Groupes linéaires définissables dans les corps p-adiques

Benjamin Druart

UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Mathématiques**

Arrêté ministérial : 7 août 2006

Présentée par

Benjamin Druart

Thèse dirigée par **Eric Jaligot, Tuna Altinel et Gérard Besson**

préparée au sein de **l'Institut Fourier**
et de **l'Ecole Doctorale MSTII**

Groupes linéaires définissables dans les corps p-adiques

Thèse soutenue publiquement le **29 juin 2015**,
devant le jury composé de :

Monsieur Tuna Altinel
Maître de Conférence, Université Claude Bernard - Lyon 1, Directeur de thèse
Madame Zoé Chatzidakis
Directrice de recherche, CNRS - Ecole Normale Supérieure Paris, Présidente
Monsieur Raf Cluckers
Chargé de Recherche, CNRS - Université de Lille 1, Rapporteur
Madame Françoise Delon
Directrice de Recherche, CNRS - Université Paris Diderot - Paris 7, Examinatrice
Monsieur Dugald Macpherson
Professor, University of Leeds, Rapporteur
Monsieur Frank Wagner
Professeur, Université Claude Bernard - Lyon 1, Examinateur

Mais quoi ! penseur, tu vas remettre en équilibre
Au fond de ton esprit, qu'occupaient d'autres soins,
L'idée avec le mot, le plus avec le moins !

[...]

Oui, je travaille, amis ! oui, j'écris, oui, je pense !
L'apaisement superbe étant la récompense
De l'homme qui, saignant, et calme néanmoins,
Tâche de songer plus afin de souffrir moins.

Victor Hugo [20]

à Eric Jaligot

Remerciements

... Malgré tout cauchemars et blessures
Les séparations les deuils les camouflets
Et tout ce qu'on voulait pourtant ce qu'on voulait
De toute sa croyance imbécile à l'azur.

Malgré tout je vous dis que cette vie fut telle
Qu'à qui voudra m'entendre à qui je parle ici
N'ayant plus sur la lèvre un seul mot que merci
Je dirai malgré tout que cette vie fut belle.

Louis Aragon [1]

Ce que Louis Aragon dit au sujet de sa vie, je peux le reprendre à mon compte pour cette thèse. On commence souvent une thèse plein d'enthousiasme et d"illusions. Au fil du temps, les échecs, les désillusions, les deuils s'accumulent et nous touchent. Certains sont liés à la recherche en mathématiques en elle-même – un travail de recherche n'est jamais un long fleuve tranquille – d'autres relèvent de la vie tout simplement. Mais quand je regarde ces quatre ans de travail, je ne peux m'empêcher d'en retenir tout le positif. Je me rends compte alors que cette thèse est jalonnée de rencontres, de personnes qui ont grandement contribué à son achévement. Il est important de leur dire merci.

Je voudrais en premier lieu remercier celui sans qui cette thèse n'aurait jamais commencé, et qui malheureusement n'est plus là pour voir son achévement. Eric Jaligot était un directeur de thèse calme et patient, il a su me montrer un aperçu enthousiaste de la recherche en mathématiques et de toute sa richesse. Sa disparition laissera en moi un sentiment d'inachevé.

Je remercie sincèrement Tuna Altinel d'avoir accepté de reprendre la direction de cette thèse. Travailler avec lui a été pour moi un vrai plaisir. Avec sa patience et son calme il a su accueillir mes idées (parfois hésitantes et imprécises), il a pu également par sa grande connaissance des mathématiques me guider pour les mener à terme. Je le remercie pour sa grande disponibilité, ses encouragements incessants et pour m'avoir parfois secoué un peu pour me mettre au travail.

Je remercie également Gérard Besson d'avoir accepté d'être mon directeur de thèse et de m'avoir aidé dans les démarches administratives.

Je souhaite remercier chaleureusement Zoé Chatzidakis d'avoir accompagné mes premiers pas dans le monde de la recherche lors de mon stage de master 2. Après, elle

a été d'une grande bienveillance sur la suite de mon parcours. Elle a accepté d'être membre de mon jury.

Je suis très reconnaissant à Raf Cluckers et Dugald Macpherson de l'intérêt qu'il ont porté à mon travail et d'avoir accepter d'en être les rapporteurs. J'ai apprécié les commentaires et les corrections qu'ils ont donnés sur cette thèse. J'ai également aimé nos discussions lors de mes passages respectivement à Lille et à Leeds.

Je remercie maintenant Françoise Delon et Frank Wagner d'avoir bien voulu faire partie du jury de cette thèse. Leur présence m'honore.

Lors de ces quatre années de thèse, j'ai pu échanger avec divers mathématiciens. Merci à Clément Lasserre pour ces deux années passées à Grenoble et pour avoir participer à cette présence de la logique à l'Institut Fourier. Je remercie également Anand Pillay, même si notre collaboration ne s'est jamais concrétisée. Dernièrement, j'ai eu la chance de travailler avec Olivier Frécon et son étudiant Vincent Carro. Je les remercie pour leur accueil à Poitiers.

Je souhaite remercier toute l'équipe de logique de Lyon pour m'avoir accueilli : Itaï Ben Yaacov, Thomas Blossier, Amador Martin-Pizzaro, Julien Melleray, Pierre Simon, Lionel Nguyen van Thé, Rizos Sklinos et particulièrement les doctorants pour nos échanges informels sur les mathématiques ou sur d'autres sujets : Juan Felipe Carmona González, Haydar Göral, Nadja Hempel, Tomas Ibarlucía, Simon Iosti, Adriane Kaïchouch et Jean-Cyrille Massicot.

Merci à Elisabeth Mironescu de m'avoir accueilli à l'Institut Camille Jordan (ICJ) et de faire en sorte que je m'y sente bien. Je remercie les équipes administratives de l'Institut Fourier et de l'ICJ pour leur aide dans les différentes démarches : Nathalie, Christine, Géraldine, Fanny, Lindsay, Francesca, Aurélie, Houda, Nabila, Maria, Laurent ...

Je tiens aussi à remercier mes compagnons de doctorat. Un grand merci particulièrement à Samy avec qui j'ai beaucoup échangé sur nos expériences respectives de la thèse. Elle était là dans les bons comme dans les mauvais moments. Je remercie les doctorants en théorie des modèles de Paris et d'ailleurs, comparses de nombreuses conférences : Luis, Silvain, Romain, Pablo, Quentin, Nathalie, Gabriel. J'ai également gardé de très bons rapports avec les étudiants du master LMFI ; merci à ceux qui m'ont accueilli à Lyon pour tous les bons moments passés dans cette ville : Sébastien, Nicolas, Nadja puis Romain ; merci à ceux qui sont restés à Paris et que j'ai pu retrouvé autour de quelques bières : Rafa, Shahin, Benoît, Catherine, Armen, Jean-Philippe. Merci à mes co-bureaux qui m'ont supporté au quotidien et qui ont su maintenir une bonne ambiance de travail et de détente dans le bureau, à Grenoble : Julien et Gang, à Lyon : Matthias, Corentin (merci d'avoir eu l'idée du "gâteau du vendredi"), Alexis, JB, Alain, Lin, Hasan, Maxime, Zeya, et Hugo. Je remercie tous les autres doctorants qui ont fait du labo (à Grenoble ou à Lyon) un lieu où il fait bon vivre : Ivan, Bérénice, Simon, Cécilia, Evrard, Xavier, Ruddy, Coline, Maxime, Thibault, Pedro, Teddy, Federico, Guillaume, Boulos et Charlotte.

Je remercie aussi l'ensemble de mes professeurs de mathématiques de mon parcours scolaire et unversitaire. Ils ont su me transmettre le goût des mathématiques et l'enthousiasme pour la recherche.

Enfin, je souhaite remercier tous mes amis et tous mes proches qui m'ont soutenu

et supporté durant ces quatre ans. Par vos encouragements, vos plaisanteries ... vous avez aussi contribué à l'achévement de cette thèse. Je ne les citerai pas car ils sont trop nombreux et j'ai peur d'en oublier.

Je remercie ma famille pour son soutien. Particulièrement mes parents pour m'avoir toujours laissé une grande liberté dans mes choix.

Table des matières

Introduction

Les nombres p-adiques ont été inventés dans les années 1900 par le mathématicien allemand K. Hensel. Le but initial est de répondre à des questions de théorie des nombres. Très vite, ils apparaissent comme un objet mathématique à part entière, ils donnent un cadre d'étude à la fois naturel et complètement différent des nombres réels. C'est tout naturellement que la théorie des modèles s'est penchée sur eux. Bien que les propriétés algébriques et topologiques des corps p-adiques sont très différentes de celles du corps des nombres réels, elle a pu observer des similitudes, ce sont notamment toutes les deux des structures NIP.

On peut estimer le début des études modèles-théoriques spécifiques sur les corps p-adiques dans les années 70, avec le résultat d'A. Macintyre sur l'élimination des quantificateurs dans ces derniers [25]. Un travail important a été fait par A. Prestel et P. Roquette pour expliciter l'axiomatisation des corps p-adiquement clos [37]. Par la suite, beaucoup de travaux ont été fait en s'inspirant du modèle du corps des nombres réels et de sa généralisation en structure o-minimales. Ainsi Denef montre l'existence d'une décomposition cellulaire pour les ensembles définissables dans les corps p-adiques [11], comme il en existe une dans les structures o-minimales. F. Delon montre que les ensembles définissables à paramètres extérieurs sont définissables à paramètres intérieurs [10], résultat déjà connu pour les réels. Dans les années 88-89, les travaux de L. van den Dries et P. Scowcroft établissent l'existence d'une dimension dans ces corps [46] et [44]. L'étude modèle-théorique des corps p-adiques est encore très actuelle comme en témoigne le résultat récent [19] sur l'élimination des imaginaires dans de tels corps.

En 1997, D. Haskell et D. Macpherson [17] introduisent la notion de p-minimalité sur le modèle de la o-minimalité dans le cas réel. Le but est de décrire les enrichissements de $\mathbb{Q}_p$ tels que les ensembles définissables restent "semblables" à des ensembles semi-algébriques. Le principal exemple connu à ce jour est $\mathbb{Q}_p^{an}$ [45] où on rajoute toutes les fonctions analytiques restreintes au langage habituel des corps $\mathcal{L}_R = \{+, -, \cdot, 0, 1\}$. R. Cluckers a beaucoup travaillé sur les structures analytiques notamment en trouvant une décomposition cellulaire pour les ensembles définissables de $\mathbb{Q}_p^{an}$ [9]. Trouver une décomposition cellulaire pour les structures p-minimales en général est une question encore très actuelle.

Notre étude sur les groupes définissables dans les corps p-adiques s'inscrit dans cette lignée, afin de comprendre ce qui est transposable du cas réel au cas p-adique. Nous avons choisi de regarder les sous-groupes de Cartan dans de tels groupes.

Dans toute étude sur les groupes de matrices, les éléments diagonalisables jouent

un rôle capital. De plus quelque soit les contextes (algébriques, topologiques ...) les éléments semi-simples (c'est à dire diagonalisables dans une extension du corps) sont "génériques" : par exemple, leur ensemble est dense dans $GL_n(\mathbb{R})$ pour la topologie usuelle ; il est de dimension maximal dans $GL_n(\mathbb{C})$... La notion de sous-groupes de Cartan sert à décrire abstraitement (c'est-à-dire en dehors du contexte linéaire) des groupes d'éléments semi-simples.

Les sous-groupes de Cartan jouent un rôle important pour les groupes de rang de Morley fini. Ils ont été très étudiés par E. Jaligot et O. Frécon : ils ont montré que tout groupe de rang de Morley fini possède un sous-groupe de Cartan [15], de plus, s'ils existent, les sous-groupes de Cartan généreux sont tous conjugués entre eux [22]. Dans [14], O. Frécon démontre, dans le cas des groupes de rang de Morley fini minimaux et simples, l'existence et la conjugaison de tous les sous-groupes de Cartan.

En 2011, E. Baro, E. Jaligot et M. Otero [2] ont généralisé ces résultats aux groupes définissables dans les structures o-minimales. Ils ont montré l'existence et la définissabilité des sous-groupes de Cartan. De plus, il n'y a qu'un nombre fini de classe de conjugaison de sous-groupe de Cartan et seule l'une d'entre elles est généreuse.

Le but initial aurait pu être de généraliser ces résultats aux corps p-adiques. Toutefois, dans le cas o-minimal, les groupes définissables et la dimension jouissent de propriétés fortes. Ainsi si $H \leq G$ sont des groupes définissables et si $\dim H = \dim G$ alors H est d'indice fini dans G [30]. Il existe une condition de chaine descendante, assurant ainsi l'existence d'une composante connexe définissable G° d'indice fini dans G pour tout groupe définissable G. De plus, une pseudo élimination des imaginaires pour les sous-groupes est présente : si $H \trianglelefteq G$ sont des sous-groupes définissables, alors G/H est un ensemble définissable.

Ces propriétés, fondamentales dans [2], sont fausses en général pour des groupes définissables dans les corps p-adiques. Le contexte n'étant pas propice pour le moment, à une étude systématique des groupes définissables dans les corps p-adiquement clos, nous nous sommes restreint aux groupes linéaires définissables, afin de comprendre les spécificités des groupes dans le contexte p-adique. Nous avons alors à notre disposition des outils sur les groupes algébriques linéaires et la notion importante de dimension développée par L. van den Dries.

Peu de travaux ont été menés sur les groupes définissables dans les corps p-adiques. On peut citer les travaux de Pillay [33] et [34]. Dans [33], il obtient un résultat sur les sous-groupes engendrés par une famille d'ensembles irréductibles, décrivant ainsi un résultat à la Zilber sur les indécomposable dans les groupes de rang de Morley fini. Dans [34], il établit une structure de groupes analytiques sur les groupes définissables dans $\mathbb{Q}_p$ afin de démontrer que tout corps définissable dans $\mathbb{Q}_p$ est une extension fini de ce dernier. On peut également citer le lemme 3.2 décrivant tous les sous-groupes-définissables de $\mathbb{Q}_p^+$.

Etudier les sous-groupes de Cartan dans les groupes linéaires revient naturellement à regarder les tores. Un tore est un groupe commutatif linéaire ne contenant que des éléments semi-simples. Ils ont été très étudiés du point de vue des groupes algébriques. Intuitivement, on peut résumer les choses ainsi : si T est un tore sur un

corps K, on a la décomposition suivante : $T = T_d \cdot T_a$ où T_d est un tore déployé, il est composé uniquement d'éléments diagonalisables dans K, et T_a est un tore anisotrope, il est composé d'éléments diagonalisables uniquement dans une extension de K. On voit facilement qu'un tore déployé est isomorphe au produit de n copies de $K^\times$.

Afin de donner une idée des spécificités des tores anisotropes, regardons le cas réel. Nous présentons ici les choses de manière informelle afin de privilégier une compréhension intuitive du phénomène. Pour diagonaliser une matrice, il faut trouver les racines du polynôme caractéristique. Les polynômes irréductibles sur $\mathbb{R}$ étant de degrés 1 ou 2, on voit facilement que les racines complexes non réelles d'un polynôme sont conjuguées deux à deux. Les éléments semi-simples de $\mathbb{R}$ sont des matrices diagonalisables dans $\mathbb{C}$. Les valeurs propres sont alors soit réelles, soit conjuguées deux à deux. Ainsi les matrices diagonalisables dans $\mathbb{C}$ seront diagonalisables par bloc dans $\mathbb{R}$ avec un bloc diagonal et des blocs de la forme :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{avec } a, b \in \mathbb{R}$$

La partie diagonale correspondra au tore déployé et la partie diagonale par blocs au tore anisotrope. On voit alors que l'étude des tores anisotrope sur $\mathbb{R}$ se résume à l'étude des tores anisotropes de dimension 1 : $SO_2(\mathbb{R})$.

Sur $\mathbb{Q}_p$, étant donné que $\widetilde{\mathbb{Q}_p}^{alg}$ est de degré infini sur $\mathbb{Q}_p$, il existe des polynômes irréductibles de degré arbitrairement grand et un tore anisotrope de dimension n n'est a priori pas un produit de tore de dimension 1. Une étude spécifique des tores anisotropes sur $\mathbb{Q}_p$ est alors nécessaire.

Les tores anisotropes sur $\mathbb{Q}_p$ seront au coeur de ce travail et apparaitront tout au long de la thèse. Nous donnerons une description complète des tores anisotropes sur $\mathbb{Q}_p$ de dimension 1. Ces derniers nous serviront à décrire tous les sous-groupes définissables de $SL_2(\mathbb{Q}_p)$. Une description algébrique des tores anisotropes de dimension quelconque sera donnée à l'aide de l'exponentielle p-adique et elle nous permettra d'établir la "semi-algébricité" des groupes linéaires commutatifs définissables dans des structures p-minimales. Enfin nous étudierons leur générosité dans $SL_2(\mathbb{Q}_p)$.

Un autre point important de notre travail sera l'étude de $SL_2(\mathcal{Q}_p)$, pour $\mathcal{Q}_p$ un corps p-adiquement clos quelconque. Nous nous penchons sur cet exemple particulier de sous-groupe linéaire définissable dans $\mathcal{Q}_p$, car il s'agit du premier exemple non trivial de tels groupes, et il nous donne une bonne vision de ce qui peut se passer dans les cas de dimension plus grande. De plus cette petite dimension, nous permet une description exhaustive des sous-groupes définissables dans $\mathcal{L}_R$, donnant ainsi une panoplie d'exemples de groupes définissables dans $\mathcal{Q}_p$. On constatera alors que chaque sous-groupe définissable de $SL_2(\mathcal{Q}_p)$ de dimension 1 contient une suite infinie de sous-groupes uniformément définissables, ce travail est inspiré du lemme 3.2 de [34].

Une partie de notre travail sera consacrée à l'étude des groupes linéaires définissables dans dans des structures p-minimales. Nous démontrerons que si $\mathcal{L}$ est un langage contenant l'exponentiel tel que $\mathbb{Q}_p$ soit une structure p-minimale dans ce

langage alors les groupes $\mathcal{L}$-définissables linéaires commutatifs sont définissablement isomorphes à un groupe semi-algébrique (c'est-à-dire définissable dans $\mathcal{L}_R$). Ce travail est inspiré des résultats dans le cas o-minimal de [32], tout en ayant ses spécificités propres. Un rôle important sera joué par l'exponentielle p-adique qui nous permettra notamment de décrire la structure algébrique des tores anisotropes de dimension quelconque. Nous introduisons aussi une notion de p-connexité afin de palier l'absence de composante connexe évoquée dans les groupes définissables de $\mathbb{Q}_p$. Il est à noter que cette étude ne nécessite pas l'utilisation d'une décomposition cellulaire pour les ensembles définissables dans les structures p-minimales.

Nous présenterons également des résultats modestes sur la généricité et la générosité dans $SL_2(\mathcal{Q}_p)$ pour $\mathcal{Q}_p$ un corps p-adiquement clos. La notion de généricité pour les groupes définissables dans les corps p-adiques a été traitée pour le cas des sous-groupes compacts dans [29].

Le premier chapitre est dédié aux préliminaires, nous y rappelons tous les éléments qui nous serviront par la suite. Le vocabulaire de base de la théorie des modèles sera présenté. Une partie importante sera consacrée aux corps p-adiques et aux corps élémentairement équivalents à ces derniers. Nous insisterons particulièrement sur la notion de dimension et ses propriétés, elle sera, en effet, au coeur de certaines démonstrations clés de notre travail. Nous donnons enfin un bref aperçu de la théorie des groupes algébriques linéaires.

Le chapitre 2 est consacré aux tores anisotropes de dimension 1 au dessus de $\mathbb{Q}_p$. Nous décrirons alors la structure modèle-théorique de ces derniers, c'est-à-dire leurs sous-groupes définissables (proposition 2.6). La structure algébrique sera, quant à elle, donnée dans le théorème 2.10. Enfin, nous nous servirons des tores anisotropes pour expliciter la structure du groupe multiplicatif d'une extension quadratique de $\mathbb{Q}_p$.

Dans le chapitre 3, nous nous intéresserons à $SL_2(\mathcal{Q}_p)$ et à ses sous-groupes définissables, pour $\mathcal{Q}_p$ un corps p-adiquement clos. Une première partie est consacrée aux sous-groupes de Cartan de $SL_2(K)$ pour K un corps sur lequel nous imposons juste qu'il soit infini, de caractéristique différente de 2 et tel que $K^\times/(K^\times)^2$ soit fini. L'étude des sous-groupes de Cartan nous permettra de définir des sous-groupes "cadres" contenant tous les sous-groupes nilpotents ou résolubles de $SL_2(K)$ (corollaire 3.7 et proposition 3.8).

Une seconde partie est dédiée à SL_2 au dessus d'un corps p-adiquement clos. La description des sous-groupes commutatifs, nilpotents et résolubles se fera à l'aide des sous-groupes cadres définis plus haut. Le tore anisotrope de dimension 1 apparaissant comme un des sous-groupes cadres, nous trouverons dans ce chapitre une application de l'étude détaillée du chapitre 2. La plupart des résultats sera démontrée dans un premier temps pour $\mathbb{Q}_p$, nous les généraliserons dans un second temps à tout corps élémentairement équivalent. L'étude des sous-groupes non résolubles se fera par des techniques sur les groupes algébriques linéaires. Nous démontrerons notamment la non existence de sous-groupe propre définissable non résoluble non borné (théorème 3.14). Enfin le tableau 3.1 résumera le chapitre en donnant un panorama de tous les sous-groupes définissables de $SL_2(\mathcal{Q}_p)$ à conjugaison près.

Dans le chapitre 4, nous aborderons un point de vue différent. Nous nous intéresserons aux groupes linéaires définissables dans les structures p-minimales et chercherons à savoir lesquels sont isomorphes à un groupe semi-algébrique. Pour répondre à cette question, l'exponentielle p-adique jouera un rôle clé. On rappellera, dans un premier temps, ses propriétés et on l'utilisera, dans un second temps, pour décrire la structure du groupe multiplicatif d'une extension finie quelconque de $\mathbb{Q}_p$ (proposition 4.4). L'absence de composante connexe étant un handicap pour les groupes définissables dans les corps p-adiques, nous introduirons une notion de p-connexité (définition 4.16) particulièrement utile pour les groupes linéaires commutatifs.

Le théorème 4.32 sera le résultat principal de ce chapitre. Il établit que si $\mathcal{L}$ est un langage étendant $\mathcal{L}_R$, contenant l'exponentielle et tel que la structure $\mathbb{Q}_p$ dans ce langage soit p-minimale, alors tout groupe linéaire commutatif définissable dans $\mathcal{L}$ est définissablement isomorphe à un groupe semi-algébrique. Pour établir ce résultat nous partirons de la décomposition de Jordan et de la décomposition des tores en partie déployée et partie anisotrope. Une étude des sous-groupes des tores sera alors nécessaire. Nous décrirons la structure algébrique d'un tore anisotrope de dimension quelconque (proposition 4.31). Le lemme 4.28 modeste en apparence sera clé pour passer du cas compact au cas non compact.

Le chapitre 5 traite des notions de généricité et générosité. Nous nous pencherons alors sur $SL_2(\mathcal{Q}_p)$, pour décrire ses sous-groupes généreux (corollaire 5.4).

Chapitre 1

Préliminaires

1.1 Vocabulaire de la théorie des modèles

La théorie des modèles est la branche des mathématiques qui étudie les structures mathématiques du point de vue de la logique du premier ordre. Pour étudier une structure, elle choisit un langage et cherche à comprendre ce qui est exprimable ou non à partir de ce langage. Nous rappelons ici le vocabulaire de base utilisé dans cette thèse. Pour plus de détails, nous nous référerons à [18]

Une *structure* $\mathfrak{M}$ est la donnée un ensemble non vide M muni d'un ensemble de fonctions $\{f_i\}_{i\in I}$, d'un ensemble de relations $\{R_j\}_{j\in J}$ et un ensemble de constantes particulières $\{c_r\}_{r\in R}$, ces éléments forment la *signature*. Pour décrire les sous-ensembles de M^n, on introduit un symbole pour chaque éléments de la signature, ces symboles et celui de l'égalité forme le *langage*. Par exemple, pour décrire un groupe, on utilisera naturellement le langage $\mathcal{L}_G = \{\cdot, ^{-1}, e\}$ avec la loi de composition '$\cdot$', l'inverse '$^{-1}$' et l'élément neutre 'e'. Pour parler d'un anneau ou d'un corps, on utilisera le langage $\mathcal{L}_R = \{+, -, \cdot, 0, 1\}$. Une *formule du premier ordre* est une suite cohérente de taille finie formée de symboles du langage, de variables, de connecteurs logiques et de quantificateurs. Les quantificateurs ne doivent porter que sur des éléments de M, on ne peut donc pas quantifier des parties de M ou des entiers. Quand une formule φ est vraie dans une structure $\mathfrak{M}$, on note $\mathfrak{M} \vDash \varphi$.

Deux structures sont *élémentairement équivalentes* si elles vérifient exactement les mêmes formules du premier ordre sans variable libre, leur *théorie* est alors l'ensemble des formules vérifiées par les deux structures, on la note $Th(\mathfrak{M})$.

Définition 1.1. *Pour une structure $\mathfrak{M}$,*

- *un ensemble $X \subseteq M^n$ est dit* définissable*, s'il existe une formule $\varphi(\bar{x}, \bar{a})$ avec un paramètre $\bar{a} \in M^m$ telle que les éléments de X sont exactement les éléments de M^n vérifiant la formule φ, on note alors $X = \varphi(M)$;*
- *une structure $\mathfrak{N} = (N, f_1, ..., R_1, ..., c_1, ...)$ est dite* définissable*, s'il existe une bijection de N vers un ensemble définissable de M^n telle que l'image de chaque graphe de fonctions f_i, de chaque relations R_i soient des ensembles définissables ;*
- *une structure $\mathfrak{N} = (N, f_1, ..., R_1, ..., c_1...)$ est* interprétable *s'il existe un sous-ensemble définissable X de M^n, une relation d'équivalence définissable E dans*

M^{2n} et une bijection f de $X/_E$ dans N telle que l'image réciproque de chaque graphe de fonction et de chaque relation de $\mathfrak{N}$ est définissable dans X.

Un *enrichissement* ou une *expansion* d'une structure $\mathfrak{M} = (M, ...)$ est une structure $\mathfrak{N} = (M, ...)$ ayant le même ensemble de base M mais auquel on a rajouter des symboles dans le langage.

Définition 1.2. *Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathcal{L}$-structures telles que $M \subseteq N$, on dit que $\mathfrak{N}$ est une* extension élémentaire *de $\mathfrak{M}$ et on note $\mathfrak{M} \preceq \mathfrak{N}$ si pour toute formule $\varphi(\bar{x})$ de $\mathcal{L}$ et tout élément $\bar{a} \in M$:*

$$\mathfrak{M} \vDash \varphi(\bar{a}) \quad \textit{si et seulement si} \quad \mathfrak{N} \vDash \varphi(\bar{a})$$

Définition 1.3. *On dit qu'une théorie T* élimine les quantificateurs *dans le langage $\mathcal{L}$, si pour toute formule $\varphi(\bar{x})$ avec au moins une variable libre, il existe une formule $\psi(\bar{x})$ de $\mathcal{L}$ sans quantificateur telle que, pour tout modèle $\mathfrak{M}$ de T :*

$$\mathfrak{M} \vDash \forall \bar{x} \quad \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$$

1.2 Corps p-adiquement clos

1.2.1 Coprs valués

Définition 1.4. *Soit Γ un groupe abélien ordonné et K un corps. Une* valuation *sur K à valeur dans Γ est une application $v : K \longrightarrow \Gamma \cup \{\infty\}$ vérifiant pour tout $x, y \in K$:*

1. *$v(x) = \infty$ si et seulement si $x = 0$;*
2. *$v(xy) = v(x) + v(y)$;*
3. *$v(x + y) \geq \min\{v(x), v(y)\}$.*

Un corps muni d'une valuation est appelé corps valué.

Si (K, v) est un corps valué, l'ensemble $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ est un anneau local et $\mathcal{M} = \{x \in K \mid v(x) > 0\}$ est son unique idéal maximal. $\mathcal{O}$ est appelé l'*anneau de valuation*. On a $\mathcal{O}^\times = \{x \in \mathcal{O} \mid v(x) = 0\} = \mathcal{O} \backslash \mathcal{M}$. Le corps $k = \mathcal{O}/_{\mathcal{M}}$ est appelé le *corps résiduel*. On appelle *application résiduelle* et on note res, la projection canonique $\mathcal{O} \longrightarrow \mathcal{O}/_{\mathcal{M}}$. Pour $x \in K$ et $\gamma \in \Gamma$, on notera $B_\gamma(x)$ les boules ouvertes de centre x et de rayon γ :

$$B_\gamma(x) = \{x \in K \mid v(x) > \gamma\}$$

On a de manière évidente l'isomorphisme $\Gamma \cong K^\times/\mathcal{O}^\times$.

Si v est une valuation sur K à valeur dans $\mathbb{Z}$, alors l'application : $|\ .\ |_v : K \longrightarrow \mathbb{R}$ défini par $|\ x\ |_v = r^{-v(x)}$ pour $r \in \mathbb{R}$ et $r > 1$ est une *valeur absolue* vérifiant pour tout $x, y \in K$:

1. $|\ x\ |_v = 0$ si et seulement si $x = 0$;
2. $|\ xy\ |_v = |\ x\ |_v |\ y\ |_v$;
3. $|\ x + y\ |_v \leq \max\{|\ x\ |_v, |\ y\ |_v\}$.

La topologie définie par cette valuation est la *topologie ultramétrique*.

Définition 1.5. *Un corps valué (K, v) est dit* hensélien *si, pour tout polynôme $f(X) \in \mathcal{O}[X]$ et $a \in \mathcal{O}$ tel que $res(f(a)) = 0$ et $res(f'(a)) \neq 0$, il existe $a' \in \mathcal{O}$ tel que $f(a') = 0$ et $res(a') = res(a)$.*

1.2.2 Corps p-adiques

Soit $p \in \mathbb{N}$ un nombre premier. Si $x \in \mathbb{Q}^\times$ alors il s'écrit $x = p^n \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ premiers entre eux et à p. On définit alors la *valeur absolue p-adique* pour $x \in \mathbb{Q}$ par :

$$| x |_p = \begin{cases} 0 & \text{si } x = 0 \\ p^{-n} & \text{si } x \neq 0 \end{cases}$$

Fait 1.6 (Théorème de Ostrowski [39, Theorem 2.2.1])**.** *Une valeur absolue non triviale sur $\mathbb{Q}$ est topologiquement équivalente à la valeur absolue usuelle $|\ .\ |$ ou à l'une des valeurs absolues p-adiques $|\ .\ |_p$ où p est un nombre premier.*

On note $\mathbb{Q}_p$ la complétion de $\mathbb{Q}$ pour la valeur absolue p-adique. Tout élément x de $\mathbb{Q}_p$ s'écrit de manière unique comme série de la forme :

$$x = \sum_{i \geq n} a_i p^i \quad \text{avec } a_i \in \{0, 1, ..., p-1\} \text{ et } n \in \mathbb{Z}$$

L'addition et la multiplication se font alors comme dans $\mathbb{Z}$ avec une écriture en base p. Si $a_n \neq 0$, on pose $v_p(x) = n \in \mathbb{Z}$ et $ac(x) = a_n$. Ainsi v_p est une valuation et $(\mathbb{Q}_p, v_p)$ est un corps valué, on appelle *anneau des entiers p-adiques* et on note $\mathbb{Z}_p$ son anneau de valuation. Son corps résiduel est $\mathbb{F}_p$. On peut alors voir que : Pour tout $x \in \mathbb{Q}_p^\times$, il existe $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$ tels que :

$$x = p^n u \quad \text{avec } n = v_p(x)$$

On note alors $ac(x) = res(p^{-v_p(x)} x)$ l'application $ac : K^\times \longrightarrow k$ et on l'appelle la *composante angulaire.*

Définition 1.7 ([38, 1.1])**.** *Une suite $(G_n, \pi_n)_{n \in \mathbb{N}}$ de groupes et de morphismes $\pi_n : G_{n+1} \longrightarrow G_n$ est appelé un* système projectif. *Un groupe G muni de morphismes $p_n : G \longrightarrow G_n$ tel que pour tout $n \in \mathbb{N}$, $p_n = \pi_n \circ p_{n+1}$, est appelé* limite projective *de la suite (G_n, π_n) s'il vérifie la propriété* universelle suivante *: pour tout groupe H et tout morphisme $r_n : H \longrightarrow G_n$ vérifiant $r_n = \pi_n \circ r_{n+1}$ $(n \in \mathbb{N})$, il existe un unique homomorphisme $\varphi : H \longrightarrow G$ telle que pour tout $n \in \mathbb{N}$, $r_n = p_n \circ \varphi$.*

On peut également définir $\mathbb{Z}_p$ comme la limite projective $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ [39, 4.7]. $\mathbb{Q}_p$ apparait alors comme le corps des fractions de $\mathbb{Z}_p$.

