\mathbb{K})$. Alors

$$kI \bullet \mathbb{K}x = \mathbb{K}(kIx) = \mathbb{K}x.$$

Donc $kI \in \mathrm{Ker}(\bullet)$, d'où $Z(SL_n(\mathbb{K})) \subset \mathrm{Ker}(\bullet)$.
Dans l'autre sens, soit $A = (a_{ij}) \in \mathrm{Ker}(\bullet)$:
Donc, pour tout $i \in \{1, \ldots, n\}$, $\mathbb{K}(Ae_i) = \mathbb{K}e_i$, donc $Ae_i \in \mathbb{K}e_i$. On peut trouver $k_i \in \mathbb{K}$ tel que $Ae_i = k_i e_i$. Soit $j \in \{1, \ldots, n\}$ tel que $j \neq i$. En regardant la j^{e} composante de cette égalité, on obtient que $a_{ji} = 0$. A est donc diagonale. Soit $e = (1, \ldots, 1) \in \mathbb{K}^n \setminus \{0\}$. Comme $A \in \mathrm{Ker}(\bullet)$, on sait que $\mathbb{K}(Ae) = \mathbb{K}e$, donc $Ae \in \mathbb{K}e$. On peut donc dire qu'il existe $k \in \mathbb{K}$ tel que $Ae = ke$. Par conséquent, pour tout $i \in \{1, \ldots, n\}$, $a_{ii} = k$. Comme $A \in SL_n(\mathbb{K})$, $A \in \{kI \mid k \in \mathbb{K} \text{ et } k^n = 1\}$, ce qui conclut la preuve.

□

Lemme 2.23. *L'action définie par* (2.18) *est 2-fois transitive.*

Démonstration. Soient $\mathbb{K}x_1, \mathbb{K}x_2, \mathbb{K}y_1, \mathbb{K}y_2 \in P_{n-1}(\mathbb{K})$ tels que $\mathbb{K}x_1 \neq \mathbb{K}x_2$ et $\mathbb{K}y_1 \neq \mathbb{K}y_2$. Il faut prouver qu'il existe $T \in SL_n(\mathbb{K})$ et $a_1, a_2 \in \mathbb{K}^*$ tels que $Tx_1 = a_1y_1$ et $Tx_2 = a_2y_2$. Comme x_1 et x_2 sont linéairement indépendants, on peut former une base $(x_1, x_2, \ldots, x_n)$ de $\mathbb{K}^n$. Donc, la matrice dont les colonnes sont ces vecteurs x_i est inversible. Soit $X \in GL_n(\mathbb{K})$ cette matrice. En écrivant y_1 et y_2 dans cette base, nous pouvons dire que $y_1 = \sum_{j=1}^{n} a_{j1}x_j$ et $y_2 = \sum_{j=1}^{n} a_{j2}x_j$.
Si $n = 2$:
Comme y_1 et y_2 sont linéairement indépendants,

$$a = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \neq 0.$$

Donc,

$$X \begin{pmatrix} a_{11} & a^{-1}a_{12} \\ a_{21} & a^{-1}a_{22} \end{pmatrix} = \left(y_1 \mid a^{-1}y_2\right).$$

Donc

$$\det(X) = \det(X) \det \begin{pmatrix} a_{11} & a^{-1}a_{12} \\ a_{21} & a^{-1}a_{22} \end{pmatrix} = \det\left(y_1 \mid a^{-1}y_2\right). \tag{2.20}$$

Comme y_1 et $a^{-1}y_2$ sont linéairement indépendants, il existe une matrice inversible T telle que $Tx_1 = y_1$ et $Tx_2 = a^{-1}y_2$. Donc $TX = \left(y_1 \mid a^{-1}y_2\right)$. Comme (2.20) et que $\det(X) \neq 0$, $\det(T) = 1$. T respecte donc bien les conditions demandées.
Si $n > 2$:
Comme y_1 et y_2 sont linéairement indépendants, on peut ajouter $n-2$ colonnes à la matrice

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \end{pmatrix}$$

pour obtenir une matrice $A = (a_{ij})$ de déterminant 1. Soient $y_i = \sum_{j=1}^{n} a_{ji}x_j$ pour $i \in \{3, \ldots, n\}$. Soit $Y \in \mathbb{K}^{n\times n}$ la matrice dont les colonnes sont les y_i. Donc $XA = Y$. D'où $Y \in GL_n(\mathbb{K})$ et $\det(X) = \det(Y)$. Par conséquent, $(y_1, \ldots, y_n)$ est une base de $\mathbb{K}^n$ et il existe une matrice $T \in GL_n(\mathbb{K})$ telle que, pour tout $i \in \{1, \ldots, n\}$, $Tx_i = y_i$. Donc $TX = Y$. De là, on peut dire que $\det(T) = 1$, et donc que T respecte bien les conditions demandées.

□

Il ne nous reste donc plus qu'une seule hypothèse à vérifier ...

Lemme 2.24. *Si l'on considère l'action définie par* (2.18)*, $G_{\mathbb{K}e_1}$ contient un sous-groupe normal abélien $A_{\mathbb{K}e_1}$ tel que $SL_n(\mathbb{K})$ est engendré par les matrices de la forme BAB^{-1} où $A \in A_{\mathbb{K}e_1}$ et $B \in SL_n(\mathbb{K})$.*

Démonstration. Prouvons d'abord que

$$G_{\mathbb{K}e_1} = \{A = (a_{ij}) \in SL_n(\mathbb{K}) \mid a_{i1} = 0 \ \forall i \in \{2, \ldots, n\}\}.$$

Si $A \in G_{\mathbb{K}e_1}$, $\mathbb{K}(Ae_1) = \mathbb{K}e_1$, donc $Ae_1 = a_{11}e_1$ et donc, pour tout $i \in \{2, \ldots, n\}$, $a_{i1} = 0$. Dans l'autre sens, si $A \in SL_n(\mathbb{K})$ est telle que, pour tout $i \in \{2, \ldots, n\}$, $a_{i1} = 0$, alors

$a_{11} \neq 0$. Donc $Ae_1 = a_{11}e_1$. D'où $\mathbb{K}(Ae_1) = \mathbb{K}e_1$, ce qui prouve que $A \in G_{\mathbb{K}e_1}$.
Soit

$$f : G_{\mathbb{K}e_1} \to GL_{n-1}(\mathbb{K}) : \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & & & \\ \vdots & & A_{n-1} & \\ 0 & & & \end{pmatrix} \to A_{n-1}.$$

Remarquons que f est bien définie puisque

$$\det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & & & \\ \vdots & & A_{n-1} & \\ 0 & & & \end{pmatrix} = a_{11} \det(A_{n-1}) \neq 0.$$

De plus, si $A, B \in G_{\mathbb{K}e_1}$,

$$\begin{aligned} f(AB) &= f\left(\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & & & \\ \vdots & & A_{n-1} & \\ 0 & & & \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & & & \\ \vdots & & B_{n-1} & \\ 0 & & & \end{pmatrix} \right) \\ &= f\left(\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ 0 & & & \\ \vdots & & A_{n-1}B_{n-1} & \\ 0 & & & \end{pmatrix} \right) \\ &= A_{n-1}B_{n-1} = f(A)f(B). \end{aligned}$$

Donc f est un morphisme de groupe. Soit $A_{\mathbb{K}e_1}$ le noyau de f. Donc $A_{\mathbb{K}e_1}$ est un sous-groupe normal de $G_{\mathbb{K}e_1}$. Puisque $A_{\mathbb{K}e_1} \subset SL_n(\mathbb{K})$, il est évident que $A_{\mathbb{K}e_1}$ est l'ensemble des matrices de la forme

$$\begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix}.$$

Or,

$$\begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & b_{12} & \dots & b_{1n} \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix}.$$

Donc $A_{\mathbb{K}e_1}$ est abélien.
Il reste à montrer que $SL_n(\mathbb{K})$ est engendré par les matrices de la forme BAB^{-1} où $A \in A_{\mathbb{K}e_1}$ et $B \in SL_n(\mathbb{K})$. Par la proposition 2.18, il suffit de prouver que les matrices de la forme $T_{ij}(b)$ où $b \in \mathbb{K}$ et $i, j \in \{1, \dots, n\}$ tels que $i \neq j$ peuvent être écrites sous la forme d'un produit fini de matrices de la forme BAB^{-1} où $A \in A_{\mathbb{K}e_1}$ et $B \in SL_n(\mathbb{K})$. Il est clair que si $b \in \mathbb{K}$ et si $j \in \{2, \dots, n\}$, alors $T_{1j}(b) \in A_{\mathbb{K}e_1}$. De plus, si $b \in \mathbb{K}$ et si $i \in \{2, \dots, n\}$,

alors $I - e_{11} - e_{jj} - e_{1j} + e_{j1} \in SL_n(\mathbb{K})$. De plus, comme

$$\begin{aligned}
&(I - e_{11} - e_{jj} - e_{1j} + e_{j1})(I - e_{11} - e_{jj} + e_{1j} - e_{j1}) \\
&= I - e_{11} - e_{jj} + e_{1j} - e_{j1} - e_{11} + e_{11} - e_{1j} - e_{jj} \\
&\quad + e_{jj} + e_{j1} - e_{1j} + e_{1j} + e_{11} + e_{j1} - e_{j1} + e_{jj} \\
&= I,
\end{aligned}$$

on sait que

$$(I - e_{11} - e_{jj} - e_{1j} + e_{j1})^{-1} = I - e_{11} - e_{jj} + e_{1j} - e_{j1}.$$

Or, puisque

$$\begin{aligned}
&(I - e_{11} - e_{jj} - e_{1j} + e_{j1})T_{1j}(-b)(I - e_{11} - e_{jj} + e_{1j} - e_{j1}) \\
&= (I - e_{11} - e_{jj} - e_{1j} + e_{j1} - be_{1j} + be_{1j} - be_{jj})(I - e_{11} - e_{jj} + e_{1j} - e_{j1}) \\
&= (I - e_{11} - e_{jj} - e_{1j} + e_{j1} - be_{jj})(I - e_{11} - e_{jj} + e_{1j} - e_{j1}) \\
&= I - e_{11} - e_{jj} + e_{1j} - e_{j1} - e_{11} + e_{11} - e_{1j} - e_{jj} + e_{jj} + e_{j1} - e_{1j} + e_{1j} + e_{11} \\
&\quad + e_{j1} - e_{j1} + e_{jj} - be_{jj} + be_{jj} + be_{j1} \\
&= I + be_{j1} \\
&= T_{j1}(b),
\end{aligned}$$

on peut dire que $T_{j1}(b)$ est engendré par les matrices de la forme BAB^{-1} où $A \in A_{\mathbb{K}e_1}$ et $B \in SL_n(\mathbb{K})$. Soient $b \in \mathbb{K}$ et $i, j \in \{2, \ldots, n\}$ tels que $i \neq j$. Remarquons que

$$\begin{aligned}
T_{1j}(1)T_{i1}(-b)T_{1j}(-1)T_{i1}(b) &= (I - be_{i1} + e_{1j})(I + be_{i1} - e_{1j}) \\
&= I + be_{i1} - e_{1j} - be_{i1} + be_{ij} + e_{1j} \\
&= I + be_{ij} \\
&= T_{ij}(b).
\end{aligned}$$

Donc, comme les matrices de la forme $T_{1i}(b)$ et $T_{i1}(b)$ où $b \in \mathbb{K}$ et $i \in \{2, \ldots, n\}$ sont engendrées par les matrices de la forme BAB^{-1} où $A \in A_{\mathbb{K}e_1}$ et $B \in SL_n(\mathbb{K})$, il en est de même pour toutes les matrices de la forme $T_{ij}(b)$ où $b \in \mathbb{K}$ et $i, j \in \{1, \ldots, n\}$ avec $i \neq j$, ce qui conclut la preuve.

