Canad. J. Math. Vol. **68** (3), 2016 pp. 571–624
http://dx.doi.org/10.4153/CJM-2015-026-3

Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques

Georges Gras

Abstract. Let $K/\mathbb{Q}$ be Galois and let $\eta \in K^\times$ be such that $\mathrm{Reg}_\infty(\eta) \neq 0$. We define the local θ-regulators $\Delta_p^\theta(\eta) \in \mathbb{F}_p$ for the $\mathbb{Q}_p$-irreducible characters θ of $G = \mathrm{Gal}(K/\mathbb{Q})$. Let V_θ be the θ-irreducible representation. A linear representation $\mathcal{L}^\theta \simeq \delta V_\theta$ is associated with $\Delta_p^\theta(\eta)$ whose nullity is equivalent to $\delta \geq 1$. Each $\Delta_p^\theta(\eta)$ yields $\mathrm{Reg}_p^\theta(\eta)$ modulo p in the factorization $\prod_\theta(\mathrm{Reg}_p^\theta(\eta))^{\phi(1)}$ of $\mathrm{Reg}_p^G(\eta) := \frac{\mathrm{Reg}_p(\eta)}{p^{[K:\mathbb{Q}]}}$ (normalized p-adic regulator). From $\mathrm{Prob}(\Delta_p^\theta(\eta) = 0$ and $\mathcal{L}^\theta \simeq \delta V_\theta) \leq p^{-f\delta^2}$ ($f \geq 1$ is a residue degree) and the Borel–Cantelli heuristic, we conjecture that for p large enough, $\mathrm{Reg}_p^G(\eta)$ is a p-adic unit or $p^{\phi(1)} \parallel \mathrm{Reg}_p^G(\eta)$ (a single θ with $f = \delta = 1$); this obstruction may be lifted assuming the existence of a binomial probability law confirmed through numerical studies (groups C_3, C_5, D_6). This conjecture would imply that for all p large enough, Fermat quotients, normalized p-adic regulators are p-adic units and that number fields are p-rational. We recall some deep cohomological results that may strengthen such conjectures.

1 Introduction

Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n de groupe de Galois G. On considère $\eta \in K^\times$. On utilise la notation exponentielle pour la conjuguaison de η par $\sigma \in G$ qui se traduit par l'écriture $(\eta^\sigma)^\tau =: \eta^{\tau\sigma}$ pour tout $\sigma, \tau \in G$. On suppose que le $\mathbb{Z}[G]$-module multiplicatif engendré par η est de $\mathbb{Z}$-rang n. Pour p assez grand, on pose

$$\mathrm{Reg}_p^G(\eta) := \mathrm{dét}\Big(\frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}})\Big)_{\sigma,\tau\in G}$$

(régulateur p-adique normalisé de η).

L'unique obstruction, pour que le principe heuristique de Borel–Cantelli conduise conjecturalement à un nombre fini de p tels que $\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod{p}$, concerne les p tels que $\mathrm{Reg}_p^G(\eta)$ est exactement divisible par une puissance minimale de p, ce qui équivaut à $\mathrm{Reg}_p^G(\eta) \sim p^{\phi(1)}$ (égalité au produit près par une unité p-adique), où ϕ (absolument irréductible) définit un caractère p-adique θ vérifiant certaines conditions (Définition 4.1). Une telle situation est *a priori* de probabilité $\frac{O(1)}{p}$, uniquement lorsque η est considéré comme une variable aléatoire.

On se propose, à partir d'heuristiques et d'expérimentations numériques, d'éliminer cette obstruction et d'aboutir au résultat probabiliste suivant, *lorsque η est fixé et $p \to \infty$.*

Reçu par la rédaction le 23 avril 2014; revu le 27 mai 2015.
Publié electronique au 28 mars 2016.
Classification (AMS) par sujet: **11F85**, 11R04, 20C15, 11C20, 11R37, 11R27, 11Y40.
Mots clés: p-adic regulators, Leopoldt–Jaulent conjecture, Frobenius group determinants, characters, Fermat quotient, Abelian p-ramification, probabilistic number theory.

Théorème 1.1 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n et de groupe de Galois G. Soit $\eta \in K^\times$ fixé, η engendrant un $\mathbb{Z}[G]$-module multiplicatif de $\mathbb{Z}$-rang n.*

(i) *Sous l'Heuristique 7.4 (existence d'une loi de probabilité binomiale convenable), la probabilité d'avoir* $\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod{p}$ *est* $\le C_\infty(\eta)\frac{1}{p^{\log_2(p)/\log(c_0(\eta))-O(1)}}$ *pour* $p \to \infty$, *où* $c_0(\eta) = \max_{\sigma\in G}(|\eta^\sigma|)$, $e^{-1} \le C_\infty(\eta) \le 1$, *et* $\log_2 = \log\circ\log$.

(ii) *Sous l'Heuristique 7.4 précédente et le principe heuristique de Borel–Cantelli, le nombre de premiers p tels que* $\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod{p}$ *est fini.*

Nous supposerons toujours que le nombre premier p considéré est assez grand, en particulier impair, non diviseur de n, non ramifié dans $K/\mathbb{Q}$, et étranger à η.

Désignons par Z_K (resp. $Z_{K,(p)}$) l'anneau des entiers (resp. des p-entiers) de K ; pour $K = \mathbb{Q}$, on obtient $\mathbb{Z}$ (resp. $\mathbb{Z}_{(p)}$). Pour toute place finie $v \mid p$ de K, on désigne par $\mathfrak{p}_v$ l'idéal premier associé à v.

Si n_p est le degré résiduel commun des places $v \mid p$ dans $K/\mathbb{Q}$, les groupes multiplicatifs des corps résiduels sont d'ordres $p^{n_p}-1$ et on a la congruence

$$\eta^{p^{n_p}-1} \equiv 1 \pmod{\mathfrak{p}_v}$$

pour tout $v \mid p$; d'où finalement $\eta^{p^{n_p}-1} = 1 + p\alpha_p(\eta)$, $\alpha_p(\eta) \in Z_{K,(p)}$, ce qui conduit par Galois aux relations $\alpha_p(\eta^\sigma) = \alpha_p(\eta)^\sigma$ pour tout $\sigma \in G$, et aux propriétés "logarithmiques" :

$$\alpha_p(\eta\,\eta') \equiv \alpha_p(\eta) + \alpha_p(\eta') \pmod{p} \text{ et } \alpha_p(\eta^\lambda) \equiv \lambda\,\alpha_p(\eta) \pmod{p}$$

(pour $\eta, \eta' \in K^\times$, $\lambda \in \mathbb{Z}$).

Ce *quotient de Fermat généralisé* $\alpha_p(\eta)$ est l'élément central de notre étude. De façon précise, les propriétés du G-module engendré par $\alpha_p(\eta)$ modulo $p\,Z_{K,(p)}$ vont préciser celles des *régulateurs p-adiques normalisés* de η, en particulier pour la recherche des (rares) solutions p conduisant à leur divisibilité par p. Les illustrations numériques sont obtenues via des programmes PARI (d'après [P]).

2 Régulateurs et Représentations : Régulateurs locaux

2.1 Logarithme p-adique : Régulateurs p-adiques

Soit p un nombre premier fixé vérifiant les hypothèses posées dans l'Introduction. On suppose que K est considéré comme un sous-corps de $\mathbb{C}_p$. Ainsi tout "plongement" de K dans $\mathbb{C}_p$ n'est autre qu'un $\mathbb{Q}$-automorphisme $\sigma \in G$.

Soit $\mathfrak{p}_0 = \mathfrak{p}_{v_0}$ un idéal premier de K au-dessus de p et soit $D_{\mathfrak{p}_0}$ son groupe de décomposition. Les places $v \mid p$ conjuguées de v_0 correspondent aux $(G : D_{\mathfrak{p}_0})$ idéaux premiers distincts $\mathfrak{p}_v := \mathfrak{p}_0^{\sigma_v}$, où $(\sigma_v)_{v\mid p}$ est un système exact de plongements représentant $G/D_{\mathfrak{p}_0}$.

On considère le $\mathbb{Q}_p[G]$-module $\prod_{v\mid p} K_v$ où $K_v = \sigma_v(K)\,\mathbb{Q}_p$ est le complété en v de K ; comme $K/\mathbb{Q}$ est Galoisienne, $K_v/\mathbb{Q}_p$ est indépendante de $v \mid p$ mais la notation K_v rappelle que cette extension locale est *munie* du plongement $\sigma_v : K \to K_v \subset \mathbb{C}_p$, ce qui permet le plongement diagonal d'image dense : $i_p = (\sigma_v)_{v\mid p} : K \to \prod_{v\mid p} K_v$ où $i_p(x) = (\sigma_v(x))_{v\mid p}$, et qui fait que $K \otimes \mathbb{Q}_p \simeq \prod_{v\mid p} K_v \simeq \mathbb{Q}_p[G]$ (théorie semi-locale). Par abus, si $x \in K$, on écrira $x \in \prod_{v\mid p} K_v$, i_p étant sous-entendue.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

2.1.1 Logarithme p-adique sur $K^\times$

Le logarithme p-adique $\log_p : K^\times \to K\mathbb{Q}_p$ est défini sur l'ensemble des $1 + px$, $x \in Z_{K,(p)}$, par la série usuelle ($p > 2$) :

$$\log_p(1 + p\,x) = \sum_{i\geq 1}(-1)^{i+1}\frac{(px)^i}{i} \equiv px \pmod{p^2}.$$

Dans le cas de $\gamma \in K^\times$, γ étranger à p, on utilise la relation fonctionnelle :

$$\log_p(\gamma) = \frac{1}{p^{n_p}-1}\log_p(\gamma^{p^{n_p}-1}) = \frac{1}{p^{n_p}-1}\log_p(1 + p\,\alpha_p(\gamma)) \equiv -p\,\alpha_p(\gamma) \pmod{p^2}.$$

Plus généralement, cette fonction $\log_p$, vue modulo p^{N+1}, $N \geq 1$, est représentée par des éléments de $Z_{K,(p)}$ et est un homomorphisme de G-modules pour la loi définie pour tout $\sigma \in G$ par $\sigma\big(\log_p(\gamma) \pmod{p^{N+1}}\big) := \log_p(\gamma^\sigma) \pmod{p^{N+1}}$, en considérant la congruence (où N' est fonction évidente de N) :

$$\sigma\big(\log_p(\gamma) \pmod{p^{N+1}}\big) \equiv \frac{1}{p^{n_p}-1}\sum_{1\leq i\leq N'}(-1)^{i+1}\frac{(p\,\alpha_p(\gamma)^\sigma)^i}{i} \pmod{p^{N+1}},$$

définissant un élément de $Z_{K,(p)}$ qui approche $\log_p(\gamma^\sigma)$ modulo p^{N+1}.

2.1.2 Rang p-adique

Soit $\eta \in K^\times$ et soit F le $\mathbb{Z}[G]$-module engendré par η. Soit

$$\mathrm{Log}_p := \log_p \circ i_p = (\sigma_v)_{v|p} \circ \log_p$$

l'homomorphisme de G-modules défini sur $K^\times$ par

$$\mathrm{Log}_p(\eta) = \big(\log_p(\eta^{\sigma_v})\big)_{v|p} \in \prod_{v|p} K_v.$$

On appelle rang p-adique de F, l'entier $\mathrm{rg}_p(F) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p\,\mathrm{Log}_p(F))$.

L'utilisation de Log_p est une simple commodité car, par conjuguaisons par les éléments de G, la connaissance de $\log_p$ entraîne celle de Log_p et inversement par projection $\prod_{v|p} K_v \to K_v$.

Pour faire le lien avec le concept de régulateur p-adique, établissons les résultats techniques suivants.

Lemme 2.1 *Soit p premier impair non ramifié dans $K/\mathbb{Q}$ et soit $\lambda \in Z_{K,(p)}$. Si $\lambda \notin pZ_{K,(p)}$, il existe $u \in K^\times$, étranger à p, tel que* $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) \not\equiv 0 \pmod{p}$.

Démonstration Pour tout $u \in K^\times$, étranger à p, considérons le plongement diagonal de λu dans $\prod_{v|p} K_v$, et soient Tr_v les traces locales $\mathrm{Tr}_{K_v/\mathbb{Q}_p}$. On a

$$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v|p}\mathrm{Tr}_v\big(\sigma_v(\lambda u)\big).$$

Par hypothèse, il existe un ensemble non vide Σ de places $v \mid p$ telles que $\sigma_v(\lambda)$ (donc $\sigma_v(\lambda u) = \sigma_v(\lambda)\,\sigma_v(u)$ pour tout u étranger à p) est une unité de K_v. Pour $v_1 \in \Sigma$, on

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

écrit

$$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v\mid p, v\neq v_1} \mathrm{Tr}_v\big(\sigma_v(\lambda u)\big) + \mathrm{Tr}_{v_1}\big(\sigma_{v_1}(\lambda u)\big) =: a + \mathrm{Tr}_{v_1}\big(\sigma_{v_1}(\lambda u)\big).$$

Comme p est non ramifié dans $K/\mathbb{Q}$, les traces résiduelles en p sont surjectives et puisque $\sigma_{v_1}(\lambda u)$ est une unité, il suffit de prendre $u \equiv 1 \pmod{\prod_{v, v\neq v_1} \mathfrak{p}_v}$ (auquel cas $a \in \mathbb{Z}_p \pmod p$ ne dépend plus de u) et $u \equiv u_1 \pmod{\mathfrak{p}_{v_1}}$ convenable tel que, par exemple, $\mathrm{Tr}_{v_1}\big(\sigma_{v_1}(\lambda u)\big) \equiv 1 - a \pmod p$ si $a \not\equiv 1 \pmod p$ (resp. $1 \pmod p$ si $a \equiv 1 \pmod p$). D'où $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) \equiv 1$ (resp. 2) $\pmod p$.[1] ∎

Le lemme suivant, valable pour tout $p > 2$ étranger à η, nous sera particulièrement utile (d'après [Wa, §5.5 et proof of Theorem 5.31]).

Lemme 2.2 *Soit $\eta \in K^\times$ et soient $\lambda(\sigma)$, $\sigma \in G$, des coefficients p-entiers de $K\mathbb{Q}_p$, non tous divisibles par p. On suppose que l'on a la relation de dépendance modulo p^{N+1}, $N \geq 1$, des vecteurs $\ell_\sigma := (\ldots, \log_p(\eta^{\tau\sigma^{-1}}), \ldots)_\tau$:*

$$\sum_{\sigma\in G} \lambda(\sigma) \log_p(\eta^{\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$$

pour tout $\tau \in G$. Alors il existe des coefficients $\lambda'(\sigma) \in \mathbb{Z}_{(p)}$, non tous divisibles par p, tels que l'on ait la relation $\sum_{\sigma\in G} \lambda'(\sigma) \log_p(\eta^{\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$ pour tout $\tau \in G$. Il en résulte la relation $\sum_{\sigma\in G} \lambda'(\sigma)\alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod p$.

Démonstration On peut toujours, modulo p^{N+1}, supposer que $\lambda(\sigma) \in Z_{K,(p)}$ pour tout $\sigma \in G$. Ici les $\log_p(\eta^{\tau\sigma^{-1}})$ sont aussi représentés modulo p^{N+1} par des éléments de $Z_{K,(p)}$ et l'algèbre linéaire correspondante est *a priori* sur le corps K.

On se ramène (par exemple) à $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda(1)) \equiv 1 \pmod p$ en multipliant la congruence par $u \in K^\times$ étranger à p convenable (Lemme 2.1). Par conjugaison par $v \in G$ on obtient $\sum_{\sigma\in G} \lambda(\sigma)^v \log_p(\eta^{v\tau\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$ pour tout $\tau \in G$, équivalent à $\sum_{\sigma\in G} \lambda(\sigma)^v \log_p(\eta^{s\,\sigma^{-1}}) \equiv 0 \pmod{p^{N+1}}$ pour tout $s \in G$.

En prenant la trace dans $K/\mathbb{Q}$ des coefficients (sommation sur v), on obtient des $\lambda'(\sigma)$ rationnels p-entiers pour tout $\sigma \in G$, avec $\lambda'(1) \equiv 1 \pmod p$. ∎

On peut donc supposer que de telles relations de dépendance linéaire modulo $p^{N+1}Z_K\mathbb{Z}_p$, $N \geq 1$, sont à coefficients dans $\mathbb{Z}_{(p)}$, car les deux notions de rang coïncident. En prenant la limite sur N, on passe de l'anneau complet $Z_K\mathbb{Z}_p$ à $\mathbb{Z}_p$.

2.1.3 Régulateurs

Puisque $\mathbb{Q}_p \mathrm{Log}_p(F)$ est le $\mathbb{Q}_p[G]$-module engendré par $\mathrm{Log}_p(\eta)$ et comme $\prod_{v\mid p} K_v$ est la représentation de G induite par la représentation K_{v_0} du groupe de décomposition $D_{\mathfrak{p}_0}$, le rang p-adique $r_p(F)$ de F est égal au $\mathbb{Q}_p$-rang du système de vecteurs $(\ldots, \log_p(\eta^{\tau\sigma^{-1}}), \ldots)_\tau$, $\sigma \in G$, donc au rang (au sens habituel d'après les lemmes) du

[1] Pour $p = 2$, $K = \mathbb{Q}(\sqrt{17})$, $\lambda = 1 + 2\sqrt{17}$, il n'y a pas de solution u étranger à 2.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

régulateur p-adique classique $\mathcal{R}_p(\eta)$ (ou déterminant de Frobenius) de η :

$$\mathcal{R}_p(\eta) := \mathrm{Frob}^G(\log_p(\eta)) := \mathrm{dét}\big(\log_p(\eta^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G}.$$

Le $\mathbb{Z}[G]$-module F est monogène au sens rappelé dans [J, §1] ou [Gr1, III.3.1.2 (ii)], auquel cas la conjecture de Jaulent [J, §2], affirme que le rang p-adique $\mathrm{rg}_p(F)$ de F est égal à son $\mathbb{Z}$-rang $\mathrm{rg}(F) := \dim_{\mathbb{Q}}(F\otimes\mathbb{Q})$ (c'est le prolongement naturel de la conjecture de Leopoldt sur le groupe des unités de K).

On notera d'abord que tout mineur d'ordre r est de façon canonique divisible par p^r puisque l'on a $\log_p(\eta) \equiv -p\alpha_p(\eta) \pmod{p^2}$ dans $Z_{K,(p)}$.

D'où les définitions suivantes.

Définitions 2.3 (i) On considère (pour $p > 2$, non ramifié, étranger à η) le déterminant $\mathrm{Reg}_p^G(\eta) := \mathrm{Frob}^G\big(\frac{-1}{p}\log_p(\eta)\big) := \mathrm{dét}\big(\frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G}$, à coefficients entiers de $K\mathbb{Q}_p$. Ce déterminant de Frobenius est appelé dans tout l'article le *régulateur p-adique normalisé de η*. On a $\mathrm{Reg}_p^G(\eta) \equiv \Delta_p^G(\eta) \pmod{p}$, où

$$\Delta_p^G(\eta) := \mathrm{Frob}^G(\alpha_p(\eta)) = \mathrm{dét}\big(\alpha_p(\eta)^{\tau\sigma^{-1}}\big)_{\sigma,\tau\in G}$$

est appelé le régulateur (normalisé) local de η (*cf.* §2.3).

(ii) Pour K Galoisien réel, le régulateur p-adique usuel $\mathcal{R}_p(K)$ est donné par un mineur d'ordre $n-1$ de $\mathrm{Frob}^G(\log_p(\varepsilon)) = \mathrm{dét}\big(\log_p(\varepsilon^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G}$, où ε est une unité de Minkowski convenable, et l'entier p-adique

$$p^{1-n}\mathcal{R}_p(K) = \mathrm{dét}\Big(\frac{-1}{p}\log_p(\varepsilon^{\tau\sigma^{-1}})\Big)_{\sigma\neq1,\tau\neq1}$$

est appelé le régulateur p-adique normalisé de K.

D'après le Lemme 2.2 et après division par p des logarithmes, on se ramène à des raisonnements d'algèbre linéaire sur $\mathbb{Z}/p^N\mathbb{Z}$, $N \geq 1$; en particulier, $\mathrm{rg}_p(F)$ est le $\mathbb{Z}/p^N\mathbb{Z}$-rang de la matrice $\big(\frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}}) \pmod{p^N}\big)_{\sigma,\tau\in G}$, N assez grand.

Si un mineur M d'ordre $\mathrm{rg}(F)$ est non nul modulo p^N, alors il donne $\mathrm{rg}_p(F)$, et c'est le point de vue pratique choisi que nous limiterons à $N = 1$, donc aux $\alpha_p(\eta)$ modulo p ; dans ce cas, $\mathrm{rg}_p(F)$ est supérieur ou égal au $\mathbb{Z}/p\mathbb{Z}$-rang de la matrice

$$\big(\alpha_p(\eta)^{\tau\sigma^{-1}} \pmod{p}\big)_{\sigma,\tau\in G}.$$

Si $\mathrm{rg}(F) = n$, alors conjecturalement, $\mathrm{dét}\big(\frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G} \sim p^e$, $e \geq 0$.

2.1.4 Forme forte de la conjecture de Leopoldt–Jaulent

Le point de vue local précédent (pour tout p sauf un nombre fini) peut s'analyser de la façon suivante.

(a) *Analyse locale.* On ne fait aucune hypothèse sur $\mathrm{rg}(F)$. Si l'on a dans F la relation $\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)} = \zeta$ (racine de l'unité), $\lambda(\sigma) \in \mathbb{Z}$ non tous nuls, alors pour tout p étranger à η on a $\sum_{\sigma\in G}\lambda(\sigma)\log_p(\eta^{\sigma^{-1}}) = 0$. Ces relations globales se transmettent

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

en les relations locales plus faibles $\sum_{\sigma\in G}\lambda(\sigma)\,\alpha_p(\eta)^{\sigma^{-1}}\equiv 0\pmod p$; elles sont dites triviales (elles ne sont pas dûes à une circonstance numérique avec des coefficients dépendant du p considéré, mais à l'existence d'une relation globale non triviale dans F donnée par des $\lambda(\sigma)\in\mathbb{Z}$).

Inversement, si l'on a, pour des entiers $\lambda(\sigma)\in\mathbb{Z}$ fixés non tous nuls, la famille de conditions locales (pour tout p sauf un nombre fini) :

$$(*)\qquad \Big(\sum_{\sigma\in G}\lambda(\sigma)\,\alpha_p(\eta)^{\sigma^{-1}}\equiv 0\pmod p\Big)_p,$$

la question est de savoir si elle est globalisable sous la forme $\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)}=\zeta$. Supposons ne disposer que des congruences $\sum_{\sigma\in G}\lambda(\sigma)\,\alpha_p(\eta)^{\sigma^{-1}}\equiv 0\pmod p$ pour tout p sauf un nombre fini, avec des $\lambda(\sigma)\in\mathbb{Z}$ non tous nuls indépendants de p.

Soit $\eta_0:=\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)}\in F$. Alors $\log_p(\eta_0)\equiv 0\pmod{p^2}$ (*i.e.*, $\mathrm{Log}_p(\eta_0)\equiv 0\pmod{p^2}$) et η_0 est, dans $\prod_{v|p}K_v^\times$, de la forme $\xi\,(1+\beta\,p)^p$, β p-entier de $\prod_{v|p}K_v$ et ξ de torsion d'ordre étranger à p (p assez grand). Donc $\eta_0\in\prod_{v|p}K_v^{\times p}$ pour presque tout p. Conjecturalement η_0 est une racine de l'unité de K (Conjecture 8.5).

(b) *Analyse globale.* Par comparaison, supposons que l'on ait, dans un cadre limite projective, des coefficients $\widehat{\lambda}(\sigma)\in\widehat{\mathbb{Z}}=\prod_p\mathbb{Z}_p$, tels que

$$\sum_{\sigma\in G}\widehat{\lambda}_p(\sigma)\mathrm{Log}_p(\eta^{\sigma^{-1}})=0,$$

pour tout p étranger à η, où pour tout $\sigma\in G$, $\widehat{\lambda}_p(\sigma)$ est la p-composante de $\widehat{\lambda}(\sigma)$. Soit $i:=(i_v)_{v,v(\eta)=0}$ le plongement diagonal $F\otimes\widehat{\mathbb{Z}}\to\widehat{U}$, où l'on a posé

$$\widehat{U}=\prod_{p,(p,\eta)=1}\Big(\prod_{v|p}U_v^1\times\prod_{v\nmid p,v(\eta)=0}\mu_p(K_v)\Big),$$

avec des notations évidentes où, pour $v\mid p$, $U_v^1=\mu_p(K_v)\times U'$, où U' est $\mathbb{Z}_p$-libre.

On pose $\widehat{\eta}_0:=\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\widehat{\lambda}(\sigma)}\in F\otimes\widehat{\mathbb{Z}}$ et on désigne par $\widehat{\eta}_{0,p}=\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\widehat{\lambda}_p(\sigma)}$ la p-composante de $\widehat{\eta}_0$ (p étranger à η).

Comme $\mathrm{Log}_p(\widehat{\eta}_{0,p})=0$ pour tout p étranger à η, on a pour toute place v de K étrangère à η, $i_v(\widehat{\eta}_0)=\xi_v$, où en général ξ_v est une racine de l'unité d'ordre diviseur de $\ell^{n_\ell}-1$, où ℓ est la caractéristique résiduelle de v (les places $v\mid p$ de K telles que ξ_v est d'ordre divisible par p sont en nombre fini). On peut donc écrire

$$i(\widehat{\eta}_0)\in i(F\otimes\widehat{\mathbb{Z}})\cap\prod_{p,(p,\eta)=1}\Big(\prod_{v,v(\eta)=0}\mu_p(K_v)\Big).$$

En utilisant l'analogue pour F de la caractérisation locale–globale de la conjecture p-adique de Leopoldt–Jaulent ([J, § 2], voir aussi [Gr1, III.3.6.6] dans le cas des unités), on peut affirmer (sous cette conjecture, même raisonnement) que l'on a

$$i(F\otimes\widehat{\mathbb{Z}})\cap\prod_{p,(p,\eta)=1}\Big(\prod_{v,v(\eta)=0}\mu_p(K_v)\Big)=i(\mu(K)).$$

On en déduit que $\widehat{\eta}_{0,p}$ est une racine de l'unité $\zeta_p\in K$ pour tout p étranger à η. Si l'on suppose de plus que $\widehat{\lambda}_p(\sigma)\equiv\lambda(\sigma)\pmod p$ pour tout $\sigma\in G$ et tout p étranger à η où les $\lambda(\sigma)$ sont des entiers rationnels donnés, alors l'élément η_0 de F défini par $\eta_0:=\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)}$ est égal à $\widehat{\eta}_{0,p}$ à une puissance p-ième locale en p près. Donc

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$\eta_0\zeta_p^{-1} \in \prod_{v|p} K_v^{\times p}$; on obtient la situation du (a) puisque $\zeta_p \neq 1$ pour un nombre fini de p, et pour p assez grand il y a bien coïncidence.

On peut donc voir notre démarche comme un affaiblissement très important de ce contexte p-adique classique concernant la conjecture de Leopoldt–Jaulent pour tout premier p. Mais en contrepartie, pour avoir des informations non vides de type p-adique, on a dû supposer l'existence de la famille d'entiers rationnels (non tous nuls) $(\lambda(\sigma))_{\sigma\in G}$ vérifiant la relation $(*)$.

2.1.5 Programme d'étude général

Notre objectif, en lien avec les commentaires p-adiques précédents, est de voir avec quelle probabilité (*a priori* très faible) le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ de η (η fixé) est divisible par p ($p \to \infty$).

Le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ se factorise en produit de puissances de χ-régulateurs $\mathrm{Reg}_p^\chi(\eta)$ (pour les caractères rationnels irréductibles χ de G). Cette factorisation ne dépend pas de p. Par contre on peut ensuite factoriser $\mathrm{Reg}_p^\chi(\eta)$ en produit de θ-composantes $\mathrm{Reg}_p^\theta(\eta)$ (pour les caractères p-adiques irréductibles $\theta \,|\, \chi$), cette factorisation dépendant du degré résiduel de p dans le corps des valeurs des caractères absolument irréductibles $\phi \,|\, \chi$ de G. On aura ensuite la congruence $\mathrm{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p}$ où le θ-régulateur local $\Delta_p^\theta(\eta)$ (défini modulo p) est la θ-composante de $\Delta_p^G(\eta) = \mathrm{Frob}^G(\alpha_p(\eta))$ (*cf.* § 2.3).

