



HAL
open science

Notion de F_p -régulateurs d'un nombre algébrique—Conjectures p -adiques

Georges Gras

► **To cite this version:**

Georges Gras. Notion de F_p -régulateurs d'un nombre algébrique—Conjectures p -adiques. 2014. hal-00936889v1

HAL Id: hal-00936889

<https://hal.science/hal-00936889v1>

Preprint submitted on 27 Jan 2014 (v1), last revised 3 Apr 2014 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

NOTION DE \mathbb{F}_p -RÉGULATEURS D'UN NOMBRE ALGÈBRIQUE 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 (en particulier étranger à n , $\text{Disc}(K)$, et η), nous définissons, par utilisation du théorème de Frobenius sur les déterminants de groupes, la famille $(\Delta_p^\theta(\eta) \in \mathbb{F}_p)_\theta$ des \mathbb{F}_p -régulateurs de η , indexée par les caractères \mathbb{Q}_p -irréductibles θ de G .

A chaque $\Delta_p^\theta(\eta)$ est associée une représentation linéaire $\mathcal{L}^\theta \simeq \delta V_\theta$ (où V_θ est la représentation de caractère θ , $0 \leq \delta \leq \varphi(1)$, avec $\varphi | \theta$ absolument irréductible) caractérisant (Théorème 3.13) les propriétés de $\Delta_p^\theta(\eta)$ dont sa nullité (équivalente à $\delta > 0$).

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 $\Delta_p^\theta(\eta)$, $\theta \neq 1$, donne le résidu modulo p du θ -régulateur R_p^θ , dans la décomposition $\text{Reg}_{K,p} = p^{n-1} \prod_{\theta \neq 1} (R_p^\theta)^{\varphi(1)}$ du régulateur p -adique classique $\text{Reg}_{K,p}$ du corps K .

Nous suggérons, à partir d’une propriété générale des déterminants de groupes et de l’existence de la représentation \mathcal{L}^θ , que pour θ de degré quelconque la “probabilité” de nullité de $\Delta_p^\theta(\eta)$ avec $\mathcal{L}^\theta \simeq \delta V_\theta$ est en $\frac{O(1)}{p^{\delta^2 f}}$, où f est le degré résiduel de p dans le corps des valeurs des caractères $\varphi | \theta$ et que la “probabilité” de nullité de plusieurs $\Delta_p^\theta(\eta)$ est égale au produit des probabilités respectives.

Nous conjecturons alors que $p^{1-n} \text{Reg}_{K,p}$, qui mesure l’ordre du p -groupe de torsion en p -ramification Abélienne au-dessus de K , est une unité p -adique sauf peut-être pour un ensemble infini de nombres premiers p de densité nulle. Pour cet ensemble de p dits “à décomposition minimale” (i.e., un unique $\Delta_p^\theta(\eta)$ est nul avec $\delta = f = 1$ qui exprime que \mathcal{L}^θ est de \mathbb{F}_p -dimension minimale $\varphi(1)$), il reste possible, η étant alors une “puissance p -ième locale partielle” en p , de justifier et de proposer une conjecture plus forte aboutissant à la même conclusion. D’autres aspects conjecturaux liés à la conjecture *ABC* sont discutés (Section 7).

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. — déterminant de groupe, caractères, régulateur p -adique, rang p -adique, conjecture de Leopoldt, quotient de Fermat, p -ramification Abélienne.

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 (in particular prime to n , $\text{Disc}(K)$, and η), we define, by use of the Frobenius theorem on group determinants, the family $(\Delta_p^\theta(\eta) \in \mathbb{F}_p)_\theta$ of \mathbb{F}_p -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 $\mathcal{L}^\theta \simeq \delta V_\theta$ (where V_θ is the representation of character θ , $0 \leq \delta \leq \varphi(1)$, with $\varphi|\theta$ absolutely irreducible) characterising (Theorem 3.13) the properties of $\Delta_p^\theta(\eta)$ including its nullity (equivalent to $\delta > 0$).

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 $\Delta_p^\theta(\eta)$, $\theta \neq 1$, gives the residue modulo p of the θ -regulator R_p^θ , in the decomposition $\text{Reg}_{K,p} = p^{n-1} \prod_{\theta \neq 1} (R_p^\theta)^{\varphi(1)}$ of the classical p -adic regulator $\text{Reg}_{K,p}$ of the field K .

We suggest, starting from a general property of group determinants and the existence of the representation \mathcal{L}^θ , that for θ of any degree the “probability” of nullity of $\Delta_p^\theta(\eta)$ with $\mathcal{L}^\theta \simeq \delta V_\theta$ is about $\frac{\varphi(1)}{p^{\delta^2 f}}$, where f is the residue degree of p in the field of values of the characters $\varphi|\theta$ and that the “probability” of nullity of several $\Delta_p^\theta(\eta)$ is equal to the product of the respective probabilities.

We conjecture that $p^{1-n} \text{Reg}_{K,p}$, which measures the order of the p -torsion group in Abelian p -ramification over K , is a p -adic unit except perhaps for an infinite set of prime numbers of zero density. For this set of p said “with minimal splitting” (i.e. a single $\Delta_p^\theta(\eta)$ is zero with $\delta = f = 1$ which expresses that \mathcal{L}^θ is of minimal \mathbb{F}_p -dimension $\varphi(1)$), it remains possible, η being then a “partial local p th power” at p , to justify and to propose a stronger conjecture leading to the same conclusion. Some other conjectural aspects related to the *ABC* conjecture are discussed (Section 7).

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 un corps de nombres de degré $n \geq 1$; quitte à travailler dans sa clôture Galoisienne, on peut toujours supposer que l’extension K/\mathbb{Q} est Galoisienne de groupe de Galois G .

On considère alors $\eta \in K^\times$. On désigne par F le groupe engendré par η et ses conjugués. On utilise la notation exponentielle pour la conjugaison de η par $\sigma \in G$ (loi de module à gauche) qui se traduit donc par l’écriture $(\eta^\sigma)^\tau =: \eta^{(\tau\sigma)}$ pour tout $\sigma, \tau \in G$.

Nous supposons 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.

Pour toute place $v|p$ on désigne par \mathfrak{p}_v l’idéal premier associé à v et, par abus, par v la valuation \mathfrak{p}_v -adique normalisée associée. 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 $\eta^{p^{n_p}-1} \equiv 1 \pmod{\mathfrak{p}_v}$ pour tout $v|p$; donc, comme par hypothèse on a $\prod_{v|p} \mathfrak{p}_v = (p)$, il vient $\eta^{p^{n_p}-1} \equiv 1 \pmod{p}$ et :

$$\eta^{p^{n_p}-1} = 1 + p \alpha_p(\eta), \quad \alpha_p(\eta) \in K, \quad v(\alpha_p(\eta)) \geq 0, \quad \forall v|p,$$

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

$$\alpha_p(\eta \eta') \equiv \alpha_p(\eta) + \alpha_p(\eta') \pmod{p} \quad \& \quad \alpha_p(\eta^\lambda) \equiv \lambda \alpha_p(\eta) \pmod{p}.$$

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. $\mathbb{Z}_{(p)}$). 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 comme ci-dessus $\beta \equiv 0 \pmod{\prod_{v|p} \mathfrak{p}_v}$ (p non ramifié) ; elle implique que si $\beta = \sum_{i=1}^n A_i e_i$ est écrit sur une $\mathbb{Z}_{(p)}$ -base $(e_i)_{i=1,\dots,n}$ de $Z_{K,(p)}$, alors on a $A_i \equiv 0 \pmod{p}$ pour $i = 1, \dots, n$.

2. Régulateurs, χ -régulateurs, et \mathbb{F}_p -régulateurs de η

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 une fois pour toutes 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} un idéal premier de K au-dessus de p et soit D son groupe de décomposition ; on fixe un système exact de plongements $\sigma_v \in G$ représentant G/D . Alors les places $v|p$ sont associées aux $(G : D)$ idéaux premiers distincts $\mathfrak{p}_v := \mathfrak{p}^{\sigma_v}$ dont le groupe de décomposition est $D_v = \sigma_v \circ D \circ \sigma_v^{-1}$.

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 $\sigma_v : K \rightarrow \mathbb{C}_p$.

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

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

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

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

Cette fonction \log , 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 :

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

en considérant la congruence :

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

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

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

$$\begin{aligned} K_{(p)}^\times &\longrightarrow \prod_{v|p} K_v . \\ \eta &\longmapsto (\log(\eta^{\sigma_v}))_{v|p} \end{aligned}$$

On appelle rang p -adique du groupe F engendré par les conjugués de η , l'entier :

$$\text{rg}_p(F) := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_p(F)).$$

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

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 $\text{Tr}_{K_v/\mathbb{Q}_p}$. On a $\text{Tr}_{K/\mathbb{Q}}(\lambda u) = \sum_{v|p} \text{Tr}_v(\sigma_v(\lambda u))$. Comme p est non ramifié dans K/\mathbb{Q} , les $\sigma_v(\lambda u)$ qui ne sont pas des unités de K_v sont divisibles par l'uniformisante locale p et sont de trace nulle modulo p ; or par hypothèse, il existe un ensemble non vide Σ de places $v|p$ telles que $\sigma_v(\lambda u)$ est une unité (tout ceci est indépendant de u étranger à p). Pour $v_0 \in \Sigma$, on écrit :

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

($a = 0$ si $|\Sigma| = 1$). Comme les traces résiduelles en p sont surjectives et que $\sigma_{v_0}(\lambda u)$ est une unité, on peut trouver u , $u \equiv 1 \pmod{\prod_{v, v \neq v_0} \mathfrak{p}_v}$, tel que par exemple $\text{Tr}_{v_0}(\sigma_{v_0}(\lambda u)) \equiv 1 - a \pmod{p}$. D'où $\text{Tr}_{K/\mathbb{Q}}(\lambda u) \equiv 1 \pmod{p}$. \square

Le lemme suivant 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 $\lambda(\sigma)$ 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 $\ell_\sigma = (\dots, \log(\eta^{\tau\sigma}), \dots)_\tau$:

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

Alors il existe des coefficients $\lambda'(\sigma) \in \mathbb{Z}_{(p)}$, non tous divisibles par p , tels que l'on ait la relation $\sum_{\sigma \in G} \lambda'(\sigma) \log(\eta^{\tau\sigma}) \equiv 0 \pmod{p^N}$ 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 $\text{Tr}_{K/\mathbb{Q}}(\lambda(1)) \equiv 1 \pmod{p}$ en multipliant la congruence par u étranger à p convenable (cf. Lemme 2.1). Par conjugaison par $\nu \in G$ on obtient $\sum_{\sigma \in G} \lambda(\sigma)^\nu \log(\eta^{\nu\tau\sigma}) \equiv 0 \pmod{p^N}$ pour tout $\tau \in G$, équivalent à $\sum_{\sigma \in G} \lambda(\sigma)^\nu \log(\eta^{s\sigma}) \equiv 0 \pmod{p^N}$ 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 $\lambda'(1) \equiv 1 \pmod{p}$. \square

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

Le rang p -adique de F est donc égal au rang sur \mathbb{Z}_p (au sens précédent) de la matrice de Frobenius :

$$(\log(\eta^{\tau\sigma}))_{\sigma, \tau \in G}.$$

Si ce rang est donné par un plus grand mineur M non nul, M est non nul modulo toute puissance p^N assez grande.

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 $\text{rg}(F) = \dim_{\mathbb{Q}}(F \otimes \mathbb{Q})$.

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 sous-déterminant d'ordre r est de façon canonique

divisible par p^r , pour tout $p > 2$, puisque l'on a, dans $Z_{K,(p)}$, la congruence $\log(\eta) \equiv \frac{1}{p^{np}-1} p \alpha_p(\eta) \equiv -p \alpha_p(\eta) \pmod{p^2}$. D'où la définition suivante :

Définition 2.3. — (i) On considère (pour p assez grand) la matrice à coefficients entiers $\mathcal{R}_p^G(\eta) := \left(\frac{-1}{p} \log(\eta^{\tau\sigma})\right)_{\sigma,\tau \in G}$, où $\frac{-1}{p} \log(\eta) \equiv \alpha_p(\eta) \pmod{p}$. Son déterminant $R_p^G(\eta)$ est appelé le régulateur p -adique normalisé de η .

(ii) Pour K Galoisien réel, le régulateur p -adique usuel $\text{Reg}_{K,p}$ est donné par un mineur d'ordre $n-1$ de la matrice $(\log(\varepsilon^{\tau\sigma}))_{\sigma,\tau \in G}$, où ε est une unité de Minkowski, et l'entier p -adique $p^{1-n} \text{Reg}_{K,p} = \left(\frac{-1}{p} \log(\varepsilon^{\tau\sigma})\right)_{\sigma \neq 1, \tau \neq 1}$ est appelé le régulateur p -adique normalisé de K .

Comme le plongement diagonal de K dans $\prod_{v|p} K_v$, au moyen de $(\sigma_v)_{v|p}$, est dense, on peut considérer que, modulo p^N , la fonction $\frac{-1}{p} \log$ est à valeurs dans K au moyen de la congruence précédente. D'après le Lemme 2.2, on peut toujours se ramener à des raisonnements 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 $\left(\frac{-1}{p} \log(\eta^{\tau\sigma}) \pmod{p^N}\right)_{\sigma,\tau \in G}$, pour N assez grand.

Si un mineur M d'ordre $\text{rg}(F)$ de la matrice $\mathcal{R}_p^G(\eta)$ est de déterminant non nul modulo p^N , 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 est a priori supérieur ou égal au \mathbb{F}_p -rang de la matrice $(\alpha_p(\eta)^{\tau\sigma})_{\sigma,\tau \in G}$. Dans [Hat], Hatada a procédé, dans quelques cas de corps de nombres, à une étude statistique de la nullité modulo p du régulateur normalisé en utilisant le fait que sa p -valuation est la p -valuation de $p \zeta_K(2-p)$.

Définition 2.4. — Si l'on a dans $F \otimes \mathbb{Q}$ la relation $\prod_{\sigma \in G} (\eta^\sigma)^{\lambda(\sigma)} = 1$, $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, alors on a, pour tout p étranger à η , les relations $\sum_{\sigma \in G} \lambda(\sigma) \log(\eta^\sigma) = 0$ qui se transmettent en les relations $\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^\sigma \equiv 0 \pmod{p}$.

Nous dirons par abus que de telles relations modulo p entre les conjugués de $\alpha_p(\eta)$ sont *formelles* pour signifier qu'elles ne sont pas dûes à une circonstance numérique pour les p considérés, mais à l'existence d'une relation dans $F \otimes \mathbb{Q}$ donnée par des $\lambda(\sigma)$ indépendants de p (on peut dire en un certain sens que la famille de relations $(\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^\sigma \equiv 0 \pmod{p})_p$ est alors globale).⁽¹⁾

Lorsque la représentation $F \otimes \mathbb{Q}$ est isomorphe à la représentation régulière $\mathbb{Q}[G]$ (cas auquel on peut se ramener par somme directe avec un G -module convenable), sa \mathbb{Q} -dimension est égale à n et il n'y a pas de relations formelles.

Lorsqu'on a le cas d'une unité de Minkowski ε d'un corps K totalement réel, il suffit de poser $\eta = a\varepsilon$, a rationnel $\neq \pm 1$, pour se ramener au cas précédent.

Notre principal objectif est de voir sous quelles conditions et avec quelle "probabilité" le régulateur normalisé $R_p^G(\eta)$ (élément de \mathbb{Z}_p à une unité p -adique près de la forme $\sqrt{m} \in K$, $m \in \mathbb{Z}$) est divisible par p assez grand. D'après ce qui précède et le Lemme 2.2, on a $R_p^G(\eta) \equiv 0 \pmod{p}$ si et seulement si il existe une relation de $\mathbb{Z}/p\mathbb{Z}$ -dépendance des vecteurs-lignes $\ell_\sigma = (\dots, \frac{-1}{p} \log(\eta^{\tau\sigma}), \dots)_\tau$, pour $\sigma \in G$.

⁽¹⁾ Réciproque : supposons que $\sum_{\sigma \in G} \lambda(\sigma) \alpha_p(\eta)^\sigma \equiv 0 \pmod{p}$ pour presque tout p , pour des $\lambda(\sigma) \in \mathbb{Q}$ indépendants de p . Soit $\Lambda := \prod_{\sigma \in G} (\eta^\sigma)^{\lambda(\sigma)} \in F \otimes \mathbb{Q}$; alors $\log(\Lambda) \equiv 0 \pmod{p^2}$ 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 Λ est une puissance p -ième locale en p . Conjecturalement Λ est une racine de l'unité de K (cf. §7.1.3, Conjecture 7.4).