□

Nous pouvons enfin rassembler tous nos lemmes et propositions pour en déduire le théorème d'Iwasawa :

Théorème 2.25 (Iwasawa)**.** *Soient $\mathbb{K}$ un corps commutatif et $n \in \mathbb{N}$ tel que $n \geq 2$. Si $|\mathbb{K}| > 3$ ou si $n > 2$, alors $PSL_n(\mathbb{K})$ est simple.*

Démonstration. Se déduit immédiatement des propositions 2.7 et 2.19, des lemmes 2.23, 2.3, 2.24 et 2.22 et de la définition 2.13.

□

2.4 Le cas $n = 2$

Dans cette section, nous nous intéresserons à voir ce qui se passe quand $n = 2$ et $|\mathbb{K}| \leq 3$. Dans la suite, $p \in \mathbb{N}_0$ sera un nombre premier et nous désignerons par $\mathbb{F}_p$ le corps à p éléments.

Lemme 2.26.

$$|P_1(\mathbb{F}_p)| = p + 1. \tag{2.21}$$

Démonstration. Comme $|\mathbb{F}_p| = p$, il y a $p^2 - 1$ vecteurs non nuls dans $\mathbb{F}_p^2$. Or, chaque droite passant par l'origine supporte exactement $p-1$ vecteurs non nuls. Donc $|P_1(\mathbb{F}_p)| = \frac{p^2-1}{p-1} = p + 1$.

□

L'action définie par (2.18) nous donne donc un morphisme

$$\varphi_p : SL_2(\mathbb{F}_p) \to S_{p+1}, \tag{2.22}$$

où S_{p+1} est le groupe symétrique d'ordre $p+1$ (voir [2], page 45 et 50). Par le lemme 2.22, $\mathrm{Ker}(\varphi_p) = Z(SL_2(\mathbb{F}_p))$. Donc, en passant au quotient, nous pouvons définir un morphisme injectif

$$\varphi'_p : PSL_2(\mathbb{F}_p) \to S_{p+1}. \tag{2.23}$$

Nous pouvons dès lors voir que $PSL_2(\mathbb{F}_2)$ n'est ni simple, ni parfait.

Proposition 2.27. *Les groupes $SL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_2)$ ne sont ni simples, ni parfaits.*

Démonstration. Nous pouvons voir que

$$SL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

De plus, par la proposition 2.21, $Z(SL_2(\mathbb{F}_2)) = \{I\}$. Donc $PSL_2(\mathbb{F}_2)$ est isomorphe à $SL_2(\mathbb{F}_2)$ et $|PSL_2(\mathbb{F}_2)| = 6$. Il suffit donc de prouver que $PSL_2(\mathbb{F}_2)$ n'est ni simple, ni parfait. Or $|S_3| = 6$. Donc le morphisme défini par (2.23) est un isomorphisme. On en déduit donc que $PSL_2(\mathbb{F}_2)$ est simple si et seulement si S_3 l'est et que $PSL_2(\mathbb{F}_2)$ est parfait si et seulement si S_3 l'est. Or, nous savons que A_3 est le noyau du morphisme défini par la signature d'une permutation (voir [2], page 54). Donc $A_3 \lhd S_3$. Vu que $|A_3| = 3$, S_3 n'est pas simple et $PSL_2(\mathbb{F}_2)$ ne l'est pas non plus. De plus, par le théorème de Lagrange, $|S_3/A_3| = 2$. S_3/A_3 est donc abélien. Par la proposition 2.6, nous pouvons dire que S_3 n'est pas parfait. $PSL_2(\mathbb{F}_2)$ ne l'est donc pas non plus.

□

Intéressons-nous maintenant à $PSL_2(\mathbb{F}_3)$.

Lemme 2.28.

$$|PSL_2(\mathbb{F}_3)| = 12. \tag{2.24}$$

Démonstration. Commençons par calculer le cardinal de $GL_2(\mathbb{F}_3)$. Pour la première colonne d'une matrice quelconque de $GL_2(\mathbb{F}_3)$, nous avons le choix entre $3^2 - 1 = 8$ vecteurs non nuls. Pour la deuxième colonne, il faut choisir un vecteur linéairement indépendant du premier. Comme il y a 3 vecteurs par droite, nous avons le choix entre $3^2 - 3 = 6$ vecteurs. Donc $|GL_2(\mathbb{F}_3)| = 8 \times 6 = 48$. De plus, puisque $|\mathbb{F}_3^*| = 2$ et que l'application

$$\det : GL_2(\mathbb{F}_3) \to \mathbb{F}_3^*$$

est surjective, on peut dire que $|SL_2(\mathbb{F}_3)| = 24$. Enfin, on remarque que, par la proposition 2.21, $|Z(SL_2(\mathbb{F}_3))| = 2$. On conclut alors par le théorème de Lagrange.

□

2. Simplicité des groupes des matrices sur un corps

Lemme 2.29. *Soit $A \in SL_2(\mathbb{F}_3)$. Si φ_3 est le morphisme défini par (2.22), alors $\varphi_3(A)$ n'est pas une transposition.*

Démonstration. Prouvons-le par l'absurde et supposons qu'il existe $x, y, z, w \in \mathbb{F}_3^2$ quatre vecteurs non colinéaires deux à deux tels que $\mathbb{F}_3(Ax) = \mathbb{F}_3 x$, $\mathbb{F}_3(Ay) = \mathbb{F}_3 y$, $\mathbb{F}_3(Az) = \mathbb{F}_3 w$ et $\mathbb{F}_3(Aw) = \mathbb{F}_3 z$. Si $Ax = x$ et $Ay = y$, alors

$$A(x|y) = (x|y).$$

Or, comme x et y sont linéairement indépendants, $A = I$, ce qui est absurde car $\varphi_3(I) = Id$. Si $Ax = 2x$ et $Ay = 2y$, alors

$$A(x|y) = 2(x|y).$$

Or, comme x et y sont linéairement indépendants, $A = 2I$, ce qui est absurde car $\varphi_3(2I) = Id$. Donc, soit $Ax = x$ et $Ay = 2y$, soit $Ax = 2x$ et $Ay = y$. Par symétrie, supposons sans perte de généralité que $Ax = x$ et $Ay = 2y$. Dès lors,

$$A(x|y) = (x|y) \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

On en déduit alors que $\det(A) = 2$, ce qui est absurde.

□

Proposition 2.30. *Le groupe $PSL_2(\mathbb{F}_3)$ est isomorphe à A_4.*

Démonstration. Soit φ_3 le morphisme défini par (2.22). Soient $x, y \in \mathbb{F}_3^2$ deux vecteurs linéairement indépendants. Il existe donc $A \in \mathbb{F}_3^{2\times 2}$ telle que $Ax = 2y$ et $Ay = 2x$. Donc

$$A(x|y) = 2(y|x).$$

Or $\det((x|y)) = -\det((y|x))$ et $\det((x|y))^{-1} = \det((x|y))$ car $\det((x|y)) \in \{1, 2\}$. Donc

$$\det(A) = 2\det((y|x))\det((x|y)) = 1.$$

On en déduit donc que $A \in SL_2(\mathbb{F}_3)$. Par le lemme précédant, $\varphi_3(A)$ ne peut être une transposition. C'est donc obligatoirement une double transposition. $\mathrm{Im}(\varphi_3)$ contient donc toutes les doubles transpositions de S_4. Soit φ_3' le morphisme défini par (2.23). Alors $\mathrm{Im}(\varphi_3')$ contient aussi toutes les doubles transpositions de S_4.

Supposons que $\mathrm{Im}(\varphi_3')$ contienne un 4-cycle. Sans perte de généralité, nous pouvons supposer que

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in \mathrm{Im}(\varphi_3').$$

Donc, comme $\mathrm{Im}(\varphi_3')$ est un sous-groupe de S_4,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \left[\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right] = \begin{pmatrix} 1 & 3 \end{pmatrix} \in \mathrm{Im}(\varphi_3'),$$

ce qui, par le lemme précédant, est absurde. $\mathrm{Im}(\varphi_3')$ ne contient donc aucun 4-cycle. Comme φ_3' est injectif et vu le lemme 2.28, $|\mathrm{Im}(\varphi_3')| = 12$. Donc, puisque $\mathrm{Im}(\varphi_3')$ ne contient aucune transposition ni aucun 4-cycle de S_4, $\mathrm{Im}(\varphi_3') = A_4$. On en déduit donc que φ_3' est l'isomorphisme recherché.

□

Lemme 2.31. *Le groupe A_4 n'est pas simple.*

Démonstration. Soit

$$K = \left\{ Id, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \right\} \subset A_4.$$

Vu que

$$\left[\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right]^{-1} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}$$

et que

$$\left[\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right] \left[\begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \right] = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix},$$

par symétrie, nous pouvons dire que K est un sous-groupe de A_4. De plus,

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \left[\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right] \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \in A_4$$

et

$$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \left[\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \right] \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \in A_4.$$

Par symétrie, nous remarquons que K est un sous-groupe normal non trivial de A_4.

□

Corollaire 2.32. *Le groupe $PSL_2(\mathbb{F}_3)$ n'est pas simple et $SL_2(\mathbb{F}_3)$ n'est pas parfait.*

Démonstration. Le fait que $PSL_2(\mathbb{F}_3)$ n'est pas simple se déduit de la proposition 2.30 et du lemme précédent.

Pour l'autre partie de la thèse, soit K le sous-groupe normal de A_4 défini dans la preuve précédente. Puisque $|A_4| = 12$ et que $|K| = 4$, par le théorème de Lagrange, $|A_4/K| = 3$. Or, tout groupe d'ordre 3 est abélien. A_4/K est donc abélien. De plus, nous avons des morphismes surjectifs

$$\pi_1 : SL_2(\mathbb{F}_3) \to PSL_2(\mathbb{F}_3), \quad \pi_2 : A_4 \to A_4/K.$$

Puisque $PSL_2(\mathbb{F}_3) \simeq A_4$, nous avons un morphisme surjectif

$$\varphi : SL_2(\mathbb{F}_3) \to A_4/K.$$

Dès lors, $SL_2(\mathbb{F}_3)/\operatorname{Ker}(\varphi)$ est isomorphe à A_4/K, qui est abélien. Puisque $\operatorname{Ker}(\varphi) \neq SL_2(\mathbb{F}_3)$, par la proposition 2.6, $SL_2(\mathbb{F}_3)$ n'est pas parfait.

□

3 Quotients des groupes des matrices sur $\mathbb{Z}$

Intéressons-nous maintenant à l'étude de $SL_n(\mathbb{Z})$. Comme dans le chapitre précédent, nous aimerions connaître la structure des sous-groupes normaux du groupe des matrices de déterminant 1. Malheureusement, vu que les entiers n'ont en général pas d'inverse dans $\mathbb{Z}$, nous n'aurons pas un résultat aussi fort que le théorème d'Iwasawa.

Cependant, nous prouverons le théorème de Mennicke, qui nous assure que les quotients non triviaux de $SL_n(\mathbb{Z})$ sont d'ordre fini. Nous obtiendrons même un résultat plus fort, à savoir que tout sous-groupe normal non trivial de $SL_n(\mathbb{Z})$ contient un m$^{\text{e}}$ sous-groupe de congruence. C'est-à-dire qu'il existe un $m \in \mathbb{N}_0$ tel que toutes les matrices congrues à l'identité modulo m appartiendront à ce sous-groupe normal.

