Densité d'un sous-groupe du groupe de Morava

Notes d'exposé du groupe de travail
formes modulaires et homotopie stable

(Paris/Strasbourg, dans le cadre de l'ANR HGRT)

Aurélien DJAMENT

avril 2009

Résumé

Dans cet exposé, on présente les résultats de l'article [BL06] relatifs à la densité de sous-groupes remarquables dans le groupe de Morava $\mathbb{S}_2$, résultat qui sera utilisé dans la suite du groupe de travail en raison du rôle de ce groupe dans la filtration chromatique de l'homotopie stable des sphères.

On suit pas à pas [BL06], sauf pour un résultat (proposition 4.1 de ces notes) dont on donne une démonstration directe élémentaire (merci à Hans-Werner Henn pour ses utiles indications à ce sujet), en excluant les nombres premiers 2 et 3, et l'on rappelle quelques définitions préliminaires pour faciliter la compréhension des objets de nature arithmétique introduits.

NB : l'ordre et le contenu de détail de ces notes ne sont pas censés coïncider avec ceux de l'exposé oral correspondant !

Table des matières

Dans tout cet exposé, p désigne un nombre premier. (Pour les démonstrations, on écartera souvent le cas $p = 2$, un peu plus compliqué comme nous le verrons.)

1 Quelques définitions préliminaires

1.1 Ordres maximaux

Définition 1.1 ([Swa70]). Soient R un anneau intègre, K son corps des fractions et A une K-algèbre unitaire de dimension finie. On appelle R-**ordre** dans A toute sous-R-algèbre L de A qui est de type fini comme R-module et qui engendre A comme K-espace vectoriel.

Un tel ordre est dit *maximal* s'il est maximal pour l'inclusion parmi les R-ordres dans A.

Pour $R = \mathbb{Z}$, on parle simplement d'ordre (maximal).

1.2 Groupe formel associé à une courbe elliptique

En géométrie algébrique, il existe une notion de *complétion formelle* $\hat{X}_Y$ dans un schéma X d'un sous-schéma fermé Y de X. Cette notion s'obtient par recollement à partir de la situation affine : si I est un idéal d'un anneau commutatif A (correspondant à un sous-schéma fermé $Spec\,(A/I)$ de $Spec\,A$), on dispose du complété de A relativement à I, défini par

$$\hat{A} = \lim_{n \in \mathbb{N}} A/I^n.$$

Par exemple, dans le schéma affine $Spec\,k[X_1, \ldots, X_n] = \mathbb{A}_k^n$, la complétion du point fermé 0 correspondant à l'idéal $(X_1, \ldots, X_n)$ est $Spec\,k[[X_1, \ldots, X_n]]$.

La construction de complétion formelle possède des propriétés de fonctorialité (qu'on n'écrira pas).

Pour les courbes elliptiques : une courbe elliptique abstraite C est un schéma avec un point fermé marqué 0, elle est munie d'une loi de groupe abélien i.e. d'un morphisme de schémas $+ : C \times C \to C$ vérifiant les propriétés habituelles.

La complétion $\hat{C}$ de C relativement au point fermé 0 va en fait fournir une loi de groupe formel.

De fait, la complétion formelle ne respecte pas le produit schématique, mais l'exemple de la droite affine suggère qu'elle le transforme en un produit complété (correspondant au spectre d'un produit tensoriel complété).

Plutôt que de rendre rigoureuses ces observations, nous nous contenterons d'indiquer ce qui se passe brièvement en termes d'équations polynomiales.

Avec une équation de Weierstrass ([Sil92], chapitre IV) : on opère d'abord le changement de variables $z = -x/y$, $w = -1/y$ dans l'équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

qui devient ainsi

$$w = f(z, w)$$

où

$$f = X^3 + a_1XY + a_2X^2Y + a_3Y^2 + a_4XY^2 + a_6Y^3 \in \mathbb{Z}[X, Y].$$

On montre de façon standard le résultat suivant :

Proposition 1.2. *Il existe un et un seul* $W \in \mathbb{Z}[a_1, \ldots, a_6][[Z]]$ *vérifiant l'équation*

$$W = f(Z, W).$$

En posant $x = Z/W$ et $y = -1/W$ (nous noterons $P(Z)$ le « point » correspondant, qui vit dans la complétion formelle de la courbe), on obtient ainsi une *solution formelle* à l'équation de Weierstrass (1).

Ensuite, en revenant à la façon dont est définie la loi de groupe sur la courbe elliptique, on peut trouver (assez facilement) une série formelle en deux variables F telle que $P(Z_1) \underset{C}{+} P(Z_2) = P(F(Z_1, Z_2))$; celle-ci est unique. (Des arguments de type *lemme de Hensel* sont sous-jacents dans tous ces raisonnements.) Le fait que $\underset{C}{+}$ définit une loi de groupe abélien sur la courbe elliptique de départ C se traduit par le fait que F est une *loi de groupe formel*.

1.3 Vecteurs de Witt

(Cf. [Ser68], ch. II, § 6 par exemple et le lemme A.2.2.15 de [Rav86] ; on rappelle que p est un nombre premier fixé.)