Comme $R_p^G(\eta)$ se factorise en produit de puissances convenables de χ -régulateurs $R_p^\chi(\eta)$ (pour les caractères rationnels irréductibles χ de G), il est alors intéressant d'étudier la divisibilité par p de ces facteurs à partir de telles relations (cf. §3.1). Cette factorisation ne dépend pas de p en un sens, par contre on peut factoriser $R_p^\chi(\eta)$ en produit de θ -régulateurs $R_p^\theta(\eta)$ (pour les caractères p -adiques irréductibles $\theta \mid \chi$), mais cette factorisation dépend (par le nombre de facteurs) du degré résiduel de p dans le corps des valeurs des caractères absolument irréductibles $\varphi \mid \theta$ de G .

Une première étude statistique montrera que la probabilité d'avoir au moins deux θ -régulateurs $R_p^\theta(\eta)$, $R_p^{\theta'}(\eta)$, nuls modulo p est 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'un unique θ -régulateur nul modulo p (cf. §3.2).

2.2. Cas général des 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). Cependant il est nécessaire d'examiner 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]).

Rappelons qu'en tant que représentation régulière on a l'isomorphisme $\mathbb{C}[G] \simeq \bigoplus_{\rho} \deg(\rho) \cdot V_{\rho}$, où 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, $\deg(\rho) = \varphi(1)$. Aussi nous convenons d'indexer les objets dépendant de ρ par la lettre φ et de ne conserver $\rho = \rho_{\varphi}$ qu'en tant qu'homomorphisme de G dans $\text{End}(V_{\varphi})$.

Comme algèbre d'endomorphismes $U = \sum_{\sigma \in G} u(\sigma) \sigma \in \mathbb{C}[G]$ agissant sur la base des $\nu \in G$, on a l'isomorphisme $\mathbb{C}[G] \simeq \bigoplus_{\varphi} \text{End}(V_{\varphi})$, avec $\text{End}(V_{\varphi}) \simeq e_{\varphi} \mathbb{C}[G]$, 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 de $\varphi(1)$ représentations irréductibles, on utilise les projecteurs issus d'une représentation matricielle (cf. [Se1], §I.2.7).

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

$$\Delta^G = \prod_{\varphi} \det \left(\sum_{\nu \in G} X_{\nu} \rho_{\varphi}(\nu^{-1}) \right)^{\varphi(1)}.$$

Il en résulte l'existence de polynômes homogènes $P^{\varphi}(X)$ ($X := (\dots, X_{\nu}, \dots)_{\nu \in G}$), de degrés $\varphi(1)$, tels que $\Delta^G = \prod_{\varphi} P^{\varphi}(X)^{\varphi(1)}$. On regroupe ensuite en produits partiels sur les caractères φ pour obtenir des caractères χ , irréductibles sur \mathbb{Q} , ou des caractères p -adiques θ , irréductibles sur \mathbb{Q}_p (cf. Définition 2.5).

La spécialisation $X_{\nu} \mapsto \frac{-1}{p} \log(\eta^{\nu})$ permet d'obtenir la factorisation :

$$R_p^G(\eta) = \prod_{\varphi} \det \left(\sum_{\nu \in G} \frac{-1}{p} \log(\eta^{\nu}) \rho_{\varphi}(\nu^{-1}) \right)^{\varphi(1)}$$

qui permet de poser :

$$R_p^\varphi(\eta) = \det\left(\sum_{\nu \in G} \frac{-1}{p} \log(\eta^\nu) \rho_\varphi(\nu^{-1})\right), \quad R_p^X(\eta) = \prod_{\varphi|X} R_p^\varphi(\eta), \quad R_p^\theta(\eta) = \prod_{\varphi|\theta} R_p^\varphi(\eta),$$

et de voir que lorsque l'on réduit $\frac{-1}{p} \log(\eta^\nu)$ modulo p on obtient $\alpha_p(\eta) \pmod{p}$. De fait l'étude modulo p de chaque $R_p^\theta(\eta)$ donne une information beaucoup plus précise que l'étude modulo p du régulateur normalisé $R_p^G(\eta) = \prod_{\theta} R_p^\theta(\eta)^{\varphi(1)}$.

On étudiera plus généralement la spécialisation $X_\nu \mapsto \alpha^\nu$, $\alpha \in Z_K$ donné, dont nous noterons encore le résultat (par abus) :

$$\Delta^G := \det(\alpha^{\tau\sigma})_{\sigma, \tau \in G},$$

où l'on rappelle que $\alpha^{\tau\sigma} = (\alpha^\sigma)^\tau$.

Par exemple, dans le contexte logarithmique précédent relatif à un nombre algébrique η pour lequel $\frac{-1}{p} \log(\eta) \equiv \alpha := \alpha_p(\eta) \pmod{p}$, nous utiliserons la notation plus précise :

$$\Delta_p^G(\eta) = \det(\alpha^{\tau\sigma})_{\sigma, \tau \in G}.$$

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 $V[X] := V[\dots, X_\nu, \dots]$ défini par $L(X) = \sum_{\nu \in G} X_\nu \nu^{-1}$. Il est tel que :

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

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

Soit $(\rho_\varphi, V_\varphi)$ la famille des représentations irréductibles non isomorphes. Dans la pratique, on prendra pour $\text{End}(V_\varphi)$ la composante $e_\varphi \mathbb{C}[G]$ associée au caractère absolument irréductible φ , soit $e_\varphi \mathbb{C}[G] = \frac{\varphi(1)}{n} \sum_{\nu \in G} \varphi(\nu^{-1}) \nu \cdot \mathbb{C}[G]$. ⁽²⁾

On utilise l'isomorphisme d'algèbres $\tilde{\rho} : V \longrightarrow \prod_{\varphi} \text{End}(V_\varphi)$ défini par :

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

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 $L(X)$:

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

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

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

Soit g le plus petit commun multiple des ordres des éléments de G : on sait que les représentations sont réalisables sur le corps $C = \mathbb{Q}(\mu_g)$ des racines g -ièmes de l'unité (cf. [Se1], § 12.3). On pourra donc toujours supposer que les a_{ij} sont des nombres algébriques p -entiers pour tout p assez grand.

Soit $\Gamma := \text{Gal}(C/\mathbb{Q})$. Etant donné une représentation absolument irréductible $\rho_\varphi : G \mapsto \text{End}_C(V_\varphi)$, on définit ses conjuguées de façon Galoisienne, de sorte que pour tout $s \in \Gamma$, ρ_φ^s est la représentation $G \mapsto \text{End}_C(V_{\varphi^s}) \simeq e_{\varphi^s} C[G]$ de caractère

⁽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 $\{E_1 = e_\varphi(1 - \sigma), E_\sigma = e_\varphi \sigma(1 - \sigma), E_\tau = e_\varphi \tau(1 - \sigma), E_{\tau\sigma} = e_\varphi \tau\sigma(1 - \sigma)\}$.

φ^s défini par $\varphi^s(\nu) = (\varphi(\nu))^s$, pour tout $s \in \Gamma$. On a, pour tout $\nu \in G$ et tout $s \in \Gamma$, $\varphi^s(\nu) = \varphi(\nu^{\omega(s)})$, où ω est le caractère $\Gamma \rightarrow (\mathbb{Z}/g\mathbb{Z})^\times$ 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 caractères irréductibles φ , on considère les trajectoires T et on pose :

$$\chi = \sum_{\varphi \in T} \varphi \quad \text{et} \quad P^\chi(X) := \prod_{\varphi \in T} P^\varphi(X).$$

Pour chaque χ , T s'identifie au groupe de Galois de C_χ/\mathbb{Q} , où C_χ est le corps des valeurs de n'importe quel conjugué de φ , et χ est à valeurs rationnelles.

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

Soit φ un caractère absolument irréductible dont la somme des \mathbb{Q} -conjugués est χ . On considère, pour tout $\nu \in G$, $\Theta(\nu) := \sum_{s \in D} \varphi^s(\nu) \in L$. Comme L est dense dans $\prod_{\mathfrak{p}|p} L_{\mathfrak{p}}$, via un plongement $x \in L \mapsto (t_{\mathfrak{p}}(x))_{\mathfrak{p}|p}$, où les $t_{\mathfrak{p}}$ représentent $\text{Gal}(C_\chi/\mathbb{Q})/D$, et que $\prod_{\mathfrak{p}|p} L_{\mathfrak{p}} = \prod_{\mathfrak{p}|p} \mathbb{Q}_p$, on appelle $\theta(\nu)$ la \mathfrak{p} -composante $t_{\mathfrak{p}}(\Theta(\nu))$ qui est dans \mathbb{Z}_p . Comme tout est ensuite considéré modulo $p\mathbb{Z}_p$, il suffit de définir les caractères θ (indexés par les $\mathfrak{p}|p$) via des congruences modulo \mathfrak{p} , de sorte que $\theta(\nu) \equiv r_{\mathfrak{p}}^\theta(\nu) \pmod{\mathfrak{p}}$, $r_{\mathfrak{p}}^\theta(\nu) \in \mathbb{Z}$.

Si l'on fixe un couple (θ, \mathfrak{p}) , les autres sont les h conjugués, donc si $\theta = \sum_{s \in D} \varphi^s$, les h conjugués de θ sont les $\theta^t = \sum_{s \in D} (\varphi^t)^s$, $t \in \text{Gal}(C_\chi/\mathbb{Q})/D$. Pour p fixé, l'entier f ne dépend que de χ et est appelé par abus le degré résiduel des caractères 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 dans C_χ/\mathbb{Q} .⁽³⁾ On pose alors :

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

(iii) On écrit $\varphi | \theta$, $\theta | \chi$, pour indiquer que φ (resp. θ) est un terme de θ (resp. χ).

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 $a_{ij}(\nu^{-1})^s$, 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 $\pi \in G$ et tout caractère irréductible φ , on a $P^\varphi(\dots, X_{\pi\nu}, \dots) = \zeta P^\varphi(\dots, X_\nu, \dots)$, où ζ est une racine de l'unité d'ordre diviseur de g .*

Démonstration. — Comme $P^\chi(X) = \prod_{s \in \text{Gal}(C_\chi/\mathbb{Q})} P^{\varphi^s}(X)$ 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 $\tilde{\rho} : V \rightarrow \prod_{\varphi} \text{End}(V_\varphi)$ commutent ; de plus, puisque

⁽³⁾L'ordre de p modulo g est un multiple de f (par exemple, pour $G = D_6$, on a $g = 6$, $f = 1$, et tout caractère φ est rationnel et p -adique pour tout p).

ρ_φ est un homomorphisme, on a la formule suivante :

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

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

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

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

Corollaire 2.7. — Pour tout $\pi \in G$ et tout caractère absolument irréductible φ , $P^\varphi(\dots, \alpha^{\pi\nu}, \dots) = \zeta P^\varphi(\dots, \alpha^\nu, \dots)$ par spécialisation $X_\nu \mapsto \alpha^\nu$, $\alpha \in Z_K$. Par conséquent, $P^\chi(\dots, \alpha^{\pi\nu}, \dots) = \pm P^\chi(\dots, \alpha^\nu, \dots)$ pour tout $\pi \in G$.⁽⁴⁾

De même, $P^\theta(\dots, \alpha^{\pi\nu}, \dots) = \zeta_p P^\theta(\dots, \alpha^\nu, \dots)$ pour tout $\pi \in G$, où ζ_p est d'ordre diviseur de p.g.c.d. ($g, p-1$).

2.2.2. Régulateurs formels. — Dans cette partie, il n'y a pas de référence à un nombre premier p et les caractères considérés sont absolument irréductibles ou rationnels. Ce qui précède conduit à définir les χ -régulateurs formels.

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

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

le déterminant de groupe associé. Les χ -régulateurs formels sont par définition les expressions (où φ est un caractère absolument irréductible divisant χ) :

$$\Delta^\chi = \prod_{\varphi | \chi} P^\varphi(X) \text{ ou, par abus, } \Delta^\chi = \prod_{\varphi | \chi} P^\varphi(\dots, \alpha^\nu, \dots), \quad \alpha \in Z_K,$$

de sorte que $\Delta^G = \prod_{\chi} (\Delta^\chi)^{\varphi(1)}$.

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

$$\begin{aligned} \Delta^1 &= \alpha + \alpha^\sigma + \alpha^{\sigma^2} + \alpha^\tau + \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2}, \\ \Delta^{\chi^1} &= \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2}, \\ \Delta^{\chi^2} &= \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha \\ &\quad + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau. \end{aligned}$$

Les deux derniers sont de la forme $\Delta \sqrt{m}$, $\Delta \in \mathbb{Q}$, où $k = \mathbb{Q}(\sqrt{m})$ est le sous corps quadratique de K et on néglige le facteur \sqrt{m} ; mais Δ^{χ^2} figure au carré dans le régulateur Δ^G et le résultat est rationnel, ce qui n'est pas le cas de Δ^{χ^1} . Ceci est spécifique des seuls caractères quadratiques.

Pour les calculs, on peut revenir aux réalisations matricielles :

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

qui conduisent à :

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

⁽⁴⁾ De fait le signe est + sauf si $\chi = \varphi$ est un caractère quadratique et $\varphi(\pi) = -1$ (cf. Lemme 2.11 (ii)).

ou encore, par spécialisation et en prenant le déterminant :

$$\Delta^{\chi_2} = \begin{vmatrix} \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} & \alpha^\sigma - \alpha^{\sigma^2} - \alpha^{\tau\sigma} + \alpha^{\tau\sigma^2} \\ -\alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau + \alpha^{\tau\sigma^2} & \alpha - \alpha^\sigma - \alpha^\tau + \alpha^{\tau\sigma} \end{vmatrix}.$$

Toujours pour le caractère χ_2 (de degré 2) et la représentation $e_{\chi_2} C[G] \simeq V_\varphi \oplus V_{\varphi^2}$, il existe deux projecteurs orthogonaux π_1, π_2 , de somme $e_{\chi_2} = \frac{1}{3}(2 - \sigma - \sigma^2)$, qui sont définis par la formule générale (cf. [Se1], §I.2.7) :

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

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

2.2.3. Régulateurs formels – 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 $\varphi : G \rightarrow \mathbb{C}^\times$; on sait que φ a pour image le groupe μ_d des racines de l'unité d'ordre égal à l'ordre d de φ . On a alors $\Delta^G = \det(X_{\tau\sigma})_{\sigma, \tau \in G} = \prod_{\varphi \in \widehat{G}} \left(\sum_{\nu \in G} \varphi(\nu^{-1})X_\nu \right)$.

Si G est produit direct de groupes cycliques G_i , alors en écrivant que $\widehat{G} = \prod_i \widehat{G}_i$,

il vient $\det(X_{\tau\sigma})_{\sigma, \tau \in G} = \prod_i \prod_{\varphi \in \widehat{G}_i} \left(\sum_{\nu \in G_i} \varphi(\nu^{-1})X_\nu \right)$. 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^s , où φ est fixé d'ordre d et où s parcourt $(\mathbb{Z}/d\mathbb{Z})^\times$. On peut donc écrire :

$$\det(X_{\tau\sigma})_{\sigma, \tau \in G} = \prod_{\chi} \prod_{\varphi|\chi} \left(\sum_{\nu \in G} \varphi(\nu^{-1})X_\nu \right).$$

Définition 2.10. — 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 $\varphi|\chi$). Les χ -régulateurs formels sont les expressions :

$$\Delta^\chi := \prod_{\varphi|\chi} \left(\sum_{\nu \in G} \varphi(\nu^{-1})X_\nu \right) \quad \text{ou} \quad \Delta^\chi := \prod_{\varphi|\chi} \left(\sum_{\nu \in G} \varphi(\nu^{-1})\alpha^\nu \right)$$

obtenu par spécialisation $X_\nu \mapsto \alpha^\nu$ pour $\alpha \in Z_K$.

Lemme 2.11. — Soit $C_\chi = \mathbb{Q}(\mu_d)$ le corps des valeurs des caractères irréductibles $\varphi|\chi$.

(i) On a $\Delta^\chi = N_{C_\chi/\mathbb{Q}} \left(\sum_{\nu \in G} \varphi(\nu^{-1})X_\nu \right) \in \mathbb{Z}[X]$.

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

Démonstration. — Le premier point est évident puisque le produit définissant Δ^χ porte sur tous les \mathbb{Q} -conjugués de φ .⁽⁵⁾

⁽⁵⁾ A ce sujet, signalons que les deux opérations “conjugaison dans C_χ/\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} .

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

$$N_{C_\chi/\mathbb{Q}} \left(\sum_{\nu \in G} \varphi(\nu^{-1}) X_{\tau\nu} \right) = N_{C_\chi/\mathbb{Q}} \left(\sum_{\nu \in G} \varphi(\nu^{-1}) X_\nu \right).$$

Donc par spécialisation avec $\alpha \in Z_K$, Δ^χ , invariant par tout $s \in \text{Gal}(C_\chi/\mathbb{Q})$ et tout $\tau \in \text{Gal}(K/\mathbb{Q})$, est un rationnel.