Contrairement au théorème d'Iwasawa, le théorème de Mennicke impose que $n > 2$. Nous prouverons dans la dernière section de ce chapitre que ce résultat est faux pour les matrices 2×2.

3.1 $N_{n,m}$, m$^{\text{e}}$ sous-groupe de congruence

Le but de cette section est de prouver que le plus petit sous-groupe normal de $SL_n(\mathbb{Z})$ contenant $T_{21}(m)$ pour un $m \in \mathbb{N}_0$ donné, est le sous-groupe de toutes les matrices de $SL_n(\mathbb{Z})$ qui sont congrues à I modulo m. Nous fixerons donc $m \in \mathbb{N}_0$, un naturel non nul quelconque.

3.1.1 Premières définitions et générateurs de $SL_n(\mathbb{Z})$

Commençons par quelques notions de théorie des groupes :

Définition 3.1. *Soient G un groupe et $A \subset G$. Le* ***sous-groupe engendré*** *par A est*

$$\langle A \rangle := \bigcap_{A \subset H \leq G} H. \tag{3.1}$$

Autrement dit, $\langle A \rangle$ est le plus petit sous-groupe de G contenant A. Si $g \in G$, nous noterons $\langle g \rangle = \langle \{g\} \rangle$.

Exemple 3.1. Dans $(\mathbb{Z}, +, 0)$, $\langle m \rangle = m\mathbb{Z}$ pour tout $m \in \mathbb{Z}$.

De même, nous pouvons définir le plus petit sous-groupe normal contenant A :

Définition 3.2. *Soient G un groupe et $A \subset G$. La* ***clôture normale*** *de A est*

$$\langle\langle A \rangle\rangle := \bigcap_{A \subset H \lhd G} H. \tag{3.2}$$

Il est trivial de vérifier que $\langle\langle A \rangle\rangle$ est le plus petit sous-groupe normal de G contenant A. Si $g \in G$, nous noterons $\langle\langle g \rangle\rangle = \langle\langle \{g\} \rangle\rangle$.

3. Quotients des groupes des matrices sur $\mathbb{Z}$

Définition 3.3. *Soient G un groupe et $g \in G$. La* ***classe de conjugaison*** *de g est*

$$Cl(g) := \left\{ xgx^{-1} | x \in G \right\}. \tag{3.3}$$

Lemme 3.1. *Soient G un groupe et $g \in G$. Notons K le sous-ensemble de G des éléments formés par des produits finis d'éléments de la forme xgx^{-1} ou $xg^{-1}x^{-1}$ où $x \in G$. Alors*

$$\langle Cl(g) \rangle = K = \langle\langle g \rangle\rangle. \tag{3.4}$$

Démonstration. Remarquons d'abord que $K \lhd G$:
Comme $I = gg^{-1}$, $I \in K$.
Si $g_1, g_2 \in K$, par définition de K, il est évident que $g_1 g_2 \in K$ et $g_1^{-1} \in K$.
Enfin, si $g_1 \in K$ et si $x \in G$, il existe $n \in \mathbb{N}_0$ et $y_i \in G$ pour $i \in \{1, \dots, n\}$ de la forme $x'gx'^{-1}$ ou $x'g^{-1}x'^{-1}$ où $x' \in G$ tels que $g_1 = y_1 \cdots y_n$. Donc

$$xg_1x^{-1} = xy_1 \cdots y_n x^{-1} = \left(xy_1x^{-1}\right) \cdots \left(xy_nx^{-1}\right) \in K.$$

On a donc bien que $K \lhd G$.
Maintenant, pour prouver que $\langle Cl(g) \rangle = K$, il suffit de voir que $Cl(g) \subset K \subset \langle Cl(g) \rangle$. Pour l'autre égalité, remarquer que $g \in K \subset \langle\langle g \rangle\rangle$.

□

Appliquons ce résultat dans le cas où $G = SL_n(\mathbb{Z})$:

Définition 3.4. *Soit $n \in \mathbb{N}_0$. Posons*

$$\mathbf{Q_{n,m}} := \langle\langle T_{21}(m) \rangle\rangle. \tag{3.5}$$

Lemme 3.2. *Soit $n \in \mathbb{N}_0$. Notons K le sous-ensemble de $SL_n(\mathbb{Z})$ des matrices formées par des produits finis de matrices de la forme $XT_{21}(m)X^{-1}$ ou $XT_{21}(-m)X^{-1}$ où $X \in SL_n(\mathbb{Z})$. Alors $K = Q_{n,m}$.*

Démonstration. Ceci est un corollaire immédiat du lemme 3.1.

□

Définissons maintenant un deuxième sous-groupe normal de $SL_n(\mathbb{Z})$:

Définition 3.5. *Soit $n \in \mathbb{N}_0$. Le* ***m^e sous-groupe de congruence*** *est défini par*

$$\mathbf{N_{n,m}} := \{A \in SL_n(\mathbb{Z}) \mid A \equiv I \ (mod\ m)\}. \tag{3.6}$$

Si $\varphi_{n,m} : SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/m\mathbb{Z})$ est le morphisme canonique entre ces deux groupes, nous remarquons que $N_{n,m} = \mathrm{Ker}(\varphi_{n,m})$. $N_{n,m}$ est donc un sous-groupe normal de $SL_n(\mathbb{Z})$.

Lemme 3.3. *Pour tout $n \in \mathbb{N}_0$,*

$$Q_{n,m} \subset N_{n,m} \tag{3.7}$$

Démonstration. Il suffit de remarquer que $Q_{n,m}$ est le plus petit sous-groupe normal de $SL_n(\mathbb{Z})$ contenant $T_{21}(m)$ et que $T_{21}(m) \in N_{n,m} \lhd SL_n(\mathbb{Z})$.

□

Finissons cette sous-section par une proposition qui nous dit que $SL_n(\mathbb{Z})$ est engendré par un nombre fini d'éléments.

Proposition 3.4. *Soit $n \in \mathbb{N}_0$. Les matrices de la forme $T_{ij}(1)$ où $i, j \in \{1, \dots, n\}$ tels que $i \neq j$ et leur inverse engendrent $SL_n(\mathbb{Z})$.*

Démonstration. Procédons par récurrence sur n :
Si $n = 1$, la thèse est triviale vu que $SL_1(\mathbb{Z}) = \{I\}$.
Supposons que la thèse est vérifiée pour $n-1$ et prouvons-la pour n :
Soit $A = (a_{ij}) \in SL_n(\mathbb{Z})$. La thèse est équivalente à prouver qu'on peut multiplier A par des matrices de la forme $T_{ij}(1)$ où $i, j \in \{1, \dots, n\}$ tels que $i \neq j$ et par leur inverse pour obtenir I. Pour ce faire, nous utiliserons les lemmes 2.9 et 2.13. En multipliant à gauche A par $T_{ij}(1)$, l'élément à la position $(i, 1)$ devient $a_{i1} + a_{j1}$. De même, en multipliant à gauche A par $T_{ij}(1)^{-1} = T_{ij}(-1)$, l'élément à la position $(i, 1)$ devient $a_{i1} - a_{j1}$, les autres éléments de la première colonne restant inchangés. Nous pouvons alors appliquer l'algorithme d'Euclide aux éléments a_{i1} où $i \in \{1, \dots, n\}$, et obtenir une matrice $A' = (a'_{ij}) \in SL_n(\mathbb{Z})$ telle qu'il existe $k \in \{1, \dots, n\}$ avec

$$a'_{k1} = (a_{i1}, i \in \{1, \dots, n\})$$

et $a'_{i1} = 0$ si $i \in \{1, \dots, n\} \backslash \{k\}$. Or, comme $\det(A) = 1$, nous savons que

$$(a_{i1}, i \in \{1, \dots, n\}) = 1.$$

Si $k \neq 1$, alors, en multipliant à gauche A' par $T_{k1}(-1)T_{1k}(1)$, nous obtenons une matrice de la forme $A'' = (a''_{ij}) \in SL_n(\mathbb{Z})$ telle que $a''_{11} = 1$ et $a''_{i1} = 0$ pour $i \in \{2, \dots, n\}$. Maintenant, en multipliant A'' à droite par $T_{1j}(-1)^{a''_{1j}}$ pour tout $j \in \{2, \dots, n\}$, nous obtenons une matrice $B = (b_{ij}) \in SL_n(\mathbb{Z})$ telle que $b_{11} = 1$, $b_{i1} = 0$ pour tout $i \in \{2, \dots, n\}$ et $b_{1j} = 0$ pour tout $j \in \{2, \dots, n\}$.
Pour obtenir I, et donc conclure la preuve, il suffit d'utiliser l'hypothèse de récurrence et le fait que, si $C, D \in \mathbb{Z}^{(n-1)\times(n-1)}$, alors

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & D & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & CD & \\ 0 & & & \end{pmatrix}.$$

□

Comme annoncé, nous aimerions montrer que, pour tout $n \geq 3$, $Q_{n,m} = N_{n,m}$. Pour ce faire, nous allons procéder par récurrence sur n. Étrangement, le cas de base de cette induction est plus difficile à montrer que le pas inductif. En effet, dans [1], Brenner avait réussi à prouver ce pas inductif mais pas le cas de base. Il a d'ailleurs conjecturé que la thèse était vérifiée pour $n \geq 2$, ce qui est faux. Nous allons donc commencer par prouver le pas inductif de la récurrence.

3.1.2 Le pas inductif

Afin d'utiliser les lemmes présentés dans cette sous-section pour prouver le cas de base, nous les prouverons également pour $n = 3$. Fixons donc $n \in \mathbb{N}$ tel que $n \geq 3$ et montrons que si $Q_{n-1,m} = N_{n-1,m}$ alors $Q_{n,m} = N_{n,m}$. Commençons par prouver un lemme qui nous permettra de trivialiser la première colonne des matrices considérées par conjugaison.