Notons $\mathbf{X} = (X_0, X_1, \ldots, X_n, \ldots)$ et $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_n, \ldots)$ deux familles infinies dénombrables d'indéterminées ; on considère par ailleurs les *polynômes de Witt*

$$W_n = \sum_{i=0}^{n} p^i T_i^{p^{n-i}} \in \mathbb{Z}[T_0, \ldots, T_m, \ldots].$$

On peut montrer :

Proposition 1.3. *Pour tout* $\varphi \in \mathbb{Z}[X, Y]$*, il existe un unique*

$$\Phi = (\phi_0, \phi_1, \ldots, \phi_n, \ldots) \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]^{\mathbb{N}}$$

tel que

$$W_n(\Phi) = \varphi(W_n(\mathbf{X}), W_n(\mathbf{Y}))$$

pour tout $n \in \mathbb{N}$*.*

Notons $\mathbf{S}$ et $\mathbf{P}$ les suites de polynômes ainsi obtenues pour $\varphi = X + Y$ et $\varphi = XY$ respectivement. Pour tout anneau commutatif A, on note $W(A)$ l'ensemble $A^{\mathbb{N}}$ muni des lois $+$ et $.$ définies par $a + b = \mathbf{S}(a, b)$ et $a.b = \mathbf{P}(a, b)$.

Proposition 1.4.

1. *Pour tout anneau commutatif* A*, ces lois font de* $W(A)$ *un anneau commutatif. On l'appelle* **anneau de Witt** *de* A*, ses éléments sont appelés* **vecteurs de Witt** *de* A*.*
2. *Cette construction définit un endofoncteur représentable de la catégorie des anneaux commutatifs.*

3. *Les polynômes de Witt W_i définissent un morphisme d'anneaux de $W(A)$ dans l'anneau produit $A^{\mathbb{N}}$; c'est un isomorphisme si p est inversible dans A.*
4. *L'anneau $W(\mathbb{F}_p)$ s'identifie à l'anneau des entiers p-adiques $\mathbb{Z}_p$.*
5. *Si A est un corps fini de caractéristique p, alors $W(A)$ est un anneau local séparé et complet (même compact : c'est une limite projective d'anneaux finis) d'idéal maximal (p) et de corps résiduel A.*
6. *Pour toute puissance q de p, chaque élément x de $W(\mathbb{F}_q)$ possède une décomposition unique*
$$x = \sum_{i \in \mathbb{N}} a_i p^i$$
avec $a_i^q = a_i$ pour tout i. De plus, avec cette écriture, l'automorphisme de $W(\mathbb{F}_q)$ induit par l'automorphisme de Frobenius de $\mathbb{F}_q$ s'obtient en élevant les coefficients a_i à la puissance p.

1.4 Algèbres de quaternions

(Cf. par exemple [Bou70], ch. III, § 2.5.)

Soit E un anneau commutatif muni d'un automorphisme involutif noté $a \mapsto \bar{a}$; on note $Tr(a) = a + \bar{a}$ et $N(a) = a\bar{a}$ pour $a \in E$. Ces éléments appartiennent en fait au sous-anneau A de E des éléments u tels que $u = \bar{u}$; on note que $N(ab) = N(a)N(b)$.

Soit γ un élément de A. On note F la A-algèbre quotient de l'algèbre associative (mais non commutative) $E < s >$ obtenue en adjoignant librement à E un générateur s par l'idéal bilatère engendré par $s^2 - \gamma$ et $sa - \bar{a}s$, pour tout $a \in E$. Cette algèbre est un E-module libre de rang 2 dont 1 et s (on note encore, par abus, s l'image de cet élément dans F) forment une base ; la multiplication est donnée par
$$(a + bs)(a' + b's) = aa' + \gamma b\bar{b}' + (\bar{a}'b + ab')s.$$

On définit *norme* et *trace* dans F comme les applications à valeurs dans A définies par

$$Tr(u) = u\bar{u} \quad \text{et} \quad N(u) = u\bar{u} \quad \text{où} \quad \overline{a + bs} = \bar{a} - bs \ ;$$

autrement dit

$$Tr(a + bs) = Tr(a) \quad \text{et} \quad N(a + bs) = N(a) - \gamma N(b).$$

On vérifie facilement que $\overline{uv} = \bar{v}\bar{u}$, d'où l'on déduit $N(uv) = N(u)N(v)$ puisque A est contenu dans le centre de F. Par conséquent, F est un corps gauche [1] si et seulement si la norme ne s'annule qu'en 0.

Les cas usuels de quaternions s'obtiennent lorsque E est une extension quadratique de A, i.e. du type $E = A[t]/(t^2 - \alpha)$, où l'involution est donnée par $\bar{t} = -t$.

[1] On rappelle que ce qualificatif rappelle la (possible) non-commutativité du corps.

1.5 Le groupe de Morava

(Références : section 0 de [BL06], appendice A.2 de [Rav86], et [Sil92] pour ce qui concerne les courbes elliptiques, par ex.)

Pour tout entier $n \in \mathbb{N}^*$, on note F_n la loi de groupe formel de Honda de hauteur n sur le corps $\mathbb{F}_{p^n}$. Cette loi est définie par $[p]_{F_n} = X^{p^n}$. (On rappelle que, pour une loi de groupe formel F et un entier i, la i-série de F est la série formelle définie par $[i]_F(X) = \underset{F}{X + \ldots + X}$, avec i facteurs.) Pour l'existence et l'unicité (à iso près) d'une telle loi et les autres résultats rappelés dans ce paragraphe, on pourra consulter [Frö68], ch. III, § 2, ainsi que l'appendice A.2 de [Rav86]. Le théorème de Dieudonné-Lubin décrit les endomorphismes de ces lois : l'anneau $\mathrm{End}\,(F_n)$, que l'on notera $\widehat{\mathcal{O}}_n$ ou simplement $\widehat{\mathcal{O}}$ ($\mathcal{O}_p$ dans [BL06]), est isomorphe à l'unique ordre maximal de la $\mathbb{Q}_p$-algèbre (unique à iso près), notée $\widehat{D}_n$ ou simplement $\widehat{D}$ (D_p dans [BL06]), de dimension n^2 qui est un corps gauche et a pour invariant $1/n$. Nous n'entrerons pas dans le détail de ces notions car nous nous bornerons au cas $n = 2$, où l'on peut donner une description explicite élémentaire de tous ces objets en termes de quaternions.

