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

Georges Gras

LES θ-RÉGULATEURS LOCAUX D'UN NOMBRE ALGÉBRIQUE CONJECTURES p-ADIQUES

par

Georges Gras

Résumé. — Soit $K/\mathbb{Q}$ une extension Galoisienne finie de degré n, de groupe de Galois G, et soit $\eta \in K^\times$. Pour tout p premier assez grand (étranger à n, $\mathrm{Disc}(K)$, et η), nous définissons, par utilisation du théorème de Frobenius sur les déterminants de groupes, la famille $\big(\Delta_p^\theta(\eta) \in \mathbb{F}_p\big)_\theta$ des θ-régulateurs locaux de η, indexée par les caractères $\mathbb{Q}_p$-irréductibles θ de G.

A chaque $\Delta_p^\theta(\eta)$ est associée une représentation linéaire $\mathcal{L}^\theta \simeq \delta\, V_\theta$, $0 \le \delta \le \varphi(1)$ (où V_θ est la représentation de caractère θ et $\varphi \,|\, \theta$ absolument irréductible) ; la représentation $\mathcal{L}^\theta$ caractérise des propriétés de $\Delta_p^\theta(\eta)$, dont sa nullité équivalente à $\delta \ge 1$ (Théorème 3.11, §3.2.3).

Lorsque $\eta \in \mathbb{Q}^\times$ et $\theta = 1$, $\Delta_p^1(\eta)$ est le p-quotient de Fermat de η. Lorsque η est une "unité de Minkowski" (pour K réel), chaque $\Delta_p^\theta(\eta)$, $\theta \ne 1$, donne le résidu modulo p de la θ-composante $\mathrm{Reg}_p^\theta(\eta)$ dans la factorisation $\prod_{\theta\ne1}(\mathrm{Reg}_p^\theta(\eta))^{\varphi(1)}$ de $p^{1-n}\mathrm{Reg}_p(K)$, où $\mathrm{Reg}_p(K)$ est le régulateur p-adique classique de K.

Nous suggérons, à partir d'une propriété générale des déterminants de groupes et de l'existence de la représentation $\mathcal{L}^\theta$, que la "probabilité" de nullité de $\Delta_p^\theta(\eta)$ avec $\mathcal{L}^\theta \simeq \delta\, V_\theta$ est en $\frac{O(1)}{p^{f\delta^2}}$ (cf. §4.3.2), où f est le degré résiduel de p dans le corps des valeurs des caractères $\varphi \,|\, \theta$, et que les $\Delta_p^\theta(\eta)$ sont des variables indépendantes.

Nous conjecturons alors que $p^{1-n}\mathrm{Reg}_p(K)$, qui mesure l'ordre du p-groupe de torsion en p-ramification Abélienne au-dessus de K, est pour p assez grand une unité p-adique sauf peut-être pour un ensemble de nombres premiers p de densité nulle. Pour ces cas dits "de p-divisibilité minimale $p^{\varphi(1)}$" (i.e., un unique $\Delta_p^\theta(\eta)$, tel que $\delta = f = 1$, est nul), il reste possible, η étant alors une "puissance p-ième locale partielle" en p, de proposer, en lien avec la conjecture ABC, une conjecture plus forte aboutissant à la même conclusion pour tout p assez grand (Section 7). D'autres aspects conjecturaux sur le quotient de Fermat sont discutés.

Nous précisons et vérifions ces propriétés par des études numériques portant sur des corps cubiques et quintiques cycliques et sur un corps non Abélien (groupe D_6), et publions les programmes "PARI" correspondants.

***Classification mathématique par sujets* (2000).** — Primary 11F85; 11C20;11R27; 11S05; Secondary 11R37; 11R29.
Mots clefs. — Frobenius group determinants; characters; p-adic regulators; p-adic rank; Leopoldt's conjecture; Fermat quotient; Abelian p-ramification; probabilistic number theory.

Je remercie Gérald Tenenbaum pour un échange relatif à la théorie probabiliste des nombres et pour d'utiles renseignements. Je remercie Henri Lombardi pour le signalement d'ambiguïtés et pour ses commentaires.

Abstract. — Let $K/\mathbb{Q}$ be a finite Galois extension of degree n, of Galois group G, and let $\eta \in K^\times$. For all large enough prime p (prime to n, $\mathrm{Disc}(K)$, and η), we define, by use of the Frobenius theorem on group determinants, the family $\big(\Delta_p^\theta(\eta) \in \mathbb{F}_p\big)_\theta$ of local θ-regulators of η, indexed by the $\mathbb{Q}_p$-irreducible characters θ of G.

At each $\Delta_p^\theta(\eta)$ is associated a linear representation $\mathcal{L}^\theta \simeq \delta\, V_\theta$, $0 \le \delta \le \varphi(1)$ (where V_θ is the representation of character θ and $\varphi \,|\, \theta$ absolutely irreducible); the representation $\mathcal{L}^\theta$ characterizes some properties of $\Delta_p^\theta(\eta)$, including its nullity equivalent to $\delta \ge 1$ (Theorem 3.11, §3.2.3).

When $\eta \in \mathbb{Q}^\times$ and $\theta = 1$, $\Delta_p^1(\eta)$ is the p-Fermat quotient of η. When η is a "Minkowski unit" (for K real), each $\Delta_p^\theta(\eta)$, $\theta \ne 1$, gives the residue modulo p of the θ-component $\mathrm{Reg}_p^\theta(\eta)$ in the factorization $\prod_{\theta \ne 1} (\mathrm{Reg}_p^\theta(\eta))^{\varphi(1)}$ of $p^{1-n}\mathrm{Reg}_p(K)$, where $\mathrm{Reg}_p(K)$ is the classical p-adic regulator of K.

We suggest, starting from a general property of group determinants and the existence of the representation $\mathcal{L}^\theta$, that the "probability" of nullity of $\Delta_p^\theta(\eta)$ with $\mathcal{L}^\theta \simeq \delta\, V_\theta$ is about $\frac{O(1)}{p^{f\delta^2}}$ (cf. §4.3.2), where f is the residue degree of p in the field of values of the characters $\varphi \,|\, \theta$, and that the $\Delta_p^\theta(\eta)$ are independent variables.

We conjecture that $p^{1-n}\mathrm{Reg}_p(K)$, which measures the order of the p-torsion group in Abelian p-ramification over K, is for p large enough a p-adic unit except perhaps for a set of prime numbers of zero density. For these cases said "of minimal p-divisibility $p^{\varphi(1)}$" (i.e., a single $\Delta_p^\theta(\eta)$, such that $\delta = f = 1$, is zero), it remains possible, η being then a "partial local pth power" at p, to propose, in connection with the ABC conjecture, a stronger conjecture leading to the same conclusion for all large enough p (Section 7). Some other conjectural aspects on the Fermat quotient are discussed.

We precise and verify these properties through numerical studies on particular cyclic cubic and quintic fields and a non-Abelian field (group D_6), and we publish the corresponding "PARI" programs.

1. Introduction

Soit $K/\mathbb{Q}$ une extension Galoisienne de degré fini $n \ge 1$, de groupe de Galois G. On considère $\eta \in K^\times$ et on désigne par F le $\mathbb{Z}[G]$-module engendré par η. On utilise la notation exponentielle pour la conjuguaison de η par $\sigma \in G$ (loi de module à gauche) qui se traduit par l'écriture $(\eta^\sigma)^\tau =: \eta^{\tau\sigma}$ pour tout $\sigma, \tau \in G$.

Nous supposerons toujours que le nombre premier p considéré est assez grand, ce qui fait que l'on peut supposer p impair, non diviseur de n, non ramifié dans $K/\mathbb{Q}$, et étranger à η. Par exemple, dans le cas où η est une unité dont les conjugués engendrent un sous-groupe d'indice fini dans le groupe des unités de K (unité de Minkowski), on peut supposer que p ne divise pas cet indice.

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 $v \,|\, p$, on désigne par $\mathfrak{p}_v$ l'idéal premier associé à v. Précisons une fois pour toutes que dans $Z_{K,(p)}$, toute congruence de la forme $\beta \equiv 0 \pmod p$ est globale et doit se lire $\beta \equiv 0$ $(\mathrm{mod}\ \prod_{v\,|\,p} \mathfrak{p}_v)$ (p non ramifié) ; elle implique que si $\beta = \sum_{i=1}^n A_i\, e_i$ est écrit sur une $\mathbb{Z}_{(p)}$-base $(e_i)_{i=1,\ldots,n}$ de $Z_{K,(p)}$, on a $A_i \equiv 0 \pmod p$ pour $i = 1, \ldots, n$.

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

$$\eta^{p^{n_p}-1} \equiv 1 \pmod{\mathfrak{p}_v} \text{ pour tout } v \,|\, p\ ;$$

par hypothèse $\prod_{v\,|\,p} \mathfrak{p}_v = (p)$, d'où $\eta^{p^{n_p}-1} \equiv 1 \pmod p$ et :

$$\eta^{p^{n_p}-1} = 1 + p\, \alpha_p(\eta), \quad \alpha_p(\eta) \in Z_{K,(p)},$$

ce qui conduit par Galois à la relation :

$$\alpha_p(\eta^\sigma) \equiv \alpha_p(\eta)^\sigma \pmod p, \quad \forall \sigma \in G,$$

et aux propriétés “logarithmiques” suivantes ($\eta, \eta' \in K^\times$, $\lambda \in \mathbb{Z}$) :

$$\alpha_p(\eta\,\eta') \equiv \alpha_p(\eta) + \alpha_p(\eta') \pmod p \ \ \& \ \ \alpha_p(\eta^\lambda) \equiv \lambda\,\alpha_p(\eta) \pmod p.$$

2. Régulateurs $\mathrm{Reg}_p^G(\eta), \mathrm{Reg}_p^\chi(\eta)$ – Régulateurs locaux $\Delta_p^\theta(\eta)$

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

On considère le $\mathbb{Q}_p$-espace vectoriel $\prod_{v\,|\,p} K_v$, de dimension n, 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 $v\,|\,p$ mais la notation K_v rappelle que cette extension locale est *munie* du plongement $\sigma_v : K \longrightarrow \mathbb{C}_p$, ce qui permet le plongement diagonal d'image dense $i_p : K \longrightarrow \prod_{v\,|\,p} K_v$ qui à $x \in K$ associe $(\sigma_v(x))_{v\,|\,p}$.

2.1.1. Logarithmes p-adiques. — Le logarithme p-adique $\log_p : K^\times \longrightarrow K\mathbb{Q}_p \subset \mathbb{C}_p$ est défini sur l'ensemble des $1 + p\,x$, $x \in Z_{K,(p)}$ par la série usuelle :

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

Dans le cas du nombre $\eta \in K^\times$, on utilise la relation fonctionnelle :

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

Cette fonction $\log_p$, vue modulo p^N, $N \geq 2$, est représentée par des éléments de $Z_{K,(p)}$ et est un homomorphisme de G-modules pour la loi définie par :

$$\sigma\big(\log_p(\eta) \pmod{p^N}\big) := \log_p(\eta^\sigma) \pmod{p^N},$$

en considérant la congruence :

$$\begin{aligned} \sigma\big(\log_p(\eta) \pmod{p^N}\big) \ &\equiv \ \frac{1}{p^{n_p} - 1}\, \sigma\Big(\sum_{1 \leq i \leq N} (-1)^{i+1} \frac{(p\,\alpha_p(\eta))^i}{i}\Big) \\ &\equiv \ \frac{1}{p^{n_p} - 1} \sum_{1 \leq i \leq N} (-1)^{i+1} \frac{(p\,\alpha_p(\eta)^\sigma)^i}{i} \pmod{p^N}, \end{aligned}$$

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

Soit $\log_{(p)} = \log_p \circ\, i_p$ l'application définie sur le groupe $K_{(p)}^\times$ des η étrangers à p par :

$$\begin{array}{ccc} K_{(p)}^\times & \longrightarrow & \prod_{v\,|\,p} K_v\ . \\ \eta & \longmapsto & \big(\log_p(\eta^{\sigma_v})\big)_{v\,|\,p} \end{array}$$

On appelle rang p-adique du $\mathbb{Z}[G]$-module F engendré par η, l'entier :

$$\mathrm{rg}_p(F) \ := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_{(p)}(F)) \ \ (\text{cf. } [\mathbf{Gr1}], \text{III.3.1.2}).$$

Lemme 2.1. — *Soit p premier impair non ramifié dans $K/\mathbb{Q}$ et soit $\lambda \in Z_{K,(p)}$. Si $\lambda \notin p\, Z_{K,(p)}$, 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 $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v\,|\,p} \mathrm{Tr}_v(\sigma_v(\lambda u))$. Par hypothèse, il existe un ensemble non vide Σ de places $v\,|\,p$ telles que $\sigma_v(\lambda)$ (donc $\sigma_v(\lambda u)$ pour tout u étranger à p) est une unité de K_v. Pour $v_0 \in \Sigma$, on écrit :

$$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v\,|\,p,\, v\neq v_0} \mathrm{Tr}_v(\sigma_v(\lambda u)) + \mathrm{Tr}_{v_0}(\sigma_{v_0}(\lambda u)) =: a + \mathrm{Tr}_{v_0}(\sigma_{v_0}(\lambda u)).$$

Comme p est non ramifié dans $K/\mathbb{Q}$, les traces résiduelles en p sont surjectives et puisque $\sigma_{v_0}(\lambda u)$ est une unité, il suffit de prendre $u \equiv 1 \pmod{\prod_{v,\, v\neq v_0} \mathfrak{p}_v}$ (auquel cas a ne dépend plus de u) et $u \equiv u_0 \pmod{\mathfrak{p}_{v_0}}$ convenable tel que par exemple $\mathrm{Tr}_{v_0}(\sigma_{v_0}(\lambda u)) \equiv 1 - a \pmod p$ 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, and 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 une relation de dépendance modulo p^N, $N \geq 2$, des vecteurs $\ell_\sigma = (\ldots, \log_p(\eta^{\tau\sigma^{-1}}), \ldots)_\tau$:*

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

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

Il en résulte aussi la relation $\sum_{\sigma\in G} \lambda'(\sigma) \alpha_p(\eta)^{\tau\sigma^{-1}} \equiv 0 \pmod p$ pour tout $\tau \in G$.

Démonstration. — On peut toujours, modulo p^N, supposer que $\lambda(\sigma) \in Z_{K,(p)}$ pour tout $\sigma \in G$. On se ramène (par exemple) à $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda(1)) \equiv 1 \pmod p$ en multipliant la congruence par u étranger à p convenable (cf. Lemme 2.1). Par conjugaison par $\nu \in G$ on obtient $\sum_{\sigma\in G} \lambda(\sigma)^\nu \log_p(\eta^{\nu\tau\sigma^{-1}}) \equiv 0 \pmod{p^N}$ pour tout $\tau \in G$, équivalent à $\sum_{\sigma\in G} \lambda(\sigma)^\nu \log_p(\eta^{s\,\sigma^{-1}}) \equiv 0 \pmod{p^N}$ pour tout $s \in G$.
En prenant la trace dans $K/\mathbb{Q}$ des coefficients (sommation sur ν), 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 $Z_{K,(p)}$-dépendance linéaire modulo p^N 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 $\mathbb{Z}_p$.

2.1.2. Régulateurs. — En utilisant l'isomorphisme $\prod_{v\,|\,p} K_v \simeq K \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p[G]$, on en déduit que le rang p-adique de F est égal au rang sur $\mathbb{Z}_p$ (au sens précédent) du déterminant de Frobenius (ou régulateur p-adique de η) :

$$\mathrm{Det}^G(\log_p(\eta)) := \det\big(\log_p(\eta^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G}$$

(voir [**Gr1**], III.3.1.8, où il est aussi fait allusion à la conjecture de Schanuel).
Si ce rang est donné par un plus grand mineur M non nul, M est non nul modulo toute puissance p^N assez grande.

[(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.

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 du groupe F est égal à son $\mathbb{Z}$-rang $\mathrm{rg}(F) := \dim_{\mathbb{Q}}(F \otimes \mathbb{Q})$.

Afin de procéder à des calculs concrets, il convient d'aménager les aspects p-adiques ci-dessus en se ramenant à des congruences modulo p^N dans $Z_{K,(p)}$. On notera d'abord que tout mineur d'ordre r est de façon canonique divisible par p^r, pour tout $p > 2$ non ramifié, puisque l'on a, dans $Z_{K,(p)}$, la congruence :

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

D'où la définition suivante :

Définition 2.3. — (i) On considère (pour p assez grand) le déterminant à coefficients entiers :

$$\mathrm{Det}^G\Big(\frac{-1}{p} \log_p(\eta)\Big) = \Big(\frac{-1}{p}\Big)^n \mathrm{Det}^G(\log_p(\eta)) = \det\Big(\frac{-1}{p} \log_p(\eta^{\tau\sigma^{-1}})\Big)_{\sigma,\tau\in G}.$$

Ce déterminant de Frobenius, désigné dans l'article par $\mathrm{Reg}_p^G(\eta)$, est appelé le régulateur p-adique normalisé de η.

On a $\mathrm{Reg}_p^G(\eta) \equiv \Delta_p^G(\eta) \pmod p$, où :

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

est appelé le régulateur (normalisé) local de η car uniquement défini modulo p.

(ii) Pour K Galoisien réel, le régulateur p-adique usuel $\mathrm{Reg}_p(K)$ est donné par un mineur d'ordre $n-1$ de $\mathrm{Det}^G(\log_p(\varepsilon)) = \det\big(\log_p(\varepsilon^{\tau\sigma^{-1}})\big)_{\sigma,\tau\in G}$, où ε est une unité de Minkowski, et l'entier p-adique $p^{1-n}\mathrm{Reg}_p(K) = \det\Big(\frac{-1}{p} \log_p(\varepsilon^{\tau\sigma^{-1}})\Big)_{\sigma\neq 1,\tau\neq 1}$ est appelé le régulateur p-adique normalisé de K (p assez grand).

Le plongement diagonal de K dans $\prod_{v\,|\,p} K_v$, au moyen de $i_p = (\sigma_v)_{v\,|\,p}$, étant dense, on peut considérer que, modulo p^N, la fonction $\frac{-1}{p}\log_p$ est à valeurs dans K. D'après le Lemme 2.2, §2.1.1, on se ramène à des raisonnement d'algèbre linéaire sur $\mathbb{Z}/p^N\mathbb{Z}$; en particulier, le rang p-adique de F est le $\mathbb{Z}/p^N\mathbb{Z}$-rang de la matrice $\big(\frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}}) \pmod{p^N}\big)_{\sigma,\tau\in G}$, pour tout N assez grand.

Si un mineur M d'ordre $\mathrm{rg}(F)$ de cette matrice est non nul, alors il donne le rang p-adique de 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, le rang p-adique de F est a priori supérieur ou égal au $\mathbb{Z}/p\mathbb{Z}$-rang de $\big(\alpha_p(\eta)^{\tau\sigma^{-1}} \pmod p\big)_{\sigma,\tau\in G}$.

Dans **[Hat]**, Hatada a procédé, pour certains corps de nombres, à une étude statistique de la nullité modulo p du régulateur normalisé en utilisant le fait que sa p-valuation est celle de $p\,\zeta_K(2-p)$, où ζ_K est la fonction zêta de K.

Remarque 2.4. — (a) *Analyse locale.* On ne fait aucune hypothèse sur le $\mathbb{Z}$-rang de F. Si l'on a dans F la relation $\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)} = 1$, $\lambda(\sigma) \in \mathbb{Z}$, alors, pour tout p étranger à η on a $\sum_{\sigma\in G} \lambda(\sigma) \log_p(\eta^{\sigma^{-1}}) = 0$, ce qui conduira pour certains caractères rationnels χ à des χ-régulateurs (notés $\mathrm{Reg}_p^\chi(\eta)$) identiquements nuls pour tout p.

Ces relations se transmettent pour tout p en les relations plus faibles :

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

entre les conjugués de $\alpha_p(\eta)$; elles sont dites triviales (elles ne sont pas dûes à une circonstance numérique pour le p considéré, mais à l'existence d'une relation dans F donnée par des $\lambda(\sigma)$ indépendants de p, ce qui sera caractérisé au Lemme 2.14, §2.2.6). Ceci n'a pas lieu si $F \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$.

Inversement, si l'on se donne à partir de η quelconque la famille de congruences :

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

(ensemble de conditions locales car les $\alpha_p(\eta)$ ne sont connus que modulo p), la question est de savoir si elles sont globalisables sous la forme $\prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)} = 1$. Supposons ne disposer que des congruences $\sum\limits_{\sigma\in G} \lambda(\sigma)\, \alpha_p(\eta)^{\sigma^{-1}} \equiv 0 \pmod p$ pour presque tout p (éventuellement au sens du §7.1), avec des $\lambda(\sigma) \in \mathbb{Z}$ indépendants de p. Soit $\Lambda := \prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)} \in F$; alors $\log_p(\Lambda) \equiv 0 \pmod{p^2}$ et Λ est, dans $\prod_{v\,|\,p} K_v$, de la forme $\xi\,(1+\beta\, p)^p$, où ξ est de torsion d'ordre étranger à p (pour tout p assez grand) ; donc $\Lambda \in \prod_{v\,|\,p} K_v^{\times p}$ pour presque tout p. Conjecturalement Λ est une racine de l'unité de K (cf. Conjecture 7.4, §7.2.3).

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

$$\sum_{\sigma\in G} \widehat\lambda_p(\sigma) \log_{(p)}(\eta^{\sigma^{-1}}) = 0, \quad \text{où } \log_{(p)} = \log_p \circ\, i_p,$$

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 $F \otimes \widehat{\mathbb{Z}} \longrightarrow \widehat U$, 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 ($U_v^1 = \mu_p(K_v) \times U'$, U' $\mathbb{Z}_p$-libre).

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

Comme $\log_{(p)}(\widehat\Lambda_p) = 0$ pour tout p étranger à η, on a pour toute place v de K étrangère à η, $i_v(\widehat\Lambda) = \xi_v$, 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 $v\,|\,p$ telles que ξ_v est d'ordre divisible par p sont en nombre fini). On peut donc écrire :

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

En supposant l'analogue pour F de la caractérisation locale–globale de la conjecture de Leopoldt–Jaulent (cf. [**J**], § 2) pour les nombres premiers p (voir aussi [**Gr1**], III.3.6.6 pour le cas du groupe des unités), on peut affirmer (sous cette conjecture pour tout p) que $i(F \otimes \widehat{\mathbb{Z}}) \bigcap \prod\limits_{p,\,(p,\eta)=1} \Big(\prod\limits_{v,\, v(\eta)=0} \mu_p(K_v)\Big) = i(\mu(K))$.

On en déduit que $\widehat\Lambda_p$ est une racine de l'unité ζ_p de K pour tout p étranger à η.

Si l'on suppose $\widehat\lambda_p(\sigma) \equiv \lambda(\sigma) \pmod p$ pour tout $\sigma \in G$ et tout p étranger à η, où les $\lambda(\sigma)$ sont des entiers rationnels donnés, alors $\Lambda := \prod_{\sigma\in G}(\eta^{\sigma^{-1}})^{\lambda(\sigma)} \in F$ est égal à $\widehat\Lambda_p$ à une puissance p-ième locale près, donc $\Lambda = \zeta_p\, \gamma_p^p$, $\gamma_p \in \prod_{v\,|\,p} K_v^{\times p}$ pour tout p étranger à η ; on obtient la situation de la Remarque 2.4 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 de ce contexte p-adique classique concernant la conjecture de Leopoldt–Jaulent ; mais en contrepartie, on a dû supposer l'existence de la famille d'entiers rationnels $(\lambda(\sigma))_{\sigma\in G}$ indépendante de p vérifiant la relation (*).

Notre principal objectif est de voir sous quelles conditions et avec quelle "probabilité" le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ est divisible par p assez grand. D'après ce qui précède et le Lemme 2.2, §2.1.1, on a $\mathrm{Reg}_p^G(\eta) \equiv 0 \pmod p$ si et seulement si il existe une relation de $\mathbb{Z}/p\mathbb{Z}$-dépendance des vecteurs-lignes $\ell_\sigma = (\ldots, \frac{-1}{p}\log_p(\eta^{\tau\sigma^{-1}}), \ldots)_\tau \equiv (\ldots, \alpha_p(\eta)^{\tau\sigma^{-1}}, \ldots)_\tau \pmod p$, pour $\sigma \in G$ (ceci sera repris au §3.1).

Comme $\mathrm{Reg}_p^G(\eta)$ se factorise en produit de puissances de χ-régulateurs $\mathrm{Reg}_p^\chi(\eta)$ (pour les caractères rationnels irréductibles χ de G), on étudie la divisibilité par p de ces facteurs. 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 $\varphi \,|\, \chi$ de G. On aura ensuite $\mathrm{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod p$ en termes de θ-régulateurs locaux de la forme $\Delta_p^\theta(\eta) := \mathrm{Det}^\theta(\alpha_p(\eta))$ (définis seulement modulo p et étudiés au §2.3).

Une première étude montrera que la probabilité d'avoir $\mathrm{Reg}_p^\theta(\eta)$ et $\mathrm{Reg}_p^{\theta'}(\eta)$ nuls modulo p, pour $\theta \neq \theta'$, est le produit des probabilités (indépendance), donc au plus en $\frac{O(1)}{p^2}$, et on pourra "exclure" cette éventualité pour tout p assez grand et se limiter au cas d'une unique θ-composante nulle modulo p (cf. §§3.2, 4.2).

2.2. Les déterminants de groupes (ou de Frobenius). — Pour nos objectifs heuristiques nous utilisons le cas Abélien très classique (cf. [**Wa**], Lemma 5.26 ou [**C**], § 2) ainsi que le cas des groupes non commutatifs pour lesquels les aspects probabilistes sont plus délicats au niveau de leurs caractères irréductibles de degrés ≥ 2 ; à cette fin nous commençons par un rappel général en termes de représentations (pour un exposé sur les représentations et les caractères, voir [**Se1**]).

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

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

$$\pi_i^\varphi = \frac{\varphi(1)}{n} \sum_{\nu \in G} a_{ii}^\varphi(\nu^{-1})\, \nu, \quad i = 1, \ldots, \varphi(1),$$

qui forment un système d'idempotents orthogonaux au-dessus de $e_\varphi = \sum_i \pi_i^\varphi$.

2.2.2. Rappels sur les déterminants de groupes (d'après [**C**]). — Soit G un groupe fini et soit $\mathrm{Det}^G(X) = \det\big(X_{\tau\sigma^{-1}}\big)_{\sigma,\tau \in G}$ le déterminant du groupe G, ou déterminant de Frobenius, en les indéterminées $X := (X_\nu)_{\nu \in G}$. On a alors la formule :

$$\mathrm{Det}^G(X) = \prod_\varphi \det\Big(\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1})\Big)^{\varphi(1)}.$$

Il en résulte l'existence de polynômes homogènes $P^\varphi(X)$, de degrés $\varphi(1)$, tels que :

$$\mathrm{Det}^G(X) = \prod_\varphi P^\varphi(X)^{\varphi(1)}.$$

On regroupe en produits partiels associés aux caractères χ, irréductibles sur $\mathbb{Q}$, ou aux caractères p-adiques θ, irréductibles sur $\mathbb{Q}_p$ (cf. Définition 2.5, §2.2.3) ; ceci définit $\mathrm{Det}^\chi(X)$ et $\mathrm{Det}^\theta(X)$. La spécialisation $X_\nu \mapsto \frac{-1}{p}\log_p(\eta^\nu)$ conduit à la factorisation (cf. Définition 2.3, §2.1) :

$$\mathrm{Det}^G\big(\tfrac{-1}{p}\log_p(\eta)\big) = \mathrm{Reg}_p^G(\eta) = \prod_\varphi \det\Big(\sum_{\nu\in G} \tfrac{-1}{p}\log_p(\eta^\nu)\,\rho_\varphi(\nu^{-1})\Big)^{\varphi(1)},$$

et on pose $\mathrm{Reg}_p^\varphi(\eta) = \det\big(\sum_{\nu\in G}\frac{-1}{p}\log_p(\eta^\nu)\,\rho_\varphi(\nu^{-1})\big)$, $\mathrm{Reg}_p^\chi(\eta) = \prod_{\varphi\,|\,\chi}\mathrm{Reg}_p^\varphi(\eta)$, et $\mathrm{Reg}_p^\theta(\eta) = \prod_{\varphi\,|\,\theta}\mathrm{Reg}_p^\varphi(\eta)$; on aura des résidus modulo p de ces régulateurs via les congruences $\frac{-1}{p}\log_p(\eta^\nu) \equiv \alpha_p(\eta)^\nu \pmod p$, $\nu\in G$, conduisant aux $\Delta_p^\theta(\eta)$.
De fait l'étude modulo p de chaque $\mathrm{Reg}_p^\theta(\eta)$ donne une information beaucoup plus précise que l'étude modulo p du régulateur normalisé $\mathrm{Reg}_p^G(\eta) = \prod_\theta \mathrm{Reg}_p^\theta(\eta)^{\varphi(1)}$.
On étudiera plus généralement la spécialisation $X_\nu \mapsto \alpha^\nu$, $\alpha\in Z_K$ donné indépendamment de tout η et p, dont nous noterons le résultat sous la forme :

$$\mathrm{Det}^G(\alpha) := \det(\alpha^{\tau\sigma^{-1}})_{\sigma,\tau\in G} = \prod_\varphi \det\Big(\sum_{\nu\in G}\alpha^\nu\,\rho_\varphi(\nu^{-1})\Big)^{\varphi(1)},$$

où l'on rappelle que $\alpha^{\tau\sigma^{-1}} = (\alpha^{\sigma^{-1}})^\tau$. Par exemple, dans le contexte logarithmique précédent relatif à un nombre algébrique $\eta\in K^\times$ pour lequel $\alpha\equiv\alpha_p(\eta) \pmod p$, nous utiliserons les régulateurs locaux (car ici α n'est défini que modulo p) :

$$\Delta_p^G(\eta) := \det(\alpha^{\tau\sigma^{-1}} \pmod p)_{\sigma,\tau\in G},$$

via leurs factorisations en θ-composantes (les θ-régulateurs locaux $\Delta_p^\theta(\eta)$).