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

- (i) $\Delta^1 = \sum_{\sigma \in G} \alpha^\sigma \in \mathbb{Z}$, pour $\varphi = 1$.
- (ii) $\Delta^\chi = \sum_{\sigma \in G} \chi(\sigma^{-1}) \alpha^\sigma$, 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 $\tau\Delta^\chi = -\Delta^\chi$; d'où $\Delta^\chi = \Delta'^\chi \cdot \sqrt{m}$, où $\Delta'^\chi \in \mathbb{Z}$. \square

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 Δ^χ pour le rationnel correspondant.

Exemple 2.12. — 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 formel :

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

et par définition les deux χ -régulateurs formels :

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

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

De même Δ^χ sera formellement nul si $\alpha \in \mathbb{Z}$, sans que Δ^1 le soit si $\alpha \neq 0$.

Les χ -régulateurs sont formellement indépendants en un sens évident (les polynômes $P^\varphi(X)$ sont irréductibles non associés).

Exemple 2.13. — 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 formel :⁽⁶⁾

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

On a donc par définition les deux χ -régulateurs formels :

$$\Delta^1 = \alpha + \alpha' + \alpha'',$$

$$\Delta^\chi = N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = \alpha^2 + \alpha'^2 + \alpha''^2 - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha.$$

⁽⁶⁾ Rappelons que $N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'')$ a la signification suivante : on définit d'abord $N_{\mathbb{Q}(j)/\mathbb{Q}}(X_1 + j^{-1}X_\sigma + j^{-2}X_{\sigma^2})$ de façon Galoisienne évidente, puis ensuite on spécialise, ce qui donne en réalité $\Delta^\chi = N_{K(j)/K}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'')$ car ici $K \cap \mathbb{Q}(j) = \mathbb{Q}$ et les deux opérations commutent, mais ce n'est pas toujours le cas.

Si par exemple $\Delta^1 = 0$ avec $\alpha \notin \mathbb{Z}$, alors :

$$\Delta^x = N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = 3N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha - j^{-1}\alpha') = 3(\alpha^2 + \alpha\alpha' + \alpha'^2),$$

qui est formellement non nul.

2.2.4. Nullité formelle des χ -régulateurs. — Soit G un groupe fini quelconque. Dans la décomposition :

$$\Delta^G = \det(\alpha^{\tau\sigma})_{\sigma,\tau} = \prod_{\chi} (\Delta^{\chi})^{\varphi(1)}, \quad \text{avec } \Delta^{\chi} = \prod_{\varphi|\chi} P^{\varphi}(\dots, \alpha^{\nu}, \dots),$$

lorsque la spécialisation via $\alpha \equiv \frac{-1}{p}\log(\eta) \pmod{p}$ résulte du logarithme p -adique de $\eta \in K^{\times}$, nous dirons que certains χ -régulateurs Δ^{χ} sont formellement nuls s'ils correspondent à une relation multiplicative dans $F \otimes \mathbb{Q}$ entre les conjugués de η (cf. Définition 2.4). De fait cette définition est indépendante de p et ne concerne que le $\mathbb{Q}[G]$ -module engendré par η .

Ces relations vont être précisées au moyen du système fondamental d'idempotents centraux orthogonaux des algèbres $\mathbb{C}[G]$ et $\mathbb{Q}[G]$.

Définition 2.14. — (i) On a, pour un corps $C \subset \mathbb{C}$ assez gros, les décompositions $C[G] = \bigoplus_{\varphi} e_{\varphi} C[G]$, avec $e_{\varphi} = \frac{\varphi(1)}{|G|} \sum_{\nu \in G} \varphi(\nu^{-1}) \nu$, et $\mathbb{Q}[G] = \bigoplus_{\chi} e_{\chi} \mathbb{Q}[G]$, où $\chi = \sum_s \varphi^s$ et $e_{\chi} = \sum_s e_{\varphi^s} = \frac{\varphi(1)}{|G|} \sum_{\nu \in G} \chi(\nu^{-1}) \nu$, où les φ^s sont les \mathbb{Q} -conjugués distincts d'un caractère irréductible $\varphi|\chi$ fixé.

(ii) Comme $1 = \sum_{\chi} e_{\chi}$, $\eta = \prod_{\chi} \eta^{e_{\chi}}$ et on dira que le χ -régulateur Δ^{χ} associé est formellement nul si $\eta^{e_{\chi}} = 1$ dans $F \otimes \mathbb{Q}$. Par extension des scalaires, on peut voir ces relations dans $F \otimes C$ et écrire par exemple que $\eta^{e_{\varphi}} = 1$.

(iii) Si on a la relation (dans $F \otimes \mathbb{Q}$) $\prod_{\nu \in G} (\eta^{\nu})^{u(\nu)} = 1$, on parlera de la relation $U := \sum_{\nu \in G} u(\nu) \nu \in \mathbb{Q}[G]$ et des φ -relations $U_{\varphi} := e_{\varphi} \cdot U \in C[G]$, ou encore des χ -relations $U_{\chi} := e_{\chi} \cdot U \in \mathbb{Q}[G]$. On peut toujours ramener ces relations à des relations dans des anneaux d'entiers convenables (voir aussi la Définition 3.3).

Remarque 2.15. — (i) Comme la représentation $e_{\varphi} C[G]$ est somme directe de $\varphi(1)$ représentations irréductibles, la définition 2.14 (ii) (i.e., $\eta^{e_{\chi}} = 1$) assure qu'aucune φ -relation non triviale n'est possible et a fortiori aucune χ -relation.

Par exemple, pour $G = D_6$ et $\varphi = \chi = \chi_2$, les relations $U_1 = \frac{1}{3}(1 - \sigma + \tau - \tau\sigma)$ et $U_2 = \frac{1}{3}(1 - \sigma^2 - \tau + \tau\sigma)$ sont deux φ -relations indépendantes telles que $e_{\varphi} U_i = U_i$, pour $i = 1, 2$, $U_1 + U_2 = e_{\varphi}$, et $U_1 U_2 = 0$ (cf. Exemple 2.9).

Ainsi on pourrait avoir la relation formelle non triviale $\eta^{1-\sigma+\tau-\tau\sigma} = 1$ sans avoir la relation $\eta^{1-\sigma^2-\tau+\tau\sigma} = 1$; on aurait donc $\eta^{e_{\chi} \cdot (U_1+U_2)} = \eta^{e_{\chi}} \neq 1$, or on vérifie facilement que le χ -régulateur Δ^{χ} est identiquement nul en raison de la première relation.

(ii) On a les formules évidentes $U_{\chi} = \sum_{\varphi|\chi} U_{\varphi}$ et $U_{\varphi} = e_{\varphi} U_{\chi}$, pour tout $\varphi|\chi$. On a par exemple, en introduisant un nombre premier p , et pour $U \in \mathbb{Q}[G]$, $U_{\chi} \equiv 0 \pmod{p}$ si et seulement si $U_{\varphi} \equiv 0 \pmod{p}$ pour tout $\varphi|\chi$ (car $U_{\varphi} = e_{\varphi} U_{\chi}$), donc si et seulement si il existe au moins un $\varphi|\chi$ tel que $U_{\varphi} \equiv 0 \pmod{p}$ (car les caractères $\varphi|\chi$ sont conjugués par $\text{Gal}(C/\mathbb{Q})$).

On notera pour toute la suite que ces congruences dans les algèbres de groupes signifient $\pmod{p\mathbb{Z}_{(p)}[G]}$ ou $\pmod{p\mathbb{Z}_{\chi,(p)}[G]}$ selon les cas, où \mathbb{Z}_{χ} est l'anneau des entiers du corps des valeurs C_{χ} des $\varphi|\chi$.

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 formelle de $\Delta^\chi = N_{C_\chi/\mathbb{Q}}\left(\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu\right)$.

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

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

(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 formelle de $\Delta^1 = \alpha + \alpha^\sigma + \alpha^{\sigma^2}$.

(ii) Les éléments $\eta \in K^\times$ tels que $N_{K/\mathbb{Q}}(\eta) = \eta^3$ (dans $F \otimes \mathbb{Q}$), donc tels que $\eta \in \mathbb{Q}^\times$, correspondent à la nullité formelle de $\Delta^\chi = N_{\mathbb{Q}(j)/\mathbb{Q}}(\alpha + j\alpha^\sigma + j^2\alpha^{\sigma^2})$.

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 $\eta^{e_1} = 1$ (i.e. de norme 1 dans $F \otimes \mathbb{Q}$) correspondent à la nullité formelle de $\Delta^1 = \text{Tr}_{K/\mathbb{Q}}(\alpha)$.

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

$$\Delta^{\chi_1} = \alpha + \alpha^\sigma + \alpha^{\sigma^2} - \alpha^\tau - \alpha^{\tau\sigma} - \alpha^{\tau\sigma^2} = (1 - \tau) \text{Tr}_{K/k}(\alpha).$$

(iii) Les éléments η tels que $\eta^{e_{\chi_2}} = 1$ sont les éléments de k^\times et conduisent à la nullité formelle de :

$$\begin{aligned} \Delta^{\chi_2} = \alpha^2 + \alpha^{2\sigma} + \alpha^{2\sigma^2} - \alpha^{2\tau} - \alpha^{2\tau\sigma} - \alpha^{2\tau\sigma^2} - \alpha\alpha^\sigma - \alpha^\sigma\alpha^{\sigma^2} - \alpha^{\sigma^2}\alpha \\ + \alpha^\tau\alpha^{\tau\sigma} + \alpha^{\tau\sigma}\alpha^{\tau\sigma^2} + \alpha^{\tau\sigma^2}\alpha^\tau. \end{aligned}$$

2.3. Définition des \mathbb{F}_p -régulateurs. — Soit $\eta \in K^\times$ et soit p assez grand. On a les congruences suivantes (cf. §2.1) :

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

Par commodité on fixe un nombre algébrique $\alpha \in Z_K$ défini par $\alpha \equiv \alpha_p(\eta) \pmod{p}$. On obtient le déterminant de Frobenius à coefficients dans Z_K :

$$\Delta_p^G(\eta) := \det(\alpha^{\tau\sigma})_{\sigma, \tau \in G}.$$

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 2.11). On considère donc :

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

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

Les Δ^χ sont les χ -régulateurs formels et les p -entiers rationnels $\Delta_p^\chi(\eta)$ (définis modulo p) les résultats de leur spécialisation (au facteur \sqrt{m} près dans le cas quadratique). Ils se factorisent au moyen des \mathbb{F}_p -régulateurs $\Delta_p^\theta(\eta)$:

Définition 2.17. — Pour tout p assez grand et pour chaque caractère \mathbb{Q}_p -irréductible θ de G , on appelle \mathbb{F}_p -régulateur de η associé à θ , l'entier p -adique $\Delta_p^\theta(\eta) := \prod_{\varphi|\theta} P^\varphi(\dots, \alpha^\nu, \dots)$. Pour $\theta|\chi$ (χ fixé), ces \mathbb{F}_p -régulateurs dépendent de la décomposition de p dans C_χ/\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)).

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

$$R_p^\theta(\eta) = \prod_{\varphi|\theta} P^\varphi\left(\dots, \frac{-1}{p}\log(\eta^\nu), \dots\right).$$

On a alors les congruences $R_p^\theta(\eta) \equiv \Delta_p^\theta(\eta) \pmod{p}$; ainsi on a $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ si et seulement si p divise $R_p^\theta(\eta)$; mais dans ce cas $p^{\varphi(1)}$ divise $R_p^G(\eta)$ puisque $R_p^G(\eta) = \prod_\theta R_p^\theta(\eta)^{\varphi(1)}$, où chaque fois $\varphi|\theta$ (cf. § 2.2.1).

Remarque 2.19. — (i) Dans le cas Abélien, $\Delta_p^\chi(\eta) := N_{C_\chi/\mathbb{Q}}\left(\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu\right)$ ($\varphi|\chi$ fixé, d'ordre $d|n$), avec la convention sur la notation $N_{C_\chi/\mathbb{Q}}$, notamment lorsque K et C_χ ne sont pas linéairement disjoints.

De même $\Delta_p^\theta(\eta) := N_{\mathfrak{p}}\left(\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu\right) \in \mathbb{Z}_{\mathfrak{p}}$, où pour $\mathfrak{p}|p$ dans L (ou C_χ), $N_{\mathfrak{p}}$ désigne la norme locale dans le complété de C_χ en \mathfrak{p} (on retrouve $\Delta_p^\chi(\eta)$ comme produit de normes locales).

(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 $\Delta_p^\theta(\eta) = \Delta_p^{\theta'}(N_{K/K'}(\eta))$ où θ' est le caractère fidèle issu de θ .

Quitte à remplacer η par $\eta' := N_{K/K'}(\eta)$ on peut toujours supposer que θ est un caractère fidèle.

2.4. Cas des χ -régulateurs pour χ d'ordre 1 ou 2. — Soit $\eta \in K^\times$ et soit $\alpha \equiv \alpha_p(\eta) \pmod{p}$, $\alpha \in \mathbb{Z}_K$.

(i) Si $\chi = \theta = 1$, le \mathbb{F}_p -régulateur correspond à $N_{K/\mathbb{Q}}(\eta) = a \in \mathbb{Q}^\times$ et est donné par $\text{Tr}_{K/\mathbb{Q}}(\alpha)$, autrement dit :

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

Le programme PARI correspondant est le suivant (pour $a = 659$) :⁽⁷⁾

```
{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 χ 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 \mathbb{F}_p -régulateur qui correspond au cas où $N_{K/k}(\eta) \in k^\times \setminus \mathbb{Q}^\times$; si $\text{Tr}_{K/k}(\alpha) =: u + v\sqrt{m} \in k$, il est donné par :

$$\Delta_p^\chi(\eta) \equiv 2v\sqrt{m} \pmod{p}.$$

⁽⁷⁾ Dans tous les programmes PARI [PARI] proposés, la compatibilité avec TeX oblige à écrire les symboles *par*, *&*, *hfill*, avec un antislash, à placer des $\$$ et des $\{ \}$ pour les exposants...

Si K est un corps quadratique réel d'unité fondamentale ε , en raison de la relation de dépendance multiplicative $\varepsilon^{1+\sigma} = \pm 1$, le \mathbb{F}_p -régulateur $\Delta_p^1(\varepsilon)$ est formellement nul. Le \mathbb{F}_p -régulateur pour le caractère quadratique est $\Delta_p^X(\varepsilon) = 2v\sqrt{m}$ (calculé via $\varepsilon^{p^{2p}-1} \equiv 1 + pv\sqrt{m} \pmod{p^2}$).

Au moyen du programme PARI ci-dessous on calcule le \mathbb{F}_p -régulateur $\Delta_p^X(\varepsilon)$ 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 $\eta = a + b\sqrt{m} \in K^\times \setminus \mathbb{Q}^\times$ de norme quelconque :