On en déduira une étude probabiliste en vue d'appliquer le principe heuristique de Borel–Cantelli.

Remarque 2.4 Le Lemme 3.8 permet de se ramener (modulo $\mathbb{Q}^\times$) à $\eta \in Z_K$, ce que l'on suppose dans les études numériques et Diophantiennes. Lorsque η entier est fixé ou varie dans un petit voisinage numérique *(au sens Archimédien et non p-adique)* et lorsque $p \to \infty$, nous parlerons de *probabilité*, par exemple, $\mathrm{Prob}\big(\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod{p}\big)$. Par contre lorsque p est fixé et η est la variable (modulo p^2 dans notre étude), la probabilité coïncide avec la densité des $\eta \in K^\times$ étrangers à p vérifiant la propriété.

Il est clair que les densités sont canoniques et se déterminent via des calculs algébriques. Comme les *probabilités* sont liées aux *densités*, on peut confondre les deux notions dès lors que celles-ci sont au plus $O(1)/p^2$, et donc exclues. Par contre, dans le cas de $O(1)/p$, la distinction est nécessaire. L'idée (développée dans [Gr2] pour les quotients de Fermat) est que conjecturalement, lorsque η est fixé, ces *probabilités* sont inférieures aux *densités* lorsque $p \to \infty$ et que, sous l'existence d'une loi binomiale pour $\mathrm{Prob}\big(\Delta_p^\theta(z) \equiv 0 \pmod{p}\big)$ (z parcourant un ensemble convenable de résidus modulo p), cette probabilité est $O(1)/p^{\log_2(p)/\log(c_0(\eta))-O(1)}$ au lieu de $O(1)/p$, où $c_0(\eta) = \max_{v\in G}(|\eta^v|)$, suggérant la finitude du nombre de cas (Théorème 1.1).

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

2.2 Représentations et déterminants de groupes (ou de Frobenius)

Nous ne faisons aucune hypothèse sur le groupe G ; à cette fin nous commençons par un rappel général en termes de représentations. Pour un exposé sur les représentations et les caractères, voir [Se1] pour le seul cas Abélien, voir [Wa, C].

2.2.1 Notations générales

En tant que représentation régulière, on a l'isomorphisme $\mathbb{C}[G] \simeq \bigoplus_\rho \deg(\rho).V_\rho$, où (ρ, V_ρ) décrit l'ensemble des représentations absolument irréductibles de G et où $\deg(\rho)$ est le degré ($\mathbb{C}$-dimension de V_ρ).

On désigne par ϕ le caractère de ρ ; par conséquent, $\deg(\rho) = \phi(1)$. Nous convenons d'indexer les objets dépendant de ρ par la lettre ϕ, *e.g.*, V_ϕ, et de ne conserver $\rho = \rho_\phi$ qu'en tant qu'homomorphisme de G dans $\mathrm{End}(V_\phi)$.

Comme algèbre d'endomorphismes $E \in \mathbb{C}[G]$, agissant sur la base des $v \in G$ par multiplication $v \mapsto E.v$, on a l'isomorphisme $\mathbb{C}[G] \simeq \bigoplus_\phi \mathrm{End}(V_\phi)$ avec $\mathrm{End}(V_\phi) \simeq e_\phi \mathbb{C}[G]$ où les $e_\phi = \frac{\phi(1)}{|G|} \sum_{v\in G} \phi(v^{-1})v$ sont les idempotents centraux orthogonaux de $\mathbb{C}[G]$. Pour la décomposition de $e_\phi\mathbb{C}[G]$ en somme directe de $\phi(1)$ représentations irréductibles isomorphes à V_ϕ, on utilise les projecteurs issus d'une représentation matricielle $M(\rho_\phi(v)) = \big(a_{ij}^\phi(v)\big)_{i,j}$ [Se1, §I.2.7] :

$$\pi_i^\phi = \frac{\phi(1)}{n} \sum_{v\in G} a_{ii}^\phi(v^{-1})v, \quad i = 1, \dots, \phi(1),$$

formant un système d'idempotents orthogonaux (non centraux) tels que $e_\phi = \sum_i \pi_i^\phi$.

2.2.2 Rappels sur les déterminants de groupes (d'après [C])

Soit G un groupe fini et soit $\mathrm{Frob}^G(X) = \mathrm{dét}(X_{\tau\sigma^{-1}})_{\sigma,\tau\in G}$ le déterminant du groupe G, ou déterminant de Frobenius, en les indéterminées $X := (X_v)_{v\in G}$. On a alors la formule

$$\mathrm{Frob}^G(X) = \prod_\phi \mathrm{dét}\Big(\sum_{v\in G} X_v \rho_\phi(v^{-1})\Big)^{\phi(1)}.$$

Il en résulte l'existence de polynômes homogènes $P^\phi(X)$, de degrés $\phi(1)$ tels que $\mathrm{Frob}^G(X) = \prod_\phi P^\phi(X)^{\phi(1)}$.

La spécialisation $X_v \mapsto \frac{-1}{p}\log_p(\eta^v)$ conduit (Définitions 2.3) à

$$\mathrm{Reg}_p^G(\eta) := \mathrm{Frob}^G\Big(\frac{-1}{p}\log_p(\eta)\Big) = \prod_\phi \mathrm{dét}\Big(\sum_{v\in G} \frac{-1}{p}\log_p(\eta^v)\rho_\phi(v^{-1})\Big)^{\phi(1)},$$

et à partir de

$$\mathrm{Reg}_p^\phi(\eta) := P^\phi\Big(\dots, \frac{-1}{p}\log_p(\eta^v), \dots\Big) = \mathrm{dét}\Big(\sum_{v\in G} \frac{-1}{p}\log_p(\eta^v)\,\rho_\phi(v^{-1})\Big),$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

on regroupe en produits partiels associés aux caractères χ, θ, irréductibles sur $\mathbb{Q}$, $\mathbb{Q}_p$, respectivement,

$$\mathrm{Reg}_p^{\chi}(\eta) = \prod_{\phi|\chi} \mathrm{Reg}_p^{\phi}(\eta) \quad \text{et} \quad \mathrm{Reg}_p^{\theta}(\eta) = \prod_{\phi|\theta} \mathrm{Reg}_p^{\phi}(\eta).$$

2.2.3 Calcul pratique des $P^{\phi}(X)$

Les polynômes $P^{\phi}(X)$ sont obtenus de la façon suivante : à partir de l'espace vectoriel $V = \mathbb{C}[G]$ (muni de la base des $v \in G$), on considère l'endomorphisme de $V[X]$ défini par $L(X) = \sum_{v\in G} X_v v^{-1}$. Il est tel que

$$\Big(\sum_{v\in G} X_v v^{-1}\Big).\tau = \sum_{v\in G} X_v v^{-1}\tau = \sum_{\sigma\in G} X_{\tau\sigma^{-1}}\sigma, \quad \forall \tau \in G.$$

Donc le déterminant de cet endomorphisme dans la base des $\tau \in G$ est le déterminant de Frobenius (défini au signe près).

Soit (ρ_ϕ, V_ϕ) la famille des représentations absolument irreductibles non isomorphes. On prendra pour $\mathrm{End}(V_\phi)$ la composante $e_\phi \mathbb{C}[G]$ associée au caractère ϕ.

On utilise l'isomorphisme d'algèbres $\widetilde{\rho}\colon V \to \prod_\phi \mathrm{End}(V_\phi)$ défini par

$$\sum_{v\in G} a(v)\, v^{-1} \longmapsto \Big(\sum_{v\in G} a(v)\, \rho_\phi(v^{-1})\Big)_\phi,$$

où $\rho_\phi(v^{-1}) = e_\phi v^{-1}$ dans l'identification précédente. D'après le théorème de Maschke on a, au niveau de l'endomorphisme $L(X)$,

$$\det_V(L(X)) = \prod_\phi \Big(\det_{V_\phi}(L^\phi(X))\Big)^{\phi(1)},$$

où $L^\phi(X) = \sum_{v\in G} X_v\, \rho_\phi(v^{-1}) \in \mathrm{End}(V_\phi[X])$. On pose $P^\phi(X) := \det_{V_\phi}(L^\phi(X))$.

Avec une réalisation matricielle $M(\rho_\phi(v)) = \big(a_{ij}^{\phi}(v)\big)_{i,j}$ des $\rho_\phi(v)$, la matrice associée à $L^\phi(X)$ est $M^\phi(X) = \big(\sum_{v\in G} a_{ij}^{\phi}(v^{-1})X_v\big)_{i,j}$, de déterminant $P^\phi(X)$.

Soit g le plus petit commun multiple des ordres des éléments de G. On sait que les représentations sont réalisables sur le corps $C_g = \mathbb{Q}(\mu_g)$ des racines g-ièmes de l'unité [Se1, §12.3].

On pourra donc toujours supposer que les $a_{ij}^{\phi}(v)$ sont des nombres algébriques p-entiers pour tout p assez grand, *i.e.*, $P^\phi(X) \in Z_{C_g,(p)}[X]$ pour tout ϕ.

Soit $\Gamma := \mathrm{Gal}(C_g/\mathbb{Q})$ (commutatif). Etant donné une représentation absolument irréductible $\rho_\phi\colon G \mapsto \mathrm{End}_{C_g}(V_\phi)$, on définit ses conjuguées de façon Galoisienne, de sorte que pour tout $s \in \Gamma$, ρ_ϕ^s est la représentation $G \mapsto \mathrm{End}_{C_g}(V_{\phi^s}) \simeq e_{\phi^s} C_g[G]$ de caractère ϕ^s défini par $\phi^s(v) = (\phi(v))^s$, pour tout $s \in \Gamma$. On a, pour tout $s \in \Gamma$, $\phi^s(v) = \phi(v^{\omega(s)})$, où ω est le caractère $\Gamma \to (\mathbb{Z}/g\mathbb{Z})^\times$ de l'action de Γ sur μ_g. On pose aussi $\phi^t(v) := \phi(v^t)$ pour tout entier t étranger à g (Γ-conjugaison).

2.2.4 Caractères rationnels et p-adiques : Idempotents

On rappelle leur détermination pratique.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

(i) *Caractères rationnels*. On pose, pour ϕ fixé

$$\chi = \sum_{s\in \mathrm{Gal}(C/\mathbb{Q})} \phi^s =: \sum_{\phi|\chi} \phi \quad \text{et} \quad P^\chi(X) := \prod_{s\in \mathrm{Gal}(C/\mathbb{Q})} P^{\phi^s}(X) =: \prod_{\phi|\chi} P^{\phi^s}(X),$$

où $C \subseteq C_g$ est le corps des valeurs de n'importe quel $\mathbb{Q}$-conjugué de ϕ.

(ii) *Caractères p-adiques*. Si $p \nmid g$, on désigne, pour χ fixé, par L et D le corps et le groupe de décomposition de p dans $C/\mathbb{Q}$. On désigne par $f = |D|$ le degré résiduel de p dans $C/\mathbb{Q}$ et par $h = [L:\mathbb{Q}]$ le nombre d'idéaux premiers $\mathfrak{p}$ au-dessus de p dans C (ou L) ; ainsi $[C:\mathbb{Q}] = hf$.

Soit $\phi \,|\, \chi$. On pose, pour tout $v \in G$, $\theta(v) := \sum_{s\in D} \phi^s(v) \in L$ et on pose alors

$$P^\theta(X) := \prod_{s\in D} P^{\phi^s}(X) =: \prod_{\phi|\theta} P^\phi(X).$$

On fixe l'un des h idéaux premiers $\mathfrak{p} \,|\, p$ de L (on dira que θ et $\mathfrak{p}$ sont associés). Comme $L_{\mathfrak{p}^t} = \mathbb{Q}_p$ pour tout $t \in \mathrm{Gal}(C/\mathbb{Q})/D$, on a des congruences de la forme $\theta(v) \equiv r_{\mathfrak{p}^t}(v) \pmod{\mathfrak{p}^t}$ dans L, $r_{\mathfrak{p}^t}(v) \in \mathbb{Z}$; les rationnels $r_{\mathfrak{p}^t}(v)$ dépendent numériquement des images résiduelles en les $\mathfrak{p}^t$ de la trace dans C/L des $\phi(v)$.

Si $\theta = \sum_{s\in D} \phi^s$ et $\mathfrak{p}$ sont associés, les h conjugués de θ sont les $\theta^t = \sum_{s\in D} (\phi^t)^s$ et on a $\theta^t(v) \equiv r_{\mathfrak{p}^{t^{-1}}}(v) \pmod{\mathfrak{p}}$ (ou encore $\theta^{t^{-1}}(v) \equiv r_{\mathfrak{p}^t}(v) \pmod{\mathfrak{p}}$). Comme les θ^t sont vus dans $\mathbb{Z}_p \subset L_\mathfrak{p}$, on écrira par abus $\theta^t(v) \equiv r_{\mathfrak{p}^{t^{-1}}}(v) \pmod{p}$.

Pour p fixé, l'entier f ne dépend que de χ et est appelé le degré résiduel des caractères ϕ, θ, et χ. On a par Γ-conjugaison, $\phi^{p^i}(v) = \phi(v^{p^i}) = \phi(v)^{s_p^i}$, où s_p est l'automorphisme de Frobenius (d'ordre f) dans $C/\mathbb{Q}$.

(iii) *Idempotents*. On pose $e_\chi = \sum_{\phi|\chi} e_\phi$ et $e_\theta = \sum_{\phi|\theta} e_\phi$, d'où $e_\chi = \sum_{\theta|\chi} e_\theta$. Les e_θ (resp. e_χ) forment un système fondamental d'idempotents orthogonaux de $\mathbb{Q}_p[G]$ (resp. $\mathbb{Q}[G]$). On peut remplacer $\mathbb{Q}_p$ (resp. $\mathbb{Q}$) par $\mathbb{Z}_p$ (resp. $\mathbb{Z}_{(p)}$) car $p \nmid g$.

De la formule $P^\phi(X) = \det_{V_\phi}(L^\phi(X))$ on déduit que $P^{\phi^s}(X) = \det_{V_{\phi^s}}(L^{\phi^s}(X))$ où $L^{\phi^s}(X) = \sum_{v\in G} X_v \, \rho_\phi^s(v^{-1})$ qui est donné via les $(a_{ij}^\phi(v^{-1}))^s$, ce qui définit le conjugué par s du polynôme $P^\phi(X)$, *i.e.*, de ses coefficients.

Théorème 2.5 (i) *Pour tout p assez grand, les polynômes $P^\chi(X)$ (resp. $P^\theta(X)$) sont à coefficients p-entiers rationnels (resp. entiers p-adiques).*

(ii) *Pour tout caractère irréductible ϕ, on a $P^\phi(\dots, X_{\pi v}, \dots) = \zeta_\pi \, P^\phi(\dots, X_v, \dots)$ pour tout $\pi \in G$, où ζ_π est une racine de l'unité d'ordre diviseur de g.*

Démonstration (i) Comme $P^\phi(X) \in Z_{C,(p)}[X]$ pour tout $\phi \,|\, \chi$, le polynôme

$$P^\chi(X) = \prod_{s\in \mathrm{Gal}(C/\mathbb{Q})} P^{\phi^s}(X)$$

est invariant par Galois et le premier point est clair. De même

$$P^\theta(X) = \prod_{s\in D} P^{\phi^s}(X) \in L[X] \subset L_\mathfrak{p}[X] = \mathbb{Q}_p[X].$$

(ii) Pour $\pi \in G$ appelons $[\pi]$ l'opérateur défini par $[\pi]X_v = X_{(\pi v)}$ pour tout $v \in G$. Alors $[\pi]$ et $\widetilde{\rho}: V[X] \to \prod_\phi \mathrm{End}(V_\phi[X])$ commutent. De plus, puisque ρ_ϕ est un

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

homomorphisme, on a la formule suivante

$$[\pi]\Big(\sum_{v\in G} X_v\rho_\phi(v^{-1})\Big) = \sum_{v\in G} X_{\pi v}\rho_\phi(v^{-1}) = \Big(\sum_{v\in G} X_v\rho_\phi(v^{-1})\Big)\rho_\phi(\pi).$$

Ensuite, comme le déterminant de $\rho_\phi(\pi) \in \mathrm{End}(V_\phi)$ est celui d'une matrice diagonale dont la diagonale est formée de racines de l'unité, on a

$$\det\Big([\pi]\Big(\sum_{v\in G} X_v\rho_\phi(v^{-1})\Big)\Big) = \zeta_\pi \det\Big(\sum_{v\in G} X_v\rho_\phi(v^{-1})\Big),$$

où ζ_π est d'ordre diviseur de l'ordre de $\rho_\phi(\pi)$ lequel est un diviseur de g. ■

Corollaire 2.6 *Pour tout $\pi \in G$ et tout caractère absolument irréductible ϕ,*

$$P^\phi(\dots, \alpha^{\pi v}, \dots) = \zeta_\pi P^\phi(\dots, \alpha^v, \dots)$$

par spécialisation $X_v \mapsto \alpha^v$, $\alpha \in Z_K$. Par conséquent,

$$P^\chi(\dots, \alpha^{\pi v}, \dots) = \pm P^\chi(\dots, \alpha^v, \dots)$$

pour tout $\pi \in G$.[2] *De même, $P^\theta(\dots, \alpha^{\pi v}, \dots) = \zeta'_\pi P^\theta(\dots, \alpha^v, \dots)$ pour tout $\pi \in G$, où ζ'_π est d'ordre diviseur de p.g.c.d. $(g, p-1)$.*

2.2.5 Déterminants numériques

Dans cette partie, il n'y a pas référence à un premier p et les caractères considérés sont absolument irréductibles ou rationnels. Ce qui précède conduit à définir les χ-déterminants de Frobenius numériques d'un $\alpha \in Z_K$ quelconque (*i.e.*, indépendants de la donnée de $\eta \in K^\times$).

Définition 2.7 Soit G un groupe fini et soit $\mathrm{Frob}^G(X)$ le déterminant de groupe associé. Les χ-déterminants (avec indéterminées et numériques) sont par définition les expressions $\mathrm{Frob}^\chi(X) = \prod_{\phi|\chi} P^\phi(X)$ et $\mathrm{Frob}^\chi(\alpha) = \prod_{\phi|\chi} P^\phi(\dots, \alpha^v, \dots)$, de sorte que $\mathrm{Frob}^G(\alpha) = \prod_\chi \big(\mathrm{Frob}^\chi(\alpha)\big)^{\phi(1)}$ (où $\phi \mid \chi$ pour chaque χ).

Exemple 2.8 Dans le cas du groupe $D_6 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, on a les χ-déterminants numériques suivants :

$$\begin{aligned}
\mathrm{Frob}^1(\alpha) &= \alpha + \alpha^\sigma + \alpha^{\sigma^2} + \alpha^\tau + \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2},\\
\mathrm{Frob}^{\chi_1}(\alpha) &= \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2},\\
\mathrm{Frob}^{\chi_2}(\alpha) &= \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha\\
&\quad + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau.
\end{aligned}$$

Les deux derniers sont de la forme $\mathrm{Frob}'.\sqrt{m}$, $\mathrm{Frob}' \in \mathbb{Q}$, où $k = \mathbb{Q}(\sqrt{m})$ est le sous corps quadratique de K et on néglige le facteur $\sqrt{m}$; mais $\mathrm{Frob}^{\chi_2}(\alpha)$ figure au carré dans le déterminant $\mathrm{Frob}^G(\alpha)$ et le résultat est rationnel, ce qui n'est pas le cas de $\mathrm{Frob}^{\chi_1}(\alpha)$. Ceci est spécifique des seuls caractères quadratiques.

[2] Signe + sauf si $\chi = \phi$ est quadratique et $\phi(\pi) = -1$.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Pour les calculs, on peut revenir aux réalisations matricielles ($C = \mathbb{Q}$, $\phi = \chi_2$) :

$$\rho_\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho_\phi(\sigma) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \rho_\phi(\sigma^2) = \begin{pmatrix} , 0 & 1 \\ -1 & -1 \end{pmatrix}$$
$$\rho_\phi(\tau) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad \rho_\phi(\tau\sigma) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \rho_\phi(\tau\sigma^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

qui conduisent (par spécialisation et en prenant le déterminant) à :

$$\sum_{\nu\in G} X_\nu \rho_\phi(\nu^{-1}) = \begin{pmatrix} X_1 - X_{\sigma^2} + X_\tau - X_{\tau\sigma} & X_\sigma - X_{\sigma^2} - X_{\tau\sigma} + X_{\tau\sigma^2} \\ -X_\sigma + X_{\sigma^2} - X_\tau + X_{\tau\sigma^2} & X_1 - X_\sigma - X_\tau + X_{\tau\sigma} \end{pmatrix},$$
$$\mathrm{Frob}^{\chi_2}(\alpha) = \begin{vmatrix} \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} & \alpha^\sigma - \alpha^{\sigma^2} - \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2} \\ -\alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau + \alpha^{\tau\sigma^2} & \alpha - \alpha^\sigma - \alpha^\tau + \alpha^{\tau\sigma} \end{vmatrix}.$$

Toujours pour le caractère χ_2 (de degré 2) et la représentation $e_{\chi_2}\,\mathbb{Q}[G] \simeq 2\,V_\phi$, il existe deux projecteurs orthogonaux π_1, π_2, de somme $e_{\chi_2} = \frac{1}{3}(2 - \sigma - \sigma^2)$ (§ 2.2.1), ce qui donne ici $\pi_1 = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma)$ et $\pi_2 = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma)$.

2.3 Les θ-régulateurs locaux

Soient $\eta \in K^\times$ et p assez grand.

2.3.1 Généralités

On fixe un entier algébrique $\alpha \in Z_K$ défini par $\alpha \equiv \alpha_p(\eta) \pmod{p}$. On obtient le déterminant à coefficients dans Z_K défini modulo p

$$\Delta_p^G(\eta) := \mathrm{Frob}^G(\alpha) = \det(\alpha^{\tau\sigma^{-1}})_{\sigma,\tau\in G} = \prod_\chi \prod_{\theta|\chi} \prod_{\phi|\theta} P^\phi(\dots, \alpha^\nu, \dots)^{\phi(1)}.$$

Si $\Delta_p^G(\eta) \notin \mathbb{Q}$, on retrouve l'existence d'un facteur $\sqrt{m}$ que l'on sait provenir de la résolvante d'un caractère quadratique de G et que l'on néglige.

Définition 2.9 Pour tout p assez grand et pour chaque caractère $\mathbb{Q}_p$-irréductible θ de G, on appelle θ-régulateur local de η, l'entier p-adique défini par

$$\Delta_p^\theta(\eta) := \prod_{\phi|\theta} P^\phi(\dots, \alpha^\nu, \dots),$$

pour $\alpha \equiv \alpha_p(\eta) := \frac{1}{p}(\eta^{p^{n_p}-1} - 1) \pmod{p}$. Pour $\theta \mid \chi$ (χ fixé), les θ-régulateurs locaux correspondants dépendent de la décomposition de p dans $C/\mathbb{Q}$ et sont au nombre de $h = [C:\mathbb{Q}]/f$, où f est leur degré résiduel (§ 2.2.4 (ii)). Ils ne sont définis que modulo p.

Remarque 2.10 On peut de la même façon écrire (pour p assez grand) que le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ est égal à $\prod_\chi \mathrm{Reg}_p^\chi(\eta)^{\phi(1)} = \prod_\theta \mathrm{Reg}_p^\theta(\eta)^{\phi(1)}$, où $\mathrm{Reg}_p^\theta(\eta) = \prod_{\phi|\theta} P^\phi\big(\dots, \frac{-1}{p}\log_p(\eta^\nu), \dots\big)$. On a alors les congruences

$$\mathrm{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p}.$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Ainsi p divise $\mathrm{Reg}_p^{\theta}(\eta)$ si et seulement si $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$; dans ce cas, il existe $e \geq 1$ tel que $p^{e\phi(1)}$ divise $\mathrm{Reg}_p^{\theta}(\eta)$ où chaque fois $\phi \,|\, \theta$ (§ 2.2.2). On parlera d'extra p-divisibilité si $e \geq 2$.

2.3.2 Remarques particulières

(i) On a $\Delta_p^{\chi}(\eta) := \mathrm{N}_{C/\mathbb{Q}}\big(P^{\phi}(\ldots,\alpha^{v},\ldots)\big) \in \mathbb{Z}$ ($\phi \,|\, \chi$ fixé), avec la convention sur la notation $\mathrm{N}_{C/\mathbb{Q}}$, notamment lorsque K et C ne sont pas linéairement disjoints. On rappelle l'exception χ quadratique.

De même $\Delta_p^{\theta}(\eta) := \mathrm{N}_{\mathfrak{p}}\big(P^{\phi}(\ldots,\alpha^{v},\ldots)\big)$, où pour $\mathfrak{p} \,|\, p$ dans C, associé à θ, $\mathrm{N}_{\mathfrak{p}}$ désigne la norme locale absolue (issue de $\mathrm{N}_{C/L}$) dans le complété de C en $\mathfrak{p}$. On retrouve $\Delta_p^{\chi}(\eta)$ comme produit des normes locales en p correspondantes.

On a les mêmes relations normiques en remplaçant Δ_p par Reg_p et α par $\frac{-1}{p}\log_p(\eta)$.

(ii) Si $H = \{v \in G,\ \phi(v) = \phi(1)\}$ est le noyau de $\phi \,|\, \theta \,|\, \chi$ (qui ne dépend que de χ) et si K' est le sous-corps de K fixe par H, on a $\Delta_p^{\theta}(\eta) = \Delta_p^{\theta'}(\mathrm{N}_{K/K'}(\eta))$ où θ' est le caractère fidèle issu de θ. Quitte à remplacer η par $\eta' := \mathrm{N}_{K/K'}(\eta)$ on peut toujours supposer que θ est un caractère fidèle.

2.3.3 Caractères χ de degré 1, d'ordre 1 ou 2

Soit $\eta \in K^{\times}$ et soit $\alpha \equiv \alpha_p(\eta) \pmod{p}$, $\alpha \in Z_K$.

(i) Si $\chi = \theta = 1$, le θ-régulateur correspond à $\mathrm{N}_{K/\mathbb{Q}}(\eta) = a \in \mathbb{Q}^{\times}$ et est donné par $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, autrement dit $\Delta_p^{1}(\eta) \equiv \frac{-1}{p}\log_p(a) \equiv \frac{1}{p}(a^{p-1}-1) \equiv q_p(a) \pmod{p}$ (quotient de Fermat de a ; pour les propriétés classiques et les utilisations du quotient de Fermat, voir [EM, GM, Gr2, Hat, H-B, KR1, KR2, OS, Si]).

Pour $a = 659$ et $p \leq 10^9$, on ne trouve que les solutions $p = 23, 131, 2221, 9161, 65983$. Voir [Gr4, Programme A-1]. Pour $a = 47$ et $a = 72$, on ne trouve aucune solution pour $p \leq 10^{11}$.

(ii) Si $\chi = \theta$ est quadratique et si $k = \mathbb{Q}(\sqrt{m})$ est le sous-corps quadratique de K fixé par le noyau de χ, on obtient un θ-régulateur qui correspond au cas où $\mathrm{N}_{K/k}(\eta) \in k^{\times} \smallsetminus \mathbb{Q}^{\times}$. Si $\mathrm{Tr}_{K/k}(\alpha) =: u + v\sqrt{m} \in k$, il est donné par

$$\Delta_p^{\theta}(\eta) \equiv (1-\tau)(u + v\sqrt{m}) \equiv 2v\sqrt{m} \pmod{p}.$$

Si K est un corps quadratique réel d'unité fondamentale ε, en raison de la relation de dépendance multiplicative $\varepsilon^{1+\sigma} = \pm 1$, les 1-régulateurs $\Delta_p^{1}(\varepsilon)$ sont trivialement nuls modulo p. Le θ-régulateur pour le caractère quadratique est $\Delta_p^{\theta}(\varepsilon) \equiv 2v\sqrt{m} \pmod{p}$ (calculé via $\varepsilon^{p^{n_p}-1} \equiv 1 + pv\sqrt{m} \pmod{p^2}$).

On calcule le θ-régulateur $\Delta_p^{\theta}(\varepsilon)$ de l'unité fondamentale $\varepsilon = 5 + 2\sqrt{6}$, pour tout $p \leq 10^9$ ($p \neq 2, 3$) (voir [Gr4, Programme A-2] valable pour tout entier quadratique). On ne trouve un θ-régulateur nul modulo p que pour $p = 7, 523$, ce qui constitue une seconde observation sur la rareté du phénomène.