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

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

Donc le déterminant de cet endomorphisme dans la base des $\tau\in G$ est le déterminant de Frobenius (défini au signe près).
Soit $(\rho_\varphi, V_\varphi)$ la famille des représentations absolument irreductibles non isomorphes. On prendra pour $\mathrm{End}(V_\varphi)$ la composante $e_\varphi\mathbb{C}[G]$ associée au caractère φ.[(2)]
On utilise l'isomorphisme d'algèbres $\widetilde{\rho} : V \longrightarrow \prod_\varphi \mathrm{End}(V_\varphi)$ défini par :

$$\sum_{\nu\in G} a(\nu)\,\nu^{-1} \longmapsto \Big(\sum_{\nu\in G} a(\nu)\,\rho_\varphi(\nu^{-1})\Big)_\varphi.$$

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

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

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

---

(2) Par exemple, pour $G = D_6$, une base de $e_\varphi\mathbb{C}[G]$, pour le caractère irréductible de degré 2, est donnée par $\{E_1 = e_\varphi(1-\sigma), E_\sigma = e_\varphi\sigma(1-\sigma), E_\tau = e_\varphi\tau(1-\sigma), E_{\tau\sigma} = e_\varphi\tau\sigma(1-\sigma)\}$.

Avec une réalisation matricielle $M(\rho_\varphi(\nu)) = \big(a_{ij}^\varphi(\nu)\big)_{i,j}$ des $\rho_\varphi(\nu)$, la matrice associée à $L^\varphi(X)$ est $M^\varphi(X) = \big(\sum_{\nu\in G} a_{ij}^\varphi(\nu^{-1})\, X_\nu\big)_{i,j}$, de déterminant $P^\varphi(X)$. On peut également revenir au procédé direct de Frobenius à partir des caractères. Soit g le plus petit commun multiple des ordres des éléments de G : on sait que les représentations sont réalisables sur le corps $C = \mathbb{Q}(\mu_g)$ des racines g-ièmes de l'unité (cf. [**Se1**], § 12.3). On pourra donc toujours supposer que les $a_{ij}^\varphi(\nu)$ sont des nombres algébriques p-entiers pour tout p assez grand.

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

Définition 2.5. — (i) *Caractères rationnels.* Comme Γ opère sur les les caractères irréductibles φ, on pose :

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

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

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

Soit φ un caractère absolument irréductible dont la somme des $\mathbb{Q}$-conjugués est χ. On considère, pour tout $\nu \in G$, $\Theta(\nu) := \sum\limits_{s\in D} \varphi^s(\nu) \in L$ puis l'image diagonale $\big(t_{\mathfrak{p}}(\Theta(\nu))\big)_{\mathfrak{p}\,|\,p} \in \prod\limits_{\mathfrak{p}\,|\,p} L_{\mathfrak{p}} = \prod\limits_{\mathfrak{p}\,|\,p} \mathbb{Q}_p$ où les $t_{\mathfrak{p}}$ représentent $\mathrm{Gal}(C_\chi/\mathbb{Q})/D$. On désigne par $\theta(\nu)$ la $\mathfrak{p}$-composante $t_{\mathfrak{p}}(\Theta(\nu))$ qui est dans $\mathbb{Z}_p$; par ce procédé on définit les caractères θ (que l'on devrait indexer par les $\mathfrak{p}\,|\,p$), via des congruences modulo $\mathfrak{p}$ de la forme $\theta(\nu) \equiv r_{\mathfrak{p}}(\nu) \pmod{\mathfrak{p}}$, $r_{\mathfrak{p}}(\nu) \in \mathbb{Z}$ pour tout $\nu \in G$. Comme θ est à valeurs dans $\mathbb{Z}_p$, on écrira par abus $\theta(\nu) \equiv r_{\mathfrak{p}}(\nu) \pmod{p}$.

Si l'on fixe un couple $(\theta, \mathfrak{p})$, les autres sont les h conjugués $(\theta^t, \mathfrak{p}^t)$ ainsi définis : si $\theta = \sum_{s\in D} \varphi^s$, les h conjugués de θ sont les $\theta^t = \sum_{s\in D} (\varphi^t)^s$, $t \in \mathrm{Gal}(C_\chi/\mathbb{Q})/D$, et on aura $\theta^t(\nu) \equiv r_{\mathfrak{p}^t}(\nu) \pmod{p}$, où les rationnels $r_{\mathfrak{p}^t}(\nu)$ dépendent numériquement des images résiduelles en les $\mathfrak{p}\,|\,p$ des traces relatives des $\varphi(\nu)$, $\varphi\,|\,\chi$.

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

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

(iii) *Idempotents.* Ecrivons $\varphi\,|\,\theta$, $\theta\,|\,\chi$ pour indiquer que φ (resp. θ) est un terme de θ (resp. χ). On pose $e_\chi = \sum_{\varphi\,|\,\chi} e_\varphi$ et $e_\theta = \sum_{\varphi\,|\,\theta} e_\varphi$; d'où $e_\chi = \sum_{\theta\,|\,\chi} e_\theta$. Les e_θ (resp. les e_χ) forment un système fondamental d'idempotents orthogonaux de $\mathbb{Q}_p[G]$ (resp. $\mathbb{Q}[G]$), à savoir $\mathbb{Q}_p[G] = \bigoplus_\theta e_\theta \mathbb{Q}_p[G]$, et $\mathbb{Q}[G] = \bigoplus_\chi e_\chi \mathbb{Q}[G]$. On peut remplacer $\mathbb{Q}_p$ (resp. $\mathbb{Q}$) par $\mathbb{Z}_p$ (resp. $\mathbb{Z}_{(p)}$) car $p \nmid g$.

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

Lemme 2.6. — *Pour tout p assez grand, les polynômes $P^\chi(X)$ (resp. $P^\theta(X)$) sont à coefficients p-entiers rationnels (resp. entiers p-adiques).*
Pour tout caractère irréductible φ, on a $P^\varphi(\ldots, X_{\pi\nu}, \ldots) = \zeta_\pi\, P^\varphi(\ldots, X_\nu, \ldots)$ pour tout $\pi \in G$, où ζ_π est une racine de l'unité d'ordre diviseur de g.

Démonstration. — Comme $P^\chi(X) = \prod_{s\in \mathrm{Gal}(C_\chi/\mathbb{Q})} P^{\varphi^s}(X)$ est invariant par Galois, le premier point est clair. De même pour $P^\theta(X) = \prod_{s\in D} P^{\varphi^s}(X)$.
Pour $\pi \in G$ appelons $[\pi]$ l'opérateur de $C[X]$ dans $C[X]$ défini par $[\pi]X_\nu = X_{(\pi\nu)}$ pour tout $\nu \in G$. Alors $[\pi]$ et $\widetilde{\rho} : V[X] \longrightarrow \prod_\varphi \mathrm{End}(V_\varphi[X])$ commutent ; de plus, puisque ρ_φ est un homomorphisme, on a la formule suivante :

$$[\pi]\Big(\sum_{\nu\in G} X_\nu\, \rho_\varphi(\nu^{-1})\Big) = \sum_{\nu\in G} X_{\pi\nu}\, \rho_\varphi(\nu^{-1}) = \Big(\sum_{\nu\in G} X_\nu\, \rho_\varphi(\nu^{-1})\Big)\, \rho_\varphi(\pi).$$

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

$$\det\Big([\pi]\Big(\sum_{\nu\in G} X_\nu \rho_\varphi(\nu^{-1})\Big)\Big) = \zeta_\pi \det\Big(\sum_{\nu\in G} X_\nu \rho_\varphi(\nu^{-1})\Big),$$

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

Corollaire 2.7. — *Pour tout $\pi \in G$ et tout caractère absolument irréductible φ, $P^\varphi(\ldots, \alpha^{\pi\nu}, \ldots) = \zeta_\pi\, P^\varphi(\ldots, \alpha^\nu, \ldots)$ par spécialisation $X_\nu \mapsto \alpha^\nu$, $\alpha \in Z_K$.*
Par conséquent, $P^\chi(\ldots, \alpha^{\pi\nu}, \ldots) = \pm P^\chi(\ldots, \alpha^\nu, \ldots)$ pour tout $\pi \in G$. [(3)]
De même, $P^\theta(\ldots, \alpha^{\pi\nu}, \ldots) = \zeta'_\pi P^\theta(\ldots, \alpha^\nu, \ldots)$ pour tout $\pi \in G$, où ζ'_π est d'ordre diviseur de p.g.c.d. $(g, p-1)$.

2.2.4. Déterminants, χ-déterminants numériques. — Dans cette partie, il n'y a pas référence à un nombre premier p et les caractères considérés sont absolument irréductibles ou rationnels. Ce qui précède conduit à définir les χ-déterminants numériques (i.e., indépendants de la donnée de $\eta \in K^\times$), à partir d'un $\alpha \in Z_K$ quelconque (ce ne sont donc pas des régulateurs au sens classique du terme).

Définition 2.8. — Soit G un groupe fini et soit :

$$\mathrm{Det}^G(X) = \det(X_{\tau\sigma^{-1}})_{\sigma,\tau\in G} = \prod_\varphi \det\Big(\sum_{\nu\in G} X_\nu\, \rho_\varphi(\nu^{-1})\Big)^{\varphi(1)} = \prod_\varphi P^\varphi(X)^{\varphi(1)}$$

le déterminant de groupe associé. Les χ-déterminants (avec indéterminées et numériques) sont par définition les expressions (sur les conjugués de α) :

$$\mathrm{Det}^\chi(X) = \prod_{\varphi\,|\,\chi} P^\varphi(X) \ \text{ et } \ \mathrm{Det}^\chi(\alpha) = \prod_{\varphi\,|\,\chi} P^\varphi(\ldots, \alpha^\nu, \ldots), \ \ \alpha \in Z_K,$$

de sorte que $\mathrm{Det}^G(\alpha) = \prod_\chi (\mathrm{Det}^\chi(\alpha))^{\varphi(1)}$ (où pour chaque χ, $\varphi\,|\,\chi$).

Exemple 2.9. — Dans le cas du groupe $D_6 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, on a les χ-déterminants numériques suivants :

$\mathrm{Det}^1(\alpha) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} + \alpha^\tau + \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2}$,

$\mathrm{Det}^{\chi_1}(\alpha) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2}$,

$$\mathrm{Det}^{\chi_2}(\alpha) = \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau.$$

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

(3) Signe + sauf si $\chi = \varphi$ est quadratique et $\varphi(\pi) = -1$ (cf. Lemme 2.10 (ii), §2.2.5).

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

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

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

qui conduisent à :

$$\sum_{\nu \in G} X_\nu \rho_\varphi(\nu^{-1}) = \begin{pmatrix} X_1 - X_{\sigma^2} + X_\tau - X_{\tau\sigma} & X_\sigma - X_{\sigma^2} - X_{\tau\sigma} + X_{\tau\sigma^2} \\ -X_\sigma + X_{\sigma^2} - X_\tau + X_{\tau\sigma^2} & X_1 - X_\sigma - X_\tau + X_{\tau\sigma} \end{pmatrix},$$

ou encore, par spécialisation et en prenant le déterminant :

$$\mathrm{Det}^{\chi_2}(\alpha) = \begin{vmatrix} \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} & \alpha^\sigma - \alpha^{\sigma^2} - \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2} \\ -\alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau + \alpha^{\tau\sigma^2} & \alpha - \alpha^\sigma - \alpha^\tau + \alpha^{\tau\sigma} \end{vmatrix}.$$

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

$$\pi_1 = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma) \ \ \& \ \ \pi_2 = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma).$$

2.2.5. Cas des groupes Abéliens. — Ce cas se déduit des études précédentes, mais il est possible d'être plus précis et d'en rester au point de vue classique des caractères de degré 1.

Soit G un groupe Abélien fini d'ordre n. On désigne par $\widehat{G}$ le groupe des caractères $\varphi : G \to \mathbb{C}^\times$; l'image de φ est le groupe μ_d des racines de l'unité d'ordre égal à l'ordre d de φ. On a alors $\mathrm{Det}^G(X) = \det(X_{\tau\sigma^{-1}})_{\sigma,\tau \in G} = \prod_{\varphi \in \widehat{G}} \Big(\sum_{\nu \in G} \varphi(\nu) X_{\nu^{-1}} \Big)$.

Si G est produit direct de groupes cycliques G_i, alors en écrivant que $\widehat{G} = \prod_i \widehat{G}_i$, il vient $\mathrm{Det}^G(X) = \prod_i \prod_{\varphi \in \widehat{G}_i} \Big(\sum_{\nu \in G_i} \varphi(\nu) X_{\nu^{-1}} \Big)$. Il en résulte que l'on peut se ramener au cas où G est cyclique d'ordre n. On a alors une décomposition par classes de caractères de même ordre $d \,|\, n$ (i.e., $\mathbb{Q}$-conjugués dans $\mathbb{Q}(\mu_d)$) : on obtient les caractères rationnels χ qui regroupent les φ^t, où φ est fixé d'ordre d et où t parcourt $(\mathbb{Z}/d\mathbb{Z})^\times$. On peut donc écrire :

$$\mathrm{Det}^G(X) = \prod_\chi \prod_{\varphi \,|\, \chi} \Big(\sum_{\nu \in G} \varphi(\nu) X_{\nu^{-1}} \Big).$$

Soit G un groupe cyclique d'ordre $n \geq 1$ et soit χ un caractère rationnel irréductible de G d'ordre $d \,|\, n$ (par abus, l'ordre commun des $\varphi \,|\, \chi$). Dans ce cas les χ-déterminants (avec indéterminées et numériques) sont les expressions :

$$\mathrm{Det}^\chi(X) := \prod_{\varphi \,|\, \chi} \Big(\sum_{\nu \in G} \varphi(\nu)\, X_{\nu^{-1}} \Big) \ \text{ et } \ \mathrm{Det}^\chi(\alpha) := \prod_{\varphi \,|\, \chi} \Big(\sum_{\nu \in G} \varphi(\nu)\, \alpha^{\nu^{-1}} \Big), \ \alpha \in Z_K.$$

Lemme 2.10. — *Soit $C_\chi = \mathbb{Q}(\mu_d)$ le corps des valeurs des caractères irréductibles $\varphi \,|\, \chi$ d'ordre d.*

(i) On a $\mathrm{Det}^\chi(X) = \mathrm{N}_{C_\chi/\mathbb{Q}} \Big(\sum_{\nu \in G} \varphi(\nu)\, X_{\nu^{-1}} \Big) \in \mathbb{Z}[X]$.

(ii) Par spécialisation $X_\nu \mapsto \alpha^\nu$, $\alpha \in Z_K$, on obtient $\mathrm{Det}^\chi(\alpha) \in \mathbb{Z}$, *sauf si $\chi = \varphi$ est un caractère quadratique correspondant à un sous-corps quadratique $\mathbb{Q}(\sqrt{m}) \subseteq K$, auquel cas* $\mathrm{Det}^\chi(\alpha) = \mathrm{Det}'^\chi(\alpha) \,.\, \sqrt{m}$, *avec* $\mathrm{Det}'^\chi(\alpha) \in \mathbb{Z}$.

Démonstration. — Le premier point est évident puisque le produit définissant $\mathrm{Det}^{\chi}(\alpha)$ porte sur tous les $\mathbb{Q}$-conjugués de φ.[4]

Les sommes $\sum_{\nu\in G} \varphi(\nu)\, X_{\nu^{-1}}$ sont des *résolvantes de Hilbert* pour lesquelles on a les relations $[\tau]\Big(\sum_{\nu\in G} \varphi(\nu)\, X_{\nu^{-1}}\Big) = \varphi(\tau) \sum_{\nu\in G} \varphi(\nu)\, X_{\nu^{-1}}$, pour tout $\tau \in G$ (cf. Lemme 2.6, §2.2.3) et $\mathrm{N}_{C_\chi/\mathbb{Q}}\Big([\tau]\Big(\sum_{\nu\in G} \varphi(\nu)\, X_{\nu^{-1}}\Big)\Big) = \mathrm{N}_{C_\chi/\mathbb{Q}}\Big(\sum_{\nu\in G} \varphi(\nu)\, X_{\nu^{-1}}\Big)$ si $C_\chi \neq \mathbb{Q}$, puisque la norme d'une racine de l'unité est 1. D'où dans ce cas par spécialisation avec $\alpha \in Z_K$:

$$\mathrm{N}_{C_\chi/\mathbb{Q}}\Big(\sum_{\nu\in G} \varphi(\nu)\, \alpha^{\tau\nu^{-1}}\Big) = \mathrm{N}_{C_\chi/\mathbb{Q}}\Big(\sum_{\nu\in G} \varphi(\nu)\, \alpha^{\nu^{-1}}\Big) = \mathrm{Det}^{\chi}(\alpha).$$

Donc, $\mathrm{Det}^{\chi}(\alpha)$, invariant par tout $s \in \mathrm{Gal}(C_\chi/\mathbb{Q})$ et tout $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, est un entier rationnel.

Si la norme dans $C_\chi/\mathbb{Q}$ est triviale (auquel cas $\chi = \varphi$ est d'ordre 1 ou 2), on a les deux χ-déterminants numériques possibles suivants :

(i) $\mathrm{Det}^{1}(\alpha) = \sum_{\sigma\in G} \alpha^{\sigma^{-1}} \in \mathbb{Z}$, pour $\chi = 1$.

(ii) $\mathrm{Det}^{\chi}(\alpha) = \sum_{\sigma\in G} \chi(\sigma)\, \alpha^{\sigma-1}$, pour χ quadratique ; alors il existe un corps quadratique $k = \mathbb{Q}(\sqrt{m}\,) \subseteq K$ (correspondant au noyau de χ) et $\tau \in G$ tels que $\tau\mathrm{Det}^{\chi}(\alpha) = -\mathrm{Det}^{\chi}(\alpha)$; d'où $\mathrm{Det}^{\chi}(\alpha) = \mathrm{Det}'^{\chi}(\alpha)\,.\,\sqrt{m}$, où $\mathrm{Det}'^{\chi}(\alpha) \in \mathbb{Z}$. □

Le cas d'un caractère quadratique étant la seule exception, on convient de négliger le facteur $\sqrt{m}$ et d'en rester à la notation $\mathrm{Det}^{\chi}(\alpha)$ pour le rationnel correspondant.

Exemple 2.11. — Dans le cas $n = 2$ ($K = \mathbb{Q}(\sqrt{m})$), si α, α' sont les conjugués de $\alpha = u + v\sqrt{m} \in Z_K$ donné, alors on a le déterminant numérique :

$\mathrm{Det}^{G}(\alpha) = \begin{vmatrix} \alpha & \alpha' \\ \alpha' & \alpha \end{vmatrix} = (\alpha+\alpha')(\alpha-\alpha'),$

et par définition les deux χ-déterminants :

$$\mathrm{Det}^{1}(\alpha) = \alpha + \alpha' = 2u, \quad \mathrm{Det}^{\chi}(\alpha) = \alpha - \alpha' = 2v\sqrt{m}.$$

Si $\alpha \notin \mathbb{Q}$ est par exemple tel que $\alpha + \alpha' = 0$, le 1-déterminant $\mathrm{Det}^{1}(\alpha)$ est nul. Par contre, le χ-déterminant $\mathrm{Det}^{\chi}(\alpha) = 2\alpha = 2v\sqrt{m}$ n'est pas nul (puisque $\alpha - \alpha' \neq 0$) et on pourra étudier ses éventuelles nullités modulo p pour tout p assez grand.

De même $\mathrm{Det}^{\chi}(\alpha)$ est nul si $\alpha \in \mathbb{Z}$, sans que $\mathrm{Det}^{1}(\alpha)$ ne soit nul si $\alpha \neq 0$.

Exemple 2.12. — Considérons le cas $n = 3$ (K corps cubique cyclique) et soient $\alpha, \alpha', \alpha''$ les conjugués de $\alpha \in Z_K$; alors on a le déterminant numérique :

$\begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \alpha' & \alpha'' & \alpha \\ \alpha'' & \alpha & \alpha' \end{vmatrix} = (\alpha+\alpha'+\alpha'')\,\mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = 3\,\alpha\alpha'\alpha'' - (\alpha^3 + \alpha'^3 + \alpha''^3).$

On a donc par définition les deux χ-déterminants :

$\mathrm{Det}^{1}(\alpha) \;= \alpha + \alpha' + \alpha''$,

$\mathrm{Det}^{\chi}(\alpha) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = \alpha^2 + \alpha'^2 + \alpha''^2 - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha.$

Si par exemple $\mathrm{Det}^{1}(\alpha) = 0$ avec $\alpha \notin \mathbb{Z}$, alors :

$$\mathrm{Det}^{\chi}(\alpha) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = 3\,(\alpha^2 + \alpha\alpha' + \alpha'^2) \neq 0.$$

[4] A ce sujet, signalons que les deux opérations "conjuguaison dans $C_\chi/\mathbb{Q}$" et "évaluation par les G-conjugués de α" ne commutent pas, sauf s'il y a disjonction linéaire de C_χ et K sur $\mathbb{Q}$.

2.2.6. 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 2.13. — Dans la décomposition $\mathrm{Det}^G(\alpha) = \prod_\chi (\mathrm{Det}^\chi(\alpha))^{\varphi(1)}$ et lorsque la spécialisation est donnée par $\alpha \equiv \alpha_p(\eta) \equiv \frac{-1}{p}\mathrm{log}_p(\eta) \pmod p$, certains χ-régulateurs locaux $\Delta_p^\chi(\eta) := \mathrm{Det}^\chi(\alpha)$ sont nuls modulo p pour tout p dès qu'il existe une relation multiplicative de la forme $\prod_{\nu\in G}(\eta^{\nu^{-1}})^{\lambda(\nu)} = 1$, $\lambda(\nu) \in \mathbb{Z}$, qui conduit à $\sum_{\nu\in G} \lambda(\nu)\, \alpha^{\nu^{-1}} \equiv 0 \pmod p$ pour tout p étranger à η.
Cette relation globale $U = \sum_{\nu\in G} \lambda(\nu)\, \nu^{-1} \neq 0$ de $\mathbb{Z}[G]$ (indépendante de p) est à distinguer des relations locales $\sum_{\nu\in G} u(\nu)\, \nu^{-1} \in \mathbb{Z}_{(p)}[G]$ (où les $u(\nu)$ dépendent de p) lorsque $\sum_{\nu\in G} u(\nu)\, \alpha^{\nu^{-1}} \equiv 0 \pmod p$ pour certains p. On rappelle l'aspect “réciproque” (cf. Remarque 2.4, §2.1.2), purement conjectural.

Lemme 2.14. — *Si l'on a* $\dim_\mathbb{Q}((F \otimes \mathbb{Q})^{e_\chi}) < \dim_\mathbb{Q}(e_\chi \mathbb{Q}[G]) = [C_\chi : \mathbb{Q}]\, \varphi(1)^2$ *(i.e., il existe $U \in \mathbb{Q}[G]$ telle que $\eta^{U_\chi} = 1$, avec $U_\chi \neq 0$), alors les χ-régulateurs locaux* $\Delta_p^\chi(\eta) := \mathrm{Det}^\chi(\alpha)$ *sont nuls modulo p pour tout p assez grand.*[5]

Dans ce cas, on dira que les $\Delta_p^\chi(\eta)$ sont *trivialement nuls modulo p*. Ceci entraîne la nullité triviale de certains $\Delta_p^\theta(\eta)$, $\theta \,|\, \chi$, à savoir ceux pour lesquels $U_\theta := e_\theta U \not\equiv 0 \pmod{\mathfrak{p}}$, pour $\mathfrak{p} \,|\, p$ associé à θ.

Remarque 2.15. — (i) Si $\varphi(1) = 1$, $\Delta_p^\chi(\eta)$ est trivialement nul modulo p si $\eta^{e_\chi} = 1$ (i.e., $U_\chi = e_\chi$), auquel cas $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ trivialement pour tout $\theta \,|\, \chi$.
(ii) Si $\varphi(1) > 1$, $\Delta_p^\chi(\eta)$ est nul modulo p s'il existe i, $1 \le i \le \varphi(1)$, tel que, par extension des scalaires, on ait, dans $F \otimes C_\chi$, $\eta^{\pi_i^\varphi} = 1$ pour $\varphi \,|\, \chi$ (cf. §2.2.1).
Par exemple, pour $G = D_6$ et $\varphi = \chi = \chi_2$, les éléments $\pi_1^\varphi = \frac{1}{3}(1 - \sigma^2 + \tau - \tau\sigma)$ et $\pi_2^\varphi = \frac{1}{3}(1 - \sigma - \tau + \tau\sigma)$ sont tels que $e_\chi \pi_i^\varphi = \pi_i^\varphi$, pour $i = 1, 2$, $\pi_1^\varphi + \pi_2^\varphi = e_\chi$, et $\pi_1^\varphi \pi_2^\varphi = 0$ (cf. Exemple 2.9, §2.2.4).
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 pour tout p assez grand en raison de la première relation.
Le fait de supposer F de $\mathbb{Z}$-rang n évite cet inconvénient. On peut toujours s'y ramener en modifiant convenablement η.
(iii) Pour $U \in \mathbb{Z}_{(p)}[G]$, on a $U_\chi = \sum_{\varphi\,|\,\chi} U_\varphi$ et $U_\varphi = e_\varphi U_\chi$. On a $U_\chi \equiv 0 \pmod p$ si et seulement si $U_\varphi \equiv 0 \pmod p$ pour au moins un (donc tout) $\varphi \,|\, \chi$ (car les $\varphi \,|\, \chi$ sont conjugués par $\mathrm{Gal}(C_\chi/\mathbb{Q})$). Ces congruences (mod p) dans les algèbres de groupes signifient selon les cas $(\mathrm{mod}\ p\,\mathbb{Z}_{(p)}[G])$ ou $(\mathrm{mod}\ p\, Z_{\chi,(p)}[G])$ (où Z_χ est l'anneau des entiers du corps des valeurs C_χ).
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 $L[G]$, seulement équivalent à $U_\varphi \equiv 0 \pmod{\mathfrak{p}}$ pour tout $\varphi \,|\, \theta$ (cf. Définition 2.5 (ii), §2.2.3, et 3.3 (iii), §3.2.1).

Exemple 2.16. — a) 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 $\Delta_p^\chi(\eta) = \mathrm{N}_{C_\chi/\mathbb{Q}}\big(\sum_{\nu\in G} \varphi(\nu)\, \alpha^{\nu^{-1}}\big)$ pour $\alpha \equiv \alpha_p(\eta) \pmod p$.

[5] Il suffit de remarquer que toute relation globale $\eta^{U_\chi} = 1$ dans $F \otimes \mathbb{Q}$, $U_\chi \neq 0$, permet d'en déduire que, pour tout p assez grand, on est dans les conditions d'application des Lemmes du §3.2 (critère de nullité modulo p des $\Delta_p^\theta(\eta)$) pour $\theta \,|\, \chi$, à partir chaque fois de $\alpha \equiv \alpha_p(\eta) \pmod p$.

Par exemple, pour $n = 3$, on a les deux idempotents rationnels :

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

Soit $\alpha \equiv \alpha_p(\eta) \pmod p$ et considérons les nullités triviales des $\Delta_p^\chi(\eta)$ modulo p.
(i) 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 $\Delta_p^1(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2}$.
(ii) Les éléments $\eta \in K^\times$ tels que $\eta^{e_\chi} = 1$ ou $\mathrm{N}_{K/\mathbb{Q}}(\eta) = \eta^3$ (dans $F \otimes \mathbb{Q}$), donc tels que $\eta \in \mathbb{Q}^\times$, correspondent à la nullité de $\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^2\, \alpha^{\sigma^1} + j\, \alpha^{\sigma^2})$.

b) Les trois idempotents relatifs au groupe D_6 sont :

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

(i) Les η tels que $\eta^{e_1} = 1$ correspondent à la nullité triviale de $\Delta_p^1(\eta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.
(ii) 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 :
$\Delta_p^{\chi_1}(\eta) = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} = (1 - \tau)\, \mathrm{Tr}_{K/k}(\alpha)$.
(iii) Les éléments η tels que $\eta^{U_{\chi_2}} = 1$ pour $U_{\chi_2} \in e_{\chi_2}\mathbb{Q}[G] \setminus \{0\}$ (Lemme 2.14 précédent) conduisent à la nullité triviale de :

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

2.3. Définition et étude des θ-régulateurs locaux. — Soit $\eta \in K^\times$ et soit p assez grand. On a les congruences suivantes (cf. §2.1) :

$$\frac{-1}{p}\log_p(\eta) \equiv \alpha_p(\eta) \pmod p \quad \text{et} \quad \alpha_p(\eta^\nu) \equiv \alpha_p(\eta)^\nu \pmod p \quad \text{pour tout } \nu \in G.$$

2.3.1. Généralités. — On fixe un nombre algébrique $\alpha \in Z_K$ défini par $\alpha \equiv \alpha_p(\eta) \pmod p$. On obtient le déterminant à coefficients dans Z_K, uniquement défini modulo p, mais représenté dans Z_K :

$$\Delta_p^G(\eta) = \mathrm{Det}^G(\alpha) = \det\big(\alpha^{\tau\sigma^{-1}}\big)_{\sigma,\tau\in G}.$$

Le groupe G opère sur $\Delta_p^G(\eta)$ par permutations des lignes ; donc $\Delta_p^G(\eta)^2$ est invariant par Galois et est donc rationnel. 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 (cf. Lemme 2.10, §2.2.5) et que l'on néglige. On considère donc :

$$\Delta_p^G(\eta) = \prod_\chi \prod_{\theta\,|\,\chi} \prod_{\varphi\,|\,\theta} P^\varphi(\ldots, \alpha^\nu, \ldots)^{\varphi(1)} =: \prod_\chi \Delta_p^\chi(\eta)^{\varphi(1)} =: \prod_\chi \prod_{\theta\,|\,\chi} \Delta_p^\theta(\eta)^{\varphi(1)},$$

où pour chaque χ (resp. θ), φ est un caractère irréductible divisant χ (resp. θ).

Définition 2.17. — 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 $\Delta_p^\theta(\eta) := \prod_{\varphi\,|\,\theta} P^\varphi(\ldots, \alpha^\nu, \ldots)$ pour $\alpha \equiv \alpha_p(\eta) := \frac{1}{p}(\eta^{p^{n_p}-1} - 1) \pmod p$.

Pour $\theta\,|\,\chi$ (χ fixé), les θ-régulateurs locaux correspondants dépendent de la décomposition de p dans $C_\chi/\mathbb{Q}$ et sont au nombre de $h = \frac{[C_\chi:\mathbb{Q}]}{f}$, où f est leur degré résiduel (cf. Définition 2.5 (ii), §2.2.3). Ils ne sont définis que modulo p.

Remarque 2.18. — On peut de la même façon écrire (pour p assez grand) que le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ est égal à $\prod_{\chi} \mathrm{Reg}_p^{\chi}(\eta)^{\varphi(1)} = \prod_{\theta} \mathrm{Reg}_p^{\theta}(\eta)^{\varphi(1)}$ où :

$$\mathrm{Reg}_p^{\theta}(\eta) = \prod_{\varphi\,|\,\theta} P^{\varphi}\big(\ldots, \tfrac{-1}{p}\mathrm{log}_p(\eta^{\nu}), \ldots\big).$$

On a alors les congruences $\mathrm{Reg}_p^{\theta}(\eta) \equiv \Delta_p^{\theta}(\eta) \pmod p$; ainsi on a p divise $\mathrm{Reg}_p^{\theta}(\eta)$ si et seulement si $\Delta_p^{\theta}(\eta) \equiv 0 \pmod p$; mais dans ce cas $p^{\varphi(1)}$ divise $\mathrm{Reg}_p^G(\eta)$ puisque $\mathrm{Reg}_p^G(\eta) = \prod_{\theta} \mathrm{Reg}_p^{\theta}(\eta)^{\varphi(1)}$, où chaque fois $\varphi\,|\,\theta$ (cf. §2.2.2).

