JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Dominique BERNARDI et Alain KRAUS

Idéaux premiers totalement décomposés et sommes de Newton

Tome 34, nº 2 (2022), p. 517-536.

https://doi.org/10.5802/jtnb.1213

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **34** (2022), 517–536

Idéaux premiers totalement décomposés et sommes de Newton

par Dominique BERNARDI et Alain KRAUS

Résumé. Soient K un corps de nombres et $f \in O_K[X]$ un polynôme irréductible unitaire à coefficients dans l'anneau d'entiers de K. On se propose d'expliciter un critère effectif, en termes du groupe de Galois de f sur K et d'une suite récurrente linéaire associée à f, permettant parfois de caractériser les idéaux premiers de O_K modulo lesquels f est totalement décomposé. Si α est une racine de f, ce critère fournit donc une caractérisation des idéaux premiers de O_K qui sont totalement décomposés dans $K(\alpha)$. Il s'applique en particulier si le degré de f est au moins 4 et le groupe de Galois de f est le groupe symétrique ou le groupe alterné.

Abstract. Let K be a number field and $f \in O_K[X]$ an irreducible monic polynomial with coefficients in its ring of integers. We give an effective criterion, in terms of the Galois group of f over K and a linear recurrent sequence associated with f, allowing in some cases the characterization of the prime ideals in O_K modulo which f is totally split. If α is a root of f, this criterion thus gives a characterization of the prime ideals in O_K which totally split in $K(\alpha)$. A particular case in which it applies is when the degree of f is at least 4 and the Galois group of f is the symmetric group or the alternating group.

1. Introduction

Soit K un corps de nombres. Notons O_K son anneau d'entiers. Soit $f \in O_K[X]$ un polynôme unitaire irréductible sur K, dont le degré sera noté k. On se préoccupe dans cet article de la question suivante (cf. [10, Question A] et [3, p. 27], dans le cas où $K = \mathbb{Q}$) :

Question 1.1. Comment caractériser les idéaux premiers $\mathfrak{p}$ de O_K tels que le polynôme f soit totalement décomposé modulo $\mathfrak{p}$ i.e. que f modulo $\mathfrak{p}$ soit séparable et ait toutes ses racines dans $O_K/\mathfrak{p}$?

Une réponse attendue consiste à expliciter une caractérisation, indépendante de tout algorithme de factorisation de f modulo $\mathfrak{p}$, permettant d'identifier ces idéaux premiers. On obtient alors, ce que l'on appelle parfois, une loi de réciprocité pour f (cf. [10, p. 1], [3, p. 32] et [11, p. 585]).

Manuscrit reçu le 8 décembre 2020, révisé le 21 juin 2021, accepté le 29 octobre 2021.
Classification Mathématique (2010). 11B83, 11R32, 11R04, 11R37, 11Y40.
Mots-clefs. Corps de nombres, groupes de Galois, idéaux premiers, suites récurrentes linéaires, corps de classes.

Par exemple, si $K = \mathbb{Q}$, une caractérisation est la suivante. Pour tout nombre premier p, notons $N_p(f)$ le nombre de racines de f modulo p. Soit x la classe de X dans la $\mathbb{Z}$-algèbre $\mathbb{Z}[X]/(p, f)$. Comme conséquence du théorème chinois, si p ne divise pas le discriminant de f, on a l'équivalence

$$N_p(f) = k \quad \Leftrightarrow \quad x^p = x. \tag{1.2}$$

La question 1.1 peut se reformuler comme suit ([10, Question B, p. 6]) : soit L/K une extension finie. Comment caractériser les idéaux premiers de O_K qui sont totalement décomposés dans L ? Si l'extension L/K est abélienne, la théorie du corps de classes fournit une réponse complète à cette question (voir par exemple [6]). Dans le cas général, une approche de ces questions repose sur l'étude des représentations galoisiennes de degré au moins 2 du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. On pourra trouver dans [10] l'état des connaissances sur ces questions.

Une réponse à la question 1.1 a été obtenue par T. et V. Dokchitser dans [4]. Ils ont en particulier démontré l'existence de polynômes $h \in K[X]$ tel que, pour presque tout idéal premier $\mathfrak{p}$ de O_K, la condition suivante soit satisfaite ([4, théorème 5.1] en prenant pour $\mathcal{C}$ la classe triviale) : posons $\mathbb{F}_q = O_K/\mathfrak{p}$ où q est le cardinal de $O_K/\mathfrak{p}$ et $A = \mathbb{F}_q[X]/(f)$. Notons $x \in A$ la classe de X, $\mathrm{Tr} : A \to \mathbb{F}_q$ la forme trace et $\alpha_1, \ldots, \alpha_k$ les racines de f dans $\overline{\mathbb{Q}}$. Alors, f est totalement décomposé modulo $\mathfrak{p}$ si et seulement si on a dans $\mathbb{F}_q$ l'égalité

$$\mathrm{Tr}\,(h(x)x^q) = \sum_{j=1}^{k} h(\alpha_j)\alpha_j \pmod{\mathfrak{p}}.$$

De plus, ils fournissent dans le théorème 5.3 de *loc. cit.* un critère, dépendant de f et h, permettant souvent en pratique d'expliciter un tel polynôme h à coefficients dans O_K.

Par ailleurs, si ce critère est satisfait, on peut alors expliciter une suite récurrente linéaire, dont les termes sont dans O_K, telle que, pour presque tout idéal premier $\mathfrak{p}$ de O_K, f est totalement décomposé modulo $\mathfrak{p}$ si et seulement si une certaine condition relative au $q+1$-ième terme de cette suite est réalisée. Dans le cas où $K = \mathbb{Q}$, on pourra aussi consulter à sujet l'article de J. Rosen [8] et en particulier son corollaire 1.3.

On se propose ici de préciser le résultat de [4] rappelé ci-dessus avec le polynôme $h = X$ (le critère ne s'applique pas avec $h = 1$). On associe alors à f la suite récurrente linéaire $(T_n)_{n\in\mathbb{N}}$ d'éléments de O_K, dont le terme T_n est la n-ième somme de Newton des racines de f dans $\overline{\mathbb{Q}}$. On obtient ainsi un critère impliquant le fait que, pour presque tout idéal premier $\mathfrak{p}$ de O_K, f est totalement décomposé modulo $\mathfrak{p}$ si et seulement si $T_{\mathrm{N}(\mathfrak{p})+1} - T_2$ appartient à $\mathfrak{p}$ (théorème 2.2). Notons $\mathrm{Gal}(f)$ le groupe de Galois de f sur K. Si on a $k \geq 4$, on démontre notamment que ce critère s'applique

si $\mathrm{Gal}(f)$ est isomorphe au groupe symétrique $\mathfrak{S}_k$ ou à son sous-groupe alterné $\mathfrak{A}_k$ (théorème 2.4). Dans le cas où $\mathrm{Gal}(f)$ n'est pas isomorphe à $\mathfrak{S}_k$ ni $\mathfrak{A}_k$, il importe dans l'utilisation du théorème 2.2 de décrire l'action de $\mathrm{Gal}(f)$ sur les racines de f. Le théorème 2.8 fournit un critère qui permet parfois de se dispenser de cette description.

À titre indicatif, si $K = \mathbb{Q}$ et $f = X^5 - X - 1$, dont le groupe de Galois est $\mathfrak{S}_5$, on obtient l'énoncé suivant (proposition 2.11, assertion 1). Soit $(T_n)_{n\in\mathbb{N}}$ la suite définie par les égalités $T_0 = 5$, $T_1 = T_2 = T_3 = 0$, $T_4 = 4$ et $T_{n+5} = T_{n+1} + T_n$ pour tout $n \in \mathbb{N}$. Alors, si $p \notin \{2, 5\}$, on a $N_p(f) = 5$ si et seulement si $T_{p+1} \equiv 0 \pmod{p}$.

Par ailleurs, soit H_K le corps de classes de Hilbert de K, qui est l'extension abélienne non ramifiée maximale de K. D'après la théorie du corps de classes, pour qu'un idéal premier de O_K soit principal il faut et il suffit qu'il soit totalement décomposé dans H_K ([6, (8.5) Corollary, p. 107]). Supposons connu le polynôme minimal f d'un élément primitif entier de l'extension H_K/K. Si $(T_n)_{n\in\mathbb{N}}$ est la suite récurrente linéaire associée à f comme précédemment, les résultats obtenus permettent alors de caractériser les idéaux premiers $\mathfrak{p}$ de O_K qui sont principaux, en terme de la différence $T_{\mathrm{N}(\mathfrak{p})+1} - T_2$. On pourra trouver deux illustrations numériques à ce sujet dans le paragraphe 9.

