Publ. Mat. **61** (2017), 475–515
DOI: 10.5565/PUBLMAT6121706

SUR LA SÉPARATION DES CARACTÈRES PAR LES FROBENIUS

Charlotte Euvrard et Christian Maire

Abstract: In this paper, we are interested in the question of separating two characters of the absolute Galois group of a number field K, by the Frobenius of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We first recall an upper bound for the norm $\mathrm{N}(\mathfrak{p})$ of the smallest such prime $\mathfrak{p}$, depending on the conductors and on the degrees. Then we give two applications: (i) find a prime number p for which $P \pmod p$ has a certain type of factorization in $\mathbb{F}_p[X]$, where $P \in \mathbb{Z}[X]$ is a monic, irreducible polynomial of square-free discriminant; (ii) on the estimation of the maximal number of tamely ramified extensions of Galois group A_n over a fixed number field K. To finish, we discuss some statistics in the quadratic number fields case (real and imaginary) concerning the separation of two irreducible unramified characters of the alterning group A_n, for $n = 5, 7, 13$.

2010 Mathematics Subject Classification: 11R44, 11R21, 11R45.

Key words: Chebotarev density theorem, Frobenius, unramified extensions, irreducible characters.

Table des matières

1. Introduction

Le théorème de Chebotarev affirme que pour une extension galoisienne de corps de nombres F/K, les automorphismes de Frobenius sont répartis dans l'ensemble des classes de conjugaison du groupe de Galois suivant une densité proportionnelle à leurs tailles. Par conséquent, en fixant une classe qui permet la séparation de deux caractères distincts du groupe de Galois en question, le théorème de Chebotarev apporte l'existence d'une infinité d'idéaux premiers $\mathfrak{p}$ pour lesquels les automorphismes de Frobenius $\sigma_\mathfrak{p}$ sont dans cette classe, et donc séparent ces caractères. L'effectivité permet de donner une borne supérieure sur la plus petite norme d'un tel idéal. Si comme il est souvent coutume pour ces questions, nous nous plaçons dans le cadre où l'hypothèse de Riemann généralisée (GRH) et la conjecture d'Artin aux fonctions L considérées sont satisfaites, la borne donnée par le théorème de Chebotarev est alors, à une constante absolue près, en $\ln^2|\mathrm{d}_F|$, où d_F est le discriminant du corps F. En particulier, quand l'extension F/K est non ramifiée, la borne est en $|G|^2\ln^2|\mathrm{d}_K|$, où $|G|$ est l'ordre du groupe de Galois de l'extension F/K.

La littérature pour ces questions est abondante ; citons Lagarias et Odlyzko [**LO**], Lagarias, Montgomery et Odlyzko [**LMO**], Serre [**Ser2**], Murty, Murty et Saradha [**MMS**], Oesterlé [**Oes**] ou plus récemment Iwaniec et Kowalski [**IK**], Bellaïche [**Bel**], Winckler [**Win**], Zaman [**Zam**], etc.

Ici nous proposons de commencer par montrer le résultat suivant qui est très certainement bien connu par les spécialistes, mais par souci de précision, nous en (re)donnons une preuve :

Théorème 1.1. *Soit K un corps de nombres de groupe de Galois absolu G_K et soient χ et χ' deux caractères de G_K, de produit scalaire $\langle\chi,\chi'\rangle$ nul. Supposons GRH et la conjecture d'Artin vraies aux fonctions L associées aux caractères de G_K. Il existe un idéal premier $\mathfrak{p}$ de K de norme $\mathrm{N}(\mathfrak{p})$ plus petite que*

$$\frac{1}{\langle\chi,\chi\rangle^2}\Big[c_1\chi(1)\chi'(1)[K:\mathbb{Q}]+c_2\big(\ln q(\chi\otimes\overline{\chi'})+\ln q(\chi\otimes\overline{\chi})\big)+c_3\langle\chi,\chi\rangle\Big]^2$$

tel que $\chi(\sigma_\mathfrak{p})\neq\chi'(\sigma_\mathfrak{p})$, où ici $\sigma_\mathfrak{p}$ désigne l'automorphisme de Frobenius associé à l'idéal premier $\mathfrak{p}$ et où les réels c_i sont des constantes absolues. (Pour un caractère θ de G_K, la quantité $q(\theta)$ désigne son conducteur arithmétique (cf. section 2 pour une définition précise).)

Remarque 1.2. Quand χ ou χ' sont ramifiés en l'idéal premier $\mathfrak{p}$, nous entendons par Frobenius en $\mathfrak{p}$, la "moyenne" du Frobenius dans l'extension associée (voir la sous-section 2.1).

Si l'on souhaite éviter un ensemble fini T de premiers de K (typiquement pour T l'ensemble des premiers ramifiés), la borne du théorème 1.1 devient

$$\frac{1}{\langle\chi,\chi\rangle^2}\Big[c_1\chi(1)\chi'(1)[K:\mathbb{Q}]+c_2\big(\ln q(\chi\otimes\overline{\chi'})+\ln q(\chi\otimes\overline{\chi})\big)+c_3\langle\chi,\chi\rangle+2\ln T\Big]^2,$$

où $\ln T=\sum_{\mathfrak{p}\in T}\ln \mathrm{N}(\mathfrak{p})$, ici $\mathrm{N}(\mathfrak{p})$ est la norme absolue de $\mathfrak{p}$.

Le résultat présenté ici semble préciser un récent travail de Rouse et Thorne dans lequel les auteurs donnent une borne pour la séparation des ensembles des valeurs propres de deux représentations irréductibles (proposition 4.1 de [**RT**]). Mais une lecture attentive de la preuve de leur résultat montre qu'en fait la borne donnée par Rouse et Thorne permet de séparer les caractères irréductibles en jeu (à partir de l'inégalité (4.6)). A noter qu'il est très facile de produire des exemples de représentations d'un groupe qui, évaluées en la même classe, ont des ensembles de valeurs propres distincts mais une trace identique (penser au groupe cyclique d'ordre 4 ou au groupe diédral d'ordre 12 pour des représentations *irréductibles*).

Ici nous présentons une preuve légèrement différente (dans l'esprit de [**LO**]) en nous efforçant d'éviter les majorations trop brutales, ce qui nous permet de donner quelques situations qui nous semblent intéressantes (voir le paragraphe 3.3.3).

Cela dit, si $\chi(1)=\chi'(1)=r$, et si $q(\chi),q(\chi')\leqslant q$ avec $\ln q>r[K:\mathbb{Q}]$, une majoration des quantités en jeu aboutit au résultat suivant (sous GRH et sous la conjecture d'Artin) :

Corollaire 1.3 (Rouse–Thorne)**.** *Sous les conditions précédentes, les paramètres locaux, $\{\alpha_{i,\rho}(\mathfrak{p})\}_i$, en $\mathfrak{p}$ de $L(s,\chi)$ (voir la section suivante pour la définition) sont différents de ceux de $L(s,\chi')$ pour un idéal premier $\mathfrak{p}$ de norme plus petite que $c_0r^2\ln^2 q$.*

Démonstration: En effet, en utilisant les propriétés des conducteurs, on obtient :

$$q(\chi\otimes\overline{\chi'})=q(\chi\otimes\overline{\chi'})\leqslant\Big(q(\chi)q(\chi')\Big)^r\leqslant q^{2r} \tag{1}$$

et le résultat découle de théorème 1.1. □

Remarque 1.4. En s'appuyant sur le livre d'Iwaniec et Kowalski [**IK**], Euvrard dans [**Euv**] rend explicite la constante précédente c_0 pour des familles de fonctions L en toute généralité.

Corollaire 1.5. *Dans le cas particulier où les caractères χ et χ' sont non ramifiés et de degré r, il existe un idéal premier $\mathfrak{p}$ de K de norme inférieure à $c_4 r^4 \ln^2 |\mathrm{d}_K|$ tel que $\chi(\sigma_\mathfrak{p}) \neq \chi'(\sigma_\mathfrak{p})$, où c_4 est une constante absolue et où d_K est le discriminant du corps K.*

Démonstration: Puisque les caractères $\chi \otimes \overline{\chi}$ et $\chi \otimes \overline{\chi'}$ sont non ramifiés, on a (cf. section 2) :

$$q(\chi \otimes \overline{\chi}) = q(\chi \otimes \overline{\chi'}) = |\mathrm{d}_K|^{r^2}.$$

La borne du théorème 1.1 devient donc

$$\frac{1}{\langle \chi, \chi \rangle^2} \Big(c_1 r^2 [K : \mathbb{Q}] + 2c_2 r^2 \ln |\mathrm{d}_K| + c_3 \langle \chi, \chi \rangle \Big)^2 \leqslant \Big(c_1 r^2 [K : \mathbb{Q}] + 2c_2 r^2 \ln |\mathrm{d}_K| + c_3 \Big)^2.$$

Pour obtenir la borne annoncée, il suffit de se rappeler que $[K : \mathbb{Q}] \leqslant \ln |\mathrm{d}_K|$ (dès que $K \neq \mathbb{Q}$). □

Si nous regardons tout spécialement la restriction au groupe alterné A_n des caractères irréductibles auto-conjugués du groupe symétrique S_n, on obtient le corollaire suivant (sous GRH et sous la conjecture d'Artin) :

Corollaire 1.6. *Soit $P \in \mathbb{Z}[X]$ un polynôme de degré n, unitaire et $\mathbb{Q}$-irréductible. Supposons son discriminant d_P égal au discriminant d'un corps quadratique.*

(i) Si $n = 2m + 1$ est impair, il existe un nombre premier p plus petit que $c_4\, b(n)^4 \ln^2 |\mathrm{d}_P|$ tel que P soit irréductible dans $\mathbb{F}_p[X]$ et où

$$b(n) = \frac{1}{2}\binom{2m}{m} \sim_{n\to\infty} \frac{2^{n-\frac{3}{2}}}{\sqrt{\pi}\sqrt{n-1}}.$$

(ii) Si $n \equiv 0 \pmod 4$, posons $m = 1 + n/4$. Alors il existe un nombre premier p plus petit que $c_4\, b(n)^4 \ln^2 |\mathrm{d}_P|$ tel que $P \pmod p$ se factorise sous la forme $Q_{2m-1}Q_{2m-3}$, où les polynômes Q_i sont des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré i et où

$$b(n) = \frac{n!}{2(\frac{n}{2}+1)(\frac{n}{2}-1)[\frac{n}{2}(\frac{n}{4})!(\frac{n}{4}-1)!]^2} \sim_{n\to\infty} \frac{2^{\frac{3}{2}} 4^n}{n^{\frac{7}{2}} \pi^{\frac{3}{2}}}.$$

(iii) Supposons que l'entier n est un carré et écrivons $n = m^2$. Alors il existe un nombre premier p plus petit que $c_4\, b(n)^4 \ln^2 |\mathrm{d}_P|$ tel que $P \pmod p$ se factorise sous la forme $Q_1 Q_3 \cdots Q_{2m-1}$, où les Q_i

sont des polynômes irréductibles de $\mathbb{F}_p[X]$ *de degré* i *et où*

$$b(n) = \frac{n!}{2\prod_{r=1}^{m} \frac{(2m-r)!}{(m-r)!}} \sim_{m\to\infty} \frac{\mathrm{e}^{m^2} m^{m^2+\frac{m}{2}+1}}{2^{\frac{3m^2+m+1}{2}} \pi^{\frac{m-1}{2}}}.$$

Ici, la constante c_4 *est absolue.*

Démonstration: Notons par F le corps de décomposition de P; soit $K = \mathbb{Q}(\sqrt{\mathrm{d}_P})$. L'extension F/K est une extension non ramifiée de groupe de Galois isomorphe à A_n (cf. théorème 3.5). Soit la classe de conjugaison $\mathcal{C}$ des éléments de S_n dont la décomposition s'écrit comme un n-cycle (ou bien, pour (ii) : comme le produit à supports disjoints d'un $(2m-1)$-cycle et d'un $(2m-3)$-cycle ou bien, pour (iii) : comme le produit $[1][3]\cdots[2m-1]$, où $[i]$ désigne un i-cycle, tous à supports disjoints). Dans A_n, cette classe $\mathcal{C}$ se décompose en deux classes de conjugaisons $\mathcal{C}_1$ et $\mathcal{C}_2$. A cette classe $\mathcal{C}$ on peut associer un caractère irréductible φ de S_n dont la restriction à A_n est la somme de deux caractères conjugués irréductibles χ_1 et χ_2. Les caractères χ_1 et χ_2 sont de même degré $b(n)$. Cette correspondance a la particularité suivante : une classe $\mathcal{C}'$ de A_n sépare les deux caractères conjugués χ_1 et χ_2 de A_n si et seulement si, $\mathcal{C}' = \mathcal{C}_i$ pour $i = 1$ ou $i = 2$. (Voir la sous-section 3.1.) Ainsi un idéal premier $\mathfrak{p}|p$ de $\mathcal{O}_K$ sépare χ_1 et χ_2 si et seulement si $\sigma_{\mathfrak{p}}$ est dans l'une des classes $\mathcal{C}_i$, *i.e.* si et seulement si le Frobenius de p est dans $\mathcal{C}$ (ici, le nombre premier p est non ramifié dans $F/\mathbb{Q}$, cf. paragraphes 3.2.1 et 3.2.3), ce qui équivaut au fait que $P \pmod p$ a la factorisation annoncée. On conclut ensuite avec le corollaire 1.5. □

Pour être complet, discutons brièvement de la "qualité" des bornes obtenues. Tout d'abord, une application "classique" du théorème de Chebotarev donne une borne en $O\big((n!)^2 \ln^2 |\mathrm{d}_P|\big)$. Ensuite, pour un polynôme P de degré impair n, notre méthode donne une borne en $O\big(\frac{4^{2n}}{n^2} \ln^2 |\mathrm{d}_P|\big)$ garantissant l'existence d'un nombre premier p avec $P \pmod p$ irréductible sur $\mathbb{F}_p[X]$ (point (i) du corollaire 1.6). Dans un récent travail, Bellaïche ([**Bel**, théorème 17]) donne une borne en $O\big(4^n(\ln|\mathrm{d}_P| + n\ln n)^2\big)$ pour tout P polynôme irréductible à coefficients dans $\mathbb{Z}$. Dans le paragraphe 3.2.4, nous nous efforçons de comparer les deux approches. Avec un minutieux travail, il est probable que la méthode de Bellaïche apporte une très bonne borne pour la situation (ii) du corollaire 1.6 (en $\mathcal{O}(2^n)$?); par contre, le point (iii) est nettement plus compliqué... c'est le cas extrême; ici la borne que l'on

obtient est légèrement meilleure que $(m^2!)^2$:

$$\frac{b(n)}{(n!)^2} \sim_{m\to\infty} \frac{\mathrm{e}^{3m^2}}{m^{3m^2-\frac{m}{2}+1}2^{\frac{3m^2+m+1}{2}}\pi^{\frac{m+1}{2}}} \ll \frac{1}{n^n},$$

ou encore

$$b(n) = O\left(\frac{(n!)^2}{n^n}\right).$$

Comme noté dans [**RT**], une borne pour la séparation de caractères associée au théorème des nombres premiers permet de majorer, pour un corps de nombres K, le nombre de caractères de degré r et de conducteur d'Artin borné par q_{Artin}. Ici, nous montrons qu'une analyse classique sur les conducteurs permet de baisser parfois cette borne : cela repose sur le fait que dans certains cas la taille du conducteur d'un produit tensoriel peut considérablement diminuer comparativement au produit des conducteurs ; cela s'explique par un télescopage favorable des valeurs propres des représentations en jeu.

Enonçons un résultat. Soit un idéal premier $\mathfrak{p}$ impair de K. Pour $n \geqslant 7$, notons par $\mathcal{N}(A_n, \mathfrak{p}, k)$ le nombre d'extensions du corps K de groupe de Galois isomorphe à A_n, non ramifiées en dehors de $\mathfrak{p}$ et dont le groupe d'inertie en $\mathfrak{p}$ est le produit de k transpositions à supports disjoints (on choisit l'entier k pair). On obtient :

Corollaire 1.7. *Sous les conditions précédentes, on a*

$$\ln \mathcal{N}(A_n, \mathfrak{p}, k) \ll [K:\mathbb{Q}]\Big((n-1)^2 \ln|\mathrm{d}_K| + 2k(n-1-k)\ln \mathrm{N}(\mathfrak{p})\Big)^2.$$

Le caractère irréductible sous-jacent est de degré $n-1$ et de conducteur d'Artin $\mathrm{N}(\mathfrak{p})^k$. Le gain ici se fait sur le terme devant $\ln \mathrm{N}(\mathfrak{p})$. En particulier, si n est pair, pour $k = n-2$, on passe de $2(n-1)(n-2)$ à $2(n-2)$. A noter ici que l'extension F/K correspondante de groupe de Galois A_n est de discriminant relatif $\mathrm{d}_{F/K} = \mathfrak{p}^{\frac{n!}{2}}$ et de discriminant absolu $\big(\mathrm{N}(\mathfrak{p})\mathrm{d}_K\big)^{\frac{n!}{2}}$.