Remarque 2.19. — (i) Dans tous les cas, $\Delta_p^{\chi}(\eta) := \mathrm{N}_{C_\chi/\mathbb{Q}}\big(P^{\varphi}(\ldots, \alpha^{\nu}, \ldots)\big) \in \mathbb{Z}$ ($\varphi\,|\,\chi$ fixé), avec la convention sur la notation $\mathrm{N}_{C_\chi/\mathbb{Q}}$, notamment lorsque K et C_χ ne sont pas linéairement disjoints. On rappelle l'exception χ quadratique.

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

Mêmes relations en remplaçant Δ par Reg et α par $\frac{-1}{p}\mathrm{log}_p(\eta)$.

(ii) Si $H = \{\nu \in G,\ \varphi(\nu) = \varphi(1)\}$ est le noyau de $\varphi\,|\,\theta\,|\,\chi$ (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.

2.3.2. Cas des χ-régulateurs locaux, 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 :

$$\Delta_p^1(\eta) \equiv \frac{-1}{p}\mathrm{log}_p(a) \equiv \frac{1}{p}(a^{p-1} - 1) \equiv q_p \pmod p \quad (p\text{-quotient de Fermat de } a).$$

Le programme PARI correspondant est le suivant (pour $a = 659$) : [6]

$\{e = 659; print("e = ", e); for(n = 1, 5*10^8, p = 2*n + 1;$
$if(isprime(p) == 1\&Mod(e, p)! = 0,$
$qp = Mod(e, p^2)^{(p-1)} - 1; if(qp == 0, print(p))))\}$

Pour $p < 10^9$, on ne trouve que les solutions $p = 23, 131, 2221, 9161, 65983$.

(ii) Si $\chi = \theta$ est quadratique et si $k = \mathbb{Q}(\sqrt{m}\,)$ est le sous-corps quadratique de K fixe par le noyau de χ, on obtient un θ-régulateur qui correspond au cas où $\mathrm{N}_{K/k}(\eta) \in k^{\times} \setminus \mathbb{Q}^{\times}$; 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 tous nuls. Le θ-régulateur pour le caractère quadratique est $\Delta_p^{\theta}(\varepsilon) \equiv 2\,v\sqrt{m} \pmod p$ (calculé via $\varepsilon^{p^{n_p}-1} \equiv 1 + p\,v\sqrt{m} \pmod{p^2}$).

Au moyen du programme PARI ci-dessous on calcule le θ-régulateur $\Delta_p^{\theta}(\varepsilon)$ de l'unité fondamentale $\varepsilon = 5 + 2\sqrt{6}$, pour tout $p < 10^9$ ($p \neq 2, 3$), mais le programme est valable pour un corps quadratique arbitraire et $\eta \in K^{\times} \setminus \mathbb{Q}^{\times}$ de norme quelconque (en modifiant m, aa, bb)) :

[6] Dans tous les programmes PARI [**P**] proposés, la compatibilité avec TeX oblige à écrire les symboles *par*, &, *hfill*, avec un antislash, à placer des *\$* et des *{ }* pour les exposants. . .

$\{m = 6; aa = 5; bb = 2; N = aa^2 - m * bb^2; print("m = ", m, "", "norme = ", N);$
$for(n = 1, 5 * 10^8, p = 2 * n + 1; if(isprime(p) == 1 \& Mod(m * N, p)! = 0, p2 = p^2;$
$a = Mod(aa, p2); b = Mod(bb, p2); P2 = x^2 - Mod(m, p2);$
$y = Mod(a + b * x, P2); z = y^{(p-1)}; U = z^{(p+1)} - 1;$
$RP = component(U, 2); rp = component(RP, 2)$ [(7)]$;$
$if(rp == 0, print(p))))\}.$

On ne trouve un θ-régulateur $\Delta_p^\theta(\varepsilon)$ nul modulo p, avec $p < 10^9$, que pour $p = 7, 523$, ce qui constitue une seconde observation sur la rareté du phénomène.

Soit $\eta = 7 + 2\sqrt{6}$ de norme 25. Le $\mathbb{Z}$-rang du groupe F engendré par η est ici égal à 2 (pas de nullités triviales). On vérifie que les p-quotients de Fermat $\Delta_p^1(\eta)$ de 25 sont tous non nuls modulo p dans l'intervalle testé. Les solutions p obtenues pour $\Delta_p^\theta(\eta) \equiv 0 \pmod p$, $\theta \neq 1$, sont $p = 11, 37, 163, 4219$.

Pour $\eta = 16 + \sqrt{123}$, de norme 133, on trouve pour $\theta \neq 1$ les deux solutions $p = 5, 751$.

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 $\dfrac{1+\sqrt{5}}{2}$ on ne trouve aucune solution dans l'intervalle testé.

3. Existence de relations $\mathbb{F}_p$-linéaires entre les conjugués de α

Soit $\eta \in K^\times$ fixé et soit p assez grand. Soit $\alpha_p(\eta) := \frac{1}{p}\big(\eta^{p^{n_p}-1} - 1\big) \in Z_{K,(p)}$; modulo p, on pourra toujours représenter $\alpha_p(\eta)$ dans Z_K. On s'intéresse à établir la relation entre la nullité modulo p de certains $\Delta_p^\theta(\eta)$ et l'existence de relations $\mathbb{F}_p$-linéaires entre les conjugués de $\alpha_p(\eta)$.

On suppose implicitement que le $\mathbb{Z}$-rang de F est égal à n.

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^ν sont $\mathbb{F}_p$-indépendants si, pour toute famille de coefficients $u(\nu) \in \mathbb{Z}_{(p)}$, la relation $\sum\limits_{\nu \in G} u(\nu)\, \alpha^{\nu^{-1}} \equiv 0 \pmod p$, dans l'anneau $Z_{K,(p)}$, implique $u(\nu) \equiv 0 \pmod p$ pour tout $\nu \in G$. On dira aussi (cf. Définition 3.3, §3.2.1) que toute relation $U = \sum\limits_{\nu \in G} u(\nu)\nu^{-1}$, associée à α, est nulle modulo $p\,\mathbb{Z}_{(p)}[G]$. Ceci est indépendant de la classe de α modulo p.

On a le résultat élémentaire suivant où l'on rappelle que $\mathrm{Det}^G(\alpha) = \det\big(\alpha^{\tau\sigma^{-1}}\big)_{\sigma,\tau}$:

Proposition 3.1. — *On suppose p assez grand afin que $\alpha \in Z_{K,(p)}$.*
(i) Les α^ν sont $\mathbb{F}_p$-indépendants si et seulement si α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$.
(ii) Les α^ν sont $\mathbb{F}_p$-indépendants si et seulement si $\mathrm{Det}^G(\alpha)$ est étranger à p.

Démonstration. — Si α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$, toute relation de la forme $\sum_{\nu\in G} u(\nu)\, \alpha^{\nu^{-1}} \equiv 0 \pmod p$, $u(\nu) \in \mathbb{Z}_{(p)}$, conduit à $u(\nu) \equiv 0 \pmod p$ pour tout $\nu \in G$.

Supposons alors que les α^ν 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 $\sum_{\nu\in G} r(\nu)\alpha^{\nu^{-1}} = 0$ avec des entiers $r(\nu)$ non tous nuls, tels que

(7) Attention, exceptionnellement on doit prendre le coefficient de $x = \sqrt{m}$ et non le terme constant.

p.g.c.d.$(r(\nu)) = 1$; d'où $r(\nu) \equiv 0 \pmod p$ pour tout $\nu \in G$ (absurde). Par conséquent α est déjà une $\mathbb{Q}$-base normale de K.
Si $\beta \in Z_{K,(p)}$, il existe des $r(\nu) \in \mathbb{Z}$ et un entier rationnel d étranger à p.g.c.d.$(r(\nu))$ tels que $d\,\beta = \sum_{\nu \in G} r(\nu)\alpha^{\nu^{-1}}$. Il est clair que $p \nmid d$ sinon tous les $r(\nu)$ sont divisibles par p. Ainsi α est une $\mathbb{Z}_{(p)}$-base normale de $Z_{K,(p)}$.
(ii) Supposons que les α^ν soient $\mathbb{F}_p$-indépendants ; comme $\alpha = \frac{1}{d}\beta$, $\beta \in Z_K$, $d \in \mathbb{Z}$, $p \nmid d$, 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, si Z_K est l'anneau des entiers de K, le conducteur $\mathfrak{f} \in \mathbb{Z}$ tel que $\mathfrak{f}\, Z_K \subseteq \bigoplus_\nu \mathbb{Z}\,\alpha^\nu$ 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 $\mathrm{Det}^G(\alpha) = \det\big(\alpha^{\tau\sigma^{-1}}\big)_{\sigma,\tau \in G}$.
Supposons $\mathrm{Det}^G(\alpha)$ étranger à p, et supposons qu'il existe des $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, non tous divisibles par p, tels que $sum_{\sigma \in G}\lambda(\sigma)\,\alpha^{\sigma^{-1}} \equiv 0 \pmod p$. Alors, par toutes les conjugaisons par $\tau \in G$, on obtient une relation $\mathbb{Z}_{(p)}$-linéaire sur les lignes de la forme $\sum_{\sigma \in G} \lambda(\sigma)(\ldots, \alpha^{\tau\sigma^{-1}}, \ldots)_\tau \equiv (\ldots, 0, \ldots)_\tau \pmod p$, d'où $\mathrm{Det}^G(\alpha) \equiv 0 \pmod p$ (absurde). □

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

Nous allons préciser les propriétés des θ-composantes de $U = \sum_{\nu \in G} u(\nu)\,\nu^{-1}$, dite relation associée, et faire le lien avec la nullité ou non des $\Delta_p^\theta(\eta)$ modulo p.

3.2. Critère de nullité modulo p des $\Delta_p^\theta(\eta)$. — Soit C_χ le corps des valeurs des caractères absolument irréductibles $\varphi \,|\, \chi$ de G, pour un caractère rationnel irréductible χ. On suppose pour simplifier que $K \cap C_\chi = \mathbb{Q}$. On notera $Z_{\chi,(p)} := Z_{C_\chi,(p)}$ l'anneau des valeurs, sur $\mathbb{Z}_{(p)}$, des $\varphi \,|\, \theta \,|\, \chi$.

3.2.1. Principaux lemmes. — On désigne par $e_\varphi = \frac{\varphi(1)}{n} \sum_{\sigma \in G} \varphi(\sigma^{-1})\,\sigma$ les idempotents centraux orthogonaux de $C_\chi[G]$, et par $\mathrm{End}_{C_\chi}(V_\varphi) \simeq e_\varphi\, C_\chi[G]$ les anneaux d'endomorphismes des représentations irréductibles V_φ correspondantes.

On a, par sommes de conjugués convenables de φ, les idempotents p-adiques et rationnels $e_\theta = \frac{\varphi(1)}{n} \sum_{\sigma \in G} \theta(\sigma^{-1})\,\sigma \in \mathbb{Z}_{(p)}[G]$ et $e_\chi = \frac{\varphi(1)}{n} \sum_{\sigma \in G} \chi(\sigma^{-1})\,\sigma \in \mathbb{Z}_{(p)}[G]$ (cf. Définition 2.5, §2.2.3 utilisant le corps de décomposition L de p dans $C_\chi/\mathbb{Q}$ et $D = \mathrm{Gal}(C_\chi/L)$).

Définition 3.3. — (i) Si $\sum_{\nu \in G} u(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod p$, $u(\nu) \in \mathbb{Z}_{(p)}$ pour tout $\nu \in G$, on appelle *relation associée* l'élément $U = \sum_{\nu \in G} u(\nu)\,\nu^{-1} \in \mathbb{Z}_{(p)}[G]$, et on définit les φ-relations $U_\varphi := e_\varphi . U \in Z_{\chi,(p)}[G]$, les θ-relations $U_\theta := e_\theta . U \in \mathbb{Z}_p[G]$, ou encore les χ-relations $U_\chi := e_\chi . U \in \mathbb{Z}_{(p)}[G]$.

Quel que soit l'anneau $\mathcal{Z}$ des coefficients, les écritures ci-dessus ne sont définies que modulo $p\,\mathcal{Z}$ (en raison de la définition de $\alpha \equiv \alpha_p(\eta) \pmod p$).

(ii) On désigne par $\mathcal{L}$ le G-module des relations associées $U \in \mathbb{Z}_{(p)}[G]$ relatives à α et p. Par abus on peut aussi voir $\mathcal{L}$ dans $\mathbb{F}_p[G]$.

Vu dans $\mathbb{F}_p[G]$, on a $\mathcal{L} = \{0\}$ si et seulement si les α^ν sont $\mathbb{F}_p$-indépendants (cf. §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 $f\varphi(1)$) est la représentation irréductible de caractère θ ; on a $0 \leq \delta \leq \varphi(1)$. Soit $\mathfrak{p}\,|\,p$ l'idéal premier de C_χ (ou L) associé à θ. On rappelle que $\theta(\nu) = \sum_{s\in D} \varphi^s(\nu) \in Z_{L,(p)}$ (pour $\varphi\,|\,\theta$) est défini via $\theta(\nu) \equiv r_\mathfrak{p}(\nu) \pmod{\mathfrak{p}}$, $r_\mathfrak{p}(\nu) \in \mathbb{Z}$; donc si $U \in \mathbb{Z}_{(p)}[G]$, $U_\theta \in Z_{L,(p)}[G]$ est congrue modulo $\mathfrak{p}$ à un élément de $\mathbb{Z}_{(p)}[G]$. On verra donc $U_\theta \pmod{p}$ dans $\mathbb{Z}_{(p)}[G]$ ou dans $Z_{L,(p)}[G] \pmod{\mathfrak{p}}$ selon le contexte.

Soit $U \in \mathbb{Z}_{(p)}[G]$ une relation ; alors on obtient $U_\varphi = \sum_{\nu\in G} u_\varphi(\nu)\,\nu^{-1} \in Z_{\chi,(p)}[G]$, avec $u_\varphi(\nu) = \frac{\varphi(1)}{n} \sum_{\tau\in G} \varphi(\tau^{-1}) u(\nu\tau)$. On rappelle que l'on a $U_\chi := e_\chi U \equiv 0 \pmod{p}$ si et seulement si $U_\varphi \equiv 0 \pmod{p}$ pour au moins un (donc tout) $\varphi\,|\,\chi$. Par contre, $U_\theta \equiv 0 \pmod{p}$ dans $\mathbb{Z}_p$ (de fait $U_\theta \in \mathfrak{p} Z_{L,(p)}$) si et seulement si $U_\varphi \equiv 0 \pmod{\mathfrak{p}}$ pour un (donc tout) $\varphi\,|\,\theta$. Donc $U_\theta \equiv 0 \pmod{\mathfrak{p}}$ n'entraîne pas $U_\chi \equiv 0 \pmod{p}$, car on ne peut conjuguer que par D.

Lemme 3.4. — *Si* $\sum\limits_{\nu\in G} u(\nu)\alpha^{\nu^{-1}} \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$, *et si* $U = \sum\limits_{\nu\in G} u(\nu)\,\nu^{-1}$, *alors* $U_\varphi\,.\,\alpha := \sum\limits_{\nu\in G} u_\varphi(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod{p}$ *pour tout caractère irréductible* φ.

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

Lemme 3.5. — *Soient* $U \in \mathcal{L}$ *et* φ *tels que* $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$. *Alors l'endomorphisme* $E_\varphi := e_\varphi \sum\limits_{\nu\in G} \alpha^\nu \nu^{-1} \in \mathrm{End}_{KC_\chi}(V_\varphi)$ *est non inversible modulo* $\mathfrak{p}$.

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

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

d'après le Lemme 3.4 ci-dessus. □

Comme E_φ est un endomorphisme de V_φ sur KC_χ, il existe un idéal premier $\mathfrak{P}\,|\,\mathfrak{p}$ de KC_χ tel que $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{P}}$. Mais toute conjugaison par $\tau \in G$ donne $E_\varphi^\tau = e_\varphi \sum\limits_{\nu\in G} \alpha^{\tau\nu}\,\nu^{-1} = e_\varphi \sum\limits_{\nu\in G} \alpha^\nu\,\nu^{-1}\,.\,(e_\varphi\tau) = E_\varphi \circ e_\varphi\tau$, et on obtient $\det(E_\varphi^\tau) = \det(E_\varphi)\det(e_\varphi\tau) \equiv 0 \pmod{\mathfrak{P}^\tau}$, d'où $\det(E_\varphi) \equiv 0 \pmod{\prod_{\tau\in G}\mathfrak{P}^\tau}$ puisque les $\det(e_\varphi\tau)$ sont inversibles.
Donc pour l'idéal premier $\mathfrak{p}\,|\,p$ de Z_χ tel que $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$ et $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{p}}$ (étendu à KC_χ), on est conduit à $P^\varphi(\ldots, \alpha^\nu, \ldots) \equiv 0 \pmod{\mathfrak{p}}$, donc à $\Delta_p^\varphi(\eta) \equiv 0 \pmod{\mathfrak{p}}$. Comme $\Delta_p^\theta(\eta)$ est la norme locale en $\mathfrak{p}$ de $\Delta_p^\varphi(\eta)$, on obtient :

Corollaire 3.6. — *Si* $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$, *on a* $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ *pour le caractère p-adique θ (au-dessus de φ) associé à $\mathfrak{p}$ (cf. Définition 2.5, §2.2.3)*

Lemme 3.7. — *Si l'endomorphisme* $E_\varphi := e_\varphi \sum\limits_{\nu\in G} \alpha^\nu\,\nu^{-1} \in \mathrm{End}_{KC_\chi}(V_\varphi)$ *est non inversible modulo* $\mathfrak{p}$, *alors il existe une φ-relation non nulle modulo $\mathfrak{p}$, de la forme* $W = \sum\limits_{\sigma\in G} w(\sigma)\sigma^{-1} \in e_\varphi\, Z_{\chi,(p)}[G]$, *telle que* $W.\,\alpha \equiv 0 \pmod{\mathfrak{p}}$.

Démonstration. — Le Lemme 2.2, §2.1 ramenant à des raisonnements $Z_{\chi,(p)}$-linéaires, il existe $W \in e_\varphi Z_{\chi,(p)}[G]$ tel que $W \not\equiv 0 \pmod{\mathfrak{p}}$ est dans le noyau de la transposée de E_φ, et on a la congruence $W\,.\,E_\varphi\,. \equiv 0 \pmod{\mathfrak{P}}$ pour $\mathfrak{P}\,|\,\mathfrak{p}$.
La relation $E_\varphi^\tau = E_\varphi \circ e_\varphi \tau$ et le fait que W est à coefficients dans $Z_{\chi,(p)}$ montrent, par conjugaisons, que la congruence a lieu modulo $\mathfrak{p}$ (étendu).
Posons $W = \sum_{\sigma\in G} w(\sigma)\sigma^{-1}$, $w(\sigma) \in Z_{\chi,(p)}$ pour tout $\sigma \in G$; la congruence $W\,.\,E_\varphi \equiv 0 \pmod{\mathfrak{p}}$ s'écrit (puisque $e_\varphi W = W$) :

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

d'où :

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

il en résulte $\sum_{\sigma\in G} w(\sigma)\alpha^{t^{-1}\sigma^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, pour tout $t \in G$, 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 $\mathfrak{p}$:

$$W = \sum_{\sigma\in G} w(\sigma)\,\sigma^{-1} \in e_\varphi Z_{\chi,(p)}[G]$$

(ceci n'entraînant pas $W \in e_\varphi \mathbb{Z}_{(p)}[G]$), telle que $W.\,\alpha \equiv 0 \pmod{\mathfrak{p}}$). □

3.2.2. Un cas particulier. — Soit $\eta \in K^\times$ et soit $\alpha = \alpha_p(\eta)$. Dans le G-module $\mathcal{L}$, considérons $U = \sum_{\nu\in G} u(\nu)\nu^{-1}$. On dispose par conjugaison des n congruences :

$$\sum_{\nu\in G} u(\nu)\,\alpha^{\tau\nu^{-1}} = \sum_{\nu\in G} u(\nu\tau)\,\alpha^{\nu^{-1}} \equiv 0 \pmod{p}, \quad \forall \tau \in G,$$

mais les relations $\sum_{\nu\in G} u(\nu\tau)\,\nu^{-1}$ (vues dans $\mathbb{F}_p[G]$) ne sont pas nécessairement $\mathbb{F}_p$-indépendantes.

Lemme 3.8. — *Le système des n relations $\big(\sum_{\nu\in G} u(\nu\tau)\,\nu^{-1}\big)_{\tau\in G}$, $u(\sigma) \in \mathbb{F}_p$ pour tout $\sigma \in G$, est de $\mathbb{F}_p$-rang 1 si et seulement si $u : G \longrightarrow \mathbb{F}_p^\times$ est un homomorphisme de groupes.*

Démonstration. — Si pour tout $\tau \in G$, il existe $\lambda(\tau) \in \mathbb{F}_p$ tel que $u(\nu\tau) = \lambda(\tau)u(\nu)$ pour tout $\nu \in G$, on a (en se ramenant par exemple à $u(1) = 1$ puisque $U \neq 0$), $u(\tau) = \lambda(\tau)$ pour tout τ, d'où $u(\nu\tau) = u(\nu)u(\tau)$ pour tout $\tau, \nu \in G$; donc $u : G \longrightarrow \mathbb{F}_p^\times$ est un homomorphisme de groupes. □

Par conséquent, l'image de u est un groupe cyclique d'ordre d diviseur de $p-1$ isomorphe à G/H où H (le noyau de u) fixe un sous-corps K' de K cyclique sur $\mathbb{Q}$ de degré d. Si l'on pose $\eta' = \mathrm{N}_{K/K'}(\eta)$, $r := u(s)$ (d'ordre d modulo p), où s est générateur dans $\mathrm{Gal}(K'/\mathbb{Q})$, on est ramené à une relation de la forme $\sum_{i=1}^{d} r^i\,\alpha'^{s^{-i}} \equiv 0 \pmod{p}$ avec $\alpha' = \mathrm{Tr}_{K/K'}(\alpha)$.
Ceci traduit la nullité modulo p de $\Delta_p^{\theta'}(\eta')$ pour le caractère θ' de K' défini par $\theta'(s) \equiv r \pmod{p}$.

Corollaire 3.9. — *Si le G-module $\mathcal{L}$ des relations $\sum_{\nu\in G} u(\nu)\,\nu^{-1} \in \mathbb{Z}_{(p)}[G]$ relatives à α est de $\mathbb{F}_p$-rang 1, alors il existe un unique caractère p-adique θ de degré 1 de G, dont le noyau fixe un sous-corps K' cyclique de K de degré d, et qui est tel que $\Delta_p^{\theta'}(\eta') \equiv \sum_{i=1}^{d} r^i\alpha'^{s^{-i}} \equiv 0 \pmod{p}$ où θ' est le caractère fidèle issu de θ.*

Remarque 3.10. — Comme $d\,|\,p-1$, p est totalement décomposé dans le corps $C_\chi = \mathbb{Q}(\mu_d)$. Donc θ est issu d'un caractère absolument irréductible φ unique. Posons $\varphi(s) = \zeta$; alors l'idéal $\mathfrak{p} = (p, \zeta - r)$ est un idéal premier au-dessus de p dans C_χ, ce qui identifie le couple $(\theta, \mathfrak{p})$ (cf. Définition 2.5 (ii), §2.2.3).

3.2.3. Résultats principaux. — Les résultats techniques des §§3.2.1, 3.2.2 conduisent à l'énoncé suivant (où p est supposé assez grand) :

Théorème 3.11. — *Soit $K/\mathbb{Q}$ une extension Galoisienne 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 $n = |G|$.*
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 $U \in \mathbb{Z}_{(p)}[G]$ relatif à $\alpha_p(\eta)$, i.e., telles que :

$$\sum_{\nu\in G} u(\nu)\,\alpha_p(\eta)^{\nu^{-1}} \equiv 0 \pmod p,\ \ u(\nu) \in \mathbb{Z}_{(p)} \text{ (cf. Définition 3.3, §3.2.1).}$$

On a alors les résultats suivants :
(i) Il existe une relation $U \not\equiv 0 \pmod{p\mathbb{Z}_{(p)}[G]}$ (i.e., $\mathcal{L}$ est non trivial) si et seulement si le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$ est divisible par p (cf. Remarque 2.18, §2.3.1).
(ii) Soit θ un caractère p-adique irréductible de G et soit f son degré résiduel (i.e., celui de p dans le corps des valeurs des caractères absolument irréductibles $\varphi\,|\,\theta$). 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 $\Delta_p^\theta(\eta)$ (cf. §2.3) est divisible par p. Dans ce cas, la $\mathbb{F}_p$-dimension de $\mathcal{L}^\theta$ est $\delta f \varphi(1)$, $1 \le \delta \le \varphi(1)$. [8]
(iii) Si $\dim_{\mathbb{F}_p}(\mathcal{L}) = 1$, alors θ est un caractère de degré 1 relatif à un sous-corps cyclique K' de K, et $\mathcal{L}$ est engendré par la θ-relation $\sum_{i=0}^{d-1} r^i\,\alpha_p(\eta')^{s^{-i}} \equiv 0 \pmod p$, où $\eta' := \mathrm{N}_{K/K'}(\eta)$, $d = [K' : \mathbb{Q}]\,\big|\,p-1$, où $r \in \mathbb{Z}$ et s générateur de $\mathrm{Gal}(K'/\mathbb{Q})$ sont tels que $\theta(s) \equiv r \pmod p$ (cf. Lemme 3.8, Corollaire 3.9 et Remarque 3.10, §3.2.2).

Démonstration. — Il reste donc à prouver le point (ii) de l'énoncé.
(a) Si $\mathcal{L}^\theta \ne \{0\}$, il existe $U = \sum_{\nu\in G} u(\nu)\,\nu^{-1} \in \mathcal{L}$ tel que $U_\theta \not\equiv 0 \pmod{\mathfrak{p}}$; donc $U_\varphi \not\equiv 0 \pmod{\mathfrak{p}}$ pour tout $\varphi\,|\,\theta$. D'après le Lemme 3.5 et le Corollaire 3.6, §3.2.1, on a $\Delta_p^\theta(\eta) \equiv 0 \pmod p$.
(b) Supposons que $\Delta_p^\theta(\eta) \equiv 0 \pmod p$; par la nullité modulo p de $\mathrm{Det}^G(\alpha)$ qui en résulte, il existe une relation de $\mathbb{F}_p$-dépendance de la forme $\sum_{\nu\in G} u(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod p$, $u(\nu) \in \mathbb{Z}_{(p)}$ non tous divisibles par p, et on a $U = \sum_{\nu\in G} u(\nu)\,\nu^{-1} \in \mathcal{L}$ (cf. Corollaire 3.2, §3.1), mais il convient d'en déduire $\mathcal{L}^\theta \ne \{0\}$.
Le cas Abélien (cf. §5.2) sera résolu de façon plus précise. D'après le Lemme 3.7, §3.2.1, il existe un caractère irréductible $\varphi\,|\,\theta$, et une φ-relation non triviale modulo $\mathfrak{p}$ de la forme $W := \sum_{\nu\in G} w(\nu)\nu^{-1}$, $w(\nu) \in Z_{\chi,(p)}$, telle que $W.\alpha \equiv 0 \pmod{\mathfrak{p}}$.
Soit L le corps de décomposition de p dans $C_\chi/\mathbb{Q}$ et soit $D = \mathrm{Gal}(C_\chi/L)$. Si $\{z, \ldots, z^f\}$ est une $Z_{L,(p)}$-base de $Z_{\chi,(p)}$, on a $w(\nu) = \sum_{i=1}^f a_i(\nu) z^i$ pour tout $\nu \in G$, $a_i(\nu) \in Z_{L,(p)}$, d'où $\sum_{\nu\in G}\sum_{i=1}^f a_i(\nu) z^i\,\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$; donc par identification sur la base des z^i on obtient le système de relations :

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

[8] On verra que l'on doit attribuer à cette éventualité la probabilité $\frac{1}{p^{f\delta^2}}$ (cf. §4.3.2).

Pour tout $i = 1, \dots, f$, et tout $\nu \in G$, il existe des $r^i_{\mathfrak p}(\nu) \in \mathbb{Z}$ tels que $a_i(\nu) \equiv r^i_{\mathfrak p}(\nu) \pmod{\mathfrak p}$, d'où $\sum_{\nu\in G} a_i(\nu)\alpha^{\nu^{-1}} \equiv \sum_{\nu\in G} r^i_{\mathfrak p}(\nu)\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak p}$, et comme $\sum_{\nu\in G} r^i_{\mathfrak p}(\nu)\alpha^{\nu^{-1}} \in K$, il vient $\sum_{\nu\in G} r^i_{\mathfrak p}(\nu)\alpha^{\nu^{-1}} \equiv 0 \pmod p$.

Puisque W est non triviale modulo $\mathfrak p$, les $r^i_{\mathfrak p}(\nu)$ ne sont pas tous nuls modulo p et il existe une relation non triviale $\sum_{\nu\in G} r^i_{\mathfrak p}(\nu)\,\alpha^{\nu^{-1}}$, $i \in \{1, \dots, f\}$. Comme W est une φ-relation, ceci se transmet à $\sum_{\nu\in G} a_i(\nu)\,\alpha^{\nu^{-1}}$ et par conséquent, $\sum_{\nu\in G} r^i_{\mathfrak p}(\nu)\,\nu^{-1}$ est une θ-relation non triviale de $\mathcal{L}$. De fait, la matrice $\big(r^i_{\mathfrak p}(\nu)\big)_{i,\nu}$ est de rang f. □

Remarque 3.12. — La $\mathbb{F}_p$-représentation irréductible V_θ de caractère θ est de dimension $f\varphi(1)$ et par extension des scalaires, on a $V_\theta \simeq fV_\varphi$; on a $\mathcal{L}^\theta \simeq \delta V_\theta$, $0 \le \delta \le \varphi(1)$, et $\mathcal{L}^\theta$ est de $\mathbb{F}_p$-dimension $\delta f\varphi(1)$.

Il est clair que $\delta = \varphi(1)$ équivaut à $\mathcal{L}^\theta = e_\theta\,\mathbb{F}_p[G]$ qui correspond à la relation $e_\theta\,\alpha \equiv 0 \pmod p$, autrement dit à un maximum de θ-relations.