Nous remercions le rapporteur de cet article pour toutes ses observations, en particulier pour la référence [4] qui nous avait échappé.

Tous les calculs numériques que ce travail a nécessités ont été effectués à l'aide des logiciels de calculs `Pari-gp` ([7]) et `Magma` ([1]).

2. Énoncés des résultats

Soit K un corps de nombres d'anneau d'entiers O_K. Soient $k \geq 2$ un entier et

$$f = X^k - a_{k-1}X^{k-1} - a_{k-2}X^{k-2} - \cdots - a_1X - a_0 \in O_K[X]$$

un polynôme irréductible sur K. Choisissons une numérotation $\alpha_1, \ldots, \alpha_k$ des racines de f dans $\overline{\mathbb{Q}}$. Posons $G = \mathrm{Gal}(f)$ le groupe de Galois de f sur K i.e. le groupe de Galois de l'extension $K(\alpha_1, \ldots, \alpha_k)/K$. On identifiera dans toute la suite G avec le sous-groupe du groupe symétrique $\mathfrak{S}_k$ associé à l'action de G sur les racines de f. Avec cette identification, on a donc pour tout $\sigma \in G$ et tout $i \in \{1, \ldots, k\}$ l'égalité

$$\sigma(\alpha_i) = \alpha_{\sigma(i)}.$$

2.1. La suite $(T_n)_{n\in\mathbb{N}}$. Pour tout entier $n \in \mathbb{N}$, on note

$$T_n = \sum_{i=1}^{k} \alpha_i^n \tag{2.1}$$

la n-ième somme de Newton des racines de f. La suite $T = (T_n)_{n\in\mathbb{N}}$ est déterminée par ses k premiers termes et vérifie la récurrence linéaire

$$T_{n+k} = a_{k-1}T_{n+k-1} + a_{k-2}T_{n+k-2} + \cdots + a_1T_{n+1} + a_0T_n$$

pour $n \in \mathbb{N}$. Tous ses termes appartiennent à O_K.

2.2. L'entier B_f. Pour tout $\sigma \in G$, notons

$$c(\sigma) = \sum_{i=1}^{k} \alpha_i\alpha_{\sigma(i)} - T_2. \tag{2.2}$$

Posons alors

$$B_f = \prod_{\sigma\in G,\sigma\neq \mathrm{Id}} c(\sigma). \tag{2.3}$$

Lemme 2.1. *L'élément B_f appartient à O_K.*

Démonstration. Soit τ un élément de G. Pour tout $\sigma \in G$, $\sigma \neq \mathrm{Id}$, on a $\tau\,(c(\sigma)) = c(\tau\sigma\tau^{-1})$, d'où l'égalité

$$\tau(B_f) = \prod_{\sigma\in G,\sigma\neq \mathrm{Id}} c(\tau\sigma\tau^{-1}).$$

L'application qui à σ associe $\tau\sigma\tau^{-1}$ est une permutation de $G \setminus \{\mathrm{Id}\}$. Il en résulte que B_f est fixé par τ, d'où le résultat. □

2.3. Le critère de décomposition. Soit Δ_f le discriminant de f. Pour tout idéal premier non nul $\mathfrak{p}$ de O_K désignons par $\mathrm{N}(\mathfrak{p})$ le cardinal de $O_K/\mathfrak{p}$ i.e. la norme de K sur $\mathbb{Q}$ de $\mathfrak{p}$. Notons $N_{\mathfrak{p}}(f)$ le nombre de racines de f modulo $\mathfrak{p}$.

Théorème 2.2. *Soit $\mathfrak{p}$ un idéal premier de O_K. Supposons que l'on ait*

$$\Delta_f B_f \not\equiv 0 \pmod{\mathfrak{p}}. \tag{2.4}$$

Alors, on a l'équivalence

$$N_{\mathfrak{p}}(f) = k \;\Leftrightarrow\; T_{\mathrm{N}(\mathfrak{p})+1} \equiv T_2 \pmod{\mathfrak{p}}. \tag{2.5}$$

Remarque 2.3. Du point de vue algorithmique, ce critère est efficace, de même que l'était le critère 1.2. En effet, il s'agit de calculer la $\mathrm{N}(\mathfrak{p})+1$-ième puissance d'un élément de l'anneau $O_K[X]/(\mathfrak{p}, f)$, ce qui se fait en temps polynomial en $k\log(\mathrm{N}(\mathfrak{p}))$.

Si B_f n'est pas nul, on obtient ainsi une loi de réciprocité pour f. Tel est le cas dans la situation suivante.

Théorème 2.4. *Supposons $k \geq 4$ et $G = \mathfrak{S}_k$ ou $G = \mathfrak{A}_k$. Alors, on a $B_f \neq 0$.*

Remarque 2.5. L'énoncé précédent n'est pas valable pour $k = 3$. Dans ce cas, on a $B_f \neq 0$ si et seulement si $a_2^2 + 3a_1 \neq 0$ (voir la démonstration de la proposition 2.9). De même, si on a $k \geq 4$ et si G n'est pas le groupe $\mathfrak{S}_k$ ni le groupe $\mathfrak{A}_k$, B_f peut être nul. Par exemple, pour $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$, on a $G = \mathbb{Z}/4\mathbb{Z} \subseteq \mathfrak{S}_4$ et $B_f = 0$. Cela étant, pour ce polynôme, il est bien connu que l'on a $N_p(f) = 4$ si et seulement si 5 divise $p - 1$. Notons qu'en général le fait que B_f soit nul ne dépend pas que du groupe de Galois de f. En effet, avec $f = X^4 - 5X^2 + 5 \in \mathbb{Q}[X]$, on a comme ci-dessus $G = \mathbb{Z}/4\mathbb{Z}$ et on vérifie que B_f est non nul.

2.4. Sur la factorisation de B_f. La norme de K sur $\mathbb{Q}$ de B_f est un entier rationnel dont le nombre de chiffres décimaux est souvent très grand, notamment si $k \geq 6$. Il est alors très difficile et généralement prohibitif de déterminer ses diviseurs premiers. Dans certains cas, on peut néanmoins y parvenir en remarquant que B_f admet une factorisation qui est reliée aux classes de conjugaison de G. Plus précisément, pour toute classe de conjugaison non triviale $\mathcal{C}$ de G, posons

$$B_{\mathcal{C}} = \prod_{\sigma \in \mathcal{C}} c(\sigma). \tag{2.6}$$

Pour tous $\tau \in G$ et $\sigma \in \mathcal{C}$, l'égalité $\tau\,(c(\sigma)) = c(\tau\sigma\tau^{-1})$, entraîne que $B_{\mathcal{C}}$ est fixé par τ, d'où

$$B_{\mathcal{C}} \in O_K. \tag{2.7}$$

L'égalité

$$B_f = \prod_{\mathcal{C}} B_{\mathcal{C}}, \tag{2.8}$$

où $\mathcal{C}$ parcourt l'ensemble des classe de conjugaison non triviales de G, fournit alors une factorisation de B_f. Par ailleurs, l'énoncé suivant facilite parfois cette factorisation.

Proposition 2.6. *Soient $\mathcal{C}$ une classe de conjugaison non triviale de G qui n'est pas formée d'éléments d'ordre 2 et $\mathcal{C}'$ la classe de conjugaison formée des inverses des éléments de $\mathcal{C}$.*

(1) *Si $\mathcal{C} = \mathcal{C}'$, alors $B_{\mathcal{C}}$ est un carré dans O_K.*
(2) *Si $\mathcal{C} \neq \mathcal{C}'$, alors on a $B_{\mathcal{C}} = B_{\mathcal{C}'}$.*

Corollaire 2.7. *Le produit des $B_{\mathcal{C}}$, où $\mathcal{C}$ parcourt l'ensemble des classes de conjugaison non triviales de G qui ne sont pas formées d'éléments d'ordre 2, est un carré dans O_K.*

Démonstration. C'est une conséquence directe de la proposition 2.6. □

2.5. Une propriété de divisibilité de B_f. Si G n'est pas $\mathfrak{S}_k$ ni $\mathfrak{A}_k$, le calcul de B_f nécessite a priori la description explicite de l'action de G sur les racines de f. On peut parfois s'en affranchir en procédant comme suit.