Cet article est également consacré à des calculs dans le cadre du corollaire 1.5 ; nous cherchons à voir l'évolution de la borne par rapport à la quantité $\ln|\mathrm{d}_K|$. Nous nous sommes alors concentrés sur des caractères non ramifiés irréductibles des groupes alternés A_5, A_7 et A_{13} au-dessus d'un corps quadratique imaginaire ou réel K. Pour ce faire, nous partons d'une famille de polynômes P_a de degré premier n (on prend $n = 5$, $n = 7$ et $n = 13$) paramétrés par un entier a dont on est assuré que le groupe de Galois est le groupe symétrique S_n. Par un bon choix de a, il en ressort une extension non ramifiée de $K := \mathbb{Q}(\sqrt{\mathrm{d}_a})$ de groupe de

Galois A_n, où d_a est le discriminant de P_a (pour nos familles on aura également $\mathrm{d}_a = \mathrm{d}_K$). En faisant varier a, on obtient alors une famille d'extensions non ramifiées de corps quadratiques K de groupes de Galois A_n. Nous comparons la norme du plus petit idéal premier séparant les caractères irréductibles de degré 3 pour A_5 (resp. de degré 10 et 14 pour A_7) avec la borne en $\ln^2|\mathrm{d}_K|$. Pour A_{13}, nous nous focalisons sur les caractères irréductibles conjugués venant d'un caractère irréductible de S_{13}.

Également, à la lumière des récents travaux de Pollack [**Pol**], nous avons fait des simulations de la moyenne

$$\lim_{X\to\infty} \mu((P_a)_a, \chi_a, \chi'_a, X),$$

où

$$\mu((P_a), \chi_a, \chi'_a, X) := \frac{\sum_{\mathrm{d}_a \leqslant X} n(\chi_a, \chi'_a)}{\sum_{\mathrm{d}_a \leqslant X} 1},$$

et où $n(\chi_a, \chi'_a)$ est la norme du plus petit idéal premier $\mathfrak{p}$ dont le Frobenius $\sigma_\mathfrak{p}$ sépare deux caractères χ_a et χ'_a irréductibles, non ramifiés et de même degré r (ne dépendant pas de a ; typiquement des caractères conjugués) du corps $\mathbb{Q}(\sqrt{\mathrm{d}_a})$ (associés aux polynômes P_a). Nos calculs semblent montrer que cette moyenne converge rapidement. Une question naturelle se pose alors au sujet du lien entre cette valeur de convergence et les caractères choisis.

Donnons en quelques lignes le plan de ce travail. La partie 2 est consacrée à la preuve du théorème 1.1 : celle-ci est classique, elle s'inspire de [**LO**], de [**Bel**] et de [**IK**]. Dans la section 3, nous donnons des applications du théorème 1.1 illustrées par les corollaires 1.6 et 1.7. La section 4 est dédiée aux expérimentations numériques ; elle se termine par une observation sur les solutions d'une équation diophantienne en relation avec des travaux de Rémond [**Rém**] et de Bugeaud [**Bug**].

Les calculs de la dernière section ont été réalisés avec GP-Pari [**PARI**] ; pour les caractères les calculs ont été réalisés avec Magma [**BCP**].

Convention. Les réels c_i qui apparaîtront tout au long de ce travail sont des constantes absolues.

Remerciements. La finalisation de ce travail a eu lieu pendant le séjour à l'automne 2015 de C. Maire à l'UMI 3457 du CNRS - Centre de Recherches Mathématiques de Montréal. Le second auteur remercie le CRM pour les très bonnes conditions de recherche mises à sa disposition.

Les auteurs remercient Georges Gras, Christophe Delaunay et le rapporteur pour leurs commentaires et pertinentes remarques.

2. Preuve du théorème 1.1

2.1. Rappels. Pour ce paragraphe, nous renvoyons par exemple vers [**Mar**] ou vers [**IK**].

Soit (ρ, V) une représentation continue (complexe) de G_K de degré r et de caractère χ. Par un argument topologique, on rappelle que le noyau $\ker(\rho)$ est un sous-groupe ouvert de G_K et donc que l'image $\mathrm{Im}(\rho)$ de ρ est finie. Soit le corps de nombres $F = \overline{K}^{\ker(\rho)}$; posons $G = \mathrm{Gal}(F/K)$. La représentation ρ se factorise à travers G.

Pour $\mathfrak{p}$ un idéal premier de K, notons par $D_\mathfrak{p} \subset \mathrm{Gal}(F/K)$ le groupe de décomposition d'un idéal premier $\mathfrak{P}|\mathfrak{p}$ de F, par $I_\mathfrak{p}$ son groupe d'inertie, posons

$$V^{I_\mathfrak{p}} = \{v \in V : \forall\, s \in I_\mathfrak{p},\ \rho(s)(v) = v\}$$

le sous-espace vectoriel de V stable par $I_\mathfrak{p}$. Notons $(\tilde{\rho}, V^{I_\mathfrak{p}})$ la représentation de $\rho_{|D_\mathfrak{p}}$: la représentation $\tilde{\rho}$ se factorise à travers le quotient $D_\mathfrak{p}/I_\mathfrak{p}$. Soit $\sigma_\mathfrak{p} \in D_\mathfrak{p}$ un relèvement de l'automorphisme de Frobenius, générateur privilégié du quotient $D_\mathfrak{p}/I_\mathfrak{p}$. Le déterminant $\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\tilde{\rho}(\sigma_\mathfrak{p}); V^{I_\mathfrak{p}})$ ne dépend pas du choix de l'idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ (ni du choix du relèvement).

La fonction L d'Artin associée à χ est alors définie par :

$$L(s,\chi) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \frac{1}{\det(\mathrm{Id} - \mathrm{N}(\mathfrak{p})^{-s}\tilde{\rho}(\sigma_\mathfrak{p}); V^{I_\mathfrak{p}})}, \quad \mathrm{Re}(s) > 1,$$

où $\mathrm{N}(\mathfrak{p}) := |\mathcal{O}_K/\mathfrak{p}|$ désigne la norme absolue d'un idéal premier $\mathfrak{p}$.

Notons par $\alpha_{i,\rho}(\mathfrak{p})$, $1 \leqslant i \leqslant r$, les valeurs propres de $\tilde{\rho}(\sigma_\mathfrak{p})$ avec la convention $\alpha_{i,\rho}(\mathfrak{p}) = 0$ si $\dim V^{I_\mathfrak{p}} = r_\mathfrak{p} < i \leqslant r$. Les complexes $\{\alpha_{i,\rho}(\mathfrak{p})\}_{1\leqslant i\leqslant r}$ sont les *paramètres locaux en* $\mathfrak{p}$ de $L(s,\chi)$.

Si $\mathfrak{p}$ est non ramifié dans F/K et $k \in \mathbb{Z}$, la quantité $\chi(\sigma_\mathfrak{p}^k)$ est bien définie et est égale à $\alpha_{1,\rho}(\mathfrak{p})^k + \cdots + \alpha_{r,\rho}(\mathfrak{p})^k$. Si $\mathfrak{p}$ est ramifié dans F/K de groupe d'inertie $I_\mathfrak{p}$, on pose

$$\chi(\sigma_\mathfrak{p}^k) := \frac{1}{|I_\mathfrak{p}|} \sum_{\substack{s\in D_\mathfrak{p} \\ s\equiv\sigma_\mathfrak{p}^k (\mathrm{mod}\, I_\mathfrak{p})}} \chi(s) \overset{(*)}{=} \alpha_{1,\rho}(\mathfrak{p})^k + \cdots + \alpha_{r_\mathfrak{p},\rho}(\mathfrak{p})^k$$
$$= \alpha_{1,\rho}(\mathfrak{p})^k + \cdots + \alpha_{r,\rho}(\mathfrak{p})^k.$$

Remarque 2.1. L'égalité $(*)$ résulte de la généralisation du concept de représentation induite : voir [**Ser1**, chapitre VII, exercice 7.1].

Pour toute puissance t d'un nombre premier, notons :

$$\Sigma_t = \{\mathfrak{p} \subset \mathcal{O}_K,\, \mathrm{N}(\mathfrak{p}) = t\}.$$

Définissons alors la fonction Λ_χ de von Mangoldt par :

$$\Lambda_\chi(n) = \sum_{t,k|n=t^k} \left(\sum_{\mathfrak{p}\in\Sigma_t} \chi(\sigma_{\mathfrak{p}}^k) \right) \ln t.$$

La fonction Λ_χ apparaît dans la dérivée logarithmique de la fonction L de la façon suivante (voir par exemple [**IK**, p. 102]) :

Proposition 2.2. *Avec les notations précédentes, on a pour* $\mathrm{Re}(s) > 1$ *:*

$$-\frac{L'}{L}(s,\chi) = \sum_{n\geqslant 1} \Lambda_\chi(n) n^{-s}.$$

Le *conducteur d'Artin* associé au caractère χ est un idéal $f(\chi)$ de l'anneau des entiers $\mathcal{O}_K$ de K : $f(\chi) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{f_\mathfrak{p}(\chi)}$, où le produit porte sur les idéaux premiers $\mathfrak{p}$ de K et où $f_\mathfrak{p}(\chi)$ est un entier naturel dépendant des groupes de ramification dans F/K d'un idéal premier $\mathfrak{P}$ de F audessus de l'idéal $\mathfrak{p}$. En particulier $f_\mathfrak{p}(\chi) = 0$ si et seulement si, $\chi_{|I_\mathfrak{p}}$ est trivial. Soyons plus précis. Si M/K désigne une extension galoisienne contenant l'extension F/K, et si l'on note $G_{i,\mathfrak{p}}$ les groupes de ramification à numérotation inférieure de $\mathfrak{p}$, on a $f_\mathfrak{p}(\chi) := \sum_{i\geqslant 0} \frac{|G_{i,\mathfrak{p}}|}{|G_{0,\mathfrak{p}}|} \operatorname{codim} V^{G_{i,\mathfrak{p}}}$, ici $G_{0,\mathfrak{p}} = I_\mathfrak{p}$. Cette quantité ne dépend pas de l'extension M/K. (Pour plus de détails voir par exemple [**Neu**, chapitre VII §11].)

Le conducteur analytique est quant à lui défini par :

$$\mathfrak{q}(s,\chi) = q(\chi)\mathfrak{q}_\infty(s,\chi),$$

où $q(\chi)$ est le *conducteur arithmétique* :

$$q(\chi) = |\mathrm{d}_K|^r \cdot \mathrm{N}_{K/\mathbb{Q}}(f(\chi))$$

et où $\mathfrak{q}_\infty(s,\chi) = \prod_{j=1}^{r[K:\mathbb{Q}]}(|s+\kappa_j|+3)$ avec $\kappa_j \in \{0,1\}$ (pour plus de détails, voir [**Neu**, chapitre VII §12]).

Donnons également la forme du facteur gamma d'une fonction L d'Artin :

$$\gamma_\chi(s) = \pi^{-s\frac{r[K:\mathbb{Q}]}{2}} \Gamma\left(\frac{s+1}{2}\right)^{\alpha[K:\mathbb{Q}]} \Gamma\left(\frac{s}{2}\right)^{\beta[K:\mathbb{Q}]},$$

où $\alpha+\beta = r$.

A ce stade, nous rappelons les conjectures utilisées dans ce travail.

Conjecture 2.3 (Hypothèse de Riemann Généralisée (GRH))**.** *Soit une fonction L d'Artin. Alors tous les zéros non-triviaux de L sont sur la droite* $\mathrm{Re}(s) = \frac{1}{2}$.

Conjecture 2.4 (Conjecture d'Artin)**.** *Toute fonction L d'Artin $L(s,\chi)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$ sauf éventuellement en $s = 1$ où il y a un pôle d'ordre égal au nombre de fois où intervient le caractère trivial dans la décomposition de χ.*

2.2. La preuve.

2.2.1. Le cas général. Nous nous inspirons de l'article de Lagarias et Odlyzko [**LO**], de Bellaïche [**Bel**] et du livre d'Iwaniec et Kowalski [**IK**].

Pour $x \in \mathbb{R}_+$ et un caractère χ de G_K, posons :

$$\theta(\chi, x) = \sum_{t \leqslant x} \sum_{\mathfrak{p} \in \Sigma_t} \chi(\sigma_{\mathfrak{p}})(x - t) \ln t,$$

$$\psi(\chi, x) = \sum_{n \leqslant x} \Lambda_\chi(n)(x - n).$$

Comme dans [**Bel**], nous allons comparer ces deux fonctions.

Soit la fonction $\chi \mapsto \mu(\chi)$ qui donne le nombre de fois où la représentation triviale intervient dans la décomposition de $\rho_{|F}$ en représentations irréductibles (ici, $F = \overline{K}^{\ker(\rho)}$).

Proposition 2.5. *Soit χ un caractère de G_K. Alors, en supposant vraie GRH et la conjecture d'Artin pour $L(s,\chi)$, on a pour $x \geq 3$:*

$$\left|\theta(\chi, x) - \frac{1}{2}\mu(\chi)x^2\right| \leqslant x^{\frac{3}{2}}\Big(c_5\chi(1)[K : \mathbb{Q}] + c_6 \ln q(\chi) + c_7\mu(\chi)\Big),$$

où $q(\chi)$ est le conducteur arithmétique du caractère χ.

Démonstration: Commençons par estimer la différence entre θ et ψ :

$$\begin{aligned}
|\theta(\chi, x) - \psi(\chi, x)| &= \left| \sum_{\substack{t,k \geqslant 2 \\ t^k \leqslant x}} \sum_{\mathfrak{p} \in \Sigma_t} \chi(\sigma_p^k)(x - t^k) \ln t \right| \\
&\leqslant x\chi(1) \sum_{k \geqslant 2} \sum_{t \leqslant x^{1/k}} \sum_{\mathfrak{p} \in \Sigma_t} \ln t \\
&\leqslant x\chi(1) \sum_{k \geqslant 2} \sum_{p \leqslant x^{1/k}} [K : \mathbb{Q}] \ln p,
\end{aligned}$$

ici la dernière somme porte sur les nombres premiers p plus petit que $x^{1/k}$.

En découpant l'intervalle de sommation, on obtient :

$$|\theta(\chi,x)-\psi(\chi,x)| \leqslant x\chi(1)[K:\mathbb{Q}]\Big(\Delta(2)+\cdots+\Delta(m)\Big),$$

où

$$\Delta(i)=\sum_{p\leqslant x^{1/i}} \ln p,$$

et où $m=\lceil \ln x/\ln 2\rceil$.