Le *groupe de Morava* $\mathbb{S}_n$ est le groupe $\mathrm{Aut}\,(F_n) = \widehat{\mathcal{O}}^\times$ des automorphismes de la loi de groupe formel F_n. On s'y intéresse comme *groupe topologique* : c'est un groupe profini (comme tous ceux que l'on rencontrera), i.e. limite (projective) de groupes finis (ce qui est fait un groupe topologique compact), c'est même un groupe analytique p-adique de dimension n^2 (on n'utilisera en revanche pas cette structure).

Dans la suite, on ne considère plus que le cas $n = 2$.

On note $\mathbb{W} = W(\mathbb{F}_{p^2})$. Par fonctorialité de W, le morphisme (involutif) de Frobenius sur $\mathbb{F}_{p^2}$ induit une involution de $\mathbb{W}$, que l'on notera $u \mapsto \bar{u}$.

On peut montrer que l'anneau $\widehat{\mathcal{O}}$ est isomorphe à la $\mathbb{W}$-algèbre de quaternions relative à cette involution et à l'élément $\gamma = p$, avec les notations du paragraphe précédent. (Dans la suite, nous *identifierons* souvent ces deux anneaux.) De plus, le corps gauche $\widehat{D}$ est isomorphe à $\widehat{\mathcal{O}} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$, et l'inclusion de $\widehat{\mathcal{O}}$ dans $\widehat{D}$ s'identifie à l'inclusion canonique $\widehat{\mathcal{O}} = \widehat{\mathcal{O}} \underset{\mathbb{Z}}{\otimes} \mathbb{Z} \hookrightarrow \widehat{\mathcal{O}} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$.

On peut décrire $\widehat{D}$ lui-même comme un corps de quaternions : l'inclusion $\mathbb{Z}_p = W(\mathbb{F}_p) \hookrightarrow W(\mathbb{F}_{p^2}) = \mathbb{W}$ induit par tensorisation par $\mathbb{Q}$ une extension de corps (commutatifs) $\mathbb{Q}_p \hookrightarrow \mathbb{W} \underset{\mathbb{Z}}{\otimes} \mathbb{Q} = \mathrm{Frac}(\mathbb{W})$ qui est *quadratique* ; $\mathbb{Q}_p$ est le corps des invariants de l'involution induite par Frobenius et la même construction de quaternions que ci-dessus procure $\widehat{D}$.

Lien avec les courbes elliptiques : soit C une courbe elliptique sur $\mathbb{F}_{p^2}$; notons $\mathcal{O}$ son anneau d'endomorphismes *sur* $\overline{\mathbb{F}}_p$. On rappelle qu'un morphisme entre deux courbes elliptiques est aussi appelé *isogénie* ; c'est par définition un morphisme de courbes algébriques qui préserve l'origine de la courbe. Un tel morphisme est nécessairement constant ou surjectif — cf. [Sil92], ch. III, § 4 et suivants, où l'on trouvera aussi de nombreuses autres propriétés des isogénies.

On dit que C est *supersingulière* si le groupe formel $\hat{C}$ associé à C est de hauteur 2 (i.e. le premier terme non nul de sa p-série est du type aX^{p^2} ; $\hat{C}$ est forcément de hauteur 1 ou 2), donc isomorphe à la loi de Honda F_2 ; on trouvera dans [Sil92], th. 3.1 différentes caractérisations de ces courbes elliptiques. Si C

est supersingulière, alors $\mathcal{O}$ est une algèbre de quaternions sur $\mathbb{Z}$, et $D = \mathcal{O} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ est une $\mathbb{Q}$-algèbre de quaternions (qu'on peut caractériser).

De surcroît, le morphisme canonique

$$\mathcal{O} \otimes \mathbb{Z}_p = \mathrm{End}(C) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p \to \mathrm{End}(\hat{C}) = \widehat{\mathcal{O}}$$

est un isomorphisme, qui s'étend en isomorphisme $D \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p \to \widehat{D}$.

2 Énoncé des résultats

2.1 Définition de sous-groupes remarquables de $\mathbb{S}_2$

La *norme* induit un épimorphisme continu de groupes topologiques $N : \mathbb{S}_2 \to \mathbb{Z}_p^\times$. Le sous-groupe fermé $Ker\, N$ de $\mathbb{S}_2$ est noté $\mathbb{S}l_2$.

Un autre sous-groupe fermé remarquable de $\mathbb{S}_2$ est son p-Sylow $\mathbb{S}_2^0$ défini comme le noyau de l'épimorphisme surjectif $\mathbb{S}_2 \to \mathbb{F}_{p^2}^\times$ associant à un automorphisme $P(X)$ de F_2 le coefficient de X (i.e. $P'(0)$). (Autrement dit, $\mathbb{S}_2^0$ est le sous-groupe des automorphismes *stricts*.)

On note $\mathbb{S}l_2^0$ l'intersection des sous-groupes $\mathbb{S}_2^0$ et $\mathbb{S}l_2$ de $\mathbb{S}_2$.

Dans tout ce qui suit, l désigne un entier supérieur ou égal à 2 et premier à p.

