Thèse

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE

UMR 7501

Strasbourg

présentée pour obtenir le grade de docteur de
l'Université de Strasbourg
Spécialité MATHÉMATIQUES

Olivier Lader

Une résolution projective pour le second groupe de Morava pour $p \geq 5$ et applications

Soutenue le 31 octobre 2013
devant la commission d'examen

Hans-Werner Henn, directeur de thèse
Christian Ausoni, rapporteur
Mark Behrens, rapporteur
Pierre Guillot, examinateur
Jean Lannes, examinateur

www-irma.u-strasbg.fr

Institut de Recherche Mathématique Avancée

UNIVERSITÉ DE STRASBOURG

Une résolution projective pour le second groupe de Morava pour $p \geq 5$ et applications

Olivier Lader

Institut de Recherche Mathématiques Avancée (IRMA),
Strasbourg

31 octobre 2013

Remerciements

Trois années se sont écoulés et voici l'aboutissement de ce travail. Ceci n'aurait pas été possible sans la présence de bon nombre de personnes. En premier lieu, je tiens à remercier mon directeur de thèse, Hans-Werner Henn, pour m'avoir permis d'étudier un tel type de problème. Sa détermination constante et ses conseils à chacun de nos rendez-vous du mardi ont largement contribué à l'aboutissement de ce travail.

J'aimerais ensuite remercier les rapporteurs Christian Ausoni et Mark Behrens qui ont bien voulu consacrer du temps à la lecture détaillée de cette thèse.

Merci également à Pierre Guillot et Jean Lannes qui me font l'honneur de participer au jury de thèse.

Je tiens aussi à remercier Nasko Karamanov pour les discussions qu'on a eu sur le sujet et Paul Goerss qui a écouté mon exposé sur mes premiers résultats et m'a soutenu cette dernière année.

Durant cette période, j'ai pu côtoyer régulièrement les membres de l'équipe d'algèbre et topologie de l'IRMA. Merci à Gaël, Christine et Pierre. J'aurais bien aimé que Jean-Louis Loday soit des nôtres en ce jour. Je n'oublierai jamais son acceuil chaleureux au sein de l'équipe.

J'aurai aussi eu l'occasion de participer à des colloques. Je salue mes collègues doctorants en topologie algébrique : Sinan, Nicolas, Hector, Kato, Paul-Arnaud.

J'aimerais témoigner ma sincère reconnaissance à Josiane Nervi-Gasparini que j'ai eu comme professeur en analyse en première année de faculté. Elle est sans doute la première personne qui m'a donné goût aux mathématiques.

Je tiens aussi à remercier mes co-bureaux Adrien, Cédric, Enrica et Romain ainsi que mes amis doctorants Alexandre, Auguste, Aurélien, Camille, Charlotte, Fabien, Jean-Stefan, Jonathan, Mathieu, Nicolas, Ranine.

Merci sincèrement à mes amis Philippe et Ambroise, avec qui j'ai passé d'excellents moments en soirée (concerts, bars, ...) ainsi qu'à Christophe, Daniel, Gilles et Prince.

Enfin, j'embrasse ma famille. Ma mère, qui m'a permis de concilier la recherche en semaine et l'agriculture le samedi. Mon père, qui supporte mes humeurs et qui aura toujours réussi à me remotiver durant toutes ces années universitaires. Mon frère Jean-Luc, Patricia, mon frère Marc et Monique. Mes neuveux Emilia, Julianna, Alessandro, Vicenzo et Georgio.

Table des matières

Introduction

Soit p un nombre premier, on note $K(n)$ la n-ème K-théorie de Morava. L'anneau de coefficient de cette théorie de cohomologie est $K(n)_* \cong \mathbb{F}_p[v_n^{\pm 1}]$, où v_n est de degré $2(p^n - 1)$. Soit $E(n)$ la théorie d'homologie de Johnson-Wilson et L_n la localisation de Bousfield relativement à $E(n)_*$. Soit X un spectre, nous avons une application naturelle $L_n X \to L_{n-1} X$. Si de plus X est p-local fini alors, d'après le théorème de convergence chromatique, l'application naturelle

$$X \longrightarrow \text{holim}\, L_n X$$

est une équivalence faible. D'autre part, les applications $L_n X \to L_{n-1} X$ induisent un pull-back homotopique :

$$\begin{tikzcd} L_n X \arrow[r] \arrow[d] & L_{K(n)} X \arrow[d] \\ L_{n-1} X \arrow[r] & L_{n-1} L_{K(n)} X \end{tikzcd}$$

Ainsi, si X est un spectre p-local fini, les éléments de bases déterminant le type d'homotopie de X sont les localisations par rapport à la K-théorie de Morava $L_{K(n)} X$. Ceci est vraie en particulier pour la sphère S^0 localisé en p.

Pour le moment les groupes d'homotopie $\pi_* L_{K(n)}(S^0)$ sont connus lorsque $n = 1$, en relation avec l'homomorphisme J, et lorsque $n = 2$ et $p > 2$. Le cas $n = 2$ et $p > 3$ a été traité par Shimomura et Yabe en 1995, malheureusement leur raisonnement n'est pas très bien compris (voir section 15.2 de [HS99] et l'introduction de [Beh12]). Avant d'aboutir au cas intégral, K. Shimomura et ses coauteurs durant les années 80 ont déterminé $\pi_*(L_{K(2)} V(0))$, où $V(0)$ est le spectre de Moore modulo p. Pour y arriver, ils ont utilisé plusieurs suites spectrales. La suite spectrale de Bockstein relativement à la multiplication par v_1 :

$$\mathrm{Ext}^s_{\mathrm{BP}_*\mathrm{BP}}(\mathrm{BP}_*,\ v_2^{-1}\mathrm{BP}_*/(p, v_1)) \otimes \mathbb{F}_p[v_1]/(v_1^\infty) \implies \mathrm{Ext}^s_{\mathrm{BP}_*\mathrm{BP}}(\mathrm{BP}_*, \mathrm{BP}_*/(p, v_1^\infty))$$

a été d'une particulière utilité. Ce premier résultat modulo (p) se trouve dans [Shi86]. Il a ensuite été résumé par H. Sadofsky dans [Sad93], puis M. Hovey et P. Strickland en ont donné encore une autre présentation dans [HS99] section 15.2.

Avec les théorèmes de changement d'anneau de Morava [Mor85], une autre approche pour déterminer les groupes d'homotopie $\pi_* L_{K(n)} X$ existe. Plus précisément, dans [DH04], sur le spectre des points fixes homotopiques, E. Devinatz et M. Hopkins montrent l'existence d'une autre suite spectrale, dite $K(n)$-local E_n-Adams :

$$E_2^{s,t} = H^s(\mathbb{G}_n, (E_n)_t X) \implies \pi_{t-s}\, L_{K(n)} X$$

Elle est convergente lorsque X est p-local et fini. C'est le cas, en particulier pour les spectres S^0 et $V(0)$.

Dans le cas $p \geq 5$ et $n = 2$, la page E_2 de la suite spectrale

$$E_2^{s,t} = H^s(\mathbb{G}_n, (E_n)_t/(p)) \implies \pi_{t-s} L_{K(n)} V(0)$$

détermine les groupes d'homotopie stable du spectre de Moore localisé. Ça provient du fait que pour que le groupe de cohomologie de la page E_2 puisse être non nulle, il faut que t soit un multiple de $2(p-1)$ et que s soit compris en 0 et 4. Ainsi la suite spectrale dégénère dès la seconde page et l'étude de $\pi_* L_{K(n)} V(0)$ devient un problème algébrique. On a donc bien une méthode indépendante de celle de K. Shimomura pour déterminer les groupes d'homotopie du spectre de Moore localisé par rapport à la seconde K-théorie de Morava.

Dans cette thèse, en se basant sur la méthode utilisée par H-W. Henn, N. Karamanov et M. Mahowald dans [HKM08] pour traiter le cas $p=3$, on détermine $H^*(\mathbb{G}_2, (E_2)_*/(p))$ pour les nombres premiers p supérieurs strictement à 3. En fait, le cas $p=3$ était particulier car la dimension cohomologique de $\mathbb{G}_2$ n'est pas finie. En revenant à la précédente suite spectrale, on déduit le même résultat que K. Shimomura concernant $\pi_* L_{K(2)} V(0)$. Enfin, on verra une seconde application, le calcul du groupe de Hopkins Pic_2. Le groupe Pic_2 est le groupe des spectres $K(2)$-locaux inversibles. Dans le cas $p \geq 5$, pour le déterminer, il suffit de calculer $H^1(\mathbb{G}_2, (E_2)_0^\times)$. Ce calcul avait été effectué par M. Hopkins dans des notes non publiées et basé sur les travaux de K. Shimomura. Nous en donnons une preuve complète basée sur notre étude de $H^*(\mathbb{G}_2, (E_2)_*/(p))$.

Précisons d'avantage. Dans le chapitre 1, nous allons introduire le groupe stabilisateur de Morava et son action sur l'anneau de Lubin-Tate. On verra que le groupe stabilisateur de Morava $\mathbb{G}_2$ se décompose comme le produit semi-direct du groupe $\mathbb{S}_2$ des automorphismes d'une certaine loi de groupe formel et du groupe de Galois $\mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$. D'après un théorème de Dieudonné-Lubin la structure du groupe $\mathbb{S}_2$ est bien connue de la théorie des groupes profinis. En fait, $\mathbb{S}_2$ s'identifie avec le groupe des unités d'une $\mathbb{Q}_p$-algèbre à division associative. Ensuite de la théorie de Lubin-Tate, on déduit une action de $\mathbb{G}_2$ sur l'anneau gradué de Lubin-Tate. Dans le cas $p \geq 5$, en considérant le sous-groupe $\mathbb{G}_2^1$, noyau du déterminant réduit, on déduit la décomposition de $\mathbb{G}_2$ suivante $\mathbb{G}_2^1 \times \mathbb{Z}_p$ et un isomorphisme de Künneth :

$$H^*(\mathbb{G}_2, (E_2)_*/(p)) \;\cong\; H^*(\mathbb{G}_2^1, (E_2)_*/(p)) \underset{\mathbb{Z}_p}{\otimes} \Lambda_{\mathbb{Z}_p}[\zeta]$$

Ainsi, il nous suffit de considérer le sous-groupe $\mathbb{G}_2^1$. Ce dernier groupe contient un p-Sylow d'indice fini noté S_2^1 et un sous-groupe fini F d'ordre $2(p^2-1)$ tels que $\mathbb{G}_2^1 = S_2^1 \rtimes F$. En utilisant la théorie des groupes p-adiques analytiques développée par M. Lazard dans [Laz65], H-W. Henn dans [Hen07] a montré l'existence d'une résolution projective de $\mathbb{Z}_p$ au-dessus de $\mathbb{G}_2^1$ de la forme :

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0 \qquad (\star)$$

où $C_0 = C_3 = \mathbb{Z}_p \uparrow_F^{\mathbb{G}_2^1}$, $C_1 = C_2 = \Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1}$ et Λ_{1-p} est une représentation linéaire du groupe F de dimension 2 au-dessus de l'anneau des entiers p-adiques. Cependant la démonstration ne donne pas explicitement les homomorphismes ∂_i. Une détermination des homomorphismes est l'objet du chapitre 2.

Le chapitre 2 est donc consacré à la détermination des différentielles de la précédente résolution projective. En utilisant le fait que $\mathbb{G}_2^1 = S_2^1 \rtimes F$, on note qu'en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module, $C_3 = C_0$ et $C_2 = C_1$ sont libres de rang un et deux respectivement. On note e_0, $((e_1)_+, (e_1)_-)$, $((e_2)_+, (e_2)_-)$ et e_3 les bases des modules C_0, C_1, C_2 et C_3 en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module. L'homomorphisme $\epsilon : C_0 \to \mathbb{Z}_p$ s'identifie avec l'homomorphisme d'augmentation $\mathbb{Z}_p[\![S_2^1]\!] \to \mathbb{Z}_p$ et donc le noyau $N_0 = \ker(\epsilon)$ est isomorphe à l'idéal d'augmentation (IS_2^1). On déterminera deux éléments $a_0, b_0 \in S_2^1$ tels que leurs classes engendrent $H_1(S_2^1, \mathbb{Z}_p) \cong S_2^1/[S_2^1, S_2^1]$, ainsi $a_0 - e$ et $b_0 - e$ déterminent des générateurs de N_0 en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module. Ensuite, on définit un homomorphisme de $\mathbb{Z}_p$-modules $d_1 : \Lambda_{1-p} \to C_0$ qui envoie une base de Λ_{1-p} en tant que $\mathbb{Z}_p$-module libre de rang deux sur les éléments $a_0 - e$ et $b_0 - e$. Comme le groupe F est d'ordre premier à p, on peut prendre la moyenne de l'homomorphisme d_1 sous l'action de F pour obtenir

un homomorphisme $\mathbb{Z}_p[F]$-linéaire, noté $\mathrm{tr}_F(d_1)$. Enfin, par extension des scalaires de $\mathbb{Z}_p[F]$ à $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$, on obtient l'homomorphisme $\partial_1 = \mathrm{tr}_F(d_1)\uparrow_F^{\mathbb{G}_2^1}: C_1 \to C_0$ qui se factorise par N_0. Ensuite, du lemme de type Nakayama (lemme 4.5 [GHMR05]), on déduit que ∂_1 est surjectif sur N_0, car $H_0(S_2^1, \partial_1)$ l'est.
Pour la seconde différentielle ∂_2 nous avons utilisé la même méthode de construction que pour ∂_1. Cependant, la complexité de l'homomorphisme ∂_1 a rendu impossible de déterminer exactement des générateurs de son noyau, noté N_1. Nous nous sommes donc contenté d'approximations suffisantes pour faire aboutir notre application au calcul des groupes de cohomologie continue $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ dans le chapitre 4. Plus précisément, nous avons cherché deux éléments $\kappa_+, \kappa_- \in C_1$ tels que

$$\begin{cases} \kappa_\pm & \equiv \ p\epsilon_\pm \quad \mathrm{mod}\,(IS_2^1)C_1 \\ \partial_1(\kappa_\pm) & \equiv \ 0 \qquad \mathrm{mod}\,\mathcal{I}N_0 \end{cases}$$

où $\mathcal{I} = (IS_2^1)(IF_1S_2^1) + (IF_1S_2^1)(IS_2^1)$ est un idéal de $\mathbb{Z}_p[\![S_2^1]\!]$. Ainsi, en utilisant le fait que ∂_1 est surjectif sur N_0, on a l'existence de $\tilde{\kappa}_\pm \in \mathcal{I}C_1$ tels que $\kappa_\pm + \tilde{\kappa}_\pm$ appartiennent à N_1. De plus, d'après l'étude de $H_0(S_2^1, \partial_1)$, on sait que $\kappa_\pm + \tilde{\kappa}_\pm$ engendrent N_1. Ensuite, il suffit de poser $d_2 : \Lambda_{1-p} \longrightarrow N_1$ qui envoie $\epsilon_\pm$ sur $\kappa_\pm + \tilde{\kappa}_\pm$ et $\partial_2 := \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}$. Enfin, on peut montrer, avec une seconde application du lemme de type Nakayama, que $\partial_2 : C_2 \to N_1$ est surjectif.
Pour la troisième différentielle ∂_3, nous avons procédé d'une manière différente via une notion de dualité ($D_G(M) = \mathrm{Hom}_G(M, \mathbb{Z}_p[\![G]\!])$) introduite et utilisée dans [HKM08].
La construction est résumée dans le théorème principal de ce chapitre, le théorème 2.10. En voici, une version moins précise.

Théorème. *Il existe une résolution projective de $\mathbb{Z}_p$ au-dessus de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$ de la forme suivante*

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$$

telle que

1. *L'homomorphisme ∂_1 est déterminé par la condition*

$$\partial_1(e_1)_+ = v\, e_0$$

   où v est un certain élément de l'idéal d'augmentation (IS_2^1).

2. *L'homomorphisme ∂_2 est égal à $\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1} \circ \alpha$, où*
   i) $d_2 : \Lambda_{1-p} \to C_1$ est un homomorphisme $\mathbb{Z}_p$-linéaire qui se factorise par N_1 et qui est explicitement connu modulo $((IS_2^1)(IF_1S_2^1) + (IF_1S_2^1)(IS_2^1))C_1$.
   ii) $\alpha : C_2 \to C_2$ est un automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire dont $\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p, \alpha)$ est égal à l'identité.

3. *L'homomorphisme $\partial_3 : C_3 \to C_2$ est déterminé par la condition*

$$\partial_3(e_3) = \frac{1}{2\epsilon_+^2}\Lambda(e_2)_+ + \frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega - \omega\Lambda\omega^{-1})(e_2)_-$$

   où Λ est un certain élément de l'idéal d'augmentation (IS_2^1) en relation avec v et $\omega \in \boldsymbol{\mu}_{p^2-1} \subset \mathbb{W}(\mathbb{F}_{p^2})^\times$ est une racine primitive p^2-1-ème de l'unité.

Dans le chapitre 3, nous allons préciser l'action de certains éléments de $\mathbb{G}_2$ sur l'anneau de Lubin-Tate modulo p, $(E_2)_*/(p) \cong \mathbb{F}_{p^2}[[u_1]][u^{\pm 1}]$. On verra que si l'on se donne g dans $\mathbb{S}_2$ et qu'on pose $t_0(g) = (g_*u)u^{-1}$, alors $g_*u_1 = t_0^{p-1}(g)u_1$ modulo (p). De ce premier fait, on déduit que l'élément $v_1 = u_1u^{1-p}$ est invariant sous l'action de $\mathbb{G}_2$ dans $(E_2)_*/(p)$. Ensuite, le résultat principal est une généralisation du corollaire 4.5 de [HKM08] au cas $p \geq 3$.

Proposition. *Si* $g \equiv 1 + g_1 S + g_2 S^2 \bmod (S^3)$, *alors*

$$t_0(g) = (g_* u)u^{-1} \equiv 1 + g_1^p u_1 - g_1 u_1^p + (g_2 - g_2^p)u_1^{p+1} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{p+1+i} + g_1^2 u_1^{2p}$$

modulo $(p,\, u_1^{2p+1})$.

La première application des précédents résultats est le calcul de $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ effectué dans le chapitre 4. Comme les modules C_i sont cycliques, les groupes $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p))$ s'injectent dans l'anneau $(E_2)_*/(p)$. Ainsi, nous pouvons identifier les deux lignes du diagramme suivant :

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{G}_2^1}(C_0, M) \arrow[r, "\partial_1^*"] \arrow[d, "\mathrm{ev}_{e_0}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_1, M) \arrow[r, "\partial_2^*"] \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_2, M) \arrow[r, "\partial_3^*"] \arrow[d, "\mathrm{ev}_{e_2}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_3, M) \arrow[d, "\mathrm{ev}_{e_3}"', "\cong"] \\
(E_2)_*^F/(p) \arrow[r, "\partial_1^*"] & (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, h_0 \oplus \mathbb{F}_p\, h_1) \arrow[r, "\partial_2^*"] & (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, g_0 \oplus \mathbb{F}_p\, g_1) \arrow[r, "\partial_3^*"] & (E_2)_*^F/(p)
\end{tikzcd}$$

L'élément $v_1 \in (E_2)_*/(p)$ est invariant sous l'action de $\mathbb{G}_2^1$, d'où les homomorphismes ∂_i^* sont $\mathbb{F}_p[v_1]$-linéaires. Posons $v_2 = u^{1-p^2}$ dans $(E_2)_*^F/(p)$, alors la famille $(v_2^s)_{s\in\mathbb{Z}}$ est libre dans le $\mathbb{F}_p[v_1]$-module topologique $(E_2)_*^F/(p)$ et engendre un sous-module dense. En d'autre termes, $(v_2^s)_{s\in\mathbb{Z}}$ est une $\mathbb{F}_p[v_1]$-base topologique. L'objet essentielle du chapitre 4, est de construire des bases adaptées aux trois différentielles. Les calculs préalable de K. Shimomura auront été particulièrement utile pour aider à déterminer ces bases aboutissant au calcul de la cohomologie continue $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$.

Théorème. *Soit* $p \geq 5$ *un nombre premier. Il existe* $(X)_s$ *des éléments homogènes de* $(E_2)_*/(p)$ *où* s *parcourt l'ensemble des entiers relatifs et* X *parcourt* $\{1, h_0, h_1, g_0, g_1, h_0 g_1\}$, *tels que :*

1. *Pour tout* $X \in \{1, h_0, h_1, g_0, g_1, h_0 g_1\}$, *il existe* $c \in \mathbb{F}_p^\times$ *tel que :*

$$(X)_s \equiv c\, X\, v_2^s \mod (p, u_1)$$

2. *On a les isomorphismes de* $\mathbb{F}_p[v_1]$*-modules gradués complets suivants :*

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(h_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(h_1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(g_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(g_1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_3, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{(h_0 g_1)_s\}
\end{aligned}$$

3. *Les homomorphismes* ∂_i^* *sont diagonales dans ces bases :*

$$
\begin{array}{rcll}
\partial_1^*(1)_{sp^n} & = & \begin{cases} 0 \\ v_1(h_1)_s \\ v_1^{a_n}(h_0)_{(sp-1)p^{n-1}} \end{cases} & \begin{array}{l} si\ s=0 \\ si\ n=0,\ s\not\equiv 0\ [p] \\ si\ n\geq 1,\ s\not\equiv 0\ [p] \end{array} \\
\partial_2^*(h_0)_{sp^n} & = & \begin{cases} 0 \\ v_1^{A_n+2}(g_1)_{sp^n+\alpha_n} \\ v_1^{p^{n+2}-p^n+A_n+2}(g_1)_{(s+1-p)p^n+\alpha_n} \end{cases} & \begin{array}{l} si\ s=0 \\ si\ n\geq 0,\ s\not\equiv 0,-1\ [p] \\ si\ n\geq 0,\ s\equiv -1\ [p^2] \end{array} \\
\partial_2^*(h_1)_{sp} & = & v_1^{p-1}(g_0)_{sp-1} & \\
\partial_3^*(g_0)_s & = & v_1(h_0g_1)_s & si\ s\not\equiv -1\ [p] \\
\partial_3^*(g_1)_{sp^n+\alpha_{n-1}} & = & v_1^{a_n}(h_0g_1)_{sp^n+\alpha_n} & si\ n\geq 1\ et\ s\not\equiv -1\ [p]
\end{array}
$$

où

$$
\begin{array}{rcll}
A_n & = & \dfrac{p^n-1}{p-1}(p+1) & \\
a_n & = & \begin{cases} p^{n-1}(p+1)-1 \\ 1 \end{cases} & \begin{array}{l} si\ n>0 \\ si\ n=0 \end{array} \\
\alpha_n & = & \dfrac{1-p^n}{p-1} &
\end{array}
$$

Remarque. Les notations choisies dans le théorème précédent sont en relation avec celles utilisées par M. Behrens dans [Beh12], le théorème 3.2, où il présente différemment les résultats de K. Shimomura et ses colaborateurs sur $\pi_*(L_{K(2)}S^0)$.

En se basant sur les démonstrations dans [GHM12] concernant l'homotopie rationnelle dans le cas $p=3$, on déduit un résultat analogue pour $p>3$.

Corollaire. *Soit $p\geq 5$ un nombre premier. Rationnellement, il existe $\zeta\in\pi_{-1}(L_{K(2)}S^0)$ et $e\in\pi_{-3}(L_{K(2)}S^0)$ induisant un isomorphisme d'algèbres*

$$\pi_*(L_{K(2)}S^0)\otimes\mathbb{Q}\cong\Lambda_{\mathbb{Q}_p}(\zeta,e)$$

La dernière application est le calcul du groupe de Hopkins Pic_2 pour $p>3$ dans le chapitre 5. Je me suis basé sur l'approche de N. Karamanov dans [Kar10] où il traite le cas $p=3$. La particularité du cas $p>3$ est que Pic_2 contient un sous-groupe d'indice deux, noté Pic_2^0 qui est isomorphe à $H^1(\mathbb{G}_2,(E_2)_0^\times)$. C'est-à-dire que le problème de déterminer le groupe de Picard de la catégorie des spectres $K(2)$-locaux devient un problème algébrique uniquement. Pour déterminer $H^1(\mathbb{G}_2,(E_2)_0^\times)$, en utilisant certains outils d'homologie algébrique, on se ramène dans un premier temps (diagramme (5.1) page 114) au calcul de $H^1(\mathbb{G}_2^1,U_1)$ où $U_1=1+\mathbb{F}_{p^2}[[u_1]]u_1\subset((E_2)_0/(p))^\times$. Enfin, pour déterminer ce dernier groupe de cohomologie, de manière analogue à l'application précédente au calcul de $H^*(\mathbb{G}_2^1,(E_2)_*/(p))$, on se réduit à un problème de construction de bases adaptées (section 5.5).

Théorème (Hopkins)**.** *Soit $p\geq 5$ un nombre premier, alors*

$$\mathrm{Pic}_2\cong\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}/2(p^2-1)$$

Chapitre 1

Anneau de Lubin-Tate et le groupe stabilisateur de Morava

Dans la première section, nous allons commencer par définir le groupe stabilisateur de Morava, l'anneau gradué de Lubin-Tate et l'action du groupe sur l'anneau. Les différentes constructions et résultats sont essentiellement extrait de la section 2 [HKM08] et de la première section de [DH95]. Les sections suivantes sont consacrées à l'introduction d'objets utiles pour le calcul des groupes de cohomologie $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$, effectué dans le chapitre 4 .

1.1 Définition de l'action

Soient p un nombre premier et n un entier naturel non nul. On note Γ_n (ou $x \underset{\Gamma_n}{+} y$) la loi de groupe formel p-typique de Honda sur $\mathbb{F}_{p^n}$ caractérisée par la relation suivante :

$$[p]_{\Gamma_n}(x) := x \underset{\Gamma_n}{+} \dots \underset{\Gamma_n}{+} x = x^{p^n}$$

Avant de donner une description de l'anneau des endomorphismes $(\mathrm{End}_{\mathbb{F}_{p^n}}(\Gamma_n), \underset{\Gamma_n}{+}, \circ)$, rappelons quelques propriétés de l'*anneau de Witt* de $\mathbb{F}_{p^n}$, noté $\mathbb{W}(\mathbb{F}_{p^n})$.

Lemme 1.1 ([Rav86] A2.2.15)**.** *Soient p un nombre premier et n un entier naturel non nul.*

a) $\mathbb{W}(\mathbb{F}_p) = \mathbb{Z}_p$ et $\mathbb{W}(\mathbb{F}_{p^n})$ est une $\mathbb{Z}_p$-algèbre.

b) $\mathbb{W}(\mathbb{F}_{p^n})$ est un anneau local complet séparé d'idéal maximal (p) et de corps résiduel $\mathbb{F}_{p^n}$.

c) Tout $x \in \mathbb{W}(\mathbb{F}_{p^n})$ peut être écrit de manière unique sous la forme $\sum_{i\geq 0} x_i p^i$ où $x_i^{p^n} - x_i = 0$ pour tout i.

d) L'automorphisme de Frobenius sur $\mathbb{F}_{p^n}$ se relève en un automorphisme σ de $\mathbb{W}(\mathbb{F}_{p^n})$ défini par

$$x^\sigma := \sum_{i\geq 0} x_i^p p^i$$

e) L'algèbre $\mathbb{W}(\mathbb{F}_{p^n})$ est isomorphe à $\mathbb{Z}_p[\omega]/(h(\omega))$ où h est un facteur irréductible de degré n de $x^{p^n} - x$.

D'après le théorème de Dieudonné-Lubin (théorème A2.2.17 [Rav86]), l'anneau des endomorphismes de Γ_n sur $\mathbb{F}_{p^n}$ est isomorphe à l'algèbre non commutative

$$\mathcal{O}_n := \mathbb{W}(\mathbb{F}_{p^n})\langle S\rangle \,/(S^n - p, \{Sx - x^\sigma S\}_{x\in\mathbb{W}})$$

Plus précisément, l'isomorphisme envoie la variable S sur l'endomorphisme x^p et un relèvement de Teichmüller a dans $\mathbb{W}$ est envoyé sur l'endomorphisme $\bar{a}x$. Contrairement aux apparences, cet isomorphisme envoie bien un entier p-adique λ sur la série $[\lambda]_{\Gamma_n}(x)$.
Au passage, on note qu'en tant que $\mathbb{W}$-module à gauche l'algèbre $\mathcal{O}_n$ est égale à la somme directe

$\mathbb{W} \oplus \mathbb{W}S \oplus \ldots \oplus \mathbb{W}S^{n-1}$ et donc que tout élément x de $\mathcal{O}_n$ peut être écrit de manière unique sous la forme $\sum_{i \geq 0} x_i S^i$ où $x_i^{p^n} = x_i \in \mathbb{W}$. De plus, x modulo (S^n) ne dépend que de $x_0, \ldots, x_{n-1}$ modulo (p).

On note $\mathbb{S}_n = \mathrm{Aut}_{\mathbb{F}_{p^n}}(\Gamma_n)$ le groupe des automorphismes de Γ_n sur $\mathbb{F}_{p^n}$ et on l'appelle le groupe stabilisateur classique de Morava. Notons $\mathcal{FG}$ la catégorie dont les objets sont les couples (R, F) où F est une loi de groupe formel sur R et morphismes de (R, F) dans (S, G) sont les couples (ϕ, f) où $\phi : R \to S$ est un homomorphisme d'anneaux et $f : \phi_* F \to G$ est un morphisme de lois de groupe formel. Alors, $\mathbb{G}_n = \mathrm{Aut}_{\mathcal{FG}}(\mathbb{F}_{p^n}, \Gamma_n)$ est le groupe stabilisateur de Morava. On a un isomorphisme

$$\mathbb{G}_n \cong \mathbb{S}_n \rtimes \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$$

où l'action du groupe de Galois est caractérisée par

$$\sigma_*(x_0 + x_1 S + \ldots + x_{n-1} S^{n-1}) = x_0^\sigma + x_1^\sigma S + \ldots + x_{n-1}^\sigma S^{n-1}$$

(σ est l'automorphisme de Frobenius).

Rappelons brièvement la théorie des déformations de Lubin-Tate développée dans [LT66]. Les rappels sont basés sur la section 1 de [DH95] et la section 4.1 de [HKM08]. Soit A un anneau gradué local complet séparé tel que son corps résiduel k soit parfait de caractéristique p contenant $\mathbb{F}_{p^n}$. On note $\mathfrak{m}$ l'idéal maximal de A et $\pi : A \twoheadrightarrow A/_{\mathfrak{m}}$ le projection sur le corps résiduel. On dit que le couple $(F,\, u)$, où $F(x, y)$ est une loi de groupe formel sur A et u une unité de A, est une *déformation* de Γ_n vers A si $\pi_* F = \Gamma_n$. Soient $(F,\, u), (G,\, v)$ deux déformations de Γ_n vers A, un $\star$-isomorphisme de F vers G est un isomorphisme de lois de groupe formel $f(x) : F \to G$ tel que $\pi_* f(x) = x$ et $f'(0)v = u$. La première condition sera représenté par le diagramme suivant :

$$\begin{tikzcd} F \arrow[r, "f(x)"] \arrow[d, squiggly] & G \arrow[d, squiggly] & \text{mod } \mathfrak{m} \\ \Gamma_n \arrow[r, "\mathrm{Id}"] & \Gamma_n & \end{tikzcd}$$

On note $\mathrm{lifts}^*_{\Gamma_n}(A)$ l'ensemble des classes à $\star$-isomorphisme près de déformation de Γ_n vers A. Au passage, notons que d'après le théorème de Cartier (A2.1.18 [Rav86]) sur les lois de groupe formel p-typiques, on déduit que toute déformation de Γ_n est $\star$-isomorphe à une déformation p-typique .

Définition 1.2. L' anneau gradué de Lubin-Tate est l'anneau

$$(E_n)_* := \mathbb{W}(\mathbb{F}_{p^n})[[u_1, \ldots, u_{n-1}]][u^{\pm 1}]$$

muni de la graduation suivante : $|u_i| = 0$ et $|u| = -2$.

Nous allons maintenant donner une version "gradué" du théorème de Lubin-Tate associée au couple $(\Gamma_n,\, \mathbb{F}_{p^n})$.

Théorème 1.3 (Lubin-Tate [LT66])**.**

1. *Il existe une déformation universelle G_n sur l'anneau $(E_n)_0$ telle que pour tout A anneau local complet séparé de corps résiduel parfait de caractéristique p et contenant $\mathbb{F}_{p^n}$, l'application*

$$\begin{array}{ccc} \mathrm{Hom}^c_{\mathbb{W}(\mathbb{F}_{p^n})\text{-}Alg}(\,((E_n)_*,\ A\,) & \longrightarrow & \mathrm{lifts}^*_{\Gamma_n}(A) \\ \phi & \longmapsto & [\,(\phi_* G_n, \phi(u))\,] \end{array}$$

est une bijection.

2. *Pour toute déformation $(F,\, u)$ de Γ_n vers A le $\star$-isomorphisme entre $(\phi_* G_n, \phi(u))$ et (F, u) est unique.*

Il est possible de donner quelques précisions sur la déformation universelle G_n. Avant, rappelons que l'anneau BP_* qui classifie les lois de groupe formel p-typiques est isomorphe à $\mathbb{Z}_{(p)}[v_1, v_2, \ldots]$ et les *générateurs de Araki* (v_i) satisfont les identités suivantes dans $\mathrm{BP}_* \otimes \mathbb{Q}$:

$$p\lambda_k = \sum_{0 \le i \le k} \lambda_i v_{k-i}^{p^i} = v_k + \lambda_1 v_{k-1}^p + \ldots + \lambda_k p^{p^k} \tag{1.1}$$

où les λ_i sont les coefficients du *logarithme de la loi p-typique universelle F* au-dessus de $\mathrm{BP}_* \otimes \mathbb{Q}$:

$$\log_F(x) = \sum_{i \ge 0} \lambda_i x^{p^i}$$

avec $\lambda_0 = 1$ et $v_0 = p$. La $[p]$-séries de F est donnée par

$$[p]_F(x) = \sum_{i \ge 0}^{F} v_i x^{p^i}$$

Considérons l'homomorphisme de BP_* vers $(E_n)_*$ défini par

$$v_i \longmapsto \begin{cases} u_i u^{1-p^i} & 1 \le i < n \\ u^{1-p^n} & i = n \\ 0 & i > n \end{cases}$$

Il induit avec F une loi de groupe formel p-typique F_n sur $(E_n)_*$. On peut montrer que la loi de groupe formel p-typique $G_n(x, y) = u^{-1} F_n(ux, uy)$ est bien une déformation universelle de Γ_n. De plus, sa $[p]$-série est

$$[p]_{G_n}(x) = px \underset{G_n}{+} u_1 x^p \underset{G_n}{+} \ldots \underset{G_n}{+} u_{n-1} x^{p^{n-1}} \underset{G_n}{+} x^{p^n}$$

et si l'on munit $(E_n)_*[[x, y]]$ de la graduation : $|x| = |y| = |u_i| = 0$ et $|u| = -2$, alors $G_n(x, y)$ est homogène de degré 0.

Soit g un élément du groupe stabilisateur classique de Morava $\mathbb{S}_n$. Nous allons rappeler comment on le fait agir sur l'anneau gradué de Lubin-Tate $(E_n)_*$. Comme $\mathcal{O}_n$ en tant $\mathbb{W}$-module à gauche est égal à la somme directe $\mathbb{W} \oplus \ldots \oplus \mathbb{W} S^{n-1}$, on déduit qu'on peut écrire un élément g de $\mathcal{O}_n^\times \cong \mathbb{S}_n$ de manière unique sous la forme suivante $\sum_{i \ge 0} g_i S^i$ où $g_i^{p^n} = g_i \in \mathbb{W}$. On note $\bar{g}_i \in \mathbb{F}_{p^n}$ la réduction modulo (p) de g_i. Ainsi, g s'identifie avec $g(x) = \sum_{i \ge 0}^{\Gamma_n} \bar{g}_i x^{p^i}$ dans $\mathbb{S}_n$. Soit $\tilde{g}(x)$ dans $(E_n)_0[[x]]$ un relèvement de $g(x)$, c'est-à-dire tel que $\tilde{g}(x) \equiv g(x)$ modulo $(p, u_1, \ldots, u_{n-1})$. Posons

$$G_n^{\tilde{g}}(x, y) := \tilde{g}^{-1} G_n(\tilde{g}x, \tilde{g}y)$$

De telle sorte que $\tilde{g}(x)$ soit un homomorphisme de la transmutée[1] $G_n^{\tilde{g}}$ vers G_n. D'après le théorème de Lubin-Tate, il existe un unique homomorphisme d'anneaux gradués locaux g_* : $(E_n)_* \longrightarrow (E_n)_*$ et un unique $\star$-isomorphisme $e_g(x)$ de $(g_* G_n,\, g_* u)$ vers $(G_n^{\tilde{g}},\, \tilde{g}'(0)u)$. D'où le diagramme suivant :

$$h_g : \quad \begin{array}{ccccc} g_* G_n & \xrightarrow{e_g} & G_n^{\tilde{g}} & \xrightarrow{\tilde{g}} & G_n \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{mod}\,(p, u_1, \ldots, u_{n-1})} \\ \Gamma_n & \xrightarrow{\mathrm{Id}} & \Gamma_n & \xrightarrow{g} & \Gamma_n \end{array} \tag{1.2}$$

1. Vocabulaire utilisé par M. Lazard dans [Laz55].

où $h_g(x) = \tilde{g}(e_g(x))$ est un isomorphisme de lois de groupe formel p-typiques. Ainsi, il peut être écrit sous la forme suivante (lemme A2.1.26 [Rav86]) :

$$h_g(x) = \sum_{i \geq 0}^{G_n} t_i(g) x^{p^i} \tag{1.3}$$

où les t_i sont des fonctions continues univoquement déterminées. D'où,

$$g_* u = h'_g(0) u = t_0(g) u \tag{1.4}$$

et

$$t_i(g) \equiv g_i \mod (p, u_1, \ldots, u_{n-1}) \tag{1.5}$$

Notation. On note $\boldsymbol{\mu}_{p^n-1}$ le sous-groupe des racines $p^n - 1$-ème de l'unité de $\mathbb{W}(\mathbb{F}_{p^n})$.

Proposition 1.4.

1. *L'action de $\mathbb{S}_n$ sur $(E_n)_*$ se fait par automorphisme continue de $\mathbb{W}(\mathbb{F}_{p^n})$-algèbres de degré 0.*
2. *Pour tout $g \in \boldsymbol{\mu}_{p^n-1}$, $g_* u_i = g^{p^i-1} u_i$ et $g_* u = g\, u$.*
3. *Soit σ l'automorphisme de Frobenius ($\sigma \in \mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$), alors quel que soit x dans $\mathbb{W}$, $\sigma_* u = u$, $\sigma_* u_1 = u_1$ et $\sigma_* x = x^\sigma$.*
4. *Pour tout g dans $\mathbb{Z}_p^\times$, $g_* u_i = u_i$ et $g_* u = gu$.*

Démonstration. 1. D'après, le théorème de Lubin-Tate, on a que l'action de $\mathbb{S}_n$ sur $(E_2)_0$ se fait par automorphisme de $\mathbb{W}(\mathbb{F}_{p^n})$-algèbres. Ensuite l'action d'un élément g de $\mathbb{S}_n$ sur u est définie par la multiplication avec $t_0(g) \in (E_2)_0$. Donc l'action sur l'anneau de Lubin-Tate $(E_2)_*$ est de degré 0 et se fait par automorphisme de $\mathbb{W}(\mathbb{F}_{p^n})$-algèbres.
2. Ce résultat se trouve dans la démonstration du lemme 22 dans [Hen07], mais nous allons tout de même en rappeler la preuve. Soit $g \in \boldsymbol{\mu}_{p^n-1}$, notons $\bar{g}$ son image dans le corps résiduel $\mathbb{F}_{p^n}$. Posons $\tilde{g}(x) = gx$, c'est un relèvement de $\bar{g}\, x$ qui induit un homomorphisme de $G_n^{\tilde{g}}$ vers G_n. Au-dessus de $(E_n)_0$, la p-série associée à $G_n^{\tilde{g}}$ est

$$\begin{aligned}
[p]_{G_n^{\tilde{g}}}(x) &= g^{-1}[p]_{G_n}(gx) \\
&= \tilde{g}^{-1}(\, pgx \underset{G_n}{+} u_1 g^p x^p \underset{G_n}{+} \ldots \underset{G_n}{+} u_{n-1} g^{p^{n-1}} x^{p^{n-1}} \underset{G_n}{+} g x^{p^n}\ ) \\
&= px \underset{G_n^{\tilde{g}}}{+} u_1 g^{p-1} x^p \underset{G_n^{\tilde{g}}}{+} \ldots \underset{G_n^{\tilde{g}}}{+} u_{n-1} g^{p^{n-1}-1} x^{p^{n-1}} \underset{G_n^{\tilde{g}}}{+} x^{p^n}
\end{aligned} \tag{1.6}$$

De l'allure de $\tilde{g}(x)$ et comme G_n est p-typique, on déduit par le lemme A2.1.26 de [Rav86] que la loi de groupe formel $G_n^{\tilde{g}}$ est p-typique. Soit $g_* : (E_n)_* \to (E_n)_*$ l'automorphisme de $\mathbb{W}(\mathbb{F}_{p^n})$-algèbres caractérisé par les relations données dans la proposition. Alors G_n et $G_n^{\tilde{g}}$ ont la même p-série et elles sont toutes les deux p-typiques, ainsi en utilisant le fait que $(\mathrm{BP}_*, \mathrm{BP}_*\mathrm{BP})$ représente l'algébroïde de Hopf des lois de groupe formel p-typiques (théorème A2.1.25) et les relations de Araki (théorème A2.2.3), on déduit que $G_n = G_n^{\tilde{g}}$. Si l'on pose $e_g(x) = x$, $h_g(x) = \tilde{g}(x)$, en particulier $h'_g(0) = g$. D'autre part le diagramme (1.2) associé est commutatif et l'automorphisme g_* convient.
3. Avec la définition de la catégorie des déformations de Γ_n vers A que j'ai utilisé il faut prendre le point 3. de la proposition comme une définition de l'action de σ et vérifier qu'elle est adaptée à l'action de $\mathbb{S}_n$. Cependant, en enrichissant la catégorie des déformations, il aurait été possible de faire apparaitre naturellement l'action du groupe de Galois. Les objets de cette catégorie enrichie sont les triplets (F, u, i) où F est une loi de groupe formel sur A, $u \in A^\times$ et $i : \mathbb{F}_{p^n} \to A/_{\mathfrak{m}}$ tels

que $\pi_* F = i_* \Gamma_n$. Dans cette catégorie, on tient en compte comment on injecte le corps de base $\mathbb{F}_{p^n}$ dans le corps résiduel de A et l'ensemble des ces injections est en correspondance avec le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$.
4. Soit g un élément du centre $\mathbb{Z}_p^\times$. L'homomorphisme d'anneaux $[.]_{G_n} : \mathbb{Z} \longrightarrow \mathrm{End}_{(E_n)_0}(G_n)$ peut être prolongé, de manière unique, en un homomorphisme continue sur $\mathbb{Z}_p$. En revenant, à la définition de l'action, on note en particulier que $h_g(x) = [g]_{G_n}(x)$ et que $e_g(x) = x$. D'où $g_* G_n = G_n$ et la restriction de g_* à $(E_2)_0$ est l'identité. De plus, l'endomorphisme $[g]_{G_n}(x)$ vérifie la propriété suivante :

$$\forall\, g \in \mathbb{Z}_p : \ [g]_{G_n}(x) \equiv gx \mod (x^2)$$

D'où $t_0(g) = g$.

□

En toute généralité, nous allons encore préciser l'action du sous-groupe $\mathbb{W}(\mathbb{F}_{p^n})^\times$ sur $(E_n)_0$ modulo $(u_1, \dots, u_{n-1})$. Ce résultat nous sera d'une particulière utilité dans le chapitre 5 sur le groupe Pic_2.

Proposition 1.5.

1. *L'action de $\mathbb{W}(\mathbb{F}_{p^n})^\times \subset \mathbb{S}_n$ sur $(E_n)_0$ est triviale modulo $(u_1, \dots, u_{n-1})$ et pour tout $g \in \mathbb{W}(\mathbb{F}_{p^n})^\times$ et tout $X \in (E_n)_0$, on a*

$$g_* u \ \equiv \ gu \mod (u_1, \dots, u_{n-1})$$

2. *L'idéal $(u_1, \dots, u_{n-1})$ est un sous-$\mathbb{Z}_p[\![\mathbb{W}(\mathbb{F}_{p^n})^\times]\!]$-module de $(E_n)_0$. Ainsi, la projection $\pi : (E_n)_0 \twoheadrightarrow \mathbb{W}(\mathbb{F}_{p^n})$ est $\mathbb{Z}_p[\![\mathbb{W}(\mathbb{F}_{p^n})^\times]\!]$-linéaire et la suite*

$$0 \longrightarrow (u_1, \dots, u_{n-1}) \longrightarrow (E_n)_0 \xrightarrow{\pi} \mathbb{W}(\mathbb{F}_{p^n}) \longrightarrow 0$$

est une suite exacte courte de $\mathbb{Z}_p[\![\mathbb{W}(\mathbb{F}_{p^n})^\times]\!]$-modules.

Démonstration. On note $G_n(x, y)$ la déformation universelle de $\Gamma_n(x, y)$, la loi de groupe formel de Honda de hauteur n, vers l'anneau de Lubin-Tate $(E_n)_0$. Posons $\tilde{G}(x, y) = \pi_* G_n(x, y)$ où π est la projection de $(E_n)_0$ sur $(E_n)_0/(u_1, \dots, u_{n-1}) \cong \mathbb{W}(\mathbb{F}_{p^n})$. Ainsi, $\tilde{G}(x, y) \equiv \Gamma_n(x, y)$ modulo (p), c'est-à-dire $\tilde{G}(x, y)$ est une déformation de $\Gamma_n(x, y)$ vers $\mathbb{W}(\mathbb{F}_{p^n})$. La p-série de $G_n(, x, y)$ est

$$[p]_{G_n}(x) = px \underset{G_n}{+} u_1 x^p \underset{G_n}{+} \dots \underset{G_n}{+} u_{n-1} x^{p^{n-1}} \underset{G_n}{+} x^{p^n}$$

D'où

$$[p]_{\tilde{G}}(x) = px \underset{\tilde{G}}{+} x^{p^n}$$

Avant de pouvoir démontrer la proposition, nous allons montrer que pour tout $a \in \mathbb{W}(\mathbb{F}_{p^n})$, il existe un endomorphisme $[a](x)$ de $\tilde{G}(x, y)$ telle que $[a](x) \equiv ax$ modulo (p).
D'après la première section *The formal Lie A-modules* de [LT65], si l'on considère $f(x) = [p]_{\tilde{G}}(x)$, il existe une unique loi de groupe formel $F_f(x, y)$ telle que $f(x)$ soit un endomorphisme de $F_f(x, y)$. Par unicité, on note que $F_f(x, y)$ est égale à $\tilde{G}(x, y)$. De plus, quel que soit $a \in \mathbb{W}(\mathbb{F}_{p^n})$, il existe une unique série $[a](x) \in \mathbb{W}(\mathbb{F}_{p^n})[[x]]$, telle que

a) $[a](x)$ commute avec la p-série de $\tilde{G}(x, y)$,

b) $[a](x) \equiv ax \mod (x^2)$.

Cette construction induit un homomorphisme continue d'anneaux

$$[.] : \mathbb{W}(\mathbb{F}_{p^n}) \longrightarrow \mathrm{End}(\tilde{G})$$

prolongeant la structure de $\mathbb{Z}_p$-module de $\mathrm{End}(\tilde{G})$. En particulier,

$$[p](x) = [p]_{\tilde{G}}(x) \equiv [p]_{\Gamma_n}(x) \mod (p)$$

D'autre part, soit $\xi \in \boldsymbol{\mu}_{p^n-1} \subset \mathbb{W}(\mathbb{F}_{p^n})^\times$ une racine p^n-1-ème de l'unité. Posons $g(x) = \xi x \in \mathbb{W}(\mathbb{F}_{p^n})[[x]]$ et $\tilde{G}^g(x,y)$ l'unique loi de groupe formel sur $\mathbb{W}(\mathbb{F}_{p^n})$ telle que $g(x)$ soit un homomorphisme de $\tilde{G}^g(x,y)$ vers $\tilde{G}(x,y)$. Alors, on déduit que

$$[p]_{\tilde{G}^g}(x) = g^{-1}[p]_{\tilde{G}}(gx) = g^{-1}\left(p\xi x \underset{\tilde{G}}{+} \xi^{p^n} x^{p^n}\right) = px \underset{\tilde{G}^g}{+} x^{p^n}$$

On note que la p-série de $\tilde{G}^g(x,y)$ s'écrit de la même manière que celle de $\tilde{G}(x,y)$. Or $\tilde{G}^g(x,y)$ et $\tilde{G}(x,y)$ sont p-typiques et donc uniquement caractérisées par leurs p-séries (théorème A2.1.27 [Rav86]), d'où $\tilde{G}^g(x,y) = \tilde{G}(x,y)$ et $g(x) = \xi x$ est un endomorphisme de $\tilde{G}(x,y)$. Ainsi, de l'unicité de la série $[\xi](x) \in \mathbb{W}(\mathbb{F}_{p^n})[[x]]$ telle que $[\xi](x)$ commute avec la p-série de $\tilde{G}(x,y)$ et $[\xi](x) \equiv \xi x$ modulo (x^2), on déduit que $[\xi](x) = \xi x$. En particulier $[\xi](x) \equiv \xi x$ modulo (p).
Rappelons (lemme 1.1) que tout élément $x \in \mathbb{W}(\mathbb{F}_{p^n})$ s'écrit de manière unique sous la forme $\sum_{i\geq 0} \xi_i p^i$ où $\xi_i \in \boldsymbol{\mu}_{p^n-1}$ pour tout i. Ainsi, on déduit par continuité de $[.] : \mathbb{W}(\mathbb{F}_{p^n}) \to \mathrm{End}(\tilde{G})$ que

$$\forall\, a \in \mathbb{W}(\mathbb{F}_{p^n}) : \quad [a](x) \equiv ax \mod (p)$$

Soit $g \in \mathbb{W}(\mathbb{F}_{p^n})^\times \subset \mathbb{S}_n$ qu'on identifie avec son image dans $\mathrm{End}_{\mathbb{F}_{p^n}}(\Gamma_n)$. Soit $\tilde{g}(x) \in (E_n)_0[[x]]$ un relèvement de $[g](x)$. Notons que $[g](x)$ est un relèvement de $g(x)$. En revenant à la construction de l'action de $\mathbb{S}_2$ sur l'anneau de Lubin-Tate, on déduit le diagramme de déformations suivant :

$$\begin{tikzcd}
g_*G_n \arrow[r, "e_g"] \arrow[d, squiggly] & G_n^{\tilde{g}} \arrow[r, "\tilde{g}"] \arrow[d, squiggly] & G_n \arrow[d, squiggly, "\mathrm{mod}\,(u_1,\ldots,u_{n-1})"] & \mathrm{lifts}_{\Gamma_n}(\,(E_n)_0\,) \\
\pi_*G_n \arrow[r, "\mathrm{Id}"] \arrow[d, squiggly] & \tilde{G} \arrow[r, "{[g]}"] \arrow[d, squiggly] & \tilde{G} \arrow[d, squiggly, "\mathrm{mod}\,(p)"] & \mathrm{lifts}_{\Gamma_n}(\,\mathbb{W}(\mathbb{F}_{p^n})\,) \\
\Gamma_n \arrow[r, "\mathrm{Id}"] & \Gamma_n \arrow[r, "g"] & \Gamma_n & \mathcal{FGL}(\,\mathbb{F}_{p^n}\,)
\end{tikzcd}$$

Par unicité de l'homomorphisme qui représente une déformation (théorème 1.3 de Lubin-Tate), on déduit que $\pi_* g_* = \pi_*$ et donc que l'action de g est triviale modulo $(u_1, \ldots, u_{n-1})$. De plus, $h_g(x) = \tilde{g} \circ e_g(x) \equiv [g](x) \equiv gx$ modulo $(u_1, \ldots, u_{n-1}, x^2)$, d'où

$$t_0(g) = h'_g(0) \equiv g \mod (u_1, \ldots, u_{n-1})$$

D'où le premier point de la proposition. Les autres points en sont des conséquences immédiates. □

Lorsque $n = 2$, on note que l'action du second groupe stabilisateur de Morava $\mathbb{S}_2$ sur l'anneau de Lubin-Tate ne dépend que des coordonnées $t_0(g)$ et $t_1(g)$ de l'endomorphisme p-typique $h_g(x)$ caractérisé par la relation (1.3). Plus précisément, on a le lemme suivant.

Lemme 1.6. *Dans $(E_2)_*$, quel que soit $g \in \mathbb{S}_2$, on a*

$$g_* u_1 = (p - p^p) t_0^{-1}(g) t_1(g) + t_0^{p-1}(g) u_1$$

L'idée de la preuve vient de celle de la proposition 4.3 de [HKM08]. D'ailleurs, nous en donnerons une version pour $p \geq 5$ avec la proposition 3.2.

Démonstration. Pour alléger les notations, je pose $G = G_n$ et $t_i(g) = t_i$. Rappelons qu'alors $[p]_G(x) = px \underset{G}{+} u_1 x^p \underset{G}{+} x^{p^2}$ et $h_g(x) = \sum_{i \geq 0}^{G} t_i x^{p^i}$ est un homomorphisme de lois de groupe formel de $g_* G$ vers G. Donc $h_g([p]_{g_* G}\, x) = [p]_G(h_g x)$ et

$$\begin{aligned} h_g([p]_{g_*G}\, x) &\equiv t_0(px \underset{(g_*G)}{+} g_* u_1 x^p) \underset{(G)}{+} t_1 p^p x^p \equiv p t_0 x + (t_0 g_* u_1 + t_1 p^p) x^p \mod (x^{p+1}) \\ [p]_G(h_g x) &\equiv p(t_0 x \underset{(G)}{+} t_1 x^p) \underset{(G)}{+} u_1 t_0^p x^p \equiv p t_0 x + (p t_1 + u_1 t_0^p) x^p \mod (x^{p+1}) \end{aligned}$$

En identifiant les coefficients devant x^p, on déduit le lemme. $\square$

1.2 Filtration et déterminant réduit

Dans cette section, on commence par rappeler quelques généralités sur les sous-groupes de $\mathbb{G}_n$ en suivant la section 2.1 de [HKM08].

Définition 1.7. On pose S_n le noyau de la projection $\mathbb{S}_n \to \mathbb{F}_{p^n}^{\times}$ restriction de la projection $\mathcal{O}_n \to \mathcal{O}_n/(S)$. On munit S_n de la filtration :

$$\forall i \in \frac{\mathbb{N}^*}{n} \quad F_i S_n = \{\ x \in S_n \,|\, x \equiv 1 \bmod (S^{ni})\ \}$$

Comme l'anneau local $\mathcal{O}_n$ est complet et séparé pour la topologie (S)-adique, on déduit que S_n est complet et séparé. C'est-à-dire

$$S_n \cong \varprojlim S_n/F_i S_n$$

De plus, pour tout i, $S_n/F_i S_n$ est un p-groupe, d'où S_n est un pro-p-groupe. D'autre part, il est immédiat que

$$\mathbb{S}_n \cong S_n \rtimes \boldsymbol{\mu}_{p^n - 1}$$

Donc S_n est un *p-Sylow* du groupe profini $\mathbb{S}_n$.

Si l'on identifie $\mathrm{gr}_i\, S_n = F_i S_n / F_{i+1/n} S_n$ avec $\mathbb{F}_{p^n}$ via l'isomorphisme qui envoie $[1 + a_{ni} S^{ni} + \ldots]$ sur a_{ni}, alors le crocher de Lie et l'application puissance p-ème P sont explicitement données de la manière suivante :

Lemme 1.8 (Lemme 3.1.4 [Hen98])**.** *Soient $\bar{a} \in \mathrm{gr}_i\, S_n$ et $\bar{b} \in \mathrm{gr}_j\, S_n$. On pose $\phi(i) = \min(i + 1, pi)$. Alors*

a) Le commutateur induit un homomorphisme de $\mathrm{gr}_i(S_n) \times \mathrm{gr}_j(S_n)$ dans $\mathrm{gr}_{i+j}(S_n)$ et on a :

$$[\bar{a}, \bar{b}] = \bar{a} \bar{b}^{p^{ni}} - \bar{b} \bar{a}^{p^{nj}}$$

b) La p-ème puissance induit un homomorphisme, noté P, de $\mathrm{gr}_i(S_n)$ dans $\mathrm{gr}_{\phi(i)}(S_n)$ et on a :

$$P\bar{a} = \begin{cases} \bar{a}^{1 + p^{ni} + \ldots + p^{(p-1)ni}} & si\ i < (p-1)^{-1} \\ \bar{a} + \bar{a}^{1 + p^{ni} + \ldots + p^{(p-1)ni}} & si\ i = (p-1)^{-1} \\ \bar{a} & si\ i > (p-1)^{-1} \end{cases}$$

Malheureusement, l'information sur le commutateur donnée dans le lemme précédent n'est pas suffisante pour la suite. Nous aurons besoin du lemme suivant.

Lemme 1.9. *Soient $a = 1 + a_iS^i + a_{i+1}S^{i+1} + \dots$ et $b = 1 + b_jS^j + b_{j+1}S^{j+1} + \dots$ deux éléments de S_n, avec $i, j \geq 1$. Alors*

$$\begin{aligned}
[a,b] \quad \equiv \quad & 1 + (a_i b_j^{\sigma^i} - a_i^{\sigma^j} b_j) S^{i+j} \\
& + \Big(a_{i+1} b_j^{\sigma^{i+1}} - a_{i+1}^{\sigma^j} b_j + a_i b_{j+1}^{\sigma^i} - a_i^{\sigma^{j+1}} b_{j+1} \Big) S^{i+j+1} \\
& - (a_i b_j^{\sigma^i} - a_i^{\sigma^j} b_j)\, a_i^{\sigma^{i+j}}\ S^{2i+j} \\
& - (a_i b_j^{\sigma^i} - a_i^{\sigma^j} b_j)\, b_j^{\sigma^{i+j}}\ S^{i+2j}
\end{aligned}$$

modulo (S^{i+j+2}).

Démonstration. Dans l'anneau complet $\mathcal{O}_n$, l'élément $a-1$ appartient à l'idéal bilatère engendré par S. Ainsi, la suite $((a-1)^n)$ tend vers zéro et $a^{-1} = 1 + \sum_{i \geq 1} (-1)^i (a_iS^i + a_{i+1}S^{i+1} + \dots)^i$ est bien défini. En particulier, on a $a^{-1} \equiv 1 - a_iS^i$ modulo (S^{i+1}). Ensuite, de la définition du commutateur $[a,b] = aba^{-1}b^{-1}$, on déduit que $[a,b] - 1$ est égal à

$$\begin{aligned}
& \Big((a-1)(b-1) - (b-1)(a-1)\Big) a^{-1} b^{-1} \\
\equiv \quad & \Big((a_iS^i + a_{i+1}S^{i+1})(b_jS^j + b_{j+1}S^{j+1}) - (b_jS^j + b_{j+1}S^{j+1})(a_iS^i + a_{i+1}S^{i+1}) \Big) a^{-1}b^{-1} \\
\equiv \quad & \Big((a_i b_j^{\sigma^j} - a_i^{\sigma^i} b_j) S^{i+j} + (a_i b_{j+1}^{\sigma^i} + a_{i+1} b_j^{\sigma^{i+1}} - a_{i+1}^{\sigma^j} b_j - a_i^{\sigma^{j+1}} b_{j+1}) S^{i+j+1} \Big) a^{-1} b^{-1}
\end{aligned}$$

modulo (S^{i+j+2}). Posons $\alpha = (a_i b_j^{\sigma^j} - a_i^{\sigma^i} b_j)$ et $\beta = (a_i b_{j+1}^{\sigma^i} + a_{i+1} b_j^{\sigma^{i+1}} - a_{i+1}^{\sigma^j} b_j - a_i^{\sigma^{j+1}} b_{j+1})$, alors

$$\begin{aligned}
[a,b] - 1 \quad & \equiv \quad (\alpha S^{i+j} + \beta S^{i+j+1})(1 - a_iS^i)(1 - b_jS^j) \\
& \equiv \quad \alpha S^{i+j} + \beta S^{i+j+1} - \alpha a_i^{\sigma^{i+j}} S^{2i+j} - \alpha b_j^{\sigma^{i+j}} S^{i+2j} \quad \mod (S^{i+j+2})
\end{aligned}$$

□

Nous allons maintenant définir certains groupes en relation avec le groupe de Morava. Notons que $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ est inclus dans le centre de $\mathbb{G}_n$.

Définition 1.10. On pose $P\mathbb{G}_n$ le groupe quotient $\mathbb{G}_n/1 + p\mathbb{Z}_p$ et $P\mathbb{S}_n$ le groupe quotient $\mathbb{S}_n/1 + p\mathbb{Z}_p$.

Pour certaines valeurs de n et p, le groupe quotient $P\mathbb{S}_n$ s'identifie avec un sous-groupe de $\mathbb{S}_n$ que nous allons définir.
Comme $\mathbb{S}_n$ est isomorphe au groupe des unités de l'anneau $\mathcal{O}_n$ et $\mathcal{O}_n$ est libre de rang n en tant que $\mathbb{W}(\mathbb{F}_{p^n})$-module, un élément x de S_n induit par multiplication à droite un automorphisme $\mathbb{W}(\mathbb{F}_{p^n})$-linéaire. D'où, un homomorphisme de groupes

$$\mathbb{S}_n \xrightarrow{.x} \mathrm{GL}_n(\mathbb{W}(\mathbb{F}_{p^n})) \xrightarrow{\det} \mathbb{W}(\mathbb{F}_{p^n})^\times$$

On peut montrer que le précédent homomorphisme se factorise par $\mathbb{Z}_p^\times$. Ensuite, on peut le prolonger en un homomorphisme

$$\mathbb{G}_n = \mathbb{S}_n \rtimes \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p) \to \mathbb{Z}_p^\times \times \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p) \twoheadrightarrow \mathbb{Z}_p^\times$$

Proposition-Définition 1.11. *On définit l'application*

$$\begin{aligned} \det : \mathbb{G}_n = \mathbb{S}_n \rtimes \mathrm{Gal}(\mathbb{F}_{p^n};\mathbb{F}_p) &\longrightarrow \mathbb{Z}_p^\times \\ (x,\sigma^i) &\longmapsto \det(.x) \end{aligned}$$

C'est un homomorphisme de groupes appelé déterminant et la composée

$$N : \mathbb{G}_n \xrightarrow{\det} \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times/\boldsymbol{\mu}_{p-1} \cong \mathbb{Z}_p$$

est appelée le déterminant réduit[2].

Définition 1.12. On note $\mathbb{G}_n^1$ le noyau du déterminant réduit N de $\mathbb{G}_n$ dans $\mathbb{Z}_p^\times/\boldsymbol{\mu}_{p-1}$ et $\mathbb{S}_n^1$ (resp. S_n^1) l'intersection de $\mathbb{G}_n^1$ avec $\mathbb{S}_n$ (resp. S_n).

Lemme 1.13.

a) Le centre $Z(\mathbb{S}_n)$ de $\mathbb{S}_n$ est égal à $\mathbb{Z}_p^\times$.

b) Si p ne divise pas n et p impair, alors le déterminant réduit induit la suite exacte courte scindée suivante

$$1 \longrightarrow S_n^1 \longrightarrow S_n \xrightarrow{N} 1 + p\mathbb{Z}_p \longrightarrow 1$$

De plus, $S_n \cong S_n^1 \times \mathbb{Z}_p$ et $PS_n \cong S_n^1$.

c) $\mathbb{G}_n^1 \cong S_n^1 \rtimes F$, où $F = \boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^n},\mathbb{F}_p)$.

Remarque. En fait, si p ne divise pas n, on a aussi $\mathbb{G}_n \cong \mathbb{G}_n^1 \times \mathbb{Z}_p$ et $P\mathbb{G}_n \cong \mathbb{G}_n^1$.

Démonstration.
a) Comme $\mathbb{Z}_p^\times$ est invariant sous l'action du groupe de Galois, on déduit facilement que $\mathbb{Z}_p^\times$ est inclus dans le centre de $\mathbb{S}_n \cong \mathcal{O}_n^\times$. Réciproquement, soit $x = x_0 + x_1 S + \ldots + x_{n-1}S^{n-1}$, avec $x_i \in \mathbb{W}$, un élément du centre. Soit $\xi \in \boldsymbol{\mu}_{p^n-1}$, comme $x\xi = \xi x$, on déduit que $x_1 = \ldots = x_{n-1} = 0$. De plus $(1+S)x_0 = x_0(1+S)$, ce qui implique que $x_0^\sigma = x_0$, c'est à dire $x = x_0 \in \mathbb{Z}_p^\times$.
b) Supposons que p ne divise pas n. La restriction du déterminant à $\mathbb{Z}_p^\times$ est la puissance n-ème. Ainsi, si l'on identifie $1+p\mathbb{Z}_p$ avec $\mathbb{Z}_p$, alors la composée

$$\mathbb{Z}_p \hookrightarrow S_n \xrightarrow{N} \mathbb{Z}_p$$

est l'application qui envoie λ sur $n\lambda$. D'où, la restriction du déterminant réduit à S_n est surjective. De plus, la suite exacte courte $S_n^1 \to S_n \to \mathbb{Z}_p$ admet une section. Les autres propriétés s'en déduisent simplement.
c) Le groupe $\mathrm{Gal}(\mathbb{F}_{p^n},\mathbb{F}_p)$ est trivialement inclus dans $\mathbb{G}_n^1$. Soit ω une racine primitive p^n-1-ème de l'unité de l'anneau de Witt $\mathbb{W}(\mathbb{F}_{p^n})$, alors

$$\det(.\omega) = \omega\,\omega^p \ldots \omega^{p^{n-1}} = \omega^{1+p+\ldots+p^{n-1}} = \omega^{(p^n-1)/(p-1)} \in \boldsymbol{\mu}_{p-1} \subset \mathbb{Z}_p^\times$$

D'où $N(\omega) = 0$ et $\boldsymbol{\mu}_{p^n-1} \subset \mathbb{G}_n^1$. De plus, on a les propriétés suivantes :

1. Remarquons que $\mathbb{S}_n^1 = \mathbb{S}_n \cap \mathbb{G}_n^1$ est égal au noyau de l'homomorphisme $\mathbb{G}_n \to \mathbb{Z}_p^\times/\boldsymbol{\mu}_{p-1} \times \mathrm{Gal}(\mathbb{F}_{p^n},\mathbb{F}_p)$ induit par le déterminant. D'autre part, S_n^1 est un p-Sylow distingué dans $\mathbb{S}_n^1$. Ainsi, S_n^1 est un sous-groupe caractéristique de $\mathbb{S}_n^1$ qui lui-même est un sous-groupe distingué de $\mathbb{G}_n$. D'où,
   S_n^1 est distingué dans $\mathbb{G}_n$.

2. Qui est parfois aussi appelée norme réduite en référence à la notion de norme réduite en théorie des nombres.

2. $S_n^1 \cap F = \{1\}$.
3. $\mathbb{G}_n^1 = S_n^1 F$: En effet, soit $g\sigma^i \in \mathbb{G}_n^1$. En revenant à l'identification $\mathbb{S}_n \cong \mathcal{O}_n^\times$, on voit immédiatement qu'il existe un entier j tel que $g\omega^j \in S_n$. Or

$$N(g\omega^j) = N(g)N(\omega^j) = N(g) = N(g\sigma^i) = 0$$

D'où $g\omega^j \in S_n^1$ et $g = (g\omega^j)\,(\omega^{-j}\sigma^i)$.

Ainsi d'un résultat classique sur les produits semi-directs, on déduit le denier point du lemme. □

On note $\mathrm{tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ l'application *trace* qui envoie x sur $x + x^p + \ldots + x^{p^{n-1}}$. Le sous-groupe S_n^1 est naturellement muni d'une filtration induite par la filtration de S_n. On note alors $\mathrm{gr}_i\, S_n^1$ le quotient $F_i S_n^1 / F_{i+\frac{1}{n}} S_n^1$.

Lemme 1.14. *Soit $i \in \mathbb{N}^*/n$, alors*

$$\mathrm{gr}_i\, S_n^1 = \begin{cases} \ker(\mathrm{tr}) & \text{si } i \in \mathbb{N}^* \\ \mathbb{F}_{p^n} & \text{sinon} \end{cases}$$

En particulier, lorsque $n = 2$, le $\mathbb{F}_p$-espace vectoriel $\ker(\mathrm{tr})$ est égal à l'espace propre de l'automorphisme de Frobenius σ associé à la valeur propre -1 et on a la décomposition en somme directe $\mathbb{F}_{p^2} = \mathbb{F}_p \oplus \ker(\mathrm{tr})$.

Définition 1.15. On note $F = \boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$ le sous-groupe de S_n.

Le groupe F est d'ordre $n(p^n - 1)$ engendré par ω une racine primitive $p^n - 1$-ème de l'unité et σ l'automorphisme de Frobenius.

1.3 Surjectivité du crochet de Lie

Dans cette section, on se place dans le cas $n = 2$, excepté pour le premier lemme. Nous allons voir que le crochet de Lie de $\mathrm{gr}\, S_2^1$ est essentiellement surjectif. Nous en déduirons des relations entre certains idéaux d'augmentations de différents sous-groupes de S_2^1.

Avant, donnons un résultat d'algèbre linéaire.

Lemme 1.16. *Considérons $\mathbb{F}_q$ avec $q = p^n$ où n est un entier naturel quelconque. Soient k un entier naturel et l'homomorphisme*

$$s : \mathbb{F}_q \otimes \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

qui envoie $a \otimes b$ sur $ab^{p^k} - ba^p$. Alors

Si $k + 1 \not\equiv 0 \bmod (n)$ alors l'homomorphisme s est surjectif.

Si $k + 1 \equiv 0 \bmod (n)$ alors l'image de s est le noyau de la trace $\mathrm{tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$.

Démonstration. L'image de l'application $\mathbb{F}_p$-linaire qui à un élément a de $\mathbb{F}_q$ associe $s(a \otimes 1) = a - a^p$ est égale au noyau de la trace. Ainsi, l'image de l'application linéaire s contient l'hyperplan $\ker(\mathrm{tr})$.

De plus, l'homomorphisme s est surjectif si et seulement s'il existe un élément $a \otimes b$ tel que son image par s ne soit pas dans l'hyperplan $\ker(\mathrm{tr})$, c'est-à-dire

$$\mathrm{tr}(s(a \otimes b)) = \mathrm{tr}(ab^{p^k}) - \mathrm{tr}(ba^p) = \mathrm{tr}(a^p(b^{p^{k+1}} - b))$$

Pour la dernière identité, on a utilisé le fait que $\operatorname{tr}(x^p) = \operatorname{tr}(x)$ pour tout $x \in \mathbb{F}_{p^n}$. Or, il existe un élément b tel que $b^{p^{k+1}} - b$ soit non nul, si et seulement si $k+1 \not\equiv 0 \bmod (n)$. Si un tel b existe, alors, comme l'application trace est non nulle, il existe $a \in \mathbb{F}_q$ tel que $s(a \otimes b) \neq 0$:

$$
\begin{tikzcd}
a \in \mathbb{F}_q \arrow[r, "a^p(b^{p^{k+1}}-b)", "\cong"'] \arrow[dr, "\operatorname{tr}(a^p(b^{p^{k+1}}-b))"'] & \mathbb{F}_q \arrow[d, "\operatorname{tr}", "\neq 0"'] \\
 & \mathbb{F}_q
\end{tikzcd}
$$

□

Proposition 1.17. *Soient $i, j \in \frac{1}{2}\mathbb{N}^*$, si i n'est pas entier alors, l'homomorphisme*

$$\operatorname{gr}_i S_2^1 \otimes \operatorname{gr}_j S_2^1 \longrightarrow \operatorname{gr}_{i+j} S_2^1$$

induit par le commutateur, est surjectif.

Remarque. Si $i, j \in \frac{1}{2}\mathbb{N}^*$ sont tous les deux entiers, alors le précédent homomorphisme induit par le commutateur est nulle.

Démonstration. Distinguons deux cas : i) Si j n'est pas entier, alors on s'intéresse à l'homomorphisme $\mathbb{F}_q \otimes \mathbb{F}_q \to \ker(\operatorname{tr})$ qui envoie $a \otimes b$ sur $ab^p - ba^p$ qui est surjectif d'après le lemme précédent.
ii) Si j est entier, alors on s'intéresse à l'homomorphisme $\mathbb{F}_q \otimes \ker(\operatorname{tr}) \to \mathbb{F}_q$ qui envoie $a \otimes b$ sur $a(b^p - b)$. Comme $\ker(\operatorname{tr})$ est distinct de $\mathbb{F}_p$, on déduit qu'il existe $b \in \ker(\operatorname{tr})$ tel que $b^p - b$ est non nul et donc que l'homomorphisme est surjectif. □

Faisons une petite parenthèse. Soit G un groupe profini, posons $C_1(G) = G$ et $C_{n+1}(G) = \overline{[G, C_n(G)]}$ la filtration centrale descendante associée. Alors de l'identité

$$1 - [x, y] = xy(\,(1 - y^{-1})(1 - x^{-1}) - (1 - x^{-1})(1 - y^{-1})\,)$$

on déduit par récurrence que

$$(IC_n(G)) \subset (IG)^{n+1}$$

quel que soit l'entier naturel n. Pour le groupe S_2^1, on a une relation analogue entre la filtration $F_i S_2^1$ et les puissances de l'idéal d'augmentation. Avant de donner la relation introduisons une notation.