Il est ensuite bien connu (voir par exemple [**Ten**]) que

$$\sum_{p\leqslant x} \ln p \leqslant c_8 x$$

et ainsi $\Delta(i)\leqslant c_8 x^{\frac{1}{i}}$. On obtient alors :

$$\begin{aligned}|\theta(\chi,x)-\psi(\chi,x)| &\leqslant xc_8\chi(1)[K:\mathbb{Q}]\Big(x^{\frac{1}{2}}+x^{\frac{1}{3}}\ln x\Big)\\ &\leqslant 2x^{\frac{3}{2}}c_8\chi(1)[K:\mathbb{Q}].\end{aligned}$$

Pour conclure il nous suffit de rappeler le lemme suivant (voir par exemple [**Bel**, lemme 6]) :

Lemme 2.6. *Soit χ un caractère de G_K. En supposant que $L(s,\chi)$ satisfait l'hypothèse de Riemann et la conjecture d'Artin, la fonction $\psi(\chi,x)$ vérifie pour tout $x\geq 3$:*

$$\left|\psi(\chi,x)-\frac{1}{2}\mu(\chi)x^2\right| \leqslant x^{\frac{3}{2}}\Big(c_9\chi(1)[K:\mathbb{Q}]+c_{10}\ln q(\chi)+c_{11}\mu(\chi)\Big).$$

Démonstration: L'utilisation de la transformée de Mellin dans l'égalité de la proposition 2.2, $-\frac{L'}{L}(s,\chi)=\sum_{n\geqslant 1}\Lambda_\chi(n)n^{-s}$, permet d'obtenir, pour $x\in\mathbb{R}$, $x\geqslant 3$:

$$\psi(\chi,x)=\frac{1}{2\mathrm{i}\pi}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty} -\frac{L'}{L}(s,\chi)\frac{x^{s+1}}{s(s+1)}\,\mathrm{d}s.$$

La preuve suit celle due à Lagarias et Odlyzko dans [**LO**]. On commence par appliquer le théorème de Cauchy en déplaçant la droite d'intégration vers la gauche (à l'infini). A la limite, sur les "trois" bords introduits, seule l'intégrale sur la droite initiale est non nulle. Ainsi $\psi(\chi,x)$ est la somme des résidus de $-\frac{L'}{L}(s,\chi)\frac{x^{s+1}}{s(s+1)}$ sur le demi-plan $\mathrm{Re}(s)\leqslant 2$. C'est le produit de Hadamard de la fonction $L(s,\chi)$ qui va nous permettre de faire le calcul. En dérivant le logarithme de ce produit, on obtient (sous la conjecture d'Artin) :

$$-\frac{L'}{L}(s,\chi)=\frac{1}{2}\ln q(\chi)+\frac{\gamma_\chi'}{\gamma_\chi}(s)-b(\chi)+\frac{\mu(\chi)}{s}+\frac{\mu(\chi)}{s-1}-\sum_{\rho\neq 0,1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right),$$

où ρ varie parmi les zéros non-triviaux de $L(s,\chi)$ différents de 0 et 1 et où $b(\chi)$ est une constante. Il reste alors à déterminer les résidus en jeu.

D'abord, il y a l'éventuel pôle en $s=1$ de la fonction $\frac{L'}{L}(s,\chi)$ d'ordre μ dont le résidu vaut -1 et qui donne donc ici $-\mu(\chi)\frac{x^2}{2}$.

Ensuite, à chaque zéro ρ non trivial de $L(s,\chi)$, la fonction $\frac{L'}{L}(s,\chi)$ a un pôle d'ordre 1, de résidu 1, cela donne donc une contribution en $\sum_\rho \frac{x^{1+\rho}}{\rho(\rho+1)}$. Or d'après la proposition 5.7, p. 102 de [**IK**], le nombre de tels zéros ρ de partie imaginaire bornée entre des réels T et $T+1$ est inférieur (à une constante près) à $\ln \mathfrak{q}(\mathrm{i}T,\chi) \leqslant \ln q(\chi) + \chi(1)[K:\mathbb{Q}]\ln(4+T)$. Ainsi, on a (se rappeler que $\mathrm{Re}(\rho)=\frac{1}{2}$) :

$$\begin{aligned}\left|\sum_\rho \frac{x^{1+\rho}}{\rho(\rho+1)}\right| &\leqslant c_{12}x^{\frac{3}{2}}\sum_{T=1}^{+\infty}\frac{\ln q(\chi)+\chi(1)[K:\mathbb{Q}]\ln(4+T)}{T^2}\\ &\leqslant c_{13}x^{\frac{3}{2}}(\ln q(\chi)+\chi(1)[K:\mathbb{Q}]).\end{aligned}$$

La fonction $\frac{L'}{L}(s,\chi)$ possède également des pôles d'ordre 1 aux zéros triviaux (de la fonction γ_χ) : ceux situés en $s=-2m-1$ pour $m\in\mathbb{N}$ donnent un résidu égal à $\alpha[K:\mathbb{Q}]$ et ceux situés en $s=-2m$ pour $m\in\mathbb{N}$ donnent un résidu égal à $\beta[K:\mathbb{Q}]$ (avec $\alpha+\beta=r=\chi(1)$). On obtient donc pour les résidus des zéros triviaux la majoration :

$$\begin{aligned}\alpha[K:\mathbb{Q}]\sum_{m=1}^{+\infty}\frac{x^{-2m}}{2m(2m+1)}+\beta[K:\mathbb{Q}]\sum_{m=1}^{+\infty}\frac{x^{1-2m}}{2m(2m-1)}&\\ \leqslant c_{14}\chi(1)[K:\mathbb{Q}]x\ln x.&\end{aligned}$$

Les résidus restants sont ceux en $s=0$ et $s=-1$. La fin est alors classique, on écrit les développements en $s=0$ et $s=-1$ de $\frac{x^{s+1}}{s(s+1)}$ et de $\frac{L'}{L}(s,\chi)$ pour obtenir que la somme des résidus cherchés est bornée par

$$c_{15}x\ln x\Big(\chi(1)[K:\mathbb{Q}]+\ln q(\chi)+\mu(\chi)\Big).$$

Finalement,

$$\left|\psi(\chi,x)-\frac{1}{2}\mu(\chi)x^2\right| \leqslant x^{\frac{3}{2}}\Big(c_9\chi(1)[K:\mathbb{Q}]+c_{10}\ln q(\chi)+c_{11}\mu(\chi)\Big),$$

avec $c_9=c_{13}+c_{14}+c_{15}$, $c_{10}=c_{13}+c_{15}$ et $c_{11}=c_{15}$. □

Terminons alors la preuve de la proposition 2.5.

$$\begin{aligned}\left|\theta(x,\chi)-\frac{1}{2}\mu(\chi)x^2\right| &\leqslant |\theta(\chi,x)-\psi(\chi,x)|+\left|\psi(\chi,x)-\frac{1}{2}\mu(\chi)x^2\right|\\ &\leqslant 2c_8x^{\frac{3}{2}}\chi(1)[K:\mathbb{Q}]\\ &\quad+x^{\frac{3}{2}}\Big(c_9\chi(1)[K:\mathbb{Q}]+c_{10}\ln q(\chi)+c_{11}\mu(\chi)\Big)\\ &\leqslant x^{\frac{3}{2}}\Big(c_5\chi(1)[K:\mathbb{Q}]+c_6\ln q(\chi)+c_7\mu(\chi)\Big),\end{aligned}$$

où $c_5=2c_8+c_9$, $c_6=c_{10}$ et $c_7=c_{11}$. □

Démonstration du théorème 1.1: La preuve repose donc sur le fait bien connu suivant : pour deux caractères distincts χ et χ' de produit scalaire nul, on a $\mu(\chi\otimes\overline{\chi'})=0$ et $\mu(\chi\otimes\overline{\chi})=\mu\geqslant 1$. On applique alors la proposition 2.5 aux caractères $\chi\otimes\overline{\chi'}$ et $\chi\otimes\overline{\chi}$ pour obtenir, pour tout $x\geq 3$:

$$\begin{aligned}&\left|\theta(x,\chi\otimes\overline{\chi'})\right|\leqslant x^{\frac{3}{2}}\Big[c_5\chi(1)\chi'(1)[K:\mathbb{Q}]+c_6\ln q(\chi\otimes\overline{\chi'})\Big],\\ &\left|\theta(x,\chi\otimes\overline{\chi})\right|-\frac{1}{2}\mu x^2\leqslant x^{\frac{3}{2}}\Big[c_5\chi(1)\chi'(1)[K:\mathbb{Q}]+c_6\ln q(\chi\otimes\overline{\chi})+c_7\mu\Big].\end{aligned}$$

Il reste à montrer l'existence d'un réel x tel que $\theta(x,\chi\otimes\overline{\chi'})\neq\theta(x,\chi\otimes\overline{\chi})$; on aura alors bien l'existence d'un idéal premier $\mathfrak{p}$ de K de norme plus petite que x et vérifiant $(\chi\otimes\overline{\chi'})(\sigma_\mathfrak{p})\neq(\chi\otimes\overline{\chi})(\sigma_\mathfrak{p})$, c'est-à-dire $\chi'(\sigma_\mathfrak{p})\neq\chi(\sigma_\mathfrak{p})$.

Notons

$$Z_1=c_5\chi(1)\chi'(1)[K:\mathbb{Q}]+c_6\ln q(\chi\otimes\overline{\chi'})$$

et

$$Z_2=c_5\chi(1)\chi'(1)[K:\mathbb{Q}]+c_6\ln q(\chi\otimes\overline{\chi})+c_7\mu.$$

Choisissons x_0 assez grand tel que $\mu^2x_0>4(Z_1+Z_2)^2$ (ainsi $\frac{1}{2}\mu\sqrt{x_0}>Z_1+Z_2$ donc $\frac{1}{2}\mu\sqrt{x_0}-Z_1>Z_2$). Raisonnons par l'absurde et supposons que $A=\theta(x_0,\chi\otimes\overline{\chi'})=\theta(x_0,\chi\otimes\overline{\chi})$. Ainsi, on a : $|A|\leqslant x_0^{\frac{3}{2}}Z_1$ et $|A-\frac{1}{2}\mu x_0^2|\leqslant x_0^{\frac{3}{2}}Z_2$ donc $\frac{1}{2}\mu x_0^2-A\geqslant\frac{1}{2}\mu x_0^2-x_0^{\frac{3}{2}}Z_1=x_0^{\frac{3}{2}}(\frac{1}{2}\mu\sqrt{x_0}-Z_1)>x_0^{\frac{3}{2}}Z_2$, d'où la contradiction. Ainsi, $\theta(x_0,\chi\otimes\overline{\chi'})\neq\theta(x_0,\chi\otimes\overline{\chi})$. □

2.2.2. En évitant un ensemble T donné. Fixons T un ensemble fini d'idéaux premiers de K. Il est possible de donner une variante du théorème 1.1 en imposant que l'idéal premier $\mathfrak{p}$ trouvé ne se trouve pas dans l'ensemble T.

Pour cela, sur le modèle de θ, introduisons

$$\tilde{\theta}(\chi, x) = \sum_{t \leq x} \sum_{\substack{\mathfrak{p} \in \Sigma_t \\ \mathfrak{p} \notin T}} \chi(\sigma_{\mathfrak{p}})(x-t) \ln t.$$

Posons $\ln T := \sum_{\mathfrak{p} \in T} \ln \mathrm{N}(\mathfrak{p})$. On a alors

$$\begin{aligned} \left|\theta(\chi, x) - \tilde{\theta}(\chi, x)\right| &= \left|\sum_{t \leq x} \sum_{\substack{\mathfrak{p} \in \Sigma_t \\ \mathfrak{p} \in T}} \chi(\sigma_{\mathfrak{p}})(x-t) \ln t\right| \\ &\leq x\chi(1) \ln T. \end{aligned}$$

Il vient ainsi pour tout $x \geq 3$:

$$\left|\tilde{\theta}(x, \chi \otimes \overline{\chi'})\right| \leqslant x^{\frac{3}{2}} \Big[c_5 \chi(1)\chi'(1)[K:\mathbb{Q}] + c_6 \ln q(\chi \otimes \overline{\chi'} + \chi(1)\chi'(1) \ln T\Big],$$

$$\begin{aligned} \left|\tilde{\theta}(x, \chi \otimes \overline{\chi}) - \frac{1}{2}\mu x^2\right| \leqslant x^{\frac{3}{2}} \Big[&c_5 \chi(1)\chi'(1)[K:\mathbb{Q}] \\ &+ c_6 \ln q(\chi \otimes \overline{\chi}) + c_7 \mu + \chi(1)\chi'(1) \ln T\Big]. \end{aligned}$$

Le corollaire suivant s'en déduit (voir remarque 1.2).

Corollaire 2.7. *Soit T un ensemble fini d'idéaux premiers de K. Alors, sous les conditions du théorème 1.1, il existe un idéal premier $\mathfrak{p}$ de K, $\mathfrak{p} \notin T$, de norme $\mathrm{N}(\mathfrak{p})$ plus petite que*

$$\frac{1}{\langle \chi, \chi \rangle^2}\Big[c_1 \chi(1)\chi'(1)[K:\mathbb{Q}] + c_2\big(\ln q(\chi \otimes \overline{\chi'}) + \ln q(\chi \otimes \overline{\chi})\big) + c_3 \langle \chi, \chi \rangle + 2 \ln T\Big]^2$$

tel que $\chi(\sigma_{\mathfrak{p}}) \neq \chi'(\sigma_{\mathfrak{p}})$.

3. Deux applications

3.1. Rappels sur les caractères de A_n. Pour cette partie, nous nous référons à [**FH**, lecture 5].

Partons du groupe symétrique S_n. Les (classes des) représentations irréductibles ρ de S_n sont en correspondance bijective avec les partitions λ de n (et donc avec les tableaux de Young). Soit φ la restriction de ρ à A_n. La représentation obtenue est : soit irréductible ; soit la somme de deux représentations irréductibles de même degré.

Le premier cas a lieu *i.e.*, $\rho_{|A_n}$ est irréductible, si et seulement si l'une des conditions équivalentes suivantes est vérifiée :

(i) le tableau de Young associé à ρ n'est pas auto-conjugué (*i.e.* symétrique) ;

(ii) $\rho \ncong \rho \otimes \rho_0$, où ρ_0 est la représentation non triviale du quotient S_n/A_n.

Quand la restriction φ de ρ à A_n se décompose en somme de deux représentations irréductibles conjuguées φ_1 et φ_2, les représentations de A_n obtenues sont conjuguées, *i.e.*, $\varphi_2 := \varphi_1 \circ f_t$, où t est une transposition quelconque et où f_t est la conjugaison par t.

Rappelons que toute représentation irréductible de A_n s'obtient de cette façon *i.e.*, comme composante de la restriction à A_n d'une représentation irréductible de S_n.

D'un autre côté, une classe de conjugaison $\mathcal{C}$ de S_n se décompose en deux classes de conjugaison de A_n si et seulement si $\mathcal{C}$ est la classe de conjugaison d'un élément dont la décomposition en cycle ne fait apparaître que des cycles de longueurs impaires et toutes différentes.

Partons alors d'un diagramme T de Young symétrique associée à la partition λ. Ce tableau donne une représentation irréductible ρ_{T} de S_n, de caractère θ_{T} dont la restriction à A_n se décompose en somme de deux caractères irréductibles χ_{T} et χ'_{T} de A_n. Si $\lambda = \lambda_1 \geq \cdots \geq \lambda_k$ est la partition associée à ρ_{T}, notons par Γ_i, $i = 1, \ldots, k$, les crochets symétriques du diagramme de Young T puis posons $q_i = |\Gamma_i|$ le cardinal de Γ_i. On peut noter que $q_i = 2(\lambda_i - i) + 1$ et que k est le plus grand entier vérifiant $\lambda_k - k \geq 0$. À ce tableau symétrique T, on associe la classe de conjugaison $\mathcal{C}_{\mathrm{T}}$ dont la décomposition des éléments s'écrit comme le produit de q_i-cycles, $i = 1, \ldots, k$ (à supports disjoints) avec $\sum_i q_i = n$. Comme les éléments q_i sont impairs et distincts (il est immédiat que $q_i > q_{i-1}$), la classe de conjugaison $\mathcal{C}_{\mathrm{T}}$ se scinde en deux classes de conjugaison $\mathcal{C}_{\mathrm{T}}^{(1)}$ et $\mathcal{C}_{\mathrm{T}}^{(2)}$ de A_n.

Réciproquement. Partons d'une classe de conjugaison $\mathcal{C}$ de S_n qui se scinde en deux classes de conjugaison de A_n. Alors $\mathcal{C} = [q_1] \cdots [q_k]$, où $[q_i]$ désigne un q_i-cycle (les supports sont disjoints), avec les q_i impairs (pouvant éventuellement prendre la valeur 1), $q_i > q_{i-1}$ et $\sum_i q_i = n$. Le diagramme de Young de la représentation ρ s'obtient simplement en imbriquant les crochets symétriques de taille $q_1, \ldots, q_k$.

Résumons dans la proposition suivante la particularité du lien entre ρ_{T} et $\mathcal{C}_{\mathrm{T}}$.

Proposition 3.1. *(i) Pour tout caractère irréductible θ de A_n différent de χ_{T} et χ'_{T}, on a $\theta(\mathcal{C}_T^{(1)}) = \theta(\mathcal{C}_T^{(2)})$.*

(ii) Pour toute classe de conjugaison $\mathcal{C}'$ de A_n différente de $\mathcal{C}_T^{(i)}$, $i=1,2$, on a $\chi_{\mathrm{T}}(\mathcal{C}') = \chi'_{\mathrm{T}}(\mathcal{C}')$. De plus, $\chi_{\mathrm{T}}(\mathcal{C}_T^{(1)}) = \chi'_{\mathrm{T}}(\mathcal{C}_T^{(2)})$ et $\chi_{\mathrm{T}}(\mathcal{C}_T^{(1)}) = \chi'_{\mathrm{T}}(\mathcal{C}_T^{(2)})$.