Pour toute classe de conjugaison $\mathcal{S}$ non triviale de $\mathfrak{S}_k$, considérons le polynôme $F_{\mathcal{S}} \in \mathbb{Z}[X_1, \ldots, X_k]$ défini par

$$F_{\mathcal{S}} = \prod_{t \in \mathcal{S}} \left(\sum_{i=1}^{k} X_i X_{t(i)} - N_2 \right) \quad \text{où} \quad N_2 = \sum_{i=1}^{k} X_i^2. \tag{2.9}$$

On vérifie que $F_{\mathcal{S}}$ est invariant sous l'action de $\mathfrak{S}_k$ sur $\mathbb{Z}[X_1, \ldots, X_k]$ (lemme 6.1). Par suite, F_S est un polynôme à coefficients dans $\mathbb{Z}$ en les polynômes symétriques élémentaires de $\mathbb{Z}[X_1, \ldots, X_k]$. Il en résulte que

$$F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) \in O_K. \tag{2.10}$$

Théorème 2.8. *On a dans O_K la congruence*

$$\prod_{\mathcal{S}} F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) \equiv 0 \pmod{B_f}, \tag{2.11}$$

où $\mathcal{S}$ parcourt l'ensemble des classes de conjugaison non triviales de $\mathfrak{S}_k$. En particulier, on a l'implication

$$\prod_{\mathcal{S}} F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) \neq 0 \ \Rightarrow \ B_f \neq 0. \tag{2.12}$$

Pour tout idéal premier $\mathfrak{p}$ de O_K tel que

$$\prod_{\mathcal{S}} F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) \not\equiv 0 \pmod{\mathfrak{p}}, \tag{2.13}$$

on a l'équivalence

$$N_{\mathfrak{p}}(f) = k \ \Leftrightarrow \ T_{\mathrm{N}(\mathfrak{p})+1} \equiv T_2 \pmod{\mathfrak{p}}. \tag{2.14}$$

Si l'on parvient à factoriser le produit des $F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k)$, on obtient alors une loi de réciprocité pour f sans calculer B_f explicitement.

2.6. Conséquences. Précisons les énoncés précédents dans quelques cas particuliers.

Proposition 2.9. *Soit $\mathfrak{p}$ un idéal premier de O_K.*

(1) *Si $k = 2$ et $\Delta_f \not\equiv 0 \pmod{\mathfrak{p}}$, on a*

$$N_{\mathfrak{p}}(f) = 2 \ \Leftrightarrow \ T_{\mathrm{N}(\mathfrak{p})+1} \equiv a_1^2 + 2a_0 \pmod{\mathfrak{p}}.$$

(2) *Si $k = 3$ et $(a_2^2 + 3a_1)\Delta_f \not\equiv 0 \pmod{\mathfrak{p}}$, on a*

$$N_{\mathfrak{p}}(f) = 3 \ \Leftrightarrow \ T_{\mathrm{N}(\mathfrak{p})+1} \equiv a_2^2 + 2a_1 \pmod{\mathfrak{p}}.$$

Proposition 2.10. *Soit* $\mathfrak{p}$ *un idéal premier de* O_K*. Supposons que* f *soit un trinôme de la forme*

$$f = X^4 - a_1X - a_0.$$

Si $2a_1a_0\Delta_f \not\equiv 0 \pmod{\mathfrak{p}}$*, on a*

$$N_{\mathfrak{p}}(f) = 4 \;\Leftrightarrow\; T_{\mathrm{N}(\mathfrak{p})+1} \equiv 0 \pmod{\mathfrak{p}}.$$

En particulier, si $K = \mathbb{Q}$ et $f = X^4 - X - 1$, pour tout nombre premier $p \neq 283$, on a

$$N_p(f) = 4 \;\Leftrightarrow\; T_{p+1} \equiv 0 \pmod{p}.$$

Selmer a démontré que pour tout $n \geq 2$ le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^n - X - 1 \in \mathbb{Q}[X]$ est le groupe symétrique $\mathfrak{S}_n$ ([9]). Dans le cas où $n \in \{5, 6, 7\}$, on a l'énoncé suivant.

Proposition 2.11. *Supposons* $K = \mathbb{Q}$*. Soit* p *un nombre premier.*

(1) *Si* $f = X^5 - X - 1$ *et* $p \notin \{2, 5\}$*, on a*

$$N_p(f) = 5 \;\Leftrightarrow\; T_{p+1} \equiv 0 \pmod{p}.$$

(2) *Si* $f = X^6 - X - 1$ *et* $p \notin \{2, 3, 7, 13, 1663\}$*, on a*

$$N_p(f) = 6 \;\Leftrightarrow\; T_{p+1} \equiv 0 \pmod{p}.$$

(3) *Si* $f = X^7 - X - 1$ *et* $p \notin \{2, 3, 7, 15961129\}$*, on a*

$$N_p(f) = 7 \;\Leftrightarrow\; T_{p+1} \equiv 0 \pmod{p}.$$

Remarque 2.12. En ce qui concerne le polynôme $f = X^8 - X - 1$, si $\mathcal{C}$ est la classe de conjugaison des 8-cycles dans $\mathfrak{S}_8$, la racine carrée de $B_{\mathcal{C}}$ est un entier possédant 830 chiffres décimaux. Il semble difficile d'obtenir sa factorisation complète en produit de nombres premiers.

Proposition 2.13. *Supposons* $K = \mathbb{Q}$ *et* $f = X^5 - 2X^4 + 2X^3 - X^2 + 1$*. Alors, le groupe de Galois de* f *est diédral d'ordre* 10*. Pour tout nombre premier* $p \notin \{3, 47\}$*, on a*

$$N_p(f) = 5 \;\Leftrightarrow\; T_{p+1} \equiv 0 \pmod{p}.$$

Terminons ce paragraphe avec l'exemple suivant.

Proposition 2.14. *Supposons* $K = \mathbb{Q}(\alpha)$ *avec* $\alpha^3 - \alpha - 1 = 0$*. Posons*

$$u = -\alpha^2 + \alpha + 2 \quad \textit{et} \quad f = X^5 + u^3X + u \in K[X].$$

Alors, f *est irréductible sur* K *et* $\mathrm{Gal}(f) = \mathfrak{S}_5$*. Soient* $\mathfrak{p}_5$ *et* $\mathfrak{p}_{61}$ *les idéaux premiers de* O_K *au-dessus de* 5 *et* 61 *qui sont de degré résiduel* 1*. Pour tout idéal premier* $\mathfrak{p}$ *de* O_K*, distinct de* $\mathfrak{p}_5$ *et* $\mathfrak{p}_{61}$*, on a*

$$N_{\mathfrak{p}}(f) = 5 \;\Leftrightarrow\; T_{\mathrm{N}(\mathfrak{p})+1} \equiv 0 \pmod{\mathfrak{p}}. \tag{2.15}$$

3. Démonstration du théorème 2.2

Il peut s'obtenir en utilisant le théorème 5.3 de [4]. Nous en fournissons ici une démonstration directe.

Soit $\mathfrak{p}$ un idéal premier de O_K. Par hypothèse, on a $\Delta_f B_f \not\equiv 0 \pmod{\mathfrak{p}}$ où B_f est défini par l'égalité (2.3). Posons $\widetilde{K} = K(\alpha_1, \ldots, \alpha_k)$ et notons $O_{\widetilde{K}}$ son anneau d'entiers. Rappelons que $G = \mathrm{Gal}(\widetilde{K}/K)$.

Le lemme qui suit ne dépend pas de l'hypothèse faite sur B_f.

Lemme 3.1. *Supposons $N_{\mathfrak{p}}(f) = k$. Alors, on a $T_{\mathrm{N}(\mathfrak{p})+1} \equiv T_2 \pmod{\mathfrak{p}}$.*

Démonstration. Par hypothèse, il existe k éléments $\beta_1 \ldots \beta_k$ de O_K tels que $f \equiv \prod_{i=1}^{k}(X - \beta_i) \pmod{\mathfrak{p}}$. Si $(V_n)_{n\in\mathbb{N}}$ est la suite des sommes de Newton des β_i, on en déduit que pour tout $n \in \mathbb{N}$ on a $T_n \equiv V_n \pmod{\mathfrak{p}}$. En conséquence, on a

$$T_{\mathrm{N}(\mathfrak{p})+1} \equiv V_{\mathrm{N}(\mathfrak{p})+1} \equiv V_2 \equiv T_2 \pmod{\mathfrak{p}},$$

la congruence centrale venant de ce que l'on a $x^{\mathrm{N}(\mathfrak{p})+1} \equiv x^2 \pmod{\mathfrak{p}}$ pour tout $x \in O_K$. □

Inversement, supposons $T_{\mathrm{N}(\mathfrak{p})+1} \equiv T_2 \pmod{\mathfrak{p}}$ et montrons que l'on a $N_{\mathfrak{p}}(f) = k$.