On note Γ le sous-groupe de $\mathbb{S}_2$ formé des éléments de $\mathcal{O}[l^{-1}]$ dont la norme est une puissance de l. C'est un sous-groupe de $\mathcal{O}[l^{-1}]^\times$; on a $\Gamma = \mathcal{O}[l^{-1}]^\times$ si l est un nombre premier.

On introduit enfin $\Gamma^1 = \Gamma \cap \mathbb{S}l_2$, sous-groupe des éléments de Γ de norme 1, et $\Lambda = \Gamma \cap \mathbb{S}l_2^0$.

2.2 Les énoncés

L'objectif de cet exposé est de comprendre les résultats suivants. (Des rappels sur la structure du groupe des éléments inversibles des entiers p-adiques sont donnés au paragraphe 3.2.)

Théorème 2.1. *1. Supposons $p > 2$ et que l est un générateur topologique de $\mathbb{Z}_p^\times$ (i.e. que le sous-groupe engendré par p est dense dans $\mathbb{Z}_p^\times$). Alors Γ est un sous-groupe dense de $\mathbb{S}_2$.*

2. Supposons $p = 2$ et que l est un générateur topologique de $\mathbb{Z}_2^\times/\{\pm 1\}$. Alors Γ est un sous-groupe dense du sous-groupe $\widetilde{\mathbb{S}}_2$ de $\mathbb{S}_2$ noyau du morphisme

$$\mathbb{S}_2 \xrightarrow{N} \mathbb{Z}_2^\times \to (\mathbb{Z}/8)^\times/\{1, l\}.$$

Dans les variantes suivantes, il n'est plus nécessaire de distinguer le cas $p = 2$ ni de faire des hypothèses additionnelles sur l.

Théorème 2.2. *Le groupe Λ est dense dans $\mathbb{S}l_2^0$.*

Corollaire 2.3. *Le groupe Γ^1 est dense dans $\mathbb{S}l_2$.*

3 Les outils de la démonstration

3.1 Outils généraux

3.1.1 Un critère élémentaire de densité

On rappelle qu'un *pro-p-groupe* est un groupe topologique limite (projective) de p-groupes finis.

Proposition 3.1 (Cf. [Ser63], § 4.2 par ex.). *Soient G un pro-p-groupe et H un sous-groupe de G. On note $\mathrm{Hom}^c(G, \mathbb{F}_p)$ le $\mathbb{F}_p$-espace vectoriel des morphismes continus de G dans le groupe additif sous-jacent à $\mathbb{F}_p$.*

Alors le sous-groupe H de G est dense si et seulement si le morphisme de restriction

$$\mathrm{Hom}^c(G, \mathbb{F}_p) \to \mathrm{Hom}^c(H, \mathbb{F}_p)$$

est injectif.

Démonstration. Deux applications continues entre espaces séparés égales sur une partie dense de la source étant nécessairement égales, la densité de H entraîne l'injectivité annoncée.

Réciproquement, si H n'est pas dense, $G/\bar{H}$ est un pro-p-groupe non trivial, il existe donc un p-groupe fini non trivial P et un épimorphisme $\varphi : G/\bar{H} \twoheadrightarrow P$. Il est bien connu que P possède forcément un sous-groupe distingué d'indice p (utiliser par exemple la non-trivialité du centre de P et une récurrence sur l'ordre, en traitant d'abord le cas abélien), ce qui procure un morphisme non trivial $P \to \mathbb{F}_p$. En le composant avec φ et la projection $G \twoheadrightarrow G/\bar{H}$, on obtient un morphisme non trivial de G vers $\mathbb{F}_p$ dont la restriction à H est triviale. □

3.1.2 Un lemme sur les ordres maximaux

Dans son § 1, l'article [BL06] (où l'on trouvera détails ou références pour les considérations vagues qui suivent) approfondit la relation entre courbes elliptiques supersingulières et ordres maximaux d'algèbres de quaternions que nous avons effleurée au paragraphe 1.5.

On peut en effet décrire l'ensemble des classes d'isomorphisme de courbes elliptiques supersingulières sur $\mathbb{F}_{p^2}$ en termes d'ordres maximaux de l'algèbre D. D'abord, on montre que deux telles courbes sont nécessairement isogènes, i.e. qu'il existe une isogénie non triviale entre les deux (on a en fait mieux : il existe une isogénie de tout degré assez grand d'une des courbes sur l'autre), ce qui ramène la classification à un problème d'endomorphismes d'une courbe fixée. Ensuite, on construit une surjection de cet ensemble de classes d'isomorphisme vers l'ensemble des classes de conjugaison d'ordres maximaux de D, dont les fibres sont explicites. Le résultat qui suit apparaît comme corollaire de ces considérations.

Proposition 3.2. *Soient $\mathcal{O}$ un ($\mathbb{Z}$-)ordre maximal de D, $\mathcal{O}'$ un $\mathbb{Z}[l^{-1}]$-ordre maximal de D et x' un élément de $\mathcal{O}'$. Alors il existe un élément de $\mathcal{O}[l^{-1}]$ possédant le même polynôme minimal que x'.*

Remarque 3.3. Les $\mathbb{Z}[l^{-1}]$-ordres maximaux de D sont exactement les $\mathcal{O}[l^{-1}]$, où $\mathcal{O}$ est un ($\mathbb{Z}$-)ordre maximal de D.

3.1.3 Un autre lemme sur les ordres maximaux

Comme dans l'article [BL06], nous admettrons le résultat suivant, cas particulier de [Swa70], prop. 9.19.