Soit $\eta = 1 + \sqrt{6}$ de norme -5. On a ici $\mathrm{rg}(F) = 2$ (pas de nullités triviales). On vérifie que les quotients de Fermat $\Delta_p^{1}(\eta)$ de -5 sont tous non nuls modulo p dans l'intervalle testé. Les solutions obtenues pour $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$, $\theta \neq 1$, sont

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$p = 11, 37, 163, 4219$. Pour $\eta = 1 + 5\sqrt{-1}$ de norme 26, on trouve pour $\theta \neq 1$ les deux solutions $p = 73, 12021953$. Pour le nombre d'or $\frac{1+\sqrt{5}}{2}$ on ne trouve aucune solution dans l'intervalle testé.

2.3.4 Critère de nullité triviale des χ-régulateurs locaux

Soit $\eta \in K^\times$ et soit F le $\mathbb{Z}[G]$-module engendré par η.

Remarque 2.11 Dans la décomposition $\mathrm{Frob}^G(\alpha) = \prod_\chi \mathrm{Frob}^\chi(\alpha)^{\phi(1)}$, lorsque $\alpha \equiv \alpha_p(\eta) \pmod p$, certains χ-régulateurs locaux $\Delta_p^\chi(\eta)$ sont nuls modulo p dès qu'il existe une relation multiplicative globale non triviale de la forme

$$\prod_{v \in G} (\eta^{v^{-1}})^{\lambda(v)} = 1, \quad \lambda(v) \in \mathbb{Z},$$

qui conduit à $\sum_{v \in G} \lambda(v) \alpha^{v^{-1}} \equiv 0 \pmod p$ pour tout p étranger à η.

Lemme 2.12 *Si l'on a* $\dim_{\mathbb{Q}}((F \otimes \mathbb{Q})^{e_\chi}) < \dim_{\mathbb{Q}}(e_\chi \mathbb{Q}[G]) = [C:\mathbb{Q}]\phi(1)^2$ *(*i.e.*, il existe* $U \in \mathbb{Q}[G]$ *telle que* $\eta^{U_\chi} = 1$*, avec* $U_\chi := e_\chi U \neq 0$*), alors les* χ*-régulateurs locaux* $\Delta_p^\chi(\eta) := \mathrm{Frob}^\chi(\alpha)$ *sont nuls modulo* p *pour tout* p *assez grand (ils sont dits trivialement nuls modulo* p*).*

Ceci entraîne la nullité triviale modulo p de certains $\Delta_p^\theta(\eta)$, $\theta \mid \chi$, à savoir ceux pour lesquels $U_\theta := e_\theta U \not\equiv 0 \pmod p$. Pour la preuve, voir les Lemmes du § 3.2 (critère de nullité modulo p des $\Delta_p^\theta(\eta)$).

Remarques 2.13 (i) Si $\phi(1) = 1$, $\Delta_p^\chi(\eta)$ trivialement nul modulo p équivaut à $\eta^{e_\chi} = 1$, *i.e.*, $U_\chi = e_\chi$, auquel cas $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ trivialement pour tout $\theta \mid \chi$.

(ii) Si $\phi(1) > 1$, $\Delta_p^\chi(\eta)$ est trivialement nul modulo p s'il existe i, $1 \leq i \leq \phi(1)$, tel que l'on ait, dans $F \otimes C$, $\eta^{\pi_i^\phi} = 1$ pour $\phi \mid \chi$ (§2.2.1).

Par exemple, pour $G = D_6$ et $\phi = \chi = \chi_2$, les éléments

$$\pi_1^\phi = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma) \quad \text{et} \quad \pi_2^\phi = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma)$$

sont tels que $e_\chi \pi_i^\phi = \pi_i^\phi$, $i = 1, 2$, $\pi_1^\phi + \pi_2^\phi = e_\chi$, et $\pi_1^\phi \pi_2^\phi = 0$, *cf.* Exemple 2.8.

Ainsi on pourrait avoir la ϕ-relation non triviale $\eta^{U_1} := \eta^{1-\sigma^2+\tau-\tau\sigma} = 1$ tandis que $\eta^{U_2} := \eta^{1-\sigma-\tau+\tau\sigma} \neq 1$, *i.e.*, $\dim_{\mathbb{Q}}(F \otimes \mathbb{Q})^{e_\chi} = 2$ pour $\dim_{\mathbb{Q}}(e_\chi \mathbb{Q}[G]) = 4$). On aurait donc $\eta^{e_\chi \cdot (U_1+U_2)} = \eta^{3e_\chi} = \eta^{3U_2} \neq 1$, or on vérifie que le χ-régulateur $\Delta_p^\chi(\eta)$ est nul modulo p en raison de la première relation.

Le fait de supposer $\mathrm{rg}(F) = n$ évite cet inconvénient. On peut toujours s'y ramener en multipliant η par η' convenable de telle sorte que (avec des notations évidentes) $(FF') \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$ et $F \cap F' = 1$.

(iii) Pour $U \in \mathbb{Z}_{(p)}[G]$, on a $U_\chi = \sum_{\phi \mid \chi} U_\phi$ et $U_\phi = e_\phi U_\chi$. On a $U_\chi \equiv 0 \pmod p$ si et seulement si $U_\phi \equiv 0 \pmod p$ pour au moins un (donc tout) $\phi \mid \chi$ (car les $\phi \mid \chi$ sont conjugués par $\mathrm{Gal}(C/\mathbb{Q})$). Ces congruences (mod p) dans les algèbres de groupes

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

signifient selon les cas $\pmod{p\mathbb{Z}_{(p)}[G]}$ ou $\pmod{pZ_{C,(p)}[G]}$ (anneau des p-entiers du corps des valeurs C des $\phi \,|\, \chi$).

Ceci n'a pas lieu pour $U_\chi = \sum_{\theta|\chi} U_\theta$ et $U_\theta = e_\theta U_\chi$ car $U_\theta \equiv 0 \pmod{p}$ dans $\mathbb{Z}_p[G]$ signifie $U_\theta \equiv 0 \pmod{\mathfrak{p}}$ dans $L[G]$ (pour θ et $\mathfrak{p}$ associés), seulement équivalent à $U_\phi \equiv 0 \pmod{\mathfrak{p}}$ pour tout $\phi \,|\, \theta$ (§2.2.4 (ii)).

Exemples 2.14 (i) $G = C_n$. Soit G cyclique d'ordre n et soit χ d'ordre $d \,|\, n$. Alors les éléments $\eta \in K^\times$ tels que $\eta^{e_\chi} = 1$ correspondent à la nullité triviale modulo p de $\Delta_p^\chi(\eta) = \mathrm{N}_{C/\mathbb{Q}}\big(\sum_{v\in G} \phi(v^{-1})\, \alpha^v\big)$. Pour $n = 3$ (pour lequel $C = \mathbb{Q}(j)$, où $j^3 = 1$, $j \neq 1$), on a les deux idempotents rationnels :

$$e_1 = \frac{1}{3}(1 + \sigma + \sigma^2), \quad e_\chi = \frac{1}{3}(2 - \sigma - \sigma^2).$$

(a) Les éléments $\eta \in K^\times$ tels que $\eta^{e_1} = 1$ (*i.e.*, de norme 1 dans $F \otimes \mathbb{Q}$), correspondent à la nullité triviale de $\Delta_p^1(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2}$.

(b) Les éléments $\eta \in K^\times$ tels que $\eta^{e_\chi} = 1$ ou $\mathrm{N}_{K/\mathbb{Q}}(\eta) = \eta^3$, donc tels que $\eta \in \mathbb{Q}^\times$, correspondent à la nullité triviale de $\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^2\alpha^\sigma + j\alpha^{\sigma^2})$.

(ii) $G = D_6$. Les trois idempotents relatifs au groupe D_6 sont

$$\begin{aligned} e_1 &= \frac{1}{6}(1 + \sigma + \sigma^2 + \tau + \tau\sigma + \tau\sigma^2), \\ e_{\chi_1} &= \frac{1}{6}\big(1 + \sigma + \sigma^2 - \big(\tau + \tau\sigma + \tau\sigma^2\big)\big), \\ e_{\chi_2} &= \frac{1}{6}(2 - \sigma - \sigma^2). \end{aligned}$$

(a) Les η tels que $\eta^{e_1} = 1$ correspondent à la nullité triviale de $\Delta_p^1(\eta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.

(b) Les éléments η tels que $\eta^{e_{\chi_1}} = 1$ sont tels que $\mathrm{N}_{K/k}(\eta) \in \mathbb{Q}^\times$, où k est le sous-corps quadratique de K, et correspondent à la nullité triviale de

$$\Delta_p^{\chi_1}(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} = (1 - \tau)\,\mathrm{Tr}_{K/k}(\alpha).$$

(c) Les éléments η tels que $\eta^{U_{\chi_2}} = 1$ pour $U_{\chi_2} \in e_{\chi_2}\mathbb{Q}[G] \setminus \{0\}$ conduisent à la nullité triviale de

$$\begin{aligned} \Delta_p^{\chi_2}(\eta) = \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha \\ + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau. \end{aligned}$$

3 Relations $\mathbb{F}_p$-linéaires entre les conjugués de α

Soit $\eta \in K^\times$ fixé et soit p assez grand. Soit $\alpha_p(\eta) := \frac{1}{p}(\eta^{p^{n_p}-1} - 1) \in Z_{K,(p)}$. On établira la relation entre la nullité modulo p de certains $\Delta_p^\theta(\eta)$ et l'existence de certaines relations $\mathbb{F}_p$-linéaires entre les conjugués de $\alpha_p(\eta)$ modulo p. On suppose implicitement que $\mathrm{rg}(F) = n$. Etablissons d'abord des généralités élémentaires.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

3.1 $\mathbb{F}_p$-indépendance

Soit $\alpha \in K$ quelconque (donc $\alpha \in Z_{K,(p)}$ pour tout p assez grand). Nous dirons que les α^v sont $\mathbb{F}_p$-indépendants si, pour toute famille de coefficients $u(v) \in \mathbb{Z}_{(p)}$, la congruence $\sum_{v\in G} u(v)\alpha^{v^{-1}} \equiv 0 \pmod{p}$, dans $Z_{K,(p)}$, implique $u(v) \equiv 0 \pmod{p}$ pour tout $v \in G$. On a le résultat suivant où l'on rappelle que $\mathrm{Frob}^G(\alpha) = \mathrm{dét}(\alpha^{\tau\sigma^{-1}})_{\sigma,\tau\in G}$.

Proposition 3.1 *Soit $\alpha \in K$. On suppose p assez grand afin que $\alpha \in Z_{K,(p)}$.*

(i) *Les α^v sont $\mathbb{F}_p$-indépendants si et seulement si α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$.*

(ii) *Les α^v sont $\mathbb{F}_p$-indépendants si et seulement si $\mathrm{Frob}^G(\alpha)$ est étranger à p.*

Démonstration (i) Si α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$, toute congruence

$$\sum_{v\in G} u(v)\alpha^{v^{-1}} \equiv 0 \pmod{p},$$

$u(v) \in \mathbb{Z}_{(p)}$, conduit à $u(v) \equiv 0 \pmod{p}$, $\forall v \in G$.

Supposons alors que les α^v soient $\mathbb{F}_p$-indépendants et qu'il existe une relation non triviale de dépendance $\mathbb{Q}$-linéaire entre les conjugués de α. Il en résulte une relation de la forme $\sum_{v\in G} r(v)\alpha^{v^{-1}} = 0$ avec des entiers $r(v)$ non tous nuls, tels que $\mathrm{p.g.c.d.}(r(v))_v = 1$, d'où $r(v) \equiv 0 \pmod{p}$ pour tout $v \in G$ (absurde). Par conséquent α est déjà une $\mathbb{Q}$-base normale de K. Si $\beta \in Z_{K,(p)} \setminus \{0\}$, il existe des $r(v) \in \mathbb{Z}$, non tous nuls, et un entier d étranger à $\mathrm{p.g.c.d.}(r(v))_v$ tels que $d\beta = \sum_{v\in G} r(v)\alpha^{v^{-1}}$. On a $p \nmid d$ sinon tous les $r(v)$ sont divisibles par p. Ainsi α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$.

(ii) Supposons que les α^v soient $\mathbb{F}_p$-indépendants ; comme $\alpha = \frac{1}{d}\beta$, $\beta \in Z_K \setminus pZ_K$, $d \in \mathbb{Z} \setminus p\mathbb{Z}$, on peut se ramener au cas d'un α entier. Comme p est assez grand, il ne divise pas le discriminant de $K/\mathbb{Q}$, et le discriminant de la $\mathbb{Z}_{(p)}$-base normale α, de $Z_{K,(p)}$, est étranger à p (en effet, le conducteur $\mathfrak{f} \in \mathbb{Z}$ tel que $\mathfrak{f}Z_K \subseteq \bigoplus_v \mathbb{Z}\alpha^v$ est non divisible par p et les deux discriminants coïncident à une unité p-adique près). Or le discriminant de la base normale α est le carré du déterminant de Frobenius $\mathrm{Frob}^G(\alpha) = \mathrm{dét}(\alpha^{\tau\sigma^{-1}})_{\sigma,\tau\in G}$.

Supposons $\mathrm{Frob}^G(\alpha)$ étranger à p et supposons qu'il existe des $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, non tous divisibles par p, tels que $\sum_{\sigma\in G} \lambda(\sigma)\alpha^{\sigma^{-1}} \equiv 0 \pmod{p}$. En conjuguant par $\tau \in G$, on obtient une relation $\mathbb{Z}_{(p)}$-linéaire sur les lignes de la forme

$$\sum_{\sigma\in G} \lambda(\sigma)(\dots, \alpha^{\tau\sigma^{-1}}, \dots)_\tau \equiv (\dots, 0, \dots)_\tau \pmod{p},$$

d'où $\mathrm{Frob}^G(\alpha) \equiv 0 \pmod{p}$ (absurde). ∎

Corollaire 3.2 *Soit $\eta \in K^\times$. Si pour p assez grand l'un au moins des θ-régulateurs locaux $\Delta_p^\theta(\eta)$ est nul modulo p, alors les $\alpha_p(\eta)^v$ ne sont pas $\mathbb{F}_p$-indépendants et il existe une relation $\mathbb{F}_p$-linéaire de la forme $\sum_{v\in G} u(v)\alpha_p(\eta)^{v^{-1}} \equiv 0 \pmod{p}$, $u(v) \in \mathbb{Z}_{(p)}$ non tous divisibles par p.*

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

3.2 Critère de nullité modulo p des $\Delta_p^\theta(\eta)$

On se réfère au §2.2.4 utilisant le corps de décomposition L de p dans $C/\mathbb{Q}$ et $D = \mathrm{Gal}(C/L)$. On suppose pour simplifier que $K \cap C = \mathbb{Q}$. On rappelle que $Z_{C,(p)}$ est l'anneau des p-entiers de C.

3.2.1 Principaux lemmes

On fixe $\alpha \equiv \alpha_p(\eta) \pmod{p}$ dans Z_K.

Définitions 3.3 (i) Si $\sum_{v\in G} u(v)\alpha^{v^{-1}} \equiv 0 \pmod{p}$, $u(v) \in \mathbb{Z}_{(p)}$ pour tout $v \in G$, on appelle *relation associée* à α l'élément $U = \sum_{v\in G} u(v)\, v^{-1} \in \mathbb{Z}_{(p)}[G]$ et on définit les ϕ-relations $U_\phi := e_\phi.U \in Z_{C,(p)}[G]$, les θ-relations $U_\theta := e_\theta.U \in Z_{L,(p)}[G]$.

(ii) On désigne par $\mathcal{L}$ le G-module des relations $U \in \mathbb{Z}_{(p)}[G]$ (définies modulo $p\mathbb{Z}_{(p)}[G]$), associées à α. Vu dans $\mathbb{F}_p[G]$, on a $\mathcal{L} = \{0\}$ si et seulement si les α^v sont $\mathbb{F}_p$-indépendants (§3.1) et on a $\mathcal{L} = \mathbb{F}_p[G]$ si et seulement si $\alpha \equiv 0 \pmod{p}$.

(iii) Pour tout caractère p-adique θ, on désigne par $\mathcal{L}^\theta \simeq \delta V_\theta$ la θ-composante $e_\theta\mathcal{L}$, où V_θ (de $\mathbb{F}_p$-dimension $f\phi(1)$) est la représentation irréductible de caractère θ. On a $0 \le \delta \le \phi(1)$.

(iv) Soit $\mathfrak{p} \mid p$ l'idéal premier de L associé à θ. On rappelle que $\theta(v) = \sum_{s\in D} \phi^s(v) \in Z_{L,(p)}$ est défini via $\theta(v) \equiv r_\mathfrak{p}(v) \pmod{\mathfrak{p}}$, $r_\mathfrak{p}(v) \in \mathbb{Z}$; si $U \in \mathbb{Z}_{(p)}[G]$, alors $U_\theta \in Z_{L,(p)}[G]$ est congrue modulo $\mathfrak{p}$ à un élément de $\mathbb{Z}_{(p)}[G]$. On verra U_θ dans $\mathbb{Z}_p[G] \pmod{p}$ ou $Z_{L,(p)}[G] \pmod{\mathfrak{p}}$ selon le contexte (Remarque 2.13).

Soit $U = \sum_{v\in G} u(v)\, v^{-1} \in \mathbb{Z}_{(p)}[G]$. Alors $U_\phi = \sum_{v\in G} u_\phi(v)v^{-1} \in Z_{C,(p)}[G]$, avec $u_\phi(v) = \frac{\phi(1)}{n} \sum_{\tau\in G} \phi(\tau^{-1})u(v\tau)$. On a alors $U_\theta = \sum_{\phi\mid\theta} U_\phi$.

Lemme 3.4 *Si $U = \sum_{v\in G} u(v)v^{-1} \in \mathcal{L}$, alors $U_\phi.\alpha := \sum_{v\in G} u_\phi(v)\,\alpha^{v^{-1}} \equiv 0 \pmod{p}$ pour tout caractère irréductible ϕ.*

Démonstration On a $U_\phi.\alpha = \frac{\phi(1)}{n} \sum_{\tau\in G} \phi(\tau^{-1})(\sum_{\sigma\in G} u(\sigma)\alpha^{\tau\sigma^{-1}}) \equiv 0 \pmod{p}$, par conjugaisons par τ de $\sum_{\sigma\in G} u(\sigma)\alpha^{\sigma^{-1}} \equiv 0 \pmod{p}$. ∎

Lemme 3.5 *Soient $U \in \mathcal{L}$, $\mathfrak{p}$ associé à θ, et $\phi \mid \theta$ tels que $U_\phi \not\equiv 0 \pmod{\mathfrak{p}}$ (condition indépendante du choix de $\phi \mid \theta$). Alors l'endomorphisme $E_\phi := e_\phi \sum_{v\in G} \alpha^v v^{-1}$ de $\mathrm{End}_{KC}(V_\phi)$ est non inversible modulo $\mathfrak{p}$.*

Démonstration Raisonnons par transposition des endomorphismes (ce qui ne change pas les déterminants). On a

$$\begin{aligned} U_\phi.E_\phi &= e_\phi \sum_{v\in G} U_\phi \alpha^v\, v^{-1} = e_\phi \sum_{v\in G} \alpha^v \sum_{\sigma\in G} u_\phi(\sigma)\sigma^{-1}v^{-1} \\ &= e_\phi \sum_{\tau\in G} \Big(\sum_{v\in G} u_\phi(v^{-1}\tau)\, \alpha^v \Big)\, \tau^{-1} = e_\phi \sum_{\tau\in G} (U_\phi.\alpha)^\tau \tau^{-1} \equiv 0 \pmod{p}, \end{aligned}$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

d'après le Lemme 3.4 ci-dessus. ■

Comme E_ϕ est un endomorphisme de V_ϕ sur KC, pour l'idéal premier $\mathfrak{p}\,|\,p$ de C tel que $U_\phi \not\equiv 0 \pmod{\mathfrak{p}}$ il existe un idéal premier $\mathfrak{P}\,|\,\mathfrak{p}$ de KC pour lequel on a $\text{dét}(E_\phi) \equiv 0 \pmod{\mathfrak{P}}$. Mais toute conjugaison par $\tau \in G$ donne

$$E_\phi^\tau = e_\phi \sum_{\nu\in G} \alpha^{\tau\nu}\nu^{-1} = e_\phi \sum_{\nu\in G} \alpha^{\nu}\nu^{-1}.(e_\phi\tau) = E_\phi \circ e_\phi\tau$$

et on obtient $\text{dét}(E_\phi^\tau) = \text{dét}(E_\phi)\,\text{dét}(e_\phi\tau) \equiv 0 \pmod{\mathfrak{P}^\tau}$, d'où

$$\text{dét}(E_\phi) \equiv 0 \pmod{\prod_{\tau\in G} \mathfrak{P}^\tau}$$

puisque les $\text{dét}(e_\phi\tau)$ sont inversibles.

Puisque $\text{dét}(E_\phi) \equiv 0 \pmod{\mathfrak{p}}$ (étendu à KC), il vient $P^\phi(\dots,\alpha^\nu,\dots) \equiv 0 \pmod{\mathfrak{p}}$ qui s'écrit $\Delta_p^\phi(\eta) \equiv 0 \pmod{\mathfrak{p}}$. Comme $\Delta_p^\theta(\eta)$ est la norme locale en $\mathfrak{p}$ de $\Delta_p^\phi(\eta)$, on obtient le corollaire suivant.

Corollaire 3.6 *Si $U_\phi \not\equiv 0 \pmod{\mathfrak{p}}$, on a $\Delta_p^\theta(\eta) \equiv 0 \pmod{\mathfrak{p}^f}$ (ou modulo p^f dans $L_\mathfrak{p} = \mathbb{Q}_p$) pour le caractère p-adique θ (au-dessus de ϕ) associé à $\mathfrak{p}$.*

Lemme 3.7 *Réciproquement, si $E_\phi := e_\phi \sum_{\nu\in G} \alpha^\nu\nu^{-1} \in \text{End}_{KC}(V_\phi)$ est non inversible modulo $\mathfrak{p}$, alors il existe une ϕ-relation non nulle modulo $\mathfrak{p}$ de la forme $W = \sum_{\sigma\in G} w(\sigma)\sigma^{-1} \in e_\phi\, Z_{C,(p)}[G]$, telle que $W.\alpha \equiv 0 \pmod{\mathfrak{p}}$.*

Démonstration Le Lemme 2.2 ramenant à des raisonnements $Z_{C,(p)}$-linéaires, il existe $W \in e_\phi Z_{C,(p)}[G]$ tel que $W \not\equiv 0 \pmod{\mathfrak{p}}$ est dans le noyau du transposé de E_ϕ, ce qui s'écrit $W.E_\phi \equiv 0 \pmod{\mathfrak{P}}$ pour $\mathfrak{P}\,|\,\mathfrak{p}$ dans KC.

La relation $E_\phi^\tau = E_\phi \circ e_\phi\tau$ et le fait que W est à coefficients dans $Z_{C,(p)}$ montrent, par conjugaisons, que la congruence a lieu modulo $\mathfrak{p}$ (étendu).

Posons $W = \sum_{\sigma\in G} w(\sigma)\sigma^{-1}$, $w(\sigma) \in Z_{C,(p)}$ pour tout $\sigma \in G$; cette congruence $W.E_\phi \equiv 0 \pmod{\mathfrak{p}}$ s'écrit successivement (puisque $e_\phi W = W$) :

$$\sum_{\nu\in G}\sum_{\sigma\in G} w(\sigma)\alpha^\nu\sigma^{-1}\nu^{-1} \equiv \sum_{\sigma\in G} w(\sigma) \sum_{t\in G} \alpha^{t^{-1}\sigma^{-1}}\, t \equiv 0 \pmod{\mathfrak{p}},$$
$$\sum_{t\in G}\Big(\sum_{\sigma\in G} w(\sigma)\alpha^{t^{-1}\sigma^{-1}}\Big)\, t \equiv 0 \pmod{\mathfrak{p}},$$

d'où $\sum_{\sigma\in G} w(\sigma)\alpha^{t^{-1}\sigma^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, $\forall t \in G$; puis $\sum_{\sigma\in G} w(\sigma)\alpha^{\sigma^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, ce qui donne la ϕ-relation associée non triviale modulo $\mathfrak{p}$ (non nécessairement dans $e_\phi\mathbb{Z}_{(p)}[G]$), $W = \sum_{\sigma\in G} w(\sigma)\,\sigma^{-1} \in e_\phi Z_{C,(p)}[G]$, telle que $W.\alpha \equiv 0 \pmod{\mathfrak{p}}$. ■

Lemme 3.8 *Dans l'étude des $\Delta_p^\theta(\eta)$, $\theta \neq 1$, on peut supposer $\eta \in Z_K$.*

Démonstration Posons $\eta = \mu.d^{-1}$, $\mu \in Z_K$, $d \in \mathbb{Z}$. On a $\alpha_p(\eta) \equiv \alpha_p(\mu) - \alpha_p(d) \pmod{p}$ et on a $\sum_{\nu\in G} u(\nu)\alpha_p(\eta)^{\nu^{-1}} \equiv \sum_{\nu\in G} u(\nu)\alpha_p(\mu)^{\nu^{-1}} \pmod{p}$, pour toute θ-relation relative à η, car $\alpha_p(d)$ est invariant par Galois et $\theta \neq 1$; d'où $\mathcal{L}^\theta(\eta) = \mathcal{L}^\theta(\mu)$ et $\Delta_p^\theta(\eta)$ et $\Delta_p^\theta(\mu)$ nuls (ou non) en même temps (Théorème 3.9 ci-après). ■

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

On supposera donc $\eta \in Z_K$ pour certains raisonnements Diophantiens (essentiellement §6, 7), mais on peut conserver $\eta \in K^\times$ dans les énoncés généraux.

3.2.2 Enoncé principal

Les résultats techniques du §3.2.1 conduisent à l'énoncé suivant (où p est supposé assez grand).

Théorème 3.9 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n de groupe de Galois G. Soit $\eta \in K^\times$ tel que le $\mathbb{Z}[G]$-module engendré par η soit de $\mathbb{Z}$-rang n. Pour tout p on pose $\eta_1 := \eta^{p^{n_p}-1} = 1 + p\alpha_p(\eta)$, $\alpha_p(\eta) \in Z_{K,(p)}$, où n_p est le degré résiduel de p dans $K/\mathbb{Q}$. Soit $\mathcal{L}$ le G-module des relations $U \in \mathbb{Z}_{(p)}[G]$ relatives à $\alpha_p(\eta)$,* i.e., *telles que :*

$$\sum_{v\in G} u(v)\alpha_p(\eta)^{v^{-1}} \equiv 0 \pmod{p}, \quad u(v) \in \mathbb{Z}_{(p)} \quad \textit{(Définitions 3.3)}.$$

Soit θ un caractère p-adique irréductible de G et soit f le degré résiduel de p dans le corps des valeurs des caractères absolument irréductibles $\phi \mid \theta$. Alors, vu dans $\mathbb{F}_p[G]$, le G-module $\mathcal{L}^\theta := e_\theta \mathcal{L}$ est de $\mathbb{F}_p$-dimension non nulle si et seulement si le θ-régulateur local $\Delta_p^\theta(\eta)$ (§2.3) est nul modulo p. Dans ce cas, la $\mathbb{F}_p$-dimension de $\mathcal{L}^\theta$ est $\delta f \phi(1)$, $1 \le \delta \le \phi(1)$.

Démonstration Si $\mathcal{L}^\theta \neq \{0\}$, il existe $U = \sum_{v\in G} u(v)v^{-1} \in \mathcal{L}$ telle que $U_\theta \not\equiv 0 \pmod{p}$. Donc $U_\phi \not\equiv 0 \pmod{\mathfrak{p}}$ pour tout $\phi \mid \theta$. D'après le Lemme 3.5 et le Corollaire 3.6, on a $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$.