Corollaire 3.13. — *(i) Lorsque $\mathcal{L}^\theta \ne \{0\}$, on obtient des relèvements de la forme $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$ pour toute θ-relation $U_\theta \in \mathcal{L}^\theta$.*

(ii) Sous la condition (iii) du théorème ($\mathcal{L} = \mathcal{L}^\theta$ de $\mathbb{F}_p$-dimension 1) et lorsque θ est un caractère fidèle, on a $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$, où $U_\theta = \sum_{k=0}^{n-1} r^k\,s^{-k}$ et où $n = |G|$ divise $p-1$ (cas totalement décomposé).

Démonstration. — Soit $\alpha := \alpha_p(\eta)$. On a $\eta_1^{U_\theta} = (1+p\,\alpha)^{U_\theta} \equiv 1+p\,U_\theta\cdot\alpha \pmod{p^2}$, et comme $U_\theta \cdot \alpha \equiv 0 \pmod p$ 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 $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$. Le cas (ii) est immédiat. □

Remarque 3.14. — D'après la Remarque 2.19 (ii), §2.3.1, le fait de remplacer η par $\eta' = \mathrm{N}_{K/K'}(\eta)$ ne modifie pas la question du nombre (fini ou non) de premiers p tels que $\Delta_p^G(\eta) \equiv 0 \pmod p$, car le nombre de sous-corps K' de K est fini auquel cas si $\Delta_p^G(\eta) \equiv 0 \pmod p$ pour une infinité de p, il existe un caractère rationnel fidèle χ' pour lequel $\Delta_p^{\chi'}(\eta') \equiv 0 \pmod p$ une infinité de fois.

3.3. Conséquences pratiques. — Donnons quelques exemples concrets. Il résulte de ce qui précède, lorsque $\Delta_p^\theta(\eta) \equiv 0 \pmod p$, que l'on peut trouver indiféremment une θ-relation $\sum_{\sigma\in G} u(\sigma)\,\sigma^{-1}$ à coefficients p-entiers rationnels, ou, pour $\varphi\,|\,\theta$, une φ-relation $\sum_{\sigma\in G} u_\varphi(\sigma)\,\sigma^{-1}$ à coefficients dans $Z_{\chi,(p)}$.

Exemple 3.15. — Pour un corps cubique cyclique K, on a $e_\chi = \frac{1}{3}(2 - \sigma - \sigma^2)$ pour $\chi \ne 1$. On a $C_\chi = \mathbb{Q}(j)$.

(i) Si p est inerte dans $C_\chi/\mathbb{Q}$, $\chi = \theta = \varphi + \varphi^s$, $f = 2$, et on montrera (cf. §5.1) que l'on obtient les θ-relations indépendantes $\alpha - \alpha^\sigma \equiv 0 \pmod p$ et $\alpha^\sigma - \alpha^{\sigma^2} \equiv 0 \pmod p$, conjuguées ($f = 2$). Donc $U = 1 - \sigma$ est telle que (avec $\varphi(\sigma) = j$) :

$$\begin{aligned} U_\varphi := e_\varphi\,U &= \frac{1}{3}(1 + j^{-1}\sigma + j^{-2}\sigma^2)(1-\sigma) = \frac{1}{3}(1 - j + (j^2-1)\,\sigma + (j - j^2)\,\sigma^2) \\ &= \frac{1}{3}(1-j)\,(1 + j^{-1}\sigma + j^{-2}\sigma^2), \end{aligned}$$

qui donne, à une unité p-adique près, $U_\varphi = 1 + j^{-1}\sigma + j^{-2}\sigma^2$ qui engendre la φ-composante $\mathcal{L}^\varphi$ associée à la relation $\Delta_p^\varphi(\eta) = \alpha + j^{-1}\alpha^\sigma + j^{-2}\alpha^{\sigma^2} \equiv 0 \pmod p$ et on a $\Delta_p^\theta(\eta) = \mathrm{N}_{C_\chi/\mathbb{Q}}(\Delta_p^\varphi(\eta)) \equiv 0 \pmod p$. Par identification sur la base

$\{1, j\}$, on retrouve les θ-relations à coefficients rationnels $\alpha - \alpha^\sigma \equiv 0 \pmod p$ et $\alpha^\sigma - \alpha^{\sigma^2} \equiv 0 \pmod p$.

(ii) Dans le cas p décomposé, il y a deux caractères p-adiques, dont $\theta = \varphi$, et on obtiendra une unique θ-relation de la forme $\Delta_p^\theta(\eta) = \alpha + r^{-1}\alpha^\sigma + r^{-2}\alpha^{\sigma^2} \equiv 0 \pmod p$ dont les conjuguées lui sont proportionnelles car $r^3 \equiv 1 \pmod p$.

D'où $U = 1 + r^{-1}\sigma + r^{-2}\sigma^2$, ce qui conduit (avec $j \equiv r \pmod{\mathfrak{p}}$ pour l'idéal premier $\mathfrak{p} \,|\, p$ associé à $\theta = \varphi$) à :

$$\begin{aligned} U_\varphi = e_\varphi U &= \tfrac{1}{3}(1 + j^{-1}\sigma + j^{-2}\sigma^2)(1 + r^{-1}\sigma + r^{-2}\sigma^2) \\ &= \tfrac{1}{3}(1 + r^{-1}j^{-2} + r^{-2}j^{-1})\,(1 + j^{-1}\sigma + j^{-2}\sigma^2) \\ &\equiv 1 + j^{-1}\sigma + j^{-2}\sigma^2 \pmod{\mathfrak{p}}, \end{aligned}$$

soit $U_\varphi = 1 + j^{-1}\sigma + j^{-2}\sigma^2$ engendrant $\mathcal{L}^\varphi$. On retrouve la θ-relation de départ à partir de $\alpha + j^{-1}\alpha^\sigma + j^{-2}\alpha^{\sigma^2} \equiv 0 \pmod{\mathfrak{p}}$ (étendu à KC_χ), qui donne ici $\alpha + r^{-1}\alpha^\sigma + r^{-2}\alpha^{\sigma^2} \equiv 0 \pmod{\mathfrak{p}}$ donc $\equiv 0 \pmod p$ (premier membre dans K).

Le conjugé θ^s de θ correspondrait à la congruence $j \equiv r \pmod{\mathfrak{p}^s}$ (équivalente à $j \equiv r^2 \pmod{\mathfrak{p}}$), mais on n'a pas nécessairement et simultanément la relation $\Delta_p^{\theta^s}(\eta) = \alpha + r^{-2}\alpha^\sigma + r^{-1}\alpha^{\sigma^2} \equiv 0 \pmod p$, ce qui conduirait à $\alpha \equiv \alpha^\sigma \equiv \alpha^{\sigma^2} \pmod p$ et la nullité modulo p de $\Delta_p^\theta(\eta)$ et de $\Delta_p^{\theta^s}(\eta)$ (probabilité en $\frac{O(1)}{p^2}$).

Exemple 3.16. — Prenons un exemple numérique (cf. §5.3.5) avec le corps K défini par le polynôme $Q = x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31$ (groupe D_6), pour $\chi = \theta = \chi_2$ de degré 2. Soit $\eta = x^5 - 2x^4 + 4x^3 - 3x^2 + x - 1$.

Pour $p = 61$, on obtient le G-module $\mathcal{L}$ à partir des trois relations $\mathbb{F}_p$-linéaires indépendantes (par programme) :

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

L'idempotent "trace" e_1 donne la relation triviale, donc le p-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} (χ_1 non trivial de degré 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 du θ-régulateur $\Delta_p^\theta(\eta)$). De fait, il s'agit d'une nullité triviale car le programme trouve 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 suivantes :

$$\tau U = 24U + 51\sigma U, \quad \tau\sigma U = 27U + 37\sigma U, \quad \tau\sigma^2 U = 10U + 34\sigma U.$$

Par la suite, nous supposerons que le $\mathbb{Z}[G]$-module F engendré par η est de $\mathbb{Z}$-rang $n = |G|$ (afin qu'il n'y ait pas de nullités triviales).

Ensuite, nous négligerons les premiers p pour lesquels au moins deux θ-régulateurs sont divisible par p, une telle probabilité étant au plus en $\frac{O(1)}{p^2}$, vu l'indépendance des θ-régulateurs associés à plusieurs caractères p-adiques (cf. §4.2 pour des statistiques numériques). 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 (tout cas contraire donnant une probabilité au plus en $\frac{O(1)}{p^2}$).

L'obstruction essentielle viendrait alors des p satisfaisant à la définition suivante :

Définition 3.17. — Un nombre premier p constitue un cas de *p-divisibilité minimale* $p^{\varphi(1)}$ (pour le régulateur normalisé $\mathrm{Reg}_p^G(\eta)$) s'il existe un unique θ tel que : $\Delta_p^\theta(\eta) \equiv 0 \pmod p$, p est totalement décomposés dans le corps des valeurs de $\varphi \,|\, \theta$ (i.e., $f = 1$), $\mathcal{L}^\theta \simeq \delta V_\theta$ est de $\mathbb{F}_p$-dimension minimale (i.e., $\delta = 1$), et $\mathrm{Reg}_p^\theta(\eta) \sim p$; dans ce cas, $\mathrm{Reg}_p^G(\eta) \sim p^{\varphi(1)}$ (cf. Remarque 2.18, § 2.3.1).

Si G est Abélien, il s'agit des $p \equiv 1 \pmod n$, où n est l'ordre de φ.

4. Expérimentations et considérations heuristiques

4.1. Méthodes probabilistes en théorie des nombres. — 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 (cf. [**T**], Chap. III.1).

Dans notre cas, E_p est pour $\eta \in K^\times$ fixé l'événement "$\Delta_p^G(\eta) \equiv 0 \pmod p$" ou "$\Delta_p^\chi(\eta) \equiv 0 \pmod p$" ($\chi$ rationnel) ou encore "$\Delta_p^\theta(\eta) \equiv 0 \pmod p$" qui n'est défini que si l'on choisit un $\theta \,|\, \chi$ pour chaque p (cf. §2.3).

Tout se joue alors sur la valeur $\Pr(E_p) = \frac{1}{p^{1+\epsilon(p,\eta)}}$, $\epsilon(p, \eta) > 0$ ou $\epsilon(p, \eta) = 0$, pour les cas de p-divisibilité minimale $p^{\varphi(1)}$ (Définition ci-dessus).

En l'absence d'arguments théoriques précis, il est d'usage de supposer que le cas $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ se produit avec une probabilité en $\frac{O(1)}{p}$.[9] Il en résulte alors que le nombre de solutions $p < x$ à $\Delta_p^G(\eta) = \prod_\theta \Delta_p^\theta(\eta)^{\varphi(1)} \equiv 0 \pmod p$ serait de l'ordre de $O(1) \sum_{p<x} \frac{1}{p}$, donc de $O(1)\mathrm{loglog}(x)$. Voir la Remarque 2.18, §2.3.1 pour l'interprétation en termes de p-divisibilités des régulateurs correspondants.

Or il est évident, puisque $\Delta_p^\theta(\eta)$ est une norme locale dans l'extension $C_\chi/\mathbb{Q}$, qu'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 $\varphi \,|\, \theta$ est de degré $\varphi(1) \geq 2$, la divisibilité par $p^{f\varphi(1)}$ intervient puisque $\Delta_p^\theta(\eta) = \prod_{\varphi \,|\, \theta} \Delta_p^\varphi(\eta)$ est élevé à la puissance $\varphi(1)$. Cependant il n'est pas clair pour autant que la "probabilité" d'être divisible par p (ou la "densité des cas observés") soit de façon précise fonction de $f\,\varphi(1)$. On verra que le degré $\varphi(1)$ n'intervient pas directement 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 " $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ & $\mathcal{L}^\theta \simeq \delta V_\theta$ " (cf. §4.3.2). On admettra donc que tous les cas de probabilité au plus en $\frac{O(1)}{p^2}$

[9] Nous utilisons par commodité un numérateur $O(1)$, toujours effectif et souvent égal à 1.

sont en nombre fini et peuvent être écartés pour p assez grand. En outre il faut s'assurer que les $\Delta_p^\theta(\eta)$ modulo p sont indépendants.

4.2. Indépendance probabiliste (sur θ) des variables $\Delta_p^\theta(\eta)$. — Nous traitons d'abord le cas du groupe D_6, par utilisation de la fonction *random*, pour déterminer deux aspect :

(i) l'indépendance des θ-régulateurs (probabilité au plus en $\frac{O(1)}{p^2}$ d'avoir deux θ-régulateurs $\Delta_p^\theta(\eta)$ et $\Delta_p^{\theta'}(\eta)$ nuls modulo p, pour $\theta \neq \theta'$) ;

(ii) la probabilité en $\frac{O(1)}{p}$ d'avoir la nullité modulo p de $\Delta_p^\theta(\eta)$ 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 $\mathbb{Q}(j)$) défini par le polynôme
$$Q = x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31.$$
On prend au hasard η modulo p^2, étranger à p, ce qui donne des α répartis aléatoirement modulo p. On peut choisir p à volonté (ici $p = 37$).

Le programme calcule les conjugués de $\alpha = \alpha_p(\eta)$ sur la base $\{x^5, x^4, x^3, x^2, x, 1\}$. La variable N_0 compte le nombre de η étrangers à p. Ensuite, chacun des trois régulateurs est calculé, et dans les variables $N_1, N_2, N_3, N_{12}, N_{13}, N_{23}, N_{123}$, on donne le nombre de cas de nullités simultanées de 1, 2 ou 3 régulateurs.

La procédure *nfgaloisconj* pour D_6 donne les automorphismes dans l'ordre :
$$1, \tau, \sigma\tau = \tau\sigma^2, \sigma^2\tau = \tau\sigma, \sigma, \sigma^2,$$
que nous avons permuté pour avoir (de e_1 à e_6) la liste $1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$.

```
{Q = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + 31; p = 37; p2 = p^2;
e1 = x;
e2 = 11/180*x^5 + 1/180*x^4 + 11/18*x^3 - 1/45*x^2 + 403/180*x + 419/180;
e3 = 13/180*x^5 - 7/180*x^4 + 13/18*x^3 - 38/45*x^2 + 509/180*x + 127/180;
e4 = -4/45*x^5 + 1/45*x^4 - 8/9*x^3 + 26/45*x^2 - 137/45*x - 91/45;
e5 = -1/60*x^5 - 1/60*x^4 - 1/6*x^3 - 4/15*x^2 - 73/60*x - 79/60;
e6 = -1/36*x^5 + 1/36*x^4 - 5/18*x^3 + 5/9*x^2 - 65/36*x + 11/36;
N0 = 0; N1 = 0; N2 = 0; N3 = 0; N12 = 0; N13 = 0; N23 = 0; N123 = 0;
for(i = 1, 1000000,
a = random(p2); b = random(p2); c = random(p2);
aa = random(p2); bb = random(p2); cc = random(p2);
Eta = Mod(a*e1^5 + b*e1^4 + c*e1^3 + aa*e1^2 + bb*e1 + cc, Q);
N = norm(Eta); if(Mod(11*N, p)! = 0, N0 = N0 + 1;
u = Mod(a, p2); v = Mod(b, p2); w = Mod(c, p2);
uu = Mod(aa, p2); vv = Mod(bb, p2); ww = Mod(cc, p2);
P = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + Mod(31, p);
P2 = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + Mod(31, p2);
y = Mod(u*x^5 + v*x^4 + w*x^3 + uu*x^2 + vv*x + ww, P2);
z = y^(p-1); t = z; for(i = 1, 5, z = z^p*t); U = component(z - 1, 2);
u1 = component(U, 1); if(u1 == 0, u1 = Mod(0, p2));
u2 = component(U, 2); if(u2 == 0, u2 = Mod(0, p2));
u3 = component(U, 3); if(u3 == 0, u3 = Mod(0, p2));
u4 = component(U, 4); if(u4 == 0, u4 = Mod(0, p2));
u5 = component(U, 5); if(u5 == 0, u5 = Mod(0, p2));
u6 = component(U, 6); if(u6 == 0, u6 = Mod(0, p2));
x1 = component(u1, 2)/p; x2 = component(u2, 2)/p; x3 = component(u3, 2)/p;
x4 = component(u4, 2)/p; x5 = component(u5, 2)/p; x6 = component(u6, 2)/p;
X1 = Mod(x1, p); X2 = Mod(x2, p); X3 = Mod(x3, p);
X4 = Mod(x4, p); X5 = Mod(x5, p); X6 = Mod(x6, p);
E1 = Mod(X1 + X2*e1 + X3*e1^2 + X4*e1^3 + X5*e1^4 + X6*e1^5, P);
E2 = Mod(X1 + X2*e2 + X3*e2^2 + X4*e2^3 + X5*e2^4 + X6*e2^5, P);
E3 = Mod(X1 + X2*e3 + X3*e3^2 + X4*e3^3 + X5*e3^4 + X6*e3^5, P);
```

```
E4=Mod(X1+X2*e4+X3*e4^2+X4*e4^3+X5*e4^4+X6*e4^5,P);
E5=Mod(X1+X2*e5+X3*e5^2+X4*e5^3+X5*e5^4+X6*e5^5,P);
E6=Mod(X1+X2*e6+X3*e6^2+X4*e6^3+X5*e6^4+X6*e6^5,P);
F1=component(E1,2);F2=component(E2,2);F3=component(E3,2);
F4=component(E4,2);F5=component(E5,2);F6=component(E6,2);
SP=F1+F2+F3;SM=F4+F5+F6;FP=SP+SM;FM=SP-SM;
RP=E1^2+E2^2+E3^2-E4^2-E5^2-E6^2-E1*E2-E2*E3-E3*E1
                                        +E4*E5+E5*E6+E6*E4;
if(FP==0,N1=N1+1);
if(FM==0,N2=N2+1);
if(RP==0,N3=N3+1);
if(FP==0&FM==0,N12=N12+1);
if(FP==0&RP==0,N13=N13+1);
if(FM==0&RP==0,N23=N23+1);
if(FP==0&FM==0&RP==0,N123=N123+1)));
print("p=",p,"","N1=",N1,"","N2=",N2,"","N3=",N3,"",
(N1+0.0)/N0,"",(N2+0.0)/N0,"",(N3+0.0)/N0);
print("N12=",N12,"","N13=",N13,"","N23=",N23,"","N123=",N123,"",
(N12+0.0)/N0,"",(N13+0.0)/N0,"",(N23+0.0)/N0,"",(N123+0.0)/N0);
print("","1/p=",1./p,"","1/p^2=",1./p^2,"","1/p^3=",1./p^3)}
```

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

On donnera au §4.4 des programmes effectuant ces statistiques à partir du calcul du rang de la matrice des coefficients des conjugués de α (groupes C_3, C_5 et D_6). Pour les groupes cycliques, le degré résiduel intervient contrairement au cas de D_6, où $f = 1$ quel que soit p, mais pour D_6 l'entier δ vaut 0, 1 ou 2.

4.3. Principes d'analyse – Linéarisation du problème. — Soit $\eta \in K^\times$ donné ; on suppose pour simplifier que le G-module engendré par η est de $\mathbb{Z}$-rang $n = |G|$ (sinon on doit tenir compte des nullités triviales).

On considère le G-module $\mathcal{L}$ engendré par les relations à coefficients p-entiers rationnels (cf. Définition 3.3, §3.2.1). Comme il a été vu dans le §3.2, la condition $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ équivaut à la non trivialité de $\mathcal{L}^\theta$ (cf. Théorème 3.11, §3.2.3) et c'est cet aspect "linéarisé" qui va permettre l'analyse probabiliste.

Le cas $\chi = \theta = 1$ a lieu pour tout groupe G et $\Delta_p^1(\eta)$ est congru modulo p au p-quotient de Fermat $q_p(a)$ de $a = \mathrm{N}_{K/\mathbb{Q}}(\eta)$. On peut admettre a priori que ce quotient de Fermat a la probabilité $\frac{1}{p}$ d'être égal à une valeur $t \pmod p$ donnée, mais nous reviendrons sur cette question au §7.5 pour suggérer que ceci semble arbitraire (voir cependant dans [**Hat**], § 2, l'étude statistique de la distribution de $q_p(2)$ modulo $p \leq 1010783$, mais p n'est ici pas très grand).

La relation $\mathrm{N}_{K/\mathbb{Q}}(\eta) = a$ se transmet à $\alpha = \alpha_p(\eta)$ via la formule $\sum_{\nu\in G} \alpha^\nu \equiv q_p(a) \pmod p$ qui constitue, pour $\theta = 1$, la θ-relation linéaire non triviale associée à la nullité modulo p de $\Delta_p^1(\eta)$ lorsque $q_p(a) \equiv 0 \pmod p$.

L'existence d'une θ-relation linéaire non triviale entre les conjugués de α peut toujours, pour la commodité numérique des programmes, s'exprimer sur n variables rationnelles de la forme $A_1, \ldots, A_n$, où les A_i sont par exemple les composantes de α sur une $\mathbb{Z}_{(p)}$-base de $Z_{K,(p)}$.

Pour introduire cet aspect statistique par le calcul, nous reprenons en détail le cas cubique cyclique, §5.1, puis le cas Abélien en toute généralité, §5.2. Dans le §5.3, nous traitons un cas non Abélien via le groupe D_6.

4.3.1. Principes heuristiques et probabilistes. — On peut poser les principes heuristiques suivants (p fixé assez grand et utilisation de la fonction *random* de PARI pour définir η étranger à p) :

(i) On peut se limiter à connaître le nombre η modulo p^2 puisque α est défini par $\alpha \equiv \frac{-1}{p}\log_p(\eta) \pmod p$.

Bien que la correspondance entre η modulo p^2 (η étranger à p) et $\alpha \equiv \frac{-1}{p}\log_p(\eta)$ modulo p soit *algébriquement* canonique, nous avons préféré partir de η afin de respecter l'aspect diophantien, d'autant que par utilisation de *random*, tous les η ne sont pas atteints. Par exemple, négliger cet aspect pour le cas $K = \mathbb{Q}$ reviendrait à utiliser la fonction *random* sur l'intervalle $[0, p-1]$ en notant le nombre de fois où 0 est pris, ce qui n'a plus rien à voir avec le sujet !

Si d'un point de vue p-adique, α parcourt de façon équiprobable l'anneau quotient $Z_{K,(p)}/(p) \simeq \mathbb{F}_p^n$, l'expérience montre que les résultats statistiques restent excellents si pour p assez grand on limite la fonction *random* (pour définir η) à un petit domaine de $(\mathbb{Z}/p^2\mathbb{Z})^n$, ce qui préserve l'aspect diophantien et démontre une uniformité (limitation obligatoire lorsque p est très grand).

(ii) Soit $(e_i)_{i=1,\ldots,n}$ une $\mathbb{Z}_{(p)}$-base de $Z_{K,(p)}$ et posons $\alpha = \sum_{i=1}^n A_i e_i$, $A_i \in \mathbb{Z}_{(p)}$; alors, modulo p, les variables A_i sont indépendantes et équiprobables dans $\mathbb{F}_p$, et ceci ne dépend pas du groupe G ni du choix de la base.

(iii) Toute relation non triviale de la forme $\sum_{\nu\in G} u(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod p$ 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).

4.3.2. Heuristique principale.— La probabilité de $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ est celle de $\mathcal{L}^\theta \neq \{0\}$ (cf. Théorème 3.11, §3.2.3). Elle est induite par le nombre de relations $\mathbb{F}_p[G]$-indépendantes. Compte tenu de la Remarque 3.12, §3.2.3, si $\mathcal{L}^\theta \simeq \delta V_\theta$, $1 \le \delta \le \varphi(1)$, on peut justifier, de la façon suivante, que l'on doit affecter à ce cas une probabilité en $\frac{O(1)}{p^{f\delta^2}}$, où f est le degré résiduel de θ (i.e., celui de p dans le corps des valeurs C_χ de $\varphi\,|\,\theta$), où l'on considère V_θ comme $\mathbb{F}_p$-représentation et ensuite, par extension des scalaires, V_θ et V_φ comme $\mathbb{F}_{p^f}$-représentations :

On a $\mathcal{L}^\theta = \bigoplus_{\varphi\,|\,\theta} \mathcal{L}^\varphi$ où $\mathcal{L}^\varphi \simeq \delta V_\varphi$. L'idée est que si $\mathcal{L}^\varphi \simeq \varphi(1)V_\varphi \simeq e_\varphi \mathbb{F}_{p^f}[G]$, (i.e., $e_\varphi\alpha \equiv 0 \pmod p$) alors la probabilité correspondante est minimale en $\frac{O(1)}{p^{f\varphi(1)^2}}$ puisque $e_\varphi\alpha$ est défini par $f\varphi(1)^2$ composantes indépendantes dans $\mathbb{F}_p$ (cf. (ii)).

Or $e_\varphi\mathbb{F}_{p^f}[G] \simeq \mathrm{End}(V_\varphi)$ comme algèbre d'endomorphismes d'un $\mathbb{F}_{p^f}$-espace vectoriel de dimension $\varphi(1)$. Par conséquent, $\mathcal{L}^\varphi \simeq \delta V_\varphi$ est alors vue comme sous-algèbre d'endomorphismes d'un $\mathbb{F}_{p^f}$-espace vectoriel de dimension δ, d'où une probabilité en $\frac{O(1)}{p^{f\delta^2}}$ d'avoir $\mathcal{L}^\varphi \simeq \delta V_\varphi$. On notera que la probabilité d'avoir tous les $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ avec chaque fois $\delta = \varphi(1)$ (i.e., $\alpha \equiv 0 \pmod p$, ou encore aux n composantes de α nulles modulo p) est $\frac{O(1)}{p^n}$ puisque $\sum_\theta f\varphi(1)^2 = |G| = n$. 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 grand (très bien confirmé par les statistiques numériques, cf. § 4.4.3).

Exemple 4.1. — Cas de $G = D_6$ ($f = 1$, $1 \le \delta \le 2$). Soit θ le caractère irréductible de degré 2 ; la représentation $e_\theta\mathbb{F}_p[G]$ est isomorphe à $2\,V_\theta$ où V_θ est de $\mathbb{F}_p$-dimension 2. On peut par exemple engendrer $e_\theta\mathbb{F}_p[G]$ de la façon suivante (cf. Remarque 2.15, §2.2.6) :

On considère les θ-relations $U_1 = 1 - \sigma^2 + \tau - \tau\sigma$ et $U_2 = 1 - \sigma - \tau + \tau\sigma$, et on vérifie que l'on a les expressions :

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

$$\begin{aligned} &\tau U_1 = -\sigma U_1,\ \ \tau\sigma U_1 = -U_1,\ \ \tau\sigma^2 U_1 = -\sigma^2 U_1,\\ &\tau U_2 = -U_2,\ \ \tau\sigma U_2 = -\sigma^2 U_2,\ \ \tau\sigma^2 U_2 = -\sigma U_2. \end{aligned}$$

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

4.4. Statistiques sur le rang de la matrice des coefficients. — Une première statistique consiste à déterminer la probabilité d'avoir au moins une relation non triviale entre les conjugués de α ; si $\alpha^\nu = \sum_{i=1}^n A_i(\nu)\, e_i$, alors la matrice $\big(A_i(\nu)\big)_{i,\nu}$ doit être de $\mathbb{F}_p$-rang strictement inférieur à n.

Nous avons vu que pour $\theta \,|\, \chi$ la probabilité de nullité modulo p de $\Delta_p^\theta(\eta)$ seul est en $\frac{1}{p^f}$, où f est le degré résiduel de θ (i.e., celui de p dans $C_\chi/\mathbb{Q}$) ; comme il y a $h = \frac{[C_\chi:\mathbb{Q}]}{f}$ tels caractères p-adiques $\theta \,|\, \chi$, la probabilité d'avoir au moins un $\Delta_p^\theta(\eta)$ nul modulo p pour $\theta \,|\, \chi$ est en $\frac{h}{p^f}$.

Par conséquent si l'on désigne par θ_i, h_i, f_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 :

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

ce que l'on peut vérifier au moyen des programmes suivants calculant, pour des η aléatoires, le nombre de cas de $\mathbb{F}_p$-rang $< n$ ($G \simeq C_3, C_5, D_6$ respectivement) :

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

```
{t=11;Q=x^3-t*x^2-(t+3)*x-1;p=43;p2=p^2;N0=0;N3=0;
for(i=1,500000,aa=random(p2);bb=random(p2);cc=random(p2);
e=Mod(aa*x^2+bb*x+cc,Q);N=norm(e);if(Mod(N,p)!=0,N0=N0+1;
a=Mod(aa,p2);b=Mod(bb,p2);c=Mod(cc,p2);
P=x^3-t*x^2-(t+3)*x-Mod(1,p);P2=x^3-t*x^2-(t+3)*x-Mod(1,p2);
y=Mod(a*x^2+b*x+c,P2);u=y^(p+1);v=u^p*y;z=v^(p-1)-1;
U=component(z,2);
```

```
u1 = component(U,1); if(u1 == 0, u1 = Mod(0,p2));
u2 = component(U,2); if(u2 == 0, u2 = Mod(0,p2));
u3 = component(U,3); if(u3 == 0, u3 = Mod(0,p2));
x1 = component(u1,2)/p; x2 = component(u2,2)/p; x3 = component(u3,2)/p;
X1 = Mod(x1,p); X2 = Mod(x2,p); X3 = Mod(x3,p);
SX1 = X1 - 2*X2 - X3*(t-2);
SX2 = -X3*(t^2+t+1) - X2*(t+1);
SX3 = X3*t + X2;
TX1 = X3*(t^2+3*t+4) + X2*(t+2) + X1;
TX2 = X3*(t^2+t+1) + X2*t;
TX3 = -X3*(t+1) - X2;
E1 = Mod(X1 + X2*x + X3*x^2, P);
E2 = Mod(SX1 + SX2*x + SX3*x^2, P);
E3 = Mod(TX1 + TX2*x + TX3*x^2, P);
F1 = component(E1,2); F2 = component(E2,2); F3 = component(E3,2); GG = [F1,F2,F3];
M = matrix(3,3,i,j,component(component(GG,i),j)); r = matrank(M);
if(r < 3, N3 = N3+1))); print("p = ",p,"",N0,"","N3 = ",N3,"",(N3+0.0)/N0);
res = Mod(p,3); if(res == Mod(1,3), print(3./p - 3./p^2 + 1./p^3));
if(res! = Mod(1,3), print(1./p + 1./p^2 - 1./p^3))}
```

On obtient les exemples suivants :
$p = 43,\ N_0 = 4999952,\ N3 = 341000,\ \frac{N_3}{N_0} = 0.068200$, probabilité 0.068685.
$p = 41,\ N_0 = 4999931,\ N3 = 124889,\ \frac{N_3}{N_0} = 0.024978$, probabilité 0.024970.