L'idéal $\mathfrak{p}$ est non ramifié dans $\widetilde{K}$ car il ne divise pas Δ_f. Soient $\mathfrak{P}$ un idéal premier de $O_{\widetilde{K}}$ au-dessus de $\mathfrak{p}$ et $\sigma \in G$ la substitution de Frobenius en $\mathfrak{P}$. Pour tout $i \in \{1, \ldots, k\}$, on a

$$\sigma(\alpha_i) = \alpha_{\sigma(i)} \quad \text{et} \quad \alpha_i^{\mathrm{N}(\mathfrak{p})} \equiv \alpha_{\sigma(i)} \pmod{\mathfrak{P}}.$$

On a donc dans $O_{\widetilde{K}}$ la congruence (égalité (2.1))

$$T_{\mathrm{N}(\mathfrak{p})+1} \equiv \sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} \pmod{\mathfrak{P}}.$$

Il en résulte que l'on a

$$\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} \equiv T_2 \pmod{\mathfrak{P}} \quad \text{i.e.} \quad c(\sigma) \equiv 0 \pmod{\mathfrak{P}}.$$

Vérifions que σ est l'identité. Supposons le contraire. Dans ce cas, on déduit des égalités (2.2) et (2.3) que $\mathfrak{P}$ divise B_f. Parce que B_f est dans O_K (lemme 2.1), on a donc

$$B_f \equiv 0 \pmod{\mathfrak{p}},$$

ce qui contredit la condition (2.4), et prouve notre assertion. Par suite, $\mathfrak{p}$ est totalement décomposé dans $\widetilde{K}$ ou ce qui revient au même dans K, d'où $N_{\mathfrak{p}}(f) = k$ ([2, Proposition 2.3.9]).

Cela établit l'équivalence (2.5) et le théorème 2.2.

4. Démonstration du théorème 2.4

Rappelons que l'on a $k \geq 4$ et $G = \mathfrak{S}_k$ ou $G = \mathfrak{A}_k$. Considérons désormais un élément $\sigma \in G$, distinct de l'identité. On va démontrer que l'on a

$$\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} \neq T_2, \tag{4.1}$$

ce qui prouvera le résultat. Pour cela, on est amené à distinguer plusieurs cas en fonction de la décomposition de σ en produit de cycles à supports disjoints. Dans chacun des cas, on va supposer que l'on a

$$\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} = T_2 \tag{4.2}$$

et aboutir à une contradiction.

Lemme 4.1. *Supposons qu'il y ait une transposition dans la décomposition de σ en produit de cycles à supports disjoints. Alors, la condition* (4.1) *est satisfaite.*

Démonstration. Soit $(\alpha_{i_1}, \alpha_{i_2})$ une transposition intervenant dans la décomposition de σ en produit de cycles à supports disjoints.

Supposons que l'on ait $\sigma = (\alpha_{i_1}, \alpha_{i_2})$. On a les égalités

$$\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} = 2\alpha_{i_1}\alpha_{i_2} + T_2 - \alpha_{i_1}^2 - \alpha_{i_2}^2 = -(\alpha_{i_1} - \alpha_{i_2})^2 + T_2. \tag{4.3}$$

La condition (4.2) implique alors $\alpha_{i_1} = \alpha_{i_2}$ et une contradiction.

On a donc $\sigma \neq (\alpha_{i_1}, \alpha_{i_2})$. Il existe ainsi dans la décomposition de σ un cycle

$$(\alpha_{i_3}, \dots, \alpha_{i_t})$$

de longueur au moins 2, dont le support est disjoint de $\{\alpha_{i_1}, \alpha_{i_2}\}$. D'après la condition (4.2), on a donc une égalité de la forme

$$2\alpha_{i_1}\alpha_{i_2} + (\alpha_{i_3}\alpha_{i_4} + \cdots + \alpha_{i_{t-1}}\alpha_{i_t} + \alpha_{i_t}\alpha_{i_3}) + P(\dots, \alpha_j, \dots) = T_2, \tag{4.4}$$

où P est un polynôme homogène de degré 2 en les α_j avec $j \neq i_1, i_2, \dots, i_t$.

Appliquons le 3-cycle $(i_1, i_2, i_3) \in \mathfrak{A}_k \subseteq G$ aux deux membres de l'égalité (4.4). On a $t \geq 4$ et on obtient ainsi

$$2\alpha_{i_2}\alpha_{i_3} + (\alpha_{i_1}\alpha_{i_4} + \cdots + \alpha_{i_{t-1}}\alpha_{i_t} + \alpha_{i_t}\alpha_{i_1}) + P(\dots, \alpha_j, \dots) = T_2. \tag{4.5}$$

Par soustraction des égalités (4.4) et (4.5), on a donc

$$2\alpha_{i_2}(\alpha_{i_1} - \alpha_{i_3}) + \alpha_{i_4}(\alpha_{i_3} - \alpha_{i_1}) + \alpha_{i_t}(\alpha_{i_3} - \alpha_{i_1}) = 0.$$

On a $\alpha_{i_1} \neq \alpha_{i_3}$, d'où

$$2\alpha_{i_2} = \alpha_{i_4} + \alpha_{i_t}.$$

En appliquant de nouveau le 3-cycle $(i_1, i_2, i_3) \in G$ aux deux membres de cette égalité, on obtient

$$2\alpha_{i_3} = \alpha_{i_4} + \alpha_{i_t},$$

d'où $\alpha_{i_2} = \alpha_{i_3}$, puis une contradiction et le résultat. □

Lemme 4.2. *Soit $p \geq 4$ un entier. Supposons qu'il existe un p-cycle dans la décomposition de σ en produit de cycles à supports disjoints. Alors, la condition* (4.1) *est satisfaite.*

Démonstration. Soit $(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_p})$ un p-cycle intervenant dans la décomposition de σ en produit de cycles à supports disjoints. On a alors une expression de la forme

$$\alpha_{i_1}\alpha_{i_2} + \alpha_{i_2}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_4} + \cdots + \alpha_{i_p}\alpha_{i_1} + P(\dots, \alpha_j, \dots) = T_2, \tag{4.6}$$

où P est un polynôme homogène de degré 2 en les α_j avec $j \notin \{i_1, \dots, i_p\}$. En appliquant le 3-cycle $(i_1, i_2, i_3) \in G$ aux deux membres de (4.6), on obtient

$$\alpha_{i_2}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_1} + \alpha_{i_1}\alpha_{i_4} + \cdots + \alpha_{i_p}\alpha_{i_2} + P(\dots, \alpha_j, \dots) = T_2. \tag{4.7}$$

Par soustraction de (4.6) et (4.7), on a donc

$$\alpha_{i_1}(\alpha_{i_2} - \alpha_{i_3} + \alpha_{i_p} - \alpha_{i_4}) + \alpha_{i_3}\alpha_{i_4} - \alpha_{i_p}\alpha_{i_2} = 0. \tag{4.8}$$

Si $p = 4$, on a alors

$$\alpha_{i_1}(\alpha_{i_2} - \alpha_{i_3}) + \alpha_{i_4}(\alpha_{i_3} - \alpha_{i_2}) = 0,$$

d'où $\alpha_{i_2} = \alpha_{i_3}$ ou $\alpha_{i_1} = \alpha_{i_4}$ et une contradiction.

Si $p \geq 5$, en appliquant le 3-cycle $(i_2, i_3, i_4) \in G$ à l'égalité (4.8), cela conduit à

$$\alpha_{i_1}(\alpha_{i_3} - \alpha_{i_4} + \alpha_{i_p} - \alpha_{i_2}) + \alpha_{i_4}\alpha_{i_2} - \alpha_{i_p}\alpha_{i_3} = 0. \tag{4.9}$$

Par soustraction de (4.8) et (4.9), il vient

$$\alpha_{i_1}(2\alpha_{i_2} - 2\alpha_{i_3}) + \alpha_{i_4}(\alpha_{i_3} - \alpha_{i_2}) + \alpha_{i_p}(\alpha_{i_3} - \alpha_{i_2}) = 0.$$

On a $\alpha_{i_2} \neq \alpha_{i_3}$, d'où

$$2\alpha_{i_1} = \alpha_{i_4} + \alpha_{i_p}.$$

En appliquant le 3-cycle $(i_1, i_2, i_3) \in G$ à cette égalité, on obtient

$$2\alpha_{i_2} = \alpha_{i_4} + \alpha_{i_p},$$

puis $\alpha_{i_1} = \alpha_{i_2}$, d'où une contradiction et le résultat. □

Compte tenu des lemmes 4.1 et 4.2, il reste à établir l'énoncé suivant.