Lemme 3.5. *Soit $A = (a_{ij}) \in SL_n(\mathbb{Z})$ telle qu'il existe $k \in \{2, \dots, n\}$ tel que $a_{k1} \neq 0$. Notons $d = (a_{i1}, i \in \{2, \dots, n\}) \in \mathbb{N}_0$. Alors, il existe $X \in SL_n(\mathbb{Z})$ de sorte que, si nous posons $XAX^{-1} = B = (b_{ij})$, alors $b_{21} = d$ et $b_{i1} = 0$ pour tout $i \in \{3, \dots, n\}$.*

Démonstration. Puisque $Y\left(XZX^{-1}\right)Y^{-1} = (YX)Z(YX)^{-1}$ pour tout $X, Y, Z \in SL_n(\mathbb{Z})$, on pourra appliquer plusieurs fois une transformation du type XAX^{-1} où $X \in SL_n(\mathbb{Z})$

pour arriver au résultat.
Ensuite, si $n = 3$, $-P_{23} \in SL_3(\mathbb{Z})$. Donc, quitte à remplacer A par $(-P_{23})A(-P_{23})$, nous pourrons permuter les éléments non diagonaux de la première colonne de A. Par contre, si $n > 3$ et si $i \in \{3, \dots, n\}$, on peut remplacer A par $(P_{ij}P_{i2})A(P_{i2}P_{ij})$ où $j \in \{3, \dots, n\}\backslash\{i\}$. Dans tous les cas, on peut donc monter un élément non diagonal de la première colonne de A en position $(2, 1)$.
Soient $k_{i2} \in \mathbb{Z}$ pour $i \in \{3, \dots, n\}$ et soit $X = I + \sum_{i=3}^{n} k_{i2}e_{i2} \in SL_n(\mathbb{Z})$. Puisque

$$\begin{aligned} X\left(I - \sum_{i=3}^{n} k_{i2}e_{i2}\right) &= I - \sum_{i=3}^{n} k_{i2}e_{i2} + \sum_{i=3}^{n} k_{i2}e_{i2} \\ &= I, \end{aligned}$$

$X^{-1} = I - \sum_{i=3}^{n} k_{i2}e_{i2}$. De plus,

$$\begin{aligned} XAX^{-1} &= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & k_{32} & 1 & \\ & \vdots & & \ddots \\ & k_{n2} & & 1 \end{pmatrix} \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & -k_{32} & 1 & \\ & \vdots & & \ddots \\ & -k_{n2} & & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & \\ a_{21} & \\ k_{32}a_{21} + a_{31} & * \\ \vdots & \\ k_{n2}a_{21} + a_{n1} & \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & -k_{32} & 1 & \\ & \vdots & & \ddots \\ & -k_{n2} & & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & \\ a_{21} & \\ k_{32}a_{21} + a_{31} & * \\ \vdots & \\ k_{n2}a_{21} + a_{n1} & \end{pmatrix}. \end{aligned}$$

Donc, en choisissant correctement les k_{i2}, on peut réduire les éléments non diagonaux de la première colonne de A modulo a_{21}. Grâce à la remarque en début de preuve et en recommençant l'opération, on peut appliquer l'algorithme d'Euclide et obtenir le résultat désiré.

□

Lemme 3.6. *Soient $i, j \in \{1, \dots, n\}$ tels que $i \neq j$. Alors il existe $X \in SL_n(\mathbb{Z})$ tel que $XT_{21}(m)X^{-1} = T_{ij}(m)$.*

La difficulté de la preuve réside dans le fait que $\det(P_{ij}) = -1$ et non 1 :

Démonstration. Séparons la preuve en plusieurs cas :

i = 1 : Si $j \neq 2$: $(P_{1j}P_{2j})T_{21}(m)(P_{2j}P_{1j}) = T_{1j}(m)$. Si par contre $j = 2$:
Soit $n = 3$ et alors $-P_{21} \in SL_n(\mathbb{Z})$ donc $(-P_{21})T_{21}(m)(-P_{21}) = T_{12}(m)$.
Soit $n > 3$ et alors $(P_{42}P_{34}P_{31}P_{23})T_{21}(m)(P_{23}P_{31}P_{34}P_{42}) = T_{12}(m)$.

i = 2 : Si $j = 1$, la thèse est triviale.
Sinon : Soit $n = 3$ et alors $-P_{1j} \in SL_n(\mathbb{Z})$ donc $(-P_{1j})T_{21}(m)(-P_{1j}) = T_{2j}(m)$.

Soit $n > 3$ et alors, il existe $k \in \{3, \dots, n\} \backslash \{j\}$. Dans ce cas, il suffit de voir que $(P_{kj}P_{1k})T_{21}(m)(P_{1k}P_{kj}) = T_{2j}(m)$.

i $\geq$ 3 : Si $j \neq 1$, on a la thèse en observant que $(P_{1j}P_{2i})T_{21}(m)(P_{2i}P_{1j}) = T_{ij}(m)$.
Par contre, si $j = 1$, on procède comme suit :
Soit $n = 3$ et alors $-P_{2i} \in SL_n(\mathbb{Z})$. Donc $(-P_{2i})T_{21}(m)(-P_{2i}) = T_{i1}(m)$.
Soit $n > 3$ et alors, il existe $k \in \{3, \dots, n\} \backslash \{i\}$. On conclut en remarquant que $(P_{ki}P_{2k})T_{21}(m)(P_{2k}P_{ki}) = T_{i1}(m)$.

□

Ce lemme montre que $T_{ij}(m) \in Q_{n,m}$. De là, on peut dire que $T_{ij}(km) \in Q_{n,m}$ pour tout $k \in \mathbb{Z}$ et pour tout $i, j \in \{1, \dots, n\}$ tels que $i \neq j$.
Avant de prouver le pas inductif de notre récurrence, nous avons besoin d'un dernier lemme :

Lemme 3.7. *Soit $H = (h_{ij}) \in N_{n,m}$. Alors, on peut, en un nombre fini d'opérations du type :*
- *transformer H en XHX^{-1} où $X \in SL_n(\mathbb{Z})$,*
- *multiplier H à gauche ou à droite par des matrices de la forme $XT_{21}(m)X^{-1}$ ou $XT_{21}(-m)X^{-1}$ où $X \in SL_n(\mathbb{Z})$,*

transformer H en une matrice $H' = (h'_{ij}) \in N_{n,m}$ telle qu'il existe $k \in \{1, \dots, n\}$ avec $h'_{kk} = 1$ et $h'_{ik} = h'_{ki} = 0$ pour tout $i \in \{1, \dots, n\} \backslash \{k\}$.

Démonstration. Remarquons d'abord que, comme $N_{n,m}$ est un sous-groupe normal de $SL_n(\mathbb{Z})$ et que $T_{21}(m) \in N_{n,m}$, la transformation de H en H' par de telles opérations, nous donnera toujours $H' \in N_{n,m}$. De plus, par le lemme 3.6, nous pouvons multiplier H par des matrices de la forme $XT_{ij}(m)X^{-1}$ ou $XT_{ij}(-m)X^{-1}$ où $X \in SL_n(\mathbb{Z})$ et où $i, j \in \{1, \dots, n\}$ sont tels que $i \neq j$.
Nous allons d'abord prouver que l'on peut obtenir une matrice H_1 ayant un de ses éléments diagonaux égal à 1 :
Si tous les éléments non diagonaux de la première colonne de H sont nuls, alors nous pouvons remplacer H par $T_{21}(m)H$ pour obtenir $h_{21} \neq 0$. Supposons donc qu'au moins un élément non diagonal de la première colonne de H est non nul. Nous pouvons alors affirmer que leur p.g.c.d. est un multiple de m, disons lm avec $l \in \mathbb{Z}_0$. Dans ce cas, nous pouvons utiliser le lemme 3.5 afin d'obtenir une matrice $B = (b_{ij}) \in N_{n,m}$ telle que $b_{21} = lm$ et $b_{i1} = 0$ pour tout $i \in \{3, \dots, n\}$.
Comme $\det(B) = 1$, il existe $s \in \{2, \dots, n\}$ tel que $b_{3s} \neq 0$. Donc, quitte à remplacer B par $BT_{s2}(m)$, on peut, sans changer les hypothèses sur la première colonne de B, supposer que $b_{32} \neq 0$. Comme $\det(B) = 1$, nous pouvons dire que $(b_{11}, l) = 1$. Donc, par le théorème de Dirichlet (théorème 1.5), il existe $c \in \mathbb{N}_0$ tel que $cb_{11} + l$ soit un nombre premier qui ne divise pas b_{32}. Posons alors $L = (l_{ij}) = T_{21}(m)^c B \in N_{n,m}$. Comme $T_{21}(m)^c = T_{21}(cm)$, nous avons $l_{32} = b_{32}$, $l_{21} = (l + cb_{11})m$ et $l_{31} = 0$. Par construction de c et comme b_{32} est divisible par m, $(l_{21}, l_{32}) = m$. Donc, comme $l_{22} \equiv 1 \ (mod\ m)$, par Bézout (lemme 1.2), il existe $d, d' \in \mathbb{Z}$ tels que $l_{22} - dl_{21} + d'l_{32} = 1$. Enfin, en transformant L par

$$H_1 = T_{12}(d)T_{23}(d')LT_{23}(-d')T_{12}(-d),$$

nous obtenons notre matrice H_1 souhaitée. En effet, les éléments de $T_{12}(d)T_{23}(d')L = (I + de_{12} + d'e_{23} + dd'e_{13})L$ en position $(2, i)$ sont, pour tout $i \in \{1, \dots, n\}$, $l_{2i} + d'l_{3i}$. Donc, l'élément de $H_1 = T_{12}(d)T_{23}(d')L(I - de_{12} - d'e_{23})$ en position $(2, 2)$ est

$$l_{22} + d'l_{32} - dl_{21} - dd'l_{31} = 1.$$

Notre matrice $H_1 = (g_{ij})$ a donc la propriété que g_{ik} et g_{ki} sont divisibles par m pour tout $i \in \{1, \dots, n\}\backslash\{k\}$ où k est tel que $g_{kk} = 1$. Pour conclure la preuve, il suffit de poser

$$H' = \prod_{\substack{i=1 \\ i\neq k}}^{n} T_{ik}(m)^{\frac{-g_{ik}}{m}} \cdot H_1 \cdot \prod_{\substack{i=1 \\ i\neq k}}^{n} T_{ki}(m)^{\frac{-g_{ki}}{m}}.$$

□

Nous sommes maintenant en mesure de prouver le pas inductif de la récurrence, dû à Brenner :

Proposition 3.8. *Soient $m, n \in \mathbb{N}_0$ tels que $n \geq 4$. Si $Q_{n-1,m} = N_{n-1,m}$ alors $Q_{n,m} = N_{n,m}$.*

Démonstration. Nous savons déjà que $Q_{n,m} \subset N_{n,m}$. Il reste donc à montrer que $N_{n,m} \subset Q_{n,m}$. Prouvons-le par l'absurde et supposons qu'il existe $H \in N_{n,m}\backslash Q_{n,m}$. Soit $H' = (h'_{ij}) \in N_{n,m}$ la matrice donnée par le lemme précédant. Donc, il existe $k \in \{1, \dots, n\}$ tel que $h'_{kk} = 1$ et $h'_{ik} = h'_{ki} = 0$ pour tout $i \in \{1, \dots, n\}\backslash\{k\}$. Si $k \neq 1$:
Soit $j \in \{2, \dots, n\}\backslash\{k\}$. Quitte à remplacer H' par $(P_{j1}P_{kj})H'(P_{kj}P_{j1})$, on peut supposer que $k = 1$. Il existe donc $A \in \mathbb{K}^{(n-1)\times(n-1)}$ telle que

$$H' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}.$$

Donc $\det(A) = \det(H') = 1$ et $A \equiv I_{n-1}$ $(mod\ m)$. Donc $A \in N_{n-1,m}$. De plus, par construction de H' et comme $T_{21}(m) \in Q_{n,m} \lhd SL_n(\mathbb{Z})$, si $H' \in Q_{n,m}$ alors $H \in Q_{n,m}$, ce qui est absurde. Donc $H' \notin Q_{n,m}$.
Or, comme $A \in Q_{n-1,m}$, par le lemme 3.2, nous pouvons dire qu'il existe $Y_i \in SL_{n-1}(\mathbb{Z})$ pour $i \in \{1, \dots, l\}$ de la forme $XT_{21}(m)X^{-1}$ ou $XT_{21}(-m)X^{-1}$ où $X \in SL_{n-1}(\mathbb{Z})$ telles que $A = Y_1 \cdots Y_l$. Dès lors, comme pour tout $B, C \in \mathbb{Z}^{(n-1)\times(n-1)}$,

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & BC & \\ 0 & & & \end{pmatrix},$$

H' est le produit fini de matrices de la forme $XT_{32}(m)X^{-1}$ ou $XT_{32}(-m)X^{-1}$ où $X \in SL_n(\mathbb{Z})$. Donc, par les lemmes 3.2 et 3.6, on en déduit que $H' \in Q_{n,m}$. Ce qui est absurde.
□

3.1.3 Le cas de base

Pour finir notre récurrence, il reste une dernière étape, et non des moindres : prouver que $Q_{3,m} = N_{3,m}$. La preuve présentée dans cette sous-section est due à Mennicke.