Proposition 3.4. *Soit $f(x) = x^2 + a_1 x + a_2$ un polynôme de $\mathbb{Q}[x]$ qui soit irréductible sur $\mathbb{R}$ et sur $\mathbb{Q}_p$. Alors il existe $\alpha \in D$ tel que $f(\alpha) = 0$.*

Si de surcroît a_1 et a_2 sont entiers sur un sous-anneau A de $\mathbb{Q}$, alors α appartient à un A-ordre maximal de D.

3.2 Structure des unités de l'anneau $\mathbb{W}$

Soient $i > 0$ un entier et $q = p^i$. On peut dévisser le groupe $W(\mathbb{F}_q)^\times$ des unités de l'anneau de Witt [2] de $\mathbb{F}_q$ en considérant le sous-groupe (fermé) $W(\mathbb{F}_q)_u$ des éléments du type $1 + pt$; avec $t \in W(\mathbb{F}_q)$. Il s'insère dans une suite exacte courte (de groupes topologiques)

$$1 \to W(\mathbb{F}_q)_u \to W(\mathbb{F}_q)^\times \to \mathbb{F}_q^\times \to 1 \tag{2}$$

dont la dernière flèche est induite par la projection $W(\mathbb{F}_q) \twoheadrightarrow \mathbb{F}_q$ sur le corps résiduel de l'anneau de Witt.

Le groupe topologique $W(\mathbb{F}_q)_u$ est isomorphe au groupe additif sous-jacent à $W(\mathbb{F}_q)$ si $p > 2$. Pour $i = 1$, cela peut se voir directement à l'aide de la structure (cyclique) des groupes $(\mathbb{Z}/(p^n))^\times$; dans le cas général, il est commode d'utiliser l'exponentiel : la série

$$exp(pt) = \sum_{n \in \mathbb{N}} \frac{p^n}{n!} t^n$$

est bien définie et convergente pour $t \in W(\mathbb{F}_q)$, car la valuation p-adique du nombre rationnel $\frac{p^n}{n!}$ est positive et tend vers l'infini avec n. En effet, cette valuation est égale à [3]

$$n - \sum_{j \in \mathbb{N}} [n/p^j] \geq n - \sum_{j \in \mathbb{N}} n/p^j = n - \frac{n}{p-1} = \frac{p-2}{p-1}\, n.$$

On voit ici la nécessité de l'hypothèse $p > 2$.

De même, la série

$$log(1 + pt) = \sum_{n \in \mathbb{N}^*} (-1)^{n+1} \frac{p^n}{n} t^n$$

converge dans $W(\mathbb{F}_q)$; on vérifie aisément que ces deux séries définissent des isomorphismes de groupes topologiques réciproques l'un de l'autre entre $W(\mathbb{F}_q)_u$ et $W(\mathbb{F}_q)$.

Pour $p = 2$, il faut utiliser la série $exp(4t)$ au lieu de $exp(2t)$ qui ne converge pas ; on obtient un isomorphisme entre $W(\mathbb{F}_q)_u$ et $W(\mathbb{F}_q) \oplus \mathbb{Z}/2$. Nous écarterons par la suite ce cas afin de simplifier les arguments.

De plus, du fait que $W(\mathbb{F}_q)$ est un pro-p-groupe et que $\mathbb{F}_q^\times$ est d'ordre premier à p, la suite exacte (2) se scinde.

[2] On utilisera ces résultats pour $i = 1$ ou 2. Le cas ($i = 1$) des entiers p-adiques est traité dans [Ser77], chap. II, § 3 par ex., pour le cas général nous avons suivi l'appendice A.2 de [Rav86].

[3] Dans ce qui suit, les crochets indiquent la partie entière d'un nombre réel.

4 Mise en œuvre de la démonstration (cas $p > 3$)

Dans toute la suite, on suppose que p est impair.

4.1 Détermination de $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2})$

On rappelle que $\mathbb{S}_2$ est le groupe des unités de l'anneau $\widehat{\mathcal{O}}$, qui est un $\mathbb{W}$-module libre de base $(1, S)$ où $S^2 = p$ et $Sa = \bar{a}S$ pour tout $a \in \mathbb{W}$. Le sous-groupe $\mathbb{S}_2^0$ de $\mathbb{S}_2$ est le groupe multiplicatif des éléments de la forme $a + bS$ pour lesquels $a - 1 \in (p)$. La fonction qui à $a + bS$ associe l'image de b dans le corps résiduel $\mathbb{F}_{p^2}$ de $\mathbb{W}$ définit un morphisme de groupes continu $t : \mathbb{S}_2^0 \to \mathbb{F}_{p^2}$, de même que sa composition avec l'automorphisme de Frobenius de $\mathbb{F}_{p^2}$. On rappelle également que $\mathbb{S}l_2^0$ désigne le sous-groupe des éléments de norme 1 de $\mathbb{S}_2^0$. L'objectif de ce paragraphe consiste à démontrer le résultat suivant [4] :

Proposition 4.1. *Les restrictions à $\mathbb{S}l_2^0$ de t et $t^p : \mathbb{S}_2^0 \to \mathbb{F}_{p^2}$ forment une base du $\mathbb{F}_{p^2}$-espace vectoriel $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2})$.*

(Pour $p = 2$, on a un énoncé analogue, avec pour résultat un espace vectoriel de dimension 4.)

Bien que ce résultat soit valable pour tout p impair, la démonstration, élémentaire, que nous donnerons ne s'appliquera pas au cas $p = 3$.