Définition 1.18. Soit $i \in \mathbb{N}^*$, on note

$$(IF_{i/2} S_2^1) = \ker(\,\mathbb{Z}_p[\![F_{i/2} S_2^1]\!] \to \mathbb{Z}_p\,)$$

l'idéal d'augmentation de l'algèbre $\mathbb{Z}_p[\![F_{i/2} S_2^1]\!]$.

Le sous-groupe $F_{i/2} S_2^1$ est un sous-groupe ouvert d'indice fini du pro-p-groupe S_2^1 et l'inclusion induit un monomorphisme d'algèbres de $\mathbb{Z}_p[\![F_{i/2} S_2^1]\!]$ dans $\mathbb{Z}_p[\![S_2^1]\!]$. Nous identifierons $\mathbb{Z}_p[\![F_{i/2} S_2^1]\!]$ avec son image dans $\mathbb{Z}_p[\![S_2^1]\!]$. On note que cette dernière sous-algèbre est compact. En particulier, l'image de $(IF_{i/2} S_2^1)$ dans $\mathbb{Z}_p[\![S_2^1]\!]$ est aussi compacte. Ainsi, si $i \leq j$, le sous-$\mathbb{Z}_p[\![F_i S_2^1]\!]$-module à gauche

$$(IF_i S_2^1)(IF_j S_2^1) + (IF_j S_2^1)(IF_i S_2^1)$$

est fermé dans $\mathbb{Z}_p[\![S_2^1]\!]$.

Corollaire 1.19.

1. *Soient $i \geq 1$ et $x \in F_{\frac{i}{2}}S_2^1$, alors il existe deux suites $(x_n) \in F_{\frac{1}{2}}S_2^1$ et $(x'_n) \in F_{\frac{i-1}{2}}S_2^1$ telles que*
$$x = \prod_{n \geq 1} [x_n, x'_n]$$

2. *Soient $i \geq 1$ et x un élément de $F_{i/2}S_2^1$ alors $1 - x$ appartient à $(IS_2^1)^i$, i.e :*
$$\forall i \geq 1 : \ (IF_{i/2}S_2^1) \subset (IS_2^1)^i$$

3. *Soit $i \geq 1$, alors*
$$\overline{[F_{i/2}S_2^1, F_{i/2}S_2^1]} = \begin{cases} F_iS_2^1 & \textit{si } i \textit{ est impair} \\ F_{i+1/2}S_2^1 & \textit{sinon} \end{cases}$$

Démonstration. 1. D'après la proposition précédente, il existe $x_1 \in F_{\frac{1}{2}}S_2^1$ et $x'_1 \in F_{\frac{i-1}{2}}$ et $x''_1 \in F_{\frac{i+1}{2}}S_2^1$ tels que $x = x''_1 [x_1, x'_1]$. Par récurrence, on obtient
$$x = x''_l \prod_{k=1}^{l} [x_k, x'_k]$$
avec $x''_l \in F_{\frac{i+l}{2}}S_2^1$, $x_k \in F_{\frac{1}{2}}S_2^1$ et $x'_k \in F_{\frac{i+k-2}{2}}S_2^1$. Ainsi en faisant tendre l vers l'infini, on a x''_l qui tend vers 1.
2. Si $i = 1$, le résultat est immédiat ($F_{\frac{1}{2}}S_2^1 = S_2^1$). Supposons par récurrence avoir démontré la propriété pour un entier i quelconque. Donnons nous un élément x de $F_{\frac{i+1}{2}}S_2^1$ et les deux suites $(x_n) \in F_{\frac{1}{2}}S_2^1$ et $(x'_n) \in F_{\frac{i-1}{2}}S_2^1$ données par le point précédent. Alors par hypothèse de récurrence, on a
$$1 - [x_i, x'_i] = x_i x'_i((1 - x_i'^{-1})(1 - x_i^{-1}) - (1 - x_i^{-1})(1 - x_i'^{-1})) \equiv 0 \mod (IS_2^1)^{i+1}$$
et en utilisant l'identité $1 - xy = (1 - x)y + 1 - y$, on obtient par passage à la limite dans le sous-groupe fermé $(IS_2^1)^i$ que $1 - x$ appartient bien à $(IS_2^1)^i$.
3. C'est une conséquence immédiate de l'étude de l'application bilinéaire induite par le commutateur dans le gradué du pro-p-groupe S_2^1. ☐

En particulier :

Corollaire 1.20. *L'abélianisé de S_2^1 est égal au quotient $S_2^1/_{F_1S_2^1}$. L'abélianisé de $F_1S_2^1$ est égal au quotient $F_1S_2^1/_{F_{5/2}S_2^1}$.*

Donnons encore une conséquence de la proposition précédente.

Corollaire 1.21. *Soient $i, j \in \frac{1}{2}\mathbb{N}^*$. Si i n'est pas entier, alors*
$$(IF_{i+j}S_2^1) \subseteq (IF_iS_2^1)(IF_jS_2^1) + (IF_jS_2^1)(IF_iS_2^1)$$

Remarque. Comme le commutateur dans le groupe S_2^1 respecte la filtration, on déduit que si $i > j$ alors $F_iS_2^1$ est distingué dans $F_jS_2^1$. Ainsi, le module $(IF_iS_2^1)(IF_jS_2^1) + (IF_jS_2^1)(IF_iS_2^1)$ est à la fois un $\mathbb{Z}_p[\![F_iS_2^1]\!]$-module et $\mathbb{Z}_p[\![F_jS_2^1]\!]$-module (à gauche et à droite).

Démonstration. Soit $x \in F_{i+j}S_2^1$, alors, d'après la proposition précédente, il existe $a_1 \in F_iS_2^1$, $b_1 \in F_jS_2^1$ et $c_1 \in F_{i+j+\frac{1}{2}}S_2^1$ tels que

$$\begin{aligned} x-1 &= c_1\,[a_1,b_1]-1 \\ &= \underbrace{c_1a_1b_1\Big((a_1^{-1}-1)(b_1^{-1}-1)-(b_1^{-1}-1)(a_1^{-1}-1)\Big)}_{(IF_iS_2^1)(IF_jS_2^1)+(IF_jS_2^1)(IF_iS_2^1)}+c_1-1 \end{aligned}$$

On continue en considérant c_1 au lieu de x et ainsi par récurrence, on construit des éléments $a_n \in F_iS_2^1$, $b_n \in F_{j+\frac{n-1}{2}}S_2^1$ et $c_n \in F_{i+j+\frac{n}{2}}S_2^1$ tels que

$$x-1=\sum_{k=1}^{n} c_ka_kb_k\Big((a_k^{-1}-1)(b_k^{-1}-1)-(b_k^{-1}-1)(a_k^{-1}-1)\Big) \quad + \quad c_n-1$$

Par passage à la limite, on déduit que $x-1$ appartient à $(IF_iS_2^1)(IF_jS_2^1)+(IF_jS_2^1)(IF_iS_2^1)$, sous-$\mathbb{Z}_p$-module fermé de (IS_2^1). □

1.4 Le module Λ_i

On pose $F=\boldsymbol{\mu}_{p^2-1}\rtimes \mathrm{Gal}(\mathbb{F}_{p^2},\mathbb{F}_p)$ sous-groupe de $\mathbb{G}_2$. On se donne ω une racine primitive de l'unité de $\mathbb{W}^\times \subset \mathbb{S}_2$ et σ l'automorphisme de Frobenius, alors F est engendré par ω et σ.

Définition 1.22. Posons[3] Λ_i le groupe $\mathbb{W}$ muni de la structure de $\mathbb{Z}_p[F]$-module suivante :

$$\forall x \in \Lambda_i : w_*x = w^i x \quad \text{et} \quad \sigma_* x = x^\sigma$$

Commençons par donner un lien entre le module Λ_i et l'anneau de Lubin-Tate ainsi que le groupe stabilisateur de Morava.

Proposition 1.23.

1. *Le module Λ_i est isomorphe au sous-$\mathbb{Z}_p[F]$-module de $(E_2)_*$ engendré par u^i.*
2. *On a des isomorphismes canoniques de $\mathbb{Z}_p[F]$-modules*

$$(IS_2^1)/(IS_2^1)^2 \longrightarrow S_2^1/\overline{[S_2^1,S_2^1]} \cong H_1(S_2^1,\mathbb{Z}_p) \longrightarrow \Lambda_{1-p}/(p)$$

Le premier envoie la classe $x-1$ sur x et le second envoie $x\equiv 1+\bar{x}S \bmod F_1S_2^1$ sur $\bar{x}$.

Démonstration.

1. C'est une conséquence immédiate de la proposition 1.4,
2. C'est un résultat donné dans la proposition 7 de [Hen07]. Rappelons brièvement une preuve. Le première isomorphisme est une application de la proposition A.11. Ensuite, d'après le corollaire 1.20,

$$H_1(S_2^1,\mathbb{Z}_p)\cong S_2^1/\overline{[S_2^1,S_2^1]} = S_2^1/F_1S_2^1 = \mathrm{gr}_{1/2}\,S_2^1 \cong \mathbb{F}_{p^2}$$

où le dernière isomorphisme envoie $x\equiv 1+\bar{x}S \bmod F_1S_2^1$ sur $\bar{x}$. De plus, soit $x\equiv 1+\bar{x}S$ modulo $F_1S_2^1$, alors

$$\begin{aligned} \omega_*x &= \omega\,x\,\omega^{-1}\equiv 1+\omega^{1-p}\bar{x}S \equiv 1+\omega_*\bar{x}S \mod F_1S_2^1 \\ \sigma_*x &= x^\sigma \equiv 1+\bar{x}^\sigma S \mod F_1S_2^1 \end{aligned}$$

Ce qui montre que le second isomorphisme est $\mathbb{Z}_p[F]$-linéaire.

3. Dans [Hen07], le $\mathbb{Z}_p[F]$-module Λ_i est noté λ_i. J'ai effectué ce changement pour éviter le conflit de notation avec les coefficients λ_i de l'exponentielle de la déformation universelle G_2. De plus, avec ce choix, les modules et groupes sont notés en majuscule et les éléments en minuscule.

$\square$

Lemme 1.24. *[Hen07, Annexe A.2]*

a) Si $i \not\equiv 0\ [p{+}1]$, Λ_i est un module cyclique indécomposable et si $i \equiv 0\ [p{+}1]$, $\Lambda_i \cong \Lambda_{i,-} \oplus \Lambda_{i,+}$, où $\Lambda_{i,\pm}$ est le sous-espace propre associé à la valeur propre ± 1 de l'automorphisme de Frobenius.

b) [Hen07, Annexe A.1] On a un isomorphisme de $\mathbb{Z}_p[F]$-modules :

$$\mathbb{Z}_p[F] \cong \bigoplus_{i \not\equiv 0\,[p+1]} \Lambda_i \ \oplus \bigoplus_{i \equiv 0\,[p+1]} (\Lambda_{i,+} \oplus \Lambda_{i,-})$$

Notons que le module Λ_i est égal à $\Lambda_{p^2 i}$ via l'identité sur $\mathbb{W}$. Quel que soit i (qu'on peut donc regarder modulo (p^2-1)) l'automorphisme de Frobenius induit un isomorphisme entre Λ_i et Λ_{pi}. Avant d'étudier le groupe $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i, \Lambda_j)$, nous allons introduire la transformation naturelle tr_F. En fait, comme l'ordre de F est premier à p, on peut construire des homomorphismes $\mathbb{Z}_p[F]$-linéaires à partir d'homomorphisme en prenant la moyenne sous l'action de F.

Définition 1.25. Pour tous M, N des $\mathbb{Z}_p[F]$-modules, on définit l'homomorphisme naturel suivant

$$\mathrm{tr}_F :\ \mathrm{Hom}(M,N) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[F]}(M,N)$$

comme suit :

$$\mathrm{tr}_F(\phi)(x) = \frac{1}{|F|} \sum_{g \in F} g_*^{-1} \phi(g_* x)$$

Notons, qu'en tant que pro-p-groupe, Λ_{1-p} est isomorphe à l'anneau $\mathbb{W}$. Posons

$$\epsilon_\pm := \omega \pm \omega^p \tag{1.7}$$

En fait, $\epsilon_\pm$ est un vecteur propre de l'automorphisme de Frobenius de $\mathbb{W}$, noté *Frob*, pour la valeur propre ± 1. On vérifie facilement que le couple (ϵ_+, ϵ_-) détermine une $\mathbb{Z}_p$-base de Λ_{1-p}.

Définition 1.26. On note (λ, μ) la base duale de (ϵ_+, ϵ_-) de $\mathbb{W}$.

En fait,

$$\lambda,\ \mu :\ \mathbb{W} \to \mathbb{Z}_p$$

sont deux formes linéaires telles que

$$\forall\, x \in \mathbb{W} :\ x = \lambda(x)\epsilon_+ + \mu(x)\epsilon_-$$

Il est immédiat que pour tout $x \in \mathbb{W}$,

$$\lambda(x) = \frac{x + x^\sigma}{2\epsilon_+} \quad \text{et} \quad \mu(x) = \frac{x - x^\sigma}{2\epsilon_-} \tag{1.8}$$

Lemme 1.27. *Le groupe $\mathrm{End}_{\mathbb{Z}_p}(\mathbb{W})$ est un $\mathbb{W}$-module libre de base (λ, μ).*

Démonstration. Soit ϕ un endomorphisme de $\mathbb{W}$, alors

$$\phi = \frac{\phi(\epsilon_+)}{2\epsilon_+}(\mathrm{Id} + \mathit{Frob}\,) + \frac{\phi(\epsilon_-)}{2\epsilon_-}(\mathrm{Id} - \mathit{Frob}\,) = \phi(\epsilon_+)\ \lambda + \phi(\epsilon_-)\ \mu$$

$\square$

Proposition 1.28. *Soient i, j deux entiers relatifs. Posons $\lambda_+ = \lambda$ et $\lambda_- = \mu$. L'homomorphisme*

$$\mathrm{tr}_F : \mathrm{Hom}(\Lambda_i, \Lambda_j) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i, \Lambda_j)$$

vérifie les relations suivantes :

$$\mathrm{tr}_F(\lambda_s \epsilon_s) \quad = \quad \begin{cases} \frac{1}{2}\ \mathrm{Id} & \text{si } i \equiv j\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \frac{s}{2}\ \mathit{Frob} & \text{si } j \equiv pi\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \epsilon_r \mapsto \frac{1+rs}{2}\epsilon_r & \text{si } i \equiv j\ [p^2-1] \text{ et } i \equiv 0\ [p+1] \\ 0 & \text{si } j \not\equiv i, pi\ [p^2-1] \end{cases}$$

pour tout $s = \pm 1$. De plus, quels que soient $s = \pm 1$ et $t = \pm 1$, si $s \neq t$ alors $\mathrm{tr}_F(\lambda_s \epsilon_t) = 0$.

Démonstration. Rappelons que les éléments ω et σ engendrent le groupe F. Soient $r, s, t = \pm 1$, dans un premier temps, notons que

$$\lambda_t(\omega^{ik}\,\epsilon_r) \quad = \quad \frac{(\omega^{ik} + rt\omega^{pik})\epsilon_r}{2\epsilon_t}$$

D'où,

$$\begin{aligned} \mathrm{tr}_F(\lambda_t\epsilon_s)(\epsilon_r) \quad &= \quad \frac{1}{|F|}\sum_{k=0}^{p^2-2} \omega^{-jk}\lambda_t(\omega^{ik}\epsilon_r)\epsilon_s + rs\omega^{-pjk}\lambda_t(\omega^{ik}\epsilon_r)\epsilon_s \\ &= \quad \frac{\epsilon_r\epsilon_s}{4(p^2-1)\epsilon_t}\sum_{k=0}^{p^2-2} \omega^{(-j+i)k} + rt\,\omega^{(-j+pi)k} + rs\,\omega^{(-pj+i)k} + r^2st\,\omega^{(-j+i)pk} \end{aligned}$$

De plus l'ordre p^2-1 de ω est premier à p, ainsi on a

$$\begin{aligned} \sum_{k=0}^{p^2-2} \omega^{(-j+i)pk} \quad &= \quad \sum_{k=0}^{p^2-2} \omega^{(-j+i)k} \\ \sum_{k=0}^{p^2-2} \omega^{(-pj+i)k} \quad &= \quad \sum_{k=0}^{p^2-2} \omega^{(-p^2j+pi)k} \quad = \quad \sum_{k=0}^{p^2-2} \omega^{(-j+pi)k} \end{aligned}$$

Donc

$$\mathrm{tr}_F(\lambda_t\epsilon_s)(\epsilon_r) \quad = \quad \frac{\epsilon_r\epsilon_s}{4(p^2-1)\epsilon_t}\sum_{k=0}^{p^2-2} (1+st)\omega^{(-j+i)k} + r(t+s)\,\omega^{(-j+pi)k}$$

Donc, si s est différent de t, la précédente somme est nulle. Supposons maintenant que $s = t$, alors

$$\mathrm{tr}_F(\lambda_s\epsilon_s)(\epsilon_r) \quad = \quad \frac{\epsilon_r}{2(p^2-1)}\sum_{k=0}^{p^2-2} \omega^{(-j+i)k} + sr\,\omega^{(-j+pi)k}$$

D'autre part, on a l'équivalence suivante :

$$\begin{cases} i \equiv j\ [p^2-1] \\ j \equiv pi\ [p^2-1] \end{cases} \iff \begin{cases} i \equiv j\ [p^2-1] \\ i \equiv 0\ [p+1] \end{cases} \iff \begin{cases} pi \equiv j\ [p^2-1] \\ i \equiv 0\ [p+1] \end{cases}$$

Ainsi,

$$\mathrm{tr}_F(\lambda_s\epsilon_s)(\epsilon_r) \quad = \quad \begin{cases} \frac{1}{2}\ \epsilon_r & \text{si } i \equiv j\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \frac{rs}{2}\epsilon_r & \text{si } j \equiv pi\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \frac{1+rs}{2}\epsilon_r & \text{si } i \equiv j\ [p^2-1] \text{ et } i \equiv 0\ [p+1] \\ 0 & \text{si } j \not\equiv i, pi\ [p^2-1] \end{cases}$$

Rappelons que si $i \equiv 0\ [p+1]$, alors $\Lambda_i = \Lambda_{i,+} \oplus \Lambda_{i,-}$. D'où, la proposition. □

Corollaire 1.29. *Soient i, j deux entiers relatifs,*

1.

$$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i, \Lambda_j) = \begin{cases} \{\, a\,\mathrm{Id}\,;\; a \in \mathbb{Z}_p \,\} & \text{si } j \equiv i\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \{\, a\,\mathit{Frob}\;;\; a \in \mathbb{Z}_p \,\} & \text{si } j \equiv pi\ [p^2-1] \text{ et } i \not\equiv 0\ [p+1] \\ \{\, a\,\mathrm{Id}_{\Lambda_{i,+}} \oplus b\,\mathrm{Id}_{\Lambda_{i,-}}\,;\; a, b \in \mathbb{Z}_p \,\} & \text{si } i \equiv j\ [p^2-1] \text{ et } i \equiv 0\ [p+1] \\ \{0\} & \text{sinon} \end{cases}$$

2. i) *Si $i \not\equiv 0\ [p+1]$, l'homomorphisme $\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi} \to \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i, \bigoplus_{j=0}^{p^2-2} \mathbb{W}u^j)$, qui envoie u^i (resp. u^{pi}) sur $\Lambda_i \xrightarrow{\mathrm{Id}} \Lambda_i \cong \mathbb{W}u^i$ (resp. $\Lambda_i \xrightarrow{Frob} \Lambda_{pi} \cong \mathbb{W}u^{pi}$), est un isomorphisme.*

   ii) *Si $i \equiv 0\ [p+1]$, l'homomorphisme $\mathbb{Z}_p u^i_+ \oplus \mathbb{Z}_p u^i_- \to \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i, \bigoplus_{j=0}^{p^2-2} \mathbb{W}u^j)$, qui envoie $u^i_\pm$ sur $\Lambda_i \twoheadrightarrow \Lambda_{i,\pm} \xrightarrow{\mathrm{Id}} \Lambda_{i,\pm} \to \Lambda_i \cong \mathbb{W}u^i$, est un isomorphisme.*

Démonstration. En utilisant le fait que l'homomorphisme tr_F est surjectif, on déduit immédiatement le premier point du corollaire. Le second point se déduit du premier et des isomorphismes $\Lambda_k \cong \mathbb{W}\, u^k$. □

Un second corollaire qui sera utile dans le chapitre 4 pour la seconde différentielle.

Corollaire 1.30. *Soient $\mathrm{tr}_F : \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_{1-p}, \Lambda_i) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, \Lambda_i)$ et $\phi : \Lambda_{1-p} \to \Lambda_i$ un homomorphisme, alors*

$$\mathrm{tr}_F(\phi) \quad = \quad \begin{cases} \frac{1}{2}\Big(\lambda(\phi(\epsilon_+)) + \mu(\phi(\epsilon_-))\Big)\ \mathrm{Id} & \text{si } \ i \equiv 1-p\ [p^2-1] \\ \frac{1}{2}\Big(\lambda(\phi(\epsilon_+)) - \mu(\phi(\epsilon_-))\Big)\ \mathit{Frob} & \text{si } \ i \equiv p-1\ [p^2-1] \\ 0 & \text{si } \ i \not\equiv \pm(1-p)\ [p^2-1] \end{cases}$$

Démonstration. L'homomorphisme ϕ est égal à

$$\lambda(\phi(\epsilon_+))\ \lambda\epsilon_+ + \mu(\phi(\epsilon_+))\ \lambda\epsilon_- + \lambda(\phi(\epsilon_-))\ \mu\epsilon_+ + \mu(\phi(\epsilon_-))\ \mu\epsilon_-$$

Ainsi, en utilisant les résultats de la preuve de la proposition, on déduit le corollaire. □

Comme suggérée dans l'annexe A.3 de [Hen07], on note que pour i premier a p, le groupe des homomorphismes $\mathbb{Z}_p[F]$-linéaires de Λ_i dans l'anneau gradué de Lubin-Tate est isomorphe à un sous-module de ce dernier. Dans le lemme suivant nous en donnons une description complète. Pour $i = 1-p$, elle nous sera utile dans le chapitre 4 sur la cohomologie à coefficients dans l'anneau de Lubin-Tate modulo (p).

Proposition 1.31.

1. *Le sous-$\mathbb{Z}_p$-module $(E_2)^F_*$ des invariants sous l'action de F de $(E_2)_*$ est la $\mathbb{Z}_p$-algèbre engendrée par $v_1 = u_1 u^{1-p}$ et $v_2 = u^{1-p^2}$, complet pour la filtration (u_1^{p+1})-adique. On note*

$$(E_2)^F_* \cong \mathbb{Z}_p[[u_1^{p+1}]][v_1, v_2^{\pm 1}] \;/\, (v_1^{p+1} v_2^{-1} - u_1^{p+1})$$

2. *On a l'isomorphisme de $\mathbb{Z}_p[F]$-modules suivant :*

$$(E_2)_* \cong\ (E_2)^F_* \otimes \bigoplus_{i=0}^{p^2-2} \ \mathbb{W}u^i$$

3. *Soit i un entier relatif, le groupe $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*)$ est naturellement muni d'une structure de $(E_2)_*^F$-module libre de rang 2. De plus,*
   i) *Si $i \not\equiv 0\ [p+1]$, l'évaluation en 1, induit un isomorphisme $(E_2)_*^F$-linéaire*
   $$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*) \xrightarrow[\cong]{\mathrm{ev}_1} (E_2)_*^F \otimes (\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi}) \ \subseteq\ (E_2)_*$$
   qui envoie $\mathrm{Id} : \Lambda_i \to \mathbb{W}u^i$ sur u^i et Frob $: \Lambda_i \to \mathbb{W}u^{pi}$ sur u^{pi}.
   ii) *Si $i \equiv 0\ [p+1]$, on a un isomorphisme $(E_2)_*^F$-linéaire*
   $$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*) \xrightarrow[\cong]{} (E_2)_*^F \otimes (\mathbb{Z}_p u_+^i \oplus \mathbb{Z}_p u_-^i) \ \subseteq\ (E_2)_*$$
   qui envoie $\Lambda_i \twoheadrightarrow \Lambda_{i,\pm} \overset{\mathrm{Id}}{\to} \Lambda_{i,\pm} \to \Lambda_i \cong \mathbb{W}u^i$ sur $u_\pm^i$.

Remarque 1.32. *Rappelons que $|v_1| = 2(p-1)$, $|v_2| = 2(p^2-1)$ et $|u_1^{p+1}| = 0$. Dans la catégorie des $\mathbb{Z}_p$-modules gradués, on a*
$$(E_2)_*^F = \prod_{s\in\mathbb{Z}} \mathbb{Z}_p[v_1]\,\{v_2^s\}$$
C'est une présentation plus simple que celle donnée dans la lemme. Elle est aussi utilisée dans [HKM08] pour traiter le cas $p = 3$ (par exemple le corollaire 5.8).

Démonstration.

1. Dans le lemme 1.4, on a vu que si $X = \sum a_{n,m} u_1^n u^m$ alors $\omega_* X = \sum \omega^{(p-1)n+m} a_{n,m} u_1^n u^m$ et une identité analogue pour $\sigma_* X$. Ainsi il suffit d'étudier les monômes de $(E_2)_*$. Soit $X = a u_1^n\, u^m$ un élément de $(E_2)_*^F$. De l'invariance sous l'action de σ on déduit immédiatement que a vie dans $\mathbb{Z}_p$. L'invariance sous l'action de ω équivaut à avoir l'identité $\omega^{n(p-1)+m} = 1$, c'est-à-dire, il existe un entier relatif k tel que $n(p-1) + m = k(1-p^2)$. Donc
   $$X = a\, u_1^n\, u^{(1-p)n+(1-p^2)k} = a v_1^n v_2^k$$
   D'autre part, $(E_2)_*$ est complet pour la filtration (u_1)-adique et $u_1^{p+1} = v_1^{p+1} v_2^{-1}$, d'où on déduit que $(E_2)_*^F$ est topologiquement engendré par v_1 et v_2.
2. C'est une conséquence de 1., en remarquant que $u_1^i u^j = (u_1 u^{1-p})^i u^{(p-1)i+j}$.
3. Soit i un entier relatif. D'après le point précédent et le second point du corollaire 1.29, on déduit que
   $$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*) &\cong (E_2)_*^F \otimes \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\, \bigoplus_{j=0}^{p^2-2} \mathbb{W}u^j) \\ &\cong \begin{cases} (E_2)_*^F \otimes \big(\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi}\big) & \text{si } i \not\equiv 0\ [p+1] \\ (E_2)_*^F \otimes \big(\mathbb{Z}_p u_+^i \oplus \mathbb{Z}_p u_-^i\big) & \text{sinon}\end{cases}\end{aligned}$$
   D'où l'on déduit que $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*)$ est libre de rang deux et le point 3.*ii*).
   Supposons maintenant que $i \not\equiv 0\ [p+1]$. Soit ϕ un homomorphisme de $\mathbb{Z}_p[F]$-modules de Λ_i dans $(E_2)_*$. Alors de la décomposition de $(E_2)_*$ et du corollaire 1.29, on déduit que $\phi(1)$ appartient à $(E_2)_*^F \otimes (\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi})$. Donc l'homomorphisme d'évaluation
   $$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_i,\,(E_2)_*) \xrightarrow{\mathrm{ev}_1} (E_2)_*^F \otimes (\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi})$$
   qui envoie ϕ sur $\phi(1)$ est bien défini.
   D'autre part, l'homomorphisme, qui envoie $P \otimes \lambda u^i + Q \otimes \mu u^{pi} \in (E_2)_*^F \otimes (\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi})$, sur l'homomorphisme $\phi \in \mathrm{Hom}_F(\Lambda_i, (E_2)_*)$, $\phi(x) = P\lambda x u^i + Q\mu x^\sigma u^{pi}$, est bien défini et induit un inverse de ev_1.

□

Corollaire 1.33.

1. *Un élément $u_1^n u^m$ de $(E_2)_*$ appartient à $(E_2)_*^F$ si et seulement si p^2-1 divise $n(p-1)+m$.
2. *Un élément $u_1^n u^m$ de $(E_2)_*$ appartient à $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$ si et seulement si p^2-1 divise $(\pm 1+n)(p-1)+m$.*

Démonstration.
1. C'est une conséquence immédiate de la preuve de 1. de la proposition.
2. Soit $u_1^n u^m$ un élément de $(E_2)_*^F \otimes (\mathbb{Z}_p u^i \oplus \mathbb{Z}_p u^{pi})$, alors il existe $\epsilon = \pm 1$, $k \in \mathbb{Z}$ tels que $u_1^n u^m = v_1^n \, v_2^k \, u^{\epsilon(1-p)}$. En identifiant les exposants de u, on a

$$m = n(p-1) + (1-p^2)k + \epsilon(1-p)$$

D'où le second point. □

Précisons encore la forme des éléments homogènes de $(E_2)_*^F = \mathrm{Hom}_{\mathbb{Z}_p[F]}(\mathbb{Z}_p, (E_2)_*)$ et de $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, (E_2)_*)$.

Corollaire 1.34.

1. *Soit X un élément de $(E_2)_*^F$ homogène, alors son degré est égal à $-2(1-p)k$ pour un certain entier k. De plus, si $k = m(p+1)+n$ avec $0 \leq n \leq p$, alors il existe (a_i) une suite d'entiers p-adiques telle*
$$X = \sum_{i \geq 0} a_i \, u_1^{(p+1)i} \, v_1^n \, v_2^m$$
2. *Soit X un élément de $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$ homogène, alors son degré est égal à $-2k(1-p)$ pour un certain entier k. De plus, si $k = m(p+1)+n$ avec $0 \leq n \leq p$, alors il existe $(a_i), (b_i)$ deux suites d'entiers p-adiques telles que*
$$X \;=\; \sum_{i \geq 0} a_i \, u_1^{(p+1)i} \, v_1^{n-1} \, v_2^m \, u^{1-p} \;+\; b_i \, u_1^{(p+1)i} \, v_1^{n+1} \, v_2^m \, u^{p-1}$$
où $a_0 = 0$ si $n = 0$.

Avant de passer à la preuve, remarquons qu'on a

$$u_1^{p+1} = v_1^{p+1} \, v_2^{-1}, \quad u_1^2 \, u^{1-p} = v_1^2 \, u^{p-1} \quad \text{et} \quad u_1^{p-1} \, u^{p-1} = v_1^{p-1} \, u^{1-p} v_2^{-1}$$

Démonstration.

1. D'après $a)$ de la proposition précédente, $u_1^n u^k$ appartient à $(E_2)_*^F$ si et seulement si $n(p-1)+k \equiv 0 \; [p^2-1]$. C'est-à-dire s'il existe m tel que $k = (m(p+1)+n)(1-p)$.
2. D'après $c)$ de la proposition précédente, $u_1^n u^k$ appartient à $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$ si et seulement si $(\pm 1+n)(p-1)+k \equiv 0 \; [p^2-1]$. C'est-à-dire s'il existe m tel que $k = (m(p+1)+(\pm 1+n))(1-p)$.

□

La description donnée dans le corollaire précédent, nous sera d'une particulière utilitée dans les chapitres 4 et 5 pour les calculs cohomologiques.

Chapitre 2

Résolution projective : n=2 et $p \geq 5$

Pour le calcul de $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ dans le chapitre 4, nous allons utiliser une approximation d'une résolution projective minimale dont l'existence est donnée par le théorème suivant.

Définition 2.1. Étant donné un $\mathbb{Z}_p[F]$-module M, on note $M\uparrow_F^{\mathbb{G}_2^1} = \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \underset{\mathbb{Z}_p[F]}{\otimes} M$ le $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module à gauche obtenu par extension des scalaires.

Théorème 2.2 ([Hen07], théorème 6)**.** *Il existe une résolution projective finie du $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module triviale $\mathbb{Z}_p$ de la forme :*

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$$

où $C_0 = C_3 = \mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}$ et $C_1 = C_2 = \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$.

Dans ce chapitre, nous allons préciser autant que nécessaire des homomorphismes ∂_i définissant une telle résolution projective.

La démarche empruntée est proche de celle utilisée dans [HKM08] la section 3 pour traiter le cas $p = 3$. La construction de ∂_i pour $i = 1, 2$ s'est fait de la manière suivante : on a cherché des générateurs de $N_i = \ker(\partial_i)$ vu comme $\mathbb{Z}_p[\![S_2^1]\!]$-module. Ce qui, d'après le lemme de Nakayama (lemme 4.5 [GHMR05] ou corollaire A.9), équivaut à chercher des éléments de N_i qui engendrent le pro-p-groupe $H_0(S_2^1, N_i)$. Pour l'homomorphisme ∂_2, on a du se contenter d'approximations de ces générateurs. Ensuite, on a défini un homomorphisme de Λ_{1-p} vers N_i rendu $\mathbb{Z}_p[F]$-linéaire après avoir pris la moyenne sous l'action de F. Par le lemme de Shapiro, on peut étendre ce dernier homomorphisme à C_i. Le troisième homomorphisme ∂_3 a été obtenue d'une manière différente via une notion de dualité ($D_G(M) = \mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M, \mathbb{Z}_p[\![G]\!])$) introduite dans [HKM08].

Avant de pouvoir donner le résultat principal (théorème 2.10) de ce chapitre, nous avons besoin d'introduire quelques notations.

Définition 2.3. On pose

$$\partial_0 = \mathrm{Id}\uparrow_F^{\mathbb{G}_2^1} : C_0 \longrightarrow \mathbb{Z}_p$$

et $N_0 = \ker \partial_0$.

Comme $\mathbb{G}_2^1$ est isomorphe au produit semi-direct $S_2^1 \rtimes F$, le module C_0 est libre de rang 1 en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module. Ainsi, N_0 s'identifie avec l'idéal d'augmentation de ce dernier. Rappelons que l'on se donne ω un générateur du sous-groupe $\boldsymbol{\mu}_{p2-1}$ des racines $p^2 - 1$-ème de l'unité de $\mathbb{W}$ et qu'on note $\epsilon_\pm$ les éléments $\omega \pm \omega^p$ de $\mathbb{W}$. D'après le corollaire A.16, en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module, $\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$ est libre de rang de 2 et $(1 \otimes \epsilon_+, 1 \otimes \epsilon_-)$ en est une base.

Définition 2.4.

a) On note $((e_i)_+, (e_i)_-)$ la base $(1 \otimes \epsilon_+, 1 \otimes \epsilon_-)$ du $\mathbb{Z}_p[\![S_2^1]\!]$-module C_i pour $i = 1, 2$.

b) Pour $i = 0, 1, 2, 3$, on pose $e_i = 1 \otimes 1$ vu comme élément de C_i. Lorsque $i = 0, 3$, e_i détermine une base de C_i en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module.

Dans le premier chapitre, nous avons vu (lemme 1.13) que le déterminant réduit induit une suite exacte courte scindée

$$1 \longrightarrow S_2^1 \longrightarrow S_2 \xrightarrow{N} 1 + p\mathbb{Z}_p \longrightarrow 1$$

Une section $s : 1 + p\mathbb{Z}_p \to S_2$ de la suite exacte courte précédente induit un isomorphisme $S_2 \cong S_2^1 \times 1 + p\mathbb{Z}_p$ et une projection $\pi : S_2 \to S_2^1$ définie par $\pi(x) = xs(N(x))^{-1}$ pour tout $x \in S_2$.
Comme $p = S^2$ dans $\mathcal{O}_2$, on déduit que pour tout $g \equiv 1 + g_1 S \mod (S^2)$ dans S_2, on a

$$\pi(g) \equiv 1 + g_1 S \mod (S^2)$$

Définition 2.5. Soit $s : 1 + p\mathbb{Z}_p \to S_2$ une section du déterminant réduit et $\pi : S_2 \to S_2^1$ la projection définie par $\pi(x) = xs(N(x))^{-1}$ pour tout $x \in S_2$.

1. On pose

$$\begin{array}{rcl} a_0 & := & \pi(\ 1 + \epsilon_+ S\ ) \\ b_0 & := & \pi(\ 1 + \epsilon_- S\ ) \end{array}$$

   et $c_0 = [a_0, b_0]$.
2. Pour tout entier i, on pose

$$\begin{array}{rcl} a_i & := & \omega^{-i} a_0 \omega^i \ = \ \pi(\ 1 + \omega^{(p-1)i}\epsilon_+ S\ ) \\ b_i & := & \omega^{-i} b_0 \omega^i \ = \ \pi(\ 1 + \omega^{(p-1)i}\epsilon_- S\ ) \end{array}$$

Finalement, a_i et b_i sont déterminés par $1+\omega^{(p-1)i}\epsilon_\pm S$ à un élément du centre $Z(S_2) = 1+p\mathbb{Z}_p$ près. D'après la proposition 1.4, l'action de $1 + p\mathbb{Z}_p$ sur $(E_2)_*/(p)$ est triviale. Ainsi, pour nos applications dans les chapitres suivants, nous n'avons pas besoin de déterminer plus précisément les éléments a_i et b_i pour pouvoir considérer leurs actions modulo (p).

Au passage, notons que pour tous $\lambda, \mu \in 1 + p\mathbb{Z}_p$ et tous $g, f \in S_2$, on a $[g\lambda, f\mu] = [g, f]$. En particulier,

$$c_0 = [a_0, b_0] = [1 + \epsilon_+ S, 1 + \epsilon_- S]$$

Remarque 2.6. *Si on définit (définition III,I.I.6.1 de [Laz65] ou à l'aide du théorème A.3) pour tout nombre p-adique x, multiple de p, l'inverse de la racine carrée*

$$(1+x)^{-1/2} := \sum_{n\in\mathbb{N}} \binom{-1/2}{n} x^n \equiv 1 - 1/2\,x + 3/8\,x^2 + \dots$$

Alors, pour tout x dans $\mathbb{W}(\mathbb{F}_{p^2})$,

$$\det((1 - x^{\sigma+1}p)^{-1/2}(1 + xS)) \quad = \quad (1 - x^{\sigma+1}p)^{-1} \begin{vmatrix} 1 & x^\sigma p \\ x & 1 \end{vmatrix} = 1$$

D'où, on définit l'application $a : \mathbb{W} \longrightarrow S_2^1$:

$$a(x) = (1 - x^{\sigma+1}p)^{-1/2}(1 + xS)$$

et alors, on pourrait définir les éléments a_0 et b_0 ainsi

$$\begin{array}{rcl} a_0 & = & a(\omega + \omega^p) \equiv 1 + \epsilon_+ S + \dfrac{\epsilon_+^2}{2} S^2 \mod (S^3) \\ b_0 & = & a(\omega - \omega^p) \equiv 1 + \epsilon_- S - \dfrac{\epsilon_-^2}{2} S^2 \mod (S^3) \end{array}$$

Lemme 2.7.

1. *Pour tout entier* i*,*
   $a_i \equiv 1 + \omega^{(p-1)i}\epsilon_+ S \mod (S^2)$,
   $b_i \equiv 1 + \omega^{(p-1)i}\epsilon_- S \mod (S^2)$,

2. $c_0 \equiv 1 - 2\epsilon_+\epsilon_- S^2 + 2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+ S^3 \mod (S^4)$

3. *Pour tout entier* $i > 0$*,*
   $\mathrm{gr}_{(2i-1)/2}\, S_2^1 \;\cong\; \mathbb{Z}/(p)\, a_0^{p^{i-1}} \;\oplus\; \mathbb{Z}/(p)\, b_0^{p^{i-1}}$,

   $\mathrm{gr}_{(2i)/2}\, S_2^1 \;\cong\; \mathbb{Z}/(p)\, c_0^{p^{i-1}}$.

Démonstration.

1. C'est une simple conséquence du fait que $p = S^2$ dans $\mathcal{O}_2$ et que a_0 et b_0 sont égaux à $1 + \epsilon_\pm S$ à multiplication par un élément de $1 + p\mathbb{Z}_p$ près.
2. Il suffit d'appliquer le lemme 1.9, pour déterminer $[1 + \epsilon_+ S, 1 + \epsilon_- S] = c_0$.
3. Les éléments ϵ_+ et ϵ_- modulo p déterminent une base de $\mathbb{F}_{p^2}$ et de plus $\epsilon_- \in \ker(\mathrm{tr}_F : \mathbb{F}_{p^2} \to \mathbb{F}_p)$. Ainsi, du lemme 1.14 et du lemme 1.8, on déduit le troisième point.

□

La figure 2.1 donne une illustration de $\mathrm{gr}_*\, S_2^1$ et des éléments a_0, b_0 et c_0.

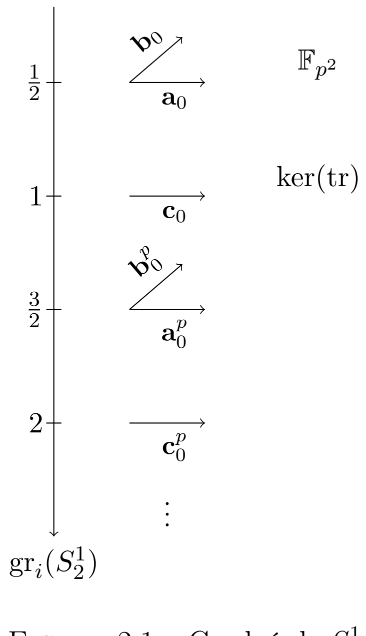

FIGURE 2.1 – Gradué de S_2^1

Définition 2.8.

1. Pour tout $g \in \mathbb{S}_2$, dans $\mathbb{Z}_p[\![\mathbb{S}_2]\!]$, on pose $\mathcal{N}(g) = e + g + \ldots + g^{p-1}$.
2. Avec les notations de la définition 1.26, pour tout entier i, on définit les entiers p-adiques $\lambda_i = \lambda(\omega^{(1-p)i}\epsilon_+)$ et $\mu_i = \mu(\omega^{(1-p)i}\epsilon_+)$.

3. Dans $\mathbb{Z}_p[\![\mathbb{S}_2]\!]$, on définit

$$\begin{aligned} v &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_+)(a_i-e)+\mu(\omega^{(1-p)i}\epsilon_+)(b_i-e) \\ \Lambda &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_+)(a_i^{-1}-e)+\mu(\omega^{(1-p)i}\epsilon_+)(b_i^{-1}-e) \\ w &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_-)(a_i-e)+\mu(\omega^{(1-p)i}\epsilon_-)(b_i-e) \end{aligned}$$

Définition 2.9. Avec les notations de la définition 1.18, on pose $I=(IS_2^1)$ et J l'idéal $(IF_1S_2^1)$ vu comme sous-groupe de $\mathbb{Z}_p[\![S_2^1]\!]$.

Rappelons que pour tous M,N des $\mathbb{Z}_p[F]$-modules, on définit l'homomorphisme naturel suivant :

$$\mathrm{tr}_F:\ \mathrm{Hom}(M,N)\longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[F]}(M,N)$$

comme suit :

$$\mathrm{tr}_F(\phi)(x)=\frac{1}{|F|}\sum_{g\in F}g^{-1}\phi(gx)$$

Maintenant, avec toutes ces notations, nous pouvons donner le théorème suivant qui résume les résultats obtenus dans ce chapitre.

Théorème 2.10. *Il existe une résolution projective de $\mathbb{Z}_p$ au-dessus de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$ de la forme suivante*

$$0\longrightarrow \mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}\xrightarrow{\partial_3}\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}\xrightarrow{\partial_2}\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}\xrightarrow{\partial_1}\mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}\xrightarrow{\mathrm{Id}\uparrow_F^{\mathbb{G}_2^1}}\mathbb{Z}_p\longrightarrow 0 \qquad (\star)$$

telle que

1. L'homomorphisme ∂_1 est déterminé par la condition

$$\partial_1(e_1)_+=v\,e_0=\frac{1}{p+1}\sum_{i=0}^{p}\lambda_i(a_i-e)e_0+\mu_i(b_i-e)e_0$$

De plus, $\partial_1(e_1)_-=w\,e_0$.

2. L'homomorphisme ∂_2 est égal à $\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}\circ\alpha$, où $d_2:\Lambda_{1-p}\to C_1$ est un homomorphisme $\mathbb{Z}_p$-linéaire qui se factorise par N_1 tel que

i) $d_2(\epsilon_+)\equiv\mathcal{N}(a_0)(e_1)_+\ +\ \frac{1}{4\epsilon_-^2}(b_0-e)(w(e_1)_+-v(e_1)_-)+\frac{1}{4\epsilon_-^2}(c_0-e)(e_1)_-$ $+\frac{p}{2}(w(e_1)_+-v(e_1)_-)$ modulo $(IJ+JI)C_1$.

ii) $d_2(\epsilon_-)\equiv\mathcal{N}(b_0)(e_1)_-\ +\ \frac{1}{4\epsilon_+^2}(a_0-e)(w(e_1)_+-v(e_1)_-)+\frac{1}{4\epsilon_+^2}(c_0-e)(e_1)_+$ $-\frac{p}{2}(w(e_1)_+-v(e_1)_-)$ modulo $(IJ+JI)C_1$.

et $\alpha:C_2\to C_2$ est un automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire tel que

$\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p,\alpha)=\mathrm{Id}_{\Lambda_{1-p}}$.

3. L'homomorphisme $\partial_3:C_3\to C_2$ est déterminé par la condition $\partial_3(e_3)=\frac{1}{2\epsilon_+^2}\Lambda(e_2)_++\frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega-\omega\Lambda\omega^{-1})(e_2)_-$.

Démonstration. Pour la construction de ∂_1 voir la proposition 2.14, celle de ∂_2 est traitée dans le théorème 2.44. Enfin pour α et ∂_3 voir le corollaire 2.52 et la proposition 2.54 □

Avant de passer à la construction des trois homomorphismes dans les trois sections suivantes, donnons certains groupes de cohomologie des groupes S_2^1 et $F_1S_2^1$.

Proposition 2.11. *Les premiers groupes d'homologie de S_2^1 et $F_1S_2^1$ sont :*

$H_*(G,M)$	$\mathbb{F}_p$				$\mathbb{Z}_p$			
	0	1	2	3	0	1	2	3
S_2^1	$\mathbb{F}_p$	$\bar{\Lambda}_{1-p}$	$\bar{\Lambda}_{1-p}$	$\mathbb{F}_p$	$\mathbb{Z}_p$	$\bar{\Lambda}_{1-p}$	0	$\mathbb{Z}_p$
$F_1S_2^1$	$\mathbb{F}_p$	$\mathbb{F}_p^3$	$\mathbb{F}_p^3$	$\mathbb{F}_p$	$\mathbb{Z}_p$	$\mathbb{Z}/p^2 \oplus (\mathbb{Z}/p)^2$	0	$\mathbb{Z}_p$

où $\bar{\Lambda}_{1-p} = \Lambda_{1-p}/(p)$.
De plus, les groupes d'homologie sont tous triviaux en degré supérieur ou égal à 4.

Démonstration. Pour $H_*(S_2^1, \mathbb{F}_p)$ et $H_*(F_1S_2^1, \mathbb{F}_p)$ voir dans [Hen07] la proposition 7 et sa preuve. Passons à l'homologie intégrale. Le premier groupe d'homologie de S_2^1 a été déterminé dans la proposition 1.23. Rappelons que si G est un pro-p-groupe alors, $H_1(G, \mathbb{Z}_p)$ est isomorphe à $G/\overline{[G,G]}$. Donc d'après le corollaire 1.20, on déduit que

$$H_1(F_1S_2^1, \mathbb{Z}_p) \cong F_1S_2^1/F_{5/2}S_2^1 \cong \mathbb{Z}/p^2 \oplus (\mathbb{Z}/p)^2$$

Considérons la suite exacte longue, associée à $\mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \to \mathbb{F}_p$:

$$0 \to H_3(S_2^1, \mathbb{Z}_p) \xrightarrow{p} H_3(S_2^1, \mathbb{Z}_p) \xrightarrow{\partial} \mathbb{F}_p \to H_2(S_2^1, \mathbb{Z}_p) \overset{p}{\twoheadrightarrow} H_2(S_2^1, \mathbb{Z}_p) \to \mathbb{F}_p^2 \underset{\cong}{\xrightarrow{\partial}} \bar{\Lambda}_{1-p} \underset{0}{\xrightarrow{p}} \bar{\Lambda}_{1-p}$$

Ainsi, d'après le corollaire A.7, avec comme anneau de base $\mathbb{Z}_p$, on déduit qu'en tout degré, le pro-p-groupe $H_*(S_2^1, \mathbb{Z}_p)$ est un $\mathbb{Z}_p$-modules de type fini. Ainsi, d'après le lemme de Nakayama (théorème A.6), $p\,H_2(S_2^1, \mathbb{Z}_p) = H_2(S_2^1, \mathbb{Z}_p)$ entraine que $H_2(S_2^1, \mathbb{Z}_p)$ est trivial. En revenant à la suite exacte longue, on déduit que $\mathbb{F}_p \otimes H_3(S_2^1, \mathbb{Z}_p) \cong \mathbb{F}_p$ et que la multiplication par p induit une injection sur le module $H_3(S_2^1, \mathbb{Z}_p)$. Donc d'après le corollaire A.9 du lemme de Nakayama, $H_3(S_2^1, \mathbb{Z}_p)$ est un pro-p-groupe cyclique dont la multiplication par p est injectif. C'est-à-dire $H_3(S_2^1, \mathbb{Z}_p) \cong \mathbb{Z}_p$.
Passons maintenant aux premiers groupes d'homologie $H_*(F_1S_2^1, \mathbb{Z}_p)$. De même qu'avant, on a

$$\begin{array}{l} 0 \longrightarrow H_3(F_1S_2^1, \mathbb{Z}_p) \xrightarrow{p} H_3(F_1S_2^1, \mathbb{Z}_p) \longrightarrow \mathbb{F}_p \xrightarrow{\partial} H_2(F_1S_2^1, \mathbb{Z}_p) \overset{p}{\twoheadrightarrow} \\ \longrightarrow H_2(F_1S_2^1, \mathbb{Z}_p) \longrightarrow \mathbb{F}_p^3 \underset{\cong}{\xrightarrow{\partial}} \mathbb{Z}/p^2 \oplus (\mathbb{Z}/p)^2 \xrightarrow{p} \mathbb{Z}/p^2 \oplus (\mathbb{Z}/p)^2 \longrightarrow \end{array}$$

On en déduit comme avant que les groupes d'homologies sont des $\mathbb{Z}_p$-modules de type fini. Donc $p\,H_2(F_1S_2^1, \mathbb{Z}_p) = H_2(F_1S_2^1, \mathbb{Z}_p)$ est trivial et de même que précédemment, $H_3(F_1S_2^1, \mathbb{Z}_p)$ est isomorphe à $\mathbb{Z}_p$.

Soit $G = S_2^1$ ou $F_1S_2^1$, alors comme pour $H_2(G, M)$, on déduit que $H_n(G, M) = 0$ pour tout $n \geq 4$. ☐

Par définition de N_0 est le noyau de l'homomorphisme $\epsilon : \mathbb{Z}_p \uparrow_F^{\mathbb{G}_2^1} \to \mathbb{Z}_p$ induit par l'identité. Comme $\mathbb{G}_2^1 \cong S_2^1 \rtimes F$, on a $\mathbb{Z}_p \uparrow_F^{\mathbb{G}_2^1} = \mathbb{Z}_p[\![S_2^1 \rtimes F]\!] \underset{\mathbb{Z}_p[F]}{\otimes} \mathbb{Z}_p \cong \mathbb{Z}_p[\![S_2^1]\!]$. D'où le diagramme de

$\mathbb{Z}_p[\![S_2^1]\!]$-modules

$$\begin{tikzcd} 0 \arrow[r] & N_0 \arrow[r] & C_0 \arrow[r, "\epsilon"] & \mathbb{Z}_p \arrow[r] & 0 \\ 0 \arrow[r] & (IS_2^1) \arrow[r] \arrow[u, "\cong"] & \mathbb{Z}_p[\![S_2^1]\!] \arrow[r, "\epsilon"] \arrow[u, "\cong"] & \mathbb{Z}_p \arrow[r] \arrow[u, "="] & 0 \end{tikzcd}$$

Dans la suite, on identifie N_0 avec l'idéal d'augmentation (IS_2^1) de $\mathbb{Z}_p[\![S_2^1]\!]$.

Corollaire 2.12. *La cohomologie des groupes S_2^1 et $F_1S_2^1$ à coefficients dans N_0 est donnée dans le tableau suivant :*

$H_\bullet(G, N_0)$	*0*	*1*	*2*	$\bullet \geq 3$
S_2^1	$\bar{\Lambda}_{1-p}$	0	$\mathbb{Z}_p$	0
$F_1S_2^1$	$H_1(F_1S_2^1, \mathbb{Z}_p) \oplus \mathbb{Z}_p^{p^2-1}$	0	$\mathbb{Z}_p$	0

Démonstration. La première ligne se déduit facilement de la suite exacte longue en homologie associée à la suite exacte courte : $N_0 \rightarrowtail \mathbb{Z}_p[\![S_2^1]\!] \twoheadrightarrow \mathbb{Z}_p$.
Pour la seconde, considérons de même la suite exacte longue en homologie :

$$0 \longrightarrow H_1(F_1S_2^1, \mathbb{Z}_p) \xrightarrow{\partial} H_0(F_1S_2^1, N_0) \longrightarrow H_0(F_1S_2^1, \mathbb{Z}_p[\![S_2^1]\!]) \longrightarrow H_0(F_1S_2^1, \mathbb{Z}_p) = \mathbb{Z}_p \longrightarrow 0$$

Posons $H = S_2^1/_{F_1S_2^1} \cong \mathbb{F}_{p^2}$ et (IH) l'idéal d'augmentation de $\mathbb{Z}_p[H]$. Alors,

$$0 \longrightarrow (IH) \longrightarrow H_0(F_1S_2^1, \mathbb{Z}_p[\![S_2^1]\!]) = \mathbb{Z}_p \underset{\mathbb{Z}_p[\![F_1S_2^1]\!]}{\otimes} \mathbb{Z}_p[\![S_2^1]\!] = \mathbb{Z}_p[H] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

est une suite exacte courte. D'où, l'on déduit une autre suite exacte courte

$$0 \longrightarrow H_1(F_1S_2^1, \mathbb{Z}_p) \xrightarrow{\partial} H_0(F_1S_2^1, N_0) \longrightarrow (IH) \longrightarrow 0$$

Comme $(IH) \cong \mathbb{Z}_p^{p^2-1}$, on déduit $H_0(F_1S_2^1, N_0)$. Les autres groupes de cohomologie se déduisent plus simplement. $\square$

2.1 Définition du premier homomorphisme ∂_1

D'après la proposition 1.23, on a un isomorphisme canonique de $\mathbb{Z}_p[F]$-modules

$$\Lambda_{1-p}/_{(p)} \longrightarrow S_2^1/_{\overline{[S_2^1, S_2^1]}} \cong H_1(S_2^1, \mathbb{Z}_p) \longrightarrow (IS_2^1)/_{(IS_2^1)^2} \cong H_0(S_2^1, N_0)$$

tel que si l'on se donne $x \equiv 1 + \bar{x}S \mod (S^2)$ dans S_2^1, alors le premier homomorphisme envoie $\bar{x}$ sur la classe de x et le second envoie la classe de x sur la classe de $(x - e)e_0$. Soit $d_1 : \Lambda_{1-p} \rightarrowtail N_0$ l'homomorphisme de $\mathbb{Z}_p$-modules tel que

$$\begin{tikzcd} \Lambda_{1-p} \arrow[rr, "d_1"] \arrow[d, two heads, "\mathrm{pr}"] & & N_0 \arrow[d, two heads] \\ \Lambda_{1-p}/_{(p)} \arrow[r, "\cong"'] & H_1(S_2^1, \mathbb{Z}_p) \arrow[r, "\cong"'] & H_0(S_2^1, N_0) \end{tikzcd}$$

En appliquant la trace $\mathrm{tr}_F : \mathrm{Hom}(\Lambda_{1-p}, N_0) \to \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, N_0)$ à d_1 et en étendant les scalaires à $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$, on obtient un homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire $\partial_1 : C_1 \to N_0$:

$$\begin{tikzcd}
C_1 = \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \arrow[rr, dashed, "\partial_1"] \arrow[dr, dashed, "\text{Shapiro}"] & & C_0 = \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \underset{\mathbb{Z}_p[F]}{\otimes} \mathbb{Z}_p \arrow[r, "\epsilon"] & \mathbb{Z}_p \\
\Lambda_{1-p} \arrow[u] \arrow[r, "\mathrm{tr}_F(d_1)"] & N_0 \arrow[ur] & &
\end{tikzcd}$$

De plus d'après le lemme A.15, $H_0(S_2^1, C_1)$ en tant que $\mathbb{Z}_p[F]$-module, est canoniquement isomorphe à Λ_{1-p}. Ainsi, par construction de ∂_1, on a

$$\begin{tikzcd}
H_0(S_2^1, C_1) \arrow[r, "\partial_{1*}"] \arrow[d, "\cong"'] & H_0(S_2^1, N_0) \arrow[d, "\cong"] \\
\Lambda_{1-p} \arrow[r, two heads, "\mathrm{tr}_F(\mathrm{pr}) = \mathrm{pr}"] & \Lambda_{1-p}/(p)
\end{tikzcd} \tag{2.1}$$

D'où ∂_{1*} est surjectif et d'après le lemme de Nakayama (corollaire A.9), l'homomorphisme ∂_1 est surjectif. En d'autres termes, pour déterminer la première différentielle ∂_1, il suffit de déterminer un relèvement d_1.

Rappelons brièvement quelques notations. On note $\epsilon_\pm$ les éléments $\omega \pm \omega^p$ de l'anneau de Witt $\mathbb{W}$. Ils forment une $\mathbb{Z}_p$-base de $\mathbb{W} \cong \Lambda_{1-p}$. On a

$$\begin{aligned}
a_0 &:= 1 + \epsilon_+ S \mod (S^2) \\
b_0 &:= 1 + \epsilon_- S \mod (S^2)
\end{aligned}$$

dans S_2^1. Alors, d'après le corollaire précédent, l'application qui, pour tous λ, μ entiers p-adiques, envoie $\lambda\epsilon_+ + \mu\epsilon_- \in \Lambda_{1-p}$ sur $\lambda(a_0 - e)e_0 + \mu(b_0 - e)e_0$ dans N_0, est un relèvement de la projection.

Notation. On note e l'élément neutre de $S_2^1 \subset \mathcal{O}_2^\times$.

L'intérêt de cette notation est de souligner la différence entre $a_0 = 1 + \epsilon_+ S + \ldots$ dans $\mathcal{O}_2$ et $a_0 - e$ dans $\mathbb{Z}_p[\![S_2^1]\!]$.

Définition 2.13.

a) Soit $d_1 : \Lambda_{1-p} \longrightarrow C_0$ l'homomorphisme de $\mathbb{Z}_p$-modules qui envoie ϵ_+ sur $(a_0 - e)e_0$ et ϵ_- sur $(b_0 - e)e_0$.

b) On pose $\partial_1 = \mathrm{tr}_F(d_1)\uparrow_F^{\mathbb{G}_2^1} : C_1 \longrightarrow C_0$ homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire, extension à $\mathbb{G}_2^1$ de la moyenne sous l'action de F de d_1.

Proposition 2.14.

1. *L'homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire $\partial_1 :\ C_1 \longrightarrow C_0$ est caractérisé par*

$$\partial_1(e_1)_+ = \frac{1}{p+1}\sum_{i=0}^{p} \lambda_i(a_i - e)e_0 + \mu_i(b_i - e)e_0 \tag{2.2}$$

2. *L'homomorphisme ∂_1 est surjectif sur N_0.*
3. *Soient $x \in \Lambda_{1-p}$ et $g \in S_2^1$ tels que $g \equiv 1 + xS \mod (S^2)$, alors*

$$\partial_1(x) \equiv (g - e)e_0 \mod (IS_2^1)N_0$$

Remarque. Si dans les calculs effectués dans la preuve suivante, on considère $\lambda(\omega^{(1-p)i}x)$ et $\mu(\omega^{(1-p)i}x)$ au lieu de λ_i et μ_i, on déduit que pour tout $X\otimes x \in \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$:

$$\partial_1(X\otimes x) = \frac{1}{(p+1)}\sum_{i=0}^{p} \lambda(\omega^{(1-p)i}x)\,X\,(a_i - e)e_0 + \mu(\omega^{(1-p)i}x)\,X\,(b_i-e)e_0$$

Démonstration. Rappelons que Λ_{1-p} est cyclique en tant que $\mathbb{Z}_p[F]$-module, ainsi l'image de $(e_1)_+$ détermine ∂_1.
Calculons maintenant $\partial_1(e_1)_+$. Par définition, (λ,μ) est la $\mathbb{Z}_p$-base duale de (ϵ_+,ϵ_-) (voir (1.8)), ainsi, quel que soit $x\in\Lambda_{1-p}$, vu comme élément de $\mathbb{W}$, on a [1]

$$x = \lambda(x)\epsilon_+ + \mu(x)\epsilon_- \quad \text{où} \quad \lambda(x) = \frac{x+x^\sigma}{2\epsilon_+} \text{ et } \mu(x) = \frac{x-x^\sigma}{2\epsilon_-}$$

Ainsi, pour tout i,

$$d_1(\omega_*^i\epsilon_+) = d_1(\omega^{(1-p)i}\epsilon_+) = \lambda_i(a_0-e)e_0 + \mu_i(b_0-e)e_0$$

où, pour rappel, $\lambda_i = \lambda(\omega^{(1-p)i}\epsilon_+)$ et $\mu_i = \mu(\omega^{(1-p)i}\epsilon_+)$. D'où, $\partial_1(\ (e_1)_+\ ) = \mathrm{tr}_F(d_1)(\epsilon_+)$ est égal à

$$\begin{aligned}
&\frac{1}{2(p^2-1)}\sum_{g\in F} g^{-1}\,d_1(\ g_*\epsilon_+\ )\\
=\ &\frac{1}{2(p^2-1)}\sum_{i=1}^{p^2-1}\big(\omega_*^{-i}\,d_1(\omega_*^i\epsilon_+) + \sigma_*^{-1}\omega_*^{-i}\,d_1(\omega_*^i\sigma_*\epsilon_+)\big)\\
=\ &\frac{1}{2(p^2-1)}\sum_{i=1}^{p^2-1}\lambda_i\omega^{-i}(a_0-e)e_0 + \mu_i\omega^{-i}(b_0-e)e_0 + \lambda_i\sigma^{-1}\omega^{-i}(a_0-e)e_0 + \mu_i\sigma^{-1}\omega^{-i}(b_0-e)e_0
\end{aligned}$$

De plus, par définition, $C_0 = \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]\underset{\mathbb{Z}_p[F]}{\otimes}\mathbb{Z}_p$, où $\mathbb{Z}_p$ est muni d'une action triviale de F. D'où, par exemple,

$$\omega^{-i}(a_0-e)e_0 = \omega^{-i}(a_0-e)\omega^i e_0 = (\omega^{-i}a_0\omega^i - e)e_0$$

En d'autres termes F agit par conjugaison sur $\mathbb{Z}_p[\![S_2^1]\!]\cong C_0$.
Pour tout $0\le i\le p^2-1$, rappelons que

$$\begin{aligned}
S_2^1 \ni a_i &= \omega^{-i}a_0\omega^i &\leftrightarrow\quad& [1+\omega^{(p-1)i}\epsilon_+S] &\in S_2/1+p\mathbb{Z}_p\\
S_2^1 \ni b_i &= \omega^{-i}b_0\omega^i &\leftrightarrow\quad& [1+\omega^{(p-1)\,i}\epsilon_-S]
\end{aligned}$$

et posons,

$$\begin{aligned}
a_i^\sigma &= \sigma^{-1}a_i\sigma &\leftrightarrow\quad& [1+\omega^{(1-p)\,i}\epsilon_+S]\\
b_i^\sigma &= \sigma^{-1}b_i\sigma &\leftrightarrow\quad& [1-\omega^{(1-p)\,i}\epsilon_-S]
\end{aligned}$$

Alors, $a_{i+k(p+1)} = a_i$ quel que soit i, de même pour les termes a_i^σ, b_i et b_i^σ. De plus, $a_i^\sigma = a_{-i}$ et $b_i^\sigma = b_{-i+(p+1)/2}$. On note aussi que les coefficients λ_i et μ_i satisfont des relations similaires : $\lambda_i = \lambda_{-i}$ et $\mu_i = \mu_{-i+(p+1)/2}$. Donc, en résumé, $\partial_1(e_1)_+$ est égal à

$$\begin{aligned}
&\frac{1}{2(p^2-1)}\sum_{i=1}^{p^2-1}\lambda_i(a_i-e)e_0 + \mu_i(b_i-e)e_0 + \lambda_i(a_i^\sigma-e)e_0 + \mu_i(b_i^\sigma-e)e_0\\
=\ &\frac{p-1}{2(p^2-1)}\sum_{i=1}^{p+1}\lambda_i(a_i-e)e_0 + \mu_i(b_i-e)e_0 + \lambda_{-i}(a_{-i}-e)e_0 + \mu_{-i+(p+1)/2}(b_{-i+(p+1)/2}-e)e_0\\
=\ &\frac{1}{p+1}\sum_{i=0}^{p}\lambda_i(a_i-e)e_0 + \mu_i(b_i-e)e_0
\end{aligned}$$

1. Ici x^σ est l'image de x par l'automorphisme de Frobenius de $\mathbb{W}$, bien que σ désigne aussi le générateur du groupe de Galois de $\mathbb{F}_{p^2}$, sous-groupe de F

Ensuite, la surjectivité a été montré en toute généralité dans le paragraphe introductif de la section. Le troisième point se lit sur le diagramme (2.1). $\square$

On note N_1 le noyau de l'homomorphisme ∂_1. De la suite exacte courte $N_1 \rightarrowtail C_1 \twoheadrightarrow N_0$, on déduit du corollaire 2.12, le lemme suivant.

Lemme 2.15. *L'homomorphisme ∂_1 induit la suite exacte courte*

$$H_0(S_2^1, N_1) \rightarrowtail \Lambda_{1-p} \twoheadrightarrow \Lambda_{1-p}/(p)$$

où le second homomorphisme est la projection.

Remarque 2.16. *Le lemme de Nakayama (corollaire A.9) ainsi que le lemme précédent montrent que deux éléments de N_1 l'engendrent en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module si leurs images dans $H_0(S_2^1, C_1) \cong \Lambda_{1-p}$ déterminent des générateurs du noyau de $H_0(S_2^1, \partial_1) \cong p\Lambda_{1-p}$. Cette propriété va nous permettre d'approximer des générateurs de N_1.*
Plus précisément, soit $\mathcal{I}$ un idéal de $\mathbb{Z}_p[\![S_2^1]\!]$, supposons qu'on ait trouvé $\kappa_\pm \in C_1$ tels que

$$\begin{cases} \kappa_\pm & \equiv p\epsilon_\pm \mod (IS_2^1)C_1 \\ \partial_1(\kappa_\pm) & \equiv 0 \mod \mathcal{I}N_0 \end{cases}$$

En utilisant le fait que ∂_1 est surjectif sur N_0, on a l'existence de $\tilde{\kappa}_\pm \in \mathcal{I}C_1$ tels que $\kappa_\pm + \tilde{\kappa}_\pm$ appartiennent à N_1. De plus, d'après le critère précédent, on sait que $\kappa_\pm + \tilde{\kappa}_\pm$ engendrent N_1. Ensuite, il suffit de poser $d_2 : \Lambda_{1-p} \longrightarrow N_1$ qui envoie $\epsilon_\pm$ sur $\kappa_\pm + \tilde{\kappa}_\pm$ et $\partial_2 = \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}$. Enfin, on peut montrer, avec une seconde application du lemme de Nakayama, que $\partial_2 : C_2 \to N_1$ est surjectif.

2.2 Approximation de générateurs du noyau de ∂_1

On rappelle qu'on note I l'idéal d'augmentation $(IS_2^1) = \ker(\mathbb{Z}_p[\![S_2^1]\!] \to \mathbb{Z}_p)$ et J l'idéal d'augmentation $(IF_1S_2^1) = \ker(\mathbb{Z}_p[\![F_1S_2^1]\!] \to \mathbb{Z}_p)$. Comme $F_1S_2^1$ est distingué dans $F_1S_2^1$, on note que pour tout $f \in F_1S_2^1$ et tous $g_1, g_2 \in S_2^1$, $g_1(f-e)(g_2-e) = (g_1fg_1^{-1}-e)g_1(g_2-e)$ appartient à JI et $(g_1-e)(f-e)g_2$ appartient à IJ. Ainsi $IJ+JI$ est un idéal bilatère de $\mathbb{Z}_p[\![S_2^1]\!]$.
Dans cette section, nous allons déterminer deux éléments κ_+ et κ_- solutions du problème posé dans la remarque 2.16 pour $\mathcal{I}$ l'idéal $IJ+JI$, c'est-à-dire, tels que

$$\begin{cases} \kappa_\pm & \equiv p\epsilon_\pm \mod (IS_2^1)C_1 \\ \partial_1(\kappa_\pm) & \equiv 0 \mod (IJ+JI)N_0 \end{cases} \tag{2.3}$$

Lemme 2.17. *L'idéal $IJ+JI$ est inclus dans J.*

Démonstration. Comme J est un idéal de $\mathbb{Z}_p[\![S_2^1]\!]$, IJ est inclus dans J. Soient $g \in S_2^1$ et $f \in F_1S_2^1$, alors, comme $F_1S_2^1$ est un sous-groupe distingué de S_2^1, l'élément

$$(f-e)(g-e) = g\underbrace{(g^{-1}fg-e)}_{\in(IF_1S_2^1)} - \underbrace{(f-e)}_{\in(IF_1S_2^1)}$$

appartient à J. D'où JI est aussi inclus dans J. $\square$

D'après ce lemme, l'approximation des générateurs de N_1 avec $\mathcal{I} = IJ + JI$ est plus précise qu'avec l'idéal $J\mathbb{Z}_p[\![S_2^1]\!]$.

Motivons le choix de l'idéal $IJ + JI$. L'homomorphisme $\partial_2 : C_2 \to C_1$ induit

$$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_2, (E_2)_*/(p)) : \ (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1}) \longrightarrow (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$$

noté ∂_2^*. Cet homomorphisme préserve le degré, ainsi en revenant au corollaire 1.34, on déduit que ∂_2^* vérifie :

$$\begin{aligned}
\partial_2^*(v_2^s\, u^{1-p}) &\equiv \sum_{i\geq 0}(\alpha_i + \beta_i u_1^2) u_1^{(p+1)i} v_2^s u^{1-p} \\
\partial_2^*(v_2^s\, u^{p-1}) &\equiv \sum_{i\geq 0}(\alpha_i' + \beta_i' u_1^{p-1}) u_1^{(p+1)i} v_2^s u^{p-1}
\end{aligned}$$

D'autre part, d'après l'avant dernier lemme (lemme 2.15) $H_0(S_2^1, N_1)$ s'injecte dans $pH_0(S_2^1, C_1)$, d'où N_1 est inclus dans $(p,\ I)C_1$. Or l'idéal (p, I) agit trivialement sur $(E_2)_*/(p, u_1)$, donc α_0 et α_0' sont nuls. Pour obtenir une information sur β_0, β_0', éventuels coefficients dominant de $\partial_2^*(v_2^s u^{1-p})$ et $\partial_2^*(v_2^s u^{p-1})$, il faut une approximation au moins modulo (u_1^p) de ∂_2^*. Or, le corollaire 3.4, nous dit que l'idéal d'augmentation $J = (IF_1 S_2^1)$ agit trivialement modulo (p, u_1^{p+1}). Malheureusement, dans notre application au calcul des groupes de cohomologie $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$, il nous faudra plus de précision. D'après la remarque 4.23, l'idéal $IJ + JI$ agit trivialement sur $(E_2)_*/(p, u_1^{p+2})$. Ainsi, avec notre approximation, on sera capable de déterminer $\alpha_0, \alpha_0', \beta_0, \beta_0'$ et en plus α_1 et β_1. En réalité, pour être plus précis, dans la preuve de la proposition 4.22 et les équations (4.10) et (4.11), on utilisera le fait que $IJ+JI$ agit trivialement sur certaines puissances de u modulo une puissance encore plus grande de u_1 et on en déduira dans ces cas le coefficient β_1.

Maintenant que nous avons vu les raisons du choix de l'idéal $IJ+JI$, explicitons la démarche empruntée pour déterminer κ_+ et κ_-. Dans un premier temps, relativement à l'idéal J, nous allons montrer (corollaire 2.28) que

$$\mathcal{N}(a_0)(e_1)_+, \quad \mathcal{N}(b_0)(e_1)_- \quad \text{et} \quad w(e_1)_+ - v(e_1)_-$$

engendrent le noyau, noté $K_{v,w}$, de l'homomorphisme

$$\phi_{v,w} : C_1/JC_1 \longrightarrow IC_0/JC_0$$

induit par $\partial_1 : C_1 \to N_0$. On a la configuration suivante :

$$\begin{tikzcd}
0 \arrow[r] & \ker \arrow[r] \arrow[d] & C_1/(IJ+JI)C_1 \arrow[r, "\partial_{1*}"] \arrow[d] & IC_0/(IJ+JI)IC_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K_{v,w} \arrow[r] & C_1/JC_1 \arrow[r, "\phi_{v,w}"] & IC_0/JC_0 \arrow[r] & 0
\end{tikzcd}$$

Ensuite, dans la sous-section 2.2.3, nous étudierons les images $\partial_1(\mathcal{N}(a_0)(e_1)_+) = \mathcal{N}(a_0)ve_0$, $\partial_1(\mathcal{N}(b_0)(e_1)_-) = \mathcal{N}(b_0)we_0$ et $\partial_1(w(e_1)_+ - v(e_1)_-) = wve_0 - vwe_0$ dans $IC_0/(IJ+JI)IC_0$. Enfin, on en déduira (théorème-définition 2.43) les éléments $\kappa_\pm$ vérifiant les conditions (2.3).