Ainsi, les seules classes de conjugaison séparant les caractères χ_{T} et χ'_{T} sont les classes $\mathcal{C}_T^{(i)}$.

Passons à des rappels sur les valeurs des caractères irréductibles de A_n.

Définition 3.2. Si χ un caractère irréductible de A_n, on note par $a(\chi) = |\{\chi(s),\, s \in A_n\}|$. C'est le nombre de valeurs prises par le caractère χ.

Rappelons que les caractères de S_n sont à valeurs entières. Si ρ est une représentation irréductible de S_n non auto-conjuguée, la restriction φ de ρ au groupe alterné A_n est irréductible. Notons par χ son caractère et par r son degré. Alors, comme pour tout $s \in A_n$, $|\chi(s)| \leqslant r$ (se rappeler que χ est de degré r et que les valeurs propres de la représentation associée sont des racines de l'unité) et que les valeurs de χ sont entières, on a $a(\chi) \leqslant 2r+1$.

Si maintenant ρ est auto-conjuguée, alors la restriction φ de ρ à A_n se décompose en somme de deux représentations irréductibles conjuguées φ_1 et φ_2. On rappelle que $\varphi_2 := \varphi_1 \circ f_t$, où t est une transposition quelconque et où f_t est la conjugaison par t. Ainsi, si c est une classe de conjugaison non décomposée d'un élément s de A_n *i.e.*, $f_t(c) = c$, on obtient $\varphi_i(c) = \frac{1}{2}\rho(c)$ et par conséquent les caractères $2 \cdot \chi_i$ des représentations $\varphi_i \oplus \varphi_i$ prennent, sur ces classes, leurs valeurs dans l'ensemble $a(\chi)$, χ étant le caractère de ρ. Il en est de même pour les classes de conjugaison c décomposées non associées à ρ. Pour les deux dernières classes *i.e.*, les classes décomposées associées à ρ, ces valeurs sortent de l'ensemble $a(\chi)$. En conclusion on a $a(\chi_i) \leqslant 2r+3$.

Exemple 3.3. Soit la représentation irréductible ρ associée à la partition $\lambda = (n-1,1)$. La représentation ρ est de degré $n-1$ et sa restriction à A_n est encore irréductible. Notons par χ_λ le caractère de ρ. Pour $1 \leqslant k \leqslant n-2$, si $\mathcal{C}_k$ est la classe de conjugaison des cycles de longueurs $(n-k)$, la règle de Murnaghan–Nakayama indique que $\chi_\lambda(\mathcal{C}_k) = k-1$, ce qui donne une minoration en $O(n)$ pour $a(\chi)$.

Si on s'intéresse à la classe de conjugaison $\mathcal{C}$ des produits de 2 transpositions (à supports disjoints), on obtient $\chi_\lambda(\mathcal{C}) = n-5$ pour $n \geqslant 4$. Plus généralement on obtient que si $\mathcal{C}'_k$ est le produit de k transpositions à supports disjoints (pour $k \leqslant \frac{n-1}{2}$) alors $\chi_\lambda(\mathcal{C}'_k) = n-2k-1$.

Exemple 3.4. Prenons n pair et soit $\mathcal{C}$ la classe de conjugaison des cycles de longueur $(n-1)$. Soit χ_{T} un caractère irréductible de tableau de Young T. La règle de Murnaghan–Nakayma indique ici que

$$\chi_{\mathrm{T}}(\mathcal{C}) = \begin{cases} 1 & \text{si T} = (1,\dots,1) \text{ ou T} = (n), \\ (-1)^{n-k-1} & \text{si T} = (k,2,1\dots,1), \\ 0 & \text{sinon.} \end{cases}$$

3.2. Polynôme à coefficients entiers modulo un nombre premier. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible de clôture galoisienne F. Supposons que $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_n$; soit $K/\mathbb{Q}$ l'unique sous-extension quadratique de $F/\mathbb{Q}$. On rappelle que $K = \mathbb{Q}(\sqrt{\mathrm{d}_P})$, où d_P est le discriminant de P.

Soit p un nombre premier non ramifié dans F/K ; notons par $\mathfrak{P}$ un idéal premier de F au-dessus de p et posons $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$. Nous allons rappeler comment obtenir la classe de conjugaison du Frobenius $\sigma_{\mathfrak{p}}$ de $\mathfrak{p}$ dans $\mathrm{Gal}(F/K) \simeq A_n$.

3.2.1. Cycles et Frobenius. Soit $F_{\mathfrak{P}}$ le complété de F par rapport à $\mathfrak{P}$. L'extension galoisienne $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ est une extension locale de groupe de Galois isomorphe à un sous-groupe de A_n.

Soit $P = P_1 \cdots P_g$ la factorisation de P en polynômes irréductibles P_i distincts dans $\mathbb{Q}_p$ de degré $d_i = e_i f_i$. Soient $(\alpha^i_{j_i})_{j_i}$ les racines de P_i dans $\overline{\mathbb{Q}_p}$. On rappelle que $F_{\mathfrak{P}} = \mathbb{Q}_p(\alpha^i_{j_i}, i = 1,\dots,g, j_i = 1,\dots,d_i)$ et que $p\mathcal{O}_M = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, où M est un corps de rupture de P et où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_M$ deux à deux distincts de degré résiduel f_i.

Précisons donc la décomposition de $\sigma_{\mathfrak{p}}$ en produit de cycles, le tout en relation avec la sous-section 3.1.

Premier cas : le nombre premier p est non ramifié dans $K/\mathbb{Q}$.

Commençons par noter que le corps $F_{\mathfrak{P}}$ contient $\mathbb{Q}_p(\sqrt{d})$.

Partons d'une racine α^i_1 de P_i : l'extension $\mathbb{Q}_p(\alpha^i_1)/\mathbb{Q}_p$ étant cyclique, son groupe de Galois est engendré par un cycle de longueur $f_i = \deg(P_i)$. Maintenant, connaître le groupe de Galois de $F_{\mathfrak{P}}/\mathbb{Q}_p$ c'est connaître son action sur les différentes racines de P. Comme l'action de $\mathrm{Gal}(F_{\mathfrak{P}}/\mathbb{Q}_p)$ sur α^i_1 s'exprime comme un f_i-cycle et que les différents cycles provenant des racines de P sont à supports disjoints, le groupe de Galois de $F_{\mathfrak{P}}/\mathbb{Q}_p$, qui est cyclique ici, est engendré par un produit de f_i-cycles à supports disjoints que nous notons σ. La conclusion dépend alors de l'extension $\mathbb{Q}_p(\sqrt{\mathrm{d}_P})/\mathbb{Q}_p$ (ou de façon équivalente, de savoir si $\sigma \in S_n - A_n$ ou

si $\sigma \in A_n$) : si l'extension n'est pas triviale, le groupe $\mathrm{Gal}(F_{\mathfrak{P}}/\mathbb{Q}_p(\sqrt{\mathrm{d}_P}))$ est engendré par σ^2 ; sinon, le groupe de Galois de $F_{\mathfrak{P}}/\mathbb{Q}_p(\sqrt{\mathrm{d}_P})$ est le même que celui de $F_{\mathfrak{P}}/\mathbb{Q}_p$, il est donc engendré par σ.

Ainsi, si le nombre premier p est inerte dans $K/\mathbb{Q}$, on a $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{P}}^2$, avec $\sigma_{\mathfrak{P}} \in S_n - A_n$, et par conséquent $\sigma_{\mathfrak{p}}$ ne donne pas deux classes de conjugaison sous l'action de A_n (voir la sous-section 3.1).

Second cas : le nombre premier p est ramifié dans $K/\mathbb{Q}$.

Dans la factorisation, $P = P_1 \cdots P_g \in \mathbb{Q}_p[X]$, supposons que pour $i = 1, \ldots, s$, les polynômes P_i sont non ramifiés et que pour $i = s+1, \ldots, g$, les polynômes P_i sont ramifiés avec $e_i = 2$. Par hypothèse : $s < g$.

Pour $1 \leqslant i \leqslant s$, le groupe de Galois de P_i est simplement un cycle de longueur f_i.

Pour $s+1 \leqslant i \leqslant g$: si $\mathbb{Q}_p(\sqrt{\mathrm{d}_P}) \nsubseteq \mathbb{Q}_p(\alpha_1^i)$, le polynôme P_i reste irréductible sur $\mathbb{Q}_p(\sqrt{\mathrm{d}_P})$ et donc le groupe de Galois de $\mathbb{Q}_p(\alpha_1^i, \sqrt{\mathrm{d}_P})/\mathbb{Q}_p(\sqrt{\mathrm{d}_P})$ est engendré par un $(2f_i)$-cycle ; si $\mathbb{Q}_p(\sqrt{\mathrm{d}_P}) \subseteq \mathbb{Q}_p(\alpha_1^i)$ alors le polynôme P_i se décompose en un produit de deux polynômes de degré f_i sur $\mathbb{Q}_p(\sqrt{\mathrm{d}_P})$ et le groupe de Galois de l'extension $\mathbb{Q}_p(\alpha_1^i, \sqrt{\mathrm{d}_P})/\mathbb{Q}_p(\sqrt{\mathrm{d}_P})$ est engendré par un produit de deux f_i-cycles.

En conclusion, $\sigma_{\mathfrak{p}}$ va être le produit de cycles à supports disjoints avec au moins ou bien un cycle de longueur pair ou bien un couple de cycles de même longueur (éventuellement de longueur 1) : par conséquent $\sigma_{\mathfrak{p}}$ ne sépare aucune paire de caractères conjugués (voir la sous-section 3.1).

3.2.2. Quand d_P est le discriminant d'un corps quadratique. Nous allons préciser le second cas de la section précédente (*i.e.* quand p est ramifié dans $K/\mathbb{Q}$) lorsque le discriminant d_P est celui d'un corps quadratique. Commençons par rappeler le résultat suivant de Kondo.

Théorème 3.5 (Kondo [**Kon**])**.** *Si le discriminant d'un polynôme P de degré n sur $\mathbb{Q}$ est le discriminant d'un corps quadratique K, alors le groupe de Galois de la clôture galoisienne $F/\mathbb{Q}$ de P est isomorphe au groupe symétrique S_n et l'extension F/K est non ramifiée de groupe de Galois isomorphe à A_n.*

La preuve utilise le fait que le groupe de Galois de $F/\mathbb{Q}$ est un sous-groupe primitif de S_n qui contient une transposition : c'est donc le groupe S_n.

Nous avons ensuite besoin du lemme suivant :

Lemme 3.6. *Partons d'un polynôme $P \in \mathbb{Z}[X]$ irréductible unitaire dont le discriminant d_P de P est le discriminant d'un corps quadratique. Soit $M = \mathbb{Q}(\theta)$ un corps de rupture de P, ici θ est une racine de P dans $\overline{\mathbb{Q}}$. Alors $\mathcal{O}_M = \mathbb{Z}[\theta]$.*

Démonstration: C'est immédiat, cela provient tout simplement du fait que comme $\mathrm{d}_M \equiv 0, 1 \pmod 4$, alors nécessairement $\mathrm{d}_M = \mathrm{d}_P$. □

Rappelons maintenant le lemme bien connu suivant (voir par exemple [**Kon**]).

Lemme 3.7. *Sous les conditions de cette section, si le nombre premier p divise d_P, on a $p\mathcal{O}_M = \mathfrak{p}_1 \cdots \mathfrak{p}_{g-1}\mathfrak{p}_g^2$, avec $f_g = 1$. Ou de façon équivalente, sur $\mathbb{F}_p$ le polynôme P se factorise de la façon suivante :*

$$P = Q_{f_1} \cdots Q_{f_{g-1}} (X - x_0)^2 \in \mathbb{F}_p[X],$$

où les polynômes Q_{f_i} sont des polynômes irréductibles de degré f_i et premiers entre eux.

Soit donc un nombre premier p ramifié. Comme $\mathcal{O}_M \simeq \mathbb{Z}[X]/(P)$, la réduction de la factorisation de $P = P_1 \cdots P_g$ dans $\mathbb{Q}_p[X]$ montre que le polynôme ramifié P_g vérifie : $P_g = (X - x_0)^2 \in \mathbb{F}_p[X]$. Soit α une racine de P_g dans $\overline{\mathbb{Q}_p}$. Comme nous l'avons vu dans le précédent paragraphe 3.2.1, nous cherchons à savoir si $\mathbb{Q}_p(\sqrt{\mathrm{d}_P}) = \mathbb{Q}_p(\alpha)$. A ce niveau, utilisons la globalité de la situation. En effet, si l'on note par ϑ le produit de f_i-cycles à supports disjoints, $i = 1, \ldots, g-1$, alors toujours d'après le paragraphe 3.2.1, le Frobenius $\sigma_{\mathfrak{p}}$ dans $\mathrm{Gal}(F/K)$ est soit (conjugué à) ϑ, soit le produit $\vartheta \cdot \tau$, où τ est une transposition à support disjoint de ϑ. Si l'on se rappelle que $\sigma_{\mathfrak{p}} \in A_n$, on voit que c'est la signature $\varepsilon(\vartheta)$ de l'élément ϑ qui permet alors de conclure.

Corollaire 3.8. *Sous les hypothèses de ce paragraphe, $\mathbb{Q}_p(\sqrt{\mathrm{d}_P}) = \mathbb{Q}_p(\alpha)$ si et seulement si $\varepsilon(\vartheta) = +1$.*

Exemple 3.9. Soit le polynôme $P = X^{11} + X + 123$ de discriminant $\mathrm{d}_P = -\ell$ avec $\ell = 22613649218372985685884825021253 9$. Ici, ℓ est un nombre premier. Ici $P = (Q_1^{(1)})^2\, Q_1^{(2)}\, Q_1^{(3)}\, Q_7 \in \mathbb{F}_\ell[X]$, où les polynômes $Q_1^{(i)}$ sont des polynômes de degré 1 et où Q_7 est un polynôme irréductible de degré 7. Ici ϑ est un 7-cycle et $\mathbb{Q}_\ell(\sqrt{\mathrm{d}_P}) = \mathbb{Q}_\ell(\alpha)$, où α est une racine de P dans $\overline{\mathbb{Q}_\ell}$ (selon les notations précédentes).

Notons alors que le groupe de décomposition de ℓ dans $F/\mathbb{Q}$ est cyclique, isomorphe à $\mathbb{Z}/14\mathbb{Z}$. Cet exemple donne une réponse pour S_{11} à la *Question arithmétique* de Bubboloni et Sonn, §1 de [**BS**]. Nous retrouvons le même phénomène pour le groupe S_{19} avec le polynôme $P = X^{19} + X + 191$.

Exemple 3.10. Soit le polynôme $P = X^5 + X + 5$ de discriminant $\mathrm{d}_P = 3 \cdot 651127$.

Sur $\mathbb{F}_3$ la factorisation de P est de la forme $(X-x_0)^2Q_3$; ainsi $\varepsilon(\vartheta) = +1$.

Sur $\mathbb{F}_{651127}$ la factorisation de P est de la forme $(X-x_0)^2Q_1Q_2$; ainsi $\varepsilon(\vartheta) = -1$. Pour ce second nombre premier $\ell = 651127$, on remarque que le groupe de décomposition de ℓ dans $F/\mathbb{Q}$ est isomorphe au groupe de Klein.

3.2.3. Frobenius et classes conjuguées. Revenons à notre contexte en supposant que le discriminant du polynôme P est sans facteurs carrés.

Partons d'un couple de caractères conjugués (χ, χ') de S_n. Soit le tableau de Young symétrique T associé aux caractères χ et χ' (voir la sous-section 3.1) ; notons $\mathcal{C}_{\mathrm{T}} = [q_1]\cdots[q_k]$ sa classe associée. On rappelle que les entiers q_i sont impairs, deux à deux distincts et que $\sum_i q_i = n$.

D'autre part soit p un nombre premier et soit $\mathfrak{p}|p$ un idéal premier de $K = \mathbb{Q}(\sqrt{\mathrm{d}_P})$. Notons par $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(F/K)$ l'automorphisme de Frobenius de l'idéal premier $\mathfrak{p}$.

Ecrivons ensuite la factorisation de P sur $\mathbb{F}_p$:

$$P = P_{f_1}\cdots P_{f_g}^{e_g} (\mathrm{mod}\, p\mathbb{F}_p[X]),$$

où les polynômes $P_{f_i} \in \mathbb{F}_p[X]$ sont irréductibles (distincts) de degré f_i avec $e_g \geq 2$.