4.4.2. Cas G cyclique d'ordre 5 (deux caractères rationnels). — Ce cas est le seul des cas étudiés pour lequel il y a (pour $p \equiv -1 \pmod 5$) deux caractères p-adiques de degré résiduel $f = 2$.

```
{Q = x^5 + x^4 - 4*x^3 - 3*x^2 + 3*x + 1; p = 13; p2 = p^2;
s1 = x; s2 = x^2 - 2; s3 = x^4 - 4*x^2 + 2; s4 = x^3 - 3*x; s5 = -x^4 - x^3 + 3*x^2 + 2*x - 1;
N0 = 0; N5 = 0;
for(i = 1,500000,
aa = random(p2); bb = random(p2); cc = random(p2); dd = random(p2); ee = random(p2);
Eta = Mod(aa*x^4 + bb*x^3 + cc*x^2 + dd*x + ee, Q);
N = norm(Eta); if(Mod(N,p)! = 0, N0 = N0+1;
a = Mod(aa,p2); b = Mod(bb,p2); c = Mod(cc,p2); d = Mod(dd,p2); e = Mod(ee,p2);
P = x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p); P2 = x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p2);
y = Mod(a*x^4 + b*x^3 + c*x^2 + d*x + e, P2);
u = y^(p+1); v = u^p*y; w = v^p*y; s = w^p*y; t = s^(p-1) - 1;
U = component(t,2);
u1 = component(U,1); if(u1 == 0, u1 = Mod(0,p2));
u2 = component(U,2); if(u2 == 0, u2 = Mod(0,p2));
u3 = component(U,3); if(u3 == 0, u3 = Mod(0,p2));
u4 = component(U,4); if(u4 == 0, u4 = Mod(0,p2));
u5 = component(U,5); if(u5 == 0, u5 = Mod(0,p2));
x1 = component(u1,2)/p; x2 = component(u2,2)/p; x3 = component(u3,2)/p;
                        x4 = component(u4,2)/p; x5 = component(u5,2)/p;
X1 = Mod(x1,p); X2 = Mod(x2,p); X3 = Mod(x3,p); X4 = Mod(x4,p); X5 = Mod(x5,p);
E1 = Mod(X5*s1^4 + X4*s1^3 + X3*s1^2 + X2*s1 + X1, P);
E2 = Mod(X5*s2^4 + X4*s2^3 + X3*s2^2 + X2*s2 + X1, P);
E3 = Mod(X5*s3^4 + X4*s3^3 + X3*s3^2 + X2*s3 + X1, P);
E4 = Mod(X5*s4^4 + X4*s4^3 + X3*s4^2 + X2*s4 + X1, P);
E5 = Mod(X5*s5^4 + X4*s5^3 + X3*s5^2 + X2*s5 + X1, P);
F1 = component(E1,2); F2 = component(E2,2); F3 = component(E3,2);
                        F4 = component(E4,2); F5 = component(E5,2);
GG = [F1,F2,F3,F4,F5];
M = matrix(5,5,i,j,component(component(GG,i),j)); r = matrank(M);
if(r < 5, N5 = N5+1))); print("p = ",p,"",N0,"","N5 = ",N5,"",(N5+0.0)/N0);
res = Mod(p,5); if(res == Mod(1,5), print(5./p - 10./p^2 + 10./p^3 - 5./p^4 + 1./p^5));
if(res^2 == Mod(-1,5), print(1./p + 1./p^4 - 1./p^5));
```

$if(res == Mod(-1,5), print(1./p + 2./p^2 - 2./p^3 - 1./p^4 + 1./p^5))\}$

Valeurs numériques obtenues :
$p = 7$, $N_0 = 499977$, $N5 = 71650$, $\frac{N_5}{N_0} = 0.14330$, probabilité 0.143214.
$p = 19$, $N_0 = 500000$, $N5 = 29033$, $\frac{N_5}{N_0} = 0.05806$, probabilité 0.057880.
$p = 31$, $N_0 = 500000$, $N5 = 75737$, $\frac{N_5}{N_0} = 0.15147$, probabilité 0.151214.

En modifiant la fin du programme comme suit :

$F1 = component(E1, 2); F2 = component(E2, 2); F3 = component(E3, 2);$
$F4 = component(E4, 2); F5 = component(E5, 2);$
$H = F1 + F2 + F3 + F4 + F5;$
$R1 = F1 + 2 * F2 + 4 * F3 + 8 * F4 + 16 * F5; R2 = F1 + 4 * F2 + 16 * F3 + 2 * F4 + 8 * F5;$
$R3 = F1 + 8 * F2 + 2 * F3 + 16 * F4 + 4 * F5; R4 = F1 + 16 * F2 + 8 * F3 + 4 * F4 + 2 * F5;$
$M = matrix(5, 5, i, j, component(component(GG, i), j));$
$if(H! = 0\&R1 == 0\&R2 == 0\&R3! = 0\&R4! = 0, N1 = N1 + 1)));$
$print("p = ", p, "", N0, "", "N1 = ", N1, "", (N1 + 0.0)/N0); print(1./p^2)$

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 cinq, à savoir par exemple pour θ_1 et θ_2 définis par $\theta_1(\sigma^{-1}) \equiv 2$, $\theta_2(\sigma^{-1}) \equiv 4 \pmod p$:

$$R_1 = \alpha + 2\alpha^{\sigma} + 4\alpha^{\sigma^2} + 8\alpha^{\sigma^3} + 16\alpha^{\sigma^4} \text{ et } R_2 = \alpha + 4\alpha^{\sigma} + 16\alpha^{\sigma^2} + 2\alpha^{\sigma^3} + 8\alpha^{\sigma^4}.$$

Pour $N_0 = 1000000$, $N_1 = 943$, on a $\frac{N_1}{N_0} = 0.000943$, et la probabilité 0.001040, ce qui montre l'indépendance des régulateurs relatifs à des caractères p-adiques d'un même caractère rationnel. Les autres combinaisons donnent des résultats semblables.

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. On doit également tester les probabilités relevant de la valeur de δ.

$\{Q = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + 31; p = 17; p2 = p^2;$
$e1 = x;$
$e2 = 11/180 * x^5 + 1/180 * x^4 + 11/18 * x^3 - 1/45 * x^2 + 403/180 * x + 419/180;$
$e3 = 13/180 * x^5 - 7/180 * x^4 + 13/18 * x^3 - 38/45 * x^2 + 509/180 * x + 127/180;$
$e4 = -4/45 * x^5 + 1/45 * x^4 - 8/9 * x^3 + 26/45 * x^2 - 137/45 * x - 91/45;$
$e5 = -1/60 * x^5 - 1/60 * x^4 - 1/6 * x^3 - 4/15 * x^2 - 73/60 * x - 79/60;$
$e6 = -1/36 * x^5 + 1/36 * x^4 - 5/18 * x^3 + 5/9 * x^2 - 65/36 * x + 11/36;$
$N0 = 0; N1 = 0; N6 = 0;$
$for(i = 1, 50000, a = random(p2); b = random(p2); c = random(p2); aa = random(p2);$
$bb = random(p2); cc = random(p2);$
$Eta = Mod(a * e1^5 + b * e1^4 + c * e1^3 + aa * e1^2 + bb * e1 + cc, Q);$
$N = norm(Eta); if(Mod(N, p)! = 0, N0 = N0 + 1;$
$u = Mod(a, p2); v = Mod(b, p2); w = Mod(c, p2); uu = Mod(aa, p2);$
$vv = Mod(bb, p2); ww = Mod(cc, p2);$
$P = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + Mod(31, p);$
$P2 = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + Mod(31, p2);$
$y = Mod(u * x^5 + v * x^4 + w * x^3 + uu * x^2 + vv * x + ww, P2);$
$z = y^{(p-1)}; t = z; for(i = 1, 5, z = z^p * t);$
$U = component(z - 1, 2);$
$u1 = component(U, 1); if(u1 == 0, u1 = Mod(0, p2));$
$u2 = component(U, 2); if(u2 == 0, u2 = Mod(0, p2));$
$u3 = component(U, 3); if(u3 == 0, u3 = Mod(0, p2));$
$u4 = component(U, 4); if(u4 == 0, u4 = Mod(0, p2));$
$u5 = component(U, 5); if(u5 == 0, u5 = Mod(0, p2));$
$u6 = component(U, 6); if(u6 == 0, u6 = Mod(0, p2));$
$x1 = component(u1, 2)/p; x2 = component(u2, 2)/p; x3 = component(u3, 2)/p;$
$x4 = component(u4, 2)/p; x5 = component(u5, 2)/p; x6 = component(u6, 2)/p;$

$X1 = Mod(x1, p); X2 = Mod(x2, p); X3 = Mod(x3, p);$
$X4 = Mod(x4, p); X5 = Mod(x5, p); X6 = Mod(x6, p);$
$E1 = Mod(X1 + X2 * e1 + X3 * e1^2 + X4 * e1^3 + X5 * e1^4 + X6 * e1^5, P);$
$E2 = Mod(X1 + X2 * e2 + X3 * e2^2 + X4 * e2^3 + X5 * e2^4 + X6 * e2^5, P);$
$E3 = Mod(X1 + X2 * e3 + X3 * e3^2 + X4 * e3^3 + X5 * e3^4 + X6 * e3^5, P);$
$E4 = Mod(X1 + X2 * e4 + X3 * e4^2 + X4 * e4^3 + X5 * e4^4 + X6 * e4^5, P);$
$E5 = Mod(X1 + X2 * e5 + X3 * e5^2 + X4 * e5^3 + X5 * e5^4 + X6 * e5^5, P);$
$E6 = Mod(X1 + X2 * e6 + X3 * e6^2 + X4 * e6^3 + X5 * e6^4 + X6 * e6^5, P);$
$F1 = component(E1, 2); F2 = component(E2, 2); F3 = component(E3, 2);$
$F4 = component(E4, 2); F5 = component(E5, 2); F6 = component(E6, 2);$
$GG = [F1, F2, F3, F4, F5, F6];$
$M = matrix(6, 6, i, j, component(component(GG, i), j)); r = matrank(M);$
$if(r < 6, N6 = N6 + 1)));$
$print("p = ", p, "", N0, "", "N6 = ", N6, "", (N6 + 0.0)/N0); print(3./p - 3./p^2 + 1./p^3)\}$

Les résultats ne dépendent pas de classes de congruences de p car on a $C_\chi = \mathbb{Q}$:

$p = 13,\ N_0 = 49954,\ N6 = 10794,\ \frac{N_6}{N_0} = 0.21607$, probabilité 0.21347.
$p = 17,\ N_0 = 49516,\ N6 = 8337,\ \frac{N_6}{N_0} = 0.16836$, probabilité 0.16629.
$p = 29,\ N_0 = 49815,\ N6 = 5056,\ \frac{N_6}{N_0} = 0.10149$, probabilité 0.09992.
$p = 31,\ N_0 = 40982,\ N6 = 3854,\ \frac{N_6}{N_0} = 0.09404$, probabilité 0.09368.
$p = 37,\ N_0 = 49998,\ N6 = 3959,\ \frac{N_6}{N_0} = 0.07918$, probabilité 0.07890.

On reprend ensuite le même programme en faisant les statistiques du cas $\delta = 2$, ce qui peut se tester en recherchant les cas où les régulateurs $\Delta_p^1(\eta)$ et $\Delta_p^{\chi_1}(\eta)$ sont non nuls modulo p et la matrice des coefficients de rang 2 ($\Delta_p^\theta(\eta) \equiv 0 \pmod p$ pour $\theta = \chi_2$ et $\mathcal{L}^\theta$ de dimension 4) ; nombre de cas dans N_6.

On remplace la fin du programme par la séquence suivante :

$GG = [F1, F2, F3, F4, F5, F6];$
$DD = (F1 + F2 + F3)^2 - (F4 + F5 + F6)^2;$
$RP = E1^2 + E2^2 + E3^2 - E4^2 - E5^2 - E6^2 - E1 * E2 - E2 * E3 - E3 * E1$
$+ E4 * E5 + E5 * E6 + E6 * E4;$
$if(RP == 0 \& DD! = 0, N1 = N1 + 1;$
$M = matrix(6, 6, i, j, component(component(GG, i), j)); r = matrank(M);$
$if(r == 2, N6 = N6 + 1))));$
$print("p = ", p, "", N0, "", "N6 = ", N6, "", (N6 + 0.0)/N0, "", 1./p^4);$
$print("N1 = ", N1, "", (N1 + 0.0)/N0, "", 1./p)\}$

On obtient les résultats suivants pour $p = 13$:

$p = 13$; $N_0 = 499541$; $N_6 = 18$; $\frac{N_6}{N_0} = 3.60 \times 10^{-5}$; $\frac{1}{p^4} = 3.50 \times 10^{-5}$; $N_1 = 34925$; $\frac{N_1}{N_0} = 0.06991$; $\frac{1}{p} = 0.07692$.

4.5. Indépendance locale des composantes sur une base. — Il reste à vérifier le caractère de "variables aléatoires indépendantes" de $A_1, \ldots, A_n$; nous ne donnerons que deux exemples numériques ($G = C_3$ et $G = D_6$), avec des programmes PARI que le lecteur peut reprendre et expérimenter comme nous allons le préciser ci-après.

4.5.1. Cas cubique. — Soit K le corps cubique cyclique défini par le polynôme $x^3 - 11x^2 - 14x - 1$, de conducteur 163. On rappelle que les nombres premiers p considérés sont assez grands.

Il s'agit de vérifier que les variables A, B, C, qui définissent $\alpha \equiv Ax^2 + Bx + C \pmod p$ sont indépendantes.

Le programme ci-dessous considère des entiers aléatoires η modulo p^2, étrangers à p ; il est clair que, *algébriquement*, $\frac{-1}{p}\log_p(\eta)$ donne uniformément tous les α

possibles modulo p, mais même la restriction de la fonction *random* à un petit sous-domaine de $(\mathbb{Z}/p^2\mathbb{Z})^3$ donne des résultats analogues.

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 $\Delta_p^\chi(\eta) \equiv 0 \pmod p$. On peut prendre $p \geq 11$ distinct de 163.

On désigne par N_0 le nombre d'entiers η modulo p^2 étrangers à p considérés, par N_1 le nombre de cas où $\Delta_p^\chi(\eta) \equiv 0 \pmod p$ (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 $\frac{1}{p^2}$.

```
{t=11; Q=x^3-t*x^2-(t+3)*x-1; p=11; p2=p^2;
N0=0; N1=0; N2=0;
for(i=1,500000,
aa=random(p2); bb=random(p2); cc=random(p2);
e=Mod(aa*x^2+bb*x+cc,Q); N=norm(e); if(Mod(N,p)!=0, N0=N0+1;
a=Mod(aa,p2); b=Mod(bb,p2); c=Mod(cc,p2);
P=x^3-t*x^2-(t+3)*x-Mod(1,p); P2=x^3-t*x^2-(t+3)*x-Mod(1,p2);
y=Mod(a*x^2+b*x+c,P2); u=y^(p+1); v=u^p*y; z=v^(p-1)-1;
U=component(z,2);
u1=component(U,1); if(u1==0, u1=Mod(0,p2));
u2=component(U,2); if(u2==0, u2=Mod(0,p2));
u3=component(U,3); if(u3==0, u3=Mod(0,p2));
x1=component(u1,2)/p; x2=component(u2,2)/p; x3=component(u3,2)/p;
X1=Mod(x1,p); X2=Mod(x2,p); X3=Mod(x3,p);
if(X3==Mod(4,p)&X2==Mod(1,p), N2=N2+1);
SX1=X1-2*X2-X3*(t-2);
SX2=-X3*(t^2+t+1)-X2*(t+1);
SX3=X3*t+X2;
TX1=X3*(t^2+3*t+4)+X2*(t+2)+X1;
TX2=X3*(t^2+t+1)+X2*t;
TX3=-X3*(t+1)-X2;
F=Mod(X1+X2*x+X3*x^2,P);
SF=Mod(SX1+SX2*x+SX3*x^2,P);
TF=Mod(TX1+TX2*x+TX3*x^2,P);
RP=F^2+SF^2+TF^2-F*SF-SF*TF-TF*F;
rp=component(RP,2); if(rp==0, N1=N1+1)));
print(p,"",N0,"",N1,"",N2,"",(N1+0.0)/N0,"",(N2+0.0)/N0,"",1./p2)}
```

Les résultats sont inchangés quelles que soient les valeurs imposées numériquement aux couples de coefficients (on commence dans le tableau ci-dessous par deux cas de degré résiduel 2 dans $\mathbb{Q}(j)/\mathbb{Q}$ et ensuite par des cas totalement décomposés) :

p	N_0	N_1	N_2	$\frac{N_1}{N_0}$	$\frac{N_2}{N_0}$	$\frac{1}{p^2}$	
5	255562	10023	10155	0.039219	0.039736	0.04	
11	499624	4127	4191	0.00826	0.008388	0.00826	
p	N_0	N_1	N_2	$\frac{N_1}{N_0}$	$\frac{N_2}{N_0}$	$\frac{1}{p^2}$	$\frac{2}{p}$
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

Toutes 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 $p \equiv 2 \pmod 3$. Naturellement, si l'on impose seulement une valeur numérique (à A, B ou C) on obtient $\frac{N_2}{N_0} \sim \frac{1}{p}$ et $\frac{1}{p^3}$ si l'on impose les trois valeurs. On a donc bien une indépendance statistique des variables A, B, C.

4.5.2. Cas de D_6. — Une étude analogue utilise le programme PARI suivant, où nc indique le nombre de composantes imposées ($1 \le nc \le 6$) :

```
{Q=x^6+9*x^4-4*x^3+27*x^2+36*x+31;p=7;p2=p^2;N0=0;N1=0;
e1=x;
e2=11/180*x^5+1/180*x^4+11/18*x^3-1/45*x^2+403/180*x+419/180;
e3=13/180*x^5-7/180*x^4+13/18*x^3-38/45*x^2+509/180*x+127/180;
e4=-4/45*x^5+1/45*x^4-8/9*x^3+26/45*x^2-137/45*x-91/45;
e5=-1/60*x^5-1/60*x^4-1/6*x^3-4/15*x^2-73/60*x-79/60;
e6=-1/36*x^5+1/36*x^4-5/18*x^3+5/9*x^2-65/36*x+11/36;
for(i=1,500000,
a=random(p2);b=random(p2);c=random(p2);
aa=random(p2);bb=random(p2);cc=random(p2);
E=Mod(a*e1^5+b*e1^4+c*e1^3+aa*e1^2+bb*e1+cc,Q);
N=norm(E);if(Mod(11*N,p)!=0,N0=N0+1;
u=Mod(a,p2);v=Mod(b,p2);w=Mod(c,p2);
uu=Mod(aa,p2);vv=Mod(bb,p2);ww=Mod(cc,p2);
P=x^6+9*x^4-4*x^3+27*x^2+36*x+Mod(31,p);
P2=x^6+9*x^4-4*x^3+27*x^2+36*x+Mod(31,p2);
y=Mod(u*x^5+v*x^4+w*x^3+uu*x^2+vv*x+ww,P2);
z=y^(p-1);t=z;for(i=1,5,z=z^p*t);U=component(z-1,2);
u1=component(U,1);if(u1==0,u1=Mod(0,p2));
u2=component(U,2);if(u2==0,u2=Mod(0,p2));
u3=component(U,3);if(u3==0,u3=Mod(0,p2));
u4=component(U,4);if(u4==0,u4=Mod(0,p2));
u5=component(U,5);if(u5==0,u5=Mod(0,p2));
u6=component(U,6);if(u6==0,u6=Mod(0,p2));
x1=component(u1,2)/p;x2=component(u2,2)/p;x3=component(u3,2)/p;
x4=component(u4,2)/p;x5=component(u5,2)/p;x6=component(u6,2)/p;
X1=Mod(x1,p);X2=Mod(x2,p);X3=Mod(x3,p);
X4=Mod(x4,p);X5=Mod(x5,p);X6=Mod(x6,p);
nc=3;if(X1==Mod(4,p)&X2==Mod(4,p)&X5==Mod(1,p),N1=N1+1)));
print(p,"",N0,"",N1,"",(N1+0.0)/N0,"",1./p^nc)}
```

Pour $p = 17$, on obtient pour trois conditions sur les composantes de α, $N_0 = 494865$, $N_1 = 111$ et $\frac{N_1}{N_0} = 0.0002243$, pour $\frac{1}{p^3} = 0.0002035$. Toutes les expérimentations numériques ont donné les résultats attendus.

4.6. Extra p-divisibilités. — Examinons le cas des p-divisibilités supérieures "non automatiques", pour voir que leur probabilité est aussi au plus en $\frac{1}{p^2}$. Rappelons la décomposition du régulateur de η :

$$\begin{aligned}\mathrm{Reg}_p^G(\eta) &= \prod_\theta \mathrm{Reg}_p^\theta(\eta)^{\varphi(1)} \quad \text{et}\\ \mathrm{Reg}_p^\theta(\eta) &= \prod_{\varphi\,|\,\theta} \mathrm{Reg}_p^\varphi(\eta) = \mathrm{N}_\mathfrak{p}\big(P^\varphi\big(\ldots, \tfrac{-1}{p}\log_p(\eta), \ldots\big)\big)\end{aligned}$$

(cf. Remarques 2.18, 2.19). Lorsque l'on est dans le cas de p-divisibilité minimale, on a par définition (cf. Définition 3.17, §3.3) $\mathrm{Reg}_p^\theta(\eta) \sim p$ et $\mathrm{Reg}_p^G(\eta) \sim p^{\varphi(1)}$.

Si l'on suppose seulement que p est totalement décomposé dans $C_\chi/\mathbb{Q}$ ($f = 1$) et qu'il existe un unique 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 $\mathrm{Reg}_p^\theta(\eta) \sim p^e$, $e \ge 2$ (donc $\mathrm{Reg}_p^G(\eta) \sim p^{e\,\varphi(1)}$), dont on veut vérifier qu'elles sont de probabilité en $\frac{O(1)}{p^2}$ (en réalité $\frac{1}{p^2} + \frac{1}{p^3} + \cdots$). Le programme suivant (pour $G = D_6$, auquel cas tout p assez grand convient) vérifie ce fait pour le régulateur :

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

lorsque $\varphi = \theta = \chi_2$ est le caractère de degré 2, où les E_i, $1 \leq i \leq 6$, sont les conjugués d'un entier quelconque de K (en effet, on peut supposer que $\frac{-1}{p}\log_p(\eta)$ est représenté par un entier arbitraire E de K). La division par $\sqrt{-3}$ permet d'avoit un entier rationnel sans élever le régulateur au carré.

On peut changer à volonté le nombre premier $p \geq 5$ (ici $p = 101$), et la borne N.

```
{Q=x^6+9*x^4-4*x^3+27*x^2+36*x+31;p=101;p2=p^2;
N=10^6;N0=0;
e1=Mod(x,Q);
e2=Mod(11/180*x^5+1/180*x^4+11/18*x^3-1/45*x^2+403/180*x+419/180,Q);
e3=Mod(13/180*x^5-7/180*x^4+13/18*x^3-38/45*x^2+509/180*x+127/180,Q);
e4=Mod(-4/45*x^5+1/45*x^4-8/9*x^3+26/45*x^2-137/45*x-91/45,Q);
e5=Mod(-1/60*x^5-1/60*x^4-1/6*x^3-4/15*x^2-73/60*x-79/60,Q);
e6=Mod(-1/36*x^5+1/36*x^4-5/18*x^3+5/9*x^2-65/36*x+11/36,Q);
rm=(e1+e2+e3)/3;"(rm=sqrt(-3))";
for(i=1,N,
a=random(400)-200;b=random(400)-200;c=random(400)-200;
aa=random(400)-200;bb=random(400)-200;cc=random(400)-200;
E1=(a*e1^5+b*e1^4+c*e1^3+aa*e1^2+bb*e1+cc);
E2=(a*e2^5+b*e2^4+c*e2^3+aa*e2^2+bb*e2+cc);
E3=(a*e3^5+b*e3^4+c*e3^3+aa*e3^2+bb*e3+cc);
E4=(a*e4^5+b*e4^4+c*e4^3+aa*e4^2+bb*e4+cc);
E5=(a*e5^5+b*e5^4+c*e5^3+aa*e5^2+bb*e5+cc);
E6=(a*e6^5+b*e6^4+c*e6^3+aa*e6^2+bb*e6+cc);
Pphi=component((E1^2+E2^2+E3^2-E4^2-E5^2-E6^2-E1*E2-E2*E3-E3*E1
                                        +E4*E5+E5*E6+E6*E4)/rm,2);
Reg=component(Pphi,1);
if(Mod(Reg,p2)==0,N0=N0+1));print(N,"",(N0+0.0)/N,"",1.0/p2)}
```

Pour $p = 101$ et 10^6 essais via *random*, on obtient une densité de cas $e \geq 2$ égale à 0.000101 pour une probabilité théorique en 0.0000980.

Pour $p = 149$, on obtient 4.60×10^{-5} pour une probabilité en 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 de p-divisibilité minimale. On peut donc considérer que pour tout p assez grand il n'y a pas d'extra p-divisibilités pour $\mathrm{Reg}_p^G(\eta)$.

5. Considérations théoriques directes sur quelques cas particuliers

Cette Section 5 est redondante par rapport à l'étude générale des Sections 2 et 3, mais elle permet une approche élémentaire et une étude numérique approfondie.

5.1. Etude directe utilisant des corps cubiques cycliques. — Pour introduire le cas Abélien général (cf. §5.2), nous détaillons le cas de corps cubiques cycliques K définis par les polynômes irréductibles ("simplest cubic fields" de Shanks [**Sh**]) $P_t := X^3 - t\,X^2 - (t+3)\,X - 1$, $t \in \mathbb{Z}$, dont les racines (conjuguées d'une unité ε) sont : x, $x^\sigma = -1 - x^{-1}$, $x^{\sigma^2} = -(1+x)^{-1}$.

Le discriminant de P_t est $D_t = (t^2 + 3\,t + 9)^2$. En outre on utilisera $\{x^2, x, 1\}$ comme $\mathbb{Z}_{(p)}$-base de $Z_{K,(p)}$ et on prendra les nombres $\eta \in K^\times$ sous la forme $\eta = a\,x^2 + b\,x + c$, $a, b, c \in \mathbb{Z}_{(p)}$.

On peut vérifier facilement que sur cette base :

$$x^\sigma = x^2 - (t+1)\,x - 2 \quad \text{et} \quad x^{\sigma^2} = -x^2 + t\,x + t + 2.$$

Donc si $\eta = a\,x^2 + b\,x + c$, les conjugués de η sont donnés par :

$$\begin{aligned}
\eta^\sigma &= (at+b)\,x^2 - (a(t^2+t+1) + b(t+1))\,x - a(t-2) - 2b + c,\\
\eta^{\sigma^2} &= (-a(t+1) - b)\,x^2 + (a(t^2+t+1) + bt)\,x + a(t^2+3t+4) + b(t+2) + c.
\end{aligned}$$

Soit F le $\mathbb{Z}[G]$-module engendré par η. Le calcul de $\eta^{p^{n_p}-1} = 1 + p\,\alpha_p(\eta)$ conduit à $\alpha_p(\eta) \equiv A\,x^2 + B\,x + C \pmod p$, $A, B, C \in \mathbb{Z}_{(p)}$.

Nous allons supposer F de $\mathbb{Z}$-rang 3 et nous intéresser au caractère rationnel $\chi \neq 1$.

Posons $\alpha = \alpha_p(\eta)$, $\alpha' = \alpha^\sigma$, $\alpha'' = \alpha^{\sigma^2}$; on rappelle que pour $\chi \neq 1$, le χ-régulateur local est :

$$\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = \alpha^2 + \alpha'^2 + \alpha''^2 - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha.$$

5.1.1. Exemples numériques. — Donnons d'abord des exemples numériques (au moyen du programme PARI écrit au §5.1.4) :

(i) Cas p inerte dans $\mathbb{Q}(j)$. Pour $t = 41$, on a $P_t = X^3 - 41\,X^2 - 44\,X - 1$, et son discriminant est $D = 1813 = 7^2.37$.

Prenons $\eta = 3\,x^2 - 2\,x + 6$ dont la norme est $353731 = 7^2.7219$.

On trouve, pour $\Delta_p^\chi(\eta) \equiv 0 \pmod p$, la solution $p = 5$, inerte dans $\mathbb{Q}(j)$. Les données numériques sont $\alpha \equiv \alpha' \equiv \alpha'' \equiv 3 \pmod p$ (provenant de la relation $\eta^{5^3-1} \equiv 1 + 5\,.\,3 \pmod{25}$). L'ensemble des conjugés de α est astreint à vérifier deux relations (conjuguées par σ) indépendantes modulo p :

$$\begin{aligned} \alpha' - \alpha &\equiv 0 \pmod p, \\ \alpha'' - \alpha' &\equiv 0 \pmod p, \end{aligned}$$

selon le principe définissant une probabilité en $\frac{O(1)}{p^2}$.

(ii) Cas p décomposé dans $\mathbb{Q}(j)$. Pour $t = 17$, le discriminant est $D = 349$. Prenons encore $\eta = 3\,x^2 - 2\,x + 6$ dont la norme est 66739. On obtient une unique solution $p < 10^9$, à $\Delta_p^\chi(\eta) \equiv 0 \pmod p$, qui est $p = 1309963$ (totalement décomposé dans $\mathbb{Q}(j)$). Les données numériques sont :

$$\begin{aligned} \alpha &\equiv 627681 + 294668\,x + 143675\,x^2 \pmod p, \\ \alpha' &\equiv 503146 + 366345\,x + 117217\,x^2 \pmod p, \\ \alpha'' &\equiv 632127 + 648950\,x + 1049071\,x^2 \pmod p. \end{aligned}$$

On vérifie que les 3 mineurs :

$$\begin{vmatrix} 294668 & 143675 \\ 366345 & 117217 \end{vmatrix}, \qquad \begin{vmatrix} 648950 & 1049071 \\ 294668 & 143675 \end{vmatrix}, \qquad \begin{vmatrix} 366345 & 117217 \\ 648950 & 1049071 \end{vmatrix},$$

sont nuls modulo p et que le rang du système est égal à 2 (une relation non triviale). Pour $r = 160549$, d'ordre 3 modulo p, et $\theta \,|\, \chi$ défini par $\theta(\sigma) = j \equiv r \pmod{\mathfrak{p}}$, on obtient l'unique relation :

$$\alpha + r^{-1}\alpha' + r^{-2}\alpha'' \equiv 0 \pmod p$$

donnant la nullité modulo p de $\Delta_p^\theta(\eta) = \mathrm{N}_{\mathfrak{p}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'')$.