Démonstration. On vérifie facilement que ces deux morphismes forment une famille libre du $\mathbb{F}_{p^2}$-espace vectoriel $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2})$; nous allons montrer qu'il est de dimension 2. Avant cela, nous commençons par donner le corollaire par lequel nous utiliserons la proposition 4.1 et quelques lemmes. □

Corollaire 4.2. *Un sous-groupe H de $\mathbb{S}l_2^0$ est dense si et seulement si le morphisme*

$$H \hookrightarrow \mathbb{S}_2^0 \xrightarrow{t} \mathbb{F}_{p^2}$$

est surjectif.

Démonstration. L'isomorphisme canonique $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_p) \simeq (\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2}))^{\mathbb{Z}/2}$ (où $\mathbb{Z}/2$ agit par l'involution de Frobenius sur $\mathbb{F}_{p^2}$) et la proposition 4.1 montrent qu'une base de $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_p)$ est constituée des morphismes $u = t + t^p$ et $v = \omega t + \omega^p t^p$, où ω désigne un générateur de $\mathbb{F}_{p^2}^\times$.

Par la proposition 3.1, un sous-groupe H de $\mathbb{S}l_2^0$ est dense si et seulement la restriction à H de u et v est une famille libre. On voit facilement que cela équivaut à la surjectivité de la restriction à H de t. □

Le sous-groupe $\mathbb{S}_2^0$ de $\mathbb{S}_2$ est formé des éléments x de $\widehat{\mathcal{O}}$ tels que $x - 1 \in (S)$, puisque $S^2 = p$. De même, on note $\mathbb{S}_2^1$ l'ensemble des x de $\widehat{\mathcal{O}}$ tels que $x - 1 \in (pS)$. C'est un sous-groupe distingué fermé de $\mathbb{S}_2^0$.

Lemme 4.3. *Il existe une application continue $R : \mathbb{S}_2^1 \to \mathbb{S}_2^0$ vérifiant les propriétés suivantes.*

1. *Pour tout $x \in \mathbb{S}_2^1$, on a $R(x)^p = x$.*

[4] Il existe plusieurs démonstrations de cet énoncé. L'article [BL06] utilise une méthode sophistiquée, adéquate pour calculer toute la cohomologie du groupe profini $\mathbb{S}l_2^0$; l'article [Hen98] (§ 3.1) indique une autre méthode.

2. Si x et y sont deux éléments permutables de $\mathbb{S}_2^1$, alors $R(xy) = R(x)R(y)$.

Démonstration. On part du développement en série

$$(1+pX)^{1/p} = 1 + \sum_{n\geq 1} a_n^p X^n \quad \Big(\text{où } a_n^p = \frac{1}{n!}\prod_{i=1}^{n}(1-(i-1)p)\Big)$$

valable dans $\mathbb{Q}[[X]]$. Cette écriture abusive signifie que le terme de droite $A(X)$ vérifie $A(X)^p = 1+pX$; on a également $A(X)A(Y) = A(X+Y+pXY)$ dans $\mathbb{Q}[[X,Y]]$. (On peut par exemple démontrer ces identités en tensorisant par $\mathbb{R}$ et constatant qu'elles sont vraies analytiquement au voisinage de 0.)

On constate ensuite que, pour $x \in \mathbb{S}_2^1$, la série $R(x) = A\big(\frac{x-1}{p}\big)$, a priori définie sur $\widehat{\mathcal{O}} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$, est à coefficients dans $\widehat{\mathcal{O}}$ et converge (vers un élément de $\mathbb{S}_2^0$ vu la forme de la série) : comme $\frac{x-1}{p} \in (S)$, la valuation p-adique de la puissance n-ième de cet élément vaut au moins $[n/2]$ (en effet, $(aS)^2 \in (p)$ pour tout $a \in \widehat{\mathcal{O}}$), tandis que la valuation p-adique de a_n^p est

$$-v_p(n!) \geq -\frac{n}{p-1} \ ;$$

l'hypothèse $p > 3$ assure donc que la valuation p-adique du terme général non seulement est toujours positive mais aussi tend vers l'infini. Cela entraîne aussitôt le lemme. □

Lemme 4.4. *1. Tout morphisme de $\mathbb{S}_2^0$ vers un p-groupe abélien élémentaire se factorise par la projection sur $\mathbb{S}_2^0/\mathbb{S}_2^1$.*

2. Tout morphisme de $\mathbb{S}l_2^0$ vers un p-groupe abélien élémentaire se factorise par la projection sur $\mathbb{S}l_2^0/\mathbb{S}l_2^1$, où l'on pose $\mathbb{S}l_2^1 = \mathbb{S}_2^1 \cap \mathbb{S}l_2$.

Démonstration. La première assertion du lemme précédent montre que tout élément de $\mathbb{S}_2^1$ est la puissance p-ième d'un élément de $\mathbb{S}_2^0$, ce qui établit le premier point.

Pour le second, d'après la deuxième assertion du lemme 4.3, pour tout $x \in \mathbb{S}l_2^1$, on a $N(R(x)) = R(x)\overline{R(x)} = R(x)R(\bar{x}) = R(N(x)) = 1$, puisque x et $\bar{x}$ commutent, de sorte que x est bien la puissance p-ième d'un élément de $\mathbb{S}l_2^0$. □

Lemme 4.5. *1. Le groupe $\mathbb{S}_2^0/\mathbb{S}_2^1$ est isomorphe au groupe dont l'ensemble sous-jacent est $(\mathbb{F}_{p^2})^2$ et la multiplication donnée par*

$$(a,b)(a',b') = (a+a'+b\bar{b}', b+b'),$$

où l'on surligne comme précédemment les éléments pour indiquer l'action de l'involution de Frobenius.