Fait 1.8 ([39, Proposition 1.1.6])**.** *$\mathbb{Q}_p$ est un corps valué de caractéristique 0.*

$\mathbb{Z}_p$ est un anneau principal, dont les seuls idéaux non triviaux sont de la forme $p^n\mathbb{Z}_p$ avec $n \in \mathbb{N}$.

Fait 1.9 ([39, 1.5.2])**.** *Muni de la topologie définie par la valuation, $\mathbb{Q}_p$ est un corps topologique complet, totalement discontinu et localement compact.*

$\mathbb{Z}_p$ est compact.

Fait 1.10 (Lemme de Hensel [39, Theorem 1.6.4]). *Soit $f \in \mathbb{Z}_p[X]$ un polynôme et $a \in \mathbb{Z}_p$, tel que $f(a) \equiv 0 \mod p\mathbb{Z}_p$ et $f'(a) \not\equiv 0 \mod p\mathbb{Z}_p$, alors il existe $a' \in \mathbb{Z}_p$ tel que $f(a') = 0$ et $a' \equiv a \mod p\mathbb{Z}_p$.*

Fait 1.11 ([40, Théorème 2, Chapitre II]). *On a la description suivante du groupe multiplicatif :*

$$\begin{aligned} &\text{pour } p \neq 2 && \mathbb{Q}_p^\times = \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \\ &\text{pour } p = 2 && \mathbb{Q}_2^\times = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \end{aligned}$$

Extensions finies de $\mathbb{Q}_p$

Soit K une extension finie de $\mathbb{Q}_p$, si on note $N : K \longrightarrow \mathbb{Q}_p$ la norme relative, on a le résultat suivant.

Fait 1.12 ([39, Theorem 2.3.4]). *Soit K une extension finie du corps $\mathbb{Q}_p$. Alors il existe une unique valeur absolue sur K qui étend la valeur absolue p-adique sur $\mathbb{Q}_p$. On la note $|-|_p$ et v_p la valuation associée.*

De plus, si le degrè de K sur $\mathbb{Q}_p$ est n, alors pour $x \in K$, on a :

$$| x |_p = | N(x) |_p^{\frac{1}{n}}$$

Si K est une extension fini de $\mathbb{Q}_p$, K est un corps valué, on note alors k son corps résiduel, $\mathcal{O}$ son anneau de valuation et Γ son groupe de valeur.

– k est une extension fini du corps $\mathbb{F}_p$, on note f son degré, et on l'appelle le *dégré résiduel* de K.

$$f = [k : \mathbb{F}_p] = \dim_{\mathbb{F}_p} k$$

– Γ est un groupe contenant $\mathbb{Z}$ comme sous-groupe fini, on note e l'indice de celui-ci, et on l'appelle *l'indice de ramification* de K.

$$e = [v_p(K) : v_p(\mathbb{Q}_p)] = [\Gamma : \mathbb{Z}]$$

On appelle *uniformisante* un élément π tel que $v_p(\pi) = \frac{1}{e}$, l'idéal maximal de $\mathcal{O}$ est donc $\pi\mathcal{O}$.

Fait 1.13 ([39, Theorem 2.4.1]). *Si K est une extension de degré n de $\mathbb{Q}_p$, alors $n = ef$.*

Fait 1.14 ([39, 2.4.3 Corollary 2 and 2.4.4 Corollary 1]). *Le nombre de racines de l'unité de K d'ordre premier à p est inférieur à $p^f - 1$.*
Le nombre de racines de l'unité de K d'ordre une puissance de p est inférieur à $\frac{ep}{p-1}$.

Remarque. Du fait précédent, on tire que si K est une extension finie de $\mathbb{Q}_p$, alors le groupe multiplicatif $K^\times$ est de torsion finie.

1.2.3 Théorie des modèles des corps p-adiques

Les différents langages pour parler de $\mathbb{Q}_p$

On peut bien sûr étudier $\mathbb{Q}_p$ comme un corps dans le langage $\mathcal{L}_R$. Il est parfois utile de parler de valuation, on adjoint alors un symbole $|$ interprété par :

$$x \mid y \quad \text{si et seulement si} \quad v_p(x) \leq v_p(y)$$

Remarquons que [3] :

$$\text{pour } p \neq 2 \qquad \mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \exists y \quad y^2 = x^2 p + 1\} \tag{1.1}$$

$$\text{pour } p = 2 \qquad \mathbb{Z}_2 = \{x \in \mathbb{Q}_2 \mid \exists y \quad y^2 = 8x^4 + 1\} \tag{1.2}$$

Ainsi le symbole $|$ est définissable dans le langage $\mathcal{L}_R$.

Il est aussi très utile de considérer $\mathbb{Q}_p$ comme un corps valué étudié dans un langage à trois sortes. Une sorte pour K le corps de base, une pour k le corps résiduel et une pour Γ le groupe de valeur. Les corps K et k sont chacun munis d'une structure de corps, le groupe Γ est étudié dans le langage $\{+, -, 0, <, \infty\}$. Nous rajoutons enfin, les symboles de fonctions $res : \mathcal{O} \longrightarrow k$ et $v_p : K \longrightarrow \Gamma$.

Dans la suite nous utiliserons le langage à une sorte $\mathcal{L}_R$ pour décrire les objets de $\mathbb{Q}_p$. Sachant que tout ensemble définissable dans le langage à une sorte est naturellement définissable dans le langage à trois sortes, nous ferons référence à ce dernier sur certains points.

La théorie de $\mathbb{Q}_p$

On appelle *corps p-adiquement clos* un corps élémentairement équivalent à $\mathbb{Q}_p$. K est un corps p-adiquement clos si :

- K est un corps valué hensélien de caractéristique 0 ;
- son corps résiduel est isomorphe à $\mathbb{F}_p$;
- son groupe de valeur est un groupe de Presburger ou $\mathbb{Z}$-groupe (ie. un groupe élémentairement équivalent à $(\mathbb{Z}, +, <, 0, 1)$;
- $v(p)$ est le plus petit élément positif du groupe de valeurs.

Par la suite $\mathcal{Q}_p$ sera un corps p-adiquement clos et $\mathcal{Z}_p$ son anneau de valuation.

Remarque. Pour notre définition de *p-adiquement clos* nous nous référons à [3]. Certains auteurs ont une définition plus large qui inclut des extensions finies de $\mathbb{Q}_p$ ([37]).

Fait 1.15 ([25])**.** *$Th(\mathbb{Q}_p)$ admet l'élimination des quantificateurs dans la langage $\mathcal{L} = \{+, -, \cdot, 0, 1, |\} \cup \{P_n \mid n \geq 2\}$, où $x \mid y$ est interprété par $v_p(x) \leq v_p(y)$ et $P_n(x)$ par $x \neq 0$ et $\exists y \quad x = y^n$.*

Fait 1.16 ([42, Theorem A22])**.** *$Th(\mathbb{Q}_p)$ est NIP.*

Groupes de Presburger

Les résultats suivants sont tirés de [27] et [24].

Définition 1.17. $(\Gamma, +, <, 0, 1)$ *est un groupe de Presburger (ou $\mathbb{Z}$-groupe) si*
- $(\Gamma, +, 0)$ *est un groupe abélien ;*
- $(\Gamma, <)$ *est un ensemble discrètement ordonné, on note* 1 *le plus petit élément strictement positif ;*
- *L'ordre est compatible avec la loi de groupe :*

$$\forall x \forall y \forall z \quad x < y \Rightarrow x + z < y + z$$

- *(Schéma d'axiomes pour tout n)*

$$\forall x \in \Gamma \ \exists y \in \Gamma \ \exists i \in \{0, ..., n-1\} \quad x = ny + i$$

Remarque. On a les propriétés suivantes :

a) si $x > y$ alors $x \geq y + 1$;

b) si $nx = 0$ alors $n = 0$ ou $x = 0$;

c) si $x = ny > 0$ alors $x \geq n$ et $x \geq y$;

d) la classe de congruence de x modulo n est unique ;

e) s'il existe, le quotient $\frac{x}{n}$ est unique.

Fait 1.18 ([27, Corollary 3.1.21])**.** *La théorie des groupes de Presburger, est une théorie complète, décidable qui admet l'élimination des quantificateurs dans le langage $\mathcal{L} = \{+, -, <, 0, 1\} \cup \{Q_n \mid n \in \mathbb{N}^{\geq 2}\}$ où $Q_n(x)$ est interprété par "x est divisible par n".*

Etudions les modèles de la théorie des groupes de Presburger : $\mathbb{Z}$ se plonge par l'homomorphisme $n \mapsto n \cdot 1$; dans chaque groupe de Presburger (on identifie $\mathbb{Z}$ à son image). $\mathbb{Z}$ est un sous-groupe convexe de Γ.

$\Gamma/\mathbb{Z}$ est un groupe abélien ordonné divisible et sans torsion. On peut alors munir $\Gamma/\mathbb{Z}$ d'une structure de $\mathbb{Q}$-espace vectoriel : Si $x \in \Gamma/\mathbb{Z}$ et $n > 0$, alors il existe un unique $y \in \Gamma/\mathbb{Z}$ avec $ny = x$ car $\Gamma/\mathbb{Z}$ est divisible sans torsion. On peut alors définir une fonction $\mathbb{Q} \times \Gamma \longrightarrow \Gamma$ défini par $(\frac{m}{n}, x) \longmapsto my$ (où $ny = x$) pour la multiplication scalaire. Les axiomes d'espace vectoriel se vérifient aisément.

On en déduit que $\Gamma/\mathbb{Z} \cong \mathbb{Q}^l$ pour un certain cardinal l.

Modèles de $Th(\mathbb{Q}_p)$

Proposition 1.19. *$\mathbb{Q}_p$ est le seul modèle de $Th(\mathbb{Q}_p)$ qui est complet et dont le groupe de valeur est $\mathbb{Z}$.*

Démonstration. Soit $K \models Th(\mathbb{Q}_p)$ complet tel que $\Gamma_K = \mathbb{Z}$. On identifie les corps résiduel k_K, $k_{\mathbb{Q}_p}$ et $\mathbb{F}_p$, et on construit un isomorphisme entre K et $\mathbb{Q}_p$. Pour $x \in K^\times$, on construit les suites $(x_n)_{n\in\mathbb{N}} \subseteq K$, $(\gamma_n)_{n\in\mathbb{N}} \subseteq \Gamma$ et $(a_{\gamma_n}) \subseteq \{0, 1, ..., p-1\}$ par récurrence :

$$\begin{cases} x_0 = x \\ \gamma_0 = v(x_0) \\ a_{\gamma_0} = ac(x_0) \end{cases} \qquad \begin{cases} x_{k+1} = x_k - p^{\gamma_k} a_{\gamma_k} = x - \sum_{n\leq k} a_{\gamma_n} p\gamma_n \\ \gamma_{k+1} = v(x_{k+1}) \\ a_{\gamma_{k+1}} = ac(x_{k+1}) \end{cases}$$

On voit que chaque élément de $K^\times$ peut ainsi s'écrire $x = \sum_{k\geq 0} a_{\gamma_k} p^{\gamma_k}$ (en effet, $v_p(x - \sum_{0\leq k\leq N} a_{\gamma_k} p^{\gamma_k}) = \gamma_N \to +\infty$). On peut alors définir l'homomorphisme :

$$\begin{array}{rccc} \varphi : & K & \longrightarrow & \mathbb{Q}_p \\ & x & \longmapsto & \sum_{k\geq 0} a_{\gamma_k} p^{\gamma_k} \\ & 0 & \longmapsto & 0 \end{array}$$

φ est un isomorphisme : l'injectivité est immédiate, la surjectivité vient de la complétude de K. □

Théorie des modèles des extensions finis de $\mathbb{Q}_p$

On considère K une extension finie de $\mathbb{Q}_p$ d'indice de ramification e et de degré résiduel f. On a ainsi que son corps résiduel k a $q = p^f$ éléments et $v(p) = e$ (1 représente le plus petit élément de son groupe de valeur). Soit $\tilde{\alpha} \in k$ tel que $k = \mathbb{F}_p(\tilde{\alpha})$, et soit $Q(X) \in \mathbb{Z}[X]$ un polynôme unitaire tel $res(Q)$ soit le polynôme minimal de $\tilde{\alpha}$ dans $\mathbb{F}_p[X]$. K étant hensélien, il existe $\alpha \in \mathcal{O}$ tel que $Q(\alpha) = 0$ et $res(\alpha) = \tilde{\alpha}$. On sait qu'il existe $\pi \in K$ tel que $\pi^e \in \mathbb{Q}_p(\alpha)$ et $ev(\pi) = v(p)$. Ainsi $K = \mathbb{Q}_p(\alpha, \pi)$. On note $P(X, Y) \in \mathbb{Z}[X, Y]$ un polynôme irréductible qui s'annule en (α, π).

La théorie de K est alors donnée par la théorie T dans le langage $\mathcal{L}_R \cup \{c_1, c_2\}$:
- K est hensélien de caractéristique 0 ;
- le corps résiduel de K a p^f éléments ;
- $Q(c_1) = 0$
- le groupe de valeurs de K est un groupe de Presburger ;
- $v(c_2)$ est le plus petit élément du groupe de valeur et $v(p) = ev(c_2)$;
- $P(c_1, c_2) = 0$.

Fait 1.20 ([6, 5.5])**.** *La théorie T admet l'élimination des quantificateurs dans le langage $\mathcal{L} = \{+, -, \cdot, 0, 1, |\} \cup \{P_n \mid n \leq 2\}$, où $x \mid y$ est interprété par $v_p(x) \leq v_p(y)$ et $P_n(x)$ par $x \neq 0$ et $\exists y \quad x = y^n$.*

Citons le "paradoxe" suivant :

Fait 1.21 ([4])**.** *Il existe un corps élémentairement équivalent à une extension finie de $\mathbb{Q}_p$ qui ne contient pas de sous-corps de codimension finie qui soit élementairement équivalent à $\mathbb{Q}_p$*

1.2.4 Dimension

Dans cette partie nous allons définir ce que nous entendons en générale par *dimension*. Nous nous référerons à la définition donnée par van den Dries dans [44] et nous énoncerons les propriétés usuelles (ou non) d'une telle dimension. Ensuite nous nous concentrerons sur le cas p-adiquement clos et le langage $\mathcal{L}_R$, pour voir les propriétés valables dans ce cas. Dans la suite de la thèse, toutes les dimensions utilisées auront les propriétés de bases énoncées en dessous, nous préciserons selon l'état de nos connaissances si d'autres propriétés peuvent s'adjoindre ou non.

Dans son article [44] van den Dries définit une dimension comme étant une application 'dim' de l'ensemble des parties définissables d'une structure $\mathfrak{M}$ dans $\mathbb{N}\cup\{-\infty\}$ vérifiant les axiomes suivants : pour tout ensemble définissable S, S_1 et S_2 de M^m :

(Dim 1) $\dim S = -\infty \Leftrightarrow S = \varnothing$, $\dim\{a\} = 0$ pour chaque $a \in M$, et $\dim M^1 = 1$.

(Dim 2) $\dim(S_1 \cup S_2) = \max\{\dim S_1, \dim S_2\}$.

(Dim 3) $\dim S^\sigma = \dim S$ pour toute permutation σ de $\{1, ..., m\}$, et où

$$S^\sigma = \{(x_{\sigma(1)}, ..., x_{\sigma(m)}) \in M^m \mid (x_1, ..., x_m) \in S\}$$

(Dim 4) Si $T \subset M^{m+1}$ est un ensemble définissable et $T_x = \{y \in M \mid (x, y) \in T\}$ pour tout $x \in M^m$, alors $T(i) = \{x \in M^m \mid \dim T_x = i\}$ (pour $i = 0, 1$) est définissable et

$$\dim\{(x, y) \in T \mid x \in T(i)\} = \dim T(i) + i$$

Fait 1.22 ([44, §1])**.** *Toutes les dimensions au sens de van den Dries vérifient les propriétés naturelles suivantes (énoncées dans [2]) :*

Définissabilité *Si $f : S_1 \longrightarrow S_2$ est une fonction définissable, alors l'ensemble $\{y \in S_2 \mid \dim f^{-1}(y) = m\}$ est définissable pour tout $m \in \mathbb{N}$.*

Additivité *Si $f : S_1 \longrightarrow S_2$ est une fonction définissable, dont les fibres sont de dimension constante m, alors $\dim S_1 = \dim Im(f) + m$.*
En particulier, $\dim(S_1 \times S_2) = \dim S_1 + \dim S_2$.

Finitude *S est fini si et seulement si $\dim S = 0$.*

Monotonicité *Si $f : S \longrightarrow K^m$, alors $\dim f(S) \leq \dim S$, et si f est injective alors $\dim f(S) = \dim S$.*
En particulier, si $S_1 \subseteq S_2$ alors $\dim S_1 \leq \dim S_2$.

Nous énonçons maintenant des propriétés supplémentaires que peut vérifier une dimension dans le cas d'un corps muni d'une topologie.

Définition 1.23. *Soit K un corps topologique et soit* dim *une dimension sur K, on dira que :*

– *la dimension est compatible avec la clôture algébrique si :*

$$\dim_K X = \dim_K \overline{X}^K = \dim_{\widetilde{K}^{alg}} \overline{X}^{\widetilde{K}^{alg}}$$

– *la dimension est compatible avec la topologie si :*

$$\text{si } X \subseteq Y \text{ et } \dim X = \dim Y \quad \text{alors} \quad X \text{ est d'intérieur non vide dans } Y$$

Dans le premier point, $\dim_K$ représente la dimension sur K au sens de van den Dries, $\overline{X}^K$ la clôture de Zariski de X dans K et $\dim_{\widetilde{K}^{alg}} \overline{X}^{\widetilde{K}^{alg}}$ représente la dimension algébro-géométrique de la clôture de Zariski de X dans $\widetilde{K}^{alg}$.

Revenons au cas p-adiquement clos. Van den Dries a montré dans [44] que les corps valués henséliens K de caractéristique 0, étudiés dans le langage $\mathcal{L}_R$, sont équipés d'une dimension dim définit pour tout sous-ensemble de K^n vérifiant les axiomes (Dim 1-4). Dans le cas de $\mathbb{Q}_p$, cette dimension correspond à celle définie dans [46]. De plus, on montre que :

Fait 1.24. *Soit K un corps valué hensélien de caractéristique 0 étudié dans le langage $\mathcal{L}_R$, alors :*
- *la dimension est compatible avec la clôture algébrique ;*
- *la dimension est compatible avec la topologie définie par la valuation.*

Pour (K, v) un corps valué, on notera $\overline{X}^v$ l'adhérence de l'ensemble $X \subseteq K^n$ pour la topologie ultramétrique définie par v. Avant d'établir ce fait, rappelons quelques résultats de [44].

Fait 1.25 ([44, 1.7])**.** *Si $K \preceq K'$ sont deux $\mathcal{L}$-structures. Si K est muni d'une dimension* $\dim_K$*, alors K' est également muni d'une dimension* $\dim_{K'}$*. De plus si $X \subseteq K^n$ est un ensemble définissable et $X' \subseteq K'^n$ est l'ensemble défini par la même formule que X, alors* $\dim_K X = \dim_{K'} X'$.

Fait 1.26. *Soit K un corps et $X \subseteq K^n$.*

1. [44, 2.12] $\dim X = \dim \overline{X}^K$
2. [44, 2.3] *Si (K^*, X^*) est une extension élémentaire $|K|^+$-saturé de (K, X) et $X \neq \emptyset$, alors*
$$\dim_K X = \max\{trdeg_K K(x) \mid x \in X^*\}$$

Fait 1.27 ([44, 2.23])**.** *K est un corps hensélien de caractéristique 0 et $X \subseteq K^n$. Si X et $\overline{X}^v$ sont définissables alors* $\dim(\overline{X}^v \setminus X) < \dim(X)$.

Démonstration du fait 1.24. • On sait par la fait 1.26 que $\dim_K X = \dim_K \overline{X}^K$. Soit $K' \succeq K$ une structure $|K|^+$-saturée et X^* est l'ensemble de K'^m défini par la même formule que X. On a par les faits 1.25 et 1.26 :

$$\dim_K X = \max\{trdeg_K K(x) \mid x \in X^*\} = \dim_{\widetilde{K'}^{alg}} X^* = \dim_{\widetilde{K'}^{alg}} \overline{X^*}^{\widetilde{K'}^{alg}} = \dim_{\widetilde{K}^{alg}} \overline{X}^{\widetilde{K}^{alg}}$$

On n'a pas besoin que X^* soit définissable dans $\widetilde{K'}^{alg}$.

• Soit $X \subseteq Y$ des ensembles définissables tels que $\dim X = \dim Y$. Raisonnons par l'absurde et supposons que X est d'intérieur vide dans Y. Cela signifie que X ne contient aucun ouvert de Y, donc pour tout $x \in X$ et $\gamma \in \Gamma$, $B_\gamma(x) \cap Y \nsubseteq X$ *i.e.* il existe $y \in Y \setminus X$ tel que $y \in B_\gamma(x) \cap Y$. Cela signifie que $Y \setminus X$ est dense dans Y pour la topologie ultramétrique, donc $\overline{Y \setminus X}^v = Y$. En utilisant le fait 1.27, on trouve $\dim((\overline{Y \setminus X}^v) \setminus (Y \setminus X)) < \dim(Y \setminus X)$ et finalement $\dim X < \dim Y$, absurde. □

1.3 Groupes algébriques linéaires

Dans cette section, On note K un corps quelconque et K' un corps algébriquement clos tel que $K \subseteq K'$. On note I_n l'élément neutre de $GL_n(K)$.

Définition 1.28. *On dit qu'un groupe linéaire algébrique G défini sur K est* algébriquement connexe *si G ne contient pas de sous-groupe algébrique propre d'indice fini.*

Fait 1.29 ([5, 1.2]). *Soit G un groupe linéaire algébrique défini sur K et G° un sous-groupe algébrique. Les assertions suivantes sont équivalentes :*

(i) G° *est le plus grand sous-groupe algébrique connexe de* G *;*

(ii) G° *est l'intersection de tous les sous-groupes algébriques d'indice fini de* G *;*

(iii) G° *est la composante connexe de* I_n *au sens de la topologie de Zariski.*

On appelle G° *la* composante algébriquement connexe *de* G.

Définition 1.30.
– *On dit que* $x \in GL_n(K)$ *est* unipotent *si* $x - I_n$ *est nilpotent, c'est à dire qu'il existe* $m \in \mathbb{N}$ *tel que* $(x - I_n)^m = 0_n$. *On a* $m \leq n$.
– *On dit que* $x \in GL_n(K)$ *est* semi-simple *si* x *est diagonalisable dans* $GL_n(\widetilde{K}^{alg})$.

Fait 1.31 (Décomposition de Jordan [5, 4.2]). *Soit $x \in GL_n(K)$, alors il existe un élément semi-simple x_s et un élément unipotent x_u tels que :*

$$x = x_s x_u = x_u x_s$$

Cette décomposition est unique. De plus il existe des fonctions f et g rationnelles sur K telles que :

$$x_s = f(x) \quad \text{et} \quad x_u = g(x)$$

Soit G un groupe linéaire algébrique. On note :

$$G_s = \{x \in G \mid x = x_s\} = \{x \in G \mid x \text{ est semi-simple}\}$$

$$G_u = \{x \in G \mid x = x_u\} = \{x \in G \mid x \text{ est unipotent}\}$$

Fait 1.32 ([5, 4.7]). *Soit $G \leq GL_n(K)$ un sous-groupe algébrique commutatif. Alors G_s et G_u sont des sous-groupes fermés et on a :*

$$G \cong G_s \times G_u$$

l'isomorphisme est algébrique.

Définition 1.33. *Un groupe algébrique $T \leq GL_n(K')$ est un* tore *s'il est algébriquement connexe et vérifie les conditions équivalentes suivantes :*
(i) T est formé d'éléments semi-simples sur K' ;
(ii) T est diagonalisable sur K' ;
(iii) T est isomorphe au produit de n copies de $K'^\times$.

Notation. Pour T un tore sur K', on note :

$$X^*(T)_K = \{\chi : T(K) \longrightarrow K^\times \text{ homomorphisme }\}$$

$$X^*(T) = \{\chi : T(K') \longrightarrow K'^\times \text{ homomorphisme }\}$$

On dit que
– T est *anisotrope* sur K, s'il est défini sur K et $X^*(T)_K = 1$.

– T est *déployé* sur K, s'il est défini sur K et s'il est isomorphe à un produit de $K^\times$.

Remarque. 1. Tout tore défini sur K (ou K-tore) est déployé sur la clôture séparable K^{sep} de K.

2. Si T est déployé sur K, alors $X^*(T)_K = \mathbb{Z}^n$ où $n = \dim T$.

Fait 1.34 ([5, 10.6])**.** *Soit K' un corps algébriquement clos, et $G \leq GL_n(K')$ un sous-groupe algébrique algébriquement connexe et résoluble.*

1. *G_u est un sous-groupe connexe.*
2. *Si T est un tore maximal alors $G = G_u \rtimes T$ (produit semi-direct).*

De plus si G est nilpotent, alors G_s est un sous-groupe de G et on a :

$$G \cong G_s \times G_u$$

Conventions

Dans cette thèse on prendra les notations et conventions suivantes :

– p sera toujours un nombre premier.

– Si K (respectivement A) est un corps (respectivement un anneau), on notera K^+ (resp. A^+) son groupe additif et $K^\times$ (resp. $A^\times$) son groupe multiplicatif.

– Si K est un corps, $\widetilde{K}^{alg}$ sera la clôture algébrique de K.

– Si G est un groupe multiplicatif, on notera $(G)^n$ le sous-groupes des puissance $n^{\text{ième}}$ de G.
Ainsi $(K^\times)^n$ sera le groupe des puissances $n^{\text{ième}}$ de K tandis que $K^{\times n}$ sera le produit direct de n copies de $K^\times$.

– Si K est un corps valué, le corps résiduel sera systématiquement noté k, le groupe de valeur Γ et l'anneau de valuation $\mathcal{O}$.

– Si K est un corps valué et $X \subseteq K^n$, on notera $\overline{X}^v$ l'adhérence pour la topologie ultramétrique. $\overline{X}^K$ sera la clôture de Zariski de X dans K et $\overline{X}^{\widetilde{K}^{alg}}$ la clôture de Zariski dans $\widetilde{K}^{alg}$.

– A l'exception du chapitre 4, *définissable* signifiera *définissable avec paramètres dans le langage $\mathcal{L}_R$.*

– Si G est un groupe et H un sous-groupe de G, le centralisateur de H dans G sera noté :

$$C_G(H) = \{x \in G \mid \forall h \in H \quad xh = hx\}$$

le centre sera :

$$Z(G) = \{x \in G \mid \forall g \in G \quad xg = gx\}$$

et le normalisateur sera noté :

$$N_G(H) = \{x \in G \mid xHx^{-1} \subseteq H\}$$

Pour $x, y \in G$, $[x, y] = x^{-1}y^{-1}xy$.

Chapitre 2

Tores anisotropes de dimension 1

Dans ce chapitre, nous nous intéressons aux tores anisotropes de dimension 1. La première partie nous donne une présentation simple d'un tel tore au dessus d'un corps quelconque. Dans la seconde section nous nous penchons sur la structure de ces tores au dessus de $\mathbb{Q}_p$. On regarde alors la structure modèle-théorique, c'est-à-dire ses sous-groupes définissables (proposition 2.6). La structure algébrique est donnée par le théorème 2.10, à l'aide d'une limite projective. Nous concluons ce chapitre en montrant le lien entre les tores anisotropes de dimension 1 et les extensions quadratiques de $\mathbb{Q}_p$. Nous en déduisons la structure algébrique du groupe multiplicatif de ces derniers (corollaire 2.12).

2.1 Tores anisotropes

Dans cette section, nous énonçons des vérités générales sur les tores anisotropes de dimension 1. K sera un corps quelconque. On rappelle le fait suivant qui nous permettra de décrire très simplement les tores anisotropes de dimension 1 :

Fait 2.1 ([28, p. 223])**.** *Soit T un K-tore. Pour toute extension $L \subseteq K^{sep}$:*

$$T(L) = Hom(X^*(T), K^{sep\times})^{G_L} \tag{2.1}$$

où $G = Gal(K^{sep}/K)$ et G_L le sous-groupe constitué des éléments de G fixant L.

La notation signifie que $T(L)$ est le groupe des homomorphismes $X^*(T) \longrightarrow K^{sep\times}$ qui commute avec l'action de G_L sur $X^*(T)$. Si $X^*(T) = \mathbb{Z}$, on peut identifier $Hom(\mathbb{Z}, K^{sep\times})$ à $K^{sep\times}$ et G_L agit sur $\mathbb{Z}$, pour $\sigma \in G_L$ on note alors $\sigma \cdot 1$ l'image de 1 par l'action de σ sur $\mathbb{Z}$. Dans ce contexte, (2.1) devient :

$$T(L) = \{x \in K^{sep\times} \mid \forall \sigma \in G_L \quad \sigma(x) = x^{\sigma\cdot 1}\}$$

Les extensions de degrés 2 d'un corps K sont de la forme $K(\sqrt{\delta}) = \{a+b\sqrt{\delta} \mid a, b \in K\}$ pour δ un non-carré de K. Les automorphismes de $K(\sqrt{\delta})$ au dessus de K sont réduits à l'identité et à $a+b\sqrt{\delta} \longmapsto \overline{a+b\sqrt{\delta}} = a-b\sqrt{\delta}$ et on a $Gal(K(\sqrt{\delta})/K) = \mathbb{Z}/2\mathbb{Z}$.

Si L est une extension galoisienne de K et $x \in L$, on définit la *norme* de x comme :

$$N(x) = \prod_{\sigma \in Gal(L/K)} \sigma(x)$$

La norme est un homomorphisme des groupes multiplicatifs : $L^\times \longrightarrow K^\times$. Si $L = K(\sqrt{\delta})$ est une extension galoisienne de degrès 2, alors $N(a + b\sqrt{\delta}) = a^2 - b^2\delta \in K$.

Pour $\delta \in K^\times \setminus (K^\times)^2$, on pose :

$$Q_\delta = \left\{ x \in K(\sqrt{\delta}) \mid N(x) = 1 \right\} = \left\{ a + b\sqrt{\delta} \in K(\sqrt{\delta}) \mid a^2 - b^2\delta = 1 \right\} \tag{2.2}$$

Proposition 2.2. *Soit T un K-tore anisotrope de dimension 1. Alors il existe $\delta \in K^\times \setminus (K^\times)^2$ tel que T est définissablement isomorphe à Q_δ.*

Démonstration. T est déployé sur une extension L galoisienne de degré fini, et $X^*(T)_L = \mathbb{Z}$. On note $G = Gal(L/K)$. Le groupe G agit sur $\mathbb{Z}$ par l'homomorphisme $\varphi : G \longrightarrow Aut(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Ainsi $F = \ker\varphi$ est distingué dans G et $G/F \cong \mathbb{Z}/2\mathbb{Z}$, et F agit trivialement sur $\mathbb{Z}$. La théorie de Galois indique qu'il existe une extension L', $K \subseteq L' \subseteq L$ telle que :

$$L' = L^F = \{x \in L \mid \forall \sigma \in F \quad \sigma(x) = x\} \quad \text{et} \quad Gal(L/L') = F$$

D'après le fait 2.1, $T(L') = Hom(\mathbb{Z}, L^\times)^F = \{x \in L^\times \mid \forall \sigma \in F \quad \sigma(x) = x\} = L'^\times$. Ainsi T est déployé sur L'.

On a $[L' : K] = 2$ donc $L' = K(\sqrt{\delta})$ avec δ un non carré de K et $Gal(L'/K) = \{id, x \to \bar{x}\} = \mathbb{Z}/2\mathbb{Z}$. D'où

$$T(K) = Hom(\mathbb{Z}, L'^\times)^{Gal(L'/K)} = \{x \in L' \mid \bar{x} = x^{-1}\} = \{x \in K(\sqrt{\delta}) \mid N(x) = 1\} = Q_\delta$$

□

2.2 Structure des groupes Q_δ

Concentrons nous maintenant sur le cas p-adique et commençons par rappeler :

Fait 2.3 ([40, Chapitre II, 3.3])**.** *Si $p \neq 2$, le groupe $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, il a pour ensemble de représentants $\{1, \alpha, p, \alpha p\}$, où $\alpha \in \mathbb{Z}_p^\times$ est tel que $res(\alpha)$ n'est pas un carré dans $\mathbb{F}_p$.*

Si $p = 2$, le groupe $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, il a pour représentants $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Il y a donc, à isomorphisme près, trois extensions de degré de 2 de $\mathbb{Q}_p$ et autant de tores anisotropes de dimension 1 pour $p \neq 2$ (et sept pour $p = 2$). On notera, dans la suite de ce chapitre, $K_\delta = \mathbb{Q}_p(\sqrt{\delta})$ ainsi que k_δ et $\mathcal{O}_\delta$ respectivement son corps résiduel et son anneau de valuation. Les cas des différents δ seront traités en parallèles, on omettra le plus souvent l'indice sans risque de confusion. K_δ étant une extension de degré 2, on remarque que K_δ est soit non ramifié (si $v_p(\delta)$ est pair), soit totalement ramifié (si $v_p(\delta)$ est impair).