Lemme 3.9. *Soit $H \in N_{3,m}$. Soit $\pi : SL_3(\mathbb{Z}) \to SL_3(\mathbb{Z})/Q_{3,m}$ le morphisme quotient canonique. Alors $\pi(H)$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$.*

Démonstration. Comme $T_{21}(m) \in Q_{3,m} \lhd SL_3(\mathbb{Z})$, si on multiplie H par $XT_{21}(m)X^{-1}$ ou par $XT_{21}(-m)X^{-1}$ où $X \in SL_3(\mathbb{Z})$, l'image $\pi(H)$ reste inchangée. De plus, si on prouve que $K = XHX^{-1}$ où $X \in SL_3(\mathbb{Z})$ est telle que $\pi(K)$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$, il en est de même pour H (puisque $\pi(H) = \pi\left(X^{-1}\right)\pi(K)\pi(X) = \pi(K)$). Soit $H' = (h'_{ij})$ la matrice donnée par lemme 3.7. Il suffit donc de montrer que $\pi(H')$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$.
Soit $k \in \{1,2,3\}$ tel que $h'_{kk} = 1$ et $h'_{ik} = h'_{ki} = 0$ pour $i \in \{1,2,3\}\backslash\{k\}$. Quitte à remplacer H' par $(-P_{k2})H'(-P_{k2})$, nous pouvons, sans perte de généralité, supposer que

$$H' = \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix} \in N_{3,m},$$

où $a, b, c, d \in \mathbb{Z}$. Vu que $\det(H') = 1$, on peut dire que $ad - bc = 1$. Donc

$$\begin{aligned} H'T_{21}(1) &= \begin{pmatrix} a & 0 & b \\ 1 & 1 & 0 \\ c & 0 & d \end{pmatrix} \\ &= \begin{pmatrix} a & 0 & b \\ ad-bc & 1 & 0 \\ c & 0 & d \end{pmatrix} \\ &= T_{21}(1)^d \begin{pmatrix} a & 0 & b \\ -bc & 1 & -bd \\ c & 0 & d \end{pmatrix} \\ &= T_{21}(1)^d T_{23}(1)^{-b} H'. \end{aligned}$$

Or, $b \equiv 0\ (mod\ m)$ et $d \equiv 1\ (mod\ m)$. Par conséquent, grâce au lemme 3.6, on peut dire que $T_{21}(1)^{d-1} \in Q_{3,m}$ et que $T_{23}(1)^{-b} \in Q_{3,m}$. Donc $\pi(H')\pi(T_{21}(1)) = \pi(T_{21}(1))\pi(H')$.
De même, puisque

$$H'T_{32}(1) = T_{32}(1)^d T_{12}(1)^b H',$$

on sait que,

$$\pi(H')\pi(T_{32}(1)) = \pi(T_{32}(1))\pi(H').$$

Or

$$T_{32}(1)T_{21}(1)T_{32}(1)^{-1}T_{21}(1)^{-1} = T_{31}(1),$$

donc

$$\pi(H')\pi(T_{31}(1)) = \pi(T_{31}(1))\pi(H').$$

Par symétrie, nous pouvons aussi affirmer que $\pi(H')$ commute également avec $\pi(T_{12}(1))$, $\pi(T_{23}(1))$ et $\pi(T_{13}(1))$. Or, par le lemme 3.4, les six matrices $T_{12}(1)$, $T_{21}(1)$, $T_{13}(1)$, $T_{31}(1)$, $T_{23}(1)$, $T_{32}(1)$ et leur inverse engendrent $SL_3(\mathbb{Z})$. Donc $\pi(H')$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$.

□

Lemme 3.10. *Soit $H \in N_{3,m}$ telle que*

$$H = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

pour certains $a, b, c, d \in \mathbb{Z}$. *Appelons également* $\pi : SL_3(\mathbb{Z}) \to SL_3(\mathbb{Z})/Q_{3,m}$ *le morphisme quotient canonique. Si* $n \in \mathbb{N}_0$, *alors, il existe une matrice* $H_n \in N_{3,m}$ *de la forme*

$$H_n = \begin{pmatrix} a & b^n & 0 \\ (-1)^{n+1}c^n & d_n & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

avec $d_n \in \mathbb{Z}$, *telle que* $\pi(H_n) = \pi(H)^n$.

Démonstration. Prouvons ce lemme par récurrence sur n. Pour $n = 1$, il suffit de prendre $d_1 = d$. Supposons que le lemme soit vérifié pour n et prouvons le pour $n + 1$:
Par le lemme précédant, nous pouvons dire que $\pi(H)$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$. Posons $K \in N_{3,m}$ telle que

$$\begin{aligned} K &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix} H \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} c & d & 0 \\ 0 & 0 & -1 \\ -a & -b & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} d & 0 & -c \\ 0 & 1 & 0 \\ -b & 0 & a \end{pmatrix}. \end{aligned}$$

Donc, puisque $\pi(H)$ est dans le centre de $SL_3(\mathbb{Z})/Q_{3,m}$,

$$\pi(K) = \pi\left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}\right) \pi(H) \pi\left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}\right)^{-1} = \pi(H).$$

Par l'hypothèse de récurrence, on peut donc affirmer que $\pi(H_nK) = \pi(H)^{n+1}$ et que

$$H_nK = \begin{pmatrix} ad & b^n & -ac \\ (-1)^{n+1}c^nd & d_n & (-1)^{n+2}c^{n+1} \\ -b & 0 & a \end{pmatrix}.$$

Soit $L = T_{13}(c)H_nKT_{12}(-b^n)$. Comme b et c sont divisibles par m, par le lemme 3.6, nous savons que $L \in N_{3,m}$ et $\pi(L) = \pi(H)^{n+1}$. De plus, vu que $H \in N_{3,m}$, nous pouvons dire que $\det(H) = 1$, donc $ad - bc = 1$. Nous pouvons dès lors calculer L :

$$\begin{aligned} L &= \begin{pmatrix} 1 & b^n & 0 \\ (-1)^{n+1}c^nd & d_n & (-1)^{n+2}c^{n+1} \\ -b & 0 & a \end{pmatrix} T_{12}(-b^n) \\ &= \begin{pmatrix} 1 & 0 & 0 \\ (-1)^{n+1}c^nd & d_{n+1} & (-1)^{n+2}c^{n+1} \\ -b & b^{n+1} & a \end{pmatrix}, \end{aligned}$$

où $d_{n+1} = d_n + (-1)^n b^n c^n d$.
En se rappelant que b et c sont divisibles par m, nous pouvons poser

$$H_{n+1} = T_{13}(m)^{\frac{b}{m}} T_{23}(m)^{\frac{(-1)^n c^n d}{m}} \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} L \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \in N_{3,m}.$$

Puisque $T_{21}(m) \in Q_{3,m} \lhd SL_3(\mathbb{Z})$ et par les lemmes 3.6 et 3.9, nous avons bien que $\pi(H_{n+1}) = \pi(L) = \pi(H)^{n+1}$. Il reste à montrer que H_{n+1} a la forme désirée :

$$\begin{aligned}
H_{n+1} &= T_{13}(m)^{\frac{b}{m}} T_{23}(m)^{\frac{(-1)^n c^n d}{m}} \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ (-1)^{n+1}c^{n+1} & -d_{n+1} & (-1)^n c^n d \\ -a & -b^{n+1} & b \end{pmatrix} \\
&= T_{13}(m)^{\frac{b}{m}} T_{23}(m)^{\frac{(-1)^n c^n d}{m}} \begin{pmatrix} a & b^{n+1} & -b \\ (-1)^n c^{n+1} & d_{n+1} & (-1)^{n+1} c^n d \\ 0 & 0 & 1 \end{pmatrix} \\
&= T_{13}(m)^{\frac{b}{m}} \begin{pmatrix} a & b^{n+1} & -b \\ (-1)^n c^{n+1} & d_{n+1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a & b^{n+1} & 0 \\ (-1)^n c^{n+1} & d_{n+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Ce qui est bien le résultat voulu.

□

Lemme 3.11. *Soit $H \in N_{3,m}$ telle que*

$$H = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

pour certains $a, b, c, d \in \mathbb{Z}$. Soient $n \in \mathbb{N}_0$ et $\epsilon \in \{-1, 1\}$ tels que $b^n \equiv \epsilon \ (mod\ a)$. Alors $H^n \in Q_{3,m}$.

Démonstration. Soit $H_n \in N_{3,m}$ donnée par le lemme précédant. Il suffit de prouver que $H_n \in Q_{3,m}$. Puisque $a \equiv 1 \ (mod\ m)$, il existe $k \in \mathbb{Z}$ tel que $a = 1 + km$. En utilisant le fait que $b^n \equiv \epsilon \ (mod\ a)$, nous déduisons que

$$-b^n - \epsilon km \equiv -\epsilon(1 + km) \equiv 0 \ (mod\ a).$$

De plus, b est divisible par m. Donc $-b^n - \epsilon km$ l'est aussi. Puisque $a = 1 + km$, a et m sont premiers entre eux. Par conséquent $-b^n - \epsilon km$ est divisible par am. Il existe donc $x \in \mathbb{Z}$ tel que $axm + b^n = -\epsilon km$. De là, posons $K_n \in N_{3,m}$ telle que

$$\begin{aligned}
K_n &= H_n T_{12}(xm) \\
&= \begin{pmatrix} a & b^n & 0 \\ (-1)^{n+1}c^n & d_n & 0 \\ 0 & 0 & 1 \end{pmatrix} T_{12}(xm) \\
&= \begin{pmatrix} a & axm + b^n & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a & -\epsilon km & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

pour certains $c', d' \in \mathbb{Z}$. La thèse est donc équivalente à montrer que $K_n \in Q_{3,m}$. De même, en posant $L_n \in N_{3,m}$ telle que

$$\begin{aligned} L_n &= T_{21}(-\epsilon)K_nT_{21}(\epsilon) \\ &= \begin{pmatrix} a & -\epsilon km & 0 \\ c' - \epsilon a & d'' & 0 \\ 0 & 0 & 1 \end{pmatrix} T_{21}(\epsilon) \\ &= \begin{pmatrix} a - \epsilon^2 km & -\epsilon km & 0 \\ c'' & d'' & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -\epsilon km & 0 \\ c'' & d'' & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

pour certains $c'', d'' \in \mathbb{Z}$, il suffit de prouver que $L_n \in Q_{3,m}$. Or, comme $L_n \in SL_3(\mathbb{Z})$, nous savons que $d'' + \epsilon c''km = 1$. Donc $L_n = T_{21}(c'')T_{12}(-\epsilon km)$, ce qui conclut la preuve puisque c'' est divisible par m.