2.2.1 Le module $K_{v,w}$

Définition 2.18. On note[2] H le p-groupe fini $S_2^1/_{F_1 S_2^1} \cong \mathbb{Z}/_p\, x \times \mathbb{Z}/_p\, y$, où x, y sont les classes de a_0 et b_0 respectivement.

Avec ces notations, on a

$$\mathbb{Z}_p[H] \cong \mathbb{Z}_p[x,y]/_{(x^p - 1, y^p - 1)}$$

D'après le théorème A.4, l'anneau $\mathbb{Z}_p[H]$ est local. On pose $(IH) := (x-1, y-1) = \ker(\mathbb{Z}_p[H] \to \mathbb{Z}_p)$.

Lemme 2.19. *On a la suite exacte courte de $\mathbb{Z}_p[H]$-modules suivante :*

$$0 \longrightarrow H_0(F_1 S_2^1, N_1) \longrightarrow \mathbb{Z}_p[H] \otimes \Lambda_{1-p} \xrightarrow{\partial_{1*}} H_0(F_1 S_2^1, N_0) \longrightarrow 0$$

Démonstration. D'après le corollaire 2.12, $H_1(F_1 S_2^1, N_0)$ est trivial, d'où la suite exacte courte

$$0 \longrightarrow H_0(F_1 S_2^1, N_1) \longrightarrow H_0(F_1 S_2^1, C_1) \xrightarrow{\partial_{1*}} H_0(F_1 S_2^1, N_0) \longrightarrow 0$$

Et d'après le lemme A.15, on a un isomorphisme canonique de $\mathbb{Z}_p[H]$-modules $H_0(F_1 S_2^1, C_1) \cong \mathbb{Z}_p[H] \otimes \Lambda_{1-p}$. $\square$

Notons aussi que d'après le corollaire 1.19,

$$\begin{aligned} H_1(F_1 S_2^1, \mathbb{Z}_p) &= (F_1 S_2^1)_{\mathrm{ab}} \cong F_1 S_2^1/_{[F_1 S_2^1, F_1 S_2^1]} \cong F_1 S_2^1/_{F_{5/2} S_2^1} \\ &\cong \mathbb{Z}/_{p^2}\, \bar{c}_0 \oplus \mathbb{Z}/_p\, \bar{a}_0^p \oplus \mathbb{Z}/_p\, \bar{b}_0^p \end{aligned}$$

L'action par conjugaison de S_2^1 sur le sous-groupe $F_1 S_2^1$ induit une structure de $\mathbb{Z}_p[H]$-module sur $(F_1 S_2^1)_{\mathrm{ab}}$. La figure 2.2 résume les différentes notations.

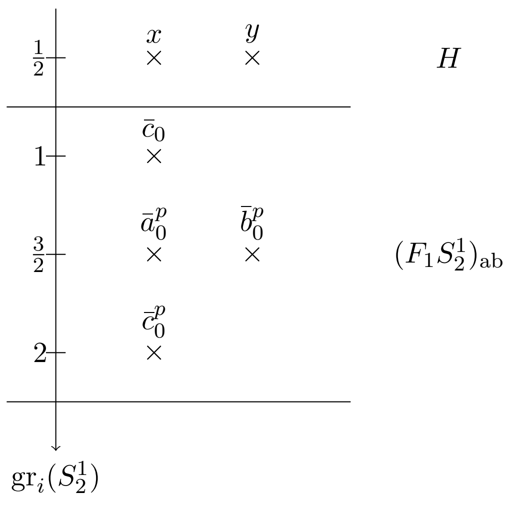

FIGURE 2.2 – Les groupes H et $(F_1 S_2^1)_{\mathrm{ab}}$

2. Le groupe H est isomorphe au groupe $H_1(S_2^1, \mathbb{Z}_p) \cong \Lambda_{1-p}/_{(p)}$. Cependant, dans cette section, il sera plus commode de les distinguer.

Proposition-Définition 2.20. *On munit $H_1(F_1S_2^1, \mathbb{Z}_p) \cong (F_1S_2^1)_{\mathrm{ab}}$ de la structure de $\mathbb{Z}_p[H]$-module induite par l'action par conjugaison de S_2^1 sur le sous-groupe $F_1S_2^1$. On pose*

1. *$\iota : (F_1S_2^1)_{\mathrm{ab}} \to H_0(F_1S_2^1, N_0)$ l'application définie par $\iota(f) = f - e \quad$ pour tout $f \in (F_1S_2^1)_{\mathrm{ab}}$.*
2. *$\mathrm{pr} : H_0(F_1S_2^1, N_0) \to (IH)$ l'homomorphisme $\mathbb{Z}_p[H]$-linéaire induit par l'inclusion de $N_0 \cong (IS_2^1)$ dans $\mathbb{Z}_p[\![S_2^1]\!]$. En particulier, pour tout $g \in S_2^1$, on a $\mathrm{pr}(g - e) = \bar{g} - e$, où $\bar{g}$ désigne la classe de g dans H.*

Alors, ι est $\mathbb{Z}_p[H]$-linéaire et on a une suite exacte courte de $\mathbb{Z}_p[H]$-modules :

$$\begin{tikzcd} 0 \arrow[r] & (F_1S_2^1)_{\mathrm{ab}} \arrow[r, "\iota"] & H_0(F_1S_2^1, N_0) \arrow[r, "\mathrm{pr}"] & (IH) \arrow[r] & 0 \end{tikzcd}$$

Démonstration. C'est une simple application de la proposition A.11 donnée en annexe. $\square$

Lemme 2.21. *Notons $\epsilon : \mathbb{Z}_p[\![S_2^1]\!] \to \mathbb{Z}_p$ l'homomorphisme d'augmentation.*

a) L'inclusion de J dans JC_0 induit un isomorphisme $J/_{J^2} \cong JC_0/_{JIC_0}$. De plus, l'inverse du morphisme envoie la classe de XY, où $X \in J$ et $Y \in C_0$, sur la classe de $\epsilon(Y)X$.

b) On a un isomorphisme de suites exactes courtes :

$$\begin{tikzcd} 0 \arrow[r] & JC_0/_{JIC_0} \arrow[r] \arrow[d, "\mathrm{Id}_J\,\epsilon"', "\cong"] & IC_0/_{JIC_0} \arrow[r] \arrow[d, "="] & IC_0/_{JC_0} \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & J/_{J^2} \arrow[r] & H_0(F_1S_2^1, N_0) \arrow[r] & (IH) \arrow[r] & 0 \end{tikzcd}$$

où l'isomorphisme $IC_0/_{JC_0} \cong (IH)$ est induit par la projection de IC_0 sur (IH).

Démonstration.

a) Comme J est inclus dans I, par passage au quotient de l'application de J dans JC_0, on déduit l'homomorphisme $\pi : J/_{J^2} \to JC_0/_{JIC_0}$.

Soit $(b_1, \ldots, b_{p^2}) \in (S_2^1)^{\times p^2}$ une famille de représentants des éléments du groupe quotient $S_2^1/_{F_1S_2^1}$ telle que $b_1 = e$. D'après le lemme A.12, on a l'isomorphisme de $\mathbb{Z}_p[\![F_1S_2^1]\!]$-modules

$$\begin{aligned} \psi : \ \mathbb{Z}_p[\![F_1S_2^1]\!]^{\oplus p^2} &\longrightarrow \mathbb{Z}_p[\![S_2^1]\!] \cong C_0 \\ (x_1, \ldots, x_{p^2}) &\longmapsto x_1e_0 + \textstyle\sum_{i=2}^{p^2} x_i(b_i - e)e_0 \end{aligned}$$

D'où, l'on déduit le diagramme de $\mathbb{Z}_p[\![F_1S_2^1]\!]$-modules

$$\begin{tikzcd} JIC_0 \arrow[r] & JC_0 \arrow[r, dashed, "\mathrm{Id}_J\,\epsilon"] & J \\ J^2 \oplus \left(J^{\oplus p^2-1}\right) \arrow[r] \arrow[u, "\cong"] & J \oplus \left(J^{\oplus p^2-1}\right) \arrow[u, "\cong"] \arrow[ur, "\mathrm{Id}_J \oplus 0"'] & \end{tikzcd}$$

où les isomorphismes verticaux sont induit par restriction de ψ. L'homomorphisme $\mathrm{Id}_J\,\epsilon : JC_0 \to J$ envoie XY, où $X \in J$ et $Y \in C_0$ sur $X\epsilon(Y)$. Du précédent diagramme, on déduit de plus que $\mathrm{Id}_J\,\epsilon$ induit un homomorphisme

$$\mathrm{Id}_J\,\epsilon : JC_0/_{JIC_0} \longrightarrow J/_{J^2}$$

Soient $X \in J$ et $Y \in C_0$, alors $XY \equiv X\epsilon(Y) \mod JIC_0$, d'où l'on déduit que $\pi : J/_{J^2} \to JC_0/_{JIC_0}$ est inversible d'inverse $\mathrm{Id}_J\,\epsilon$.

b) La projection de IC_0 sur (IH) induit un homomorphisme $IC_0/_{JC_0} \to (IH)$ tel qu'on ait le diagramme suivant

$$\begin{tikzcd}
0 \arrow[r] & JC_0/_{JIC_0} \arrow[r] \arrow[d, "\mathrm{Id}_J\,\epsilon"', "\cong"] & IC_0/_{JIC_0} \arrow[r] \arrow[d, "="] & IC_0/_{JC_0} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H_1(F_1S_2^1, \mathbb{Z}_p) \arrow[r] & H_0(F_1S_2^1, N_0) \arrow[r] & (IH) \arrow[r] & 0
\end{tikzcd}$$

Le première ligne induite par les inclusions $JIC_0 \subset JC_0 \subset IC_0$ est exacte et la seconde ligne est aussi exacte d'après la proposition-définition précédente. Enfin, d'après le lemme des cinq, on déduit que l'homomorphisme vertical de droite est aussi un isomorphisme .

□

Définition 2.22. Avec les notations de la proposition-définition précédente, on pose $\phi_{v,w} = \mathrm{pr} \circ \partial_{1*}$:

$$\begin{tikzcd}
\mathbb{Z}_p[H] \otimes \Lambda_{1-p} \arrow[r, two heads, "\partial_{1*}"] \arrow[dr, two heads, "\phi_{v,w}"'] & H_0(F_1S_2^1, N_0) \arrow[d, two heads, "\mathrm{pr}"] \\
 & (IH)
\end{tikzcd}$$

et $K_{v,w}$ le noyau de $\phi_{v,w}$.

Remarque 2.23. *Du lemme précédent, on déduit que $K_{v,w}$ est isomorphe au noyau de l'homomorphisme*

$$C_1/_{JC_1} \longrightarrow IC_0/_{JC_0}$$

induit par $\partial_1 : C_1 \to N_0$. En effet, on a le diagramme suivant :

$$\begin{tikzcd}
0 \arrow[r] & \ker \arrow[r] \arrow[d, "\cong"] & C_1/_{JC_1} \arrow[r, "\partial_{1*}"] \arrow[d, "\cong"] & IC_0/_{JC_0} \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & K_{v,w} \arrow[r] & \mathbb{Z}_p[H] \otimes \Lambda_{1-p} \arrow[r, "\phi_{v,w}"] & (IH) \arrow[r] & 0
\end{tikzcd}$$

Notation. *Pour ne pas alourdir les notations, jusqu'à la fin de cette sous-section, j'identifie v et w avec leurs images par la projection* pr *dans (IH).*

Ainsi, par définition de v, w (définition 2.8) et ∂_1 (théorème 2.10), on note que

$$\phi_{v,w}(1 \otimes \epsilon_+) = v \qquad \text{et} \qquad \phi_{v,w}(1 \otimes \epsilon_-) = w$$

De plus, comme Λ_{1-p} est libre de rang 2 en tant que $\mathbb{Z}_p$-module, $\mathbb{Z}_p[H] \otimes \Lambda_{1-p}$ est libre de rang 2 en tant que $\mathbb{Z}_p[H]$-module dont $(1 \otimes \epsilon_+, 1 \otimes \epsilon_-)$ est une base. Nous allons utiliser cette base pour identifier $\mathbb{Z}_p[H] \otimes \Lambda_{1-p}$ et $\mathbb{Z}_p[H]^{\oplus 2}$.

Par construction, l'homomorphisme ∂_1 est surjectif sur N_0, d'où $\phi_{v,w}$ est aussi surjectif. On a la suite exacte courte suivante :

$$\begin{tikzcd}
0 \arrow[r] & K_{v,w} \arrow[r] & \mathbb{Z}_p[H]^{\oplus 2} \cong \mathbb{Z}_p[H] \otimes \Lambda_{1-p} \arrow[r, "\phi_{v,w}"] & (IH) \arrow[r] & 0 \\
 & & (P,Q) \arrow[r, mapsto] & Pv + Qw &
\end{tikzcd} \tag{2.4}$$

Le lemme suivant donne une caractérisation de l'ensemble des surjections de $\mathbb{Z}_p[H]^{\oplus 2}$ sur (IH).

Lemme 2.24. *Soient $\phi_1, \phi_2 : \mathbb{Z}_p[H]^{\oplus 2} \longrightarrow (IH)$ deux homomorphismes surjectifs, alors il existe un automorphisme α de $\mathbb{Z}_p[H]^{\oplus 2}$ tel qu'on ait :*

$$\begin{tikzcd} \mathbb{Z}_p[H]^{\oplus 2} \arrow[r, two heads, "\phi_1"] \arrow[d, "\alpha"', "\cong"] & (IH) \arrow[d, "="] \\ \mathbb{Z}_p[H]^{\oplus 2} \arrow[r, two heads, "\phi_2"] & (IH) \end{tikzcd}$$

Démonstration. Comme ϕ_2 est surjectif par hypothèse et $\mathbb{Z}_p[H]^{\oplus 2}$ est projectif, on a l'existence de l'homomorphisme α tel que le diagramme commute.
Par un résultat classique d'homologie des groupes profinis (par exemple le lemme 6.8.6 [RZ10]), en utilisant le fait que $(IH) = \ker(\mathbb{Z}_p[H] \twoheadrightarrow \mathbb{Z}_p)$, on a

$$\mathrm{Tor}_0^{\mathbb{Z}_p[H]}(\mathbb{F}_p, (IH)) \cong \mathrm{Tor}_1^{\mathbb{Z}_p[H]}(\mathbb{F}_p, \mathbb{Z}_p) = H_1(H, \mathbb{F}_p) \cong H/[H,H], H^p = H \cong \mathbb{F}_{p^2}$$

Appliquons maintenant $\mathrm{Tor}_0^{\mathbb{Z}_p[H]}(\mathbb{F}_p, \_)$ au diagramme précédent :

$$\begin{tikzcd} \mathbb{F}_p \oplus \mathbb{F}_p \arrow[r, two heads] \arrow[d, "\alpha"'] & \mathbb{F}_{p^2} \arrow[d, "="] \\ \mathbb{F}_p \oplus \mathbb{F}_p \arrow[r, two heads] & \mathbb{F}_{p^2} \end{tikzcd}$$

D'où, on déduit que $\mathrm{Tor}_0^{\mathbb{Z}_p[H]}(\mathbb{F}_p, \alpha)$ est un isomorphisme. Comme $\mathrm{Tor}_1^{\mathbb{Z}_p[H]}(\mathbb{F}_p, \mathbb{Z}_p[H]^{\oplus 2})$ est trivial, l'homomorphisme $\mathrm{Tor}_1^{\mathbb{Z}_p[H]}(\mathbb{F}_p, \alpha)$ est surjectif. Donc d'après le lemme de Nakayama (corollaire A.9), α est un isomorphisme. □

On peut donc espérer déduire des informations sur $\phi_1 = \phi_{v,w}$ à partir d'informations sur $\phi_2 = \phi_{x-1,y-1}$ et α. On verra dans les résultats suivants qu'on peut effectivement déterminer assez précisément l'homomorphisme α (voir le diagramme (2.8)) et en déduire trois générateurs de $K_{v,w}$ (corollaire 2.28).

Soit $\psi_{v,w} : K_{v,w} \to (IH)$ l'homomorphisme qui envoie le couple (P, Q) du noyau $K_{v,w}$ sur Pv. Nous avons alors la suite exacte courte suivante :

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ann}(v) \oplus \mathrm{Ann}(w) \arrow[r] & K_{v,w} \arrow[r, "\psi_{v,w}"] & \mathrm{Im}\,\psi_{v,w} \arrow[r] & 0 \\ & & (P,Q) \arrow[r, mapsto] & Pv = -Qw & \end{tikzcd} \tag{2.5}$$

Ainsi pour déterminer des générateurs de $K_{v,w}$, il suffit de déterminer des générateurs de $\mathrm{Ann}(v)$, $\mathrm{Ann}(w)$ et $\mathrm{Im}\,\psi_{v,w}$.
Avant, un petit lemme technique qui nous sera encore une fois utile dans la section suivante.

Lemme 2.25. *Les éléments $l_i = \omega^{(1-p)i} + \omega^{(p-1)i}$ et $m_i = \omega^{(1-p)i} - \omega^{(p-1)i}$ de l'anneau de Witt $\mathbb{W}$, vérifient la propriété suivante :*

$$\forall\, P(X) \in \mathbb{W}[X] : \quad \sum_{i=0}^{p} l_i P(m_i) = \sum_{i=0}^{p} m_i P(l_i) = 0$$

Un petit rappel : Soit ξ une racine n-ème de l'unité. Soit k un entier naturel, alors ξ^k est une racine $d = \frac{n}{n \wedge k}$-ème de l'unité. On a

$$\sum_{i=1}^{n} \xi^{ki} = \begin{cases} n & \text{si } n \mid k \\ 0 & \text{sinon} \end{cases}$$

Démonstration. Pour démontrer le lemme, il suffit de considérer les monômes X^k. Soit k un entier naturel, montrons donc que

$$\Delta_k = \sum_{i=0}^{p} l_i m_i^k \quad \text{et} \quad \Delta'_k = \sum_{i=0}^{p} m_i l_i^k$$

sont nuls. Développons ces expressions :

$$\begin{aligned}
\Delta_k &= \sum_{i=0}^{p} l_i m_i^k \\
&= \sum_{i=0}^{p} (\omega^{(1-p)i} + \omega^{(p-1)i})(\omega^{(1-p)i} - \omega^{(p-1)i})^k \\
&= \sum_{i=0}^{p} \sum_{l+m=k} (-1)^m \binom{k}{l} \left(\omega^{(1-p)i(1+l-m)} + \omega^{(1-p)i(-1+l-m)}\right) \\
&= \sum_{l+m=k} \binom{k}{l} (-1)^m \sum_{i=0}^{p} (\omega^{(1-p)i(1+l-m)} + \omega^{(1-p)i(-1+l-m)})
\end{aligned}$$

et

$$\begin{aligned}
\Delta'_k &= \sum_{i=0}^{p} m_i l_i^k \\
&= \sum_{i=0}^{p} (\omega^{(1-p)i} - \omega^{(p-1)i})(\omega^{(1-p)i} + \omega^{(p-1)i})^k \\
&= \sum_{l+m=k} \binom{k}{l} \sum_{i=0}^{p} (\omega^{(1-p)i(1+l-m)} - \omega^{(1-p)i(-1+l-m)})
\end{aligned}$$

Lorsque $-1 + l - m$ et $1 + l - m$ ne sont pas divisible par $p + 1$, alors, comme ω^{1-p} est une racine primitive $(p + 1)$-ème de l'unité, les sommes sur i sont nuls. D'autre part, il y a une correspondance entre les couples (l, m) tels que $-1 + l - m \equiv 0\ [p + 1]$ et les couples (l', m') tels que $1 + l' - m' \equiv 0\ [p + 1]$: $(l', m') = (m, l)$. D'où Δ'_k est nul.
Pour Δ_k, notons de plus que la condition $-1+l-m \equiv 0\ [p+1]$ implique $l+m \equiv 1\ [2]$, c'est-à-dire m et $m' = l$ ne sont pas de même parité. D'où, sur la somme sur l, m, il y a des compensations de telle sorte que Δ_k soit nul. $\square$

On rappelle que dans cette section, on identifie les éléments v et w avec leurs images dans (IH) via l'homomorphisme $N_0 \twoheadrightarrow H_0(F_1 S_2^1, N_0) \twoheadrightarrow (IH)$, où le second homomorphisme est induit par la projection $\mathbb{Z}_p[\![S_2^1]\!] \twoheadrightarrow \mathbb{Z}_p[H]$.

Proposition 2.26. *Il existe $v', w' \in \mathbb{Z}_p[H]$ tels que :*

1. $v' \equiv w' \equiv 1 \mod (p,\ (IH))$
2. $v = v'(x - 1)$ *et* $w = w'(y - 1)$.

En particulier, v' et w' sont des unités de l'anneau local $\mathbb{Z}_p[H]$.

Remarque. Le point clé de la preuve est l'utilisation de la formule d'interpolation de la fonction puissance (proposition A.3 ou paragraphe III.1.1.6 *La fonction puissance* de [Laz65], page 73) pour l'identité (2.6).

En utilisant l'isomorphisme de $S_2^1/F_1S_2^1$ avec $\Lambda_{1-p}/(p)$ (proposition 1.23), on obtient les identités suivantes :

$$\begin{array}{rcccll} a_i & \equiv & 1+\omega^{(p-1)i}\epsilon_+ S & \equiv & a_0^{\lambda(\omega^{(p-1)i}\epsilon_+)}\, b_0^{\mu(\omega^{(p-1)i}\epsilon_+)} & \mod F_1S_2^1 \\ b_i & \equiv & 1+\omega^{(p-1)i}\epsilon_- S & \equiv & a_0^{\lambda(\omega^{(p-1)i}\epsilon_-)}\, b_0^{\mu(\omega^{(p-1)i}\epsilon_-)} & \mod F_1S_2^1 \end{array}$$

d'où, en revenant à la définition de v et w (définition 2.8), on a

$$\begin{aligned} v &= \mathrm{pr}\big(\frac{\epsilon_+}{p+1}\sum_{i=0}^{p}\lambda_i(a_i-e)e_0+\mu_i(b_i-e)e_0\big) \\ &= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_+)x^{\lambda(\omega^{(p-1)i}\epsilon_+)}y^{\mu(\omega^{(p-1)i}\epsilon_+)}+\mu(\omega^{(1-p)i}\epsilon_+)x^{\lambda(\omega^{(p-1)i}\epsilon_-)}y^{\mu(\omega^{(p-1)i}\epsilon_-)} \\ w &= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_-)x^{\lambda(\omega^{(p-1)i}\epsilon_+)}y^{\mu(\omega^{(p-1)i}\epsilon_+)}+\mu(\omega^{(1-p)i}\epsilon_-)x^{\lambda(\omega^{(p-1)i}\epsilon_-)}y^{\mu(\omega^{(p-1)i}\epsilon_-)} \end{aligned}$$

Démonstration. Nous allons procéder en plusieurs étapes :

a) Montrons que $v \equiv 0 \bmod (x-1)$: on se place donc dans $\mathbb{Z}_p[H]/(x-1) \subset \mathbb{W}[H]/(x-1)$. En interpolant la fonction puissance (proposition A.3), on a [3]

$$\begin{aligned} v &\equiv \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_+)y^{\mu(\omega^{(p-1)i}\epsilon_+)}+\mu(\omega^{(1-p)i}\epsilon_+)y^{\mu(\omega^{(p-1)i}\epsilon_-)} \\ &\equiv \frac{1}{p+1}\sum_{i=0}^{p}\sum_{k\geq 0}(*\,l_i\binom{*\,m_i}{k}-*\,m_i\binom{*\,l_i}{k})(y-1)^k \qquad (2.6) \\ &\equiv \frac{1}{p+1}\sum_{k\geq 0}\left(\sum_{i=0}^{p}l_iP_k(m_i)-m_iQ_k(l_i)\right)(y-1)^k \end{aligned}$$

où $P_k(X)$ et $Q_k(X)$ appartiennent à $\mathbb{W}[X]$. Ainsi, d'après le lemme 2.25, dans la précédente somme double, les sommes sur i sont nulles et on en déduit que v est nul modulo $(x-1)$.

b) Soit v' dans $\mathbb{Z}_p[H]$ tel que $v=(x-1)v'$. Par construction de ∂_1 (proposition-définition 2.14), $(x-1)v'$ est congru à $x-1$ modulo $(IS_2^1)^2$. Soit l un nombre p-adique et $v'' \in (IH)$ tels que $v'=l+v''$ et ϕ l'isomorphisme de $(IH)/(IH)^2$ sur H. Alors $\phi(v-(x-1))=\phi((l-1)(x-1))=x^{l-1}$ est nul, ainsi $l=1+kp$ pour un certain entier p-adique k et $v'=1+pk+v''$ est congru à 1 modulo l'idéal maximal $(p,x-1,y-1)$ de l'anneau local $\mathbb{Z}_p[H]$ (théorème A.4). Donc v' est une unité.

c) Idem pour w : Modulo $(y-1)$,

$$\begin{aligned} w &= \frac{1}{p+1}\sum_{i=0}^{p}\lambda(\omega^{(1-p)i}\epsilon_-)x^{\lambda(\omega^{(p-1)i}\epsilon_+)}+\mu(\omega^{(1-p)i}\epsilon_-)x^{\lambda(\omega^{(p-1)i}\epsilon_-)} \\ &= \frac{1}{p+1}\sum_{k\geq 0}\sum_{i=0}^{p}(*\,m_i\binom{*\,l_i}{k}+*\,l_i\binom{*\,m_i}{k})(x-1)^k \end{aligned}$$

De même, que pour v, w est nul modulo $(y-1)$. Et on déduit aussi qu'il existe w' une unité tel que $w=w'(y-1)\equiv y-1 \bmod (IH)^2$.

3. Le symbole $*$ désigne un élément de $\mathbb{W}$ fixé qui ne dépend ni de i ni de k.

$\square$

Remarque. On a vu dans la preuve, le résultat suivant : Quel que soit l'élément v de (IH), s'il existe v' tel que $v = (x-1)v' \equiv x - 1 \mod (IH)^2$ alors v' est une unité.

Notation. Rappelons que si G est un groupe profini et $g \in G$, on pose $\mathcal{N}(g) = \sum_{i=0}^{p-1} g^i$ dans $\mathbb{Z}_p[\![G]\!]$.

Corollaire 2.27. *On a les propriétés suivantes :*

1. $\mathrm{Ann}(v) = (\mathcal{N}(x)) = \mathrm{Ann}(1-x) = \{\sum_{i,j} \alpha_{ij} x^i y^j;\ \forall\, i, j, k :\ \alpha_{ij} = \alpha_{kj}\ \}$
2. $\mathrm{Ann}(w) = (\mathcal{N}(y))$
3. $\mathrm{Im}\,\psi_{v,w} = (vw) = \mathrm{Im}\,\psi_{x-1,y-1} = \{\sum_{i,j} \alpha_{ij} x^i y^j; \forall\, i, j :\ \sum_i \alpha_{ij} = \sum_j \alpha_{ij} = 0\,\}$

Démonstration. On note que $x\mathcal{N}(x) = \mathcal{N}(x)$, donc l'idéal $(\mathcal{N}(x))$ est inclus dans $\mathrm{Ann}(x-1)$. Soit $\sum c_{ij} x^i y^j$ un élément de l'annulateur de $x-1$, alors :

$$(1-x) \sum_{i,j} c_{ij} x^i y^j = \sum_{i,j} (c_{ij} - c_{i-1,j}) x^i y^j = 0$$

D'où l'on déduit que l'annulateur de $x-1$ est l'idéal engendré par $\mathcal{N}(x)$. L'annulateur de v est égal à celui de $x-1$ car, tout simplement, ils diffèrent par multiplication par une unité. D'où le premier point du corollaire. Le second point est analogue. Montrons le dernier point : comme $v = v'(x-1)$ et $w = w'(y-1)$ où v', w' sont des unités, l'idéal (vw) coïncide avec $((x-1)(y-1))$, l'homomorphisme

$$\begin{aligned} \alpha : \mathbb{Z}_p[H]^{\oplus 2} &\longrightarrow \mathbb{Z}_p[H]^{\oplus 2} \\ (P, Q) &\longmapsto (Pv', Qw') \end{aligned} \tag{2.7}$$

est un automorphisme et on a le diagramme suivant :

$$\begin{tikzcd} 0 \arrow[r] & K_{v,w} \arrow[r] \arrow[d] & \mathbb{Z}_p[H]^{\oplus 2} \arrow[r, "\phi_{v,w}"] \arrow[d, "\alpha", "\cong"'] & (IH) \arrow[r] \arrow[d, "="] & 0 \\ 0 \arrow[r] & K_{x-1,y-1} \arrow[r] & \mathbb{Z}_p[H]^{\oplus 2} \arrow[r, "\phi_{x-1,y-1}"] & (IH) \arrow[r] & 0 \end{tikzcd} \tag{2.8}$$

Ainsi, d'après le lemme des 5, on déduit que la restriction de α à $K_{v,w}$ induit un isomorphisme sur $K_{x-1,y-1}$.
Soit $(P, Q) \in K_{v,w}$, alors

$$\psi_{v,w}(P, Q) = Pv = Pv'(x-1) = \psi_{x-1,y-1}(Pv', Qw')$$

Donc, l'image de $\psi_{v,w}$ est incluse dans l'image de $\psi_{x-1,y-1}$. Or, comme v' et w' sont inversibles, on déduit de la même manière l'inclusion inverse et $\mathrm{Im}\,\psi_{x-1,y-1} = \mathrm{Im}\,\psi_{v,w}$.
Nous allons maintenant décrire $\mathrm{Im}\,\psi_{x-1,y-1}$. Posons I l'idéal des éléments $\sum_{i,j} c_{i,j} x^i y^j$ tels que $\sum_i c_{ij}$ et $\sum_j c_{ij}$ soient nulles. Il est immédiat que $\mathrm{Im}\,\psi_{x-1,y-1}$ est incluse dans l'intersection des idéaux $(x-1)$ et $(y-1)$, donc en particulier est incluse dans I. Soient $u = \sum c_{ij} x^i y^j$ un élément de I, alors :

$$u = \sum_{i,j} c_{i,j} (x^i - 1)(y^j - 1) = u'(x-1)(y-1)$$

pour un certain u' dans $\mathbb{Z}_p[H]$. Ainsi, $u = \psi_{x-1,y-1}(u'(y-1), -u'(x-1))$. En résumé, on a :

$$\mathrm{Im}\,\psi_{v,w} = \mathrm{Im}\,\psi_{x-1,y-1} = I = ((x-1)(y-1)) = (vw)$$

$\square$

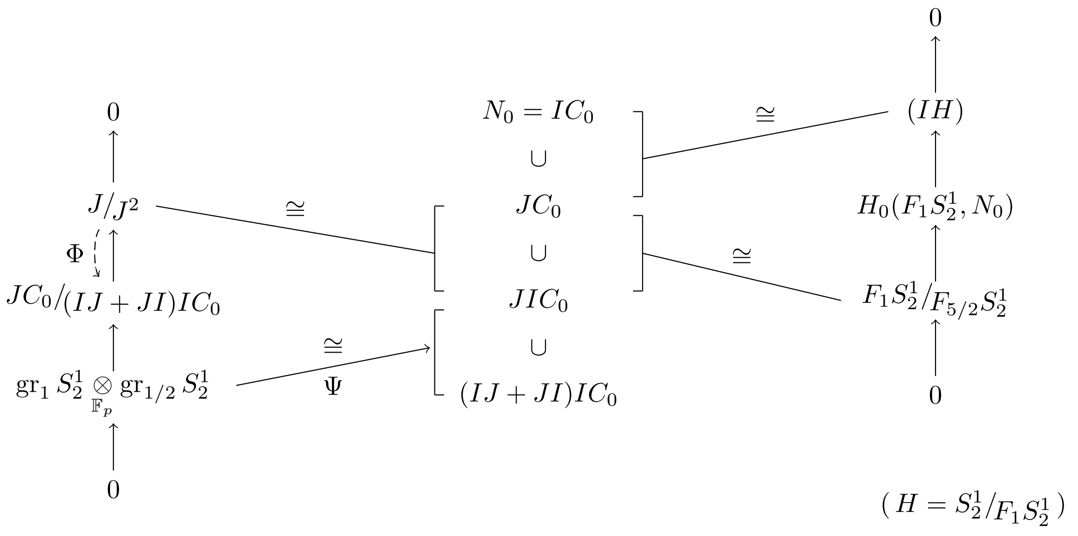

FIGURE 2.3 – Sous-modules de N_0.

En revenant à la suite exacte courte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ann}(v) \oplus \mathrm{Ann}(w) & \longrightarrow & K_{v,w} & \xrightarrow{\psi_{v,w}} & \mathrm{Im}\, \psi_{v,w} & \longrightarrow & 0 \\ & & & & (P,Q) & \longmapsto & Pv = -Qw & & \end{array}$$

et en utilisant les générateurs données dans le corollaire précédent, on déduit immédiatement les générateurs de $K_{v,w}$.

Corollaire 2.28. *Le $\mathbb{Z}_p[H]$-module $K_{v,w}$, vu comme sous-module de $C_1/_{JC_1}$, est engendré par les classes de $\mathcal{N}(a_0)(e_1)_+$, $\mathcal{N}(b_0)(e_1)_-$ et $w(e_1)_+ - v(e_1)_-$.*

Remarque 2.29. *En fait, en poursuivant l'étude de $H_0(F_1S_2^1, \partial_1)$, on a pu montrer qu'il existe deux entiers p-adiques λ' et μ' tels que l'image des éléments*

$$\mathcal{N}(a_0)(e_1)_+ + \left(\frac{1}{4\epsilon_-^2}(b_0 - e) - \lambda' p\right)(w(e_1)_+ - v(e_1)_-)$$
$$\mathcal{N}(b_0)(e_1)_- + \left(\frac{1}{4\epsilon_+^2}(a_0 - e) - \mu' p\right)(w(e_1)_+ - v(e_1)_-)$$

par ∂_1 appartiennent à $J\,N_0$. C'est-à-dire, ils déterminent une solution du problème posé dans la remarque 2.16 relativement à l'idéal $\mathcal{I} = J$. Ce fait, nous a guidé pour déterminer $\kappa_\pm$. D'autre part, comme $(IJ + JI)IC_0 \subset JIC_0$ (lemme 2.17), cette propriété est une conséquence du théorème-définition 2.43.

Avant de considérer l'image des trois générateurs dans le quotient $JC_0/_{(IJ+JI)IC_0}$, nous allons décomposer ce dernier module.

2.2.2 Filtration de N_0

Notons la succession d'inclusions suivantes :

$$(IJ + JI)N_0 \quad \subset \quad JIC_0 = JN_0 \quad \subset \quad JC_0 \quad \subset \quad N_0 = IC_0$$

Dans cette section, nous allons compléter l'étude des différents quotients commencée dans le lemme 2.21. La figure 2.3 page 48 en donne un résumé.

Dans le lemme suivant, nous donnons une liste de sous-groupes de $(IJ+JI)I \cong (IJ+JI)IC_0$. Ces inclusions, nous serons utiles dans la proposition suivantes ainsi que dans les sous-sections suivantes.

Lemme 2.30. *Les sous-groupes de $\mathbb{Z}_p[\![S_2^1]\!]$,*

$$(IF_{3/2}S_2^1)I, \quad (IF_{5/2}S_2^1), \quad p(IF_{3/2}S_2^1), \quad I(IF_2S_2^1), \quad pJI, \quad pIJ, \quad JIJ \quad et \quad J^2$$

sont inclus dans $(IJ+JI)I$.

Démonstration. D'après le corollaire 1.21, on a en particulier,

$$(IF_{3/2}S_2^1) \subseteq (IF_{1/2}S_2^1)(IF_1S_2^1) + (IF_1S_2^1)(IF_{1/2}S_2^1)$$

D'où l'inclusion de $(IF_{3/2}S_2^1)I$.
D'après le corollaire 1.19 sur la relation entre la filtration de S_2^1 et les puissances de l'idéal I, on a que $(IF_{3/2}S_2^1) \subset I^3$ et que $J \subset I^2$. Ainsi, par une seconde application du corollaire 1.21, on a

$$\begin{aligned}(IF_{5/2}S_2^1) &\subseteq J(IF_{3/2}S_2^1) + (IF_{3/2}S_2^1)J \\ &\subseteq JI^3 + (JI+IJ)I^2 \\ &\subseteq (IJ+JI)I\end{aligned}$$

Soit $f \in F_{3/2}S_2^1$, alors

$$p(f-e) = \underbrace{f^p - e}_{\in (IF_{5/2}S_2^1)} - \sum_{i=2}^{p} \binom{p}{i} \underbrace{(f-e)^i}_{\in J^2} \equiv 0 \mod (IJ+JI)I$$

D'où, $p(IF_{3/2}S_2^1) \subset (IJ+JI)I$.
Soient $g \in S_2^1$ et $f \in F_2S_2^1$, comme $(IF_{5/2}S_2^1)$ et $(IF_{3/2}S_2^1)I$ sont inclus dans $(IJ+JI)I$, on a

$$(g-e)(f-e) = \underbrace{(f-e)}_{\in (IF_{3/2}S_2^1)}(g-e) + \underbrace{([f,g]-e)}_{\in (IF_{5/2}S_2^1)}gf \quad \in (IJ+JI)I$$

D'après la proposition 1.23, $H_0(S_2^1, I) \cong H_1(S_2^1, \mathbb{Z}_p) \cong \mathbb{F}_{p^2}$ et donc $pI \subset I^2$. On en déduit que les idéaux pIJ et pJI sont inclus dans $(IJ+JI)I$.
Enfin, les deux dernières inclusions se déduisent de l'inclusion $J \subset I^2$. □

Proposition 2.31.

1. *L'homomorphisme $J \otimes I$ dans $JIC_0/(IJ+JI)IC_0$ qui envoie $X \otimes Y$ sur XYe_0, induit un homomorphisme*

$$\Psi : J/J^2 + (IF_{3/2}S_2^1) \otimes I/I^2 \longrightarrow JIC_0/(IJ+JI)IC_0$$

De plus, Ψ est un surjectif.

2. *L'homomorphisme de J dans JC_0 qui envoie X sur Xe_0 induit un homomorphisme*

$$\Phi : J/J^2 \longrightarrow JC_0/(IJ+JI)IC_0$$

De plus, Φ est injectif.

3. *L'homomorphisme Φ induit une section de la projection de $JC_0/(IJ+JI)IC_0$ sur JC_0/JIC_0. C'est-à-dire :*

$$\begin{tikzcd} JC_0/(IJ+JI)IC_0 \arrow[r] & JC_0/JIC_0 \arrow[r] & 0 \\ & J/J^2 \arrow[ul, dashed, "\Phi"] \arrow[u, "\cong"'] & \end{tikzcd}$$

4. *On a le diagramme suivant*

$$\begin{tikzcd} 0 \arrow[r] & JIC_0/(IJ+JI)IC_0 \arrow[r] & JC_0/(IJ+JI)IC_0 \arrow[r] & JC_0/JIC_0 \arrow[r] & 0 \\ 0 \arrow[r] & J/J^2 + (IF_{3/2}S_2^1) \otimes I/I^2 \arrow[r] \arrow[u, "\Psi", "\cong"'] & JC_0/(IJ+JI)IC_0 \arrow[r, "\mathrm{Id}_J\,\epsilon"'] \arrow[u, "="] & J/J^2 \arrow[r] \arrow[u, "\cong"'] \arrow[ul, dashed, "\Phi"'] & 0 \end{tikzcd}$$

où les deux lignes sont des suites exactes courtes scindées.

Démonstration.

1. D'après le lemme précédent, J^2 et $(IF_{3/2}S_2^1)I$ sont inclus dans $(IJ+JI)I$. Ainsi, on en déduit que l'homomorphisme surjectif $J \otimes I$ dans $JIC_0/(IJ+JI)IC_0$ qui envoie $X \otimes Y$ sur XYe_0, passe au quotient en un homomorphisme

$$\Psi : \ J/J^2 + (IF_{3/2}S_2^1) \otimes I/I^2 \longrightarrow JIC_0/(IJ+JI)IC_0$$

surjectif.

2. De l'inclusion de J dans I^2, on déduit que Φ est bien défini. L'injectivité se déduit du diagramme suivant

$$\begin{tikzcd} 0 \arrow[r] & H_1(F_1S_2^1, \mathbb{Z}_p) \arrow[rr, "\iota"] \arrow[dr, "\Phi"] & & H_0(F_1S_2^1, N_0) \arrow[r, "\mathrm{pr}"] & (IH) \arrow[r] & 0 \\ & & N_0/(IJ+JI)N_0 \arrow[ur, two heads] & & & \end{tikzcd}$$

Le fait que la première ligne du diagramme est exacte a été vu dans la proposition-définition 2.20.

3. C'est immédiat par définition de Φ et le lemme 2.21 pour identifier J/J^2 avec JC_0/JIC_0.
4. La construction du diagramme se déduit des points précédents.

$\square$

Lemme 2.32. *L'homomorphisme*

$$\mathrm{gr}_1 S_2^1 \underset{\mathbb{F}_p}{\otimes} \mathrm{gr}_{1/2} S_2^1 \ \longrightarrow\ J/J^2 + (IF_{3/2}S_2^1) \underset{\mathbb{Z}_p}{\otimes} I/I^2$$

qui envoie la classe de $f \otimes g$ sur $(f-e)\otimes(g-e)$, est un isomorphisme.

Démonstration. Rappelons que pour tout pro-p-groupe G, on a $(IG)/(IG)^2 \cong G/\overline{[G,G]}$ (lemme 6.8.6 [RZ10]). D'après le corollaire 1.20, $(S_2^1)_{\mathrm{ab}}$ est égal au quotient $\mathrm{gr}_{1/2} S_2^1$ et l'homomorphisme

$$(S_2^1)_{\mathrm{ab}} = \mathrm{gr}_1 S_2^1 \longrightarrow I/I^2$$

qui envoie la classe de g sur la classe de $g-e$ est un isomorphisme. De même, l'homomorphisme

$$(F_1 S_2^1)_{\mathrm{ab}} = F_1 S_2^1 /_{F_{5/2} S_2^1} \longrightarrow J/_{J^2}$$

qui envoie la classe de f sur la classe de $f-e$, est un isomorphisme. D'autre part, dans le quotient $J/_{J^2 + (IF_{3/2}S_2^1)}$ par rapport au quotient $J/_{J^2}$, on ajoute la relation $f = e$ pour tout $f \in F_{3/2}S_2^1$. D'où, l'homomorphisme

$$\mathrm{gr}_1 S_2^1 = F_1 S_2^1 /_{F_{3/2} S_2^1} \longrightarrow J/_{J^2 + (IF_{3/2}S_2^1)}$$

est aussi un isomorphisme et on a le lemme. □

Le résultat suivant donne une précision sur l'homomorphisme Ψ, mais ce fait ne sera pas utilisé dans la suite.

Lemme 2.33. *L'homomorphisme*

$$\Psi : J/_{J^2 + (IF_{3/2}S_2^1)} \otimes I/_{I^2} \longrightarrow JIC_0/_{(IJ+JI)IC_0}$$

est un isomorphisme.

Démonstration. Il nous reste à montrer que Ψ est injectif. On vient de voir dans le lemme précédent que $\mathrm{gr}_1 S_2^1 \otimes \mathrm{gr}_{1/2} S_2^1$ est isomorphe à $J/_{J^2 + (IF_{3/2}S_2^1)} \otimes I/_{I^2}$. En particulier $(c_0-e)\otimes(a_0-e)$ et $(c_0-e)\otimes(b_0-e)$ déterminent une $\mathbb{F}_p$-base de $J/_{J^2 + (IF_{3/2}S_2^1)} \otimes I/_{I^2}$ et l'homomorphisme Ψ les envoie sur $(c_0-e)(a_0-e)$ et $(c_0-e)(b_0-e)$ respectivement. Ainsi, pour montrer que Ψ est injectif, il suffit de montrer que les deux éléments précédents sont linéairement indépendants dans le $\mathbb{F}_p$-espace vectoriel $JIC_0/_{(IJ+JI)IC_0}$.
Posons $P = S_2^1/_{F_{3/2}S_2^1}$, c'est un groupe d'ordre p^3. Posons $\mathcal{I} = \ker(\mathbb{F}_p[P] \to \mathbb{F}_p)$ l'idéal d'augmentation de $\mathbb{F}[P]$ et

$$\mathrm{gr}_*(\,\mathbb{F}_p[P]\,) = \bigoplus_{k\geq 0} \mathcal{I}^k/_{\mathcal{I}^{k+1}}$$

Comme $J \subset I^2$, on déduit l'existence de l'homomorphisme

$$JI/_{(IJ+JI)} \to \mathcal{I}^3/_{\mathcal{I}^4}$$

Montrons que $(c_0-e)(a_0-e)$ et $(c_0-e)(b_0-e)$ sont linéairement indépendants dans $\mathcal{I}^3/_{\mathcal{I}^4}$. Pour ce faire, nous allons appliquer le théorème de Jennings-Quillen (théorème 3.14.6 [Ben98]) au p-groupe P. Notons x, y et z les classes de a_0, b_0 et c_0 dans P respectivement. Le groupe P est engendré par x et y d'ordres p et $z = [x,y]$ qui est aussi d'ordre p (P est un groupe extra-spécial d'ordre p^3). Ainsi, le sous-groupe engendré par les commutateurs $[P,P]$ est égal $\mathbb{Z}/_p\, z$ le centre de P et $P^p = \{e\}$. Avec les notations de la section 3.14 *Modules for p-groups* de [Ben98], la filtration de P par les sous-groupes de dimension [4] est donc

$$\{e\} = \Gamma_3(P) \quad \subset \quad \Gamma_2(P) = \mathbb{Z}/_p\, z \quad \subset \quad \Gamma_1(P) = P$$

Ainsi,

$$\mathrm{Jen}_*(P) = \bigoplus_{r\geq 0} \Gamma_r(P)/_{\Gamma_{r+1}(P)} = \mathrm{gr}_{1/2} S_2^1 \oplus \mathrm{gr}_1 S_2^1$$

4. "Dimension subgroups"

Alors, d'après le théorème de Jennings-Quillen, on a un isomorphisme d'algèbres graduées

$$U\ \mathrm{Jen}_*(S_2^1/_{F_{3/2}S_2^1}) \longrightarrow \mathrm{gr}_*\ \mathbb{F}_p[S_2^1/_{F_{3/2}}]$$

En particulier, on en déduit que

$$(\mathrm{gr}_{1/2}\, S_2^1)^{\otimes 3} \quad \oplus \quad \mathrm{gr}_1\, S_2^1 \otimes \mathrm{gr}_{1/2}\, S_2^1 \quad \cong \quad \mathcal{I}^3/_{\mathcal{I}^4}$$

et donc que $(z-e)(x-e)$ et $(z-e)(y-e)$ sont linéairement indépendants. D'où Ψ est un injectif. ☐

Remarque 2.34. *De l'existence des homomorphismes*

$$\mathrm{gr}_1\, S_2^1 \otimes \mathrm{gr}_{1/2}\, S_2^1 \xrightarrow{\cong} J/_{J^2} + (IF_{3/2}S_2^1) \ \otimes\ I/_{I^2} \xrightarrow{\Phi} JIC_0/_{(IJ+JI)IC_0}$$

et

$$F_1 S_2^1/_{F_{5/2}S_2^1} \xrightarrow{\cong} J/_{J^2} \xrightarrow{\Psi} JC_0/_{(IJ+JI)IC_0}$$

On déduit que quels que soient $g \in S_2^1$, $f \in F_1 S_2^1$ et $\lambda, \mu \in \mathbb{Z}_p$, on a

$$\begin{aligned} (f^\lambda - e)(g^\mu - e) &\equiv \lambda\mu(f-e)(g-e) \mod (IJ+JI)N_0 \\ f^\lambda - e &\equiv \lambda(f-e) \mod (IJ+JI)N_0 \end{aligned}$$

Ces résultats seront utilisés dans la sous-section suivante.

2.2.3 Le module N_0 quotienté par $(IJ+JI)N_0$

Rappelons qu'en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module N_0 est isomorphe à l'idéal d'augmentation I. Ainsi, de l'inclusion de $(IJ+JI)I$ dans JI, on déduit le diagramme suivant :

$$\begin{tikzcd} 0 \arrow[r] & \ker \arrow[r] \arrow[d] & C_1/_{(IJ+JI)C_1} \arrow[r, "\partial_{1*}"] \arrow[d] & IC_0/_{(IJ+JI)IC_0} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & K_{v,w} \arrow[r] & C_1/_{JC_1} \arrow[r, "\phi_{v,w}"] & IC_0/_{JC_0} \arrow[r] & 0 \end{tikzcd}$$

Ainsi, d'après le corollaire 2.28, les éléments du noyau de l'homomorphisme sur la première ligne du diagramme précédent sont des combinaisons linéaires de $\mathcal{N}(a_0)(e_1)_+$, $\mathcal{N}(b_0)(e_1)_-$ et $w(e_1)_+ - v(e_1)_-$.

Pour pouvoir déterminer nos deux générateurs κ_+ et κ_- vérifiant les conditions (2.3), nous allons procéder en trois étapes :

- Nous allons déterminer une relation entre $\mathcal{N}(a_0)v$ (resp. $\mathcal{N}(b_0)w$) et $a_0^p - e$ (resp. $b_0^p - e$) modulo $(IJ+JI)I$ (proposition 2.38).
- Nous allons déterminer une relation entre $(a_0-e)(wv-vw)$ (resp. $(b_0-e)(wv-vw)$) et a_0, b_0 et c_0 (proposition 2.42).
- Des relations précédentes, on en déduira des solutions κ_+ et κ_- (théorème 2.43).

Lemme 2.35. *Soit $g \in S_2^1$,*

a) Le groupe $\mathcal{N}(g)JI$ est inclus dans $(IJ+JI)I$.

b) Le groupe $\mathcal{N}(g)(IF_{3/2}S_2^1)$ est inclus dans $(IJ+JI)I$.

Démonstration. a) Soient $f \in F_1 S_2^1$ et $h \in S_2^1$, alors

$$\begin{aligned} \mathcal{N}(g)(f-e)(h-e) &\equiv \sum_{i=0}^{p-1}(g-e+e)(f-e)(h-e) \\ &\equiv p(f-e)(h-e) \\ &\equiv 0 \quad (IJ+JI)I \end{aligned}$$

Pour la dernière congruence, on a utilisé le fait que $H_0(S_2^1, I) \cong H_1(S_2^1, \mathbb{Z}_p)$ est de p-torsion et donc que $pI \subset I^2$. On en déduit l'inclusion.

b) Soit $f \in F_{3/2}S_2^1$, alors, comme d'après le lemme 2.30 $(IF_{3/2}S_2^1)I$ est inclus dans $(IJ+JI)I$, on a

$$\begin{aligned} \mathcal{N}(g)(f-e) &= \sum_{i=0}^{p-1} g^i(f-e)g^{-i} - \sum_{i=0}^{p-1} g^i \underbrace{(f-e)(g^{-i}-e)}_{\in (IF_{3/2}S_2^1)I} \\ &\equiv \sum_{i=0}^{p-1}(g^i f g^{-i} - e) \quad \mod (IJ+JII) \end{aligned}$$

Ainsi, en utilisant l'homomorphisme $\Phi : H_1(F_1S_2^1, \mathbb{Z}_p) \cong F_1S_2^1/F_{5/2}S_2^1 \to I/(IJ+JI)I$, dans $I/(IJ+JI)I$, on a

$$\mathcal{N}(g)(f-1) \quad = \quad \sum_{i=0}^{p-1}(g^i f g^{-i} - e) = \Phi(\prod_{i=0}^{p-1} g^i f g^{-i}) = \Phi(\prod_{i=0}^{p-1} f[f^{-1}, g^i]\,) = \Phi(f^p \prod_{i=0}^{p-1}[f^{-1}, g^i]\,)$$

L'élément f appartient à $F_{3/2}S_2^1$ et comme S_2^1 est p-valué, f^p appartient à $F_{5/2}S_2^1$ et sa classe est triviale dans le quotient $F_1S_2^1/F_{5/2}S_2^1$. De plus, la classe de $[f^{-1}, g^i]$ appartient au sous-groupe $F_2S_2^1/F_{5/2}S_2^1 = \mathrm{gr}_2\, S_2^1$. En référence au lemme 1.8 sur le commutateur, on se donne $g_1, f_3 \in \mathbb{W}$ tels que $g \equiv 1 + g_1 S \mod (S^2)$ et $f \equiv 1 + f_3 S^3 \mod (S^4)$. Au passage, notons que $g^i \equiv 1 + i g_1 S \mod (S^2)$. Dans $\mathcal{O}_2$ modulo (S^5), on a alors,

$$\begin{aligned} \prod_{i=0}^{p-1}[f, g^i] &\equiv 1 + \sum_{i=0}^{p-1} i(f_3 g_1^p - f_3^p g_1)S^4 \\ &\equiv 1 + p\,\frac{p-1}{2}(f_3 g_1^p - f_3^p g_1)\, S^4 \\ &\equiv 1 \quad \mod (S^5) \end{aligned}$$

D'où, le produit $\prod g^i f g^{-i}$ est trivial dans $F_1S_2^1/F_{5/2}S_2^1$.

Ainsi, dans le quotient $I/(JI+IJ)I$, l'élément $\mathcal{N}(g)(f-1)$ est trivial. D'où l'on déduit le second point du lemme.

□

Avant de considérer les éléments v et w, nous avons encore besoin d'un petit lemme. On désigne par $Z(S_2)$ le centre $1 + p\mathbb{Z}_p$ de S_2 et on rappelle que $PS_2 = S_2/1+p\mathbb{Z}_p \cong S_2^1$ (lemme 1.13).

Lemme 2.36. *Soit $g \in S_2^1$. Soient $0 \le l, m < p$ tels que $g = 1 + (l\epsilon_+ + m\epsilon_-)S \mod (S^2)$. Alors*

$$g \equiv a_0^l b_0^m c_0^{-lm/2} \equiv b_0^m a_0^l c_0^{lm/2} \quad \mod F_{3/2}S_2^1$$

Démonstration. Soient $0 \leq l, m \leq p-1$. Modulo (S^3),

$$\begin{aligned}(1+\epsilon_- S)^{-m}(1+\epsilon_+ S)^{-l} &\equiv (1 - m\epsilon_- S + \frac{m(m+1)}{2}\epsilon_-^2 S^2)\,(1 - l\epsilon_+ S - \frac{l(l+1)}{2}\epsilon_+^2 S^2) \\ &\equiv 1 - (l\epsilon_+ + m\epsilon_-)S + (\frac{m(m+1)}{2}\epsilon_+^2 + lm\epsilon_-\epsilon_+ - \frac{l(l+1)}{2}\epsilon_-^2)S^2\end{aligned}$$

d'où

$$\begin{aligned}&\Big(1+(l\epsilon_+ + m\epsilon_-)S\Big)(1+\epsilon_- S)^{-m}\,(1+\epsilon_- S)^{-l} \\ \equiv\; &\Big(1+(l\epsilon_+ + m\epsilon_-)S\Big)\,\Big(1 - (l\epsilon_+ + m\epsilon_-)S + (\frac{m(m+1)}{2}\epsilon_+^2 + lm\epsilon_-\epsilon_+ - \frac{l(l+1)}{2}\epsilon_-^2)S^2\Big) \\ \equiv\; &1 + (\frac{m(m+1)}{2}\epsilon_+^2 + lm\epsilon_-\epsilon_+ - \frac{l(l+1)}{2}\epsilon_-^2)S^2 \\ \equiv\; &\Big(1 + lm\epsilon_-\epsilon_+ S^2\Big)\,\Big(1 + \underbrace{(\frac{m(m+1)}{2}\epsilon_+^2 - \frac{(l(l+1)}{2}\epsilon_-^2)}_{\in\mathbb{Z}_p}\,p\Big) \bmod (S^3)\end{aligned}$$

Or, les éléments a_0, b_0 et c_0 de S_2^1 sont tels que

$$\begin{aligned}a_0 &\equiv 1+\epsilon_+ S \mod Z(S_2) \\ b_0 &\equiv 1+\epsilon_- S \mod Z(S_2) \\ c_0 &= [a_0, b_0] \equiv 1 - 2\epsilon_+\epsilon_- S^2 \mod (S^3)\end{aligned}$$

Ainsi, on en déduit que

$$g\, b_0^{-m}\, a_0^{-l} \equiv c_0^{-lm/2} \mod F_{3/2}S_2^1 \,.\, Z(S_2)$$

Comme c_0 commute avec a_0 et b_0 modulo $F_{3/2}S_2^1$, on a

$$g \equiv a_0^l\, b_0^m\, c_0^{-lm/2} \mod F_{3/2}S_2^1 \,.\, Z(S_2)$$

C'est-à-dire $g^{-1}a_0^l\, b_0^m\, c_0^{-lm/2}$ appartient à $S_2^1 \cap (F_{3/2}S_2^1 \,.\, Z(S_2)) = F_{3/2}S_2^1$ et donc on a la première congruence. De même, on obtient la seconde congruence. □

En particulier, on en déduit que

$$v \equiv \frac{1}{p+1}\sum_{i=0}^{p} \lambda_i\,(a_0^{\lambda_{-i}} b_0^{\mu_{-i}} c_0^{\frac{-1}{2}\lambda_{-i}\mu_{-i}} - e) + \mu_i(a_0^{\lambda'_{-i}} b_0^{\mu'_{-i}} c_0^{\frac{-1}{2}\lambda'_{-i}\mu'_{-i}} - e) \tag{2.9}$$

$$w \equiv \frac{1}{p+1}\sum_{i=0}^{p} \lambda'_i\,(a_0^{\lambda_{-i}} b_0^{\mu_{-i}} c_0^{\frac{-1}{2}\lambda_{-i}\mu_{-i}} - e) + \mu'_i(a_0^{\lambda'_{-i}} b_0^{\mu'_{-i}} c_0^{\frac{-1}{2}\lambda'_{-i}\mu'_{-i}} - e) \tag{2.10}$$

modulo $(IF_{3/2}S_2^1)C_0$.

Lemme 2.37.
a) Il existe $A \in \mathbb{Z}_p[\![S_2^1]\!]$, tels que

$$\begin{aligned}A &\equiv 1 \mod I \\ v &\equiv (a_0 - e)A \mod (IF_{3/2}S_2^1)\mathbb{Z}_p[\![S_2^1]\!] + JI\end{aligned}$$

b) Il existe $B \in \mathbb{Z}_p[\![S_2^1]\!]$, tels que

$$\begin{aligned}B &\equiv 1 \mod I \\ w &\equiv (b_0 - e)B \mod (IF_{3/2}S_2^1)\mathbb{Z}_p[\![S_2^1]\!] + JI\end{aligned}$$

Démonstration. Soient i, j, k trois entiers, alors

$$\begin{aligned} a_0^i b_0^j c_0^k - e &\equiv (a_0^i - e) b_0^j c_0^k + (c_0^k - e)(b_0^j - e) + (b_0^j - e) + (c_0^k - e) \mod (IF_{3/2}S_2^1)C_0 \\ &\equiv (a_0 - e)A_{i,j,k} + D_{i,j,k} + B_{i,j,k} + (c_0 - e)C_{i,j,k} \end{aligned}$$

où $A_{i,j,k}, B_{i,j,k}, C_{i,j,k} \in \mathbb{Z}_p[\![S_2^1]\!]$ et $D_{i,j,k} \in JI$. Ainsi, en revenant à l'identité (2.9), on déduit que

$$v \equiv (a_0 - e)A + D + B + (c_0 - e)C \mod (IF_{3/2}S_2^1)C_0$$

pour certains éléments A, B, C, D dans $\mathbb{Z}_p[\![S_2^1]\!]$. De plus,

$$\begin{aligned} A &= \frac{1}{p+1} \sum_{i=0}^{p} \lambda_i \, (e + \ldots + a_0^{\lambda_{-i}-1}) b_0^{\mu_{-i}} c_0^{\frac{-1}{2}\lambda_{-i}\mu_{-i}} + \mu_i (e + \ldots + a_0^{\lambda'_{-i}-1}) b_0^{\mu'_{-i}} c_0^{\frac{-1}{2}\lambda'_{-i}\mu'_{-i}} \\ &\equiv \frac{1}{4(p+1)} \sum_{i=0}^{p} l_i^2 - m_i^2 \equiv 1 \mod I \end{aligned}$$

et d'après le lemme 2.25,

$$\begin{aligned} C &= \frac{1}{p+1} \sum_{i=0}^{p} \lambda_i (e + \ldots + c_0^{\frac{-1}{2}\lambda_{-i}\mu_{-i}-1}) + \mu_i (e + \ldots + c_0^{\frac{-1}{2}\lambda'_{-i}\mu'_{-i}-1}) \\ &\equiv \frac{-1}{8(p+1)} \sum_{i=0}^{p} -l_i^2 m_i - m_i^2 l_i \equiv 0 \mod I \end{aligned}$$

Donc $(c_0 - e)C \in JI$. En utilisant la formule d'interpolation de la puissance (proposition A.3), on a

$$\begin{aligned} B &= \frac{1}{p+1} \sum_{i=0}^{p} \lambda_i \, (b_0^{\mu_{-i}} - e) + \mu_i (b_0^{\mu'_{-i}} - e) \\ &= \frac{1}{p+1} \sum_{i=0}^{p} l_i \sum_{j \geq 0} \binom{-\frac{\epsilon_+}{\epsilon_-} m_i}{j} (b_0 - e)^j + m_i \binom{l_i}{j} (b_0 - e)^j \\ &= 0 \end{aligned}$$

où pour la dernière identité, nous avons utilisé le lemme 2.25. De même, on montre la seconde propriété. □

Proposition 2.38.

1. $\mathcal{N}(a_0)v \equiv a_0^p - e \mod (IJ + JI)I$.
2. $\mathcal{N}(b_0)w \equiv b_0^p - e \mod (IJ + JI)I$.

Démonstration. D'après le lemme 2.35 et avec les notations du lemme précédent, on a

$$\mathcal{N}(a_0)v \equiv (a_0^p - e)A \mod (IJ + JI)I$$

En revenant aux inclusions du lemme 2.30, on note que $(IF_{3/2}S_2^1)I \subset (IJ + JI)I$, d'où

$$\mathcal{N}(a_0)v \equiv \underbrace{(a_0^p - e)}_{\in (IF_{3/2}S_2^1)} \underbrace{A}_{\equiv 1 \bmod I} \equiv a_0^p - e \mod (IJ + JI)I$$

La seconde congruence de la proposition se démontre de manière analogue. □

Nous allons maintenant approximer le commutateur $wv - vw$.

Lemme 2.39. *On a,*

$$wv - vw \equiv e - c_0 + 2\epsilon_-^2(a_0^p - e) + 2\epsilon_+^2(b_0^p - e)$$

modulo $(IF_2S_2^1)\mathbb{Z}_p[\![S_2^1]\!] + JI$.

Démonstration. Pour alléger les notations, notons $\{.,.\}$ le commutateur dans l'algèbre $\mathbb{Z}_p[\![S_2^1]\!]$ (i.e : $\{X,Y\} := XY - YX$). L'élément $wv - vw$ est égal à

$$\begin{aligned}
& \frac{1}{(p+1)^2}\sum_{i,j=0}^{p}\Big(\lambda'_i\lambda_j\{a_i - e, a_j - e\} + \lambda'_i\mu_j\{a_i - e, b_j - e\} \\
& \quad + \mu'_i\lambda_j\{b_i - e, a_j - e\} + \mu'_i\mu_j\{b_i - e, b_j - e\}\Big) \\
= \; & \frac{1}{(p+1)^2}\sum_{i,j=0}^{p}\Big(\lambda'_i\lambda_j([a_i,a_j] - e)a_ja_i + \lambda'_i\mu_j([a_i,b_j] - e)b_ja_i \\
& \quad + \mu'_i\lambda_j([b_i,a_j] - e)a_jb_i + \mu'_i\mu_j([b_i,b_j] - e)b_jb_i\Big) \\
\equiv \; & \sum_{i,j=0}^{p}\lambda'_i\lambda_j([a_i,a_j] - e) + \lambda'_i\mu_j([a_i,b_j] - e) + \mu'_i\lambda_j([b_i,a_j] - e) + \mu'_i\mu_j([b_i,b_j] - e) \mod JI
\end{aligned}$$

On note X cette dernière expression. Rappelons que, $a_i \equiv 1 + \omega^{(p-1)i}\epsilon_+S$ et $b_i \equiv 1 + \omega^{(p-1)i}\epsilon_-S$ modulo le centre $Z(S_2)$ de S_2. Posons $m_{i,s} = \omega^{(1-p)i} + s\omega^{(p-1)i}$ pour $s = \pm 1$, alors

$$\begin{cases}
\lambda_j = \frac{\epsilon_+}{2\epsilon_+}(\omega^{(1-p)j} + \omega^{(p-1)j}) = \frac{\epsilon_+}{2\epsilon_s}\, m_{j,s} & \text{où } s = 1\\
\mu_j = \frac{\epsilon_+}{2\epsilon_-}(\omega^{(1-p)j} - \omega^{(p-1)j}) = \frac{\epsilon_+}{2\epsilon_s}\, m_{j,s} & \text{où } s = -1
\end{cases}$$

$$\begin{cases}
\lambda'_i = \frac{\epsilon_-}{2\epsilon_+}(\omega^{(1-p)i} - \omega^{(p-1)i}) = \frac{\epsilon_t}{2\epsilon_+}\, m_{i,t} & \text{où } t = -1\\
\mu'_i = \frac{\epsilon_-}{2\epsilon_+}(\omega^{(1-p)i} + \omega^{(p-1)i}) = \frac{\epsilon_t}{2\epsilon_+}\, m_{i,t} & \text{où } t = 1
\end{cases}$$

D'où, X est égal à

$$\begin{aligned}
& \sum_{s,t=\pm 1}\sum_{i,j=0}^{p}\frac{\epsilon_t}{4\epsilon_s}m_{i,t}\, m_{j,s}\,\Big([1 + \omega^{(p-1)i}\epsilon_{-t}S, 1 + \omega^{(p-1)j}\epsilon_sS] - e\Big) \\
= \; & \sum_{s,t=\pm 1}\frac{\epsilon_t}{4\epsilon_s}\sum_{i,j=0}^{p}(\omega^{(1-p)i} + t\omega^{(p-1)i})(\omega^{(1-p)j} + s\omega^{(p-1)j})\,\Big([1 + \omega^{(p-1)i}\epsilon_{-t}S, 1 + \omega^{(p-1)j}\epsilon_sS] - e\Big)
\end{aligned}$$

Pour alléger les notations, posons $\xi = \omega^{1-p}$, alors

$$X \;=\; \sum_{s,t=\pm 1}\frac{\epsilon_t}{4\epsilon_s}\sum_{i,j=0}^{p}\Big(\xi^{i+j} + s\xi^{i-j} + t\xi^{j-i} + st\xi^{-i-j}\Big)\,\big([1 + \xi^{-i}\epsilon_{-t}S, 1 + \xi^{-j}\epsilon_sS] - e\big)$$

En particulier X appartient à J. De l'isomorphisme de J/J^2 sur $(F_1S_2^1)_{\mathrm{ab}} = F_1S_2^1/F_{5/2}S_2^1$, on déduit que $J/J^2 + (IF_2S_2^1)$ est isomorphe à $F_1S_2^1/F_2S_2^1$. D'autre part, en revenant à la définition de la filtration de S_2^1 : $F_{\frac{i}{2}}S_2^1 = \{g \in S_2^1 :\ g \equiv 1 \mod (S^i)\}$, on remarque que l'homomorphisme $F_{\frac{i}{2}}S_2^1/F_iS_2^1$ dans $\mathrm{gr}_{\frac{i}{2}}S_2^1 \oplus \ldots \oplus \mathrm{gr}_{\frac{i-1}{2}}$, qui envoie la classe de $g = 1 + g_iS^i + \ldots + g_{2i-1}S^{2i-1} + \ldots$ sur $(g_i, \ldots, g_{2i-1})$, est bien définie et induit un isomorphisme de groupes. On pose,

$$\varphi :\ J/J^2 + (IF_2S_2^1) \xrightarrow{\cong} F_1S_2^1/F_2S_2^1 \xrightarrow{\cong} \mathrm{gr}_1\, S_2^1 \oplus \mathrm{gr}_{3/2}\, S_2^1$$

l'homomorphisme tel que pour tout $g = 1 + g_2S^2 + g_3S^3 \mod (S^4)$, on a $\varphi(g-e) = (g_2, g_3)$. Remarquons que

$$\xi^p = \omega^{(1-p)p} = \omega^{p-1} = \xi^{-1}$$

et que $\epsilon_s^\sigma = s\epsilon_s$. D'après le lemme 1.9 sur le crochet de Lie dans $\mathcal{O}_2$, on a

$$[1+\xi^{-i}\epsilon_{-t}S, 1+\xi^{-j}\epsilon_s S] \equiv 1 + \epsilon_s\epsilon_{-t}(s\xi^{j-i} + t\xi^{i-j})S^2 - \epsilon_s\epsilon_{-t}(s\xi^{j-i}+t\xi^{i-j})(\xi^{-i}\epsilon_s + \xi^{-j}\epsilon_{-t})S^3$$

modulo (S^4). Ainsi,

$$\varphi([1+\xi^{-i}\epsilon_s S, 1+\xi^{-j}\epsilon_{-t}S] - e) = \Big(\epsilon_s\epsilon_{-t}(s\xi^{j-i}+t\xi^{i-j}),\ -\epsilon_s\epsilon_{-t}(s\xi^{j-i}+t\xi^{i-j})(\xi^{-i}\epsilon_s + \xi^{-j}\epsilon_{-t}) \Big)$$

et $\varphi(X)$ est égale à

$$\sum_{s,t=\pm1} \frac{\epsilon_t\epsilon_{-t}}{4} \sum_{i,j=0}^{p} \Big(\xi^{i+j} + s\xi^{i-j} + t\xi^{j-i} + st\xi^{-i-j}\Big)\Big(s\xi^{j-i} + t\xi^{i-j}, -(s\xi^{j-i}+t\xi^{i-j})(\xi^{-i}\epsilon_s + \xi^{-j}\epsilon_{-t})\Big)$$

Maintenant, comme $\xi = \omega^{1-p}$ est une racine $p+1$-ème de l'unité [5], la première coordonnée de $\varphi(X)$ est égale à

$$\sum_{i,j=0}^{p} \Big(\xi^{i+j} + s\xi^{i-j} + t\xi^{j-i} + st\xi^{-i-j}\Big)\Big(s\xi^{j-i} + t\xi^{i-j}\Big) = s^2 + t^2 = 2$$

et la seconde coordonnée de $\varphi(X)$ est égale à,

$$\begin{aligned}
& \sum_{i,j=0}^{p} \Big(\xi^{i+j} + s\xi^{i-j} + t\xi^{j-i} + st\xi^{-i-j}\Big)\Big(-(s\xi^{j-i}+t\xi^{i-j})(\xi^{-i}\epsilon_s + \xi^{-j}\epsilon_{-t}) \Big) \\
= & \sum_{i,j=0}^{p} \Big(\xi^{i+j} + s\xi^{i-j} + t\xi^{j-i} + st\xi^{-i-j}\Big)\Big(s\xi^{j-2i} + s\xi^{-i} + t\xi^{-j} + t\xi^{i-2j} \Big) \\
= & \ 0
\end{aligned}$$

D'où,

$$\varphi(X) = (\sum_{s,t=\pm1} \frac{1}{2}\epsilon_{-s}\epsilon_s, 0) = (2\epsilon_+\epsilon_-, 0)$$

D'après le lemme 2.40,

$$\begin{aligned}
c_0 &\equiv 1 - 2\epsilon_+\epsilon_- S^2 + 2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+ S^3 \mod (S^4) \\
a_0^p &\equiv (1+\epsilon_+S)^p \equiv 1 + \epsilon_+ S^3 \mod (S^4) \\
b_0^p &\equiv (1+\epsilon_-S)^p \equiv 1 + \epsilon_- S^3 \mod (S^4)
\end{aligned}$$

Donc, comme ϵ_-^2 et ϵ_+^2 sont des entiers p-adiques,

$$\begin{aligned}
\varphi(c_0^{-1} - e + 2\epsilon_-^2(a_0^p - e) + 2\epsilon_+^2(b_0^p - e)) &= (2\epsilon_+\epsilon_-, -2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+) + (0, 2\epsilon_-^2\epsilon_+) + (0, 2\epsilon_+^2\epsilon_-) \\
&= (2\epsilon_+\epsilon_-, 0) \\
&= \varphi(X)
\end{aligned}$$

En résumé, on a bien

$$wv - vw \equiv e - c_0 + 2\epsilon_-^2(a_0^p - e) + 2\epsilon_+^2(b_0^p - e) \mod (IF_2S_2^1)\mathbb{Z}_p[\![S_2^1]\!] + J^2 + JI$$

Or, $J^2 \subset JI$, d'où la congruence du lemme. □

5. Il peut être utile de se souvenir que $\sum_{i=0}^{p} \xi^{ki} = 0$ si et seulement si $p+1$ divise k.

Avant de pouvoir considérer les éléments $(b_0 - e)(wv - vw)$ et $(a_0 - e)(wv - vw)$ modulo $(IJ + JI)I$, nous devons approximer certains commutateurs de S_1^1.