```
{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)^(8); if(rp == 0, print(p)))).}
```

On ne trouve un \mathbb{F}_p -régulateur $\Delta_p^X(\varepsilon)$ 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 et les deux régulateurs formels sont non nuls. 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 $\Delta_p^X(\eta) \equiv 0 \pmod{p}$ sont $p = 11, 37, 163, 4219$.

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

Pour $\eta = 1 + 5\sqrt{-1}$ de norme 26, on trouve pour $\chi \neq 1$ les deux solutions $p = 73, 12021953$.

Pour $\eta = 1 + \sqrt{-1}$, le \mathbb{Z} -rang de F est 1 car on a $(1 + \sqrt{-1})^4(1 - \sqrt{-1})^{-4} = 1$ et de fait η peut être remplacé par 2 pour le calcul des p -quotients de Fermat.

Pour le nombre d'or $\frac{1+\sqrt{5}}{2}$ 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 $\alpha = \alpha_p(\eta)$ (défini modulo p) ; on peut toujours supposer que $\alpha \in Z_K$ ou au moins $\alpha \in Z_{K,(p)}$. 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 α .

3.1. \mathbb{F}_p -indépendance. — 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 $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$, dans l'anneau $Z_{K,(p)}$ des p -entiers de K , implique $u(\nu) \equiv 0 \pmod{p}$ pour tout $\nu \in G$. On dira (cf. Définition 3.3) que toute relation $U = \sum_{\nu \in G} u(\nu) \nu$ associée à α est nulle modulo $pZ_{(p)}[G]$. Ceci est indépendant du choix du représentant α .

On a le résultat élémentaire suivant où l'on rappelle que $\Delta_p^G(\eta) = \det(\alpha^{\tau\sigma})_{\sigma,\tau}$ et que p est supposé assez grand :

⁽⁸⁾ Attention, exceptionnellement on doit prendre le coefficient de $x = \sqrt{m}$ et non le terme constant.

Proposition 3.1. — (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 $\Delta_p^G(\eta)$ est étranger à p .

Démonstration. — Si α est une $\mathbb{Z}_{(p)}$ -base normale de $Z_{K,(p)}$, toute relation de la forme $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$, 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 $\sum_{\nu \in G} r(\nu) \alpha^\nu = 0$ avec des entiers $r(\nu)$ non tous nuls, tels que $\text{p.g.c.d.}(r(\nu)) = 1$; 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 un entier rationnel d étranger à $\text{p.g.c.d.}(r(\nu))$ tel que $d\beta = \sum_{\nu \in G} r(\nu) \alpha^\nu$, $r(\nu) \in \mathbb{Z}$. 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. On prend p assez grand ne divisant pas le discriminant de K/\mathbb{Q} , alors 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 $\Delta_p^G(\eta) = \det(\alpha^{\tau\sigma})_{\sigma, \tau \in G}$.

Si $\Delta_p^G(\eta) \not\equiv 0 \pmod{p}$, toute relation $\mathbb{Z}_{(p)}$ -linéaire sur les lignes, de la forme $\sum_{\sigma \in G} \lambda(\sigma) (\dots, \alpha^{\tau\sigma}, \dots)_\tau \equiv (\dots, 0, \dots)_\tau \pmod{p}$, $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, implique $\lambda(\sigma) \equiv 0 \pmod{p}$ pour tout $\sigma \in G$, ou encore, la condition $\sum_{\sigma \in G} \lambda(\sigma) \alpha^{\tau\sigma} \equiv 0 \pmod{p}$ pour tout $\tau \in G$, implique $\lambda(\sigma) \equiv 0 \pmod{p}$ pour tout $\sigma \in G$. Par conjugaison cette condition est équivalente au fait que $\sum_{\sigma \in G} \lambda(\sigma) \alpha^\sigma \equiv 0 \pmod{p}$ avec $\lambda(\sigma) \in \mathbb{Z}_{(p)}$, implique $\lambda(\sigma) \equiv 0 \pmod{p}$ pour tout $\sigma \in G$ (\mathbb{F}_p -indépendance des α^ν). \square

Corollaire 3.2. — Si pour p assez grand l'un au moins des \mathbb{F}_p -régulateurs $\Delta_p^\theta(\eta)$ est divisible par 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 $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$ non tous divisibles par p .

Cette relation admet, dans K^\times , le relèvement $\eta_1^{\sum_{\nu \in G} u(\nu) \nu} := \prod_{\nu \in G} (\eta^\nu)^{u(\nu)} \equiv 1 \pmod{p^2}$, où l'on a posé $\eta_1 = \eta^{p^{np}-1} \equiv 1 \pmod{p}$ (cf. § 2.1).

Nous allons préciser les propriétés des θ -composantes (pour les caractères p -adiques θ) de la relation $U = \sum_{\nu \in G} u(\nu) \nu$, 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 $C \subseteq \mathbb{Q}(\mu_g)$ une extension contenant les valeurs des caractères absolument irréductibles φ de G et soit $Z_{C,(p)}$ l'anneau des p -entiers de C . On suppose pour simplifier que $K \cap C = \mathbb{Q}$. On notera $Z_{\chi,(p)} := Z_{C_\chi,(p)} \subseteq Z_{C,(p)}$ l'anneau des valeurs, sur $\mathbb{Z}_{(p)}$, des $\varphi | \theta | \chi$, pour tout caractère rationnel irréductible χ .

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 $C[G]$, et par $\text{End}(V_\varphi) \simeq e_\varphi C[G]$ 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).

Définition 3.3. — (i) Si $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$, on parlera de la *relation associée* $U = \sum_{\nu \in G} u(\nu) \nu \in \mathbb{Z}_{(p)}[G]$, des φ -relations $U_\varphi := e_\varphi \cdot U$ à coefficients dans $Z_{\chi, (p)}$, des θ -relations $U_\theta := e_\theta \cdot U$ à coefficients dans \mathbb{Z}_p , ou encore des χ -relations $U_\chi := e_\chi \cdot U$ à coefficients dans $\mathbb{Z}_{(p)}$ (cf. Définition 2.14). Quel que soit l'anneau \mathcal{Z} des coefficients, les écritures sont considérées modulo $p\mathcal{Z}$.

(ii) On désigne par \mathcal{L} le G -module des relations $U \in \mathbb{Z}_p[G]$ modulo p relatives à α . C'est un idéal de $\mathbb{Z}_p[G]$. 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 $\alpha = 0$.

(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 $U = \sum_{\nu \in G} u(\nu) \nu \in \mathcal{L}$. On a $U_\varphi = \sum_{\nu \in G} u_\varphi(\nu) \nu$, $u_\varphi(\nu) = \frac{\varphi(1)}{n} \sum_{\tau \in G} u(\tau^{-1}\nu) \varphi(\tau^{-1}) \in Z_{\chi, (p)}$, pour tout $\nu \in G$. Comme on a $\varphi(s) = \varphi(t^{-1}st)$ pour tout $s, t \in G$, on a aussi (en posant $\tau = \nu t \nu^{-1}$), $u_\varphi(\nu) = \frac{\varphi(1)}{n} \sum_{\tau \in G} u(\nu \tau^{-1}) \varphi(\tau^{-1})$, pour tout $\nu \in G$.

On a $U_\theta = \sum_{\varphi|\theta} U_\varphi \in \mathbb{Z}_p[G]$ pour le caractère p -adique irréductible θ au-dessus de φ , avec $U_\theta = \sum_{\nu \in G} u_\theta(\nu) \nu$, où $u_\theta(\nu) = \frac{\varphi(1)}{n} \sum_{\tau \in G} u(\tau^{-1}\nu) \theta(\tau^{-1}) \in \mathbb{Z}_p$.

Puisque $U_\varphi = e_\varphi U_\theta$ et $U_\theta = \sum_{\varphi|\theta} U_\varphi$, on a $U_\theta \equiv 0 \pmod{p}$ si et seulement si $U_\varphi \equiv 0 \pmod{p}$ pour au moins un caractère $\varphi|\theta$ (auquel cas ceci a lieu par conjugaison pour tout $\varphi|\theta$). Ceci ne vaut que si $U \in \mathcal{L}$.

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

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

Lemme 3.5. — Soit φ irréductible tel que $U_\varphi \not\equiv 0 \pmod{p}$. Alors l'endomorphisme $E_\varphi := e_\varphi \sum_{\nu \in G} \alpha^\nu \nu \in \text{End}(V_\varphi) \simeq e_\varphi C[G]$ est non inversible modulo p .

Démonstration. — Considérons $U_\varphi^* := \sum_{\sigma \in G} u_\varphi(\sigma) \sigma^{-1} \in Z_{\chi, (p)}[G]$ (on a $U_\varphi^* \not\equiv 0 \pmod{p}$) ; calculons l'image de U_φ^* par l'endomorphisme E_φ ; on a :

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

d'après le Lemme 3.4 par conjugaisons par τ . \square

Remarque 3.6. — Comme E_φ est un endomorphisme de V_φ sur KC , il existe un idéal premier \mathfrak{P} de KC au-dessus de p tel que $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{P}}$. Mais toute conjugaison par $\tau \in G$ donne $E_\varphi^\tau = e_\varphi \sum_{\nu \in G} \alpha^{\tau\nu} \nu = (e_\varphi \tau^{-1}) \cdot e_\varphi \sum_{\nu \in G} \alpha^\nu \nu$, et on obtient $\det(E_\varphi^\tau) = \det(e_\varphi \tau^{-1}) \det(E_\varphi) \equiv 0 \pmod{\mathfrak{P}^\tau}$, d'où $\det(E_\varphi) \equiv 0 \pmod{\prod_{\tau \in G} \mathfrak{P}^\tau}$ puisque les $\det(e_\varphi \tau^{-1})$ sont inversibles.

Donc il existe un idéal premier $\mathfrak{p} | p$ de Z_χ tel que $\det(E_\varphi) \equiv 0 \pmod{\mathfrak{p}}$, ce qui conduit à $P^\varphi(\dots, \alpha^\nu, \dots) \equiv 0 \pmod{\mathfrak{p}}$, donc à $\Delta_p^\varphi(\eta) \equiv 0 \pmod{\mathfrak{p}}$. Comme $\Delta_p^\theta(\eta)$ est dans le \mathfrak{p} -complété du corps de décomposition, qui est \mathbb{Q}_p , on peut écrire $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ pour le caractère p -adique θ au-dessus de φ (cf. Définition 2.5)

Lemme 3.7. — Si l'endomorphisme $E_\varphi := e_\varphi \sum_{\nu \in G} \alpha^\nu \nu \in \text{End}(V_\varphi)$ est non inversible modulo p , alors il existe une φ -relation $W = \sum_{\sigma \in G} w(\sigma) \sigma^{-1} \in e_\varphi Z_{\chi, (p)}[G]$, $W \notin p Z_{\chi, (p)}[G]$, qui est dans le noyau de E_φ .

Démonstration. — Soit $Z_{\chi, K}$ l'anneau des entiers du corps $C_\chi K$. Il existe donc $W \in e_\varphi Z_{\chi, K}[G]$ tel que $W \not\equiv 0 \pmod{p}$ est dans le noyau de E_φ . Écrivons $W = \sum_{\sigma \in G} w(\sigma) \sigma^{-1}$, $w(\sigma) \in Z_{\chi, K}$. L'égalité $E_\varphi \cdot W = 0$ s'écrit alors :

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

En multipliant cette égalité par $\tau \in G$ on obtient :

$$\sum_{\sigma \in G} w(\sigma) \sum_{s \in G} \alpha^{s\sigma} \tau s \equiv \sum_{\sigma \in G} w(\sigma) \sum_{t \in G} \alpha^{\tau^{-1}t\sigma} t \equiv 0 \pmod{p}, \quad \forall \tau \in G,$$

équivalente par conjugaison à $\sum_{\sigma \in G} w(\sigma)^\tau \sum_{t \in G} \alpha^{t\sigma} t \equiv 0 \pmod{p}$, pour tout $\tau \in G$.

Par utilisation du Lemme 2.2 et en prenant la trace on obtient une relation non triviale de la forme suivante (les coefficients dans $Z_{\chi, (p)}$ sont encore notés $w(\sigma)$ par abus) :

$$\sum_{t \in G} \left(\sum_{\sigma \in G} w(\sigma) \alpha^{t\sigma} \right) t \equiv 0 \pmod{p};$$

d'où $\sum_{\sigma \in G} w(\sigma) \alpha^{t\sigma} \equiv 0 \pmod{p}$, pour tout $t \in G$, puis $\sum_{\sigma \in G} w(\sigma) \alpha^\sigma \equiv 0 \pmod{p}$, ce qui donne la φ -relation non triviale $\sum_{\sigma \in G} w(\sigma) \sigma \in e_\varphi \mathcal{L}$ dans le noyau de E_φ . \square

3.2.2. Un cas particulier. — Dans le G -module \mathcal{L} , considérons $U = \sum_{\nu \in G} u(\nu) \nu$.

On dispose par “conjugaison” des n relations :

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

non nécessairement \mathbb{F}_p -indépendantes, au sens des combinaisons linéaires des n vecteurs $(\dots, u(\tau^{-1}\nu), \dots)_{\nu \in G}$, $\tau \in G$, vus dans \mathbb{F}_p^n .

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

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

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 $\eta' = N_{K/K'}(\eta)$, $r := u(s^{-1})$ (d'ordre d modulo p), où s est générateur dans $\text{Gal}(K'/\mathbb{Q})$, on est ramené à une relation de la forme $\sum_{i=1}^d r^{-i} \alpha'^{s^i} \equiv 0 \pmod{p}$ avec $\alpha' = \text{Tr}_{K/K'}(\alpha)$. Ceci traduit la nullité modulo p de $\Delta_p^{\theta'}(\eta')$ pour un caractère θ' convenable de K' .

Corollaire 3.9. — *Si le G -module \mathcal{L} des relations $\sum_{\nu \in G} u(\nu) \nu \in \mathbb{Z}_{(p)}[G]$ 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 $\Delta_p^{\theta'}(\eta') \equiv 0 \pmod{p}$ où θ' est le caractère fidèle issu de θ .*

Remarque 3.10. — Comme $d \mid p - 1$, 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 car $N_{C_\chi/\mathbb{Q}}(\zeta - r) = \Phi_d(r)$, où Φ_d est le d -ième polynôme cyclotomique, et comme r est d'ordre d modulo p , $\Phi_d(r) \equiv 0 \pmod{p}$. On a $\sum_{i=0}^{d-1} \varphi(s^{-i}) \beta^{s^i} \equiv \sum_{i=0}^{d-1} r^{-i} \beta^{s^i} \equiv 0 \pmod{\mathfrak{p}}$, ce qui identifie le couple (θ, \mathfrak{p}) et donne $\Delta_p^\theta(\eta) \equiv \sum_{i=0}^{d-1} r^{-i} \beta^{s^i} \pmod{p}$ (cf. Définition 2.5 (ii)), alors que $\Delta_p^\chi(\eta) = N_{C_\chi/\mathbb{Q}}(\sum_{i=0}^{d-1} \varphi(s^{-i}) \beta^{s^i}) \equiv 0 \pmod{p}$.

3.2.3. Résultats principaux. — Les résultats techniques des §§ 3.2.1, 3.2.2 conduisent à l'énoncé suivant :

Proposition 3.11. — *Soit $\eta \in K^\times$ et soit θ un caractère p -adique irréductible de G . On a $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ si et seulement si $\mathcal{L}^\theta \neq \{0\}$ dans $\mathbb{F}_p[G]$ (cf. Définition 3.3 (iii)).*

Démonstration. — (i) Si $\mathcal{L}^\theta \neq \{0\}$, il existe $U = \sum_{\nu \in G} u(\nu) \nu \in \mathcal{L}$ tel que $U_\theta \not\equiv 0 \pmod{p}$. D'après le Lemme 3.5 et la Remarque 3.6, on a $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$.

(ii) Supposons que $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$; par la nullité modulo p de $\Delta_p^G(\eta)$ qui en résulte, il existe une relation de \mathbb{F}_p -dépendance de la forme $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$, $u(\nu) \in \mathbb{Z}_{(p)}$ non tous divisibles par p , et on a $U = \sum_{\nu \in G} u(\nu) \nu \in \mathcal{L}$, mais il convient de montrer que $U_\theta \not\equiv 0 \pmod{p}$.

Le cas Abélien (cf. § 5.1) sera résolu de façon plus précise. D'après le Lemme 3.7, pour un caractère irréductible $\varphi \mid \theta$, on a une φ -relation non triviale de la forme $W := \sum_{\sigma \in G} w(\sigma) \sigma$, $w(\sigma) \in Z_{\chi, (p)}$. Mais rien ne prouve que $W = e_\varphi U$, $U \in \mathcal{L}$.

Soit L le corps de décomposition de p dans C_χ/\mathbb{Q} et soit $D = \text{Gal}(C_\chi/L)$. Si $\{z, \dots, z^f\}$ 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 $\sum_{\nu \in G} \sum_{i=1}^f a_i(\nu) z^i \alpha^\nu \equiv 0 \pmod{p}$; donc par identification sur la base des z^i on obtient le système de relations :

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

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

Puisque W est non triviale, les $r_{\mathfrak{p}}^i(\nu)$ ne sont pas tous nuls modulo p et il existe au moins une relation non triviale $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \nu$ (pour un $i \in \{1, \dots, f\}$ et un $\mathfrak{p} \mid p$). Comme W est une φ -relation, ceci se transmet à $\sum_{\nu \in G} a_i(\nu) \nu$ et par conséquent $\sum_{\nu \in G} r_{\mathfrak{p}}^i(\nu) \nu$ est une θ -relation non triviale de \mathcal{L} . \square

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

Ce qui précède conduit à l'énoncé suivant (où p est supposé assez grand) :

Théorème 3.13. — Soit K/\mathbb{Q} une extension Galoisienne de groupe de Galois G . Soit $\eta \in K^\times$; on suppose que le $\mathbb{Z}[G]$ -module engendré par η est de \mathbb{Z} -rang $n = |G|$ (i.e. $F \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$). Pour tout p on pose $\eta_1 := \eta^{p^{n-1}} = 1 + p\alpha_p(\eta)$, $\alpha_p(\eta) \in Z_K$, 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.,

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

On a alors les résultats suivants :

(i) Il existe au moins 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 $R_p^G(\eta)$ est divisible par p (cf. Remarque 2.18).

(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, le G -module $\mathcal{L}^\theta := e_\theta \mathcal{L}$ est de \mathbb{F}_p -dimension non nulle (et alors multiple de $f\varphi(1)$) si et seulement si le \mathbb{F}_p -régulateur $\Delta_p^\theta(\eta)$ (cf. § 2.3) est divisible par p .

(iii) Si $\dim_{\mathbb{F}_p}(\mathcal{L}) = 1$, alors θ est un caractère 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 $\eta' := N_{K/K'}(\eta)$, $d = [K' : \mathbb{Q}]p - 1$, où $r \in \mathbb{Z}$ et s générateur de $\text{Gal}(K'/\mathbb{Q})$ sont tels que $\theta(s) \equiv r \pmod{p}$ (cf. Lemme 3.8, Corollaire 3.9 et Remarque 3.10).

Corollaire 3.14. — (i) Lorsque $\mathcal{L}^\theta \neq \{0\}$, on obtient des relèvements de la forme $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$ pour toute θ -relation $U_\theta \in \mathcal{L}^\theta$ (cf. Corollaire 3.2).

(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 $\eta_1^{U_\theta} = (1 + p\alpha)^{U_\theta} \equiv 1 + pU_\theta \cdot \alpha \pmod{p^2}$, et comme $U_\theta \cdot \alpha \equiv 0 \pmod{p}$ par définition, il vient : $\eta_1^{U_\theta} = 1 + p^2\beta \equiv (1 + p\beta)^p \pmod{p^3}$, avec $\beta \in Z_{K,(p)}$. Donc $\eta_1^{U_\theta} = (1 + p\gamma)^p$, $\gamma \in \prod_{v|p} K_v^\times$, et $\eta = \eta^{p^{n-1}} \eta_1^{-1}$ implique $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$. Le cas (ii) est immédiat. \square

Remarque 3.15. — D'après la Remarque 2.19 (ii), le fait de remplacer η par $\eta' = N_{K/K'}(\eta)$ 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 pour montrer de quoi il s'agit. Il résulte de ce qui précède que l'on peut trouver indifféremment une θ -relation $\sum_{\sigma \in G} u(\sigma) \sigma$ à coefficients p -entiers rationnels, ou, pour $\varphi|\theta$, une φ -relation $\sum_{\sigma \in G} u_\varphi(\sigma) \sigma$ à coefficients dans $Z_{\chi,(p)}$.

Exemple 3.16. — Pour un corps cubique cyclique, on a $e_\chi = \frac{1}{3}(2 - \sigma - \sigma^2)$.

(i) Si p est inerte dans $\mathbb{Q}(j)/\mathbb{Q}$, $\chi = \theta = \varphi + \varphi^s$, $f = 2$, et on montrera (cf. § 4.6) que l'on obtient les θ -relations indépendantes $\alpha - \alpha^\sigma \equiv 0 \pmod{p}$ et $\alpha^\sigma - \alpha^{\sigma^2} \equiv 0 \pmod{p}$, qui sont conjuguées ($f = 2$).

Donc $U = 1 - \sigma$ est telle que (pour $\varphi(\sigma) = j$) :

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

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}^φ associée à la relation $\alpha + j^{-1}\alpha^\sigma + j^{-2}\alpha^{\sigma^2} \equiv 0 \pmod{p}$. 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 $\alpha + r^{-1}\alpha^\sigma + r^{-2}\alpha^{\sigma^2} \equiv 0 \pmod{p}$ 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'un des deux idéaux premiers $\mathfrak{p} | p$ associé à $\theta = \varphi$) à :

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

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

Le conjugué 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 $\alpha + r^{-2}\alpha^\sigma + r^{-1}\alpha^{\sigma^2} \equiv 0 \pmod{p}$, ce qui conduirait à $\alpha \equiv \alpha^\sigma \equiv \alpha^{\sigma^2} \pmod{p}$ (probabilité $\frac{1}{p^2}$).

Exemple 3.17. — Prenons le cas d'un exemple numérique (cf. § 6.1, 6.1.4) avec le corps K défini par le polynôme $Q = x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31$ (groupe de Galois D_6), pour $\chi = \theta = \chi_2$ de degré 2.

Pour $p = 61$, $\eta = x^5 - 2x^4 + 4x^3 - 3x^2 + x - 1$, on obtient le G -module \mathcal{L} engendré par les trois relations \mathbb{F}_p -linéaires indépendantes, conjuguées (par σ et σ^2) :

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

Il est clair que 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 la nullité modulo p du \mathbb{F}_p -régulateur $\Delta_p^{\chi_1}(\eta)$).

Pour $\theta = \chi$ (de degré 2), le \mathbb{F}_p -régulateur $\Delta_p^\theta(\eta)$ est nul modulo p 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. En effet, pour la θ -relation définie ci-dessus :

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

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 supposons que le groupe F engendré par les conjugués de η est de \mathbb{Z} -rang $n = |G|$ (afin qu'il n'y ait pas de régulateurs formellement nuls, ce cas étant sans intérêt pour l'étude de $\Delta_p^G(\eta)$ nul modulo p pour tout p).

Ensuite, il est entendu que nous négligerons les premiers p pour lesquels au moins deux \mathbb{F}_p -régulateurs sont divisible par p , en admettant qu'une telle probabilité est au plus en $\frac{O(1)}{p^2}$, vu l'indépendance des \mathbb{F}_p -régulateurs associés à deux caractères p -adiques différents (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 -adique θ de G sous réserve d'un \mathcal{L}^θ minimal (le cas contraire pour \mathcal{L}^θ étant très rare).

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

Définition 3.18. — Un nombre premier p assez grand est dit à *décomposition minimale* (relativement à $\eta \in K^\times$) s'il existe un unique θ tel que $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ pour lequel p est totalement décomposé dans le corps C_χ des valeurs de $\varphi|\theta$ (cas qui contient celui où $C_\chi = \mathbb{Q}$) et si la représentation $\mathcal{L}^\theta \simeq \delta V_\theta$ est de \mathbb{F}_p -dimension minimale $\varphi(1)$ (i.e., $\delta = 1$).

Dans le cas Abélien il s'agit des $p \equiv 1 \pmod{n}$ où n est l'ordre de θ .

Nous reviendrons Section 7 sur ce type de cas en envisageant certaines conjectures.

4. Considérations probabilistes

4.1. Généralités. — En l'absence d'arguments théoriques précis, il est d'usage de supposer que le cas $R_p^\theta(\eta) \equiv 0 \pmod{p}$ se produit avec la probabilité $\frac{1}{p}$. Il en résulte alors que le nombre de solutions $p < B$ serait en $\sum_{p < B} \frac{1}{p}$, donc en $\log \log(B)$, et de même pour la nullité modulo p de $R_p^G(\eta) = \prod_\theta R_p^\theta(\eta)^{\varphi(1)}$ qui serait en $\frac{O(1)}{p}$.

Or il est évident que puisque $R_p^\theta(\eta)$ est une norme locale dans l'extension C_χ/\mathbb{Q} , un tel régulateur 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 $p^{\varphi(1)}$ intervient également puisque $R_p^\theta(\eta) = \prod_{\varphi|\theta} R_p^\varphi(\eta)$ est élevé à la puissance $\varphi(1)$ (où $R_p^\varphi(\eta)$ est un polynôme homogène de degré $\varphi(1)$ en les α^σ). Cependant il n'est pas clair pour autant que la "probabilité" d'être divisible par p (ou que la densité des cas observés) soit de façon précise fonction de $\frac{1}{p^f}$ et/ou $\frac{1}{p^{\varphi(1)}}$.

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 au carré sous la forme $\frac{1}{p^{\delta^2 f}}$. En outre il faut mesurer le fait que les $R_p^\theta(\eta)$ sont indépendants.

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

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

(ii) la probabilité en $\frac{1}{p}$ d'avoir la nullité modulo p de $\Delta_p^\theta(\eta)$ pour le caractère $\theta = \chi_2$ de degré 2 de D_6 , 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 .

Le programme calcule les conjugués de α 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);
```