Supposons $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ et soit $\alpha \equiv \alpha_p(\eta) \pmod{p}$, $\alpha \in Z_{K,(p)}$; par la nullité modulo p de $\mathrm{Frob}^G(\alpha)$ qui en résulte, il existe une relation de $\mathbb{F}_p$-dépendance de la forme $\sum_{v\in G} u(v)\alpha^{v^{-1}} \equiv 0 \pmod{p}$, $u(v) \in \mathbb{Z}_{(p)}$ non tous divisibles par p, et on a $U = \sum_{v\in G} u(v)v^{-1} \in \mathcal{L}$ (Corollaire 3.2), mais il convient d'en déduire $\mathcal{L}^\theta \neq \{0\}$. D'après le Lemme 3.7, il existe, pour $\phi \mid \theta$, une ϕ-relation non triviale modulo $\mathfrak{p}$ de la forme $W := \sum_{v\in G} w(v)v^{-1}$, $w(v) \in Z_{C,(p)}$, telle que $W.\alpha \equiv 0 \pmod{\mathfrak{p}}$.

Si $\{z, \dots, z^f\}$ est une $Z_{L,(p)}$-base de $Z_{C,(p)}$, on a $w(v) = \sum_{i=1}^f a_i(v)z^i$, avec $a_i(v) \in Z_{L,(p)}$ pour tout i et tout v, d'où $\sum_{v\in G}\sum_{i=1}^f a_i(v)z^i\alpha^{v^{-1}} \equiv 0 \pmod{\mathfrak{p}}$; par identification sur la base des z^i on obtient le système de relations dans $Z_{KL,(p)}$,

$$\sum_{v\in G} a_i(v)\alpha^{v^{-1}} \equiv 0 \pmod{\mathfrak{p}}, \ i = 1, \dots, f.$$

Pour tout i et tout v, il existe des $r_{\mathfrak{p}}^i(v) \in \mathbb{Z}$ tels que $a_i(v) \equiv r_{\mathfrak{p}}^i(v) \pmod{\mathfrak{p}}$, d'où $\sum_{v\in G} a_i(v)\alpha^{v^{-1}} \equiv \sum_{v\in G} r_{\mathfrak{p}}^i(v)\alpha^{v^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, et comme $\sum_{v\in G} r_{\mathfrak{p}}^i(v)\alpha^{v^{-1}} \in K$, il vient $\sum_{v\in G} r_{\mathfrak{p}}^i(v)\alpha^{v^{-1}} \equiv 0 \pmod{p}$. Puisque W est une ϕ-relation non triviale modulo $\mathfrak{p}$, les $r_{\mathfrak{p}}^i(v)$ ne sont pas tous nuls modulo p et il existe une relation non triviale $\sum_{v\in G} r_{\mathfrak{p}}^i(v)\alpha^{v^{-1}}$ pour au moins un indice $i \in \{1, \dots, f\}$. Comme W est une ϕ-relation, ceci se transmet à $\sum_{v\in G} a_i(v)\,\alpha^{v^{-1}}$ et par conséquent, $\sum_{v\in G} r_{\mathfrak{p}}^i(v)v^{-1}$ (ϕ-relation invariante par D) est une θ-relation non triviale de $\mathcal{L}$. De fait on peut démontrer que la matrice $\left(r_{\mathfrak{p}}^i(v)\right)_{i,v}$ est de rang f. ∎

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Corollaire 3.10 *Lorsque $\mathcal{L}^\theta \neq \{0\}$, on obtient des relèvements de la forme $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$ pour toute θ-relation $U_\theta \in \mathcal{L}^\theta$.*

Démonstration On a $\eta_1^{U_\theta} = (1+p\alpha_p(\eta))^{U_\theta} \equiv 1+p\,U_\theta\cdot\alpha_p(\eta) \pmod{p^2}$, et comme $U_\theta \cdot \alpha_p(\eta) \equiv 0 \pmod{p}$ par définition, il vient $\eta_1^{U_\theta} = 1 + p^2\beta$, $\beta \in Z_{K,(p)}$. Donc $\eta_1^{U_\theta} = (1+p\gamma)^p$, $\gamma \in \prod_{v|p} K_v$, et $\eta = \eta^{p^{n_p}}\eta_1^{-1}$ implique $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$. ∎

4 Considérations heuristiques et Expérimentations

4.1 Méthodes probabilistes

Si des événements E_p, indexés par les nombres premiers, sont indépendants et de probabilités $\Pr(E_p)$, on peut appliquer le principe heuristique de Borel–Cantelli qui consiste à dire que si la série $\sum_p \Pr(E_p)$ converge, alors la conjecture naturelle est que les événements E_p sont réalisés un nombre fini de fois et que si elle diverge, ils sont réalisés une infinité de fois avec une densité en rapport [T, Chapitre III.1]. Dans notre cas, E_p est, pour $\eta \in K^\times$ fixé, l'événement "$\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod{p}$" ou "$\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$" pour un choix de θ pour chaque p (§2.3).

Dans le cas général, puisque $\mathrm{Reg}_p^\theta(\eta)$ est norme locale dans l'extension $C/\mathbb{Q}$, un tel régulateur local est soit étranger à p, soit divisible par p^f où f est le degré résiduel de p dans cette extension. De même, si le caractère irréductible $\phi \mid \theta$ est de degré $\phi(1) \geq 2$, alors $\mathrm{Reg}_p^G(\eta)$ est divisible par $p^{f\phi(1)}$. On verra que le degré $\phi(1)$ n'intervient pas pour les probabilités mais que, par contre, le nombre δ tel que $\mathcal{L}^\theta \simeq \delta V_\theta$ intervient, ainsi que f, sous la forme $\frac{O(1)}{p^{f\delta^2}}$ qui est la probabilité d'avoir "$\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ et $\mathcal{L}^\theta \simeq \delta V_\theta$" (§4.2.2).

Nous négligerons les p pour lesquels au moins deux θ-régulateurs $\Delta_p^\theta(\eta)$ sont divisible par p, une telle probabilité étant au plus en $\frac{O(1)}{p^2}$, vu l'indépendance des θ-régulateurs locaux (§4.3). Il restera alors le cas $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ pour un unique caractère p-adiquel θ de G sous réserve d'avoir $f = 1$ et la représentation $\mathcal{L}^\theta$ minimale. On aura alors $\mathrm{Reg}_p^G(\eta) \sim p^{e\phi(1)}$ avec $e = 1$, le cas $e \geq 2$ étant aussi de probabilité au plus en $\frac{O(1)}{p^2}$ (§4.6).

L'obstruction pour l'utilisation du principe heuristique de Borel–Cantelli viendrait alors des p satisfaisant à la définition suivante.

Définition 4.1 Un nombre premier p constitue un cas de *p-divisibilité minimale* (pour le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$) si $\mathcal{L}^\theta \neq 0$ (*i.e.*, $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$) pour un unique caractère p-adique irréductible θ de G vérifiant en outre les conditions suivantes.

(i) p est totalement décomposé dans C, *i.e.*, $f = 1$.
(ii) $\mathcal{L}^\theta \simeq V_\theta$, *i.e.*, $\delta = 1$.
(iii) $\mathrm{Reg}_p^\theta(\eta) \sim p$, *i.e.*, $\mathrm{Reg}_p^G(\eta) \sim p^{\phi(1)}$ n'a pas d'extra p-divisibilités.

Si G est Abélien, il s'agit de certains $p \equiv 1 \pmod{d}$, où d est l'ordre de $\phi \mid \theta$. Si $G = 1$ (situation du quotient de Fermat d'un rationnel), ceci a lieu pour tout p.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

4.2 Principes d'analyse : Linéarisation du problème

Soit $\eta \in Z_K$ donné. On suppose pour simplifier que le G-module engendré par η est de $\mathbb{Z}$-rang n.

4.2.1 Densités vs probabilités

On peut vérifier expérimentalement les principes heuristiques suivants par utilisation de la fonction *random* de PARI pour définir un entier γ quelconque de K étranger à p (de fait on s'intéresse seulement aux classes modulo p^2 de γ).

(i) Si d'un point de vue p-adique, $\alpha_p(\gamma) \pmod p$ parcourt l'anneau quotient $Z_{K,(p)}/(p) \simeq \mathbb{F}_p^n$, l'expérience montre que les résultats statistiques restent excellents si on limite γ à un petit domaine *Archimédien* (défini par exemple par $|c_i| \ll p$ pour les composantes c_i de γ sur une base ou par $\max_{v\in G}(|\gamma^v|) \ll p$), ce qui préserve l'aspect Diophantien et démontre une répartition uniforme (limitation obligatoire lorsque p^n est très grand). Dans [H-B] il est d'ailleurs démontré la répartition uniforme des quotients de Fermat et il est facile de conjecturer que c'est général.

Comme expliqué dans la Remarque 2.4, il faut distinguer la notion de probabilité (γ fixé et $p \to \infty$) de celle de densité, purement algébrique, lorsqu'elles sont égales à $\frac{O(1)}{p}$. Nous établissons, (§ 6 et 7) l'analogue de l'étude conduite dans [Gr2] pour le quotient de Fermat (avec vérifications numériques pour les groupes C_3, D_6), ce qui constitue une justification sérieuse des conjectures du § 8.

(ii) Soit $(e_i)_{i=1,\dots,n}$ une $\mathbb{Z}_{(p)}$-base de $Z_{K,(p)}$ et $\alpha_p(\gamma) = \sum_{i=1}^n A_i e_i$, $A_i \in \mathbb{Z}_{(p)}$. Alors, modulo p, les variables A_i sont indépendantes et équiprobables dans $\mathbb{F}_p$ et ceci ne dépend pas de K ni du choix de la base. Toute relation non triviale de la forme $\sum_{v\in G} u(v)\,\alpha_p(\gamma)^{v^{-1}} \equiv 0 \pmod p$ se traduit par une relation non triviale analogue sur les A_i (ceci résulte du fait que les conjugués des e_j sont des formes linéaires en les e_i indépendantes de p).

4.2.2 Heuristique principale

La probabilité (issue de la densité correspondante) de $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ est celle de $\mathcal{L}^\theta \neq \{0\}$ (Définitions 3.3, Théorème 3.9). Si $\mathcal{L}^\theta \simeq \delta V_\theta$, $1 \le \delta \le \phi(1)$, on peut justifier, de la façon suivante, que l'on doit affecter à ce cas une probabilité au plus $\frac{O(1)}{p^{f\delta^2}}$, où f est le degré résiduel de θ, où l'on considère V_θ comme $\mathbb{F}_p$-représentation et ensuite, par extension des scalaires, $V_\theta \otimes \mathbb{F}_{p^f}$ et V_ϕ comme $\mathbb{F}_{p^f}$-représentations.

On a $\mathcal{L}^\theta \otimes \mathbb{F}_{p^f} = \bigoplus_{\phi|\theta} \mathcal{L}^\phi$ où $\mathcal{L}^\phi \simeq \delta V_\phi$. L'idée part alors du fait que lorsque $\mathcal{L}^\phi \simeq \phi(1)V_\phi \simeq e_\phi \mathbb{F}_{p^f}[G]$ (*i.e.*, $e_\phi \alpha_p(\eta) \equiv 0 \pmod p$), la probabilité correspondante est $\frac{O(1)}{p^{f\phi(1)^2}}$ (minimale) puisque $e_\phi \alpha_p(\eta)$ est défini par $f\phi(1)^2$ composantes $\mathbb{F}_p$-indépendantes ($\mathbb{F}_p$-dimension de $\phi(1)V_\phi$).

Or $e_\phi \mathbb{F}_{p^f}[G] \simeq \mathrm{End}(V_\phi)$ comme algèbre d'endomorphismes d'un $\mathbb{F}_{p^f}$-espace de dimension $\phi(1)$. Par conséquent, $\mathcal{L}^\phi \simeq \delta V_\phi$ est alors vue comme sous-algèbre d'endomorphismes d'un $\mathbb{F}_{p^f}$-espace de dimension δ, d'où une probabilité-densité $\frac{O(1)}{p^{f\delta^2}}$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

d'avoir $\mathcal{L}^{\phi} \simeq \delta V_{\phi}$, *i.e.*, $\mathcal{L}^{\theta} \simeq \delta V_{\theta}$. Le cas $f = \delta = 1$ constitue le cas où la notion de probabilité doit se substituer à celle de densité.

On notera que la probabilité d'avoir tous les $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$ avec chaque fois $\delta = \phi(1)$, *i.e.*, $\alpha_p(\eta) \equiv 0 \pmod{p}$, équivalent aux n composantes de $\alpha_p(\eta)$ nulles modulo p, est alors $\frac{O(1)}{p^n}$ puisque $\sum_{\theta} f\phi(1)^2 = |G| = n$. Ce qui montre la cohérence de l'heuristique proposée.

Le cas non trivial le plus fréquent est $\delta = 1$ (le degré résiduel f dépend canoniquement de p contrairement à δ qui est "numérique"). Par exemple, le passage de $\delta = 1$ à $\delta = 2$ (pour $f = 1$) fait passer les probabilités de $\frac{O(1)}{p}$ à $\frac{O(1)}{p^4}$, quasi nulle pour $p \to \infty$ (très bien confirmé par les statistiques numériques, *cf.* § 4.4.3).

Exemple 4.2 Cas de $G = D_6$ ($f = 1, 1 \leq \delta \leq 2$). Soit θ le caractère irréductible de degré 2. La représentation $e_{\theta}\mathbb{F}_p[G]$ est isomorphe à $2V_{\theta}$ où V_{θ} est de $\mathbb{F}_p$-dimension 2. On peut engendrer $e_{\theta}\mathbb{F}_p[G]$ de la façon suivante (Remarque 2.13 (ii)) :

$$
\begin{gathered}
U_1 = 1 - \sigma^2 + \tau - \tau\sigma, \quad \sigma U_1 = \sigma - 1 + \tau\sigma^2 - \tau, \quad \sigma^2 U_1 = -U_1 - \sigma U_1,\\
U_2 = 1 - \sigma - \tau + \tau\sigma, \quad \sigma U_2 = -\sigma^2 + \sigma + \tau - \tau\sigma^2, \quad \sigma^2 U_2 = -U_2 - \sigma U_2,\\
\tau U_1 = -\sigma U_1, \quad \tau\sigma U_1 = -U_1, \quad \tau\sigma^2 U_1 = -\sigma^2 U_1,\\
\tau U_2 = -U_2, \quad \tau\sigma U_2 = -\sigma^2 U_2, \quad \tau\sigma^2 U_2 = -\sigma U_2.
\end{gathered}
$$

Les éléments $U_1, \sigma U_1, U_2, \sigma U_2$ forment une $\mathbb{F}_p$-base de l'espace des θ-relations, ce qui justifie la probabilité $\frac{O(1)}{p}$ seulement pour le cas $\delta = 1$, mais $\frac{O(1)}{p^4}$ pour $\delta = 2$.

4.3 Indépendance probabiliste (sur θ) des variables $\Delta_p^{\theta}(\gamma)$

Traitons le cas du groupe D_6, par utilisation de la fonction *random*, pour vérifier deux aspects :

- l'indépendance des θ-régulateurs (probabilité au plus $\frac{O(1)}{p^2}$ d'avoir deux θ-régulateurs $\Delta_p^{\theta}(\gamma)$ et $\Delta_p^{\theta'}(\gamma)$ nuls modulo p, pour $\theta \neq \theta'$) ;
- la probabilité $\frac{O(1)}{p}$ d'avoir la nullité modulo p de $\Delta_p^{\theta}(\gamma)$ pour le caractère $\theta = \chi_2$ de degré 2, le cas des caractères de degré 1 étant analogue.

On considère le corps K (composé de $\mathbb{Q}(\sqrt[3]{2})$ et de $\mathbb{Q}(j)$, où j désigne une racine cubique de l'unité) défini par le polynôme $Q = x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31$.

On prend au hasard γ modulo p^2, étranger à p, ce qui donne des $\alpha = \alpha_p(\gamma)$ répartis modulo p. On a calculé [Gr4, Programme A-3] les conjugués de α sur la base $\{x^5, x^4, x^3, x^2, x, 1\}$. La variable N_0 est le nombre de γ étrangers à p. Les variables $N_1, N_2, N_3, N_{12}, N_{13}, N_{23}, N_{123}$ donnent le nombre de cas de nullités simultanées de 1, 2, ou 3 régulateurs (caractères respectifs χ_0, χ_1, χ_2 de degré 2).

Pour $p = 13$ on obtient les valeurs suivantes : $N_0 = 999115$, $N_1 = 76820$, $N_2 = 77009$, $N_3 = 82239$, $N_{12} = 5898$, $N_{13} = 6301$, $N_{23} = 6453$, $N_{123} = 442$, et les densités

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

respectives :

$$\frac{N_1}{N_0} = 0.076888,\ \frac{N_2}{N_0} = 0.07707,\ \frac{N_3}{N_0} = 0.0823,$$
$$\frac{N_{12}}{N_0} = 0.00590,\ \frac{N_{13}}{N_0} = 0.006306,\ \frac{N_{23}}{N_0} = 0.006458,\ \frac{N_{123}}{N_0} = 0.0004424$$

avec $\frac{1}{p} = 0.07692$, $\frac{1}{p^2} = 0.005917$, $\frac{1}{p^3} = 0.000455$, d'où les probabilités attendues.

Pour $p = 37$ on obtient les valeurs suivantes : $N_0 = 999952$, $N_1 = 27153$, $N_2 = 27054$, $N_3 = 27747$, $N_{12} = 718$, $N_{13} = 761$, $N_{23} = 755$, $N_{123} = 16$, et les densités respectives :

$$\frac{N_1}{N_0} = 0.0271543,\ \frac{N_2}{N_0} = 0.027055,\ \frac{N_3}{N_0} = 0.0277483,$$
$$\frac{N_{12}}{N_0} = 0.000718,\ \frac{N_{13}}{N_0} = 0.000761,\ \frac{N_{23}}{N_0} = 0.000755,\ \frac{N_{123}}{N_0} = 1.600 \times 10^{-5}$$

avec $\frac{1}{p} = 0.027027$, $\frac{1}{p^2} = 0.00073046$, $\frac{1}{p^3} = 1.97 \times 10^{-5}$.

4.4 Statistiques sur le rang de la matrice des composantes

Une première statistique consiste à déterminer la probabilité d'avoir au moins une relation non triviale entre les conjugués de α. Si $\alpha^v = \sum_{i=1}^{n} A_i(v)e_i$, alors la matrice $\big(A_i(v)\big)_{i,v}$ doit être de $\mathbb{F}_p$-rang strictement inférieur à n. Pour $\theta \mid \chi$, la probabilité de nullité modulo p de $\Delta_p^\theta(\gamma)$ seul est $1/p^{f\delta^2}$; celle d'avoir au moins un $\Delta_p^\theta(\gamma)$ nul modulo p pour $\theta \mid \chi$ est $h/p^{f\delta^2}$. Par conséquent, si l'on désigne par h_i, f_i, δ_i les paramètres ci-dessus pour la totalité des caractères p-adiques de G (regroupés par caractères rationnels χ_i), la probabilité théorique d'obtenir une matrice de $\mathbb{F}_p$-rang $< n$ est donnée par

$$\sum_i \frac{h_i}{p^{f_i\delta_i^2}} - \sum_{i<j} \frac{h_i}{p^{f_i\delta_i^2}} \frac{h_j}{p^{f_j\delta_j^2}} + \sum_{i<j<k} \frac{h_i}{p^{f_i\delta_i^2}} \frac{h_j}{p^{f_j\delta_j^2}} \frac{h_k}{p^{f_k\delta_k^2}} - \cdots,$$

ce que l'on peut vérifier au moyen de programmes calculant, pour des γ aléatoires, le nombre de cas de $\mathbb{F}_p$-rang $< n$ ($G \simeq C_3, C_5, D_6$ respectivement dans les variables N_3, N_5, N_6). Chaque groupe G est donné via un polynôme définissant K, mais l'expérience numérique montre que la nature des résultats probabilistes dépend uniquement de G et non du choix de K ou du polynôme le définissant.

4.4.1 Cas G cyclique d'ordre 3 (deux caractères rationnels)

On utilise le polynôme de Shanks $P = x^3 - 11x^2 - 14x - 1$. Dans le cas $p \equiv 1 \pmod 3$ on a trois caractères p-adiques de degré résiduel $f = 1$; dans le cas $p \equiv 2 \pmod 3$ on a un caractère p-adique de degré résiduel $f = 2$ et le caractère unité. On obtient les exemples suivants (voir [Gr4, Programme A-4)] où N_0 est le nombre de cas testés :

$p = 41$, $N_0 = 4999931$, $N_3 = 124889$, $\frac{N_3}{N_0} = 0.024978$, probabilité 0.024970.

$p = 43$, $N_0 = 4999952$, $N_3 = 341000$, $\frac{N_3}{N_0} = 0.068200$, probabilité 0.068685.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

4.4.2 Cas G cyclique d'ordre 5 (deux caractères rationnels)

C'est le seul des cas étudiés pour lequel il y a (pour $p \equiv -1 \pmod 5$) deux caractères p-adiques de degré résiduel $f = 2$. Valeurs numériques obtenues (voir [Gr4, Programme A-5.1]) :

$$p = 7, N_0 = 499977, N_5 = 71650, \tfrac{N_5}{N_0} = 0.14330, \text{ probabilité } 0.143214.$$
$$p = 19, N_0 = 500000, N_5 = 29033, \tfrac{N_5}{N_0} = 0.05806, \text{probabilité } 0.057880.$$
$$p = 31, N_0 = 500000, N_5 = 75737, \tfrac{N_5}{N_0} = 0.15147, \text{ probabilité } 0.151214.$$

En modifiant la fin du programme (voir [Gr4, Programme A-5.2]), on teste la fréquence de nullité modulo p des θ-régulateurs relatifs à deux caractères p-adiques ($p = 31$ totalement décomposé), et deux seulement parmi les quatre non triviaux, à savoir par exemple pour θ_1 et θ_2 définis par $\theta_1(\sigma^{-1}) \equiv 2$, $\theta_2(\sigma^{-1}) \equiv 4 \pmod p$:

$$\Delta_p^{\theta_1}(\gamma) = \alpha + 2\alpha^{\sigma} + 4\alpha^{\sigma^2} + 8\alpha^{\sigma^3} + 16\alpha^{\sigma^4},$$
$$\Delta_p^{\theta_2}(\gamma) = \alpha + 4\alpha^{\sigma} + 16\alpha^{\sigma^2} + 2\alpha^{\sigma^3} + 8\alpha^{\sigma^4}.$$

Pour $N_0 = 1000000$, $N_1 = 943$ (nombre de nullités simultanées des deux régulateurs), on a $\frac{N_1}{N_0} = 0.000943$ et la probabilité 0.001040, ce qui montre l'indépendance des régulateurs relatifs aux caractères p-adiques d'un même caractère rationnel.

4.4.3 Cas G diédral d'ordre 6 (trois caractères rationnels et p-adiques)

Dans ce cas on a $h = f = 1$ pour tous les caractères. Les résultats ne dépendent pas de classes de congruences de p car $C = \mathbb{Q}$ (voir [Gr4, Programme A-6.1]) :

$$p = 13, N_0 = 49954, N_6 = 10794, \tfrac{N_6}{N_0} = 0.21607, \text{ probabilité } 0.21347.$$
$$p = 17, N_0 = 49516, \mathbb{N}_6 = 8337, \tfrac{N_6}{N_0} = 0.16836, \text{ probabilité } 0.16629.$$
$$p = 29, N_0 = 49815, N_6 = 5056, \tfrac{N_6}{N_0} = 0.10149, \text{ probabilité } 0.09992.$$
$$p = 31, N_0 = 40982, N_6 = 3854, \tfrac{N_6}{N_0} = 0.09404, \text{ probabilité } 0.09368.$$
$$p = 37, N_0 = 49998, N_6 = 3959, \tfrac{N_6}{N_0} = 0.07918, \text{ probabilité } 0.07890.$$

On reprend ensuite le même programme en faisant les statistiques du cas $\delta = 2$ pour le caractère χ_2 de degré 2, ce qui peut se tester en recherchant le nombre N_2 de cas où les régulateurs $\Delta_p^1(\gamma)$ et $\Delta_p^{\chi_1}(\gamma)$ sont non nuls modulo p et la matrice des composantes de rang 2. Ceci équivaut à $\Delta_p^{\theta}(\gamma) \equiv 0 \pmod p$ pour $\theta = \chi_2$ et $\mathcal{L}^{\theta}$ de dimension 4 (voir [Gr4, Programme A-6.2]). On obtient les résultats suivants pour $p = 13$.

$$N_0 = 499541\,;\, N_2 = 18\,;\, \tfrac{N_2}{N_0} = 3.60 \times 10^{-5}\,;\, \frac{1}{p^4} = 3.50 \times 10^{-5}\,;$$
$$N_1 = 34925(\text{nombre de } \Delta_p^{\chi_2}(\gamma) \equiv 0 \pmod p)\,;\, \tfrac{N_1}{N_0} = 0.06991\,;\, \frac{1}{p} = 0.07692.$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

4.5 Indépendance locale des composantes sur une base

Il reste à vérifier le caractère de "variables aléatoires indépendantes" de $A_1, \dots, A_n$; nous ne donnerons que deux exemples numériques ($G = C_3$ et $G = D_6$).

4.5.1 Cas cubique cyclique

Soit K le corps cubique cyclique défini par le polynôme $x^3 - 11x^2 - 14x - 1$, de conducteur 163. Il s'agit de vérifier que les variables A, B, C, qui définissent $\alpha \equiv Ax^2 + Bx + C \pmod{p}$ sont indépendantes.

On considère [Gr4, Programme A-7] des entiers aléatoires γ modulo p^2, étrangers à p dans un petit sous-domaine de $(\mathbb{Z}/p^2\mathbb{Z})^3$. Ensuite on calcule, par exemple, le nombre de couples (A, B) (resp. (B, C), (C, A)) ayant une valeur fixée arbitrairement dans $\mathbb{F}_p^2$, puis le nombre de cas où $\Delta_p^{\chi}(\gamma) \equiv 0 \pmod{p}$.

On désigne par N_0 le nombre d'entiers γ modulo p^2 étrangers à p considérés, par N_1 le nombre de cas où $\Delta_p^{\chi}(\gamma) \equiv 0 \pmod{p}$ (χ rationnel $\neq 1$), par N_2 le nombre de couples (A, B) ayant la valeur imposée modulo p, et le programme calcule les proportions $\frac{N_1}{N_0}$, $\frac{N_2}{N_0}$, ainsi que $\frac{2}{p}$ ou $\frac{1}{p^2}$.

Dans le tableau ci-dessous, on commence par deux cas de degré résiduel 2 dans $\mathbb{Q}(j)/\mathbb{Q}$ ($j^3 = 1$, $j \neq 1$) et on poursuit par des cas totalement décomposés :

p	N_0	N_1	N_2	$\frac{N_1}{N_0}$	$\frac{N_2}{N_0}$	$\frac{1}{p^2}$	$\frac{2}{p}$
5	255562	10023	10155	0.039219	0.039736	0.04	
11	499624	4127	4191	0.00826	0.008388	0.00826	
7	498553	132167	10275	0.2651	0.0206	0.0204	0.286
13	392751	57826	2401	0.1472	0.006113	0.005917	0.154
19	499907	51293	1421	0.1025	0.00284	0.00277	0.105

Les proportions $\frac{N_2}{N_0}$ sont proches de $\frac{1}{p^2}$. Dans les cas $p \equiv 1 \pmod{3}$ les proportions $\frac{N_1}{N_0}$ sont proches de $\frac{2}{p}$ (existence de deux caractères p-adiques), et proches de $\frac{1}{p^2}$ dans le cas $p \equiv 2 \pmod{3}$. Si l'on impose seulement une valeur numérique on obtient une proportion proche de $\frac{1}{p}$, et de $\frac{1}{p^3}$ si l'on impose les trois valeurs.

4.5.2 Cas diédral D_6

Une étude analogue utilise [Gr4, Programme A-8] et donne les résultats attendus. Pour $p = 17$, on obtient pour trois conditions sur les six composantes de α, $N_0 = 494865$, $N_3 = 111$, et $\frac{N_3}{N_0} = 0.0002243$, pour $\frac{1}{p^3} = 0.0002035$.

4.6 Extra p-divisibilités des régulateurs

Rappelons la décomposition du régulateur normalisé de η (Remarque 2.10 et § 2.3.2) :

$$\mathrm{Reg}_p^G(\eta) = \prod_{\theta} \mathrm{Reg}_p^{\theta}(\eta)^{\phi(1)} \quad \text{et} \quad \mathrm{Reg}_p^{\theta}(\eta) = \mathrm{N}_{\mathfrak{p}}\Big(P^{\phi}\big(\dots, \frac{-1}{p}\log_p(\eta^{\nu}), \dots\big)\Big)$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Dans le cas de p-divisibilité minimale (Définition 4.1), on a $\mathrm{Reg}_p^{\theta}(\eta) \sim p$ pour un unique θ et $\mathrm{Reg}_p^{G}(\eta) \sim p^{\phi(1)}$.