Remarque. On a par le fait 1.12, pour $x \in K$, $| N(x) |_p^{\frac{1}{2}} = | x |_p$. Donc si $N(x) = 1$, alors $| x |_p = 1$ et $x \in \mathcal{O}^\times$. Ainsi on a $Q_\delta \subseteq \mathcal{O}^\times$.

Les sections suivantes cherchent à décrire plus spécifiquement et de l'intérieur le groupe Q_δ. Dans la suite, pour plus de clarté, on séparera systématiquement les cas $p \neq 2$ et $p = 2$: les résultats sont similaires exceptés pour quelques valeurs spécifiques et les démonstrations sont les mêmes mutatis mutandis. C'est pourquoi nous développerons les résultats dans le cas $p \neq 2$. De plus, pour les besoin du raisonnement nous travaillerons avec des valeurs spécifiques de δ : à chaque fois δ sera l'un des éléments $\{\alpha, p, \alpha p\}$ représentants les non-carrés de $\mathbb{Q}_p^\times$ pour $p \neq 2$ et l'un des $\{-1, \pm 2, \pm 5, \pm 10\}$ pour $p = 2$. Dans chaque cas, on a $0 \leq v_p(\delta) \leq 1$.

2.2.1 Sous-groupes définissables

On pose :

$$\text{pour } p \neq 2 \text{ et } n \geq 0 \quad Z_{n,\delta} = (1 + p^{2n}\delta\mathbb{Z}_p + p^n\mathbb{Z}_p\sqrt{\delta}) \cap Q_\delta \tag{2.3}$$

$$\text{pour } p = 2 \text{ et } n \geq 1 \quad Z_{n,\delta} = (1 + p^{2n-1}\delta\mathbb{Z}_2 + p^n\mathbb{Z}_2\sqrt{\delta}) \cap Q_\delta \tag{2.4}$$

Pour la même raison que précédemment, il nous arrivera d'omettre le δ et d'écrire, sans confusion possible, simplement Z_n pour $Z_{n,\delta}$.

Lemme 2.4. – *Si $p \neq 2$ et pour $a+b\sqrt{\delta} \in Z_{0,\delta}$ avec $\delta \in \{p, \alpha p\}$ (resp. $a+b\sqrt{\delta} \in Z_{1,\delta}$ avec $\delta = \alpha$), alors pour tout $n \in \mathbb{N}$:*

$$b \in p^n\mathbb{Z}_p^\times \text{ si et seulement si } a \in 1 + p^{2n}\delta\mathbb{Z}_p^\times$$

– *Si $p = 2$ et pour $a + b\sqrt{\delta} \in Z_{1,\delta}$ avec $v_p(\delta) = 1$ (resp. $a + b\sqrt{\delta} \in Z_{2,\delta}$ avec $v_p(\delta) = 0$), alors pour tout $n \in \mathbb{N}^*$:*

$$b \in p^n\mathbb{Z}_2^\times \text{ si et seulement si } a \in 1 + p^{2n-1}\delta\mathbb{Z}_2^\times$$

Démonstration. • Nous traiterons en premier le cas $p \neq 2$, soit $a + b\sqrt{\delta} \in Z_0$ avec $b \in p^n\mathbb{Z}_p^\times$ alors a est tel que $a^2 - b^2\delta = 1$. On a $a^2 = 1 + b^2\delta$ donc $a^2 \in 1 + p^{2n}\delta\mathbb{Z}_p^\times$. On prouve que $a^2 \in 1 + p^{2n}\delta\mathbb{Z}_p^\times$ si et seulement si $a \in 1 + p^{2n}\delta\mathbb{Z}_p^\times$:
si $a = 1 + p^{2n}\delta u$ avec $u \in \mathbb{Z}_p^\times$ alors $a^2 = 1 + 2p^{2n}\delta u + p^{4n}\delta^2u^2 \in 1 + p^{2n}\delta\mathbb{Z}_p^\times$ (car $p \neq 2$) ;
si $a = 1 + p^k\delta u$ avec $k \neq 2n$, alors $a^2 \in 1 + p^k\delta\mathbb{Z}_p^\times$ et $a^2 \notin 1 + p^{2n}\delta\mathbb{Z}_p^\times$.

Maintenant si $a \in 1+p^{2n}\delta\mathbb{Z}_p^\times$, on montre que $v_p(b) = n$. On a $b^2\delta = a^2 - 1 \in p^{2n}\delta\mathbb{Z}_p^\times$, donc $2v_p(b) + v_p(\delta) = 2n + v_p(\delta)$ alors $v_p(b) = n$.

• Pour $p = 2$ nous raisonnons de la même manière. Il nous suffit de prouver que si $a \in 1+2^k\delta\mathbb{Z}_2^\times$, alors $a^2 \in 1+2^{k+1}\delta\mathbb{Z}_2^\times$: si $u \in \mathbb{Z}_2^\times$, on a $(1+2^k\delta u)^2 = 1+2^{k+1}\delta(u+2^{k-1}\delta u^2) \in 1 + 2^{k+1}\delta\mathbb{Z}_2^\times$. □

A partir de maintenant, on suppose que $p \neq 2$, les mêmes démonstrations fonctionneront pour $p = 2$ mutatis mutandis.

Remarque. Commençons par remarquer que les $Z_{n,\delta}$ sont des sous-groupes de Q_δ : soit $x, y \in Z_{n,\delta}$, $x = 1 + p^{2n}\delta a + p^n b\sqrt{\delta}$ et $y = 1 + p^{2n}\delta a' + p^n b'\sqrt{\delta}$, on a

$$xy = 1 + p^{2n}\delta(a + a' + bb' + p^{2n}\delta aa') + p^n(b + b' + p^{2n}\delta ab' + p^{2n}\delta a'b)\sqrt{\delta} \tag{2.5}$$

$$x^{-1} = \overline{x} = 1 + p^{2n}\delta a - p^n b\sqrt{\delta}$$

Aussi les sous-groupes $Z_{n,\delta}$ forment une chaine descendante infinie de sous-groupes définissables.

Avant de montrer la proposition décrivant les sous-groupes définissables de Q_δ, établissons le lemme technique suivant :

Lemme 2.5. *Pour $p \neq 2$, $\delta \in \{p, \alpha p\}$ et $n \geq 0$ (ou pour $\delta = \alpha$ et $n \geq 1$).*

1. $Z_{n,\delta}/Z_{n+1,\delta} \cong \mathbb{Z}/p\mathbb{Z}$
2. *si $x \in Z_{n,\delta} \setminus Z_{n+1,\delta}$ alors $x^{p^r} \in Z_{n+r,\delta} \setminus Z_{n+r+1,\delta}$*

Lemme 2.5 bis. *Pour $p = 2$, $v_p(\delta) = 1$ et $n \geq 1$ (ou pour $v_p(\delta) = 0$ et $n \geq 2$).*

1. $Z_{n,\delta}/Z_{n+1,\delta} \cong \mathbb{Z}/p\mathbb{Z}$
2. *Si $x \in Z_{n,\delta} \setminus Z_{n+1,\delta}$ alors $x^{p^r} \in Z_{n+r,\delta} \setminus Z_{n+r+1,\delta}$*

Démonstration du lemme 2.5. 1. On définit :

$$\begin{array}{rccc} \varphi : & Z_{n,\delta} & \longrightarrow & \mathbb{Z}_p/p\mathbb{Z}_p \\ & 1 + p^{2n}\delta a + p^n b\sqrt{\delta} & \longmapsto & b \mod p\mathbb{Z}_p \end{array}$$

(2.5) montre que φ est un homomorphisme surjectif bien défini du groupe $Z_{n,\delta}$ dans le groupe additif $\mathbb{Z}_p/p\mathbb{Z}_p$. Par le lemme 2.4, on voit que son noyau est $Z_{n+1,\delta}$, donc $Z_{n,\delta}/Z_{n+1,\delta} \cong \mathbb{Z}/p\mathbb{Z}$.

2. Montrons par récurrrence sur r que :

$$\text{si } \; x = 1 + p^{2n}\delta a + p^n b\sqrt{\delta} \text{ , alors } x^r = 1 + p^{2n}\delta a' + p^n(rb + p^{2n}\delta b')\sqrt{\delta} \text{ avec } a', b' \in \mathbb{Z}_p$$

Pour $r = 1$, c'est évident.

On suppose maintenant que $x^r = 1 + p^{2n}\delta a' + p^n(rb + p^{2n}\delta b')\sqrt{\delta}$, alors :

$$\begin{aligned} x^r x &= (1 + p^{2n}\delta a' + p^n(rb + p^{2n}\delta b')\sqrt{\delta})(1 + p^{2n}\delta a + p^n b\sqrt{\delta}) \\ &= 1 + p^{2n}\delta(a + a' + b(rb + p^{2n}\delta b') + p^{2n}\delta aa') \\ &\qquad + p^n((r+1)b + p^{2n}\delta b' + p^{2n}\delta a'b + p^{2n}\delta a(rb + p^{2n}\delta b'))\sqrt{\delta} \\ x^{r+1} &= 1 + p^{2n}\delta a'' + p^n((r+1)b + p^{2n}\delta b'')\sqrt{\delta} \end{aligned}$$

Donc si $x \in 1 + p^{2n}\delta\mathbb{Z}_p^\times + p^n\mathbb{Z}_p^\times\sqrt{\delta} \subseteq Z_{n,\delta} \setminus Z_{n+1,\delta}$ alors $x^p = 1 + p^{2n}\delta A + p^{n+1}B\sqrt{\delta}$ avec $B \in \mathbb{Z}_p^\times$, et par le lemme 2.4 $A \in p^2\mathbb{Z}_p^\times$, i.e. $x^p \in Z_{n+1,\delta} \setminus Z_{n+2,\delta}$.

Une autre récurrence montre que $x^{p^r} \in Z_{n+r,\delta} \setminus Z_{n+r+1,\delta}$.

□

Proposition 2.6. *Pour $p \neq 2$ et $\delta \in \{p, \alpha p\}$ (respectivement pour $\delta = \alpha$).*

1. *$Z_{0,\delta}$ (respectivement $Z_{1,\delta}$) est d'indice fini dans Q_δ.*
2. *Les $Z_{n,\delta}$ sont les seuls sous-groupes définissables de $Z_{0,\delta}$ (respectivement $Z_{1,\delta}$).*

Proposition 2.6 bis. *Pour $p = 2$ et δ un non carré tel que $v_p(\delta) = 1$ (respectivement $v_p(\delta) = 0$).*

1. *$Z_{1,\delta}$ (respectivement $Z_{2,\delta}$) est d'indice fini dans Q_δ.*
2. *Les $Z_{n,\delta}$ sont les seuls sous-groupes définissables de $Z_{1,\delta}$ (respectivement $Z_{2,\delta}$).*

Démonstration de la proposition 2.6. Nous allons travailler avec $\delta \in \{p, \alpha p\}$, les autres cas sont similaires :

1. On considère $\mathbb{Q}_p(\sqrt{\delta})$ l'extension quadratique de $\mathbb{Q}_p$ et k son corps résiduel, k est un corps fini. Soit ψ l'homomorphisme de groupe suivant :

$$\begin{array}{rccc} \psi : & Q_\delta & \longrightarrow & k^\times \\ & a + b\sqrt{\delta} & \longmapsto & res(a + b\sqrt{\delta}) \end{array}$$

   On voit que $\ker \psi = Z_{0,\delta}$ et $Z_{0,\delta}$ est d'indice fini.

2. Soit $H \leq Z_{0,\delta}$ un sous-groupe définissable non trivial. On voit par le point 2. du lemme 2.5 que $Z_{0,\delta}$ n'a pas de torsion, donc H est infini. Alors $\dim H = 1 = \dim Z_{0,\delta}$ et H est d'intérieur non vide dans $Z_{0,\delta}$ (fait 1.24), donc H est ouvert dans $Z_{0,\delta}$. Maintenant il suffit de montrer que les $Z_{n,\delta}$ sont les seuls sous-groupes ouverts.

   La démonstration est inspirée de celle du lemme 3.2 de [34]. Les $Z_{n,\delta}$ forment une base de voisinages ouverts de I dans Q_δ. Soit $H \leq Z_{0,\delta}$ un sous-groupe ouvert. H contient un voisinage ouvert de l'identité $Z_{n,\delta}$. On note n_0 le plus petit entier tel que $Z_{n_0,\delta} \subseteq H$. Si $H \neq Z_{n_0,\delta}$, alors il existe $x \in H \cap Z_{n_1,\delta}$ avec $n_1 < n_0$. Quitte à remplacer x par un certain x^{p^k}, on peut supposer que $x \in Z_{n_0-1,\delta} \setminus Z_{n_0,\delta}$. On a $Z_{n_0-1,\delta}/Z_{n_0,\delta} \cong \mathbb{Z}/p\mathbb{Z}$ donc x^t avec $0 \leq t \leq p-1$ est un système complet des représentants des classes modulo $Z_{n_0,\delta}$. Donc $Z_{n_0-1,\delta} \subseteq H$ ce qui contredit la minimalité de n_0.

□

2.2.2 Structure algébrique de Q_δ

Lemme 2.7. *Pour $p \neq 2$ et $\delta \in \{p, \alpha p\}$ (resp. $\delta = \alpha$) :*

1. *Soit $b \in \mathbb{Z}_p$ (resp. $b \in p\mathbb{Z}_p$), il existe un et un seul $x \in Z_0$ (resp. $x \in Z_1$) tel que $x = a + b\sqrt{\delta}$ avec $a \in 1 + p\mathbb{Z}_p$ (resp. $a \in 1 + p^2\mathbb{Z}_p$) ;*
2. *Soit $x = a + b\sqrt{\delta}$, $x' = a' + b'\sqrt{\delta}$ des éléments de Z_0 (resp. Z_1) et $n \geq 0$ (resp. $n \geq 1$) :*

$$x \equiv x' \mod Z_n \quad ssi \quad b \equiv b' \mod p^n\mathbb{Z}_p$$

3. *$Z_0 = \varprojlim Z_0/Z_n$ (resp. $Z_1 = \varprojlim Z_1/Z_n$).*

Démonstration. Nous traitons le cas $\delta \in \{p, \alpha p\}$ (i.e. $v_p(\delta) = 1$),

1. *Existence :* Soit $b \in \mathbb{Z}_p$, alors $1 + b^2\delta$ est un carré dans $\mathbb{Q}_p$ car $v_p(b^2\delta) > 0$, de plus si $u \in \mathbb{Z}_p$ est tel que $u^2 = 1 + b^2\delta$ alors $res(u^2) = 1$ et $res(u) = \pm 1$. Il suffit alors de prendre a tel que $a^2 = 1 + b^2\delta$ et $res(a) = 1$. Il vient que $N(a + b\sqrt{\delta}) = 1$ et, par la démonstration du lemme 2.4, $a \in 1 + \delta\mathbb{Z}_p$.
   Unicité : Soit $x = a + b\sqrt{\delta}$ et $x' = a' + b'\sqrt{\delta}$ avec $a = 1 + \delta\bar{a}$ et $a' = 1 + \delta\bar{a}'$, tels que $b = b'$. Donc $a^2 = a'^2 = 1 + b^2\delta$. Il vient que $1 + 2\delta\bar{a} + \delta^2\bar{a}^2 = 1 + 2\delta\bar{a}' + \delta^2\bar{a}'^2$ et $(\bar{a} - \bar{a}')(2 + \delta(\bar{a} + \bar{a}')) = 0$. Comme $v_p(\delta) > 0$, on trouve $\bar{a} = \bar{a}'$ et finalement $a = a'$.
2. $\Rightarrow$ / Soit $x = 1 + \delta\bar{a} + b\sqrt{\delta} \in Z_0$ et $x'' = 1 + p^{2n}\delta\bar{a}'' + p^n b''\sqrt{\delta} \in Z_n$, on a

$$xx'' = 1 + \delta(\bar{a} + \bar{a}''p^{2n} + \bar{a}\bar{a}''p^{2n}\delta + bb''p^n) + (b + p^n b'' + p^{2n}\delta\bar{a}''b + p^n\delta\bar{a}b'')\sqrt{\delta}$$

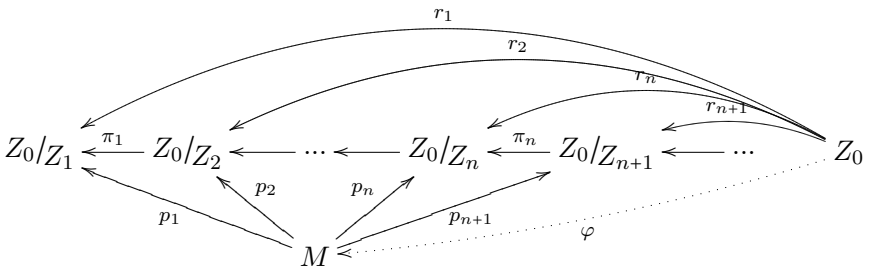
   Il vient que si $x = a + b\sqrt{\delta}$ et $x' = a' + b'\sqrt{\delta}$ sont des éléments de Z_0 et s'il existe $x'' \in Z_n$ tel que $x' = xx''$ alors $b \equiv b' \mod p^n$.
   $\Leftarrow$ / Soit $x = 1 + \delta\bar{a} + b\sqrt{\delta}$ et $x' = 1 + \delta\bar{a}' + b'\sqrt{\delta}$ des éléments de Z_0. Supposons $b \equiv b' \mod p^n$ et montrons que $\delta\bar{a} \equiv \delta\bar{a}' \mod p^n$. On écrit $b' = b + p^n r$ avec $r \in \mathbb{Z}_p$, donc

$$(1 + \delta\bar{a}')^2 = 1 + b'^2\delta = 1 + b^2\delta + 2bp^n r\delta + p^{2n}r^2\delta = (1 + \delta\bar{a})^2 + p^n R$$

   avec $R \in \mathbb{Z}_p$. Il vient que $(1 + \delta\bar{a}')^2 - (1 + \delta\bar{a})^2 = 2\delta\bar{a}' + \bar{a}'^2\delta^2 - 2\delta\bar{a} - \bar{a}^2\delta^2 = (\delta\bar{a}' - \delta\bar{a})(2 + (\bar{a} + \bar{a}')\delta)$ est divisible par p^n. On a donc $\delta\bar{a}' \equiv \delta\bar{a} \mod p^n$ car $v_p(2 + (\bar{a} + \bar{a}')\delta) = 0$. Aussi :

$$xx'^{-1} = 1 + \delta(\bar{a} + \bar{a}' + \delta\bar{a}\bar{a}' - b(b + p^n r)) + (b - b - p^n r - \delta\bar{a}b - \delta\bar{a}p^n r + b\delta\bar{a}')\sqrt{\delta}$$

   Puisque $\delta\bar{a}' - \delta\bar{a}$ est divisible par p^n, il vient que $b - b - p^n r - \delta\bar{a}b - \delta\bar{a}p^n r + \delta\bar{a}'b = b(\delta\bar{a}' - \delta\bar{a}) - p^n(r - \delta\bar{a}r) \in p^n\mathbb{Z}_p$, et par le lemme 2.4 que $xx'^{-1} \in Z_n$.
3. On note M la limite projective formelle des Z_0/Z_n(définition 1.7). On a :



$$M = \left\{(x_1, x_2, ..., x_n, ...) \in \prod_{i \in \mathbb{N}^*} Z_0/Z_i \mid \forall n \in \mathbb{N}^* \quad \pi_n(x_{n+1}) = x_n\right\}$$

   Par la propriété universelle de la limite projective, on sait qu'il existe un homomorphisme $\varphi : Z_0 \longrightarrow M$ tel que pour tout $n \geq 1$, $p_n \circ \varphi = r_n$. Montrons que φ est un isomorphisme. Pour l'injectivité, soit $x, x' \in Z_0$ tel que $\varphi(x) = \varphi(x')$, on a alors $p_n(\varphi(x)) = p_n(\varphi(x'))$ et $r_n(x) = r_n(x')$ pour tout $n \in \mathbb{N}^*$, ainsi

$xx'^{-1} \in Z_n$ pur tout $n \geq 1$. D'où $x = x'$ car $\bigcap_{n\in\mathbb{N}^*} Z_n = 1$. Pour la surjectivité, prenons $x = (x_1, x_2, ..., x_n, ...) \in M$, on pose $x_i = a_i + b_i\sqrt{\delta}$, on a $\pi_n(x_{n+1}) = x_n$ c'est-à-dire $x_{n+1} \equiv x_n \mod Z_n$ donc par 2. $b_{n+1} \equiv b_n \mod p^n$. Par définition de $\mathbb{Z}_p$ comme limite projective, on peut construire b tel que $b \equiv b_n \mod p^n$ pour tout $n \in \mathbb{N}^*$. Par 1. il existe $x' \in Z_0$ tel que $x' = a + b\sqrt{\delta}$, on a alors par 2. $r_n(x') = x_n$ c'est-à-dire $\varphi(x') = x$.

Le cas $\delta = \alpha$ se traite de manière identique, les calculs sont identiques et la conclusion relève du fait que $v_p(a\delta) > 0$ ou $v_p(b\delta) > 0$, même si $v_p(\delta) = 0$. □

Corollaire 2.8. *Pour $p \neq 2$ et $\delta \in \{p, \alpha p\}$ (respectivement $\delta = \alpha$), on a :*

$$Q_\delta = \varprojlim_{n\geq 0} Q_\delta/Z_n \quad (\text{resp. } Q_\delta = \varprojlim_{n\geq 1} Q_\delta/Z_n)$$

Démonstration. Par le lemme précédent, on a $Z_0 = \varprojlim Z_0/Z_n$, la démonstration de $Q_\delta = \varprojlim Q_\delta/Z_n$ se fait de manière similaire : on cherche à établir un isomorphisme avec la limite projective formelle M. L'injectivité est identique. Pour la surjectivité, on se ramène à Z_0. Soit $x = (x_0, x_1, ..., x_n, ...) \in M$, on pose alors $x'' = xx_0^{-1} = (1, x_1x_0^{-1}, ..., x_nx_0^{-1}, ...)$ et on a pour tout $n \geq 1$, $x''_n = x_nx_0^{-1} \in Z_0/Z_n$ car $x''_0 = 1$. Par le lemme précédent, il existe $x' \in Z_0$ tel que $r_n(x') = x''_n$. Il suffit alors de prendre $x'x_0 \in Q_\delta$ comme antécédent de x : on a bien $r_n(x'x_0) = x_n$. □

Lemme 2.7 bis. *Pour $p = 2$ et δ tel que $v_p(\delta) = 1$ (respectivement δ tel que $v_p(\delta) = 0$) :*

1. *Soit $b \in p\mathbb{Z}_p$ (resp. $b \in p^2\mathbb{Z}_p$), il existe un et un seul $x \in Z_1$ (resp. $x \in Z_2$) tel que $x = a + b\sqrt{\delta}$;*
2. *Soit $x = a + b\sqrt{\delta}$, $x' = a' + b'\sqrt{\delta}$ des éléments de Z_1 (resp. Z_2) et $n \geq 1$ (resp. $n \geq 2$) :*
$$x \equiv x' \mod Z_n \quad ssi \quad b \equiv b' \mod p^n$$
3. *$Z_1 = \varprojlim Z_1/Z_n$ (resp. $Z_2 = \varprojlim Z_2/Z_n$).*

Rappelons le lemme suivant [40, p. 31] :

Fait 2.9. *Soit $0 \to A \to E \to B \to 0$ une suite exacte de groupes commutatifs (notés additivement), avec A et B finis d'ordres a et b premiers entre eux. Soit B' l'ensemble des $x \in E$ tels que $bx = 0$. Le groupe E est somme directe de A et de B' ; de plus B' est le seul sous-groupe de E isomorphe à B.*

Théorème 2.10. *Pour $p \neq 2$, on a les isomorphismes suivants :*
Si $\delta \in \{p, \alpha p\}$, alors $Q_\delta \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p$
Si $\delta = \alpha$, alors $Q_\delta \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}_p$.

Démonstration. • Pour $\delta \in \{p, \alpha p\}$, montrons que $Q_\delta \cong \mathbb{Z}/2\mathbb{Z} \times Z_0$.

$\{-1, 1\}$ et Z_0 sont des sous-groupes distingués d'intersection triviale. Soit $a + b\sqrt{\delta} \in Q_\delta$, on a vu que $v_p(b) = n \geq 0$ (remarque page 23) et $a^2 \in 1 + p^{2n+1}\mathbb{Z}_p^\times$, donc

$a \in 1 + p^{2n+1}\mathbb{Z}_p^\times$ ou $a \in -1 + p^{2n+1}\mathbb{Z}_p^\times$ (sinon il existerait $u \in \mathbb{Z}/p^{2n+1}\mathbb{Z}$, $u \notin \{1,-1\}$ tel que $u^2 \equiv 1 \mod p^{2n+1}$). Ainsi $Q_\delta = Z_0 \cup -Z_0$ et $Q_\delta \cong \mathbb{Z}/2\mathbb{Z} \times Z_0$.

Il reste à montrer que $Z_0 \cong \mathbb{Z}_p$. On suit la démonstration du théorème 2 de [40, Chapitre II]. Soit $\varepsilon \in Z_0 \setminus Z_1$, par le lemme 2.5, on a $\varepsilon^{p^k} \in Z_k \setminus Z_{k+1}$. Soit ε_n l'image de ε dans Z_0/Z_n. On a $(\varepsilon_n)^{p^n} = 1$ et $(\varepsilon_n)^{p^{n-1}} \neq 1$. Comme Z_0/Z_n est d'ordre p^n, c'est un groupe cyclique engendré par ε_n. Notons alors $\theta_{n,\varepsilon}$ l'isomorphisme $z \longmapsto \varepsilon_n^z$ de $\mathbb{Z}/p^n\mathbb{Z}$ sur Z_0/Z_n. Le diagramme

$$\begin{array}{ccc} \mathbb{Z}/p^{n+1}\mathbb{Z} & \xrightarrow{\theta_{n+1,\varepsilon}} & Z_0/Z_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\theta_{n,\varepsilon}} & Z_0/Z_n \end{array}$$

est commutatif. On en conclut que les $\theta_{n,\varepsilon}$ définissent un isomorphisme θ_ε de $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z}$ sur $Z_0 = \varprojlim Z_0/Z_n$.

• Pour $\delta = \alpha$, montrons que $Q_\delta/Z_1 \cong \mathbb{Z}/(p+1)\mathbb{Z}$.

On note $\tilde{\alpha} = res(\alpha)$, ainsi le corps résiduel de $\mathbb{Q}_p(\sqrt{\alpha})$ est $k = \mathbb{F}_p(\sqrt{\tilde{\alpha}})$. On considère l'homomorphisme de groupe $res : Q_\delta \longrightarrow \mathbb{F}_p(\sqrt{\tilde{\alpha}})^\times$ de noyau Z_1. Aussi $res(Q_\delta)$ est un sous-groupe de $\mathbb{F}_p(\sqrt{\tilde{\alpha}})^\times$ qui est cyclique, donc $res(Q_\delta)$ est cyclique. On en déduit que $Q_\delta/Z_1 \cong \mathbb{Z}/r\mathbb{Z}$ pour un certain r. On considère alors l'homomorphisme de groupe norme :

$$\begin{array}{rccc} N: & \mathbb{F}_p(\sqrt{\tilde{\alpha}})^\times & \longrightarrow & \mathbb{F}_p^\times \\ & a + b\sqrt{\tilde{\alpha}} & \longmapsto & a^2 - b^2\tilde{\alpha} \end{array}$$

Par [40, chap. IV, prop. 4] l'application est surjective donc $|\mathbb{F}_p(\sqrt{\tilde{\alpha}})^\times| = |\mathbb{F}_p^\times| \cdot |\ker N|$ donc $|\ker N| = \frac{p^2-1}{p-1} = p+1$. Ainsi $|res(Q_\delta)| = |\{x \in \mathbb{F}_p(\sqrt{\tilde{\alpha}}) \mid N(x) = 1\}| = p+1$, et $Q_\delta/Z_1 \cong \mathbb{Z}/(p+1)\mathbb{Z}$.

Montrons $Q_\delta \cong Q_\delta/Z_1 \times Z_1$. Appliquons le fait 2.9 à la suite exacte :

$$1 \longrightarrow Z_1/Z_n \longrightarrow Q_\delta/Z_n \longrightarrow Q_\delta/Z_1 \longrightarrow 1$$

On a bien $|Q_\delta/Z_1| = p+1$ et $|Z_1/Z_n| = p^{n-1}$ premiers entre eux, donc :

$$Q_\delta/Z_n \cong Q_\delta/Z_1 \times Z_1/Z_n \quad \text{pour tout } n \geq 1$$

Il vient par passage à la limite :

$$\varprojlim Q_\delta/Z_n \cong Q_\delta/Z_1 \times \varprojlim Z_1/Z_n$$

$$Q_\delta \cong Q_\delta/Z_1 \times Z_1$$

On montre de la même manière que précédemment que $Z_1 \cong \mathbb{Z}_p$. D'où le résultat. □

Théorème 2.10 bis. *Pour $p = 2$, on a les isomorphismes suivants :*

Si δ est un non carré de $\mathbb{Q}_2$ tel que $v_p(\delta) = 1$ alors $Q_\delta \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

Si δ est un non carré de $\mathbb{Q}_2$ vérifiant $v_p(\delta) = 0$ alors $Q_\delta/Z_{2,\delta} \leq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $Z_{2,\delta} \cong \mathbb{Z}_2$.

Démonstration. • Supposons que $v_p(\delta) = 1$. Soit $a + b\sqrt{\delta} \in Q_\delta$, on a $a^2 - b^2\delta = 1$ donc $1 + b^2\delta = a^2$ est un carré de $\mathbb{Q}_2$ donc $1 + b^2\delta \equiv 1 \mod 8$, alors 8 divise $b^2\delta$ donc 2 divise b car $v_p(\delta) = 1$. On a aussi $a^2 \equiv 1 \mod 8$, en particulier $a^2 \equiv 1 \mod 4$ donc

$$a \equiv 1 \quad \text{ou} \quad a \equiv 3 \mod 4$$

Si $x = a + b\sqrt{\delta}$ et $x' = a' + b'\sqrt{\delta}$ sont deux éléments de Q_δ, montrons que :

$$x \equiv x' \mod Z_1 \quad \text{si et seulement si} \quad a \equiv a' \mod 4$$

On a :

$$xx'^{-1} = (a + b\sqrt{\delta})(a' - b'\sqrt{\delta}) = (aa' - bb'\delta) + (a'b - b'a)\sqrt{\delta} \tag{2.6}$$

On sait que $v_p(b) \geq 1$ et $v_p(b') \geq 1$ donc $a'b - b'a \in 2\mathbb{Z}_2$. Ainsi $xx'^{-1} \in Z_1$ ssi $aa' - bb'\delta \equiv 1 \mod 4$ ssi $aa' \equiv 1 \mod 4$ ssi $a \equiv a' \mod 4$ car a et a' sont congrus à 1 ou 3 modulo 4. On a ainsi montré que $Q_\delta/Z_1 \cong \mathbb{Z}/2\mathbb{Z}$. En constatant que $\mathbb{Z}/2\mathbb{Z}$ est réalisé dans Q_δ par $\{-1, 1\}$ ($-1 \notin Z_1$), on conclut que $Q_\delta \cong \mathbb{Z}/2\mathbb{Z} \times Z_1$. On montre, comme pour $p \neq 2$ que $Z_1 \cong \mathbb{Z}_2$.

• Supposons que $v_p(\delta) = 0$. Soit $a + b\sqrt{\delta} \in Q_\delta$, on procède de la même manière et on montre que $v_p(b) \geq 2$ et $a^2 \equiv 1 \mod 8$ donc

$$a \equiv 1 \quad \text{ou} \quad a \equiv 3 \quad \text{ou} \quad a \equiv 5 \quad \text{ou} \quad a \equiv 7 \mod 8$$

Si $x = a + b\sqrt{\delta}$ et $x' = a' + b'\sqrt{\delta}$ sont deux éléments de Q_δ, par (2.6), on montre que :

$$x \equiv x' \mod Z_2 \quad \text{ssi} \quad a \equiv a' \mod 8$$

Il y a donc au plus quatre classes modulo Z_2 dans Q_δ et on voit que $Q_\delta/Z_1 \leq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On a de même que précédemment $Z_2 \cong \mathbb{Z}_2$. □

2.3 Tores anisotropes et groupe multiplicatif d'une extension quadratique

On a, jusqu'à présent, considéré les tores anisotropes du point de vue formel des groupes. Replaçons maintenant notre étude dans le contexte des extensions de degré 2. Dans cette partie, on ne traitera que le cas $p \neq 2$, on garde les mêmes notations :

On note $K = \mathbb{Q}_p(\sqrt{\delta})$. On montre d'abord que

$$\mathcal{O}^\times = k^\times \times (1 + \pi\mathcal{O})^\times$$

Soit f le degré résiduel de K. On considère le polynôme $F(x) = x^{p^f-1} - 1$, on a $F'(x) = (p^f - 1)x^{p^f-2}$. Tout $\bar{a} \in k^\times$ est solution de $F(x) = 0$ et de plus $F'(\bar{a}) = -\bar{a}^{-1} \neq 0$. Soit $a' \in \mathcal{O}$ tel que $res(a') = \bar{a}$, on a alors $res(F(a')) = 0$ et $res(F'(a')) \neq 0$. Par hensélianité, il existe $a \in \mathcal{O}$ avec $res(a) = \bar{a}$ et $F(a) = 0$. On pose alors $V = \{x \in \mathcal{O} \mid x^{p^f-1} = 1\}$ le groupe des racines $(p^f - 1)^{\text{ième}}$ de l'unité, V possède donc bien $(p^f - 1)$ éléments, et $V \cong k^\times$. On a $res^{-1}(1) = 1 + \pi\mathcal{O}$ et $V \cap (1 + \pi\mathcal{O}) = \{1\}$ donc $\mathcal{O}^\times = V \times (1 + \pi\mathcal{O})$.