$F1 = \text{component}(E1, 2); F2 = \text{component}(E2, 2); F3 = \text{component}(E3, 2);$
 $F4 = \text{component}(E4, 2); F5 = \text{component}(E5, 2); F6 = \text{component}(E6, 2);$
 $SP = F1 + F2 + F3; SM = F4 + F5 + F6; FP = SP + SM; FM = SP - SM;$
 $RP = E1^2 + E2^2 + E3^2 - E4^2 - E5^2 - E6^2 - E1 * E2 - E2 * E3 - E3 * E1$
 $+ E4 * E5 + E5 * E6 + E6 * E4;$

$if(FP == 0, N1 = N1 + 1);$
 $if(FM == 0, N2 = N2 + 1);$
 $if(RP == 0, N3 = N3 + 1);$
 $if(FP == 0 \& FM == 0, N12 = N12 + 1);$
 $if(FP == 0 \& RP == 0, N13 = N13 + 1);$
 $if(FM == 0 \& RP == 0, N23 = N23 + 1);$
 $if(FP == 0 \& FM == 0 \& RP == 0, N123 = N123 + 1));$
 $print("p = ", p, ", ", "N1 = ", N1, ", ", "N2 = ", N2, ", ", "N3 = ", N3, ", ",$
 $(N1 + 0.0)/N0, ", ", (N2 + 0.0)/N0, ", ", (N3 + 0.0)/N0);$
 $print("N12 = ", N12, ", ", "N13 = ", N13, ", ", "N23 = ", N23, ", ", "N123 = ", N123, ", ",$
 $(N12 + 0.0)/N0, ", ", (N13 + 0.0)/N0, ", ", (N23 + 0.0)/N0, ", ", (N123 + 0.0)/N0);$
 $print(", ", "1/p = ", 1./p, ", ", "1/p^2 = ", 1./p^2, ", ", "1/p^3 = ", 1./p^3)}$

Pour $p = 13$ on obtient les valeurs suivantes :

$N_0 = 999115 ; N_1 = 76820 ; N_2 = 77009 ; N_3 = 82239 ;$
 $N_{12} = 5898 ; N_{13} = 6301 ; N_{23} = 6453 ; N_{123} = 442,$

ce qui donne 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 :

$N_0 = 999952 ; N_1 = 27153 ; N_2 = 27054 ; N_3 = 27747 ;$
 $N_{12} = 718 ; N_{13} = 761 ; N_{23} = 755 ; N_{123} = 16,$

ce qui donne les densités respectives :

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

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

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 1 ou 2.

4.3. Principe d'analyse. — 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 χ -régulateurs formellement nuls).

On considère le G -module \mathcal{L} engendré par les relations à coefficients p -entiers rationnels (cf. Définition 3.3). 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 $\mathcal{L}^\theta \simeq \delta V_\theta$ (cf. Proposition 3.11) 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 de $a = N_{K/\mathbb{Q}}(\eta)$. 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 § 7.4 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 $N_{K/\mathbb{Q}}(\eta) = a$ est indépendante de p et se transmet à $\alpha = \alpha_p(\eta)$ via la formule $\sum_{\nu \in G} \alpha^\nu \equiv q_p \pmod{p}$ qui constitue, pour $\theta = 1$, la θ -relation linéaire non triviale associée à la nullité modulo p de $\Delta_p^1(\eta)$ lorsque $q_p \equiv 0 \pmod{p}$.

On a vu également au § 4.2 que l'on pouvait implicitement supposer qu'il existe au plus un unique θ pour lequel $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$.

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

La difficulté probabiliste vient du fait que pour un caractère θ de degré $\varphi(1) \geq 2$, le \mathbb{F}_p -espace \mathcal{L}^θ est de dimension $\delta f \varphi(1)$, $0 \leq \delta \leq \varphi(1)$, où f est le degré résiduel de θ . De plus, si on a une relation, les relations conjuguées ne sont plus "probabilistes".

Pour introduire cet aspect statistique par le calcul, nous illustrons numériquement le cas cubique cyclique, § 4.6, puis, Section 5, le cas Abélien en toute généralité. Dans la Section 6, nous traitons un cas non Abélien via le groupe D_6 .

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

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

Bien que la correspondance entre η modulo p^2 (η étranger à p) et $\alpha \equiv \frac{-1}{p} \log(\eta)$ 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 $\theta = 1$ 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 !

Il est clair d'un point de vue p -adique que, pour tout θ , 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 (limitation obligatoire lorsque p est très grand).

(ii) Si $(e_i)_{i=1, \dots, n}$ est une $\mathbb{Z}_{(p)}$ -base de $Z_{K,(p)}$ et si l'on pose $\alpha = \sum_{i=1}^n A_i e_i$, $A_i \in \mathbb{Z}_{(p)}$, 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 $\sum_{\nu \in G} u(\nu) \alpha^\nu \equiv 0 \pmod{p}$ 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).

(iv) La probabilité de $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ est celle de $\mathcal{L}^\theta \neq \{0\}$. Elle est induite par le nombre de relations $\mathbb{F}_p[G]$ -indépendantes. Compte tenu de la Remarque 3.12, si $\mathcal{L}^\theta \simeq \delta V_\theta$, $1 \leq \delta \leq \varphi(1)$, on verra que l'on doit affecter à ce cas une probabilité en $\frac{O(1)}{p^{\delta^2 f}}$, où f est le degré résiduel de θ . Le cas non trivial le plus fréquent est $\delta = 1$ (f dépend trivialement de p contrairement à δ qui est "numérique").

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

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

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

$$\tau U_1 = U_1, \tau\sigma U_1 = \sigma^2 U_1, \tau\sigma^2 U_1 = \sigma U_1, \tau U_2 = \sigma U_2, \tau\sigma U_2 = U_2, \tau\sigma^2 U_2 = \sigma^2 U_2.$$

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 $\delta = 1$ mais en $\frac{O(1)}{p^4}$ pour $\delta = 2$ (très bien confirmé par les statistiques numériques).

4.4. Statistiques à partir du 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 $(A_i(\nu))_{i,\nu}$ doit être de \mathbb{F}_p -rang strictement inférieur à n .

Nous avons vu, et nous le justifierons encore, que la probabilité de nullité modulo p de $\Delta_p^\theta(\eta)$ seul est $\frac{1}{p^f}$, où f est le degré résiduel de θ (i.e., celui de p dans C_χ/\mathbb{Q}) ; comme il y a $h = \frac{|C_\chi:\mathbb{Q}|}{f}$ tels caractères p -adiques $\theta \mid \chi$, la probabilité d'avoir au moins un $\Delta_p^\theta(\eta)$ nul modulo p est $\frac{h}{p^f}$. 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 (avec des notations évidentes), la probabilité théorique d'obtenir une matrice de \mathbb{F}_p -rang $< n$ est donnée par :

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

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 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 \mathbb{F}_p -régulateurs relatifs à deux caractères p -adiques ($p = 31$ totalement décomposé), et deux seulement parmi les cinq, à savoir par exemple :

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

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; 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 = matranks(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 congruences modulo p car on a $C_X = \mathbb{Q}$:

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

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 $\Delta_p^{X^1}(\eta)$ 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}^θ de dimension 4).