Proposition 3.11. *L'automorphisme de Frobenius $\sigma_{\mathfrak{p}}$ sépare les caractères χ et χ' si et seulement si, $e_g = 1$ et la famille des f_i est égale à la famille des q_i. En particulier, les entiers f_i sont impairs et deux à deux distincts.*

Démonstration: Supposons que $\sigma_{\mathfrak{p}}$ sépare le couple de caractères conjugués (χ, χ'). D'après le paragraphe 3.2.1, le nombre premier p est décomposé dans $\mathbb{Q}(\sqrt{\mathrm{d}_P})/\mathbb{Q}$ et ainsi $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{P}}$ (sans oublier que $e_g = 1$). Or d'après la proposition 3.1, $\sigma_{\mathfrak{p}}$ est un produit de q_i-cycles d'où l'égalité entre le famille des f_i et celle des q_i.

Réciproquement. Si $\mathfrak{P}$ est non ramifié et tel que $\sigma_{\mathfrak{P}}$ s'écrit comme un produit de q_i-cycles à supports disjoints avec q_i impairs. Alors $\sigma_{\mathfrak{P}} \subset A_n$ et p est donc décomposé dans $K/\mathbb{Q}$. Ainsi $\sigma_{\mathfrak{P}} = \sigma_{\mathfrak{p}}$ et $\sigma_{\mathfrak{p}}$ sépare bien le couple (χ, χ'). □

Exemple 3.12. Soit n impair. Partons du caractère irréductible φ associé à la partition $n = ((n+1)/2, 1, \ldots, 1)$; le tableau de Young associé est symétrique et la classe de conjugaison associée est la classe des n-cycles. Le caractère φ est de degré $b_0(n)$ où

$$b_0(n) = \frac{(n-1)!}{\left[\left(\frac{n-1}{2}\right)!\right]^2} \sim \frac{2^{n-\frac{1}{2}}}{\sqrt{\pi}\sqrt{n-1}}.$$

Alors il existe deux caractères irréductibles distincts χ et χ' de A_n de degré $b(n) = \frac{b_0(n)}{2}$ qui sont séparés uniquement par la classe de conjugaison d'un n-cycle. Dans le cas où ce n-cycle correspond à la classe de conjugaison du Frobenius $\sigma_{\mathfrak{p}}$, $\mathfrak{p}|p$, le nombre premier p est décomposé dans $K/\mathbb{Q}$ et $\mathrm{N}(\mathfrak{p}) = p$. A noter que la proportion de nombres premiers p dont le Frobenius appartient à la classe d'un n-cycle est égale à $\frac{(n-1)!}{n!} = \frac{1}{n}$.

En conclusion, dans le cadre d'un polynôme P de discriminant d_P sans facteurs carrés, les caractères χ et χ' sont séparés par les Frobenius $\sigma_{\mathfrak{p}}$ de $\mathfrak{p}|p$ si et seulement si P est irréductible dans $\mathbb{F}_p[X]$.

Exemple 3.13. Le point (ii) du corollaire 1.6 correspond à la représentation irréductible ρ_T dont le tableau de Young a pour partition $n = \left(\frac{n}{4}+1, \frac{n}{4}+1, 2, \ldots, 2\right)$; elle est associée à la classe $\mathcal{C}_T = \left[\frac{n}{2}+1\right]\left[\frac{n}{2}-1\right]$. En utilisant la "formule des crochets" (voir, par exemple, la formule 4.12, p. 50 de [**FH**]), nous trouvons

$$b(n) = \frac{1}{2}\frac{n!}{(\frac{n}{2}+1)(\frac{n}{2}-1)[\frac{n}{2}(\frac{n}{4})!(\frac{n}{4}-1)!]^2} \sim_{n\to\infty} \frac{2^{\frac{3}{2}}4^n}{n^{\frac{7}{2}}\pi^{\frac{3}{2}}}.$$

Le point (iii) correspond au tableau de Young symétrique de partition $n = m^2 = (m, m, \ldots, m)$ et à la classe $\mathcal{C}_T = [2m-1][2m-3]\cdots[1]$. On obtient :

$$b(n) = \frac{1}{2}\frac{n!}{\prod_{r=1}^{m}\frac{(2m-r)!}{(m-r)!}} \sim_{m\to\infty} \frac{\mathrm{e}^{m^2} m^{m^2+\frac{m}{2}+1}}{2^{\frac{3m^2+m+1}{2}}\pi^{\frac{m-1}{2}}}.$$

3.2.4. La méthode de Bellaïche. Revenons sur la borne donnée par Bellaïche dans le contexte des groupes S_n.

Théorème 3.14 (Bellaïche [**Bel**, théorème 3])**.** *Soit $F/\mathbb{Q}$ une extension galoisienne de groupe de Galois G isomorphe au groupe S_n que l'on suppose non ramifiée en dehors de l'ensemble Σ. Soit $\mathcal{C}$ une classe de conjugaison de S_n. Le plus petit nombre premier p tel que le Frobenius $\sigma_p \in \mathcal{C}$ vérifie*

$$p \leqslant c_{16}\Psi(\mathcal{C})^2 \ln^2(M),$$

où $M = \prod_{\ell\in\Sigma}\ell$. Ici

$$\Psi(\mathcal{C}) = \sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathcal{C})|\chi(1),$$

$\mathrm{Irr}(G)$ *désignant l'ensemble des caractères irréductibles de G.*

Démonstration: C'est donc simplement une application du théorème 3 de [**Bel**] : si $\mathbb{I}_{\mathcal{C}}$ désigne la fonction indicatrice de $\mathcal{C}$, en suivant les notations de [**Bel**] et en s'apppuyant sur sa proposition 16, on a :

$$\varphi_G(\mathcal{C}) \leq \frac{\lambda(\mathbb{I}_{\mathcal{C}})}{\mu(\mathbb{I}_{\mathcal{C}})} = \lambda(\mathbb{I}_{\mathcal{C}})\frac{|G|}{|\mathcal{C}|}$$

et

$$\lambda(\mathbb{I}_{\mathcal{C}}) = \sum_{\chi\in\mathrm{Irr}\,G} |\langle\chi, \mathbb{I}_{\mathcal{C}}\rangle|\chi(1) = \frac{|\mathcal{C}|}{|G|}\sum_{\chi\in\mathrm{Irr}\,G} |\chi(\mathcal{C})|\chi(1). \qquad \square$$

Remarque 3.15. Comme noté par le rapporteur, le corollaire 1.5 peut se déduire du théorème 13 de [**Bel**] en prenant l'ensemble $D = \{g \in G,\ \chi(g) \neq \chi'(g)\}$ et la fonction $f = (\chi - \chi')\overline{(\chi - \chi)}$.

Prenons alors une classe de conjugaison $\mathcal{C} = [q_1]\cdots[q_k]$ dont la restriction à A_n se décompose en deux classes de conjugaison. La méthode que nous proposons ici, basée sur la séparation des caractères, donne l'inégalité $p \leqslant c_4\left[\frac{\chi_{\mathrm{T}}(1)}{2}\right]^4 \ln^2|\mathrm{d}_P|$, où χ_{T} est le caractère irréductible associé à la classe $\mathcal{C}$ de tableau de Young symétrique T formé par un empilement des crochets symétriques de longueur q_i, $i = 1, \ldots, k$.

On en arrive à la comparaison des quantités

$$\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathcal{C})|\chi(1) = \sum_{\lambda \text{ partition de } S_n} |\chi_\lambda(\mathcal{C})|\chi_\lambda(1) \quad \text{et} \quad \left[\frac{\chi_{\mathrm{T}}(1)}{2}\right]^2.$$

Donnons quelques exemples.

Exemple 3.16. Pour n impair, prenons le tableau de Young T de partition $\left(\frac{n+1}{2}, 1, \ldots, 1\right)$. Comme nous l'avons vu dans l'exemple 3.12, $\left[\frac{\chi_{\mathrm{T}}(1)}{2}\right]^2 \sim \frac{2^{2n-3}}{\pi(n-1)}$.

D'un autre côté, en notant $\mathcal{C}_T$ la classe de conjugaison associée aux cycles de longueur n, on a $\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathcal{C}_{\mathrm{T}})|\chi(1) = 2^{n-1}$.

Exemple 3.17. Pour n pair, prenons le tableau de Young symétrique T de partition $\left(\frac{n}{2}, 2, 1, \ldots, 1\right)$; ici $\mathcal{C}_T = [n-1][1]$.

On obtient

$$\chi_T(1) = \frac{4(n-2)!}{n\left[\left(\frac{n}{2}-2\right)!\right]^2} \sim \frac{n^{\frac{1}{2}}2^{n-\frac{3}{2}}}{\sqrt{\pi}}$$

d'où $\left[\frac{\chi_{\mathrm{T}}(1)}{2}\right]^2 \sim \frac{n2^{2n-5}}{\pi}$. D'un autre côté, avec les calculs de l'exemple 3.4, on trouve :

$$\begin{aligned}\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathcal{C})|\chi(1) &= |\chi_{(1,\dots,1)}(\mathcal{C})|\chi_{(1,\dots,1)}(1) + |\chi_{(n)}(\mathcal{C})|\chi_{(n)}(1)\\ &\quad + \sum_{k=2}^{n-2} |\chi_{(k,2,1,\dots,1)}(\mathcal{C})|\chi_{(k,2,1\dots,1)}(1)\\ &= 2 + \sum_{k=2}^{n-2} \frac{n!}{(n-1)k(n-k)(k-2)!(n-k-2)!}\\ &= n2^{n-2} - 2^n + 2^2.\end{aligned}$$

Exemple 3.18. Soit le groupe S_9 et soit le tableau de Young associé à la partition $\lambda = (3,3,3)$. C'est un tableau symétrique dont la classe de conjugaison C associée a pour décomposition [3][2][1]. Le caractère χ_{T} est de degré 42. A l'aide de Magma, on a $\sum_{\chi\in\mathrm{Irr}(G)} |\chi(\mathcal{C})|\chi(1) = 1286$.

Question 3.19. *Pour certains diagrammes de Young symétriques, le comportement asymptotique de la quantité introduite par Bellaïche est meilleur. Est-ce que c'est vrai pour tous les diagrammes symétriques ?*

3.3. Sur les extensions non ramifiées d'un corps de nombres. *On continue toujours à supposer GRH et la conjecture d'Artin vraies pour les fonctions L considérées.*

3.3.1. Un exemple de base : le p-rang du groupe des classes. La version effective du théorème de Chebotarev et un argument élémentaire de dénombrement permettent de donner une borne supérieure pour le nombre $n(p)$ de caractères abéliens non ramifiés d'ordre p de K et ainsi de majorer le p-rang $d_p \operatorname{Cl}_K$ du groupe des classes Cl_K de K. Cette méthode ne donne pas la meilleure borne mais, néanmoins, d'une part, conjecturalement, le résultat obtenu pour le p-rang n'est pas si mauvais que ça et puis d'autre part, elle a le mérite de s'étendre à d'autres situations ce que nous ferons à la fin de cette section (en s'inspirant de [**RT**]).

Précisons cette méthode. Soit l'entier X qui, pour tout couple de caractères distincts de degré 1 (χ,χ') non ramifiés et d'ordre p, assure l'existence d'un idéal premier $\mathfrak{p}$ de K tel que $\mathrm{N}(\mathfrak{p}) \leqslant X$ et tel que $\chi(\sigma_{\mathfrak{p}}) \neq \chi'(\sigma_{\mathfrak{p}})$. Notons que quand $\sigma_{\mathfrak{p}}$ varie, les valeurs de $\chi(\sigma_{\mathfrak{p}})$ et de $\chi'(\sigma_{\mathfrak{p}})$ se trouvent dans un ensemble de cardinal p. Les caractères χ de degré 1 et d'ordre p sont donc déterminés par les valeurs $\chi(\sigma_{\mathfrak{p}})$, avec $\mathrm{N}(\mathfrak{p}) \leqslant X$: il y a au plus p^N caractères de ce type. Le théorème des nombres premiers donne ensuite l'existence d'une constante c_{17} telle que

$$|\{\mathfrak{p} \in \mathcal{O}_K,\, \mathrm{N}(\mathfrak{p}) \leqslant X\}| \leqslant c_{17}[K:\mathbb{Q}]X/\ln X.$$

En conclusion, on a :

$$\ln(n(p)) \leqslant c_{17} \ln(p)[K : \mathbb{Q}]X/\ln(X).$$

Théorème 3.20. *Soit χ un caractère de degré 1 non ramifé et non trivial de G_K. Il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ de norme $\mathrm{N}(\mathfrak{p}) \leqslant c_4 \ln^2 |\mathrm{d}_K|$ tel que $\chi(\sigma_\mathfrak{p}) \neq 1$.*

On en déduit alors facilement :

Corollaire 3.21. *Soient χ et χ' deux caractères non ramifiés distincts de K de degré 1 et d'ordre p. Alors il existe un idéal premier $\mathfrak{p}$ de K de norme $\mathrm{N}(\mathfrak{p}) \leqslant c_4 \ln^2 |\mathrm{d}_K|$ tel que $\chi(\mathfrak{p}) \neq \chi'(\mathfrak{p})$.*

Démonstration: En effet, il suffit d'appliquer le théorème 3.20 à $\varphi = \chi\overline{\chi'}$ puis de noter que φ est de degré 1. □

En conclusion, on obtient :

Corollaire 3.22. *Pour tout corps de nombres K,*

$$d_p \mathrm{Cl}_K = \frac{1}{\ln(p)} \ln(n(p)) \leqslant c_{17}[K : \mathbb{Q}] \frac{c_4 \ln^2 |\mathrm{d}_K|}{\ln c_4 + 2 \ln\ln |\mathrm{d}_K|}.$$

Rappelons alors à ce niveau la question suivante :

Question 3.23 (Serre [**Ser2**, §2.5])**.** *A-t-on $\mathrm{N}(\mathfrak{p}) \ll_\varepsilon \ln^{1+\varepsilon} |\mathrm{d}_K|$?*

Dans le cadre du p-rang du groupe des classes, cette question est à rapprocher de l'inégalité facile du théorème de Brauer–Siegel (voir par exemple le lemme 2 du chapitre XVI, p. 322 de [**Lan**]) qui aboutit au résultat suivant :

Théorème 3.24. *Pour tout corps de nombres, on a :*

$$d_p \mathrm{Cl}_K \leqslant c_{18} \frac{1}{\ln p} \ln |\mathrm{d}_K|.$$

Remarque 3.25. En particulier à K fixé, le théorème de Brauer–Siegel indique bien que $d_p \mathrm{Cl}_K = 0$ pour p assez grand. Ce qui n'est pas le cas de l'inégalité du corollaire 3.22.

Remarque 3.26. Par deux approches différentes, la théorie analytique des nombres apporte deux estimations pour $d_p \mathrm{Cl}_K$. La première peut être adaptée à tout groupe simple $\mathcal{S}$ (ce sera l'objet de la section à venir). Quant à la seconde, elle découle de la formule analytique du nombre de classes et donc propre au groupe des classes.

Pour tenter d'être complet, citons également les travaux plus récents d'Ellenberg–Venkatesh [**EV1**], [**EV2**] et d'Ellenberg [**Ell**], pour une approche utilisant la géométrie des nombres.

3.3.2. Caractères de degré $r > 1$. Étant donné un groupe simple $\mathcal{S}$ fixé, une question naturelle consiste à chercher un résultat sur le modèle du p-rang du groupe des classes.

Fixons donc un groupe simple $\mathcal{S}$ et soit χ un caractère non trivial de $\mathcal{S}$ (de plus petit degré $r > 1$).

Notons par $k(\mathcal{S})$ le nombre de classes de conjugaison de $\mathcal{S}$ et soit $a(\chi)$ le nombre de valeurs prises par χ (c'est une extension de la définition 3.2). Commençons par la première estimation suivante pour $a(\chi)$.

Lemme 3.27. *On a :* $a(\chi) \leqslant k(\mathcal{S}) \leqslant 1 + \frac{|\mathcal{S}|-1}{r^2}$.

Démonstration: Cela provient simplement de la formule $\sum_\psi \psi(1)^2 = |\mathcal{S}|$, la somme portant sur les caractères irréductibles de $\mathcal{S}$, et du fait que le nombre de représentations irréductibles d'un groupe fini est égal à son nombre de classes de conjugaison. □

Rappelons maintenant le résultat de Collins qui précise le théorème de Jordan sur les sous-groupes simples de $\mathrm{Gl}_n(\mathcal{C})$.