Lemme 4.3. *Supposons que σ soit un produit de 3-cycles à supports disjoints. Alors, la condition* (4.1) *est satisfaite.*

Démonstration. Étape 1. Supposons que σ soit un 3-cycle, soit $\sigma = (\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3})$. Toutes les racines de f autres que $\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}$ étant fixées par σ, on a

$$\alpha_{i_1}\alpha_{i_2} + \alpha_{i_2}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_1} + \sum_{j \notin \{i_1,i_2,i_3\}} \alpha_j^2 = T_2. \tag{4.10}$$

On a $k \geq 4$ et en appliquant le cycle $(i_2, i_3, i_4) \in G$ aux deux membres de cette égalité, on obtient

$$\alpha_{i_1}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_4} + \alpha_{i_4}\alpha_{i_1} + \alpha_{i_2}^2 + \sum_{j \notin \{i_1,i_2,i_3,i_4\}} \alpha_j^2 = T_2. \tag{4.11}$$

Par soustraction de (4.10) et (4.11), il vient

$$\alpha_{i_1}(\alpha_{i_2} - \alpha_{i_4}) + \alpha_{i_3}(\alpha_{i_2} - \alpha_{i_4}) + \alpha_{i_4}^2 - \alpha_{i_2}^2 = 0.$$

On a $\alpha_{i_2} \neq \alpha_{i_4}$, d'où

$$\alpha_{i_1} + \alpha_{i_3} = \alpha_{i_2} + \alpha_{i_4}.$$

En appliquant le 3-cycle (i_1, i_2, i_3) aux deux membres de cette égalité, on obtient

$$\alpha_{i_2} + \alpha_{i_1} = \alpha_{i_3} + \alpha_{i_4},$$

puis $\alpha_{i_3} - \alpha_{i_2} = \alpha_{i_2} - \alpha_{i_3}$, d'où $\alpha_{i_2} = \alpha_{i_3}$ et une contradiction.

Étape 2. Supposons que σ soit un produit de au moins deux 3-cycles à supports disjoints

$$(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}) \quad \text{et} \quad (\alpha_{i_4}, \alpha_{i_5}, \alpha_{i_6}).$$

On a donc une expression de la forme

$$\alpha_{i_1}\alpha_{i_2} + \alpha_{i_2}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_1} + \alpha_{i_4}\alpha_{i_5} + \alpha_{i_5}\alpha_{i_6} + \alpha_{i_6}\alpha_{i_4} + P(\dots, \alpha_j, \dots) = T_2, \tag{4.12}$$

où P est un polynôme homogène de degré 2 en les α_j, $j \notin \{i_1, i_2, i_3, i_4, i_5, i_6\}$. En appliquant le 3-cycle $(i_2, i_3, i_4) \in G$ aux deux membres de (4.12), on obtient

$$\alpha_{i_1}\alpha_{i_3} + \alpha_{i_3}\alpha_{i_4} + \alpha_{i_4}\alpha_{i_1} + \alpha_{i_2}\alpha_{i_5} + \alpha_{i_5}\alpha_{i_6} + \alpha_{i_6}\alpha_{i_2} + P(\dots, \alpha_j, \dots) = T_2. \tag{4.13}$$

Par soustraction de (4.12) et (4.13), on a donc

$$\alpha_{i_1}(\alpha_{i_2} - \alpha_{i_4}) + \alpha_{i_3}(\alpha_{i_2} - \alpha_{i_4}) + \alpha_{i_5}(\alpha_{i_4} - \alpha_{i_2}) + \alpha_{i_6}(\alpha_{i_4} - \alpha_{i_2}) = 0.$$

On a $\alpha_{i_2} \neq \alpha_{i_4}$, d'où

$$\alpha_{i_1} + \alpha_{i_3} = \alpha_{i_5} + \alpha_{i_6}.$$

En appliquant le 3-cycle (i_1, i_2, i_3) aux deux membres, il vient

$$\alpha_{i_2} + \alpha_{i_1} = \alpha_{i_5} + \alpha_{i_6},$$

d'où $\alpha_{i_3} = \alpha_{i_2}$. On a ainsi une contradiction et le résultat. □

Cela termine la démonstration du théorème 2.4.

5. Démonstration de la proposition 2.6

Soient $\mathcal{C}$ une classe de conjugaison non triviale de G qui n'est pas formée d'éléments d'ordre 2 et $\mathcal{C}'$ la classe de conjugaison formée des inverses des éléments de $\mathcal{C}$.

Supposons $\mathcal{C} = \mathcal{C}'$. Pour tout $\sigma \in G$, $\sigma \neq 1$, on a

$$c(\sigma) = c\left(\sigma^{-1}\right). \tag{5.1}$$

D'après l'hypothèse faite, pour tout $\sigma \in \mathcal{C}$ on a $\sigma \neq \sigma^{-1}$. Soit X un système de représentants des paires $\{\sigma, \sigma^{-1}\}$ lorsque σ parcourt $\mathcal{C}$ i.e. X est une partie de $\mathcal{C}$ contenant exactement un élément des paires $\{\sigma, \sigma^{-1}\}$ pour $\sigma \in \mathcal{C}$. Posons

$$x = \prod_{s \in X} c(s).$$

D'après l'égalité (5.1), le produit des $c(s)$ pour $s \in X$ ne dépend pas du système de représentants X choisi et on a

$$B_{\mathcal{C}} = x^2. \tag{5.2}$$

Par ailleurs, soit τ un élément de G. Pour tout $s \in X$, on a $\tau\left(c(s)\right) = c\left(\tau s \tau^{-1}\right)$. De plus, quand s parcourt X, $\tau s \tau^{-1}$ parcourt un autre système de représentants. On a donc $\tau(x) = x$, par suite x est dans O_K, d'où la première assertion.

En ce qui concerne la seconde assertion, en posant $\mathcal{C} = \{s_1, \ldots, s_r\}$, on a $\mathcal{C}' = \{s_1^{-1}, \ldots, s_r^{-1}\}$. Les égalités (2.6) et (5.1) impliquent alors le résultat.

6. Démonstration du théorème 2.8

Soit $\mathcal{S}$ une classe de conjugaison non triviale de $\mathfrak{S}_k$.

Lemme 6.1. *Le polynôme $F_{\mathcal{S}}$ est invariant sous l'action de $\mathfrak{S}_k$*

Démonstration. Elle est analogue à celle du lemme 2.1. En effet, soit $\tau \in \mathfrak{S}_k$. D'après (2.9), on a les égalités

$$\tau.F_{\mathcal{S}} = \prod_{t \in \mathcal{S}} \left(\sum_{i=1}^{k} X_{\tau(i)} X_{\tau t(i)} - N_2 \right) = \prod_{t \in \mathcal{S}} \left(\sum_{j=1}^{k} X_j X_{\tau t \tau^{-1}(j)} - N_2 \right).$$

L'application de $\mathcal{S}$ dans $\mathcal{S}$ qui à t associe $\tau t \tau^{-1}$ étant une bijection, on a donc $\tau.F_{\mathcal{S}} = F_{\mathcal{S}}$. □

Rappelons que l'on a

$$F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) = \prod_{\sigma \in \mathcal{S}} \left(\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} - T_2 \right). \tag{6.1}$$

Comme conséquence directe du lemme 6.1, on en déduit l'énoncé qui suit i.e. la condition (2.10).

Corollaire 6.2. *L'élément $F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k)$ est dans O_K.*

Lemme 6.3. *Soit $\mathcal{S}_0$ la classe de conjugaison des transpositions de $\mathfrak{S}_k$. On a*

$$F_{\mathcal{S}_0}(\alpha_1, \ldots, \alpha_k) = (-1)^{\frac{k(k-1)}{2}} \Delta_f. \tag{6.2}$$

Démonstration. Il y a $k(k-1)/2$ transpositions dans $\mathfrak{S}_k$ et on a (cf. (4.3))

$$F_{\mathcal{S}_0}(\alpha_1, \ldots, \alpha_k) = (-1)^{\frac{k(k-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{k(k-1)}{2}} \Delta_f. \qquad \square$$

Le théorème 2.8 se déduit comme suit. D'après l'égalité (6.1), on a

$$\prod_{\mathcal{S}} F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k) = \prod_{\sigma \in \mathfrak{S}_k, \sigma \neq 1} \left(\sum_{i=1}^{k} \alpha_i \alpha_{\sigma(i)} - T_2 \right).$$

On déduit alors de (2.6)-(2.8) et du corollaire 6.2 que B_f divise dans O_K le produit des $F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k)$, d'où les conditions (2.11) et (2.12). Le théorème 2.2 et le lemme 6.3 entraînent alors le résultat.