$\{Q = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + 31; p = 17; p2 = p^2;$
 $e1 = x;$
 $e2 = 11/180 * x^5 + 1/180 * x^4 + 11/18 * x^3 - 1/45 * x^2 + 403/180 * x + 419/180;$
 $e3 = 13/180 * x^5 - 7/180 * x^4 + 13/18 * x^3 - 38/45 * x^2 + 509/180 * x + 127/180;$
 $e4 = -4/45 * x^5 + 1/45 * x^4 - 8/9 * x^3 + 26/45 * x^2 - 137/45 * x - 91/45;$
 $e5 = -1/60 * x^5 - 1/60 * x^4 - 1/6 * x^3 - 4/15 * x^2 - 73/60 * x - 79/60;$
 $e6 = -1/36 * x^5 + 1/36 * x^4 - 5/18 * x^3 + 5/9 * x^2 - 65/36 * x + 11/36;$
 $N0 = 0; N6 = 0;$
 $for(i = 1, 50000, a = random(p2); b = random(p2); c = random(p2); aa = random(p2);$
 $bb = random(p2); cc = random(p2);$
 $Eta = Mod(a * e1^5 + b * e1^4 + c * e1^3 + aa * e1^2 + bb * e1 + cc, Q);$
 $N = norm(Eta); if(Mod(N, p) != 0, N0 = N0 + 1;$
 $u = Mod(a, p2); v = Mod(b, p2); w = Mod(c, p2); uu = Mod(aa, p2);$
 $vv = Mod(bb, p2); ww = Mod(cc, p2);$
 $P = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + Mod(31, p);$
 $P2 = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + Mod(31, p2);$
 $y = Mod(u * x^5 + v * x^4 + w * x^3 + uu * x^2 + vv * x + ww, P2);$
 $z = y^{(p-1)}; t = z; for(i = 1, 5, z = z^p * t);$
 $U = component(z - 1, 2);$
 $u1 = component(U, 1); if(u1 == 0, u1 = Mod(0, p2));$
 $u2 = component(U, 2); if(u2 == 0, u2 = Mod(0, p2));$
 $u3 = component(U, 3); if(u3 == 0, u3 = Mod(0, p2));$
 $u4 = component(U, 4); if(u4 == 0, u4 = Mod(0, p2));$
 $u5 = component(U, 5); if(u5 == 0, u5 = Mod(0, p2));$
 $u6 = component(U, 6); if(u6 == 0, u6 = Mod(0, p2));$
 $x1 = component(u1, 2)/p; x2 = component(u2, 2)/p; x3 = component(u3, 2)/p;$
 $x4 = component(u4, 2)/p; x5 = component(u5, 2)/p; x6 = component(u6, 2)/p;$
 $X1 = Mod(x1, p); X2 = Mod(x2, p); X3 = Mod(x3, p);$
 $X4 = Mod(x4, p); X5 = Mod(x5, p); X6 = Mod(x6, p);$
 $E1 = Mod(X1 + X2 * e1 + X3 * e1^2 + X4 * e1^3 + X5 * e1^4 + X6 * e1^5, P);$
 $E2 = Mod(X1 + X2 * e2 + X3 * e2^2 + X4 * e2^3 + X5 * e2^4 + X6 * e2^5, P);$
 $E3 = Mod(X1 + X2 * e3 + X3 * e3^2 + X4 * e3^3 + X5 * e3^4 + X6 * e3^5, P);$
 $E4 = Mod(X1 + X2 * e4 + X3 * e4^2 + X4 * e4^3 + X5 * e4^4 + X6 * e4^5, P);$
 $E5 = Mod(X1 + X2 * e5 + X3 * e5^2 + X4 * e5^3 + X5 * e5^4 + X6 * e5^5, P);$
 $E6 = Mod(X1 + X2 * e6 + X3 * e6^2 + X4 * e6^3 + X5 * e6^4 + X6 * e6^5, P);$
 $F1 = component(E1, 2); F2 = component(E2, 2); F3 = component(E3, 2);$
 $F4 = component(E4, 2); F5 = component(E5, 2); F6 = component(E6, 2);$
 $GG = [F1, F2, F3, F4, F5, F6];$
 $DD = (F1 + F2 + F3)^2 - (F4 + F5 + F6)^2;$
 $RP = E1^2 + E2^2 + E3^2 - E4^2 - E5^2 - E6^2 - E1 * E2 - E2 * E3 - E3 * E1$
 $+ E4 * E5 + E5 * E6 + E6 * E4;$
 $if(RP == 0 & DD != 0, N1 = N1 + 1;$
 $M = matrix(6, 6, i, j, component(component(GG, i), j)); r = matranks(M);$

```

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. Analyse locale du problème. — Il reste cependant à vérifier le caractère de “variables aléatoires indépendantes” de A_1, \dots, A_n ; nous ne donnerons que deux exemples numériques ($G = C_3$ et $G = D_6$), 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 strictement aléatoires.

Le programme ci-dessous considère des entiers aléatoires $\eta = ax^2 + bx + c$ modulo p^2 , étrangers à p ; il est clair que, algébriquement, $\frac{-1}{p} \log(\eta)$ donne une fois et une seule 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 $\Delta_p^X(\eta) \equiv 0 \pmod{p}$. L'utilisateur 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 $\Delta_p^X(\eta) \equiv 0 \pmod{p}$, 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 $\frac{2}{p}$ (le facteur 2 venant de l'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 :

```
{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 3 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. Etude directe à partir de corps cubiques cycliques. — Pour introduire le cas Abélien général (cf. Section 5), nous détaillons le cas de corps cubiques cycliques K définis par les polynômes irréductibles (“simplest cubic fields” de Shanks [Sh]) $P_t := X^3 - tX^2 - (t+3)X - 1$, $t \in \mathbb{Z}$, 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 $D_t = (t^2 + 3t + 9)^2$. 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 $\eta = ax^2 + bx + c$, $a, b, c \in \mathbb{Z}_{(p)}$. On peut vérifier facilement que sur cette base :

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

Donc si $\eta = ax^2 + bx + c$, 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 groupe engendré par η et ses conjugués. Le calcul de $\eta^{p^{np}-1} = 1 + p\alpha_p(\eta)$ conduit à $\alpha_p(\eta) \equiv Ax^2 + Bx + C \pmod{p}$, $A, B, C \in \mathbb{Z}_{(p)}$. Nous allons supposer F de \mathbb{Z} -rang 3 et nous intéresser au caractère χ d’ordre 3.

Posons $\alpha = \alpha_p(\eta)$, $\alpha' = \alpha_p(\eta)^\sigma$, $\alpha'' = \alpha_p(\eta)^{\sigma^2}$; on rappelle que pour χ d’ordre 3, le \mathbb{F}_p -régulateur est :

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

4.6.1. Exemples numériques. — Donnons d’abord des exemples numériques (au moyen du programme PARI écrit au § 4.6.4) :

(i) Cas p inerte dans $\mathbb{Q}(j)$. Pour $t = 41$, on a $P_t = X^3 - 41X^2 - 44X - 1$, et son discriminant est $D = 1813 = 7^2 \cdot 37$. Prenons $\eta = 3x^2 - 2x + 6$ dont la norme est $353731 = 7^2 \cdot 7219$.

On trouve, pour $\Delta_p^X(\eta) \equiv 0 \pmod{p}$, 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 $\eta^{5^3-1} \equiv 1 + 5 \cdot 3 \pmod{25}$). L’ensemble des conjugués de α est astreint à vérifier deux relations 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 $\eta = 3x^2 - 2x + 6$ dont la norme est 66739. On obtient une unique solution $p < 10^9$, à $\Delta_p^X(\eta) \equiv 0 \pmod{p}$, qui est $p = 1309963$ (décomposé dans $\mathbb{Q}(j)$). Les données numériques sont :

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

On vérifie que les 3 mineurs :

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

sont nuls modulo p .

Pour $r = 160549$, d'ordre 3 modulo p , on a les relations suivantes entre les couples de coefficients de x et x^2 :

$$\begin{aligned} (294668, 143675) &\equiv r(366345, 117217) \pmod{p}, \\ (648950, 1049071) &\equiv r(294668, 143675) \pmod{p}, \\ (366345, 117217) &\equiv r(648950, 1049071) \pmod{p}. \end{aligned}$$

Ceci donne l'unique relation (donnant la nullité modulo p d'un $\Delta_p^\theta(\eta)$) :

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

4.6.2. *Analyse théorique des exemples précédents pour le \mathbb{Z} -rang 3.* — La nullité de $\Delta_p^X(\eta)$ modulo p s'écrit :

$$\Delta_p^X(\eta) \equiv N_{K(j)/K}(\alpha - \alpha'' - j(\alpha'' - \alpha')) \equiv 0 \pmod{p}.$$

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

$$\begin{aligned} \alpha' &= Ax'^2 + Bx' + C =: A'x^2 + B'x + C', \\ \alpha'' &= Ax''^2 + Bx'' + C =: A''x^2 + B''x + C'', \end{aligned}$$

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 :

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

On en déduit que l'ensemble des relations modulo p entre A, B, C conduit à la probabilité cherchée (cf. § 4.3.2).

Considérons le schéma suivant et supposons $\Delta_p^X(\eta) \equiv 0 \pmod{p}$:

$$\begin{array}{ccc} \alpha, \alpha', \alpha'' \in K & \xrightarrow{\langle s \rangle} & K(j) \quad \mathfrak{P} \\ \downarrow & & \downarrow \langle \sigma \rangle \\ \mathbb{Q} & \xrightarrow{\quad} & \mathbb{Q}(j) \quad \mathfrak{p} \end{array}$$

Puisque $\Delta_p^X(\eta) = N_{K(j)/K}(\alpha + j^{-1}\alpha' + j^{-2}\alpha'') = N_{K(j)/K}(\alpha - \alpha - j(\alpha' - \alpha'')) \equiv 0 \pmod{p}$, 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) :

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

et de même avec \mathfrak{P}^{σ^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 4.6.1 (i)). D'où une probabilité en $\frac{O(1)}{p^2}$. 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 $\alpha - \alpha' - r(\alpha' - \alpha'') \equiv 0 \pmod{p}$ (étendu à K).

Notons que ceci signifie que $\alpha - \alpha' - j(\alpha' - \alpha'')$ est seulement dans l'idéal \mathfrak{p} (étendu à K) et non nécessairement dans \mathfrak{p}^s . Ceci conduit dans K à :

$$\Delta_p^\theta(\eta) \equiv \alpha + r^{-1}\alpha' + r^{-2}\alpha'' \equiv 0 \pmod{p}.$$

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

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

En utilisant les relations précédentes :

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

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 4.6.1 (ii). On a obtenu une relation entre A et B (probabilité en $\frac{2}{p}$).

4.6.3. *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 relation formelle $\alpha + \alpha' + \alpha'' \equiv 0 \pmod{p}$ (provenant de $N_{K/\mathbb{Q}}(\eta) = \pm 1$). 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 régulateur plus simple :

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

qui, au facteur 3 près, s'écrit $\Delta_p^\chi(\eta) = N_{K(j)/K}(\alpha - j\alpha')$.

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 $\alpha \equiv \alpha' \equiv \alpha'' \equiv 0 \pmod{p}$ du cas inerte (i) vu pour le \mathbb{Z} -rang 3 deviennent ici $\alpha \equiv 0 \pmod{p}$ puisque $\alpha + \alpha' + \alpha'' \equiv 0 \pmod{p}$).

4.6.4. *Programme PARI général.* — Ce programme, valable pour les \mathbb{Z} -rangs 2 et 3, peut s'utiliser en modifiant les valeurs de t, a, b, c ; 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, " ", "p mod 3 = ", 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. Méthode générale directe pour le cas Abélien

5.1. Généralités. — On peut supposer que G est cyclique d'ordre $n \geq 2$ et que χ est le caractère rationnel de G d'ordre n ; soit ζ une racine primitive n -ième de l'unité. On a ici $C_\chi = \mathbb{Q}(\zeta)$ et $\Delta_p^\chi(\eta) = N_{K(\zeta)/K} \left(\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu \right)$, pour $\varphi | \chi$ fixé.

La condition $\Delta_p^\chi(\eta) \equiv 0 \pmod{p}$ implique par des raisonnements connus (cf. Corollaire 2.7 et Proposition 3.11) :

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

Soient L le corps de décomposition de p dans $\mathbb{Q}(\zeta)/\mathbb{Q}$ et $D = \text{Gal}(\mathbb{Q}(\zeta)/L)$; on désigne par f le degré résiduel en p . Alors $\{\zeta, \dots, \zeta^f\}$ est une L -base de $\mathbb{Q}(\zeta)$

(et une KL -base de $K(\zeta)$). Posons $\varphi(\nu^{-1}) = \sum_{i=1}^f a_i(\nu^{-1}) \zeta^i$, $a_i(\nu^{-1}) \in Z_{L,(p)}$

pour tout $\nu \in G$. Il vient $\sum_{\nu \in G} \varphi(\nu^{-1}) \alpha^\nu = \sum_{i=1}^f \zeta^i \sum_{\nu \in G} a_i(\nu^{-1}) \alpha^\nu \equiv 0 \pmod{\mathfrak{p}}$.

Comme il y a inertie dans $K(\zeta)/KL$, il en résulte $\sum_{\nu \in G} a_i(\nu^{-1}) \alpha^\nu \equiv 0 \pmod{\mathfrak{p}}$, pour $i = 1, \dots, f$, en voyant ici \mathfrak{p} dans L étendu à LK .

Il existe alors des p -entiers rationnels $r_i(\nu^{-1})$ tels que $a_i(\nu^{-1}) \equiv r_i(\nu^{-1}) \pmod{\mathfrak{p}}$ dans L , ce qui conduit à $\sum_{\nu \in G} r_i(\nu^{-1}) \alpha^\nu \equiv 0 \pmod{\mathfrak{p}}$, $i = 1, \dots, f$; d'où finalement $\sum_{\nu \in G} r_i(\nu^{-1}) \alpha^\nu \equiv 0 \pmod{p}$, $i = 1, \dots, f$.

La matrice $(r_i(\nu^{-1}))_{\nu \in G, 1 \leq i \leq f}$ est de \mathbb{F}_p -rang f ; en effet, soit $H = \{\nu_1, \dots, \nu_f\}$ un sous-ensemble de G tel que $\varphi(\nu_i^{-1}) = \zeta^i, i = 1, \dots, f$; alors la matrice $(a_j(\nu_i^{-1}))_{i,j}$ est la matrice unité I_f d'ordre f .

Il en résulte un système de f relations indépendantes (cf. Théorème 3.13 (ii, iii)) définissant \mathcal{L}^θ pour un caractère p -adique $\theta | \chi$ (cf. Définitions 2.5 (ii) et 3.3 (ii)) :

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

correspondant à une probabilité en $\frac{O(1)}{p^f}$. De fait, chacun des $h = [L : \mathbb{Q}]$ régulateurs $\Delta_p^\theta(\eta)$ a une probabilité de nullité égale à $\frac{1}{p^f}$. On peut donc se limiter aux cas $f = 1$.

Remarque 5.1. — Considérons le cas p totalement décomposé dans $\mathbb{Q}(\zeta)/\mathbb{Q}$, correspondant à $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ caractères p -adiques. Soit s un générateur de G et soit $\varphi(s) \equiv r \pmod{\mathfrak{p}}$ dans $\mathbb{Q}(\zeta)$, ce qui fixe le caractère θ . On a donc la seule relation $\sum_{i=1}^n r^{-i} \alpha^{s^i} \equiv 0 \pmod{p}$.

Soit $\{e^\sigma, \sigma \in G\}$ une $\mathbb{Z}_{(p)}$ -base normale de $Z_{K,(p)}$ et soit $\alpha = \sum_{\tau \in G} A_\tau e^\tau, A_\tau \in \mathbb{Z}_{(p)}$. Alors $\sum_{\nu \in G} r(\nu)^{-1} \alpha^\nu = \sum_{\tau \in G} A_\tau \sum_{\sigma \in G} r(\tau\sigma^{-1})^{-1} e^\sigma \equiv 0 \pmod{p}$; d'où $\sum_{\tau \in G} r(\tau\sigma^{-1})^{-1} A_\tau \equiv 0 \pmod{p}$ pour tout $\sigma \in G$. De par la congruence $r(\tau\sigma^{-1})^{-1} \equiv \varphi(\tau^{-1}\sigma) = \varphi(\tau^{-1})\varphi(\sigma) \pmod{\mathfrak{p}}$ on voit immédiatement que la matrice $(r(\tau\sigma^{-1})^{-1})_{\sigma,\tau}$ est seulement de rang 1.

On est donc ramené à la relation analogue $\sum_{\tau \in G} r(\tau)^{-1} A_\tau \equiv 0 \pmod{p}$.

Le cas totalement décomposé conduit en première approximation à la probabilité la plus grande (en $\frac{O(1)}{p}$) car $f = \delta = 1$, mais on examinera § 7.4 un autre point de vue.

5.2. 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 $\mathbb{Q}(\mu_{11})$.

5.2.1. 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 :

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

qui correspond à l'ordre naturel 1, $\sigma, \sigma^2, \sigma^3, \sigma^4$, 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 $N_{K/\mathbb{Q}}(\eta) = -60589$, et les solutions pour $p < 10^7$ sont $p = 31, 101, 39451$, tous décomposés dans $\mathbb{Q}(\zeta_5)$. Considérons les données numériques pour $p = 31$:

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

Pour $r = 4$ qui est tel que $\zeta_5 \equiv r \pmod{\mathfrak{p}}$, on a immédiatement comme prévu :

$$\alpha + r^{-1}\alpha^\sigma + r^{-2}\alpha^{\sigma^2} + r^{-3}\alpha^{\sigma^3} + r^{-4}\alpha^{\sigma^4} \equiv 0 \pmod{p}$$

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 $N_{K/\mathbb{Q}}(\eta) = 303623$, 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 .

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 $\frac{1}{p^4}$.

(iii) Pour $aa = 10; bb = -7; cc = -3; dd = 1; ee = -2$, on a $N_{K/\mathbb{Q}}(\eta) = 1358171$, 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 $\alpha + \zeta_5\alpha^\sigma + \zeta_5^2\alpha^{\sigma^2} + \zeta_5^3\alpha^{\sigma^3} + \zeta_5^4\alpha^{\sigma^4}$ 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 $K(\zeta_5)$:

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

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 (θ, \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 :

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

qui vérifient le système de deux congruences ci-dessus.

On a les deux relations indépendantes $1 - \sigma^2 + 49(\sigma^4 - \sigma^3)$ & $\sigma^4 - \sigma + 49(\sigma^3 - \sigma^2)$, la seconde étant conjuguée par σ^4 de la première. D'où une probabilité en $\frac{2}{p^2}$ (deux choix pour la congruence $\sqrt{5} \equiv 20 \pmod{p}$).

5.2.2. *Calcul de la densité des $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$.* — Le programme ci-dessous reprend le cas précédent 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, 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);
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 : $N_1 = 17$, $\frac{N_1}{N_0} = 3.40 \cdot 10^{-5}$ pour $\frac{1}{p^4} = 3.50 \cdot 10^{-5}$.