Lemme 2.40.

a) $c_0 \equiv 1 - 2\epsilon_+\epsilon_- S^2 + 2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+ S^3 \mod (S^4)$

b) $(1 + \epsilon_+ S)^p \equiv 1 + \epsilon_+ S^3 + \frac{p-1}{2}\epsilon_+^2 S^4 \mod (S^5)$

c) $(1 + \epsilon_- S)^p \equiv 1 + \epsilon_- S^3 - \frac{p-1}{2}\epsilon_-^2 S^4 \mod (S^5)$

d) $c_0^p \equiv 1 - 2\epsilon_+\epsilon_- S^4 \mod (S^5)$

Démonstration. Pour la première congruence, on applique le lemme 1.9.
Ensuite, on note que

$$(1 + \epsilon_+ S)^p \quad = \quad 1 + \epsilon_+ S^3 + \frac{p-1}{2}\epsilon_+^{p+1} S^4 + \frac{(p-1)(p-2)}{6}\epsilon_+^{1+p+p^2} S^5 \mod (S^5)$$

Comme $p > 3$, on déduit que les précédents coefficients sont entiers et donc la seconde congruence.
La troisième congruence se traite de manière analogue.
La dernière congruence résulte immédiatement du lemme 1.8. □

Lemme 2.41.

a) $[a_0, b_0^p] \equiv c_0^p \mod F_{5/2}S_2^1$.

b) $[b_0, a_0^p] \equiv c_0^{-p} \mod F_{5/2}S_2^1$.

c) $[a_0, c_0] \equiv b_0^{4\epsilon_+^2 p} c_0^{4\epsilon_+^2 p} \mod F_{5/2}S_2^1$.

d) $[b_0, c_0] \equiv a_0^{4\epsilon_-^2 p} c_0^{-4\epsilon_-^2 p} \mod F_{5/2}S_2^1$.

Démonstration. D'après le lemme 1.8 sur la structure d'algèbre de Lie mixte de S_2^1 et le lemme 2.40, dans $\mathcal{O}_2$,

$$\begin{aligned} [1 + \epsilon_+ S, 1 + \epsilon_- S^3] &\equiv 1 - 2\epsilon_-\epsilon_+ S^4 \equiv c_0^p \mod (S^5) \\ [1 + \epsilon_- S, 1 + \epsilon_+ S^3] &\equiv 1 + 2\epsilon_-\epsilon_+ S^4 \equiv c_0^{-p} \mod (S^5) \end{aligned}$$

Or, de l'homomorphisme injectif $S_2/_{F_{5/2}S_2} \to \left(\mathcal{O}_2/_{(S^5)}\right)^\times$, on déduit que

$$[a_0, b_0^p] \equiv c_0^p \mod F_{5/2}S_2 \,.\, Z(S_2) \quad \text{et} \quad [b_0, a_0^p] \equiv c_0^{-p} \mod F_{5/2}S_2 \,.\, Z(S_2)$$

Comme les éléments de part et d'autre de la congruence sont dans $S_2^1 \cong PS_2$, on déduit les deux premières congruences du lemme.
De même, mais en utilisant le lemme 1.9, donnant une approximation plus précise du commutateur, on a

$$\begin{aligned} & [1 + \epsilon_+ S, 1 - 2\epsilon_+\epsilon_- S^2 + 2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+ S^3] \\ \equiv\ & 1 + (\epsilon_+(-2\epsilon_-\epsilon_+)^\sigma - (-2\epsilon_-\epsilon_+)\epsilon_+)S^3 \\ & +(\epsilon_+(2(\epsilon_+ + \epsilon_-)\epsilon_-\epsilon_+)^\sigma - (2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+)\epsilon_+)S^4 \\ & -(\epsilon_+(-2\epsilon_-\epsilon_+)^\sigma - (-2\epsilon_-\epsilon_+)\epsilon_+)\epsilon_+^p S^4 \\ \equiv\ & 1 + 4\epsilon_-\epsilon_+^2 S^3 - 8\epsilon_-\epsilon_+^3 S^4 \mod (S^5) \\ \equiv\ & b_0^{4\epsilon_+^2 p} c_0^{4\epsilon_+^2 p} \mod F_{5/2}S_2^1 \,.\, Z(S_2) \end{aligned}$$

et

$$\begin{aligned} & [1+\epsilon_- S, 1-2\epsilon_+\epsilon_- S^2 + 2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+ S^3] \\ = \; & 1 + (\epsilon_-(-2\epsilon_-\epsilon_+)^\sigma - (-2\epsilon_-\epsilon_+)\epsilon_-)S^3 \\ & +(\epsilon_-(2(\epsilon_+ + \epsilon_-)\epsilon_-\epsilon_+)^\sigma - (2(\epsilon_- + \epsilon_+)\epsilon_-\epsilon_+)\epsilon_-^{\sigma^3})S^4 \\ & -(\epsilon_-(-2\epsilon_-\epsilon_+)^\sigma - (-2\epsilon_-\epsilon_+)\epsilon_-)\epsilon_-^p S^4 \\ = \; & 1 + 4\epsilon_-^2\epsilon_+ S^3 + 8\epsilon_-^3\epsilon_+ S^4)c_0 \mod (S^5) \\ = \; & a_0^{4\epsilon_-^2 p} c_0^{-4\epsilon_-^2 p} \quad \mod F_{5/2}S_2^1 \,.\, Z(S_2) \end{aligned}$$

D'où les deux dernières congruences du lemme. □

Proposition 2.42. *On a*

1. $(b_0 - e)(wv - vw) = -4\epsilon_-^2(a_0^p - e) - (c_0 - e)(b_0 - e) + 2p\epsilon_-^2(c_0 - e) \mod (IJ + JI)I$

2. $(a_0 - e)(wv - vw) = -4\epsilon_+^2(b_0^p - e) - (c_0 - e)(a_0 - e) - 2p\epsilon_+^2(c_0 - e) \mod (IJ + JI)I$

Démonstration. Ainsi, d'après le lemme précédent et le lemme 2.41 donnant des sous-groupes de $(IJ + JI)I$, on a

$$\begin{aligned} (g-e)(wv-vw) &= (g-e)\Big(e - c_0 + 2\epsilon_-^2(a_0^p - e) + 2\epsilon_+^2(b_0^p - e)\Big) \\ &\equiv (e - c_0)(g-e) + \underbrace{\Big(2\epsilon_-^2(a_0^p - e) + 2\epsilon_+^2(b_0^p - e)\Big)}_{\in (IF_{3/2}S_2^1)}\underbrace{(g-e)}_{\in I} \\ & \quad -([g, c_0] - e)c_0 g + 2\epsilon_-^2([g, a_0^p] - e) + 2\epsilon_+^2([g, b_0^p] - e) \\ &\equiv (e - c_0)(g-e) - ([g, c_0] - e) + 2\epsilon_-^2([g, a_0^p] - e) + 2\epsilon_+^2([g, b_0^p] - e) \end{aligned}$$

modulo *modulo*$(IJ + JI)I$. D'après le lemme 2.41 et en utilisant l'isomorphisme $F_1S_2^1/F_{5/2}S_2^1 \cong J/J^2$, on a

$$\begin{aligned} [b_0, c_0] - e &\equiv 4\epsilon_-^2(a_0^p - e) - 4p\epsilon_-^2(c_0 - e) \mod J^2 \\ [a_0, c_0] - e &\equiv 4\epsilon_+^2(b_0^p - e) + 4p\epsilon_+^2(c_0 - e) \mod J^2 \\ [a_0, b_0^p] - e &\equiv p(c_0 - e) \mod J^2 \\ [b_0, a_0^p] - e &\equiv -p(c_0 - e) \mod J^2 \end{aligned}$$

De plus, $J^2 \subseteq (IJ + JI)I$, d'où

$$\begin{aligned} (b_0 - e)(wv - vw) &\equiv (e - c_0)(b_0 - e) - ([b_0, c_0] - e) + 2\epsilon_-^2([b_0, a_0^p] - e) + 2\epsilon_+^2([b_0, b_0^p] - e) \\ &\equiv -(c_0 - e)(b_0 - e) - 4\epsilon_-^2(a_0^p - e) + 4p\epsilon_-^2(c_0 - e) - 2p\epsilon_-^2(c_0 - e) \\ &\equiv -(c_0 - e)(b_0 - e) - 4\epsilon_-^2(a_0^p - e) + 2p\epsilon_-^2(c_0 - e) \mod (IJ + JI)I \end{aligned}$$

De même, on montre la seconde congruence. □

En résumé, dans $I/(IJ + JI)I$, on a

$$\begin{aligned} \mathcal{N}(a_0)v + \frac{1}{4\epsilon_-^2}(b_0 - e)(wv - vw) &= \frac{-1}{4\epsilon_-^2}(c_0 - e)(b_0 - e) + \frac{p}{2}(c_0 - e) \\ \mathcal{N}(b_0)w + \frac{1}{4\epsilon_+^2}(a_0 - e)(wv - vw) &= \frac{-1}{4\epsilon_+^2}(c_0 - e)(a_0 - e) - \frac{p}{2}(c_0 - e) \end{aligned}$$

Rappelons que $(e_1)_\pm = 1 \otimes \epsilon_\pm$ dans $C_1 \cong \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$ et que $((e_1)_+, (e_1)_-)$ est une base de C_1 en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module.

Théorème-Définition 2.43. *On pose*

$$\begin{aligned}
\kappa_+ &:= \mathcal{N}(a_0)(e_1)_+ + \frac{1}{4\epsilon_-^2}\Big((b_0-e)(w(e_1)_+ - v(e_1)_-) + (c_0-e)(e_1)_-\Big) + \frac{p}{2}(w(e_1)_+ - v(e_1)_-)\\
\kappa_- &:= \mathcal{N}(b_0)(e_1)_- + \frac{1}{4\epsilon_+^2}\Big((a_0-e)(w(e_1)_+ - v(e_1)_-) + (c_0-e)(e_1)_+\Big) - \frac{p}{2}(w(e_1)_+ - v(e_1)_-)
\end{aligned}$$

Ce sont deux éléments de C_1, qui à l'addition d'un élément de $(IJ+JI)C_1$ près, déterminent deux éléments de N_1.

Démonstration. D'après la proposition 2.14,

$$\partial_1(e_1)_+ \equiv (a_0-e)e_0 \mod IN_0 \quad \text{et} \quad \partial_1(e_1)_- \equiv (b_0-e)e_0 \mod IN_0$$

D'où

$$\begin{aligned}
\partial_1(\kappa_+) &\equiv \mathcal{N}(a_0)ve_0 + \frac{1}{4\epsilon_-^2}\left((b_0-e)(wv-vw) + (c_0-e)(b_0-e)\right)e_0 - \frac{p}{2}(wv-vw)e_0\\
&\equiv \frac{p}{2}(c_0-e)e_0 + \frac{p}{2}(wv-vw)e_0\\
&\equiv -\partial_1(\kappa_-) \mod (IJ+JI)N_0
\end{aligned}$$

Ainsi, en revenant à la congruence du lemme 2.39 et en utilisant certaines des inclusions du lemme 2.30, on a

$$\begin{aligned}
p(wv-vw) &\equiv -p(c_0-e) + 2\epsilon_-^2\underbrace{p(a_0^p-e)}_{p(IF_{3/2}S_2^1)} + 2\epsilon_+^2\underbrace{p(b_0^p-e)}_{p(IF_{3/2}S_2^1)} \mod p(IF_2S_2^1) + pJI\\
&\equiv -p(c_0-e) \mod (IJ+JI)I
\end{aligned}$$

Enfin, la seconde assertion du théorème est une simple conséquence du fait que $\partial_1 : C_1 \to N_0$ est un homomorphisme surjectif $\mathbb{Z}_p[\![S_2^1]\!]$-linéaire. □

2.3 Définition du second homomorphisme ∂_2

D'après le théorème-définition précédent, il existe $\tilde{\kappa}_\pm \in (IJ+JI)C_1$ tels que $\kappa_\pm + \tilde{\kappa}_\pm$ appartiennent à N_1 et

$$\begin{aligned}
\kappa_+ + \tilde{\kappa}_+ \equiv \mathcal{N}(a_0)(e_1)_+ \equiv p(e_1)_+ \mod I\,C_1\\
\kappa_- + \tilde{\kappa}_- \equiv \mathcal{N}(b_0)(e_1)_- \equiv p(e_1)_- \mod I\,C_1
\end{aligned}$$

Soit d_2 l'homomorphisme qui, pour tous λ, μ entiers p-adiques, envoie $\lambda\epsilon_+ + \mu\epsilon_- \in \Lambda_{1-p}$ sur $\lambda(\kappa_+ + \tilde{\kappa}_+) + \mu(\kappa_- + \tilde{\kappa}_-)$ dans N_1. Alors, avec la suite exacte courte en homologie donnée dans le lemme 2.15, on déduit le diagramme suivant

$$\begin{tikzcd}
\Lambda_{1-p} \arrow[r, "d_2"] \arrow[dr, "p\,\mathrm{Id}_{\Lambda_{1-p}}"'] & N_1 \arrow[r] \arrow[d, two heads] & C_1 \arrow[r, "\partial_1"] \arrow[d, two heads] & N_0 \arrow[r] \arrow[d, two heads] & 0\\
0 \arrow[r] & H_0(S_2^1, N_1) \arrow[r] & \Lambda_{1-p} \arrow[r, "\partial_{1*}"] & \Lambda_{1-p}/(p) \arrow[r] & 0
\end{tikzcd}$$

Proposition-Définition 2.44.

1. *On pose $d_2 : \Lambda_{1-p} \to N_1$ l'homomorphisme définie par $d_2(\epsilon_\pm) := \kappa_\pm + \tilde{\kappa}_\pm$.*
2. *On pose*

$$\partial_2 = \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1} :\ C_2 \longrightarrow N_1.$$

C'est un homomorphisme de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules surjectif.

Démonstration. Il nous faut montrer que ∂_2 est surjectif. Comme pour la première différentielle ∂_2, on a

$$\begin{tikzcd}
H_0(S^1_2, C_2) \arrow[rr, "\partial_{2*}"] \arrow[d, "\cong"'] & & H_0(S^1_2, N_1) \arrow[d, "\cong"] \\
\Lambda_{1-p} \arrow[rr, "\mathrm{tr}_F(p\,\mathrm{Id}_{\Lambda_{1-p}}) = p\,\mathrm{Id}_{\Lambda_{1-p}}"] & & p\Lambda_{1-p}
\end{tikzcd}$$

Donc $H_0(S^1_2, \partial_2)$ est surjectif et d'après le lemme de Nakayama (corollaire A.9), la différentielle ∂_2 est surjective sur N_1. □

2.4 Définition du troisième homomorphisme ∂_3

Nous allons utiliser une notion de dualité introduite dans la section 3.4 de [HKM08] pour définir le troisième homomorphisme. A propos de cette notion de dualité, j'ai aussi eu accès à un manuscrit intitulé "Duality for G-modules" rédigé par Hans-Werner Henn.
Avant d'introduire cette notion, nous sommes amenés à considérer une autre structure de $\mathbb{Z}_p[\![G]\!]$-module à gauche sur $\mathbb{Z}_p[\![G]\!]$.

Lemme 2.45. *Soit G un groupe profini. On définit une structure de $\mathbb{Z}_p[\![G]\!]$-module (à gauche) sur $\mathbb{Z}_p[\![G]\!]$ ainsi : $g_*h := hg^{-1}$ et on note ce $\mathbb{Z}_p[\![G]\!]$-module $\mathbb{Z}_p[\![G]\!]^{\circlearrowleft}$. Alors l'homomorphisme*

$$\begin{aligned} \Psi : \ \mathbb{Z}_p[\![G]\!] &\longrightarrow \mathbb{Z}_p[\![G]\!]^{\circlearrowleft} \\ g &\longmapsto g^{-1} \end{aligned}$$

est un isomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules.

Démonstration. Ce résultat est immédiat pour les groupes finis et on déduit le cas général par passage à la limite inverse. □

Définition 2.46. Soient G un groupe profini virtuellement pro-p et analytique et M un $\mathbb{Z}_p[\![G]\!]$-module de type fini, on pose

$$DM := D_G M := \mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M, \mathbb{Z}_p[\![G]\!])$$

muni de la structure de $\mathbb{Z}_p[\![G]\!]$-module définie par la relation suivante : $(g_*\phi)(m) := \phi(m)g^{-1}$ pour tous $g \in G$, $\phi \in D_G M$ et $m \in M$. Nous appellerons DM le dual de M et au lieu de noter le dual d'un homomorphisme f par Df, on le notera $f^\vee$.

Remarque. Les hypothèses sur G et M sont là uniquement pour garantir que $D_G M$ est profini.

Nous allons maintenant construire un isomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules entre les modules C_i et leurs duaux respectifs. Avant de faire cela, donnons une sorte d'adjonction.

Proposition 2.47 (voir la proposition 3.7 de [HKM08])**.** *Soit G un groupe profini virtuellement pro-p et analytique, soient M_1, M_2 deux $\mathbb{Z}_p[\![G]\!]$-modules de type fini.*

1. *Un homomorphisme $\alpha : M_1 \longrightarrow \mathrm{Hom}(M_2, \mathbb{Z}_p[\![G]\!])$ induit un homomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules de M_1 dans DM_2 si et seulement si son adjoint $\hat{\alpha} : M_1 \otimes M_2 \longrightarrow \mathbb{Z}_p[\![G]\!]$ qui envoie (m_1, m_2) sur $\alpha(m_1)(m_2)$ vérifie les deux propriétés suivantes :*
   - *i)* $\forall g \in G,\ \forall m_1 \in M_1,\ \forall m_2 \in M_2 : \quad \hat{\alpha}(m_1 \otimes gm_2) = g\hat{\alpha}(m_1 \otimes m_2).$
   - *ii)* $\forall g \in G,\ \forall m_1 \in M_1,\ \forall m_2 \in M_2 : \quad \hat{\alpha}(gm_1 \otimes m_2) = \hat{\alpha}(m_1 \otimes m_2)g^{-1}.$

2. *Soit H un sous-groupe fermé de G. L'homomorphisme*

$$\begin{array}{rcl} \Phi : D_H(M)\uparrow_H^G & \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p[\![H]\!]}(M, \mathbb{Z}_p[\![G]\!]) & \longrightarrow D_G(M\uparrow_H^G) \\ x\otimes\phi & \longmapsto (\varphi :\ m \mapsto \phi(m)x^{-1}) & \\ & \varphi & \longmapsto (x\otimes m \mapsto x\varphi(m)) \end{array}$$

est un isomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules.

3. *Soient H un sous-groupe fermé de G et $\alpha : M_1 \longrightarrow D_H M_2$ un isomorphisme de $\mathbb{Z}_p[H]$-modules, alors*

$$\beta :\ M_1\uparrow_H^G \xrightarrow{\alpha\uparrow_H^G} (D_H M_2)\uparrow_H^G \xrightarrow{\Psi\otimes(D_H M_2)} D_G(M_2\uparrow_H^G)$$

défini par

$$\beta(X\otimes m_1)(Y\otimes m_2) = Y\alpha(m_1)(m_2)\Psi(X),$$

est un isomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules.

Remarque. Si l'on munit $M_1\otimes M_2$ de l'action de $G\times G$ terme à terme, i.e : $(g_1,g_2)_*(m_1\otimes m_2) := g_1m_1\otimes g_2m_2$ et $\mathbb{Z}_p[\![G]\!]$ de l'action de $G\times G$ suivante : $(g_1,g_2)_*x := g_2xg_1^{-1}$. Alors α définit un homomorphisme de M_1 dans DM_2 si et seulement si $\hat{\alpha}$ est un homomorphisme de $\mathbb{Z}_p[\![G\times G]\!]$-modules. C'est-à-dire, on a un isomorphisme

$$\mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M_1, DM_2) \cong \mathrm{Hom}_{\mathbb{Z}_p[\![G\times G]\!]}(M_1\otimes M_1, \mathbb{Z}_p[\![G]\!])$$

Dans le cas des groupes finis, le dual que nous avons construit est isomorphe au dual plus conventionnel :

Lemme 2.48. *Soient H un groupe fini et M un $\mathbb{Z}_p[H]$-module, on munit* $\mathrm{Hom}(M,\mathbb{Z}_p)$ *de sa structure de $\mathbb{Z}_p[H]$-module usuelle, i.e : $h_*\phi(m) := \phi(h^{-1}m)$. Alors*

$$\begin{array}{rcl} \Theta :\ \mathrm{Hom}(M,\mathbb{Z}_p) & \longrightarrow & D_H M \\ \phi & \longmapsto & \left(\ m \mapsto \sum_{h\in H}\phi(hm)h^{-1}\ \right) \end{array}$$

est un isomorphisme de $\mathbb{Z}_p[H]$-modules.

Démonstration. Soient $\phi\in\mathrm{Hom}(M,\mathbb{Z}_p)$, $g\in H$ et $m\in M$, alors

$$\begin{array}{rcl} \Theta(\phi)(g_*m) & = & \sum_{h\in H}\phi(hgm)g(hg)^{-1} = g\sum_{h\in H}\phi(hm)h^{-1} \\ \Theta(g_*\phi)(m) & = & \sum_{h\in H}\phi(g^{-1}hm)(g^{-1}h)^{-1}g^{-1} = \sum_{h\in H}\phi(hm)h^{-1}g^{-1} \end{array}$$

De le première identité, on déduit que $\Theta(\phi)$ est $\mathbb{Z}_p[H]$-linéaire et que Θ est bien défini. De la seconde identité, on déduit que Θ est aussi $\mathbb{Z}_p[H]$-linéaire.
Il nous reste à montrer que Θ est un isomorphisme. On regarde $\mathbb{Z}_p[H]$ comme un $\mathbb{Z}_p$-module libre, pour tout g dans H, on définit l'homomorphisme $\mathrm{pr}_g : \mathbb{Z}_p[H] \twoheadrightarrow \mathbb{Z}_p$ qui envoie h sur 1 lorsque $h = g$ et 0 sinon. Alors, $\mathrm{pr}_1(gx) = \mathrm{pr}_{g^{-1}}(x)$, d'où l'on déduit sans peine que pr_{1*} est l'inverse de Θ. Le fait que Θ est un homomorphisme de $\mathbb{Z}_p[H]$-modules est une simple vérification. $\square$

Soient G un groupe profini virtuellement pro-p et analytique et H un sous-groupe fini de G. D'après le lemme précédent appliqué au module triviale $\mathbb{Z}_p$, on a l'isomorphisme suivant

$$\begin{aligned} \mathbb{Z}_p \cong \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}_p) &\longrightarrow D_H \mathbb{Z}_p \\ \lambda &\longmapsto (\, m \mapsto \lambda m \textstyle\sum_{h\in H} h^{-1} \,) \end{aligned}$$

Enfin d'après le troisième point de la proposition précédente, on a un isomorphisme

$$\alpha : \mathbb{Z}_p \uparrow_H^G \longrightarrow D_G(\mathbb{Z}_p \uparrow_H^G)$$

défini par $\hat{\alpha}(X \otimes \lambda) \otimes (Y \otimes \mu) := \lambda\mu Y \sum_{h\in H} h\Psi(X)$.

Rappelons que $C_0 = C_3 = \mathbb{Z}_p \uparrow_F^{\mathbb{G}_2^1}$. D'où, la définition suivante.

Définition 2.49. Pour $i = 0, 3$, on pose $\alpha_i : C_i \longrightarrow D_{\mathbb{G}_2^1} C_{3-i}$, l'isomorphisme de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules caractérisé par

$$\hat{\alpha}_i(X \otimes \lambda) \otimes (Y \otimes \mu) := \lambda\mu Y \sum_{f\in F} f\Psi(X)$$

pour tous $\lambda, \mu \in \mathbb{Z}_p$ et tous $X, Y \in \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$.

Nous allons maintenant considérer $C_2 = C_1 = \Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1}$. Soit i un entier relatif. L'homomorphisme $\Lambda_i \otimes \Lambda_{-i} \longrightarrow \mathbb{Z}_p$ qui envoie $x \otimes y$ sur $xy + (xy)^\sigma$ induit un isomorphisme de $\mathbb{Z}_p[F]$-modules $\Lambda_i \cong \mathrm{Hom}(\Lambda_{-i}, \mathbb{Z}_p)$. En appliquant le lemme précédent, on déduit un isomorphisme entre Λ_i et $D_F(\Lambda_{-i})$ dont l'adjoint est

$$\begin{aligned} \Lambda_i \otimes \Lambda_{-i} &\longrightarrow \mathbb{Z}_p[F] \\ x \otimes y &\longmapsto \textstyle\sum_{f\in F} \Big(x f_* y + (x f_* y)^\sigma \Big) f^{-1} \end{aligned} .$$

D'où, du dernier point de la proposition précédente, on a que

$$\alpha : \Lambda_i \uparrow_F^{\mathbb{G}_2^1} \longrightarrow D_{\mathbb{G}_2^1}(\Lambda_{-i} \uparrow_F^{\mathbb{G}_2^1})$$

$$\alpha(X \otimes x)(Y \otimes y) = Y \sum_{f\in F} \Big(x f_* y + (x f_* y)^\sigma \Big) f^{-1} \Psi(X)$$

définit un isomorphisme. Lorsque $i = 1 - p$, on notera que l'automorphisme de Frobenius, induit un isomorphisme de $\mathbb{Z}_p[F]$-modules entre Λ_{1-p} et Λ_{p-1}, d'où l'isomorphisme de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules

$$\Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1} \xrightarrow{Frob \uparrow_F^{\mathbb{G}_2^1}} \Lambda_{p-1} \uparrow_F^{\mathbb{G}_2^1} \longrightarrow D_{\mathbb{G}_2^1}(\Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1}) \tag{2.11}$$

Définition 2.50. Pour $i = 1, 2$, on pose $\alpha_i : C_i \longrightarrow D_{\mathbb{G}_2^1} C_{3-i}$, l'isomorphisme de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules défini précédemment et dont l'adjoint est défini par

$$\hat{\alpha}_i(X \otimes x) \otimes (Y \otimes y) := Y \sum_{f\in F} \langle x^\sigma, f_* y \rangle f^{-1} \Psi(X)$$

pour tous $x, y \in \Lambda_{1-p}$ et tous $X, Y \in \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$ et où

$$\langle x, y \rangle := xy + (xy)^\sigma$$

D'après le théorème 6 de [Hen07], il existe un troisième homomorphisme ∂_3 qui complète notre résolution projective :

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$$

On note alors que si l'on précompose ∂_3 par un automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire, on a encore une suite exacte.

Proposition 2.51.

1. *Il existe un homomorphisme $\bar{\epsilon}$ tel qu'on ait une suite exacte de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules*

$$0 \longrightarrow D_{\mathbb{G}_2^1}C_0 \xrightarrow{\partial_1^\vee} D_{\mathbb{G}_2^1}C_1 \xrightarrow{\partial_2^\vee} D_{\mathbb{G}_2^1}C_2 \xrightarrow{\partial_3^\vee} D_{\mathbb{G}_2^1}C_3 \xrightarrow{\bar{\epsilon}} \mathbb{Z}_p \longrightarrow 0$$

2. *On pose $\delta_i := \alpha_i \partial_{4-i}^\vee \alpha_{i-1}^{-1}$ et $\epsilon' := \bar{\epsilon}\alpha_0$. Quitte à précomposer ∂_3 par un automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire et à multiplier ϵ' par une unité p-adique, il existe un isomorphisme $f_\bullet$: $DC_{3-\bullet} \to C_\bullet$ de complexes de chaînes tel que*

$$\begin{tikzcd}
 & 0 \arrow[r] & C_3 \arrow[rr, dashed, "\delta_3"] \arrow[dl, "\alpha_3"'] \arrow[ddl, bend left, "="] & & C_2 \arrow[rr, dashed, "\delta_2"] \arrow[dl, "\alpha_2"'] \arrow[ddl, bend left] & & C_1 \arrow[rr, dashed, "\delta_1"] \arrow[dl, "\alpha_1"'] \arrow[ddl, bend left] & & C_0 \arrow[rr, dashed, "\epsilon'"] \arrow[dl, "\alpha_0"'] \arrow[ddl, bend left] & & \mathbb{Z}_p \arrow[r] \arrow[dl, "="'] \arrow[ddl, bend left] & 0 \\
0 \arrow[r] & DC_0 \arrow[rr, "\partial_1^\vee"] \arrow[d, "f_3"'] & & DC_1 \arrow[rr, "\partial_2^\vee"] \arrow[d, "f_2"'] & & DC_2 \arrow[rr, "\partial_3^\vee"] \arrow[d, "f_1"'] & & DC_3 \arrow[rr, "\bar{\epsilon}"] \arrow[d, "f_0"'] & & \mathbb{Z}_p \arrow[rr] \arrow[d, "="'] & & 0 \\
0 \arrow[r] & C_3 \arrow[rr, "\partial_3"] & & C_2 \arrow[rr, "\partial_2"] & & C_1 \arrow[rr, "\partial_1"] & & C_0 \arrow[rr, "\epsilon"] & & \mathbb{Z}_p \arrow[rr] & & 0
\end{tikzcd}$$

et

$$\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p, f_2\alpha_2) = \mathrm{Id}$$

Démonstration.

1. Comme (C_*, ∂_*) est une résolution projective, pour tout entier n,

$$H^n(\mathbb{G}_2^1, \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]) \cong H_n(\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_*, \mathbb{Z}_p[\![\mathbb{G}_2^1]\!])) \cong H_n(D(C_*))$$

En adaptant la preuve de la proposition 5 de [Str00] pour le groupe $\mathbb{G}_n$ au groupe $\mathbb{G}_2^1$, on a que les précédents groupes de cohomologie sont nuls sauf lorsque $n = 3$ et dans ce cas vaut $\mathbb{Z}_p$ avec une action triviale de $\mathbb{G}_2^1$ à droite. Ainsi, on a l'exactitude de la suite duale en les DC_i pour $i = 1, 2, 3$ et l'action de $\mathbb{G}_2^1$ sur $\mathrm{Coker}\,\partial_3^\vee = H^3(\mathbb{G}_2^1, \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]) \cong \mathbb{Z}_p$ est triviale. D'où l'existence d'un homomorphisme $\bar{\epsilon}$ de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules tel qu'on ait la suite exacte de la proposition.

2. Nous avons donc deux résolutions projectives C_* et $D_{\mathbb{G}_2^1}C_*$ de $\mathbb{Z}_p$ au-dessus de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$. Ainsi, par le lemme fondamentale de l'algèbre homologique, il existe un homomorphisme $f_* : D_{\mathbb{G}_2^1}C_* \to C_*$ de complexes de chaînes.
D'après la proposition 2.11,

$$H_*(\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_*) = H_*(S_2^1, \mathbb{F}_p) \cong \begin{cases} \mathbb{F}_p & \text{si } n = 0, 3 \\ \mathbb{F}_p^2 & \text{si } n = 1, 2 \\ 0 & \text{sinon} \end{cases}$$

Or, par définition des modules C_i (définition 2.3), on a

$$\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{F}_p, C_*) \cong \mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_* \cong \begin{cases} \mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} \mathbb{Z}_p[\![S_2^1]\!] \cong \mathbb{F}_p & \text{si } n = 0, 3 \\ \mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} \mathbb{Z}_p[\![S_2^1]\!]^{\oplus 2} \cong \mathbb{F}_p^2 & \text{si } n = 1, 2 \\ 0 & \text{sinon} \end{cases}$$

Ainsi, en comparant $H_*(\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_*)$ et $\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_*$, on déduit que les différentielles du complexe $\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_*$ sont nulles. De même, si l'on pose $\tilde{C}_*$ la résolution dont les modules sont les C_i et les différentielles sont les homomorphismes δ_i, alors les différentielles du complexe $\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} \tilde{C}_*$ sont aussi nulles.
Maintenant, comme l'homomorphisme de complexes de chaînes $f_*\alpha_*$ réalise un relèvement de l'identité sur $\mathbb{Z}_p$, on déduit qu'il induit un isomorphisme en homologie. En résumé, on a le diagramme suivant :

$$\begin{tikzcd} H_*(\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} \tilde{C}_*) \arrow[r, "\cong"] \arrow[d, "="'] & H_*(\mathbb{F}_p \underset{\mathbb{Z}_p[\![S_2^1]\!]}{\otimes} C_*) \arrow[d, "="] \\ \mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{F}_p, \tilde{C}_*) \arrow[r] & \mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{F}_p, C_*) \end{tikzcd}$$

Donc, $\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{F}_p, f_*\alpha_*)$ est un isomorphisme. De plus, comme les modules C_i sont libres en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-modules, on a $\mathrm{Tor}_1^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{F}_p, C_i) = 0$ et d'après le lemme de Nakayama (corollaire A.9), $f_*\alpha_*$ est un isomorphisme. Par construction α_* est un isomorphisme, d'où l'on déduit que f_* est aussi un isomorphisme.
Nous allons maintenant modifier certains homomorphismes pour obtenir les relations annoncées. Comme, $f_2\alpha_2$ est un $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-automorphisme, il induit un $\mathbb{Z}_p[F]$-automorphisme de

$$\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p, C_2) \cong \Lambda_{1-p}$$

D'après la proposition 1.29, il existe $\lambda_2 \in \mathbb{Z}_p^\times$ tel que $f_2\alpha_2 \equiv \lambda_2 \,\mathrm{Id}$ modulo l'idéal (IS_2^1). On remplace $f_\bullet$ par $\lambda_2^{-1} f_\bullet$, ainsi $\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p, f_2\alpha_2) = \mathrm{Id}$. Au passage, pour que le dernier carré de droite du diagramme de la proposition reste commutatif, il faut multiplier $\bar{\epsilon}$ par λ_2^{-1}.
Posons $\phi = f_3\alpha_3$, on note que le diagramme suivant est encore commutatif :

$$\begin{tikzcd} & C_3 \arrow[dl, "\alpha_3"'] \arrow[ddl, bend left, "="] & & & & & \\ 0 \arrow[r] & DC_0 \arrow[r, "\partial_1^\vee"] \arrow[d, "\alpha_3^{-1}"'] & DC_1 \arrow[r, "\partial_2^\vee"] \arrow[d, "f_2"] & DC_2 \arrow[r, "\phi^*\partial_3^\vee"] \arrow[d, "f_1"] & DC_3 \arrow[r, "\bar{\epsilon}(\phi^*)^{-1}"] \arrow[d, "f_0(\phi^*)^{-1}"] & \mathbb{Z}_p \arrow[r] \arrow[d, "="] & 0 \\ 0 \arrow[r] & C_3 \arrow[r, "\partial_3\phi"] & C_2 \arrow[r, "\partial_2"] & C_1 \arrow[r, "\partial_1"] & C_0 \arrow[r, "\epsilon"] & \mathbb{Z}_p \arrow[r] & 0 \end{tikzcd}$$

On remplace ∂_3 par $\partial_3\phi$, f_0 par $f_0(\phi^*)^{-1}$, $\bar{\epsilon}$ par $\bar{\epsilon}(\phi^*)^{-1}$, pour obtenir les homomorphismes vérifiant les propriétés recherchées.

$\square$

Corollaire 2.52. *Avec les notations de la proposition précédente, posons $\alpha^{-1} = f_2\alpha_2$. La suite*

$$0 \longrightarrow C_3 \xrightarrow{\delta_3} C_2 \xrightarrow{\partial_2\alpha} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$$

est une résolution projective de $\mathbb{Z}_p$ au-dessus de $\mathbb{G}_2^1$.

Avant de préciser l'homomorphisme δ_3, introduisons un analogue de l'élément v :

Définition 2.53. On pose [6]

$$\Lambda := \frac{1}{p+1}\sum_{i=0}^{p} \lambda_i(a_i^{-1} - e) + \mu_i(b_i^{-1} - e)$$

Proposition 2.54. *L'homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire $\delta_3 : C_3 \longrightarrow C_2$ est caractérisé par*

$$\delta_3(e_3) = \frac{1}{2\epsilon_+^2}\Lambda(e_2)_+ + \frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega - \omega\Lambda\omega^{-1})(e_2)_-$$

Rappelons quelques identités :

$$a_i = \omega^{-i}a_0\omega^i, \qquad \sigma^{-1}a_i\sigma = a_{-i}, \qquad b_i = \omega^{-i}b_0\omega^i, \qquad \sigma^{-1}b_i\sigma = b_{-i+(p+1)/2}$$

$$\partial_1(e_1)_+ = \frac{1}{p+1}\sum_{i=0}^{p} \lambda_i(a_i - e) + \mu_i(b_i - e)$$

et

$$\lambda_i = \frac{\omega^{(1-p)i} + \omega^{(p-1)i}}{2}, \quad \mu_i = \frac{\omega^{(1-p)i} - \omega^{(p-1)i}}{2\epsilon_-}\epsilon_+$$

Comme ω est d'ordre $p^2 - 1$, on déduit que les sommes $\sum_{i=0}^{p} \lambda_i$ et $\sum_{i=0}^{p} \mu_i$ sont nuls. Ainsi,

$$\partial_1(e_1)_+ = \frac{1}{p+1}\sum_{i=0}^{p} \lambda_i a_i + \mu_i b_i$$

Démonstration. Par construction de δ_3,

$$\partial_1^\vee \alpha_3 = \alpha_2\delta_3$$

Évaluons le membre de gauche de la précédente identité,

$$\begin{aligned}
(p+1)\partial_1^\vee\alpha_3(e_3, (e_1)_+) &= \hat{\alpha}_3(e_3, \partial_1(e_1)_+) \\
&= \partial_1(e_1)_+ \sum_{f\in F} f \\
&= \sum_{i=0}^{p}\sum_{j=0}^{p^2-2} (\lambda_i a_i + \mu_i b_i)(\omega^j + \sigma\omega^j) \\
&= \sum_{i=0}^{p}\sum_{j=0}^{p^2-2} \lambda_i\omega^j a_{i+j} + \lambda_i\sigma\omega^j a_{-i+j} + \mu_i\omega^j b_{i+j} + \mu_i\sigma\omega^j b_{-i+j+(p+1)/2} \\
&= \sum_{i=0}^{p}\sum_{j=0}^{p^2-2} \lambda_{i-j}\, \omega^j a_i + \lambda_{j-i}\, \sigma\omega^j a_i + \mu_{i-j}\, \omega^j b_i + \mu_{-i+j+(p+1)/2}\, \sigma\omega^j b_i
\end{aligned}$$

6. Avec les notations du lemme 2.45, $\Lambda = \Psi(v)$. Je note cet élément Λ dont le dessin est le symétrique de v pour marquer la relation de passage à une sorte d'inverse.

Passons au second membre, donnons nous $Z_\pm \in \mathbb{Z}_p[\![S_2^1]\!]$ tels que $(p+1)\delta_3(e_3) = Z_+(e_2)_+ + Z_-(e_2)_-$, ils sont uniquement déterminés car C_2 est $\mathbb{Z}_p[\![S_2^1]\!]$-libre de rang 2. Alors,

$$\begin{aligned}(p+1)\hat{\alpha}_2\delta_3(e_3\otimes(e_1)_+) &= \hat{\alpha}_2(Z_+(e_2)_+ + Z_-(e_2)_-)\otimes(e_1)_+\\ &= \sum_{f\in F}\langle\epsilon_+, f_*\epsilon_+\rangle f^{-1}\Psi(Z_+)\\ &\quad+\sum_{f\in F}\langle\epsilon_-^\sigma, f_*\epsilon_+\rangle f^{-1}\Psi(Z_-)\\ &= \sum_{j=0}^{p^2}\Big(\langle\epsilon_+,\omega_*^{-j}\epsilon_+\rangle\omega^j + \langle\epsilon_+,\omega^{-j}\sigma_*\epsilon_+\rangle\sigma\omega^j\Big)\Psi(Z_+)\\ &\quad-\Big(\langle\epsilon_-,\omega_*^{-j}\epsilon_+\rangle\omega^j + \langle\epsilon_-,\omega^{-j}\sigma_*\epsilon_+\rangle\sigma\omega^j\Big)\Psi(Z_-)\end{aligned}$$

En comparant les termes des deux précédentes expressions, on devine[7] que $\Psi(Z_+)$, $\Psi(Z_-)$ sont de la forme suivante :

$$\begin{aligned}\Psi(Z_+) &= \sum_{i=0}^{p} x_i a_i + y_i b_i\\ \Psi(Z_-) &= \sum_{i=0}^{p} x'_i a_i + y'_i b_i\end{aligned}$$

où x_i, x'_i, y_i, y'_i sont des entiers p-adiques. Avec ces notations, on a

$$\begin{aligned}\hat{\alpha}_2\delta_3(e_3\otimes(e_1)_+) = &\sum_{j=0}^{p^2}\sum_{i=0}^{p}\Big(\langle\epsilon_+,\omega_*^{-j}\epsilon_+\rangle\omega^j(x_ia_i+y_ib_i) + \langle\epsilon_+,\omega^{-j}\sigma_*\epsilon_+\rangle\sigma\omega^j(x_ia_i+y_ib_i)\\ &-\langle\epsilon_-,\omega_*^{-j}\epsilon_+\rangle\omega^j(x'_ia_i+y'_ib_i) - \langle\epsilon_-,\omega^{-j}\sigma_*\epsilon_+\rangle\sigma\omega^j(x'_ia_i+y'_ib_i)\Big)\end{aligned}$$

Par identification des coefficients de ces expressions en les fa_i, fb_i où f parcourt les éléments de F, on déduit que ce dernier terme est égal à $\partial_1^\vee\alpha_3(e_3,(e_1)_+)$ si

$$\begin{aligned}\lambda_{i-j} &= \langle\epsilon_+,\omega_*^{-j}\epsilon_+\rangle x_i - \langle\epsilon_-,\omega_*^{-j}\epsilon_+\rangle x'_i && \omega^j a_i\\ \lambda_{-i+j} &= \langle\epsilon_+,\omega^{-j}\sigma_*\epsilon_+\rangle x_i - \langle\epsilon_-,\omega^{-j}\sigma_*\epsilon_+\rangle x'_i && \sigma\omega^j a_i\\ \mu_{i-j} &= \langle\epsilon_+,\omega_*^{-j}\epsilon_+\rangle y_i - \langle\epsilon_-,\omega_*^{-j}\epsilon_+\rangle y'_i && \omega^j b_i\\ \mu_{-i+j+(p+1)/2} &= \langle\epsilon_+,\omega^{-j}\sigma_*\epsilon_+\rangle y_i - \langle\epsilon_-,\omega^{-j}\sigma_*\epsilon_+\rangle y'_i && \sigma\omega^j b_i\end{aligned}$$

quels que soient $0 \le i \le p$ et $0 \le j < p^2-1$. Or,

$$\begin{aligned}\langle\epsilon_+,\omega_*^{-j}\epsilon_+\rangle &= \epsilon_+^2(\omega^{(p-1)j}+\omega^{(1-p)j}) = 2\epsilon_+^2\lambda_j\\ \langle\epsilon_-,\omega_*^{-j}\epsilon_+\rangle &= -2\epsilon_-^2\mu_j\end{aligned}$$

et $\sigma_*\epsilon_+ = \epsilon_+$, $\lambda_i = \lambda_{-i}$, $\mu_{-i+(p+1)/2} = \mu_i$, d'où le système de conditions que doivent vérifier les coefficients devient :

$$\forall\, 0 \le j < p^2-1 : \qquad \begin{cases}\lambda_{i-j} &= 2\epsilon_+^2\lambda_j x_i + 2\epsilon_-^2\mu_j x'_i\\ \mu_{i-j} &= 2\epsilon_+^2\lambda_j y_i + 2\epsilon_-^2\mu_j y'_i\end{cases} \tag{2.12}$$

7. Il y a une raison tout de même qui provient du fait que les fa_i et fb_i, où f parcourt le groupe F, sont deux à deux distincts dans $\mathbb{G}_2^1 = S_2^1 \rtimes F$ et même distincts dans $\mathbb{G}_2^1/_{F_1}S_2^1$.

En considérant les équations pour $j = 0, 1$, on voit qu'il faut poser

$$\begin{cases} x_i & := \frac{1}{2\epsilon_+^2}\lambda_i \\ x'_i & := \frac{1}{2\epsilon_-^2\mu_1}(\lambda_{i-1} - \lambda_1\lambda_i) \\ y_i & := \frac{1}{2\epsilon_+^2}\mu_i \\ y'_i & := \frac{1}{2\epsilon_-^2\mu_1}(\mu_{i-1} - \lambda_1\mu_i) \end{cases}$$

Vérifions qu'ils conviennent, soit $0 \leq j < p^2 - 1$ (on peut se restreindre à $0 \leq j \leq p$ à cause de la périodicité des λ_j et μ_j). Pour alléger les notations, je pose $\xi = \omega^{1-p}$,

$$\begin{aligned} 4(2\epsilon_+^2\lambda_j x_i + 2\epsilon_-^2\mu_j x'_i) &= 4(\lambda_j\lambda_i + \frac{\mu_j}{\mu_1}(\lambda_{i-1} - \lambda_1\lambda_i)) \\ &= (\xi^j + \xi^{-j})(\xi^i + \xi^{-i}) + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}\Big(2\xi^{i-1} + 2\xi^{-i+1} - (\xi + \xi^{-1})(\xi^i + \xi^{-i})\Big) \\ &= \xi^{i-j} + \xi^{j-i} + \xi^{i+j} + \xi^{-i-j} + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}\Big(\xi^{i-1} + \xi^{-i+1} - \xi^{i+1} - \xi^{-i-1}\Big) \\ &= \xi^{i-j} + \xi^{j-i} + \xi^{i+j} + \xi^{-i-j} + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}(-\xi + \xi^{-1})(\xi^i - \xi^{-i}) \\ &= \xi^{i-j} + \xi^{j-i} + \xi^{i+j} + \xi^{-i-j} - (\xi^j - \xi^{-j})(\xi^i - \xi^{-i}) \\ &= 2(\xi^{i-j} + \xi^{j-i}) \end{aligned}$$

De même, on vérifie que (y_i, y'_i) est solution :

$$\begin{aligned} 4\frac{\epsilon_-}{\epsilon_+}(2\epsilon_+^2\lambda_j y_i + 2\epsilon_-^2\mu_j y'_i) &= 4\frac{\epsilon_-}{\epsilon_+}(\lambda_j\mu_i + \frac{\mu_j}{\mu_1}(\mu_{i-1} - \lambda_1\mu_i)) \\ &= (\xi^j + \xi^{-j})(\xi^i - \xi^{-i}) + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}\Big(2\xi^{i-1} - 2\xi^{-i+1} - (\xi + \xi^{-1})(\xi^i - \xi^{-i})\Big) \\ &= \xi^{i-j} - \xi^{j-i} + \xi^{i+j} - \xi^{-i-j} + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}\Big(\xi^{i-1} - \xi^{-i+1} - \xi^{i+1} + \xi^{-i-1}\Big) \\ &= \xi^{i-j} - \xi^{j-i} + \xi^{i+j} - \xi^{-i-j} + \frac{\xi^j - \xi^{-j}}{\xi - \xi^{-1}}(\xi - \xi^{-1})(-\xi^i - \xi^{-i}) \\ &= \xi^{i-j} - \xi^{j-i} + \xi^{i+j} - \xi^{-i-j} - (\xi^j - \xi^{-j})(\xi^i + \xi^{-i}) \\ &= 2(\xi^{i-j} - \xi^{j-i}) \end{aligned}$$

Donc, les coefficients x_i, x'_i, y_i et y'_i sont solutions du système d'équations (2.12). Comme $\lambda_{i-j} = 2\epsilon_+^2\lambda_j x_i + 2\epsilon_-^2\mu_j x'_i$ et $x_i = \frac{1}{2\epsilon_+^2}\lambda_i$, on déduit que pour tout i, j

$$x'_i = \frac{1}{2\epsilon_-^2\mu_j}(\lambda_{i-j} - \lambda_j\lambda_i)$$

En particulier, pour $j = \pm 1$, on a

$$\begin{cases} x'_i & = \frac{1}{2\epsilon_-^2\mu_1}(\lambda_{i-1} - \lambda_1\lambda_i) \\ x'_i & = \frac{1}{2\epsilon_-^2\mu_{-1}}(\lambda_{i+1} - \lambda_{-1}\lambda_i) = \frac{-1}{2\epsilon_-^2\mu_1}(\lambda_{i+1} - \lambda_1\lambda_i) \end{cases}$$

Pour la dernière identité, on a utilisé le fait que $\lambda_{-1} = \lambda_1$ et $\mu_{-1} = -\mu_1$. Ainsi,

$$x'_i = \frac{1}{4\epsilon_-^2\mu_1}(\lambda_{i-1} - \lambda_{i+1})$$

De même, on montre que y'_i est égal à $\frac{1}{4\epsilon_+^2\mu_1}(\mu_{i-1} - \mu_{i+1})$. En résumé,

$$\begin{aligned} \delta_3(e_3) &= \frac{1}{p+1}\sum_{i=0}^{p}\frac{1}{2\epsilon_+^2}\Big(\lambda_i(a_i^{-1} - e) + \mu_i(b_i^{-1} - e)\Big)(e_2)_+ \\ &\quad + \frac{1}{p+1}\sum_{i=0}^{p}\frac{1}{4\epsilon_-^2\mu_1}\Big((\lambda_{i-1} - \lambda_{i+1})(a_i^{-1} - e) + (\mu_{i-1} - \mu_{i+1})(b_i^{-1} - e)\Big)(e_2)_- \end{aligned}$$

Enfin, notons encore les relations suivantes :

$$a_i^{-1} = \omega^{-i} a_0^{-1} \omega^i = \omega^{-1} a_{i-1}^{-1} \omega = \omega a_{i+1}^{-1} \omega^{-1}$$

ainsi,

$$\delta_3(e_3) = \frac{1}{2\epsilon_+^2} \Lambda(e_2)_+ + \frac{1}{4\epsilon_-^2 \mu_1} (\omega^{-1} \Lambda \omega - \omega \Lambda \omega^{-1})(e_2)_-$$

□

CHAPITRE 3

Sur l'action du groupe stabilisateur de Morava

Dans ce chapitre, nous allons donner une approximation de la déformation universelle $G_2(x,y)$. Nous l'utiliserons ensuite pour généraliser au cas $p \geq 3$ le corollaire 4.5 de [HKM08] qui donne une approximation de l'application t_0.

Dans ce chapitre p désigne un nombre premier impair.

3.1 La déformation universelle G_2

En utilisant les rappels sur la construction de la déformation universelle $G_2(x,y)$ donnés dans le premier chapitre, nous allons rappeler l'allure des premiers coefficients de $G_2(x,y)$.

Notation. Pour tout entier naturel n, posons $B_n(x,y) = (x+y)^n - x^n - y^n$ et le polynôme de Lazard associé :

$$C_n(x,y) = \begin{cases} \frac{1}{q}B_n(x,y) & \text{si } n \text{ est une puissance d'un nombre premier } q, \\ B_n(x,y) & \text{sinon.} \end{cases}$$

Lemme 3.1. *Pour tout $1 \leq i \leq p$, il existe $P_{p+i(p-1)}(x,y)$ un polynôme à coefficients dans $\mathbb{Z}_{(p)}$ et homogène de degré $p+i(p-1)$ tel que*

$$G_2(x,y) = x + y - \frac{u_1}{1-p^{p-1}}C_p(x,y) + \sum_{i=1}^{p} u_1^{i+1}P_{p+i(p-1)}(x,y) - \frac{1}{1-p^{p^2-1}}C_{p^2}(x,y) \mod (x,y)^{p^2+1}$$

Démonstration. Revenons à la loi de groupe formelle p-typique universelle $F(x,y)$ définie sur l'anneau gradué $\mathrm{BP}_* = \mathbb{Z}_{(p)}[v_1, v_2, \ldots]$, où $|v_i| = 2(p^i-1)$. On rappelle que si l'on pose $|x| = |y| = -2$, alors $F(x,y)$ est homogène de degré -2. C'est-à-dire si l'on se donne $a_{i,j} \in \mathrm{BP}_*$ les coefficients de $F(x,y)$, i.e :

$$F(x,y) = x + y + \sum_{i,j>0} a_{i,j}\, x^i\, y^j$$

alors, $|a_{i,j}| = -2 + 2(i+j)$. Comme, $|v_1| = 2(p-1)$ et $|v_2| = 2(p^2-1)$, on déduit qu'il existe des polynômes $P_{p+i(p-1)}(x,y), P(x,y) \in \mathbb{Z}_{(p)}[x,y]$ homogènes de degré $-2(p+i(p-1))$ tels que

$$F(x,y) = x + y + \sum_{i=0}^{p} v_1^{i+1}P_{p+i(p-1)}(x,y) + v_2P(x,y) \mod (x,y)^{p^2+1}.$$

Ensuite, notons $\log(x)$ (resp. $\exp(x)$) le logarithme (resp. l'exponentielle) de $F(x,y)$ vu comme loi de groupe formel à coefficients dans $\mathbb{Q} \otimes \mathrm{BP}_* = \mathbb{Q}[\lambda_1, \ldots]$. Des relations de Araki, on déduit que

$$\log(x) \equiv x + \lambda_1 x^p + \lambda_2 x^{p^2} \equiv x + \frac{v_1}{p-p^p}x^p + \frac{1}{p-p^{p^2}}\left(v_2 + \frac{v_1^{p+1}}{p-p^p} \right)x^{p^2} \mod (x^{p^3})$$

D'où, l'exponentielle, inverse de la série $\log(x)$ est de la forme suivante

$$\exp(x) \equiv x - \lambda_1 x^p + \ldots - \lambda_2 x^{p^2} \mod (x^{p^2+1})$$

où les termes qui ne sont pas écrit explicitement dépendent uniquement de λ_1. Enfin, de la relation $F(x,y) = \exp(\log x + \log y)$, on déduit que $F(x,y)$ est de la forme suivante :

$$x + y - \lambda_1 p C_p(x,y) + \ldots - \lambda_2 p C_{p^2}(x,y) \mod (x,y)^{p^2+1}$$

D'où $F(x,y)$ est congrue à

$$x + y - \frac{v_1}{1-p^{p-1}} C_p(x,y) + \sum_{i=1}^{p} v_1^{i+1} P_{p+i(p-1)}(x,y) - \frac{v_2}{1-p^{p^2-1}} C_{p^2}(x,y) \mod (x,y)^{p^2+1}$$

Soit $\phi : \mathrm{BP}_* \to (E_2)_*$ défini par

$$v_i \longmapsto \begin{cases} u_i u^{1-p^i} & i < n \\ u^{1-p^n} & i = n \\ 0 & i > n \end{cases}$$

et posons $F_2 = \phi_* F$. Alors, $G_2(x,y) = u^{-1} F_2(ux, uy)$ est congru à

$$x + y - \frac{u_1}{1-p^{p-1}} C_p(x,y) + \sum_{i=1}^{p} u_1^{i+1} P_{p+i(p-1)}(x,y) - \frac{1}{1-p^{p^2-1}} C_{p^2}(x,y)$$

modulo $(x,y)^{p^2+1}$. □

Remarque. Notons $\log(x)$ le logarithme de G_2 au dessus de $\mathbb{Q} \otimes (E_2)_0$. À l'aide de la formule d'inversion de Lagrange, on peut montrer que

$$\exp(x) = \log^{-1}(x) \equiv x - \lambda_1 x^p f(\lambda_1 x^{p-1}) - \lambda_2 x^{p^2} \mod (x^{p^2+1})$$

où

$$f(x) = \sum_{n=0}^{p} \frac{(-1)^n}{n+1} \binom{p(n+1)}{n} x^n$$

Ainsi, en utilisant le fait qu'au dessus de $\mathbb{Q} \otimes (E_2)_0$, $G_2(x,y) = \exp(\log x + \log y)$, on peut montrer que pour tout $1 \leq i < p$,

$$P_{p+i(p-1)}(x,y) \quad := \quad \frac{1}{(1-p^{p-1})^j} \sum_{j=0}^{i} \frac{(-1)^j}{j+1} \binom{p(j+1)}{j} \binom{p+j(p-1)}{i-j} (x+y)^{p+jp-i} (x^p + y^p)^{i-j}$$

3.2 Action modulo (p)

Comme dans la section 4 de [HKM08], nous allons approximer la fonction t_0 qui permet de définir l'action du groupe de Morava sur l'anneau gradué de Lubin-Tate modulo (p).

La proposition suivante est une généralisation de la proposition 4.3 de [HKM08]. Le point $d)$ ne sera pas utilisé dans la suite.

Proposition 3.2. *Soit $g \in \mathbb{S}_n$.*

a) $g_* u_1 = t_0^{p-1} u_1 \mod (p)$

b) $t_0 + t_0^{p(p-1)} t_1 u_1^p = u_1 t_1^p + t_0^{p^2} \mod (p)$

c) $t_1 \equiv t_1^{p^2} + t_2^p u_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} u_1^{i+1} t_1^{pi} t_0^{p^2(p-i)} \mod (p,\, u_1^{p+1})$

d) Si $g \equiv 1 \bmod (S^2)$ alors $t_2 \equiv u_1 t_3^p + t_2^{p^2} \bmod (p,\, u_1^2)$.

Remarque. A propos du point *c)*. Avec le logiciel Pari GP, j'ai pu vérifier pour $p = 3, 5, 7, 11, 13$, qu'on a la formule suivante :

$$-t_0^{p^2-1} t_1 u_1^{p+1} + t_1 = \sum_{i=1}^{p-1} -\frac{1}{p}\binom{p}{i} t_0^{ip^2} t_1^{p(p-i)} u_1^{p+1-i} + t_2^p u_1 + t_1^{p^2} \quad \bmod (p,\, u_1^{2p+1}) \tag{3.1}$$

et ensuite, j'ai pu trouver une preuve de la congruence modulo (p, u_1^{p+1}).

Démonstration. On se place au-dessus de l'anneau $(E_2)_*/(p)$. Pour alléger les notations, on pose $G = G_2$ et $t_i = t_i(g)$.
Comme la série formelle $h_g(x)$ définie un homomorphisme de lois de groupe formel de $g_*G(x, y)$ vers $G(x, y)$, on a :

$$\sum_{i\geq 0}^{G} t_i (g_*(u_1)x^p \underset{g_*G}{+} x^{p^2})^{p^i} = h_g([p]_{g_*G}\, x) = [p]_G(h_g x) = u_1 (\sum_{i\geq 0}^{G} t_i x^{p^i})^p \underset{G}{+} (\sum_{i\geq 0}^{G} t_i x^{p^i})^{p^2}$$

a), b) On en déduit que modulo (x^{p^2+1}),

$$t_0(g_*(u_1)x^p + x^{p^2}) + t_1(g_*(u_1)x^p)^p \equiv u_1(t_0 x + t_1 x^p)^p + t_0^{p^2} x^{p^2} \quad \bmod (x^{p^2+1})$$

d'où par identification des coefficients devant x^p et x^{p^2}, on déduit les identités *a)* et *b)* successivement.
c) Nous allons comparer les coefficients devant x^{p^3}. Commençons par

$$\begin{aligned} & h_g([p]_{g_*G} x) \\ \equiv\ & t_0 \left(g_* u_1 x^p \underset{g_*G}{+} x^{p^2} \right) \underset{G}{+} t_1 \left(g_* u_1\, x^p \underset{g_*G}{+} x^{p^2} \right)^p \underset{G}{+} t_2 \left(g_* u_1\, x^p \underset{g_*G}{+} x^{p^2} \right)^{p^2} \\ \equiv\ & t_0 \left(t_0^{p-1} u_1 x^p \underset{g_*G}{+} x^{p^2} \right) \underset{G}{+} t_1 t_0^{(p-1)p} u_1^p\, x^{p^2} + t_1 x^{p^3} \quad \bmod (u_1^{p+1}, x^{p^3+1}) \end{aligned}$$

Ainsi, le coefficient est égal à $t_1 + c$, où c est le coefficient devant x^{p^3} de

$$t_0 \left(t_0^{p-1} u_1 x^p \underset{g_*G}{+} x^{p^2} \right) \underset{G}{+} t_1 t_0^{(p-1)p} u_1^p\, x^{p^2}$$

Posons $X = t_0^{p-1} u_1 x^p$, $Y = x^{p^2}$ et $Z = t_1 t_0^{(p-1)p} u_1^p\, x^{p^2}$, alors

$$\begin{aligned} t_0 \left(X \underset{g_*G}{+} Y \right) \underset{G}{+} Z &= t_0(X \underset{g_*G}{+} Y) + Z + \sum_{i,j>0} * (t_0 X \underset{g_*G}{+} Y)^i Z^j \\ &\equiv t_0(X \underset{g_*G}{+} Y) + Y + Z + \sum_{i,j>0} * Y^i Z^j - Y \\ &\equiv t_0(X \underset{g_*G}{+} Y) + Y \underset{G}{+} Z - Y \qquad \bmod (u_1^{p+1}, x^{p^3+1}) \end{aligned}$$

D'après le lemme précédent,

$$\begin{aligned} Y \underset{G}{+} Z &\equiv Y + Z - C_{p^2}(Y, Z) \\ &\equiv Y + Z - * x^{p^4} \\ &\equiv Y + Z \quad \bmod (u_1^{p+1}, x^{p^3+1}) \end{aligned}$$

Il reste à considérer $t_0(X \underset{g_*G}{+} Y)$, en appliquant encore une fois le lemme précédent, on a

$$X \underset{g_*G}{+} Y \quad \equiv \quad X + Y + u_1 \sum_{i=0}^{p} u_1^i P_{p+(p-1)i}(X,Y) - C_{p^2}(X,Y)$$

En revenant à la définition de X et Y, on note que dans la somme sur i, pour avoir une constante fois x^{p^3}, il faut nécessairement élever X à la puissance p. Or u_1X^p est divisible par u_1^{p+1}, d'où le coefficient devant x^{p^3} de $X \underset{g_*G}{+} Y$ est égal au coefficient devant x^{p^3} de l'expression suivante :

$$X + Y - C_{p^2}(X,Y) = t_0^{p-1}u_1x + x^{p^2} - \sum_{i=1}^{p^2-1} * x^{pi+p^2(p^2-i)}$$

Or $pi+p^2(p^2-i) = (p-1)(p^3-pi)+p^3 > p^3$ lorsque $i < p^2$. Donc le coefficient est nul et $c = 0$. Passons maintenant au coefficient devant x^{p^3} de

$$\begin{aligned}
[p]_G(h_gx) \quad & \equiv \quad u_1\left(t_0x \underset{G}{+} t_1x^p \underset{G}{+} t_2x^{p^2} \underset{t}{+} \underset{3}{} x^{p^3}\right)^p \underset{G}{+} \left(t_0x \underset{G}{+} t_1x^p \underset{G}{+} t_2x^{p^2} \underset{G}{+} t_3x^{p^3}\right)^{p^2} \\
& \equiv \quad u_1\left(t_0x \underset{G}{+} t_1x^p\right)^p \underset{G}{+} t_0^{p^2}x^{p^2} + u_1t_2^px^{p^3} + t_1^{p^2}x^{p^3} \mod (u_1^{p+1}, x^{p^3+1})
\end{aligned}$$

D'après le lemme précédent, on a

$$\begin{aligned}
u_1\left(t_0x \underset{G}{+} t_1x^p\right)^p \quad & \equiv \quad u_1t_0^px^p + u_1t_1^px^{p^2} - u_1C_{p^2}(t_0x, t_1x^p)^p \\
& \equiv \quad u_1t_0^px^p + u_1t_1^px^{p^2} \mod (u_1^{p+1}, x^{p^3+1})
\end{aligned}$$

Ainsi

$$[p]_G(h_gx) \quad \equiv \quad \left(u_1t_0^px^p + u_1t_1^px^{p^2}\right) \underset{G}{+} t_0^{p^2}x^{p^2} + u_1t_2^px^{p^3} + t_1^{p^2}x^{p^3} \mod (u_1^{p+1}, x^{p^3+1})$$

Posons $A = u_1t_0^px^p$, $B = u_1t_1^px^{p^2}$ et $C = t_0^{p^2}x^{p^2}$. Comme avant, on note que pour obtenir un terme de la forme un coefficient fois x^{p^3} dans $(A+B) \underset{G}{+} C$ à partir de A, il faut nécessairement élever A à la puissance p. Ainsi, il ne peut être multiplié avec B dans notre calcul modulo (u_1^{p+1}). Donc le coefficient devant x^{p^3} de $(A+B) \underset{G}{+} C$ coïncide avec celui devant x^{p^3} de $A \underset{G}{+} C + B \underset{G}{+} C$. Avec le même raisonnement que pour $X \underset{g_*G}{+} Y$, on déduit que le coefficient devant x^{p^3} de $A \underset{G}{+} C$ est nul. Il nous reste donc à considérer $B \underset{G}{+} C$. D'après le lemme précédent, on a

$$\begin{aligned}
B \underset{G}{+} C \quad & \equiv \quad u_1t_1^px^{p^2} + t_0^{p^2}x^{p^2} - u_1C_p(u_1t_1^px^{p^2},\, t_0^{p^2}x^{p^2}) + \sum_{i=1}^{p} P_{p+i(p-1)}(*x^{p^2}, *x^{p^2}) - C_{p^2}(*x^{p^2}, *x^{p^2}) \\
& \equiv \quad u_1t_1^px^{p^2} + t_0^{p^2}x^{p^2} - u_1C_p(u_1t_1^px^{p^2},\, t_0^{p^2}x^{p^2}) + \sum_{i=1}^{p} *\ x^{p^2(p+i(p-1))} - *x^{p^4} \\
& \equiv \quad u_1t_1^px^{p^2} + t_0^{p^2}x^{p^2} - u_1C_p(u_1t_1^p,\, t_0^{p^2})x^{p^3} \mod (u_1^{p+1}, x^{p^3+1})
\end{aligned}$$

Donc le coefficient devant x^{p^3} de la série formelle $[p]_G(h_gx)$ est congrue à

$$u_1t_2^p + t_1^{p^2} - u_1C_p(u_1t_1^p,\, t_0^{p^2})$$

modulo (u_1^{p+1}). D'où la congruence c).
d) Soit $g \equiv 1 \bmod (S^2)$, déterminons le coefficient de x^{p^4} modulo (u_1^2). On a

$$\begin{aligned} h_g([p]_{g_*G}\, x) &\equiv t_0\Big(g_*(u_1)x^p \underset{g_*G}{+} x^{p^2}\Big) \underset{G}{+} t_1\Big(g_*(u_1)x^p \underset{g_*G}{+} x^{p^2}\Big)^p \underset{G}{+} t_2\Big(g_*(u_1)x^p \underset{g_*G}{+} x^{p^2}\Big)^{p^2} \\ &\quad \underset{G}{+} t_3\Big(g_*(u_1)x^p \underset{g_*G}{+} x^{p^2}\Big)^{p^3} \\ &\equiv t_0\left(t_0^{p-1}u_1x^p \underset{g_*G}{+} x^{p^2}\right) \underset{G}{+} t_1x^{p^3} + t_2x^{p^4} \quad \bmod (u_1^p, x^{p^4+1}) \end{aligned}$$

Soient i, j, k trois entiers tels que $pi + p^2j + p^3k = p^4$, alors p divise i, d'où le coefficient devant x^{p^4} de

$$t_0\left(t_0^{p-1}u_1x^p \underset{g_*G}{+} x^{p^2}\right) \underset{G}{+} t_1x^{p^3}$$

est nul modulo (u_1^p). Ainsi, le coefficient devant x^{p^4} de $h_g([p]_{g_*G}\, x)$ est t_2 modulo (u_1^p). D'autre part,

$$\begin{aligned} h_g([p]_{g_*G}\, x) &\equiv u_1(\ t_0x \underset{G}{+} t_1x^p \underset{G}{+} t_2x^{p^2} \underset{(G)}{+} t_3x^{p^3}\ )^p \underset{G}{+} (\ t_0x \underset{G}{+} t_1x^p \underset{(G)}{+} t_2x^{p^2}\ )^{p^2} \\ &\equiv u_1(\ t_0x \underset{G}{+} t_1x^p \underset{G}{+} t_2x^{p^2}\ )^p \underset{G}{+} (\ t_0x \underset{G}{+} t_1x^p\ )^{p^2} + (\ u_1t_3^p + t_2^{p^2}\ )x^{p^4} \quad \bmod (u_1^2, x^{p^4+1}) \end{aligned}$$

Ainsi, le coefficient devant x^{p^4} est $u_1t_3^p + t_2^{p^2} + e$. Or $t_1 \equiv g_1 \equiv 0 \bmod (u_1)$, d'où

$$\begin{aligned} &u_1(\ t_0x \underset{G}{+} t_1x^p \underset{G}{+} t_2x^{p^2}\ )^p \underset{G}{+} (\ t_0x \underset{G}{+} t_1x^{p^2}\ )^{p^2} \\ \equiv\ &u_1(\ t_0x \underset{G}{+} t_2x^{p^2}\ )^p \underset{G}{+} (t_0x)^{p^2} \quad \bmod (u_1^2, x^{p^4+1}) \end{aligned}$$

De même qu'avant si $ip + jp^2$ est égal à p^4 alors i est divisible par p. D'où le coefficient de degré p^4 de l'expression précédente est égale au coefficient de degré p^4 de $u_1(\ t_0x \underset{G}{+} t_2x^{p^2}\ )^p$. D'après le lemme 3.3, il nous faut trouver le coefficient de degré p^4 d'une série formelle de la forme suivante

$$u_1(t_0x + t_2x^{p^2} + \sum_{i\geq 1} P_{1+(q-1)i}(t_0x, t_2x^{p^2}))^p$$

or $P_{1+(q-1)i}(t_0x, t_2x^{p^2}) = \sum_{1\leq j\leq (q-1)i} a_{ij}t_0^jt_2^{(q-1)i-j}x^{(p^2-1)(ip^2-j)}$ et p^2-1 ne divise pas p^3. Ce qui implique que le coefficient e est nul. □

Lemme 3.3 (cf. lemme 4.4 [HKM08]). *On a*

$$G_2(x, y) \equiv x + y + \sum_{i\geq 1} P_{1+(p^2-1)i}(x, y) \quad \bmod (p, u_1)$$

où $P_{1+(p^2-1)i}$ *est homogène de degré* $1 + (p^2-1)i$ *symétrique sans les termes* $x^{1+(p^2-1)i}$ *et* $y^{1+(p^2-1)i}$.

Démonstration. Par définition de G_2, il suffit de montrer le résultat pour F_2 (voir page 15). Considérons la graduation sur $(E_2)_*$ donnée dans la partie 1. Soient P_j des polynômes homogènes de degré $-2j$, tels que :

$$F_2(x, y) = x + y + \sum_{j\geq 1} P_j(x, y) \ \bmod (p,\ u_1)$$

Comme F_2 est homogène de degré -2, on déduit que les coefficients de P_j appartiennent à $(E_2)_{2j-2}$. De plus les coefficients sont dans l'adhérence du sous-anneau engendré par $|v_1| = |u_1 u^{1-p}| = 2(p-1)$ et $|v_2| = |u^{1-p^2}| = 2(p^2-1)$. Or on regarde modulo (p, u_1), donc p^2-1 divise $j-1$. □

Corollaire 3.4 (cf. corollaire 4.5 [HKM08]). *Si $g \equiv 1 + g_1 S + g_2 S^2 \bmod (S^3)$, alors*

$$t_0 \equiv 1 + g_1^p u_1 - g_1 u_1^p + (g_2 - g_2^p) u_1^{p+1} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{p+1+i} + g_1^2 u_1^{2p} \mod (p,\, u_1^{2p+1})$$

$$t_1 \equiv g_1 + g_2^p u_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{i+1} \mod (p,\, u_1^{p+1})$$

Remarque 3.5. *En particulier, on a*

$$t_0 \equiv 1 + g_1^p u_1 - g_1 u_1^p + (g_2 - g_2^p) u_1^{p+1} + g_1^p u_1^{p+2} + \frac{p-1}{2} g_1^{2p} u_1^{p+3} \mod (p,\, u_1^{p+4})$$

Dans la suite, pour les différentes applications, on aura juste besoin de la congruence précédente et pas celle du corollaire.

Au passage, pour tout $g \in \mathbb{S}_2$, comme $g_* u_1 \equiv t_0(g)^{p-1} u_1 \mod (p)$ et $g_* u = t_0(g) u$, on déduit du corollaire qu'un élément $g \equiv 1 \bmod (S^2)$ (i.e : $g \in F_1 S_2$) agit trivialement sur $(E_2)_*/(p)$ modulo (u_1^{p+1}). De même, un élément $g \equiv 1 \mod (S^3)$ (i.e : $g \in F_{3/2} S_2$) agit trivialement sur $(E_2)_*/(p)$ modulo (u_1^{2p+1}).