2. Le groupe $\mathbb{S}l_2^0/\mathbb{S}l_2^1$ est isomorphe au sous-groupe du groupe précédent formé des éléments (a,b) tels que $a + \bar{a} = b\bar{b}$.

3. Ce dernier groupe est lui-même isomorphe à l'ensemble $\mathbb{F}_p \times \mathbb{F}_{p^2}$ muni de la loi

$$(x,y)(x',y') = (x+x'+\frac{y\bar{y}'-\bar{y}y'}{\omega}, y+y')$$

où ω est un élément de $\mathbb{F}_{p^2}^\times$ tel que $\overline{\omega} = -\omega$.

4. Il existe une suite exacte courte non scindée

$$0 \to \mathbb{F}_p \to \mathbb{S}l_2^0/\mathbb{S}l_2^1 \to \mathbb{F}_{p^2} \to 0.$$

Par conséquent, l'épimorphisme $\mathbb{S}l_2^0/\mathbb{S}l_2^1 \to \mathbb{F}_{p^2}$ induit un isomorphisme

$$\mathrm{Hom}\,(\mathbb{F}_{p^2}, C) \xrightarrow{\simeq} \mathrm{Hom}\,(\mathbb{S}l_2^0/\mathbb{S}l_2^1, C)$$

pour tout p-groupe abélien élémentaire C.

Démonstration. Le premier point provient du calcul

$$(1+pa+bS)(1+pa'+b'S) \equiv 1 + p(a+a'+b\bar{b}') + (b+b')S \pmod{pS} ;$$

le deuxième s'en déduit par le calcul de la norme

$$N(1+pa+bS) \equiv 1 + p(a+\bar{a}-b\bar{b}) \pmod{pS}.$$

Le troisième s'en déduit par le changement de variables $x = \frac{a-\bar{a}}{\omega}$, $y = b$, qui s'inverse par $a = \frac{\omega x + y\bar{y}}{2}$ compte-tenu de la relation $a + \bar{a} = y\bar{y}$, ce qui donne après calcul la formule annoncée.

La dernière assertion s'obtient soit par calcul direct, soit en remarquant que la troisième décrit $\mathbb{S}l_2^0/\mathbb{S}l_2^1$ comme extension de $\mathbb{F}_p$ par le p-groupe abélien élémentaire $V = \mathbb{F}_{p^2}$ correspondant à l'élément de

$$H^2(V; \mathbb{F}_p) \simeq \Lambda^2(V^*) \oplus V^*$$

donné par la forme bilinéaire alternée

$$(t,u) \mapsto \frac{t\bar{u} - \bar{t}u}{\omega}$$

qui est non nulle, d'où le caractère non scindé de l'extension. □

Fin de la démonstration de la proposition 4.1. Le lemme 4.4 montre que $\mathrm{Hom}^c(\mathbb{S}l_2^0, \mathbb{F}_{p^2}) \simeq \mathrm{Hom}^c(\mathbb{S}l_2^0/\mathbb{S}l_2^1, \mathbb{F}_{p^2})$. Le lemme 4.5 prouve ensuite que ce $\mathbb{F}_{p^2}$-espace vectoriel est de dimension 2, ce qui achève la démonstration. □

4.2 Démonstration du théorème 2.2

On choisit des entiers r_1 et r_2 premiers à p de sorte que r_1 soit un carré mod p et que r_2 ne le soit pas. On pose alors

$$\alpha_i = -\frac{pr_i + 2}{l^{mp(p-1)}} \qquad (i = 1, 2)$$

où $m \in \mathbb{N}$ est choisi assez grand pour $\alpha_i^2 < 4$ pour $i \in \{1, 2\}$.

On considère alors les polynômes

$$f_i(x) = x^2 + \alpha_i x + 1 \qquad (i = 1, 2).$$

Ils sont irréductibles sur $\mathbb{R}$, puisque leur discriminant $\Delta_i = \alpha_i^2 - 4$ est strictement négatif ; ils sont également irréductibles sur $\mathbb{Q}_p$. En effet, il suffit de vérifier que les Δ_i ne sont pas des carrés dans $\mathbb{Z}_p$ (si le carré d'un élément de $\mathbb{Q}_p$ appartient

à $\mathbb{Z}_p$, c'est le carré d'un élément de $\mathbb{Z}_p$), ce qu'ils ne sont déjà pas dans $\mathbb{Z}/(p^2)$. En effet, la relation $l^{p-1} \equiv 1 \pmod{p}$ entraîne $l^{p(p-1)} \equiv 1 \pmod{p^2}$ puis $\Delta_i \equiv 4pr_i \pmod{p^2}$. Mais comme r_i est premier à p, $4pr_i$ ne peut être un carré mod p^2.

Appliquant la proposition 3.4, on en déduit l'existence d'éléments x_i de D tels que $f_i(x_i) = 0$. Comme les f_i sont à coefficients dans $\mathbb{Z}[l^{-1}]$, les x_i appartiennent à des ordres $\mathbb{Z}[l^{-1}]$-maximaux de D. La proposition 3.2 montre qu'on peut supposer que les x_i appartiennent à $\mathcal{O}[l^{-1}]$.

Les x_i sont de norme 1, car leur conjugué est l'autre racine de l'équation $f_i(x) = 0$. Ainsi, $x_i \in \Gamma^1$.