7. Les éléments $F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k)$ pour $k \in \{3, 4\}$

Pour toute classe de conjugaison non triviale $\mathcal{S}$ de $\mathfrak{S}_k$, posons par commodité

$$R_{\mathcal{S}} = F_{\mathcal{S}}(\alpha_1, \ldots, \alpha_k). \tag{7.1}$$

Si $\mathcal{S}_0$ est la classe de conjugaison des transpositions, le lemme 6.3 permet de déterminer simplement $R_{\mathcal{S}_0}$. Dans le cas où $k \in \{3, 4\}$ et $\mathcal{S} \neq \mathcal{S}_0$, on exprime ci-dessous $R_{\mathcal{S}}$ en un polynôme des fonctions symétriques élémentaires $e_1, \ldots, e_k$ des racines α_i de f,

$$e_1 = \sum_{i=1}^{k} \alpha_i, \quad e_2 = \sum_{i<j} \alpha_i \alpha_j, \quad \ldots \ .$$

7.1. Cas où $k = 3$. Soit $\mathcal{S}_1$ la classe des 3-cycles de $\mathfrak{S}_3$. On a les égalités

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 - T_2 = \alpha_1\alpha_3 + \alpha_2\alpha_1 + \alpha_3\alpha_2 - T_2 = -e_1^2 + 3e_2,$$

d'où

$$R_{\mathcal{S}_1} = (e_1^2 - 3e_2)^2. \tag{7.2}$$

7.2. Cas où $k = 4$. On vérifie avec `Magma` les égalités suivantes.

Soit $\mathcal{S}_1$ la classe des doubles transpositions de $\mathfrak{S}_4$. On a

$$R_{\mathcal{S}_1} = -e_1^6 + 8e_1^4e_2 - 4e_1^3e_3 - 20e_1^2e_2^2 + 24e_1^2e_4 + 8e_1e_2e_3 + 16e_2^3 - 64e_2e_4 + 8e_3^2. \tag{7.3}$$

Soit $\mathcal{S}_2$ la classe des 3-cycles. En posant

$$g = 3e_3e_1^5 - (e_2^2 + 3e_4)e_1^4 - 19e_3e_2e_1^3 + (6e_2^3 + 16e_4e_2 + 8e_3^2)e_1^2 + (30e_3e_2^2 + 8e_3e_4)e_1 - 9e_2^4 - 24e_4e_2^2 - 24e_3^2e_2 - 16e_4^2,$$

on a

$$R_{\mathcal{S}_2} = g^2. \tag{7.4}$$

Soit $\mathcal{S}_3$ la classe des 4-cycles. On a

$$R_{\mathcal{S}_3} = (e_1^6 - 8e_1^4e_2 + e_1^3e_3 + 21e_1^2e_2^2 - 3e_1^2e_4 - 3e_1e_2e_3 - 18e_2^3 + 8e_2e_4 + e_3^2)^2. \tag{7.5}$$

8. Démonstrations des propositions 2.9, 2.10, 2.11, 2.13 et 2.14

Reprenons sans autre précision les notations du paragraphe 7.

8.1. La proposition 2.9.

(1). Supposons $k = 2$. On a $e_1 = a_1$ et $e_2 = -a_0$, d'où

$$T_2 = \alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = e_1^2 - 2e_2 = a_1^2 + 2a_0.$$

Par ailleurs, on a

$$B_f = 2\alpha_1\alpha_2 - T_2 = -(\alpha_1 - \alpha_2)^2 = -\Delta_f,$$

d'où l'assertion (théorème 2.2).

(2). Supposons $k = 3$. On a $e_1 = a_2$, $e_2 = -a_1$ et $e_3 = a_0$. On a donc

$$T_2 = a_2^2 + 2a_1.$$

D'après le lemme 6.3 et l'égalité (7.2), on obtient

$$R_{\mathcal{S}_0}R_{\mathcal{S}_1} = -\Delta_f(a_2^2 + 3a_1)^2.$$

Le théorème 2.8 entraîne alors l'assertion. □

8.2. La proposition 2.10.

On a

$$e_1 = e_2 = 0 \quad e_3 = a_1, \quad e_4 = -a_0 \quad \text{et} \quad T_2 = 0.$$

D'après le lemme 6.3 et les égalités (7.3)–(7.5), on a

$$R_{\mathcal{S}_0}R_{\mathcal{S}_1}R_{\mathcal{S}_2}R_{\mathcal{S}_3} = 2^{11}\Delta_f e_3^6 e_4^4,$$

d'où le résultat (théorème 2.8).

8.3. La proposition 2.11. Posons $A = \mathbb{Z}[X]/(p, f)$. C'est un $\mathbb{F}_p$-espace vectoriel de dimension k. Notons $\mathrm{Tr}_{A/\mathbb{F}_p}$ la forme trace. On utilisera à de nombreuses reprises l'équivalence (1.2) ainsi que l'égalité

$$\mathrm{Tr}_{A/\mathbb{F}_p}\left(x^{p+1}\right) = T_{p+1} + p\mathbb{Z}. \tag{8.1}$$

Rappelons que pour chaque exemple considéré dans l'énoncé de cette proposition, on a $G = \mathfrak{S}_k$. Par ailleurs, on a $T_2 = 0$.

(1). On a $\Delta_f = 19.151$. En déterminant une approximation numérique des racines de f, on vérifie que l'on a

$$B_f = -2^4.5^{19}.7^2.19.151.467^2.761^2.2477.$$

Si $p \in \{19, 151\}$, f n'est pas séparable modulo p, donc $N_p(f) \neq 5$. On a $T_{20} = 9$ et en utilisant l'égalité (8.1), on vérifie que $T_{152} \equiv 74 \pmod{151}$. L'équivalence annoncée est donc vraie dans ce cas.

Soit p un diviseur premier de B_f distinct de $2, 5, 19, 151$. En utilisant l'équivalence (1.2), on constate que l'on a $N_p(f) \neq 5$. On a aussi $T_8 = 4$, $T_{468} \equiv 250 \pmod{467}$, $T_{762} \equiv 355 \pmod{761}$ et $T_{2478} \equiv 695 \pmod{2477}$. En particulier, on a $T_{p+1} \not\equiv 0 \pmod{p}$, d'où le résultat (théorème 2.2).

On notera que l'on a $T_3 = T_6 = 0$ et $N_2(f) = N_5(f) = 0$, donc les nombres premiers 2 et 5 doivent être exclus.

(2). On a $\Delta_f = 67.743$. La démarche utilisée pour démontrer la première assertion permet à nouveau de conclure. En déterminant une approximation numérique des racines de f, on vérifie que la décomposition de B_f en produit de nombres premiers est donnée par l'égalité

$$\begin{aligned} B_f = 2^{72}.3^4.7^2.13^2.41^2.47^5.67.79^3.281^2.347^2.743.1151^4.1283^2.1319^2 \\ .1663^2.951697.1395487^2.6367393^2.17122219.136254761^2 \\ .57785936129^2.123530989187^2.885187290897569369^2. \end{aligned}$$

En appliquant l'équivalence (1.2) et l'égalité (8.1) avec chaque diviseur premier de B_f, on obtient le résultat annoncé.

(3). On a $\Delta_f = -776887$. Dans ce cas, en procédant comme ci-dessus, on constate que l'entier B_f possède 1723 chiffres décimaux et nous ne sommes pas parvenus à le factoriser directement. Afin d'obtenir cette factorisation, on a utilisé l'égalité (2.8). Pour chaque classe de conjugaison $\mathcal{S}$ de $\mathfrak{S}_7$, on a donc explicité l'entier $B_{\mathcal{S}}$. Pour chaque classe $\mathcal{S}$, on adopte la notation $B_{\mathcal{S}} = B_v$, dans laquelle $v = [\ell_1, \ldots, \ell_t]$ est un vecteur dont les composantes sont les longueurs des cycles intervenant dans la décomposition des éléments

de $\mathcal{S}$ en produit de cycles à supports disjoints. On obtient les résultats suivants :

$$B_{[7]} = \left(2^{25}.\ 7^{66}.\ 109625712257228705413093659048732974 27\right)^2,$$

$$B_{[1,6]} = \left(7^{63}.\ 5087.\ 615078503681.\ p.q\right)^2,$$

où

$$p = 23153222992271849404101 17,$$

$$q = 10318066303272996732213608045791326901482896 4041,$$

$$B_{[2,5]} = (3^3.\ 7^{42}.544012054068222545343624664 07.\ 12465343146107543637577772425 93)^2,$$

$$B_{[3,4]} = \left(31.\ 584352520781031924793770439 61\right)^4,$$

$$B_{[1,1,5]} = (3.\ 7^{21}.\ 107.\ 109622861.\ 314517883.\ 87453951749.\ 96257721299.\ 473705767399763)^2,$$

$$B_{[1,2,4]} = \left(2^{21}.\ 7^{42}.\ 29^2.\ 107.\ 15961129.\ 24534049.\ 198331229.\ 671794760853523.\ p.q\right)^2,$$