Si l'on suppose seulement que p est totalement décomposé dans $C/\mathbb{Q}$ ($f = 1$) et qu'il existe θ tel que $\mathrm{Reg}_p^{\theta}(\eta) \equiv \Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$ (avec $\delta = 1$), on a de possibles extra p-divisibilités $\mathrm{Reg}_p^{\theta}(\eta) \sim p^e$, $e \geq 2$ (donc $\mathrm{Reg}_p^{G}(\eta) \sim p^{e\phi(1)}$ si θ est unique), dont on veut vérifier qu'elles sont de probabilité $O(1)/p^2$.

Dans [Gr4, Programme A-9], pour $K = \mathbb{Q}(j, \sqrt[3]{2})$, $G = D_6$ (auquel cas tout p assez grand convient pour le test), on vérifie ce fait pour le régulateur :

$$\mathrm{Reg}_p^{\chi_2}(\eta) = \tfrac{1}{\sqrt{-3}}\Big(E_1^2 + E_2^2 + E_3^2 - E_4^2 - E_5^2 - E_6^2 - E_1.E_2 - E_2.E_3 - E_3.E_1 + E_4.E_5 + E_5.E_6 + E_6.E_4 \Big) \in \mathbb{Z},$$

où les E_i, $1 \leq i \leq 6$, sont les conjugués d'un entier de K (en effet, on peut supposer que $\frac{-1}{p}\log_p(\eta)$ est représenté modulo p^2 par un entier arbitraire $E \in K$).

Pour $p = 101$ et 10^6 essais via *random*, on obtient une densité de cas $e \geq 2$ égale à 1.01×10^{-4} pour une probabilité théorique 0.98×10^{-4}. Pour $p = 149$, on obtient 4.60×10^{-5} pour une probabilité 4.50×10^{-5}.

Le cas des caractères de degré 1 n'offre aucune difficulté (sous la condition $f = 1$) et nous ferons l'hypothèse heuristique qu'il en va de même pour tout groupe et tout caractère dans le cas p-décomposé, et en particulier que $P^{\phi}(\ldots, \frac{-1}{p}\log_p(\eta^{\nu}), \ldots)$ peut avoir toute valuation p-adique avec la probabilité correspondante. Il serait intéressant de démontrer que cette propriété des polynômes $P^{\phi}(X)$ est universelle.

5 Etude numérique de deux cas particuliers

5.1 Cas Abélien

On peut toujours se ramener au cas où G est cyclique d'ordre $n > 2$, engendré par σ (voir §2.3.3 pour les cas $n \leq 2$).

5.1.1 Exemple du sous-corps réel maximal de $\mathbb{Q}(\mu_{11})$

Recherche des solutions p telles que $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$. On considère $\eta = ax^4 + bx^3 + cx^2 + dx + e$ avec $x = \zeta_{11} + \zeta_{11}^{-1}$ (voir [Gr4, Programmes A-11 et A-10]).

($\bullet$) Pour $\eta = -2x^4 + x^3 - 3$, les solutions $p \leq 10^7$ sont $p = 31, 101, 39451$, tous décomposés dans $\mathbb{Q}(\zeta_5)$.

Considérons les données numériques pour $p = 31$:

$$\begin{aligned}
\alpha &\equiv 25x^4 + 10x^3 + 7x^2 + 21x + 29 \pmod{p}\\
\alpha^{\sigma} &\equiv 4x^4 + 15x^3 + 25x^2 + 7x + 16 \pmod{p}\\
\alpha^{\sigma^2} &\equiv 26x^4 + 20x^3 + 26x^2 + 18x + 22 \pmod{p}\\
\alpha^{\sigma^3} &\equiv 17x^4 + 6x^3 + 21x^2 + 24x + 4 \pmod{p}\\
\alpha^{\sigma^4} &\equiv 21x^4 + 11x^3 + 14x^2 + 23x + 19 \pmod{p}
\end{aligned}$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Pour $r = 4$, qui est tel que $\theta(\sigma) \equiv r \pmod{\mathfrak{p}}$ pour un couple $(\theta, \mathfrak{p})$, on a immédiatement, comme prévu : $\Delta_p^{\theta}(\eta) = \alpha + r^{-1}\alpha^{\sigma} + r^{-2}\alpha^{\sigma^2} + r^{-3}\alpha^{\sigma^3} + r^{-4}\alpha^{\sigma^4} \equiv 0 \pmod{p}$ identiquement sur la base $\{x^4, x^3, x^2, x, 1\}$.

(•) Pour $\eta = 10x^4 - 7x^3 + x - 2$, on trouve l'unique solution $p = 7$, premier cas totalement inerte dans $\mathbb{Q}(\zeta_5)$. Le programme donne tous les conjugués de α nuls modulo p (d'où en plus $\Delta_p^1(\eta) \equiv 0 \pmod{p}$).

Il est clair que le cas inerte dans $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ est très rare. D'ailleurs, p est petit pour compenser une probabilité $\frac{O(1)}{p^4}$.

(•) Pour $\eta = 10x^4 - 7x^3 - 3x^2 + x - 2$, on trouve $p = 79$ (deux caractères p-adiques θ de degré résiduel $f = 2$; p décomposé dans $L = \mathbb{Q}(\sqrt{5})$).

La résolvante $\alpha + \zeta_5\alpha^{\sigma} + \zeta_5^2\alpha^{\sigma^2} + \zeta_5^3\alpha^{\sigma^3} + \zeta_5^4\alpha^{\sigma^4}$ (qui correspond à $\Delta_p^{\phi}(\eta)$ pour $\phi(\sigma) = \zeta_5^{-1}$) se décompose de la façon suivante sur la base relative $\{1, \zeta_5\}$. On a la relation $\zeta_5^2 - \zeta_5\frac{\sqrt{5}-1}{2} + 1 = 0$ qui définit le polynôme irréductible de ζ_5 sur $\mathbb{Q}(\sqrt{5})$. On obtient alors

$$\zeta_5^3 = -\zeta_5\frac{\sqrt{5}-1}{2} + \frac{1-\sqrt{5}}{2}, \quad \zeta_5^4 = -\zeta_5 + \frac{\sqrt{5}-1}{2},$$

et le système de relations dans $K(\zeta_5)$ exprimant $\Delta_p^{\phi}(\eta) \equiv 0 \pmod{\mathfrak{p}}$:

$$\alpha - \alpha^{\sigma^2} + \frac{\sqrt{5}-1}{2}(\alpha^{\sigma^4} - \alpha^{\sigma^3}) \equiv 0 \pmod{\mathfrak{p}}$$
$$\alpha^{\sigma} - \alpha^{\sigma^4} + \frac{\sqrt{5}-1}{2}(\alpha^{\sigma^2} - \alpha^{\sigma^3}) \equiv 0 \pmod{\mathfrak{p}}.$$

Ensuite, l'idéal $\mathfrak{p}$ est, par exemple, défini par la congruence $\sqrt{5} \equiv 20 \pmod{\mathfrak{p}}$, d'où $\frac{\sqrt{5}-1}{2} \equiv 49 \pmod{\mathfrak{p}}$ ce qui définit les coefficients $r_i(v)$, $i = 1, 2$, et $(\theta, \mathfrak{p})$.

On a donc obtenu deux relations linéaires à coefficients rationnels indépendantes.

$$\alpha - \alpha^{\sigma^2} + 49\,(\alpha^{\sigma^4} - \alpha^{\sigma^3}) \equiv 0 \pmod{p}$$
$$\alpha^{\sigma^4} - \alpha^{\sigma} + 49\,(\alpha^{\sigma^3} - \alpha^{\sigma^2}) \equiv 0 \pmod{p}.$$

Les données numériques pour α et ses conjugués sont

$$\alpha \equiv 37x^4 + 13x^3 + 19x^2 + 3x + 10 \pmod{p}$$
$$\alpha^{\sigma} \equiv 75x^4 + 24x^3 + 45x^2 + 73x + 33 \pmod{p}$$
$$\alpha^{\sigma^2} \equiv 5x^4 + 51x^3 + 22x^2 + 60x + 1 \pmod{p}$$
$$\alpha^{\sigma^3} \equiv 70x^4 + 33x^3 + 40x^2 + 8x + 77 \pmod{p}$$
$$\alpha^{\sigma^4} \equiv 50x^4 + 37x^3 + 32x^2 + 14x + 22 \pmod{p}$$

qui vérifient le système des deux congruences ci-dessus.

On a les deux relations indépendantes définissant $\mathcal{L}^{\theta} \simeq V_{\theta}$ de $\mathbb{F}_p$-dimension 2 : $1 - \sigma^2 + 49(\sigma^4 - \sigma^3)$ et $\sigma^4 - \sigma + 49(\sigma^3 - \sigma^2)$, la seconde étant conjuguée par σ^4 de la première, d'où la probabilité $\frac{2}{p^2}$ (deux choix $\sqrt{5} \equiv \pm 20 \pmod{\mathfrak{p}}$).

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Calcul de la densité des $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ en fonction de f. Dans [Gr4, Programme A-12], on reprend le cas précédent et s'intéresse aux différents degrés résiduels possibles de p dans $\mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1})/\mathbb{Q}$ pour vérifier que la probabilité pour $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ est bien $O(1)/p^f$.

On affiche les probabilités théoriques selon le cas ($f = 1, 2, 4$) et le nombre N_1 de solutions rapporté au nombre N_0 de η testés.

- Pour $p = 31$, le degré résiduel est égal à 1 et on trouve les valeurs suivantes : $N_1 = 61505$, $\frac{N_1}{N_0} = 0.1230$ pour $\frac{4}{p} - \frac{6}{p^2} + \frac{4}{p^3} - \frac{1}{p^4} = 0.12292$.
- Pour $p = 19$, le degré résiduel est égal à 2 et on trouve les valeurs suivantes : $N_1 = 2756$, $\frac{N_1}{N_0} = 0.005512$ pour $\frac{2}{p^2} - \frac{1}{p^4} = 0.00553$
- Pour $p = 13$, le degré résiduel est égal à 4 et on trouve les valeurs suivantes : $N_1 = 17$, $\frac{N_1}{N_0} = 3.40 \times 10^{-5}$ pour $\frac{1}{p^4} = 3.50 \times 10^{-5}$.

5.2 Cas du groupe D_6

On désigne par $k = \mathbb{Q}(\sqrt{m})$ le sous-corps quadratique de K et par χ_1 et χ_2 les deux caractères rationnels (et p-adiques) irréductibles non triviaux de D_6. On utilise encore $K = \mathbb{Q}(\sqrt[3]{2}, j)$ où j désigne une racine cubique de l'unité ($m = -3$).

5.2.1 Rappels

On étudie les trois χ-régulateurs locaux $\Delta_p^\chi(\eta)$, chaque fois supposés non trivialement nuls modulo p (pas de χ-relations dans F). On a $\alpha = \alpha_p(\eta)$, $\alpha' = \alpha^\sigma$, $\alpha'' = \alpha^{\sigma^2}$, $\beta = \alpha^\tau$, $\beta' = \alpha^{\tau\sigma} = \alpha'^\tau$, $\beta'' = \alpha^{\tau\sigma^2} = \alpha''^\tau$.

Cas de $\Delta_p^1(\eta)$. On a donc $\mathrm{N}_{K/\mathbb{Q}}(\eta) = a \neq \pm 1$, auquel cas $\Delta_p^1(\eta)$ est le quotient de Fermat de a.

Cas $\Delta_p^{\chi_1}(\eta)$. On a $\mathrm{N}_{K/k}(\eta) \in k^\times \smallsetminus \mathbb{Q}^\times$ et on suppose que

$$\Delta_p^{\chi_1}(\eta) = \alpha + \alpha' + \alpha'' - \beta - \beta' - \beta'' \equiv 0 \pmod p.$$

Si $A = \alpha + \alpha' + \alpha'' =: u + v\sqrt{m}$, alors $\Delta_p^{\chi_1}(\eta) = A - A^\tau = 2v\sqrt{m} \equiv 0 \pmod p$. On a donc la seule condition $v \equiv 0 \pmod p$, ce qui conduit à une probabilité $\frac{O(1)}{p}$.

Cas $\Delta_p^{\chi_2}(\eta)$ (considéré au facteur $\sqrt{m}$ près). On a $\dim((F \otimes \mathbb{Q})^{e_\chi}) = 4$ (cas d'un caractère de degré 2), ce qui conduit, pour $\phi = \theta = \chi_2$, à la condition

$$\Delta_p^\theta(\eta) = \alpha^2 + \alpha'^2 + \alpha''^2 - \beta^2 - \beta'^2 - \beta''^2 - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha + \beta\beta' + \beta'\beta'' + \beta''\beta \equiv 0 \pmod p$$

(*cf.* Exemple 2.8). Le calcul des trois représentations $\mathcal{L}^{\theta'} \simeq \delta' V_{\theta'}$, $0 \leq \delta' \leq \phi'(1)$, permet de savoir quels sont les $\Delta_p^{\theta'}(\eta)$ nuls modulo p, même si l'on peut écarter les cas où $\Delta_p^1(\eta)$ ou $\Delta_p^{\chi_1}(\eta)$ est nul modulo p.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Commençons par des exemples relatifs au caractère p-adique $\theta = \chi_2$. Le Programme A-13 de [Gr4] calcule les conjugués de α sur la base des puissances de $x = \sqrt[3]{2} + j$. Ceci permet de trouver les relations de $\mathbb{F}_p$-dépendance de ces conjugués sous la forme $c_1\alpha + c_2\alpha^{\sigma} + c_3\alpha^{\sigma^2} + c_4\alpha^{\tau} + c_5\alpha^{\tau\sigma} + c_6\alpha^{\tau\sigma^2} \equiv 0 \pmod{p}$.

5.2.2 Cas $\eta = x^5 - 3x^4 - 7x^2 + x - 1$

On trouve les solutions $p = 7, 13, 69677, 387161$, pour $p \leq 10^7$.

- Pour $p = 7$, on a les données numériques suivantes :

$$\begin{aligned}
\alpha &\equiv 0x^5 + 2x^4 + 1x^3 + 1x^2 + 5x + 0 \pmod{p}\\
\alpha^{\sigma} &\equiv 1x^5 + 1x^4 + 6x^3 + 3x^2 + 5x + 2 \pmod{p}\\
\alpha^{\sigma^2} &\equiv 0x^5 + 2x^4 + 3x^3 + 0x^2 + 4x + 0 \pmod{p}\\
\alpha^{\tau} &\equiv 0x^5 + 5x^4 + 6x^3 + 6x^2 + 2x + 6 \pmod{p}\\
\alpha^{\tau\sigma} &\equiv 0x^5 + 5x^4 + 4x^3 + 0x^2 + 3x + 6 \pmod{p}\\
\alpha^{\tau\sigma^2} &\equiv 6x^5 + 6x^4 + 1x^3 + 4x^2 + 2x + 4 \pmod{p},
\end{aligned}$$

  qui conduisent aux deux $\mathbb{F}_p$-relations linéaires indépendantes $\alpha - \alpha^{\sigma} + \alpha^{\tau} - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p}$ et $\alpha - \alpha^{\sigma^2} + \alpha^{\tau} - \alpha^{\tau\sigma} \equiv 0 \pmod{p}$, et leur relèvements $\eta_1^{1-\sigma+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}$, et $\eta_1^{1-\sigma^2+\tau-\tau\sigma} \equiv 1 \pmod{p^2}$. Pour la θ-relation $U = 1 - \sigma + \tau - \tau\sigma^2$ on obtient $\sigma^2 U = -U - \sigma U$, $\tau U = -\sigma^2 U$, $\tau\sigma U = -\sigma U$, $\tau\sigma^2 U = -U$, et U engendre un espace de dimension 2 ($\mathcal{L}^{\theta} \simeq V_{\theta}$).
- Pour $p = 13$, on obtient les relations $\alpha - \alpha^{\sigma^2} + \alpha^{\tau} - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p}$, et $\alpha^{\sigma^2} - \alpha^{\sigma} + \alpha^{\tau\sigma} - \alpha^{\tau} \equiv 0 \pmod{p}$ et leur relèvements $\eta_1^{1-\sigma^2+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}$, et $\eta_1^{\sigma^2-\sigma+\tau\sigma-\tau} \equiv 1 \pmod{p^2}$.

  Pour la θ-relation $U = 1 - \sigma^2 + \tau - \tau\sigma^2$, on a $\sigma^2 U = -U - \sigma U$, $\tau U = U$, $\tau\sigma U = \sigma^2 U$, $\tau\sigma^2 = \sigma U$ ($\mathcal{L}^{\theta} \simeq V_{\theta}$).
- Dans le cas de $p = 69677$, on trouve les combinaisons

$$(c_1, c_2, c_3, c_4, c_5, c_6) = (53404, 39540, 46410, 69676, 1, 0)$$

  et $(23267, 16273, 30137, 69676, 0, 1)$ et une conclusion analogue aux précédentes.

5.2.3 Cas $\eta = x^5 - x^4 - 7x^2 + x - 1$, $p = 7$

On obtient quatre relations $\mathbb{F}_p$-linéaires indépendantes dont $\alpha^{\tau} - \alpha \equiv 0 \pmod{p}$, $\alpha + \alpha^{\sigma} + \alpha^{\sigma^2} \equiv 0 \pmod{p}$, et leurs conjuguées. Donc les trois régulateurs sont nuls modulo p. Mais pour θ, $\mathcal{L}^{\theta}$ est engendré par $U = e_{\theta}(1 - \tau)$ et par σU. On a $\sigma^2 U = -U - \sigma U$, $\tau U = -U$, $\tau\sigma U = -\sigma^2 U$, et $\tau\sigma^2 U = -\sigma U$ ($\mathcal{L}^{\theta} \simeq V_{\theta}$).

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

5.2.4 Cas $\eta = x^5 - 2x^4 + 4x^3 - 3x^2 + x - 1$, $p = 61$

Le G-module $\mathcal{L}$ est engendré par les trois relations $\mathbb{F}_p$-linéaires indépendantes (voir [Gr4, Programme A-13]

$$19\alpha + 56\alpha^{\sigma} + 46\alpha^{\sigma^2} + \alpha^{\tau} \equiv 0 \pmod{p},$$
$$46\alpha + 19\alpha^{\sigma} + 56\alpha^{\sigma^2} + \alpha^{\tau\sigma^2} \equiv 0 \pmod{p},$$
$$56\alpha + 46\alpha^{\sigma} + 19\alpha^{\sigma^2} + \alpha^{\tau\sigma} \equiv 0 \pmod{p}.$$

L'idempotent e_1 donne la relation triviale (car $19+56+46+1 \equiv 0 \pmod{61}$). Donc le quotient de Fermat $\Delta_p^1(\eta)$ est non nul modulo p.

On obtient la χ_1-relation correspondante à l'idempotent e_{χ_1} en faisant la somme des trois relations, ce qui donne $\alpha + \alpha^{\sigma} + \alpha^{\sigma^2} - \alpha^{\tau} - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p}$ (d'où pour $\theta = \chi_1$, la nullité modulo p du θ-régulateur $\Delta_p^{\theta}(\eta)$).

De fait, il s'agit d'une nullité triviale, le programme trouvant que tout p est solution pour $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$ (les conjugués de η vérifient $\eta^{1+\sigma+\sigma^2-\tau-\tau\sigma-\tau\sigma^2} = 1$). Les choix de η étant faits au hasard, ce fait est une pure coïncidence.

Pour $\theta = \chi_2$ (de degré 2), le θ-régulateur $\Delta_p^{\theta}(\eta)$ est nul modulo p (non trivialement) et cela correspond à la θ-relation suivante en appliquant $e_{\theta} = \frac{1}{3}(2 - \sigma - \sigma^2)$:

$$-\alpha + 36\alpha^{\sigma} + 26\alpha^{\sigma^2} + 21\alpha^{\tau} + 20\alpha^{\tau\sigma} + 20\alpha^{\tau\sigma^2} \equiv 0 \pmod{p}.$$

Notons que par conjugaison, cette dernière relation engendre un $\mathbb{F}_p$-espace de dimension 2 (autrement dit $\mathcal{L}^{\theta} \simeq V_{\theta}$). En effet, pour la θ-relation correspondante,

$$U = -1 + 36\sigma + 26\sigma^2 + 21\tau + 20\tau\sigma + 20\tau\sigma^2,$$

on a par définition $\sigma^2 U = -U - \sigma U$ et on trouve les relations $\tau U = 24U + 51\sigma U$, $\tau\sigma U = 27U + 37\sigma U$, $\tau\sigma^2 U = 10U + 34\sigma U$.

5.2.5 Cas $\eta = 3x^5 - 20x^4 + 15x^3 + 16x^2 + 9x + 21$, $p = 7$

On obtient

$$\alpha \equiv \alpha^{\sigma} \equiv \alpha^{\sigma^2} \equiv 6x^5 + 2x^4 + 4x^3 + 3x^2 + 6 \pmod{p},$$
$$\alpha^{\tau} \equiv \alpha^{\tau\sigma} \equiv \alpha^{\tau\sigma^2} \equiv x^5 + 5x^4 + 3x^3 + 4x^2 + 6 \pmod{p}.$$

Ce cas où le G-module $\mathcal{L}^{\theta}$ est de $\mathbb{F}_p$-dimension 4 ($\mathcal{L}^{\theta} \simeq 2V_{\theta} \simeq e_{\theta}\,\mathbb{F}_p[G]$) est très rare, comme on l'a vu au §4.4.3 (probabilité $\frac{O(1)}{p^4}$), car on doit prendre η de telle sorte que $\mathrm{rg}(F) = 6$ et qu'aucun des $\Delta_p^{\chi}(\eta)$, $\chi = 1, \chi_1$, ne soit nul modulo p, ce qui est le cas ici.

6 Ensembles de résidus modulo p dans Z_K

L'application du principe de Borel–Cantelli ne dépend que de l'obstruction de p-divisibilité minimale (Définition 4.1). Aussi nous proposons dans cette section et la suivante de lever cette obstruction au moyen de la même heuristique que celle utilisée dans

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

[Gr2] pour le quotient de Fermat. Le point fondamental étant de faire intervenir la métrique Archimédienne simultanément avec les métriques p-adiques.

6.1 Définitions d'ensembles de résidus.

6.1.1 Rappels sur le quotient de Fermat (voir [Gr2] et [Gr5]).

Dans le cas $K = \mathbb{Q}$, on travaille dans l'ensemble de résidus $\mathcal{I}_p := [1, p[$ pour trouver les $z \in \mathcal{I}_p$ tels que $\Delta_p^1(z) = q_p(z) \equiv 0 \pmod{p}$ ou plus généralement $\Delta_p^1(z) \equiv u \pmod{p}$ pour $u \in [0, p[$ donné. On étudie alors les invariants $m_p(u)$ (nombre de $z \in \mathcal{I}_p$ tels que $\Delta_p^1(z) \equiv u \pmod{p}$) et $M_p = \max_{u\in[0,p[}(m_p(u))$ (nombre maximal de répétitions du quotient de Fermat).

Ensuite, on constate la stabilité de $M_p = O(\log(p))$, pour tout p, le fait qu'un $u_0 \in [0, p[$ tel que $m_p(u_0) = M_p$ est aléatoire, et que la proportion de quotients de Fermat atteints dans $[0, p[$, par au moins un $z \in \mathcal{I}_p$, tend vers $1 - e^{-1} \approx 0.63212$ lorsque $p \to \infty$.

C'est l'analyse de ces résultats numériques qui suggère l'existence d'une loi de probabilité binomiale sur les $m_p(u)$, $u \in [0, p[$, de paramètres $(p-1, \frac{1}{p})$, donnant

$$\mathrm{Prob}(m_p(u) \geq m) = \frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} \quad ([\mathrm{Gr2}, \S 4]).$$

En particulier, la probabilité d'avoir $m_p(u) \geq 1$, *i.e.*, $u \in [0, p[$ atteint, est précisément rapidement égale à $1 - e^{-1} \approx 0.63212$ lorsque $p \to \infty$.

Si on applique cette heuristique à $a \geq 2$ fixé et lorsque $\Delta_p^1(a) \equiv 0 \pmod{p}$, $p \to \infty$, les solutions $z \in \mathcal{I}_p$ à $\Delta_p^1(z) \equiv 0 \pmod{p}$ sont au moins au nombre de $h := \left\lfloor \frac{\log(p)}{\log(a)} \right\rfloor$ ($z = a^j$, $1 \leq j \leq h$, dites *solutions exceptionnelles*), auquel cas, un calcul analytique élémentaire donne une probabilité de la forme

$$\mathrm{Prob}\big(q_p(a) \equiv 0 \pmod{p}\big) \leq \frac{O(1)}{p^{\log_2(p)/\log(a)-O(1)}}, \quad \text{pour } p \to \infty.$$

Comme $M_p = O(\log(p))$ et que $M_p \geq m_p(0) \geq h$ dans le cas de telles solutions exceptionnelles, on peut dire que $M_p \approx m_p(0) \approx h = O(\log(p))$, même si de fait $M_p > m_p(0)$ pour les raisons qui seront expliquées au § 7.2.6 (i).

Lorsque $m_p(0) = O(\log(p))$ (voire $m_p(0) = M_p$) sans qu'il existe nécessairement $a \ll p$ tel que $\Delta_p^1(a) \equiv 0 \pmod{p}$, on parlera de *solutions abondantes* pour les $z \in \mathcal{I}_p$ tels que $\Delta_p^1(z) \equiv 0 \pmod{p}$. Ceci veut dire qu'un nombre presque maximal de répétitions à $\Delta_p^1(z) \equiv u \pmod{p}$ a lieu pour $u = 0$. Le cas de solutions exceptionnelles est un cas particulier (plus rare) de solutions abondantes.

6.1.2 Généralisation en dimension $n > 1$.

Dans le cas d'un corps $K \neq \mathbb{Q}$, l'anneau des entiers Z_K est de $\mathbb{Z}$-dimension $n > 1$, et de même pour Z_K/pZ_K comme $\mathbb{F}_p$-espace vectoriel. Par conséquent, un ensemble $\mathcal{I}_p$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

naturel dans ce cas est

$$\mathcal{I}_p = \Big\{ \sum_{i=1}^{n} z_i e_i, z_i \in \,]-\frac{p}{2}, \frac{p}{2}[\ \forall i \Big\},$$

où $(e_i)_{i=1,\ldots,n}$ est une $\mathbb{Z}$-base de Z_K. L'autre choix $z_i \in [1, p[$ n'est pas possible car on a besoin d'un ensemble complet de résidus qui soit aussi "Archimédien", c'est-à-dire de la forme $\{z \in Z_K, |z_i|_\infty < R\}$, où R dépend simplement de p, comme ici $R = \frac{p}{2}$, car contrairement au cas $n = 1$, $e_1 = 1$, on ne contrôle plus les questions de signes (notamment pour K non réel).

Comme en dimension 1, le principe fondamental consiste encore à considérer $\eta \in Z_K$ fixé et des $p \to \infty$, tels que $\Delta_p^\theta(\eta) \equiv 0 \pmod p$, pour remarquer que les premières puissances η^j de η sont encore dans $\mathcal{I}_p$ (Lemme 6.5) et vérifient $\Delta_p^\theta(\eta^j) \equiv 0 \pmod p$ (Théorème 6.6), donnant $O(\log(p))$ solutions exceptionnelles conduisant à la même conclusion que dans le cas $K = \mathbb{Q}$.

Par contre, pour $n > 1$, l'étude probabiliste des $\Delta_p^\theta(z)$, $z \in \mathcal{I}_p$ (en particulier le calcul des $m_p(u)$ et de M_p), est numériquement inaccessible pour de grands nombres premiers p (programme utilisant des boucles à p^n calculs) et il faut définir un autre procédé permetant d'utiliser de grands p tout en conservant la pertinence statistique.

Auparavant on peut juste donner un aperçu de ces calculs dans $\mathcal{I}_p$ en dimension $n > 1$ au moyen du corps cubique cyclique $K = \mathbb{Q}(x)$, $x = \zeta_7 + \zeta_7^{-1}$, où ζ_7 est une racine 7-ième de l'unité [Gr4, Programme B].

On écrit $z = ax^2 + bx + c \in \mathcal{I}_p$, $a, b, c \in \,]-\frac{p}{2}, \frac{p}{2}[$. Pour se limiter aux conditions de la Définition 4.1, on suppose $p \equiv 1 \pmod 3$ et on fixe $\theta \neq 1$ (défini au moyen de r d'ordre 3 modulo p).