Théorème 3.28 (Collins [**Col**])**.** *Soit $\mathcal{S} \hookrightarrow \mathrm{Gl}_n(\mathcal{C})$ un groupe simple. Alors si $n \geqslant 71$, on a $|\mathcal{S}| \leqslant (n+1)!$.*

En d'autres termes, ce résultat donne une borne inférieure asymptotique (suivant $|\mathcal{S}|$) sur le degré minimal r des représentations non triviales des groupes simples. Associée au lemme 3.27, on obtient (pour $r \geqslant 71$)

$$a(\chi) \ll \frac{(r+1)!}{r^2}.$$

Revenons au contexte arithmétique. Soit un entier $k \geq 1$. Supposons que le corps de nombres K admette une extension galoisienne non ramifiée de groupe de Galois G vérifiant $G \simeq \mathcal{S} \times \overset{(k)}{\cdots} \times \mathcal{S}^k$. Alors $\hat{G} \simeq \prod_{i=1}^k \hat{\mathcal{S}}$, isomorphisme en un sens évident. Considérons ensuite les caractères irréductibles de G de la forme $\varphi_i = \mathbf{1} \otimes \cdots \mathbf{1} \otimes \chi \otimes \mathbf{1} \cdots \otimes \mathbf{1}$, où l'on rappelle que χ est un caractère non trivial de degré r (que l'on peut supposer minimal) et où $\mathbf{1}$ est le caractère trivial. Les caractères φ_i sont irréductibles de degré r et ils prennent les mêmes valeurs que le caractère χ.

Soient alors $i \neq j$. Par le corollaire 1.5, on sait qu'il existe un idéal premier $\mathfrak{p}$ de norme plus petite que

$$X = c_4 r^4 \ln^2 |\mathrm{d}_K|$$

et tel que $\varphi_i(\sigma_\mathfrak{p}) \neq \varphi_j(\sigma_\mathfrak{p})$. En d'autres termes, l'idéal premier $\mathfrak{p}$ sépare les caractères φ_i et φ_j. Posons $N = \mathrm{card}\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathrm{N}(\mathfrak{p}) \leqslant X\}$.

La famille $(\varphi_j(\sigma_{\mathfrak{p}_1}), \dots, \varphi_j(\sigma_{\mathfrak{p}_N}))$, où $\mathfrak{p}_i$ est le i-ème idéal premier de norme plus petite que X, est donc représentative d'un caractère φ_j. D'autre part, pour chaque $i \in [\![1, N]\!]$ et tout entier $j \in \{1, \dots, k\}$, la quantité $\varphi_j(\sigma_{\mathfrak{p}_i})$ peut prendre au maximum $a(\chi)$ valeurs différentes. Ainsi, on obtient :

$$k \leqslant a(\chi)^N.$$

Souvenons nous ensuite que $N \leqslant c_{17}[K : \mathbb{Q}]X/\ln X$, pour obtenir :

Théorème 3.29. *Sit K un corps de nombres. Soit $\mathcal{S}$ un groupe fini simple, r le plus petit degré d'une représentation non-triviale de $\mathcal{S}$, χ un tel caractère de degré r, $a(\chi)$ le nombre de valeurs distinctes prises par χ. Soit k le plus grand entier tel qu'il existe une extension galoisienne de K, ramifiée nulle-part, de groupe de Galois $\mathcal{S}^k$. Alors*

$$\ln(k) \leqslant c_4 c_{17} \frac{\ln a(\chi)}{\ln r} r^4 [K : \mathbb{Q}] \ln^2 |\mathrm{d}_K|.$$

Rouse et Thorne dans [**RT**] donne l'inégalité $\ln(k) \ll r^5[K : \mathbb{Q}] \ln^2 |\mathrm{d}_K|$ faisant donc apparaître une puissance r^5.

Revenons à l'estimation issue de l'inégalité donnée par Collins : pour r assez grand, $\ln a(\chi) \ll r \ln r \dots$ ce qui redonne le résultat de Rouse et Thorne. Mais comme le montre le cas du groupe alterné, cette majoration peut être nettement améliorée.

Exemple 3.30. Dans le cas du groupe alterné $\mathcal{S} = A_n$, on a $a(\chi) \leqslant 2r + 3$ (voir page 490) et ainsi la borne du théorème 3.29 est en r^4. Plus précisément, si l'on prend le diagramme de Young T de partition $\lambda = (n-1, 1)$, alors le caractère χ_{T} associé est de degré $n-1$ (pour $n \geq 7$, c'est le caractère non trivial de plus petit degré) et $a(\chi_T) = \mathcal{O}(n)$. Ainsi on obtient ici : $\ln(k) \ll_K n^4$.

Remarque 3.31. Lorsque $r = 1$, le corollaire 3.22 s'obtient avec une approche légèrement différente. En effet, soit le groupe simple $\mathcal{S} = \mathbb{Z}/p\mathbb{Z}$. On considère les caractères φ_i de la forme $\varphi = \chi_1 \otimes \cdots \otimes \chi_k$, où les caractères χ_i sont de degré 1. Ces caractères sont de degré $1^k = 1$. La borne du corollaire 1.5 n'est pas impactée et cette démarche apporte alors $(p-1)^k$ caractères d'ordre p.

3.3.3. Une variante : les extensions modérèment ramifiées d'un corps de nombres. Dans la section précédente, comme les représentations en jeu sont non ramifiées, les conducteurs sont réduits à leurs plus simples expressions. Dans cette section, nous reprenons ces calculs pour des situations où les conducteurs de produit tensoriel se "simplifient".

Commençons par donner une remarque.

Remarque 3.32. Soit ρ une représentation de caractère χ. L'ensemble des valeurs prises par $\chi(\sigma_{\mathfrak{p}})$, quand $\mathfrak{p}$ varie, peut différer de l'ensemble des valeurs du caractère χ : cette différence provient des places ramifiées et de la définition de $\chi(\sigma_{\mathfrak{p}})$ dans ce cas particulier. Par contre, on a de façon évidente

$$|\{\chi(\sigma_{\mathfrak{p}}),\, \mathfrak{p} \subset \mathcal{O}_K\}| \leqslant a(\chi) + |\Sigma|,$$

où Σ est l'ensemble des idéaux premiers $\mathfrak{p}$ ramifiés (à travers χ).

Soit A une matrice carrée, de taille $r \times r$, à coefficients complexes. Si A est d'ordre 2, on définit la *signature* de A comme étant le couple (r_+, r_-), où r_+ (respectivement r_-) est le nombre de valeurs propres de A égales à $+1$ (resp. à -1).

Soit $\rho\colon G_K \to \mathrm{Gl}_r(\mathbb{C})$ une représentation continue de caractère χ. Pour $\tau \in G_K$ tel que $\rho(\tau)$ est d'ordre 2, la signature de τ (relativement à ρ) est la signature de $\rho(\tau)$. Remarquons alors que $\rho(\tau)$ et $\rho^{-1}(\tau) = \overline{\rho}(\tau)$ ont même signature.

A présent, on s'intéresse aux représentations ρ (ou aux caractères χ) un *peu ramifiées* dans le sens suivant : si la représentation ρ est ramifiée en $\mathfrak{p}$ alors le groupe d'inertie de $\mathfrak{p}$ se factorise à travers un élément $\tau_{\mathfrak{p}}$ d'ordre 2. Si (r_+, r_-) est la signature de $\rho(\tau_{\mathfrak{p}})$, on dit alors que la représentation ρ est de $\mathfrak{p}$-signature (r_+, r_-).

Ainsi, si $\mathfrak{p}$ est au-dessus d'un nombre premier impair, la ramification en $\mathfrak{p}$ est modérée.

Lemme 3.33. *Soient $\mathfrak{p}$ un idéal premier ne divisant pas 2. Soient ρ et ρ' deux représentations (de caractères χ et χ') peu ramifiées en $\mathfrak{p}$ ayant pour conducteur local : $f_{\mathfrak{p}}(\chi) = p^k$ et $f_{\mathfrak{p}}(\chi') = p^{k'}$. Alors*

$$f_{\mathfrak{p}}(\chi \otimes \chi') = p^{k'(r-k)+k(r'-k')},$$

où r (respectivement r') est le degré de ρ (resp. de ρ').

Démonstration: C'est très facile. Partons de ρ. Comme la ramification est modérée, on a $\rho(G_{i,\mathfrak{p}}) = \{1\}$, pour $i \geqslant 1$. L'action de $G_{0,\mathfrak{p}}$ se factorise sur V à travers $\rho(\tau_{\mathfrak{p}})$ et la codimension de $V^{G_{0,\mathfrak{p}}}$ est exactement le nombre de valeurs propres de ρ valant -1. Ainsi ici ρ et ρ' sont de $\mathfrak{p}$-signatures $(r-k, k)$ et $(r'-k', k')$, et alors $\rho \otimes \rho'$ est une représentation de $\mathfrak{p}$-signature $\big(kk' + (r-k)(r'-k'), k(r'-k') + k'(r-k)\big)$, d'où le résultat. □

Les situations intéressantes pour nous sont celles où la borne brutale : $f_{\mathfrak{p}}(\chi\otimes\chi') \leqslant r' f_{\mathfrak{p}}(\chi) + r f_{\mathfrak{p}}(\chi')$ est très mauvaise. Typiquement, supposons

$r = r'$ puis que les représentations ρ et ρ' sont de même $\mathfrak{p}$-signature $(0, r)$ ou encore que $f_\mathfrak{p}(\chi) = f_\mathfrak{p}(\chi') = p^r$. Alors, d'après le lemme 3.33, $f_\mathfrak{p}(\chi \otimes \chi') = 0$.

Notons par $\mathcal{N}(\mathfrak{p}^r)$ le nombre de caractères de degré r peu ramifiés en $\mathfrak{p}$ ($\mathfrak{p} \nmid 2$) et ayant pour conducteur $\mathfrak{p}^r$. Appliquant la stratégie de la section précédente, on obtient

$$\ln(\mathcal{N}(\mathfrak{p}^r)) \ll r^5 [K : \mathbb{Q}] \ln^2 |\mathrm{d}_K|.$$

Cette non dépendance en $\mathfrak{p}$ n'est pas surprenante... en effet, comme les représentations en jeu sont de $\mathfrak{p}$-conducteur $\mathfrak{p}^r$, cela signifie que $\rho(\tau_\mathfrak{p}) = -I_r$, où I_r est la matrice identité. Donc $\rho(\tau_\mathfrak{p})$ est dans le centre de $\mathrm{Im}(\rho)$: le corps $F := \overline{K}^{\ker(\rho)}$ est une extension quadratique totalement et modérément ramifiée d'une extension non-ramifiée de F_0/K. La théorie du corps de classes indique que, étant donnée F_0, l'extension F/F_0 est unique.

Il faut donc aller un peu plus loin pour trouver une illustration non triviale.

Corollaire 3.34. *Sous les conditions précédentes,*

$$\ln \mathcal{N}(\mathfrak{p}^k)) \ll r[K : \mathbb{Q}] \Big(r^2 \ln |\mathrm{d}_K| + 2k(r-k) \ln \mathrm{N}(\mathfrak{p}) \Big)^2.$$

Retournons de nouveau vers les groupes alternés A_n, pour $n \geq 7$.

Un élément $\tau \in S_n$ est dit de longueur k si τ est le produit de k transpositions (à supports disjoints). On remarque que tout élément d'ordre 2 de A_n est le produit de k transpositions (à supports disjoints) pour un certain entier pair k.

Soit alors ρ l'unique représentation de A_n de degré $n-1$ et de caractère χ. D'après l'exemple 3.3, si τ est de longueur k, alors $\chi(\tau) = n - 1 - 2k$. Comme $\chi(\tau)$ est la somme de $+1$ et de -1, on a facilement que $\rho(\tau)$ est de signature $(n-k-1, k)$.

Notons par $\mathcal{N}(A_n, \mathfrak{p}, k)$ le nombre d'extensions du corps K de groupe de Galois isomorphe à A_n non ramifiée en dehors de $\mathfrak{p}$ et dont le groupe d'inertie en $\mathfrak{p}$ est le produit de k transpositions à supports disjoints.

Une synthèse de nos précédents résultats et discussions nous permet d'obtenir le corollaire suivant :

Corollaire 3.35. *Sous les conditions précédentes, on a*

$$\ln \mathcal{N}(A_n, \mathfrak{p}, k) \ll [K : \mathbb{Q}] \Big((n-1)^2 \ln |\mathrm{d}_K| + 2k(n-1-k) \ln \mathrm{N}(\mathfrak{p}) \Big)^2.$$

Remarque 3.36. Il est facile d'adapter un tel résultat au cas où $\mathfrak{p} | 2$.

Remarque 3.37. Il est possible de reprendre ces deux derniers corollaires en prenant un ensemble Σ d'idéaux premiers ramifiés non nécessairement réduit à un élément. Typiquement soit $\mathcal{N}(\Sigma,k)$ le nombre de caractères de degré r non ramifiés en dehors de Σ, peu ramifiés en $\mathfrak{p}\in\Sigma$ avec pour conducteur local $\mathfrak{p}^k$. Regardons l'évolution de $\mathcal{N}(\Sigma,k)$ suivant Σ. Quand la quantité $|\Sigma|$ est bornée, les inégalités des corollaires 3.34 et 3.35 restent valables. Par contre, si on cherche à connaître l'évolution suivant la croissance de $|\Sigma|$, on obtient la borne

$$\ln(a(\chi)+|\Sigma|)\frac{\big(\ln \mathrm{d}_K+2k(r-k)\sum_{\mathfrak{p}\in\Sigma}\ln \mathrm{N}(\mathfrak{p})\big)^2}{\ln|\Sigma|}\ll_{K,r,k}\left(\sum_{\mathfrak{p}\in\Sigma}\ln \mathrm{N}(\mathfrak{p})\right)^2.$$

4. Expérimentations numériques avec le groupe A_n

Nous allons nous placer dans le contexte des extensions non ramifiées de groupe de Galois le groupe alterné A_n pour tester la borne du corollaire 1.5 : déterminer l'idéal premier de plus petite norme dont le Frobenius sépare des caractères irréductibles de même degré. Selon le théorème 1.1, une borne est donnée en fonction du carré du logarithme du discriminant du corps de base et des puissances quatrièmes des degrés des représentations. Rappelons que par la théorie du corps de classes, les extensions abéliennes sont liées au groupe des classes (et leurs caractères irréductibles sont de degré 1). Pour les extensions non ramifiées de groupes de Galois simples (non abéliens !), il n'y a plus la théorie du corps de classes.

4.1. Familles et expérimentations. Nos calculs vont se faire dans des familles de trinômes irréductibles $P\in\mathbb{Q}[X]$: $P=X^n-uX+v$, avec $u,v\in\mathbb{Q}$. De telles familles ont été étudiées par de nombreux auteurs (Yamamoto [**Yam**], Uchida [**Uch**], etc.).

Rappelons le critère d'Uchida :

Théorème 4.1 (Uchida [**Uch**]). *Soit $P=X^\ell-uX+v\in\mathbb{Q}[X]$ un polynôme irréductible de corps des racines F. Si ℓ est un nombre premier et si $((\ell-1)u,\ell v)=1$, alors le groupe de Galois de P est isomorphe au groupe S_ℓ et l'extension $F/\mathbb{Q}(\sqrt{\mathrm{d}_P})$ est non ramifiée.*

Soient $\alpha_1,\dots,\alpha_n\in\mathbb{C}$ les racines de P. Notons par $M=\mathbb{Q}(\alpha_1)$ un corps de rupture de P, par $F=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ le corps de décomposition de P et soit $\mathrm{d}_P:=\prod_{i<j}(\alpha_i-\alpha_j)^2$ le discriminant de P. Pour un trinôme $P=X^n-uX+v$, $u,v\in\mathbb{Q}$, un calcul classique montre que :

$$\mathrm{d}_P=(-1)^{n(n-1)/2}\Big(n^nv^{n-1}-(n-1)^{n-1}u^n\Big).$$

Posons $K=\mathbb{Q}(\sqrt{\mathrm{d}_P})$.