On note $\widetilde{Q_\delta} = res(Q_\delta) = res(Q_\delta \cap V) \subseteq k^\times$ et $Q'_\delta = Q_\delta \cap (1+\pi\mathcal{O})$. On constate que $Q'_\delta = Z_{0,\delta}$ pour $\delta \in \{p, \alpha p\}$ (resp. $Q'_\delta = Z_{1,\delta}$ pour $\delta = \alpha$). On a par le théorème 2.10 :

$$Q_\delta \cong \widetilde{Q_\delta} \times Q'_\delta$$

Proposition 2.11. *Pour $p \neq 2$, et si $K = \mathbb{Q}_p(\sqrt{\delta})$ pour δ un non carré de $\mathbb{Q}_p$, alors :*

$$(1+\pi\mathcal{O})^\times = Q'_\delta \times (1+p\mathbb{Z}_p)^\times \quad \text{où} \quad Q'_\delta = Q_\delta \cap (1+\pi\mathcal{O})$$

Démonstration. • Si $\delta \in \{p, \alpha p\}$, alors $\pi = \sqrt{\delta}$, $v_p(\pi) = \frac{1}{2}$ et $k = \mathbb{F}_p$. On a $Z_n = (1 + p^{2n}\delta\mathbb{Z}_p + p^n\sqrt{\delta}\mathbb{Z}_p) \cap Q_\delta$, et $Q'_\delta = Z_0$.

Pour $x \in Q'_\delta$, $x \neq 1$, il existe n_0 minimal tel que $x \in Z_{n_0}$ ($x \notin Z_{n_0-1}$), alors $v_p(x-1) = n_0 + \frac{1}{2}$, donc si $x \in Q'_\delta$ alors $v_p(x) \in \frac{1}{2} + \mathbb{N}$. Si $x \in \mathbb{Q}_p \cap (1+\pi\mathcal{O}) = 1 + p\mathbb{Z}_p$, $x \neq 1$, alors $v_p(x-1) \in 1 + \mathbb{N}$. On a donc bien $\mathbb{Q}_p \cap Q'_\delta = \{1\}$.

Si $z \in (1+\pi\mathcal{O}) \cap \mathbb{Q}_p = 1 + p\mathbb{Z}_p$, alors $N(z) = z^2 = (1+pu)^2 = 1 + 2pu + p^2u^2 \in 1 + p\mathbb{Z}_p$, pour un certain $u \in \mathbb{Z}_p$. Si $x \in 1 + \pi\mathcal{O}$,

$$\begin{aligned} N(x) &= N(1 + \sqrt{\delta}(a + b\sqrt{\delta})) \\ &= N(1 + a\sqrt{\delta} + b\delta) \\ &= (1+b\delta)^2 - (a\sqrt{\delta})^2\delta \\ &= 1 + 2b\delta + b^2\delta^2 - a\delta^2 \quad \in 1 + p\mathbb{Z}_p \text{ (car } v_p(\delta) = 1) \end{aligned}$$

Comme tous les éléments de $1 + p\mathbb{Z}_p$ sont des carrés, si $x \in 1 + \pi\mathcal{O}$ alors on sait qu'il existe $z \in 1 + p\mathbb{Z}_p$ tel que $N(x) = z^2$. On pose $x = zy$, on a $N(x) = N(z) = z^2$, donc $N(y) = 1$ et $y \in Q'_\delta$. Ainsi $x = zy$ avec $z \in \mathbb{Q}_p$ et $y \in Q'_\delta$. On en déduit l'égalité voulue.

• Si $\delta = \alpha$, alors $\pi = p$, $v_p(\pi) = 1$ et si $\tilde{\alpha} = res(\alpha)$, alors $\tilde{\alpha}$ n'est pas un carré dans $\mathbb{F}_p$ et $k = \mathbb{F}_p(\sqrt{\tilde{\alpha}})$. On a $Z_n = (1 + p^{2n}\mathbb{Z}_p + \sqrt{\alpha}p^n\mathbb{Z}_p) \cap Q_\delta$ pour $n \geq 1$.

Pour $x \in Q'_\delta$ et $x \neq 1$, alors il existe $n_0 \geq 1$ minimal tel que $x \in Z_{n_0}$, ainsi $ac(x-1) \in \sqrt{\tilde{\alpha}} \cdot \mathbb{F}_p^\times$. Si $x \in (1+p\mathcal{O}) \cap \mathbb{Q}_p = 1 + p\mathbb{Z}_p$, alors $ac(x-1) \in \mathbb{F}_p^\times$. Ainsi on a $\mathbb{Q}_p \cap Q'_\delta = \{1\}$. On montre comme précédemment que $1 + \pi\mathcal{O} = (1 + p\mathbb{Z}_p) \cdot \mathbb{Q}'_\delta$. □

Remarque. Si $\delta \in \{p, \alpha p\}$, alors $k = \mathbb{F}_p$ et $\widetilde{Q_\delta} = \widetilde{Q_\delta} \cap \mathbb{F}_p = \{-1, 1\}$.

Si $\delta = \alpha$, alors $\tilde{\alpha} = res(\alpha)$ n'est pas un carré dans $\mathbb{F}_p$ et $k = \mathbb{F}_p(\tilde{\alpha})$. On a alors $\widetilde{Q_\delta} \cap \mathbb{F}_p^\times = \{a \in \mathbb{F}_p \mid a^2 = 1\} = \{-1, 1\}$. On montre que $\widetilde{Q_\delta} \cdot \mathbb{F}_p = (k^\times)^2$: on a $N((k^\times)^2) = (\mathbb{F}_p^\times)^2$, donc si $x \in (k^\times)^2$ alors il existe $z \in \mathbb{F}_p^\times$ et y avec $N(y) = 1$ tels que $x = zy$ donc $(k^\times)^2 \subseteq \widetilde{Q_\delta} \cdot \mathbb{F}_p^\times$. Comme $|(k^\times)^2| = \frac{p^2-1}{2}$ et $|\widetilde{Q_\delta} \cdot \mathbb{F}_p^\times| = \frac{(p+1)(p-1)}{2}$, on en déduit l'égalité cherchée.

Corollaire 2.12. *Pour $p \neq 2$, on a :*

$$\mathcal{O}^\times \cong k^\times \times \mathbb{Z}_p^{+2}$$
$$K^\times \cong \mathbb{Z} \times k^\times \times \mathbb{Z}_p^{+2}$$

Démonstration. Le premier isomorphisme résulte de l'égalité $\mathcal{O}^\times = V \times (1+\pi\mathcal{O})^\times$ et de la propriété 2.11.

Pour le second isomorphisme, on remarque que tout élément x de K s'écrit $x = \pi^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{O}^\times$, on a alors l'égalité $K^\times = \{\pi^n; n \in \mathbb{Z}\} \times \mathcal{O}^\times$. L'isomorphisme voulu est immédiat. □

Conclusion

On a établi à l'aide d'une limite projective l'isomorphisme : $Q_\delta \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}_p$ (pour $p \neq 2$). Cet isomorphisme n'est, a priori, pas définissable. On peut alors légitimement se poser la question si $\mathcal{Q}_p$ est un corps élémentairement équivalent à $\mathbb{Q}_p$, est-ce qu'on a l'isomorphisme $Q_\delta \cong \mathbb{Z}/n\mathbb{Z} \times \mathcal{Z}_p$? De même pour $K = \mathcal{Q}_p(\sqrt{\delta})$, a-t-on $\mathcal{O}^\times \cong k^\times \times \mathcal{Z}_p^{+2}$?

On a remarqué dans l'introduction qu'une connaissance des tores anisotropes de dimension 1 ne donne, a priori, aucune information sur les tores de dimension plus grande. Peut-on alors généraliser les résultats obtenu ici en dimension quelconque : si T est un tore anisotrope de dimension n, a-t-on $T \cong \widetilde{T} \times \mathbb{Z}_p^{+n}$ où $\widetilde{T}$ est un groupe fini ? Si K est une extension de degré n de $\mathbb{Q}_p$, a-t-on $K^\times \cong \mathbb{Z} \times k^\times \times \mathbb{Z}_p^{+n}$?

Nous répondrons de manière partielle à ces questions dans le chapitre 4.

Chapitre 3

Sous-groupes définissables de SL_2 au dessus d'un corps p-adiquement clos

Ce chapitre reprend l'essentiel des résultats de [13]. Le but est de décrire l'ensemble des sous-groupes $\mathcal{L}_R$-définissables de $SL_2(\mathcal{Q}_p)$ pour $\mathcal{Q}_p$ un corps p-adiquement clos. Il est divisé en deux parties :

La première partie est très générale : elle traite de $SL_2(K)$ pour K un corps quelconque sur lequel on impose juste qu'il soit infini, de caractéristique différente de 2 et tel que $K^\times/(K^\times)^2$ soit fini. Le point de départ est l'étude des sous-groupes de Cartan, nous nous référons à la définition de ces derniers par Chevalley qui s'énonce pour un groupe quelconque. Le théorème 3.6 nous décrit alors tous les sous-groupes de Cartan à conjugaison près de $SL_2(K)$. Par la suite, nous arrivons à décrire des "sous-groupes cadres" qui contiennent tous les sous-groupes nilpotents ou résolubles de $SL_2(K)$. Le corollaire 3.7 et la proposition 3.8 nous donne une description de ces sous-groupes cadres.

Dans la seconde partie, nous nous penchons plus particulièrement sur le cas p-adiquement clos. Nous utilisons alors les outils modèle-théoriques développés dans ce contexte particulièrement la dimension et ses liens avec la topologie ultramétrique. Nous nous intéressons aux sous-groupes définissables commutatifs, nilpotents et résolubles c'est-à-dire les sous-groupes définissables des sous-groupes cadres évoqués dans la première partie (proposition 3.12 et théorème 3.13). Pour traiter le cas non résoluble, nous séparerons les cas borné et non borné. La décomposition de Bruhat pour $SL_2(\mathcal{Q}_p)$ nous permettra de décrire le cas non borné tandis que nous nous référerons à un théorème de J.P. Serre [41, Chap II, 1.3, Proposition 2] pour le cas borné.. Enfin le tableau 3.1 résume le chapitre en donnant un panorama complet des sous-groupes définissables de $SL_2(\mathcal{Q}_p)$.

3.1 Sous-groupes de Cartan

Dans cette section, K sera un corps infini tel que $K^\times/(K^\times)^2$ est fini et $carK \neq 2$.

Définition 3.1. *Soit G un groupe. Un sous-groupe de Cartan est un sous-groupe C tel que :*

1. *C est un sous-groupe nilpotent maximal ;*
2. *tout sous-groupe X d'indice fini dans C, est d'indice fini dans son normalisateur $N_G(X)$.*

Remarque. Si G est un groupe infini, alors tout sous-groupe de Cartan est infini. En effet, si C est un sous-groupe de Cartan fini de G, alors $\{1\}$ est un sous-groupe d'indice fini de C mais est d'indice infini dans $N_G(\{1\}) = G$, ce qui est absurde.

Pour tout $\delta \in K^\times \setminus (K^\times)^2$, on pose :

$$Q_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in SL_2(K) \mid a \in K^\times \right\}$$
$$Q_\delta = \left\{ \begin{pmatrix} a & b \\ b\delta & a \end{pmatrix} \in SL_2(K) \mid a, b \in K \text{ et } a^2 - b^2\delta = 1 \right\}$$

Remarque. On considère l'homomorphisme :

$$\begin{array}{rccc} \varphi : & SL_2(K) & \longrightarrow & K(\sqrt{\delta}) \\ & \begin{pmatrix} a & b \\ b\delta & a \end{pmatrix} & \longmapsto & a + b\sqrt{\delta} \end{array}$$

φ défini bien un isomorphisme entre Q_δ et $\{x \in K(\sqrt{\delta}) \mid N(x) = 1\}$. Ce qui justifie l'emploi de la même notation que pour parler des tores anisotropes de dimension 1 (cf. Chapitre 3, 2.2).

Lemme 3.2. *On a les égalités suivantes sur les centralisateurs :*

$$\forall x \in Q_1 \setminus \{I, -I\} \quad C_{SL_2(K)}(x) = Q_1$$
$$\forall x \in Q_\delta \setminus \{I, -I\} \quad C_{SL_2(K)}(x) = Q_\delta$$

Démonstration. Un calcul matriciel très simple assure le résultat. □

Proposition 3.3. *Les groupes Q_1 et Q_δ sont des sous-groupes de Cartan de $SL_2(K)$.*

Démonstration. Le groupe Q_1 est abélien et son normalisateur est :

$$N_{SL_2(K)}(Q_1) = Q_1 \cdot < w > \qquad \text{où} \qquad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Pour X un sous-groupe de Q_1, si $g \in N_{SL_2(K)}(X)$ et $x \in X$, alors, en utilisant le lemme 3.2 :

$$Q_1 = C_{SL_2(K)}(x) = C_{SL_2(K)}(x^g) = C_{SL_2(K)}(x)^g = Q_1^g$$

Ainsi $N_{SL_2(K)}(X) \leq N_{SL_2(K)}(Q_1) = Q_1 \cdot < w >$, et comme, pour $t \in Q_1$, on a $t^w = w^{-1}tw = t^{-1}$, il vient que $N_{SL_2(K)}(X) = Q_1 \cdot < w >$. Si X est d'indice fini r dans Q_1,

alors X est d'indice $2r$ dans $N_{SL_2(K)}(X)$. On note Γ_i la série centrale descendante de $N_{SL_2(K)}(Q_1)$, on peut voir que pour t dans Q_1, on a $[w,t] = t^2$ et on a :

$$\begin{aligned}\Gamma_0 &= N_{SL_2(K)}(Q_1)\\ \Gamma_1 &= [N_{SL_2(K)}(Q_1), N_{SL_2(K)}(Q_1)] = (Q_1)^2\\ \Gamma_i &= [N_{SL_2(K)}(Q_1), \Gamma_{i-1}] = (Q_1)^{2^i}\end{aligned}$$

Puisque $Q_1 \cong K^\times$, on peut conclure que Γ_i n'atteint jamais $\{I\}$: Q_1 est infini et $(Q_1)^{2^i}$ est d'indice fini dans $(Q_1)^{2^{i-1}}$ (en effet $(Q_1)^{2^{i-1}}/(Q_1)^{2^i}$ est en bijection avec $K^\times/(K^\times)^2$). Ainsi $N_{SL_2(K)}(Q_1)$ n'est pas nilpotent. Par la condition de normalisateur pour les groupes nilpotents, si Q_1 est strictement contenu dans un sous-groupe nilpotent C, alors $Q_1 < N_C(Q_1) \leq C$, or $N_C(Q_1) = Q_1 \cdot < w >$ qui n'est pas nilpotent, absurde. On a ainsi montré que Q_1 est bien un sous-groupe de Cartan.

Pour $\delta \in K^\times \setminus (K^\times)^2$, le groupe Q_δ est abélien. Comme pour tout sous-groupe X de Q_δ non contenu dans $Z(SL_2(K))$, $C_{SL_2(K)}(X) = Q_\delta$, on a ainsi $N_{SL_2(K)}(X) = N_{SL_2(K)}(Q_\delta) = Q_\delta$ et si X est d'indice fini dans Q_δ alors X est d'indice fini dans son normalisateur. Par la condition de normalisateur pour les groupes nilpotents, Q_δ est nilpotent maximal. □

Proposition 3.4. *1.* $Q_1^{SL_2(K)} = \{A \in SL_2(K) \mid tr(A)^2 - 4 \in (K^\times)^2\} \cup \{I, -I\}$

2. pour $\delta \in K^\times \setminus (K^\times)^2$*, il existe* $n \in \mathbb{N}$ *et* $\mu_1, ..., \mu_n \in GL_2(K)$ *tel que :*

$$\bigcup_{i=1}^{n} Q_\delta^{\mu_i \cdot SL_2(K)} = \{A \in SL_2(K) \mid tr(A)^2 - 4 \in \delta \cdot (K^\times)^2\} \cup \{I, -I\}$$

On pose :

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \mid u \in K \right\} \cup \left\{ \begin{pmatrix} -1 & u \\ 0 & -1 \end{pmatrix} \mid u \in K \right\} \quad \text{et} \quad U^+ = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \mid u \in K \right\}$$

Si $A \in SL_2(K)$ satisfait $tr(A)^2 - 4 = 0$, alors $tr(A) = 2$ ou $tr(A) = -2$ et A est un conjugué d'un élément de U. Dans ce cas, on dira (par abus de langage dans ce chapitre) que A est *unipotent*. Il suit de la Proposition 3.4 :

Corollaire 3.5. *On a la partition suivante :*

$$SL_2(K) \setminus \{I, -I\} = (U \setminus \{I, -I\})^{SL_2(K)} \sqcup (Q_1 \setminus \{I, -I\})^{SL_2(K)} \sqcup \bigsqcup_{\delta \in K^\times/(K^\times)^2} \bigcup_{i=1}^{n} (Q_\delta^{\mu_i} \setminus \{I, -I\})^{SL_2(K)}$$

Remarque. Si δ et δ' dans $K^\times$ sont dans la même classe modulo $(K^\times)^2$, alors, par la proposition 3.4, si $x' \in Q_{\delta'}^{\mu'}$ avec $\mu' \in GL_2(K)$, alors il existe $x \in Q_\delta$, $\mu \in GL_2(K)$ et $g \in SL_2(K)$, tel que $x' = x^{\mu \cdot g}$, donc, par le lemme 3.2, $Q_{\delta'} = C_{SL_2(K)}(x') = C_{SL_2(K)}(x)^{\mu \cdot g} = Q_\delta^{\mu \cdot g}$. C'est pourquoi, il est légitime dans le corollaire 3.5 de parler de Q_δ à conjugaison près pour $\delta \in K^\times/(K^\times)^2$.

Démonstration de la Proposition 3.4. • Si $A \in Q_1^{SL_2(K)}$, alors il existe $P \in SL_2(K)$ tel que :

$$A = P\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}P^{-1}$$

avec $a \in K^\times$. On a $tr(A) = a + a^{-1}$ donc $tr(A)^2 - 4 = (a + a^{-1})^2 - 4 = (a - a^{-1})^2$ et $tr(A)^2 - 4 \in (K^\times)^2$.

Réciproquement, soit $A \in SL_2(K)$ avec $tr(A)^2 - 4$ un carré de $K^\times$. Le polynôme caractéristique est $\chi_A(X) = X^2 - tr(A)X + 1$ et son discriminant $\Delta = tr(A)^2 - 4$ est un carré, donc χ_A a deux racines distinctes dans K et A est diagonalisable dans $GL_2(K)$. Il existe $P \in GL_2(K)$, et $D \in SL_2(K)$ diagonale telle que $A = PDP^{-1}$, si

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

on pose

$$\widetilde{P} = \begin{pmatrix} \frac{\alpha}{det(P)} & \beta \\ \frac{\gamma}{det(P)} & \delta \end{pmatrix}$$

et on a $\widetilde{P} \in SL_2(K)$ et $A = \widetilde{P}D\widetilde{P}^{-1} \in Q_1^{SL_2(K)}$.

• Si $A \in Q_\delta^{\mu \cdot SL_2(K)} \setminus \{I, -I\}$ avec $\mu \in GL_2(K)$, alors $tr(A) = 2a$ et il existe $b \neq 0$ telle que $a^2 - b^2\delta = 1$. Donc $tr(A)^2 - 4 = 4a^2 - 4 = 4(b^2\delta + 1) - 4 = (2b)^2\delta \in \delta \cdot (K^\times)^2$.

Réciproquement, on procède comme dans le cas réel avec la racine $i \in \mathbb{C}$. Le discriminant de χ_A, $\Delta = tr(A)^2 - 4$ est un carré dans $K(\sqrt{\delta})$, et le polynôme caractéristique χ_A a deux racines dans $K(\sqrt{\delta})$: $\lambda_1 = a + b\sqrt{\delta}$ et $\lambda_2 = a - b\sqrt{\delta}$ (avec $a, b \in K$). Pour les deux valeurs propres λ_1 et λ_2, les vecteurs propres associés de A sont :

$$v_1 = \begin{pmatrix} x + y\sqrt{\delta} \\ x' + y'\sqrt{\delta} \end{pmatrix} \quad \text{et} \quad v_2 = \begin{pmatrix} x - y\sqrt{\delta} \\ x' - y'\sqrt{\delta} \end{pmatrix}$$

Dans la base $\{(x, x'), (y, y')\}$, la matrice A s'écrit :

$$\begin{pmatrix} a & b \\ b\delta & a \end{pmatrix}$$

On peut conclure qu'il existe $P \in GL_2(K)$ tel que :

$$A = P\begin{pmatrix} a & b \\ b\delta & a \end{pmatrix}P^{-1}$$

On a prouvé que $Q_\delta^{GL_2(K)} = \left\{A \in SL_2(K) \mid tr(A)^2 - 4 \in \delta \cdot (K^\times)^2\right\} \bigcup \{I, -I\}$.

Etudions la conjugaison dans $GL_2(K)$ et dans $SL_2(K)$. Pour la démonstration, on note : $S = SL_2(K)$, $G = GL_2(K)$ et on pose :

$$Ext(S) = \{f \in Aut(S) \mid f(M) = M^P \text{ pour } M \in S, P \in G\}$$

$$Int(S) = \{f \in Aut(S) \mid f(M) = M^P \text{ pour } M \in S, P \in S\}$$

Soit $P, P' \in G$ et $M \in S$ alors :

$$M^P = M^{P'} \Leftrightarrow P^{-1}MP = P'^{-1}MP' \Leftrightarrow P'P^{-1}M = MP'P^{-1} \Leftrightarrow P'P^{-1} \in C_G(M)$$

Donc P et P' définissent le même automorphismes si et seulement si $P'P^{-1} \in C_G(S) = Z(G) = K^\times \cdot I_2$, alors $Ext(S) \cong GL_2(K)/Z(G) \cong PGL_2(K)$, et de manière similaire $Int(S) \cong SL_2(K)/Z(S) \cong PSL_2(K)$. Il est connu [31, remarque 2.10, chapitre IV] que $PGL_2(K)/PSL_2(K) \cong K^\times/(K^\times)^2$. Finalement $Int(S)$ est un sous-groupe normal d'indice fini $Ext(S)$, et il existe $\mu_1, ..., \mu_n \in GL_2(K)$ tels que :

$$Q_\delta^{GL_2(K)} = Q_\delta^{\mu_1 \cdot SL_2(K)} \cup ... \cup Q_\delta^{\mu_n \cdot SL_2(K)}$$

□

Théorème 3.6. *Les sous-groupes Q_1, Q_δ (pour $\delta \in K^\times \setminus (K^\times)^2$) et les conjugués extérieurs $Q_\delta^{\mu_i}$ (pour $\mu_1, ..., \mu_n \in GL_2(K)$) sont les seuls sous-groupes de Cartan de $SL_2(K)$ à conjugaison près.*

Démonstration. Il est clair que l'image d'un sous-groupe de Cartan par un automorphisme est encore un sous-groupe de Cartan. Pour la démonstration, on notera $S = SL_2(K)$ et B le sous-groupe suivant de $SL_2(K)$:

$$B = \left\{ \begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \mid t \in K^\times, u \in K \right\}$$

Avec ces notations, on peut facilement vérifier que pour $g \in U \setminus \{I, -I\}$ que $C_S(g) = U$ et $N_S(U) = B$. De plus il est clair que tout $q \in B$ peut être écrit comme $q = tu$ où $t \in Q_1$ et $u \in U$.

On considère C un sous-groupe de Cartan de $SL_2(K)$. Nous allons montrer que C est conjugué à Q_1 ou à l'un des Q_δ^μ (pour $\delta \in K^\times \setminus (K^\times)^2$ et $\mu \in GL_2(K)$). Premièrement prouvons que C ne peut contenir d'élément unipotent autre que I ou $-I$. Comme un conjugué d'un sous-groupe de Cartan est encore un sous-groupe de Cartan, il suffit de montrer que $C \cap U = \{I, -I\}$.

Raisonnons par l'absurde, soit $u \in C$ un élément de $U \setminus \{I, -I\}$, u est dans $C \cap B$. Si $\alpha \in N_S(C \cap B)$, alors on a $u^\alpha \in C \cap B$, et comme $tr(u^\alpha) = tr(u) = \pm 2$, u^α est dans U. C'est pourquoi $U = C_S(u) = C_S(u^\alpha) = C_S(u)^\alpha = U^\alpha$ et donc α est dans$N_S(U) = B$. Il vient que $N_S(C \cap B) \leq B$ et finalement $N_C(C \cap B) = C \cap B$. Par condition de normalisateur sur les groupes nilpotents $C \cap B$ ne peut être un sous-groupe propre de C, donc $C \cap B = C$ et $C \leq B$.

Il est connu (voir par exemple [43, Chapter 4, Theorem 2.9]) que si C est un groupe nilpotent et si $H \trianglelefteq C$ est un sous-groupe normal non trivial, alors $H \cap Z(C)$ n'est pas réduit à l'élément neutre. On suppose que $C \not\leq U^+$, comme $C \leq B = N_S(U^+)$, $C \cap U^+$ est normal dans C, et donc $C \cap U^+$ contient un élément non trivial x du centre $Z(C)$. Pour $q \in C \setminus U^+$, il y a $t \in Q_1 \setminus \{I\}$ et $u \in U$ tel que $q = tu$. Nous avons $[x, q] = I$, comme $[x, tu] = [x, u][x, t]^u$, on a $[x, t] = I$ et $t = -I$ car $C_S(x) = U$. C'est pourquoi $C \leq U$. Puisque C est nilpotent maximal et U abélien, $C = U$. Mais U ne peut pas être un sous-groupe de Cartan car il est d'indice infini dans son normalisateur B. Absurde.

Comme C ne contient pas d'élément unipotent, C intersecte un conjugué de Q_1 ou de l'un des Q_δ^μ (pour $\delta \in K^\times \setminus (K^\times)^2$ et $\mu \in GL_2(K)$) par le corollaire 3.5, on note Q ce sous-groupe. Montrons que $C = Q$. Soit x dans $C \cap Q$, et $\alpha \in N_C(C \cap Q)$, alors $x^\alpha \in Q$, et par le lemme 3.2, $Q = C_S(x^\alpha) = C_S(x)^\alpha = Q^\alpha$. Ainsi $\alpha \in N_S(Q)$, et $N_C(C \cap Q) \leq N_S(Q)$.

Premier cas Q est un conjugué de Q_1, alors $N_S(Q) = Q \cdot < w' >$ où $w' = w^g$ si $Q = Q_1^g$. On a aussi $w'^2 \in Q$ et $t^{w'} = t^{-1}$ pour $t \in Q$. On peut vérifier que $N_S(Q \cdot < w' >) = Q \cdot < w' >$, si $w' \in C$ alors $N_C(Q \cdot < w' > \cap C) = Q \cdot < w' > \cap C$, par la condition de normalisateur $C \leq Q \cdot < \omega' >$. Si n est le degrès de nilpotence de C, et $t \in C \cap Q$ alors $[t, w', w', ..., w'] = t^{2^n} = 1$, donc t est une racine $(2^n)^{\text{ième}}$ de l'unité, donc $C \cap Q$ et $C = (C \cap Q) \cdot < w >$ sont finis, ce qui contredit l'infinité des sous-groupes de Cartan. Donc $w' \notin C$. Alors $N_C(Q \cap C) \leq Q \cap C$, il vient, par la condition de normalisateur, que $C \leq Q$, et par maximalité de C, on a $C = Q$.

Second cas Q est un conjugué de Q_δ (pour $\delta \in K^\times \setminus (K^\times)^2$), alors $N_S(Q) = Q$. De manière similaire on a $C = Q$.

□

Corollaire 3.7. *Soit H un sous-groupe nilpotent infini de $SL_2(K)$, alors H est un sous-groupe d'un conjugué de U, Q_1 ou Q_δ (pour un certain $\delta \in K^\times/(K^\times)^2$).*

Démonstration. La demonstration précédente montre que si H est nilpotent et intersecte (à conjuguaison près) U, Q_1 ou Q_δ, alors $H \leq U$, $H \leq Q_1$ ou $H \leq Q_\delta$ respectivement. On conclus par le corollaire 3.5 □

Remarque. En particulier, tout sous-groupe nilpotent de $SL_2(K)$ est commutatif.

Pour X un sous-ensemble de K^n, on note $\overline{X}^K$ la clôture de Zariski de X dans K^n, (c'est-à-dire l'intersection de tous les sous-ensembles algébriques de K^n contenant X), et $\overline{X}^{\widetilde{K}^{alg}}$ la clôture de X dans $\widetilde{K}^{alg\ n}$. On sait par [8, Chap. II, Sect. 5, Théorème 3] que si H est un sous-groupe de $GL_n(K)$ alors $\overline{H}^K$ et $\overline{H}^{\widetilde{K}^{alg}}$ sont des groupes algébrique et $\overline{H}^K = GL_n(K) \cap \overline{H}^{\widetilde{K}^{alg}}$. Pour Y un groupe algébrique au dessus d'un corps K, on note Y° la composante connexe algébrique de Y, c'est à dire l'intersection de de tous les sous-groupes algébriques d'indice fini de Y. Par le fait 1.29 c'est le plus petit sous-groupe algébrique d'indice fini dans Y.

Proposition 3.8. *Soit H un sous-groupe résoluble maximal $SL_2(K)$. Alors H est le nomalisateur d'un sous-groupe de Cartan ou un conjugué du groupe B.*

Démonstration. Notons $\overline{H}^\circ$ la composante algébriquement connexe de la clôture de Zariski de H dans $SL_2(\widetilde{K}^{alg})$. Par [5, 2.4] $\overline{H}^\circ$ est un sous-groupe connexe résoluble de $SL_2(\widetilde{K}^{alg})$, donc $\overline{H}^\circ$ est un conjugué d'un sous-groupe de $\overline{B}$ [5, Theorem 11.1], où

$$\overline{B} = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in SL_2(\widetilde{K}^{alg}) \mid a \in \widetilde{K}^{alg\times} \text{ et } b \in \widetilde{K}^{alg} \right\}$$

Si $H \leq \overline{H}^\circ$, par le corollaire 3.5 il y a deux possibilités : soit $\overline{H}^\circ$ contient uniquement des éléments semi-simples, soit il contient des éléments unipotents non triviaux. Dans le premier cas $\overline{H}^\circ$ est un tore, donc H est aussi un tore dans $SL_2(K)$, i.e. H est un sous-groupe de Cartan (par maximalité). Dans le second cas, on note $(\overline{H}^\circ)_u$ l'ensemble de tous les éléments unipotents de $\overline{H}^\circ$. On sait par le fait 1.34, que $(\overline{H}^\circ)_u$ est un sous-groupe de $\overline{H}^\circ$ et $\overline{H}^\circ$ normalise $(\overline{H}^\circ)_u$. On peut observer que $H_u = (\overline{H}^\circ)_u \cap H$, donc H normalise H_u et H est un conjugué de B.

Sinon, $H \cap \overline{H}^\circ$ est un sous-groupe normal d'indice fini dans H. On sait que $\overline{H}^\circ$ est conjugué à un sous-groupe de $\overline{B}$, i.e. $\overline{H}^\circ \leq \overline{B}^g$ où $g \in SL_2(\widetilde{K}^{alg})$. On peut supposer que $g = I$ et si $H \not\leq \overline{B}$, alors il existe $h \in H$ tel que $\overline{B}^h \neq \overline{B}$. C'est pourquoi $H \cap \overline{H}^\circ \leq \overline{B}^h \cap \overline{B}$, or $\overline{B}^h \cap \overline{B}$ est un tore, il vient que H normalise le tore $H \cap \overline{H}^\circ$, i.e. par maximalité, H est le normalisateur d'un sous-groupe de Cartan. □

Fait 3.9. *Du fait 1.34, on peut en déduire que les sous-groupes définissables de B sont les suivants :*

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in SL_2(K) \mid a \in P \text{ et } b \in Z \right\}$$

où P est un sous-groupe définissable de $K^\times$ et Z est un sous-groupe définissable de K^+ tel que $P \cdot Z \subseteq Z$.