Il se pose alors le problème de la pondération des valeurs $m_p(u)$ et M_p (très grandes). Nous avons calculé les quantités

$$m'_p(0) = \frac{m_p(0)}{N_p}, \quad M'_p = \frac{n\,(p-1)\,M_p}{N_p}, \quad \text{où} \quad N_p = p^3 - 1$$

ou $(p-1)^3$ (selon que $n_p = 3$ ou 1) est le nombre de triplets (a, b, c) tels que z soit étranger à p. Ces quantités coïncident avec les expressions du cas $n = 1$. On désigne par u un élément de $[0, p[$ qui réalise M_p.

Le cas de M'_p est plus difficile en ce qui concerne une éventuelle constante multiplicative (le facteur n semble cohérent dans la mesure où il tient compte de l'action de G sur $\mathcal{I}_p$ lorsque celui-ci est un G-module, cas où la base choisie est une base normale). On obtient encore $M'_p = O(\log(p))$.

Pour les $p < 67$, la valeur de

$$\frac{M'_p}{\log(p)} = \frac{3(p-1)M_p}{N_p \times \log(p)}$$

est voisine de 1, mais il semble que cette quantité soit décroissante et rapidement majorée par 1. Le cas de $p = 61$ est particulier car $u = 0$ (solutions exceptionnelles :

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$m'_p = 1.92651$, $\frac{M'_p}{\log(p)} = 1.41159$) :

$p = 67$	$n_p = 3$	$u = 9$	$N_p = 300762$
$m'_p(0) = 0.98046$	$M_p = 4732$	$M'_p = 3.11520$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.74354$
$p = 73$	$n_p = 3$	$u = 5$	$N_p = 389016$
$m'_p(0) = 0.99537$	$M_p = 5568$	$M'_p = 3.09161$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.72290$
	...	...	
$p = 139$	$n_p = 1$	$u = 72$	$N_p = 2628072$
$m'_p(0) = 0.99107$	$M_p = 19322$	$M'_p = 3.04379$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.61684$
$p = 151$	$n_p = 3$	$u = 75$	$N_p = 3442950$
$m'_p(0) = 0.97416$	$M_p = 23458$	$M'_p = 3.06600$	$\frac{3(p-1)M_p}{N_p \times \log(p)} = 0.61108$

6.1.3 Autre approche en dimension $n > 1$

Le problème est multiplicatif car les $O(\log(p))$ premières puissances de η doivent appartenir à l'ensemble Archimédien $I_p \subseteq \mathbb{J}_p$ (à définir) qui doit contenir les solutions exceptionnelles lorsque $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$. De plus, l'aspect numérique nécessite de travailler dans une "structure de dimension 1" par analogie avec le cas $K = \mathbb{Q}$.

Donnons pour cela les définitions suivantes.

Définitions 6.1 On fait choix d'une base d'entiers $(e_i)_{i=1,\dots,n}$ de K et pour tout $\gamma \in Z_K$ on pose $\gamma = \sum_{i=1}^n c_i e_i$, $c_i \in \mathbb{Z}$ pour tout i.

(i) On appelle résidu modulo p de γ l'entier $[\gamma]_p := \sum_{i=1}^n [c_i]_p e_i$ de Z_K, avec $[c_i]_p \in]-\frac{p}{2}, \frac{p}{2}]$ et $c_i \equiv [c_i]_p \pmod{p}$.

(ii) On définit l' ensemble de résidus $I_p(\gamma) := \{[\gamma^k]_p, k \in [1, p[\}$.

(iii) On désigne par $z = \sum_{i=1}^n z_i e_i$, $z_i \in]-\frac{p}{2}, \frac{p}{2}]$ pour tout i, un élément quelconque de $I_p(\gamma)$.

Dans le cas $n = 1$ du quotient de Fermat de $\eta = a$ fixé, si $\gamma = g$ est une racine primitive modulo $p > 2$, $I_p(g) := \{[g^k]_p,\ k \in [1, p[\} = \{-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}\}$ (à l'ordre près). L'ensemble $\{[a^k]_p,\ k \in [1, p[\} \subseteq I_p(g)$ présente une périodicité si a n'est pas racine primitive modulo p et il convient de ne pas baser l'étude statistique sur cet ensemble, mais sur $I_p(g)$. De plus le groupe des racines de l'unité (ici ± 1) doit être pris en compte. Dans le cas général, soit μ_K le groupe des racines de l'unité du corps K. On désigne par D l'ordre de η dans $(Z_K/p\,Z_K)^\times \simeq \prod_{v|p} F_v^\times$, $F_v \simeq \mathbb{F}_{p^{n_p}}$, et par $d \mid D$ l'ordre de η dans $(\prod_{v|p} F_v^\times)/i_p(\mu_K)$, où η est supposé engendrer un $\mathbb{Z}[G]$-module de rang n. On a le résultat suivant pour tout p assez grand :

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Lemme 6.2 (i) *Il existe $\gamma \in Z_K$ tel que $[\eta]_p = [\gamma^{(p^{n_p}-1)/D}]_p$.*
(ii) *Si $n_p > 1$, alors d (donc D) ne divise pas $p-1$.*
(iii) *On a $D \geq d \geq \frac{\log(p-1)}{\log(c_0(\eta))}$ où $c_0(\eta) = \max_{\sigma\in G}(|\eta^\sigma|)$.*

Démonstration (i) Pour tout $v \mid p$, soit $g_v \in Z_K$ dont l'image dans $F_v^\times$ est génératrice, et soit η_v l'image de η. On pose $\eta_v = g_v^{\lambda_v}$ puis $\eta_v = g_v^{\lambda\,\mu_v}$ où $\lambda = \text{p.g.c.d.}\,((\lambda_v)_v)$. Alors $(g_v^{\mu_v})_v$ est d'ordre $p^{n_p}-1$. Il suffit de prendre $\gamma \in Z_K$ dont l'image diagonale dans $\prod_{v|p} F_v^\times$ est égale à $(g_v^{\mu_v})_v$ pour obtenir $\eta \equiv \gamma^\lambda \pmod{p}$. Quitte à remplacer γ par γ^μ, μ étranger à $p^{n_p}-1$, on peut supposer $\lambda = \frac{p^{n_p}-1}{D}$.

(ii) Soit $v \mid p$ et soit $\tau_v \in G$ l'automorphisme de Frobenius correspondant ; il est tel que $\eta^{\tau_v} \equiv \eta^p \pmod{\mathfrak{p}_v}$ dans K, d'où $\eta^{\tau_v-1} \equiv \eta^{p-1} \pmod{\mathfrak{p}_v}$. Si l'on suppose $\eta^{p-1} \equiv \zeta \pmod{p}$, $\zeta \in \mu_K$ d'ordre $r \geq 1$, alors $\eta^{r(\tau_v-1)} \equiv 1 \pmod{\mathfrak{p}_v}$, ce qui s'écrit $\eta^{r\tau_v} \equiv \eta^r \pmod{\mathfrak{p}_v}$. Or l'entier $\eta^{r\tau_v} - \eta^r$ n'est pas nul car η^r n'est pas dans un sous-corps strict de K et si $\mathcal{D}(\eta^r)$ est son discriminant, c'est un entier rationnel non nul et non divisible par p pour tout p assez grand (absurde). Mais ceci n'exclue pas encore le cas $D < p-1$ (e.g. $p = 22271$, $n_p = 3$, $D = 35$ où $5 \mid p-1$, $7 \mid p^2+p+1$).

(iii) On a $\eta^d = \zeta + \Lambda p$, où $\zeta \in \mu_K$, $\Lambda \in Z_K \setminus \{0\}$. A conjugaison près, on peut supposer $|\Lambda| \geq 1$. Il vient $|\eta|^d \geq |\Lambda|\,p - |\zeta| \geq p-1$ et $d \geq \frac{\log(p-1)}{\log(|\eta|)} \geq \frac{\log(p-1)}{\log(c_0(\eta))}$. ∎

L'ensemble $\{[\gamma^t]_p, t \in [0, p^{n_p}[\}$ est réunion de p^{n_p-1} ensembles $I_p^{(\lambda)} = \{[\gamma^{\lambda p+k}]_p$, $k \in [0, p[\}$, $\lambda \in [0, p^{n_p-1}[$. Une première heuristique consiste à dire que ces $I_p^{(\lambda)}$ ont même comportement statistique en ce qui concerne les nombres $m_p(u)$ et M_p. On peut donc en général considérer l'ensemble $I_p(\gamma) := \{[\gamma^k]_p,\ k \in [1, p[\}$. Distinguons deux cas au plan de l'expérimentation numérique.

a) Cas $n_p > 1$. On a en général $|I_p(\eta)| = p-1$ sauf si $D < p$ (*e.g.*, $p = 5$, $n_p = 2$, $\eta^3 \equiv 1 \pmod{p}$). Mais lorsque $p \to \infty$ on peut justifier l'heuristique suivante :

Heuristique 6.3 *On suppose que K est distinct de $\mathbb{Q}$ et d'un corps quadratique. Les premiers p, pour lesquels $n_p > 1$ et η est d'ordre D modulo p avec $D < p$, sont en nombre fini.*

Posons $n = n_p g_p$ et soit $(\eta_v)_{v|p}$ l'image de η dans $\prod_{v|p} F_v^\times$. Dire que η est d'ordre diviseur de D modulo p équivaut aux g_p conditions indépendantes $\eta_v^D = 1$ pour tout $v \mid p$ dont la probabilité est $(\frac{D}{p^{n_p}-1})^{g_p} \sim \frac{D^{g_p}}{p^{n_p g_p}}$. Si l'on somme sur les $D < p$, on obtient l'ordre de grandeur majorant $O(1)\frac{p^{g_p+1}}{p^{n_p g_p}} = O(1)\frac{1}{p^{n_p g_p - g_p - 1}}$, ce qui est clair pour $(n_p-1)g_p > 2$ et oblige à une étude particulière du cas $n_p = 1$ et du cas où K est un corps quadratique et p inerte.[3]

Dans ce dernier cas, on peut trouver une "structure de dimension 1" de la façon suivante. On remplace η par $\eta' = \eta^{\tau-1}$ où τ, générateur de G, est aussi le Frobenius en p ; on a donc $\eta' \equiv \eta^{p-1} \pmod{p}$ et η' est d'ordre $D' \mid p+1$ modulo p. On peut donc trouver γ d'ordre $p+1$ modulo p tel que $I_p(\gamma)$ contienne $\eta' \equiv \gamma^{(p+1)/D'} \pmod{p}$. Comme $\eta^{2\tau} = \eta^{\tau+1}\eta' =: a\eta'$, la théorie de $\Delta_p^\theta(\eta)$ est identique à celle de $\Delta_p^\theta(\eta')$ pour

[3]Pour les cas cubiques et quartiques ($n_p = 2$), voir [Gr6] en complément pour justification.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$\theta \neq 1$ et en outre, η' est indépendant de p et reste "petit". On aura encore $[\eta'^j]_p = \eta'^j$ pour $1 \leq j \leq h' = O(h)$ car $D' > h'$ comme dans le Lemme 6.2.

Remarque 6.4 En utilisant un argument analytique de [T], on peut remplacer $O(1)\frac{1}{p^{npg_p - g_p - 1}}$ par l'expression : $C_\epsilon \frac{1}{p^{npg_p - g_p - \epsilon}}$ (pour tout $\epsilon > 0$ et p assez grand), ce qui permet d'éliminer les cas cubiques et quartiques, mais non le cas quadratique pour lequel on a conjecturalement une infinité de solutions p (*cf.* [Gr6]).

Le Lemme 6.2 (ii) renforce cette heuristique. Ainsi on basera l'étude statistique sur $I_p = I_p(\eta)$. On admet, comme dans le cas du quotient de Fermat [H-B], que les $\Delta_p^\theta(z)$ sont uniformément répartis à partir de tout ensemble à $p-1$ éléments formé de résidus z engendrés par les puissances d'un entier fixé.

b) Cas $n_p = 1$ (p totalement décomposé dans K). L'ordre D de η modulo p est diviseur de $p-1$ et la probabilité pour que cet ordre soit un diviseur strict de $p-1$ est $1 - \frac{\phi(p-1)}{p-1}$ qui grossièrement se situe entre $\frac{1}{2}$ et $1 - \frac{1.781}{\log_2(p)}$. On ne peut donc pas considérer $I_p(\eta)$. On utilise le Lemme 6.2 (i) pour créer un ensemble de résidus de la forme $I_p(\gamma) = \{[\gamma^k]_p, k \in [1, p[\}$ qui contient $[\eta]_p$ et qui a $p-1$ éléments. On peut toujours choisir γ tel que $[\eta]_p = [\gamma^{(p-1)/D}]_p$.

D'après le Lemme 6.2 (iii), $I_p(\gamma)$ contient $d = O(\log(p))$ résidus distincts de la forme $[\eta^j]_p$ pour $1 \leq j \leq d$ qui ne sont pas dans μ_K.

Pour les expérimentations numériques, on utilisera $I_p = I_p(\gamma)$ engendré par un γ ayant les bonnes propriétés génératrices car le but est de vérifier la validité de l'existence d'une loi de probabilité binomiale sur les valeurs des $m_p(u)$, ce qui est une propriété de I_p et non d'un de ses éléments ; autrement dit, I_p doit être l'analogue de $I_p(g)$ en dimension 1 et si l'on étudie η fixé (analogue de $a \geq 2$ en dimension 1) lorsque $p \to \infty$, on peut dire que η appartient à un $I_p(\gamma)$ convenable dans lequel l'heuristique s'applique (comme pour $a \in I_p(g)$).

Les programmes ne font pas la distinction entre η et γ dans la mesure où les cas $|I_p| < p-1$ sont rares. On supprime de I_p les éventuelles racines de l'unité $\zeta \in \mu_K$ car $\alpha_p(\zeta) = 0$ modifierait les statistiques (on rencontre déjà ce cas en dimension 1 où $\{-1, 1\} \subset I_p =]-\frac{p-1}{2}, \frac{p-1}{2}[$).

Ensuite, pour le calcul des $m_p(u)$ et de M_p relatifs à I_p, on va montrer que si $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ (analogue de $q_p(a) \equiv 0 \pmod{p}$), on a $\Delta_p^\theta(\eta^j) \equiv 0 \pmod{p}$ (analogue de $q_p(a^j) \equiv 0 \pmod{p}$), pour tout $j \leq h = O(\log(p))$ (Lemme 6.5 et Théorème 6.6 ci-après).

6.1.4 Principe Archimédien fondamental

Si, par exemple, $\eta = \gamma = 2 + i \in \mathbb{Z}[i]$ avec $i^2 = -1$, on a $\eta^2 = 3 + 4i$, $\eta^3 = 2 + 11i$, $\eta^4 = -7 + 24i$, $\eta^5 = -38 + 41i$, $\eta^6 = -117 + 44i$, $\eta^7 = -278 - 29i, \ldots$. On voit que si $p \to \infty$, les résidus $[\eta^j]_p$ vont coïncider avec les valeurs exactes non réduites, η^j, pour un nombre fini d'indices j, et ensuite on aura les résidus correspondants ; pour $p = 47$ on obtiendra $]-\frac{p}{2}, \frac{p}{2}[= [-23, 23]$ et

$$I_p = \Big\{ [\eta]_p = \eta, [\eta^2]_p = \eta^2, [\eta^3]_p = \eta^3, [\eta^4]_p = -7 - 23i,$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$$[\eta^5]_p = 9 - 6i, [\eta^6]_p = -23 - 3i, [\eta^7]_p = 4 + 18i, \dots \Big\}.$$

De façon précise, on a le résultat suivant.

Lemme 6.5 *Soit $\eta \in Z_K \setminus \{0\}$, non racine de l'unité, et soit $c_0(\eta) = \max_{\sigma\in G}(|\eta^\sigma|)$. Alors il existe une constante explicite $\Gamma(K) \geq 1$, indépendante de η et p, telle que $[\eta^j]_p = \eta^j$ pour*

$$1 \leq j \leq \frac{\log(p-1) - \log(2\,\Gamma(K))}{\log(c_0(\eta))} < \frac{\log(p-1)}{\log(c_0(\eta))}$$

(comme $|\mathrm{N}_{K/\mathbb{Q}}(\eta)| \geq 1$ et que η n'est pas une racine de l'unité, on a $c_0(\eta) > 1$).

Démonstration Posons $\eta^j = \sum_{i=1}^n A_{j,i} e_i$, $A_{j,i} \in \mathbb{Z}$ pour tout $i = 1, \dots, n$. On a $\eta^{j\sigma} = \sum_{i=1}^n A_{j,i} e_i^\sigma$ pour tout $\sigma \in G$. La matrice $(e_i^\sigma)_{i,\sigma}$ est inversible (le carré de son déterminant est le discriminant du corps K) ; les coefficients Γ_i^σ de la matrice inverse sont des éléments de K indépendants de η, p, j, et $A_{j,i} = \sum_{\sigma\in G} \Gamma_i^\sigma\, \eta^{j\,\sigma}$, $i = 1, \dots, n$.

Une condition suffisante pour que $|A_{j,i}| < \frac{1}{2}\, p$ pour tout i, est qu'un majorant commun de ces nombres soit majoré par $\frac{1}{2}\,(p-1)$. Or on a

$$\Big|\sum_{\sigma\in G} \Gamma_i^\sigma\, \eta^{j\,\sigma}\Big| \leq \sum_{\sigma\in G} |\Gamma_i^\sigma|\,|\eta^{j\,\sigma}| \leq c_0(\eta)^j \sum_{\sigma\in G} |\Gamma_i^\sigma|.$$

Posons $\max_{i=1,\dots,n}(\sum_{\sigma\in G} |\Gamma_i^\sigma|) =: \Gamma(K)$ (maximum des sommes des lignes) ; alors il suffit d'avoir $c_0(\eta)^j\, \Gamma(K) \leq \frac{1}{2}(p-1)$, d'où le résultat.

Si $1 = \sum_{k=1}^n \lambda_k e_k$, $\lambda_k \in \mathbb{Z}$, on a $\sum_{\sigma\in G} \Gamma_i^\sigma \times 1^\sigma = \sum_{\sigma\in G} \sum_{k=1}^n \Gamma_i^\sigma \lambda_k e_k^\sigma = \sum_{k=1}^n \delta_{i,k}\lambda_k = \lambda_i$ pour tout i ; il existe au moins un i tel que $\sum_{\sigma\in G} |\Gamma_i^\sigma| \geq 1$. ∎

Le cas général est donc analogue à celui du quotient de Fermat et conduit au résultat suivant avec les notations du Lemme 6.5.

Théorème 6.6 *Soit $\eta \in Z_K$ engendrant un $\mathbb{Z}[G]$-module de rang n. Soit p assez grand et soit $I_p = I_p(\gamma)$ (Définition 6.1) tel que $|I_p| = p-1$ et $\eta \in I_p$. Soit θ un caractère p-adique irréductible de G.*

Si $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ on a $z_j := \eta^j \in I_p$ et $\Delta_p^\theta(z_j) \equiv 0 \pmod p$ pour tout j tel que $1 \leq j \leq h$, où

$$h = h_p(\eta) := \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\eta))}\,;$$

en outre, $z_j \notin \mu_K$.

Démonstration Posons $\eta = [\gamma^e]_p$. Le cas $n_p > 1$ où $\gamma = \eta$ est évident puisque $e = 1$. Si $n_p = 1$ et $\eta = \gamma^{\frac{p-1}{D}}$, $e = (p-1)/D$ et le Lemme 6.2 (iii) montre que $D \geq d \geq \log(p-1)/\log(c_0(\eta)) > h$; par conséquent les conditions $eh \leq p-1$ et $z_j \notin \mu_K$ sont toujours vérifiées. On sait que $\alpha_p(\eta^j) \equiv j\alpha_p(\eta) \pmod p$ quel que soit j et que l'on a $\eta \equiv \gamma^e \pmod p$, $e \in [1, p[$. Si l'on se restreint aux $j \leq h$, on a $\eta^j \equiv \gamma^{ej} \pmod p$ et $\eta^j = [\eta^j]_p = [\gamma^{ej}]_p =: z_j \in I_p$ puisque $ej \leq p-1$.

Par définition des G-modules $\mathcal{L}^\theta$ (dont la non trivialité est équivalente à la nullité du Δ_p^θ correspondant), on a $\mathcal{L}^\theta(\eta^j) = \mathcal{L}^\theta(\eta)$ dans $\mathbb{F}_p[G]$ car toute θ-relation

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$\sum_{v\in G} u(v)\alpha_p(\eta)^{v^{-1}} \equiv 0 \pmod{p}$ issue de $\mathcal{L}^\theta(\eta)$ équivaut à :

$$\sum_{v\in G} u(v)\alpha_p(\eta^j)^{v^{-1}} \equiv j.\sum_{v\in G} u(v)\alpha_p(\eta)^{v^{-1}} \equiv 0 \pmod{p},$$

$j \le h$ n'étant jamais divisible par p. Donc les $\Delta_p^\theta(\eta^j)$, caractérisés via les $\mathcal{L}^\theta(\eta^j)$, sont tous nuls modulo p dès que $\Delta_p^\theta(\eta)$ l'est, et comme il a été dit, $\eta^j \in I_p$ pour $1 \le j \le h$.

Il en résulte l'existence d'au moins $h = O(\log(p))$ solutions exceptionnelles, relativement à η. ■

7 Elimination de l'obstruction de p-divisibilité minimale

7.1 Les invariants $m_p(u)$ et M_p

Pour p, θ ,et $u \in [0, p[$ donnés, soit $m_p(u)$ le nombre de $z \in I_p$ ayant un θ-régulateur $\Delta_p^\theta(z)$ congru à u modulo p. On désigne par $M_p = \max_{u\in[0,p[}(m_p(u))$ le *nombre maximal de répétitions*. On suppose être dans une partie des conditions de la Définition 4.1 pour p et θ, *i.e.*, $f = \delta = 1$.

On obtient alors une stabilité remarquable pour M_p, fonction très régulière de p pouvant faire l'objet de l'heuristique suivante comme dans le cas des quotients de Fermat (§ 6.1.1).

Heuristique 7.1 *Pour tout $p \ge 2$ et tout caractère p-adique irréductible θ de G, donnés tels que $f = \delta = 1$ (Définition 4.1), le nombre $M_p = \max_{u\in[0,p[}(m_p(u))$ de résidus $z \in I_p$ ayant, modulo p, même θ-régulateur local, est $O(\log(p))$.*

Comme la valeur moyenne de $m_p(0)$ est proche de 1, le cas abondant, *i.e.*, lorsque $m_p(0) = O(\log(p))$, est plus fréquent que le cas exceptionnel, *i.e.*, lorsque $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, engendrant $h = O(\log(p))$ solutions dans I_p de la forme η^j, $j = 1, \dots, h$.

7.2 Expérimentations numériques

Donnons maintenant des justifications numériques des propriétés de $m_p(u)$ et M_p. Dans les programmes et résultats ci-après, on part d'une valeur numérique très simple de γ (l'expérience montre une grande stabilité des résultats par rapport à ce choix) et on calcule l'ensemble I_p des résidus z de la forme $[\gamma^k]_p$, $k = 1, \dots, p-1$, puis les valeurs $\Delta_p^\theta(z) \pmod{p}$ que l'on gère dans une liste L afin de déterminer $m_p(0)$ et $M_p = m_p(u_0)$ pour un u_0 convenable.

On prendra $\gamma = \eta$ si I_p vérifie les conditions évoquées au § 6.1.3.

7.2.1 Cas cubique cyclique, p inerte dans $\mathbb{Q}(j)$ ($j^3 = 1$, $j \ne 1$), $\theta \ne 1$

Dans ce cas l'étude statistique des $\Delta_p^\theta(z)$, pour $z \in I_p$, n'est pas nécessaire comme on vient de l'expliquer puisque d'après l'heuristique principale 4.2.2, on aurait

$$\mathrm{Prob}(\Delta_p^\theta(z) \equiv 0 \pmod{p}) = \frac{O(1)}{p^2}.$$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

On peut cependant calculer les valeurs $m_p(0)$ et M_p pour constater que $m_p(0) > 0$ est très rare et afin de voir ce qu'il en est pour M_p.

Ici $K = \mathbb{Q}(x)$, $x = \zeta_7 + \zeta_7^{-1}$, est le corps cubique cyclique de conducteur 7, $G = \{1, \sigma, \sigma^2\}$, et $p \equiv -1 \pmod 6$ ou encore $f = 2$. Pour $\theta \neq 1$, on a

$$\Delta_p^\theta(z) = \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha$$

(où $\alpha = \alpha_p(z)$), qui est rationnel modulo p (voir [Gr4, Programme B-1]).

Soit I_p engendré par $\gamma = x^2 + 2$; sur les 328 nombres premiers $p \equiv -1 \pmod 6$, $5999 < p < 11999$, on a $m_p(0) > 0$ pour uniquement 5 valeurs de p ($p = 6761, 7937, 8861, 9941, 10739$) et donc 323 cas où $m_p(0) = 0$. Mais les cas $m_p(0) > 0$ trouvés proviennent tous du fait qu'il existe $d \mid p-1$, $d \neq p-1$, tel que $\gamma^d \equiv \rho \pmod p$, où ρ est un rationnel ; ainsi pour $z = [\rho^d]_p$, $\Delta_p^\theta(z)$ est trivialement nul modulo p, et ces cas sont à exclure comme expliqué au § 6.1.3.

Dans le cas $p \equiv 1 \pmod 6$, $6001 < p < 12001$, on trouvera 134 valeurs de p pour lesquelles $m_p(0) = 0$, sur 327 nombres premiers, et les nombres $m_p(0) \neq 0$ auront des valeurs plus grandes en moyenne.

Par contre, M_p ne semble pas dépendre de la décomposition de p dans $\mathbb{Q}(j)$.

On a extrait les exemples suivants pour $p \equiv -1 \pmod 6$; le paramètre $u_0 \in [0, p[$ fournit une valeur (parmi plusieurs *a priori*) telle que $M_p = m_p(u_0)$:

$$\begin{array}{lll} p = 59999 & n_p = 3 & u_0 = 25910 \\ m_p(0) = 0 & M_p = 7 & M_p/\log(\mathrm{p}) = 0.63624 \end{array}$$

$$\begin{array}{lll} p = 60017 & n_p = 1 & u_0 = 51505 \\ m_p(0) = 0 & M_p = 7 & M_p/\log(\mathrm{p}) = 0.63622 \end{array}$$

$$\begin{array}{lll} p = 60029 & n_p = 3 & u_0 = 19677 \\ m_p(0) = 0 & M_p = 7 & M_p/\log(\mathrm{p}) = 0.63621 \end{array}$$

$$\begin{array}{lll} p = 60041 & n_p = 3 & u_0 = 59841 \\ m_p(0) = 0 & M_p = 8 & M_p/\log(\mathrm{p}) = 0.72708 \end{array}$$

On a, par exemple, $m_p(0) = 0$ et $M_p = 8$ pour $p = 60041$ ($u_0 = 59841$), et on obtient les résidus $z = [\gamma^j]_p$ suivants solutions à $\Delta_p^\theta(z) \equiv 59841 \pmod p$).

exposant	résidus $[\gamma^j]_p$
12869	$-17167\,x^2 + 1730\,x + 28097$
31327	$17781\,x^2 + 4775\,x + 25387$
32191	$3615\,x^2 - 27037\,x - 25973$
39129	$6079\,x^2 + 24215\,x + 18753$
44870	$-11178\,x^2 + 24638\,x + 12843$
54374	$3053\,x^2 - 24995\,x - 12010$
56394	$-3461\,x^2 + 16186\,x + 7608$
56651	$-19244\,x^2 - 9845\,x + 3277$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

7.2.2 Cas cubique cyclique, p décomposé dans $\mathbb{Q}(j)$ ($j^3 = 1$, $j \neq 1$)

On a donc $p \equiv 1 \pmod 6$ ou encore $f = 1$. Il y a deux θ-régulateurs p-adiques $\Delta_p^\theta(z) = \alpha + r^2\alpha^\sigma + r\alpha^{\sigma^2}$, où $\alpha = \alpha_p(z)$ et où r est l'un des deux éléments d'ordre 3 mod p.