Nous nous concentrons sur des familles de trinômes P_a de degré n à un seul paramètre, pour $n = 5$, 7 et 13, dont les groupes de Galois sous-jacents sont isomorphes à S_n. Ici, a est un paramètre qui va varier dans l'ensemble des nombres naturels $\mathbb{N}$. Pour un tel entier a, le groupe de Galois de F/K est isomorphe à A_n et si par exemple d_a est sans facteurs carrés, alors F/K est non ramifiée. Nous ressortons ensuite deux caractères χ_a et χ'_a de même degré (typiquement des caractères conjugués) et nous cherchons donc la plus petite norme $n(\chi_a, \chi'_a)$ de l'idéal premier $\mathfrak{p}$ dont le Frobenius sépare les caractères étudiés.

Nous déterminerons également pour X assez grand la quantité

$$\mu((P_a), \chi_a, \chi'_a, X) := \frac{\sum_{\mathrm{d}_a \leqslant X} n(\chi_a, \chi'_a)}{\sum_{\mathrm{d}_a \leqslant X} 1}.$$

Un point clef est de bien nous assurer que ces familles sont "exhaustives" en vérifiant que celles-ci contiennent une sous-famille de paramètres $(a_k)_k$ telle que : (i) le polynôme P_{a_k} est irréductible ; (ii) le groupe de Galois du corps des racines de P_{a_k} est S_n ; (iii) la quantité $n(\chi_{a_k}, \chi'_{a_k})$ peut être aussi grande que possible.

Nos expérimentations consistent à faire varier a entre 1 et 300000 pour le groupe alterné A_{13} (jusqu'à 500000 pour les groupes alternés A_5 et A_7). A chaque valeur de a permettant au polynôme P_a de satisfaire les conditions du théorème 4.1, nous calculons le discriminant d_a ainsi que la norme du plus petit idéal premier dont le Frobenius sépare les caractères χ_a et χ'_a. Pour des raisons de lisibilité, nous nous limitons à l'affichage de la plus grande norme lorsque a varie entre n et $n + 100$.

Le deuxième graphique obtenu correspond à l'évolution de $\mu((P_a), \chi_a, \chi'_a, x)$ lorsque x varie entre 1 et 300000 pour le groupe alterné A_{13} (jusqu'à 500000 pour les groupes alternés A_5 et A_7). Pour les mêmes raisons, nous utilisons un point par tranche de 1000.

4.1.1. Le groupe A_5. Commençons par le polynôme $P_a = X^5 + X + a$ de discriminant $\mathrm{d}_a = 5^5a^4 + 4^4$. On s'intéresse aux paramètres a pour lesquels d_a est le discriminant d'un corps quadratique. Alors nécessairement a est impair et la condition sur d_a est équivalente au fait que d_a est sans facteurs carrés. Si tel est le cas, le groupe de Galois sous-jacent est S_5, il fournit ainsi une extension non ramifiée F_a/K_a de groupe de Galois A_5 au-dessus du corps quadratique réel $K_a = \mathbb{Q}(\sqrt{\mathrm{d}_a})$.

Dans A_5, il y a cinq classes de conjugaison $\mathcal{C}_1 = (1)$, $\mathcal{C}_2 = (123)$, $\mathcal{C}_3 = (12)(34)$, $\mathcal{C}_4 = (12345)$ et $\mathcal{C}_5 = (21345)$ et deux caractères irréductibles

et conjugués χ et χ' de degré 3 provenant d'un caractère irréductible de S_5 de degré 6.

On cherche l'idéal premier $\mathfrak{p} \subset \mathcal{O}_K$ de plus petite norme pour lequel les caractères χ_a et χ'_a de degré 3 de $\mathrm{Gal}(F_a/K_a) \simeq A_5$ en le Frobenius $\sigma_\mathfrak{p}$ sont différents. Cela équivaut à déterminer le plus petit nombre premier p pour lequel $P_a \in \mathbb{F}_p[X]$ est irréductible.

Testons l'exhaustivité de la famille. Soient $p_1 = 2, \dots, p_k$ les k premiers nombres premiers et soit $a_k = -2 - p_2 \cdots p_k$. La factorisation de P_{a_k} dans $\mathbb{F}_7[X]$ indique que P_{a_k} est irréductible sur $\mathbb{Q}$. Par le résultat d'Uchida (théorème 4.1), l'extension sous-jacente est de groupe de Galois S_5. D'autre part pour $i = 2, \dots, k$, on a $P_{a_k}(1) \equiv 0 \pmod{p_i}$ et on peut vérifier que P_{a_k} est également réductible dans $\mathbb{F}_2[X]$. Par conséquent, le plus petit nombre premier p dont le Frobenius sépare les caractères χ_a et χ'_a est plus grand que p_{k+1}. Comme $\ln|\mathrm{d}_{a_k}| \sim_{k\to\infty} \mathrm{Cte} \cdot \ln p_1 \cdots p_k \sim_k \mathrm{Cte} \cdot p_k$ la borne de séparation des caractères χ_{a_k} et χ'_{a_k} donnée par le corollaire 1.5 est alors en p_k^2 (à une constante près)… à comparer donc avec l'idéal premier de plus petite norme qui sépare χ_a et χ'_a, de norme au moins p_{k+1}.

Notons à ce niveau que, sous GRH, $p_{k+1} \leqslant p_k + p_k^{1/2+\varepsilon}$ (cf. [**Nic**]).

Le plus grand nombre premier obtenu, dans les 183962 corps quadratiques étudiés, est 313 pour le polynôme $X^5 + X + 180895$ de discriminant $3 \cdot 7 \cdot 43 \cdot 3705685202388396493027 \approx 3.4 \cdot 10^{24}$.

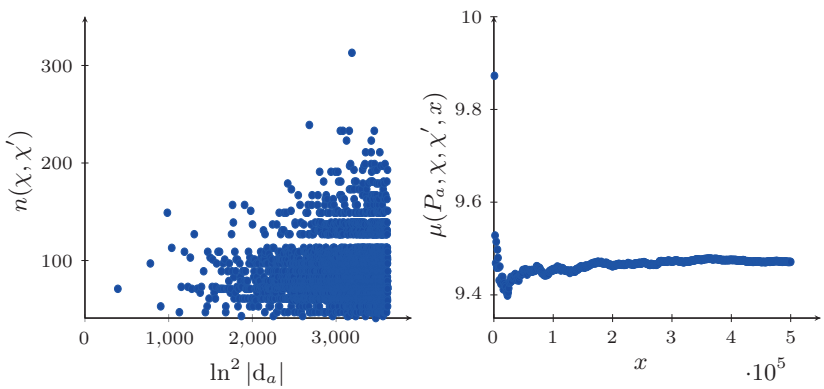

Figure 1. Pour les caractères de degré 3 de A_5 définis par $P_a = X^5 + X + a$.

De la même façon, considérons la famille de polynômes $P_a = X^5 - aX + 1$ avec a tel que P_a est irréductible et tel que d_a est sans facteurs carrés. Ici $\mathrm{d}_a = 5^5 - 4^4 a^5$ et les corps quadratiques $K = \mathbb{Q}(\sqrt{\mathrm{d}_a})$ sont imaginaires.

En posant $a_k = 2 + p_2 \dots p_k$, la famille de polynômes P_{a_k} vérifie bien les conditions d'exhaustivité voulues : comme a_k est premier à 5 (condition nécessaire pour que d_a soit sans facteurs carrés), le groupe de Galois sous-jacent est S_5 ; la réduction dans $\mathbb{F}_7$ donne l'irréductibilité ; comme pour le cas précédent, $P_{a_k}(1) \equiv 0 \pmod{p_i}$ pour $i = 2, \dots, k$ et ainsi le plus petit nombre premier p dont le Frobenius sépare les caractères χ_a et χ'_a associés aux 5-cycles est plus grand que p_{k+1}.

Quand $1 \leqslant a \leqslant 500000$, nous obtenons une famille de 341266 corps à étudier. Le plus grand nombre premier obtenu est 331 pour le polynôme $X^5 - 153032X + 1$, de discriminant $-3 \cdot 2129 \cdot 3363987086007650773200841 \approx -2.2 \cdot 10^{28}$.

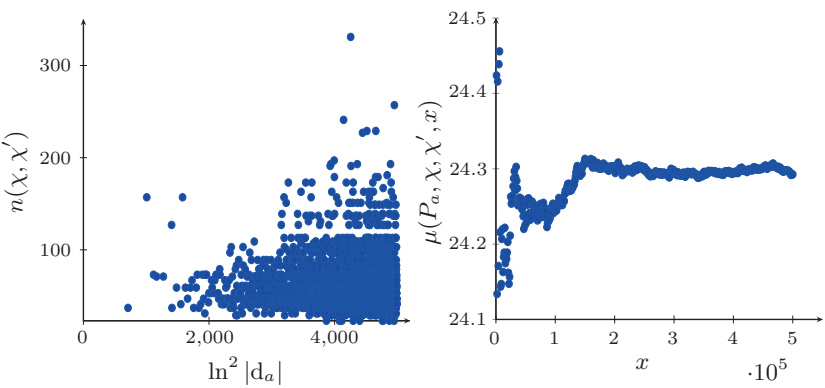

FIGURE 2. Pour les caractères de degré 3 de A_5 définis par $P_a = X^5 - aX + 1$.

4.1.2. Le groupe A_7. Dans A_7, il y a deux caractères irréductibles de degré 10 et deux caractères irréductibles de degré 14.

Les caractères de degré 10. Comme pour les caractères irréductibles de degré 3 de A_5, les deux caractères irréductibles de degré 10 sont conjugués et proviennent d'un même caractère irréductible de S_7. Ils sont séparés par le Frobenius $\sigma_{\mathfrak{p}}$ lorsque celui-ci est un 7-cycle, ce qui équivaut au fait que $P \in \mathbb{F}_p[X]$ est irréductible.

Pour $1 \leqslant a \leqslant 500000$, considérons les polynômes irréductibles de la forme $P_a = X^7 - 2X + a$, dont les discriminants sont sans facteurs carrés (cela implique $(a, 6) = 1$) : on obtient une famille de 150072 corps.

En posant $a_k = 1 + p_1 \dots p_k$, le polynôme P_{a_k} vérifie bien les conditions d'exhaustivité : sa réduction modulo 3 donne son irréductibilité, le résultat d'Uchida montre que le groupe sous-jacent est S_7 et comme $P_{a_k}(1) \equiv 0 \pmod{p_i}$ pour $i = 2, \dots, k$, on obtient bien que le plus petit nombre premier pour lequel P_{a_k} est irréductible dans $\mathbb{F}_p$ est supérieur à p_{k+1}.

Dans la liste obtenue, on note que le plus grand nombre premier obtenu est 461 pour le polynôme $X^7 - 2X + 432131$ de discriminant $-5 \cdot 11 \cdot 199 \cdot 26796293 \cdot 138350621 \cdot 1321621877863261503 19 \approx 5.4 \cdot 10^{40}$.

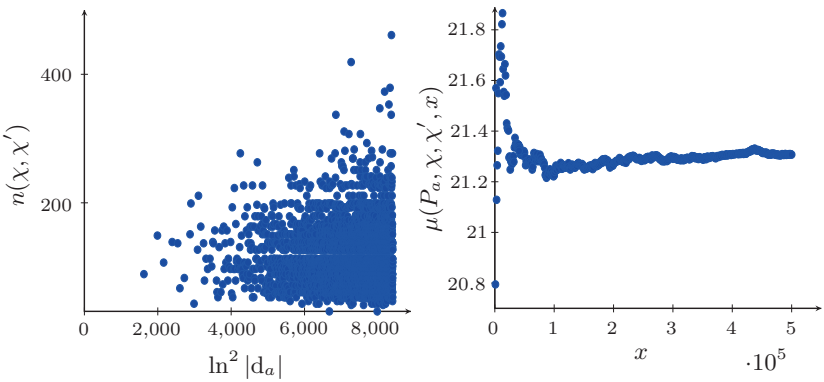

Figure 3. Pour les caractères de degré 10 de A_7 définis par $P_a = X^7 - 2X + a$.

Les caractères de degré 14. Les deux caractères irréductibles de degré 14 proviennent des partitions $(4, 3)$ et $(5, 2)$, ils ne sont pas conjugués. Les caractères χ et χ' ont les mêmes polynômes caractéristiques pour 6 classes de conjugaison mais n'ont pas les mêmes pour 3 classes : ce sont les classes où intervient au moins un 3-cycle. (Il y a donc les 3-cycles, les produits de deux 3-cycles et le produit d'un 3-cycle avec deux transpositions.) Ainsi le Frobenius $\sigma_{\mathfrak{p}}$ sépare les caractères de degré 14 si et seulement si il est dans une classe contenant un 3-cycle.

Utilisons nos observations des paragraphes 3.2.1 et 3.2.2.

Si p est non ramifié *i.e.*, si p ne divise pas d_P, on a vu que ou bien $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{P}}$ ou bien $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{P}}^2$. Dans le premier cas, $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si, $\sigma_{\mathfrak{P}}$ contient un 3-cycle, si et seulement si, la factorisation de P dans $\mathbb{F}_p[X]$ contient un facteur irréductible de degré 3. Dans le second cas, $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si, $\sigma_{\mathfrak{P}}$ contient un 3-cycle ou un 6-cycle, si et seulement si, la factorisation de P dans $\mathbb{F}_p[X]$ contient un facteur irréductible de degré 3 ou un facteur irréductible de degré 6.

Si p est ramifié, alors $\sigma_{\mathfrak{p}}$ contient un 3-cycle si et seulement si, la factorisation de P dans $\mathbb{F}_p[X]$ contient un facteur irréductible de degré 3 (un facteur irréductible de degré 6 ne peut pas apparaître).

En conclusion le nombre premier p sépare les caractères de degré 14 si et seulement si, la factorisation de $P \in \mathbb{F}_p[X]$ contient un facteur irréductible de degré 3 ou de degré 6 (sous la condition sur d_P).

Soit la famille $P_a = X^7 - X + a$. En posant $a_k = p_3 \dots p_k$, le polynôme P_{a_k} vérifie bien les conditions voulues : P_a est irréductible modulo 2 ; comme $X^7 - X \equiv X(X-1)(X+1)(X^2-X+1)(X^2+X+1) \pmod{p_i}$, le plus petit nombre premier pour lequel on peut trouver un 3-cycle est supérieur à p_{k+1}.

Sur les 162866 corps étudiés, la plus grande norme de nombre premier obtenue est $83^2 = 6889$ pour le polynôme $X^7 - X + 254005$, de discriminant $-29 \cdot 47 \cdot 337 \cdot 4815197637447681406111736229405 49 \approx 2.3 \cdot 10^{39}$.

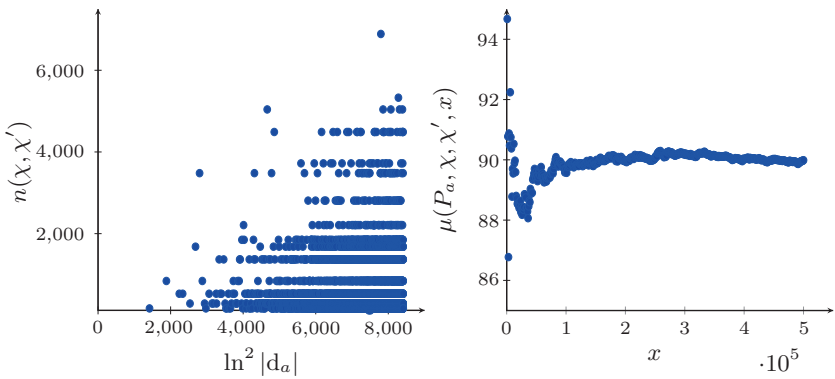

FIGURE 4. Pour les caractères de degré 14 de A_7 définis par $P_a = X^7 - X + a$.

4.1.3. Le groupe A_{13}. Il y a 3 couples de caractères irréductibles provenant de tableaux de Young symétriques :

— un couple de caractères de degré 462 séparés par les cycles de longueur 13 et donc par les Frobenius des nombres premiers p pour lesquels P est irréductible dans $\mathbb{F}_p[X]$;

— un couple de caractères de degré 8008 séparés par les Frobenius des nombres premiers p pour lesquels $P = Q_9 Q_3 Q_1 \in \mathbb{F}_p[X]$, où les polynômes Q_i sont irréductibles de degré i ;

— un couple de caractères de degré 4290 séparés par les Frobenius des nombres premiers p pour lesquels $P = Q_7Q_5Q_1 \in \mathbb{F}_p[X]$, où les polynômes Q_i sont irréductibles de degré i.

Soit $P_a = X^{13} + X + a$.