Démonstration. Commençons par montrer la seconde congruence. D'après la relation c) de la proposition précédente et le fait que $t_i \equiv g_i \bmod (u_1)$,

$$\begin{aligned} t_1 &\equiv t_1^{p^2} + u_1 t_2^p - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} t_1^{pi} t_0^{p^2(p-i)} \\ &\equiv g_1^{p^2} + u_1 g_2^p - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} g_1^{pi} \\ &\equiv g_1 + u_1 g_2^p - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} g_1^{pi} \mod (u_1^{p+1}) \end{aligned}$$

Avant de montrer le premier point avec la bonne précision, donnons une congruence plus faible. D'après l'identité *b*) de la proposition : $t_0 = t_0^{p^2} + u_1 t_1^p - t_0^{p(p-1)} t_1 u_1^p$, on déduit que $t_0 = 1 + g_1^p u_1$ modulo (u_1^3). Ainsi, en appliquant cette première approximation de t_0 et celle de t_1 à l'identité *b*) de la proposition, on a

$$\begin{aligned} t_0 &= t_0^{p^2} + u_1 t_1^p - t_0^{p(p-1)} t_1 u_1^p \\ &\equiv 1 + u_1(g_1^p + g_2^{p^2} u_1^p - g_1 u_1^{2p}) - (1 + g_1 u_1^p)^{p-1}(g_1 + g_2^p u_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} g_1^{pi}) u_1^p \\ &\equiv 1 + u_1(g_1^p + g_2^{p^2} u_1^p - g_1 u_1^{2p}) - (g_1 + g_2^p u_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} u_1^{i+1} g_1^{pi}) u_1^p - (p-1) g_1^2 u_1^{2p} \\ &\equiv 1 + u_1 g_1^p - g_1 u_1^p + (g_2 - g_2^p) u_1^{p+1} + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} g_1^{pi} u_1^{p+1+i} + g_1^2 u_1^{2p} \mod (u_1^{2p+1}) \end{aligned}$$

□

Corollaire 3.6. *Soient $g \equiv 1 + g_1 S + g_2 S^2 \mod (S^3)$, s un entier relatif et k un entier naturel. Supposons que $g_2 \in \mathbb{F}_p \subset \mathbb{F}_{p^2}$.*

i) $t_0(g^k) \equiv t_0(1 + kg_1 S)$ *modulo* $(p,\ u_1^{2p+1})$.

ii) $t_0(g)^s \equiv (1 + g_1^p u_1)^s - sg_1 u_1^p - s(s-1) g_1^{p+1} u_1^{p+1}$
$+s\Big(g_1^p - \binom{s-1}{2} g_1^{2p+1}\Big) u_1^{p+2} + s\Big((\frac{p-1}{2} + s - 1) g_1^{2p} - \binom{s-1}{3} g_1^{3p+1}\Big) u_1^{p+3}$ *modulo* $(p,\ u_1^{p+4})$.

iii) $t_0(g^k)^s \equiv (1 + kg_1^p u_1)^s - skg_1 u_1^p - s(s-1) k^2 g_1^{p+1} u_1^{p+1}$
$+sk(g_1^p - \binom{s-1}{2} k^2 g_1^{2p+1}) u_1^{p+2} + s(\frac{p-1}{2} k^2 g_1^{2p} - \binom{s-1}{3} k^4 g_1^{3p+1}) u_1^{p+3}$ *modulo* $(p,\ u_1^{p+4})$.

Démonstration. i) Comme $g^k \equiv 1 + kg_1 S + (\frac{k^2}{2} g_1^{p+1} + g_2) S^2 \mod (S^3)$ et que $g_1^{p+1}, g_2 \in \mathbb{F}_p$, on déduit immédiatement du corollaire précédent que $t_0(g^k) \equiv t_0(1 + kg_1 S)$ modulo (p, u_1^{2p+1}).

ii) Comme nous sommes en caractéristique p, $t_0(g)^{p^2} \equiv 1 \mod (p, u_1^{p^2})$. Ainsi, $t_0(g)^s$ avec la précision demandée dans le point ii) ne dépend que de s modulo (p^2). On identifie s avec le reste de se division euclidienne par p^2 et nous allons appliquer les formules du binômes classiques. On a

$$\begin{aligned}
& t_0(g)^s \\
\equiv\ & (1 + g_1^p u_1 - g_1 u_1^p + g_1^p u_1^{p+2} + \frac{p-1}{2} g_1^{2p} u_1^{p+3})^s \\
\equiv\ & (1 + g_1^p u_1)^s + s\Big(1 + g_1^p u_1\Big)^{s-1} \Big(- g_1 u_1^p + g_1^p u_1^{p+2} + \frac{p-1}{2} g_1^{2p} u_1^{p+3}\Big) \\
\equiv\ & (1 + g_1^p u_1)^s + s\Big(1 + (s-1) g_1^p u_1 + \binom{s-1}{2} g_1^{2p} u_1^2 + \binom{s-1}{3} g_1^{3p} u_1^3\Big) \times \\
& \Big(- g_1 u_1^p + g_1^p u_1^{p+2} + \frac{p-1}{2} g_1^{2p} u_1^{p+3}\Big) \\
\equiv\ & (1 + g_1^p u_1)^s - sg_1 u_1^p + sg_1^p u_1^{p+2} + \frac{p-1}{2} sg_1^{2p} u_1^{p+3} - s(s-1) g_1^{p+1} u_1^{p+1} + s(s-1) g_1^{2p} u_1^{p+3} \\
& -s\binom{s-1}{2} g_1^{2p+1} u_1^{p+2} - s\binom{s-1}{3} g_1^{3p+1} u_1^{p+3} \\
\equiv\ & (1 + g_1^p u_1)^s - sg_1 u_1^p - s(s-1) g_1^{p+1} u_1^{p+1} \\
& +s\Big(g_1^p - \binom{s-1}{2} g_1^{2p+1}\Big) u_1^{p+2} + s\Big((\frac{p-1}{2} + s - 1) g_1^{2p} - \binom{s-1}{3} g_1^{3p+1}\Big) u_1^{p+3}
\end{aligned}$$

modulo $(p,\ u_1^{p+4})$.

iii) En utilisant le point précédent, on a

$$\begin{aligned}
t_0(g^k) &\equiv t_0(1 + kg_1 S)^s \\
&\equiv (1 + kg_1^p u_1)^s - skg_1 u_1^p - s(s-1) k^2 g_1^{p+1} u_1^{p+1} \\
&\quad +s(kg_1^p - \binom{s-1}{2} k^3 g_1^{2p+1}) u_1^{p+2} + s(\frac{p-1}{2} k^2 g_1^{2p} - \binom{s-1}{3} k^4 g_1^{3p+1}) u_1^{p+3}
\end{aligned}$$

modulo $(p,\ u_1^{p+4})$.

$\square$

$$(E_2)_*^F/(p) \xrightarrow{\partial_1^*} (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, h_0 \oplus \mathbb{F}_p\, h_1) \xrightarrow{\partial_2^*} (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, g_0 \oplus \mathbb{F}_p\, g_1) \xrightarrow{\partial_3^*} (E_2)_*^F/(p)$$

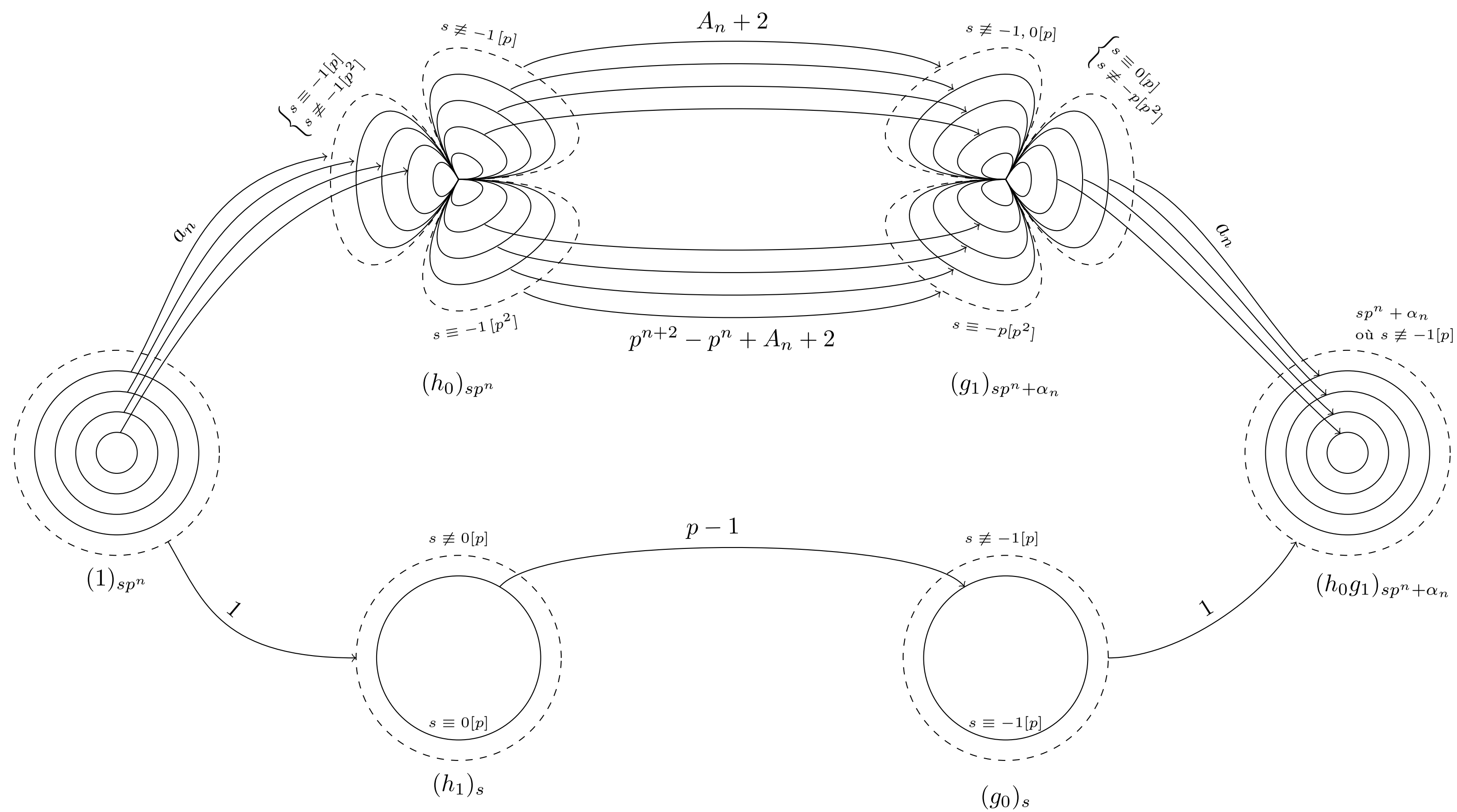

Figure 3.1 – La figure de Hopkins et Mahowald pour $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$

Chapitre 4

Cohomologie à coefficients dans $(E_2)_*$ modulo p

Dans ce chapitre, nous allons, à l'aide de l'approximation de la résolution projective C_* donnée dans le théorème 2.10, déterminer les groupes de cohomologie continue $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$. L'anneau $(E_2)_*/(p)$ étant muni d'une structure de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module profini, en utilisant par exemple le développement fait dans la section 9.8 *Cohomology groups from resolutions* de [Wil98]), on a :

$$H^*(\mathbb{G}_2^1, (E_2)_*/(p)) = H_*(\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_*, (E_2)_*/(p)))$$

où C_* est la résolution projective déterminée dans le théorème 2.10.
D'après la proposition 1.31 et le lemme de Shapiro, le complexe de chaînes $\mathrm{Hom}_{\mathbb{G}_2^1}(C_*, (E_2)_*/(p))$ s'identifie à un nouveau complexe de chaînes plus abordable pour les calculs :

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{G}_2^1}(C_0, M) \arrow[r, "\partial_1^*"] \arrow[d, "\mathrm{ev}_{e_0}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_1, M) \arrow[r, "\partial_2^*"] \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_2, M) \arrow[r, "\partial_3^*"] \arrow[d, "\mathrm{ev}_{e_2}"', "\cong"] & \mathrm{Hom}_{\mathbb{G}_2^1}(C_3, M) \arrow[d, "\mathrm{ev}_{e_3}"', "\cong"] \\
(E_2)_*^F/(p) \arrow[r, "\partial_1^*"] & (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, h_0 \oplus \mathbb{F}_p\, h_1) \arrow[r, "\partial_2^*"] & (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, g_0 \oplus \mathbb{F}_p\, g_1) \arrow[r, "\partial_3^*"] & (E_2)_*^F/(p)
\end{tikzcd}$$

où $M = (E_2)_*/(p)$, $h_0 = u^{1-p}$ et $h_1 = u^{p-1}$ sont dans l'image de ev_{e_1} et $g_0 = u^{1-p}$ et $g_1 = u^{p-1}$ sont dans l'image de ev_{e_2}.

Soit g un élément du groupe stabilisateur de Morava $\mathbb{S}_2$, d'après le lemme 1.6, modulo (p), on a $g_*u_1 \equiv t_0(g)^{p-1}u_1$ et $g_*u = t_0(g)u$, d'où $g_*v_1 \equiv v_1$. Donc $\mathbb{F}_p[v_1]$ est inclus dans $H^0(\mathbb{G}_2^1, (E_2)_*/(p))$, ainsi la multiplication à gauche induit une structure de $\mathbb{F}_p[v_1]$-module sur $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p))$ et les homomorphismes ∂_i^* sont $\mathbb{F}_p[v_1]$-linéaires et continues. De la description de $(E_2)_*/(p)$ donnée dans la proposition 1.31 et ses corollaires, on déduit que la famille d'élément $\mathcal{B} := (v_2^s)_{s\in\mathbb{Z}}$ est $\mathbb{F}_p[v_1]$-libre et engendre un sous-module dense. La famille $\mathcal{B}$ est une sorte de base topologique. Plus précisément, si l'on munit $\mathbb{F}_p[v_1]$ de la topologie discrète, alors le $\mathbb{F}_p[v_1]$-module gradué $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p))$ est complet pour la topologie induite par la filtration (v_1)-adique. Dans la catégorie des $\mathbb{F}_p[v_1]$-modules gradués complets, on a

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{v_2^s\}, \quad \text{pour } i = 0, 3 \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{v_2^s\, u^{1-p}\} \,\oplus\, \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{v_2^s\, u^{p-1}\}, \quad \text{pour } i = 1, 2
\end{aligned}$$

On notera aussi que l'homomorphisme ∂_1^* est uniquement déterminé par l'image des éléments de la famille $(v_2^s)_{s\in\mathbb{Z}}$.

Lemme 4.1. *1. Soit $(v_{2,s})_{s\in\mathbb{Z}}$ une famille d'éléments de $(E_2)_*^F/(p)$ tels que $v_{2,s} \equiv v_2^s$ modulo (u_1) alors,*

$$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\,\{v_{2,s}\}$$

où $i = 0, 3$.

2. *Soient* $(\zeta_{0,s})_{s\in\mathbb{Z}}$ *et* $(\zeta_{1,s})_{s\in\mathbb{Z}}$ *deux familles d'éléments de* $(E_2)^F_*/(p)$ *tels que* $\zeta_{i,s} \equiv v_2^s$ *modulo* (u_1) *alors,*

$$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{\zeta_{0,s}u^{1-p}\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{\zeta_{1,s}u^{p-1}\}$$

où $i = 1, 2$.

Le théorème suivant résume les différents résultats concernant ces bases et la figure 3.1 en donne une illustration graphique suggérée par Hopkins et Mahowald (voir [Sad93]). Dans la figure 3.1, les cercles concentriques et les boucles représentent des ensembles de la forme $\{(X)_{sp^n};\ n \text{ fixé}\}$ ou $\{(X)_{sp^n+\alpha_n};\ n \text{ fixé}\}$, où $X \in \{1, h_0, h_1, g_0, g_1, h_0g_1\}$ et plus le diamètre est petit plus n est grand.

Théorème 4.2. *Soit* $p \geq 5$ *premier. Il existe* $(X)_s$ *des éléments homogènes de* $(E_2)_*/(p)$ *où* s *parcourt l'ensemble des entiers relatifs et* X *parcourt* $\{1, h_0, h_1, g_0, g_1, h_0g_1\}$*, tels que :*

1. *Pour tout* $X \in \{1, h_0, h_1, g_0, g_1, h_0g_1\}$*, il existe* $c \in \mathbb{F}_p^\times$ *tel que :*

$$(X)_s \equiv c\, X\, v_2^s \mod (p, u_1)$$

2. *On a les isomorphismes de* $\mathbb{F}_p[v_1]$*-modules gradués complets suivants :*

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(g_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(g_1)_s\} \\
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_3, (E_2)_*/(p)) &\cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_0g_1)_s\}
\end{aligned}$$

3. *Les homomorphismes* ∂_i^* *sont diagonales dans ces bases :*

$$\begin{aligned}
\partial_1^*(1)_{sp^n} &= \begin{cases} 0 & si\ s = 0 \\ v_1(h_1)_s & si\ n = 0,\ s \not\equiv 0\ [p] \\ v_1^{a_n}\,(h_0)_{(sp-1)p^{n-1}} & si\ n \geq 1,\ s \not\equiv 0\ [p] \end{cases} \\
\partial_2^*(h_0)_{sp^n} &= \begin{cases} 0 & si\ s = 0 \\ v_1^{A_n+2}\,(g_1)_{sp^n+\alpha_n} & si\ n \geq 0,\ s \not\equiv 0, -1\ [p] \\ v_1^{p^{n+2}-p^n+A_n+2}\,(g_1)_{(s+1-p)p^n+\alpha_n} & si\ n \geq 0,\ s \equiv -1\ [p^2] \end{cases} \\
\partial_2^*(h_1)_{sp} &= v_1^{p-1}(g_0)_{sp-1} \\
\partial_3^*(g_0)_s &= v_1(h_0g_1)_s \qquad si\ s \not\equiv -1\ [p] \\
\partial_3^*(g_1)_{sp^n+\alpha_{n-1}} &= v_1^{a_n}\,(h_0g_1)_{sp^n+\alpha_n} \qquad si\ n \geq 1\ et\ s \not\equiv -1\ [p]
\end{aligned}$$

où

$$\begin{aligned}
A_n &= \frac{p^n-1}{p-1}(p+1) \\
a_n &= \begin{cases} p^{n-1}(p+1) - 1 & si\ n > 0 \\ 1 & si\ n = 0 \end{cases} \\
\alpha_n &= \frac{1-p^n}{p-1}
\end{aligned}$$

Remarque. Les précédentes relations entre les différents éléments sont semblables à celles données dans les formules sur les différentielles de la suite spectrale v_1-BSS citées par Behrens dans [Beh12], le théorème 3.2. On remarque une identification plus précise que le simple isomorphisme du au changement d'anneaux $H^*(M_1^1) \cong H^*(\mathbb{G}_2;\ (E_2)_*/(p, v_1^\infty))$.

De la construction de ces bases, on déduit facilement les groupes $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ en utilisant le fait que les différentielles sont des homomorphismes $\mathbb{F}_p[v_1]$-linéaires entre modules libres. A première vue, la description de ces groupes de cohomologie peut facilement être donnée en terme de produit de $\mathbb{F}_p[v_1]$-module. Nous allons montrer qu'en fait les différents sous-modules sont en somme directe. Avant, notons le lemme suivant.

Lemme 4.3. *Soient a, b, t des nombres réels, s un entier et q un entier naturel. Supposons que $a \leq 0 \leq b$.*
a) Si $b - a < q$ et $a \leq t \leq b$ alors, $a \leq t + qs \leq b$ implique $s = 0$.
b) Si $b - a < q$ alors, il existe en plus un entier s tel que $a \leq t + qs \leq b$.

Corollaire 4.4. *Soit $p \geq 5$ premier.*

1.

$$\begin{aligned}
H^0(\mathbb{G}_2^1, (E_2)_*/(p)) &\cong \mathbb{F}_p[v_1]\,(1)_0 \\
H^1(\mathbb{G}_2^1, (E_2)_*/(p)) &\cong \mathbb{F}_p[v_1]\,(h_0)_0 \oplus \bigoplus_{s\not\equiv 0} \mathbb{F}_p\,(h_1)_s \quad \oplus \bigoplus_{n>0,\ s\not\equiv 0} \mathbb{F}_p[v_1]/(v_1^{a_n})\,(h_0)_{(sp-1)p^{n-1}} \\
H^2(\mathbb{G}_2^1, (E_2)_*/(p)) &\cong \bigoplus_{s\not\equiv 0,-1} \mathbb{F}_p[v_1]/(v_1^{A_n+2})\,(g_1)_{sp^n+\alpha_n} \\
&\quad \oplus \bigoplus_{s\equiv -1} \mathbb{F}_p[v_1]/(v_1^{p^{n+2}-p^n+A_n+2})\,(g_1)_{sp^{n+1}+\alpha_n} \\
&\quad \oplus \bigoplus_{n>0} \mathbb{F}_p[v_1]/(v_1^{p-1})\,(g_0)_{sp^n-1} \\
H^3(\mathbb{G}_2^1, (E_2)_*/(p)) &\cong \bigoplus_{s\not\equiv -1} \mathbb{F}_p[v_1]/(v_1^{a_n})\,(h_0 g_1)_{sp^n+\alpha_n}
\end{aligned}$$

où les congruences relativement à la variable s sont modulo (p).

2.

$$H^n(\mathbb{G}_2^1, (E_2)_0/(p)) = \begin{cases} \mathbb{F}_p\ (1)_0 & si\ n = 0 \\ \mathbb{F}_p\ (h_0 g_1)_0 & si\ n = 3 \\ 0 & sinon \end{cases}$$

Remarques.
- On déduit en particulier que l'inclusion du module trivial $\mathbb{F}_p$ dans $(E_2)_0/(p)$ induit un isomorphisme $\mathbb{F}_p \cong H^0(\mathbb{G}_2^1, (E_2)_0/(p))$.
- Une autre présentation du précédent corollaire se trouve dans [HS99], la proposition 15.2.

Démonstration. 1. Du théorème, on déduit immédiatement que l'homomorphisme qui va des sommes directes données dans le corollaire dans $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ est injectif.
Rappelons que $v_1^{p+1} v_2^{-1} = u_1^{p+1}$ appartient à $(E_2)_0^F/(p)$, et les modules $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, (E_2)_*/(p))$ sont complets pour la topologie induite par la filtration (u_1^{p+1})-adique de $(E_2)_*^F/(p)$. Soit $X \in \{1, h_0, h_1, g_0, g_1, h_0 g_1\}$, par définitions des éléments $(X)_t$, on note que

$$u_1^{(p+1)i}(X)_t \equiv v_1^{(p+1)i}(X)_{t-i} \mod (u_1^{(p+1)i+1})$$

Ainsi, pour montrer la surjectivité, il nous suffit de montrer qu'en chaque dimension cohomologique et qu'en tout degré, qu'il n' y a qu'un nombre fini d'éléments de la forme $v_1^k(X)_s$, où $X \in \{1, h_0, h_1, g_0, g_1, h_0g_1\}$. Rappelons que $|v_1| = 2(p-1)$, $|v_2| = 2(p^2-1)$, $|h_0| = |g_0| = 2(p-1)$ et $|h_1| = |g_1| = 2(1-p)$. Ainsi, d'après la proposition 1.31, on note que le degré d'un élément est nécessairement de la forme $2(p-1)t$ pour un certain entier relatif t.
Soit $t \in \mathbb{Z}$, supposons que $2(p-1)t$ est le degré du

- 0-cocycle $v_1^k(1)_0$. Alors, $k = t$ est uniquement déterminé.
- 1-cocycle $(h_1)_s$. Alors, $t = (p+1)s$ et s est uniquement déterminé.
- 1-cocycle $v_1^k(h_0)_{(sp-1)p^{n-1}}$, où $n \geq 1$, $s \not\equiv 0[p]$ et $0 \leq k < p^n + p^{n-1} - 1$. Alors $t = k + 1 + (sp-1)p^{n-1}(p+1)$, ainsi on a

$$0 \leq t - 1 + (sp-1)p^{n-1}(p+1) < (p+1)p^{n-1} - 1$$

  D'après le lemme précédent, pour n fixé, il y a au plus un entier s qui convient. De plus, si n est tel que $(p+1)p^{n-1} > t$ alors nécessairement $s = 0$, or $s \not\equiv 0[p]$. D'où un nombre fini de solution.
- 2-cocycle $v_1^k(h_0)_0$. Alors $t = k+1$ et k est uniquement déterminé.
- 2-cocycle $v_1^k(g_1)_{sp^n+\alpha_n}$ où $s \not\equiv 0, -1[p]$ et $0 \leq k < A_n+2$. Alors $t = k-1+(sp^n+\alpha_n)(p+1)$ et

$$0 \leq \frac{t+1}{p+1} - sp^n + \frac{p^n-1}{p-1} < \frac{p^n-1}{p-1} + \frac{2}{p+1} \quad \Rightarrow \quad \frac{1-p^n}{p-1} \leq \frac{t+1}{p+1} - sp^n \leq 0$$

  Notons que $\frac{p^n-1}{p-1} < p^n$, ainsi, d'après le lemme précédent, pour un entier n fixé, il existe au plus un entier s solution et si n est tel que $\frac{1-p^n}{p-1} \leq \frac{t+1}{p+1}$ alors il n'y a pas de solution non nul.
- 2-cocycle $v_1^k(g_1)_{sp^{n+1}+\alpha_n}$ où $s \equiv -1[p]$ et $0 \leq k < p^{n+2} - p^n + A_n + 2$. Alors $t = k - 1 + (sp^{n+1} + \alpha_n)(p+1)$ et

$$\begin{aligned} & 0 \leq \frac{t+1}{p+1} - sp^{n+1} + \frac{p^n-1}{p-1} < (p-1)p^n + \frac{p^n-1}{p-1} + \frac{2}{p+1} \\ \Rightarrow \quad & \frac{1-p^n}{p-1} \leq \frac{t+1}{p+1} - sp^{n+1} \leq (p-1)p^n \end{aligned}$$

  Notons que $(p-1)p^n - \frac{1-p^n}{p-1} = p^{n+1} - p^n + \frac{p^n-1}{p-1} < p^{n+1}$, ainsi on conclut de la même manière que pour le cas précédent.
- 2-cocycle $v_1^k(g_0)_{sp-1}$ où $0 \leq k \leq p-1$. Alors, $t = k - 1 + (sp-1)(p+1)$ et $0 \leq t + 1 - (sp-1)(p+1) < p - 1$. Ainsi d'après le lemme précédent, il existe au plus un entier s solution.
- 3-cocycle $(h_0g_1)_s$ où $s \not\equiv\equiv -1[p]$. Alors $k = (p+1)s$ et s est uniquement déterminé.
- 3-cocycle $v_1^k(h_0g_1)_{sp^n+\alpha_n}$ où $n \geq 1$, $s \not\equiv -1[p]$ et $0 \leq k < p^{n-1}(p+1) - 1$. Alors, $t = k + (sp^n + \alpha_n)(p+1)$ et

$$0 \leq \frac{t}{p+1} - sp^n + \frac{p^n-1}{p-1} < p^{n-1} \quad \Rightarrow \quad 0 \leq \frac{t(p-1)}{p+1} - 1 + (1 - s(p-1))p^n < p^{n-1}(p-1)$$

  On applique une dernière fois le lemme précédent pour voir à nouveau que pour n fixé, il existe au plus une solution s et si n est assez grand, il n'y a pas de solution s.

2. Il suffit de reprendre la preuve du point précédent avec $t = 0$. □

Le corollaire suivant, nous sera utile dans le chapitre 5 sur le groupe de Picard algébrique.

Corollaire 4.5. *Soit $p \geq 5$ premier,*

1. $H^n(\mathbb{G}_2^1,(E_2)_0) = \begin{cases} \mathbb{Z}_p & si\ n=0,3 \\ 0 & sinon \end{cases}$
2. *L'inclusion* $\mathbb{Z}_p \to (E_2)_0$ *induit un isomorphisme* $\mathbb{Z}_p \cong H^0(\mathbb{G}_2^1,(E_2)_0)$.
3. $H^0(\mathbb{G}_2^1,(E_2)_0^\times) \cong \mathbb{Z}_p^\times$.

Démonstration. 1. De la suite exacte longue en cohomologie associé à $(E_2)_0 \xrightarrow{p} (E_2)_0 \to (E_2)_0/(p)$, on déduit une suite exacte de la forme $H^n(\mathbb{G}_2^1,(E_2)_0) \xrightarrow{p} H^n(\mathbb{G}_2^1,(E_2)_0) \to 0$ pour $n \neq 0,3$. Ainsi, d'après le lemme de Nakayama (théorème A.6) appliqué aux groupes de cohomologie qui sont en particulier profinis, on a que ces derniers groupes de cohomologie sont triviaux. Soit $n=0,3$, on a alors la suite exacte courte suivante :

$$0 \to H^n(\mathbb{G}_2^1,(E_2)_0) \xrightarrow{p} H^n(\mathbb{G}_2^1,(E_2)_0) \to \mathbb{F}_p \to 0$$

De plus, les groupes de cohomologies sont des $\mathbb{Z}_p$-modules de type fini, d'où le corollaire.

2. L'inclusion $i : \mathbb{Z}_p \to (E_2)_0$ est un homomorphismes de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-modules, où $\mathbb{Z}_p$ est muni d'une action triviale. D'après le corollaire précédent, la réduction de l'inclusion modulo (p) induit un isomorphisme. De plus, on a le diagramme suivant :

$$\begin{tikzcd} \mathbb{Z}_p = H^0(\mathbb{G}_2^1,\mathbb{Z}_p) \arrow[r, "\mathrm{mod}\,(p)"] \arrow[d, "i^*"'] & H^0(\mathbb{G}_2^1,\mathbb{F}_p) \cong \mathbb{F}_p \arrow[d, "\cong"] \\ \mathbb{Z}_p \cong H^0(\mathbb{G}_2^1,(E_2)_0) \arrow[r, "\mathrm{mod}\,(p)"] & H^0(\mathbb{G}_2^1,(E_2)_0/(p)) \cong \mathbb{F}_p \end{tikzcd}$$

D'où, le second point du lemme.

3. Par définition, $H^0(\mathbb{G}_2^1,(E_2)_0^\times)$ est le sous-module de $(E_2)_0^\times$ des éléments invariants sous l'action de $\mathbb{G}_2^1$, ainsi $H^0(\mathbb{G}_2^1,(E_2)_0^\times) = H^0(\mathbb{G}_2^1,(E_2)_0) \cap (E_2)_0^\times$.

□

4.1 Les groupes d'homotopie stable rationnelle de $L_{K(2)}S^0$

Dans cette section, on montre dans le cas $p \geq 5$ des résultats équivalents à ceux donnés dans [GHM12] pour $p=3$.

Proposition 4.6 (cf. proposition 4.2 [GHM12])**.** *Supposons que* $p \geq 5$,

1. *Pour tout* $t \not\equiv 0[p-1]$, $H^*(\mathbb{G}_2,(E_2)_{2t}) = 0$.
2. *Pour tout* $t=(p-1)p^k m$ *avec* m *est premier à* p, *on a* $p^{k+1}H^*(\mathbb{G}_2,(E_2)_{2t}) = 0$.

Démonstration. Rappelons que u est de degré -2.

1. Soit $\boldsymbol{\mu}_{p-1}$ le sous-groupe des racines $p-1$-ème de l'unité de $\mathbb{Z}_p$. On se donne ξ un générateur de ce dernier groupe. De la description de $\mathbb{G}_2$, on voit que $\boldsymbol{\mu}_{p-1}$ est un sous-groupe du centre de $\mathbb{G}_2$. Ainsi, on a une suite spectrale Lyndon-Hochschild-Serre :

$$H^m(\mathbb{G}_2/\boldsymbol{\mu}_{p-1}, H^n(\boldsymbol{\mu}_{p-1},(E_2)_{-2t}) \Rightarrow H^{m+n}(\mathbb{G}_2,(E_2)_{-2t})$$

La multiplication avec $|\boldsymbol{\mu}_{p-1}|$ est un isomorphisme de $(E_2)_{-2t}$, ainsi par un argument classique utilisant le transfert en cohomologie, on déduit que $H^p(\boldsymbol{\mu}_{p-1},(E_2)_{-2t})$ est trivial lorsque $m>0$. Ainsi la suite spectrale dégénère. D'après le lemme 1.4, le groupe $\boldsymbol{\mu}_{p-1}$ agit trivialement sur $(E_2)_0$ et $\xi_* u^t = \xi^t u^t$, donc $H^0(\boldsymbol{\mu}_{p-1},(E_2)_{-2t})$ est trivial lorsque $t \not\equiv 0[p-1]$. D'où, en revenant à la suite spectrale, on a bien le point 1. de la proposition.

2. Supposons que $t = (p-1)p^k m$ avec m premier à p. Comme p ne divise pas 2, on a $\mathbb{G}_2 \cong \mathbb{G}_2^1 \times \mathbb{Z}_p$ où $\mathbb{Z}_p$ s'identifie avec le sous-groupe engendré par $\psi = 1+p$ dans $\mathbb{Z}_p^\times$ le centre de $\mathbb{G}_2$. On applique encore une fois la suite spectrale de Lyndon-Hochschild-Serre :

$$H^p(\mathbb{G}_2^1, H^q(\mathbb{Z}_p, (E_2)_{-2t})) \Rightarrow H^{p+q}(\mathbb{G}_2, (E_2)_{-2t})$$

Notons que la suite

$$0 \longrightarrow \mathbb{Z}_p[\![\mathbb{Z}_p]\!] \xrightarrow{\psi-1} \mathbb{Z}_p[\![\mathbb{Z}_p]\!] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

est une résolution projective (voir lemme A.17). D'où

$$H^*(\mathbb{Z}_p, (E_2)_{-2t}) = H^*(\ (E_2)_{-2t} \xrightarrow{\psi-1} (E_2)_{-2t} \longrightarrow 0 \longrightarrow \dots\ )$$

D'autre part, en utilisant le fait que $(1+p)^{p^k} \equiv 1\ [p^{k+1}]$, on peut montrer que

$$\begin{aligned}(\psi-1)_* u^t &= (\psi^t - 1)u^t \\ &= ((1+p)^{(p-1)mp^k} - 1)u^t \\ &\equiv (p-1)p^{k+1} m u^t \mod (p^{k+2})\end{aligned}$$

On en déduit que $H^*(\mathbb{Z}_p, (E_2)_{-2t})$ est de p^{k+1}-torsion.

□

Corollaire 4.7. *Soit $X = S^0$ ou $V(0)$ le spectre de Moore. La page $E_2^{*,*}$ de la suite spectrale d'Adams-Novikov*

$$E_2^{s,t} = H^s(\mathbb{G}_2, (E_2)_t X) \Rightarrow \pi_{t-s}(L_{K(2)}X)$$

dégénère sans problème d'extension. Plus précisément, pour tout $m \in \mathbb{Z}$,

$$\pi_m(L_{K(2)}X) \cong \begin{cases} H^s(\mathbb{G}_2, (E_2)_{m+s}X) & \text{si } m \equiv -s\ [2(p-1)] \text{ pour un certain } 0 \le s \le 4, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. La première propriété de la proposition, nous dit que les groupes d'homologie non triviaux sur la page E_2 sont éparses. Il faut en effet que t soit un multiple de $2(p-1)$ pour que $E_2^{s,t}$ puisse être non trivial. D'autre part, le p-Sylow de $\mathbb{G}_2$ est un groupe à dualité de Poincaré de dimension 4. Ainsi, on a une ligne d'annulation sur la page E_2, i.e : pour tout $s \geq 4$ et pour tout t, $E_2^{s,t} = 0$. D'où, l'on déduit qu'il n'y a pas de différentielle non triviale à partir de la page E_2. La convergence de la suite spectrale, nous donne alors les isomorphismes. □

Théorème 4.8. *En degré 0, on a*

$$H^n(\mathbb{G}_2, (E_2)_0) \cong \begin{cases} \mathbb{Z}_p & \text{si } n = 0,1,3 \text{ ou } 4 \\ 0 & \text{sinon} \end{cases}$$

Démonstration. On rappelle que $\mathbb{G}_2^1$ est le noyau du déterminant réduit (définition 1.11). Comme p ne divise pas n, on a $\mathbb{G}_2 \cong \mathbb{G}_2^1 \times \mathbb{Z}_p$. Ainsi, $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \cong \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \hat{\otimes} \mathbb{Z}_p[\![\mathbb{Z}_p]\!]$. D'après la proposition 1.4, l'action de $\mathbb{Z}_p \cong 1 + p\mathbb{Z}_p$ est triviale sur $(E_2)_0$. Soit M le module $(E_2)_0$ vu comme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module et N le $\mathbb{Z}_p[\![\mathbb{Z}_p]\!]$-module trivial $\mathbb{Z}_p$, alors $M \hat{\otimes} N$ muni de l'action diagonale de $\mathbb{G}_2 \cong \mathbb{G}_2^1 \times \mathbb{Z}_p$ est naturellement isomorphe à $(E_2)_0$ en tant que $\mathbb{Z}_p[\![\mathbb{G}_2]\!]$-module.
D'autre part, en utilisant la résolution projective C_* de $\mathbb{Z}_p$ au-dessus de $\mathbb{G}_2^1$ et la résolution libre

$$0 \longrightarrow \mathbb{Z}_p[\![\mathbb{Z}_p]\!] \xrightarrow{\psi-1} \mathbb{Z}_p[\![\mathbb{Z}_p]\!] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

de $\mathbb{Z}_p$ au-dessus de U_1, notée P_*, on déduit l'isomorphisme suivant

$$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2]\!]}(C_*\hat{\otimes}P_*,(E_2)_0)\cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_*,(E_2)_0)\hat{\otimes}\,\mathrm{Hom}_{\mathbb{Z}_p[\![U_1]\!]}(P_*,\mathbb{Z}_p)$$

Comme $H^*(U_1,\mathbb{Z}_p)=\Lambda(\zeta)=\mathbb{Z}_p[\zeta]/(\zeta^2)$, où ζ est un générateur de $H^1(U_1,\mathbb{Z}_p)$, est constituée de $\mathbb{Z}_p$-modules libres, l'on déduit de l'isomorphisme de Künneth (profini), l'isomorphisme suivant :

$$H^*(\mathbb{G}_2,(E_2)_0)\cong H^*(\mathbb{G}_2^1,(E_2)_0)\,\hat{\otimes}\,\Lambda(\zeta)$$

D'après le proposition 5.5.3 de [RZ10], comme $\Lambda(\zeta)$ est de type fini, le produit tensoriel complété coïncide avec le produit tensoriel algébrique.
D'après le corollaire 4.5, les groupes de cohomologie $H^*(\mathbb{G}_2^1,(E_2)_0)$ sont isomorphe à $\mathbb{Z}_p$ en degré 0 et 3 et sinon triviaux. D'où le théorème. □

Une deuxième conséquence de l'isomorphisme de Künneth,

Corollaire 4.9. *Rationnellement, il existe $\zeta\in\pi_{-1}(L_{K(2)}S^0)$ et $e\in\pi_{-3}(L_{K(2)}S^0)$ induisant un isomorphisme d'algèbres*

$$\pi_*(L_{K(2)}S^0)\otimes\mathbb{Q}\cong\Lambda_{\mathbb{Q}_p}(\zeta,e)$$

4.2 Action de v, w et Λ

Avant de passer aux groupes de cohomologie. Remarquons que les éléments v, w et Λ qui interviennent dans la définition des homomorphismes ∂_1, ∂_2 et ∂_3, sont en particulier dans $\mathbb{Z}_p[\![S_2^1]\!]$. La proposition suivante précise leurs actions sur l'anneau de Lubin-Tate modulo (p).

Proposition 4.10. *Soit s un entier relatif, posons $R_s:=\frac{1}{2}(\binom{s}{p+2}-s\binom{s-1}{2})(\epsilon_+^2-\epsilon_-^2)$. On a*

$$\begin{aligned} v_*u^s &\equiv \epsilon_+(su_1+(\binom{s}{p}-s)u_1^p+(s+R_s)u_1^{p+2})u^s\\ \Lambda_*u^s &\equiv -v_*u^s\\ w_*u^s &\equiv \epsilon_-(-su_1+(\binom{s}{p}-s)u_1^p-(s+R_s)u_1^{p+2})u^s \end{aligned}$$

modulo (p,u_1^{p+4}).

Remarque. Finalement, modulo (u_1^{p+4}), $\Lambda_*=-v_*$ alors que $(g^{-1}-e)_*\neq-(g-e)_*$ en générale. Le fait de prendre la moyenne sous l'action de F élimine les puissances de u_1 à l'origine de la précédente différence.

Démonstration. Tous les calculs dans cette preuve se feront modulo (p,u_1^{p+4}).
Rappelons que si g est un élément de $\mathbb{S}_2$, alors $g_*u:=t_0(g)u$. Donc, en revenant à la définition de v, w et Λ, pour déterminer leurs action sur u^s, il faut au préalable calculer $t_0(a_i^{\pm1})^s$ et $t_0(b_i^{\pm1})^s$. Soient s un entier premier à p et $k=\pm1$. Posons $\xi=\omega^{p-1}$, alors $\xi^p=\xi^{-1}$. D'après le corollaire 3.6, on a :

$$\begin{aligned} (a_{i*}^ku^s)u^{-s} &= t_0(a_i^k)^s = t_0(1+k\xi^i\epsilon_+S)^s\\ &\equiv 1+\sum_{j\geq1}\binom{s}{j}k^j\xi^{-ij}\epsilon_+^ju_1^j-sk\xi^i\epsilon_+u_1^p-s(s-1)\epsilon_+^2u_1^{p+1}\\ &\quad +ks\left(\xi^{-i}\epsilon_+-\binom{s-1}{2}\xi^{-i}\epsilon_+^3\right)u_1^{p+2}+s\left((\frac{p-1}{2}+s-1)\xi^{-2i}\epsilon_+^2-\binom{s-1}{3}\xi^{-2i}\epsilon_+^4\right)u_1^{p+3}\\ (a_{i*}^ku^s)u^{-s} &= t_0(b_i^k)^s = t_0(1+k\xi^i\epsilon_-S)^s\\ &\equiv 1+\sum_{j\geq1}\binom{s}{j}k^j\xi^{-ij}(-\epsilon_-)^ju_1^j-ks\xi^i\epsilon_-u_1^p+s(s-1)\epsilon_-^2u_1^{p+1}\\ &\quad +ks\left(-\xi^{-i}\epsilon_--\binom{s-1}{2}\xi^{-i}\epsilon_-^3\right)u_1^{p+2}+s\left((\frac{p-1}{2}+s-1)\xi^{-2i}\epsilon_-^2+\binom{s-1}{3}\xi^{-2i}\epsilon_-^4\right)u_1^{p+3} \end{aligned}$$

D'autre part,

$$\begin{aligned}
\xi^{-i}+\xi^{i} &= \omega^{(1-p)i}+\omega^{(p-1)i}=2\lambda_i=2\mu_i' \\
\xi^{-i}-\xi^{i} &= \omega^{(1-p)i}-\omega^{(p-1)i}=\frac{2\epsilon_-}{\epsilon_+}\mu_i=\frac{2\epsilon_+}{\epsilon_-}\lambda_i'
\end{aligned}$$

Ainsi, en revenant à la définition de v, w et Λ, on a

$$\begin{aligned}
v &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda_i(a_i-e)+\mu_i(b_i-e), \\
\Lambda &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda_i(a_i^{-1}-e)+\mu_i(b_i^{-1}-e), \\
w &:= \frac{1}{p+1}\sum_{i=0}^{p}\lambda_i'(a_i-e)+\mu_i'(b_i-e),
\end{aligned}$$

on note que v, w et Λ sont des combinaisons d'éléments de la forme :

$$\sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})(a_i-e) \quad \text{et} \quad \sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})(b_i-e)$$

Précisons l'action de la première somme en lien avec les a_i :

$$\begin{aligned}
&(\sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})(a_i^k-e)_*u^s)u^{-s} \\
&\equiv \sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})\Big[\sum_{j=1}^{p+4}\binom{s}{j}k\xi^{-ij}\epsilon_+^j u_1^j-ks\xi^i\epsilon_+u_1^p-s(s-1)\epsilon_+^2u_1^{p+1} \\
&\qquad +ks\left(\xi^{-i}\epsilon_+-\binom{s-1}{2}\xi^{-i}\epsilon_+^3\right)u_1^{p+2}+s\left((\frac{p-1}{2}+s-1)\xi^{-2i}\epsilon_+^2-\binom{s-1}{3}\xi^{-2i}\epsilon_+^4\right)u_1^{p+3}\Big] \\
&\equiv \sum_{i=0}^{p}\sum_{j=1}^{p+4}\binom{s}{j}k^j(\xi^{-i(1+j)}\pm\xi^{-i(1-j)})\epsilon_+^ju_1^j-ks\epsilon_+u_1^p+\pm ks(\epsilon_+-\binom{s-1}{2}\epsilon_+^3)u_1^{p+2} \\
&\equiv \pm ks\epsilon_+u_1+k(\binom{s}{p}-s)\epsilon_+u_1^p+\pm k\Big(\binom{s}{p+2}\epsilon_+^2+s-s\binom{s-1}{2}\epsilon_+^2\Big)\epsilon_+u_1^{p+2} \qquad (A_\pm)
\end{aligned}$$

Pour la dernière identité, j'ai utilisé la propriété suivante :

$$\sum_{i=1}^{p+1}\xi^{ki}=\begin{cases}p+1 & \text{si } p+1\mid k\\ 0 & \text{sinon}\end{cases}$$

sachant que les seuls entiers j compris entre 1 et $p+4$ tels que $1\pm j\equiv 0\ [p+1]$ sont p pour le signe plus et respectivement $1, p+2$ pour le signe moins. Au passage, on remarque qu'on aurait pu factoriser le paramètre k. Considérons maintenant la seconde somme en lien avec les b_i :

$$\begin{aligned}
&(\sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})(b_i^k-e)_*u^s)s^{-s} \\
&\equiv \sum_{i=0}^{p}(\xi^{-i}\pm\xi^{i})\Big[\sum_{j\geq 1}\binom{s}{j}k^j\xi^{-ij}(-\epsilon_-)^ju_1^j-ks\xi^i\epsilon_-u_1^p+s(s-1)\epsilon_-^2u_1^{p+1} \\
&\qquad +ks\left(-\xi^{-i}\epsilon_--\binom{s-1}{2}\xi^{-i}\epsilon_-^3\right)u_1^{p+2}+s\left((\frac{p-1}{2}+s-1)\xi^{-2i}\epsilon_-^2+\binom{s-1}{3}\xi^{-2i}\epsilon_-^4\right)u_1^{p+3}\Big] \\
&\equiv \sum_{i=0}^{p}\sum_{j=1}^{p+4}\binom{s}{j}k^j(\xi^{-i(1+j)}\pm\xi^{-i(1-j)})(-\epsilon_-)^ju_1^j-ks\epsilon_-u_1^p-k\pm s(\epsilon_-\binom{s-1}{2}\epsilon_-^3)u_1^{p+2} \\
&\equiv -\pm ks\epsilon_-u_1+k(\binom{s}{p}-s)\epsilon_-u_1^p+\pm k\Big(\binom{s}{p+2}\epsilon_-^2-s-s\binom{s-1}{2}\epsilon_-^2\Big)\epsilon_-u_1^{p+2} \qquad (B_\pm)
\end{aligned}$$

En revenant à la définition des éléments v et Λ, on note que pour obtenir une approximation de $v_* u^s$ (resp. $\Lambda_* u^s$), il suffit de calculer $\frac{1}{2}((A_+) + \frac{\epsilon_+}{\epsilon_-}(B_-))$ avec $k = 1$ (resp. $k = -1$) :

$$\begin{aligned} v_* u^s &\equiv \epsilon_+ (s u_1 + (\binom{s}{p} - s) u_1^p + (s + R_s) u_1^{p+2}) u^s \\ \Lambda_* u^s &\equiv -v_* u^s \end{aligned}$$

De même, on calcul $\frac{1}{2}(\frac{\epsilon_-}{\epsilon_+}(A_-) + (B_+))$ avec $k = 1$, pour obtenir,

$$w_* u^s \equiv \epsilon_- (-s u_1 + (\binom{s}{p} - s) u_1^p - (s + R_s) u_1^{p+2}) u^s.$$

$\square$

4.3 La première différentielle

On rappelle que $h_0 = u^{1-p}$ et $h_1 = u^{p-1}$, d'après la proposition 1.31,

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0, (E_2)_*/(p)) \arrow[r, "\partial_1^*"] \arrow[d, "\mathrm{ev}_{e_0}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p)) \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] \\ (E_2)_*^F \arrow[r] & (E_2)_*^F/(p) \otimes (\mathbb{F}_p\, h_0 \oplus \mathbb{F}_p\, h_1) \end{tikzcd}$$

et

$$\partial_1^*(\epsilon_+\, v_1^i\, v_2^j\,) = (\partial_1(e_1)_+)_*\, v_1^i\, v_2^j = v_*\, v_1^i\, v_2^j$$

L'homomorphisme ∂_1^* est $\mathbb{F}_p[v_1]$-linéaire. D'autre part, comme $\partial_1(e_1)_+$ s'identifie avec un élément de l'idéal d'augmentation (IS_2^1) de l'algèbre $\mathbb{Z}_p[\![S_2^1]\!]$, on déduit que

$$\mathbb{F}_p[v_1] \subseteq \ker \partial_1^* \tag{4.1}$$

En fait, nous verrons en fin de cette section qu'il y a égalité. Nous construirons aussi de nouvelles bases de telle sorte que l'homomorphisme ∂_1^* soit diagonal dans ces bases.

Avant de déterminer les premiers coefficients de $\partial_1^*(v_2^s)$, à l'aide du corollaire 1.34 sur la structure de $(E_2)_*^F/(p)$ et du fait que l'action du groupe de Morava sur l'anneau gradué de Lubin-Tate se fait par automorphisme de degré 0, on déduit le lemme suivant.

Lemme 4.11. *Soit X un élément de $(E_2)^F_{2(p^2-1)s}$, alors il existe $(\lambda_i), (\mu_i)$ deux suites de nombres p-adiques telles que*

$$\partial_1^*(X) = \sum_{i \geq 0} \lambda_i\, u_1^{(p+1)i}\, v_1\, h_1\, v_2^s + \mu_i\, u_1^{(p+1)i}\, v_1^p\, h_0\, v_2^{s-1}$$

Le fait que l'action de $\mathbb{G}_2$ se fait automorphismes d'anneaux permet aussi de déduire le lemme suivant.

Lemme 4.12. *Soit X un élément de $(E_2)_*^F/(p)$, alors $\partial_1^*(X^p) = \partial_1^*(X)^p$.*

Lemme 4.13. *Soient $s = pq + r$ un entier relatif avec $0 \leq r < p$, alors*

$$\begin{aligned} \partial_1^*(v_2^s) &\equiv s\, v_1\, h_1\, v_2^s + (\, q - s\,)\, v_1^p\, h_0\, v_2^{s-1} + (s + R_s) v_1^{p+2} h_1 v_2^{s-1} \mod (u_1^{2p+1}) \\ \partial_1^*(v_2^{sp}) &\equiv s\, v_1^p\, h_0\, v_2^{sp-1} \mod (u_1^{2p+1}) \end{aligned}$$

Démonstration. Par définition, $\partial_1(\epsilon_+) = v$. Soit s un entier relatif, d'après la proposition 4.10,

$$\partial_1(1)_* u^s = \epsilon_+^{-1} v_* u^s \quad \equiv \quad s u_1 u^s + \left(\binom{s}{p} - s \right) u_1^p u^s + (s + R_s) u_1^{p+2} u^s \quad \mod (u_1^{p+4})$$

où $R_s := \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$. D'après le corollaire A.2, si l'on se donne $s = s_0 + s_1 p + \dots$ écrit en base p, alors $\binom{s}{p} \equiv s_1$ $[p]$. Donc, si $q \in \mathbb{Z}$ est le quotient de la division euclidienne de s par p, alors

$$\partial_{1*}(v_2^s) \quad \equiv \quad s u_1 v_2^s + (q - s) u_1^p v_2^s + (s + R_s) u_1^{p+2} v_2^s \quad \mod (u_1^{p+2})$$

Ce qui avec les identités $u_1 = h_1 v_1$, $u_1^p = h_0 v_1^p v_2^{-1}$, $u_1^{p+1} = v_1^{p+1} v_2^{-1}$ et $v_* u^{sp} = (v_* u^s)^p$, donne la première congruence. Pour la seconde, on applique la précédente avec sp au lieu de s et en utilisant une seconde fois le corollaire A.2, on note que $R_{sp} = 0$. □

Remarque 4.14. *Rappelons que par définition $h_0 = u^{1-p}$, $h_1 = u^{p-1}$ et $v_2 = u^{1-p^2}$. D'où*

$$h_0^p = h_1 v_2 \quad \textit{et} \quad h_1^p = h_0 v_2^{-1}$$

Proposition-Définition 4.15. *Soit s un entier relatif premier à p.*

a) On pose $(1)_0 := 1 \in \ker \partial_1^*$.

b) On pose $(1)_s := v_2^s$ alors

$$\partial_1^*(1)_s \equiv s\, v_1\, h_1\, v_2^s \quad \mod (u_1^p)$$

c) On pose

$$(1)_{sp^n} := \begin{cases} v_2^{sp} & \textit{si } n = 1 \\ v_2^{sp^2} - s v_1^{p^2-1} v_2^{sp^2-p+1} & \textit{si } n = 2 \\ (1)_{sp^{n-1}}^p - 2s v_1^{p^n+p^{n-1}-p-1} v_2^{sp^n-p^{n-1}+1} & \textit{si } n > 2 \end{cases}$$

élément homogène de degré $2(p^2-1)sp^n$ tel que

$$\partial_1^*(1)_{sp^n} \equiv \begin{cases} s\, v_1^{p^n+p^{n-1}-1}\, h_0\, v_2^{sp^n-p^{n-1}} & \textit{si } n = 1 \\ 2s\, v_1^{p^n+p^{n-1}-1}\, h_0\, v_2^{sp^n-p^{n-1}} & \textit{si } n > 1 \end{cases}$$

modulo $(u_1^{(p+1)p^{n-1}})$.

Remarque. On note que par construction, $(1)_{sp^n} \equiv v_2^{sp^n}$ modulo (u_1).

Démonstration. Il nous reste à prouver le troisième point pour $n > 1$. Pour $n = 2$, d'après le lemme précédent, on a

$$\partial_1(1)_{sp}^p \quad \equiv \quad s\, v_1^{p^2}\, h_0^p\, v_2^{sp^2-p} \ \equiv \ s\, v_1^{p^2}\, h_1\, v_2^{sp^2-p+1} \quad \mod (u_1^{2p^2+p})$$

et modulo $(u_1^{(p+1)p+p+1})$,

$$\partial_1^*(v_1^{p^2-1} v_2^{sp^2-p+1}) \quad \equiv \quad v_1^{p^2+1} h_1 v_2^{sp^2-p+1} - 2 v_1^{p^2+p-1} h_0 v_2^{sp^2-p}$$

D'où, la congruence annoncée pour $n = 2$. Supposons par récurrence sur $n > 2$ qu'on a la congruence annoncée pour $\partial_1^*(1)_{sp^{n-1}}$. Alors,

$$\partial_1(1)_{sp^{n-1}}^p \quad \equiv \quad 2s\, h_1 v_1^{p^n+p^{n-1}-p} v_2^{sp^n-p^{n-1}+1} \quad \mod (u_1^{(p+1)p^{n-1}})$$

D'après le lemme précédent, modulo $(u_1^{(p+1)p^{n-1}})$,

$$\begin{aligned} & \partial_1^*(v_1^{p^n+p^{n-1}-p-1}v_2^{sp^n-p^{n-1}+1}) \\ \equiv \ & v_1^{p^n+p^{n-1}-p}h_1v_2^{sp^n-p^{n-1}+1} - v_1^{p^n+p^{n-1}-1}h_0v_2^{sp^n-p^{n-1}} \end{aligned}$$

D'où, l'on déduit $\partial_1^*(1)_{sp^n}$. □

Définition 4.16. Soient s un entier relatif premier à p et n un entier naturel, on pose

$$\begin{aligned} (h_1)_s &:= v_1^{-1}\,\partial_1^*(1)_s \\ (h_0)_{(sp-1)p^n} &:= v_1^{-p^{n+1}-p^n+1}\,\partial_1^*(1)_{sp^{n+1}} \end{aligned}$$

Avec ces notations, on a

$$\partial_1^*(1)_{sp^n} = \begin{cases} 0 & \text{si } t = s = 0, \\ v_1(h_1)_s & \text{si } n = 0,\ s \wedge p = 1 \\ v_1^{p^n+p^{n-1}-1}\,(h_0)_{(sp-1)p^{n-1}} & \text{si } n \geq 1,\ s \wedge p = 1 \end{cases}$$

Il est immédiat que les éléments $(h_1)_s$ et $(h_0)_s$, qui ont été défini, sont $\mathbb{F}_p[v_1]$-linéairement indépendants. Donc,

Corollaire 4.17 (cf. corollaire 5.4 [HKM08])**.**
On a un isomorphisme de $\mathbb{F}_p[v_1]$-modules $H^0(\mathbb{G}_2^1, (E_2)_*) \cong \mathbb{F}_p[v_1]$.

L'homomorphisme ∂_2^* est aussi $\mathbb{F}_p[v_1]$-linéaire et la multiplication par v_1 induit un endomorphisme injectif de $(E_2)_*^F \otimes (\mathbb{F}_p h_0 \oplus \mathbb{F}_p h_1)$, ainsi $(h_1)_s$ et $(h_0)_{(sp-1)p^n}$ appartiennent au noyau de ∂_2^*. D'autre part, du lemme 4.1 qui donne une condition suffisante pour avoir une $\mathbb{F}_p[v_1]$-base topologique, on déduit le corollaire suivant :

Corollaire 4.18.

1. *La famille d'éléments $(\,(1)_s\,)_{s\in\mathbb{Z}}$ est une $\mathbb{F}_p[v_1]$-base topologique de $(E_2)_*^F/(p)$.*
2. *La réunion des ensembles*

$$\{\,(h_0)_{(sp-1)p^n}\,;\ s \not\equiv 0\,[p] \ \textit{et}\ n \in \mathbb{N}\,\},\quad \{\,h_0v_2^{(sp^2-1)p^n}\,;\ s \in \mathbb{Z}\ \textit{et}\ n \in \mathbb{N}\,\},\quad \{\,h_0v_2^s\,;\ s \not\equiv -1\,[p]\,\},$$
$$\{\,(h_1)_s\,;\ s \not\equiv 0\,[p]\,\},\quad \textit{et}\quad \{\,h_1v_2^{ps}\,;\ s \in \mathbb{Z}\,\}$$

détermine une $\mathbb{F}_p[v_1]$-base topologique de $(E_2)_*^F/(p) \otimes (\mathbb{F}_p h_0 \oplus \mathbb{F}_p h_1)$.

Dans la section suivante, nous allons chercher à remplacer les éléments

$$\{\,h_0v_2^{(sp^2-1)p^n}\,;\ s \in \mathbb{Z} \text{ et } n \in \mathbb{N}\,\},\quad \{\,h_0v_2^s\,;\ s \not\equiv -1\,[p]\,\}\quad \text{et}\quad \{\,h_1v_2^{ps}\,;\ s \in \mathbb{Z}\,\}$$

de telle sorte qu'ils soient adaptés à l'homomorphisme ∂_2^*.

4.4 La seconde différentielle

Dans le chapitre 2 Résolution projective : $n = 2$ et $p \geq 5$, le théorème 2.10, nous avons approximé un homomorphisme $d_2 : \Lambda_{1-p} \to N_1$ tel que sa composée avec la projection $N_1 \to$

$H_0(S_2^1, N_1)$ soit surjective. Nous en avons déduit $\partial_2 = \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1} \circ \alpha$ où $\alpha : C_2 \to C_2$ est un automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire tel que $H_0(S_2^1, \alpha)$ soit l'identité. D'où le diagramme suivant :

$$\begin{tikzcd}
(E_2)_*^F \arrow[r, "\partial_1^*"] & (E_2)_*^F \otimes (\mathbb{F}_p h_0 \oplus \mathbb{F}_p h_1) \arrow[r, "\partial_2^*"] \arrow[dr, "\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1 *}"'] & (E_2)_*^F \otimes (\mathbb{F}_p g_0 \oplus \mathbb{F}_p g_1) \\
& & (E_2)_*^F \otimes (\mathbb{F}_p g_0 \oplus \mathbb{F}_p g_1) \arrow[u, "\alpha^*"]
\end{tikzcd}$$

Nous allons donc dans un premier temps trouver des bases diagonalisant $\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1 *}$ ensuite il nous suffira d'appliquer α^* à la famille libre des images par $\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1 *}$. Au passage, notons que par hypothèse sur α, on a que pour tout $X \in (E_2)_*^F \otimes (\mathbb{F}_p g_0 \oplus \mathbb{F}_p g_1)$,

$$\alpha^*(X) \equiv X \mod (u_1)X$$

Ainsi les images par α gardent les mêmes propriétés de congruence. Pour alléger les notations, dans toute la section, on identifie $\mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}$ avec ∂_2.

Comme pour la première différentielle, on identifie ∂_2^* avec la seconde ligne du diagramme suivant.

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p)) \arrow[r, "\partial_2^*"] \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*/(p)) \arrow[d, "\mathrm{ev}_{e_2}"', "\cong"] \\
(E_2)_*^F \otimes (\,\mathbb{F}_p\, h_0 \oplus \mathbb{F}_p\, h_1\,) \arrow[r] & (E_2)_*^F \otimes (\,\mathbb{F}_p\, g_0 \oplus \mathbb{F}_p\, g_1\,)
\end{tikzcd}$$

Au lieu de calculer le terme $\partial_2^*(e_1)_+$ et d'étudier son action, nous allons, comme dans [HKM08], tirer profit de la relation $\partial_2 = \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}$ en procédant par étapes.

Plus précisément, en utilisant le fait que Λ_{1-p} est libre de rang deux en tant que $\mathbb{Z}_p$-module dont (ϵ_+, ϵ_-) est une base, on a que $\mathrm{Hom}(\Lambda_{1-p}, (E_2)_*)$ est isomorphe à $(E_2)_* \oplus (E_2)_*$. D'où, le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, M) \arrow[r, "d_2^*"] \arrow[d, "\cong"', "\mathrm{ev}_{e_1}"] & \mathrm{Hom}(\Lambda_{1-p}, M) \arrow[r, "\mathrm{tr}_F"] \arrow[d, "\cong"', "\mathrm{ev}_{(\epsilon_+, \epsilon_-)}"] & \mathrm{Hom}_F(\Lambda_{1-p}, M) \arrow[r, "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, M) \arrow[d, "\cong"', "\mathrm{ev}_{e_2}"] \\
(E_2)_*^F \otimes (\,\mathbb{Z}_p h_0 \oplus \mathbb{Z}_p h_1\,) \arrow[r] & (E_2)_* \oplus (E_2)_* \arrow[rr, "\mathrm{tr}_F"] & & (E_2)_*^F \otimes (\,\mathbb{Z}_p g_0 \oplus \mathbb{Z}_p g_1\,)
\end{tikzcd}$$

où, pour alléger les notations, on note M l'anneau $(E_2)_*$.

On note *Frob* : $\mathbb{W} \to \mathbb{W}$ le relevé de l'automorphisme de Frobenius de $\mathbb{F}_{p^2}$, ainsi avec les notations du premier chapitre, $\mathit{Frob}\,(x) = x^\sigma$ pour tout $x \in \mathbb{W}$. En revenant au corollaire 1.30 et au fait que le sous-$\mathbb{Z}_p[F]$-module de $(E_2)_*$ engendré par u^i est isomorphe à Λ_i, on déduit le lemme suivant.

Lemme 4.19. *Soient $\phi : \Lambda_{1-p} \longrightarrow \mathbb{W}$ un homomorphisme de $\mathbb{Z}_p$-modules et $i \neq \pm(1-p)$ $[p^2-1]$ un entier relatif, alors*

$$\begin{aligned}
\mathrm{tr}_F(\phi u^{1-p}) &= \frac{1}{2}\Big(\lambda(\phi(\epsilon_+)) + \mu(\phi(\epsilon_-))\Big)\ \mathrm{Id}\, u^{1-p} \\
\mathrm{tr}_F(\phi u^{p-1}) &= \frac{1}{2}\Big(\lambda(\phi(\epsilon_+)) - \mu(\phi(\epsilon_-))\Big)\ \mathit{Frob}\, u^{p-1} \\
\mathrm{tr}_F(\phi u^{i}) &= 0
\end{aligned}$$

où (λ, μ) est la $\mathbb{Z}_p$-base duale de la base (ϵ_+, ϵ_-) de $\mathbb{W}$ (définition 1.26).

D'après la proposition 1.31 et ses corollaires, $\{\, u_1^i u^j;\ j-(1-p)i \equiv \pm(1-p)\ [p^2-1] \,\}$ engendre un sous-module dense de $(E_2)_*^F \otimes (\,\mathbb{Z}_p g_0 \oplus \mathbb{Z}_p g_1\,)$. Ainsi, on déduit du lemme précédent,

Proposition 4.20. *La transformation naturelle* tr_F *appliquée à* $\mathrm{Hom}(\Lambda_{1-p},(E_2)_*)$ *induit l'homomorphisme*

$$\mathrm{tr}_F :\ (E_2)_* \oplus (E_2)_* \longrightarrow (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$$

dont l'image du couple $(x_+ u_1^i u^j, x_- u_1^i\, u^j)$*, où* $x_\pm \in \mathbb{W}$*, est :*

$$\begin{cases} \frac{1}{2}(\lambda(x_+) \pm \mu(x_-))\, u_1^i\, u^j & \textit{si } j-(1-p)i \equiv \pm(1-p)\ [p^2-1] \\ 0 & \textit{sinon} \end{cases}$$

Démonstration. Soient $(x_+ u_1^i u^j, x_- u_1^i\, u^j)$, où $x_\pm \in \mathbb{W}$, alors

$$\begin{aligned} \mathrm{ev}^{-1}_{(\epsilon_+,\epsilon_-)}(x_+ u_1^i u^j, x_- u_1^i\, u^j) :\ \Lambda_{1-p} &\longrightarrow (E_2)_* \\ \epsilon_\pm &\longmapsto x_\pm \end{aligned}$$

D'où l'on déduit la proposition du lemme précédent. $\square$

Définition 4.21. On pose $\mathrm{tr}_\pm : (E_2)_* \to (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$ la restriction au premier et au second facteur de tr_F respectivement.

Passons maintenant à d_2^* qu'on identifie avec l'homomorphisme horizontale inférieur du diagramme suivant :

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1,(E_2)_*) \arrow[r, "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1},(E_2)_*) \arrow[r, "d_2^*"] & \mathrm{Hom}(\Lambda_{1-p},(E_2)_*) \arrow[d, "\mathrm{ev}_{(\epsilon_+,\epsilon_-)}", "\cong"'] \\ (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1}) \arrow[u, "\mathrm{ev}_{e_1}^{-1}", "\cong"'] \arrow[rr] & & (E_2)_* \oplus (E_2)_* \end{tikzcd}$$

Soit $u_1^i u^s$ un monôme de $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1})$, on associe $(\mathrm{Id}\circ d_2)u_1^i u^s : \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \to \mathbb{W}u_1^i u^s)$ et $(\,\textit{Frob} \circ d_2)u_1^i u^s : \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \to \mathbb{W}u_1^i u^s$, définis dans les diagrammes suivant :

$$\begin{tikzcd} \Lambda_{1-p} \arrow[d] \arrow[dr, "\mathrm{Id}\, u_1^i u^s"] & \\ \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \arrow[r, dashed, "\exists !"] & \mathbb{W}u_1^i u^s \subset (E_2)_* \\ \Lambda_{1-p} \arrow[u, "d_2"] \arrow[ur, dotted, "(\mathrm{Id}\circ d_2)u_1^i u^s"'] & \end{tikzcd} \qquad \begin{tikzcd} \Lambda_{1-p} \arrow[d] \arrow[dr, "\textit{Frob}\, u_1^i u^s"] & \\ \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \arrow[r, dashed, "\exists !"] & \mathbb{W}u_1^i u^s \subset (E_2)_* \\ \Lambda_{1-p} \arrow[u, "d_2"] \arrow[ur, dotted, "(\textit{Frob}\circ d_2)u_1^i u^s"'] & \end{tikzcd}$$

Alors, l'homomorphisme $\mathrm{ev}_{e_1}^{-1}$ envoie $u^{1-p}v_1^i v_2^j$ (resp. $u^{p-1}v_1^i v_2^j$) sur $\mathrm{Id}\, u^{1-p}v_1^i v_2^j$ (resp. $\textit{Frob}\, u^{p-1}v_1^i v_2^j$). Ainsi, on déduit que :

$$\begin{aligned} d_2^*(u^{1-p}v_1^i v_2^j) &= ev_{(\epsilon_+,\epsilon_-)}\Big(\ (\mathrm{Id}\circ d_2)u^{1-p}v_1^i v_2^j\ \Big) \\ &= (d_2(e_1)_+ u^{1-p}v_1^i v_2^j,\ d_2(e_1)_- u^{1-p}v_1^i v_2^j) \\ d_2^*(u^{p-1}v_1^i v_2^j) &= (\check{d}_2(e_1)_+ u^{p-1}v_1^i v_2^j,\ \check{d}_2(e_1)_- u^{p-1}v_1^i v_2^j) \end{aligned}$$

où $\check{d}_2(e_2)_\pm := Frob \uparrow_F^{\mathbb{G}_2^1} (d_2(e_2)_\pm)$. D'où

$$\begin{array}{rcll} \partial_2^*(u^{1-p}v_1^i v_2^j) & = & \mathrm{tr}_+(\ d_2(e_2)_+ u^{1-p}v_1^i v_2^j\ ) + \mathrm{tr}_-(\ d_2(e_2)_- u^{1-p}v_1^i v_2^j\ ) & (4.2) \\ \partial_2^*(u^{p-1}v_1^i v_2^j) & = & \mathrm{tr}_+(\ \check{d}_2(e_2)_+ u^{p-1}v_1^i v_2^j\ ) + \mathrm{tr}_-(\ \check{d}_2(e_2)_- u^{p-1}v_1^i v_2^j\ ) & (4.3) \end{array}$$

Le développement précédent est encore vrai si l'on regarde l'anneau gradué de Lubin-Tate modulo (p). Dans le reste de cette section, c'est ce que nous allons faire.

Comme $\partial_2^* = \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_2, (E_2)_*/(p))$ est $\mathbb{F}_p[v_1]$-linéaire, ainsi il nous suffit de calculer les images des éléments $h_0 v_2^s$ et $h_1 v_2^s$. D'après le corollaire 4.18, on peut se limiter à certaines valeurs de s. La proposition suivante nous donne une méthode pour les calculer.

Proposition 4.22. *Avec les notations de la proposition définition 2.44, on pose* $\check{\kappa}_\pm = Frob \uparrow_F^{\mathbb{G}_2^1} (\kappa_\pm)$. *Soit s un entier relatif. On a,*

1. $\partial_2^*(h_0 v_2^s) = \mathrm{tr}_+(\ \kappa_+ h_0 v_2^s\ ) + \mathrm{tr}_-(\ \kappa_- h_0 v_2^s\ )$ *modulo* (u_1^{p+3}),
2. $\partial_2^*(h_1 v_2^s) = \mathrm{tr}_+(\ \check{\kappa}_+ h_1 v_2^s\ ) + \mathrm{tr}_-(\ \check{\kappa}_- h_1 v_2^s\ )$ *modulo* (u_1^{2p}).

De plus, si $s \equiv 0, 1[p]$ alors,

$$\partial_2^*(h_0 v_2^s) = \mathrm{tr}_+(\ \kappa_+ h_0 v_2^j\ ) + \mathrm{tr}_-(\ \kappa_- h_0 v_2^s\ ) \text{ modulo } (u_1^{2p+2}).$$

Remarque. Une petite parenthèse sur les éléments de $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*/(p))$ dont une description plus précise est donnée par dans la proposition 1.31 et son corollaire. Notons que

$$\begin{array}{rcl} u_1^2\, g_0 & = & v_1^2\, g_1 \\ u_1^{p+1}\, g_0 & = & v_1^{p+1}\, g_0\, v_2^{-1} \\ u_1^{p+3}\, g_0 & = & v_1^{p+3}\, g_1\, g_1^{-1} \\ u_1^{2p+2}\, g_0 & = & v_1^{2(p+1)}\, g_0\, v_2^{-2} \\ u_1^{p-1}\, g_1 & = & v_1^{p-1}\, g_0\, v_2^{-1} \\ u_1^{p+1}\, g_1 & = & v_1^{p+1}\, g_1\, v_2^{-1} \\ u_1^{2p}\, g_1 & = & v_1^{2p}\, g_0\, v_2^{-2} \end{array}$$

appartiennent à $(E_2)_*^F \otimes (\,\mathbb{F}_p u^{1-p} \oplus \mathbb{F}_p u^{p-1}\,)$. Réciproquement, un élément $u_1^i h_0$ avec $0 < i \leq 2p+2$ ou un élément $u_1^i h_1$ avec $0 < i \leq 2p$ s'il appartient à $(E_2)_*^F \otimes (\,\mathbb{F}_p u^{1-p} \oplus \mathbb{F}_p u^{p-1}\,)$ alors il est de la forme précédente. En particulier, un calcul modulo (u_1^{p+4}), peut être affiné à cause de la répartition des puissances de u_1 dans le module précédent.