□

Avant de pouvoir prouver le cas de base de notre récurrence, prouvons d'abord un lemme d'arithmétique :

Lemme 3.12. *Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$ et $(a, b) = 1$. Alors, il existe $a', a'' \in \mathbb{Z}_0$ dans la progression arithmétique $a + tb$ et $n', n'' \in \mathbb{N}_0$ tels que $(n', n'') = 1$, $b^{n'} \equiv \pm 1 \ (mod\ a')$ et $b^{n''} \equiv \pm 1 \ (mod\ a'')$.*

Démonstration. Comme au moins un des deux entiers a et b est impair, nous pouvons distinguer deux cas :

$b \not\equiv 0 \pmod 4$ ou $a \equiv -1 \pmod 4$: Si b est divisible par 4, alors $a \equiv -1 \ (mod\ 4)$. Donc par le théorème de Dirichlet (théorème 1.5), on peut trouver un nombre premier p dans la suite arithmétique $a + tb$ tel que $p \equiv -1 \ (mod\ 4)$.
Par contre, si b n'est pas divisible par 4 :
Si $b \equiv 2 \ (mod\ 4)$ et $a \equiv 1 \ (mod\ 4)$, alors les nombres de la forme $a + b + 4t'b$ sont toujours dans la progression arithmétique $a + tb$. De plus, il sont tous congrus à -1 modulo 4 et $(a+b, 4b) = 1$ car a est impair et $(a, b) = 1$. Donc, par Dirichlet, on peut trouver un nombre premier p dans la suite arithmétique $a+tb$ tel que $p \equiv -1 \ (mod\ 4)$.
Sinon, les nombres de la forme $a+b^2(-1-a)+4t'b$ sont toujours dans la progression arithmétique $a + tb$. De plus, si b est impair, ils sont congrus à $a + (-1 - a) \equiv -1$ modulo 4 car $b^2 \equiv 1 \ (mod\ 4)$. Si b est pair, a est impair et $a \not\equiv 1 \ (mod\ 4)$, donc, $a \equiv -1 \ (mod\ 4)$ et b^2 est divisible par 4. Donc, ils seront tous congrus à -1 modulo 4. Or, $\big(a + b^2(-1 - a), 4b\big) = 1$. Donc, par Dirichlet, il existe un nombre premier p dans la suite arithmétique $a + tb$ tel que $p \equiv -1 \ (mod\ 4)$. Dans tous les cas, un tel nombre premier existe bien.
Puisque p est de la forme $a + tb$ et que $(a, b) = 1$: $(b, p) = 1$. Soit $n \in \mathbb{N}_0$ l'ordre de b modulo p (voir définition 1.6). Dès lors, comme p est premier, $\varphi(p) = p - 1$ et donc $n \mid p - 1$. Soit $p - 1 = 2^e {q_1}^{e_1} \cdots {q_i}^{e_i}$ la factorisation première de $p - 1$. On peut donc dire que $(-p, bq_1 \cdots q_i) = 1$ et $(-1, bq_1 \cdots q_i) = 1$. Toujours par le théorème de Dirichlet, on peut trouver deux nombres premiers distincts r et r' tels que r soit de la forme $-p + tbq_1 \cdots q_i$ et r' de la forme $-1 + tbq_1 \cdots q_i$.

Posons $a' = rr'$. Donc $a' \equiv (-p)(-1) \equiv a \ (mod\ b)$, d'où on déduit que a' est bien dans la suite arithmétique $a+tb$. Soit $n' \in \mathbb{N}_0$ l'ordre de b modulo a'. On a donc bien $b^{n'} \equiv 1 \ (mod\ a')$.
De plus, $n' \mid \varphi(a') = (r-1)(r'-1)$. Or, comme $n \mid p-1$, les seuls diviseurs premiers impairs de n sont les q_k. Si on peut trouver k tel que $q_k \mid n'$, alors : soit $q_k \mid r-1$ donc $q_k \mid p+1$ ce qui est absurde car $q_k \mid p-1$; soit $q_k \mid r'-1$ et donc $q_k \mid 2$, ce qui est aussi absurde. Donc n et n' n'ont pas de facteur impair en commun. Si n est impair, nous avons la thèse en posant $n'' = n$ et $a'' = p$.
Sinon, on pose $n'' = \frac{n}{2}$ et $a'' = p$. Alors, comme $\left(b^{n''}\right)^2 - 1$ est divisible par p, nous avons bien $b^{n''} \equiv \pm 1 \ (mod\ a'')$. De plus, n'' est impair car sinon, $4 \mid n$ et donc $4 \mid p-1$; or $p \equiv -1 \ (mod\ 4)$. Donc $(n'', n') = 1$, ce qui achève le premier cas.

$\mathbf{b \equiv 0 \ (mod\ 4)}$ et $\mathbf{a \equiv 1 \ (mod\ 4)}$: Nous pouvons utiliser le premier cas avec $-a$ et $-b$ pour trouver $-a'$ et $-a''$ de la forme $-a-tb$ et $n', n'' \in \mathbb{N}_0$ tels que $(n', n'') = 1$, $b^{n'} \equiv \pm 1 \ (mod\ -a')$ et $b^{n''} \equiv \pm 1 \ (mod\ -a'')$. Donc $b^{n'} \equiv \pm 1 \ (mod\ a')$ et $b^{n''} \equiv \pm 1 \ (mod\ a'')$, ce qui conclut la démonstration.

□

Prouvons maintenant le cas de base de la récurrence :

Lemme 3.13.

$$Q_{3,m} = N_{3,m}.$$

Démonstration. Nous savons déjà que $Q_{3,m} \subset N_{3,m}$. Prouvons l'inclusion inverse :
Pour ce faire, considérons $H \in N_{3,m}$. Soit H' la matrice donnée par lemme 3.7. Vu que $T_{21}(m) \in Q_{3,m} \lhd SL_3(\mathbb{Z})$, la thèse est équivalente à prouver que $H' \in Q_{3,m}$. De plus, quitte à remplacer H' par $(-P_{13})H'(-P_{13})$ ou par $(-P_{23})H'(-P_{23})$, nous pouvons, sans perte de généralité, supposer que

$$H' = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in N_{3,m},$$

où $a, b, c, d \in \mathbb{Z}$. Quitte à remplacer H' par $T_{12}(m)H'$, nous pouvons aussi supposer que $b \neq 0$. Comme $\det(H') = 1$, $(a, b) = 1$. Soient $a', a'' \in \mathbb{Z}_0$ et $n', n'' \in \mathbb{N}_0$ donnés par le lemme précédant. Posons également $t', t'' \in \mathbb{Z}$ tels que $a' = a + t'b$ et $a'' = a + t''b$. Par ailleurs,

$$\begin{aligned} T_{21}(-t')H'T_{21}(t') &= \begin{pmatrix} a & b & 0 \\ c - at' & d - bt' & 0 \\ 0 & 0 & 1 \end{pmatrix} T_{21}(t') \\ &= \begin{pmatrix} a' & b & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} \in N_{3,m} \end{aligned}$$

pour certains $c', d' \in \mathbb{Z}$. De plus, puisque $b^{n'} \equiv \pm 1 \ (mod\ a')$, nous pouvons utiliser le lemme 3.11 et en déduire que $\left(T_{21}(-t')H'T_{21}(t')\right)^{n'} \in Q_{3,m}$. Donc $T_{21}(-t')H'^{n'}T_{21}(t') \in Q_{3,m}$. Par conséquent, $H'^{n'} \in Q_{3,m}$. De même, $H'^{n''} \in Q_{3,m}$. Or $(n', n'') = 1$. Donc, par Bézout, il existe des entiers x et y tels que $xn' + yn'' = 1$. Donc $H'^{xn'} \in Q_{3,m}$ et $H'^{yn''} \in Q_{3,m}$. Donc $H' = H'^{xn'+yn''} \in Q_{3,m}$.

□

Théorème 3.14. *Soient* $n, m \in \mathbb{N}_0$ *tels que* $n \geq 3$*. Alors,*

$$Q_{n,m} = N_{n,m}.$$

Démonstration. La preuve se fait par récurrence sur n grâce au lemme précédant et à la proposition 3.8.

□

3.2 Théorème de Mennicke

Cette section va avoir pour but de présenter un corollaire du théorème précédent, décrivant les sous-groupes normaux de $SL_n(\mathbb{Z})$. Fixons $n \in \mathbb{N}$ un nombre naturel tel que $n \geq 3$.

Lemme 3.15. *Soit* $A = (a_{ij}) \in SL_n(\mathbb{Z})$ *une matrice telle que* $a_{ij} = \delta_{ij}$ *pour tout* $i, j \in \{1, \ldots, n\}$ *où* $i > 2$*. Alors* $T_{21}(a_{12}) \in \langle\langle A \rangle\rangle$ *et* $T_{21}((a_{12}, 1 - a_{11})) \in \langle\langle A \rangle\rangle$*.*

Démonstration. Puisque les $n-2$ dernières lignes de A sont celles de l'identité, et que $\det(A) = 1$, nous pouvons dire que $a_{11}a_{22} - a_{12}a_{21} = 1$. De plus, si nous posons $A^{-1} = (b_{ij})$, par la méthode des cofacteurs, nous pouvons dire que $b_{11} = a_{22}$, $b_{12} = -a_{12}$, $b_{21} = -a_{21}$, $b_{22} = a_{11}$ et $b_{i1} = b_{i2} = 0$ pour tout $i \in \{3, \ldots, n\}$. Or,

$$\begin{aligned} T_{23}(-1)AT_{23}(1) &= \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} - 1 & a_{24} & \ldots & a_{2n} \\ 0 & 0 & 1 & & & \\ \vdots & \vdots & & \ddots & & \\ 0 & 0 & & & & 1 \end{pmatrix} T_{23}(1) \\ &= \begin{pmatrix} a_{11} & a_{12} & a_{13} + a_{12} & a_{14} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} + a_{22} - 1 & a_{24} & \ldots & a_{2n} \\ 0 & 0 & 1 & & & \\ \vdots & \vdots & & \ddots & & \\ 0 & 0 & & & & 1 \end{pmatrix} \in \langle\langle A \rangle\rangle. \end{aligned}$$

Donc

$$\begin{aligned} A^{-1}T_{23}(-1)AT_{23}(1) &= I + (a_{22}a_{12} - a_{12}(a_{22} - 1))e_{13} + (-a_{21}a_{12} + a_{11}(a_{22} - 1))e_{23} \\ &= I + a_{12}e_{13} + (1 - a_{11})e_{23} \in \langle\langle A \rangle\rangle. \end{aligned}$$

On peut donc en déduire que

$$\begin{aligned} P_{12}P_{23} \begin{pmatrix} 1 & & a_{12} & & \\ & 1 & 1 - a_{11} & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} P_{23}P_{12} &= P_{12} \begin{pmatrix} 1 & a_{12} & & & \\ & 1 & & & \\ & 1 - a_{11} & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} P_{12} \\ &= \begin{pmatrix} 1 & & & & \\ a_{12} & 1 & & & \\ 1 - a_{11} & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \in \langle\langle A \rangle\rangle. \end{aligned}$$

Puisque, si $x, y \in \mathbb{Z}$,

$$T_{23}(-1)\begin{pmatrix} 1 & & & & \\ x & 1 & & & \\ y & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} T_{23}(1) = \begin{pmatrix} 1 & & & & \\ x-y & 1 & & & \\ y & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

et

$$T_{32}(-1)\begin{pmatrix} 1 & & & & \\ x & 1 & & & \\ y & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} T_{32}(1) = \begin{pmatrix} 1 & & & & \\ x & 1 & & & \\ y-x & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

nous pouvons utiliser l'algorithme d'Euclide et en déduire que

$$T_{21}((a_{12}, 1-a_{11})) \in \langle\langle A \rangle\rangle.$$

Nous concluons en remarquant que

$$T_{21}(a_{12}) = T_{21}((a_{12}, 1-a_{11}))^{\frac{a_{12}}{(a_{12}, 1-a_{11})}} \in \langle\langle A \rangle\rangle.$$