5.1.2. Analyse théorique des exemples précédents. — La nullité de $\Delta_p^\chi(\eta)$ modulo p s'écrit :

$$\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}\big(\alpha - \alpha'' - j(\alpha'' - \alpha')\big) \equiv 0 \pmod p.$$

Posons $\alpha \equiv A\,x^2 + B\,x + C \pmod p$. Toute relation entre α, α', α'' (modulo p) peut se traduire exclusivement sur les coefficients A, B, C : en effet, par conjugaison de $\alpha = A\,x^2 + B\,x + C$, on obtient (en posant $x' = x^\sigma$ et $x'' = x^{\sigma^2}$) :

$$\alpha' = A\,x'^2 + B\,x' + C =: A'\,x^2 + B'\,x + C',$$

$$\alpha'' = A\,x''^2 + B\,x'' + C =: A''\,x^2 + B''\,x + C'',$$

ce qui conduit au résultat via les formules explicites $x' = x^2 - (t+1)\,x - 2$ et $x'' = -x^2 + tx + t + 2$, qui donnent A', B', C', A'', B'', C'' par des transformations linéaires indépendantes de p, à savoir :

$$\begin{array}{lll} A' = At+B, & B' = -A(t^2+t+1)-B(t+1), & C' = -A(t-2)-2B+C \\ A'' = -A(t+1)-B, & B'' = A(t^2+t+1)+Bt, & C'' = A(t^2+3t+4)+B(t+2)+C. \end{array}$$

On en déduit que l'ensemble des relations modulo p entre A, B, C conduit à la probabilité cherchée (cf. §§4.3.1, 4.3.2).
Considérons le schéma suivant et supposons $\Delta_p^{\chi}(\eta) \equiv 0 \pmod p$:

$$\begin{tikzcd} \alpha, \alpha', \alpha'' \in K \arrow[r, dash, "\langle s \rangle"] \arrow[d, dash] & K(j) \ \mathfrak{P} \arrow[d, dash, "\langle \sigma \rangle"] \\ \mathbb{Q} \arrow[r, dash] & \mathbb{Q}(j) \ \mathfrak{p} \end{tikzcd}$$

Puisque $\Delta_p^{\chi}(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha - \alpha - j(\alpha' - \alpha'')) \equiv 0$ $\pmod p$, nécessairement $\alpha - \alpha' - j(\alpha' - \alpha'') \equiv 0 \pmod{\mathfrak{P}}$ dans $K(j)$, pour au moins un idéal premier $\mathfrak{P}$ au-dessus de p dans $K(j)$. Soit $\mathfrak{p}$ l'idéal premier de $\mathbb{Q}(j)$ au-dessous de $\mathfrak{P}$.

On obtient, par conjugaison par σ (cf. Corollaire 2.7, §2.2.3) :

$$\alpha' - \alpha'' - j(\alpha'' - \alpha) \equiv j\,(\alpha - \alpha' - j(\alpha' - \alpha'')) \equiv 0 \pmod{\mathfrak{P}^{\sigma}},$$

et de même avec $\mathfrak{P}^{\sigma^2}$; par conséquent $\alpha - \alpha' - j(\alpha' - \alpha'')$ appartient à tous les idéaux premiers au-dessus de $\mathfrak{p}$ dans $K(j)$, d'où $\alpha - \alpha' - j(\alpha' - \alpha'') \equiv 0 \pmod{\mathfrak{p}}$ (étendu à $K(j)$). Distinguons selon la décomposition de p dans $\mathbb{Q}(j)/\mathbb{Q}$.

(i) Cas p inerte dans $\mathbb{Q}(j)/\mathbb{Q}$. L'unique idéal $\mathfrak{p}$ est l'étendu de (p) dans $\mathbb{Q}(j)$. Nécessairement $\alpha - \alpha' - j(\alpha' - \alpha'') \equiv 0 \pmod p$ dans $K(j)$; comme $\{1, j\}$ est une K-base de $K(j)$ et que $\alpha - \alpha' - j(\alpha' - \alpha'') \in Z_K$, il vient $\alpha \equiv \alpha' \equiv \alpha''$ $\pmod p$ (en un sens, α est rationnel modulo p), ce qui conduit à :

$$A \equiv 0 \pmod p, \quad B \equiv 0 \pmod p$$

(cas de l'exemple (i) du §5.1.1). D'où une probabilité en $\dfrac{O(1)}{p^2}$. Le coefficient C n'est lié par aucune condition.

(ii) Cas p décomposé dans $\mathbb{Q}(j)/\mathbb{Q}$. Soient $\mathfrak{p}$ et $\mathfrak{p}^s$ les deux idéaux premiers de $\mathbb{Q}(j)$ au-dessus de p. D'après ce qui précède, on a $\alpha - \alpha' - j(\alpha' - \alpha'') \equiv 0$ $\pmod{\mathfrak{p}}$ (étendu à $K(j)$). Soit r un rationnel tel que $j \equiv r \pmod{\mathfrak{p}}$; alors $\alpha - \alpha' - j(\alpha' - \alpha'') \equiv \alpha - \alpha' - r(\alpha' - \alpha'') \equiv 0 \pmod{\mathfrak{p}}$ (étendu à $K(j)$), et comme $\alpha - \alpha' - r(\alpha' - \alpha'') \in K$, cette congruence est vraie par conjugaison par s, d'où $\alpha - \alpha' - r(\alpha' - \alpha'') \equiv 0 \pmod p$. Ceci conduit dans K à :

$$\Delta_p^{\theta}(\eta) = \mathrm{N}_{\mathfrak{p}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') \equiv \alpha + r^{-1}\alpha' + r^{-2}\alpha'' \equiv 0 \pmod{\mathfrak{p}}.$$

On en déduit (une seule relation et deux choix pour r) une probabilité en $\dfrac{2}{p}$.
Comme dans le cas inerte, on peut voir comment ces relations se transmettent à A, B, C ; il vient, puisque $r^{-1} \equiv r^2 \pmod p$:

$$\begin{aligned} A + r^2 A' + r A'' &\equiv 0 \pmod p, \\ B + r^2 B' + r B'' &\equiv 0 \pmod p, \\ C + r^2 C' + r C'' &\equiv 0 \pmod p. \end{aligned}$$

En utilisant les relations précédentes :

$$A' = At+B,\qquad B' = -A(t^2+t+1)-B(t+1),\ C' = -A(t-2)-2B+C$$
$$A'' = -A(t+1)-B, B'' = A(t^2+t+1)+Bt,\qquad C'' = A(t^2+3t+4)+B(t+2)+C,$$

on obtient le système suivant :

$$\begin{aligned} A(t(2r^2+1)+r^2+2)+B(2r^2+1) &\equiv 0 \pmod p\\ A(r-r^2)(t^2+t+1)+B(rt-r^2(t+1)+1) &\equiv 0 \pmod p\\ A(r(t^2+3t+4)-r^2(t-2))+B((t+2)-2r^2) &\equiv 0 \pmod p. \end{aligned}$$

Ce système en A et B (C ne figure pas) est de rang 1 et est alors équivalent à la seule relation $B \equiv -(t+\frac{r-1}{2+1})\,A \equiv (r-t)\,A \pmod p$. En résumé on obtient $B-(r^2-t)\,A \equiv 0 \pmod p$. Ceci est illustré par l'exemple numérique (ii) du §5.1.1. On a obtenu une relation entre A et B fonction de r (probabilité en $\frac{2}{p}$).

5.1.3. Cas où F est de $\mathbb{Z}$-rang 2. — Lorsque η est un éléments non trivial de norme ± 1, le $\mathbb{Z}$-rang de F est égal à 2 et on a la nullité triviale modulo p de $\Delta_p^1(\eta) = \alpha+\alpha'+\alpha''$ (provenant de $\mathrm{N}_{K/\mathbb{Q}}(\eta) = \pm 1$). Cette relation peut être utilisée pour simplifier les calculs, mais elle ne doit induire aucune modification de la probabilité de nullité modulo p de $\Delta_p^\chi(\eta)$ pour $\chi \neq 1$. Le programme donné ci-dessous permet de s'assurer de ce fait.

On est donc conduit au χ-déterminant plus simple :

$$\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha+j^{-1}\alpha'+j^{-2}\alpha'') = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha(1-j)-\alpha'(j-j^2)),$$

qui, au facteur 3 près, s'écrit $\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha - j\,\alpha')$.

Donnons un seul exemple dans le cas inerte, particulièrement rare : pour $t = 33$ ($D = 1197 = 9.7.19$) et $p = 17$ on trouve que α et ses conjugués sont nuls modulo p (en effet les relations $\alpha \equiv \alpha' \equiv \alpha'' \pmod p$ du cas inerte (i) vu pour le $\mathbb{Z}$-rang 3 deviennent ici $\alpha \equiv 0 \pmod p$ puisque $\alpha+\alpha'+\alpha'' \equiv 0 \pmod p$)).

5.1.4. Programme PARI général. — Ce programme, valable pour les $\mathbb{Z}$-rangs 2 et 3, peut s'utiliser en modifiant les valeurs de t, aa, bb, cc ; il recherche les solutions $p < 10^8$ et donne les conjugués de α :

```
{t=13;Q=x^3-t*x^2-(t+3)*x-1;D=t^2+3*t+9;
aa=0;bb=1;cc=0;e=Mod(aa*x^2+bb*x+cc,Q);N=norm(e);
print("t=",t," ","Discriminant=",D," ",aa," ",bb," ",cc," ",N);
for(k=2,5*10^7,p=2*k+1;if(isprime(p)==1&Mod(D*N,p)!=0,p2=p^2;
a=Mod(aa,p2);b=Mod(bb,p2);c=Mod(cc,p2);
P=x^3-t*x^2-(t+3)*x-Mod(1,p);P2=x^3-t*x^2-(t+3)*x-Mod(1,p2);
y=Mod(a*x^2+b*x+c,P2);u=y^(p+1);v=u^p*y;z=v^(p-1)-1;
U=component(z,2);
u1=component(U,1);if(u1==0,u1=Mod(0,p2));
u2=component(U,2);if(u2==0,u2=Mod(0,p2));
u3=component(U,3);if(u3==0,u3=Mod(0,p2));
x1=component(u1,2)/p;x2=component(u2,2)/p;x3=component(u3,2)/p;
X1=Mod(x1,p);X2=Mod(x2,p);X3=Mod(x3,p);
SX1=X1-2*X2-X3*(t-2);
SX2=-X3*(t^2+t+1)-X2*(t+1);
SX3=X3*t+X2;
TX1=X3*(t^2+3*t+4)+X2*(t+2)+X1;
TX2=X3*(t^2+t+1)+X2*t;
TX3=-X3*(t+1)-X2;
F=Mod(X1+X2*x+X3*x^2,P);
SF=Mod(SX1+SX2*x+SX3*x^2,P);
TF=Mod(TX1+TX2*x+TX3*x^2,P);
RP=F^2+SF^2+TF^2-F*SF-SF*TF-TF*F;rp=component(RP,2);
```

$if(rp == 0, print("p = ", p, "", "pmod3 = ", component(Mod(p, 3), 2));$
$print("coefficients\, de\, alpha,\ alpha',\ alpha''\ :\ X1 + X2 * x + X3 * x^2 : ");$
$print("coefficients\, de\, alpha",\ X1, "\ \ ", X2, "\ \ ", X3);$
$print("coefficients\, de\, s.alpha", SX1, "\ \ ", SX2, "\ \ ", SX3);$
$print("coefficients\, de\, t.alpha", TX1, "\ \ ", TX2, "\ \ ", TX3)))))\}$

5.2. Etude directe du cas Abélien général. — On peut toujours se ramener au cas où G est cyclique d'ordre $n > 2$ (voir § 2.3.2 pour les cas $n \leq 2$).

5.2.1. Résultat général. — Soit χ le caractère rationnel de G d'ordre n ; soit ζ une racine primitive n-ième de l'unité. On a $C_\chi = \mathbb{Q}(\zeta)$ et le χ-régulateur local :

$$\Delta_p^\chi(\eta) = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\Big(\sum_{\nu\in G}\varphi(\nu)\alpha^{\nu^{-1}}\Big),$$

pour $\varphi \,|\, \chi$ fixé. La condition $\Delta_p^\chi(\eta) \equiv 0 \pmod p$ implique par des raisonnements connus (cf. Corollaire 2.7, §2.2.3) :

$$\sum_{\nu\in G}\varphi(\nu)\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}} \ \ \text{(idéal premier de } \mathbb{Q}(\zeta) \text{ étendu à } K(\zeta)\text{)}.$$

Soient L le corps de décomposition de p dans $\mathbb{Q}(\zeta)/\mathbb{Q}$ et $D = \mathrm{Gal}(\mathbb{Q}(\zeta)/L)$; on désigne par f le degré résiduel en p. Alors $\{\zeta, \ldots, \zeta^f\}$ est une L-base de $\mathbb{Q}(\zeta)$ (et une KL-base de $K(\zeta)$). Posons $\varphi(\nu) = \sum_{i=1}^f a_i(\nu)\,\zeta^i$, $a_i(\nu) \in Z_{L,(p)}$ pour tout $\nu \in G$. Il vient $\sum_{\nu\in G}\varphi(\nu)\,\alpha^{\nu^{-1}} = \sum_{i=1}^f \zeta^i \sum_{\nu\in G} a_i(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$.
Comme il y a inertie dans $K(\zeta)/KL$, il en résulte $\sum_{\nu\in G} a_i(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, pour $i = 1, \ldots, f$, en voyant ici $\mathfrak{p}$ dans L et étendu à KL.
Il existe alors des p-entiers rationnels $r_i(\nu)$ tels que $a_i(\nu) \equiv r_i(\nu) \pmod{\mathfrak{p}}$ dans L, ce qui conduit à $\sum_{\nu\in G} r_i(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod{\mathfrak{p}}$, $i = 1, \ldots, f$; d'où finalement $\sum_{\nu\in G} r_i(\nu)\,\alpha^{\nu^{-1}} \equiv 0 \pmod p$, $\ i = 1, \ldots, f$.
La matrice $\big(r_i(\nu)\big)_{\nu\in G,\, 1\leq i\leq f}$ est de $\mathbb{F}_p$-rang f ; en effet, soit $H = \{\nu_1, \ldots, \nu_f\}$ un sous-ensemble de G tel que $\varphi(\nu_j) = \zeta^j$, $j = 1, \ldots, f$; alors la sous-matrice $\big(a_i(\nu_j)\big)_{i,j}$ et donc la sous-matrice $\big(r_i(\nu_j)\big)_{i,j}$, est la matrice unité I_f d'ordre f.

Il en résulte un système de f relations indépendantes définissant $\mathcal{L}^\theta$ pour un caractère p-adique $\theta \,|\, \chi$ (cf. Définitions 2.5 (ii), §2.2.3 et 3.3 (ii), §3.2.1) :

$$\sum_{\nu\in G} r_i(\nu)\alpha^{\nu^{-1}} \equiv 0 \pmod p, \quad i = 1, \ldots, f,$$

correspondant à une probabilité en $\frac{O(1)}{p^f}$. Chacun des $h = [L : \mathbb{Q}]$ régulateurs $\Delta_p^\theta(\eta) = \mathrm{N}_\mathfrak{p}(\sum_{\nu\in G}\varphi(\nu)\,\alpha^{\nu^{-1}})$ (cf. Remarque 2.19 (i)) a une probabilité de nullité modulo p en $\frac{O(1)}{p^f}$. On peut donc se limiter au ca $f = 1$ qui conduit à la probabilité la plus grande (en $\frac{O(1)}{p}$ car $f = \delta = 1$).

5.2.2. Exemple du sous-corps réel maximal de $\mathbb{Q}(\mu_{11})$. — Les programmes PARI suivants traitent le cas du sous-corps réel maximal K de $\mathbb{Q}(\mu_{11})$.

a) Recherche des solutions p telles que $\Delta_p^\chi(\eta) \equiv 0 \pmod p$. On peut changer à volonté les coefficients aa, bb, cc, dd, ee sur la base $\{x^4, x^3, x^2, x, 1\}$ des puissances de $x = \zeta_{11} + \zeta_{11}^{-1}$. Attention, la liste des conjugués de x :

$s1 = x, s2 = x^2-2, s3 = x^4-4*x^2+2, s4 = x^3-3*x, s5 = -x^4-x^3+3*x^2+2*x-1,$

qui correspond à l'ordre naturel 1, σ, σ^2, σ^3, σ^4, est donnée dans le désordre par la procédure *nfgaloisconj* de PARI.

$\{Q = x^5 + x^4 - 4 * x^3 - 3 * x^2 + 3 * x + 1;$
$s1 = x; s2 = x^2 - 2; s3 = x^4 - 4 * x^2 + 2; s4 = x^3 - 3 * x; s5 = -x^4 - x^3 + 3 * x^2 + 2 * x - 1;$

```
aa=2;bb=1;cc=2;dd=0;ee=-3;Eta=Mod(aa*x^4+bb*x^3+cc*x^2+dd*x+ee,Q);
N=norm(Eta);print("norme(eta)=",N);print("");
for(k=1,5*10^6,p=2*k+1;if(isprime(p)==1&Mod(11*N,p)!=0,p2=p^2;
a=Mod(aa,p2);b=Mod(bb,p2);c=Mod(cc,p2);d=Mod(dd,p2);e=Mod(ee,p2);
P=x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p);P2=x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p2);
y=Mod(a*x^4+b*x^3+c*x^2+d*x+e,P2);
u=y^(p+1);v=u^p*y;w=v^p*y;s=w^p*y;t=s^(p-1)-1;
U=component(t,2);
u1=component(U,1);if(u1==0,u1=Mod(0,p2));
u2=component(U,2);if(u2==0,u2=Mod(0,p2));
u3=component(U,3);if(u3==0,u3=Mod(0,p2));
u4=component(U,4);if(u4==0,u4=Mod(0,p2));
u5=component(U,5);if(u5==0,u5=Mod(0,p2));
x1=component(u1,2)/p;x2=component(u2,2)/p;x3=component(u3,2)/p;
                              x4=component(u4,2)/p;x5=component(u5,2)/p;
X1=Mod(x1,p);X2=Mod(x2,p);X3=Mod(x3,p);X4=Mod(x4,p);X5=Mod(x5,p);
e1=Mod(X5*s1^4+X4*s1^3+X3*s1^2+X2*s1+X1,P);
e2=Mod(X5*s2^4+X4*s2^3+X3*s2^2+X2*s2+X1,P);
e3=Mod(X5*s3^4+X4*s3^3+X3*s3^2+X2*s3+X1,P);
e4=Mod(X5*s4^4+X4*s4^3+X3*s4^2+X2*s4+X1,P);
e5=Mod(X5*s5^4+X4*s5^3+X3*s5^2+X2*s5+X1,P);
A=e5*e4+e4*e3+e3*e2+e2*e1+e1*e5;
B=e5*e3+e4*e2+e3*e1+e2*e5+e1*e4;
C=e5^2+e4^2+e3^2+e2^2+e1^2;
RP=C*(C-A-B)-(A+B)^2+5*A*B;rp=component(RP,2);if(rp==0,print(p);
print(component(e1,2));print(component(e2,2));print(component(e3,2));
print(component(e4,2));print(component(e5,2));g=Mod(p,5);print("g=",g))))}
```

(i) Pour $aa=-2; bb=1; cc=0; dd=0; ee=-3$, on a $\mathrm{N}_{K/\mathbb{Q}}(\eta)=-60589$, et les solutions pour $p<10^7$ sont $p=31, 101, 39451$, tous décomposés dans $\mathbb{Q}(\zeta_5)$. Considérons les données numériques pour $p=31$:

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

Pour $r=4$, qui est tel que $\theta(\sigma)\equiv r \pmod p$, 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 $\{x^4, x^3, x^2, x, 1\}$.

(ii) Pour $aa=10; bb=-7; cc=0; dd=1; ee=-2$, on a $\mathrm{N}_{K/\mathbb{Q}}(\eta)=303623$, et 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 en $\dfrac{O(1)}{p^4}$.

(iii) Pour $aa=10; bb=-7; cc=-3; dd=1; ee=-2$, on a $\mathrm{N}_{K/\mathbb{Q}}(\eta)=1358171$, et on trouve la solution $p=79$ (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 $\Delta_p^{\varphi}(\eta)$ pour $\varphi(\sigma)=\zeta_5^{-1}$) 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 $\zeta_5^3=-\zeta_5\frac{\sqrt{5}-1}{2}+\frac{1-\sqrt{5}}{2}$, $\zeta_5^4=-\zeta_5+\frac{\sqrt{5}-1}{2}$ et le système de relations dans $K(\zeta_5)$ exprimant $\Delta_p^{\varphi}(\eta) \equiv 0 \pmod{\mathfrak{p}}$:

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

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 $r_i(\nu)$, $i = 1, 2$ et le couple $(\theta, \mathfrak{p})$. On a donc obtenu deux relations linéaires à coefficients rationnels indépendantes :

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

Les données numériques pour α et ses conjugués sont respectivement :

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

qui vérifient le système de deux congruences ci-dessus.
On a les deux relations indépendantes, définissant $\mathcal{L}^{\theta} \simeq V_{\theta}$ de $\mathbb{F}_p$-dimension 2, $1 - \sigma^2 + 49\,(\sigma^4 - \sigma^3)$ & $\sigma^4 - \sigma + 49\,(\sigma^3 - \sigma^2)$, la seconde étant conjuguée par σ^4 de la première. D'où une probabilité en $\frac{2}{p^2}$ (deux choix pour la congruence $\sqrt{5} \equiv 20 \pmod{\mathfrak{p}}$).

b) Calcul de la densité des $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$. Le programme ci-dessous reprend le cas précédent du sous-corps réel maximal de $\mathbb{Q}(\mu_{11})$ et s'intéresse aux différents degrés résiduels possibles pour vérifier que la probabilité pour $\Delta_p^{\theta}(\eta) \equiv 0 \pmod{p}$ est bien en $\frac{O(1)}{p^f}$.
On affiche les probabilités théoriques selon le cas ($f = 1, 2, 4$).

```
{Q=x^5+x^4-4*x^3-3*x^2+3*x+1;p=19;p2=p^2;N0=0;N1=0;
s1=x;s2=x^2-2;s3=x^4-4*x^2+2;s4=x^3-3*x;s5=-x^4-x^3+3*x^2+2*x-1;
for(i=1,5*10^5,
aa=random(p2);bb=random(p2);cc=random(p2);dd=random(p2);ee=random(p2);
Eta=Mod(aa*x^4+bb*x^3+cc*x^2+dd*x+ee,Q);
N=norm(Eta);if(Mod(N,p)!=0,N0=N0+1;
a=Mod(aa,p2);b=Mod(bb,p2);c=Mod(cc,p2);d=Mod(dd,p2);e=Mod(ee,p2);
P=x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p);P2=x^5+x^4-4*x^3-3*x^2+3*x+Mod(1,p2);
y=Mod(a*x^4+b*x^3+c*x^2+d*x+e,P2);
u=y^(p+1);v=u^p*y;w=v^p*y;s=w^p*y;t=s^(p-1)-1;
U=component(t,2);
u1=component(U,1);if(u1==0,u1=Mod(0,p2));
u2=component(U,2);if(u2==0,u2=Mod(0,p2));
u3=component(U,3);if(u3==0,u3=Mod(0,p2));
u4=component(U,4);if(u4==0,u4=Mod(0,p2));
u5=component(U,5);if(u5==0,u5=Mod(0,p2));
x1=component(u1,2)/p;x2=component(u2,2)/p;x3=component(u3,2)/p;
                                  x4=component(u4,2)/p;x5=component(u5,2)/p;
X1=Mod(x1,p);X2=Mod(x2,p);X3=Mod(x3,p);X4=Mod(x4,p);X5=Mod(x5,p);
e1=Mod(X5*s1^4+X4*s1^3+X3*s1^2+X2*s1+X1,P);
e2=Mod(X5*s2^4+X4*s2^3+X3*s2^2+X2*s2+X1,P);
e3=Mod(X5*s3^4+X4*s3^3+X3*s3^2+X2*s3+X1,P);
e4=Mod(X5*s4^4+X4*s4^3+X3*s4^2+X2*s4+X1,P);
e5=Mod(X5*s5^4+X4*s5^3+X3*s5^2+X2*s5+X1,P);
```

```
A = e5 * e4 + e4 * e3 + e3 * e2 + e2 * e1 + e1 * e5;
B = e5 * e3 + e4 * e2 + e3 * e1 + e2 * e5 + e1 * e4;
C = e5^2 + e4^2 + e3^2 + e2^2 + e1^2;
RP = C*(C-A-B)-(A+B)^2+5*A*B; rp = component(RP,2); if(rp == 0, N1 = N1+1)));
print(p,"", N0,"", N1,"", (N1 + 0.0)/N0);
print("4/p - 6/p^2 + 4/p^3 - 1/p^4 = ", 4./p - 6./p^2 + 4./p^3 - 1./p^4);
print("2/p^2 - 1/p^4 = ", 2./p^2 - 1./p^4);
print("1/p^4 = ", 1./p^4)}
```

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 $\frac{1}{p^4} = 3.50 \times 10^{-5}$.

5.3. Etude directe du 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 pose $\alpha = \alpha_p(\eta)$.

5.3.1. 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 pose $\alpha' = \alpha^\sigma$, $\alpha'' = \alpha^{\sigma^2}$, $\beta = \alpha^\tau$, $\beta' = \alpha^{\tau\sigma} = \alpha'^\tau$, $\beta'' = \alpha^{\tau\sigma^2} = \alpha''^\tau$.

(i) 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 p-quotient de Fermat de a.

(ii) Cas $\Delta_p^{\chi_1}(\eta)$; on a $\mathrm{N}_{K/k}(\eta) \in k^\times \setminus \mathbb{Q}^\times$ 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 en $\frac{O(1)}{p}$, la trace modulo p dans K/k étant surjective.

(iii) 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 $\varphi = \theta = \chi_2$, à la condition (cf. Exemple 2.9, §2.2.4) :

$$\begin{aligned} \Delta_p^\theta(\eta) &= \alpha^2 + \alpha'^2 + \alpha''^2 - \beta^2 - \beta'^2 - \beta''^2 \\ &\qquad - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha + \beta\beta' + \beta'\beta'' + \beta''\beta \equiv 0 \pmod p. \end{aligned}$$

Le calcul des trois représentations $\mathcal{L}^{\theta'} \simeq \delta' V_{\theta'}$, $0 \leq \delta' \leq \varphi'(1)$, 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 (sinon, la nullité supplémentaire de $\Delta_p^\theta(\eta)$ conduit à une probabilité au plus en $\frac{O(1)}{p^2}$, et on peut exclure ce nombre premier).

Commençons par des exemples numériques (θ désigne le caractère p-adique χ_2).

5.3.2. Programme PARI pour D_6 et le calcul de $\mathcal{L}^\theta$ et $\Delta_p^\theta(\eta)$. — Ce programme 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 (attention, on doit calculer le noyau de la transposée de la matrice des coefficients sur la base $\{x^5, x^4, x^3, x^2, x, 1\}$). Le résultat de "matker(MM)" donne les vecteurs $(c_1, c_2, c_3, c_4, c_5, c_6)$ tels que :

$$c_1\alpha + c_2\alpha^\sigma + c_3\alpha^{\sigma^2} + c_4\alpha^\tau + c_5\alpha^{\tau\sigma} + c_6\alpha^{\tau\sigma^2} \equiv 0 \pmod p.$$

```
{Q = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + 31; D = poldisc(Q);
e1 = x;
e2 = 11/180*x^5 + 1/180*x^4 + 11/18*x^3 - 1/45*x^2 + 403/180*x + 419/180;
e3 = 13/180*x^5 - 7/180*x^4 + 13/18*x^3 - 38/45*x^2 + 509/180*x + 127/180;
e4 = -4/45*x^5 + 1/45*x^4 - 8/9*x^3 + 26/45*x^2 - 137/45*x - 91/45;
e5 = -1/60*x^5 - 1/60*x^4 - 1/6*x^3 - 4/15*x^2 - 73/60*x - 79/60;
e6 = -1/36*x^5 + 1/36*x^4 - 5/18*x^3 + 5/9*x^2 - 65/36*x + 11/36;
a = 1; b = -3; c = 0; aa = -7; bb = 1; cc = -1;
Eta = Mod(a*e1^5 + b*e1^4 + c*e1^3 + aa*e1^2 + bb*e1 + cc, Q);
N = norm(Eta); print("norme(eta) = ", N); print("");
for(k = 3, 5*10^6, p = 2*k + 1; if(isprime(p) == 1&Mod(D*N, p)! = 0, p2 = p^2;
u = Mod(a, p2); v = Mod(b, p2); w = Mod(c, p2);
uu = Mod(aa, p2); vv = Mod(bb, p2); ww = Mod(cc, p2);
P = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + Mod(31, p);
P2 = x^6 + 9*x^4 - 4*x^3 + 27*x^2 + 36*x + Mod(31, p2);
y = Mod(u*x^5 + v*x^4 + w*x^3 + uu*x^2 + vv*x + ww, P2);
z = y^(p-1); t = z; for(i = 1, 5, z = z^p*t);
U = component(z - 1, 2);
u1 = component(U, 1); if(u1 == 0, u1 = Mod(0, p2));
u2 = component(U, 2); if(u2 == 0, u2 = Mod(0, p2));
u3 = component(U, 3); if(u3 == 0, u3 = Mod(0, p2));
u4 = component(U, 4); if(u4 == 0, u4 = Mod(0, p2));
u5 = component(U, 5); if(u5 == 0, u5 = Mod(0, p2));
u6 = component(U, 6); if(u6 == 0, u6 = Mod(0, p2));
x1 = component(u1, 2)/p; x2 = component(u2, 2)/p; x3 = component(u3, 2)/p;
x4 = component(u4, 2)/p; x5 = component(u5, 2)/p; x6 = component(u6, 2)/p;
X1 = Mod(x1, p); X2 = Mod(x2, p); X3 = Mod(x3, p);
X4 = Mod(x4, p); X5 = Mod(x5, p); X6 = Mod(x6, p);
E1 = Mod(X1 + X2*e1 + X3*e1^2 + X4*e1^3 + X5*e1^4 + X6*e1^5, P);
E2 = Mod(X1 + X2*e2 + X3*e2^2 + X4*e2^3 + X5*e2^4 + X6*e2^5, P);
E3 = Mod(X1 + X2*e3 + X3*e3^2 + X4*e3^3 + X5*e3^4 + X6*e3^5, P);
E4 = Mod(X1 + X2*e4 + X3*e4^2 + X4*e4^3 + X5*e4^4 + X6*e4^5, P);
E5 = Mod(X1 + X2*e5 + X3*e5^2 + X4*e5^3 + X5*e5^4 + X6*e5^5, P);
E6 = Mod(X1 + X2*e6 + X3*e6^2 + X4*e6^3 + X5*e6^4 + X6*e6^5, P);
RP = E1^2 + E2^2 + E3^2 - E4^2 - E5^2 - E6^2 - E1*E2 - E2*E3 - E3*E1
                                              +E4*E5 + E5*E6 + E6*E4;
rp = component(RP, 2); if(rp == 0, print(p));
F1 = component(E1, 2); F2 = component(E2, 2); F3 = component(E3, 2);
F4 = component(E4, 2); F5 = component(E5, 2); F6 = component(E6, 2);
print(F1); print(F2); print(F3); print(F4); print(F5); print(F6);
GG = [F1, F2, F3, F4, F5, F6];
M = matrix(6, 6, i, j, component(component(GG, i), j)); print(M);
MM = mattranspose(M); K = matker(MM); print(matker(MM)))))}
```

5.3.3. Cas $\eta = x^5 - 3x^4 - 7x^2 + x - 1$. — On a $\mathrm{N}(\eta) = 12393229477$ et on trouve les solutions $p = 7, 13, 69677, 387161$, pour $p < 10^7$.