Démonstration. Par construction,

$$d_2(e_2)_\pm \equiv \kappa_\pm \mod (IJ + JI)C_1$$

où $I = (IS_2^1)$ et $J = (IF_1 S_2^1)$.
Soit $g \equiv 1 + g_1 S + g_2 S^2 \mod [S^3]$ un élément quelconque de S_2^1, alors

$$\begin{array}{rcll} t_0(g) & \equiv & 1 + g_1^p u_1 - g_1 u_1^p + (g_2 - g_2^p) u_1^{p+1} & \mod (u_1^{p+2}) \\ \Rightarrow\ t_0(g)^k & \equiv & 1 + k g_1^p u_1 + \dbinom{k}{2} g_1^{2p} u_1^2 & \mod (u_1^3) \end{array}$$

Soit $f \equiv 1 + f_2 S^2 \mod (S^3)$ un élément de $F_1 S_2^1$, alors $(f - e)$ agit trivialement sur $u^{(1-p)s}$ modulo (u_1^{p+1}). Plus précisément, si l'on pose $f' = f_2 - f_2^p$, alors

$$t_0(f)^k - 1 \equiv (1 + f' u_1^{p+1})^k - 1 \equiv k f' u_1^{p+1} \mod (u_1^{2p+1})$$

Ainsi, modulo (u_1^{p+4}),

$$\begin{aligned}
(g-e)(f-e)_* u^k &\equiv kf'(g-e)_* u_1^{p+1} u^k \\
&\equiv kf'(t_0^{k+p^2-1}(g)-1)u_1^{p+1}u^k \\
&\equiv kf'((k-1)g_1^p u_1^{p+2} + \binom{k+p^2-1}{2} g_1^{2p} u_1^{p+3}) u^{(1-p)k} \\
&\equiv kf'\Big((k-1)g_1^p u_1^{p+2} + \binom{k-1}{2} g_1^{2p} u_1^{p+3}\Big) u^{(1-p)k} \mod (u_1^{p+4}) \qquad (4.4)
\end{aligned}$$

et

$$\begin{aligned}
(f-e)(g-e)_* u^k &\equiv kg_1^p (f-e)_* u_1 u^k + \binom{k}{2} g_1^{2p} (f-e)_* u_1^2 u^k \\
&\equiv kg_1^p (t_0^{k+p-1}(f)-1) u_1 u^k + \binom{k}{2} g_1^{2p} (t_0^{k+2(p-1)}(f)-1) u_1^2 u^k \\
&\equiv k(k-1) g_1^p f' u_1^{p+2} u^k + \binom{k}{2}(k-2) g_1^{2p} f' u_1^{p+3} u^k \mod (u_1^{p+4}) \qquad (4.5)
\end{aligned}$$

En particulier $(IJ+JI)$ agit trivialement modulo (u_1^{p+2}). Donc à l'aide de la description des éléments de $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2]\!]}(C_2, (E_2)_*/(p))$ faite dans la remarque précédente, on déduit les deux premières congruences de la proposition.
Passons à la dernière congruence. Supposons que $s \equiv 0, 1, [p]$. Posons $k = 1 - p + (1-p^2)s$, alors $k \equiv 1, 2\,[p]$. D'où, le coefficient devant u_1^{p+3} dans les expressions (4.4) et (4.5) est nul. En utilisant à nouveau la description des éléments, on déduit la précision annoncée sur la dernière congruence. □

Remarque 4.23. *Dans la précédente preuve, on a vu en particulier que l'idéal $IJ+JI$ agit trivialement sur $(E_2)_*/(p, u_1^{p+2})$.*

Lemme 4.24. *Quel que soit x dans $(E_2)_*^F \otimes (\mathbb{F}_p u^{1-p} \oplus \mathbb{F}_p u^{p-1})$, on a*

$$\partial_2^*(x^p) = \partial_2^*(x)^p$$

Démonstration. En introduction du chapitre précédent, nous avons vu que pour $i = 1, 2$, le module $C_i = \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} = \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \underset{\mathbb{Z}_p[F]}{\otimes} \Lambda_{1-p}$, en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module, est libre de rang 2 dont $((e_i)_+, (e_i)_-) := (1\otimes\epsilon_+, 1\otimes\epsilon_-)$ est une base. Ainsi, il existe $S^\pm \in \mathbb{F}_p[\![S_2^1]\!]$ tels que $\partial_2(e_2) = S^+(e_1)_+ + S^-(e_1)_+$. On a donc

$$\begin{aligned}
\partial_2^*((h_0 v_1^i v_2^j)^p) &= \partial_2^*(h_1 v_1^{pi} v_2^{pj+1}) \\
&= S_*^+ \, \mathit{Frob}\,(\epsilon_+) h_1 v_1^{pi} v_2^{pj+1} + S_*^- \, \mathit{Frob}\,(\epsilon_-) h_1 v_1^{pi} v_2^{pj+1} \\
&= S_*^+ \epsilon_+^p h_0^p v_1^{pi} v_2^{pj} + S_*^- \epsilon_-^p h_0^p v_1^{pi} v_2^{pj} \\
&= \partial_2^*(h_0 v_1^i v_2^j)^p \\
\partial_2^*((h_1 v_1^i v_2^j)^p) &= \partial_2^*(h_0 v_1^{pi} v_2^{pj-1}) \\
&= S_*^+ \epsilon_+ h_0 v_1^{pi} v_2^{pj-1} + S_*^- \epsilon_- h_0 v_1^{pi} v_2^{pj-1} \\
&= S_*^+ \, \mathit{Frob}\,(\epsilon_+)^p h_1^p v_1^{pi} v_2^{pj} + S_*^- \, \mathit{Frob}\,(\epsilon_-)^p h_1^p v_1^{pi} v_2^{pj} \\
&= \partial_2^*(h_1 v_1^i v_2^j)^p
\end{aligned}$$

D'où par linéarité et continuité de ∂_2^*, on déduit le lemme. □

4.4.1 L'action de κ_+ et κ_-

Rappelons la définition de $\kappa_\pm$ et $\check{\kappa}_\pm$, modulo (p),

$$\begin{aligned}
\kappa_+ &= \mathcal{N}(a_0)(e_1)_+ + \frac{1}{4\epsilon_-^2}\Big((b_0-e)(w(e_1)_+ - v(e_1)_-) + (c_0-e)(e_1)_-\Big)\\
\kappa_- &= \mathcal{N}(b_0)(e_1)_- + \frac{1}{4\epsilon_+^2}\Big((a_0-e)(w(e_1)_+ - v(e_1)_-) + (c_0-e)(e_1)_+\Big)\\
\check{\kappa}_+ &= \mathcal{N}(a_0)(e_1)_+ + \frac{1}{4\epsilon_-^2}\Big((b_0-e)(w(e_1)_+ + v(e_1)_-) - (c_0-e)(e_1)_-\Big)\\
\check{\kappa}_- &= -\mathcal{N}(b_0)(e_1)_- + \frac{1}{4\epsilon_+^2}\Big((a_0-e)(w(e_1)_+ + v(e_1)_-) + (c_0-e)(e_1)_+\Big).
\end{aligned}$$

Ainsi, on voit qu'ils sont la somme de trois types de termes :

i) $\mathcal{N}(g)(e_1)_\pm$, où $g \in S_2^1$.

ii) $(\,g-e\,)\kappa_3$, où $g \in S_2^1$ et $\kappa_3 = (w(e_1)_+ - v(e_1)_-)$.

iii) $(c_0-e)(e_1)_\pm$

L'étude d'une approximation de l'action de ces types d'éléments est l'objet de la proposition suivante, de la proposition 4.27 et du lemme 4.28.

Proposition 4.25. *Supposons que $p>5$. Soient $x \in \mathbb{W}^\times$ et $g \equiv 1 + xS \bmod (S^2)$ dans S_2^1. Soit s un entier relatif, alors*

$$\mathcal{N}(g)_* u^s \equiv -\binom{s}{p-1} x^{1-p} u_1^{p-1} u^s \equiv \begin{cases} -x^{1-p}u_1^{p-1}u^s, & \text{si } s \equiv -1\ [p] \\ 0 & \text{sinon} \end{cases}$$

modulo (u_1^{p+4}). Si $p=5$, il faut ajouter le terme $s\binom{s-1}{3}x^{3p+1}u_1^{p+3}$.

Dans la preuve de la proposition ci-dessus, nous avons besoin d'un petit résultat concernant la somme des puissances k-ème des entiers. Soient k et n deux entiers naturels, on note :

$$S_k(n) = 1^k + 2^k + \ldots + n^k$$

Lemme 4.26. *Soit k un entier, dans $\mathbb{Z}/_{p\mathbb{Z}}$, on a*

$$S_k(p-1) = \begin{cases} -1 & \text{si } k \equiv 0\ [p-1], \\ 0 & \text{sinon} \end{cases}$$

Démonstration du lemme. Il est immédiat que $S_0(p-1) = -1$. Les éléments de $\mathbb{F}_p^\times$ sont d'ordre $p-1$, $S_{p-1}(p-1)$ vaut aussi -1. Soit $k \in \mathbb{N}$, alors

$$\begin{aligned}
-1 &= (p-1+1)^{k+1} - 1\\
&= \sum_{m=1}^{p-1}\big((m+1)^{k+1} - m^{k+1}\big)\\
&= \sum_{m=1}^{p-1}\sum_{r=0}^{k}\binom{k+1}{r} m^r\\
&= \sum_{r=0}^{k}\binom{k+1}{r} S_r(p-1)\\
&= -1 + \sum_{r=1}^{k-1}\binom{k+1}{r} S_r(p-1) + (k+1)S_k(p-1)
\end{aligned}$$

Donc par récurrence sur k, on déduit que pour tout $1 \le k < p-1$, $S_k(p-1) = 0$. D'autre part, $S_{kp}(p-1) = S_k(p-1)$, d'où le lemme. □

Démonstration de la proposition. Supposons que $p > 5$. Soit s un entier relatif. D'après le corollaire 3.6, on a

$$\begin{aligned}
\sum_{k=0}^{p-1} t_0(g^k)^s &\equiv \sum_{k=0}^{p-1}(1+kx^pu_1)^s - skxu_1^p - s(s-1)k^2x^{p+1}u_1^{p+1} \\
&\quad + s(kx^p - \binom{s-1}{2}k^3x^{2p+1})u_1^{p+2} + s(\frac{p-1}{2}k^2x^{2p} - \binom{s-1}{3}k^4x^{3p+1})u_1^{p+3} \\
&\equiv 1 + \sum_{k=1}^{p-1}(1+kx^pu_1)^s - \sum_{k=0}^{p-1} s\binom{s-1}{3}k^4x^{3p+1}u_1^{p+3} \qquad (4.6)\\
&\equiv 1 + \sum_{k=1}^{p-1}\sum_{i=0}^{p+4}\binom{s}{i}k^ix^{pi}u_1^i \\
&\equiv 1 + \binom{s}{0}(p-1) + \binom{s}{p-1}(p-1)x^{1-p}u_1^{p-1} \quad \bmod (u_1^{p+4})
\end{aligned}$$

D'où,

$$\mathcal{N}(g)_*u \equiv -\binom{s}{p-1}x^{1-p}u_1^{p-1}u^s \bmod (u_1^{p+4})$$

Alors, d'après le corollaire A.2 sur la réduction modulo p des coefficients binomiaux généralisés, si l'on note $\bar{s}$ le reste de la division euclidienne de s par p, on a

$$\binom{s}{p-1} = \binom{\bar{s}}{p-1} = \begin{cases} 1 & \text{si } \bar{s} = p-1 \\ 0 & \text{sinon} \end{cases}$$

Lorsque $p = 5$, la seconde somme de (4.6) n'est pas nulle, d'où la seconde partie de la proposition. □

Pour alléger les notations, on rappelle qu'on pose $\kappa_3 = (w(e_1)_+ - v(e_1)_-)$.

Proposition 4.27. *Soient $x \in \mathbb{W}^\times$ et $g \equiv 1 + xS \bmod (S^2)$ dans S_2^1. Soit t un entier relatif, posons $R_t := \frac{1}{2}(\binom{t}{p+2} - t\binom{t-1}{2})(\epsilon_+^2 - \epsilon_-^2)$.*

1. *L'élément $-(2\epsilon_+\epsilon_-)^{-1}\,(g-e)\kappa_{3*}\,u^{(1-p)t}$ est congrue à*

$$\begin{aligned}
&\equiv t(t-1)x^pu_1^2u^t + \ldots + t(\binom{t+p-1}{p} + 1 - t)xu_1^{p+1}u^t \\
&\quad + t\Big(\binom{t+p-1}{p+2}x^{2p+1} + (t-1)(x^p - \binom{t-2}{2}x^{2p+1})\Big)u_1^{p+3}u^t \\
&\quad + (t+R_t)(t-2)x^pu_1^{p+3}u^t
\end{aligned}$$

   modulo (u_1^{p+4}).

2. *On a*

$$(g-e)\breve{\kappa}_{3*}u^t \equiv 2\epsilon_+\epsilon_-\, t(\binom{t}{p} - t\,)\,x^p\; u_1^{p+1}\,u^t$$

   modulo (u_1^{p+2}).

Démonstration. On se place dans $(E_2)_*/(p, u_1^{p+4})$. Soit t un entier relatif. Alors, d'après la proposition 4.10,

$$\begin{aligned}
v_*u^t &\equiv \epsilon_+(\,tu_1 + (\binom{t}{p} - t\,)u_1^p + (t+R_t)u_1^{p+2}\,)u^t \\
w_*u^t &\equiv \epsilon_-(\,-tu_1 + (\binom{t}{p} - t\,)u_1^p - (t+R_t)u_1^{p+2}\,)u^t
\end{aligned}$$

1. Par définition, $\kappa_3 = w\epsilon_+ - v\epsilon_-$, donc $\check{\kappa}_3 = w\epsilon_+ + v\epsilon_-$, d'où

$$\kappa_{3*}\, u^t \equiv -2\epsilon_+\epsilon_-(\, tu_1 + (t+R_t)u_1^{p+2})u^t \tag{4.7}$$
$$\check{\kappa}_{3*}\, u^t \equiv 2\epsilon_+\epsilon_-(\, \binom{t}{p} - t\,)\, u_1^p u^t \tag{4.8}$$

D'après *ii*) du corollaire 3.6,

$$\begin{aligned}
& (g-e)_* u_1 u^t \\
\equiv\ & ((1+x^p u_1)^{t+p-1} - 1)u_1 u^t \\
& \quad -(t-1)xu_1^{p+1}u^t + \ldots + (t-1)(x^p - \binom{t+p-2}{2}x^{2p+1})u_1^{p+3}u^t \\
\equiv\ & \Big[\, (t-1)x^p u_1^2 + \ldots + (\binom{t+p-1}{p} + 1 - t)xu_1^{p+1} + \ldots \\
& \quad + \Big(\binom{t+p-1}{p+2}x^{2p+1} + (t-1)(x^p - \binom{t-2}{2}x^{2p+1})\Big)u_1^{p+3}\,\Big]u^t
\end{aligned}$$

et

$$(g-e)_* u_1^{p+2}u^t \equiv (t-2)x^p u_1^{p+3}u^t$$

Ainsi, en revenant à (4.7), on a que $(-2\epsilon_+\epsilon_-)^{-1}(g-e)_*\kappa_{3*}u^t$ est congrue à

$$\begin{aligned}
\equiv\ & t(t-1)x^p u_1^2 u^t + \ldots + t(\binom{t+p-1}{p} + 1 - t)xu_1^{p+1}u^t \\
& + t\Big(\binom{t+p-1}{p+2}x^{2p+1} + (t-1)(x^p - \binom{t-2}{2}x^{2p+1})\Big)u_1^{p+3}u^t \\
& + (t+R_t)(t-2)x^p u_1^{p+3}u^t
\end{aligned}$$

2. De même, en revenant à (4.8), on a

$$\mathrm{pr}_{0,1}(\,(g-e)_* u_1^p u^t\,) \equiv tx^p u_1^{p+1}u^t + \ldots$$

et

$$\mathrm{pr}_{p+1}\,(g-e)\check{\kappa}_{3*}u^t \equiv 2\epsilon_+\epsilon_-\ t(\,\binom{t}{p} - t\,)\, x^p\ u_1^{p+1}u^t + \ldots$$

□

Lemme 4.28. *Soit s un entier relatif, alors*

$$(c_0 - e)_* u^s \equiv -4s\epsilon_+\epsilon_- u_1^{p+1}u^s \bmod (u_1^{2p+1})$$

Démonstration. Comme $c_0 \equiv 1 - 2\epsilon_+\epsilon_- S^2 \mod (S^3)$, d'après le corollaire 3.4, on a

$$\begin{aligned}
t_0(c_0) &\equiv 1 - 4\epsilon_+\epsilon_- u_1^{p+1} \mod (u_1^{2p+1}) \\
(c_0 - e)_* u^s &\equiv ((1 - 4\epsilon_+\epsilon_- u_1^{p+1})^s - 1)u^s \\
&\equiv -4s\epsilon_+\epsilon_- u_1^{p+1}u^s \bmod (u_1^{2p+1})
\end{aligned}$$

□

Nous pouvons maintenant approximer les images des éléments $h_0 v_2^s$ et $h_1 v_2^s$ par ∂_{2*}, en utilisant les propositions 4.20, 4.22, 4.25, 4.27 et le lemme 4.28.

Proposition 4.29. *Soit s un entier relatif. On a,* *i)* $\partial_2^*(\, h_0 v_2^s\,) \equiv \frac{s(s+1)}{2}\; v_1^2\, g_1\, v_2^s - \frac{s+1}{2}(\binom{s}{p} - s + 2)\; v_1^{p+1}\, g_0\, v_2^{s-1} \mod (u_1^{p+3})$.

ii) $\partial_2^*(h_1 v_2^{sp}) \equiv -v_1^{p-1}\, g_0\, v_2^{sp-1} + \frac{s-1}{2}\; v_1^{p+1}\, g_1\, v_2^{sp-1} \mod (u_1^{2p})$.

De plus, si $s \equiv 0, 1\,[p]$ *alors,*

$$\partial_2^*(\, h_0 v_2^s\,) \equiv \frac{s(s+1)}{2}\; v_1^2\, g_1\, v_2^s - \frac{s+1}{2}(\binom{s}{p} - s + 2)\; v_1^{p+1}\, g_0\, v_2^{s-1} + \beta_s\, v_1^{p+3}\, g_1\, v_2^{s-1} \quad \mod (u_1^{2p+2})$$

où β_s *est égal à*

$$\frac{s+1}{2}\Big(s + (-\binom{s}{p+2} + s\binom{s-1}{2})(\epsilon_-^2 - \epsilon_+^2)\Big) + \frac{s-1}{2}\Big(s + 1 + \frac{1}{2}(\binom{1-p+s}{p+2} - (s+1)\binom{s}{2})(\epsilon_+^2 - \epsilon_-^2)\Big)$$

Démonstration. Modulo (u_1^{p+4}). Soit s un entier relatif, l'image par l'application tr_+ de $\kappa_+ h_0 v_2^s = \kappa_+ u^{(1-p)(1+(p+1)s)}$ est congrue à

$$\begin{aligned}
& \frac{-\epsilon_+\epsilon_-}{2\epsilon_-^2} s(s+1)\epsilon_-^p u_1^2 h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_-^2}(s+1)(\binom{(1-p)(p+1)s}{p} - s)\epsilon_- u_1^{p+1} h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_-^2}(s+1)\Big(\binom{(1-p)(p+1)s}{p+2}\epsilon_-^{2p+1} + s(\epsilon_-^p - \binom{s-1}{2}\epsilon_-^{2p+1})\Big)u_1^{p+3} h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_-^2}(s+1+R_{(1-p)(1+(p+1)s)})(s-1)\epsilon_-^p u_1^{p+3} h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-^2}{\epsilon_-^2}(s+1)u_1^{p+1} h_0 v_2^s \\
\equiv\; & \frac{\epsilon_+}{2} s(s+1) u_1^2 h_0 v_2^s \\
& -\frac{\epsilon_+}{2}(s+1)(\binom{s}{p} - s + 2)u_1^{p+1} h_0 v_2^s \\
& -\frac{\epsilon_+}{2}(s+1)\Big(\binom{s}{p+2}\epsilon_-^2 + s(-1 - \binom{s-1}{2}\epsilon_-^2)\Big)u_1^{p+3} h_0 v_2^s \\
& +\frac{\epsilon_+}{2}(s+1+R_{(1-p)(1+(p+1)s)})(s-1)u_1^{p+3} h_0 v_2^s
\end{aligned}$$

L'image par l'application tr_- de $\kappa_- h_0 v_2^s$ est congrue à

$$\begin{aligned}
& \frac{-\epsilon_+\epsilon_-}{2\epsilon_+^2} s(s+1)\epsilon_+^p u_1^2 h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_+^2}(s+1)(\binom{s}{p} - s)\epsilon_+ u_1^{p+1} h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_+^2}(s+1)\Big(\binom{s}{p+2}\epsilon_+^{2p+1} + s(\epsilon_+^p - \binom{s-1}{2}\epsilon_+^{2p+1})\Big)u_1^{p+3} h_0 v_2^s \\
& -\frac{\epsilon_+\epsilon_-}{2\epsilon_+^2}(s+1+R_{(1-p)(1+(p+1)s)})(s-1)\epsilon_+^p u_1^{p+3} h_0 v_2^s \\
& -\frac{\epsilon_+^2\epsilon_-}{\epsilon_+^2}(s+1)u_1^{p+1} h_0 v_2^s \\
\\
\equiv\; & \frac{-\epsilon_-}{2} s(s+1) u_1^2 h_0 v_2^s \\
& -\frac{\epsilon_-}{2}(s+1)(\binom{s}{p} - s + 2)u_1^{p+1} h_0 v_2^s \\
& -\frac{\epsilon_-}{2}(s+1)\Big(\binom{s}{p+2}\epsilon_+^2 + s(1 - \binom{s-1}{2}\epsilon_+^2)\Big)u_1^{p+3} h_0 v_2^s \\
& -\frac{\epsilon_-}{2}(s+1+R_{(1-p)(1+(p+1)s)})(s-1)u_1^{p+3} h_0 v_2^s
\end{aligned}$$

Du corollaire 4.20, on déduit que $\partial_2^*(\, h_0 v_2^s\,)$ est égal à

$$
\begin{aligned}
& \mathrm{tr}_F(\kappa_+ h_0 v_2^s, \kappa_- h_0 v_2^s) \\
\equiv\ & \frac{1}{2} s(s+1) v_1^2 g_1 v_2^s \\
& -\frac{1}{2}(s+1)(\binom{s}{p} - s + 2) v_1^{p+1} g_0 v_2^{s-1} \\
& +\frac{1}{2}(s+1)\Big(s + (-\binom{s}{p+2} + s\binom{s-1}{2})(\epsilon_-^2 - \epsilon_+^2)\Big) v_1^{p+3} g_1 v_2^{s-1} \\
& +\frac{1}{2}\Big(s+1+\frac{1}{2}(\binom{1-p+s}{p+2} - (s+1)\binom{s}{2})(\epsilon_+^2 - \epsilon_-^2)\Big)(s-1) u_1^{p+3} h_0 v_2^s
\end{aligned}
$$

et on pose

$$
\begin{aligned}
\beta_s \quad = \quad & \frac{s+1}{2}\Big(s + (-\binom{s}{p+2} + s\binom{s-1}{2})(\epsilon_-^2 - \epsilon_+^2)\Big) \\
& + \frac{s-1}{2}\Big(s+1+\frac{1}{2}(\binom{1-p+s}{p+2} - (s+1)\binom{s}{2})(\epsilon_+^2 - \epsilon_-^2)\Big)
\end{aligned}
$$

Modulo (u_1^{p+2}). De même, l'image par l'application tr_+ de $\check{\kappa}_+ h_1 v_2^{sp} = \check{\kappa}_+ u^{(1-p)(-1+(p+1)sp)}$ est congrue à

$$
\begin{aligned}
& -\binom{sp-1}{p-1}\epsilon_+ \epsilon_+^{1-p} u_1^{p-1} h_1 v_2^{sp} \\
& +\frac{\epsilon_+\epsilon_-}{2\epsilon_-^2}\,(sp-1)(\,\binom{(1-p)(-1+(p+1)sp)}{p} - sp + 1\,)\,\epsilon_-^p\ u_1^{p+1} h_1 v_2^{sp} \\
& +\epsilon_+(sp-1) u_1^{p+1} h_1 v_2^{sp} \\
\equiv\ & -\epsilon_+ u_1^{p-1} h_1 v_2^{sp} + \epsilon_+(\frac{s-1}{2}\,)\ u_1^{p+1} h_1 v_2^{sp}
\end{aligned}
$$

et l'image par l'application tr_- de $\check{\kappa}_- h_1 v_2^{sp} = \check{\kappa}_- u^{(1-p)(-1+(p+1)sp)}$ est congrue à

$$
\begin{aligned}
& \binom{sp-1}{p-1}\epsilon_- \epsilon_-^{1-p} u_1^{p-1} h_1 v_2^{sp} \\
& +\frac{\epsilon_+\epsilon_-}{2\epsilon_+^2}\,(sp-1)(\,\binom{p-1+sp)}{p} - sp + 1\,)\,\epsilon_+^p\ u_1^{p+1} h_1 v_2^{sp} \\
& -\epsilon_-(sp-1) u_1^{p+1} h_1 v_2^{sp} \\
\equiv\ & -\epsilon_- u_1^{p-1} h_1 v_2^{sp} + \epsilon_- \frac{1-s}{2}\ u_1^{p+1} h_1 v_2^{sp}
\end{aligned}
$$

D'où,

$$\partial_2^*(h_1 v_2^{sp}) \quad \equiv \quad -v_1^{p-1} g_0 v_2^{sp-1} + \frac{s-1}{2} v_1^{p+1} g_1 v_2^{sp-1}$$

□

Précisons encore l'image $\partial_2^*(\, h_0 v_2^s\,)$ dans deux cas particulier :

Corollaire 4.30. *Soit k un entier relatif, alors modulo (u_1^{2p+2}),*

i) $\partial_2^*(\, h_0 v_2^{kp^2-p+1}\,) \equiv v_1^2 g_1\ v_2^{kp^2-p+1} +\ v_1^{p+3}\ g_1\ v_2^{kp^2-p}$

ii) $\partial_2^*(\, h_0 v_2^{(kp+1)p}\,) \equiv -\frac{3}{2}\ v_1^{p+1}\ g_0\ v_2^{(kp+1)p-1} - \frac{1}{2}\ v_1^{p+3}\ g_1\ v_2^{(kp+1)p-1}$

Démonstration. C'est une simple application de la proposition précédente et du corollaire A.2 pour déterminer les coefficients binomiaux modulo (p). □

4.4.2 Complétion de la base adaptée

Maintenant, nous pouvons construire des bases diagonalisant l'homomorphisme ∂_2^* et complétant celles que nous avons déterminées en étudiant la première différentielle ∂_1^* (voir corollaire 4.18).

Théorème-Définition 4.31.

1. *Quels que soient $s \not\equiv 0, -1\,[p]$ et $n \geq 1$, il existe $(h_0)_{sp^n} \in (E_2)_*^F/(p) \otimes (\mathbb{F}_p h_0 \oplus \mathbb{F}_p h_1)$ homogène de degré $2(p-1+(p^2-1)p^n)$, tel que :*

$$\begin{array}{rcl} (h_0)_{sp^n} & \equiv & h_0\, v_2^{sp^n} \bmod (u_1^2) \\ \partial_2^*((h_0)_{sp^n}) & \equiv & c\, v_1^{A_n+2}\, v_2^{-p^{n-1}-\ldots-1}\, g_1\, v_2^{sp^n} \bmod (u_1^{A_n+3}) \end{array}$$

où $A_n = (p^{n-1}+\ldots+1)(p+1)$ et $c \in \mathbb{F}_p^\times$.

2. *Quels que soient l'entier relatif s et $n \geq 2$, il existe $(h_0)_{(sp^2-1)p^{n-2}} \in (E_2)_*^F/(p) \otimes (\mathbb{F}_p h_0 \oplus \mathbb{F}_p h_1)$ homogène de degré $2(p-1+(p^2-1)(sp^2-1)p^n)$, tel que :*

$$\begin{array}{rcl} (h_0)_{(sp^2-1)p^{n-2}} & \equiv & h_0\, v_2^{(sp^2-1)p^{n-2}} \bmod (u_1^2) \\ \partial_2^*((h_0)_{(sp^2-1)p^{n-2}}) & \equiv & c\, v_1^{p^n-p^{n-2}+A_{n-2}+2}\, v_2^{-p^{n-3}-\ldots-1}\, g_1\, v_2^{(sp-1)p^{n-1}} \bmod (u_1^{p^n-p^{n-2}+A_{n-2}+3}) \end{array}$$

où $c \in \mathbb{F}_p^\times$.

Démonstration. Comme $h_0 = g_0 = u^{1-p}$ et $h_1 = g_1 = u^{p-1}$, on a les relations suivantes :

$$h_0^p = h_1\, v_2 \quad \text{et} \quad h_1^p = h_0\, v_2^{-1}$$

Nous allons utiliser la proposition précédente et son corollaire tout au long de la démonstration.

Construction des éléments $(h_0)_{sp^n}$:

Soit $s \not\equiv 0, -1\,[p]$. Nous allons les construire par récurrence sur l'entier n. L'initialisation se fait en distinguant deux cas :

- Supposons que $s \not\equiv 1\,[p]$. D'après le lemme 4.10,

$$\begin{array}{rcl} v_1(h_0 v_2^s)^p - \partial_1^*(v_2^{sp+1}) & \equiv & h_1\, v_1\, v_2^{sp+1} - h_1\, v_1\, v_2^{sp+1} + (1-s)\, h_0\, v_1^p\, v_2^{sp} \\ & \equiv & (1-s)\, h_0\, v_1^p\, v_2^{sp} \bmod (u_1^{p+2}) \end{array} \tag{4.9}$$

En particulier ce dernier terme est divisible par v_1^p. D'autre part, comme $\partial_2^* \circ \partial_1^* = 0$, on a

$$\begin{array}{rcl} \partial_2^*(v_1^{1-p}(h_0 v_2^s)^p - v_1^{-p}\partial_1^*(v_2^{sp+1})) & \equiv & v_1^{1-p}\partial_2^*(h_0 v_2^s)^p \\ & \equiv & \dfrac{s(s+1)}{2} v_1^{p+1}\, g_0\, v_2^{sp-1} \bmod (u_1^{p+4}) \end{array}$$

On pose

$$\begin{array}{rcl} (h_0)_{sp} & := & \dfrac{1}{1-s}\left(v_1^{1-p}\,(h_0\, v_2^s)^p - v_1^{-p}\partial_1^*(v_2^{sp+1}) - \dfrac{s(s+1)}{2}\, v_1^2\, h_1\, v_2^{sp}\right) \\ & \equiv & h_0\, v_2^{sp} \bmod (u_1^2) \end{array}$$

D'où

$$\partial_2^*(\,(h_0)_{sp}\,) \equiv \frac{s(s+1)}{4} v_1^{p+3}\, g_1\, v_2^{sp-1} \bmod (u_1^{p+4}) \tag{4.10}$$

- Soit $s = kp+1$. D'après le corollaire précédent,

$$\partial_2^*(\, h_0 v_2^{(kp+1)p} - \frac{3}{2} v_1^2 h_1 v_2^{(kp+1)p}\,) \equiv -\frac{1}{2}\, v_1^{p+3}\, g_1\, v_2^{(kp+1)p-1} \quad \mathrm{mod}\,(u_1^{p+4}) \tag{4.11}$$

On pose donc

$$\begin{aligned}(h_0)_{(kp+1)p} &= h_0 v_2^{(kp+1)p} - \frac{3}{2} v_1^2 h_1 v_2^{(kp+1)p} \\ &\equiv h_0 v_2^{(kp+1)p} \quad \mathrm{mod}\,(u_1^2)\end{aligned}$$

Maintenant, supposons par récurrence sur l'entier $n \geq 1$ qu'on ait construit

$$(h_0)_{sp^n} \equiv h_0\, v_2^{sp^n}\ \mathrm{mod}\,(u_1^2)$$

tel que

$$\partial_2^*((h_0)_{sp^n}) \equiv c\, v_1^{A_n+2}\, v_2^{-p^{n-1}-\ldots-1}\, g_1\, v_2^{sp^n}\ \mathrm{mod}\,(u_1^{A_n+3})$$

où $A_n = (p^{n-1}+\ldots+1)(p+1)$, pour un certain entier $n \geq 1$. Au passage,

$$A_n p + p + 1 = (p^n + \cdots + p)(p+1) + p + 1 = A_{n+1}$$

On a

$$\begin{aligned}(h_0)_{sp^n}^p &\equiv h_1\, v_2^{sp^{n+1}+1}\ \mathrm{mod}\,(u_1^{2p}) \\ \partial_1^*(v_2^{sp^{n+1}+1}) &= h_1\, v_1\, v_2^{sp^{n+1}+1} - h_0\, v_1^p\, v_2^{sp^{n+1}}\ \mathrm{mod}\,(u_1^{p+2})\end{aligned}$$

En utilisant l'hypothèse de récurrence,

$$\begin{aligned}\partial_2^*(v_1 (h_0)_{sp^n}^p - \partial_1^*(v_2^{sp^{n+1}+1})) &\equiv v_1 \partial_2^*((h_0)_{sp^n})^p \\ &\equiv c\, v_1^{(A_n+2)p+1}\, v_2^{-p^n-\ldots-p}\, g_1^p\, v_2^{sp^{n+1}} \\ &\equiv c\, v_1^{(A_n+2)p+1}\, v_2^{-p^n-\ldots-p-1}\, g_0\, v_2^{sp^{n+1}} \\ &\equiv c\, v_1^{(A_n+2)p+1}\, g_0\, v_2^{kp-1}\ \mathrm{mod}\,(u_1^{(A_n+3)p+1}) \\ &\equiv c\, v_1^{A_{n+1}+p}\, g_0\, v_2^{kp-1}\ \mathrm{mod}\,(u_1^{A_{n+1}+2p})\end{aligned}$$

où $k = -p^{n-1} - \ldots - 1 + sp^n$. On pose

$$\begin{aligned}(h_0)_{sp^{n+1}} &:= v_1^{1-p} (h_0)_{sp^n}^p - v_1^{-p}\, \partial_1^*(v_2^{sp^{n+1}+1}) - c\, v_1^{A_{n+1}+1-p}\, h_1\, v_2^{kp} \\ &\equiv h_0\, v_2^{sp^{n+1}}\ \mathrm{mod}\,(u_1^2)\end{aligned}$$

Donc,

$$\partial_2^*(\,(h_0)_{sp^{n+1}}\,) \equiv -c\, v_1^{A_{n+1}+2}\, v_2^{-p^n-\ldots-1}\, g_1\, v_2^{sp^{n+1}}\ \mathrm{mod}\,(u_1^{A_{n+1}+3}) \tag{4.12}$$

Construction des éléments $(h_0)_{(sp^2-1)p^{n-2}}$ *:*

Soit s un entier relatif et $n \geq 2$. En jouant à nouveau avec les puissances p-ème,

$$\begin{aligned}\partial_2^*(\, h_0 v_2^{sp^2-1}\,) &\equiv \partial_2^*(\, h_1\, v_2^{sp}\,)^p \\ &\equiv -v_1^{(p-1)p}\, g_0^p\, v_2^{(sp-1)p} \\ &\equiv -v_1^{p^2-p}\, g_1\, v_2^{(sp-1)p+1}\ \mathrm{mod}\,(u_1^{(p+1)p})\end{aligned}$$

Posons,

$$(h_0)_{sp^2-1} = h_0\, v_2^{sp^2-1} + v_1^{p^2-p-2}\, h_0\, v_2^{sp^2-p+1}$$

Ainsi, d'après le corollaire précédent,

$$\begin{aligned}\partial_2^*(\,(h_0)_{sp^2-1}\,) &\equiv v_1^{p^2-p-2+p+3}\, v_2^{sp^2-p} \\ &\equiv v_1^{p^2-p^0+A_0+2}\, v_2^0\, g_1\, v_2^{sp^2-p} \mod (u_1^{p^2+2})\end{aligned} \tag{4.13}$$

Supposons par récurrence sur l'entier $n \geq 2$, qu'on ait construit

$$(h_0)_{(sp^2-1)p^{n-2}} \equiv h_0\, v_2^{(sp^2-1)p^n} \mod (u_1^2)$$

tel que

$$\partial_2^*((h_0)_{(sp^2-1)p^{n-2}}) \equiv c\, v_1^{p^n-p^{n-2}+A_{n-2}+2}\, v_2^{-p^{n-3}-\ldots-1}\, g_1\, v_2^{(sp-1)p^{n-1}} \mod (u_1^{p^n-p^{n-2}+A_{n-2}+3})$$

où la constante c est non nul. Comme précédemment, remarquons que

$$\begin{aligned}(h_0\, v_2^{(sp^2-1)p^{n-2}})^p &= h_1 v_2^{(sp^2-1)p^{n-1}+1} \\ \partial_1^*(\, v_2^{(sp^2-1)p^{n-1}+1}\,) &\equiv v_1\, h_1\, v_2^{(sp^2-1)p^{n-1}+1} + ((sp^2-1)p^{n-2}-1)\, v_1^p\, h_0\, v_2^{(sp^2-1)p^{n-1}}\end{aligned}$$

Par hypothèse de récurrence,

$$\begin{aligned}&\partial_2^*(\,-v_1^{1-p}(h_0)^p_{(sp^2-1)p^{n-2}} + v_1^{-p}\partial_1^*(\, v_2^{(sp^2-1)p^{n-1}+1}\,)\,) \\ \equiv\; & c\, v_1^{p^{n+1}-p^{n-1}+A_{n-2}p+2p+1-p}\, v_2^{-p^{n-2}-\ldots-p}\, g_1^p\, v_2^{(sp-1)p^n} \\ \equiv\; & c\, v_1^{p^{n+1}-p^{n-1}+A_{n-1}}\, v_2^{-p^{n-2}-\ldots-1}\, g_0\, v_2^{(sp-1)p^n} \\ \equiv\; & c\, v_1^{p^{n+1}-p^{n-1}+A_{n-1}}\, g_0\, v_2^{kp-1} \mod (u_1^{p^{n+1}-p^{n-1}+A_{n-1}+2p-1})\end{aligned}$$

où $k = (sp-1)p^{n-1} - p^{n-1} - \ldots - 1$. On pose donc,

$$\begin{aligned}(h_0)_{(sp^2-1)p^{n-1}} &= \frac{1}{1+p^{n-2}}\Big(-v_1^{1-p}(h_0\, v_2^{(sp^2-1)p^{n-2}})^p \\ &\qquad + v_1^{-p}\partial_1^*(\, v_2^{(sp^2-1)p^{n-1}+1}\,) \\ &\qquad + c\, v_1^{p^{n+1}-p^{n-1}+A_{n-1}+1-p}\, h_1\, v_2^{kp}\Big) \\ &\equiv h_0\, v_2^{(sp^2-1)p^{n-1}} \mod (u_1^2)\end{aligned}$$

Donc,

$$\begin{aligned}\partial_2^*(\,(h_0)_{(sp^2-1)p^{n-1}}\,) &\equiv -\frac{c}{1+p^{n-2}}\, v_1^{p^{n+1}-p^{n-1}+A_{n-1}+2}\, g_1\, v_2^{kp-1} \\ &\equiv -\frac{c}{1+p^{n-2}}\, v_1^{p^{n+1}-p^{n-1}+A_{n-1}+2}\, v_2^{-p^{n-2}-\ldots-1} g_1\, v_2^{(sp-1)p^n}\end{aligned} \tag{4.14}$$

modulo $(u_1^{p^{n+1}-p^{n-1}+A_{n-1}+3})$.

□

Définition 4.32.
a) Pour tout entier $n \geq 0$ et tout entier relatif s non nul, on pose

$$(g_1)_{sp^n+\alpha_n} := \begin{cases} v_1^{-A_n-2}\, \partial_2^*(h_0)_{sp^n} & \text{si } s \not\equiv -1, 0\ [p] \\ v_1^{-p^{n+2}+p^n-A_n-2}\, \partial_2^*(h_0)_{(s+p-1)p^n} & \text{si } s \equiv -p\ [p^2] \end{cases}$$

b) Pour tout entier relatif s, on pose

$$(g_0)_{sp-1} := v_1^{1-p}\, \partial_2^*(h_1)_{sp}$$

4.4.3 Le cocycle $(h_0)_0$

Dans le théorème précédent, nous n'avons pas construit l'élément $(h_0)_0$. Pour le construire, nous allons extraire une sous-suite convergente. Considérons la suite $\big(v_2^{-p^n}(h_0)_{p^n}\big)_{n\in\mathbb{N}}$ de l'anneau $(E_2)_{2(p-1)}/(p)$. En tant que $(E_2)_0/(p)$-module, $(E_2)_{2(p-1)}/(p)$ est libre de rang 1. En particulier, il est compact et on peut extraire une sous-suite convergente de la suite précédente (un argument plus algébrique est de voir que $(E_2)_{2(p-1)}/(p) = \mathbb{F}_{p^2}[[u_1]]h_0$ et que les coefficients ne peuvent prendre qu'un nombre fini de valeurs, d'où l'on peut extraire une sous-suite par récurrence qui définie une série formelle en u_1).

Définition 4.33. On se donne $\big(v_2^{-p^{n(k)}}(h_0)_{p^{n(k)}}\big)_{k\in\mathbb{N}}$ une sous-suite convergente et on pose

$$(h_0)_0 := \lim_{k\longrightarrow\infty} v_2^{-p^{n(k)}}(h_0)_{p^{n(k)}} \in (E_2)_{2(p-1)}/(p)$$

Lemme 4.34. *Soit n un entier naturel et $S(u_1)\in\mathbb{F}_p[[u_1^{p+1}]]$, alors*

$$\partial_2^*(\,v_2^{p^n}S(u_1)h_0\,) \equiv v_2^{p^n}\partial_2^*(S(u_1)h_0) \mod (u_1^{p^n})$$

Démonstration. Rappelons que $\partial_2^*(v_2^{p^n}S(u_1)h_0) = \partial_2(e_2)_+ v_2^{p^n}S(u_1)h_0$ et que par construction (proposition-définition 2.44) l'élément $\partial_2(e_2)_+$ appartient à $(IS_2^1)C_1$. Soit $g\in S_2^1$, alors

$$\begin{aligned}(g-e)_*(v_2^{p^n}u_1^i h_0) &= t_0(g)^{(1-p^2)p^n}v_2^{p^n}g_*(u_i^i h_0) - v_2^{p^n}u_1^i h_0\\ &\equiv v_2^{p^n}(g-e)_*(u_1^i h_0) \mod (u_1^{p^n})\end{aligned}$$

D'où, par continuité de l'action, on déduit le lemme. □

Proposition 4.35. *L'élément $(h_0)_0$ appartient au noyau de ∂_2^*.*

Démonstration. D'après un résultat bien connu sur les groupes profinis (lemme 5.1.4 [RZ10]),

$$\mathrm{Hom}_F(\Lambda_{1-p},(E_2)_{2(p-1)}/(p)) \cong \varprojlim_k \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p},\mathbb{F}_{p^2}[u_1]/(u_1^k)\ h_0) \cong \varprojlim_k \mathbb{F}_p[u_1]/(u_1^k)\ h_0$$

Soient k un entier naturel quelconque et N un entier naturel tel que $A_N+2 = (p^{N-1}+\ldots+1)(p+1)+2 \geq k$ et $p^N\geq k$. Soit $n\geq N$, alors du lemme précédent, on déduit le diagramme suivant

$$\begin{tikzcd}
\mathbb{F}_p[u_1]/(u_1^k)\ h_0 \arrow[r, "\partial_2^*"] \arrow[d, "\times v_2^{p^n}"', "\cong"] & \mathbb{F}_p[u_1]/(u_1^k)\ h_0 \arrow[d, "\times v_2^{p^n}"', "\cong"] \\
\mathbb{F}_p[u_1]/(u_1^k)\ h_0 v_2^{p^n} \arrow[r, "\partial_2^*"] & \mathbb{F}_p[u_1]/(u_1^k)\ h_0 v_2^{p^n}
\end{tikzcd}$$

De plus en utilisant le théorème précédent, $\partial_2(v_2^{p^n}(h_0)_{p^n})\equiv 0$ modulo (u_1^k). Ainsi, par passage à la limite, on déduit que $\partial_2^*(h_0)_0 = 0$. □

Une autre construction d'un élément $(h_0)_0$

D'après le lemme 1.6, $g_*u_1 = t_0^{p-1}(g)u_1 + (p-p^p)t_0^{-1}(g)t_1(g)$ et $g_*u^{1-p} = t_0(g)^{1-p}u^{1-p}$, d'où

$$\begin{aligned}g_*v_1 &= g_*u_1\, g_*u^{1-p} = u_1u^{1-p} + (p-p^p)t_0^{-p}(g)t_1(g)\,)\,u^{1-p}\\ &\equiv v_1 + pt_0^{-p}(g)t_1(g)h_0 \mod (p^2)\end{aligned}$$

$(h_0 = u^{1-p})$.

Notons $\partial_1^\star$ l'homomorphisme intégral :

$$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_1,(E_2)_*) : (E_2)_*^F \longrightarrow (E_2)_*^F \otimes (\mathbb{Z}_p h_0 \oplus \mathbb{Z}_p h_1)$$

Lemme 4.36. *On a* $\partial_1^\star(v_1) \equiv ph_0$ *modulo* (p^2, pu_1).

Démonstration. D'après le lemme 1.6 et par définition de v_1, on a

$$\begin{aligned}
\partial_1^\star(v_1) &= \frac{1}{(p+1)\epsilon_+}\sum_{i=0}^{p}\Big(\lambda_i(a_i-e)+\mu_i(b_i-e)\Big)_* v_1 \\
&\equiv \frac{p}{(p+1)\epsilon_+}\sum_{i=0}^{p}\Big(\lambda_i t_0^{-p}(a_i)t_1(a_i)+\mu_i t_0^{-p}(b_i)t_1(b_i)\Big)_* h_0 \quad \bmod (p^2,u_1)
\end{aligned}$$

Or, d'après le corollaire 3.4, modulo (p, u_1)

$$\begin{aligned}
\sum_{i=0}^{p}\lambda_i t_0^{-p}(a_i)t_1(a_i) &\equiv \sum_{i=0}^{p}\lambda_i\omega^{(p-1)i}\epsilon_+ \equiv \frac{p+1}{2}\epsilon_+ \\
\sum_{i=0}^{p}\lambda_i t_0^{-p}(b_i)t_1(b_i) &\equiv \sum_{i=0}^{p}\mu_i\omega^{(p-1)i}\epsilon_- \equiv \frac{p+1}{2}\epsilon_+
\end{aligned}$$

D'où, la congruence. $\square$

En particulier, on en déduit que $\partial_1^\star(v_1)$ est divisible par p. De plus, comme $(E_2)_*$ est sans p-torsion, $\frac{1}{p}\partial_1^\star(v_1)$ est un 2-cocycle non nul, c'est-à-dire un élément dans le noyau de $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_2, (E_2)_*)$. D'après le lemme, cet élément est congrue à h_0 modulo (p, u_1). Ainsi, $(h_0)_0$ la réduction modulo (p) de $\frac{1}{p}\partial_1^\star(v_1)$ convient.

4.5 La troisième différentielle

On rappelle (définition 2.8) que

$$\Lambda := \frac{1}{p+1}\sum_{i=0}^{p}\lambda_i(a_i^{-1}-e)+\mu_i(b_i^{-1}-e)$$

et (proposition 2.10) que

$$\partial_3(e_3) = \frac{1}{2\epsilon_+^2}\Lambda(e_2)_+ + \frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega - \omega\Lambda\omega^{-1})(e_2)_- \tag{4.15}$$

Rappelons le résultat de la proposition 4.10. Soit s un entier relatif, on note $R_s := \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$. Alors, modulo (u_1^{p+4}),

$$\Lambda_* u^s \equiv -v_* u^s \equiv -\epsilon_+(su_1 + (\binom{s}{p} - s\,)u_1^p + (s+R_s)u_1^{p+2})u^s$$

Proposition 4.37. *Soit s un entier relatif, alors*

1. $\partial_3^*(g_0 v_2^s) \equiv -(s+1)\, v_1\, v_2^s - (1+s+R_{1-p+s})\, v_1^{p+2}\, v_2^{s-1} \quad \bmod (u_1^{2p+3})$

2. $\partial_3^*(g_1 v_2^s) \equiv -(\binom{s+p-1}{p} - s + 1)\, v_1^p\, v_2^{s-1} \quad \bmod (u_1^{2p+1})$

où $R_s = \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$.

Démonstration. Afin de traiter les deux congruences en même temps, rappelons que $g_0 = u^{1-p}$ et $g_1 = u^{p-1}$. Soit $k = \pm 1$, alors $k = 1$ (resp. $k = -1$) correspond à g_0 (resp. g_1) qui induit l'identité $\Lambda_{1-p} \to \mathbb{W}u^{1-p} \subset (E_2)_*$ (resp. l'automorphisme de Frobenius $\Lambda_{1-p} \to \mathbb{W}u^{p-1}$).
Posons

$$\begin{array}{rcl} \alpha & = & k+s \\ \beta & = & \binom{k-kp+s}{p} - k - s \\ \gamma & = & k+s+R_{k-kp+(1-p^2)s} \end{array}$$

alors, d'après la relation (4.15) concernant $\partial_3(e_3)$ et l'étude de l'action de Λ, on a

$$\begin{array}{rl} & \partial_3^*(u^{k(1-p)}v_2^s) \\ \equiv & \frac{1}{2\epsilon_+^2}\Lambda_* u^{k(1-p)}v_2^s\epsilon_+ + \frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega - \omega\Lambda\omega^{-1})_* u^{k(1-p)}v_2^s\epsilon_- \\ \equiv & \frac{1}{2\epsilon_+^2}\Lambda_* u^{k(1-p)}v_2^s\epsilon_+ + k\frac{1}{4\epsilon_-^2\mu_1}(\omega_*^{-1}\Lambda_*\omega^{k(1-p)} - \omega_*\Lambda_*\omega^{-k(1-p)})u^{k(1-p)}v_2^s\epsilon_- \\ \equiv & \frac{-1}{2}\Big(\alpha\, u_1 + \beta\, u_1^p + \gamma\, u_1^{p+2}\Big)u^{k(1-p)}v_2^s \\ & -\frac{k\epsilon_+}{4\epsilon_-\mu_1}\omega_*^{-1}\Big(\alpha\, u_1 + \beta\, u_1^p + \gamma\, u_1^{p+2}\Big)\omega^{k(1-p)}u^{k(1-p)}v_2^s \\ & +\frac{k\epsilon_+}{4\epsilon_-\mu_1}\omega_*\Big(\alpha\, u_1 + \beta\, u_1^p + \gamma\, u_1^{p+2}\Big)\omega^{-k(1-p)}u^{k(1-p)}v_2^s \\ \equiv & \frac{-1}{2}\Big(\alpha\, u_1 + \beta\, u_1^p + \gamma\, u_1^{p+2}\Big)u^{k(1-p)}v_2^s \\ & -\frac{k\epsilon_+}{4\epsilon_-\mu_1}\Big(\alpha\,\omega^{(1-k)(1-p)}\, u_1 + \beta\,\omega^{(-1-k)(1-p)}\, u_1^p + \gamma\,\omega^{(1-k)(1-p)}\, u_1^{p+2}\Big)\omega^{k(1-p)}u^{k(1-p)}v_2^s \\ & +\frac{k\epsilon_+}{4\epsilon_-\mu_1}\Big(\alpha\,\omega^{(k-1)(1-p)}u_1 + \beta\,\omega^{(1+k)(1-p)}u_1^p + \gamma\,\omega^{(k-1)(1-p)}u_1^{p+2}\Big)\omega^{-k(1-p)}u^{k(1-p)}v_2^s \\ \equiv & \frac{-1}{2}\Big(\alpha\, u_1 + \beta\, u_1^p + \gamma\, u_1^{p+2}\Big)u^{k(1-p)}v_2^s \\ & -\frac{k\epsilon_+}{4\epsilon_-\mu_1}\Big(\alpha\,\omega^{1-p}u_1 + \beta\,\omega^{p-1}u_1^p + \gamma\,\omega^{1-p}u_1^{p+2}\Big)u^{k(1-p)}v_2^s \\ & +\frac{k\epsilon_+}{4\epsilon_-\mu_1}\Big(\alpha\,\omega^{p-1}u_1 + \beta\,\omega^{1-p}u_1^p + \gamma\,\omega^{p-1}u_1^{p+2}\Big)u^{k(1-p)}v_2^s \quad \mathrm{mod}\,(u_1^{p+4}) \end{array}$$

Notons que

$$\frac{\epsilon_+}{2\epsilon_-}(\omega^{k(1-p)} - \omega^{-k(1-p)}) = k\mu_1$$

d'où,

$$\begin{array}{rl} & \partial_3^*(u^{k(1-p)}v_2^s) \\ \equiv & \frac{-1}{2}\Big((1-k)(k+s)u_1 \\ & +(1+k)(\ \binom{k-kp+s}{p} - k - s\ )u_1^p \\ & +(1-k)(k+s+R_{k-kp+(1-p^2)s})u_1^{p+2}\Big)u^{k(1-p)}v_2^s \quad \mathrm{mod}\,(u_1^{p+4}) \end{array}$$

Ensuite pour aboutir à la précision annoncée dans les congruences de la proposition, on utilise la fait que ∂_3^* est un homomorphisme de degré 0 et que $u_1^t \in (E_2)_0^F/(p)$ implique t est un multiple de $p+1$. □

Dans le théorème-définition 4.31 et la définition 4.32, on a construit des éléments $(g_0)_{sp^n}$ et $(g_1)_{sp^n}$ pour certaines valeurs de s et n. Ils forment une famille libre qui complétée par les éléments

$$\begin{array}{ll} g_0 v_2^s & \text{pour } s \not\equiv -1[p] \\ g_1 v_2^{sp^{n+1}+\alpha_n} & \text{pour } n \geq 1, \quad s \not\equiv -1[p] \end{array}$$

défini une base topologique de $(E_2)_* \otimes (\mathbb{F}_p g_0 \oplus \mathbb{F}_p g_1)$. La raison est une simple application du lemme suivant et du lemme 4.1.

Lemme 4.38. *Les ensembles*

$$\{\, \frac{1-p^n}{p-1} + sp^n;\ n \geq 0 \text{ et } s \not\equiv -1, 0[p]\,\}, \quad \{\, \frac{1-p^n}{p-1} + sp^{n+1};\ n \geq 0 \text{ et } s \equiv -1[p]\,\}$$

$$\{\, \frac{1-p^n}{p-1} + sp^{n+1};\ n \geq 0 \text{ et } s \not\equiv -1[p]\,\}$$

forment une partition de l'ensemble des entiers relatifs.

Démonstration. Soit t un entier relatif, alors il existe un unique entier n et un unique entier relatif m premier à p tels que $(p-1)t - 1 = mp^n$. En particulier, $m+1$ est divisible par $p-1$. Notons s le quotient de $m+1$ par $p-1$. Alors, la condition $m \not\equiv 0\,[p]$ équivaut à $s \not\equiv -1\,[p]$. De plus, on a l'identité

$$t = \frac{1}{p-1}(1 + mp^n) = \frac{1-p^n}{p-1} + sp^n.$$

D'où la partition. □

D'après la proposition précédente, on a que pour tout $s \not\equiv -1[p]$,

$$\partial_3^*(g_0 v_2^s) \equiv -(s+1)\, v_1\, v_2^s \mod (u_1^2)$$

qui est non nul.

Notation. Pour tout entier naturel n, on note $\alpha_n = \frac{1-p^n}{p-1} = -1 - p - \ldots - p^{n-1}$.

Définition 4.39. Soient $s \not\equiv -1[p]$ et $n = 0$, on pose

$$(g_0)_{sp^n+\alpha_n} := g_0 v_2^s$$

et

$$(h_0 g_1)_{sp^n} := \frac{-1}{s+1} v_1^{-1} \partial_3^*(g_0 v_2^s) \equiv v_2^{sp^n}$$

Considérons maintenant le second type de termes.

Définition 4.40. Soient $s \not\equiv -1[p]$ et $n \geq 1$. On pose

$$\begin{array}{rcl} (g_1)_{sp} & := & g_1 v_2^{sp} \\ (g_1)_{sp^{n+1}+\alpha_n} & := & v_1^{-p-1}\left(\left(v_1^{p-1}(g_1)_{sp^n+\alpha_{n-1}}\right)^p + \partial_2^*(h_1 v_2^{sp^{n+1}+p\alpha_{n-1}})\right) \\ & & +\ (-1)^n(s+1)\, v_1^{p^n(p+1)-p-3} g_0 v_2^{sp^{n+1}+\alpha_{n+1}+1} \\ (h_0 h_1)_{sp^n+\alpha_n} & := & v_1^{-p^{n-1}(p+1)+1}\partial_3^*((g_1)_{sp^n+\alpha_{n-1}}) \end{array}$$

pour tout entier $n > 0$.

Théorème 4.41. *Pour tout entier $n \geq 1$ et tout entier $s \not\equiv -1$ $[p]$, modulo (u_1),*

$$(g_1)_{sp^n+\alpha_{n-1}} \equiv \begin{cases} g_1 v_2^{sp^n+\alpha_{n-1}} & si\ n=1 \\ \frac{-1}{2} g_1 v_2^{sp^n+\alpha_{n-1}} & si\ n=2 \\ -g_1 v_2^{sp^n+\alpha_{n-1}} & si\ n>2 \end{cases}$$

et

$$\partial_3^*((g_1)_{sp^n+\alpha_{n-1}}) \equiv (-1)^n (s+1)\ v_1^{p^{n-1}(p+1)-1}\ v_2^{sp^n+\alpha_n} \mod (u_1^{p^{n-1}(p+1)})$$

Démonstration. Soit $s \not\equiv -1$ $[p]$. Pour $n=1$, on a

$$\begin{aligned} \partial_3^*(g_1 v_2^{sp}) &\equiv -(\binom{sp+p-1}{p} - sp + 1)\ v_1^p\ v_2^{sp-1} \\ &\equiv -(s+1)\ v_1^p\ v_2^{sp-1} \mod (u_1^{p+1}) \end{aligned}$$

Supposons par récurrence sur $n \geq 1$ qu'on a

$$\partial_3^*((g_1)_{sp^n+\alpha_{n-1}}) \equiv (-1)^n (s+1)\ v_1^{p^{n-1}(p+1)-1}\ v_2^{sp^n+\alpha_n} \mod (u_1^{p^{n-1}(p+1)})$$

Notons que $\alpha_n = \frac{1-p^n}{p-1} = p\alpha_{n-1} - 1$. Ainsi, d'après la proposition 4.29, on a

$$\begin{aligned} & v_1^{p-1}\Big((g_1)_{sp^n+\alpha_{n-1}}\Big)^p + \partial_2^*(h_1 v_2^{sp^{n+1}+p\alpha_n}) \\ \equiv\ & v_1^{p-1} g_0 v_2^{sp^{n+1}+\alpha_n} - v_1^{p-1} g_0 v_2^{sp^{n+1}+\alpha_n} + \frac{sp^n+\alpha_{n-1}-1}{2} v_1^{p+1} g_1 v_2^{sp^{n+1}+\alpha_{n-1}} \\ \equiv\ & \begin{cases} -\frac{1}{2}\ v_1^{p+1}\ g_1\ v_2^{sp^{n+1}+\alpha_{n-1}} & \text{si } n=1 \\ -v_1^{p+1}\ g_1\ v_2^{sp^{n+1}+\alpha_{n-1}} & \text{si } n>1 \end{cases} \mod (u_1^{2p}) \end{aligned}$$

D'où, la première congruence. Rappelons que

$$R_{1-2p+kp^2} = R_{1-2p} = \frac{1}{2}(\binom{1+(p-2)p}{p+2} - \binom{-2p}{2})(\epsilon_+^2 - \epsilon_-^2) = 0$$

Ainsi, en utilisant la proposition précédente, modulo $(u_1^{p^n(p+1)})$, on a

$$\begin{aligned} \partial_3^*((g_1)_{sp^{n+1}+\alpha_n}) &\equiv v_1^{-2}\partial_3^*((g_1)_{sp^n+\alpha_{n-1}})^p + (-1)^n(s+1) v_1^{p^n(p+1)-p-3} \partial_3^*(g_0 v_2^{sp^{n+1}+\alpha_{n+1}+1}) \\ &\equiv (-1)^n (s+1)\, v_1^{p^n(p+1)-p-2} v_2^{sp^{n+1}+p\alpha_n} \\ &\quad -(-1)^n(s+1)(\alpha_{n+1}+2)\, v_1^{p^n(p+1)-p-2} v_2^{sp^{n+1}+\alpha_{n+1}+1} \\ &\quad -(-1)^n(s+1)(1+\alpha_{n+1}+1+R_{1-2p}) v_1^{p^n(p+1)-1} v_2^{sp^{n+1}+\alpha_{n+1}} \\ &\equiv (-1)^{n+1}(s+1) v_1^{p^n(p+1)-1} v_2^{sp^{n+1}+\alpha_{n+1}} \end{aligned}$$

□

Chapitre 5

Le groupe Pic_2 de Hopkins

Commençons par rappeler brièvement la définition du groupe Pic_2 de Hopkins, introduit et étudié pour la première fois dans [Str92] et approfondi dans [HMS94]. L'objet de ce chapitre est de déterminer un sous-groupe d'indice 2 du groupe Pic_2 qui dans le cas $p \geq 5$ est connue pour être isomorphe à $H^1(\mathbb{G}_2, (E_2)_0^\times)$.

Définition 5.1. Soit Z un spectre $K(n)$-local. On dit que Z est inversible si Z est inversible dans la catégorie symétrique monoïdale des spectres $K(n)$-locaux, c'est-à-dire s'il existe un spectre $K(n)$-local W tel que

$$L_{K(n)}(Z \wedge W) = L_{K(n)}S^0$$

On note Pic_n le groupe des classes d'isomorphismes de tels spectres où la multiplication est donnée par

$$(X, Y) \mapsto L_{K(n)}(X \wedge Y)$$

Dans [HMS94], on construit un foncteur $\mathcal{K}_{n,*}(-)$ se comportant essentiellement comme une complétion de $E(n)_*(-)$ la théorie d'homologie de Johnson-Wilson.

Théorème 5.2 (theorem 1.3 [HMS94])**.** *Les propriétés suivantes sont équivalentes :*

1. $L_{K(n)}Z \in \mathrm{Pic}_n$
2. $\dim_{K(n)_*}(K(n)_*Z) = 1$.
3. $\mathcal{K}_{n,*}(Z) \cong \mathcal{K}_{n,*}(S^k)$ *pour un certain* k.

Lorsque $p \geq 5$, il a été établi (voir [HMS94] section 7 ou [Str92] page 51) que Pic_2 admet un sous-groupe d'indice 2, noté Pic_2^0 qui est isomorphe à un groupe de Picard $\mathrm{Pic}_2^{\mathrm{alg},0}$ d'une certaine catégorie monoïdale de modules sur l'anneau de Lubin-Tate et muni d'une action du groupe stabilisateur de Morava. De plus, $\mathrm{Pic}_2^{\mathrm{alg},0}$ est isomorphe à $H^1(\mathbb{G}_2, (E_2)_0^\times)$. L'objet de ce chapitre est de calculer $H^1(\mathbb{G}_2, (E_2)_0^\times)$. Ce qui permettra dans le cas $p \geq 5$ de démontrer le théorème suivant et ceci avec une méthode sensiblement équivalente à celle utilisée par M. Hopkins dans des notes non publiées.

Théorème 5.3 (Hopkins, Karamanov)**.** *Soit p un nombre premier impair, alors*

$$\mathrm{Pic}_2^{\mathrm{alg}} \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/2(p^2-1)$$

5.1 Groupe de Picard des G-modules

Pour plus de clarté, je commence par rappeler le paragraphe 8. *Digression on Picard Groups of G-modules* de [HMS94]. Soient R un anneau abélien profini et G un groupe profini qui agit par automorphisme continue d'anneaux sur R.

Définition 5.4. Soit M un R-module profini muni d'une action continue de G, on dit que M est un **R-G-module**, ou un R-module avec une action de G compatible, si quel que soient $g \in G$, $\lambda \in R$ et $m \in M$: $g_*(\lambda m) = (g_*\lambda)(g_*m)$. En d'autres termes, le diagramme suivant commute.

$$\begin{tikzcd} R \underset{R}{\otimes} M \arrow[r, "g\times g"] \arrow[d] & R \underset{R}{\otimes} M \arrow[d] \\ M \arrow[r, "g"] & M \end{tikzcd}$$

Étant donné M, N deux R-G-modules, on définit une structure de R-G-module sur $M \underset{R}{\otimes} N$ via l'action diagonale de G et on note ce R-G-module $M \otimes N$. On note R-G-Mod la catégorie symétrique monoïdale des R-G-modules.

Un premier exemple de R-G-module est R lui-même.

Définition 5.5. Soit M un objet de la catégorie symétrique monoïdale R-G-Mod, on dit qu'il est inversible s'il existe un module N vérifiant $M \otimes N \cong R$.

Lemme 5.6 (lemme 8.2 [HMS94])**.** *Si R est local, M, N sont deux R-modules tels que $M \otimes N \cong R$ et M est de type fini alors $M \cong R$. Si, de plus, R est noethérien, on peut omettre l'hypothèse sur M.*

Corollaire 5.7 (corollaire 8.3 [HMS94])**.** *Si R est un anneau local noethérien profini commutatif muni d'une action par automorphisme d'anneaux d'un groupe profini G. Alors, un R-G-module M est inversible si et seulement si la structure sous-jacente de R-module de M est libre de rang un.*

Soit R un anneau profini commutatif, muni d'une action par automorphisme d'anneaux d'un groupe profini G. On suppose de plus que pour tout R-G-module M, M est *inversible* si et seulement si $M \cong R$ en tant que R-modules.
Soit M un R-G-module inversible. Soit e un générateur de M en tant que R-module, on associe une application

$$\phi_{M,e} :\ G \longrightarrow R^\times$$

caractérisée par $\phi_{M,e}(x)e = x_*e$ pour tout x dans G. On note alors que pour tous $x, y \in G$, on a

$$\phi_{M,e}(xy)e = (xy)_*e = x_*(\phi_{M,e}(y)e) = x_*(\phi_{M,e}(y))\phi_{M,e}(x)e$$

c'est-à-dire, $\phi_{M,e}(xy) = x_*(\phi_{M,e}(y))\phi_{M,e}(x)$. Réciproquement, si l'on se donne une application $\phi : G \to R^\times$ telle que $\phi(xy) = \phi(x)\,(x_*\phi(y))$, appelée dérivation, alors le module $M = R$ muni de l'action caractérisée par $x_*e = \phi(x)e$ pour tout x dans G est un R-G-module inversible.
En particulier, se donner un R-G-module inversible à isomorphisme près équivaut à se donner une dérivation. D'où les classes d'isomorphismes de R-G-modules inversibles forment un ensemble.

Définition 5.8. Soit R un anneau profini commutatif, muni d'une action par automorphisme d'anneaux d'un groupe profini G. On suppose de plus que pour tout R-G-module M, M est *inversible* si et seulement si $M \cong R$ en tant que R-modules. On note $\mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})$ le groupe abélien des classes d'isomorphisme de R-G-module inversible muni de l'addition : $[M] + [N] = [M \otimes N]$.

Avant de décrire $\mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})$, donnons une précisions sur les dérivations.

Définition 5.9. Soit G un groupe profini et M un G-module, on dit qu'une application continue $d : G \longrightarrow M$ est une **dérivation** si $d(xy) = d(x) + x_* d(y)$.
Soit $a \in M$, la **dérivation intérieure** associée à a est la dérivation $d_a : G \longrightarrow M$ définie par $d_a(x) = x_* a - a$. On note $\mathrm{IDer}_G(M)$ le groupe des dérivations intérieures de G dans M.

Lemme 5.10 (page 165 [Wil98])**.** *Le groupe de cohomologie continue $H^1(G, M)$ est isomorphe au groupe des dérivations quotienté par le sous-groupe des dérivations intérieures.*

Proposition 5.11 (proposition 8.4 [HMS94])**.** *Soit R un anneau profini commutatif unitaire, muni d'une action par automorphisme continue d'anneaux d'un groupe profini G. On suppose de plus que pour tout R-G-module M, M est inversible si et seulement si $M \cong R$ en tant que R-modules. L'homomorphisme*

$$\begin{array}{rcl} \mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod}) & \longrightarrow & H^1(G, R^\times) \\ [M] & \longmapsto & [\phi_{M,e}] \end{array}$$

est un isomorphisme.

Avant de passer au calcul de $H^1(\mathbb{G}_2, (E_2)_0^\times)$. Précisons la topologie du groupe de Picard $\mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})$ sous certaines hypothèses sur l'anneau R.
Soit R un anneau profini commutatif, muni d'une action par automorphisme d'anneaux d'un groupe profini G. On suppose de plus que R est local et complet pour la topologie $\mathfrak{m}$-adique où $\mathfrak{m}$ est l'idéal maximal de R. D'après le corollaire précédent, on note que tout R-G-module M, M est *inversible* si et seulement si $M \cong R$ en tant que R-modules. Ainsi, la proposition précédente s'applique.
Supposons de plus qu'il existe une résolution projective C_* de R au-dessus de l'algèbre profini $R[\![G]\!]$ telle que les modules C_* soient de type fini. Soit $M = \varprojlim M_\alpha$ une limite inverse de $R[\![G]\!]$-modules finis, comme

$$\mathrm{Hom}_{R[\![G]\!]}(C_*, M) = \varprojlim \, \mathrm{Hom}_{R[\![G]\!]}(C_*, M_\alpha)$$

est une limite inverse de groupes finis, il est profini. Par exactitude du foncteur limite inverse dans la catégorie des groupes profinis (proposition 2.2.4 [RZ10]), on déduit que

$$H^*(G, M) = \varprojlim \, H^*(G, M_\alpha)$$

est profini.
Soit n un entier naturel, posons $\mathbb{U}_n(R) = \{x \in R;\ x \equiv 1 \mod \mathfrak{m}^n\} \subset R^\times$. Soient $x, y \in R^\times$, alors

$$x \equiv y \mod \mathfrak{m}^n \quad \Longleftrightarrow \quad x\,y^{-1} \in \mathbb{U}_n(R)$$

D'où, l'on déduit que $R^\times/\mathbb{U}_n(R) \cong (R/\mathfrak{m}^n)^\times$ et

$$H^1(G, R^\times) \cong \varprojlim \, H^1(G, (R/\mathfrak{m}^n)^\times)$$

Ainsi, les groupes

$$\ker\left(H^1(G, R^\times) \longrightarrow H^1(G, (R/\mathfrak{m}^n)^\times)\right)$$

forment une base de voisinages de zéro dans $H^1(G, R^\times)$. Notons que les anneaux $R/\mathfrak{m}^n$ sont aussi locaux. Ainsi, d'après la proposition précédente, on déduit que $\mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})$ est isomorphe à la limite inverse des groupes $\mathrm{Pic}(R/\mathfrak{m}^n\text{-}G\text{-}\mathrm{Mod})$. D'où le lemme suivant.

Lemme 5.12. *Soit R un anneau profini commutatif, muni d'une action par automorphisme d'anneaux d'un groupe profini G. On suppose de plus que R est local et complet pour la topologie $\mathfrak{m}$-adique où $\mathfrak{m}$ est l'idéal maximal de R. Les sous-groupes*

$$\mathcal{U}_n = \{\ [M] \in \mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})\,;\ \ M \otimes (R/\mathfrak{m}^n)^\times \cong (R/\mathfrak{m}^n)^\times\ \}$$

déterminent une base de la topologie du groupe de Picard $\mathrm{Pic}(R\text{-}G\text{-}\mathrm{Mod})$.

5.2 Le groupe de Picard algébrique $\mathrm{Pic}_2^{\mathrm{alg},0}$

Définition 5.13. On pose $\mathrm{Pic}_2^{\mathrm{alg},0}$ le groupe $\mathrm{Pic}((E_2)_0\text{-}\mathbb{G}_2\text{-}\mathrm{Mod})$.

Avant de calculer $\mathrm{Pic}_2^{\mathrm{alg},0}$, construisons plusieurs modules inversibles particuliers. Rappelons que $(E_n)_0 = \mathbb{W}[[u_1, \ldots, u_{n-1}]]$ est un anneau local complet séparé.

Définition 5.14. Soit R un anneau local d'idéal maximal $\mathfrak{m}$, on pose

$$\mathbb{U}_1(R) = \{ x \in R : \ x \equiv 1 \mod \mathfrak{m} \}$$

On a la décomposition suivante :

$$(E_n)_0^\times \cong \mathbb{F}_{p^n}^\times \oplus \mathbb{U}_1((E_n)_0)$$

Comme $\mathbb{F}_{p^n}^\times$ est d'ordre premier à p et $\mathbb{U}_1((E_n)_0$ est un pro-p-groupe, cette décomposition est vraie en tant que $\mathbb{Z}_p[\![\mathbb{G}_n]\!]$-module. Ainsi, les projections sur les facteurs directs sont $\mathbb{Z}_p[\![\mathbb{G}_n]\!]$-linéaires.
Rappelons que le groupe stabilisateur de Morava $\mathbb{G}_n$ est isomorphe au produit semi-direct $S_n \rtimes F$ où $F = \boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$.

Proposition-Définition 5.15. *Les applications suivantes :*

1. *L'application $t_0 : \mathbb{G}_n \to (E_n)_0^\times$ définie dans le chapitre 1 ((1.4) page 16).*
2. $\tilde{t}_0 : \mathbb{G}_n \xrightarrow{t_0} (E_n)_0^\times \twoheadrightarrow \mathbb{U}_1((E_n)_0)$.
3. *Le déterminant réduit $N : \mathbb{G}_n \to \mathbb{Z}_p^\times/\boldsymbol{\mu}_{p-1} \cong \mathbb{U}_1(\mathbb{Z}_p) \hookrightarrow (E_n)_0^\times$, défini dans la proposition-définition 1.11.*
4. $\Omega : \mathbb{G}_n \xrightarrow{t_0} (E_n)_0^\times \twoheadrightarrow \mathbb{F}_{p^n}^\times$. *Elle vérifie :*

$$\forall g \in S_n \ \forall \xi \in \boldsymbol{\mu}_{p^n-1} : \quad \Omega(g\xi) = \xi \quad \textit{et} \quad \Omega(g\sigma) = 1$$

où $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$ est l'automorphisme de Frobenius.

sont des dérivations.

Démonstration. 1. Pour tout $g \in \mathbb{G}_n$, $g_* u = t_0(g) u$ et $(E_n)_{-2}$ est un $(E_n)_0$-$\mathbb{G}_n$-module, d'où t_0 est une dérivation.