6. Étude du cas du groupe D_6

6.1. Programme général pour 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 étudie donc les trois régulateurs, chaque fois supposés non formellement nuls.

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) Si $\Delta^1 \neq 0$, cela signifie que $N_{K/\mathbb{Q}}(\eta) = a \neq \pm 1$, auquel cas, $\Delta_p^1(\eta)$ est le p -quotient de Fermat de a .

(ii) Pour $\Delta^{X_1} \neq 0$, on a $N_{K/k}(\eta) \in k^\times \setminus \mathbb{Q}^\times$ et on suppose que :

$$\Delta_p^{X_1}(\eta) = \alpha + \alpha' + \alpha'' - \beta - \beta' - \beta'' \equiv 0 \pmod{p}.$$

Si $A = \alpha + \alpha' + \alpha'' =: u + v\sqrt{m}$, alors $\Delta_p^{X_1}(\eta) = A - A^\tau = 2v\sqrt{m} \equiv 0 \pmod{p}$; on a donc la seule condition $v \equiv 0 \pmod{p}$, ce qui conduit à une probabilité en $\frac{1}{p}$, la trace modulo p dans K/k étant surjective.

(iii) Pour $\Delta^{X_2} \neq 0$ (considéré au facteur \sqrt{m} près qui est étranger à p), on a $\eta \in K^\times \setminus k^\times$. On est donc dans le cas d'une représentation de degré 2, ce qui conduit, pour $\theta = \chi_2$, à la condition (cf. Exemple 2.9) :

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

Le calcul des trois $\mathcal{L}^{\theta'} \simeq \delta'V_{\theta'}$, $0 \leq \delta' \leq \varphi'(1)$, 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 $\Delta_p^{X_1}(\eta)$ est nul modulo p (sinon, la nullité supplémentaire de $\Delta_p^\theta(\eta)$ conduit pour le p considéré à une probabilité en $\frac{1}{p^2}$, et on peut exclure ce nombre premier).

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

6.1.1. Programme PARI pour D_6 et le calcul de $\Delta_p^\theta(\eta)$. — 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 :

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

$\{Q = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + 31; D = \text{poldisc}(Q);$

$e1 = x;$

$e2 = 11/180 * x^5 + 1/180 * x^4 + 11/18 * x^3 - 1/45 * x^2 + 403/180 * x + 419/180;$

$e3 = 13/180 * x^5 - 7/180 * x^4 + 13/18 * x^3 - 38/45 * x^2 + 509/180 * x + 127/180;$

$e4 = -4/45 * x^5 + 1/45 * x^4 - 8/9 * x^3 + 26/45 * x^2 - 137/45 * x - 91/45;$

$e5 = -1/60 * x^5 - 1/60 * x^4 - 1/6 * x^3 - 4/15 * x^2 - 73/60 * x - 79/60;$

$e6 = -1/36 * x^5 + 1/36 * x^4 - 5/18 * x^3 + 5/9 * x^2 - 65/36 * x + 11/36;$

$a = 1; b = -3; c = 0; aa = -7; bb = 1; cc = -1;$

$Eta = \text{Mod}(a * e1^5 + b * e1^4 + c * e1^3 + aa * e1^2 + bb * e1 + cc, Q);$

$N = \text{norm}(Eta); \text{print}(\text{"norme(eta) = "}, N); \text{print}(\text{""});$

$\text{for}(k = 3, 5 * 10^6, p = 2 * k + 1; \text{if}(\text{isprime}(p) == 1 \& \text{Mod}(D * N, p)! = 0, p2 = p^2);$

$u = \text{Mod}(a, p2); v = \text{Mod}(b, p2); w = \text{Mod}(c, p2);$

$uu = \text{Mod}(aa, p2); vv = \text{Mod}(bb, p2); ww = \text{Mod}(cc, p2);$

$P = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + \text{Mod}(31, p);$

$P2 = x^6 + 9 * x^4 - 4 * x^3 + 27 * x^2 + 36 * x + \text{Mod}(31, p2);$

$y = \text{Mod}(u * x^5 + v * x^4 + w * x^3 + uu * x^2 + vv * x + ww, P2);$

$z = y^{(p-1)}; t = z; \text{for}(i = 1, 5, z = z^p * t);$


```

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))))}

```

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

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

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

qui conduisent immédiatement aux deux θ -relations indépendantes :

$$\alpha - \alpha^\sigma + \alpha^\tau - \alpha^{\tau\sigma^2} \equiv 0 \pmod{p} \quad \& \quad \alpha - \alpha^{\sigma^2} + \alpha^\tau - \alpha^{\tau\sigma} \equiv 0 \pmod{p},$$

et leur relèvements :

$$\eta_1^{1-\sigma+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}, \quad \eta_1^{1-\sigma^2+\tau-\tau\sigma} \equiv 1 \pmod{p^2},$$

où $\eta_1 = \eta^{p^{np}-1}$. La seconde relation est la conjuguée par τ de la première.

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 :

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

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 :

$$\eta_1^{1-\sigma^2+\tau-\tau\sigma^2} \equiv 1 \pmod{p^2}, \quad \eta_1^{\sigma^2-\sigma+\tau\sigma-\tau} \equiv 1 \pmod{p^2}.$$

Dans ce cas, la seconde relation est la conjuguée par σ^2 de la première.

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) :

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

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

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

6.1.3. *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 :

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

Donc les trois \mathbb{F}_p -régulateurs sont nuls modulo p .

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

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

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 \mathbb{F}_p -régulateur $\Delta_p^\theta(\eta)$ est nul modulo p (voir Exemple 3.17 pour les détails numériques).

6.1.5. *Cas* $p = 7$, $\eta = 3x^5 - 20x^4 + 15x^3 + 16x^2 + 9x + 21$. — On obtient :

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

Ce cas où le G -module \mathcal{L}^θ est de \mathbb{F}_p -dimension 4 ($\mathcal{L}^\theta \simeq 2V_\theta \simeq e_\theta \mathbb{F}_p[G]$) est très rare, comme on l'a vu § 4.4, 4.4.3, car on doit prendre η de telle sorte que F soit de \mathbb{Z} -rang 6 et qu'aucun des χ -régulateurs, $\chi = 1, \chi_1$, ne soit nul modulo p , ce qui est le cas ici ; par conséquent il est facile de voir que cela correspond au cas

où pour un p particulier (ici $p = 7$), η est proche (modulo p^2) d'un élément non trivial du sous-corps quadratique de K (probabilité en $\frac{1}{p^4}$).

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

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

d'où les relations :

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

donnant la nullité modulo 13 de $\Delta_p^1(\eta)$ et de $\Delta_p^\theta(\eta) = \alpha - \alpha^{\sigma^2} - \alpha^\tau + \alpha^{\tau\sigma}$ (pour $\theta = \chi_2$), mais non celle de $\Delta_p^{\chi_1}(\eta)$.

Ceci montre que F est de \mathbb{Z} -rang 6.

Remarque 6.1. — Dans tous les exemples numériques précédents, on vérifie que les éléments $U_1 = \frac{1}{3}(1 - \sigma + \tau - \tau\sigma)$ et $U_2 = \frac{1}{3}(1 - \sigma^2 - \tau + \tau\sigma)$ de $e_\theta \mathbb{F}_p[G]$ (cf. Remarque 2.15) 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). Le \mathbb{F}_p -espace obtenu est de dimension $\delta\varphi(1)$, $1 \leq \delta \leq 2$, et la probabilité associée est en $\frac{O(1)}{p^{\delta^2}}$.

On peut aussi retrouver ces relations en considérant le déterminant $\Delta^\theta(\eta)$ (cf. Exemple 2.9) qui est de la forme $\begin{vmatrix} A & B \\ C & D \end{vmatrix}$ avec $A^{\tau\sigma} = -A$, $C^{\tau\sigma} = -C$, et $B^\sigma = -A$, $D^\sigma = -C$; comme il existe $\lambda \in K$ tel que $(A, B) = \lambda(C, D)$, il en résulte immédiatement que λ , invariant par G , est rationnel modulo p .

6.2. Interprétation locale concernant η . — L'idée est de voir dans quelle mesure η est, lorsque $\Delta_p^\theta(\eta) \equiv 0 \pmod{p}$ pour un caractère p -adique θ , "en partie" une puissance p -ième locale en p .

6.2.1. Cas G cyclique d'ordre n et θ de degré résiduel $f = 1$. — On a donc $n \mid p-1$ (décomposition minimale, d'après la Définition 3.18). Reprenons le résultat du

Corollaire 3.14 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 .

L'opérateur U_θ n'est pas inversible dans $\mathbb{F}_p[G]$ car on a $U_\theta(r-s) \equiv 0 \pmod{p}$, d'où l'interprétation suivante utilisant l'algèbre $\mathbb{Z}_{(p)}[\xi]$ où ξ est une racine primitive n -ième de l'unité convenable dans \mathbb{C} . On suppose $n > 2$.

On remarque que $e_\theta := \frac{1}{n} \sum_{k=0}^{n-1} r^{-k} s^k = \frac{1}{n} U_\theta$ est l'idempotent de $\mathbb{F}_p[G]$ correspondant au caractère p -adique θ défini par $\theta(s) \equiv r \pmod{p}$. L'application de $\mathbb{Z}_{(p)}[X]$ dans $e_\theta \mathbb{F}_p[G]$ qui à X associe $e_\theta s$ a pour noyau l'idéal maximal $(p, X - r)$; or le n -ième polynôme cyclotomique $\Phi_n(X)$ est dans cet idéal car $p \equiv 1 \pmod{n}$ est totalement décomposé dans $\mathbb{Q}(\mu_n)$. Donc par factorisation, on obtient un isomorphisme de $\mathbb{Z}_{(p)}[\xi]/(p, r - \xi)$ sur $e_\theta \mathbb{F}_p[G]$ qui à ξ associe $e_\theta s$, et où $\mathfrak{p} := (p, r - \xi)$ est un idéal premier de $\mathbb{Z}_{(p)}[\xi]$ au-dessus de p .

Le caractère φ issu de θ est tel que $\varphi(s) = \xi$; on considère, dans $K^\times \otimes C_\chi$, la φ -composante $K_\varphi^\times := (K^\times \otimes C_\chi)^{e_\varphi}$; alors $\xi = \varphi(s)$ opère par $y^\xi = y^s$, pour

tout $y \in K_\varphi^\times$, auquel cas l'écriture $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$ conduit à $\eta^{U_\theta(r-\xi)} = \lambda^{p(r-\xi)}$, $\lambda \in \prod_{v|p} K_v^\times$; comme dans $\mathbb{Z}_{(p)}[G]$ on a $U_\theta(r-s) = cp$, $c \in \mathbb{Z}_{(p)}^\times$ ⁽⁹⁾, il vient $\eta = \Lambda^{r-s}$ puisqu'il n'y a pas de p -torsion dans $\prod_{v|p} K_v^\times$ pour p assez grand. 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 § 7.1.1, § 7.1.2 qui reprennent cet aspect.

6.2.2. Cas d'un caractère de degré quelconque. — Le relèvement $\eta_1^{U_\theta} \equiv 1 \pmod{p^2}$ a lieu avec une θ -relation non triviale $U_\theta := \sum_{\nu \in G} u(\nu)\nu \in \mathcal{L}^\theta$. On a $\eta_1^{U_\theta} = (1+p\gamma)^p \in \prod_{v|p} K_v^{\times p}$, et la relation $\eta = \eta^{p^{np}} \eta_1^{-1}$ conduit à $\eta^{U_\theta} \in \prod_{v|p} K_v^{\times p}$, mais l'interprétation de η comme "puissance \mathfrak{p} -ième" dans $\prod_{v|p} K_v^\times$ n'est plus possible pour θ de degré > 1 . Dans la section suivante on considèrera cette écriture comme une propriété de "puissance p -ième locale partielle" (dans la mesure où $\mathcal{L}^\theta \neq \{0\}$), selon la définition suivante :

Définition 6.2. — 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 :

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

On dira que η est puissance p -ième locale partielle 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 $tf\varphi(1)$, $0 \leq t \leq \varphi(1) - 1$, où f est le degré résiduel de θ (cf. Définition 2.5 (ii)).

Remarque 6.3. — On a $F^p \subseteq F \cap K^{\times p} \subseteq F_0$. Comme par hypothèse on a $F \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$, et que F est sans p -torsion (p assez grand), on a $F/F^p \simeq \mathbb{F}_p[G]$ et même $F \cap K^{\times p} = F^p$ (en particulier, $\dim_{\mathbb{F}_p}(F/F^p)^{e_\theta} = f\varphi(1)^2$ pour tout θ par hypothèse). Donc la condition $\dim_{\mathbb{F}_p}(F/F_0) < n$ indique bien qu'il existe θ tel que la composante $(F/F_0)^{e_\theta}$ n'est pas maximale, donc qu'il existe $U_\theta \in e_\theta \mathbb{Z}_{(p)}[G]$ telle que η^{U_θ} est puissance p -ième locale en p , non puissance p -ième globale dans K^\times ; ce qui équivaut à $\dim_{\mathbb{F}_p}(\mathcal{L}^\theta) = \delta f\varphi(1)$, $\delta \geq 1$.

Remarque 6.4. — a) En résumé, l'obstruction fondamentale pour l'éventuelle finitude de l'ensemble des premiers p tels que $\Delta_p^G(\eta) \equiv 0 \pmod{p}$ provient des nombres premiers p à décomposition minimale, assez grands, à savoir (cf. Définition 3.18) :

- (i) il existe un unique caractère p -adique irréductible θ de G 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 $\varphi|\theta$ (cf. Théorème 3.13 et Corollaire 3.14), i.e. $f = 1$.
- (iii) la représentation \mathcal{L}^θ des θ -relations (cf. Définition 3.3 (iii)) est irréductible, ce qui est équivalent à $\dim_{\mathbb{F}_p}(\mathcal{L}^\theta) = \varphi(1)$ (i.e., $\delta = 1$).

b) L'hypothèse F de \mathbb{Z} -rang n n'est pas essentielle ; en son absence, il faut tenir compte des \mathbb{F}_p -régulateurs formellement nuls.

⁽⁹⁾ On peut toujours choisir r modulo p de telle sorte que $r^n - 1 \not\equiv 0 \pmod{p^2}$.

7. Conjectures et spéculations p -adiques

Nous proposons diverses conjectures en partant de la plus “évidente” (Conjecture 7.2) à condition d'admettre la conjecture ABC , pour aller vers des généralisations aux corps de nombres (Conjectures 7.4 et 7.7). L'obstruction essentielle étant les cas de probabilités en $\frac{1}{p}$ pour les p à décomposition minimale (cf. Définition 3.18 et Remarque 6.4) (cas du quotient de Fermat par exemple), nous proposons § 7.4 une approche pouvant modifier ce point de vue.

7.1. Retour sur le cas des caractères d'ordre 1 ou 2. — Nous revenons sur des cas particuliers déjà évoqués (cf. § 2.4).

7.1.1. Cas d'un rationnel. — On considère $K = \mathbb{Q}$ et un rationnel $a \neq \pm 1$. Si p est un nombre premier impair étranger à a , on a le résultat élémentaire suivant qui est un cas particulier du Corollaire 3.14 (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 $a = u^p$, $u \in \mathbb{Q}_p^\times$, $a^{p-1} = (u^{p-1})^p \equiv 1 \pmod{p^2}$. \square

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.⁽¹⁰⁾ L'étude statistique montre même 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 :

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

On peut considérer cet énoncé comme un principe local-global diophantien comme il en existe en théorie du corps de classes (alors purement algébriques comme le “principe de Hasse” pour les puissances appelé dans la Proposition 7.5 ci-après).

On sait que souvent ces principes restent valables lorsqu'on remplace “presque tout p ” par un ensemble infini (ou fini) convenable, mais non effectif en général. Citons par exemple une forme très simple (corps des rationnels) du théorème de Schmidt–Chevalley (ou 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 :*

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

⁽¹⁰⁾ Silverman prouve que pour tout $a \geq 2$, l'ensemble de ces nombres premiers $p \leq x$ est de cardinal $\gg \log(x)$. 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 $\gg \frac{\log(x)}{\log(\log(x))}$, toujours sous la conjecture ABC .

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 "aléatoires" tels que $a^{p-1} \equiv 1 \pmod{p^2}$, ceci est suffisant pour assurer que a est puissance p -ième dans \mathbb{Q}_p^\times pour presque tout p , donc (sous la conjecture 7.2) est égal à ± 1 .

7.1.2. 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 alors $m > 0$ et que η est une unité ε non triviale de $\mathbb{Q}(\sqrt{m})$ (nullité formelle de Δ^1) ; 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 encore 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'analogie de la Conjecture 7.2.