Écrivons $x_i = a_i + b_i S$, avec $a_i, b_i \in \mathbb{W}$. Comme les α_i sont congrus à -2 modulo (p), donc a fortiori modulo (S), on obtient $a_i^2 - 2a_i + 1 \in (S)$, d'où $a_i - 1 \in (p)$, de sorte que $x_i \in \Lambda$; écrivons $a_i = 1 + pa_i'$. Il vient

$$-\alpha_i = Tr(x_i) = 2 + pTr(a_i') \qquad \text{(somme des racines)}$$

et

$$1 = N(x_i) = 1 + pTr(a_i') + p^2 N(a_i') - pN(b_i)$$

d'où

$$N(b_i) = Tr(a_i') + pN(a_i') = pN(a_i') - \frac{\alpha_i + 2}{p} \equiv r_i \pmod{p}.$$

Avec les notations du paragraphe 4.1, cela donne

$$t(x_i)\overline{t(x_i)} = r_i \in \mathbb{F}_p$$

(on l'on note encore r_i, par abus, l'image de cet entier modulo p). Si les éléments $t(x_1)$ et $t(x_2)$ de $\mathbb{F}_{p^2}$ étaient linéairement dépendants sur $\mathbb{F}_p$, leurs normes dans $\mathbb{F}_p^\times$ auraient la même image dans $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$, ce qui est contraire à l'hypothèse faite sur les r_i. On en conclut que $(t(x_1), t(x_2))$ est une $\mathbb{F}_p$-base de $\mathbb{F}_{p^2}$, ce qui montre, d'après le corollaire 4.2, que Λ est dense dans $\mathbb{S}l_2^0$, comme souhaité.

4.3 Démonstration du théorème 2.1 et du corollaire 2.3

Démonstration du corollaire 2.3. On dispose d'une suite exacte courte

$$1 \to \mathbb{S}l_2^0 \to \mathbb{S}l_2 \to \mathbb{Z}/(p+1) \to 0,$$

où le groupe cyclique d'ordre $p+1$ est à penser ici comme le sous-groupe de $\mathbb{F}_{p^2}^\times$ des éléments de norme 1 dans $\mathbb{F}_p$ (le dernier morphisme est donné par la réduction modulo (S) dans $\widehat{\mathcal{O}}$). Il suffit de montrer qu'on peut relever le générateur de $\mathbb{Z}/(p+1)$ en un élément de Γ^1 pour déduire le corollaire 2.3 du théorème 2.2. Soient $\bar{f}(x) = x^2 + \tilde{a}x + 1$ le polynôme minimal sur $\mathbb{F}_p$ de ce générateur (on rappelle que $\mathbb{Z}/(p+1)$ est vu dans $\mathbb{F}_{p^2}^\times$), a un entier dont la classe dans $\mathbb{F}_p$ est $\tilde{a}$ et $\alpha = al^{-m(p-1)}$, où l'entier m est choisi assez grand pour que $\alpha^2 < 4$. Le polynôme $X^2 + \alpha X + 1$ est irréductible sur $\mathbb{R}$ et sur $\mathbb{Q}_p$ (puisque sa réduction $\bar{f}$ à $\mathbb{F}_p$ est déjà irréductible) : comme dans la démonstration du théorème 2.2, on en déduit l'existence d'une racine de ce polynôme dans $\mathcal{O}[l^{-1}]$. Cette racine appartient à Γ^1 car elle est de norme 1 (produit des racines), et sa réduction modulo (S) est une racine de $\bar{f}$, donc un générateur de notre groupe cyclique, comme souhaité. □

Démonstration du théorème 2.1. La suite exacte de groupes topologiques

$$1 \to \mathbb{S}l_2 \to \mathbb{S}_2 \xrightarrow{N} \mathbb{Z}_p^\times \to 1$$

montre qu'il s'agit d'établir l'existence d'un élément x de Γ tel que $N(x)$ soit un générateur topologique de $\mathbb{Z}_p^\times$. Comme l est supposé être un tel générateur, on va produire un $x \in \Gamma$ tel que $N(x) = l$.

Par un résultat général (proposition 1.1 de [BL06]), pour m entier assez grand, il existe $\alpha \in \mathcal{O}$ tel que $N(\alpha) = l^{2m+1}$. Alors $x = l^{-m}\alpha \in \Gamma$ convient. □

Références

[BL06] M. Behrens & T. Lawson – « Isogenies of elliptic curves and the Morava stabilizer group », *J. Pure Appl. Algebra* **207** (2006), no. 1, p. 37–49.

[Bou70] N. Bourbaki – *Éléments de mathématique. Algèbre. Chapitres 1 à 3*, Hermann, Paris, 1970.

[Frö68] A. Fröhlich – *Formal groups*, Lecture Notes in Mathematics, No. 74, Springer-Verlag, Berlin, 1968.

[Hen98] H.-W. Henn – « Centralizers of elementary abelian p-subgroups and mod-p cohomology of profinite groups », *Duke Math. J.* **91** (1998), no. 3, p. 561–585.

[Rav86] D. C. Ravenel – *Complex cobordism and stable homotopy groups of spheres*, Pure and Applied Mathematics, vol. 121, Academic Press Inc., Orlando, FL, 1986.

[Ser63] J.-P. Serre – *Cohomologie galoisienne*, Cours au Collège de France, vol. 1962, Springer-Verlag, Berlin, 1962/1963.

[Ser68] — , *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser77] — , *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977, Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Sil92] J. H. Silverman – *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Swa70] R. G. Swan – *K-theory of finite groups and orders*, Lecture Notes in Mathematics, Vol. 149, Springer-Verlag, Berlin, 1970.