Le corollaire 3.7 et la proposition 3.8 sonts vrais pour tout sous-groupe de $SL_2(K)$ sans condition dédéfinissabilité ou d'algébricité. Q_1, Q_δ, U et B apparaissent comme des sous-groupes cadres contenant, à conjugaison près, tous les sous-groupes nilpotents ou résolubles de $SL_2(K)$. Ces sous-groupes cadres sont définissables avec paramètre dans le pure langage des groupes : tout sous-groupe nilpotent Q_1, Q_δ ou U est le centralisateur d'un de ses éléments non central, et $B = N_S(C_S(u))$ pour $u \in U \setminus \{-I, I\}$. Ils sont naturellement définissable dans K avec le langage des corps. Avant de nous pencher sur la structure fine des sous-groupes définissables dans $\mathcal{Q}_p$ pour le langage des corps. Remarquons que les sous-groupes définissables dans le langage des corps sont interprétables dans $SL_2(K)$ pour le pure langage des groupes.

Proposition 3.10. *Soit K un corps infini de caractéristique différente de 2. Alors le corps $(K, +, -, \cdot, 0, 1)$ est interprétable dans le pur groupe $(SL_2(K), \cdot)$.*

Démonstration. Le sous-groupe Q_1 agit sur U :

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & t^2 u \\ 0 & 1 \end{pmatrix}$$

Pour la démonstration, nous identifions la matrice $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \in Q_1$ avec $t \in K^\times$ et nous choisissons un élément u_0 dans U et son inverse u_1.

On considère A l'ensemble $Q_1 \times Q_1$ quotienté par la relation d'équivalence :

$$(t_0, t_1) \sim (t'_0, t'_1) \quad \text{ssi} \quad u_0^{t_0} \cdot u_1^{t_1} = u_0^{t'_0} \cdot u_1^{t'_1} \text{ dans } SL_2(K) \quad (\text{ i.e. } \quad t_0 - t_1^2 = t_0'^2 - t_1'^2 \text{ dans } K)$$

Il nous reste à contruire une bijection entre A et K et à définir l'addition et la multplication du corps dans A. Remarquons premièrement que pour tout $x \in K$

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$$

On voit alors que l'application $\varphi : A \longrightarrow K$, $(t_0, t_1) \mapsto t_0^2 - t_1^2$ est une bijection.

Enfin l'addition et la multiplication de K sont données par :

$$(t_0, t_1) + (t_0', t_1') = (t_0'', t_1'') \quad \text{ssi} \quad u_0^{t_0} u_1^{t_1} u_0^{t_0'} u_1^{t_1'} = u_0^{t_0''} u_1^{t_1''}$$

$$(t_0, t_1) \cdot (t_0', t_1') = (t_0'', t_1'') \quad \text{ssi} \quad u_0^{t_0 t_0'} u_0^{t_1 t_1'} u_1^{t_0 t_1'} u_1^{t_1 t_0'} = u_0^{t_0''} u_1^{t_1''}$$

□

3.2 Le cas p-adiquement clos

Dans cette section $\mathcal{Q}_p$ est un corps p-adiquement clos.

3.2.1 Sous-groupes définissables et dimension

Remarque. On peut aisément vérifier qu'on a $\dim Q_1 = \dim Q_\delta = \dim U = 1$, et $\dim B = 2$. Alors le corollaire 3.7 et la proposition 3.8 montrent que :

1. Si H est un sous-groupe définissable nilpotent de $SL_2(\mathcal{Q}_p)$ alors $\dim H = 1$.
2. Si H est un sous-groupe définissable résoluble de $SL_2(\mathcal{Q}_p)$ alors $\dim H \leq 2$.

La proposition suivante nous en donne la réciproque.

Proposition 3.11. *$\mathcal{Q}_p$ est un corps p-adiquement clos. Soit H un sous-groupe définissable infini de $SL_2(\mathcal{Q}_p)$. On a les équivalences suivantes :*

1. $\dim H = 1$ *si et seulement si H est commutatif ou H est un sous-groupe d'un conjugué de $N_{SL_2(\mathcal{Q}_p)}(Q_1)$.*
2. $\dim H = 2$ *si et seulement si H est un sous-groupe non nilpotent d'un conjugué de B.*
3. $\dim H = 3$ *si et seulement si H est non résoluble.*

Démonstration. Par la proposition 3.8, il suffit de montrer les deux premiers points : On note comme précédemment $\overline{H}^\circ$, la composante algébriquement connexe de la clôture de Zariski de H dans $\widetilde{\mathcal{Q}_p}^{alg}$.

1. $\overline{H}^\circ$ est de dimension 1 dans $\widetilde{\mathcal{Q}_p}^{alg}$, donc par [21, 20.1], $\overline{H}^\circ$ est commutatif.
   - si $H < \overline{H}^\circ$, H est commutatif ;
   - si non, $H \cap \overline{H}^\circ$ est un sous-groupe normal d'indice fini dans H, alors H normalise un sous-groupe commutatif d'indice fini. Donc $H \leq N_{SL_2(\mathcal{Q}_p)}(T)$ où T est conjugué à Q_1.
2. Supposons que $\overline{H}^\circ$ est de dimension 2 dans $\widetilde{\mathcal{Q}_p}^{alg}$, en particulier c'est un groupe connexe de rang de Morley fini, par [7, Theorem 6], $\overline{H}^\circ$ est résoluble. On sait par la démonstration de la proposition 3.8, que H est un conjugué d'un sous-groupe de B.

□

3.2.2 Sous-groupes commutatifs définissables

Dans cette section, nous nous intéressons à la description des sous-groupes définissables commutatifs de $SL_2(\mathcal{Q}_p)$ où $\mathcal{Q}_p$ est un corps p-adiquement clos. Définissable signifie ici définissable dans $\mathcal{L}_R$. Nous savons déjà qu'ils sont, à conjugaison près, des sous-groupes de U, Q_1 ou Q_δ (avec $\delta \in \mathcal{Q}_p^\times \setminus (\mathcal{Q}_p^\times)^2$). Il nous reste alors à décrire les sous-groupes définissables de U, Q_1 et Q_δ.

Nous savons que $U^+ \cong \mathcal{Q}_p^+$, alors les sous-groupes définissables de U^+ correspondent aux sous-groupes définissables de $\mathcal{Q}_p^+$. Un sous-groupe de $\mathcal{Q}_p^+$ est infini donc de dimension 1, ainsi c'est un sous-groupe ouvert de $\mathcal{Q}_p^+$. Les sous-groupes ouverts de $\mathbb{Q}_p^+$ sont de la forme $p^n\mathbb{Z}_p$ avec $n \in \mathbb{Z}$ [34, Lemma 3.2], donc ce sont les seuls sous-groupes définissables de $\mathbb{Q}_p^+$. Pour $\mathcal{Q}_p$ un corps p-adiquement clos, nous avons la même propriété : les sous-groupes définissables de $\mathcal{Q}_p^+$ sont de la forme $a_\gamma \mathcal{Z}_p$ où $v_p(a_\gamma) = \gamma \in \Gamma$.

Pour $Q_1 \cong \mathcal{Q}_p^\times$, montrons le résultat suivant :

Proposition 3.12. *Soit $\mathcal{Q}_p$ un corps p-adiquement clos et H un sous-groupe définissable infini de $\mathcal{Q}_p^\times$.*

1. *Si H est borné, alors il existe $\gamma_0 \in \Gamma^{>0}$ et $a_{\gamma_0} \in \mathcal{Q}_p$ avec $v_p(a_{\gamma_0}) = \gamma_0$ tel que H contient $1 + a_{\gamma_0}\mathcal{Z}_p$ comme sous-groupe d'indice fini au plus $(p-1)$ pour $p \neq 2$ (et au plus 2, pour $p = 2$).*
2. *Si H n'est pas borné alors il existe $\gamma_0 \in \Gamma^{>0}$, $n \in \mathbb{N}$ et $\{a_\gamma\}_{\gamma\in\Gamma} \subseteq \mathcal{Q}_p$ et $b_{\gamma_0} \in \mathcal{Q}_p$ avec $v_p(a_\gamma) = \gamma$ et $v_p(b_{\gamma_0}) = \gamma_0$, tel que H contient $\{a_\gamma; \gamma \in n\Gamma\} \cdot (1 + b_{\gamma_0}\mathcal{Z}_p)$ comme sous-groupe d'indice fini au plus $(p-1)$ pour $p \neq 2$ (et au plus 2, pour $p = 2$).*

Démonstration. 1. Supposons que $p \neq 2$ et travaillons dans $\mathbb{Q}_p$. Comme H est borné, $H \leq \mathbb{Z}_p^\times$. Notons H_0 la partie sans torsion de H, alors $H_0 \leq 1 + p\mathbb{Z}_p$. Il est bien connu que $1 + p\mathbb{Z}_p \cong (\mathbb{Z}_p, +)$, nous allons suivre le raisonnement de Pillay dans $\mathbb{Z}_p$ [34, Lemma 3.2]. Comme $\dim H_0 = 1 = \dim(1 + p\mathbb{Z}_p)$, H_0 contient un voisinage ouvert de 1. Ainsi il existe $n \in \mathbb{N}$ tel que $1 + p^n\mathbb{Z}_p \subseteq H_0$. Soit n_0 le plus petit tel n. Montrons que $H_0 = 1 + p^{n_0}\mathbb{Z}_p$. Raisonnons par l'absurde, et considérons x dans H_0 tel que $x \notin 1 + p^{n_0}\mathbb{Z}_p$. Il est facile de remarquer que si $x \in 1 + p^n\mathbb{Z}_p$, alors $x^p \in 1 + p^{n+1}\mathbb{Z}_p$, donc en remplacant x par une puissance $p^{\text{ième}}$ correcte de x, on peut supposer que $x \in 1 + p^{n_0-1}\mathbb{Z}_p$. Comme $(1 + p^{n_0-1}\mathbb{Z}_p)/(1 + p^{n_0}\mathbb{Z}_p) \cong \mathbb{Z}/p\mathbb{Z}$ et $\{x^i; 0 \leq i < p\}$ forme un système complet de représentants des classes modulo $1 + p^{n_0}\mathbb{Z}_p$ dans $1 + p^{n_0-1}\mathbb{Z}_p$, donc $1 + p^{n_0-1}\mathbb{Z}_p \subseteq H_0$, ce qui est absurde et $H_0 = 1 + p^{n_0}\mathbb{Z}_p$. Le nombre d'éléments de torsion de H est fini et au plus $(p-1)$, donc H_0 est d'indice fini au plus $(p-1)$ dans H. Alors, comme $1 + p^n\mathbb{Z}_p$ est définissable, on a montré que

$$\mathbb{Q}_p \vDash \forall \bar{a}\ (\text{"}\varphi(x, \bar{a}) \text{ définit un sous groupe de } \mathbb{Q}_p^\times\text{"}) \to \exists b\ \exists x_1, ..., x_{p-1} \bigwedge_{0\leq i\leq p-1} \varphi(x_i, \bar{a}) \wedge \forall y\ (\varphi(y, \bar{a}) \to \bigvee_{0\leq i\leq p-1} y \cdot x_i^{-1} \in 1 + b\mathbb{Z}_p)$$

Alors la propriété est vraie pour tout corps p-adiquement clos, ce qui termine la démonstration. Pour $p = 2$, la même démonstration fonctionne en remplaçant $1 + p\mathbb{Z}_p$ par $1 + 4\mathbb{Z}_2$.

2. On appelle $H_1 = H \cap \mathcal{Z}_p^\times$. On peut aisément vérifier que deux éléments de H sont dans la même classe modulo H_1 si et seulement si ils ont la même valuation. De plus, comme Γ est un $\mathbb{Z}$-groupe, et $v_p(H)$ est un sous-groupe définissable de Γ alors $v_p(H)$ est de la forme $n\Gamma$ pour un certain $n \in \mathbb{N}$. En effet par l'élimination des quantificateurs dans les groupes de Presburger (fait 1.18), on sait que les ensembles définissables de Γ sont des unions finies d'intervalles ou d'ensembles de la forme $n\Gamma$ pour $n \in \mathbb{Z}$; donc les sous-groupes définissables sont de la forme $n\Gamma$. Alors on peut choisir $a_\gamma \in H$ tel que $v_p(a_\gamma) = \gamma$ et $\{a_\gamma ; \gamma \in n\Gamma\}$ forme un ensemble de représentants des classes modulo H_1 dans H. On sait par 1. qu'il existe $\gamma_0 \in \Gamma$ et $b_{\gamma_0} \in K$ avec $v_p(b_{\gamma_0}) = \gamma_0$ tel que $1 + b_{\gamma_0}\mathcal{Z}_p$ est d'indice fini au plus $p-1$ dans H_1 si $p \neq 2$ (et au plus 2 si $p = 2$), il en est de même pour $\{a_\gamma ; \gamma \in n\Gamma\} \cdot (1 + b_{\gamma_0}\mathcal{Z}_p)$ dans H.

□

Remarque. La proposition 3.12 ne dit pas que le sous-groupe $\{a_\gamma ; \gamma \in n\Gamma\} \cdot (1 + b_{\gamma_0}\mathcal{Z}_p)$ est définissable. Il arrive qu'il soit définissable, par exemple le sous-groupe $P_{p-1}(\mathbb{Q}_p^\times) = \{x \in \mathbb{Q}_p^\times \mid \exists y\ y^{p-1} = x\} = \{p^n ; n \in (p-1)\mathbb{Z}\} \cdot (1 + p\mathbb{Z})$ est définissable. La question de la définissabilité de $\{a_\gamma ; \gamma \in n\Gamma\} \cdot (1 + b_{\gamma_0}\mathcal{Z}_p)$ est encore ouverte.

Le but est maintenant d'étudier les sous-groupes définissables de Q_δ. On a déjà vu (remarque p. 34) que les sous-groupes Q_δ sont définissablement isomorphes aux tores anisotropes de dimension 1, dont on a décrit les sous-groupes définissable dans le cas de $\mathbb{Q}_p$ (Propositions 2.6 et 2.6 bis).

On peut généraliser ces résultats à un corps p-adiquement clos $\mathcal{Q}_p$. On considère une suite $(a_\gamma)_{\gamma \in \Gamma}$ d'éléments de $\mathcal{Q}_p$ indéxés par le groupe de valeur Γ tels que $v_p(a_\gamma) = \gamma$. On a, pour tout $\gamma \in \Gamma$:

$$a_\gamma \mathcal{Z}_p = \{x \in \mathcal{Q}_p \mid v_p(x) \geq \gamma\}$$

On défini l'équivalent des $Z_{n,\delta}$ comme :

$$Z_{\gamma,\delta} := \left\{ \begin{pmatrix} a & b \\ b\delta & a \end{pmatrix} \in SL_2(\mathcal{Q}_p) \mid b \in a_\gamma \mathcal{Z}_p, a \in 1 + a_{2\gamma}\delta\mathcal{Z}_p \text{ et } a^2 - b^2\delta = 1 \right\}$$

Nous avons le résultat suivant :

Théorème 3.13. *Si $\mathcal{Q}_p$ est un corps p-adiquement clos. Pour $p \neq 2$ et $\delta \in \{p, \alpha p\}$ (respectivement pour $\delta = \alpha$).*

1. *$Z_{0,\delta}$ (respectivement $Z_{1,\delta}$) est d'indice fini dans Q_δ.*
2. *Les $Z_{\gamma,\delta}$ sont les seuls sous-groupes définissables de $Z_{0,\delta}$ (respectivement $Z_{1,\delta}$).*

Démonstration. La propriété étant vrai pour $\mathbb{Q}_p$ (Propositions 2.6 et 2.6 bis), on raisonne par équivalence élémentaire. Les sous-groupes $Z_{\gamma,\delta}$ sont uniformément définissables par $\varphi(x, a_\gamma)$. Comme Q_δ est définissable sans paramètre, pour toute formule $\psi(x, \bar{b})$ à paramètre $\bar{b}$ dans $\mathcal{Q}_p$, on a :

$$\mathbb{Q}_p \vDash \exists g_1, ..., g_n \in Q_\delta \forall x \in Q_\delta \quad \bigvee_{i=1}^{n} \varphi(g_i^{-1}x, 1)$$

$\mathbb{Q}_p \models \forall \bar{b}$ ("$\psi(x,\bar{b})$ définit un sous-groupe de Q_δ") $\longrightarrow \exists a \forall x$ $(\psi(x,\bar{b}) \longleftrightarrow \varphi(x,a))$

On peut en déduire la propriété pour $\mathcal{Q}_p$. □

Pour $p = 2$, on définit de même :

$$Z_{\gamma,\delta} := \left\{ \begin{pmatrix} a & b \\ b\delta & a \end{pmatrix} \in SL_2(K) \mid b \in a_\gamma \mathcal{Z}_2, a \in 1 + a_{2\gamma-1}\delta\mathcal{Z}_2 \text{ et } a^2 - b^2\delta = 1 \right\}$$

on a encore :

Théorème 3.13 bis. *Si $\mathcal{Q}_2$ est un corps p-adiquement clos, pour $p = 2$ et si $v_p(\delta) = 1$ (respectivement si $v_p(\delta) = 0$).*

1. *$Z_{1,\delta}$ (respectivement $Z_{2,\delta}$) est d'indice fini dans Q_δ.*
2. *Les $Z_{\gamma,\delta}$ sont les seuls sous-groupes définissables de $Z_{1,\delta}$ (respectivement $Z_{2,\delta}$).*

Remarque. Par le fait 3.9, nous connaissons alors les sous-groupes définissables de B.

3.2.3 Sous-groupes définissables non résolubles

Pour $x \in SL_2(\mathcal{Q}_p)$, on appelle valuation de x le minimum $v_p(x)$ des valuations p-adiques de ces coefficients. Un sous-groupe H de $SL_2(\mathcal{Q}_p)$ est dit *borné* s'il existe $m \in \Gamma$ tel que :

$$\forall x \in H \quad v_p(x) \geq m$$

Remarque. Pour $\mathbb{Q}_p$, et pour H un sous-groupe définissable de $SL_2(\mathbb{Q}_p)$, *borné* signifie exactement *compact*.

Démonstration. Par [39, chapitre 2, 3.2], les compacts de $\mathbb{Q}_p^n$ sont les fermés bornés. Il suffit donc de remarquer qu'un sous-groupe définissable de $SL_2(\mathbb{Q}_p)$ est fermé. En effet, si G est un sous-groupe définissable de $SL_2(\mathbb{Q}_p)$ alors $\overline{G}^{\mathbb{Q}_p}$ est un fermé de Zariski, donc fermé pour la topologie ultramétrique ; de plus $\dim G = \dim \overline{G}^{\mathbb{Q}_p}$ donc G est d'intérieur non vide dans $\overline{G}^{\mathbb{Q}_p}$, donc G est fermé dans $\overline{G}^{\mathbb{Q}_p}$. □

Théorème 3.14. *Pour $\mathcal{Q}_p$ un corps p-adiquement clos et H un sous-groupe définissable de $SL_2(\mathcal{Q}_p)$. Si H est non résoluble et non borné, alors $H = SL_2(\mathcal{Q}_p)$.*

Le théorème reste vrai pour tout corps valué K hensélien de caractéristique 0 dont le groupe de valeur est un $\mathbb{Z}$-groupe. Par exemple, K peut être une extension finie d'un corps-adiquement clos.

Démonstration. H n'est pas résoluble, donc par la proposition 3.11, on a $\dim H = 3 = \dim SL_2(\mathcal{Q}_p)$, et H contient un voisinage de l'identité (fait 1.24), alors

$$\begin{pmatrix} 1 + a_{\gamma_1}\mathcal{Z}_p & a_{\gamma_2}\mathcal{Z}_p \\ a_{\gamma_3}\mathcal{Z}_p & 1 + a_{\gamma_4}\mathcal{Z}_p \end{pmatrix} \cap SL_2(\mathcal{Q}_p) \subseteq H$$

avec $a_{\gamma_i} \in \mathcal{Q}_p$ tels que $v(a_{\gamma_i}) = \gamma_i$. En particulier :

$$\begin{pmatrix} 1 & a_{\gamma_2}\mathcal{Z}_p \\ 0 & 1 \end{pmatrix} \subseteq H$$

On note $Z = a_{\gamma_2}\mathcal{Z}_p$.

H n'est pas borné donc, par le corollaire 3.5 en raisonnant à conjugaison près, $H \cap Q_1$ ou $H \cap U$ n'est pas borné (on a vu, en effet, dans la remarque p. 23 que les Q_δ pour $\delta \in \mathcal{Q}_p^\times \setminus (\mathcal{Q}_p^\times)^2$ étaient bornés)

1. Si $H \cap Q_1$ n'est pas borné : on note P le sous-groupe de $K^\times$ tel que :

$$H \cap Q_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in SL_2(\mathcal{Q}_p) \mid a \in P \right\}$$

Soit $x \in \mathcal{Q}_p$ et $t \in P$ tel que $v(t) < v(xa_{\gamma_2}^{-1})$. Alors il existe $u \in \mathcal{Z}_p$ tel que $x = ta_{\gamma_2}u$. Il vient que $P \cdot Z = \mathcal{Q}_p$. De

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}\begin{pmatrix} t^{-1} & u \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & tu \\ 0 & 1 \end{pmatrix}$$

on en déduit que $U^+ \subseteq H$, on peut montrer la même chose pour la transposé ${}^tU^+ \subseteq H$. Par

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -t^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix} \tag{3.1}$$

$$\text{et} \quad \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \tag{3.2}$$

on conclut que $w \in H$ et $Q_1 \subseteq H$. Finalement $B \subseteq H$. La décomposition de Bruhat [5, 14.12] pour $SL_2(\mathcal{Q}_p)$ affirme que $SL_2(\mathcal{Q}_p) = B \sqcup BwB$, où w est la matrice définie page 34. Il vient que $H = SL_2(\mathcal{Q}_p)$.

2. Si $H \cap U^+$ est non borné, alors $U^+ \subseteq H$ parce que chaque sous-groupe propre définissable de U^+ est borné. On sait aussi que

$$\begin{pmatrix} 1 & 0 \\ a_{\gamma_3}\mathcal{O} & 1 \end{pmatrix} \subseteq H$$

Si $\gamma_3 \leq 0$, alors par (3.1), $w \in H$. Sinon, on prend $t \in K$ tel que $v(t) \geq \gamma_3$, alors par (3.1) :

$$\begin{pmatrix} 0 & -t^{-1} \\ t & 0 \end{pmatrix}, \begin{pmatrix} 0 & -t^{-2} \\ t^2 & 0 \end{pmatrix} \in H \text{ et } \begin{pmatrix} 0 & -t^{-1} \\ t & 0 \end{pmatrix}\begin{pmatrix} 0 & -t^{-2} \\ t^2 & 0 \end{pmatrix} = \begin{pmatrix} -t & 0 \\ 0 & -t^{-1} \end{pmatrix} \in H$$

Dans tous les cas, H contient un élément de Q_1 de valuation non-nulle. Comme Γ est un $\mathbb{Z}$-groupe, tout sous-groupe définissable de Γ est soit trivial soit non borné. En effet, pour $\varphi(x, \bar{a})$ une formule, on a

$$\mathbb{Z} \vDash \forall \bar{a}\ \text{"}\varphi(x,\bar{a}) \text{ definit un sous-groupe de } \mathbb{Z}\text{"} \longrightarrow \forall x\ [\varphi(x,\bar{a}) \to \exists y\ (y > x \wedge \varphi(y,\bar{a}))]$$

Comme $v(P)$ est un sous-groupe définissable non trivial de Γ, il est non borné et $H \cap Q_1$ est non borné. On conclut en utilisant le premier cas.

□

Remarque. Une conséquence du théorème précédent est que $SL_2(\mathcal{Q}_p)$ est définissablement connexe (cela signifie qu'il ne contient pas de sous-groupe propre définissable d'indice fini).

Fait 3.15 ([41, Chap II, 1.3, Proposition 2])**.** *Pour $\mathcal{Q}_p$ un corps p-adiquement clos et H un sous-groupe définissable de $SL_2(\mathcal{Q}_p)$. Si H est borné alors H est contenu dans un conjugué de $SL_2(\mathcal{Z}_p)$.*

On note :

$$H_{\gamma,\eta_1,\eta_2} = \begin{pmatrix} 1+a_\gamma\mathcal{Z}_p & a_{\eta_1}\mathcal{Z}_p \\ a_{\eta_2}\mathcal{Z}_p & 1+a_\gamma\mathcal{Z}_p \end{pmatrix} \cap SL_2(\mathcal{Q}_p) \quad \text{avec } v_p(a_\gamma)=\gamma \text{ et } v_p(a_{\eta_i})=\eta_i$$

Si $\eta_1+\eta_2 \geq \gamma \geq 0$, alors H_{γ,η_1,η_2} est un sous-groupe de $SL_2(\mathcal{Q}_p)$, et c'est un voisingage de l'identité. Les groupes de la forme H_{γ,η_1,η_2} sont des exemples de sous-groupes définissables non résolubles et bornés de $SL_2(\mathcal{Q}_p)$. La proposition suivante nous donne une sorte de réciproque de ce fait :

Proposition 3.16. *Soit $\mathcal{Q}_p$ un corps p-adiquement clos et H un sous-groupe définissable de $SL_2(\mathcal{Q}_p)$. Si H est borné et non résoluble et si w normalise H, alors à conjuguaison près :*

- *soit, il existe $\gamma,\eta \in \Gamma$ et $a_\gamma, a_\eta \in K$ avec $v_p(a_\gamma)=\gamma$ et $v_p(a_\eta)=\eta$ tels que $H_{\gamma,\eta,\eta}$ est un sous-groupe de H d'indice fini au plus $2(p-1)$ si $p \neq 2$ (ou au plus 4 si $p=2$), où :*

$$H_{\gamma,\eta,\eta} = \begin{pmatrix} 1+a_\gamma\mathcal{Z}_p & a_\eta\mathcal{Z}_p \\ a_\eta\mathcal{Z}_p & 1+a_\gamma\mathcal{Z}_p \end{pmatrix} \cap SL_2(\mathcal{Q}_p) \quad \text{où } 2\eta \geq \gamma > 0$$

- *soit $H = SL_2(\mathcal{Z}_p)$.*

Démonstration. Raisonnons dans $\mathbb{Q}_p$, à conjugaison près, on peut supposer que $H \leq SL_2(\mathbb{Z}_p)$. On note $B_H = B \cap H$, on sait par le fait 3.9, que :

$$B_H = \begin{pmatrix} P & Z \\ 0 & P \end{pmatrix} \quad \text{avec } Z = p^n\mathbb{Z}_p \text{ et } 1+p^k\mathbb{Z}_p \leq P \text{ d'indice fini au plus } (p-1)$$

pour un certain $n \geq 0$ et $k \geq 1$.

• Si $2n \geq k$, alors il existe un sous-groupe H' tel que $B_H \leq H' \leq H$ et tel que H' soit de la forme $\begin{pmatrix} P & Z \\ Z & P \end{pmatrix}$ (il suffit de prendre $H' = B_H \cdot V$ où V est un voisinage de l'identité dans $SL_2(\mathbb{Q}_p)$). Quitte à remplacer H' par $\pm H'$, on peut supposer que $-I \in H'$. Comme $H'^w = H'$, le sous-groupe $H' \cup wH'$ contient H' comme sous-groupe d'indice 2. De même, on peut supposer que $-I \in H$ et H est d'indice au plus 2 dans le sous-groupe $H \cup wH$. Par la décomposition de Bruhat [5, 14.12], $H \cup wH = B_H \cup B_H w B_H$. Comme $B_H \subseteq H'$ et $w \in H' \cup wH'$, on a $H \cup wH = H' \cup wH'$, alors H' est un sous-groupe d'indice au plus 2 dans H. Pour

$$\begin{pmatrix} x(1+p^k a) & p^n b \\ p^n c & x'(1+p^k d) \end{pmatrix} \in H'$$

où x, x' sont des racines $p^{\text{ième}}$ de l'unité et a, b, c, $d \in \mathbb{Z}_p$, et comme le déterminant est 1, on voit que $xx' = 1$, et donc

$$\begin{pmatrix} x(1+p^k a) & p^n b \\ p^n c & x'(1+p^k d) \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x' \end{pmatrix} \begin{pmatrix} 1+p^k a & x^{-1}p^n b \\ x'^{-1}p^n c' & 1+p^k d \end{pmatrix}$$

En d'autres termes, $H_{k,n,n}$ est un sous-groupe d'indice fini au plus $(p-1)$ dans H' donc au plus $2(p-1)$ dans H.

• Si $2n < k$ et $n > 0$, alors B_H et B_H^w engendre un sous-groupe H' de la forme $\begin{pmatrix} P' & Z \\ Z & P' \end{pmatrix}$ où P' est un sous-groupe de $\mathbb{Q}_p^\times$ avec $1 + p^{2n}\mathbb{Z}_p \leq P'$ d'indice fini au plus $(p-1)$ et $P < P'$. Ce qui est absurde, car $H' \cap B$ doit être contenu dans B_H.

• Si $2n < k$ et $n = 0$, alors $\begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \subseteq H$, et par l'action de w, $\begin{pmatrix} 1 & 0 \\ \mathbb{Z}_p & 1 \end{pmatrix} \subseteq H$.

Par (3.1) et (3.2) on peut conclure que $w \in H$, $\begin{pmatrix} \mathbb{Z}_p^\times & 0 \\ 0 & \mathbb{Z}_p^\times \end{pmatrix} \subseteq H$ et $\begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & \mathbb{Z}_p^\times \end{pmatrix} \subseteq H$.
Par la décomposition de Bruhat sur $SL_2(\mathbb{Z}_p)$, on a $H = SL_2(\mathbb{Z}_p)$.

Par équivalence élémentaire, on peut maintenant aisément déduire la proposition pour tous les corps p-diquement clos $\mathcal{Q}_p$: pour $\varphi(\bar{x}, \bar{a})$ une formule, comme $H_{\gamma,\eta,\eta}$ est définissable par $\psi(\bar{x}, \bar{b})$

$\mathcal{Q}_p \vDash \forall \bar{a}$ "$\varphi(\bar{x}, \bar{a})$ définit un sous-groupe borné de $SL_2(\mathcal{Q}_p)$ de dimension 3 et normalisé par w"

$$\longrightarrow \left[\exists \bar{b}\ \exists \bar{x}_1, ..., \bar{x}_{2(p-1)} \bigwedge_{0 \leq i \leq 2(p-1)} \varphi(\bar{x}_i, \bar{a}) \ \wedge\ \forall \bar{y}\ (\varphi(\bar{y}, \bar{a}) \to \bigvee_{0 \leq i \leq 2(p-1)} \psi(\bar{y} \cdot \bar{x}_i^{-1}, \bar{b})) \right]$$

□

Conjecture. *Pour $\mathcal{Q}_p$ un corps p-adiquement clos et H un sous-groupe définissable de $SL_2(\mathcal{Q}_p)$. Si H est borné et non résoluble et si w ne normalise pas H alors, à conjugaison près, il existe $\gamma, \eta_1, \eta_2 \in \Gamma$ tels que $H_{\gamma,\eta,\eta}$ est un sous-groupe de H d'indice fini au plus $2(p-1)$ si $p \neq 2$ (ou au plus 4 si $p = 2$).*

Le tableau 3.1 suivant résume la description de tous les sous-groupes définissables de $SL_2(\mathcal{Q}_p)$ à conjugaison près pour $\mathcal{Q}_p$ un corps p-adiquement clos :

Propriétés algébriques	Dimension	Sous-groupes cadres	Sous-groupes définissables dans $\mathcal{Q}_p$
Nilpotent	1	U and U_+	$\begin{pmatrix} 1 & a_\gamma \mathcal{Z}_p \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} \pm 1 & a_\gamma \mathcal{Z}_p \\ 0 & \pm 1 \end{pmatrix}$
	1	Q_1	virtuellement $\begin{pmatrix} 1 + a_{\gamma_0} \mathcal{Z}_p & 0 \\ 0 & 1 + a_{\gamma_0} \mathcal{Z}_p \end{pmatrix}$ ou $\begin{pmatrix} \{b_\gamma\}_{\gamma \in n\Gamma} \cdot (1 + a_{\gamma_0} \mathcal{Z}_p) & 0 \\ 0 & \{b_\gamma\}_{\gamma \in n\Gamma} \cdot (1 + a_{\gamma_0} \mathcal{Z}_p) \end{pmatrix}$
	1	Q_δ	$Z_{\gamma,\delta}$ pour $\gamma \in \Gamma^{>0}$
Résoluble non nilpotent	1	$N_G(Q_1) = Q_1 \cdot < w >$	
	2	B	$\begin{pmatrix} P & Z \\ 0 & P \end{pmatrix}$ avec $P \leq \mathcal{Q}_p^\times$, $Z \leq \mathcal{Q}_p^+$ et $P \cdot Z \subseteq Z$
Non résoluble, compact	3		contenu dans $SL_2(\mathcal{Z}_p)$
Non résoluble, non compact	3		$SL_2(\mathcal{Q}_p)$

TABLE 3.1 – Les sous-groupes définissables de $SL_2(\mathcal{Q}_p)$ à conjugaison près

Chapitre 4

Groupes linéaires définissables dans une structure p-minimale

Introduction

Dans le chapitre précédent nous avons décrit les sous-groupes définissables de $SL_2(\mathbb{Q}_p)$ pour le langage des corps. Une question naturelle est alors de se demander quels sont les sous-groupes définissables pour un langage plus riche. Un moyen efficace est alors d'étudier les enrichissement p-minimaux des corps p-adiquement clos. La notion de p-minimalité est l'équivalent pour les p-adiques de la notion de o-minimalité ; elle cherche à décrire les enrichissements tels que les ensembles définissables restent similaires aux ensembles $\mathcal{L}_R$-définissables. Un exemple courant est $\mathbb{Q}_p^{an}$, il s'agit de la structure $\mathbb{Q}_p$ où on a étendu le langage en rajoutant toutes les fonctions analytiques restreintes. Etudions les sous-groupes définissables de $SL_2(\mathbb{Q}_p^{an})$.