On peut envisager que ce processus est valable pour le cas général où $\eta \in K^\times$ serait "puissance p -ième locale partielle" pour une infinité de p au sens du § 6.2 (cf. Définition 6.2).

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

7.1.3. Conjecture générale sur les puissances p -ièmes locales. — Le cas rationnel (Conjecture 7.2) a montré la vraisemblance du type d'énoncé suivant qui correspond à l'écriture $\eta^{p^n-1} - 1 = p\alpha$ 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 θ) et une probabilité en $\frac{O(1)}{p^n}$, $n = |G|$, puisque $\sum_{\theta} f \varphi(1)^2 = \sum_{\varphi} \varphi(1)^2 = n$.

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 :

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) :

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 $v \notin \Sigma$, alors $\eta \in K^{\times p}$.⁽¹¹⁾*

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 $\eta \in K^{\times p}$.

⁽¹¹⁾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 formel général et un raisonnement nettement moins fort portant sur des ensembles "probabilistes" T finis.

La différence opère en deux temps pour la Conjecture 7.4 : partant de p et de l'ensemble \mathcal{P}_p des p -places de K , on commence par dire que η est puissance p -ième locale pour tout $v \in \mathcal{P}_p$ (i.e., on prend l'ensemble infini $\Sigma = \mathcal{P}_K \setminus \mathcal{P}_p$, où \mathcal{P}_K est l'ensemble des places de K , 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 $T = \mathcal{P}_p$), 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.

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

7.1.4. Cas particulier du groupe des unités – Spiegelungssatz. — Le cas où η est une unité 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 S .*

Si η vérifie la condition $\eta \in K_v^{\times p}$ pour toute place $v \in S \cup \mathcal{P}_p$, alors $\eta \in K^{\times p}$.

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

La Conjecture 7.4 porte seulement sur \mathcal{P}_p au lieu de $S \cup \mathcal{P}_p$ pour S fini bien choisi (ce qui est insuffisant pour avoir une puissance p -ième globale), mais on suppose dans la conjecture que cette hypothèse faible est vraie pour presque tout p .

En outre, les deux systèmes d'hypothèses coïncident si le p -groupe des classes du corps $K(\mu_p)$ 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 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} .

Si l'on est dans la situation où 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. § 6.2.2) 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 $\mathcal{C}_{K'}$ de la façon suivante : soit $\mathcal{C}_{K'}^{\mathcal{P}'_p}$ le quotient de $\mathcal{C}_{K'}$ 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 $s \in \text{Gal}(K'/K)$. Alors c'est la θ^* -composante de $\mathcal{C}_{K'}^{\mathcal{P}'_p}$ qui est non triviale.

Revenons à l'écriture $\eta_1 := \eta^{p^{n-1}} = 1 + p\alpha$, $\alpha \in Z_K$, 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 $\mathfrak{P} \mid p$ 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 en \mathfrak{P}'). 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 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 \mathbb{F}_p -régulateur $\Delta_p^\theta(\eta)$ ($\theta \neq 1$), est équivalente à l'existence d'une θ^* -extension non ramifiée p -décomposée de $K(\mu_p)$, 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 différente : prenons l'exemple de $a \in \mathbb{Q}^\times$, $a \neq \pm 1$. Alors la Proposition 7.5 n'est plus valable car elle ne s'applique que si l'idéal (a) est puissance p -ième d'idéal dans K , ce qui ne peut avoir lieu pour une infinité de p (contrairement aux unités), mais si $a^{p-1} \equiv 1 \pmod{p^2}$ l'extension $\mathbb{Q}'(\sqrt[p]{a})/\mathbb{Q}$ est non ramifiée (et décomposée) en p mais ramifiée en les places de \mathbb{Q}' divisant a ; si S 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 $H'^{S'}$ comme p -extension Abélienne non ramifiée en dehors des places de l'ensemble S' des idéaux premiers de \mathbb{Q}' au-dessus de S (ce dernier ne dépendant pas de p).

Or cette p -extension $H'^{S'}/\mathbb{Q}'$ est finie (c'est essentiellement un p -corps de rayon $K'_{\mathfrak{m}'}$, \mathfrak{m}' construit sur S') et joue donc un rôle analogue à celui de H' . Bien que l'aspect conjectural paraisse ici différent, l'infinitude de p donnant un p -quotient de Fermat nul modulo p , peut conduire à des raisonnements analogues.

7.2. Conjectures sur les \mathbb{F}_p -régulateurs $\Delta_p^\theta(\eta)$. — Les résultats de la Section 3 (Théorème 3.13 et Corollaire 3.14 généralisant en un sens le Lemme 7.1) invitent à proposer les conjectures suivantes plus fortes que celles du § 7.1, même si aucun cas particulier de preuve ne semble disponible actuellement.

Pour éviter le cas des χ -régulateurs formellement nuls (cf. Définition 2.14 (ii) et Remarque 2.15), on suppose que le G -module engendré par η est de \mathbb{Z} -rang n .

La première conjecture se justifie en raison de l'écriture de type "quotient de Fermat" : $\eta^{p^{np}-1} - 1 = p\alpha$, lorsque α satisfait à des relations de la forme $U_\theta \cdot \alpha \equiv 0 \pmod{p}$ avec $U_\theta \not\equiv 0 \pmod{p\mathbb{Z}_p[G]}$ (condition beaucoup plus faible que $U = 1$ qui correspond au " $\alpha \equiv 0 \pmod{p}$ " à la base de la conjecture 7.4).

Conjecture 7.7. — *Soit K/\mathbb{Q} une extension Galoisienne de degré n . Soit $\eta \in K^\times$ tel que le groupe engendré par η et ses conjugués soit de \mathbb{Z} -rang n . Si pour une infinité de p , η est une puissance p -ième locale partielle (cf. Définition 6.2), alors η est une racine de l'unité de K .*

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

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 groupe engendré par η et ses conjugués soit de \mathbb{Z} -rang n , et soit $R_p^G(\eta)$ le régulateur p -adique normalisé de η . Alors pour tout premier p assez grand $R_p^G(\eta)$ est une unité p -adique.*

Remarque 7.9. — (i) 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.

(ii) Si η et ses conjugués n'engendrent pas un groupe de rang maximum, ceci veut dire que certains χ -régulateurs sont formellement nuls et la conjecture ne porte alors que sur les autres χ -régulateurs (cf. §2.2.4).

(iii) Pour le régulateur classique du groupe des unités d'un corps K réel, le caractère unité n'entre pas en jeu, et pour un corps quadratique réel la conjecture de Leopoldt est triviale, mais le fait que pour l'unité fondamentale ε , $p^{-1} \log(\varepsilon)$ soit une unité p -adique pour tout p assez grand, reste conjectural même pour un seul corps quadratique fixé (comme $\mathbb{Q}(\sqrt{2})$).

7.3. Conjectures en p -ramification Abélienne. — Soit $H_{(p)}^{\text{pra}}$ 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 $\mathcal{T}_p = \text{Gal}(H_{(p)}^{\text{pra}}/\widehat{K}_{(p)})$. Dans ce cas, pour tout p assez grand, $|\mathcal{T}_p|$ a même valuation p -adique que le régulateur normalisé $p^{1-n} \text{Reg}_{K,p}$ du corps K (voir [Gr2] pour des compléments sur ces questions).

Alors la Conjecture 7.8 implique la conjecture suivante (au moins pour les corps réels, mais toute partie “—” éventuelle est trivialement finie) :

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

Une conjecture nettement plus faible consiste à dire que pour tout p assez grand, $|\mathcal{T}_p| \sim p^{1-n} \text{Reg}_{K,p} \sim \prod_{\theta \neq 1} R_p^\theta(\varepsilon)^{\varphi(1)}$ (où ε est une unité de Minkowski fixée) est soit trivial soit égal à $p^{\varphi(1)}$ (à une unité p -adique près), en raison d'un unique facteur $R_p^\theta(\varepsilon)$ divisible par p avec $\theta \neq 1$ de degré résiduel $f = 1$ et \mathcal{L}^θ irréductible (i.e., décomposition minimale de p , cf. Définition 3.18). En effet, une divisibilité strictement plus grande 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 $\delta^2 f \geq 2$, où δ est le nombre de représentations irréductibles V_θ dans \mathcal{L}^θ (probabilité en $\frac{O(1)}{p^{\delta^2 f}}$). A fortiori, le cas $p^e \mid R_p^\theta(\varepsilon)$, avec $e \geq 2$, est possible, mais de probabilité en $\frac{O(1)}{p^e}$.

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 $R_p^\theta(\varepsilon)$ (ou $\Delta_p^\theta(\varepsilon)$) est divisible par p pour $p \equiv 1 \pmod{d}$ où d est l'ordre de θ .

Remarque 7.11. — On en déduirait aussi des propriétés analogues sur le résidu de la fonction zêta p -adique, au moins pour un corps totalement réel (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) ; on aurait alors conjecturalement $\frac{\zeta_K(2-p)}{\zeta_{\mathbb{Q}}(2-p)} \sim |\mathcal{T}_p| \sim 1$ pour p assez grand.

7.4. Analyse probabiliste alternative pour $q_p(a) \equiv 0 \pmod{p}$. — Soit $a \in \mathbb{Q}^\times$, $a \neq \pm 1$ fixé. Soit $p > 2$ un nombre premier étranger à a (de toutes façons p assez grand selon le point de vue adopté). Soit $m \mid p-1$ 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 :

$$\Phi_m(a) = \prod_{t \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})} (a - \xi^t)$$

qui est dans $p\mathbb{Z}_{(p)}$, où Φ_m est le m -ième polynôme cyclotomique. Si $a = \frac{u}{v}$, $\Phi_m(a) = v^{-\phi(m)} \prod_t (u - v \xi^t)$, et seul le numérateur $A := \prod_t (u - v \xi^t)$ est concerné.

Puisque dans le corps $\mathbb{Q}(\xi)$, p est totalement décomposé, il existe un unique idéal premier $\mathfrak{p} | p$ de $\mathbb{Q}(\xi)$ tel que $(u - v \xi) = \mathfrak{p} \mathfrak{a}$, où \mathfrak{a} est un idéal entier de $\mathbb{Q}(\xi)$.

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 écarte de \mathfrak{a}). Autrement dit, si l'on pose :

$$A = \prod_{k=1}^e \ell_k^{n_k}, \ell_1 < \ell_2 < \dots < \ell_e,$$

tous les premiers ℓ_k sont congrus à 1 modulo m , et p est l'un des plus petits $\ell \equiv 1 \pmod{m}$ a priori possibles (le plus petit si $m = p - 1$).

Il existe une suite finie $\{p_j, j = 1, \dots, g\}$ de nombres premiers $p_j \equiv 1 \pmod{m}$, susceptibles d'être des ℓ_k divisant A ; ils sont limités par la condition $p_g \leq A$ (cas possible si A est un nombre premier) et d'autres conditions car si A n'est pas premier, il faut tenir compte de la borne \sqrt{A} , etc. Dans ce contexte, on peut conjecturer que les p_j d'un certain ordre de grandeur sont tous a priori possibles, comme diviseurs de A , avec une probabilité qui est sans doute une fonction strictement décroissante de j , mais qui ne donne aucun avantage particulier à p . Considérons l'exemple numérique suivant :

$p = 101$, $a = 5$ qui est d'ordre 25 modulo p . On a $\Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$. D'où $\Phi_{25}(5) = 95397958987501 = 101 \times 251 \times 401 \times 9384251$, ce qui donne :

$$A = 944534247401 = 251 \times 401 \times 9384251$$

(tous les diviseurs sont congrus à 1 modulo $m = 25$). On voit alors que si l'on considère $p' = 251$, alors $\Phi_{25}(5) = p' \times 101 \times 401 \times 9384251$ qui conduit à une symétrie entre les probabilités de nullités modulo p et p' de $q_p(5)$ et $q_{p'}(5)$.

Le nombre g des premiers p_j est très grand, mais si l'on attribuait à chacun la probabilité $\frac{1}{p_j}$ de diviser A , il semble qu'on aboutirait à des contradictions numériques vu la présence assez systématique de grands nombres premiers, comme le montre le petit extrait PARI suivant avec $p = 101$ et $5 \leq a \leq 16$ (5 est ramifié) :

```
{for(a = 5, 30, for(i = 26, 26, p = prime(i); if(Mod(a, p)! = Mod(0, p),
m = znorder(Mod(a, p)); P = polcyclo(m); x = a; A = eval(P)/p;
print(a, "", m, "", factor(A))))})}
```

a	m	A
5	25	[251, 1; 401, 1; 9384251, 1]
6	10	[11, 1]
7	100	[5, 1; 13001, 1; 25301, 1; 38327966300231909291101, 1]
8	100	[5, 1; 1201, 1; 8101, 1; 63901, 1; 268501, 1; 13334701, 1; 1182468601, 1]
9	50	[5, 1; 394201, 1; 61070817601, 1]
10	4	[1, 0]
11	100	[2248313994601, 1; 1993099906542710819727884501, 1]
12	100	[5, 1; 1201, 1; 700936801, 1; 2334798291701, 1; 14807687049800501, 1]
13	50	[57751, 1; 3258254426373251, 1]
14	10	[5, 1; 71, 1]
15	100	[1801, 1; 115201, 1; 5276658969583784209292870346873232901, 1]
16	25	[5, 1; 251, 1; 601, 1; 1801, 1; 4051, 1; 8101, 1; 268501, 1]

Les cas où A est divisible par le carré d'un nombre premier ℓ sont rarissimes ; on a trouvé par exemple $a = 14$, $p = 29$, $m = 28$, $A = 29^2 \times 3361 \times 176597$, ce qui donne donc $q_{29}(14) \equiv 0 \pmod{29}$.

Plus généralement, considérons la fonction $\tilde{\Phi}_m(a) := \frac{\Phi_m(a)}{\text{p.g.c.d.}(\Phi_m(a), m)}$ destinée à éliminer les facteurs premiers ramifiés qui n'interviennent pas dans l'étude. De même, les diviseurs premiers de a ne divisent pas les $\tilde{\Phi}_m(a)$.

Le produit sur $m \geq 1$ des $\tilde{\Phi}_m(a)$ semble avoir des propriétés de régularité intéressantes. Considérons l'aspect numérique donné par le programme suivant :

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

Pour $a = 14$, on obtient $\prod_{m=1}^{40} \tilde{\Phi}_m(a) =$

3×5×11×13×17×19×23×29²×31×37×41×43×47×61×67×71×79×101×103×113×137×157×191×193×
197×211×223×397×461×547×811×911×937×1033×1061×2347×2851×3361×3761×4027×5393×7307×
10627×13109×15511×16097×18973×26981×61001×100621×132049×176597×698521×761437×
1154539×1383881×1948981×2249861×7027567×8108731×14525237×51111761×110256001×
1427145211×1475750641×2239000891×11737870057×25581350023×29914249171×141405986837×
299113818931×56693904845761×77312552100349×758855846709601×11284732320255809×14837
638311110071×22771730193675277×396530555859061913×459715689149916492091×39211413
30646275580183×77720275181800334933851×2984619585279628795345143571×62233081779326
83558580086481×26063080998214179685167270877966651.

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 $\tilde{\Phi}_m(a)$ pour l'unique l'indice m égal à l'ordre de 14 modulo p . Seul 29 est au carré ; le programme du § 2.4. donne pour $p < 10^9$ les deux solutions 29 ($m = 28$) et 353 ($m = 352$). Toute autre expérimentation numérique est analogue.

Ces observations sont très insuffisantes, mais la probabilité $\frac{1}{p}$ paraît tout aussi arbitraire car on est dans un cadre multiplicatif (comment factoriser A) et non dans une structure additive de résidus modulo p . Or dès qu'elle serait par exemple en $\frac{1}{p^{1+\epsilon}}$, 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 bien conscience du fait que les conjectures ci-dessus 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 $\frac{O(1)}{p^2}$, on ne voit pas bien la possibilité d'une infinité de solutions p puisque la somme des $\frac{1}{p^2}$ est très petite ($\sum_{p \geq 2} \frac{1}{p^2} = 0.45$, $\sum_{p \geq 100} \frac{1}{p^2} = 0.0018$, et $\sum_{p \geq 10000} \frac{1}{p^2} = 9.10^{-6}$). De toutes façons il reste le cas des nombres premiers p à *décomposition minimale* (cf. Définition 3.18 ou Remarque 6.4), en nombre infini avec une densité connue via le théorème de Chebotarev, c'est-à-dire lorsqu'un unique caractère p -adique irréductible 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 et que le G -module \mathcal{L}^θ est minimal.

Dans ce cas, le “nombre prévisible” de solutions $p < B$ est a priori en $O(1)\log\log(B)$ sur le seul plan analytique, sauf si les remarques du § 7.4 aboutissent 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.

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>
- [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.
- [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>
- [PARI] 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>
- [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.