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

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

qui conduisent immédiatement aux deux $\mathbb{F}_p$-relations linéaires indépendantes :

$\alpha - \alpha^{\sigma} + \alpha^{\tau} - \alpha^{\tau\sigma^2} \equiv 0 \pmod p$ & $\alpha - \alpha^{\sigma^2} + \alpha^{\tau} - \alpha^{\tau\sigma} \equiv 0 \pmod p$, et leur relèvements $\eta_1^{1-\sigma+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}$, $\eta_1^{1-\sigma^2+\tau-\tau\sigma} \equiv 1 \pmod{p^2}$.

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 ($\mathcal{L}^\theta \simeq V_\theta$).

b) Pour $p = 13$, on a les données numériques suivantes :

$$\begin{array}{lllllllll}
\alpha & \equiv & 9x^5 & + 0x^4 & + 1x^3 & + 2x^2 & + 10x & + 0 & \pmod p \\
\alpha^\sigma & \equiv & 3x^5 & + 8x^4 & + 4x^3 & + 7x^2 & + 9x & + 6 & \pmod p \\
\alpha^{\sigma^2} & \equiv & 11x^5 & + 9x^4 & + 4x^3 & + 4x^2 & + 7x & + 0 & \pmod p \\
\alpha^\tau & \equiv & 0x^5 & + 2x^4 & + 11x^3 & + 4x^2 & + 7x & + 0 & \pmod p \\
\alpha^{\tau\sigma} & \equiv & 5x^5 & + 1x^4 & + 11x^3 & + 7x^2 & + 9x & + 6 & \pmod p \\
\alpha^{\tau\sigma^2} & \equiv & 11x^5 & + 6x^4 & + 8x^3 & + 2x^2 & + 10x & + 0 & \pmod p,
\end{array}$$

qui conduisent ici à :

$\alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma^2} \equiv 0 \pmod p$ & $\alpha^{\sigma^2} - \alpha^\sigma + \alpha^{\tau\sigma} - \alpha^\tau \equiv 0 \pmod p$ et leur relèvements $\eta_1^{1-\sigma^2+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}$, $\eta_1^{\sigma^2-\sigma+\tau\sigma-\tau} \equiv 1 \pmod{p^2}$.

Pour la θ-relation $U = 1 - \sigma^2 + \tau - \tau\sigma^2$, on a $\sigma^2 U = -U - \sigma U$, $\tau U = U$, $\tau\sigma U = \sigma^2 U$, $\tau\sigma^2 = \sigma U$ ($\mathcal{L}^\theta \simeq V_\theta$).

c) Dans le cas de $p = 69677$, on trouve (modulo p) :

$$\begin{array}{llllllll}
\alpha & \equiv & 59144x^5 & + 25387x^4 & + 5395x^3 & + 69261x^2 & + 5560x & + 65182 \\
\alpha^\sigma & \equiv & 33305x^5 & + 7449x^4 & + 67108x^3 & + 3673x^2 & + 9338x & + 28342 \\
\alpha^{\sigma^2} & \equiv & 18122x^5 & + 61456x^4 & + 57729x^3 & + 9640x^2 & + 34177x & + 61498 \\
\alpha^\tau & \equiv & 1290x^5 & + 27633x^4 & + 41529x^3 & + 16366x^2 & + 3270x & + 35656 \\
\alpha^{\tau\sigma} & \equiv & 47848x^5 & + 11928x^4 & + 47652x^3 & + 55209x^2 & + 6965x & + 8976 \\
\alpha^{\tau\sigma^2} & \equiv & 49322x^5 & + 5501x^4 & + 59295x^3 & + 54882x^2 & + 10367x & + 61315\,,
\end{array}$$

et les combinaisons $(c_1, c_2, c_3, c_4, c_5, c_6)$:

$$(53404, 39540, 46410, 69676, 1, 0) \ \ \& \ \ (23267, 16273, 30137, 69676, 0, 1).$$

5.3.4. Cas $p = 7$, $\eta = x^5 - x^4 - 7x^2 + x - 1$. — 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 :

$$\begin{array}{lllllll}
\alpha & \equiv & 6x^5 & & + 4x^3 & + 5x^2 & + \quad 3 \\
\alpha^\sigma & \equiv & 4x^5 & + 4x^4 & + 1x^3 & + 3x^2 & + 5x + 1 \\
\alpha^{\sigma^2} & \equiv & 4x^5 & + 3x^4 & + 2x^3 & + 6x^2 & + 2x + 3 \\
\alpha^\tau & \equiv & 6x^5 & + & 4x^3 & + 5x^2 & + \quad 3 \\
\alpha^{\tau\sigma} & \equiv & 4x^5 & + 3x^4 & + 2x^3 & + 6x^2 & + 2x + 3 \\
\alpha^{\tau\sigma^2} & \equiv & 4x^5 & + 4x^4 & + 1x^3 & + 3x^2 & + 5x + 1\,.
\end{array}$$

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 $\sigma^2 U = -U - \sigma U$, $\tau U = -U$, $\tau\sigma U = -\sigma^2 U$, $\tau\sigma^2 U = -\sigma U$ ($\mathcal{L}^\theta \simeq V_\theta$).

5.3.5. Cas $p = 61$, $\eta = x^5 - 2x^4 + 4x^3 - 3x^2 + x - 1$. — On obtient :

$$\begin{array}{llllllll}
\alpha & \equiv & 8x^5 & + 32x^4 & + 26x^3 & + 31x^2 & + 55x & + 18 \\
\alpha^\sigma & \equiv & 15x^5 & + 44x^4 & + 11x^3 & + 21x^2 & + 34x & + 25 \\
\alpha^{\sigma^2} & \equiv & 38x^5 & + 46x^4 & + 24x^3 & + 9x^2 & + 33x & + 44 \\
\alpha^\tau & \equiv & 5x^5 & + 58x^4 & + 43x^3 & + 17x^2 & + 47x & + 16 \\
\alpha^{\tau\sigma} & \equiv & 31x^5 & + 7x^4 & + 22x^3 & + 55x^2 & + 36x & + 56 \\
\alpha^{\tau\sigma^2} & \equiv & 25x^5 & + 57x^4 & + 57x^3 & + 50x^2 & + 39x & + 15\,.
\end{array}$$

D'où trois relations $\mathbb{F}_p$-linéaires indépendantes, conjuguées (par σ et σ^2) de la relation $19\alpha + 56\alpha^\sigma + 46\alpha^{\sigma^2} + \alpha^\tau \equiv 0 \pmod p$; la somme des trois relations donne $\alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} \equiv 0 \pmod p$ (nullité de $\Delta_p^{\chi_1}(\eta)$).

Pour $\theta = \chi_2$ de degré 2, le θ-régulateur $\Delta_p^\theta(\eta)$ est nul modulo p (voir Exemple 3.16, §3.3 pour les détails numériques et de fait la nullité triviale de $\Delta_p^\theta(\eta)$ car dans cet exemple on a par hasard $\eta^{1+\sigma+\sigma^2-\tau-\tau\sigma-\tau\sigma^2} = 1$).

5.3.6. Cas $p = 7$, $\eta = 3x^5 - 20x^4 + 15x^3 + 16x^2 + 9x + 21$. — 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 ($\mathcal{L}^\theta \simeq 2\,V_\theta \simeq e_\theta\,\mathbb{F}_p[G]$) est très rare, comme on l'a vu au §4.4.3 (probabilité en $\frac{O(1)}{p^4}$), car on doit prendre η de telle sorte que F soit de $\mathbb{Z}$-rang 6 et qu'aucun des $\Delta_p^\chi(\eta)$, $\chi = 1, \chi_1$, ne soit nul modulo p, ce qui est le cas ici.

Il est facile de voir que cela correspond au cas où η est proche (modulo p^2) d'un élément non trivial du sous-corps quadratique de K.

Il se trouve que $p = 13$ est aussi solution et donne les conjugués suivants :

$$\begin{array}{lcllllll}
\alpha & \equiv & 2x^5 & + 3x^4 & + 7x^3 & + 8x^2 & + 3x & + 12 \\
\alpha^\sigma & \equiv & 2x^5 & + 5x^4 & + x^3 & + 3x^2 & + 8x & + 4 \\
\alpha^{\sigma^2} & \equiv & 7x^5 & + 12x^4 & + 11x^3 & + 2x^2 & + 2x & + 10 \\
\alpha^\tau & \equiv & 12x^5 & + 7x^4 & + 3x^3 & + 8x^2 & + 3x & + 12 \\
\alpha^{\tau\sigma} & \equiv & 4x^5 & + 3x^4 & + 7x^3 & + 2x^2 & + 2x & + 10 \\
\alpha^{\tau\sigma^2} & \equiv & 12x^5 & + 9x^4 & + 10x^3 & + 3x^2 & + 8x & + 4\ ,
\end{array}$$

d'où les trois $\mathbb{F}_p$-relations linéaires indépendantes :

$$4\alpha+5\alpha^\sigma+5\alpha^{\sigma^2}+\alpha^\tau \equiv 5\alpha+5\alpha^\sigma+4\alpha^{\sigma^2}+\alpha^{\tau\sigma} \equiv 5\alpha+4\alpha^\sigma+5\alpha^{\sigma^2}+\alpha^{\tau\sigma^2} \equiv 0 \pmod p,$$

donnant la nullité modulo 13 de $\Delta_p^1(\eta)$ et $\Delta_p^\theta(\eta)$ (relation associée définissant $\mathcal{L}^\theta$, $U = 1 - \sigma^2 - \tau + \tau\sigma$), et non celle de $\Delta_p^{\chi_1}(\eta)$; F est bien de $\mathbb{Z}$-rang 6.

Remarque 5.1. — Les éléments $U_1 = 1 - \sigma^2 + \tau - \tau\sigma$, $U_2 = 1 - \sigma - \tau + \tau\sigma$ de $e_\theta\,\mathbb{F}_p[G]$ (cf. Remarque 2.15, §2.2.6) forment une base, et permettent d'exprimer toutes les θ-relations trouvées par combinaisons $\mathbb{F}_p[G]$-linéaires (des coefficients de la forme $a + b\sigma$ étant suffisants en raison des relations de conjugaison de U_1, U_2) ; ceci s'applique à tous les exemples numériques précédents.

Le $\mathbb{F}_p$-espace obtenu est de dimension $\delta\varphi(1)$, $1 \leq \delta \leq 2$, et la probabilité associée est en $\frac{O(1)}{p^{\delta^2}}$ puisqu'ici $f = 1$ (cf. §4.3.2).

6. Interprétation locale concernant η

L'idée est de voir dans quelle mesure η est "en partie" une puissance p-ième locale en p lorsque $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ pour un caractère p-adique θ, tout particulièrement dans le cas $f = \delta = 1$ et pour une p-divisibilité minimale $p^{\varphi(1)}$, d'après la Définition 3.17, §3.3. Commençons par un cas particulier bien connu :

6.1. Cas d'un caractère de degré 1, d'ordre $n \,|\, p-1$. — Reprenons le résultat du Corollaire 3.13, §3.2.3 avec $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$, où $U_\theta = \sum_{k=0}^{n-1} r^k\, s^{-k}$, r d'ordre n modulo p, s générateur de G. Ici $\Delta_p^\theta(\eta) = \mathrm{N}_\mathfrak{p}\big(\sum_{k=0}^{n-1} \varphi(s^k)\, \alpha^{s^{-k}}\big) \equiv \sum_{k=0}^{n-1} r^k\, \alpha^{s^{-k}} \pmod{\mathfrak{p}}$. L'écriture $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$ conduit à $\eta^{U_\theta(r-s)} = \lambda^{p(r-s)}$, $\lambda \in \prod_{v\,|\,p} K_v^\times$; comme dans $\mathbb{Z}_{(p)}[G]$ on a $U_\theta\,(r-s) = c\,p$, $c \in \mathbb{Z}_{(p)}^\times$ [10], il vient $\eta = \Lambda^{r-s}$, $\Lambda \in \prod_{v\,|\,p} K_v^\times$ (pas de p-torsion dans $\prod_{v\,|\,p} K_v^\times$ pour p assez grand).

[10] On peut toujours choisir r modulo p de telle sorte que $r^n - 1 \not\equiv 0 \pmod{p^2}$.

Le caractère $\varphi \,|\, \theta$ est tel que $\varphi(s) = \xi$, racine primitive n-ième de l'unité dans $\mathbb{C}$, et il définit $\mathfrak{p} = (p, r-\xi)$ associé à θ ; on considère la φ-composante $(K^\times \otimes C_\chi)^{e_\varphi}$; alors $\xi = \varphi(s)$ opère par $y^\xi = y^s$, pour tout $y \in (K^\times \otimes C_\chi)^{e_\varphi}$. On peut alors (en vue des aspects conjecturaux de la Section 7) dire par abus de langage que $\eta = \Lambda^{r-\xi}$ est une "puissance $\mathfrak{p}$-ième" dans $\prod_{v \,|\, p} K_v^\times$.
Dans le cas χ d'ordre 1 ou 2, voir les §7.2.1, §7.2.2 qui reprennent cet aspect.

6.2. Cas d'un caractère de degré quelconque. — Soit G un groupe fini et soit θ l'un de ses caractères p-adiques irréductibles tel que $\Delta_p^\theta(\eta) \equiv 0 \pmod p$ (i.e., $\mathcal{L}^\theta \neq \{0\}$). Le relèvement $\eta_1^{U_\theta} \equiv 1 \pmod {p^2}$ a lieu avec une θ-relation non triviale $U_\theta := \sum\limits_{\nu \in G} u(\nu)\, \nu^{-1} \in \mathcal{L}^\theta$. On a $\eta_1^{U_\theta} = (1 + p\,\gamma)^p \in \prod\limits_{v \,|\, p} K_v^{\times p}$, et la relation $\eta = \eta^{p^{n_p}} \eta_1^{-1}$ conduit aussi à $\eta^{U_\theta} \in \prod\limits_{v \,|\, p} K_v^{\times p}$, mais l'interprétation de η comme "puissance $\mathfrak{p}$-ième" dans $\prod\limits_{v \,|\, p} K_v^\times$ n'est plus possible lorsque $\varphi \,|\, \theta$ est de degré ≥ 2.
Dans la section suivante on considèrera cette écriture comme une propriété de "puissance p-ième locale partielle en p", selon la définition suivante qui fait le lien avec le Lemme 2.14 sur les questions de nullités triviales :

Définition 6.1. — Soit $\eta \in K^\times$. On suppose que le $\mathbb{Z}[G]$-module F engendré par η est de $\mathbb{Z}$-rang $n = |G|$. Soit p un nombre premier fixé assez grand et soit :

$$F_0 := \Big\{ \eta_0 \in F,\ \eta_0 \in \prod_{v \,|\, p} K_v^{\times p} \Big\}.$$

On dira que η est puissance p-ième locale partielle en p si $\dim_{\mathbb{F}_p}(F/F_0) < n$.

Cette définition est équivalente à l'existence d'un caractère p-adique irréductible θ tel que $\dim_{\mathbb{F}_p}(F/F_0)^{e_\theta} < f\,\varphi(1)^2$, donc de la forme $t f\,\varphi(1)$, $0 \leq t \leq \varphi(1) - 1$, où f est le degré résiduel de θ (cf. Définition 2.5 (ii), §2.2.3).

Remarque 6.2. — Comme par hypothèse F est de $\mathbb{Z}$-rang n et sans p-torsion (pour p assez grand), on a $F/F^p \simeq \mathbb{F}_p[G]$ (en particulier, $\dim_{\mathbb{F}_p}(F/F^p)^{e_\theta} = f\,\varphi(1)^2$ pour tout θ).

(i) Il en résulte que la condition $\dim_{\mathbb{F}_p}(F/F_0) < n$ indique qu'il existe θ tel que la composante $(F/F_0)^{e_\theta}$ n'est pas maximale, donc qu'il existe $U_\theta \in e_\theta \mathbb{Z}_{(p)}[G]$ non triviale telle que η^{U_θ} est puissance p-ième locale en p, non puissance p-ième globale dans $K^\times$ (car $F \cap K^{\times p} = F^p$) ; ceci équivaut à $\dim_{\mathbb{F}_p}(\mathcal{L}^\theta) = \delta f\,\varphi(1)$, $\delta \geq 1$.

(ii) De fait on a $F/F_0 \simeq \mathbb{F}_p[G]/\mathcal{L}$, d'où $(F/F_0)^{e_\theta} \simeq e_\theta \mathbb{F}_p[G]/\mathcal{L}^\theta$, ce qui donne la relation $t = \varphi(1) - \delta$. Dire que $\eta \in \prod_{v \,|\, p} K_v^{\times p}$, c'est dire que $F_0 = F$, donc que $\mathcal{L} = \mathbb{F}_p[G]$ de probabilité $\frac{O(1)}{p^n}$, cas qui peut être écarté pour $n > 1$.

Remarque 6.3. — En résumé, l'obstruction fondamentale pour l'éventuelle finitude de l'ensemble des p tels que $\Delta_p^G(\eta) = \prod_\theta \Delta_p^\theta(\eta)^{\varphi(1)} \equiv 0 \pmod p$ provient des cas de p-divisibilité minimale $p^{\varphi(1)}$, à savoir (cf. Définition 3.17, §3.3) :

(i) il existe un unique caractère p-adique irréductible θ tel que $\Delta_p^\theta(\eta) \equiv 0 \pmod p$,

(ii) p est totalement décomposé dans le corps des valeurs C_χ du caractère irréductible $\varphi \,|\, \theta$ (i.e., $f = 1$) et $\mathrm{Reg}_p^G(\eta) \sim p^{\varphi(1)}$ (cf. Remarque 2.18, § 2.3.1),

(iii) la représentation $\mathcal{L}^\theta \simeq \delta V_\theta$ des θ-relations (cf. Définition 3.3 (iii), §3.2.1) est irréductible, ce qui est équivalent à $\dim_{\mathbb{F}_p}(\mathcal{L}^\theta) = \varphi(1)$ (i.e., $\delta = 1$, cf. Théorème 3.11, §3.2.3).

7. Conjectures et spéculations p-adiques

7.1. Généralités. — Nous proposons diverses conjectures en partant de la plus “évidente” (Conjecture 7.2, §7.2.1) en relation avec la conjecture ABC, pour aller vers des généralisations aux corps de nombres (Conjectures 7.4, §7.2.3 et 7.7, §7.3). L'obstruction essentielle étant donnée par les cas de probabilités en $\frac{O(1)}{p}$ pour les cas de p-divisibilité minimale $p^{\varphi(1)}$ de $\mathrm{Reg}_p^G(\eta)$ (cf. Définition 3.17, §3.3, et Remarque ci-dessus), nous proposons §7.5 une approche pouvant modifier ce point de vue (étude limitée au cas du quotient de Fermat).

Dans le cadre de la théorie probabiliste des nombres (cf. §4.1), il convient de préciser des questions de densités au niveau des hypothèses des énoncés. En théorie algébrique des nombres on parle par exemple de *“presque tout nombre premier p”* pour signifier *“pour tout nombre premier p sauf pour un ensemble Σ fini”*. Or on peut remplacer cette propriété par la suivante, plus faible :

pour tout nombre premier p sauf pour un ensemble Σ de premiers p tels que :

$$\big|\{p \in \Sigma,\ p \leq x\}\big| = o\Big(\frac{x}{\log(x)}\Big),$$

qui permet un ensemble infini d'exceptions de densité nulle (cf. **[T]**, Chap. III.3.1). On peut également envisager l'hypothèse plus faible “*pour un ensemble infini de p*” (non nécessairement de densité 1). Les énoncés de la Section 7 sont donnés sous la forme forte (algébrique), mais on pourra considérer les formes faibles pour le choix de Σ (infini de densité nulle), ou le point de vue “*pour une infinité de p*”.

7.2. Retour sur le cas des caractères d'ordre 1 ou 2. — Nous revenons sur des cas particuliers déjà évoqués (cf. §2.3.2).

7.2.1. Cas d'un rationnel. — On considère $K = \mathbb{Q}$ et un rationnel $a \in \mathbb{Q}^\times$, $a \neq \pm 1$. Si p est un nombre premier impair étranger à a, on a le résultat élémentaire suivant qui est un cas particulier du Corollaire 3.13, §3.2.3 (pour $\theta = 1$ et $U_\theta = 1$) :

Lemme 7.1. — *Le p-quotient de Fermat de a est nul modulo p si et seulement si $a \in \mathbb{Q}_p^{\times p}$.*

Démonstration. — Si $a^{p-1} = 1 + p^2\, b$, b p-entier, alors $a = a^p(1 + p^2\, b)^{-1} \in \mathbb{Q}_p^{\times p}$ (car $p \neq 2$). Si $a = u^p$, $u \in \mathbb{Q}_p^\times$, $a^{p-1} = (u^{p-1})^p \equiv 1 \pmod{p^2}$. □

Une question cruciale, pour $a \neq \pm 1$, est l'existence ou non d'une infinité de nombres premiers p tels que $a^{p-1} \equiv 1 \pmod{p^2}$.

On sait, d'après un résultat de Silverman **[Si]**, que sous la conjecture ABC l'ensemble des nombres premiers p tels que $a^{p-1} \not\equiv 1 \pmod{p^2}$ est infini.[11] 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 qui devient un théorème si l'on admet la conjecture ABC (cf. §7.1 pour les différentes acceptions de *“pour presque tout p”* à partir de *“pour tout p sauf un nombre fini”*) :

Conjecture 7.2. — *Soit $a \in \mathbb{Q}^\times$; si $a \in \mathbb{Q}_p^{\times p}$ pour presque tout p alors $a = \pm 1$.*

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

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 rappelé Proposition 7.5, §7.2.3). On pourra le qualifier de *principe local–global diophantien.*

Ces principes algébriques restent valables lorsqu'on remplace "presque tout p" par un ensemble de p infini (ou fini) convenable restreint, mais non effectif en général. Citons par exemple une forme très simple du théorème de Schmidt–Chevalley (un cas de principe de Hasse) qui s'énonce pour tous les corps de nombres et qui est à la base des propriétés idéliques du corps de classes (cf. **[Gr1]**, III.4.3) :

Proposition 7.3. — *Soit A un sous-$\mathbb{Z}$-module de type fini de $\mathbb{Q}^\times$. Soit e un entier fixé ; alors il existe une infinité d'ensembles finis T, de nombres premiers étrangers à A, qui ont la propriété suivante :*

$$\{x \in A,\ \ x \equiv 1 \pmod p),\ \forall p \in T\} \subseteq \mathbb{Q}^{\times e}.$$

On peut imaginer qu'un principe local–global diophantien existe dans le cas des p-quotients de Fermat de $a \in \mathbb{Q}^\times$, auquel cas on peut conjecturer que si l'on dispose d'un ensemble infini (même de densité nulle) de nombres premiers p tels que $a^{p-1} \equiv 1 \pmod{p^2}$, ceci est suffisant pour assurer que a est égal à ± 1.

7.2.2. Cas de l'unité d'un corps quadratique $K = \mathbb{Q}(\sqrt{m})$. — Si $\eta = x+y\sqrt{m}$ est non rationnel de norme a, on a $\eta^{p^2-1} = 1+p\,\alpha$, $\alpha = u+v\sqrt{m}$, d'où $\Delta_p^\chi(\eta) \equiv 2v\sqrt{m} \pmod p$ pour $\chi \neq 1$. On a $\Delta_p^\chi(\eta) \equiv 0 \pmod p$ si et seulement si $v \equiv 0 \pmod p$.

Supposons $m > 0$ et que η est une unité ε non triviale de $\mathbb{Q}(\sqrt{m})$ (nullité triviale modulo p de $\Delta_p^1(\varepsilon)$) ; on a $u \equiv 0 \pmod p$ et encore $\Delta_p^\chi(\varepsilon) \equiv 2v\sqrt{m} \pmod p$; la nullité modulo p de $\Delta_p^\chi(\varepsilon)$ implique $\alpha \equiv 0 \pmod p$, et ε est puissance p-ième locale. Au plan conjectural, on est ramené à la situation précédente d'un rationnel. Autrement dit, il suffirait que l'on démontre (via une forme adéquate de la conjecture ABC) que la relation $\varepsilon^{p^2-1} \not\equiv 1 \pmod{p^2}$ a lieu pour une infinité de p, pour pouvoir énoncer l'analogue pour ε de la Conjecture ci-dessus.
On peut envisager que ce processus est valable pour le cas général où $\eta \in K^\times$ serait "puissance p-ième locale partielle en p" (cf. Définition 6.1, §6.2) pour une infinité de p.

Ceci suppose d'abord la résolution du cas des puissances p-ièmes locales en p au sens commun, condition évidemment plus forte que celle de puissance p-ième locale partielle en p ; c'est l'objet du point suivant.

7.2.3. Conjecture générale sur les puissances p-ièmes locales. — Le cas rationnel (Conjecture 7.2, §7.2.1) a montré la vraissemblance du type d'énoncé suivant qui correspond à l'écriture $\eta^{p^{n_p}-1} - 1 = p\,\alpha$ dans le cas (statistiquement très exceptionnel) où $\alpha \equiv 0 \pmod p$ qui correspond à la condition $\mathcal{L} = \mathbb{F}_p[G]$ ($\delta = \varphi(1)$ pour tout caractère p-adique θ de G) et une probabilité en $\prod_\theta \frac{O(1)}{p^{f\varphi(1)^2}} = \frac{O(1)}{p^n}$, $n = |G|$, puisque $\sum_\theta f\,\varphi(1)^2 = \sum_\varphi \varphi(1)^2 = n$ (cf. Remarque 6.2, §6.2 et §4.3.2).

Ceci pourrait être une généralisation du théorème de Silverman (cas rationnel), qui utiliserait ici la conjecture ABC pour les corps de nombres, mais la conjecture peut être posée indépendamment (se reporter aussi au §7.1 pour les différentes acceptions de l'hypothèse *"pour presque tout nombre premier p"*) :

Conjecture 7.4. — *Soit K un corps de nombres et soit $\eta \in K^\times$. Si pour presque tout nombre premier p on a $\eta \in \prod_{v\,|\,p} K_v^{\times p}$, alors η est une racine de l'unité de K.*

Cet énoncé est à comparer au “principe de Hasse” pour les puissances, beaucoup plus fort, et qui est le suivant (cf. [**Gr1**], II.6.3.3). Soit $\mathcal{P}\ell_K$ (resp. $\mathcal{P}\ell_p$) l'ensemble des places de K (resp. des p-places de K) :

Proposition 7.5. — *Soit $\eta \in K^\times$. Soit p un nombre premier fixé et soit Σ un ensemble fini de places de K. Si η est puissance p-ième locale pour toute place $v \in \mathcal{P}\ell_K \setminus \Sigma$, 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 $\eta \in K^{\times p}$.(12)

La différence opère en deux temps pour la Conjecture 7.4 ci-dessus : partant de p et de l'ensemble $\mathcal{P}\ell_p$, on commence par dire que η est puissance p-ième locale pour tout $v \in \mathcal{P}\ell_p$ (i.e., on prend l'ensemble infini $\Sigma = \mathcal{P}\ell_K \setminus \mathcal{P}\ell_p$, ce qui n'entraîne pas $\eta \in K^{\times p}$ comme on le vérifie facilement ; ou encore on peut dire qu'on essaye de prendre $T = \mathcal{P}\ell_p$), mais ensuite dans la Conjecture 7.4 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, donc une racine de l'unité.

La conjecture “ultime” qui fait le lien avec la théorie des $\Delta_p^\theta(\eta)$ est la Conjecture 7.8 de la section suivante, §7.3.

Auparavant, examinons le cas général des unités qui conforte l'analyse précédente.

7.2.4. Cas particulier du groupe des unités – Spiegelungssatz. — Le cas où η est une unité d'un corps de nombres K quelconque met en jeu l'énoncé spécifique suivant (cf. [**Gr1**], II.6.3.8) :

Proposition 7.6. — *Soit η une unité de K. Soit p un nombre premier fixé et soit S 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.*
Si $\eta \in K_v^{\times p}$ pour toute place $v \in S \cup \mathcal{P}\ell_p$, alors $\eta \in K^{\times p}$.

Par exemple, pour $p = 3$, $\eta = 1 + \sqrt{2}$ (unité fondamentale), on a $\eta^8 \equiv 1 + 3\sqrt{2}$ (mod 9), et comme le 3-groupe de classes de $\mathbb{Q}(\sqrt{-6})$ (donc celui de K') est trivial ($S = \emptyset$), η^m est localement un cube en 3 si et seulement si $3 \,|\, m$. Autrement dit, le 3-quotient de Fermat de η ne pouvait pas être nul modulo 3.

La Conjecture 7.4, §7.2.3 porte seulement sur $\mathcal{P}\ell_p$ au lieu de $S \cup \mathcal{P}\ell_p$ pour S 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 si le p-groupe des classes du corps K' est trivial ($S = \emptyset$), mais on peut être plus précis à ce sujet.

Faisons quelques rappels classiques (voir par exemple [**Gr1**], I.6.3.1 et II.1.6.3) en supposant pour fixer les idées que η est une unité de Minkowski du corps

(12)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 (cf. §7.1).

totalement réel K ; on peut toujours faire en sorte que η soit non puissance ℓ-ième globale pour tout premier ℓ. Comme d'habitude les premiers p considérés sont assez grands et en particulier non ramifiés dans $K/\mathbb{Q}$.

S'il existe une θ-relation $U_\theta \not\equiv 0 \pmod{p\mathbb{Z}_{(p)}[G]}$ pour laquelle $\eta^{U_\theta} \in \prod_{v\,|\,p} K_v^{\times p}$ (cf. §6.2) alors l'extension $K'(\sqrt[p]{\eta^{U_\theta}})/K'$ est non ramifiée et p-décomposée ce qui conduit, par la théorie du corps de classes, à une information sur le p-groupe des classes $\mathcal{C}\ell_{K'}$ de la façon suivante : soit $\mathcal{C}\ell_{K'}^{\mathcal{P}\ell'_p}$ le quotient de $\mathcal{C}\ell_{K'}$ par le p-sous-groupe des classes des idéaux premiers $\mathfrak{P}'\,|\,p$ 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 $\mathcal{C}\ell_{K'}^{\mathcal{P}\ell'_p}$ qui est non triviale.