Remarque. Par [45] et [12], on sait que $\mathbb{Q}_p^{an}$ est équipé d'une notion de dimension au sens de van den Dries. De plus la dimension vérifie la propriété suivante :

$$\text{si } X \subseteq Y \text{ et } \dim X = \dim Y \quad \text{alors} \quad X \text{ est d'intérieur non vide dans } Y$$

Toutefois dans $\mathbb{Q}_p^{an}$ la dimension n'est pas compatible avec la clôture algébrique.

Alors pour K une $\mathcal{L}_{an}$ extension élémentaire de $\mathbb{Q}_p^{an}$ et H un sous-groupe infini définissable de $SL_2(K)$, on a les implications suivantes :

1. $\dim H = 1 \Leftarrow H$ est commutatif ou H est un sous-groupe d'un conjugué de $N_{SL_2(K)}(Q_1)$.
2. $\dim H = 2 \Leftarrow H$ est un sous-groupe non nilpotent d'un conjugué de B.
3. $\dim H = 3 \Rightarrow H$ n'est pas résoluble.

De plus les démonstrations de la partie 3.2.2 et 3.2.3 n'utilisant que la compatibilité de la dimension avec la topologie, les résultats sont transposables au cas $\mathbb{Q}_p^{an}$. Ainsi les sous-groupes commutatifs, nilpotents et résolubles de $SL_2(\mathbb{Q}_p^{an})$ seront les mêmes que $SL_2(\mathbb{Q}_p)$. On peut également énoncer un résultat similaire au théorème 3.14 et à la proposition 3.16 en remplaçant "résoluble" par de "dimension 3".

Regardons maintenant le cas général et posons-nous la question de savoir si les groupes linéaires définissables dans un enrichissement p-minimal de $\mathbb{Q}_p$ sont les mêmes que ceux $\mathcal{L}_R$-définissables ? Le but du chapitre est de répondre à cette question dans le cas commutatif. Le théorème 4.32 montre que les sous-groupes linéaires commutatifs définissables dans un certain enrichissement p-minimal de $\mathcal{Q}_p$ sont définissablement isomorphes à des groupes $\mathcal{L}_R$-définissables.

Dans un premier temps, nous rappellerons quelques fait essentiels sur l'exponentielle p-adique, élément capital de notre travail dans ce chapitre. Nous l'utiliserons immédiatement pour décrire la structure algébrique du groupe multiplicatif d'une extension finie de $\mathbb{Q}_p$. Ensuite, nous nous attarderons sur la notion de p-minimalité et nous expliciterons les propriétés de la dimension utiles à notre étude. La section suivante sera consacrée à la notion de p-connexité que nous introduisons pour palier la non-existence de la composante connexe dans $\mathcal{Q}_p$.

Le travail, à proprement parler, sur les groupes linéaires définissables dans les structures p-minimales commencera dans la quatrième section. Le point clé est la proposition 4.25 nous donnant une décomposition des groupes définissables linéaires commutatifs en produit de sous-groupes plus petits. Nous étudierons alors chacun de ces sous-groupes et leur définissabilité afin d'établir le théorème 4.32. Nous soulignons le rôle important du lemme 4.28 non trivial qui nous permet de traiter le cas non compact. La proposition 4.31 nous donne une description du tore anisotrope en dimension quelconque répondant ainsi aux questions de la fin du chapitre 2.

4.1 Préliminaires sur l'exponentielle et le logarithme p-adiques

Dans cette partie, on définit et on donne les premières propriétés de la fonction exponentielle sur $\mathbb{Q}_p$ et sur une extension finie K quelconque de $\mathbb{Q}_p$.

Soit K un corps valué complet extension finie de $\mathbb{Q}_p$ tel que $v_p(p) = 1$. On rappelle les conventions choisies : $\mathcal{O}$ est son anneau de valuation, Γ son groupe de valeurs, et k son corps résiduel. Si K est une extension finie de degré n, on note e son indice de ramification ($= [\Gamma : \mathbb{Z}]$), et f son degré résiduel ($= [k : \mathbb{F}_p]$), alors $n = ef$. On a alors $\Gamma = \frac{1}{e}\mathbb{Z}$, on note π une uniformisante de $\mathcal{O}$, l'idéal maximal de $\mathcal{O}$ est $\pi\mathcal{O}$.

4.1.1 Définition et premières propriétés

Dans cette thèse, on s'intéresse à la fonction exponentielle pour ses propriétés algébriques : elle établit, en effet, un isomorphisme entre une partie du groupe additif et une partie du groupe multiplicatif , et le logarithme est sa réciproque. On peut définir la fonction exp comme une fonction analytique définie sur toute extension finie K de $\mathbb{Q}_p$. Rappelons le fait suivant :

Fait 4.1 ([39, 4.1, chap. 5]). *Si K est une extension finie de $\mathbb{Q}_p$ et $x \in K$:*
- *La série $\sum_{n\geq 0} \frac{x^n}{n!}$ converge pour $v_p(x) > \frac{1}{p-1}$.*
- *La série $\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n$ converge pour $v_p(x) > 0$.*

On note alors $E_p = \{x \in K \mid v_p(x) > \frac{1}{p-1}\}$, et on pose pour $x \in E_p$:

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n!}$$

$$\log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n$$

Sur $\mathbb{Q}_p$, pour $p \neq 2$, on a $E_p = p\mathbb{Z}_p$ et pour $p = 2$, on a $E_p = 4\mathbb{Z}_2$. Les fonctions exp et log ainsi définies jouissent d'un bon nombre de propriétés en commun avec celle définies sur $\mathbb{R}$. Rappelons les :

Fait 4.2 ([39, 4.2, chap. 5])**.** *Soit $x, y \in E_p$,*

1. $v_p(\log(1+x)) = v_p(x)$
   $v_p(\exp(x)) = 0$
   $v_p(1-\exp(x)) = v_p(x)$
2. $\exp(\log(1+x)) = 1+x$
   $\log(\exp(x)) = x$
3. $\exp(x+y) = \exp(x)\cdot\exp(y)$

Fait 4.3. 1. $\exp(E_p) = 1+E_p$ *et* $\log(1+E_p) = E_p$

2. $\exp : (E_p, +) \longrightarrow (1+Ep, \cdot)$ *est un isomorphisme.*
3. *Si K est une extension finie, pour $r \in \Gamma$ tel que $r > \frac{1}{p-1}$, on a* $\exp(\pi^r\mathcal{O}) = 1+\pi^r\mathcal{O}$ *et* $\log(1+\pi^r\mathcal{O}) = \pi^r\mathcal{O}$
4. $v_p(\exp(x)-\exp(y)) = v_p(x-y)$
   $v_p(\log(x)-\log(y)) = v_p(x-y)$

Sur $\mathbb{Q}_p$, exp établit un isomorphisme entre $p\mathbb{Z}_p^+$ et $(1+p\mathbb{Z}_p)^\times$ (pour $p \neq 2$) et entre $4\mathbb{Z}_2$ et $(1+4\mathbb{Z}_2)^\times$.

Remarque. Les propriétés algébriques de la fonction exp sont exprimables par une formule du premier ordre. Si exp est un symbole de notre langage, alors dans tout $\mathcal{Q}_p$ modèle élémentairement équivalent à $\mathbb{Q}_p$ dans ce langage, la fonction exp sera un isomorphisme entre $\mathcal{Z}_p^+$ et $(1+p\mathcal{Z}_p)^\times$ (pour $p \neq 2$).

4.1.2 Groupe multiplicatif et exponentielle

En suivant le raisonnement fait sur $\mathbb{Q}_p$, l'exponentielle va nous permettre de décrire la structure algébrique du groupe multiplicatif d'une extension finie de $\mathbb{Q}_p$.

Proposition 4.4. *Avec les notations précédentes, si K est une extension finie de $\mathbb{Q}_p$, alors :*

$$K^\times \cong \Gamma \times k^\times \times (1+\pi\mathcal{O})^\times$$

– *si l'indice de ramification e de K vérifie $e < p-1$, alors*

$$(1+\pi\mathcal{O})^\times \cong \pi\mathcal{O} \cong \mathbb{Z}_p^n$$

– *sinon,* $e \geq p-1$*, alors* $(1+\pi\mathcal{O})^\times$ *contient un sous-groupe d'indice fini* p^r *avec* $r = \lfloor \frac{e}{p-1} \rfloor$ *isomorphe à* $\mathcal{O}^+$ *donc à* $\mathbb{Z}_p^n$*.*

Démonstration. On cherche à étudier la structure de $K^\times$. On a $\mathcal{O}^\times = \{x \in \mathcal{O} \mid v_p(x) = 0\}$. On remarque que $\{\pi^\gamma; \gamma \in \Gamma\}$ est un sous-groupe de $K^\times$ qui est isomorphe à $(\Gamma, +)$. On établit ainsi :

$$K^\times \cong \Gamma \times \mathcal{O}^\times$$

Etudions la structure de $\mathcal{O}^\times$.

On considère le polynôme $F(x) = x^{p^f-1} - 1$, on a $F'(x) = (p^f - 1)x^{p^f-2}$. Tout $\bar{a} \in k^\times$ est solution de $F(x) = 0$ et de plus $F'(\bar{a}) = -\bar{a}^{-1} \neq 0$. Soit $a' \in \mathcal{O}$ tel que $res(a') = \bar{a}$, on a alors $res(F(a')) = 0$ et $res(F'(a')) = 0$. Par henselianité, il existe $a \in \mathcal{O}$ avec $res(a) = \bar{a}$ et $F(a) = 0$. On pose alors $V = \{x \in \mathcal{O} \mid x^{p^f-1} = 1\}$ le groupe des racines $(p^f-1)^{\text{ième}}$ de l'unité, V possède donc bien (p^f-1) éléments, et $V \cong k^\times$.

On a $Ker(res) = 1 + \pi\mathcal{O}$ et $V \cap (1+\pi\mathcal{O}) = \{1\}$ donc $\mathcal{O}^\times = V \times (1+\pi\mathcal{O})$. On a établi l'isomorphisme :

$$K^\times \cong \Gamma \times k^\times \times (1+\pi\mathcal{O})$$

• Si $e < p-1$ alors $v_p(\pi) = \frac{1}{e} > \frac{1}{p-1}$, donc $E_p = \pi\mathcal{O}$. Ainsi l'exponentielle réalise l'isomorphisme $(1+\pi\mathcal{O}, \cdot) \cong (\pi\mathcal{O}, +)$ (fait 4.3). Il vient :

$$K^\times \cong \Gamma \times k^\times \times \mathcal{O}^+$$

• Si $e \geq p-1$, alors $v_p(\pi) \leq \frac{1}{p-1}$, et $E_p \subsetneq \pi\mathcal{O}$. On a $E_p = \pi^{r+1}\mathcal{O}$ avec $r = \lfloor \frac{e}{p-1} \rfloor$. Par le fait 4.3, on a $1 + \pi^{r+1}\mathcal{O} \cong \pi^{r+1}\mathcal{O} \cong \mathcal{O}$. Le sous-groupe $(1+\pi^r\mathcal{O})$ est d'indice p^r dans $1+\pi\mathcal{O}$, en effet pour $n \in \{1, ..., r\}$, $(1+\pi^n\mathcal{O})/(1+\pi^{n+1}\mathcal{O}) \cong \mathcal{O}/\pi\mathcal{O} \cong \mathbb{Z}/p\mathbb{Z}$.

K est une extension fini du corps $\mathbb{Q}_p$, donc K est un $\mathbb{Q}_p$-espace vectoriel, ainsi $K^+ \cong \mathbb{Q}_p^{+n}$ et $\mathcal{O}^+ \cong \mathbb{Z}_p^{+n}$. □

On peut affiner la proposition précédente en donnant une description précise de la structure de $(1+\pi\mathcal{O})^\times$ valable dans les différents cas :

Proposition 4.4 bis. *Avec les notations précédentes, si* K *est une extension finie de* $\mathbb{Q}_p$*, alors :*

$$K^\times \cong \Gamma \times k^\times \times (1+\pi\mathcal{O})^\times$$

De plus $(1+\pi\mathcal{O}, \cdot) \cong H \times (\mathbb{Z}_p^n, +)$ *où* H *est un groupe fini.*

Démonstration. On munit $(1+\pi\mathcal{O})^\times$ d'une structure de $\mathbb{Z}_p$-module. Soit $x, y \in 1+\pi\mathcal{O}$, on définit l'addition modulaire par :

$$x \boxplus y = x \cdot y$$

Pour définir la multiplication par un scalaire, rappelons que $1+E_p$ l'ensemble d'arrivée de l'exponentielle est un sous-groupe d'indice fini p^r dans $(1+\pi\mathcal{O})^\times$ (où $r = \lfloor \frac{e}{p-1} \rfloor$). Soit $\lambda \in \mathbb{Z}_p$, on a :

$$\lambda = \lambda_1 + p^r\lambda_2 \quad \text{avec } \lambda_1 \in \mathbb{Z} \text{ et } \lambda_2 \in \mathbb{Z}_p$$

on définit alors la multiplication scalaire par :

$$\lambda \boxdot x = x^{\lambda_1} \cdot \exp(\lambda_2 \log(x^{p^r}))$$

Comme $\lambda_1 \in \mathbb{Z}$, x^{λ_1} est bien défini, de plus comme $1+E_p$ est d'indice p^r dans $1+\pi\mathcal{O}$, si $x \in 1+\pi\mathcal{O}$ alors $x^{p^r} \in 1+E_p$, donc $\exp(\lambda_2 \log(x^{p^r}))$ est bien défini. Il est facile de vérifier que la définition de la multiplication scalaire ne dépend pas du choix de λ_1 et λ_2, les axiomes de modules sont également facilement vérifiés.

Ainsi $1+\pi\mathcal{O}$ est un $\mathbb{Z}_p$-module. De plus, comme $1+E_p$ est d'indice fini dans $1+\pi\mathcal{O}$ et que $1+E_p$ est isomorphe à $\mathbb{Z}_p^n$ par l'exponentielle, on sait que tout élément $x \in 1+\pi\mathcal{O}$ s'écrit :

$$x = g_i \cdot \exp(\lambda_1 e_1 + ... \lambda_n e_n)$$

$$x = g_i \boxplus (\lambda_1 \boxdot \exp(e_1)) \boxplus ... \boxplus (\lambda_n \boxdot \exp(e_n))$$

où $g_i \in 1+\pi\mathcal{O}$ pour $i \in \{1, ..., p^r\}$ sont les représentants des classes de $1+\pi\mathcal{O}$ modulo $1+E_p$; $\lambda_j \in \mathbb{Z}_p$ et $\exp(e_j) \in 1+E_p$ pour $j \in \{1, ..., n\}$. Ainsi $1+\pi\mathcal{O}$ est finiment engendré et $1+\pi\mathcal{O}$ est un $\mathbb{Z}_p$-module de type fini. $\mathbb{Z}_p$ étant un anneau principal $1+\pi\mathcal{O}$ se décompose de la manière suivante ([23, théorème 3.7.3]) :

$$1+\pi\mathcal{O} \cong H \oplus F$$

où F est un module libre de type fini, donc isomorphe à $\mathbb{Z}_p^n$ et H est la partie de torsion de $1+\pi\mathcal{O}$ donc est finie (fait 1.14). □

4.2 Préliminaires sur les structures p-minimales

La notion de *p-minimalité* a été introduite en 1997, par D. Haskell et D. Macpherson dans [17]. Il s'agit de définir pour les corps p-adiques un équivalent de la o-minimalité. On rappelle ici la définition et quelques propriétés de base des structures p-minimales.

A l'inverse d'une structure o-minimale, on ne définit pas la p-minimalité pour une grande classe de structure. On considère un corps valué avec un $\mathbb{Z}$-groupe comme groupe de valeur, étudié dans le langage $\mathcal{L}_d = \{+, -, \cdot, 0, 1, |\} \cup \{P_n\}_{n\in\mathbb{N}} \cup \{c_1, ..., c_d\}$, où $x \mid y$ sera interprété par $v(x) \leq v(y)$, $P_n(x)$ par $\exists y \quad x = y^n$, les constantes seront telles que $\{c_1 + p\mathcal{O}, c_2 + p\mathcal{O}, ..., c_d + p\mathcal{O}\}$ est une base de $\mathcal{O}/p\mathcal{O}$. On imposera de plus que pour tout $K' \equiv K$:

- Tout ensemble infini définissable de K est d'intérieur non vide.
- Tout ensemble définissable non vide du groupe de valeur Γ' qui est borné admet un plus grand élément.

Dans ce chapitre, on s'intéressera uniquement aux enrichissements p-minimaux de $\mathbb{Q}_p$ ou d'un corps élémentairement équivalent. Remarquons que :

- Sur $\mathbb{Q}_p$, les langages $\mathcal{L}_d$ et $\mathcal{L}_R$ ont la même capacité d'expressivité : ce qui est définissable avec l'un est définissable avec l'autre. Dans la suite du chapitre on utilisera indifféremment les deux langages.
- Nous n'utilisons pas la même définition de *p-adiquement clos* que les auteurs de [17]. Dans cette section et dans cette section uniquement, nous nous référerons à la leur, qui inclut la notre.

Définition 4.5. *Soit $\mathcal{L}'_d$ un langage étendant $\mathcal{L}_d$, et $(\mathcal{K}, v)$ une $\mathcal{L}'_d$-structure. On dit que $\mathcal{K}$ est une structure p-minimale, si pour toute structure $\mathcal{K}'$ élémentairement équivalente à $\mathcal{K}$, tout ensemble $\mathcal{L}'_d$- définissable de K' est définissable sans quantificateur dans $\mathcal{L}_d$.*

Fait 4.6 ([17, Theorem 2.2])**.** *Tout enrichissement p-minimale d'une $\mathcal{L}_d$-structure est p-adiquement clos.*

Définition 4.7. *Soit $\mathcal{K}$ un enrichissement p-minimal d'un corps valué. Soit X un ensemble définissable de K^n. La dimension topologique de X,* $\operatorname{topdim} X$ *est le plus grand entier $m \in \mathbb{N}$ tel qu'il existe une projection $\pi : K^n \to K^m$ telle que $\pi(X)$ est d'intérieur non vide dans K^m.*

Fait 4.8 ([17, Theorem 3.2])**.** *Pour $X_1, ..., X_r$ des ensembles définissables de K^n :*

$$\operatorname{topdim}(X_1 \cup ... \cup X_r) = max\{\operatorname{topdim} X_1, ..., \operatorname{topdim} X_r\}$$

Fait 4.9 ([17, Theorem 6.2])**.** *Soit $\mathcal{K}$ un enrichissement p-minimal d'un corps p-adiquement clos. Alors* acl *a la propriété de l'échange pour $Th(\mathcal{K})$.*

On sait alors que acl définit une dimension de la manière suivante : Un ensemble $\{a_1, ..., a_n\}$ est dit algébriquement indépendant si $a_i \notin \operatorname{acl}(\{a_j; j \neq i\})$. Par le fait précédent, si $Z \subseteq K$, alors deux sous-ensembles algébriquement indépendants ont la même cardinalité. On appelle rang de Z, $\operatorname{rg} Z$, ce nombre. Si Z est énuméré par un uple $\bar{z}$, on note $\operatorname{rg}(\bar{z})$.

Définition 4.10. *Soit $\mathcal{K}$ un enrichissement p-minimal d'un corps p-adiquement clos. Soit $X \subseteq K^n$, un ensemble défini par une formule $\varphi(\bar{x}, \bar{a})$ à paramètre dans A. La dimension algébrique de X,* $\operatorname{algdim} X$*, est le plus grand $r \in \mathbb{N}$ tel que dans une extension élémentaire $\mathcal{K}' \succcurlyeq \mathcal{K}$, il existe $\bar{x}$ tel que $\mathcal{K}' \models \varphi(\bar{x}, \bar{a})$ et $\operatorname{rg}(\bar{x}\bar{a}) - \operatorname{rg}(\bar{a}) = r$.*

Fait 4.11 ([17, Theorem 6.3])**.** *Soit $\mathcal{K}$ un enrichissement p-minimal d'un corps p-adiquement clos. Si $X \subseteq K^n$ est un ensemble définissable alors*

$$\operatorname{topdim} X = \operatorname{algdim} X$$

A l'avenir, on notera $\dim X$ cette dimension.

Définition 4.12. *Une théorie T est* algébriquement bornée *si pour tout modèle $\mathfrak{M} \models T$, et toute formule $\varphi(x, \bar{y})$ il existe un entier n_φ tel que pour tout $\bar{a} \in M^n$ l'ensemble $\{x \in M \mid \mathfrak{M} \models \varphi(x, \bar{a})\}$ est infini si et seulement si il est de cardinal plus grand que n_φ.*

Fait 4.13 ([17, Lemma 4.3])**.** *Si $\mathcal{K}$ est un enrichissement p-minimal d'un corps p-adiquement clos alors $Th(\mathcal{K})$ est algébriquement bornée.*

Fait 4.14. *Soit $\mathcal{K}$ un enrichissement p-minimal d'un corps p-adiquement clos. Alors la dimension vérifie les propriétés suivantes pour S, S_1 et S_2 des ensembles définissable dans $\mathcal{K}$:*

Définissabilité *Si $f : S_1 \longrightarrow S_2$ est une fonction définissable, alors l'ensemble $\{y \in S_2 \mid \dim(f^{-1}(y) = m\})$ est définissable pour tout $m \in \mathbb{N}$.*

Additivité *Si $f : S_1 \longrightarrow S_2$ est une fonction définissable, dont les fibres sont de dimension contante m, alors $\dim S_1 = \dim Im(f) + m$.*
En particulier, $\dim(S_1 \times S_2) = \dim S_1 + \dim S_2$.

Finitude *S est fini si et seulement si $\dim S = 0$.*

Monotonicité *Si $f : S \longrightarrow K^m$ est une fonction définissable, alors $\dim f(S) \leq \dim S$, et si f est injective alors $\dim f(S) = \dim S$.*
En particulier, si $S_1 \subseteq S_2$ alors $\dim S_1 \leq \dim S_2$.

Démonstration. Il nous suffit de vérifier les axiomes de van den Dries énoncés page 16. Les axiomes (Dim 1-3) sont facilement vérifiés par topdim .

Pour démontrer (Dim 4), prenons $T \subseteq K^{m+1}$ un ensemble définissable, notons $T_{\bar{x}} = \{y \in K \mid (\bar{x}, y) \in T\} \subseteq K$ pour $\bar{x} \in K^m$ et $T(i) = \{\bar{x} \in K^m \mid \dim T_{\bar{x}} = i\}$ (pour $i = 0, 1$). Comme $\mathcal{K}$ est une structure p-minimale, l'ensemble définissable $T_{\bar{x}} \subseteq K$ est définissable dans $\mathcal{L}_d$ et on a $\dim T_{\bar{x}} = 1$ si et seulement si $T_{\bar{x}}$ infini. De plus, puisque $Th(\mathcal{K})$ est algébriquement bornée, $T(i)$ est définissable par :

$$\bar{x} \in T(0) \leftrightarrow \exists^{<n_T} y \quad (\bar{x}, y) \in T$$

$$\bar{x} \in T(1) \leftrightarrow \exists^{\geq n_T} y \quad (\bar{x}, y) \in T$$

On a $\dim\{(\bar{x}, y) \in K \mid \bar{x} \in T(i)\} = \dim T(i) + i$ par la définition de topdim .

□

Exemple. Soit $Y = (Y_1, ..., Y_n)$, on note $\mathbb{Z}_p < Y >$ l'anneau des séries entières $f(Y) = \sum_\nu a_\nu Y^\nu \in \mathbb{Z}_p[[Y]]$ telles que $\mid a_\nu \mid_p \longrightarrow 0$ quand $|\nu| \longrightarrow \infty$ (pour $\nu = (\nu_1, ..., \nu_n)$, on note $|\nu| = \nu_1 + ... + \nu_n$). Pour $f \in \mathbb{Z}_p < Y >$, $f(Y) = \sum_\nu a_\nu Y^\nu$, on définira la fonction analytique restreinte associée $f : \mathbb{Q}_p^n \longrightarrow \mathbb{Q}_p$ par :

$$f(y) = \begin{cases} \sum_\nu a_\nu y^\nu & \text{pour } y \in \mathbb{Z}_p^n \\ 0 & \text{sinon} \end{cases}$$

On considère le langage $\mathcal{L}_{an}$, où on étend le langage $\mathcal{L}_d$ en ajoutant un symbole de fonction n-aire pour chaque fonction analytique restreinte $f \in \mathbb{Z}_p < Y >$. On note $\mathbb{Q}_p^{an}$ la structure de $\mathbb{Q}_p$ étudiée dans le langage $\mathcal{L}_{an}$.

Fait 4.15 ([45, Theorem B])**.** *Les extensions $\mathcal{L}_{an}$-élémentaires de $\mathbb{Q}_p$ sont p-minimales.*

4.3 p-connexité

Nous introduisons ici une nouvelle notion : la *p-connexité*. Cette dernière nous servira d'équivalent à la notion de *connexité* très utile dans le cas o-minimale, mais sans consistance dans le cas p-adique. Nous définissons la p-connexité dans le cas d'un groupe abstrait, aucune référence à la théorie des modèles n'est nécessaire. Nous en donnons ici les première propriétés, que l'on attend naturellement d'une certaine notion de connexité.

On fixe un nombre premier p.

Définition 4.16. *Soit G un groupe.*
- *On dit que G est p-connexe s'il ne contient pas de sous-groupe propre normal d'indice premier à p (i.e. tous ses sous-groupes normaux d'indice fini sont d'indice divisible par p).*
- *On dit que G est p'-connexe si tous ses sous-groupes normaux d'indice fini sont d'indice premier à p.*
- *On dit que G est p'-divisible si pour tout n premier à p, pour tout $x \in G$ il existe $y \in G$ tel que $x = y^n$.*

Exemple. On sait que $\mathbb{Q}_p^+$ est connexe (car $\mathbb{Q}_p^+$ est divisible), donc est p-connexe.

Proposition 4.17. *Si G est un groupe p'-divisible alors G est p-connexe.*

Démonstration. On suppose que G est p'-divisible. Soit H un sous-groupe normal d'indice fini n. On a G/H fini d'ordre n et p'-divisible. On a pour tout x dans G/H, $x^n = e$ donc seul e est divisible par n donc n n'est pas premier à p. Ainsi G ne contient pas de sous-groupe normal d'indice premier à p. □

Exemple. $\mathbb{Z}_p^+$ est p'-divisible donc il est p-connexe. Plus précisément tout sous-groupe $\mathcal{L}_R$-définissable de $\mathbb{Q}_p^+$ est p-connexe.

Remarque. Si $\mathfrak{M}$ et $\mathfrak{M}'$ sont deux structures élémentairement équivalentes, et si G est un groupe définissable dans $\mathfrak{M}$ et si G' est le groupe défini par la même définition que G dans $\mathfrak{M}'$, alors G est p'-divisible si et seulement si G' est p'-divisible. Ils seront alors tous les deux p-connexes.

Proposition 4.18. *Soit G un groupe commutatif.*

1. *Si G est p-connexe alors les sous-groupes d'indice fini sont d'indice p^k avec $k \in \mathbb{N}$.*
2. *Si G est p-connexe alors tout sous-groupe d'indice fini est p-connexe.*

Démonstration.
1. Soit $H \leq G$ d'indice fini n. Si n n'est pas premier à p alors il s'écrit $p^k m$ avec $k \in \mathbb{N}$ et m premier à p. Aussi G/H est d'ordre $p^k m$, on note H' son p-sous-groupe de Sylow. Donc HH' est un sous-groupe normal de G d'ordre m premier à p, ce qui est absurde.
2. C'est un simple corollaire du point précédent.

□

Proposition/Définition 4.19. *Soit G un groupe, il existe un plus grand sous-groupe normal de G p-connexe. On le note $G^\square$.*

On appelle $G^\square$ la composante p-connexe *de G.*

Exemple. Si $G = \mathbb{Q}_p^\times$ alors $G^\square = 1 + p\mathbb{Z}_p$. Si K est une extension finie de $\mathbb{Q}_p$ et si $G = K^\times$, alors $G^\square = (1 + \pi\mathcal{O})^\times$.

Démonstration. On donnera deux constructions différentes (par le bas et par le haut) de $G^\square$.

Soit $\{G_i\}_{i\in I}$ l'ensemble des sous-groupes normaux p-connexes de G. On muni I d'un bon ordre et on pose :

$$\begin{cases} \Lambda_0 &= G_0 \\ \Lambda_{i+1} &= \Lambda_i \cdot G_{i+1} \quad \text{(si } i+1 \text{ est un ordinal successeur)} \\ \Lambda_\lambda &= \bigcup_{i<\lambda} \Lambda_i \quad \text{(si } \lambda \text{ est un ordinal limite)} \end{cases}$$

On montre par induction que Λ_λ pour $\lambda \leq \mid I \mid$ est un sous-groupe normal p-connexe de G.

G_0 est un sous-groupe normal p-connexe. Si Λ_i est un sous-groupe normal p-connexe, alors $\Lambda_{i+1} = \Lambda_i \cdot G_{i+1}$ est également un sous-groupe normal. Λ_{i+1} est p-connexe : soit H un sous-groupe normal de Λ_{i+1}. Supposons que H soit d'indice fini premier à p dans Λ_{i+1}. Le sous-groupe $H \cap \Lambda_i$ est un sous-groupe normal de Λ_i et par le deuxième théorème d'isomorphisme $\Lambda_i/H \cap \Lambda_i \cong \Lambda_i \cdot H/H$. Comme H est d'indice fini premier à p dans Λ_{i+1}, il l'est aussi dans $\Lambda_i \cdot H$. On a ainsi montré que $H \cap \Lambda_i$ est un sous-groupe normal d'indice fini premier à p dans Λ_i, ce qui est absurde par hypothèse d'induction.

Pour λ un ordinal limite, on a immédiatement que Λ_λ est un sous-groupe normal. Si H est un sous-groupe normal d'indice fini premier à p, alors par le deuxième théorème d'isomorphisme, on montre que $H \cap \Lambda_i$ pour $i < \lambda$ est un sous-groupe d'indice fini premier à p de Λ_i ce qui contredit l'hypothèse d'induction.

On a ainsi montré que $\Lambda_{|I|}$ est le plus grand sous-groupe normal p-connexe de G, il est engendré par tous les sous-groupes normaux p-connexes de G, on le note $G^\square$.

On peut également construire $G^\square$ par le haut. On pose alors :

$$\begin{cases} \Gamma_0 &= G \\ \Gamma_{i+1} &= \bigcap\{H \trianglelefteq \Gamma_i \mid [\Gamma_i : H] \text{ premier à } p\} \quad \text{(si } i+1 \text{ est un ordinal successeur)} \\ \Gamma_\lambda &= \bigcap_{i<\lambda} \Gamma_i \quad \text{(si } \lambda \text{ est un ordinal limite)} \end{cases}$$

Remarquons que cette suite est stationnaire dès que Γ_i est p-connexe, auparavant la suite $\{\Gamma_i\}$ est strictement décroissante. Puisque le nombre de sous-groupes d'un groupe est limité (borné par $2^{|G|}$), il vient que la suite $\{\Gamma_i\}$ est stationnaire à partir d'un certain rang κ, ainsi Γ_κ est p-connexe.