□

Regardons ce qui se passe sur une colonne :

Lemme 3.16. *Soit $A = (a_{ij}) \in SL_n(\mathbb{Z})$ telle qu'il existe $k \in \{2, \dots, n\}$ tel que $a_{k1} \neq 0$. Posons $d = (a_{i1}, i \in \{2, \dots, n\})$. Alors $T_{21}(d) \in \langle\langle A \rangle\rangle$ et, pour tout $i \in \{2, \dots, n\}$, $T_{21}(a_{i1}) \in \langle\langle A \rangle\rangle$.*

Démonstration. Soit $B = (b_{ij}) \in \langle\langle A \rangle\rangle$ donnée par le lemme 3.5. Donc $b_{21} = d$ et $b_{i1} = 0$ pour tout $i \in \{3, \dots, n\}$. Notons $B^{-1} = (c_{ij})$. Pour tout $r \in \{2, \dots, n\}$, nous pouvons dire que

$$\begin{aligned} T_{1r}(1)BT_{1r}(-1)B^{-1} &= \begin{pmatrix} b_{11}+b_{r1} & \dots & b_{1r}+b_{rr} & \dots & b_{1n}+b_{rn} \\ d & \dots & b_{2r} & \dots & b_{2n} \\ 0 & \dots & b_{3r} & \dots & b_{3n} \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & b_{nr} & \dots & b_{nn} \end{pmatrix} T_{1r}(-1)B^{-1} \\ &= \begin{pmatrix} b_{11}+b_{r1} & \dots & b_{1r}+b_{rr}-b_{11}-b_{r1} & \dots & b_{1n}+b_{rn} \\ d & \dots & b_{2r}-d & \dots & b_{2n} \\ 0 & \dots & b_{3r} & \dots & b_{3n} \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & b_{nr} & \dots & b_{nn} \end{pmatrix} B^{-1} \\ &\in \langle\langle A \rangle\rangle. \end{aligned}$$

Soit Q_r cette matrice. Les $n-2$ dernières lignes de Q_r sont celles de l'identité. De plus, l'élément en position $(2,1)$ est $-dc_{r1}$ et celui en $(2,2)$ est $1-dc_{r2}$. En transformant cette matrice par $(-P_{12})Q_r(-P_{12})$ si $n=3$ et par $P_{n-1,n}P_{12}Q_rP_{12}P_{n-1,n}$ si $n>3$, nous obtenons

une matrice $Q = (q_{ij}) \in \langle\langle A \rangle\rangle$ telle que $q_{11} = 1 - dc_{r2}$, $q_{12} = -dc_{r1}$ et $q_{ij} = \delta_{ij}$ si $i, j \in \{1, \dots, n\}$ et si $i > 2$. Donc, par le lemme précédant, $T_{21}(d(c_{r1}, c_{r2})) \in \langle\langle Q \rangle\rangle \subset \langle\langle A \rangle\rangle$ pour tout $r \in \{2, \dots, n\}$. Supposons qu'il existe un nombre premier p tel que p divise c_{r1} et c_{r2} pour tout $r \in \{2, \dots, n\}$. Alors, il ne divise ni c_{11} ni c_{12}, sinon il diviserait $\det(B^{-1}) = 1$. De plus, puisque $\sum_{i=1}^{n} b_{1i}c_{i2} = 0$, p divise b_{11} et puisque $\sum_{i=1}^{n} b_{2i}c_{i1} = 0$, p divise b_{21}. Donc, comme $b_{i1} = 0$ pour tout $i \in \{3, \dots, n\}$, p divise $\det(B)$, ce qui est absurde. Donc $(c_{r1}, c_{r2}, r \in \{2, \dots, n\}) = 1$. Par Bézout, on peut trouver $k_2, \dots, k_n \in \mathbb{Z}$ tels que $\sum_{r=2}^{n} k_r d(c_{r1}, c_{r2}) = d$. Donc

$$\prod_{r=2}^{n} T_{21}(d(c_{r1}, c_{r2}))^{k_r} = T_{21}(d) \in \langle\langle A \rangle\rangle.$$

De plus, si $i \in \{2, \dots, n\}$,

$$T_{21}(d)^{\frac{a_{i1}}{d}} = T_{21}(a_{i1}) \in \langle\langle A \rangle\rangle.$$

□

Dans la suite de cette section, fixons N, un sous-groupe normal de $SL_n(\mathbb{Z})$ différent de $\{I\}$ et de $\{\pm I\}$.

Définition 3.6. *Soit $A = (a_{ij}) \in N$ tel que $A \neq \pm I$. Nous noterons*

$$\boldsymbol{\mu}(\mathbf{A}) := (a_{ij},\ a_{ii} - a_{jj};\ i, j \in \{1, \dots, n\}, i \neq j) \in \mathbb{N}_0. \tag{3.8}$$

Remarquons que ce p.g.c.d. est bien défini puisque nous avons évité les cas où A était un multiple de l'identité.

Exemple 3.2. Si

$$A = \begin{pmatrix} -5 & -6 & -3 \\ 3 & -2 & -6 \\ 3 & 3 & 1 \end{pmatrix} \in N,$$

alors

$$\mu(A) = (\underbrace{-6, -3, 3, -6, 3, 3}_{a_{ij}}, \underbrace{-3, -6, -3}_{a_{ii}-a_{jj}}) = 3.$$

Définition 3.7. *Notons* $\boldsymbol{m(N)} \in \mathbb{N}_0$ *le naturel défini par*

$$m(N) := (\mu(A), A \in N \setminus \{\pm I\}). \tag{3.9}$$

Nous remarquerons que, là aussi, le p.g.c.d. est bien défini vu que N est différent de $\{I\}$ et de $\{\pm I\}$.

Lemme 3.17. *Soit $A = (a_{ij}) \in N$ tel que $A \neq \pm I$. Alors $T_{21}(\mu(A)) \in \langle\langle A \rangle\rangle$.*

Démonstration. Soit $r \in \{1, \dots, n\}$. S'il existe $k_r \in \{1, \dots, n\} \setminus \{r\}$ avec $a_{k_r r} \neq 0$, définissons $d_r = (a_{ir}, i \in \{1, \dots, n\}, i \neq r)$. Sinon, posons $d_r = 0$. Par lemme 3.16, $T_{21}(d_1) \in \langle\langle A \rangle\rangle$. De même, si $r \in \{2, \dots, n\}$, posons $P = (-P_{1r})A(-P_{1r})$ si $n = 3$ et $P = P_{ij}P_{1r}AP_{1r}P_{ij}$ si $n > 3$ où $i, j \in \{2, \dots, n\} \setminus \{r\}$ sont des indices distincts quelconques. Dans les deux cas, $P \in \langle\langle A \rangle\rangle$ et les éléments non-diagonaux de la première colonne de P sont les éléments non diagonaux de la r^{e} colonne de A. Donc, par le lemme 3.16, $T_{21}(d_r) \in \langle\langle P \rangle\rangle \subset \langle\langle A \rangle\rangle$ pour tout $r \in \{1, \dots, n\}$ et $T_{21}(a_{ij}) \in \langle\langle A \rangle\rangle$ pour tout $i, j \in \{1, \dots, n\}$ où $i \neq j$.

Soient $i, j \in \{1, \dots, n\}$ tels que $i \neq j$ et $a_{ii} \neq a_{jj}$. Posons

$$B = (b_{kl}) = T_{ij}(1)AT_{ij}(-1) \in \langle\langle A \rangle\rangle.$$

Nous savons que $b_{ij} = a_{ij} + a_{jj} - (a_{ii} + a_{ji})$. Quitte à remplacer B par $P_{kj}P_{j1}BP_{j1}P_{kj}$ où $k \in \{2, \dots, n\} \setminus \{j\}$, nous pouvons supposer que $a_{ij} + a_{jj} - (a_{ii} + a_{ji})$ est un élément non-diagonal de la première colonne de B. Par lemme 3.16, $T_{21}(a_{ij} + a_{jj} - a_{ii} - a_{ji}) \in \langle\langle A \rangle\rangle$. Donc,

$$\begin{aligned} T_{21}(a_{ij} + a_{jj} - a_{ii} - a_{ji})T_{21}(a_{ji})T_{21}(-a_{ij}) &= T_{21}(a_{ij} + a_{jj} - a_{ii})T_{21}(-a_{ij}) \\ &= T_{21}(a_{jj} - a_{ii}) \in \langle\langle A \rangle\rangle. \end{aligned}$$

Or, comme $\mu(A) = (d_r, a_{jj} - a_{ii};\ r, i, j \in \{1, \dots, n\}, i \neq j)$, par Bézout, il existe des entiers $k_r, k_{ij} \in \mathbb{Z}$ pour $r, i, j \in \{1, \dots, n\}, i \neq j$ tels que

$$\mu(A) = \sum_{r=1}^{n} k_r d_r + \sum_{\substack{i,j=1 \\ i \neq j}}^{n} k_{ij}(a_{jj} - a_{jj}).$$

Par conséquent,

$$T_{21}(\mu(A)) = \prod_{r=1}^{n} T_{21}(d_r)^{k_r} \cdot \prod_{\substack{i,j=1 \\ i \neq j}}^{n} T_{21}(a_{jj} - a_{ii})^{k_{ij}} \in \langle\langle A \rangle\rangle.$$

□

Proposition 3.18. *Si $N \lhd SL_n(\mathbb{Z})$ est tel que $N \neq \{I\}$ et $N \neq \{\pm I\}$, alors $Q_{n,m(N)} \subset N$.*

Démonstration. Nous devons prouver que $T_{21}(m(N)) \in N$. Par définition de $m(N)$ et par Bézout, nous pouvons dire qu'il existe $t \in \mathbb{N}_0$, $A_1, \dots A_t \in N \setminus \{\pm I\}$ et $k_1, \dots k_t \in \mathbb{Z}$ tels que

$$m(N) = \sum_{i=1}^{t} k_i \mu(A_i).$$

Or, par le lemme précédant, $T_{21}(\mu(A_i)) \in \langle\langle A_i \rangle\rangle \subset N$ pour tout $i \in \{1, \dots, t\}$. Donc

$$T_{21}(m(N)) = \prod_{i=1}^{t} T_{21}(\mu(A_i))^{k_i} \in N.$$

□

Nous pouvons en déduire un théorème sur les sous-groupes normaux de $SL_n(\mathbb{Z})$, dû à Mennicke :

Théorème 3.19 (Mennicke)**.** *Soient $n \in \mathbb{N}_0$ et $N \lhd SL_n(\mathbb{Z})$ tels que $n \geq 3$, $N \neq \{I\}$ et $N \neq \{\pm I\}$. Alors, il existe $m \in \mathbb{N}_0$ tel que $N_{n,m} \subset N$.*

Démonstration. Suit immédiatement de la proposition précédente et du théorème 3.14.

□

Ce théorème nous dit que si $n \geq 3$, tout groupe non trivial de $SL_n(\mathbb{Z})$ contient un sous-groupe de congruence.