Revenons à l'écriture $\eta_1 := \eta^{p^{n_p}-1} = 1 + p\,\alpha$, $\alpha \in Z_K$, et considérons l'extension $K'(\sqrt[p]{\eta}) = K'(\sqrt[p]{\eta_1})$ de K', qui est p-ramifiée (i.e., non ramifiée en dehors de p) ; pour chaque $\mathfrak{P}'\,|\,p$ dans K' le $\mathfrak{P}'$-conducteur est $\mathfrak{P}'^{p+1-r}$ où r est le plus grand entier tel que la congruence $\eta_1 \equiv x'^p \pmod{\mathfrak{P}'^r}$, $x' \in K'^\times$, ait une solution x'. Comme p est totalement ramifié dans K'/K (indice de ramification $p-1$ pour p assez grand), (p) s'écrit $\prod_{\mathfrak{P}'\,|\,p} \mathfrak{P}'^{p-1}$ dans K'.

Soit $\mathfrak{P}\,|\,p$ dans K. Si $\alpha \in \mathfrak{P}$, alors $\alpha \in \mathfrak{P}'^{p-1}$ dans K' et on vérifie facilement que, localement, η_1 est puissance p-ième en $\mathfrak{P}'$ (non ramification de $K'(\sqrt[p]{\eta})/K'$ en $\mathfrak{P}'$ et $\mathfrak{P}'$-décomposition). Si $\alpha \notin \mathfrak{P}$, on vérifie que la congruence $1 + p\,\alpha \equiv x'^p \pmod{\mathfrak{P}'^r}$ implique nécessairement $r = p-1$, d'où un $\mathfrak{P}'$-conducteur égal à $\mathfrak{P}'^2$ (ramification).

Appliquant ceci à η^{U_θ}, il en résulte que toute θ-relation non triviale sur les conjugués de α, c'est-à-dire toute nullité modulo p d'un θ-régulateur $\Delta_p^\theta(\eta)$ $(\theta \neq 1)$, est équivalente à l'existence d'une θ^*-extension non ramifiée p-décomposée de K', de degré une puissance non triviale 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 peut paraître excessive.

En dehors du cas des unités on a une situation un peu différente : prenons pour $K = \mathbb{Q}$ l'exemple de $a \in \mathbb{Q}^\times$, $a \neq \pm 1$. Alors la Proposition 7.6, §7.2.4 n'est plus valable car elle ne s'applique que si l'idéal (a) est puissance p-ième d'idéal dans K, 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 remplacer le p-corps de classes de Hilbert H' de $\mathbb{Q}'$ par sa généralisation $H'^{T'}$ comme p-extension Abélienne maximale non ramifiée en dehors des places de l'ensemble T' des idéaux premiers de $\mathbb{Q}'$ au-dessus de T (T ne dépend pas de p).

Cette p-extension $H'^{T'}/\mathbb{Q}'$ est finie (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'. Bien que l'aspect conjectural paraisse ici différent, l'infinitude des p donnant un p-quotient de Fermat nul modulo p, peut se voir dans ce cadre.

7.3. Conjectures sur les θ-régulateurs locaux $\Delta_p^\theta(\eta)$. — Les résultats de la Section 3 (Théorème 3.11 et Corollaire 3.13, §3.2.3 généralisant en un sens le Lemme 7.1, §7.2.1) invitent à proposer les conjectures suivantes plus fortes que celles du §7.2, même si aucun cas particulier de preuve ne semble connu.

Pour éviter le cas des χ-régulateurs trivialement nuls (cf. Remarques 2.13, 2.15 et Lemme 2.14, §2.2.6), on suppose le G-module engendré par η de $\mathbb{Z}$-rang n.

La première conjecture se justifie en raison de l'écriture de type "quotient de Fermat" : $\eta^{p^{n_p}-1}-1 = p\,\alpha$, lorsque α satisfait à des relations de la forme $U_\theta\,.\,\alpha \equiv 0 \pmod p$ avec $U_\theta \not\equiv 0 \pmod{p\mathbb{Z}_p[G]}$ (i.e., $\mathcal{L}^\theta \simeq \delta V_\theta$, $\delta \geq 1$), pour au moins un θ, condition beaucoup plus faible que $U = 1$ qui correspond au "$\alpha \equiv 0 \pmod p$" à la base de la Conjecture 7.4, §7.2.3, c'est-à-dire à $\mathcal{L} \simeq \mathbb{F}_p[G]$ de probabilité $\frac{O(1)}{p^n}$).

Conjecture 7.7. — *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. Alors pour tout p assez grand, η n'est pas une puissance p-ième locale partielle en p (cf. Définition 6.1, §6.2).*

L'énoncé suivant est équivalent au précédent. On rappelle (cf. Définition 2.17, Remarque 2.18, §2.3.1) que pour tout caractère p-adique θ, $\mathrm{Reg}_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod p$ et que $\mathrm{Reg}_p^G(\eta) = p^{-n}\det\big(\log_p(\eta^{\tau\sigma})\big)_{\sigma,\tau\in G}$ (le régulateur p-adique normalisé de η, cf. Définition 2.3 (i), §2.1) se factorise en $\mathrm{Reg}_p^G(\eta) = \prod_\theta \mathrm{Reg}_p^\theta(\eta)^{\varphi(1)}$.

Conjecture 7.8. — *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 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 premier p assez grand $\mathrm{Reg}_p^G(\eta)$ est une unité p-adique.

Remarque 7.9. — (i) Les Conjectures 7.7, 7.8, peuvent s'énoncer sous une hypothèse plus faible qui consiste à remplacer "*presque tout p*" au sens algébrique par "*presque tout p*" au sens du §7.1.

(ii) La Conjecture 7.8 implique celle de Leopoldt–Jaulent [**J**], au moins pour presque tout p, mais il est préférable d'admettre cette dernière et de dire que la Conjecture 7.8 en est une version plus forte (voir la Remarque 2.4, (a) et (b)).

(iii) La version très raisonnable des conjectures précédentes est que les p assez grands tels que η est puissance p-ième locale partielle en p, sont les cas de p-divisibilité minimale $p^{\varphi(1)}$ (cf. Remarques 6.2, 6.3, § 6.2).

7.4. Conjectures en p-ramification Abélienne. — Soit $H_{(p)}^{\mathrm{pra}}$ la p-extension Abélienne p-ramifiée (i.e., non ramifiée en dehors de p) maximale d'un corps de nombres Galoisien K (réel). Soit $\widehat{K}_{(p)}$ le composé des $\mathbb{Z}_p$-extensions de K et soit $\mathcal{T}_p = \mathrm{Gal}\big(H_{(p)}^{\mathrm{pra}}/\widehat{K}_{(p)}\big)$. Dans ce cas, pour tout p assez grand, $|\mathcal{T}_p|$ a même valuation p-adique que le régulateur normalisé du corps K, $p^{1-n}\,\mathrm{Reg}_p(K) \sim \prod\limits_{\theta\neq 1} \mathrm{Reg}_p^\theta(\varepsilon)^{\varphi(1)}$, où ε est une unité de Minkowski fixée (voir [**Gr1**], § III.2.6.5, [**Gr2**], § 3, pour des compléments sur ces questions).

Alors la Conjecture 7.8 est reformulée par la conjecture suivante (au moins pour les corps réels, toute partie $\mathcal{T}_p^-$ éventuelle étant triviale dès que p est assez grand) :

Conjecture 7.10. — *L'invariant $\prod\limits_p \mathcal{T}_p$ est fini pour tout corps de nombres.*

La version raisonnable nettement plus faible consiste à dire que pour tout p assez grand, $|\mathcal{T}_p|$ est soit trivial soit égal à $p^{\varphi(1)}$ (à une unité p-adique près), en raison d'un unique facteur $\mathrm{Reg}_p^\theta(\varepsilon)$ divisible par p avec $\theta \neq 1$ de degré résiduel $f = 1$ et $\mathcal{L}^\theta \simeq V_\theta$ (i.e., p-divisibilité minimale). En effet, tout autre cas résulte ou bien de la nullité modulo p d'au moins deux $\Delta_p^\theta(\varepsilon)$ pour des caractères p-adiques distincts (probabilité au plus en $\frac{O(1)}{p^2}$), ou bien de la nullité modulo p d'un unique $\Delta_p^\theta(\varepsilon)$

avec $f\delta^2 \geq 2$ (probabilité en $\frac{O(1)}{p^{f\delta^2}}$, cf. §4.3.2), le cas $p^e \,|\, \mathrm{Reg}_p^\theta(\varepsilon)$, $e \geq 2$, lorsque $f = \delta = 1$, étant de probabilité au plus en $\frac{O(1)}{p^2}$ (cf. § 4.6).

Dans le cas Abélien, ceci impliquerait que les seuls p assez grands pour lesquels $|\mathcal{T}_p| \equiv 0 \pmod p$ sont ceux pour lesquels un unique $\mathrm{Reg}_p^\theta(\varepsilon)$ est exactement divisible par p pour $p \equiv 1 \pmod d$ où d est l'ordre de φ.

De fait, dans le cadre des "Théorèmes principaux", on aurait (par exemple pour l'invariant $\mathcal{T}_p$ précédent) la conjecture raisonnable suivante :

Conjecture 7.11. — *Soit $K/\mathbb{Q}$ une extension Galoisienne réelle finie de groupe de Galois G. Alors, pour tout p assez grand il existe au plus un caractère p-adique irréductible $\theta \neq 1$ de G de degré résiduel $f = 1$ pour lequel $\mathcal{L}^\theta \simeq V_\theta$ (i.e., $\delta = 1$), tel que $\mathcal{T}_p \simeq e_\theta\, \mathbb{F}_p[G]$ (module G-cyclique d'ordre $p^{\varphi(1)}$, $\varphi \,|\, \theta$).*

Remarque 7.12. — On en déduirait aussi des propriétés analogues sur le résidu de la fonction zêta p-adique (cf. [**Coa**] (Appendix) et [**Se2**]). Dans [**Hat**], est utilisé le fait que lorsque la p-valuation de $\zeta_K(2-p)$ est négative, alors elle vaut -1 (cf. [**Se2**], Théorème 6) ; dans le cadre de la Conjecture 7.10 ci-dessus, on aurait alors conjecturalement $\dfrac{\zeta_K(2-p)}{\zeta_{\mathbb{Q}}(2-p)} \sim |\mathcal{T}_p| \sim 1$ pour tout p assez grand, et sur un plan cohomologique, on aurait $\mathrm{H}^2(\mathcal{G}_p, \mathbb{Z}_p) \simeq \mathcal{T}_p^* = 1$ pour tout p assez grand, où $\mathcal{G}_p$ est le groupe de Galois de la pro-p-extension p-ramifiée maximale de K. Plus faiblement, on aurait $\dfrac{\zeta_K(2-p)}{\zeta_{\mathbb{Q}}(2-p)} \sim p^{\varphi(1)}$ et $\mathrm{H}^2(\mathcal{G}_p, \mathbb{Z}_p) \sim p^{\varphi(1)}$ (pour les cas de p-divisibilité minimale).

7.5. Analyse probabiliste alternative pour $q_p(a) \equiv 0 \pmod p$. — Soit $a \in \mathbb{Q}^\times$, $a \neq \pm 1$ fixé. Soit p un nombre premier étranger à a (de toutes façons p est assez grand selon le point de vue adopté). Soit $m = o_p(a) \,\big|\, p-1$ l'ordre de a modulo p et soit ξ une racine primitive m-ième de l'unité dans $\mathbb{C}$; alors on peut écrire $a^m - 1 = \prod_{j=1}^m (a - \xi^j) \equiv 0 \pmod p$. Comme m est l'ordre de a modulo p, c'est le facteur de $a^m - 1$ défini par :

$$\Phi_m(a) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} (a - \xi^t)$$

qui est dans $p\,\mathbb{Z}_{(p)}$, où Φ_m est le m-ième polynôme cyclotomique. De façon précise on a la relation $q_p(a) := \dfrac{a^{p-1}-1}{p} = \dfrac{\Phi_m(a)}{p} \times \prod_{\substack{d|p-1 \\ d\neq m}} \Phi_d(a)$, $\prod_{\substack{d|p-1 \\ d\neq m}} \Phi_d(a) \not\equiv 0 \pmod p$.

Si $a = \frac{u}{v}$, $\Phi_m(a) = v^{-\phi(m)} \prod_t (u - v\,\xi^t)$ et le numérateur $\Phi_m(u,v) := \prod_t (u - v\,\xi^t)$ est seul concerné. On pose :

$$\widetilde{\Phi}_m(a) := \frac{\Phi_m(u,v)}{\text{p.g.c.d.}\,(\Phi_m(u,v), m)}$$

pour éliminer les facteurs premiers p' ramifiés dans $\mathbb{Q}(\xi)/\mathbb{Q}$ qui n'interviennent pas car $m' := o_{p'}(a)$ est un diviseur strict de m (e.g. $p = 19$, $a = 8$, $m = 6$, $\Phi_6(8) = 3 \times 19$ qui introduit $p' = 3$ avec $o_{p'}(8) = 2$ et $\Phi_2(8) = 9$ comme attendu).

On peut donc aussi définir un quotient de Fermat normalisé $\widetilde{q}_p(a) := \dfrac{\widetilde{\Phi}_{o_p(a)}(a)}{p}$; dans tous les cas on remplace $q_p(a)$ et $\widetilde{q}_p(a)$ par leurs représentants dans $[0, p[$.

Puisque dans le corps $\mathbb{Q}(\xi)$, p est totalement décomposé, il existe un idéal premier $\mathfrak{p} \,|\, p$ de $\mathbb{Q}(\xi)$ tel que $(u - v\,\xi)\,\mathbb{Z}[\xi] = \mathfrak{p}^{n_p}\,\mathfrak{a}$, $n_p \geq 1$ et $\mathfrak{p} \nmid \mathfrak{a}$, où $\mathfrak{a}$ est un idéal entier de $\mathbb{Q}(\xi)$; de plus, $\mathfrak{a}$ est étranger à p car les congruences $u - v\,\xi \equiv 0 \pmod{\mathfrak{p}}$ et $u - v\,\xi \equiv 0 \pmod{\mathfrak{p}' \,|\, p}$, $\mathfrak{p}' \neq \mathfrak{p}$, conduisent, par la conjugaison non triviale

$\xi \mapsto \xi^t$ qui transforme $\mathfrak{p}'$ en $\mathfrak{p}$, à $u - v\,\xi \equiv 0 \pmod{\mathfrak{p}}$ et $u - v\,\xi^t \equiv 0 \pmod{\mathfrak{p}}$, d'où $v\,(\xi^t - \xi) \equiv 0 \pmod{\mathfrak{p}}$ (absurde).

Si $\mathfrak{l}$ est un idéal premier divisant $\mathfrak{a}$, la congruence $\xi \equiv a \pmod{\mathfrak{l}}$ montre que $\mathfrak{l}$ est totalement décomposé dans $\mathbb{Q}(\xi)/\mathbb{Q}$ (sauf les éventuels $\mathfrak{l} \,|\, \ell \,|\, m$, ramifiés que l'on a écartés). Autrement dit, si l'on pose :

$$\widetilde{\Phi}_m(a) = \prod_{k=1}^{e} \ell_k^{n_k}, \quad \ell_1 < \ell_2 < \ldots < \ell_e, \ \ n_k \geq 1, \quad m = o_p(a),$$

tous les premiers ℓ_k sont congrus à 1 modulo m et p est l'un d'eux ; en outre on a $\ell \,|\, \widetilde{\Phi}_m(a)$ si et seulement si $o_\ell(a) = m$. Il en résulte aussi que pour un tel $\ell = \ell_k$ (en posant $\ell - 1 = h\,m$), ℓ est totalemment décomposé dans l'extension Galoisienne $\mathbb{Q}(\mu_{\ell-1})(\sqrt[h]{a})/\mathbb{Q}$ puisque a est localement de la forme b^h modulo ℓ (ℓ ne divise pas a et n'est pas ramifié dans cette extension). Ces questions d'ordres modulo p sont liées à des techniques issues de la conjecture d'Artin sur les racines primitives et de la démonstration de Hooley (voir [**Mo**] pour un exposé exhaustif).

On voit alors que la condition $q_{\ell_k}(a) = 0$ est équivalente à $n_k \geq 2$, et pour un entier m fixé les seuls nombres premiers p vérifiant à la fois $o_p(a) = m$ et $q_p(a) = 0$ sont les nombres premiers ℓ_k tels que $n_k \geq 2$.

Ainsi, la recherche des quotients de Fermat nuls est de nature multiplicative, a priori différente de celle des quotients de Fermat $1, 2, \ldots, p-1$. En effet, le cas $q_{\ell_k}(a) = 0$ se lit sur l'exposant n_k tandis qu'autrement, $\widetilde{q}_{\ell_k}(a) \equiv \prod_{j \neq k} \ell_j^{n_j} \pmod{\ell_k}$ dépend des autres diviseurs premiers selon une congruence aléatoire.
Il serait utile de connaître déjà la probabilité pour les entiers $\widetilde{\Phi}_m(a)$ (qui ne sont pas "quelconques" car $\ell_k \equiv 1 \pmod{m}$ élimine les petits carrés) d'avoir un facteur carré non trivial, celle d'un entier pris au hasard étant assez grande (égale à $1 - \frac{6}{\pi^2} \sim 0.392$) ; nous renvoyons aux techniques de [**T**] qui peuvent le permettre.
Les cas où $\widetilde{\Phi}_m(a)$ est divisible par le carré d'un nombre premier ℓ sont en effet rarissimes ; par exemple, pour $a = 14$ et $p = 29$, on a $m = o_p(a) = 28$ avec

$$\widetilde{\Phi}_m(a) = 29^2 \times 3361 \times 176597,$$

ce qui donne donc $q_{29}(14) = 0$.
Considérons l'exemple numérique suivant : $a = 12$ et $m = 35$; on a $\Phi_{35}(x) = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$, qui conduit à :
$\widetilde{\Phi}_{35}(12) = 72872404828019704577129461 = 71 \times 491 \times 806821 \times 6089651 \times 425455031.$
Les premiers $p = 71, 491, 806821, 6089651, 425455031$ jouent des rôles symétriques mais leurs quotients de Fermat sont tous non nuls. Si l'on attribuait en général la probabilité $\frac{1}{\ell_k}$ d'avoir $n_k \geq 2$, il semble qu'on aboutirait à des contradictions numériques vu la présence assez systématique de petits et grands nombres premiers et le fait que cette probabilité dépend de l'ordre de grandeur de $\widetilde{\Phi}_m(a)$.

Le produit sur $m \geq 1$ des $\widetilde{\Phi}_m(a)$ a des propriétés de régularité intéressantes.

Considérons l'aspect numérique donné par le programme suivant :

$\{a = 14; A = 1; for(m = 1, 40, P = polcyclo(m); x = a; B = eval(P);$
$B = B/gcd(B, m); A = A * B); print(a); print(factor(A))\}$

Pour $a = 14$, on obtient $\prod_{m=1}^{40} \widetilde{\Phi}_m(a) =$
$3 \times 5 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29^2 \times 31 \times 37 \times 41 \times 43 \times 47 \times 61 \times 67 \times 71 \times 79 \times 101 \times 103 \times 113 \times 137 \times 157 \times 191 \times 193 \times$
$197 \times 211 \times 223 \times 397 \times 461 \times 547 \times 811 \times 911 \times 937 \times 1033 \times 1061 \times 2347 \times 2851 \times 3361 \times 3761 \times 4027 \times 5393 \times 7307 \times$
$10627 \times 13109 \times 15511 \times 16097 \times 18973 \times 26981 \times 61001 \times 100621 \times 132049 \times 176597 \times 698521 \times 761437 \times$
$1154539 \times 1383881 \times 1948981 \times 2249861 \times 7027567 \times 8108731 \times 14525237 \times 51111761 \times 110256001 \times$

1427145211×1475750641×2239000891×11737870057×25581350023×29914249171×141405986837×299113818931×56693904845761×77312552100349×758855846709601×11284732320255809×14837638311110071×22771730193675277×396530555859061913×459715689149916492091×3921141330646275580183×77720275181800334933851×2984619585279628795345143571×6223308177932683558580086481×26063080998214179685167270877966651.

On constate une progression rapide mais régulière des nombres premiers obtenus, qui doivent tous apparaître au fur et à mesure que la borne sur m (ici 40) augmente ; en effet, si p est fixé, il apparaît comme diviseur de $\widetilde{\Phi}_m(a)$ pour l'unique indice m égal à $o_p(a)$. Seul 29 est au carré (le programme du §2.3.2. donne pour $p < 10^9$ les deux solutions 29 ($m = 28$) et 353 ($m = 352$)).

Remarque 7.13. — Signalons la propriété d'uniformité suivante qui concerne essentiellement la totalité des quotients de Fermat non nuls, et non la valeur 0. Si l'on calcule la somme $\frac{1}{N}\sum\limits_{j=1}^{N}\frac{q_{p_j}(a)}{p_j}$, $\;q_{p_j}(a) \in]\,0, p_j\,[$, pour la suite des nombres premiers étrangers à a ($p_1 = 2$, $p_2 = 3$, $\dots$, p_N), il y a une convergence vers $\frac{1}{2}$ tout à fait remarquable et indépendante de a. Ceci s'explique sans doute par le fait que la valeur moyenne de $q_p(a)$ pour p fixé et a variable est $\frac{p}{2}$. Si l'on pose, pour a fixé, $q_{p_j}(a) = u_j p_j$, $0 < u_j < 1$, la valeur moyenne de la variable aléatoire u_j est $\frac{1}{2}$ et ces variables sont indépendantes (cf. [**EM**], [**H-B**], [**He**], [**OS**] pour d'autres résultats et références liés au quotient de Fermat).

On peut vérifier la propriété ci-dessus au moyen du programme suivant qui calcule aussi (dans N_0) le nombre de $q_{p_j}(a)$ égaux à une valeur donnée (ici 0) :

$\{for(i = 1, 100, e = random(1111); print(\text{"}e = \text{"}, e); N = 0; N0 = 0; S = 0.0;$
$if(Mod(e, 2) == Mod(1, 2), f = Mod((e-1)/2, 2); S = S + component(f, 2)/2);$
$for(n = 1, 5 * 10^8, p = 2 * n + 1;$
$if(isprime(p) == 1\&Mod(e, p)! = Mod(0, p), N = N + 1;$
$qp = Mod(e, p^2)^{(p-1)} - 1; q = component(qp, 2)/p; if(q == 0, N0 = N0 + 1);$
$S = S + q/p)); M = S/N; print(N, \text{""}, N0, \text{""}, M))\}$

On trouve par exemple (dans l'ordre donné par la fonction *random*) :

$e = 839$, $\quad N = 50847532$, $N_0 = 2$, $M = 0.49999204844300$,
$e = 736$, $\quad N = 50847532$, $N_0 = 4$, $M = 0.50002594430610$,
$e = 748$, $\quad N = 50847531$, $N_0 = 2$, $M = 0.49998373833438$,
$e = 240$, $\quad N = 50847531$, $N_0 = 1$, $M = 0.50001538843784$.

Remarque 7.14. — On peut conjecturer que la probabilité $\Pr\big(q_p(a) = 0\big)$ dépend d'une fonction de la forme $\frac{1}{x^{1+\epsilon(x,y)}}$, $\;\epsilon(x, y) > 0$, $\;$ pour $x = p$, $y = a$. .
Si $\Pr\big(q_p(a) = 0\big) = \frac{1}{p^{1+\epsilon(p,a)}}$ et $\Pr\big(q_p(a) = q\big) = u$ pour tout $q \neq 0$, u indépendant de q, alors on obtient $(p-1)\,u + \frac{1}{p^{1+\epsilon(p,a)}} = 1$, d'où $u - \frac{1}{p} = \frac{1 - p^{-\epsilon(p,a)}}{p\,(p-1)}$ et u peu discernable de $\frac{1}{p}$. Il resterait à tester une fonction $\epsilon(x, y) > 0$ telle que $\sum\limits_{p}\frac{1}{p^{1+\epsilon(p,a)}} < \infty$. Comme me l'a fait remarquer G. Tenenbaum, cette convergence a lieu dès que $\epsilon(x, y) = \frac{C\log(\log(\log(x)))}{\log(x)}$, $\;C > 1$. Il reste à tenter des statistiques en comparaison avec une probabilité de ce type (C pouvant dépendre de a) ; on note que $u - \frac{1}{p} \sim \frac{1}{p^2}$ avec une telle fonction ϵ.

Ces observations sont très insuffisantes, mais la probabilité $\frac{1}{p}$ paraît tout aussi arbitraire car on est dans un cadre multiplicatif (comment factoriser $\widetilde{\Phi}_m(a)$) et non dans une structure additive de résidus modulo p. Or si cette probabilité était comme envisagé ci-dessus, les conséquences seraient importantes, y compris pour les corps de nombres pour lesquels les $\Delta_p^\theta(\eta)$ sont une généralisation très canonique des $q_p(a) = \Delta_p^1(a)$.

8. Conclusion

Nous avons conscience du fait que les conjectures précédentes sont particulièrement téméraires, mais nous avons essayé de donner un maximum de justifications, en particulier par le fait que lorsque les probabilités sont au plus en $\frac{O(1)}{p^2}$, les principes heuristiques de type Borel–Cantelli suggèrent un nombre fini de solutions p à $\Delta_p^G(\eta) \equiv 0 \pmod p$ et même aucune solution la plupart du temps puisque la somme des $\frac{1}{p^2}$ est très petite :

$$\sum_{p\geq 2} \frac{1}{p^2} = 0.45, \ \ \sum_{p\geq 100} \frac{1}{p^2} = 0.0018, \text{ et } \ \sum_{p\geq 10000} \frac{1}{p^2} = 9 \times 10^{-6}.$$

De toutes façons il reste les cas de p-divisibilité minimale $p^{\varphi(1)}$ pour $\mathrm{Reg}_p^G(\eta)$ (cf. Définition 3.17, §3.3, ou Remarque 6.3, §6.2, ainsi que § 4.6), c'est-à-dire lorsqu'un unique caractère p-adique θ est concerné par la congruence $\Delta_p^\theta(\eta) \equiv 0 \pmod p$, que p est totalement décomposé dans le corps des valeurs C_χ de $\varphi \,|\, \theta$, et que le G-module $\mathcal{L}^\theta$ est minimal. Rappelons que les p totalement décomposés dans C_χ sont en nombre infini avec une densité connue via le théorème de Dirichlet (tous les nombres premiers si $C_\chi = \mathbb{Q}$ comme dans le cas de $G = D_6$).

Dans ce cas, le “nombre prévisible” de solutions $p < x$ est en $O(1)\mathrm{loglog}(x)$ sauf si le point de vue du §7.5 généralisé aboutit à des constantes, même très grandes.

Mais s'il doit y avoir une certaine cohérence des mathématiques, on peut alors croire que de telles conjectures (a priori inaccessibles à l'heure actuelle) sont légitimes, comme la conjecture ABC et ses nombreuses variantes. Voir par exemple à son sujet le texte de Waldschmidt [**W**] pour l'importante liste d'applications et conséquences qui montrent bien que les aspects diophantiens de la théorie des nombres reposent sur un certain nombre de propriétés “structurelles” plus fortes que celles habituellement accessibles, mais hélas difficiles.

Par exemple, on peut dire que la conjecture de Leopoldt–Jaulent sur la non nullité des régulateurs p-adiques semble une forme extrêmement faible de la réalité.

De fait, ces conjectures suscitent de nombreuses propriétés, et il convient aussi d'envisager de vastes expérimentations numériques.

Références

[Coa] J. Coates, *p-adic L-functions and Iwasawa's theory*, In: Proc. of Durham Symposium 1975, New York-London (1977), 269–353.

[C] K. Conrad, *The origin of representation theory*, Enseign. Math. 44 (1998), 361–392. `http://www.math.uconn.edu/~kconrad/articles/groupdet.pdf`

[EM] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. 66 (1997), 1353–1365. `http://www.ams.org/journals/mcom/1997-66-219/S0025-5718-97-00843-0/S0025-5718-97-00843-0.p`

[GM] H. Graves and M.R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory 133 (2013), 1809–1813. `http://www.sciencedirect.com/science/article/pii/S0022314X12003368`

[Gr1] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2003; second corrected printing 2005. http://www.springer.com/mathematics/numbers/book/978-3-540-44133-5

[Gr2] G. Gras, *On the structure of the Galois group of the Abelian closure of a number field*, Journal de Théorie des Nombres de Bordeaux (à paraître).

[Hat] K. Hatada, *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at* $2-p$, Comment. Math. Univ. St. Pauli 36 (1987), 41–51.
Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients, Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci. 12 (1988), 1–2.

[H-B] D.R. Heath-Brown, *An Estimate For Heilbronn's Exponential Sum*, In: Conference in honor of Heini Halberstam, Analytic Number Theory, 2 (1996), Birkhüser 1996.

[He] G. Helms, *Fermat-quotients, références bibliographiques.* http://go.helms-net.de/math/expdioph/fermatquotient/directory/index.htm

[J] Jaulent, J-F., *Sur l'indépendance ℓ-adique de nombres algébriques*, Jour. Number Theory 20 (1985), 149–158. http://www.sciencedirect.com/science/article/pii/0022314X85900356

[Mo] P. Moree, *Artin's Primitive Root Conjecture – A Survey*, In: The John Selfridge Memorial Volume, Integers, Vol. 12, 6 (2012), 1305–1416. http://www.degruyter.com/view/j/integ.2012.12.issue-6/integers-2012-0043/integers-2012-004

[OS] A. Ostafe and I.E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discrete Math. 25, 1 (2011), 50–71. http://arxiv.org/pdf/1001.1504.pdf

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

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

[Se2] J-P. Serre, *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C.R. Acad. Sci. Paris 287, Série I (1978), 183–188.

[Sh] D. Shanks, *The Simplest Cubic Fields*, Mathematics of Computation 28 (1974), 1137–1152.

[Si] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, Jour. of Number Theory 30 (1988), 226–237. http://www.sciencedirect.com/science/article/pii/0022314X88900194

[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3e édition revue et augmentée, Coll. Échelles, Belin 2008. http://iecl.univ-lorraine.fr/~Gerald.Tenenbaum/ITAN08/

[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.pdf

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

---

3 Avril 2014

Georges Gras, Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans.
E-mail : g.mn.gras@wanadoo.fr • *url :* http://monsite.orange.fr/maths.g.mn.gras/