Par définition de $G^\square$, on a $\Gamma_\kappa \leq G^\square$. Montrons par induction que pour tout ordinal $i \leq \kappa$, on a $G^\square \leq \Gamma_i$. On a $G^\square \leq \Gamma_0$. Si $G^\square \leq \Gamma_i$, montrons que $G^\square$ est contenu dans tout sous-groupe normal d'indice fini premier à p. Soit H un sous-groupe normal de Γ_i d'indice fini premier à p. Ainsi $H \cap G^\square$ est un sous-groupe normal d'indice fini de $G^\square$. On a par le second théorème d'isomorphisme $G^\square/H \cap G^\square \cong HG^\square/H$, H est d'indice premier à p dans Γ_i donc également dans $HG^\square$. Donc si $G^\square \neq H \cap G^\square$ alors $G^\square$ contient un sous-groupe d'indice premier à p, absurde. Ainsi $G^\square \leq \Gamma_{i+1}$. Si λ est un ordinal limite, et si $G^\square \leq \Gamma_i$ pour tout $i < \lambda$, alors $G^\square \leq \Gamma_\lambda$. Il vient que $\Gamma_\kappa = G^\square$. □

Proposition 4.20. *Si G est un groupe commutatif, alors $G^\square$ est d'indice infini ou premier à p dans G.*

Démonstration. Si $G^\square$ est d'indice fini, on note alors $n = p^k m$ l'ordre de $G/G^\square$, et $G'/G^\square$ son p-sous-groupe de Sylow. On voit que G' est un sous-goupe p-connexe, ce qui contredit la maximalité de $G^\square$. □

Définition 4.21. *Soit G et G' des groupes, on dit que $\varphi : G \longrightarrow G'$ est un p-morphisme si φ est un morphisme de groupes et $\ker\varphi$ est p-connexe.*

Proposition 4.22. *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes.*

1. *Si G est p-connexe alors $\varphi(G)$ est p-connexe.*
2. *Si $\varphi(G)$ est p-connexe et φ est un p-morphisme, alors G est p-connexe.*
3. *Si φ est un p-morphisme, alors $\varphi(G^{\square}) = \varphi(G)^{\square}$.*

Lemme 4.23. *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes et H un sous-groupe de G. On suppose que H est d'indice fini dans G, alors $\varphi(H)$ est d'indice fini dans $\varphi(G)$ et $H \cap \ker\varphi$ d'indice fini dans $\ker\varphi$, de plus on a :*

$$[G : H] = [\varphi(G) : \varphi(H)] \cdot [\ker\varphi : H \cap \ker\varphi] \tag{4.1}$$

Démonstration. On a $\varphi^{-1}(\varphi(H)) = H \cdot \ker\varphi$. $H \subseteq H \cdot \ker\varphi$ donc $H \cdot \ker\varphi$ est d'indice fini dans G. Si $G = H \cdot \ker\varphi \cup g_1 H \cdot \ker\varphi \cup ... \cup g_n H \cdot \ker\varphi$, alors $\varphi(G) = \varphi(H) \cup \varphi(g_1)\varphi(H) \cup ... \cup \varphi(g_n)H$, ainsi $\varphi(H)$ est d'indice fini dans $\varphi(G)$ et $[\varphi(G) : \varphi(H)] \leq [G : H \cdot \ker\varphi]$. De même, on montre que $[G : H \cdot \ker\varphi] \leq [\varphi(G) : \varphi(H)]$. On sait que $[G : H] = [G : H \cdot \ker\varphi][H \cdot \ker\varphi : H]$, or par le second théorème d'isomorphisme $H \cdot \ker\varphi/H \cong \ker\varphi/H \cap \ker\varphi$; on obtient ainsi l'égalité voulue. □

Démonstration de la proposition 4.22.

1. On a $\varphi(G) = G/\ker\varphi$. Pour $H/\ker\varphi$ un sous-groupe distingué de $G/\ker\varphi$, on a par le troisième théorème d'isomorphisme
$$(G/\ker\varphi)/(H/\ker\varphi) \cong G/H$$
Donc si $\varphi(G)$ contient un sous-groupe normal d'indice fini premier à p, il en est de même pour G, ce qui n'est pas le cas.
2. Si G contient un sous-groupe normal H d'indice fini premier à p, alors par (4.1) $\varphi(H)$ est d'indice fini premier à p dans $\varphi(G)$ car $\ker\varphi$ ne possède pas de sous-groupe d'indice premier à p.
3. $\varphi(G^{\square})$ est p-connexe. Si $H \trianglelefteq \varphi(G)$ est p-connexe alors $\varphi^{-1}(H)$ est un sous-groupe normal p-connexe de G par 2. donc contenu dans $G^{\square}$, donc $H \subseteq \varphi(G^{\square})$. Ainsi $\varphi(G^{\square})$ est le plus grand sous-groupe normal p-connexe de $\varphi(G)$ donc $\varphi(G^{\square}) = \varphi(G)^{\square}$.

□

4.4 Groupes linéaires définissables et semi-algébriques

Dans cette section, nous allons étudier des groupes linéaires dans un enrichissement p-minimal d'un corps p-adiquement clos. Précisons d'abord le cadre de notre étude.

On remarque facilement que toutes les extensions finies K de $\mathbb{Q}_p$ sont définissables dans $\mathcal{L}_R$. On considère le langage $\mathcal{L}_{\exp}$ étendant le langage $\mathcal{L}_R$ contenant pour toute extension finie K de $\mathbb{Q}_p$ un symbole de fonction $\exp_K$ représentant la

fonction exponentielle définie sur K. Commençons par monter que toute extension $\mathcal{L}_{\exp}$-élémentaire de $\mathbb{Q}_p$ est p-minimale. Soit $\mathcal{Q}_p$ une telle extension élémentaire de $\mathbb{Q}_p$.

Toute extension finie K de $\mathbb{Q}_p$ étant définissable, l'ensemble de définition E_p de $\exp_K$ sera définissable. Si $\mathcal{K}$ est une extension finie de $\mathcal{Q}_p$, alors $\exp_K$ établira un isomorphisme entre $E_p^+ = \{x \in \mathbb{K} \mid v_p(x) > \frac{1}{p-1}\}$ et $(1+E_p)^\times$.

Si $\varphi_K(\bar{x}, \bar{b})$ est une formule définissant K dans $\mathbb{Q}_p$ et si $x \in K$ est représentée par $\bar{x} = (x_1, ..., x_m)$ avec $x_i \in \mathbb{Q}_p$, alors la fonction $x \longmapsto x^n$ sera représentée par une fonction

$$(x_1, ..., x_m) \longmapsto (P_{1,n}(\bar{x}), ..., P_{m,n}(\bar{x}))$$

où $P_{i,n}$ est un polynôme en les variables $x_1, ..., x_m$. Ainsi la série $x \longmapsto \sum\limits_{n\geq 0} \frac{x^n}{n!}$ sera représentée par une fonction

$$(x_1, ..., x_m) \longmapsto (\sum_{n\geq 0} \frac{P_{1,n}(\bar{x})}{n!}, ..., \sum_{n\geq 0} \frac{P_{m,n}(\bar{x})}{n!})$$

La fonction $\exp_K$ sera une fonction analytique sur $\mathbb{Z}_p^m$. Ainsi $\mathcal{L}_{\exp} \subseteq \mathcal{L}_{an}$ et $\mathcal{Q}_p$ sera une structure p-minimale.

A partir de maintenant, on considérera un langage $\mathcal{L}$ étendant $\mathcal{L}_{\exp}$ tel que la structure $\mathbb{Q}_p$ dans ce langage $\mathcal{L}$ soit p-minimale, et $\mathcal{Q}_p$ sera une extension $\mathcal{L}$-élémentaire de $\mathbb{Q}_p$. Un ensemble définissable dans $\mathcal{L}_R$ sera dit *semi-algébrique*, et un ensemble définissable dans $\mathcal{L}_{an}$ sera dit *sous-analytique*. S'il n'est pas précisé de langage, *définissable* signifiera définissable dans le langage $\mathcal{L}$.

Nous commençons cette section par une proposition générale sur les $\mathbb{Z}_p$-modules. C'est une proposition qui est déjà connue pour tous les anneaux principaux, mais dont nous donnons tout de même une démonstration dans notre cas afin de bien connaître les mécanismes en jeu.

On notera $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{Q}_p^n$, et $v_p(\mathbf{x}) = \min\{v_p(x_1), ..., v_p(x_n)\}$.

Proposition 4.24. *Les sous-$\mathbb{Z}_p$-modules de $\mathbb{Z}_p^m$ sont des $\mathbb{Z}_p$-modules libres de type fini, en particulier, ils sont semi-algébriques.*

Démonstration. Soit H un sous-$\mathbb{Z}_p$-module de $\mathbb{Z}_p^m$. Commençons par supposer H ouvert dans $\mathbb{Z}_p^m$. Ainsi il existe $n \in \mathbb{Z}$ tel que $p^n\mathbb{Z}_p^m \leq H$, choisissons n le plus petit possible. On a :

$$H/p^n\mathbb{Z}_p^m \leq \mathbb{Z}_p^m/p^n\mathbb{Z}_p^m = \left(\mathbb{Z}_p/p^n\mathbb{Z}_p\right)^m$$

Aussi $H/p^n\mathbb{Z}_p^m$ est un groupe abélien de type fini, plus précisement, c'est un $\mathbb{Z}/p^n\mathbb{Z}$-module libre de type fini. On note $\bar{\mathbf{e_1}}, ..., \bar{\mathbf{e_k}}$ une base de $H/p^n\mathbb{Z}_p^m$ et $\mathbf{e_1}, ..., \mathbf{e_k} \in H$ des représentants de $\bar{\mathbf{e_1}}, ..., \bar{\mathbf{e_k}}$ respectivement. $\mathbf{e_1}, ..., \mathbf{e_k}$ forment un système libre de vecteurs dans le $\mathbb{Z}_p$-module $\mathbb{Z}_p^m$: supposons, en effet, qu'il existe $\lambda_1, ..., \lambda_k \in \mathbb{Z}_p$ tels que

$$\lambda_1\mathbf{e_1} + ... + \lambda_k\mathbf{e_k} = 0$$

alors en projetant sur $H/p^n\mathbb{Z}_p^m$ on a

$$\lambda_1\bar{\mathbf{e_1}} + ... + \lambda_k\bar{\mathbf{e_k}} = 0$$

donc $\lambda_1, ..., \lambda_k$ sont congrus à 0 modulo p^n. Ainsi p^n divise λ_i pour $i \in \{1, ..., k\}$ et si $\lambda_i' = \lambda_i/p^n$, on a $\lambda_1'\mathbf{e_1} + ... + \lambda_k'\mathbf{e_k} = 0$, par le même raisonnement on trouve $\lambda_i' \equiv 0 \mod p^n$, il vient que $\lambda_i \equiv 0 \mod p^N$ pour tout N donc $\lambda_i = 0$. $\{\mathbf{e_1}, ..., \mathbf{e_k}\}$ est un système libre de $\mathbb{Z}_p^m$ donc c'est un système libre de l'espace vectoriel $\mathbb{Q}_p^m$. On complète $\mathbf{e_1}, ..., \mathbf{e_k}$ en une base $\mathbf{e_1}, ..., \mathbf{e_k}, \mathbf{e_{k+1}}, ..., \mathbf{e_m}$ de l'espace vectoriel telle que $\mathbf{e_{k+1}}, ..., \mathbf{e_m} \in p^n\mathbb{Z}_p^m$. Il vient que

$$H = \mathbb{Z}_p\mathbf{e_1} \oplus ... \oplus \mathbb{Z}_p\mathbf{e_k} \oplus \mathbb{Z}_p\mathbf{e_{k+1}} \oplus ... \oplus \mathbb{Z}_p\mathbf{e_m}$$

En effet, soit $x \in H$, si on note $\rho : H \longrightarrow H/p^n\mathbb{Z}_p^m$ la projection canonique, alors $\rho(x) = \lambda_1\bar{\mathbf{e_1}} + ... + \lambda_k\bar{\mathbf{e_k}}$ avec $\lambda_i \in \{0, 1, 2, ..., p^n - 1\}$, on pose $\zeta = \lambda_1\mathbf{e_1} + ... + \lambda_k\mathbf{e_k}$. On a $\rho(x) = \rho(\zeta)$ donc $x - \zeta \in p^n\mathbb{Z}_p^m$. En constatant que $p^n\mathbf{e_1}, ..., p^n\mathbf{e_k}, \mathbf{e_{k+1}}, ..., \mathbf{e_m}$ est une base de $p^n\mathbb{Z}_p^m$, on a bien $x \in \mathbb{Z}_p\mathbf{e_1} \oplus ... \oplus \mathbb{Z}_p\mathbf{e_m}$. L'inclusion réciproque relève juste de la définition de sous-$\mathbb{Z}_p$-module.

Si H n'est pas ouvert, on considère E le sous-espace vectoriel de $\mathbb{Q}_p^m$ engendré par H : l'espace vectoriel E est de la forme $\mathbb{Q}_p \cdot H$. Soit $\mathbf{e_1}, ..., \mathbf{e_k}$ une base de E, il existe $\lambda_1, ..., \lambda_k \in \mathbb{Q}_p$ tels que $\lambda_1\mathbf{e_1}, ..., \lambda_k\mathbf{e_k} \in H$ donc $\lambda_1\mathbb{Z}_p\mathbf{e_1} \oplus ... \oplus \lambda_k\mathbb{Z}_p\mathbf{e_k} \subseteq H$ donc H est ouvert dans E et on se ramène au cas précédent.

□

Proposition 4.25. *Pour $p \neq 2$, soit H un groupe algébrique linéaire commutatif défini sur $\mathcal{Q}_p$. On pose G la composante p-connexe de $H(\mathcal{Q}_p)$. Alors G est semi-algébriquement isomorphe à un groupe de la forme :*

$$T \times (1 + p\mathcal{Z}_p)^{\times m} \times \mathcal{Q}_p^{+l}$$

où T est un tore anisotrope défini sur $\mathcal{Q}_p$.

Démonstration. Par la décomposition de Jordan, on a $H \cong H_s \times H_u$, cet isomorphisme est rationnel donc semi-algébrique [5, 4.7].

H_u est commutatif, donc $H_u(\mathcal{Q}_p)$ est polynomialement (ie. semi-algébriquement) isomorphe à $\mathcal{Q}_p^{+l}$ [34, Fact 2.4]. $\mathcal{Q}_p^+$ est divisible donc $\mathcal{Q}_p^+$ est p-connexe.

H_s est un tore, donc par [5, 8.15], $H_s = H_d \cdot H_a$, où H_d est la partie tore déployé et H_a est la partie tore anisotrope, de plus $H_a \cap H_d$ est fini. Comme $H_d(\mathcal{Q}_p)$ est un tore déployé, H_d est polynomialement isomorphe à $\mathcal{Q}_p^{\times m}$, ainsi $H_d(\mathcal{Q}_p)^\square = (1 + p\mathcal{Z}_p)^{\times m}$. Le tore $H_a(\mathcal{Q}_p)$ est anisotrope, on note T sa composante p-connexe. Comme $(1 + p\mathcal{Z}_p)^{\times m}$ est sans torsion, $(1 + p\mathcal{Z}_p)^{\times n} \cap T = \{1\}$ et le produit est direct et $H_s(\mathcal{Q}_p)^\square = T \times (1 + p\mathcal{Z}_p)^{\times m}$. □

Remarque. Pour $p = 2$, le même raisonnement est valable mais $1+p\mathcal{Z}_p = 1+2\mathcal{Z}_2 = \mathcal{Z}_2^\times$ contient de la torsion. Pour éliminer cette torsion, il suffit de prendre $1 + 4\mathcal{Z}_2$. On obtient ainsi :

Proposition 4.25 bis. *Pour $p = 2$, soit H un groupe algébrique linéaire commutatif défini sur $\mathcal{Q}_2$. On pose G la composante p-connexe de $H(\mathcal{Q}_p)$. Alors G contient un sous-groupe d'indice fini semi-algébriquement isomorphe à un groupe de la forme :*

$$T \times (1 + 4\mathcal{Z}_2)^{\times m} \times \mathcal{Q}_2^{+l}$$

où T est un tore anisotrope défini sur $\mathcal{Q}_2$.

Lemme 4.26. *Si H est un sous-groupe $\mathcal{L}$-définissable de $(\mathbb{Z}_p^m, +)$, alors H est un sous-$\mathbb{Z}_p$-module, en particulier H est semi-algébrique et semi-algébriquement isomorphe à $\mathbb{Z}_p^{m'}$, avec $m' \leq m$.*

Démonstration. Il suffit de montrer que si $\mathbf{x} \in H$ et $\lambda \in \mathbb{Z}_p$, alors $\lambda\mathbf{x} \in H$. Si H est ouvert, alors il existe $n \in$ tel que $p^n\mathbb{Z}_p^m \subseteq H$ et pour tout $\mathbf{z} \in H$, $\mathbf{z} + p^n\mathbb{Z}_p^m \subseteq H$. On a $\lambda = \lambda_1 + p^n\lambda_2$ avec $\lambda_1 \in \mathbb{Z}$ et $\lambda_2 \in \mathbb{Z}_p$, alors $\lambda\mathbf{x} = \lambda_1\mathbf{x} + p^n\lambda_2\mathbf{x}$. $\lambda_1\mathbf{x} \in H$ car H est un sous-groupe et donc $\lambda\mathbf{x} \in H$.

Si H n'est pas ouvert, on pose $m' = \dim H$, il existe donc une projection $\rho : \mathbb{Z}_p^m \longrightarrow \mathbb{Q}_p^{m'}$ telle que $\rho(H)$ est d'intérieur non vide, et les fibres de ρ sont finies. En effet, H étant un groupe et ρ un morphisme, les fibres sont toutes isomorphes à $\ker\rho$. Si elles étaient infinies, alors elles seraient de dimension supérieure à 1 et $\dim H \geq m' + 1$ (Fait 4.14). Ainsi $\ker\rho$ est trivial car $\mathbb{Z}_p^m$ n'a pas de sous-groupe fini, et ρ définit bien un isomorphisme sur son image. $\rho(H)$ est d'intérieur non vide. Etant un sous-groupe, il est ouvert, donc si $\lambda \in \mathbb{Z}_p$ et $\mathbf{x} \in H$, alors $\lambda\rho(\mathbf{x}) \in \rho(H)$. D'où $\lambda\mathbf{x} = \rho^{-1}(\rho(\lambda\mathbf{x})) = \rho^{-1}(\lambda\rho(\mathbf{x})) \in H$. □

Lemme 4.26 bis. *Si H est un sous-groupe $\mathcal{L}$-définissable de $(\mathcal{Z}_p^m, +)$, alors H est semi-algébrique et semi-algébriquement isomorphe à $\mathcal{Z}_p^{m'}$.*

Démonstration. La propriété est vraie pour $\mathbb{Q}_p$, d'après le lemme précédent. Il suffit de voir qu'elle s'exprime par un énoncé du premier ordre pour la montrer pour tout $\mathcal{Q}_p$ extension $\mathcal{L}$-élémentaire de $\mathbb{Q}_p$:

$$\mathbb{Q}_p \vDash \forall \bar{b}\ \text{"}\varphi(\bar{x}, \bar{b}) \text{ définit un sous-groupe de } \mathbb{Z}_p^m\text{"} \longrightarrow \exists \bar{a}_1, ..., \bar{a}_{m'} \in \mathbb{Z}_p^m$$
$$(\forall \bar{x}\ (\varphi(\bar{x}, \bar{b}) \longleftrightarrow \exists \lambda_1, ...\lambda_m \in \mathbb{Z}_p \quad \bar{x} = \lambda_1\bar{a}_1 + ... + \lambda_m\bar{a}_{m'}))$$

□

Lemme 4.27.
1. *Les endomorphismes $\mathcal{L}$-définissables de $(\mathcal{Z}_p, +)$ sont de la forme : $x \mapsto ax$ avec $a \in \mathcal{Z}_p$, en particulier, ils sont semi-algébriques ;*
2. *Les endomorphismes $\mathcal{L}$-définissables de $(\mathcal{Q}_p, +)$ sont de la forme : $x \mapsto ax$ avec $a \in \mathcal{Q}_p$, ils sont semi-algébriques ;*
3. *Les endomorphismes $\mathcal{L}$-définissables de $(1 + p\mathcal{Z}_p, \cdot)$ sont de la forme : $x \mapsto x^a$ avec $a \in \mathcal{Z}_p$.*

Remarque. Comme $\exp \in \mathcal{L}$, pour $x \in 1 + p\mathcal{Z}_p$ et $a \in \mathcal{Z}_p$, on définit, x^a par

$$x^a = \exp(a \log(x))$$

Tout élément de $1 + p\mathcal{Z}_p$ admettant une racine n^{ieme} pour n premier à p, on constate que si $a \in \mathbb{Q} \cap \mathbb{Z}_p$, alors $x \mapsto x^a$ est un endomorphisme semi-algébrique de $(1 + p\mathcal{Z}_p, \cdot)$.

Démonstration. Etablissons les résultats pour $\mathbb{Q}_p$, par équivalence élémentaire ils resteront vrais pour $\mathcal{Q}_p$.

1. Si $1 \mapsto a$ alors $n \mapsto an$ pour $n \in \mathbb{Z}$, par [17, 5.4] un endomorphisme définissable est continu à un endroit donc partout. Comme $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, il vient que les seuls endomorphismes définissables de $\mathbb{Z}_p^+$ sont de la forme $x \mapsto ax$ avec $a \in \mathbb{Z}_p$.
2. idem avec $\mathbb{Q}$.
3. On utilise l'isomorphisme entre $(1+p\mathbb{Z}_p)^\times$ et $\mathbb{Z}_p^+$ donné par exp et log qui sont dans $\mathcal{L}$:

$$\begin{array}{ccc} (1+p\mathbb{Z}_p)^\times & \xrightarrow{f} & (1+p\mathbb{Z}_p)^\times \\ \log \downarrow & & \uparrow \exp \\ p\mathbb{Z}_p & \xrightarrow{g} & p\mathbb{Z}_p \end{array}$$

   Si f est un endomorphisme $\mathcal{L}$-définissable de $(1+p\mathbb{Z}_p)^\times$, alors il existe un endomorphisme définissable g de $p\mathbb{Z}_p$ tel que $f = \exp \circ g \circ \log$ ainsi $f(x) = \exp(g(\log(x))) = \exp(a\log(x)) = x^a$.

□

Lemme 4.28. *Soit G est sous-$\mathbb{Z}_p$-module d'un $\mathbb{Q}_p$-espace vectoriel S. Si G est non borné, alors il existe $\mathbf{x} \in G$, $x \neq 0$ tel que pour tout $\lambda \in \mathbb{Q}_p$, $\lambda\mathbf{x} \in G$.*

Démonstration. On considère $S' = \mathbb{Q}_p G$ le sous-espace vectoriel de S engendré par G. Raisonnons par récurrence sur la dimension de S' (en tant qu'espace vectoriel).

Si la dimension de S' (en tant qu'espace vectoriel) est 1, $S' = <\mathbf{e_1}>$ comme pour tout $n \in \mathbb{N}$, il existe $\mathbf{x}_n \in G$ tel que $v_p(\mathbf{x}_n) \leq -n$, on a de manière évidente :

$$G = \bigcup_{n\in\mathbb{N}} \mathbf{x}_n\mathbb{Z}_p = \mathbb{Q}_p\mathbf{e_1}$$

La propriété est ainsi vérifiée au rang 1.

Si S' est de dimension m (en tant qu'espace vectoriel), on note $\mathbf{e_1}, ..., \mathbf{e_m}$ une base de S'. On voit que G est ouvert dans S', en effet par définition de S' il existe μ_1, ..., $\mu_m \in \mathbb{Q}_p$ tels que $\mu_1\mathbf{e_1}, ..., \mu_m\mathbf{e_m} \in G$, ainsi $\mu_1\mathbb{Z}_p\mathbf{e_1} \oplus ... \oplus \mu_m\mathbb{Z}_p\mathbf{e_m} \subseteq G$. Donc il existe n_0 tel que $p^{n_0}\mathbb{Z}_p\mathbf{e_1} \oplus ... \oplus p^{n_0}\mathbb{Z}_p\mathbf{e_m} \subseteq G$, pour simplifier les notations on supposera $n_0 = 0$. Comme G est non borné, pour tout $n \in \mathbb{N}$, il existe $\mathbf{x}_n \in G \cap S$ tel que $v_p(\mathbf{x}_n) \leq -n$, on note :

$$\mathbf{x}_n = \lambda_1^{(n)}\mathbf{e_1} + ... + \lambda_m^{(n)}\mathbf{e_m}$$

On pose $\zeta_n = \max\{v_p(\lambda_1^{(n)}), ..., v_p(\lambda_m^{(n)})\} - \min\{v_p(\lambda_1^{(n)}), ..., v_p(\lambda_m^{(n)})\} \in \mathbb{N}$. On peut supposer que $\min\{v_p(\lambda_1^{(n)}), ..., v_p(\lambda_m^{(n)})\} = -n$.

• Si $\{\zeta_n\}_{n\in\mathbb{N}}$ est bornée, notons N une borne. On a :

$$\lambda_i^{(n)} = p^{-n}p^{k_i^{(n)}}u_i^{(n)} \quad \text{avec } k_i^{(n)} \in \{0, ..., N\} \text{ et } u_i^{(n)} \in \mathbb{Z}_p^\times$$

Ainsi pour tout $n \in \mathbb{N}$, on a $(k_1^{(n)}, ..., k_m^{(n)}) \in \{0, ..., N\}^m$. Il y a un nombre fini de choix de $(k_1^{(n)}, ..., k_m^{(n)})$. Comme il y a un nombre infini de $\mathbf{x}_n$ possible, il y a par le "principe des tiroirs" une infinité de $\mathbf{x}_n$ qui ont la même combinaison $(k_1, ..., k_m)$. On extrait alors une sous-suite $(\mathbf{x'}_n)_{n\in\mathbb{N}}$ dont les coordonnées dans la base $(\mathbf{e_1}, ..., \mathbf{e_m})$ sont pour tout $n \in \mathbb{N}$ et $i \in \{1, ..., m\}$:

$$\lambda_i^{(n)} = p^{-n} p^{k_i} u_i^{(n)}$$

(quitte à multiplier par une puissance de p convenable, on peut toujours supposer que $-n = \min\{v_p(\lambda_1^{(n)}), ..., v_p(\lambda_m^{(n)}\})$) On remarque que k_i ne dépend pas de n. Ainsi :

$$\mathbf{x'}_n = \sum_{1\le i\le m} p^{-n} p^{k_i} u_i^{(n)} \mathbf{e_i} \quad \text{et} \quad \mathbf{x'}_{n+1} = \sum_{1\le i\le m} p^{-n-1} p^{k_i} u_i^{(n+1)} \mathbf{e_i}$$

Pour tout n, on effectue le calcul suivant :

$$\mathbf{x''}_n = \mathbf{x'}_n - p\frac{u_1^{(n)}}{u_1^{(n+1)}}\mathbf{x'}_{n+1} = 0\mathbf{e_1} + \sum_{2\le i\le m} p^{-n} p^{k_i} (u_i^{(n)} - \frac{u_1^{(n)}}{u_1^{(n+1)}} u_i^{(n+1)})\mathbf{e_i} \in G \qquad (4.2)$$

Si l'ensemble $\{n \in \mathbb{N} \mid \mathbf{x''}_n \neq 0\}$ est fini, alors cela signifie qu'il existe un rang n_1 à partir duquel $\mathbf{x''_n} = 0$ pour tout $n \geq n_1$. Ainsi pour $n \geq n_1$ et $1 \leq i \leq m$, on a $u_i^{(n)} - \frac{u_1^{(n)}}{u_1^{(n+1)}} u_i^{(n+1)} = 0$ et $\frac{u_i^{(n)}}{u_1^{(n)}} = \frac{u_i^{(n+1)}}{u_1^{(n+1)}} = z_i$, aussi pour $n \geq n_1$:

$$\mathbf{x'_n} = \sum_{1\le i\le m} p^{-n} p^{k_i} u_1^{(n)} z_i \mathbf{e_i}$$

en posant $z_1 = 1$. On considère alors :

$$\mathbf{x} = \sum_{1\le i\le m} p^{k_i} z_i \mathbf{e_i} \in G \cap S$$

et pour $\lambda \in \mathbb{Q}_p$ ($\lambda = p^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$) :

– si $n \geq 0$, alors $\lambda\mathbf{x} \in G$, car G est un $\mathbb{Z}_p$-module ;

– si $n < 0$, alors $\lambda\mathbf{x} = \frac{u}{u_1^{(n)}}\mathbf{x'}_{-n} \in G$.

Ainsi on a montré qu'il existe $\mathbf{x} \in G$ tel que $\forall\lambda \in \mathbb{Q}_p$, $\lambda\mathbf{x} \in G$.

Si l'ensemble $\{n \in \mathbb{N} \mid \mathbf{x''}_n \neq 0\}$ est infini. On a $\{\mathbf{x''}_n\}_{n\in\mathbb{N}} \subseteq < \mathbf{e_2}, ...\mathbf{e_m} >$, ainsi $G \cap < \mathbf{e_2}, ..., \mathbf{e_m} >$ est un sous-$\mathbb{Z}_p$-module qui est non borné, donc par hypothèse de récurrence il existe $\mathbf{x} \in G$ tel que pour tout $\lambda \in \mathbb{Q}_p$ $\lambda\mathbf{x} \in G$.

• Si $\{\zeta_n\}_{n\in\mathbb{N}}$ est non borné. Quitte à extraire une sous-suite et à renommer les indices, on peut supposer que $v_p(\lambda_m^{(n)}) = \min\{v_p(\lambda_1^{(n)}), ..., v_p(\lambda_m^{(n)})\} = -n$ pour tout $n \in \mathbb{N}$. Il existe $i_0 \in \{1, 2, ..., m\}$ tel que

$$\forall\omega\exists n \in \mathbb{N} \quad v_p(\lambda_{i_0}^{(n)}) - v_p(\lambda_m^{(n)}) \geq \omega \qquad (4.3)$$

Quitte à changer les indices, on peut supposer $i_0 = 1$. Nous allons montrer que $G \cap < \mathbf{e_2}, ..., \mathbf{e_m} >$ est non borné. Soit ω et n tels que (4.3) soit vérifié, on a :

$$\mathbf{x}_n = p^{-n+\omega} u_1^{(n)} \mathbf{e_1} + \sum_{i=2}^{m} p^{-n} u_i^{(n)} \mathbf{e_i} \quad \text{avec} \begin{cases} u_i^{(n)} \in \mathbb{Z}_p \text{ pour } i \in \{1, ..., m-1\} \\ u_m^{(n)} \in \mathbb{Z}_p^\times \end{cases}$$

$$p^{n-\omega}\mathbf{x}_n = u_1^{(n)}\mathbf{e_1} + \sum_{i=2}^{m} p^{-\omega}u_i^{(n)}\mathbf{e_i} \in G$$

Comme $u_1^{(n)}\mathbf{e_1} \in \mathbb{Z}_p\mathbf{e_1} \subseteq G$, alors $\sum_{i=2}^{m} p^{-\omega}u_i^{(n)}\mathbf{e_i} \in G$. Et $G \cap < \mathbf{e_2}, ..., \mathbf{e_m} >$ est non borné, et on conclut grâce à l'hypothèse de récurrence. □

Lemme 4.29. *Les sous-groupes $\mathcal{L}$-définissables de $\mathcal{Q}_p^{+l}$ sont semi-algébriques, et semi-algébriquement isomorphes à $\mathcal{Q}_p^{l_1} \times \mathcal{Z}_p^{l_2}$ pour $l_1 + l_2 \leq l$.*

Démonstration. On raisonnera dans $\mathbb{Q}_p$, le résultat pouvant s'énoncer par une formule du premier ordre, il sera vrai pour $\mathcal{Q}_p$. Soit G un sous-groupe définissable de $\mathbb{Q}_p^{+l}$, on peut démontrer comme dans le lemme 4.26 que G est un sous-$\mathbb{Z}_p$-module. On note :

$$G' = \{x \in G \mid \forall \lambda \in \mathbb{Q}_p \quad \lambda x \in G\}$$

On montre facilement que G' est un sous-espace vectoriel de $\mathbb{Q}_p^l$. On considère S un suplémentaire de G' dans $\mathbb{Q}_p^l$. Comme $\mathbb{Q}_p^l = G' \oplus S$ en tant qu'espace vectoriel, on obtient aisément la décomposition de G en produit direct de sous-groupes $G = G' \times (G \cap S)$. Le groupe G' est semi-algébrique et semi-algébriquement isomorphe à $\mathbb{Q}_p^{l_1}$.

Par le lemme 4.28, si $G \cap S$ est non borné, il existe $x \in G \cap S$ tel que pour tout $\lambda \in \mathbb{Q}_p$, $\lambda x \in G \cap S$ donc $x \in G'$, ce qui est absurde. Donc il existe n tel que $G \cap S \subseteq p^n\mathbb{Z}_p^{l-l_1}$, et par le lemme 4.26, on en déduit que $G \cap S$ est semi-algébriquement isomorphe à $\mathbb{Z}_p^{l_2}$ pour $l_2 \leq l - l_1$. □

On rappelle le fait suivant qui nous permettra de décrire la structure d'un tore anisotrope de dimension quelconque.

Fait 4.30 ([36, Theorem BTR])**.** *Soit K un corps muni d'une valuation non triviale et non archimédienne. Soit T un K-tore.*

T est anisotrope si et seulement si T est borné.

Proposition 4.31. *Soit T un $\mathcal{Q}_p$-tore anisotrope de dimension n. Alors T se décompose de la manière suivante :*

$$T = \widetilde{T} \times T^{\square}$$

où $\widetilde{T} \cong res(T)$ est fini, et $T^{\square}$ est la composante p-connexe de T. Plus précisement $T^{\square}$ contient un sous-groupe d'indice fini (une puissance de p) $\mathcal{L}_{\exp}$-définissablement isomorphe au groupe additif $\mathcal{Z}_p^n$.