Corollaire 3.20. *Soient $n \in \mathbb{N}_0$ et $N \lhd SL_n(\mathbb{Z})$ tels que $n \geq 3$, $N \neq \{I\}$ et $N \neq \{\pm I\}$. Alors $|SL_n(\mathbb{Z})/N| < +\infty$.*

Démonstration. Soit $m \in \mathbb{N}_0$ donné par le théorème de Mennicke. Comme $N_{n,m} \lhd SL_n(\mathbb{Z})$, nous pouvons dire que $N_{n,m} \lhd N$. Donc, par le Troisième Théorème d'isomorphisme (théorème 1.7), $SL_n(\mathbb{Z})/N \simeq \frac{SL_n(\mathbb{Z})/N_{n,m}}{N/N_{n,m}}$. Il suffit donc de prouver que $|SL_n(\mathbb{Z})/N_{n,m}| < +\infty$. Pour ce faire, remarquons que si $A, B \in SL_n(\mathbb{Z})$ sont telles que $A \equiv B \ (mod\ m)$, alors $AB^{-1} \equiv I \ (mod\ m)$ et donc $AN_{n,m} = BN_{n,m}$. Il n'y a donc que m valeurs possibles pour les entrées des matrices de $SL_n(\mathbb{Z})/N_{n,m}$. Il y a donc au plus m^{n^2} éléments dans $SL_n(\mathbb{Z})/N_{n,m}$.

□

3.3 Le cas $n = 2$

Le but de cette dernière section est de montrer que le théorème de Mennicke n'est plus valide dans le cas $n = 2$. La démonstration reposera sur un théorème de Poincaré qui sera donné sans preuve.

Proposition 3.21. *Le groupe des matrices inversibles* 2×2 *sur* $\mathbb{Z}$, $GL_2(\mathbb{Z})$, *peut être caractérisé de la façon suivante :*

$$GL_2(\mathbb{Z}) = \left\{A \in \mathbb{Z}^{2\times 2} \mid |\det(A)| = 1\right\}. \tag{3.10}$$

Démonstration. Si $A \in GL_2(\mathbb{Z})$, alors $\det(A)\det(A^{-1}) = 1$. Donc $\det(A)$ est inversible dans $\mathbb{Z}$. Les seuls inversibles dans $\mathbb{Z}$ étant 1 et -1, nous pouvons dire que $|\det(A)| = 1$. Nous avons donc bien l'inclusion $GL_2(\mathbb{Z}) \subset \left\{A \in \mathbb{Z}^{2\times 2} \mid |\det(A)| = 1\right\}$.

L'autre inclusion est due au fait que 1 et -1 sont inversibles dans $\mathbb{Z}$. On peut donc construire l'inverse des éléments de $\left\{A \in \mathbb{Z}^{2\times 2} \mid |\det(A)| = 1\right\}$ par la méthode des cofacteurs.

□

Proposition 3.22. *Le centre de* $GL_2(\mathbb{Z})$ *est donné par*

$$Z(GL_2(\mathbb{Z})) = \{\pm I\}. \tag{3.11}$$

Démonstration. L'inclusion $\{\pm I\} \subset Z(GL_2(\mathbb{Z}))$ est évidente. Dans l'autre sens, soit $A = (a_{ij}) \in Z(GL_2(\mathbb{Z}))$. Puisque $AT_{12}(1) = T_{12}(1)A$, nous pouvons dire que $A(I + e_{12}) = (I + e_{12})A$. Dès lors, $Ae_{12} = e_{12}A$, ce qui donne

$$\begin{pmatrix} 0 & a_{11} \\ 0 & a_{21} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} \\ 0 & 0 \end{pmatrix}.$$

Par conséquent, $a_{11} = a_{22}$ et $a_{21} = 0$. De manière symétrique, nous pouvons prouver que $a_{12} = 0$. Nous voyons donc que $A = a_{11}I$. Dès lors, puisque par la proposition précédente, $\det(A) = \pm 1$, nous pouvons dire que $A \in \{\pm I\}$.

□

Le centre d'un groupe étant toujours un sous-groupe normal, la définition suivante est légitime.

Définition 3.8. *Le* ***groupe projectif général linéaire*** *de dimension* 2 *sur* $\mathbb{Z}$ *est le quotient*

$$PGL_2(\mathbb{Z}) := GL_2(\mathbb{Z})/Z(GL_2(\mathbb{Z})). \tag{3.12}$$

Pour la suite, définissons trois éléments particuliers de $PGL_2(\mathbb{Z})$:

$$r = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \{\pm I\},\ s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \{\pm I\},\ t = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \{\pm I\}. \tag{3.13}$$

Remarquons que ces trois éléments sont d'ordre 2 puisque $r^2 = s^2 = t^2 = \{\pm I\}$. De plus, l'ordre de rs est aussi 2. En effet,

$$rs = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \{\pm I\},\ (rs)^2 = \{\pm I\}.$$

Enfin, l'ordre de st est 3, puisque

$$st = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \{\pm I\},\ (st)^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \{\pm I\},\ (st)^3 = \{\pm I\}.$$

Lemme 3.23. *Les éléments r, s, t engendrent $PGL_2(\mathbb{Z})$.*

Démonstration. Remarquons d'abord que

$$tr = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \{\pm I\} \in \langle r, s, t \rangle.$$

De plus,

$$strs = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \{\pm I\} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \{\pm I\} \in \langle r, s, t \rangle.$$

Donc, par la proposition 3.4, $PSL_2(\mathbb{Z}) \subset \langle r, s, t \rangle$. Or, par la proposition 3.21 et le Troisième Théorème d'isomorphisme,

$$|PGL_2(\mathbb{Z})/PSL_2(\mathbb{Z})| = |GL_2(\mathbb{Z})/SL_2(\mathbb{Z})| = 2.$$

Dès lors, $\langle r, s, t \rangle = PSL_2(\mathbb{Z})$ ou $\langle r, s, t \rangle = PGL_2(\mathbb{Z})$. Pour conclure, il suffit de remarquer que $r \notin PSL_2(\mathbb{Z})$ et donc que $\langle r, s, t \rangle = PGL_2(\mathbb{Z})$.

□

Énonçons maintenant un théorème de Poincaré, sans donner de preuve.

Théorème 3.24 (Poincaré)**.** *Le groupe $PGL_2(\mathbb{Z})$ est "universel parmi les groupes engendrés par trois éléments a, b, c tels que $a^2 = b^2 = c^2 = 1$ et tels que les ordres de ab et de bc sont respectivement 2 et 3".*

C'est-à-dire, pour tout groupe H contenant $a, b, c \in H$ respectant les propriétés citées ci-dessus, il existe un et un seul morphisme de groupe

$$\alpha : PGL_2(\mathbb{Z}) \to H$$

tel que $\alpha(r) = a$, $\alpha(s) = b$ et $\alpha(t) = c$.

Démonstration. Voir [4], section IV.F.

□

Dans $Isom(\mathbb{R}^2)$, le groupe des isométries de $\mathbb{R}^2$, considérons trois éléments particuliers. Soient $a, b, c \in Isom(\mathbb{R}^2)$ les symétries orthogonales d'axes $y = 0$, $x = 1$ et $y = \tan(\frac{\pi}{6})x$ respectivement. Il évident que $a^2 = b^2 = c^2 = 1$.

De plus, nous savons que la composée de deux symétries orthogonales d'axes non parallèles, est une rotation dont le centre est le point d'intersection des axes et d'angle égal au double de l'angle formé par ces axes.

ab est donc une rotation de centre $(1,0)$ et d'angle π, bc est une rotation de centre $(1, \tan(\frac{\pi}{6}))$ et d'angle $-\frac{2\pi}{3}$ et ca est une rotation de centre $(0,0)$ et d'angle $\frac{-\pi}{3}$. Les ordres de ab, bc et ca sont donc respectivement 2, 3 et 6.

Soient $H = \langle a, b, c\rangle$ et $\alpha : PGL_2(\mathbb{Z}) \to H$ le morphisme donné par le théorème de Poincaré. Posons également $\beta : PSL_2(\mathbb{Z}) \to H$, la restriction de α à $PSL_2(\mathbb{Z})$.

Lemme 3.25.

$$|PSL_2(\mathbb{Z})/\operatorname{Ker}(\beta)| = +\infty. \tag{3.14}$$

Démonstration. Puisque $rs, tr \in PSL_2(\mathbb{Z})$, les rotations ab et ca appartiennent à $\operatorname{Im}(\beta)$. De plus, ab est une symétrie centrale de centre $(1,0)$ et $(ca)^3$ est une symétrie centrale de centre $(0,0)$. Donc, si $(x,y) \in \mathbb{R}^2$,

$$\left[(ab)(ca)^3\right](x,y) = (ab)(-x,-y) = (x+2, y).$$

Soit $g = (ab)(ca)^3 \in \operatorname{Im}(\beta)$. Nous pouvons donc dire que g est une translation de vecteur $(2,0)$. Dès lors, $g^n \in \operatorname{Im}(\beta)$ est une translation de vecteur $(2n,0)$, pour tout $n \in \mathbb{N}_0$. Ceci implique que $|\operatorname{Im}(\beta)| = +\infty$. Or, β engendre un isomorphisme tel que $PSL_2(\mathbb{Z})/\operatorname{Ker}(\beta) \simeq \operatorname{Im}(\beta)$, ce qui conclut la preuve.

□

Lemme 3.26.

$$\operatorname{Ker}(\beta) \neq \{\{\pm I\}\}. \tag{3.15}$$

Démonstration. Comme $\beta(tr) = ca$ et que ca est d'ordre 6, nous savons que $(tr)^6 \in \operatorname{Ker}(\beta)$. Pour conclure la preuve, il suffit alors de remarquer que

$$(tr)^6 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}\{\pm I\},$$

puisque $tr = T_{12}(1)\{\pm I\}$.

□

Nous sommes maintenant prêts à montrer que le théorème de Mennicke n'est pas valide pour les matrices 2×2.

Proposition 3.27. *Il existe* $N \lhd SL_2(\mathbb{Z})$ *tel que* $N \neq \{I\}$, $N \neq \{\pm I\}$ *et*

$$|SL_2(\mathbb{Z})/N| = +\infty. \tag{3.16}$$

Démonstration. Soit

$$N = \{A \in SL_2(\mathbb{Z}) \mid A\{\pm I\} \in \operatorname{Ker}(\beta)\}.$$

Puisque $\operatorname{Ker}(\beta)$ est un sous-groupe normal de $PSL_2(\mathbb{Z})$, il est trivial de vérifier que $N \lhd SL_2(\mathbb{Z})$. De plus, puisque $\operatorname{Ker}(\beta) \neq \{\{\pm I\}\}$, nous pouvons dire que $\{\pm I\} \subsetneqq N$. Enfin, par le Troisième Théorème d'isomorphisme,

$$SL_2(\mathbb{Z})/N \simeq \frac{SL_2(\mathbb{Z})/\{\pm I\}}{N/\{\pm I\}} = PSL_2(\mathbb{Z})/\operatorname{Ker}(\beta).$$

Donc, puisque, par le lemme 3.25, $|PSL_2(\mathbb{Z})/\operatorname{Ker}(\beta)| = +\infty$, nous pouvons en conclure que $|SL_2(\mathbb{Z})/N| = +\infty$.

□

Bibliographie

[1] J. L. Brenner. *The Linear Homogeneous Group, III.* Annals of Mathematics **71** (1960), 210–222.

[2] Marino Gran. Algèbre multilinéaire et théorie des groupes. Syllabus MAT1231, Université catholique de Louvain, 2009-2010.

[3] Nathan Jacobson. Basic Algebra I. San Francisco : W H Freeman and Company, 1974.

[4] Bernard Maskit. *Kleinian groups.* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **287** (1988), Springer-Verlag, Berlin.

[5] Jens L. Mennicke. *Finite Factor Groups of the Unimodular Group.* Mathematisches Institut An Der Technischen Hochschule, Braunschweig (1964), 31–37.