où $\quad p = 93177762039493501, \quad q = 109006671100672702120494325 31,$

$$B_{[1,3,3]} = \left(2^{28}.\ 7^7.\ 1085687\right)^4,$$

$$B_{[2,2,3]} = \left(31.\ 13132283.\ 161620073077054859.\ 183574845951173009\right)^2,$$

$$B_{[1,1,1,4]} = \left(4936189.\ 725938918439654319174389\right)^2,$$

$$B_{[1,1,2,3]} = \left(7^{42}.\ 32717.\ 43670581.\ 406364687865676005970873636906651 7857\right)^2,$$

$$B_{[1,2,2,2]} = -7^{21}.\ 761.\ 7679513.\ 25839993284328785428639,$$

$$B_{[1,1,1,1,3]} = 7^{28},$$

$$B_{[1,1,1,2,2]} = -2^{21}.\ 17.\ 191.\ 5087.\ 15031.\ 28627874657408393618159298227,$$

$$B_{[1,1,1,1,1,2]} = 776887.$$

Pour $p = 776887$, qui est au signe près le discriminant de f, on a $T_{p+1} \equiv 115287 \pmod{p}$. En ce qui concerne les autres diviseurs premiers des $B_{[v]}$, l'équivalence (1.2) et l'égalité (8.1) permettent alors d'obtenir le résultat.

Notons que pour $p = 15961129$, on a $N_p(f) = 1$ et $T_{p+1} \equiv 0 \pmod{p}$, donc ce nombre premier est à exclure. Par ailleurs, on constate que, conformément à la proposition 2.6, les entiers $B_{\mathcal{S}}$ pour lesquels $\mathcal{S}$ n'est pas formée d'éléments d'ordre 2 sont des carrés. Cela termine la démonstration de la proposition 2.11.

8.4. La proposition 2.13. On a $\Delta_f = 47^2$ et $T_2 = 0$, f est irréductible sur $\mathbb{Q}$ et $\mathrm{Gal}(f)$ est diédral d'ordre 10 (cf. [5]). On vérifie que l'on a

$$\prod_{\mathcal{S}} F_{\mathcal{S}}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = -3^2.5^{10}.11^4.13^4.19^2.23^3.41^2.47^3.281^2,$$

où $\mathcal{S}$ parcourt l'ensemble des classes de conjugaison non triviales de $\mathfrak{S}_5$. D'après la condition (2.11) l'ensemble des diviseurs premiers de B_f est donc contenu dans

$$\{3, 5, 11, 13, 19, 23, 41, 47, 281\}.$$

Le théorème 2.8 entraîne alors le résultat.

8.5. La proposition 2.14. On a

$$\Delta_f = 18441\alpha^2 - 621100\alpha + 1031256.$$

Il y a deux idéaux premiers dans O_K au-dessus de 5 et on a la factorisation $5O_K = \mathfrak{p}_5\mathfrak{q}_5$, où le degré résiduel de $\mathfrak{p}_5$ vaut 1 et où celui de $\mathfrak{q}_5$ vaut 2. De plus, on a $\mathfrak{p}_5 = (u)$. Il en résulte que f est un polynôme d'Eisenstein en l'idéal $\mathfrak{p}_5$. En particulier, f est irréductible sur K.

Par ailleurs, 13 est inerte dans K et f se décompose en deux facteurs irréductibles de degré 2 et 3 modulo $13O_K$. Il en résulte que $\mathrm{Gal}(f)$ contient une transposition. Le polynôme f étant irréductible sur K, $\mathrm{Gal}(f)$ contient un 5-cycle. On en déduit que $\mathrm{Gal}(f) = \mathfrak{S}_5$.

Pour chaque classe de conjugaison $\mathcal{S}$ de $\mathfrak{S}_5$, on note, comme dans l'alinéa 3 ci-dessus, $B_{\mathcal{S}} = B_v$, où $v = [\ell_1, \ldots, \ell_t]$ est un vecteur indiquant les longueurs des cycles intervenant dans la décomposition des éléments de $\mathcal{S}$ en produit de cycles à supports disjoints. On obtient les résultats suivants :

$$B_{[5]} = (-413075\alpha^2 + 640600\alpha - 39900)^2,$$
$$B_{[1,4]} = (48990625\alpha^2 - 38715625\alpha - 41359375)^2,$$
$$B_{[2,3]} = (16516\alpha^2 - 187975\alpha + 309206)^2,$$
$$B_{[1,1,3]} = (-14041\alpha^2 - 368900\alpha + 619144)^2,$$
$$B_{[1,2,2]} = 31472487500\alpha^2 - 24902178125\alpha - 26712984375,$$
$$B_{[1,1,1,2]} = \Delta_f.$$

Notons $\mathrm{N}_{K/\mathbb{Q}}(B_v)$ la norme de K sur $\mathbb{Q}$ de B_v. On vérifie que l'on a

$$\mathrm{N}_{K/\mathbb{Q}}(B_{[5]}) = 5^{24}, \quad \mathrm{N}_{K/\mathbb{Q}}(B_{[1,4]}) = -5^{32},$$
$$\mathrm{N}_{K/\mathbb{Q}}(B_{[2,3]}) = 5^9.181.307.167449, \quad \mathrm{N}_{K/\mathbb{Q}}(B_{[1,1,3]}) = 5^9.2707.15639581,$$
$$\mathrm{N}_{K/\mathbb{Q}}(B_{[1,2,2]}) = -5^{26}.61.70956089917,$$
$$\mathrm{N}_{K/\mathbb{Q}}(\Delta_f) = 5^9.23.367.1613.20101.$$

Pour chacun des idéaux premiers de O_K divisant les B_v, il s'agit alors de vérifier s'ils satisfont ou non l'équivalence (2.15). D'après les égalités précédentes, mis à part les idéaux premiers $\mathfrak{p}_5$ et $\mathfrak{q}_5$ au-dessus de 5, ils sont tous de degré résiduel 1.

En ce qui concerne $\mathfrak{p}_5$ et $\mathfrak{q}_5$, on a $\mathrm{N}(\mathfrak{p}_5) = 5$ et $\mathrm{N}(\mathfrak{q}_5) = 25$. On constate que $T_6 = 0$ et que T_{26} appartient à $\mathfrak{q}_5$. Par ailleurs, on a $\alpha \equiv 2 \pmod{\mathfrak{p}_5}$, d'où $u \in \mathfrak{p}_5$ et f modulo $\mathfrak{p}_5$ est X^5. On a donc $N_{\mathfrak{p}_5}(f) = 1$ et $\mathfrak{p}_5$ est à exclure. On a $u \equiv 3\alpha \pmod{\mathfrak{q}_5}$ donc f modulo $\mathfrak{q}_5$ est $X^5 + (7\alpha+2)X + 3\alpha$. On vérifie alors que l'on a $N_{\mathfrak{q}_5}(f) = 5$, ainsi $\mathfrak{q}_5$ n'est pas à exclure.

Examinons l'équivalence (2.15) pour les autres idéaux premiers de O_K qui divisent $B_{[2,3]}$. Il existe un unique idéal premier $\mathfrak{p}$ de O_K de degré 1 au-dessus de 181. On a $\alpha \equiv 30 \pmod{\mathfrak{p}}$, d'où l'on déduit que $T_{182} \equiv 57 \pmod{\mathfrak{p}}$ et $N_{\mathfrak{p}}(f) = 3$, donc $\mathfrak{p}$ n'est pas à exclure. Par ailleurs, il y a trois idéaux premiers de degré 1 au-dessus de 307 et un seul divise $B_{[2,3]}$. Notons-le $\mathfrak{q}$. On a $\alpha \equiv 100 \pmod{\mathfrak{q}}$, d'où $T_{308} \equiv 255 \pmod{\mathfrak{q}}$ et $N_{\mathfrak{q}}(f) = 1$, ainsi $\mathfrak{q}$ n'est pas à exclure. De même, il y a trois idéaux premiers de degré 1 au-dessus de 167449. En notant $\mathfrak{q}$ celui qui divise $B_{[2,3]}$, on a $\alpha \equiv 30636 \pmod{\mathfrak{q}}$, d'où $T_{167450} \equiv 51379 \pmod{\mathfrak{q}}$, $N_{\mathfrak{q}}(f) = 2$ et la même conclusion. Les autres diviseurs premiers des B_v se traîtent de façon analogue.