Démonstration. On sait par le fait 4.30 que T est définissablement isomorphe à un sous-groupe du groupe multiplicatif de l'anneau de valuation $\mathcal{O}^\times$ d'une extension fini K de $\mathcal{Q}_p$. Comme $\mathcal{O}^\times \cong k^\times \times (1 + \pi\mathcal{O})^\times$ et $\mathcal{O}^{\times\square} = 1 + \pi\mathcal{O}$, on a $\widetilde{T} \cong T \cap k$ et $T^{\square} = T \cap (1 + \pi\mathcal{O})$ et la décomposition est immédiate.

En travaillant dans le modèle standard $\mathbb{Q}_p$, on sait par la proposition 4.4, que si K' est une extension finie de $\mathbb{Q}_p$ et $\mathcal{O}'$ son anneau de valuation, alors $(1+\pi\mathcal{O}')^\times$ contient le sous-groupe $(1+\pi^{r+1}\mathcal{O})$ d'indice p^r tel que $\exp_{K'}$ établisse un isomorphisme entre

$(1+\pi^{r+1}\mathcal{O})$ et $\pi^{r+1}\mathcal{O}^+ \cong \mathbb{Z}_p^m$. Par équivalence $\mathcal{L}$-élémentaire, on obtient que $(1+\pi\mathcal{O})^\times$ contient un sous-groupe G' d'indice p^r tel que $\exp_K$ établisse un isomorphisme entre G' et $\pi^{r+1}\mathcal{O} \cong \mathcal{Z}_p^m$. Ainsi $T' = G' \cap T^\square$ est isomorphe à un sous-groupe $\mathcal{L}$-définissable de $\mathcal{Z}_p^m$ donc isomorphe à $\mathcal{Z}_p^{m'}$ par le lemme 4.26 bis. Aussi $T^\square$ contient un sous-groupe d'indice fini, isomorphe à $\mathcal{Z}_p^{m'}$. □

Théorème 4.32. *Soit G un sous-groupe $\mathcal{L}$-définissable commutatif p-connexe de $GL_n(\mathcal{Q}_p)$, alors :*
- *G est définissable dans le langage $\mathcal{L}_{\exp}$;*
- *G est $\mathcal{L}_{\exp}$-définissablement isomorphe à un groupe semi-algébrique ;*
- *G est virtuellement de la forme $\mathcal{Z}_p^l \times \mathcal{Q}_p^{l'}$.*

Démonstration. Pour $p \neq 2$, on considère $G' = \overline{G}^{\widetilde{\mathcal{Q}_p}^{alg}\square}(\mathcal{Q}_p)$ la composante p-connexe de la clôture de Zariski de G. G' est algébrique, commutatif et p-connexe donc $G' \cong T \times (1+p\mathcal{Z}_p)^{\times m} \times \mathcal{Q}_p^{+r}$ (proposition 4.25) . A l'aide des fonctions exp et $\exp_K$ G' est isomorphe à un groupe contenant comme sous-groupe d'indice fini $\mathcal{Z}_p^n \times \mathcal{Z}_p^m \times \mathcal{Q}_p^r$ (proposition 4.31). G est, à isomorphisme près, un sous-groupe de ce dernier donc, en le plongeant dans $\mathcal{Q}_p^{r+m+n}$, on voit que G est définissablement isomorphe à $\mathcal{Z}_p^l \times \mathcal{Q}_p^{l'}$ (lemmes 4.26 bis et 4.29).

Pour $p = 2$, avec les mêmes notations G' contient un sous-groupe d'indice fini isomorphe à $T \times (1+4\mathcal{Z}_2)^{\times m} \times \mathcal{Q}_2^{+r}$. Par la proposition 4.31, ce dernier contient un sous-groupe d'indice fini isomorphe à $\mathcal{Z}_2^n \times \mathcal{Z}_2^m \times \mathcal{Q}_2^r$, on peut alors conclure de la même manière. □

On termine le chapitre par un lemme, qui peut servir à extension du théorème 4.32 au cas nilpotent.

Lemme 4.33. *Soit G un sous-groupe $\mathcal{L}$-définissable p-connexe, commutatif de $GL_n(\mathcal{Q}_p)$ et soit H un sous-groupe définissable de G tel que G/H soit sans torsion, alors il existe un sous-groupe $\mathcal{L}$-définissable H' tel que $G = H \times H'$.*

Démonstration. En raisonnant à isomorphisme $\mathcal{L}$-définissable près, on peut supposer que G contient un sous-groupe G_1 d'indice fini de la forme $\mathcal{Z}_p^l \times \mathcal{Q}_p^m$ (Proposition 4.32). On plonge G_1 dans $\mathcal{Q}_p^{m+l}$, par les lemmes 4.29 et 4.26 bis, $H_1 = H \cap G_1$ est de la forme :

$$H_1 = \mathcal{Z}_p\mathbf{e_1} \oplus ... \oplus \mathcal{Z}_p\mathbf{e_{l'}} \oplus \mathcal{Q}_p\mathbf{e'_1} \oplus ... \oplus \mathcal{Q}_p\mathbf{e'_{m'}}$$

où $\{\mathbf{e_1}, ..., \mathbf{e_{l'}}, \mathbf{e'_1}, ..., \mathbf{e'_{m'}}\}$ est un système libre de l'espace vectoriel $\mathcal{Q}_p^{l+m}$, on le complète système en une base à l'aide des vecteurs $\{\mathbf{e''_1}, ..., \mathbf{e''_{m''}}\}$ et on pose $H'_1 = \mathcal{Q}_p\mathbf{e''_1} \oplus ... \oplus \mathcal{Q}_p\mathbf{e''_{m''}} \cap \mathcal{Z}_p^l \times \mathcal{Q}_p^m$. Le groupe G/H étant sans torsion, cela nous assure que $\mathcal{Q}_p\mathbf{e_1} \oplus ... \oplus \mathcal{Q}_p\mathbf{e_{l'}} \oplus \mathcal{Q}_p\mathbf{e'_1} \oplus ... \oplus \mathcal{Q}_p\mathbf{e'_{m'}} \cap \mathcal{Z}_p^l \times \mathcal{Q}_p^m = H_1$. On a ainsi que $G_1 = H_1 \times H'_1$.

HG_1 est d'indice fini n dans G, et soit $\{a_i\}_{0\leq i\leq n}$ les représentants des classes modulo H'_1 qui représentent les cosets modulo HG_1. Ainsi $H' = \bigcup_{0\leq i\leq n} a_i H'_1$ est un sous-groupe définissable de G tel que $G = H \times H'$. □

Chapitre 5

Généricité et générosité

La notion importante de généricité a été particulièrement développée par B. Poizat pour les groupes dans des théories stables [35]. Dans tout groupe qui admet une notion géométrique de dimension, on s'attend à pouvoir caractériser la généricité en termes de dimension maximal. Le terme *généreux* a été introduit par E. Jaligot dans [22] afin de montrer un théorème de conjugaison.

Le but de ce chapitre est de dire quels sous-groupes définissables de $SL_2(\mathcal{Q}_p)$ sont généreux. Nous allons montré que le seul sous-groupe de Cartan généreux est Q_1 à conjugaison près. Cela généralise un résultat similaire pour les corps réellement clos, démontré dans [2].

Définition 5.1. – *Une partie X d'un groupe G est dite* générique *si G peut être recouvert par un nombre fini de translatés de X :*

$$G = \bigcup_{i=1}^{n} g_i \cdot X$$

– *X est* généreux *si l'union de ses conjugués $X^G = \bigcup_{g \in G} X^g$ est générique.*

Remarque. Si G est un sous-groupe définissable dans un corps p-adiquement clos, alors la généricité implique d'être de dimension maximale. La réciproque est fausse : $\dim \mathbb{Z}_p = \dim \mathbb{Q}_p$ mais $\mathbb{Z}_p$ n'est pas générique dans $(\mathbb{Q}_p, +)$.

Commençons par une proposition générale, vraie pour tout corps valué.

Proposition 5.2. *Soit (K, v) un corps valué.*

1. *L'ensemble $W = \{A \in SL_2(K) \mid v(tr(A)) < 0\}$ est générique dans $SL_2(K)$.*
2. *L'ensemble $W' = \{A \in SL_2(K) \mid v(tr(A)) \geq 0\}$ n'est pas générique dans $SL_2(K)$.*

Démonstration. 1. On considère les matrices :

$$A_1 = I, \quad A_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \quad \text{et} \quad A_4 = \begin{pmatrix} 0 & -b^{-1} \\ b & 0 \end{pmatrix}$$

avec $v(a) > 0$ et $v(b) > 0$.

Montrons par l'absurde que $SL_2(K) = \bigcup_{i=1}^{4} A_iW$. Supposons qu'il existe

$$M = \begin{pmatrix} x & y \\ u & t \end{pmatrix} \in SL_2(K)$$

tel que $M \notin \bigcup_{i=1}^{4} A_iW$.

Comme $M \notin A_1W \bigcup A_2W$, on a $x + t = \varepsilon$ et $y - u = \delta$ avec $v(\varepsilon) \geq 0$ et $v(\delta) \geq 0$. Comme $M \notin A_3W$, on a $ax + a^{-1}t = \eta$ avec $v(\eta) \geq 0$. On en déduit $t = \frac{\eta - a\varepsilon}{a^{-1}-a}$. De même, il vient de $M \notin A_4W$ que $u = \frac{\theta + b\delta}{b^{-1}-b}$ avec θ vérifiant $v(\theta) \geq 0$.

Comme $v(a) > 0$, on a $v(a^{-1} - a) < 0$. De $v(\eta - a\varepsilon) \geq \min\{v(\eta); v(a\varepsilon)\} \geq 0$, on en déduit que $v(t) = v(\frac{\eta - a\varepsilon}{a^{-1}-a}) = v(\eta - a\varepsilon) - v(a^{-1} - a) > 0$. De même $v(u) > 0$. Il vient que $v(x) = v(\varepsilon - t) \geq 0$ et $v(y) \geq 0$.

C'est pourquoi $v(det(M)) = v(xt - uy) \geq \min\{v(xt), v(uy)\} > 0$ et alors $det(M) \neq 1$, ce qui est absurde.

2. On montre que la famille de matrices $(M_x)_{x \in K^\times}$ ne peut être recouverte par un nombre fini de $SL_2(K)$-translatés de W', où :

$$M_x = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$$

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(K)$. Alors $tr(A^{-1}M_x) = dx + ax^{-1}$. Si $v(x) > \max\{|v(a)|, |v(d)|\}$ alors $v(tr(A^{-1}M_x)) < 0$ et $M_x \notin AW'$.

C'est pourquoi pour toute famille finie $\{A_j\}_{i \leq n}$, il existe $x \in K$ tel que $M_x \notin \bigcup_{j=1}^{n} A_jW'$. □

Remarque. On remarque que les ensembles W et W' forment une partition de $SL_2(K)$. Ils sont tous les deux définissables dans le langage des corps si la valuation v est définissable.

On se concentre maintenant sur $\mathbb{Q}_p$. Rappelons que si $p \neq 2$ alors un élément $x \in \mathbb{Q}_p^\times$ est un carré si et seulement si $v_p(x)$ est paire et $ac(x)$ est un carré dans $\mathbb{F}_p$. Pour $p = 2$, un élément $x \in \mathbb{Q}_2$ peut être écrit $x = 2^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_2^\times$, alors x est un carré si n est paire et $u \equiv 1 \mod 8$ [40].

Lemme 5.3. *$W \subseteq Q_1^{SL_2(\mathbb{Q}_p)}$ et pour $\delta \in \mathbb{Q}_p^\times \setminus (\mathbb{Q}_p^\times)^2$ et $\mu \in GL_2(\mathbb{Q}_p)$, $Q_\delta^{\mu \cdot SL_2(\mathbb{Q}_p)} \subseteq W'$, de plus $U^{SL_2(\mathbb{Q}_p)} \subseteq W'$.*

Démonstration. Soit $A \in SL_2(\mathbb{Q}_p)$ avec $v_p(tr(A)) < 0$.
Pour $p \neq 2$, comme $v_p(tr(A)) < 0$, on a $v_p(tr(A)^2 - 4) = 2v_p(tr(A))$ et $ac(tr(A)^2 - 4) = ac(tr(A)^2)$, donc $tr(A)^2 - 4$ est un carré dans $\mathbb{Q}_p$.
Pour $p = 2$, on peut écrire $tr(A) = 2^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$. Alors $tr(A)^2 - 4 = 2^{2n}(u^2 - 4 \cdot 2^{-2n})$. Comme $n \leq -1$, $u^2 - 4 \cdot 2^{-2n} \equiv u^2 \equiv 1 (\mod 8)$, donc $tr(A)^2 - 4 \in (\mathbb{Q}_2^\times)^2$.

Dans tous les cas, par la proposition 3.4, $W \subseteq Q_1^{SL_2(\mathbb{Q}_p)}$ et en passant au complémentaire, $Q_\delta^{\mu \cdot SL_2(\mathbb{Q}_p)} \subseteq W'$, et $U^{SL_2(\mathbb{Q}_p)} \subseteq W'$. □

On peut maintenant conclure avec le corollaire suivant, similaire à [2, Remark 9.8] :

Corollaire 5.4. *Soit $\mathcal{Q}_p$ un corps p-adiquement clos.*

1. *Le sous-groupe de Cartan Q_1 est généreux dans $SL_2(\mathcal{Q}_p)$.*
2. *Les sous-groupes de Cartan Q_δ^μ (pour $\delta \in \mathcal{Q}_p^\times \setminus (\mathcal{Q}_p^\times)^2$ et $\mu \in GL_2(\mathcal{Q}_p)$) ne sont pas généreux dans $SL_2(\mathcal{Q}_p)$.*
3. *U n'est pas généreux.*

Démonstration. Le lemme 5.3 montre que $Q_1^{SL_2(\mathbb{Q}_p)}$ est générique. $Q_1^{SL_2(\mathbb{Q}_p)}$ est définissable sans paramètre, appelons $\varphi(x)$ la formule qui le défini, donc

$$\mathbb{Q}_p \vDash \exists a_1, ..., a_n \in S \quad \forall x \in S \quad \bigvee_{i=1}^{n} \varphi(a_i^{-1} x)$$

$\mathcal{Q}_p$ satisfait la même formule et Q_1 est généreux dans $SL_2(\mathcal{Q}_p)$. De même, si Q_δ et U étaient généreux dans $SL_2(\mathcal{Q}_p)$ pour un modèle $\mathcal{Q}_p$, alors par équivalence élémentaire ils seraient généreux dans $SL_2(\mathbb{Q}_p)$, ce qui n'est pas le cas. □

Remarque. Si K est un corps élémentairement équivalent à une extension finie de $\mathbb{Q}_p$, la même caractérisation des carrés dans $K^\times$ est valable, donc le même résultat que le Corollaire 5.4 est vrai.

Perspectives

Pour conclure cette thèse, nous donnons dans ce chapitre quelques perspectives qui se dégagent de ce travail. Nous partirons systématiquement des résultats établis afin d'essayer de distinguer des développements possibles. Nous donnerons par la suite quelques pistes, non encore abouties, pour démontrer ces conjectures. Dans ce qui suit, nous conservons les notations introduites tout au long du document.

Chaînes de sous-groupes et composantes p-connexes

Dans le chapitre 3, il apparaît que tout sous-groupe infini $\mathcal{L}_R$-définissable de $SL_2(\mathcal{Q}_p)$ contient une chaîne infinie de sous-groupes définissables. Au chapitre 4, après avoir introduit la notion de p-connexité, nous constatons que tout groupe linéaire commutatif $\mathcal{L}$-définissable possède une composante p-connexe non triviale et semi-algébrique.

Conjecture. *Soit G un groupe définissable dans un corps p-adiquement clos. Alors*
- *G contient une chaîne infinie de sous-groupes définissables.*
- *la composante p-connexe $G^{\square}$ existe, elle est non triviale et définissable.*

Ces questions sont importantes pour plusieurs raisons. Tout d'abord $\mathbb{Q}_p$ étant une structure NIP, on sait que tout groupe définissable possède une composante connexe $G^{\circ\circ}$ qui est type-définissable, toutefois il arrive dans certain modèle qu'elle soit triviale (exemple : $\mathbb{Z}_p^{\circ\circ} = \{0\}$). L'existence d'une composante p-connexe définissable non triviale pour tout groupe définissable dans $\mathbb{Q}_p$ palierait à ce problème sans avoir besoin de passer à un modèle saturé. Il se peut que pour une utilisation optimale de la p-connexité, on doive rajouter une condition de définissabilité des sous-groupes dans la définition de cette dernière.

Il est naturel en théorie des modèles d'étudier les groupes avec des conditions de chaînes. Existe-t-il une condition de chaîne pour les groupes définissables dans $\mathbb{Q}_p$ autre que celle de Baldwin-Saxl ?

Groupes linéaires commutatifs définissables dans des structures p-minimales

Nous avons démontré (théorème 4.32) que si $\mathcal{L} \supseteq \mathcal{L}_{\exp}$ et si $\mathbb{Q}_p$ vu dans le langage $\mathcal{L}$ est une structure p-minimale, alors un groupe linéaire commutatif p-connexe

$\mathcal{L}$-définisable est $\mathcal{L}$-définissablement isomorphe à un groupe semi-algébrique. Une question naturelle est alors de savoir si on peut affiner ce résultat en ne supposant pas $\mathcal{L}_{\exp} \subseteq \mathcal{L}$.

Pour construire $\mathcal{L}_{\exp}$, on a besoin d'ajouter un symbole $\exp_K$ représentant la fonction exponentielle sur chaque extension finie K de $\mathbb{Q}_p$. Est-ce vraiment nécessaire ? Autrement dit $\exp_K$ est-il définissable dans $\mathcal{L}_R \cup \{\exp_{\mathbb{Q}_p}\}$? La réponse à cette question n'est pas triviale. Actuellement nous ne penchons vers aucune hypothèse. Dans le cas réel, il est évident que l'exponentielle complexe n'est pas définissable à partir de l'exponentielle réelle, mais le fait que $K^\times$ et $\mathbb{Q}_p^\times$ sont proches en termes de structure est un signe du fait qu'on ne puisse pas généraliser, a priori, ce résultat à $\mathbb{Q}_p$. Dans ce contexte, on peut citer le travail de N. Mariaule dans [26] où il utilise un langage $\mathcal{L}_{pEC}$ proche de notre $\mathcal{L}_{exp}$, il démontre que la théorie de $\mathbb{Z}_p$ dans ce langage est décidable.

Il est également utile de pouvoir décrire les sous-groupes $\mathcal{L}$-définissables de $(1+p\mathcal{Z}_p)^{\times m}$ et du tore anisotrope T sans avoir recours à l'exponentielle, et notamment d'exhiber les sous-groupes semi-algébriques de ces derniers. L'étude de la semi-algébricité de $x \mapsto x^a$ pour $a \in \mathbb{Z}_p$ sera un point important pour décrire les sous-groupes semi-algébriques de $(1+p\mathcal{Z}_p)^{\times m}$. La partie la plus délicate restera de décrire les sous-groupes définissables du tore anisotrope autrement que comme l'image par l'exponentielle de sous-groupes de $\mathbb{Z}_p^n$. On voit déjà que les ensembles $T \cap (1+\pi^n\mathcal{O})$ forment des sous-groupes semi-algébriques. Y en a-t-il d'autres ? Si on regarde le cas du tore anisotrope de dimension 1, on a (pour $p \neq 2$) $(1+\pi\mathcal{O})^\times = T^\square \times \mathbb{Z}_p^\times$, d'autre part $\exp_K : \pi\mathcal{O}^+ \longrightarrow (1+\pi\mathcal{O})^\times$ et $\exp_K(p\mathbb{Z}_p) = 1+p\mathbb{Z}_p$ car $\exp_K$ prolonge $\exp_{\mathbb{Q}_p}$. On a $\mathcal{O}^+ \cong \mathbb{Z}_p^2$ et si on identifie $\mathbb{Z}_p \times \{0\}$ à $\mathbb{Z}_p$ dans $\mathcal{O}$, il n'est pas clair que $\exp_K(\{0\} \times \mathbb{Z}_p) = T^\square$. Plus généralement, si on identifie $\mathcal{O}^+$ à $\mathbb{Z}_p^n$, il ne semble pas évident de décrire $\exp_K(\mathbb{Z}_p^{(i)})$ où $\mathbb{Z}_p^{(i)} = \{(0,...,0)\} \times \mathbb{Z}_p \times \{(0,...,0)\}$ à la $i^{\text{ième}}$ place, ni même de savoir si cette image est semi-algébrique.

Le théorème 4.32 porte sur les groupes commutatifs p-connexes. Peut-on généraliser ce résultat aux groupes non p-connexes ?

Conjecture. *Soit G un sous-groupe $\mathcal{L}$-définissable commutatif de $GL_n(\mathcal{Q}_p)$ alors G est définissablement isomorphe à un groupe semi-algébrique.*

Plus précisément, G est virtuellement isomorphe à

$$\{(a_{1,\gamma_1},...,a_{m,\gamma_m}) \in \mathcal{Q}_p^m \mid v_p(a_{i,\gamma_i}) = \gamma_i \text{ et } \gamma_i \in n_i\Gamma\} \cdot G^\square$$

Cette conjecture se base sur la proposition 3.12 où on obtient un résultat similaire pour les sous-groupes définissables de Q_1. Si $G^\square$ est d'indice fini dans G, alors la semi-algébricité est evidente. Dans le cas contraire, on voit dans la proposition 4.25 qu'un groupe linéaire commutatif se décompose en terme de $\mathcal{Q}_p^+$, de $\mathcal{Q}_p^\times$ et de tore anisotrope. Parmi ceux-là, seul le groupe multiplicatif $\mathcal{Q}_p^\times$ possède une composante p-connexe d'indice infinie. Il devient important alors de décrire les cosets de $\mathcal{Q}_p^{\times\square}$ en termes définissables. Pour établir ce résultat, il faut décrire les sous-groupes $\mathcal{L}$-définissables en termes d'ouverts, et expliciter l'image par la valuation d'un groupe multiplicatif ouvert dans le groupe de valeurs Γ.

Groupes linéaires nilpotents définissables dans des structures p-minimales

Le théorème 4.32 est établi pour les groupes commutatifs. Il est naturel de se poser la question de ce qu'il en est dans les cas nilpotents ou résolubles. Dans [32], où le cas o-minimal est traité, un résultat est donné pour le cas nilpotent et un contre-exemple est donné pour le cas résoluble.

Conjecture. *Si G est un groupe $\mathcal{L}$-définissable nilpotent p-connexe, alors G est définissablement isomorphe à un groupe semi-algébrique.*

La preuve de [32] n'est pas adaptable directement au cas p-adique. En effet, il est montré qu'un groupe nilpotent unipotent connexe définissable dans un enrichissement o-minimal d'un corps réellement clos est algébrique, ce qui est faux dans le cas p-adique. Il semble envisageable de faire un raisonnement par récurrence sur la classe de nilpotence du groupe.

Les contre-exemples développés dans [32], pour le cas résolubles semblent facilement transposables au cas p-adique. La semi-algébricité des exemples donnés se traduit par le définissabilité de $(\mathbb{Q}_p, +, \cdot, \exp)$ dans $(\mathbb{Q}_p, +, \cdot)$. Or exp ne semble pas définissable dans $(\mathbb{Q}_p, +, \cdot)$ [16].

Généricité et Générosité

Dans le corollaire 5.4, on établit que Q_1 est le seul sous-groupe de Cartan généreux de $SL_2(\mathcal{Q}_p)$ à conjugaison près. Ce résultat est-il généralisable en dimension supérieure ? Et dans le cas général, peut-on obtenir un résultat similaire à [2], où E. Baro, E. Jaligot et M. Otero démontrent que dans un groupe définissable dans une structure o-minimale, un seul sous-groupe de Cartan est généreux ?

La définition que nous donnons de la généricité est issue du contexte stable [35]. Dans le contexte des groupes définissables dans les corps p-adiques, la généricité bénéficie-t-elle des mêmes propriétés ? En particulier, la généricité à gauche est-elle équivalente à la généricité à droite ? Dans [29], A. Onshuus et A. Pillay répondent positivement à cette question dans le cas compact.

Index

Bibliographie

[1] Louis Aragon. Que la vie en vaut la peine. *Les yeux et la mémoire*, 1954.

[2] Elias Baro, Eric Jaligot, and Margarita Otero. Cartan subgroups of groups definable in o-minimal structures. arXiv :1109.4349v2 [math.GR], 2011.

[3] Luc Bélair. Panorama of p-adic model theory. *Annales des Sciences Mathématiques du Québec*, 36(1) :43–73, 2013.

[4] Luc Bélair, Lou van den Dries, and Angus Macintyre. Elementary equivalence and codimension in p-adic fields. *manuscripta mathematica*, 62 :219–225, 1988.

[5] Armand Borel. *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer, second enlarged edition edition, 1991.

[6] Zoé Chatzidakis. Théorie des modèles des corps valués. disponible sur http ://www.logique.jussieu.fr/ zoe/, 2008.

[7] Gregory Cherlin. Groups of small morley rank. *Annals of Mathematical Logic*, 17 :1–28, 1979.

[8] Claude Chevalley. *Théorie des groupes de Lie II. Groupes algébriques.* Hermann, Paris, 1951.

[9] Raf Cluckers. Analytic p-adic cell decomposition and integrals. *Trans. Amer. Math. Soc.*, 356 :1489–1499, 2004.

[10] Françoise Delon. Définissabilité avec paramètres extérieurs dans $\mathbb{Q}_p$ et $\mathbb{R}$. *Proceedings of the American Mathematical Society*, 106(1) :193–198, 1989.

[11] Jan Denef. p-adic semi-algebraic sets and cell decomposition. *Journal für die Reine und Angewandte Mathematik*, 369 :154–166, 1986.

[12] Jan Denef and Lou van den Dries. p-adic end real subanalytic sets. *Annals of Mathematics*, 128(1) :79–138, 1988.

[13] Benjamin Druart. Definable subgroups in sl_2 over a p-adically closed fields. arXiv :1501.06834v1, 2015.

[14] Olivier Frécon. Conjugacy of carter subgroups in groups of finite morley rank. *Journal of Mathematical Logic*, 8(1) :41–92, 2008.

[15] Olivier Frécon and Eric Jaligot. The existence of carter subgroups in groups of finite morley rank. *Journal of Group Theory*, 8 :623–633, 2005.

[16] Deirdre Haskell, Ehud Hrushovski, and Dugald Macpherson. Unexpected imaginaries in valued fields with analytic structure. *Journal of Symbolic Logic*, 78(2) :523–542, 2013.

[17] Deirdre Haskell and Dugald Macpherson. A version of o-minimality for the p-adics. *Journal of Symbolic Logic*, 62(4) :1075–1092, 1997.

[18] Wilfrid Hodges. *Model Theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1993.

[19] Ehud Hrushovski, Ben Martin, Silvain Rideau, and Raf Cluckers. Definable equivalence relations and zeta fonctions of groups. arXiv :math/0701011v3, 2015.

[20] Victor Hugo. Je travaille. *Toute la lyre*, ? ?

[21] James E. Humphreys. *Linear Algebraic Groups*. Graduate Texts in Mathematics. Springer, 1998.

[22] Eric Jaligot. Generix never gives up. *J. Symbolic Logic*, 71(2) :599–610, 2006.

[23] Serge Lang. *Algèbre*. DUNOD, 3ème edition, 2004.

[24] David Llewellyn-Jones. *Presburger Arithmetic and Pseudo-Recursive Saturation*. PhD thesis, University of Birmingham, 2001.

[25] Angus MacIntyre. On definable subsets of p-adic fields. *The Journal of Symbolic Logic*, 41(3) :605–610, 1976.

[26] Nathanaël Mariaule. p-adic exponential ring, p-adic schanuel's conjecture and decidability. arXiv : 1408.0900v1, August 2014.

[27] David Marker. *Model Theory : An Introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer, 2002.

[28] James S. Milne. Basic theory of affine groupe schemes. Available at www.jmilne.org/math/, 2012.

[29] Alf Onshuus and Anand Pillay. Definable groups and compact p-adic lie groups. *Journal of London Mathematical Society-Second series*, 78(1) :233–247, 2008.

[30] Margarita Otero. A survey on groups definable in o-minimal structures. In *Model Theory with Applications to Algebra and Analysis*, volume 350 of *London Mathematical Society Lecture Note Series*, pages 177–206. Cambridge University Press, 2008.

[31] Daniel Perrin. *Cours d'algèbre*. collection CAPES/Agrégation. ellipses, 1996.

[32] Y. Peterzil, P. Pillay, and S. Starchenko. Linear groups definable in o-minimal structures. *Journal of Algebra*, 247 :1–23, 2002.

[33] Anand Pillay. An application of model theory to real and p-adic algebraic groups. *Journal of Algebra*, 126 :139–146, 1989.

[34] Anand Pillay. On fields definable in $\mathbb{Q}_p$. *Archive for Mathematical Logic*, 29 :1–7, 1989.

[35] Bruno Poizat. *Groupes stables*. Nur al-Mantiq wal-Ma'rifah [Light of Logic and Knowledge], 2. Bruno Poizat, Lyon, 1987. Une tentative de conciliation entre la géométrie algébrique et la logique mathématique. [An attempt at reconciling algebraic geometry and mathematical logic].

[36] Gopal Prasad. Elementary proof of a theorem of bruhat-tits-rousseau and of a theorem of tits. *Bulletin de la Société Mathématique de France*, 110 :197–202, 1982.

[37] Alexander Prestel and Peter Roquette. *Formally p-adic fields*, volume 1050 of *Lecture Notes in Mathematics*. Springer-Verlag, 1984.

[38] Luis Ribes and Pavel Zalesski. *Profinite Groups*. Springer, 2000.

[39] Alain M. Robert. *A Course in p-adic Analysis*. Number 198 in Graduate Texts in Mathematics. Springer, 2000.

[40] Jean-Pierre Serre. *Cours d'arithmétique*. le mathématicien. puf, 1970.

[41] Jean-Pierre Serre. *Arbres, amalgames,* SL_2. Number 46 in astérisque. Société Mathématqiue de France, third edition, 1983.

[42] Pierre Simon. *A guide to NIP Theories*. Lecture Notes in Logic. ASL- Cambridge University Press, to be published.

[43] Michio Suzuki. *Group Theory II*, volume 248 of *Grundlehren der matematischen Wissenschaften*. Springer, 1986.

[44] Lou van den Dries. Dimension of definable sets, algebraic boundness and henselian fields. *Annals of Pure and Applied Logic*, 45 :189–209, 1989.

[45] Lou van den Dries, Deirdre Haskell, and Dugald Macpherson. One-dimensional p-adic subanalytic sets. *Journal of London Mathematical Society*, 49 :1–20, 1999.

[46] Lou van den Dries and Philip Scowcroft. On the structure of semialgebraic sets over p-adic fields. *The Journal of Symbolic Logic*, 53(4) :1138–1164, 1988.

Groupes linéaires définissables dans les corps p-adiques

Résumé

Cette thèse est consacrée à l'étude des groupes linéaires définissables dans les corps p-adiques. Les tores anisotropes jouent un rôle central tout au long de ce travail. Nous donnons une description modèle-théorique et algébrique des $\mathbb{Q}_p$-tores anisotropes de dimension 1.
L'étude des sous-groupes de Cartan de $SL_2(\mathcal{Q}_p)$ (où $\mathcal{Q}_p$ est un corps élémentairement équivalent à $\mathbb{Q}_p$) nous permet de donner une description complète de tous les sous-groupes définissables de $SL_2(\mathcal{Q}_p)$.
Nous nous intéressons également aux groupes linéaires définissables dans des enrichissements p-minimaux d'un corps p-adiquement clos. Nous introduisons une notion de p-connexité pour les groupes. Et nous établissons que tout groupe linéaire commutatif p-connexe définissable dans une telle structure est isomorphe à un groupe semi-algébrique.
Enfin des résultats sur la généricité et la générosité dans $SL_2(\mathbb{Q}_p)$ sont donnés.

Mots-clefs

théorie des modèles, groupes définissables, p-adique, p-minimalité, p-connexité

Linear groups definable in p-adic fields

Abstract

This thesis is dedicated to the study of linear definable groups in p-adic fields. Anisotropic tori play an important role in this work. We give a model-theoretic and algebraic description of anisotropic $\mathbb{Q}_p$-tori of dimension 1.
The study of Cartan subgroups in $SL_2(\mathcal{Q}_p)$ (where $\mathcal{Q}_p$ is a field elementarily equivalent to $\mathbb{Q}_p$) permit us to give a complete description of all definable subgroups of $SL_2(\mathcal{Q}_p)$.
We are seeing also linear groups definable in p-minimal expansions of p-adically closed fields. We introduce a notion of p-connexity for groups. We establish that every linear commutative p-connected group definable in such structure is isomorphic to a semi-algebraic group.
Finally some results on genericity and generosity in $SL_2(\mathbb{Q}_p)$ are given.

Keywords

model theory, definable groups, p-adic, p-minimality, p-connectedness