2. Vu que la projection est un homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_n]\!]$-linéaire, $\tilde{t}_0$ est aussi une dérivation.
3. L'action de $\mathbb{G}_n$ sur $\mathbb{Z}_p^\times \subset (E_n)_0^\times$ est triviale, d'où l'on déduit que l'homomorphisme N : $\mathbb{S}_n \to \mathbb{U}_1(\mathbb{Z}_p)$ est un homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_n]\!]$-linéaire.
4. D'après la congruence (1.5), pour tout $g \in S_n^1$, $t_0(g) \equiv 1$ modulo $(p, u_1, \ldots, u_{n-1})$ et l'action de g sur $\boldsymbol{\mu}_{p^n-1}$ est triviale. Ainsi, d'après le proposition 1.4, pour tout $g \in S_n$ et tout $\xi \in \boldsymbol{\mu}_{p^n-1}$, on a

$$t_0(g\xi) = t_0(g) g_* t_0(\xi) \equiv \xi \mod (p, u_1, \ldots, u_{n-1})$$

et $t_0(g\sigma) = t_0(g) g_* 1 \equiv 1$ modulo $(p, u_1, \ldots, u_{n-1})$.

□

Revenons au cas $n = 2$ et $p \geq 5$. Comme l'anneau $(E_2)_0 = \mathbb{W}[[u_1]]$ est local profini noethérien, d'après la proposition 8.4 de [HMS94], le groupe $\mathrm{Pic}((E_2)_0\text{-}\mathbb{G}_2\text{-}\mathrm{Mod})$ est isomorphe à $H^1(\mathbb{G}_2, (E_2)_0^\times)$. Pour déterminer le précédent groupe de cohomologie, nous allons le décomposer à l'aide de suite exacte courte induite cohomologie par des sous-groupes et sous-modules. Un résumé est donné dans le diagramme 5.1 page 114. Le partie la plus technique est le calcul de $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}[[u_1]]^\times)$ effectué dans la section 5.5.

Lemme 5.16.
a) Nous avons la suite exacte courte suivante

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow H^1(\mathbb{G}_2, (E_2)_0^\times) \longrightarrow H^1(\mathbb{G}_2^1, (E_2)_0^\times) \longrightarrow 0$$

b) Le groupe de cohomologie $H^1(\mathbb{G}_2^1, (E_2)_0^\times)$ est isomorphe à $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}[[u_1]]^\times)$.

Démonstration. a) On rappelle que $\mathbb{G}_2/\mathbb{G}_2^1 \cong 1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$ et que $\mathbb{Z}_p$ s'injecte dans le centre de $\mathbb{G}_2$.
Comme $\mathbb{Z}_p$ est de dimension cohomologique 1, la page E_2 de la suite spectrale de Lyndon-Hochschild-Serre (théorème A.18) associée à $\mathbb{G}_2^1 \triangleleft \mathbb{G}_2$ est concentrée sur deux colonnes. Ainsi, on déduit la suite exacte suivante :

$$0 \longrightarrow H^1(\mathbb{Z}_p, H^0(\mathbb{G}_2^1, (E_2)_0^\times)) \xrightarrow{\text{inf}} H^1(\mathbb{G}_2, (E_2)_0^\times) \xrightarrow{\text{res}} H^0(\mathbb{Z}_p, H^1(\mathbb{G}_2^1, (E_2)_0^\times)) \xrightarrow{\text{d}} 0$$

D'après le corollaire 4.5, le sous-module $\mathbb{Z}_p^\times$ de $(E_2)_0^\times$ est égal à $H^0(\mathbb{G}_2^1, (E_2)_0^\times)$. De plus, d'après la proposition 1.4, l'action de $\mathbb{G}_2/\mathbb{G}_2^1 \cong 1 + p\mathbb{Z}_p \subset \mathbb{G}_2^1$ sur $(E_2)_0$ est triviale, d'où

$$H^1(\mathbb{Z}_p, H^0(\mathbb{G}_2^1, (E_2)_0^\times)) \quad \cong \quad H^1(\mathbb{Z}_p, \mathbb{Z}_p^\times) = \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}/p-1 \oplus \mathbb{Z}_p) \cong \mathbb{Z}_p,$$

l'action de $\mathbb{G}_2/\mathbb{G}_2^1$ sur $H^1(\mathbb{G}_2^1, (E_2)_0^\times)$ est aussi triviale et

$$H^0(\mathbb{Z}_p, H^1(\mathbb{G}_2^1, (E_2)_0^\times)) \quad \cong \quad H^1(\mathbb{G}_2^1, (E_2)_0^\times)$$

b) En considérant les relations entre l'exponentielle et le logarithme dans les anneaux valués complets (section III.I.I de [Laz65]), on déduit l'existence de la suite exacte courte suivante :

$$1 \longrightarrow (E_2)_0 \xrightarrow{\exp(p\_)} (E_2)_0^\times \longrightarrow \mathbb{F}_{p^2}[[u_1]]^\times \longrightarrow 1$$

Ainsi, du corollaire 4.5, on déduit le suite exacte suivante :

$$0 = H^1(\mathbb{G}_2^1, (E_2)_0) \longrightarrow H^1(\mathbb{G}_2^1, (E_2)_0^\times) \longrightarrow H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}[[u_1]]^\times) \longrightarrow H^2(\mathbb{G}_2^1, (E_2)_0) = 0$$

D'où le lemme. $\square$

Définition 5.17. Posons $U_1 = \{x \in \mathbb{F}_{p^2}[[u_1]];\ x \equiv 1 \mod (u_1)\}$ sous-groupe de $(E_2)_0^\times/(p)$.

Lemme 5.18. *En tant que $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module, $\mathbb{F}_{p^2}[[u_1]]^\times \cong \mathbb{F}_{p^2}^\times \oplus U_1$ et*

$$H^1(\mathbb{G}_2^1, (E_2)_0^\times) \cong H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \times H^1(\mathbb{G}_2^1, U_1)$$

Démonstration. Comme l'ordre de $\mathbb{F}_{p^2}^\times$ est premier à p, on déduit que la décomposition donnée dans le lemme est bien une décomposition en tant que $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module. Le foncteur $H^1(\mathbb{G}_2^1, \_)$ est additif, d'où la seconde partie du lemme. $\square$

Dans un premier temps, nous allons déterminer $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times)$.

Proposition 5.19. *Soient p un nombre premier, n un entier naturel,* Gal *le groupe de Galois* $\mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$*. On munit $\mathbb{F}_{p^n}^\times$ de l'action de $\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}$ telle que l'action de $\boldsymbol{\mu}_{p^n-1}$ est triviale et $\sigma_* x = x^p$ pour tout x, où σ est l'automorphisme de Frobenius. Alors,*

$$H^1(\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal},\ \mathbb{F}_{p^n}^\times) \ \cong\ H^1(\boldsymbol{\mu}_{p^n-1},\ \mathbb{F}_{p^n}^\times) \ \cong\ \mathbb{Z}/(p^n-1)$$

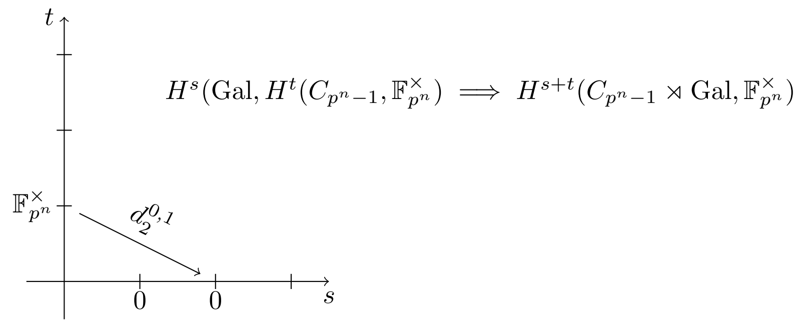

FIGURE 5.1 – Une suite spectrale LHS

Remarque. Un petit rappel, soient a, n deux entiers naturels. Du théorème de Gauss, on déduit que pour tout entier x, $ax \equiv 0[n]$ est équivalent à $x \equiv 0[\frac{n}{a \wedge n}]$, où $a \wedge n$ désigne le pgcd de a et n. D'où la suite exacte courte :

$$0 \longrightarrow \mathbb{Z}/_{a \wedge n} \xrightarrow{\frac{n}{a\wedge n}} \mathbb{Z}/_n \xrightarrow{a} a\mathbb{Z}/_n \cong \mathbb{Z}/_{\frac{n}{a\wedge n}} \longrightarrow 0$$

et $\mathrm{Coker}(\mathbb{Z}/_n \xrightarrow{a} \mathbb{Z}/_n) \cong \mathbb{Z}/_{a \wedge n}$.

Démonstration. Nous allons considérer la suite spectrale de Lyndon-Hochschild-Serre associée au produit semi-direct $\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}$:

$$H^s(\mathrm{Gal}, H^t(\boldsymbol{\mu}_{p^2-1}, \mathbb{F}_{p^2}^\times)) \Rightarrow H^{s+t}(\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}, \mathbb{F}_{p^2}^\times)$$

Comme on le voit dans la figure 5.1, il nous faut calculer $E_2^{s,t}$ pour $(s,t) = (0,1), (1,0)$ et $(0,2)$. En utilisant, la résolution standard du groupe cyclique Gal, d'ordre n, on déduit que :

$$\begin{aligned} H^*(\mathrm{Gal}, H^0(\boldsymbol{\mu}_{p^n-1}, \mathbb{F}_{p^n}^\times)) &\cong H^*(\mathbb{Z}/_{p^n-1} \xrightarrow{p-1} \mathbb{Z}/_{p^n-1} \xrightarrow{1+\ldots+p^{n-1}} \mathbb{Z}/_{p^n-1} \xrightarrow{p-1} \ldots) \\ &\cong \begin{cases} \mathbb{Z}/_{p-1} & \text{si } * = 0 \\ 0 & \text{si } * > 0 \end{cases} \end{aligned}$$

D'autre part, d'après le lemme A.21, $H^1(\boldsymbol{\mu}_{p^n-1}, \mathbb{Z}/_{p^n-1}) \cong \mathbb{Z}/_{p^n-1}$ muni d'une action triviale de Gal. Ainsi

$$\begin{aligned} H^*(\mathrm{Gal}, H^1(\boldsymbol{\mu}_{p^n-1}, \mathbb{F}_{p^n}^\times)) &\cong H^*(\mathbb{Z}/_{p^n-1} \xrightarrow{0} \mathbb{Z}/_{p^n-1} \xrightarrow{n} \mathbb{Z}/_{p^n-1} \xrightarrow{0} \ldots) \\ &\cong \begin{cases} \mathbb{Z}/_{p^n-1} & \text{si } * = 0 \\ \mathbb{Z}/_{p^n-1 \wedge n} & \text{sinon} \end{cases} \end{aligned}$$

En revenant à la figure 5.1, on déduit que $H^1(\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}, \mathbb{F}_{p^n}^\times) \cong E_2^{0,1} \cong \mathbb{Z}/_{p^n-1}$. ☐

Lemme 5.20.

a) $H^n(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \cong H^n(\boldsymbol{\mu}_{p^2-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p), \mathbb{F}_{p^2}^\times)$ *pour tout* $n \geq 0$.

b) $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \cong \mathbb{Z}/_{p^2-1}$.

Démonstration. a) Considérons la suite exacte courte

$$1 \longrightarrow S_2^1 \longrightarrow \mathbb{G}_2^1 \longrightarrow F \longrightarrow 1$$

D'après le lemme A.22 la cohomologie $H^*(S_2^1, \mathbb{F}_{p^2}^\times)$ est concentrée en degré 0. D'où

$$H^p(F, H^q(S_2^1, \mathbb{F}_{p^2}^\times)) = \begin{cases} 0 & \text{si } q > 0 \\ H^p(F, \mathbb{F}_{p^2}^\times) & \text{si } q = 0 \end{cases}$$

Ainsi, la suite spectrale de Lyndon-Hochschild-Serre : $H^p(F, H^q(S_2^1, \mathbb{F}_{p^2}^\times)) \Rightarrow H^{p+q}(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times)$ est dégénérée et

$$\forall p \geq 0 \quad H^p(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \cong H^p(F, \mathbb{F}_{p^2}^\times)$$

b) Il suffit d'utiliser l'isomorphisme précédent et la proposition précédente.

□

Théorème 5.21. *Le groupe de cohomologie $H^1(\mathbb{G}_2^1, U_1)$ est isomorphe à $\mathbb{Z}_p$ et est engendré par la classe de la dérivation $\tilde{t}_0$.*

Le démonstration du théorème précédent est l'objet de la section 5.5 *Cohomologie à coefficients dans U_1*. La démarche de la preuve du précédent théorème est basée sur celle de N. Karamanov dans [Kar10], où il y traite le cas $p = 3$.

Théorème 5.22 (Hopkins)**.** *Soit $p \geq 5$, alors*

$$\mathrm{Pic}_2^{\mathrm{alg},0} \cong H^1(\mathbb{G}_2, (E_2)_0^\times) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/(p^2-1)$$

Démonstration. D'après les résultats précédents, on a

$$H^1(\mathbb{G}_2^1, (E_2)_0^\times) \cong H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}[[u_1]]^\times) \cong H^1(\mathbb{G}_2^1, U_1) \times H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2-1}^\times) \cong \mathbb{Z}_p \times \mathbb{Z}/p^2 - 1$$

Donc, en revenant à la suite exacte courte du lemme 5.16, on a

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow H^1(\mathbb{G}_2, (E_2)_0^\times) \longrightarrow \mathbb{Z}_p \times \mathbb{Z}/(p^2-1) \longrightarrow 0$$

En utilisant le fait que $\mathbb{Z}_p$ est libre, on peut se ramener à une suite exacte de la forme suivante :

$$0 \longrightarrow \mathbb{Z}_p^2 \longrightarrow H^1(\mathbb{G}_2, (E_2)_0^\times) \longrightarrow \mathbb{Z}/(p^2-1) \longrightarrow 0$$

Ainsi, d'après le lemme suivant, on déduit le théorème. □

Lemme 5.23. *Soient A, B et C trois groupes abéliens topologiques formant une suite exacte courte : $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$. Supposons de plus que :*

i) C est un groupe abélien fini discret.

ii) La multiplication avec l'ordre de C induit un automorphisme de A.

Alors,

$$B \cong A \times C$$

Corollaire 5.24. *Avec les notations de la proposition 5.15, on a*

1. *La dérivation $\tilde{t}_0 : \mathbb{G}_2 \to (E_2)_0^\times$ induit un générateur du groupe $H^1(\mathbb{G}_2/\mathbb{G}_2^1, \mathbb{Z}_p^\times) \cong \mathbb{Z}_p$.*
2. *La dérivation $N : \mathbb{G}_2 \to (E_2)_0^\times$ induit un générateur du groupe $H^1(\mathbb{G}_2^1, \mathbb{U}_1(\mathbb{F}_{p^2}[[u_1]])) \cong \mathbb{Z}_p$.*
3. *La dérivation $\Omega : \mathbb{G}_2 \to (E_2)_0^\times$ correspondant à l'inclusion de $\boldsymbol{\mu}_{p^2-1}$ dans $\mathbb{W}^\times \subset (E_2)_0^\times$ induit un générateur du groupe $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}) \cong \mathbb{Z}/p^2 - 1$.*

De plus ces trois dérivations déterminent un isomorphisme entre $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/_{(p^2-1)}$ et le groupe $\mathrm{Pic}_2^{\mathrm{alg},0}$.

Démonstration. D'après tout ce qu'on vient de voir dans cette section, on déduit le diagramme suivant :

$$\begin{tikzcd}
 & & & 0 \\
 & & & H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \cong \mathbb{Z}/p^2-1 \arrow[u] \\
0 \arrow[r] & H^1(\mathbb{Z}_p, H^0(\mathbb{G}_2^1, (E_2)_0^\times)) \arrow[r, "\inf"] \arrow[d, phantom, "\cong"] & H^1(\mathbb{G}_2, (E_2)_0^\times) \arrow[r, "\mathrm{res}"] & H^0(\mathbb{Z}_p, H^1(\mathbb{G}_2^1, (E_2)_0^\times)) \arrow[r] \arrow[u] \arrow[d, phantom, "\cong"] & 0 \\
 & H^1(\mathbb{Z}_p, \mathbb{Z}_p^\times) \cong \mathbb{Z}_p & & H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}[[u_1]]^\times) & \\
 & & & H^1(\mathbb{G}_2^1, \mathbb{U}_1(\mathbb{F}_{p^2}[[u_1]])) \cong \mathbb{Z}_p \arrow[u] \\
 & & & 0 \arrow[u]
\end{tikzcd} \tag{5.1}$$

Les suites courtes horizontale et verticale sont exactes. Rappelons que $H^1(G, M)$ s'identifie avec le quotient du groupe des dérivations $\mathrm{Der}_G(M)$ par le groupe des dérivations intérieures. Ainsi, on note que le premier homomorphisme

$$H^1(\mathbb{Z}_p, H^0(\mathbb{G}_2^1, (E_2)_0^\times)) \xrightarrow{\inf} H^1(\mathbb{G}_2, (E_2)_0^\times)$$

envoie la classe d'une dérivation $d : \mathbb{G}_2/_{\mathbb{G}_2^1} \to ((E_2)_0^\times)^{\mathbb{G}_2^1}$ sur la classe de la dérivation

$$\inf([d]) = [\ \mathbb{G}_2 \twoheadrightarrow \mathbb{Z}_p \xrightarrow{d} ((E_2)_0^\times)^{\mathbb{G}_2^1} \longrightarrow (E_2)_0^\times\ ]$$

Le second homomorphisme

$$H^1(\mathbb{G}_2, (E_2)_0^\times) \xrightarrow{\mathrm{res}} H^0(\mathbb{G}_2^1, \mathbb{F}_p[[u_1]]^\times)$$

envoie la classe d'une dérivation $d : \mathbb{G}_2 \to (E_2)_0^\times$ sur la classe de la dérivation

$$\mathrm{res}([d]) = [\ \mathbb{G}_2^1 \longrightarrow \mathbb{G}_2 \xrightarrow{d} (E_2)_0^\times \xrightarrow{\mathrm{mod}(u_1)} \mathbb{F}_p[[u_1]]^\times\ ]$$

Enfin, d'après le théorème 5.21, la dérivation $\tilde{t}_0$ induit un générateur du groupe

$$H^1(\mathbb{G}_2^1, \mathbb{U}_1(\mathbb{F}_{p^2}[[u_1]])) \cong \mathbb{Z}_p.$$

En revenant à la définition de la dérivation N, on déduit qu'elle induit un générateur du groupe

$$H^1(\mathbb{Z}_p, H^0(\mathbb{G}_2^1, (E_2)_0^\times)) \cong H^1(\mathbb{Z}_p, \mathbb{Z}_p^\times) \cong \mathbb{Z}_p.$$

Pour finir, la dérivation Ω associée à l'action de F induit un générateur de $H^1(\mathbb{G}_2^1, \mathbb{F}_{p^2}^\times) \cong \mathbb{Z}/_{(p^2-1)}$. □

Nous allons encore redémontrer que $H^1(\mathbb{G}_2, (E_2)_0^\times)$ et le groupe des endomorphismes $\mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$-équivariants de l'anneau de Witt $\mathbb{W}$ sont isomorphes (isomorphisme (8.7) dans [Beh12]).

D'après la proposition 1.5, on déduit de l'homomorphisme $\mathbb{Z}_p[\![\mathbb{W}^\times]\!]$-linéaire $(E_2)_0^\times \twoheadrightarrow \mathbb{W}^\times$, qui envoie u_1 sur zéro, un homomorphisme en cohomologie $H^1(\mathbb{G}_2, (E_2)_0^\times) \to H^1(\mathbb{W}^\times, \mathbb{W}^\times)^{\mathrm{Gal}} \cong \mathrm{End}_c(\mathbb{W}^\times)^{\mathrm{Gal}}$.

Corollaire 5.25. *L'homomorphisme*

$$\begin{array}{ccc} H^1(\mathbb{G}_2, (E_2)_0^\times) & \longrightarrow & \mathrm{End}_c(\mathbb{W}^\times)^{\mathrm{Gal}} \\ [\mathbb{G}_2 \xrightarrow{d} (E_2)_0^\times] & & [\mathbb{W}^\times \hookrightarrow \mathbb{G}_2 \xrightarrow{d} (E_2)_0^\times \twoheadrightarrow (E_2)_0^\times/(u_1) \cong \mathbb{W}^\times] \end{array}$$

est un isomorphisme. De plus,
- *l'image de $[\mathbb{G}_2 \xrightarrow{t_0} (E_2)_0^\times]$ est l'endomorphisme identité de $\mathbb{W}^\times$.*
- *l'image de $[\mathbb{G}_2 \xrightarrow{\det} (E_2)_0^\times]$ est la norme de $\mathbb{W}^\times$ qui envoie x sur $x^{1+\sigma}$.*

Démonstration. Nous avons déjà vu que l'homomorphisme est bien défini. Montrons que c'est un isomorphisme. De l'isomorphisme

$$\mathbb{W} \times \boldsymbol{\mu}_{p^2-1} \to \mathbb{W}^\times$$

qui envoie (x, ζ) sur $\zeta \exp(px)$, on déduit, comme dans la preuve du théorème 8.1 de [Beh12], que

$$H^1(\mathbb{W}^\times, \mathbb{W}^\times)^{\mathrm{Gal}} \cong \mathrm{End}_c(\mathbb{W}^\times)^{\mathrm{Gal}} \cong \mathrm{End}_c(\mathbb{W})^{\mathrm{Gal}} \times \mathrm{End}_c(\mathbb{F}_{p^2}^\times)^{\mathrm{Gal}} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p^2-1)$$

De plus, le groupe profini $\mathrm{End}_c(\mathbb{W}^\times)^{\mathrm{Gal}}$ est engendré par l'application identité et la norme de $\mathbb{W}^\times$. Or, d'après la proposition 1.5, pour tout $a \in \mathbb{W}^\times$,

$$t_0(a) = (a_* u)u^{-1} \equiv a \mod (u_1)$$

et

$$\det(a) = \begin{vmatrix} a & 0 \\ 0 & a^\sigma \end{vmatrix} = a^{1+\sigma}$$

Ainsi, $[t_0]$ et $[\det]$ sont envoyés sur des générateurs et l'homomorphisme donné dans le corollaire est surjectif. D'autre part, nous avons vu que les groupes considérés dans le corollaire sont isomorphes à $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}/(p^2-1)$. Un endomorphisme continue surjectif de ce dernier groupe est nécessairement un isomorphisme, d'où le corollaire. □

5.3 Le cocycle associé à $\tilde{t}_0$

Dans cette section, nous allons établir un homomorphisme de complexes de chaînes de la résolution par des modules de permutations C_* (voir $(\star)$ page 34)

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0,$$

où $C_0 = C_3 = \mathbb{Z}_p \uparrow_F^{\mathbb{G}_2^1}$ et $C_1 = C_2 = \Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1}$, dans la résolution standard B_* de $\mathbb{Z}_p$ au-dessus du groupe $\mathbb{G}_2^1$. Ensuite, nous allons décrire l'image de la dérivation $t_0 : \mathbb{G}_2^1 \longrightarrow (E_2)_0^\times$ dans $\mathrm{Hom}_{\mathbb{G}_2^1}(C_1, (E_2)_0^\times)$.

Les premiers modules de la résolution standard sont

$$\begin{array}{rcl} B_0 & := & \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \\ B_1 & := & \mathbb{Z}_p[\![\mathbb{G}_2^1 \times \mathbb{G}_2^1]\!] \\ B_2 & := & \mathbb{Z}_p[\![\mathbb{G}_2^1 \times \mathbb{G}_2^1 \times \mathbb{G}_2^1]\!] \end{array}$$

et les premières différentielles associées sont caractérisées par les relations suivantes :

$$\begin{array}{rcl} \epsilon(g) & := & 1 \\ \delta_1(g,h) & := & g-h \\ \delta_2(f,g,h) & := & (g,h)-(f,h)+(f,g) \end{array}$$

Rappelons quelques notations et définitions du chapitre 2 concernant la première différentielle $\partial_1 : C_1 \to C_0$. On a fixé $\omega \in \mathbb{W}$ une racine p^2-1-ème de l'unité qui engendre $\boldsymbol{\mu}_{p^2-1}$ (le sous-groupe des relèvements de Teichmüller) et on note $\epsilon_\pm$ les éléments $\omega \pm \omega^p$. En particulier, (ϵ_+, ϵ_-) est une base de $\mathbb{W}$ en tant que $\mathbb{Z}_p$-module et qui diagonalise l'automorphisme de Frobenius. Les éléments a_i et b_i dans S_2^1 sont tels que pour tout entier i,

$$\begin{array}{rcll} a_0 & \equiv & 1+\epsilon_+ S & \mod (S^2) \\ b_0 & \equiv & 1+\epsilon_- S & \mod (S^2) \\ a_i & = & \omega^{-i} a_0 \omega^i & \\ b_i & = & \omega^{-i} b_0 \omega^i & \end{array}$$

On note

$$\lambda_i = \frac{\omega^{(1-p)i} + \omega^{(p-1)i}}{2} \quad \text{et} \quad \mu_i = \frac{(\omega^{(1-p)i} + \omega^{(p-1)i})\epsilon_+}{2\epsilon_-}.$$

Alors, d'après le théorème 2.10, on a

$$\partial_1((e_1)_+) = \frac{1}{p+1} \sum_{i=0}^{p} \lambda_i (a_i - 1) e_0 + \mu_i (b_i - 1) e_0$$

Lemme 5.26. *Il existe*

i) $f_0 : C_0 \longrightarrow \mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$ *l'homomorphisme* $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$*-linéaire tel que*

$$f_0(e_0) = \frac{1}{2(p^2-1)} \sum_{f \in F} f$$

ii) $f_1 : C_1 \longrightarrow \mathbb{Z}_p[\![\mathbb{G}_2^1 \times \mathbb{G}_2^1]\!]$ *l'homomorphisme* $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$*-linéaire tel que*

$$f_1((e_1)_+) = \frac{1}{2(p^2-1)(p+1)} \sum_{i=0}^{p} \sum_{f \in F} \lambda_i (a_i f, f) + \mu_i (b_i f, f)$$

De plus, on a le diagramme commutatif suivant :

$$\begin{tikzcd} C_1 \arrow[r, "\partial_1"] \arrow[d, "f_1"] & C_0 \arrow[r, "\epsilon"] \arrow[d, "f_0"] & \mathbb{Z}_p \arrow[r] \arrow[d, "="] & 0 \\ \mathbb{Z}_p[\![\mathbb{G}_2^1 \times \mathbb{G}_2^1]\!] \arrow[r, "\delta_1"] & \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \arrow[r, "\epsilon"] & \mathbb{Z}_p \arrow[r] & 0 \end{tikzcd}$$

D'après le lemme fondamental de l'algèbre homologique, on peut prolonger (f_0, f_1) en $f_* : C_* \longrightarrow B_*$ une équivalence homotopique.

Démonstration. Les propriétés concernant f_0 sont de l'ordre de la simple vérification. Pour l'homomorphisme f_1, revenons à la définition de $\partial_1 := \mathrm{tr}_F(d_1)\uparrow_F^{\mathbb{G}_2^1}$ où $d_1 : \Lambda_{1-p} \longrightarrow \mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}$ est défini de la manière suivante : $d_1(x) = \lambda(x)(a_0 - 1) + \mu(x)(b_0 - 1)$ où $x = \lambda(x)\epsilon_+ + \mu(x)\epsilon_-$. Donc

$$\begin{aligned}
\partial_1(1 \otimes x) &= \frac{1}{2(p^2-1)} \sum_{g \in F} g_*^{-1} d_1(g_* x) \\
&= \frac{1}{2(p^2-1)} \sum_{g \in F} g_*^{-1}\Big(\lambda(g_*x)(a_0 - 1) + \mu(g_*x)(b_0 - 1)\Big) \\
f_0\partial_1(1 \otimes x) &= \frac{1}{4(p^2-1)^2} \sum_{g \in F}\sum_{f \in F} g_*^{-1}\Big(\lambda(g_*x)(a_0 f - f) + \mu(g_*x)(b_0 f - f)\Big)
\end{aligned}$$

Or $\delta_1(g, h) = g - h$, d'où l'on pose

$$f_1(1 \otimes x) = \frac{1}{4(p^2-1)^2} \sum_{g \in F}\sum_{f \in F} g_*^{-1}\Big(\lambda(g_*x)(a_0 f, f) + \mu(g_*x)(b_0 f, f)\Big)$$

Cet homomorphisme restreint à Λ_{1-p} est $\mathbb{Z}_p[F]$-linéaire. On obtient par extension des scalaires un homomorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire tel que le diagramme donné dans le lemme commute. D'autre part, posons $N(F) = \frac{1}{2(p^2-1)} \sum_{f \in F} f$ dans $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$, alors, en munissant $\mathbb{G}_2^1 \times \mathbb{G}_2^1$ d'une action diagonale à droite, on a

$$\begin{aligned}
f_1(1 \otimes \epsilon_+) &= \left(\frac{1}{2(p^2-1)} \sum_{g \in F} \lambda(g_*\epsilon_+)(g^{-1}a_0, g^{-1}) + \mu(g_*x)(g^{-1}b_0, g^{-1})\right) N(F) \\
&= \left(\frac{1}{2(p^2-1)} \sum_{g \in F} \lambda(g_*\epsilon_+)(g^{-1}a_0 g, 1) + \mu(g_*x)(g^{-1}b_0 g, 1)\right) N(F)
\end{aligned}$$

Ainsi, en revenant à l'étude de l'homomorphisme ∂_1 (section 2.14), on déduit le lemme. □

Avant de pouvoir définir le cocycle qui nous intéresse pour le calcul de $H^1(\mathbb{G}_2^1, U_1)$, nous avons encore besoin d'énoncer quelques propriétés des dérivations.

Lemme 5.27. *Soient G un groupe profini et R un anneau profini. On munit $R[\![G \times G]\!]$ de la structure de $R[\![G]\!]$-module induite par l'action diagonale de G sur $G \times G$. Soit $d : G \longrightarrow R^\times$ une application continue, on lui associe l'unique homomorphisme de $R[\![G]\!]$-module $\tilde{d} : R[\![G \times G]\!] \longrightarrow R^\times$ tel que*

$$\forall\, x \in G : \tilde{d}(1, x) = d(x)$$

Alors,

1. *L'application d est une dérivation si et seulement si $\tilde{d}$ est un cocycle de $\mathrm{Hom}_{R[G]}(B_*, R^\times)$ de degré 1 où B_* est la résolution standard.*
2. *Si d est une dérivation alors,*
   a) *Quels que soient $x, y \in G$, on a $\tilde{d}(x, y) = x_* d(x^{-1}y)$.*
   b) *Quels que soient $x, y \in G$, on a $\tilde{d}(xy, y) = d(xy)^{-1}\, d(y)$.*

Démonstration. Les propriétés *1.* et *2.a)* sont standards. Supposons que $d : G \longrightarrow R^\times$ est une dérivation, alors $d(e) = 1$. Pour tout $x \in G$, on a $1 = d(xx^{-1}) = d(x)x_*d(x^{-1})$, c'est-à-dire $x_*d(x^{-1}) = d(x)^{-1}$. Soient $x, y \in G$, alors

$$\begin{aligned}
\tilde{d}(xy, y) &= (xy)_* d((xy)^{-1}y) \\
&= (xy)_*\Big(d((xy)^{-1})\,(xy)_*^{-1} d(y)\Big) \\
&= (xy)_* d((xy)^{-1})\, d(y) \\
&= d(xy)^{-1}\, d(y)
\end{aligned}$$

$\square$

Proposition-Définition 5.28. *On note τ la composée*

$$\mathbb{G}_2^1 \xrightarrow{\tilde{t}_0} \mathbb{U}_1(\,(E_2)_0\,) \twoheadrightarrow U_1 = \mathbb{U}_1(\,\mathbb{F}_{p^2}[[u_1]]\,)$$

De plus, l'homomorphisme induit $\tilde{\tau} f_1 : \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \longrightarrow U_1$ est un cocycle, au sens où il appartient au noyau de $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_2, U_1)$*, et on a*

$$\tilde{\tau} f_1(e_1) \equiv 1 - u_1 \mod (u_1^2)$$

Démonstration. De la proposition 5.15, on déduit que τ est bien une dérivation.
Il est donc immédiat, d'après le lemme 5.26, que $\tilde{\tau} f_1$ est un cocyle. Il nous reste à vérifier la congruence. Toujours d'après le lemme 5.26, on a

$$\begin{aligned}\tilde{\tau}\, f_1(\epsilon_+) &= \tilde{\tau}(\frac{1}{2(p^2-1)(p+1)} \sum_{i=0}^{p} \sum_{f \in F} \lambda_i(a_i f, f) + \mu_i(b_i f, f)) \\ &= \left(\prod_{i=0}^{p} \prod_{f \in F} \tilde{\tau}(a_i f, f)^{\lambda_i} \tilde{\tau}(b_i f, f)^{\mu_i} \right)^{\frac{1}{2(p^2-1)(p+1)}}\end{aligned}$$

D'après le lemme précédent, on a $\tilde{t}_0(a_i f, f) = t_0(a_i f)^{-1} t_0(f)$. Soit ω un générateur de $\boldsymbol{\mu}_{p^2-1} \subset F$ et σ l'automorphisme de Frobenius, alors ω et σ engendrent F. D'après la proposition 1.4, on a $t_0(a_i\sigma) = (a_i\sigma)_* u/u = t_0(a_i)$, $t_0(\sigma) = 1$ et

$$t_0(a_i\omega^j)^{-1} t_0(\omega^j) = \frac{u}{(a_i\omega^j)_* u} \frac{\omega^j_* u}{u} = \frac{\omega^j u}{\omega^j\,(a_{i*}u)} = t_0(a_i)^{-1}$$

De même, $t_0(a_i\omega^j\sigma)^{-1} t_0(\omega^j\sigma) = t_0(a_i)^{-1}$. Ces relations sont encore vraies pour τ et on déduit que

$$\tilde{\tau}\, f_1(\epsilon_+) \quad = \quad \left(\prod_{i=0}^{p} \tau(a_i)^{-\lambda_i} \tau(b_i)^{-\mu_i} \right)^{\frac{1}{p+1}}$$

D'après le corollaire 3.4 sur l'application t_0 et par définition des a_i, b_i éléments de S_2^1 (lemme 2.7), on a

$$\begin{aligned}\tau(a_i) &\equiv 1 + \omega^{(1-p)i} \epsilon_+ u_1 \mod (u_1^2) \\ \tau(b_i) &\equiv 1 - \omega^{(1-p)i} \epsilon_- u_1 \mod (u_1^2)\end{aligned}$$

Notons $U_2 = \{X \in U_1;\ X \equiv 1 \mod (u_1^2)\}$, l'application $\phi : U_1/_{U_2} \to \mathbb{F}_{p^2}$, qui envoie la classe d'un élément $1 + x_1 u_1 + \dots$ sur x_1, est un isomorphisme continue de pro-p-groupes. Rappelons aussi que $\lambda_i = \frac{1}{2}(\omega^{(1-p)i} + \omega^{(p-1)i})$ et $\mu_i = \frac{\epsilon_+}{2\epsilon_-}(\omega^{(1-p)i} - \omega^{(p-1)i})$ où ω est une racine p^2-1-ème de l'unité fixée. Ainsi l'image par le précédent isomorphisme ϕ de $\tilde{\tau}\, f_1(\epsilon_+)$ est

$$-\sum_{i=0}^{p} \lambda_i \omega^{(1-p)i} \epsilon_+ - \mu_i \omega^{(1-p)i} \epsilon_- \;=\; -\epsilon_+ \sum_{i=0}^{p} \left(\frac{1}{2}(\omega^{(1-p)2i} + 1) - \frac{1}{2}(\omega^{(1-p)2i} - 1) \right) \;=\; -\epsilon_+$$

D'où, la congruence concernant $\tilde{\tau} f_1(e_2) = \left(\tilde{\tau} f_1(\epsilon_+)\right)^{1/\epsilon_+}$. $\square$

5.4 Le sous-groupe U_1 de $\mathbb{F}_{p^2}[[u_1]]^\times$

Avant de passer au calcul de $H^1(\mathbb{G}_2^1, U_1)$, nous allons étudier les groupes U_1^F et $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$ qui apparaissent dans le complexe de chaînes $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_*, U_1)$.

Définition 5.29. Soit $n \geq 1$ un entier naturel, on pose

$$U_n = \{x \in \mathbb{F}_{p^2}[[u_1]];\ x \equiv 1 \mod (u_1^n)\,\}$$

L'action du groupe stabilisateur de Morava sur l'anneau de Lubin-Tate, induit une structure de $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module sur les U_n.

Remarque. Bien que les U_n soient munis d'une structure de module sur une algèbre, je vais garder la notation multiplicative. Ainsi l'analogue d'une combinaison linaire sera un produit de termes élevés à une certaine puissance.

Rappelons que d'après la proposition 1.4, l'action de $F = \boldsymbol{\mu}_{p^2-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$ sur U_1 est caractérisée par les relations suivantes :

$$\begin{aligned} \omega_* u_1 &= \omega^{p-1} u_1 \\ \sigma_* x u_1 &= x^p u_1 \end{aligned}$$

On notera aussi que U_1 est un pro-p-groupe abélien dont les sous-groupes U_n constituent une base de voisinages ouverts de l'élément neutre.

Proposition 5.30.

a) Le groupe $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\mathbb{Z}_p\!\uparrow_F^{\mathbb{G}_2^1}, U_1) \cong U_1^F$ *est isomorphe à* $\prod_{p\nmid k} \mathbb{Z}_p\ \{(1+u_1^{(p+1)k})\}$.

b) Soit $(b_k)_{p\nmid k}$ *une famille d'éléments de* U_1^F *tels que* $b_k \equiv 1 + u_1^{(p+1)k}$ *modulo* $U_{(p+1)k+1}$. *Cette famille d'éléments détermine un isomorphisme :*

$$U_1^F \ \cong \prod_{p\nmid k} \mathbb{Z}_p\ \{b_k\}$$

Démonstration. Soit $x = 1 + \sum_{i\geq 1} x_i u_1^i$ un élément de U_1^F, comme x est stable par l'action du groupe de Galois, il appartient en particulier à $1 + \mathbb{F}_p[[u_1]]u_1$. D'autre part, pour tout $1 \leq j < p^2-1$, $x = \omega_*^j x = 1 + \sum \omega^{(p-1)ji} x_i u_1^i$, d'où l'on déduit que $x \in U_1^F$ si et seulement si x s'écrit sous la forme $1 + \sum_{i>0} x_i u_1^{(p+1)i}$ avec $x_i \in \mathbb{F}_p$. Ensuite, un petit raisonnement par récurrence, montre que $x \in U_1^F$ peut aussi s'écrire de manière unique sous la forme suivante $\prod_{i\in\mathbb{N}} (1+u_1^{(p+1)i})^{x_i}$ où $0 \leq x_i < p$. En utilisant le fait que $\mathbb{Z}$ est un anneau factoriel, on déduit [1] que

$$\begin{aligned} x &= \prod_{n\geq 0} \prod_{p\nmid s} (1+u_1^{(p+1)s})^{x_{sp^n}\,p^n} \\ &= \prod_{p\nmid s} (1+u_1^s)^{\lambda_s} \end{aligned}$$

où $\lambda_s = \sum_{n\geq 0} x_{sp^n} p^n$ est un entier p-adique. D'où, l'on déduit le premier point.
Comme $U_1^F \subset \mathbb{F}_p[[u_1]]^\times$, la preuve du second point est immédiate. □

1. J'ai changé l'ordre dans un double produit et utilisé le fait que ça n'affecte pas la valeur du double produit.

Nous allons maintenant considérer $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}, U_1)$, qui d'après le lemme de Shapiro est isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$. Pour tout entier naturel k et pour $r = 1, p$, posons

$$\tilde{\zeta}_{r,k} : \Lambda_{1-p} \longrightarrow U_1$$

défini comme suit :

$$\tilde{\zeta}_{r,k}(x) \quad = \quad (1+\epsilon_+ u_1^{r+k(p+1)})^{\lambda(x)}(1+r'\epsilon_- u_1^{r+k(p+1)})^{\mu(x)}$$

où $r' = -1, 1$ si $r = 1, p$ respectivement. Malheureusement, cet homomorphisme n'est en général pas $\mathbb{Z}_p[F]$-linéaire car, par exemple pour $r = 1$ et $k = 0$,

$$\omega_*\tilde{\zeta}_{1,0}(1) = 1 + \omega^{p-1}u_1 \neq (1+\epsilon_+ u_1)^{\alpha_{1-p}}(1+\epsilon_- u_1)^{\beta_{1-p}} = \tilde{\zeta}_{1,0}(\omega_* 1)$$

où α_i et β_i désignent les entiers p-adiques tels que $\omega^i = \alpha_i\epsilon_+ + \beta_i\epsilon_-$. Cependant, en utilisant la transformation naturelle tr_F (moyenne sous l'action de F), nous allons obtenir des éléments de $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$.
Avant, de préciser ces éléments, un petit lemme sur la structure de $\mathbb{Z}_p[F]$-module de U_n/U_{2n}.

Lemme 5.31. *Soit $n \geq 1$.*

1. *Pour alléger les notations, notons $\bar{\Lambda}_{1-p}$ le $\mathbb{Z}_p[F]$-module $\Lambda_{1-p}/(p)$. Soit $1 \leq k \leq n$, alors l'application*

$$\begin{array}{ccc} U_n/U_{n+k} & \longrightarrow & \bar{\Lambda}_{(p-1)n} \oplus \ldots \oplus \bar{\Lambda}_{(p-1)(n+k-1)} \\ 1 + x_n u_1^n + \ldots + x_{n+k-1}u_1^{n+k-1} & \longmapsto & (x_n, \ldots, x_{n+k-1}) \end{array}$$

   est un isomorphisme $\mathbb{Z}_p[F]$-linéaire.

2. *L'application*

$$\begin{array}{ccc} \mathbb{Z}_p^n & \longrightarrow & U_n/U_{2n} \\ (\lambda_n, \ldots, \lambda_{2n-1}) & \longmapsto & \prod_{i=n}^{2n-1}(1+u_1^i)^{\lambda_i} \equiv 1 + \lambda_n u_1^n + \ldots + \lambda_{2n-1}u_1^{2n-1} \end{array}$$

   définit un homomorphisme de groupes.

Démonstration. Le second point est immédiat. Pour le premier point, on note que l'application vu comme application de U_n/U_{n+k} dans $\mathbb{F}_{p^2}u_1^n \oplus \ldots \mathbb{F}_{p^2}u_1^{n+k-1}$ définie bien un homomorphisme de groupes. De plus, d'après la proposition 1.4 et la définition 1.22 du module Λ_i, on a que $\mathbb{F}_{p^2}u_1^j \cong \Lambda_{(p-1)j}$, d'où l'on déduit que l'homomorphisme est $\mathbb{Z}_p[F]$-linéaire. □

Définition 5.32. Soient $r = 1, p$ et k un entier naturel, on pose

$$\begin{array}{rccc} \zeta_{r,k} : & \Lambda_{1-p} & \longrightarrow & U_1 \\ & x & \longmapsto & \left(\prod_{g\in F} g_*^{-1}\tilde{\zeta}_{r,k}(g_* x)\right)^{\frac{1}{|F|}} \end{array}$$

Pour tout $r = 1, p$ et tout $k \in \mathbb{N}$, du lemme précédent, on note que

$$\mathrm{gr}_{r+(p+1)k}\, U_1 = U_{r+(p+1)k}/U_{r+(p+1)k+1} \cong \begin{cases} \bar{\Lambda}_{p-1} & \text{si } k = 1 \\ \bar{\Lambda}_{1-p} & \text{si } k = p \end{cases}$$

Lemme 5.33. *L'homomorphisme* $\zeta_{r,k} : \Lambda_{1-p} \to U_1$ *est un homomorphisme* $\mathbb{Z}_p[F]$*-linéaire tel que*

$$\zeta_{r,k}(x) = \begin{cases} 1 + x^p\, u_1^{1+(p+1)k} \mod U_{2(r+(p+1)k)} & \textit{si } r = 1 \\ 1 + x\, u_1^{p+(p+1)k} \mod U_{2(r+(p+1)k)} & \textit{si } r = p \end{cases}$$

Remarque. En particulier, dans $(E_2)_0/(p)$, on a

$$\begin{aligned} \zeta_{1,k}(1) &\equiv 1 + u_1^{1+(p+1)k} \mod U_{1+(p+1)k+p+2} \quad \text{si } k > 0 \\ \zeta_{p,k}(1) &\equiv 1 + u_1^{p+(p+1)k} \mod U_{p+(p+1)k)+p+4} \quad \text{si } k > 0 \end{aligned}$$

Démonstration. Posons $n = r + (p+1)k$. D'après le lemme précédent et par définition de $\zeta_{r,k}$, on déduit que ce dernier homomorphisme se factorise de la manière suivante :

$$\begin{tikzcd} \Lambda_{1-p} \arrow[r, "\zeta_{r,k}"] \arrow[dr, "\mathrm{tr}_F(\zeta)"'] & U_{r+(p+1)k}/U_{2(r+(p+1)k)} \cong \bar{\Lambda}_{(p-1)n} \oplus \ldots \oplus \bar{\Lambda}_{(p-1)(2n-1)} \\ & \bar{\Lambda}_{(p-1)r} \cong \bar{\Lambda}_{\pm(1-p)} \arrow[u, hook] \end{tikzcd}$$

où

$$\zeta = \begin{cases} \Lambda_{1-p} \xrightarrow{\sigma} \Lambda_{p-1} \twoheadrightarrow \bar{\Lambda}_{p-1} & \text{si } r = 1 \\ \Lambda_{1-p} \twoheadrightarrow \bar{\Lambda}_{1-p} & \text{si } r = p \end{cases}$$

Comme ζ est $\mathbb{Z}_p[F]$-linéaire, $\mathrm{tr}_F(\zeta) = \zeta$ et on déduit le lemme. □

Proposition 5.34. *Soit* $\phi : \Lambda_{1-p} \longrightarrow U_1$ *un homomorphisme* $\mathbb{Z}_p[F]$*-linéaire non trivial. Alors, il existe* $r \in \{1, p\}$, $k \in \mathbb{N}$ *et* $0 \leq \lambda < p$ *tels que*

$$\phi \equiv \zeta_{r,k}^{\lambda} \mod U_{r+1+(p+1)k}$$

Démonstration. Soit $\phi : \Lambda_{1-p} \to U_1$ un homomorphisme $\mathbb{Z}_p[F]$-linéaire. Soit n le plus grand indice tel que l'image de ϕ soit incluse dans U_n. Alors, de même que pour le lemme précédent, on déduit la factorisation suivante :

$$\begin{tikzcd} \Lambda_{1-p} \arrow[r, "\phi"] \arrow[dr] & U_n/U_{2n} \cong \bar{\Lambda}_{(p-1)n} \oplus \ldots \oplus \bar{\Lambda}_{(p-1)(2n-1)} \\ & \bar{\Lambda}_{(p-1)n} \arrow[u, hook] \end{tikzcd}$$

D'après le corollaire 1.29, on déduit que

$$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, \bar{\Lambda}_{(1-p)n}) \cong \begin{cases} \mathbb{Z}/p\,\{\Lambda_{1-p} \xrightarrow{\sigma} \Lambda_{p-1} \twoheadrightarrow \bar{\Lambda}_{p-1}\} & \text{si } (p-1)n \equiv 1-p \ [p^2-1] \\ \mathbb{Z}/p\,\{\Lambda_{1-p} \twoheadrightarrow \bar{\Lambda}_{p-1}\} & \text{si } (p-1)n \equiv -(1-p) \ [p^2-1] \\ \{0\} & \text{sinon} \end{cases}$$

La condition $(p-1)n \equiv \pm(1-p)\ [p^2-1]$ équivaut à $n \equiv \pm 1\ [p+1]$. Ensuite, on conclut à l'aide du lemme précédent. □

Un premier corollaire obtenu par récurrence.

Corollaire 5.35. *Soit* $\phi \in \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$. *Il existe* $(a_i), (b_i)$ *deux suites à coefficients dans l'ensemble* $\{0, 1, \ldots, p-1\}$ *uniquement déterminées telles que*

$$\phi = \prod_{i \in \mathbb{N}} \zeta_{1,i}^{a_i}\, \zeta_{p,i}^{b_i}$$

Ce dernier résultat n'est pas satisfaisant car on voudrait bien comprendre $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$ en tant que $\mathbb{Z}_p$-module. Avant, comme, Λ_{1-p} est cyclique, l'homomorphisme

$$\mathrm{ev}_1 : \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1) \longrightarrow U_1$$

est injectif, ainsi nous allons identifier $\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1)$ avec son image dans U_1 :

Définition 5.36. On pose $U_1^\Lambda = \mathrm{Im}(\mathrm{ev}_1 : \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1) \to U_1) \subset 1 + \mathbb{F}_p[[u_1]]u_1$.

Soit s un entier non nul, notons que

$$\begin{aligned}
\zeta_{p,s-1}^p(1) &\equiv (1 + u_1^{-1+(p+1)s})^p \\
&\equiv 1 + u_1^{1+(p+1)(sp-1)} \\
&\equiv \zeta_{1,sp-1}(1) \mod U_{2+(p+1)(sp-1)} \\
\zeta_{1,s}^p(1) &\equiv (1 + u_1^{1+(p+1)s})^p \\
&\equiv 1 + u_1^{p+(p+1)sp} \\
&\equiv \zeta_{p,sp}(1) \mod U_{p+(p+1)sp+1}
\end{aligned}$$

On va identifier $\zeta_{r,s}$ avec $\zeta_{r,s}(1) \in U_1^\Lambda$.

Proposition 5.37. *Les éléments $\zeta_{1,s}$ où $s \not\equiv -1[p]$ et $\zeta_{p,s}$ où $s \not\equiv 0[p]$ déterminent un isomorphisme de pro-p-groupes :*

$$U_1^\Lambda \cong \prod_{s \not\equiv -1[p]} \mathbb{Z}_p \{\zeta_{1,s}\} \oplus \prod_{s \not\equiv 0[p]} \mathbb{Z}_p \{\zeta_{p,s}\}$$

Démonstration. Notons ϕ l'homomorphisme de la proposition allant du produit dans U_1^Λ. D'après le corollaire 5.35 et les identités précédentes, on déduit que les éléments considérés dans la proposition engendrent bien U_1^λ, c'est-à-dire que ϕ est surjectif.
Ensuite, notons que si $s \not\equiv -1[p]$, alors $1+(p+1)s \not\equiv 0[p]$ et que si $s \not\equiv 0[p]$ alors $p+(p+1)s \not\equiv 0[p]$ et on a

$$\zeta_{r,s} \equiv 1 + u_1^{r+(p+1)s} \mod U_{r+(p+1)s+1}$$

Ainsi, en revenant au besoin à la démonstration du point *a)* du lemme 5.30, on déduit que les éléments considérés dans la proposition sont linéairement indépendants dans U_1 et donc ϕ est injectif. □

5.5 Cohomologie à coefficients dans U_1

Nous allons utiliser la résolution projective de $\mathbb{Z}_p$ au-dessus de $\mathbb{G}_2^1$ pour le calcul de $H^1(\mathbb{G}_2^1, U_1)$. Rappelons qu'elle est de la forme suivante :

$$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} \mathbb{Z}_p \longrightarrow 0$$

où $C_3 = C_0 = \mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}$ et $C_2 = C_1 = \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$. Dans le chapitre précédent, nous avons noté ∂_i^* la différentielle induite $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_i, (E_2)_*/(p))$.

Définition 5.38. Soit $i = 0, 1, 2, 3$, on pose $\partial_i^\times = \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_i, U_1)$.

Comme les modules C_i sont cycliques, l'évaluation $\mathrm{ev}_{e_i} : \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_i, U_1) \to U_1$ est un isomorphisme sur son image. Ainsi, avec les notations de la section précédente, on a le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0,U_1) \arrow[r, "\partial_1^\times"] \arrow[d, "\mathrm{ev}_{e_0}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1,U_1) \arrow[r, "\partial_2^\times"] \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2,U_1) \arrow[d, "\mathrm{ev}_{e_2}"', "\cong"] \\
U_1^F \arrow[r] & U_1^\Lambda \arrow[r] & U_1^\Lambda
\end{tikzcd}$$

On identifie les homomorphismes $\partial_i^\times$ de la première ligne du diagramme précédent avec ceux de la seconde ligne. À l'aide du lemme 5.31, nous allons faire le lien entre $\partial_i^\times$ et ∂_i^*.

Lemme 5.39. *Soit s un entier naturel, alors,*

1. $\partial_1^\times(1+u_1^{(p+1)s}) \equiv 1 + \partial_1^*(u_1^{(p+1)s})$ *modulo* $U_{2(p+1)s}$.
2. *Soit $s \in \mathbb{N}$,*

$$\partial_1^\times(1+u_1^{(p+1)s}) \equiv 1 - su_1^{1+(p+1)s} + (\binom{-s}{p} + s)u_1^{p+(p+1)s} + (-s+R_{-s})u_1^{1+(p+1)(s+1)}$$

modulo $U_{\min(2(p+1)s,(p+1)s+p+4)}$ *où* $R_s := \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$.

Remarque. On notera que si $s \geq 2$, alors $2(p+1)s \geq (p+1)s + p + 4$.

Démonstration. 1. Soit s un entier naturel, alors l'image réciproque de $1+u_1^{(p+1)s}$ par l'homomorphisme d'évaluation ev_{e_0} est l'homomorphisme $\mathrm{ev}_{e_0}^{-1}(1+u_1^{(p+1)s}) : C_0 \to U_1$ qui envoie λe_0 sur $(1+u_1^{(p+1)s})^\lambda$. Ainsi, son image par $\partial_1^\times$ est

$$\begin{array}{ccccc}
C_1 & \xrightarrow{\partial_1} & C_0 & \longrightarrow & U_{(p+1)s} \\
(e_1)_+ & \longmapsto & ve_0 & \longmapsto & \left(\prod_{i=0}^{p+1} a_{i*}(1+u_1^{(p+1)s})^{\lambda_i}\, b_{i*}(1+u_1^{(p+1)s})^{\mu_i}\right)^{\frac{1}{p+1}}
\end{array}$$

ainsi, du lemme 5.31, on déduit que

$$\partial_1^\times(1+u_1^{(p+1)s}) \equiv 1 + \partial_1^*(u_1^{(p+1)s}) \mod (U_{2(p+1)s})$$

2. Du point précédent et du lemme 4.13, on déduit que, modulo $U_{\min(2(p+1)s,(p+1)s+p+4)}$,

$$\begin{aligned}
\partial_1^\times(1+u_1^{(p+1)s}) &\equiv 1 + \partial_1^*(u_1^{(p+1)s}) \\
&\equiv 1 - su_1^{1+(p+1)s} + (\binom{-s}{p} + s)u_1^{p+(p+1)s} + (-s+R_{-s})u_1^{1+(p+1)(s+1)}
\end{aligned}$$

où $R_s := \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$.

$\square$

Avant de chercher à déterminer des bases adaptées à l'homomorphisme $\partial_1^\times$, nous avons encore besoin de deux petits résultats techniques.

Lemme 5.40. *Soit $M = \prod_{\mathbb{N}} \mathbb{Z}_p \{e_i\}$ muni de la topologie produit.*

a) Soient α un automorphisme continue de M et β un endomorphisme continue de M, alors $\alpha + p\beta$ est un automorphisme continue de M.

b) Soient $a_{ij} \in \mathbb{Z}_p$, $(c_i) \in (p)^{\mathbb{N}}$ et $\phi : \mathbb{N}^* \to \mathbb{N}$ une application telle que, pour tout entier n,

i) $\phi(n) < n$,

ii) $\#\phi^{-1}\{n\} < \infty$.

Posons $b_0 = e_0$ et pour tout $i \in N^*$, posons

$$b_i = c_i e_{\phi(i)} + e_i + \sum_{j>i} a_{ij} e_j$$

L'endomorphisme de M qui envoie e_i sur b_i pour tout $i \in \mathbb{N}$ est bien défini et est un automorphisme continue. En d'autres termes, la famille $(b_i)_{i\in\mathbb{N}}$ détermine une base topologique de M.

Démonstration.

a) La série $\left(\sum_{n\geq 0} (p\alpha^{-1}\beta)^n\right)\alpha^{-1}$ converge dans l'anneau des endomorphismes de M et détermine un inverse de $\alpha + p\beta$.

b) Notons $\alpha : M \to M$ l'endomorphisme continue tel que $\alpha(e_i) = e_i + \sum_{j>i} a_{ij} e_j$. Il est immédiat que α est un automorphisme. Notons $\beta : M \to M$ l'endomorphisme continue qui envoie e_i sur $c_i e_{\phi(i)}$. Comme $\#\phi^{-1}\{n\} < \infty$, on déduit que l'endomorphisme β est bien défini. On conclut en appliquant le point précédent.

□

Rappelons que $C_1 = C_2 = \Lambda_{1-p} \uparrow_F^{\mathbb{G}_2^1}$. Afin de pouvoir distinguer $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, U_1)$ et $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, U_1)$, nous allons introduire les notations suivantes :

Définition 5.41. Pour tout $r = 1, p$ et tout $s \not\equiv -1[p]$ si $r = 1$ et $s \not\equiv 0[p]$ si $r = p$, on pose

a) $\eta_{r,s} = \zeta_{r,s}(e_1) \in U_1 \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, U_1)$.

b) $\gamma_{r,s} = \zeta_{r,s}(e_2) \in U_1 \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, U_1)$.

Le choix de la lettre grecque η, sorte d'équivalent [2] de la lettre h, est pour souligner l'analogie avec h_0, h_1 dans $\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p))$. Plus précisément, on a les identités $u_1 = v_1 h_1$ et $u_1^p = v_1^p h_0 v_2^{-1}$.

Définition 5.42. Pour tout entier naturel n, on pose

$$\mathcal{A}_n := \frac{(-p)^n - 1}{p+1} = -1 + p - \ldots + (-p)^{n-1}$$

Les éléments $\mathcal{A}_n$ vérifient la relation suivante :

$$\mathcal{A}_{n+1} = -p\mathcal{A}_n - 1$$

Encore un petit résultat d'arithmétique.

Lemme 5.43.

a) Quel que soit $t \in \mathbb{N}$, il existe un unique entier $n \geq 0$ et un unique entier $s \not\equiv (-1)^{n+1}\,[p]$ tels que $t = \mathcal{A}_n + sp^n$ et $s > (-1)^{n+1}$.

b) Pour tout entier s et tout entier n, on a

$$1 + (p+1)(\mathcal{A}_n + sp^n) \quad = \quad ((-1)^n + (p+1)s)p^n$$

2. `http://fr.wikipedia.org/wiki/H_(lettre)`

Remarque 5.44. *Notons que*

$$\mathcal{A}_0 = 0 \quad et \quad \mathcal{A}_1 = -1$$

et du premier point du lemme précédent, on déduit la partition suivante :

$$\mathbb{N} = \{\, s \in \mathbb{N};\ s \not\equiv -1[p]\,\} \bigcup \{\, \mathcal{A}_n + sp^n;\ s \not\equiv (-1)^{n+1}\,[p] \ \ et\ s > (-1)^{n+1} \ \ et\ n > 0\,\}$$

Démonstration. Soit t un entier naturel, alors il existe un unique entier r et un unique entier $n \geq 0$ tels que $(p+1)t + 1 = (r + (-1)^n)p^n$, $r \not\equiv (-1)^{n+1}\,[p]$ et $r > (-1)^{n+1}$. Cette équation modulo $(p+1)$ devient $1 \equiv (-1)^n r + 1\ [p+1]$, d'où $p+1$ divise r. Soit s le quotient de r par $p+1$, alors $s \equiv r \not\equiv (-1)^n\,[p]$ et

$$(p+1)t + 1 = (s(p+1) + (-1)^n)p^n \quad \Longleftrightarrow \quad t = \frac{(-p)^n - 1}{p+1} + sp^n$$

D'où le premier point du lemme. Le second point se vérifie facilement. □

Proposition-Définition 5.45.

1. *On pose*

$$\begin{cases} [1]_s := 1 + u_1^{(p+1)s} & où\ s \not\equiv 0, -1[p] \\ [1]_{\mathcal{A}_n + sp^n} := 1 + u_1^{(p+1)(\mathcal{A}_n + sp^n)} & où\ n = 1\ \ et\ s \not\equiv (-1)^{n+1}\,[p] \\ [1]_{\mathcal{A}_n + sp^n} := \left(1 + u_1^{(p+1)(\mathcal{A}_{n-2} + sp^{n-2})}\right)^{-p^2} \left(1 + u_1^{(p+1)(\mathcal{A}_n + sp^n)}\right) & où\ n \geq 2\ \ et\ s \not\equiv (-1)^{n+1}\,[p] \end{cases}$$

alors, les éléments $[1]_{p \nmid s}$ déterminent l'isomorphisme suivant

$$U_1^F \cong \prod_{s \not\equiv 0[p]} \mathbb{Z}_p\ \{[1]_s\}$$

2. *On a*

$$\partial_1^{\times}[1]_{\mathcal{A}_n + sp^n} \equiv \begin{cases} \eta_{1,s}^{-s} & où\ n = 0\ \ et\ s \not\equiv 0, -1[p]\ \ et\ s \geq 0 \\ \eta_{p,s-1}^{p}\ \eta_{p,sp-1}^{-s-1} & où\ n = 1\ \ et\ s \not\equiv 1, -1\ [p]\ \ et\ s > 1 \\ \eta_{p,s-1}^{p}\ \eta_{1,sp} & où\ n = 1\ \ et\ s \equiv -1\ [p]\ \ et\ s > 1 \\ \eta_{p,\mathcal{A}_n + sp^n}^{-2} & où\ n > 1\ \ et\ s \not\equiv (-1)^{n+1}\ [p]\ \ et\ s > (-1)^{n+1} \end{cases}$$

3. *On pose*

$$[\eta_1]_s := \partial_1^{\times}[1]_s \qquad où\ s \not\equiv 0, -1[p]\ \ et\ s \geq 0$$

$$[\eta_1]_{sp} := \partial_1^{\times}[1]_{sp-1} \qquad où\ s \equiv -1\ [p]\ \ et\ s \geq 1$$

$$[\eta_p]_{\mathcal{A}_n + sp^n} := \begin{cases} \partial_1^{\times}[1]_{\mathcal{A}_n + sp^n} & où\ n = 1\ \ et\ s \not\equiv 1, -1\ [p]\ \ et\ s > 1 \\ \partial_1^{\times}[1]_{\mathcal{A}_n + sp^n} & où\ n > 1\ \ et\ s \not\equiv (-1)^{n+1}\ [p]\ \ et\ s > (-1)^{n+1} \end{cases}$$

Si l'on ajoute les éléments

$$\begin{cases} \eta_{1,0} & \\ \eta_{1,sp} & où\ s \not\equiv -1\ [p]\ \ et\ s \geq 1 \\ \eta_{p,s} & où\ s \not\equiv 0, -1\ [p]\ \ et\ s \geq 1 \\ \eta_{p,\mathcal{A}_1 + sp} & où\ s \equiv -1\ [p]\ \ et\ s > 1 \end{cases} \tag{5.2}$$

alors, ils déterminent un isomorphisme entre $U_1^{\Lambda} \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, U_1)$ et leur produit au-dessus de $\mathbb{Z}_p$.

Remarques 5.46.

- *On notera que si l'on pose* $\eta_1 = u_1$ *et* $\eta_p = u_1^p$ *alors, dans la précédente proposition, nous avons respecté la convention suivante : Pour tout* $X \in \{1, \eta_0, \eta_p\}$ *et tout* $s \in \mathbb{N}$,

$$[X]_s \equiv 1 + X u_1^{(p+1)s} + \dots \quad \bmod U_1^p$$

Cette notation est sensiblement analogue à celle utilisée dans le théorème 4.2.

- *D'après le corollaire 4.4,* $H^0(\mathbb{G}_2^1, (E_2)_0/(p)) = \mathbb{F}_p(1)_0$. *Comme* $U_1 = \mathbb{U}_1((E_2)_0/(p))$, *on déduit que* $H^0(\mathbb{G}_2^1, U_1) = \mathbb{F}_p(1)_0 \cap U_1 \cong \{1\}$. *Chose qu'on peut aussi déduire à partir de la proposition précédente.*

Pour déterminer une base de U_1^F et une base de U_1^Λ adaptées à l'homomorphisme $\partial_1^\times$, la différence essentielle avec le calcul de $H^*(\mathbb{G}_2^1, (E_2)_*/(p))$ est que le fait de pouvoir élever à la puissance p les éléments par exemple $(1)_s$ avait permis de définir par récurrence la base $(1)_{sp^n}$. Maintenant, pour le calcul de $H^*(\mathbb{G}_2^1, U_1)$, le fait d'élever les éléments à la puissance p n'est rien d'autre que la multiplication avec le scalaire p.
D'autre part, le fait que $(1+u_1)^{-1}$ soit définie et que $(1+u_1^{-1})$ ne l'est pas, implique quelques subtilités dans les calculs... Relativement à la puissance p, on notera aussi que si $X \in U_1$ est tel que

$$X \equiv 1 + * u_1^{1+(p+1)s} + * u_1^{p+(p+1)s} \quad \bmod U_{(p+1)(s+1)}$$

alors

$$X^p \equiv 1 + * u_1^{p+(p+1)sp} + 0\, u_1^{1+(p+1)(sp+1)} \quad \bmod U_{(p+(p+1)s)p}$$

Démonstration. 1. En vue d'une application du point *b)* du lemme 5.40, posons, E_k le sous-ensemble

$$\{\, \mathcal{A}_n + sp^n;\ s \not\equiv (-1)^{n+1}\,[p] \text{ et } s \geq (-1)^{n+1} \text{ et } n \geq k \,\}$$

et $\phi : E_2 \longrightarrow E_0$, définie de la manière suivante :

$$\phi(\mathcal{A}_n + sp^n) = \mathcal{A}_{n-2} + sp^{n-2}$$

Par unicité de l'écriture $\mathcal{A}_n + sp^n$ (lemme 5.43), on déduit que la fonction ϕ est injective. D'où, d'après le lemme 5.40, les éléments $b_s = [1]_s$ déterminent un isomorphisme entre U_1^F et leur produit au-dessus de $\mathbb{Z}_p$.

2. Nous allons utiliser le lemme 5.39 et le lemme A.2,

   a) Soit $s \not\equiv 0, -1\,[p]$,

$$\partial_1^\times [1]_s = \partial_1^\times (1 + u_1^{(p+1)s}) \equiv \eta_{1,s}^{-s} \quad \bmod U_{2+(p+1)s}$$

   On note que $s = 1$ fait partie de ce cas de figure. Ainsi, dans les autres cas, on a $s > 1$ et dans la congruence 2. du lemme 5.39 le minimum de $2(p+1)s$ et $(p+1)s + p + 4$ est $(p+1)s + p + 4$.

   b) Supposons que $n > 0$. Distinguons plusieurs cas :

i) Si $n=1$ et $s \not\equiv 1,-1$ $[p]$ $(s>0)$: Notons que $\mathcal{A}_1=-1$. D'après le second point du lemme 5.39, on a modulo $U_{(p+1)(sp-1)+p+1}$,

$$\begin{aligned}
\partial_1^{\times}[1]_{sp-1} &= \partial_1^{\times}(1+u_1^{(p+1)(sp-1)}) \\
&\equiv 1+u_1^{1+(p+1)(sp-1)}+(\binom{-sp+1}{p}-1)u_1^{p+(p+1)(sp-1)} \\
&\equiv 1+u_1^{-p+(p+1)sp}+(\binom{-s}{1}\binom{1}{0}-1)u_1^{p+(p+1)(sp-1)} \\
&\equiv 1+u_1^{(p+(p+1)(s-1))p}-(s+1)u_1^{p+(p+1)(sp-1)}
\end{aligned} \tag{5.3}$$

D'autre part, d'après le lemme 5.33, on déduit facilement que

$$\eta_{p,s-1}^{p}\ \eta_{p,\mathcal{A}_1+sp}^{-s-1} \equiv 1+u_1^{(p+(p+1)(s-1))p}-(s+1)u_1^{p+(p+1)(sp-1)} \quad \mathrm{mod}\ U_{(p+1)sp}$$

D'où,

$$\partial_1^{\times}[1]_{\mathcal{A}_1+sp} \equiv \eta_{p,s-1}^{p}\ \eta_{p,\mathcal{A}_1+sp}^{-s-1} \quad \mathrm{mod}\ U_{(p+1)sp}$$

ii) Si $n=1$ et $s\equiv -1[p]$: Remarquons les identités suivantes

$$R_{-sp+1} = \frac{1}{2}(\binom{-sp+1}{p+2}-\binom{-sp}{2})(\epsilon_+^2-\epsilon_-^2)=0$$

(vraie dans $\mathbb{F}_p$). Ainsi, en réutilisant (5.3) et le lemme 5.39, on a modulo $U_{(p+1)(sp-1)+p+4}$,

$$\begin{aligned}
\partial_1^{\times}[1]_{sp-1} &\equiv 1+u_1^{(p+(p+1)(s-1))p}-(s+1)u_1^{p+(p+1)(sp-1)} \\
&\quad +(1+R_{-sp+1})u_1^{1+(p+1)sp} \\
&\equiv \eta_{p,s-1}^{p}\ \eta_{1,sp}
\end{aligned}$$

Pour la dernière congruence, nous avons encore une fois utilisé le lemme 5.33 sur $\eta_{r,s}$.

iii) Si $n>2$, $s\not\equiv(-1)^{n+1}$ $[p]$ et $s\geq(-1)^{n+1}$. Rappelons que

$$1+(p+1)(\mathcal{A}_n+sp^n) = ((-1)^n+(p+1)s)p^n$$

D'autre part, $\mathcal{A}_n=\frac{(-p)^n-1}{p+1}\equiv -1+p$ $[p^2]$. Ainsi, modulo $U_{(p+1)(\mathcal{A}_n+sp^n+p+1)}$,

$$\begin{aligned}
\partial_1^{\times}(1+u_1^{(p+1)(\mathcal{A}_n+sp^n)}) &\equiv 1+u_1^{1+(p+1)(\mathcal{A}_n+sp^n)}+(\binom{-\mathcal{A}_n-sp^n}{p}-1)u_1^{p+(p+1)(\mathcal{A}_n+sp^n)} \\
&\equiv 1+u_1^{((-1)^n+(p+1)s)p^n}+(\binom{1-p}{p}-1)u_1^{p+(p+1)(\mathcal{A}_n+sp^n)} \\
&\equiv \left(1+u_1^{(-1)^n+(p+1)s}\right)^{p^n}(1+u_1^{p+(p+1)(\mathcal{A}_{2n}+sp^{2n})})^{-2} \\
&\equiv \left(1+u_1^{(-1)^n+(p+1)s}\right)^{p^n}\eta_{p,\mathcal{A}_n+sp^n}^{-2} \quad \mathrm{mod}\ U_{(p+1)(\mathcal{A}_n+sp^n+1)}
\end{aligned}$$

Donc,

$$\partial_1^{\times}[1]_{\mathcal{A}_n+sp^n} \equiv \partial_1^{\times}\left(\left(1+u_1^{(p+1)(\mathcal{A}_{n-2}+sp^{n-2})}\right)^{-p^2}\left(1+u_1^{(p+1)(\mathcal{A}_n+sp^n)}\right)\right)\equiv \eta_{p,\mathcal{A}_n+sp^n}^{-2}$$

3. C'est une simple application du point *b)* du lemme 5.40.

□

Définition 5.47. Avec les notations de la proposition-définition 5.28, on pose $[\eta_1]_0 := \mathrm{ev}_1(\tilde{\tau} f_1)$ dans U_1.

Lemme 5.48. *L'élément $[\eta_1]_0$ est un cocycle, dans le sens où il appartient au noyau de $\partial_2^\times$: $U_1^\Lambda \longrightarrow U_1^\Lambda$. De plus, ce n'est pas un cobord et on a*

$$[\eta_1]_0 \equiv 1 - u_1 \mod U_2$$

Démonstration. D'après la proposition-définition 5.28, $[\eta_1]_0$ est bien un cocycle et vérifie la congruence donnée dans le lemme. Pour montrer que ce n'est pas un cobord, il suffit de voir qu'en l'ajoutant à l'image de la base de U_1^F qu'on a construit dans la proposition-définition précédente, on a encore une famille topologiquement libre. □

Afin de pouvoir calculer $H^1(\mathbb{G}_2^1, U_1)$, il nous faut encore comprendre les images par $\partial_2^\times$ des éléments (5.2). Comme pour le premier homomorphisme, on déduit du lemme 5.31 une relation entre $\partial_2^\times$ et ∂_2^*.

Lemme 5.49. *Soient $r = 1, p$ et $s \in \mathbb{N}$, alors*

$$\partial_2^\times(\eta_{r,(p+1)s}) \equiv 1 + \partial_2^*(\eta_{r,(p+1)s}) \mod U_{2(r+(p+1)s)}$$

Notons les identités suivantes : $u_1 = v_1 h_1$, $u_1^p = v_1^p h_0 v_2^{-1}$ et $u_1^{p+1} = v_1^{p+1} v_2^{-1}$. D'où l'on déduit que, dans $(E_2)_0/(p)$, on a

$$\begin{aligned} u_1^{1+(p+1)s} &= v_1^{1+(p+1)s} h_1 v_2^{-s} \\ u_1^{p+(p+1)s} &= v_1^{p+(p+1)s} h_0 v_2^{-s-1} \end{aligned}$$

L'inclusion $U_1 \subset (E_2)_*/(p)$ induit une inclusion de U_1^Λ dans $(E_2)_*^F/(p) \otimes (\mathbb{F}_p\, u^{1-p} \oplus \mathbb{F}_p\, u^{p-1})$.