En prenant $a_k = -2 + p_3 \cdots p_k$, le polynôme P_{a_k} vérifie la condition d'exhaustivité pour les caractères de degré 462 : la réduction modulo 43 donne l'irréductibilité et le résultat d'Uchida indique que le groupe de Galois sous-jacent est S_{13}. Comme $P_{a_k}(1) \equiv 0 \pmod{p_i}$ pour $i = 2, \ldots, k$, le plus petit nombre premier pour lequel P_{a_k} est irréductible dans $\mathbb{F}_p$ est bien supérieur à p_{k+1}.

Soit la famille de paramètres impairs (a_k) tel que $a_k \equiv 0 \pmod{3 \cdot 5 \cdot 11 \cdot 13 \cdots p_k}$ et tel que $a_k \equiv 1 \pmod 7$. Le polynôme P_{a_k} vérifie bien la condition d'exhaustivité : la factorisation modulo 7 donne son irréductibilité et le résultat d'Uchida indique que le groupe de Galois sous-jacent est S_{13} ; la factorisation $P_{a_k} \equiv X^{13} + X = X(X^4 + 1)(X^8 - X^4 + 1)$ montre qu'il ne peut apparaître ni de 9-cycle ni de produit d'un 5-cycle avec un 7-cycle. Cette famille passe le test d'exhaustivité pour les caractères de degré 8008 et 4290.

Nous nous intéressons donc aux polynômes $P_a = X^{13} + X + a$, irréductibles, pour lesquels les discriminants sont sans facteurs carrés. Cela représente 84374 corps.

Pour les caractères de degré 462, le plus grand nombre premier obtenu est 929 pour le polynôme $X^{13} + X + 247285$.

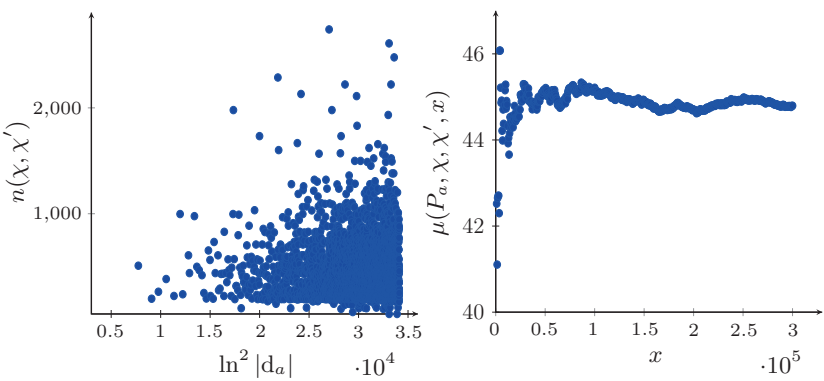

Figure 5. Pour les caractères de degré 462 de A_{13} définis par $P_a = X^{13} + X + a$.

Pour la séparation des caractères de degré 4290, le plus grand nombre premier obtenu est 2741 pour le polynôme $X^{13} + X + 55355$.

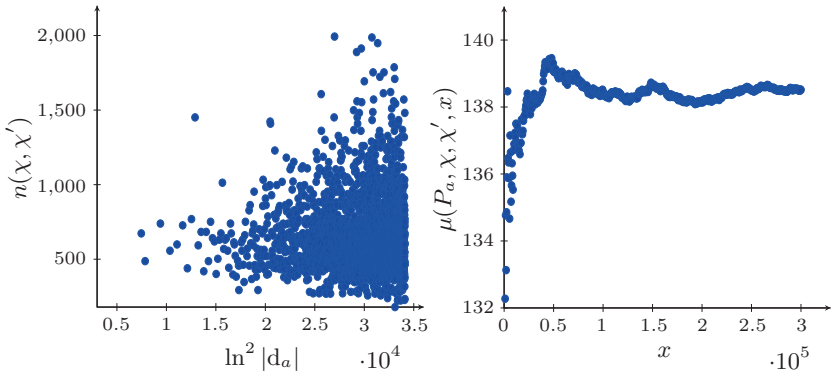

Figure 6. Pour les caractères de degré 4290 de A_{13} définis par $P_a = X^{13} + X + a$.

Pour les caractères de degré 8008, le plus grand nombre premier obtenu est alors 1993 pour le polynôme $X^{13} + X + 54983$.

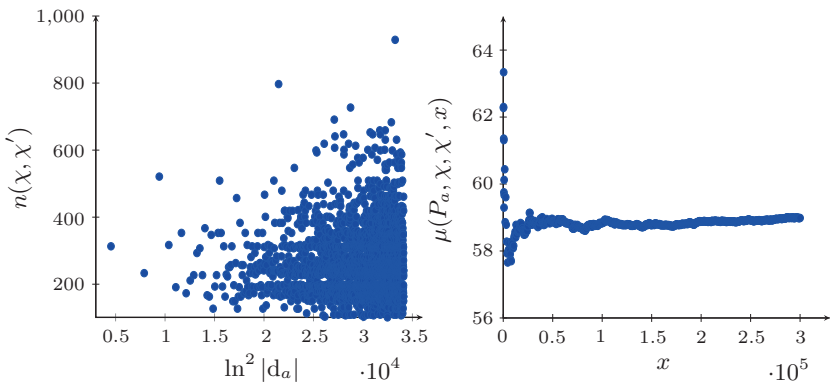

Figure 7. Pour les caractères de degré 8008 de A_{13} définis par $P_a = X^{13} + X + a$.

Remarque 4.2. Pour le groupe A_{13}, regardons la variation de la borne du corollaire 1.5 en fonction du degré r lorsque $\ln |\mathrm{d}_K|$ varie "peu", en lisant en parallèle et "verticalement" les trois diagrammes. Par exemple, le ratio entre $r = 8008$ et $r = 462$ est de 52 ; le carré de ce ratio, voire la puissance 4-ème de ce ratio, est alors à comparer aux axes des ordonnées des graphes associés aux caractères en question.

4.2. Sur une question diophantienne. Pour finir revenons à la famille de polynômes $P_a = X^n - aX + 1$ de discriminant $\mathrm{d}_a = n^n - (n-1)^{n-1}a^n$. Si l'on s'assure que le polynôme P_a est irréductible, que $n \geq 5$ est premier (pour simplifier, on peut prendre $n = 5$) et que $(a, n) = 1$, alors le résultat d'Uchida [**Uch**] évoqué précédemment, indique que le corps de décomposition de P_a est une extension non ramifiée de groupe de Galois A_n au-dessus de $\mathbb{Q}(\sqrt{\mathrm{d}_a})$.

Soit $\mathrm{d} < 0$ un entier négatif sans facteurs carrés et soit le corps quadratique $K = \mathbb{Q}(\sqrt{\mathrm{d}})$.

Intéressons nous à la problématique suivante : quand a varie, connaître le nombre de fois où il apparaît une extension non ramifiée au-dessus de K de groupe de Galois A_n, le tout donné par un polynôme P_a. Ou encore, d'après le résultat d'Uchida, déterminer les entiers a tels $\mathrm{d}_a = \mathrm{d}b^2$, où b est un entier. On tombe ainsi sur l'équation diophantienne (hyperelliptique) suivante :

$$n^n - (n-1)^{n-1}X^n = \mathrm{d}Y^2 \tag{2}$$

et à ses solutions entières. C'est une équation de genre $g = (n-1)/2 > 1$. D'après les travaux de Siegel, on sait que l'équation (2) n'a qu'un nombre fini de solutions entières. Se posent alors deux questions : (a) quel est le nombre de solutions ? ; (b) quelle est la taille des solutions ?

Commençons par regarder la question du nombre de solutions. Le résultat principal de Rémond dans [**Rém**] sur l'effectivité du résulat de Siegel montre pour notre situation que le nombre de couples N entiers (X, Y) solutions de (2) est au plus $\exp\big(5^{n^4} n \ln n \ln(n \ln n)\big)$ et ainsi

$$\ln N \ll 5^{n^4} n \ln n.$$

Supposons à présent que l'entier $n = \ell$ est un nombre premier. Si le polynôme P_a est irréductible, il donne lieu alors à une extension non ramifiée de groupe de Galois A_n au-dessus du corps $\mathbb{Q}(\sqrt{\mathrm{d}_a})$. D'autre part, d'après l'exemple 3.30, si $\mathcal{N}(A_n)$ désigne le nombre d'extensions non ramifiées linéairement indépendantes de K de groupe de Galois A_n, alors

$$\ln \mathcal{N}(A_n) \ll n^4.$$

Les quantités N et $\mathcal{N}(A_n)$ donnent chacune à leur façon une borne sur le nombre d'extensions de groupe de Galois A_n non ramifiées données par la famille des polynômes $(P_a)_a$ au-dessus d'un corps quadratique K fixé.

A ce stade, on peut voir apparaître plusieurs questions. Typiquement : (i) Peut-on abaisser la borne de Rémond dans notre contexte ? (ii) Soient $a \neq a'$ tels que $\mathrm{d}_a = \mathrm{d}_{a'} b^2$. Les corps de décomposition associés aux polynômes P_a et $P_{a'}$ peuvent ils être identiques ?

Une autre direction est d'aller vers la problématique de la taille des solutions de l'équation (2), c'est à dire en direction de la question de l'effectivité de la méthode de Baker. Notre référence pour cette question est le travail [**Bug**] de Bugeaud.

Trouver une borne sur la hauteur des solutions entières de l'équation de départ (2) revient à trouver une borne sur la hauteur des solutions de l'équation

$$\alpha X^n = Y^2 + \beta, \tag{3}$$

où $\alpha = \mathrm{d}(n-1)^{n-1}$ et $\beta = \mathrm{d}n^n$.

En appliquant alors le résultat principal de [**Bug**], on trouve que si (x, y) est solution de (3), alors

$$|y| \ll \exp\Big((4\beta)^{10n} \alpha^{4n} (\ln 4\alpha\beta)^{8n}\Big),$$

ce qui grossièrement donne

$$\ln |y| \ll n^{(10+\varepsilon)n^2}.$$

En pratique les formes linéaires montrent pour certaines équations toute leur puissance et la question suivante doit être lue dans ce cadre :

Question 4.3. *Est-il possible de baisser significativement la borne sur $|y|$? Concrètement, prenons $n = 5$. Etant donné d (pas trop grand), trouver toutes les solutions entières de l'équation* (2) *(en particulier quand celle-ci en a au moins une).*

Références

[BCP] W. Bosma, J. Cannon et C. Playoust, The Magma algebra system. I: The user language, Computational algebra and number theory (London, 1993), *J. Symbolic Comput.* **24(3–4)** (1997), 235–265. DOI: 10.1006/jsco.1996.0125.

[Bel] J. Bellaïche, Théorème de Chebotarev et complexité de Littlewood, *Ann. Sci. Éc. Norm. Supér. (4)* **49(3)** (2016), 579–632.

[BS] D. Bubboloni et J. Sonn, Intersective S_n polynomials with few irreducible factors, *Manuscripta Math.* **151(3)** (2016), 477–492. DOI: 10.1007/s00229-016-0848-9.

[Bug] Y. Bugeaud, Bounds for the solutions of superelliptic equations, *Compositio Math.* **107(2)** (1997), 187–219. DOI: 10.1023/A:1000130114331.

[Col] M. J. Collins, On Jordan's theorem for complex linear groups, *J. Group Theory* **10(4)** (2007), 411–423. DOI: 10.1515/JGT.2007.032.

[Ell] J. S. Ellenberg, Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups, in: *"Computational Arithmetic Geometry"*, Contemp. Math. **463**, Amer. Math. Soc., Providence, RI, 2008, pp. 45–48. DOI: 10.1090/conm/463/09045.

[EV1] J. S. Ellenberg et A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math. (2)* **163(2)** (2006), 723–741. DOI: 10.4007/annals.2006.163.723.

[EV2] J. S. Ellenberg et A. Venkatesh, Reflection principles and bounds for class group torsion, *Int. Math. Res. Not. IMRN* **2007** (2007), no. 1, Art. ID rnm002, 18 pp. DOI: 10.1093/imrn/rnm002.

[Euv] C. Euvrard, Majoration explicite sur le nombre de coefficients suffisants pour déterminer une fonction L, *J. Théor. Nombres Bordeaux* **29(1)** (2017), 51–83. DOI: 10.5802/jtnb.969.

[FH] W. Fulton et J. Harris, *"Representation Theory"*, A first course, Readings in Mathematics, Graduate Texts in Mathematics **129**, Springer-Verlag, New York, 1991. DOI: 10.1007/978-1-4612-0979-9.

[IK] H. Iwaniec et E. Kowalski, *"Analytic Number Theory"*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. DOI: 10.1090/coll/053.

[Kon] T. Kondo, Algebraic number fields with the discriminant equal to that of a quadratic number field, *J. Math. Soc. Japan* **47(1)** (1995), 31–36. DOI: 10.2969/jmsj/04710031.

[LMO] J. C. Lagarias, H. L. Montgomery et A. M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, *Invent. Math.* **54(3)** (1979), 271–296. DOI: 10.1007/BF01390234.

[LO] J. C. Lagarias et A. M. Odlyzko, Effective versions of the Chebotarev density theorem, in: *"Algebraic Number Fields*: *L-functions and Galois Properties"* (Proc. Sympos.,

Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[Lan] S. LANG, *"Algebraic Number Theory"*, Second edition, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994. DOI: 10.1007/978-1-4612-0853-2.

[Mar] J. MARTINET, Character theory and Artin L-functions, in: *"Algebraic Number Fields*: *L-functions and Galois Properties"* (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 1–87.

[MMS] M. RAM MURTY, V. KUMAR MURTY ET N. SARADHA, Modular forms and the Chebotarev density theorem, *Amer. J. Math.* **110(2)** (1988), 253–281. DOI: 10.2307/2374502.

[Neu] J. NEUKIRCH, *"Algebraic Number Theory"*, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999. DOI: 10.1007/978-3-662-03983-0.

[Nic] J.-L. NICOLAS, Répartition des nombres premiers, *Séminaire Delange–Pisot–Poitou. Théorie des nombres* **9(2)** (1967–68), exp. n. G6, G1–G4.

[Oes] J. OESTERLÉ, Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée, *Astérisque* **61** (1979), 165–167.

[PARI] THE PARI GROUP, PARI/GP version 2.6.1. http://pari.math.u-bordeaux.fr/.

[Pol] P. POLLACK, The smallest inert prime in a cyclic number field of prime degree, *Math. Res. Lett.* **20(1)** (2013), 163–179. DOI: 10.4310/MRL.2013.v20.n1.a13.

[Rém] G. RÉMOND, Nombre de points rationnels des courbes, *Proc. Lond. Math. Soc. (3)* **101(3)** (2010), 759–794. DOI: 10.1112/plms/pdq005.

[RT] J. ROUSE ET F. THORNE, On the existence of large degree Galois representations for fields of small discriminant, *Pacific J. Math.* **271(1)** (2014), 243–256. DOI: 10.2140/pjm.2014.271.243.

[Ser1] J.-P. SERRE, *"Linear Representations of Finite Groups"*, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics **42**, Springer-Verlag, New York-Heidelberg, 1977.

[Ser2] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401.

[Ten] G. Tenenbaum, *"Introduction à la théorie analytique et probabiliste des nombres"*, Second edition, Cours Spécialisés **1**, Société Mathématique de France, Paris, 1995.

[Uch] K. Uchida, Unramified extensions of quadratic number fields, II, *Tôhoku Math. J. (2)* **22(2)** (1970), 220–224. DOI: 10.2748/tmj/1178242816.

[Win] B. Winckler, Théorème de Chebotarev effectif, Preprint (2013). arXiv:1311.5715.

[Yam] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7(1)** (1970), 57–76.

[Zam] A. Zaman, Bounding the least prime ideal in the Chebotarev Density Theorem, Preprint (2015). arXiv:1508.00287.

Charlotte Euvrard:
Laboratoire de Mathématiques de Besançon
UMR 6623 CNRS
Université Bourgogne France-Comté
16 route de Gray
25030 Besançon cedex, et

École Nationale Supérieure de Mécanique et des Microtechniques
26 chemin de l'Épitaphe
25030 Besançon cedex
France
E-mail address: charlotte.euvrard@univ-fcomte.fr

Christian Maire:
Laboratoire de Mathématiques de Besançon
UMR 6623 CNRS
Université Bourgogne Franche-Comté
16 route de Gray
25030 Besançon cedex
France
E-mail address: christian.maire@univ-fcomte.fr

Primera versió rebuda el 26 d'octubre de 2015,
darrera versió rebuda el 10 d'octubre de 2016.