Dans ce cas, $\Delta_p^\theta(z)$ est une "résolvante de Hilbert modulo p" qui est congrue à un rationnel modulo l'idéal premier $\mathfrak{p}$ associé à θ. Mais le Programme B-2 de [Gr4] donne $\Delta_p^\theta(z) = u_2x^2 + u_1x + u_0$ qui suppose que l'on utilise une congruence de la forme $x \equiv R \pmod{\mathfrak{p}}$ afin d'obtenir $\Delta_p^\theta(z) \equiv u \pmod p$. On procède autrement : pour avoir un rationnel, on multiplie $\Delta_p^\theta(z)$ par $H := x + rx^\sigma + r^2x^{\sigma^2} \pmod p$ qui sert de "résolvante conjuguée" une fois pour toutes ; elle n'est pas divisible par p.

On engendre I_p au moyen de $\gamma = x^2 + 2$. On a extrait les exemples suivants :

$$\begin{array}{lll} p = 60037 & n_p = 3 & u = 26443 \\ m_p(0) = 0 & M_p = 8 & M_p/\log(\mathrm{p}) = 0.72709 \end{array}$$

$$\begin{array}{lll} p = 60091 & n_p = 3 & u = 32679 \\ m_p(0) = 1 & M_p = 7 & M_p/\log(\mathrm{p}) = 0.63615 \end{array}$$

$$\begin{array}{lll} p = 60103 & n_p = 1 & u = 22560 \\ m_p(0) = 0 & M_p = 9 & M_p/\log(\mathrm{p}) = 0.81789 \end{array}$$

$$\begin{array}{lll} p = 60127 & n_p = 3 & u = 55712 \\ m_p(0) = 1 & M_p = 7 & M_p/\log(\mathrm{p}) = 0.63612 \end{array}$$

7.2.3 Exemple de $M_p = m_p(u)$ pour $u > 0$

Toujours dans $K = \mathbb{Q}(x)$, avec $x = \zeta_7 + \zeta_7^{-1}$, on considère $\gamma = -5x^2 + 2x + 3$ [Gr4, Programme B-3]. Pour $p = 5011$, on obtient un nombre maximal $M_p = 7$ de $z \in I_p$ tels que $\Delta_p^\theta(z) \equiv u_0 \pmod p$ pour $u_0 = 418$ (on a par ailleurs $m_p(0) = 1$ et $M_p/\log(\mathrm{p}) = 0.82165$) :

exposant	résidus $[\gamma^j]_p$
1233	$2043x^2 - 540x - 359$
1297	$810x^2 + 74x + 1078$
1932	$-1415x^2 + 962x - 1352$
2465	$577x^2 + 1380x + 1727$
2941	$-1735x^2 - 172x + 1553$
3848	$1168x^2 - 816x + 70$
4339	$-320x^2 - 426x + 468$

7.2.4 Cas diédral d'ordre 6

On considèrs le corps $K = \mathbb{Q}(j, \sqrt[3]{2})$ (où j désigne une racine cubique de l'unité), à groupe de Galois $G = D_6 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, et l'unique caractère p-adique irréductible θ de degré 2 pour lequel (en posant $\alpha = \alpha_p(z)$) :

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$$\Delta_p^\theta(z) = \frac{1}{\sqrt{-3}}\Big(\alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau \Big).$$

On utilise ici I_p engendré par $\gamma = 2x^5 + 2x^3 + x - 1$ [Gr4, Programme B-4] :

$p = 3559 \quad u_0 = 2946$
$m_p(0) = 1 \quad M_p = 6 \quad M_p/\log(\mathrm{p}) = 0.73374$

$p = 3571 \quad u_0 = 2286$
$m_p(0) = 1 \quad M_p = 5 \quad M_p/\log(\mathrm{p}) = 0.61120$

$p = 3581 \quad u_0 = 1$
$m_p(0) = 0 \quad M_p = 7 \quad M_p/\log(\mathrm{p}) = 0.85539$

$p = 3583 \quad u_0 = 1852$
$m_p(0) = 0 \quad M_p = 6 \quad M_p/\log(\mathrm{p}) = 0.73314$

On considère $\gamma = x^5 + 2x^4 - 2x^3 - x + 1$. Pour $p = 1709$, on obtient $m_p(0) = 1$ et $M_p = 6$ pour $u_0 = 487$ (on a $M_p/\log(\mathrm{p}) = 0.80605$) ; d'où le tableau des $z = [\gamma^j]_p$ tels que $\Delta_p^\theta(z) \equiv 487 \pmod{p}$.

exposant	résidus $[\gamma^j]_p$
51	$-179x^5 + 718x^4 + 739x^3 + 688x^2 + 553x - 159$
81	$-212x^5 - 730x^4 - 634x^3 + 849x^2 - 161x - 556$
759	$-649x^5 + 324x^4 - 729x^3 + 675x^2 - 423x + 149$
1079	$552x^5 - 364x^4 + 136x^3 + 52x^2 + 799x + 335$
1291	$651x^5 + 584x^4 + 334x^3 + 263x^2 + 437x + 624$
1567	$99x^5 + 566x^4 - 292x^3 + 152x^2 + 529x - 645$

Nous allons examiner dans quelle mesure il est possible d'avoir $m_p(0) = O(\log(p))$ (solutions abondantes) en dehors du cas des solutions exceptionnelles, point important pour justifier l'existence d'une loi de probabilité binomiale.

7.2.5 Cas où $m_p(0) = O(\log(p))$ en dehors du cas exceptionnel

On se propose de donner des exemples numériques de nombres premiers p où I_p (engendré par $\gamma = \eta \ll p$) possède $m_p(0) = O(\log(p))$ solutions $z \in I_p$ à $\Delta_p^\theta(z) \equiv 0 \pmod{p}$ sans que ces solutions soient de la forme $\mu^j = [\mu^j]_p$, $1 \le j \le h' = \left\lfloor \frac{\log(p-1) - \log(2\,\Gamma(K))}{\log(c_0(\mu))} \right\rfloor$ dans le cas exceptionnel où l'on aurait $\Delta_p^\theta(\mu) \equiv 0 \pmod{p}$, $\mu \ll p$.

L'expérimentation numérique montre qu'il y en a aussi rarement que dans le cas exceptionnel et nous conclurons sur ces différents cas au § 7.2.6.

Cas $G = 1$. Bien que cela ait été abordé dans [Gr2] (tableau du § 4.3.1 donnant des couples $(p, m_p(0))$ avec $m_p(0) \ge 6$), on peut par comparaison revoir le cas du quotient de Fermat pour lequel on a toujours $I_p = [1, p[$. On obtient le tableau suivant

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

dans lequel on a fixé $a = 14$, pour trouver des cas où $q_p(a) \equiv 0 \pmod{p}$ (solutions exceptionnelles a^j) et les cas où $m_p(0) = O(\log(p))$ (solutions z abondantes), pour tous les p tels que $3 \le p \le 10007$ [Gr4, Programme B-0].

p	$u \in [0, p[$ tels que $q_p(z) = u$ pour $M_p = m_p(u)$	M_p	$m_p(0)$
$p = 11$	abondantes $(z = 3, 9)$ $u = 0, 5$	$M_p = 2$	$m_p(0) = 2$
$p = 29$	exceptionnelles $(z = 14)$ $u = 24, 16, 1$	$M_p = 3$	$m_p(0) = 1$
$p = 353$	exceptionnelles $(z = 14, 196)$ $u = 297, 275$	$M_p = 6$	$m_p(0) = 2$
$p = 653$	abondantes $(z = 84, 120, 197, 287, 410)$ $u = 0, 99, 360, 241, 353, 617, 119, 399$	$M_p = 5$	$m_p(0) = 5$
$p = 4909$	abondantes $(z = 2189, 2234, 2406, 3266, 4649)$ $u = 0, 4651, 2785, 3967, 648, 3544, 3322, 2381,$ $1843, 3465, 1089, 1483, 4171$	$M_p = 5$	$m_p(0) = 5$
$p = 5107$	abondantes $(560, 1209, 1779, 2621, 4295, 4361)$ $u = 0, 2705, 4159$	$M_p = 6$	$m_p(0) = 6$

Cas $G = C_3$ ([Gr4, Programme B-5]). On utilise le corps cubique cyclique de conducteur 7 et I_p engendré par $\gamma = x^2 + x + 2$.

Pour $p = 2053$ (le plus petit exemple avec $M_p = m_p(0) = 7$) on obtient les résidus $z = [\gamma^j]_p$ suivants tels que $\Delta_p^\theta(z) \equiv 0 \pmod{p}$ (pour l'unique $u_0 = 0$).

exposant	résidus $[\gamma^j]_p$
186	$871\,x^2 - 930\,x + 496$
500	$57\,x^2 + 272\,x + 478$
559	$-691\,x^2 - 1003\,x - 881$
1399	$258\,x^2 + 1002\,x - 349$
1870	$-375\,x^2 - 212\,x + 240$
1981	$-464\,x^2 + 818\,x - 783$
2034	$121\,x^2 + 610\,x + 524$

L'exemple est clair puisque les exposants j ne sont pas les premières puissances d'un $\mu \in I_p$, $\mu \ll p$, et qu'il n'y a pas d'autres solutions.

Pour I_p engendré par $\gamma = 2\,x^2 + x + 3$ et $p = 1987$, on a $M_p = m_p(0) = 5$ pour $u = 1026, 454, 282, 180, 0, 1734, 117, 325, 1225$ et un tableau analogue de résidus pour $u_0 = 0$.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Pour $\gamma = 2x^2 + x + 2$, $p = 37, 307, 2347$ donnent des solutions abondantes non exceptionnelles. Seul $p = 79$ conduit à un cas mixte ($M_p = m_p(0) = 4$), avec $u = 0, 71$ et le tableau de résidus pour $u_0 = 0$.

exposant	résidus $[\gamma^j]_p$
1	$2x^2 + x + 2$
2	$17x^2 + 8x + 4$
20	$19x^2 - 11x + 15$
354	$-35x^2 - 33x + 19$

Cas diédral de degré 6 ([Gr4, Programme B-6]). Le caractère θ de degré 2 permet de confirmer les calculs précédents. Pour des solutions abondantes, le $m_p(0) \approx M_p$ maximum, égal à 6, est donné par l'exemple suivant, où I_p, pour $p = 331$, est engendré par l'entier $\gamma = -x^5 + x^4 - x^3 - x^2 + 1$.

exposant	résidus $[\gamma^j]_p$
48	$59x^5 - 46x^4 - 87x^3 + 141x^2 + 158x + 40$
102	$-61x^5 - 114x^4 + 119x^3 + 11x^2 - 125x - 120$
138	$-123x^5 - 122x^4 - 79x^3 - 61x^2 + 22x - 71$
155	$91x^5 + 100x^4 + 136x^3 + 138x^2 + 152x + 147$
180	$152x^5 - 8x^4 - 59x^3 - 165x^2 + 92x - 131$
322	$49x^5 - 158x^4 - 13x^3 - 14x^2 - 33x - 23$

Pour $\gamma = -x^5 - x^4 + x^3 - x^2 - x + 1$, $p = 379$, on a un cas de solutions abondantes avec $M_p = m_p(0) = 5$ et les résidus suivants :

exposant	résidus $[\gamma^j]_p$
49	$-147x^5 - 39x^4 - 73x^3 + 138x^2 + 40x + 129$
104	$-169x^5 - 105x^4 - 45x^3 - 180x^2 - 174x + 7$
149	$-91x^5 + 48x^4 - 155x^3 + 62x^2 + 183x + 35$
223	$-178x^5 - 14x^4 - 101x^3 + 150x^2 - 189x + 107$
304	$-103x^5 + 131x^4 + 3x^3 + 165x^2 + 140x + 189$

On a les exemples suivants dans les intervalles de variations des 81 valeurs de $\gamma = ax^5 + bx^4 + cx^3 + dx^2 + ex + 1$ (coefficients dans $\{-1, 0, 1\}$) du programme pour $2000 \leq p \leq 2500$).

(a) Pour $\gamma = x^5 - x^4 - x + 1$ et $p = 2441$, on a $m_p(0) = 2$, $M_p = 6$ (avec $u_0 = 1426$) pour une solution exceptionnelle (mais $h = 1$ seulement) et le tableau suivant.

exposant	résidus $[\gamma^j]_p$
1	$x^5 - x^4 - x + 1$
915	$-442x^5 - 129x^4 - 125x^3 - 651x^2 - 645x + 376$

Pour $u_0 = 1426$, on obtient le tableau suivant des z rélisant $M_p = m_p(u_0)$.

exposant	résidus $[\gamma^j]_p$
1839	$-169x^5 - 867x^4 - 402x^3 - 891x^2 - 357x - 680$
2034	$35x^5 - 939x^4 - 181x^3 + 388x^2 - 841x - 226$
2054	$449x^5 - 212x^4 + 1097x^3 - 651x^2 + 1191x - 478$
2171	$688x^5 - 525x^4 - 635x^3 + 334x^2 + 181x - 783$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$$\begin{array}{ll} 2194 & -909\,x^5 + 335\,x^4 - 1136\,x^3 - 1033\,x^2 - 970\,x + 557 \\ 2353 & 780\,x^5 - 1126\,x^4 + 968\,x^3 - 264\,x^2 - 294\,x - 107 \end{array}$$

(b) Pour $\gamma = x^5 - x^4 + x^3 - x^2 + 1$ et $p = 2441$, on a $M_p = m_p(0) = 5$ ($u = 2158, 2057, 724, 359, 0, 717$) pour des solutions abondantes et un tableau analogue.

(c) Pour $\gamma = x^5 - x^3 - x + 1$ et $p = 2087$, on a aussi $M_p = m_p(0) = 5$ (avec $u = 1335, 950, 670, 1840, 506, 1541, 1102, 280, 1973, 60, 0$) pour des solution sabondantes.

(d) Sur les 81 générateurs γ on trouve encore 4 cas de solutions exceptionnelles et 4 cas de solutions abondantes distincts.

7.2.6 Conclusions : Remarques fondamentales

Examinons les caractéristiques des notions de solutions exceptionnelles et abondantes. Le nombre η est fixé et $p \to \infty$.

(i) Solutions exceptionnelles. Si $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, ceci engendre au moins h solutions $z_j = \eta^j = [\eta^j]_p \in I_p$, $j = 1, \ldots, h$, et on a $m_p(0) \geq h = O(\log(p))$ (solutions aussi abondantes). Si l'on admet que $M_p = O(\log(p))$, on obtient $M_p \geq m_p(0) \geq h$. On aura souvent $M_p > m_p(0) \geq h$ compte tenu du fait que $M_p = m_p(u_0)$, $u_0 \in [0, p[$, et que $u_0 = 0$ est moins probable même si plusieurs u réalisent M_p ; de plus, $M_p > m_p(0)$, lorsque $u_0 \neq 0$, s'explique par le fait que si $\Delta_p^\theta(z) \equiv u_0 \pmod{p}$, alors en général $\Delta_p^\theta(\eta^k z) \equiv u_0 \pmod{p}$ (évident pour les $\Delta_p^\theta(\bullet)$ linéaires en les conjugués de $\alpha_p(\bullet)$; voir [Gr2, § 4.2.2 (δ)] pour le quotient de Fermat).

(ii) Solutions abondantes. Si $\Delta_p^\theta(\eta) \not\equiv 0 \pmod{p}$ et $m_p(0) = O(\log(p))$ on a donc $O(\log(p))$ solutions $z'_i \in I_p$, $i = 1, \ldots, h' := m_p(0)$ où cette fois les solutions z'_i sont *a priori* arbitrairement distribuées dans I_p (rappelons que d'après [H-B], les valeurs du quotient de Fermat sont uniformément réparties modulo p et que c'est probablement très général).

(iii) Le cas exceptionnel. Alors ce cas peut être vu comme le cas où, *par hasard*, η fait partie des solutions z'_j, auquel cas *on a nécessairement* $z'_1 = \eta$, $z'_2 = \eta^2, \ldots, z'_h = \eta^h$, avec un complément de type z'_i, sans que l'on puisse dire que les puissances successives de η constituent des relations de dépendance probabiliste. De plus on obtiendra des cas "mixtes", *i.e.*, lorsqu'il existe $\mu \neq \eta$ dans I_p, $\mu \ll p$, tel que $\Delta_p^\theta(\mu) \equiv 0 \pmod{p}$ donnant $h' \ll O(\log(p))$ solutions en partie exceptionnelles.

Il résulte de tout ceci que les deux cas (i) et (ii) sont de probabilités voisines, le cas exceptionnel étant moins probable par définition, auquel cas la considération du seul cas "abondant" est cohérente avec l'existence d'une loi de probabilité classique pour l'ensemble des solutions z'_i qui ne sont soumises à aucune condition.

Autrement dit, le cas "exceptionnel" ne serait pas particulier en dépit des apparences et serait donc susceptible au plus de la même probabilité comme pour le quotient de Fermat [Gr2, § 4.3.2], qui devient $O(\frac{1}{p^2})$ pour $p > p_0$ très grand, ce que nous allons reprendre.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Remarque 7.2 Le nombre η étant donné, on peut comparer la probabilité d'avoir un nombre premier p tel que $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ (solutions exceptionnelles), avec celle d'avoir $\Delta_p^\theta(\eta) \equiv u \pmod p$, *pour u fixé dans $\mathbb{N}$ indépendamment de p* (ce qui est le cas de $u = 0$). L'aspect numérique oblige à prendre u "fixé petit" et à rechercher les nombres premiers p tels que $\Delta_p^\theta(\eta) \equiv u \pmod p$. On constate alors le même degré de rareté quel que soit u.

Par exemple, si $\eta = x^2 - 3x + 2$ ($x = \zeta_7 + \zeta_7^{-1}$, [Gr4, Programme B-7]), on a dans l'intervalle $7 < p \le 60000001$ les rares couples de solutions $(p, u) = (61, 0), (5419, 0), (19, 1), (37, 2), (3229, 3), (43, 4), (31, 5), (613, 5), (\varnothing, 6), (79, 7), (42712981, 7)$.

On peut utiliser des u négatifs et on obtient des résultats semblables, comme $(607, -1), (143137, -1)$.

7.3 Sur l'existence d'une loi binomiale pour $m_p(u)$

Outre les justifications précédentes, on peut compléter l'analyse de la façon quantitative suivante qui résulte d'un calcul numérique très simple effectué dans le cas des quotients de Fermat $q_p(z)$, $z \in [1, p[$ et dans le cas des régulateurs locaux $\Delta_p^\theta(z)$, $z \in I_p$, pour le groupe D_6 et θ de degré 2 ([Gr4, Programmes B-8, B-12, B-13], le dernier testant des probabilités plus générales).

Dans les deux premiers nous avons calculé la moyenne (sur un grand nombre de nombres premiers p) des proportions C/N, où pour p fixé, C est le nombre de valeurs $u \in [0, p[$ telles qu'il existe au moins un $z \in [2, p-1[$ (resp. $z \in I_p$) tel que $q_p(z) \equiv u \pmod p$ (resp. $\Delta_p^\theta(z) \equiv u \pmod p$). La remarquable proximité du résultat avec $1 - e^{-1} \approx 0.632120$ conduit à la conjecture/heuristique suivante.

Conjecture 7.3 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n et de groupe de Galois G. On suppose être dans le cas $f = \delta = 1$ (cf. Définition 4.1) pour p et le caractère p-adique irréductible θ de G. Alors la valeur moyenne de la proportion de $u \in [0, p[$ de la forme $\Delta_p^\theta(z) \pmod p$, $z \in I_p$ (Définition 6.1), $p \to \infty$, est égale à $1 - e^{-1} \approx 0.632120$.*

Le programme pour C_3 donne la valeur 0.632133 et celui pour D_6 donne 0.631711. Or comme on le rappelle au point (iv) ci-dessous, c'est aussi la probabilité (sous l'existence de la loi binomiale) de l'existence d'au moins une solution $z \in I_p$ à $\Delta_p^\theta(z) \equiv u \pmod p$ pour u fixé.

Enfin dans un complément [Gr5], nous avons estimé la valeur numérique moyenne de M_p pour la loi de probabilité binomiale de paramètres $\left(p-1, \frac{1}{p}\right)$, lorsque $p \to \infty$ (nous ignorons si un calcul théorique est connu).

7.3.1 Seconde heuristique principale

Ainsi, les arguments précédents suggèrent l'existence d'une loi binomiale de paramètres $(p-1, \frac{1}{p})$, car on peut considérer que l'on réalise les $p-1$ "tirages" $z \in I_p$ pour lesquels on regarde combien de fois on obtient l'événement $\Delta_p^\theta(z) \equiv u \pmod p$, $u \in [0, p[$ donné. Le second paramètre $\frac{1}{p}$ est une approximation de $\mathrm{Prob}(\Delta_p^\theta(z) \equiv$

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

$u \pmod p$). De fait on peut vérifier que toute modification mineure de ces paramètres ne change pas la conclusion.

Heuristique 7.4 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n et de groupe de Galois G. On suppose être dans le cas $f = \delta = 1$ (cf. Définition 4.1) pour p et le caractère p-adique irréductible θ de G. Soit $u \in [0, p[$ fixé. Soit $m \in [0, p[$, $m \ll p$; alors la probabilité d'avoir au moins m valeurs $z_1, \dots, z_m \in I_p$ telles que $\Delta_p^\theta(z_j) \equiv u \pmod p$ pour $j = 1, \dots, m$, est donnée par l'expression :*

$$\mathrm{Prob}(m_p(u) \geq m) = \frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j}.$$

Nous renvoyons à [Gr2, § 4.4] pour des calculs identiques aux faits suivants à partir de la formule plus simple :

$$\mathrm{Prob}(m_p(u) \geq m) = 1 - (1 - \frac{1}{p})^p \frac{p}{p-1} \sum_{j=0}^{m-1} \frac{1}{(p-1)^j} \times \binom{p-1}{j}.$$

(i) $\frac{1}{p^{p-1}} \sum_{j=m}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \frac{1}{p^m} \binom{p-1}{m}$ pour tout $m \leq p-1$.

(ii) $\mathrm{Prob}(m_p(u) \geq m) \approx 1 - 0.3678 \times \sum_{j=0}^{m-1} \frac{1}{(p-1)^j} \times \binom{p-1}{j}$.

(iii) La probabilité d'avoir 0 solutions est proche de $e^{-1} \approx 0.3678$.

(iv) Celle d'avoir au moins une solution est proche de $1 - e^{-1} \approx 0.63212$; pour au moins 3 (resp. 4) solutions, on obtient 0.0803 (resp. 0.0189).

Pour une confirmation expérimentale, voir [Gr4, Programme 14].

Dans le cadre de p-divisibilité minimale pour p et θ, on obtient les résultats suivants, où $h = \frac{\log(p-1) - \log(2\Gamma(K))}{\log(c_0(\eta))}$ avec $c_0(\eta) = \max_{\sigma \in G}(|\eta^\sigma|)$ (Lemme 6.5).

Lemme 7.5 ([Gr2, Lemme 4.6])

(i) *On a pour $p \to \infty$ l'encadrement*

$$\exp\Big(-1 + \frac{1}{p}\Big(h + \frac{1}{2}\Big)\Big) < \frac{p^{-(p-1)} \sum_{j=h}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j}}{p^{-h} \binom{p-1}{h}} \leq 1.$$

(ii) *Il en résulte* $\mathrm{Prob}(\Delta_p^\theta(\eta) \equiv 0 \pmod p) < C_\infty(\eta) \times \frac{1}{p^h} \binom{p-1}{h}$ *pour $p \to \infty$ où $C_\infty(\eta)$ est comprise entre $e^{-1} \approx 0.36788$ et 1.*

Lemme 7.6 ([Gr2, Lemme 4.7]) *La série* $\sum_{p>2} \frac{1}{p^h} \binom{p-1}{h}$ *est convergente.*

Ainsi on obtient le Théorème 1.1 qui n'est modifié, par rapport au cas du quotient de Fermat, que par la constante effective $c_0(\eta)$ et le terme $O(1)$ qui peut être précisé.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

8 Conjectures p-adiques

8.1 Introduction

Le résultat très général précédent conduit à plusieurs conséquences ou interprétations que nous appelons *Conjectures* dans la mesure où nous considérons que, sous la seconde Heuristique principale 7.4, tout se ramène à celle de Borell–Cantelli. Ces conjectures proviennent toutes de l'utilisation convenable d'un régulateur p-adique d'un $\eta \in K^\times$ et de ses θ-composantes, pour $p \to \infty$, sachant que l'on peut toujours se ramener à $\eta \in Z_K$ pour les aspects Archimédiens des raisonnements probabilistes ($\theta \neq 1$, *cf.* Lemme 3.8).

En théorie algébrique des nombres on parle de "presque tout nombre premier p" pour signifier "tout nombre premier p sauf un ensemble Σ fini". Or d'autres définitions plus faibles sont possibles en théorie probabiliste des nombres [T, Chapitre III.3.1]. Les énoncés de cette section seront donnés sous la forme forte (algébrique).

Que nos heuristiques soient exactes ou non, ces conjectures sont posées indépendamment et certaines semblent très naturelles et crédibles.

8.2 Interprétation locale de $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$

Soit $\eta \in K^\times$ et soit θ un caractère p-adique irréductible de G tel que $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$. D'après le Corollaire 3.10 , c'est équivalent à l'existence d'une θ-relation non triviale $U_\theta := \sum_{\nu \in G} u(\nu)\, \nu^{-1} \in \mathcal{L}^\theta$ telle que $\eta^{U_\theta} \in \prod_{\nu \mid p} K_\nu^{\times p}$.

On va considérer cette écriture comme une propriété de "puissance p-ième locale partielle en p" de η, selon la définition suivante.

Définition 8.1 Soit $\eta \in K^\times$. On suppose que le $\mathbb{Z}[G]$-module F engendré par η est de $\mathbb{Z}$-rang n. Soit p un nombre premier assez grand et soit

$$F_{(p)} := \left\{ \eta_0 \in F,\ \eta_0 \in \prod_{\nu \mid p} K_\nu^{\times p} \right\}.$$

On dira que η est *puissance p-ième locale partielle en p* si $\dim_{\mathbb{F}_p}(F/F_{(p)}) < n$.

Dans le cadre de cette définition, on a la suite exacte

$$0 \longrightarrow \mathcal{L}(\eta) \longrightarrow \mathbb{F}_p[G] \longrightarrow F/F_{(p)} \to 1,$$

obtenue en associant à $U \in \mathbb{F}_p[G]$ l'élément $\eta^{(p^{n_p}-1).U}$ modulo $F_{(p)}$.

Remarques 8.2 Comme par hypothèse F est de $\mathbb{Z}$-rang n et sans p-torsion (pour tout p assez grand), on a $F/F^p \simeq \mathbb{F}_p[G]$ (en particulier, $\dim_{\mathbb{F}_p}(F/F^p)^{e_\theta} = f\phi(1)^2$ pour tout θ, où f est le degré résiduel de θ, *cf.* § 2.2.4 (ii)).

Il en résulte les faits suivants.

(i) La condition $\dim_{\mathbb{F}_p}(F/F_{(p)}) < n$ est équivalente à l'existence d'une θ-relation $U_\theta \in e_\theta \mathbb{Z}_{(p)}[G]$, non triviale modulo p, telle que η^{U_θ} est dans $F_{(p)}$ et est non puissance p-ième globale dans $K^\times$ car $F \cap K^{\times p} = F^p$ pour p assez grand. En effet, on a $F \subseteq E^S$ (groupe des S-unités) où S est un ensemble fini convenable d'idéaux premiers de K. Si l'on suppose p assez grand de telle sorte que p ne divise pas les ordres

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

des groupes de torsion $\mathrm{tor}_{\mathbb{Z}}(E^S)$ et $\mathrm{tor}_{\mathbb{Z}}(E^S/F)$, alors F est facteur direct dans E^S et $E^S = F \oplus H$. Si $\eta' \in F$ est tel que $\eta' = x^p$, $x \in K^\times$, alors $x \in E^s$ et il s'écrit $x = x_F \times x_H$, d'où $x_H^p = 1$, $x_H = 1$ et $\eta' = x_F^p \in F^p$.

(ii) On a $(F/F_{(p)})^{e_\theta} \simeq e_\theta \mathbb{F}_p[G]/\mathcal{L}^\theta$ de dimension $tf\phi(1)$, $0 \le t \le \phi(1)$, ce qui donne la relation $t = \phi(1) - \delta$ puisque $\mathcal{L}^\theta \simeq \delta V_\theta$ et de $\mathbb{F}_p$-dimension $\delta f \phi(1)$.