Pour l'unique idéal premier $\mathfrak{p}_{61}$ de O_K de degré 1 au-dessus de 61, on a $\alpha \equiv 57 \pmod{\mathfrak{p}_{61}}$, d'où $T_{62} \in \mathfrak{p}_{61}$ et $N_{\mathfrak{p}_{61}}(f) = 1$, donc $\mathfrak{p}_{61}$ ne satisfait pas l'équivalence (2.15), d'où le résultat.

9. Remarque sur les idéaux premiers principaux d'un corps de nombres

Considérons un corps de nombres K. Les idéaux premiers non nuls de O_K qui sont principaux sont exactement ceux qui sont totalement décomposés dans le corps de classes de Hilbert H_K de K ([6, (8.5) Corollary, p. 107]). Connaissant H_K, les résultats précédent permettent donc d'obtenir un critère caractérisant les idéaux premiers principaux de O_K.

Soit $f \in O_K[X]$ le polynôme minimal d'un élément primitif entier de l'extension H_K/K. Soit $(T_n)_{n\in\mathbb{N}}$ la suite d'éléments de O_K associée à f par l'égalité (2.1).

On se limitera ici à expliciter deux exemples illustrant cette situation.

Exemple 9.1. Prenons $K = \mathbb{Q}\left(\sqrt{-5}\right)$ dont le nombre de classes vaut 2. On a $H_K = K\left(\sqrt{-1}\right)$, d'où $f = X^2 + 1$ et $\Delta_f = -20$. Il en résulte que pour tout idéal premier $\mathfrak{p}$ de O_K, on a $N_{\mathfrak{p}}(f) = 2$ si et seulement si $\mathfrak{p}$ est principal (*loc. cit.* et [2, Proposition 2.3.9]). Par suite,

$$\mathfrak{p} \text{ est principal } \Leftrightarrow \mathrm{N}(\mathfrak{p}) \equiv 1 \pmod 4. \tag{9.1}$$

On peut retrouver ce fait en remarquant que la suite $(T_n)_{n\in\mathbb{N}}$ associée à f est définie par $T_n = 2$ si $n \equiv 0 \pmod 4$, $T_n = -2$ si $n \equiv 2 \pmod 4$, $T_n = 0$ si $n \equiv 1 \pmod 2$. D'après la proposition 2.9, pour tout idéal premier $\mathfrak{p}$ de O_K, on a donc $N_{\mathfrak{p}}(f) = 2$ si et seulement si $\mathrm{N}(\mathfrak{p}) \equiv 1 \pmod 4$, d'où l'équivalence (9.1).

Exemple 9.2. Prenons $K = \mathbb{Q}(\beta)$ avec $\beta^4 + 7\beta^2 - 2\beta + 14 = 0$. Le groupe de Galois sur $\mathbb{Q}$ de la clôture galoisienne de K est $\mathfrak{A}_4$. Le groupe des classes de K est cyclique d'ordre 4 i.e. on a $\mathrm{Gal}\,(H_K/K) = \mathbb{Z}/4\mathbb{Z}$. En utilisant `Magma`, on constate que le polynôme $f = X^4 - (\beta^2 + 3)X^2 - 1$ convient. La suite $(T_n)_{n\in\mathbb{N}}$ associée à f est définie par les égalités $T_0 = 4$, $T_1 = 0$, $T_2 = 2(\beta^2 + 3)$, $T_3 = 0$, $T_{n+4} = (\beta^2 + 3)T_{n+2} + T_n$ pour tout $n \in \mathbb{N}$.

Lemme 9.3. *Soit $\mathfrak{p}$ un idéal premier de O_K de caractéristique résiduelle impaire. Alors,*

$$\mathfrak{p} \textit{ est principal } \Leftrightarrow T_{\mathrm{N}(\mathfrak{p})+1} \equiv 2(\beta^2 + 3) \pmod{\mathfrak{p}}. \tag{9.2}$$

Démonstration. Il y a deux idéaux premiers $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de O_K au-dessus de 2, chacun d'indice de ramification 2, et deux idéaux premiers de O_K au-dessus de 5 dont un seul $\mathfrak{p}_5$ est de degré résiduel 1. On vérifie que l'on a

$$\Delta_f O_K = \mathfrak{p}_1^8 \mathfrak{p}_2^{16} \mathfrak{p}_5^4. \tag{9.3}$$

Par ailleurs, on a

$$e_1 = 0, \quad e_2 = \beta^2 + 3, \quad e_3 = 0, \quad e_4 = -1.$$

Les seuls éléments d'ordre 4 de $\mathfrak{S}_4$ sont les 4-cycles. On déduit alors du théorème 2.8 que B_f divise l'entier $R_{\mathcal{S}_3}$ défini par l'égalité (7.5). On a

$$R_{\mathcal{S}_3} = 4e_2^2(9e_2^2 + 4)^2 = -9\beta^2 + 18\beta - 41.$$

On constate que l'on a

$$(-9\beta^2 + 18\beta - 41)O_K = \mathfrak{p}_2^4 \mathfrak{q},$$

où $\mathfrak{q}$ est l'idéal premier de O_K au-dessus de 80233 de degré résiduel 1. D'après le théorème 2.2, pour tout idéal premier $\mathfrak{p}$ de O_K, distinct de $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_5$ et $\mathfrak{q}$, l'équivalence (9.2) est satisfaite.

Les idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2$ ne sont pas principaux. On a les égalités $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = 2$ et $T_3 = 0$, donc pour ces deux idéaux $\mathfrak{p}_i$ on a $T_{\mathrm{N}(\mathfrak{p}_i)+1} \equiv 2(\beta^2+3) \pmod{\mathfrak{p}_i}$. L'idéal $\mathfrak{p}_5$ n'est pas principal et on a $T_6 \not\equiv 2(\beta^2 + 3) \pmod{\mathfrak{p}_5}$.

Par ailleurs, $\mathfrak{q}$ est principal et on a $T_{\mathrm{N}(\mathfrak{q})+1} \equiv 2(\beta^2+3) \pmod{\mathfrak{q}}$, d'où le résultat. □

Remarque 9.4. Par exemple, l'idéal premier $\mathfrak{p}_{13}$ de O_K au-dessus de 13 de degré 1 est principal, on a $\mathfrak{p}_{13} = (\beta^3/2 - \beta^2/2 + 2\beta - 4)$ et on vérifie que l'on a $v_{\mathfrak{p}_{13}}\left(T_{14} - 2(\beta^2+3)\right) = 1$. C'est l'idéal premier de O_K de plus petite norme qui soit principal.

Bibliographie

[1] W. Bosma, J. Cannon & C. Playoust, « The Magma Algebra System I : The User Language », *J. Symb. Comput.* **24** (1997), n° 3-4, p. 235-265, voir aussi `http://magma.maths.usyd.edu.au/magma/`.

[2] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer, 2000.

[3] C. S. Dalawat, *Splitting primes*, CRC Press, 2012.

[4] T. Dokchitser & V. Dokchitser, « Identifying Frobenius elements in Galois groups », *Algebra Number Theory* **7** (2013), n° 6, p. 1325-1352.

[5] The LMFDB Collaboration, « The L-functions and Modular Forms Database », 2013, `http://www.lmfdb.org`.

[6] J. Neukirch, *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften, vol. 280, Springer, 1986.

[7] The PARI Group, « PARI/GP version `2.12.1` », 2019, available from `http://pari.math.u-bordeaux.fr/`.

[8] J. Rosen, « A finite analogue of the ring of algebraic numbers », *J. Number Theory* **208** (2020), p. 59-71.

[9] E. S. Selmer, « On the irreducibility of certain trinomials », *Math. Scand.* **4** (1956), p. 287-302.

[10] J. Weinstein, « Reciprocity laws and Galois representations : recent breakthroughs », *Bull. Am. Math. Soc.* **53** (2016), n° 1, p. 1-39.

[11] B. F. Wyman, « What is a Reciprocity Law ? », *Am. Math. Mon.* **79** (1972), p. 571-586, correction in *ibid.* **80** (1973), p. 281.

Dominique Bernardi
Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche
UMR 7586 CNRS - Paris Diderot,
4 Place Jussieu,
75005 Paris, France
E-mail: `dominique.bernardi@imj-prg.fr`

Alain Kraus
Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche
UMR 7586 CNRS - Paris Diderot,
4 Place Jussieu,
75005 Paris, France
E-mail: `alain.kraus@imj-prg.fr`