Lemme 5.50.

1. *Soit $s > 0$. Modulo $U_{p+(p+1)(s+1)}$,*

$$\partial_2^\times(\eta_{1,sp}) \equiv 1 - u_1^{p+(p+1)sp} - \frac{s+1}{2} u_1^{1+(p+1)(sp+1)}$$

2. *Soit $s > 0$. Modulo $U_{1+(p+1)(s+2)}$,*

$$\partial_2^\times(\eta_{p,s}) \equiv 1 + \frac{s(s+1)}{2} u_1^{1+(p+1)(s+1)} + \frac{s}{2}(\binom{-s-1}{p} + s + 3) u_1^{p+(p+1)(s+1)}$$

3. *Soit $s > 0$. Modulo $U_{1+(p+1)sp}$,*

$$\partial_2^\times(\eta_{p,sp-2}) \equiv (1 + u_1^{p+(p+1)(s-1)})^p\, (1 + (s-1) u_1^{p+(p+1)(sp-1)})$$

4. *Soient $n > 1$, $s \not\equiv (-1)^{n+1}$ $[p]$ et $s \geq (-1)^{n+1}$. Modulo $U_{p+(p+1)(\mathcal{A}_n + sp^n + 1)}$,*

$$\partial_2^\times(\eta_{p,\mathcal{A}_n + sp^n - 1}) \equiv 1 + u_1^{1+(p+1)(\mathcal{A}_n + sp^n)} + u_1^{1+(p+1)(\mathcal{A}_n + sp^n + 1)}$$

5. *Soit $s \geq 1$. Modulo $U_{p+(p+1)(sp^2-p+1)}$,*

$$\partial_2^\times(\eta_{p,sp^2-p-1}) \equiv 1 - \frac{3}{2} u_1^{p+(p+1)(sp^2-p)} - \frac{1}{2} u_1^{1+(p+1)(sp^2-p+1)}$$

Démonstration. Nous allons utiliser la proposition 4.29 et le lemme précédent,

1. Comme $s > 0$, $2(1+(p+1)sp) > 1+(p+1)(sp+1)$. Ainsi, modulo $U_{p+(p+1)(sp+1)}$,

$$\begin{aligned}\partial_2^\times(\eta_{1,sp}) &\equiv 1+\partial_2^*(u_1^{1+(p+1)sp})\\ &\equiv 1+v_1^{1+(p+1)sp}\partial_2^*(h_1v_2^{-sp})\\ &\equiv 1-v_1^{p+(p+1)sp}g_0v_2^{-sp-1}-\frac{s+1}{2}v_1^{1+(p+1)(sp+1)}g_1v_2^{-sp-1}\\ &\equiv 1-u_1^{p+(p+1)sp}-\frac{s+1}{2}u_1^{1+(p+1)(sp+1)}\end{aligned}$$

2. Comme $2(p+(p+1)s) \geq p+2+(p+1)(s+1)$, on déduit que modulo $U_{1+(p+1)(s+2)}$

$$\begin{aligned}\partial_2^\times(\eta_{p,s}) &\equiv 1+\partial_2^*(u_1^{p+(p+1)s})\\ &\equiv 1+v_1^{p+(p+1)s}\partial_2^*(h_0v_2^{-s-1})\\ &\equiv 1+\frac{s(s+1)}{2}v_1^{2+p+(p+1)s}g_1v_2^{-s-1}+\frac{s}{2}(\binom{-s-1}{p}+s+3)v_1^{p+(p+1)(s+1)}g_0v_2^{-s-2}\\ &\equiv 1+\frac{s(s+1)}{2}u_1^{2+p+(p+1)s}+\frac{s}{2}(\binom{-s-1}{p}+s+3)u_1^{p+(p+1)(s+1)}\end{aligned}$$

3. On applique tout simplement le point précédent, ainsi modulo $U_{1+(p+1)sp}$,

$$\begin{aligned}\partial_2^\times(\eta_{p,sp-2}) &\equiv 1+u_1^{1+(p+1)(sp-1)}-(\binom{-sp+1}{p}+1)u_1^{p+(p+1)(sp-1)}\\ &\equiv 1+u_1^{(p+(p+1)(s-1))p}+(s-1)u_1^{p+(p+1)(sp-1)}\end{aligned}$$

4. D'après le lemme 5.43 et avec les hypothèses de la proposition, on déduit que $\mathcal{A}_n+tp^n-1 \geq 2$. De plus, comme $n > 1$, $\mathcal{A}_n+tp^n-1 = tp^n+(-p)^{n-1}+\ldots-p^2+p-2$ peut s'écrire sous la forme suivante : kp^2+p-2, ainsi, d'après le corollaire 4.30, on a modulo $U_{p+(p+1)(\mathcal{A}_n+sp^n+1)}$,

$$\begin{aligned}\partial_2^\times(\eta_{p,\mathcal{A}_n+sp^n-1}) &\equiv 1+\partial_2^*(v_1^{p+(p+1)(\mathcal{A}_n+sp^n-1)}\,h_0\,v_2^{-kp^2-p+1})\\ &\equiv 1+u_1^{1+(p+1)(\mathcal{A}_n+sp^n)}+u_1^{1+(p+1)(\mathcal{A}_n+sp^n+1)}\end{aligned}$$

5. Commençons par remarquer que si t est un entier naturel alors,

$$2(p+(p+1)t) > p+(p+1)(t+2) \iff (p+1)(t-2) > -p$$

Soit $s \geq 1$, alors $sp^2-p+1 > p+1 \geq 2$, d'où

$$\begin{aligned}\partial_2^\times(\eta_{p,sp^2-p-1}) &\equiv 1+\partial_2^*(v_1^{p+(p+1)(sp^2-p-1)}\,h_0\,v_2^{-sp^2+p}\\ &\equiv 1-\frac{3}{2}u_1^{p+(p+1)(sp^2-p)}-\frac{1}{2}u_1^{1+(p+1)(sp^2-p+1}\end{aligned}$$

□

Nous pouvons maintenant modifier la famille d'éléments (5.2), en une famille adaptée à l'homomorphisme $\partial_2^\times$.

Proposition-Définition 5.51. *Avec les notations de la définition 5.41, de la définition 5.47 et de la proposition-définition 5.45,*

1. *Posons*

$$\begin{cases}[\eta_1]_{sp} := \eta_{1,sp} & \text{où } s \not\equiv -1\ [p] \text{ et } s \geq 1\\ [\eta_p]_s := \eta_{p,s} & \text{où } s \not\equiv 0,-1,-2\ [p] \text{ et } s \geq 1\\ [\eta_p]_{\mathcal{A}_n+sp^n-1} := \eta_{p,\mathcal{A}_n+sp^n-1} & \text{où } n = 1,2 \text{ et } s \not\equiv (-1)^{n+1}\ [p] \text{ et } s > (-1)^{n+1}\\ [\eta_p]_{\mathcal{A}_n+sp^n-1} := \eta_{p,\mathcal{A}_n+sp^n-1}\ \eta_{p,\mathcal{A}_{n-2}+sp^{n-2}-1}^{-p^2} & \text{où } n > 2 \text{ et } s \not\equiv (-1)^{n+1}\ [p] \text{ et } s > (-1)^{n+1}\end{cases}$$

Alors, les éléments $[\eta_1]_s$ *pour* $s \in \mathbb{N}$ *et* $s \not\equiv -1\ [p]$ *et* $[\eta_p]_s$ *pour* $s \in \mathbb{N}$ *et* $s \not\equiv 0\ [p]$ *déterminent l'isomorphisme suivant :*

$$U_1^{\Lambda} \cong \prod_{s \not\equiv -1\,[p]} \mathbb{Z}_p \,\{[\eta_1]_s\} \oplus \prod_{s \not\equiv 0\,[p]} \mathbb{Z}_p \,\{[\eta_p]_s\}$$

2. *On a*

$$\begin{aligned}
\partial_2^{\times}[\eta_1]_{sp} &\equiv \gamma_{1,s}^{-p}\,\gamma_{1,sp+1}^{-(s+1)/2} && \text{où } s \not\equiv -1\ [p] \text{ et } s \geq 1\\
\partial_2^{\times}[\eta_p]_{s} &\equiv \gamma_{1,s+1}^{s(s+1)/2} && \text{où } s \not\equiv 0,-1,-2\ [p] \text{ et } s \geq 1\\
\partial_2^{\times}[\eta_p]_{\mathcal{A}_n+sp^n-1} &\equiv \begin{cases} \gamma_{p,s-1}^{p}\,\gamma_{p,sp-1}^{s-1} \\ \gamma_{1,s-1}^{p^2}\,\gamma_{1,\mathcal{A}_2+sp^2+1} \\ \gamma_{1,\mathcal{A}_n+sp^n+1} \end{cases} && \begin{aligned} &\text{où } n=1 \text{ et } s \not\equiv 1\ [p] \text{ et } s>1\\ &\text{où } n=2 \text{ et } s \not\equiv -1\ [p] \text{ et } s>-1\\ &\text{où } n>2 \text{ et } s \not\equiv (-1)^{n+1}\ [p] \text{ et } s>(-1)^{n+1}\end{aligned}\\
\partial_2^{\times}[\eta_p]_{\mathcal{A}_1+sp} &\equiv \gamma_{1,s}^{-3p/2}\,\gamma_{1,sp+1}^{-1/2} && \text{où } s \equiv -1\,[p] \text{ et } s>1
\end{aligned}$$

3. *On pose*

$$\begin{aligned}
[\gamma_1]_{sp+1} &:= \partial_2^{\times}[\eta_1]_{sp} && \text{où } s \not\equiv -1\ [p]\\
[\gamma_1]_{sp+1} &:= \partial_2^{\times}[\eta_p]_{\mathcal{A}_1+sp} && \text{où } s \equiv -1\\
[\gamma_1]_{s} &:= \partial_2^{\times}[\eta_p]_{s-1} && \text{où } s \not\equiv 1,0,-1\ [p]\\
[\gamma_p]_{sp-1} &:= \partial_2^{\times}[\eta_p]_{\mathcal{A}_1+sp-1} && \text{où } s \not\equiv 1\ [p]\\
[\gamma_1]_{\mathcal{A}_n+sp^n+1} &:= \partial_2^{\times}[\eta_p]_{\mathcal{A}_n+sp^n-1} && \text{où } n \geq 2 \text{ et } s \not\equiv (-1)^{n+1}\ [p]
\end{aligned}$$

Ces éléments forment une famille libre de $U_1^{\Lambda} \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, U_1)$.

Démonstration. 1. Pour montrer que les éléments $[1]_{\mathcal{A}_n+sp^n-1}$ où $n > 2$ et $s \not\equiv (-1)^n[p]$ sont linéairement indépendants, on utilise le point *b*) du lemme 5.40 avec l'application $\phi(\mathcal{A}_n + sp^n - 1) = \mathcal{A}_{n-2} + sp^{n-2} - 1$ qui est injective d'après le lemme 5.43. Ainsi, on déduit le premier point de la proposition.

2. Nous allons utiliser dans l'ordre les congruences du lemme 5.50.

a) Soit $s \not\equiv -1\,[p]$,

$$\partial_2^{\times}(\eta_{1,ps}) \quad\equiv\quad (1-u_1^{1+(p+1)s})^p\left(1-\frac{s+1}{2}u_1^{1+(p+1)(sp+1)}\right) \;\equiv\; \gamma_{1,s}^{-p}\,\gamma_{1,sp+1}^{-\frac{s+1}{2}}$$

b) Soit $s \not\equiv 0,-1,-2\,[p]$:

$$\partial_2^{*}(\gamma_{p,s}) \quad\equiv\quad (1+\frac{s(s+1)}{2}u_1^{1+(p+1)(s+1)}) \;\equiv\; \gamma_{1,s+1}^{s(s+1)/2}$$

c) Notons que

$$\{\mathcal{A}_n + sp^n - 1;\ s \not\equiv (-1)^{n+1},\ s \geq (-1)^{n+1},\ n>0\} = \{t \equiv -2\,[p]\}$$

Distinguons plusieurs cas :

i) Soit $s \not\equiv 1\,[p]$, alors

$$\partial_2^{\times}[\eta_p]_{\mathcal{A}_1+sp-1} \quad\equiv\quad \partial_2^{\times}[\eta_p]_{sp-2} \;\equiv\; (1+u_1^{p+(p+1)(s-1)})^p\,(1+(s-1)u_1^{p+(p+1)(sp-1)})$$

ii) Soient $n \geq 2$ et $s \not\equiv (-1)^{n+1}\,[p]$, alors

$$\begin{aligned}
\partial_2^{\times}(\eta_{p,\mathcal{A}_n+sp^n-1}) &\equiv (1+u_1^{1+(p+1)(\mathcal{A}_n+sp^n)})\,(1+u_1^{1+(p+1)(\mathcal{A}_n+sp^n+1)})\\
&\equiv (1+u_1^{(-1)^n+(p+1)s})^{p^n}\,(1+u_1^{1+(p+1)(\mathcal{A}_n+sp^n+1)})\\
&\equiv \begin{cases} \gamma_{1,s}^{p^{2k}}\,\gamma_{1,\mathcal{A}_{2k}+sp^{2k}+1} & \text{où } s \not\equiv -1\,[p]\\ \gamma_{p,s-1}^{p^{2k+1}}\,\gamma_{1,\mathcal{A}_{2k+1}+sp^{2k+1}+1} & \text{où } s \not\equiv 1\,[p]\end{cases}
\end{aligned}$$

D'où, les congruences pour les cas $n = 2$ et $n > 2$.

d) Soit $s \equiv -1[p]$, alors $\mathcal{A}_1 + sp = tp^2 - p - 1$ pour un certain entier p. Ainsi,

$$\partial_2^\times[\eta_p]_{\mathcal{A}_1+sp} \equiv \partial_2^\times[\eta_p]_{tp^2-p-1} \quad \equiv \quad \gamma_{1,tp-1}^{-3p/2}\,\gamma_{1,tp^2-p+1}^{-1/2}$$

3. Rappelons que $\mathcal{A}_n = \frac{(-p)^n-1}{p+1} \equiv -1\,[p]$ pour tout $n > 0$. Notons que les ensembles

$$\{sp+1 :\ s > 0\},\ \{s :\ s \not\equiv 1, 0, -1\,[p]\},\ \{sp-1 :\ s \not\equiv 1\,[p]\}$$
$$\text{et } \{\mathcal{A}_n + sp^n + 1 :\ s \not\equiv (-1)^{n+1}\,[p] \text{ et } n \geq 2\}$$

sont disjoints. Ainsi, une dernière application des lemmes 5.43 et 5.40 permet de déduire que les éléments $[\gamma_1]_*$ et $[\gamma_p]_*$, définis dans la proposition-définition, sont linéairement indépendants.

□

Nous pouvons maintenant déterminer le groupe de cohomologie $H^1(\mathbb{G}_2^1, U_1)$.

Démonstration du théorème 5.21. D'après les propositions-définitions 5.45 et 5.51 et le lemme 5.48, on a le diagramme suivant :

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0, U_1) \arrow[r, "\partial_1^\times"] \arrow[d, "\mathrm{ev}_{e_0}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, U_1) \arrow[r, "\partial_2^\times"] \arrow[d, "\mathrm{ev}_{e_1}"', "\cong"] & \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, U_1) \arrow[d, "\mathrm{ev}_{e_2}"', "\cong"] \\
U_1^F \arrow[r, "\partial_1^\times"] \arrow[d, "\cong"] & U_1^\Lambda \arrow[r, "\partial_2^\times"] \arrow[d, "\cong"] & U_1^\Lambda \arrow[d, "\cong"] \\
\prod_{s\not\equiv 0[p]} \mathbb{Z}_p\{[1]_s\} \arrow[r] & \begin{array}{c} \mathbb{Z}_p\,\{[\eta_1]_0\} \\ \oplus \\ \prod\limits_{s\not\equiv -1[p] \text{ et } s\neq 0} \mathbb{Z}_p\,\{[\eta_1]_s\} \\ \oplus \\ \prod_{s\not\equiv 0[p]} \mathbb{Z}_p\,\{[\eta_p]_s\} \end{array} \arrow[r] & \begin{array}{c} \prod_{s\not\equiv -1[p]} \mathbb{Z}_p\,\{[\gamma_1]_s\} \\ \oplus \\ \prod_{s\not\equiv 0[p]} \mathbb{Z}_p\,\{[\gamma_p]_s\} \end{array}
\end{tikzcd}$$

et

$$\partial_1^\times[1]_{\mathcal{A}_n+sp^n} = \begin{cases} [\eta_1]_s & \text{où } n = 0 \text{ et } s \not\equiv 0, -1[p] \text{ et } s \geq 0 \\ [\eta_p]_{sp-1} & \text{où } n = 1 \text{ et } s \not\equiv 1, -1\,[p] \text{ et } s > 1 \\ [\eta_1]_{sp} & \text{où } n = 1 \text{ et } s \equiv -1\,[p] \text{ et } s > 1 \\ [\eta_p]_{\mathcal{A}_n+sp^n} & \text{où } n > 1 \text{ et } s \not\equiv (-1)^{n+1}\,[p] \text{ et } s > (-1)^{n+1} \end{cases}$$

$$\begin{aligned}
\partial_2^\times[\eta_1]_0 &= 0 & & \\
\partial_2^\times[\eta_1]_{sp} &= [\gamma_1]_{sp+1} & & \text{où } s \not\equiv -1\,[p] \text{ et } s \geq 1 \\
\partial_2^\times[\eta_p]_{\mathcal{A}_1+sp} &= [\gamma_1]_{sp+1} & & \text{où } s \equiv 1\,[p] \text{ et } s > 1 \\
\partial_2^\times[\eta_p]_s &= [\gamma_1]_{s+1} & & \text{où } s \not\equiv 0, -1, -2\,[p] \text{ et } s \geq 1
\end{aligned}$$

$$\partial_2^\times[\eta_p]_{\mathcal{A}_n+sp^n-1} = \begin{cases} [\gamma_p]_{\mathcal{A}_1+sp} & \text{où } n = 1 \text{ et } s \not\equiv 1\,[p] \text{ et } s > 1 \\ [\gamma_1]_{\mathcal{A}_n+sp^n+1} & \text{où } n \geq 2 \text{ et } s \not\equiv (-1)^{n+1}\,[p] \text{ et } s > (-1)^{n+1} \end{cases}$$

D'où le théorème. $\square$

A.1 Interpolation de la fonction puissance

Dans le chapitre III, le paragraphe (I.I.6) *La fonction puissance* de [Laz65], M. Lazard définit l'expression $(x-1)^{\lambda}$ pour un entier p-adique λ et x un élément d'une $\mathbb{Z}_p$-algèbre qui en tant que $\mathbb{Z}_p$-module est complet et dont les puissances $(x-1)^n$ tendent vers zéro. Précisons :

Dans l'anneau $\mathbb{Q}[[t]]$, des séries formelles en t et à coefficients rationnels, on a

$$\frac{1}{1-t} = 1 + t + t^2 + \ldots \qquad \text{et} \qquad \frac{d^n}{dt^n}\frac{1}{1-t} = \frac{n!}{(1-t)^{n+1}}$$

D'où

$$\begin{aligned}
(1-t)^{-n} &= (1+t+t^2+\ldots)^n \\
&= \frac{1}{(n-1)!}\frac{d^{n-1}}{dt^{n-1}}\frac{1}{1-t} = \sum_{k\geq 0}\frac{1}{(n-1)!}\frac{d^{n-1}}{dt^{n-1}}t^k \\
&= \sum_{k\geq n-1}\frac{k(k-1)\ldots(k-n+2)}{(n-1)!}t^{k-n+1} = \sum_{k\geq n-1}\binom{k}{n-1}t^{k-n+1} \\
&= \sum_{k\geq 0}\binom{k+n-1}{n-1}t^k = \sum_{k\geq 0}\binom{k+n-1}{k}t^k \\
&= \sum_{k\geq 0}\binom{-n}{k}(-t)^k
\end{aligned}$$

En fait, comme $1+t+t^2+\ldots$ est un inversible dans $\mathbb{Z}[[t]]$. On déduit que dans $\mathbb{Z}[[t]]$, pour tout entier relatif n, on a la formule du Binôme :

$$(1-t)^n = \sum_{k\geq 0}\binom{n}{k}(-t)^k \tag{A.1}$$

Proposition A.1. *Soient A un anneau commutatif et I un idéal de A tels que A soit complet pour la filtration I-adique. Soit x un élément de l'anneau A tel que $x-1$ appartient à l'idéal I. Alors x est une unité et la fonction puissance associée admet un développement en série de Taylor, i.e : quel que soit l'entier relatif n, on a :*

$$x^n = \sum_{k\geq 0}\binom{n}{k}(x-1)^k$$

Démonstration. Par hypothèse, l'homomorphisme $\phi : \mathbb{Z}[[t]] \to A$ qui envoie t sur $1-x$ est bien définie et est continue. Ainsi, de l'identité (A.1), on déduit que $x = \phi(1-t)$ est une unité et

$$x^n = \phi(1-t)^n = \phi(\sum_{k\geq 0}\binom{n}{k}(-t)^k) = \sum_{k\geq 0}\binom{n}{k}(x-1)^k$$

□

Dans cette thèse, on utilisera essentiellement le résultat précédent dans l'anneau $(E_2)_0$, qui est complet pour la filtration (u_1)-adique. Quel que soit x dans $(E_2)_*$, la suite des puissances $(xu_1)^k$ converge vers zéro et donc l'expression $(1+xu_1)^k$ est bien définie pour tout entier relatif k et admet un développement en série de Taylor :

$$(1+xu_1)^n = \sum_{k\geq 0} \binom{n}{k} (xu_1)^k$$

Corollaire A.2. *Soient n un entier relatif et m un entier naturel, vus comme des entiers p-adiques. On se donne $n = \sum_i n_i p^i$ et $m = \sum_i m_i p^i$ où $0 \leq n_i, m_i \leq p-1$. Alors*

$$\binom{n}{m} = \prod_{i>0} \binom{n_i}{m_i} \mod (p)$$

En particulier, quel que soit $0 \leq m \leq p-1$, le coefficient binomial $\binom{n}{m}$ modulo (p) ne dépend que de n modulo (p). Plus généralement,

$$\forall\, k \in \mathbb{N} \;\; \forall n, n' \in \mathbb{N} \;\; \forall\, 0 \leq m < p^k - 1 : \quad n \equiv n' \; [p^k] \Rightarrow \binom{n}{m} \equiv \binom{n'}{m} \; [p]$$

Démonstration. D'après la proposition, dans $\mathbb{F}_p[[x]]$, on a $\sum \binom{n}{i} x^i = (1+x)^n = \prod (1+x^{p^i})^{n_i}$. En comparant les coefficients des séries formelles, on déduit les congruences du corollaire. □

Soit t un générateur du groupe $U_1 = 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$, alors l'homomorphisme $\mathbb{Z}_p \to U_1$ qui envoie λ sur t^λ est un isomorphe (si $p = 2$, $U_1 = 1 + 4\mathbb{Z}_2$). Considérons l'homomorphisme de pro-p-groupes continue

$$\rho : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p[\![U_1]\!]$$

tel que pour tout entier p-adique λ, $\rho(\lambda) = t^\lambda$. Du théorème de Mahler ([Laz65], III.1.2.4) appliqué à la fonction ρ, nous allons déduire la proposition suivante.

Proposition A.3 (Interpolation de la puissance p-adique)**.** *Soit t un générateur de $\mathbb{Z}_p$ vu comme pro-p-groupe. Quel que soit le nombre p-adique λ, on a dans $\mathbb{Z}_p[\![U_1]\!]$*

$$t^\lambda = \sum_{n\geq 0} \binom{\lambda}{n} (t-e)^n$$

Remarques.

- On déduit plus généralement que, quel que soit g dans un pro-p-groupe G, dans $\mathbb{Z}_p[\![G]\!]$, on a
$$g^\lambda = \sum_{n\geq 0} \binom{\lambda}{n} (g-e)^n$$
Pour ce faire il suffit de considérer l'application continue : $\mathbb{Z}_p[\![U_1]\!] \to \mathbb{Z}_p[\![G]\!]$, qui envoie t sur g.
- Cette formule d'interpolation est utile dans la preuve de la proposition 2.26 pour l'égalité (2.6) et dans la preuve du lemme 2.37.

Démonstration. D'après le théorème de Mahler ([Laz65], III.1.2.4) appliqué à la fonction ρ, quel que soit le nombre p-adique λ,

$$t^\lambda = \sum_{n\in\mathbb{N}} \binom{\lambda}{n} \Delta^n \rho(0)$$

Calculons la différence d'ordre n de ρ à l'origine :

$$\begin{aligned}\Delta^n\rho(0) &= (T-\mathrm{Id})^n\rho(0)\\ &= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}T^i\rho(0)\\ &= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}t^i\\ &= (t-e)^n\end{aligned}$$

où T est l'opérateur de translation sur les fonctions $Tf(\lambda) = f(\lambda+1)$. □

A.2 Algèbres des pro-p-groupes et le lemme de Nakayama

Commençons par citer textuellement deux théorèmes de [Laz65] :

Théorème A.4 ([Laz65], II.2.1.6)**.** *Soient G un p-groupe fini, et $A = \mathbb{Z}_p[G]$ son algèbre à coefficients entiers p-adiques. Notons I l'idéal d'augmentation de A, et $R = I + (p)$ l'idéal engendré par I et p. Alors A est un anneau local, dont le radical est R. La topologie R-adique de A et sa topologie de $\mathbb{Z}_p$-module libre de rang fini coïncident. L'anneau local A est compact.*

Théorème A.5 ([Laz65], II.2.2.2)**.** *Soit G un pro-p-groupe. Son algèbre complétée $\mathbb{Z}_p[\![G]\!]$ est un anneau local et une $\mathbb{Z}_p$-algèbre topologique compacte. Les idéaux ouverts de $\mathbb{Z}_p[\![G]\!]$ constituent un système fondamentale de voisinage de zéro. Si R désigne le radical de Jacobson de $\mathbb{Z}_p[\![G]\!]$, la topologie R-adique est plus fine que la topologie de $\mathbb{Z}_p[\![G]\!]$, ce qui signifie que tout voisinage de zéro contient R^n à partir d'une certaine valeur de $n \in \mathbb{N}$. Si G est de type fini la topologie de $\mathbb{Z}_p[\![G]\!]$ est sa topologie R-adique. Enfin il existe une injection canonique de $\mathbb{Z}_p[G]$ sur une sous-algèbre dense de $\mathbb{Z}_p[\![G]\!]$ (ce qui justifie le nom d'algèbre de groupe complétée), et la restriction de cette injection à G est un homéomorphisme de G sur son image.*

Remarque. Réciproquement, d'après la proposition 7.5.3 de [Wil98], si R est un anneau commutatif profini et G un groupe profini tels que $R[\![G]\!]$ est un anneau local profini, alors R et G sont pro-p pour un certain premier p.

Avant de passer à une première application. Nous allons donner une version profini du lemme de Nakayama.

Théorème A.6 (Lemme de Nakayama [BH97])**.** *Soient A un anneau profini et I un idéal à gauche de A tels que $I^n \to 0$. Soit M un A-module profini, alors $IM = M$ implique $M = 0$.*

Remarque. Se théorème s'applique en particulier aux pro-p-groupes abéliens avec comme anneau de base l'anneau des entiers p-adiques et I l'idéal engendré par p.

Démonstration. Soit U un voisinage ouvert de 0 dans M, comme M est profini, on peut choisir U tel que U soit un sous-A-module. Soit $x \in M$, alors par continuité du produit dans M et par hypothèse sur l'idéal I, il existe $U_x \subseteq M$ voisinage ouvert de x et $n >> 0$ un entier naturel tel que

$$I^n \times U_x := \{\, av;\ a \in I^n \text{ et } v \in U_x \,\} \subseteq U$$

Les U_x forment un recouvrement du compact M, ainsi on peut en extraire un recouvrement finie : $U_1, \ldots, U_m$. D'autre part, comme $IM = M$, on a $I^nM = M$ pour tout entier n. Soit n assez grand tel que $I^n \times U_i \subseteq U$ pour $i = 1, \ldots, n$. Maintenant comme U est un sous-A-module, on déduit que $M = I^nM \subset U$. Donc le seul voisinage ouvert de 0 dans l'espace topologique séparé M est M lui-même. C'est-à-dire $M = \{0\}$. □

Comme pour le lemme de Nakayama classique, on déduit le corollaire suivant.

Corollaire A.7. *Soient A un anneau profini et I un idéal à gauche de A tels que $I^n \to 0$. Soit M un A-module profini tel que $M/_{IM}$ est un $A/_I$-module de type fini, alors M est de type fini.*

Démonstration. Soient $x_1, \ldots, x_n$ les relevés dans M d'une famille génératrice de $M/_{IM}$. Notons N le sous-A-module engendré par les $x_1, \ldots, x_n$. En particulier N est profini. D'autre part, $I(M/_N) = (IM + N)/_N$ et par construction la composée $N \to M \to M/_{IM}$ est surjective. Donc $N + IM = M$ et $I(M/_N) = M/_N$. Donc d'après le théorème $M/_N = \{0\}$ et $M = N$. □

Donnons un cas particulier du théorème précédent.

Corollaire A.8 (lemme de Nakayama)**.** *Soient G un pro-p-groupe de type fini et M un $\mathbb{Z}_p[\![G]\!]$-module profini. Si $\mathrm{Tor}_0^{\mathbb{Z}_p[\![G]\!]}(\mathbb{F}_p, M) = \mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} M$ est trivial alors M est trivial.*

Remarque. Les prop-p-groupes considérés ici sont tous de type fini.

Démonstration. Soit R le radical de Jacobson de $\mathbb{Z}_p[\![G]\!]$. D'après le théorème A.5, l'idéal R est égal au noyau de la projection $\mathbb{Z}_p[\![G]\!] \to \mathbb{F}_p$ et $R^n \to 0$. Par hypothèse, $\mathrm{Tor}_0^{\mathbb{Z}_p[\![G]\!]}(\mathbb{F}_p, M) \cong M/_{RM}$ est trivial, ainsi d'après le théorème précédent, le module M est trivial. □

Corollaire A.9 ([GHMR05], lemme 4.3)**.** *Soit G une pro-p-groupe de type fini et $f : M \to N$ un homomorphisme de $\mathbb{Z}_p[\![G]\!]$-modules profinis.*

a) Si

$$\mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} f : \mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} M \to \mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} N$$

est surjectif alors f est surjectif.

b) Si

$$\mathrm{Tor}_q(\mathbb{F}_p, f) : \mathrm{Tor}_q^{\mathbb{Z}_p[\![G]\!]}(\mathbb{F}_p, M) \to \mathrm{Tor}_q^{\mathbb{Z}_p[\![G]\!]}(\mathbb{F}_p, N)$$

est un isomorphisme pour $q = 0$ et est surjectif pour $q = 1$, alors f est un isomorphisme.

Démonstration. a) Supposons que $\mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} f$ est surjectif. Soit K le conoyau de f, alors par hypothèse $\mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} K$ est trivial et donc d'après le lemme de Nakayama, on a que K est trivial c'est-à-dire f est surjectif.

b) Supposons que $\mathrm{Tor}_q(\mathbb{F}_p, f)$ est un isomorphisme lorsque $q = 0$ et est surjectif lorsque $q = 1$. Alors, d'après le point précédent, f est surjectif. Posons K le noyau de cet homomorphisme. On a la suite exacte longue suivante :

$$\mathrm{Tor}_1(\mathbb{F}_p, M) \twoheadrightarrow \mathrm{Tor}_1(\mathbb{F}_p, N) \xrightarrow{0} \mathrm{Tor}_0(\mathbb{F}_p, K) \xrightarrow{0} \mathrm{Tor}_0(\mathbb{F}_p, M) \xrightarrow{\cong} \mathrm{Tor}_0(\mathbb{F}_p, N) \longrightarrow 0$$

Donc $\mathrm{Tor}_0(\mathbb{F}_p, K) = 0$ et, d'après le lemme de Nakayama, l'homomorphisme f est injectif. □

Corollaire A.10. *Soit G une pro-p-groupe de type fini et M un $\mathbb{Z}_p[\![G]\!]$-module complet.*

a) Si $\mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} M$ est de type fini, alors M l'est aussi.

b) Si M est de type fini et est projectif, alors M est libre.

Démonstration. a) Il suffit d'appliquer le corollaire précédent à un homomorphisme $f : \mathbb{Z}_p[\![G]\!]^n \twoheadrightarrow M$ tel que $\mathrm{Tor}_0(\mathbb{F}_p, f)$ soit surjectif.

b) voir corollaire 7.5.4 dans [Wil98]. □

Remarque. Étant donnée que $\mathbb{F}_p \underset{\mathbb{Z}_p[\![G]\!]}{\otimes} \mathbb{Z}_p \cong \mathbb{F}_p$, les trois résultats précédents restent vrais lorsqu'on remplace $\mathbb{F}_p$ par $\mathbb{Z}_p$.

A.3 Homologie et sous-groupes

Soit G un pro-p-groupe, on note (IG) l'idéal d'augmentation :

$$0 \longrightarrow (IG) \longrightarrow \mathbb{Z}_p[\![G]\!] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

Rappelons que l'homomorphisme

$$H_1(G, \mathbb{Z}_p) \cong G/_{\overline{[G,G]}} \longrightarrow H_0(G, (IG)) \cong (IG)/_{(IG)^2}$$

qui envoie g sur $g-1$, est un isomorphisme (lemme 6.8.6 [RZ10]). En particulier, on a[1] la propriété suivante :

$$\forall\, \lambda \in \mathbb{Z}_p \qquad g^{\lambda} - 1 \equiv \lambda(g-1) \mod (IG)^2 \tag{A.2}$$

Le résultat suivant est une adaptation du théorème 6.3 du chapitre VI *Cohomology of Groups* dans [HS97] au cas des groupes profinis.

Proposition A.11. *Soient G un groupe profini et K un sous-groupe ouvert distingué de G. On suppose que K est un pro-p-groupe. On pose H le groupe fini $G/_K$. Alors, on a la suite exacte courte de $\mathbb{Z}_p[H]$-modules suivant :*

$$\begin{array}{ccccccccc} 0 \longrightarrow & H_1(K, \mathbb{Z}_p) & \longrightarrow & H_0(K, (IG)) & \longrightarrow & (IH) & \longrightarrow 0 \\ & \bar{k} & \longmapsto & k-1 & & & \\ & & & g-1 & \longmapsto & \bar{g}-1 & \end{array} \tag{A.3}$$

où $\bar{g}$ est la classe de g dans le groupe quotient H et on a identifié $H_1(K, \mathbb{Z}_p)$ avec l'abélianisé $K/_{\overline{[K,K]}}$.

Démonstration. D'après le corollaire 5.7.2 de [RZ10], $\mathbb{Z}_p[\![G]\!]$ est un $\mathbb{Z}_p[\![H]\!]$-module libre au-dessus de $H = G/_K$ et

$$H_0(K, \mathbb{Z}_p[\![G]\!]) = \mathbb{Z}_p \underset{\mathbb{Z}_p[\![K]\!]}{\otimes} \mathbb{Z}_p[\![G]\!] \cong \mathbb{Z}_p[H].$$

Donc, la suite exacte courte $(IG) \to \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p$ induit en homologie la suite exacte de $\mathbb{Z}_p[H]$-modules

$$\begin{tikzcd} 0 \arrow[r] & H_1(K,\mathbb{Z}_p) \arrow[r, tail, "\partial"] & H_0(K,(IG)) \arrow[rr] \arrow[dr] & & \mathbb{Z}_p[H] \arrow[r, two heads, "\epsilon"] & \mathbb{Z}_p \arrow[r] & 0 \\ & & & (IH) \arrow[ur] & & & \end{tikzcd}$$

On en déduit une suite exacte courte semblable à celle de la proposition. Il nous reste à montrer qu'on peut remplacer la différentielle ∂ par le morphisme annoncé dans la proposition.
Notons qu'on a le diagramme suivant :

$$\begin{tikzcd} 0 \arrow[r] & (IK) \arrow[r] \arrow[d, "\iota"] & \mathbb{Z}_p[\![K]\!] \arrow[r] \arrow[d] & \mathbb{Z}_p \arrow[r] \arrow[d, "="] & 0 \\ 0 \arrow[r] & (IG) \arrow[r] & \mathbb{Z}_p[\![G]\!] \arrow[r] & \mathbb{Z}_p \arrow[r] & 0 \end{tikzcd}$$

1. On peut aussi déduire cette propriété de la formule d'interpolation de la puissance (proposition A.3).

Ainsi, par naturalité de l'homologie, on a

$$\begin{tikzcd}
H_1(K,\mathbb{Z}_p) \arrow[r, tail, "\partial", "\cong"'] \arrow[d, "="] & H_0(K,(IK)) \arrow[r] \arrow[d, "\iota_*"] & H_0(K,\mathbb{Z}_p[\![K]\!]) \arrow[r, two heads] \arrow[d] & H_0(K,\mathbb{Z}_p) \arrow[d, "="] \\
H_1(K,\mathbb{Z}_p) \arrow[r, tail, "\partial"] & H_0(K,(IG)) \arrow[r] & \mathbb{Z}_p[H] \arrow[r, two heads] & \mathbb{Z}_p
\end{tikzcd}$$

D'où, en considérant le carré de gauche du diagramme précédent, on déduit la suite exacte courte suivante

$$0 \longrightarrow H_1(K,\mathbb{Z}_p) \cong H_0(K,(IK)) \xrightarrow{\iota_*} H_0(K,(IG)) \longrightarrow (IH) \longrightarrow 0$$

où le premier homomorphisme envoie la classe d'un élément k de $H_1(K,\mathbb{Z}_p) \cong K/_{\overline{[K,K]}}$ sur la classe de $k-1$. Notons cet homomorphisme ϕ. Vérifions qu'avec l'action par conjugaison sur $H_1(K,\mathbb{Z}_p)$, le morphisme ϕ est $\mathbb{Z}_p[H]$-linéaire. Soient $g \in G$ et $k \in K$ alors, dans $H_0(K,(IG))$,

$$\phi(g_*(k-1)) - g_*\phi(k-1) \quad = \quad g(k-1)g^{-1} - g(k-1) \;=\; \underbrace{g(k-1)g^{-1}}_{(IK)}\underbrace{g(g^{-1}-1)}_{(IG)} \;=\; 0$$

C'est-à-dire ϕ est bien $\mathbb{Z}_p[H]$-linéaire. □

Lemme A.12. *Soit K un sous-groupe ouvert de G, on note H le groupe fini $G/_K$. Soit $(b_1,\ldots,b_m) \in G^m$ une famille de représentants des éléments du groupe quotient H telle que $b_1 = e$.*

a) L'homomorphisme

$$\begin{aligned} \psi : \mathbb{Z}_p[\![K]\!]^{\oplus m} &\longrightarrow \mathbb{Z}_p[\![G]\!] \\ (x_1,\ldots,x_m) &\longmapsto x_1 + \textstyle\sum_{i=2}^m x_i(b_i - e) \end{aligned}$$

est un isomorphisme de $\mathbb{Z}_p[\![K]\!]$-modules.

b) L'homomorphisme précédent induit l'isomorphisme de $\mathbb{Z}_p[\![K]\!]$-modules suivant

$$(IK)(IG) \cong (IK)^2 \oplus \bigoplus_{i=2}^m (IK)(b_i - e)$$

De plus, si K est distingué dans G, alors $(IK)(IG)$ est un idéal bilatère de l'algèbre $\mathbb{Z}_p[\![G]\!]$.

Démonstration. Considérons le diagramme commutatif de $\mathbb{Z}_p[\![K]\!]$-modules :

$$\begin{tikzcd}
0 \arrow[r] & (IK) \oplus \mathbb{Z}_p[\![K]\!]^{\oplus m-1} \arrow[r] \arrow[d] & \mathbb{Z}_p[\![K]\!]^{\oplus m} \arrow[r, "\varepsilon'"] \arrow[d, "\psi"] & \mathbb{Z}_p \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & (IG) \arrow[r, hook] & \mathbb{Z}_p[\![G]\!] \arrow[r, "\varepsilon"] & \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

où les homomorphismes sont définis comme suit :

$$\begin{aligned} \varepsilon'(x_1,\ldots,x_m) &= \epsilon(x_1) \\ \psi(x_1,\ldots,x_m) &= x_1 + \sum_{i=2}^m x_i(b_i - e) \end{aligned}$$

Le groupe K est un sous-groupe ouvert du groupe profini G, ainsi (corollaire 5.7.2 [RZ10]) $\mathbb{Z}_p[\![G]\!]$ est $\mathbb{Z}_p[\![K]\!]$-module libre au-dessus de $(b_1, \ldots, b_n)$. Donc, il existe une unique homomorphisme $\mathbb{Z}_p[K]$-linéaire $\phi : \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p[\![K]\!]^{\oplus m}$ tel que pour tout $1 \leq i \leq m$,

$$\phi(b_i) \quad = \quad \begin{cases} (e, 0, \ldots, 0) & \text{si } i = 1 \\ (e, 0, \ldots, 0, \underset{i}{e}, 0, \ldots, 0) & \text{sinon} \end{cases}$$

Après une simple vérification, on voit que ϕ est l'inverse de ψ. D'après le lemme des 5, la restriction de Ψ au noyau de ϵ' est aussi un isomorphisme $\mathbb{Z}_p[\![K]\!]$-linéaire sur le noyau de ϵ, l'idéal d'augmentation de G. Ainsi, on déduit les isomorphismes annoncés dans le lemme.
Supposons que K est distingué dans G. Soient $g \in G$, $P \in (IK)$ et $Q \in (IG)$, comme K est distingué dans G, $gPQ = (gPg^{-1})gQ$ appartient $(IK)(IG)$. D'où, l'on déduit que $(IK)(IG)$ est un idéal bilatère de l'algèbre $\mathbb{Z}_p[\![G]\!]$. □

Passons maintenant à l'extension des scalaires entre groupes profinis.

Définition A.13. Soit F un sous-groupe d'un groupe profini G. Soit M un $\mathbb{Z}_p[\![F]\!]$-module, on définit l'extension des scalaires de M à $\mathbb{Z}_p[\![G]\!]$ comme étant le module

$$M\uparrow_F^G := \mathbb{Z}_p[\![G]\!] \underset{\mathbb{Z}_p[\![F]\!]}{\hat{\otimes}} M$$

muni de la structure de $\mathbb{Z}_p[\![G]\!]$-module à gauche induite par l'action à gauche sur $\mathbb{Z}_p[\![G]\!]$.

Proposition A.14 (Cf. proposition 5.5.3 [RZ10])**.** *Soit A une algèbre profini, soient M un A-module profini à droite et N un A-module profini à gauche. Si M ou N est de type fini, alors le produit tensoriel complété $M\hat{\otimes}_A N$ est isomorphe au produit tensoriel $M \otimes_A N$.*

Dans ce contexte, nous avons le lemme de Shapiro : Pour tout $\mathbb{Z}_p[\![G]\!]$-module N,

$$\mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(M\uparrow_F^G, N) \cong \mathrm{Hom}_{\mathbb{Z}_p[\![F]\!]}(M, N)$$

Lemme A.15. *Soient S un pro-p-groupe, T sous-groupe ouvert de S et F un groupe fini agissant sur S et par restriction sur T. Posons $G = S \rtimes F$. Soit M un $\mathbb{Z}_p[\![F]\!]$-module de type fini, alors, on a un isomorphisme de $\mathbb{Z}_p[S/T]$-modules*

$$H_0(T, M\uparrow_F^G) \cong \mathbb{Z}_p[S/T] \underset{\mathbb{Z}_p}{\otimes} M$$

Démonstration. Il suffit de revenir à la définition de l'extension des scalaires et d'utiliser la proposition 5.8.1 de [RZ10], pour remarquer la suite d'isomorphismes de $\mathbb{Z}_p[T/S]$-modules suivante

$$\begin{aligned} H_0(T, M\uparrow_F^G) &\cong \mathbb{Z}_p \underset{T}{\otimes} (\mathbb{Z}_p[\![G]\!] \underset{F}{\otimes} M) \\ &\cong \mathbb{Z}_p \underset{T}{\otimes} (\mathbb{Z}_p[\![S]\!] \otimes M) \\ &\cong \mathbb{Z}_p[S/T] \underset{\mathbb{Z}_p}{\otimes} M \end{aligned}$$

□

Lemme A.16. *Avec les notations du premier chapitre, en particulier la définition 1.22, le $\mathbb{Z}_p[\![S_2^1]\!]$-module $\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$ est libre de rang 2.*

Démonstration. On applique encore une fois la proposition 5.8.1 de [RZ10], pour obtenir :

$$\Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1} \quad = \quad \mathbb{Z}_p[\![\mathbb{G}_2^1]\!] \underset{F}{\otimes} \Lambda_{1-p} \cong \mathbb{Z}_p[\![S_2^1]\!] \otimes \Lambda_{1-p} \cong \mathbb{Z}_p[\![S_2^1]\!]^{\oplus 2}$$

□

Avant de terminer cette section du l'homologie, donnons encore une résolution projective, bien connue, du groupe $\mathbb{Z}_p$ lui-même.

Lemme A.17. *Soit p un nombre premier impair, posons $U_1 = 1+p\mathbb{Z}_p \cong \mathbb{Z}_p$. Soit t un générateur topologique de U_1. La suite*

$$0 \longrightarrow \mathbb{Z}_p[\![U_1]\!] \xrightarrow{t-e} \mathbb{Z}_p[\![U_1]\!] \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$$

est exacte et définie une résolution libre de $\mathbb{Z}_p$ au-dessus de U_1.

Démonstration. L'augmentation ϵ est clairement surjective. L'idéal d'augmentation (IU_1) est engendré par $t-e$ (lemme 6.3.2 [RZ10]), d'où l'exactitude au centre de la suite. Il nous reste à montrer que la multiplication par $t-e$ est injective. Pour ce faire, on utilise l'exactitude du foncteur limite inverse sur la catégorie des groupes profinis (proposition 2.2.4 [RZ10]). Notons qu'on a le diagramme suivant

$$\begin{tikzcd}
0 \arrow[r] & (1+\ldots+t^{p^{n+1}-1}) \cong \mathbb{Z}_p \arrow[r] \arrow[d, "\times p"] & \mathbb{Z}_p[t]/(t^{p^{n+1}}-1) \arrow[r, "t-1"] \arrow[d] & \mathbb{Z}_p[t]/(t^{p^{n+1}}-1) \arrow[r, "\epsilon"] \arrow[d] & \mathbb{Z}_p \arrow[r] & 0 \\
0 \arrow[r] & (1+\ldots+t^{p^{n}-1}) \cong \mathbb{Z}_p \arrow[r] & \mathbb{Z}_p[t]/(t^{p^{n}}-1) \arrow[r, "t-1"] & \mathbb{Z}_p[t]/(t^{p^{n}}-1) \arrow[r, "\epsilon"] & \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

En passant à la limite inverse, on déduit que

$$\ker(t-1) = \varprojlim(\ldots \xrightarrow{p} \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_p \xrightarrow{p} \ldots) = 0$$

□

A.4 Cohomologie des groupes profinis

Théorème A.18 (Suite spectrale de Lyndon-Hochschild-Serre, 6.8.2 [Wei94])**.** *Soient G un groupe fini, H un sous-groupe distingué et M un G-module. On a deux suites spectrales dans le premier quadrant :*

$$E^2_{p,q} = H_p(G/H,\, H_q(H,M)) \Rightarrow H_{p+q}(G,M)$$
$$E_2^{p,q} = H^p(G/H,\, H^q(H,M)) \Rightarrow H^{p+q}(G,M)$$

Les homomorphismes de bords $H_*(G,M) \to H_*(G/H, M_H)$ et $H_*(H,M) \to H_*(G,M)$ de la première suite spectrale sont induit par les homomorphismes de coinflation et de corestriction. Les homomorphismes de bords $H^*(G/H, M^H) \to H^*(G,A)$ et $H^*(G,A) \to H^*(H,A)^{G/H}$ dans la second suite spectrale sont induit par les homomorphismes d'inflation et de restriction.

Remarque. Pour mémoire, la différentielle $d^r_{p,q}$ (resp. $d_r^{p,q}$) de la page E^r (resp. E_r) va de $E^r_{p,q}$ dans $E^r_{p-r,q+r-1}$ (resp. de $E_r^{p,q}$ dans $E_r^{p+r,q-r+1}$).
Au passage, la démonstration donnée dans [RZ10] ne s'applique a priori qu'aux modules discrets. Mais, en utilisant le développement fait dans le chapitre 9 *Cohomology of profinite groups* de [Wil98], on voit que l'on peut adapter la preuve au cas des G-modules (topologiques).

Corollaire A.19 (five-term exact sequence 6.8.3 [Wei94])**.** *Les suites exactes de petits degrés dans la suite spectrale de Lyndon-Hochschild-Serre sont :*

i) $H_2(G,M) \xrightarrow{\text{coinf}} H_2(G/H, M_H) \xrightarrow{\text{d}} H_1(H,M)_{G/H} \xrightarrow{\text{cor}} H_1(G,M) \xrightarrow{\text{coinf}} H_1(G/H, M_H) \longrightarrow 0$

ii) $0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G,M) \xrightarrow{\text{res}} H^1(H,M)^{G/H} \xrightarrow{\text{d}} H^2(G/H, M^H) \xrightarrow{\text{inf}} H^2(G,M)$

Si l'on veut utiliser la suite spectrale de Lyndon-Hochschild-Serre pour le calcul de $H^1(G, M)$, on voit qu'il faut déterminer $H^0(G/H, H^1(H, M))$. Une première question qui se pose est de déterminer la structure de $G/_H$-module de $H^1(H, M)$. Nous allons uniquement considérer un cas particulier.

Lemme A.20. *Soient M un G-module et H un sous-groupe distingué fermé du groupe profini G. Si H agit trivialement sur M, alors $H^1(H, M) \cong \mathrm{Hom}(H, M)$ et l'action de G/H sur M est définie comme suit :*

$$(g_*\phi)(h) = g\phi(g^{-1}hg)$$

Comme conséquence immédiate, on a le lemme suivant.

Lemme A.21. *Soient p un nombre premier et n un entier naturel. On note $\boldsymbol{\mu}_{p^n-1}$ le groupe des unités du corps fini $\mathbb{F}_{p^n}$ et Gal le groupe de Galois de ce dernier corps vu comme extension de $\mathbb{F}_p$. On munit $\mathbb{F}_{p^n}^\times$ d'une structure de $\mathbb{Z}_p[\boldsymbol{\mu}_{p^n-1} \rtimes \mathrm{Gal}]$-module en laissant agir $\boldsymbol{\mu}_{p^n-1}$ trivialement et le groupe de Galois Gal par son action naturelle. Alors*

$$H^1(\boldsymbol{\mu}_{p^n-1}, \mathbb{F}_{p^n}^\times) \cong \mathbb{Z}/_{(p^n - 1)}$$

est muni d'une action triviale du groupe de Galois Gal.

Remarque. On peut même dire plus. Comme $\boldsymbol{\mu}_{p^n-1}$ admet une résolution projective cyclique d'ordre 2, on déduit que tous les groupes de cohomologie $H^*(\boldsymbol{\mu}_{p^n-1}, \mathbb{F}_{p^n}^\times)$ sont isomorphe soit au groupe de cohomologie en degré 0, soit au groupe de cohomologie en degré 1. De plus, les isomorphismes sont $\mathbb{Z}_p[\mathrm{Gal}]$-linéaires.

Lemme A.22. *Soient G un pro-p-groupe et M un G-module fini d'ordre premier à p, alors, quel que soit $n > 0$, $H^n(G, M) = 0$.*

Démonstration. D'après le corollaire 6.5.6 de [RZ10], $H^n(G, M) = \varinjlim H^n(G/U, M^U)$ où U parcours l'ensemble des sous-groupes distingués ouverts de G. On en déduit qu'on peut se restreindre au cas où G est un p-groupe fini. Dans ce cas, on a la diagramme bien connu suivant

$$\begin{tikzcd}
H^n(G,M) \arrow[r, "\mathrm{res}_1^G"] \arrow[dr, "\cong", "{[G,1]}"'] & H^n(1,M) = 0 \arrow[d, "\mathrm{cor}_1^G"] \\
 & H^n(G,M)
\end{tikzcd}$$

Le fait que l'homomorphisme trivial soit un isomorphisme implique la trivialité des groupes de cohomologie. $\square$

Lemme A.23. *Soient G un groupe profini, M un pro-p-groupe muni d'une structure de G-module. Soit A un groupe abélien fini d'ordre premier à p. Alors,*

$$\mathrm{Hom}(A, H^n(G, M)) = 0$$

Démonstration. Soient $f : A \to H^n(G, M)$ un homomorphisme et x un élément de A. On a $|A|f(x) = f(|A|x) = 0$, or la multiplication avec $|A|$ induit un automorphisme de $H^n(G, M)$. D'où $f(x) = 0$. $\square$

Formulaire

Chapitre 1. *Anneau de Lubin-Tate et le groupe stabilisateur de Morava.*

Γ_2 loi de groupe formel de Honda : $[p]_{\Gamma_2}(x) = x^{p^2}$. page 13

$\mathbb{W} = \mathbb{W}(\mathbb{F}_{p^2})$ anneau de Witt de corps résiduel $\mathbb{F}_{p^2}$. page 13

$\omega \in \boldsymbol{\mu}_{p^2-1} \subset \mathbb{W}^\times$ générateur du groupe cyclique $\boldsymbol{\mu}_{p^2-1}$. page 16

$\sigma \in \mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$ automorphisme de Frobenius.

$\mathcal{O}_2 = \mathbb{W}\langle S\rangle / (S^2 - p, \{Sx - x^\sigma S\}_{x\in\mathbb{W}})$. page 13

$\mathcal{O}_2 \cong \mathrm{End}_{\mathbb{F}_{p^2}}(\Gamma_2)$, $S \mapsto x^p$ et $w \in \boldsymbol{\mu}_{p^2-1} \mapsto \bar{w}x$.

$(E_2)_* = \mathbb{W}[[u_1]][u^{\pm 1}]$. page 14

G_2 déformation universelle : $[p]_{G_2}(x) = px \underset{G_2}{+} u_1 x^p \underset{G_2}{+} x^{p^2}$. page 14

$\mathbb{S}_2 = \mathrm{Aut}_{\mathbb{F}_{p^2}}(\Gamma_2)$. page 14

$g_* u = t_0(g) u$, pour tout $g \in \mathbb{S}_2$. page 15

$g_* u_1 = (p - p^p) t_0^{-1}(g) t_1(g) + t_0^{p-1}(g) u_1$, pour tout $g \in \mathbb{S}_2$. page 19

$S_2 = \ker(\mathbb{S}_2 \to \mathcal{O}_2^\times / (S) \cong \mathbb{F}_{p^2}^\times)$. page 19

$\det : \mathbb{G}_2 = \mathbb{S}_2 \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}; \mathbb{F}_p) \longrightarrow \mathbb{Z}_p^\times$, $(x, \sigma^i) \mapsto \det(.x)$. page 21

$N : \mathbb{G}_2 \xrightarrow{\det} \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p / \boldsymbol{\mu}_{p-1} \cong \mathbb{Z}_p$. page 21

$\mathbb{G}_2^1 = \ker(N)$ et $S_2^1 = \mathbb{G}_2^1 \cap S_2$. page 21

$\mathbb{G}_2 \cong \mathbb{G}_2^1 \times \mathbb{Z}_p$. page 21

$\mathbb{G}_2^1 \cong S_2^1 \rtimes F, \quad F = \boldsymbol{\mu}_{p^2-1} \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}, \mathbb{F}_p)$. page 21

$F_i S_2^1 = \{\ x \in S_2^1 \,|\, x \equiv 1 \bmod (S^{2i})\ \}$ pour tout $i \in \frac{\mathbb{N}^*}{2}$.

$\mathrm{gr}_i\, S_2^1 = \begin{cases} \ker(\mathrm{tr}) = \{x \in \mathbb{F}_{p^2};\, x^p = -x\} & \text{si } i \in \mathbb{N}^* \\ \mathbb{F}_{p^2} & \text{sinon} \end{cases}.$ page 22

$\Lambda_i \cong \mathbb{W}u^i$ le $\mathbb{Z}_p[F]$-module : $w_* x = w^i x$ et $\sigma_* x = x^\sigma$. page 25

$\mathrm{tr}_F :\ \mathrm{Hom}(M, N) \to \mathrm{Hom}_{\mathbb{Z}_p[F]}(M, N)$, $\mathrm{tr}_F(\phi)(x) = \frac{1}{|F|}\sum_{g\in F} g_*^{-1}\phi(g_* x)$. page 26

$\epsilon_\pm = \frac{\omega \pm \omega^p}{2} \in \mathbb{W}^\times$, $\epsilon_\pm^\sigma = \pm\epsilon_\pm$. page 26

λ, μ : $\mathbb{W} \to \mathbb{Z}_p$ formes linéaires : $\lambda(x) = \frac{x + x^\sigma}{2\epsilon_+}$ et $\mu(x) = \frac{x - x^\sigma}{2\epsilon_-}$. page 26

$x = \lambda(x)\epsilon_+ + \mu(x)\epsilon_-$ pour tout $x \in \mathbb{W}$.

$v_1 = u_1 u^{1-p}$ et $v_2 = u^{1-p^2}$ éléments de $(E_2)_*^F$. page 28

$(E_2)_*^F \cong \mathbb{Z}_p[[u_1^{p+1}]][v_1, v_2^{\pm 1}] \,/\, v_1^{p+1} v_2^{-1} - u_1^{p+1}$. page 28

$\mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, (E_2)_*) \cong (E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1}) \;\subseteq\; (E_2)_*$. page 28

Chapitre 2. *Résolution projective : $n = 2$ et $p > 3$.*

$C_0 = C_3 = \mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}$ et $C_1 = C_2 = \Lambda_{1-p}\uparrow_F^{\mathbb{G}_2^1}$. page 31

$0 \longrightarrow C_3 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z}_p \longrightarrow 0$, résolution projective du $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-module trivial $\mathbb{Z}_p$.

$C_0 \cong \mathbb{Z}_p[\![S_2^1]\!]$ en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module. page 36

$N_0 = \ker(\partial_1) \underset{S_2^1}{\cong} (IS_2^1) = \ker(\mathbb{Z}_p[\![S_2^1]\!] \to \mathbb{Z}_p)$. page 36

$((e_i)_+, (e_i)_-)$ la base $(1 \otimes \epsilon_+, 1 \otimes \epsilon_-)$ de C_i en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module, où $i = 1, 2$. page 31

$e_i = 1 \otimes 1$ base de C_i en tant que $\mathbb{Z}_p[\![S_2^1]\!]$-module, où $i = 0, 3$.

$a_0 = 1 + \epsilon_+ S \in P\mathbb{G}_2 \cong \mathbb{G}_2^1$. page 32

$b_0 = 1 + \epsilon_- S \in P\mathbb{G}_2 \cong \mathbb{G}_2^1$.

$a_i = \omega^{-i}\, a_0\, \omega$ et $b_i = \omega^{-i}\, b_0\, \omega$.

$\lambda_i = \lambda(\omega^{(1-p)i}\epsilon_+)$ et $\mu_i = \mu(\omega^{(1-p)i}\epsilon_+)$. page 33

$\lambda_i = \lambda_{-i} = -\lambda_{-i+(p+1)/2}$ et $\mu_i = \mu_{-i+(p+1)/2} = -\mu_{-i}$.

$v = \frac{1}{p+1}\sum_{i=0}^{p} \lambda(\omega^{(1-p)i}\epsilon_+)(a_i - 1) + \mu(\omega^{(1-p)i}\epsilon_+)(b_i - 1)$. page 33

$w = \frac{1}{p+1}\sum_{i=0}^{p} \lambda(\omega^{(1-p)i}\epsilon_-)(a_i - 1) + \mu(\omega^{(1-p)i}\epsilon_-)(b_i - 1)$.

$\partial_1(e_1)_+ = v$ et $\partial_1(e_1)_- = w$. page 37

$\mathcal{N}(g) = 1 + g + \ldots + g^{p-1} \in \mathbb{Z}_p[\![\mathbb{S}_2]\!]$ pour tout $g \in \mathbb{S}_2$. page 33

$d_2 : \Lambda_{1-p} \to C_1$ homomorphisme $\mathbb{Z}_p$-linéaire tel que page 60

$d_2(\epsilon_+) \equiv \mathcal{N}(a_0)(e_1)_+ \;+\; \frac{1}{4\epsilon_-^2}(b_0 - 1)(w(e_1)_+ - v(e_1)_-) + \frac{1}{4\epsilon_-^2}(c_0 - 1)(e_1)_-$
$\quad + p(w(e_1)_+ - v(e_1)_-)$ modulo $(IJ + JI)C_1$.

$d_2(\epsilon_-) \equiv \mathcal{N}(b_0)(e_1)_- \;+\; \frac{1}{4\epsilon_+^2}(a_0 - 1)(w(e_1)_+ - v(e_1)_-) + \frac{1}{4\epsilon_+^2}(c_0 - 1)(e_1)_+$
$\quad - p(w(e_1)_+ - v(e_1)_-)$ modulo $(IJ + JI)C_1$.

$\alpha : C_2 \to C_2$ automorphisme $\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]$-linéaire tel que $\mathrm{Tor}_0^{\mathbb{Z}_p[\![S_2^1]\!]}(\mathbb{Z}_p, \alpha) = \mathrm{Id}_{\Lambda_{1-p}}$. page 66

$\partial_2 = \mathrm{tr}_F(d_2)\uparrow_F^{\mathbb{G}_2^1}\;\alpha$.

$\Lambda = \frac{1}{p+1}\sum_{i=0}^{p} \lambda(\omega^{(1-p)i}\epsilon_+)(a_i^{-1}-1) + \mu(\omega^{(1-p)i}\epsilon_+)(b_i^{-1}-1).$ page 66

$\partial_3(e_3) = \frac{1}{2\epsilon_+^2}\Lambda(e_2)_+ + \frac{1}{4\epsilon_-^2\mu_1}(\omega^{-1}\Lambda\omega - \omega\Lambda\omega^{-1})(e_2)_-.$ page 66

Chapitre 3. *Sur l'action du groupe stabilisateur de Morava*

$G_2(x,y) = x + y - \frac{u_1}{1-p^{p-1}}C_p(x,y) + \sum_{i=1}^{p} u_1^{i+1}P_{p+i(p-1)}(x,y) + P(x,y) \mod (x,y)^{p^2+1}.$

$t_0(g) \equiv 1 + g_1^p u_1 - g_1 u_1^p + (g_2 - g_2^p)u_1^{p+1} + g_1^p u_1^{p+2} + \frac{p-1}{2}g_1^{2p}u_1^{p+3} \mod (p,\ u_1^{p+4}),$
où $g \equiv 1 + g_1 S + g_2 S^2 \mod (S^3)$. page 76

$t_0(g^k) \equiv t_0(1 + kg_1 S)$ modulo $(p,\ u_1^{2p+1})$, où $g \equiv 1 + g_1 S + g_2 S^2 \mod (S^3)$ avec $g_2 \in \mathbb{F}_p$.

$t_0(g)^s \equiv (1 + g_1^p u_1)^s - sg_1 u_1^p - s(s-1)g_1^{p+1}u_1^{p+1}$
$+s\Big(g_1^p - \binom{s-1}{2}g_1^{2p+1}\Big)u_1^{p+2} + s\Big((\frac{p-1}{2} + s - 1)g_1^{2p} - \binom{s-1}{3}g_1^{3p+1}\Big)u_1^{p+3}$
modulo $(p,\ u_1^{p+4})$, où $g \equiv 1 + g_1 S + g_2 S^2 \mod (S^3)$ avec $g_2 \in \mathbb{F}_p$. page 77

Chapitre 4. *Cohomologie à coefficient dans $(E_2)_*$ modulo p*

$h_0 = u^{1-p}$ et $h_1 = u^{p-1}$ éléments de $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1}) \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*)$.

$g_0 = u^{1-p}$ et $g_1 = u^{p-1}$ éléments de $(E_2)_*^F \otimes (\mathbb{Z}_p u^{1-p} \oplus \mathbb{Z}_p u^{p-1}) \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*)$.

$u_1 = h_1 v_1, \quad u_1^p = h_0 v_1^p v_2^{-1} \quad$ et $\quad u_1^{p+1} = v_1^{p+1}v_2^{-1}$.

$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_0, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(1)_s\}.$ page 80

$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_1, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_1)_s\}.$

$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_2, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(g_0)_s\} \oplus \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(g_1)_s\}.$

$\mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(C_3, (E_2)_*/(p)) \cong \prod_{s\in\mathbb{Z}} \mathbb{F}_p[v_1]\{(h_0 g_1)_s\}.$

$(X)_s \equiv c\,X\,v_2^s \mod (p, u_1)$, où $c \in \mathbb{F}_p^\times$ dépend de $X \in \{1, h_0, h_1, g_0, g_1, h_0 g_1\}$.

$A_n = \frac{p^n-1}{p-1}(p+1) = (p^{n-1} + \ldots + 1)(p+1).$ page 80

$$a_n = \begin{cases} p^{n-1}(p+1) - 1 & n > 0, \\ 1 & n = 0. \end{cases}$$

$\alpha_n = \frac{1-p^n}{p-1} = -p^{n-1} - \ldots - 1.$

$R_s = \frac{1}{2}(\binom{s}{p+2} - s\binom{s-1}{2})(\epsilon_+^2 - \epsilon_-^2)$ dans $\mathbb{F}_p$ pour tout entier relatif s. page 85

$v_* u^s \equiv \epsilon_+(su_1 + (\ \binom{s}{p} - s\ )u_1^p + (s + R_s)u_1^{p+2})u^s \mod (p, u_1^{p+4}).$ page 85

$\Lambda_* u^s \equiv -v_* u^s \mod (p, u_1^{p+4})$.

$w_* u^s \equiv \epsilon_-(-su_1 + (\binom{s}{p} - s)u_1^p - (s + R_s)u_1^{p+2})u^s \mod (p, u_1^{p+4})$.

Chapitre 5. *Le groupe* Pic_2 *de Hopkins*

$\mathrm{Pic}_2^{\mathrm{alg},0} = \mathrm{Pic}((E_2)_0\text{-}\mathbb{G}_2\text{-}\mathrm{Mod})$. page 110

$\tilde{t}_0 : \mathbb{G}_n \xrightarrow{t_0} (E_n)_0^\times \twoheadrightarrow \mathbb{U}_1((E_n)_0)$. page 110

$U_n = \{x \in \mathbb{F}_{p^2}[[u_1]];\ x \equiv 1 \mod (u_1^n) \}$. page 119

$U_1^F \cong \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\mathbb{Z}_p\uparrow_F^{\mathbb{G}_2^1}, U_1) \cong \prod_{p\nmid k} (1 + u_1^{(p+1)k})^{\mathbb{Z}_p}$. page 119

$\zeta_{r,k}(x) = \begin{cases} 1 + x^p\, u_1^{1+(p+1)k} & \mod U_{2(r+(p+1)k)} \quad \text{si } r = 1, \\ 1 + x\, u_1^{p+(p+1)k} & \mod U_{2(r+(p+1)k)} \quad \text{si } r = p. \end{cases}$ page 121

$U_1^\Lambda = \mathrm{Im}(\mathrm{ev}_1 : \mathrm{Hom}_{\mathbb{Z}_p[F]}(\Lambda_{1-p}, U_1) \to U_1) \subset 1 + \mathbb{F}_p[[u_1]]u_1$. page 122

$U_1^\Lambda \cong \prod_{s\not\equiv -1[p]} \mathbb{Z}_p \{\zeta_{1,s}\} \quad \oplus \quad \prod_{s\not\equiv 0[p]} \mathbb{Z}_p \{\zeta_{p,s}\}$ page 122

$\partial_i^\times = \mathrm{Hom}_{\mathbb{Z}_p[\![\mathbb{G}_2^1]\!]}(\partial_i, U_1)$. page 122

$\mathcal{A}_n := \frac{(-p)^n - 1}{p+1} = -1 + p - \ldots + (-p)^{n-1}$. page 124

$\mathbb{N} = \{ s \in \mathbb{N};\ s \not\equiv -1[p] \} \bigcup \{ \mathcal{A}_n + sp^n;\ s \not\equiv (-1)^{n+1} [p] \text{ et } s > (-1)^{n+1} \text{ et } n > 0 \}$. page 124

$1 + (p + 1)(\mathcal{A}_n + sp^n) = ((-1)^n + (p + 1)s)p^n$.

Bibliographie

[Beh12] Mark Behrens. The homotopy groups of $S_{E(2)}$ at $p \geq 5$ revisited. *Adv. Math.*, 230(2) :458–492, 2012.

[Ben98] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[BH97] P. N. Balister and S. Howson. Note on Nakayama's lemma for compact Λ-modules. *Asian J. Math.*, 1(2) :224–229, 1997.

[Bro82] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[DH95] Ethan S. Devinatz and Michael J. Hopkins. The action of the Morava stabilizer group on the Lubin-Tate moduli space of lifts. *Amer. J. Math.*, 117(3) :669–710, 1995.

[DH04] Ethan S. Devinatz and Michael J. Hopkins. Homotopy fixed point spectra for closed subgroups of the Morava stabilizer groups. *Topology*, 43(1) :1–47, 2004.

[GHM12] Paul Goerss, Hans-Werner Henn, and Mark Mahowald. The rational homotopy of the K(2)-local sphere and the chromatic splitting conjecture for the prime 3 and level 2. *arXiv :1210.7031*, 2012.

[GHMR05] Paul Goerss, Hans-Werner Henn, Mark Mahowald, and Charles Rezk. A resolution of the $K(2)$-local sphere at the prime 3. *Ann. of Math. (2)*, 162(2) :777–822, 2005.

[Hen98] Hans-Werner Henn. Centralizers of elementary abelian p-subgroups and mod-p cohomology of profinite groups. *Duke Math. J.*, 91(3) :561–585, 1998.

[Hen07] Hans-Werner Henn. On finite resolutions of $K(n)$-local spheres. 342 :122–169, 2007.

[HKM08] Hans-Werner Henn, Nasko Karamanov, and Mark Mahowald. The homotopy of the K(2)-local Moore spectrum at the prime 3 revisited. *arXiv :0811.0235v1*, 2008.

[HMS94] Michael J. Hopkins, Mark Mahowald, and Hal Sadofsky. Constructions of elements in Picard groups. 158 :89–126, 1994.

[HMS13] Olga Holtz, Volker Mehrmann, and Hans Schneider. Matrices that commute with their derivative. On a letter from Schur to Wielandt. *Linear Algebra Appl.*, 438(5) :2574–2590, 2013.

[HS97] P. J. Hilton and U. Stammbach. *A course in homological algebra*, volume 4 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[HS99] Mark Hovey and Neil P. Strickland. Morava K-theories and localisation. *Mem. Amer. Math. Soc.*, 139(666) :viii+100, 1999.

[Kar10] Nasko Karamanov. On Hopkins' Picard group Pic_2 at the prime 3. *Algebr. Geom. Topol.*, 10(1) :275–292, 2010.

[Laz55] Michel Lazard. Sur les groupes de Lie formels à un paramètre. *Bull. Soc. Math. France*, 83 :251–274, 1955.

[Laz65] Michel Lazard. Groupes analytiques p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (26) :389–603, 1965.

[LT65] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. *Ann. of Math. (2)*, 81 :380–387, 1965.

[LT66] Jonathan Lubin and John Tate. Formal moduli for one-parameter formal Lie groups. *Bull. Soc. Math. France*, 94 :49–59, 1966.

[Mor85] Jack Morava. Noetherian localisations of categories of cobordism comodules. *Ann. of Math. (2)*, 121(1) :1–39, 1985.

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

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, second edition, 2010.

[Sad93] Hal Sadofsky. Hopkins' and Mahowald's picture of Shimomura's v_1-Bockstein spectral sequence calculation. 146 :407–418, 1993.

[Shi86] Katsumi Shimomura. On the Adams-Novikov spectral sequence and products of β-elements. *Hiroshima Math. J.*, 16(1) :209–224, 1986.

[Str92] N. P. Strickland. On the p-adic interpolation of stable homotopy groups. 176 :45–54, 1992.

[Str00] N. P. Strickland. Gross-Hopkins duality. *Topology*, 39(5) :1021–1033, 2000.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[Wil98] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

Dans les années 80, Shimomura a déterminé les groupes d'homotopie du spectre de Moore $V(0)$ localisé par rapport à $K(2)$ la deuxième K-théorie de Morava. Plus tard, avec les travaux de Devinatz et Hopkins est apparu une autre suite spectrale convergeant vers les précédents groupes d'homotopies. Lorsque le paramètre premier p de la théorie $K(2)$ est supérieur ou égal à cinq, la précédente suite spectrale dégénère. Ainsi, déterminer ces groupes d'homotopie revient à calculer les groupes de cohomologie du groupe stabilisateur de Morava à coefficients dans l'anneau de Lubin-Tate modulo p.
En 2007, Henn a démontré l'existence, lorsque $p \geq 5$, d'une résolution projective du groupe de Morava de longueur quatre. Dans cette thèse, nous précisons une telle résolution projective. On l'applique ensuite au calcul effectif des groupes de cohomologie à coefficients dans l'anneau de Lubin-Tate modulo p. Enfin, on donne une seconde application, en redémontrant un résultat de Hopkins non publié sur le groupe de Picard de la catégorie des spectres $K(2)$-locaux.

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE
UMR 7501
Université de Strasbourg et CNRS
7 Rue René Descartes
67 084 STRASBOURG CEDEX

Tél. 03 68 85 01 29
Fax 03 68 85 03 28

www-irma.u-strasbg.fr
irma@math.unistra.fr

IRMA 2013/011
http ://tel.archives-ouvertes.fr/tel-00875761
ISSN 0755-3390