(iii) Dire que $\eta \in F_{(p)}$, c'est dire que $F_{(p)} = F$, donc que $\mathcal{L} = \mathbb{F}_p[G]$, de probabilité $\frac{O(1)}{p^n}$, cas qui peut être écarté pour $n > 1$ et $p \to \infty$.

8.3 Cas des caractères d'ordre 1 ou 2

Nous revenons sur des cas particuliers déjà évoqués (§ 2.3.3).

8.3.1 Cas d'un rationnel

On considère $K = \mathbb{Q}$ et un rationnel $a \in \mathbb{Q}^\times$, $a \ne \pm 1$. Si p est un nombre premier impair étranger à a, on a le résultat élémentaire suivant qui est un cas particulier de ce qui précède (pour $\theta = 1$ et $U_\theta = 1$) :

Lemme 8.3 *Le quotient de Fermat $\frac{a^{p-1}-1}{p}$ de a est nul modulo p si et seulement si $a \in \mathbb{Q}_p^{\times p}$.*

Or on sait, d'après un résultat de Silverman [Si] lorsque $a \in \mathbb{N}$, $a \ge 2$, que sous la conjecture *ABC* l'ensemble des premiers p tels que $a^{p-1} \not\equiv 1 \pmod{p^2}$ est infini.[4]

L'étude statistique montre que ce résultat est une forme très faible de la réalité. Autrement dit, on a la propriété conjecturale très raisonnable suivante.

Conjecture 8.4 *Soit $a \in \mathbb{Q}^\times$. Si $a \in \mathbb{Q}_p^{\times p}$ pour tout premier p sauf un nombre fini, alors $a = \pm 1$.*

On peut considérer cet énnoncé comme un principe local–global très particulier par rapport à ceux qui existent en théorie du corps de classes (alors purement algébriques comme le "principe de Hasse" pour les puissances, voir Proposition 8.6).

On pourra le qualifier de *principe local–global Diophantien* dans la mesure où "$a \in \mathbb{Q}_p^{\times p}$ pour presque tout p" serait équivalent à "$a \in \mathbb{Q}^{\times p}$ pour presque tout p".

8.3.2 Cas d'une unité d'un corps quadratique $K = \mathbb{Q}(\sqrt{m})$

Si $\eta = x + y\sqrt{m}$, on a $\eta^{p^{n_p}-1} = 1 + p\alpha_p(\eta)$, $\alpha_p(\eta) = u + v\sqrt{m}$, d'où $\Delta_p^\theta(\eta) \equiv 2v\sqrt{m} \pmod{p}$ pour $\theta \ne 1$. On a $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ si et seulement si $v \equiv 0 \pmod{p}$.

[4] Silverman a prouvé que pour tout entier $a \ge 2$, l'ensemble de ces nombres premiers $p \le x$ est de cardinal $\ge c \log(x)$. Ce résultat a été étendu par Graves et Murty [GM] aux $p \equiv 1 \pmod{k}$, pour tout $k \ge 2$ fixé, auquel cas, l'ensemble de ces $p \le x$ est de cardinal $\ge c \frac{\log(x)}{\log(\log(x))}$, toujours sous la conjecture *ABC*.

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

Supposons $m > 0$ et que η est une unité ε de $\mathbb{Q}(\sqrt{m})$. On a $u \equiv 0 \pmod{p}$ et encore $\Delta_p^\theta(\varepsilon) \equiv 2v\sqrt{m} \pmod{p}$. La nullité modulo p de $\Delta_p^\theta(\varepsilon)$ implique $\alpha_p(\eta) \equiv 0 \pmod{p}$ et ε est puissance p-ième locale. Au plan conjectural, on est ramené à la situation précédente d'un rationnel. Donc il suffirait que l'on démontre (via une forme adéquate de la conjecture ABC) que la relation $\varepsilon^{p^{n_p}-1} \not\equiv 1 \pmod{p^2}$ a lieu pour une infinité de p, pour pouvoir énoncer l'analogue pour ε de la Conjecture 8.4. Puis le fait que si $\varepsilon^{p^{n_p}-1} \equiv 1 \pmod{p^2}$ pour presque tout p, alors $\varepsilon = \pm 1$.

8.4 Généralisation en degré n

On pourra envisager que le processus précédent est valable pour le cas général où $\eta \in K^\times$ serait "puissance p-ième locale partielle en p" (Définition 8.1) pour presque tout p. Ceci suppose d'abord l'analyse du cas des puissances p-ièmes locales en p au sens commun.

8.4.1 Conjecture sur les puissances p-ièmes locales

Le cas rationnel (Conjecture 8.4) a montré la vraisemblance du type d'énoncé suivant correspondant à l'écriture : $\eta^{p^{n_p}-1} - 1 = p\,\alpha_p(\eta)$, dans le cas (statistiquement très exceptionnel) où $\alpha_p(\eta) \equiv 0 \pmod{p}$ (équivalent à $\mathcal{L} = \mathbb{F}_p[G]$) de probabilité $\frac{O(1)}{p^n}$ (Remarque 8.2 et § 4.2.2).

Conjecture 8.5 *Soit K un corps de nombres et soit $\eta \in K^\times$. Si $\eta \in \prod_{v|p} K_v^{\times p}$ pour tout premier p sauf un nombre fini, alors η est une racine de l'unité de K.*

Ceci pourrait provenir d'une généralisation du théorème de Silverman, qui utiliserait ici la conjecture ABC pour les corps de nombres (voir par exemple le texte de Waldschmidt [W] pour l'importante liste d'applications et conséquences). Mais la conjecture peut être posée indépendamment.

Cet énoncé est à comparer au très classique "principe de Hasse" pour les puissances, beaucoup plus fort, et qui est le suivant [Gr1, II.6.3.3]. Soit $\mathcal{P}_K$ (resp. $\mathcal{P}_p$) l'ensemble des places de K (resp. des p-places de K).

Proposition 8.6 *Soient $\eta \in K^\times$ et p un nombre premier ; soit Σ un ensemble fini de places de K. Si η est puissance p-ième locale pour toute place $v \in \mathcal{P}_K \setminus \Sigma$, alors $\eta \in K^{\times p}$. Il existe une infinité d'ensembles finis T (non effectifs) de places de K tels que si η est puissance p-ième locale pour toute place $v \in T$, alors $\eta \in K^{\times p}$.*[5]

[5]Les énoncés classiques supposent toujours que Σ est fini (simple élimination de places pathologiques) afin de pouvoir utiliser les théorèmes de densité (Chebotarev) qui s'expriment en termes de progressions particulières de densités canoniques ; or pour être certain que de telles suites (en nombre fini), nécessaires à la preuve, rencontrent bien le complémentaire de Σ, celui-ci doit être "presque tout", dès lors que s'il lui manquait une famille infinie (inconnue), il se pourrait que "par hasard" elle contienne les Frobenius dont on a besoin. On voit bien la distance qu'il peut y avoir entre un raisonnement algébrique général et un raisonnement sur des hypothèses nettement moins fortes portant par exemple sur des ensembles Σ de densité nulle (§ 8.1).

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

La différence par rapport au principe de Hasse opère en deux temps : partant de p et de l'ensemble $\mathcal{P}_p$, on commence par dire dans la Conjecture 8.5 que η est puissance p-ième locale pour tout $v \in \mathcal{P}_p$ (*i.e.*, on prend l'ensemble infini $\Sigma = \mathcal{P}_K \setminus \mathcal{P}_p$; ou encore on peut dire qu'on essaye de prendre $T = \mathcal{P}_p$), mais ensuite on suppose que cette propriété locale (de type "Hasse faible") est vraie pour presque tout p, auquel cas η serait conjecturalement dans $K^{\times p}$ pour presque tout p (principe local-global Diophantien), donc une racine de l'unité.

La conjecture "ultime" qui fait le lien avec la théorie des $\Delta_p^\theta(\eta)$ est la Conjecture 8.9 du § 8.5. Auparavant, examinons le cas général des unités des corps de nombres qui conforte l'analyse précédente.

8.4.2 Cas particulier du groupe des unités : Spiegelungssatz

On a l'énoncé spécifique suivant [Gr1, II.6.3.8].

Proposition 8.7 *Soient η une unité de K et p un nombre premier ; soit S_p un ensemble fini de places de K tel que le p-groupe des classes de $K' := K(\mu_p)$ soit engendré par les p-classes des idéaux premiers $\mathfrak{P}_{v'}$ de K' pour les places v' de K' au-dessus de celles de S_p. Si $\eta \in K_v^{\times p}$ pour toute place $v \in S_p \cup \mathcal{P}_p$, alors $\eta \in K^{\times p}$.*

La Conjecture 8.5 porte seulement sur les $\mathcal{P}_p$ au lieu des $S_p \cup \mathcal{P}_p$ pour S_p fini bien choisi (insuffisant pour avoir une puissance p-ième globale), mais on suppose dans la conjecture que cette hypothèse faible est vraie pour presque tout p. Les deux systèmes d'hypothèses coïncident lorsque le p-groupe des classes du corps K' est trivial ($S_p = \varnothing$), mais on peut être plus précis [Gr1, I.6.3.1 et II.1.6.3].

Soit η une unité de Minkowski du corps totalement réel K ; on peut toujours choisir η non puissance ℓ-ième globale pour tout premier ℓ. S'il existe une θ-relation $U_\theta \not\equiv 0 \pmod{p\mathbb{Z}_{(p)}[G]}$ pour laquelle $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$ (*i.e.*, $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$, cf. § 8.2), alors l'extension $N' := K'(\sqrt[p]{\eta^{U_\theta}})$ de K' est non ramifiée et p-décomposée ce qui conduit, par la théorie du corps de classes, à l'information suivante : soit $\mathcal{C}\ell_{K'}^{\mathcal{P}'_p}$ le quotient du p-groupe des classes $\mathcal{C}\ell_{K'}$ par le p-sous-groupe des classes des idéaux premiers $\mathfrak{P}' \mid p$ dans K' et soit $\theta^* := \omega\theta^{-1}$, où ω est le caractère de Teichmüller p-adique défini, à partir d'une racine primitive p-ième de l'unité ζ_p, par $\zeta_p^s = \zeta_p^{\omega(s)}$ pour tout $s \in \mathrm{Gal}(K'/K)$. Alors c'est la θ^*-composante de $\mathcal{C}\ell_{K'}^{\mathcal{P}'_p}$ qui est non triviale et $\mathrm{Gal}(N'/K')$ est isomorphe à un quotient de $(\mathcal{C}\ell_{K'}^{\mathcal{P}'_p})^{e_{\theta^*}}$. Ceci équivaut à l'existence d'une θ^*-extension N' non ramifiée p-décomposée de K', de degré puissance de p, contenue dans $K'(\sqrt[p]{F})/K'$, où F (indépendant de p) est le G-module engendré par η. Une telle situation pour une infinité de p paraît excessive.

En dehors du cas des unités on a une situation un peu différente : prenons pour $K = \mathbb{Q}$ l'exemple de $\eta = a \in \mathbb{Q}^\times$, $a \neq \pm 1$. Alors la Proposition 8.7 n'est plus valable car elle ne s'applique que si l'idéal $\eta\, Z_K$ est puissance p-ième d'idéal. Mais si $a^{p-1} \equiv 1 \pmod{p^2}$, l'extension $\mathbb{Q}'(\sqrt[p]{a})/\mathbb{Q}'$ est non ramifiée en p (et p-décomposée) mais ramifiée en les places de $\mathbb{Q}'$ divisant a. Si T est l'ensemble des diviseurs premiers de a, on doit alors

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

remplacer le p-corps de classes de Hilbert H' de $\mathbb{Q}'$ par sa généralisation $H'^{T'}$, la p-extension Abélienne maximale non ramifiée en dehors des places de l'ensemble T' des idéaux premiers de $\mathbb{Q}'$ au-dessus de T. Cette p-extension $H'^{T'}/\mathbb{Q}'$ est finie car T ne contient pas p (c'est essentiellement un p-corps de rayon $K'_{\mathfrak{m}'}$, $\mathfrak{m}'$ construit sur T') et joue donc un rôle analogue à celui de H' ; ici on aura $\theta^* = 1^* = \omega$ et une analyse analogue.

8.5 Conjectures sur les régulateurs p-adiques $\mathrm{Reg}_p^G(\eta)$

Les résultats du § 8.2 invitent à proposer les conjectures suivantes plus fortes que celles des §§ 8.3, 8.4.

Conjecture 8.8 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n, de groupe de Galois G. Soit $\eta \in K^\times$ tel que le $\mathbb{Z}[G]$-module F engendré par η soit de $\mathbb{Z}$-rang n. Alors pour tout p assez grand, η n'est pas une puissance p-ième locale partielle en p,* i.e., $\left\{\eta_0 \in F,\ \eta_0 \in \prod_{v\mid p} K_v^{\times p}\right\} = F^p$, *équivalent à $\mathcal{L}(\eta) = \{0\}$.*

L'énoncé suivant est de fait équivalent au précédent. On rappelle que pour tout caractère p-adique irréductible θ de G, on a $\mathrm{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod p$ et que

$$\mathrm{Reg}_p^G(\eta) := p^{-n}\ \mathrm{dét}\big(\log_p(\eta^{\tau\sigma})\big)_{\sigma,\tau\in G}$$

(le régulateur p-adique normalisé de η, Définitions 2.3 (i)) se factorise en $\mathrm{Reg}_p^G(\eta) = \prod_\theta \mathrm{Reg}_p^\theta(\eta)^{\phi(1)}$ (Remarque 2.10).

Conjecture 8.9 *Soit $K/\mathbb{Q}$ une extension Galoisienne de degré n, de groupe de Galois G. Soit $\eta \in K^\times$ tel que le $\mathbb{Z}[G]$-module engendré par η soit de $\mathbb{Z}$-rang n, et soit $\mathrm{Reg}_p^G(\eta)$ le régulateur p-adique normalisé de η. Alors pour tout p assez grand, $\mathrm{Reg}_p^G(\eta)$ est une unité p-adique.*

Remarque 8.10 La Conjecture 8.9 implique celle de Leopoldt–Jaulent [J] pour tout premier p sauf un nombre fini, mais il est préférable d'admettre cette dernière, très classique, et de dire que la Conjecture 8.9 en est une version plus forte (cf. § 2.1.4, (a) et (b)). Par négation, on obtient que s'il existe une infinité de p tels que $\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod p$, alors le $\mathbb{Z}$-rang du $\mathbb{Z}[G]$-module engendré par η est $< n$.

8.6 Conjectures en p-ramification Abélienne

Soit $H^{p\mathrm{ra}}$ la p-extension Abélienne p-ramifiée (*i.e.*, non ramifiée en dehors de p) maximale d'un corps de nombres Galoisien K réel satisfaisant à la conjecture de Leopoldt pour tout p. Soit $\widehat{K}$ la $\mathbb{Z}_p$-extension cyclotomique de K et soit $\mathcal{T}_p = \mathrm{Gal}(H^{p\mathrm{ra}}/\widehat{K})$. Pour tout p assez grand, $|\mathcal{T}_p|$ a même valuation p-adique que le régulateur normalisé de K, $p^{1-n}\mathcal{R}_p(K) \sim \prod_{\theta\neq 1} \mathrm{Reg}_p^\theta(\varepsilon)^{\phi(1)}$, où ε est une unité de Minkowski fixée [Gr1, III.2.6.5)].

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

La Conjecture 8.9 implique la conjecture suivante que l'on peut énoncer pour les corps non nécessairement Galoisiens car pour $K' \subseteq K$, $\mathcal{T}_p(K')$ s'injecte dans $\mathcal{T}_p(K)$, et toute composante $\mathcal{T}_p^\theta$, θ impair, est triviale pour tout p assez grand car liée à la θ-composante du p-groupe des classes de K [Gr1, III.2.6.1, Fig. 2.2].

Conjecture 8.11 *L'invariant $\prod_p \mathcal{T}_p$ est fini pour tout corps de nombres.*

Remarques 8.12 Rappelons qu'un corps K quelconque, tel que $\mathcal{T}_p = 1$ sous la conjecture de Leopoldt, est dit *p-rationnel* et que dans ce cas l'arithmétique de K se trivialise largement (voir une synthèse des propriétés dans [Gr1, IV.3 (b)],[MN], et les liens avec la p-régularité dont les prémices se trouvent dans [Gr3], [JN], sans parler d'une abondante bibliographie ultérieure sur le sujet). Pour K réel et pour tout $p \geq 2$, la p-rationalité entraîne facilement la conjecture de Greenberg [Gre], ce qui éclaire le contexte.

On en déduirait des propriétés analogues sur le résidu de la fonction zêta p-adique [Coa, Appendix], [Se2]. Lorsque la p-valuation de $\zeta_K(2-p)$ est négative, elle vaut -1 [Se2, Théorème 6]. Dans le cadre de la Conjecture 8.11, on aurait alors $\frac{\zeta_K(2-p)}{\zeta_{\mathbb{Q}}(2-p)} \sim |\mathcal{T}_p| = 1$ pour tout p assez grand [Hat].

Soit S l'ensemble formé des p-places de K et des places à l'infini, et soit $G_S(K)$ le groupe de Galois de l'extension algébrique S-ramifiée maximale de K, *i.e.*, non ramifiée en dehors de S. Alors sur un plan cohomologique, on aurait $\mathrm{H}^2(G_S(K), \mathbb{Z}_p) \simeq \mathcal{T}_p^* = 1$, pour tout p assez grand.

8.7 Justifications cohomologiques plus générales

Nous faisons ici quelques commentaires sur des résultats dont le niveau mathématique dépasse largement toute approche heuristique, mais cette confrontation nous a semblée très convaincante. On pourra se référer aux différents articles de [BK] dont [Ko, Ng].

La principale idée directrice, liée à la conjecture de Bloch–Kato, est qu'il existe, de façon assez systématique, des invariants globaux *finis* dont les spécialisations p-adiques, de nature cohomologique, sont les objets arithmétiques (plus ou moins classiques) d'un corps de nombres K (comme les p-groupes de classes, les groupes $\mathcal{T}_p$ de p-ramification, des régulateurs p-adiques, certains groupes de cohomologie étale, etc.). Ce point de vue conjectural est universellement admis, d'autant plus que des preuves en ont été apportées assez largement. Rappelons succintement l'essentiel des résultats connus.

On part des notations du § 8.6. Pour $m \in \mathbb{Z}$, soit $\mathbb{Z}_p(m)$ le $G_S(K)$-module $\mathbb{Z}_p$ muni de l'action définie par le caractère χ^m, où $\chi : G_S(K) \to \mathbb{Z}_p^\times$ est le caractère de l'action de $G_S(K)$ sur μ_{p^∞}.

On dit que K est (p, m)-rationnel si $\mathrm{H}^2(G_S(K), \mathbb{Z}_p(m))$ est trivial ; la p-rationalité usuelle évoquée au § 8.6 correspond à $m = 0$ qui semble être le cas le plus délicat. La finitude de $\mathrm{H}^2(G_S(K), \mathbb{Z}_p(m))$ équivaut à un m-analogue de la conjecture de Leopoldt en termes de "régulateurs p-adiques" convenables. Les résultats sur la finitude

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press

d'objets globaux dont les spécialisations p-adiques sont les $\mathrm{H}^2(G_S(K),\mathbb{Z}_p(m))$, pour m fixé, sont les suivants (d'après des indications privées de Thong Nguyen Quang Do) :

(i) Pour $m \geq 2$, c'est une conséquence de la "conjecture de Quillen–Lichtenbaum" maintenant Théorème de Voevodsky. La finitude découle alors de celle du groupe de K-théorie $\mathrm{K}_{2m-2}(Z_K)$ via un isomorphisme (non trivial) de la forme ($p > 2$)

$$\mathrm{K}_{2m-2}(Z_K) \otimes \mathbb{Z}_p \simeq \mathrm{H}^2(G_S(K),\mathbb{Z}_p(m)).$$

(ii) Le cas $m = 1$ correspond, sous une forme voisine (due au fait que le groupe de cohomologie n'est pas fini à cause du groupe de Brauer), à la conjecture de Gross, et le cas $m < 0$ est peu ou pas connu : si $m < 0$ est impair, alors $\mathrm{H}^2(G_S(K),\mathbb{Z}_p(m))$ est fini ; le cas $m < 0$ pair est inconnu.

(iii) Le cas $m = 0$ définit le cadre "conjecture de Leopoldt et p-groupe de torsion $\mathcal{T}_p$, dual de $\mathrm{H}^2(G_S(K),\mathbb{Z}_p)$", cadre pour lequel une situation analogue est donc conjecturée dans la lignée des travaux "motiviques" précédents de Voevodsky.

Aussi notre approche Diophantienne conjecturale est-elle renforcée par les profonds résultats rappelés ci-dessus, l'intérêt étant que la notion de régulateur p-adique (normalisé) d'un nombre algébrique quelconque est beaucoup plus générale.

9 Conclusion

Nous avons essayé de donner un maximum de justifications, en particulier par le fait que lorsque les probabilités d'une propriété de p-divisibilité de $\mathrm{Reg}_p^G(\eta)$ sont au plus $\frac{O(1)}{p^2}$, les principes heuristiques de type Borel–Cantelli suggèrent un nombre fini de solutions p et même aucune solution la plupart du temps puisque la somme des $\frac{1}{p^2}$ est très petite ($\sum_{p\geq 2}\frac{1}{p^2} \approx 0.45$, $\sum_{p\geq 10^4}\frac{1}{p^2} \approx 9\times 10^{-6}$).

Il reste les cas de p-divisibilité minimale $\mathrm{Reg}_p^G(\eta) \sim p^{\phi(1)}$ (Définition 4.1) pouvant faire obstruction si l'Heuristique 7.4 est inexacte ; dans ce cas, le "nombre prévisible" de solutions $p \leq x$ serait $O(1)\log_2(x) + O(1)$ et les invariants arithmétiques p-adiques correspondants (vus au § 8.7) auraient, pour tout p assez grand, une structure de G-module minimale canonique, *e.g.*, $\mathrm{H}^2(G_S(K),\mathbb{Z}_p) \simeq V_\theta$ pour θ tel que $f = \delta = 1$.

Il serait enfin utile d'avoir une estimation analytique de M_p qui précise les notions de solutions exceptionnelles et abondantes (§ 7.1 ; voir également [Gr5]).

Mais s'il doit y avoir une certaine cohérence des mathématiques, on peut alors croire que de telles conjectures de finitude sont légitimes. Par exemple, on peut déduire de cette étude que la conjecture de Leopoldt–Jaulent sur la non nullité des régulateurs p-adiques est une forme extrêmement faible de la réalité.

Remerciements Je remercie Gérald Tenenbaum pour d'utiles renseignements en théorie probabiliste des nombres, Henri Lombardi et Thong Nguyen Quang Do pour ses commentaires "cohomologiques" éclairant nos conjectures issues de la forme forte de la conjecture de Leopoldt–Jaulent, et Ján Mináč pour son amical soutien dans la réalisation des objectifs de cet article. Je remercie enfin vivement le Rapporteur anonyme pour sa lecture attentive et ses remarques.

Références

[P] K. Belabas et al., *Pari/gp* Version 2.5.3 Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[Coa] J. Coates, *p-adic L-functions and Iwasawa's theory*. Dans : Algebraic number fields : *L*-functions and Galois properties Academic Press, London, 1977, pp. 269–353.

[BK] J. Coates, A. Raghuram, A. Saikia, et R. Sujatha (Eds), *The Bloch–Kato conjecture for the Riemann Zeta function*, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).

[C] K. Conrad, *The origin of representation theory*. Enseign. Math. **44**(1998), 361–392.

[CDP] R. Crandall, K. Dilcher, et C. Pomerance, *A search for Wieferich and Wilson primes*. Math. Comp. **66**(1997), no. 217, 433–449. http://dx.doi.org/10.1090/S0025-5718-97-00791-6

[EM] R. Ernvall et T. Metsänkylä, *On the p-divisibility of Fermat quotients*. Math. Comp. **66**(1997), 1353–1365. http://dx.doi.org/10.1090/S0025-5718-97-00843-0

[Gr1] G. Gras, *Class field theory. From theory to practice*. Springer Monographs in Mathematics, Springer-Verlag 2003 ; second corrected printing 2005. http://dx.doi.org/10.1007/978-3-662-11323-3

[Gr2] G. Gras, *Étude probabiliste des quotients de Fermat*. Functiones et Approximatio, Commentarii Mathematici, Vol. 54, 1 (2016). https://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[Gr3] G. Gras, *Remarks on K_2 of number fields*. J. Number Theory **23**(1986), 322–335. http://dx.doi.org/10.1016/0022-314X(86)90077-6

[Gr4] G. Gras, *Programmes PARI*. https://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[Gr5] G. Gras, *Compléments heuristiques et probabilistes sur les quotients de Fermat*, 2016 (preprint). https://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[Gr6] G. Gras, *On the order modulo p of an algebraic number.* 2016 (submitted). https://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[GM] H. Graves et M. R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*. J. Number Theory **133**(2013), 1809–1813. http://dx.doi.org/10.1016/j.jnt.2012.10.012

[Gre] R. Greenberg, *Iwasawa theory—past and present*. In : Class field theory - its centenary and prospect (Tokyo 1998). Adv. Stud. Pure Math, 30. Math. Soc. Japan, Tokyo, 2001, pp. 335–385.

[Hat] K. Hatada, *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2 - p$*. Comment. Math. Univ. St. Paul. **36**(1987), no. 1, 41–51.

[H-B] R. Heath-Brown, *An estimate For Heilbronn's exponential sum*. In : Conference in honor of Heini Halberstam. Analytic Number Theory, 2 (1996), Birkhüser 1996. http://eprints.maths.ox.ac.uk/157/1/heilbron.pdf

[J] J-F. Jaulent, *Sur l'indépendance ℓ-adique de nombres algébriques*. J. Number Theory **20**(1985), no. 2, 149–158. http://dx.doi.org/10.1016/0022-314X(85)90035-6

[JN] J-F. Jaulent et T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers, et ramification restreinte*. J. Théor. Nombres Bordeaux **5**(1993), 343–363. http://dx.doi.org/10.5802/jtnb.98

[KR1] W. Keller et J. Richstein, *Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$*. Math. Comp. **74**(2004), no. 250, 927–936. http://dx.doi.org/10.1090/S0025-5718-04-01666-7

[KR2] ———, *The continuing search for Wieferich primes*. Math. Comp. **75**(2005), no. 251, 1559–1563. http://dx.doi.org/10.1090/S0025-5718-05-01723-0,

[Ko] M. Kolster, *The norm residue theorem and the Quillen-Lichtenbaum conjecture*, Dans : J. Coates, et al., eds. The Bloc—Kato conjecture for the Riemann Zeta function, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).

[MN] A. Movahhedi et T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*. Dans : Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math. 81, Birkhäuser, Boston, 1990, pp. 155–200.

[Ng] T. Nguyen Quang Do, *On the Determinantal approach to the Tamagawa number conjecture*. Dans : J. Coates et al. eds., The Bloch–Kato conjecture for the Riemann Zeta function, Conf. July 2012, London Math. Soc. Lecture Note Series (2015).

[OS] A. Ostafe et I. E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*. SIAM J. Discrete Math. **25**(2011), no. 1, 50–71. http://dx.doi.org/10.1137/100798466

[Se1] J-P. Serre, *Représentations linéaires des groupes finis*, cinquième édition corrigée et augmentée de nouveaux exercices, Coll. Méthodes, Hermann 1998.

[Se2] _____, *Sur le résidu de la fonction zêta p-adique d'un corps de nombres.* C. R. Acad. Sci. Paris **287**(1978), no. 4, A183–A188.
[Sh] I. E. Shparlinski, *On vanishing Fermat quotients and a bound of the Ihara sum.* Kodai Math. J. **36**(2013), no. 1, 99–108. http://dx.doi.org/10.2996/kmj/1364562722
[Si] J. H. Silverman, *Wieferich's criterion and the abc-conjecture.* J. Number Theory **30**(1988), no. 2, 226–237. http://dx.doi.org/10.1016/0022-314X(88)90019-4
[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres.* 3^e édition, Coll. Échelles, Belin 2008.
[W] M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences* Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics (2013). http://www.math.jussieu.fr/~miw/articles/pdf/abcLahore2013VI
[Wa] L. C. Washington, *Introduction to cyclotomic fields*. Graduate Texts in Math. 83, Springer-Verlag, New York, 1997. http://dx.doi.org/10.1007/978-1-4612-1934-7

Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans, France
courriel: g.mn.gras@wanadoo.fr

https://doi.org/10.4153/CJM-2015-026-3 Published online by Cambridge University Press